Finite Fields and Their Applications 46 (2017) 280–303

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Existence of some special primitive normal elements over finite fields

Anju *, R.K. Sharma

Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, 110016, India

A R T I C L E I N F O

Article history:
Received 29 December 2016
Received in revised form 7 April 2017
Accepted 10 April 2017
Available online 28 April 2017
Communicated by D. Panario

MSC:
12E20
11T23

Keywords:
Finite field
Character
Normal element
Primitive element

A B S T R A C T

In this article, we establish a sufficient condition for the existence of a primitive element $\alpha \in \mathbb{F}_q$ such that for any matrix $\begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_q)$ of rank 2, the element $(a\alpha^2 + b\alpha + c)/(d\alpha + e)$ is a primitive element of $\mathbb{F}_q$, where $q = 2^k$ for some positive integer k. We also give a sufficient condition for the existence of a primitive normal element $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that $(a\alpha^2+b\alpha+c)/(d\alpha+e)$ is a primitive element of $\mathbb{F}_{q^n}$ for every matrix $\begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_{q^n})$ of rank 2.

1. Introduction

Throughout the paper, $\mathbb{F}_q$ denotes a finite field of order $q = p^k$, for some prime p and some positive integer k, and $\mathbb{F}_{q^n}$ denotes an extension of $\mathbb{F}_q$ of degree n. A generator of the cyclic multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is known as a *primitive element* of $\mathbb{F}_q$. Any

* Corresponding author.
E-mail addresses: anjugju@gmail.com (Anju), rksharmaiitd@gmail.com (R.K. Sharma).

http://dx.doi.org/10.1016/j.ffa.2017.04.004

field $\mathbb{F}_q$ has $\phi(q-1)$ primitive elements, where ϕ is the Euler's phi-function. A basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is called a *normal basis*, and α is called a *normal element* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. If, in addition, α is also a primitive element of $\mathbb{F}_{q^n}$, then the basis is said to be a *primitive normal basis*. Normal bases are of great importance in coding theory, cryptography, signal processing, etc. [1,18,19]. It is well known [17, Theorem 2.35], that $\mathbb{F}_{q^n}$ has a normal element over $\mathbb{F}_q$ for every q and n. Basic results on normal bases over finite fields can be found in [2].

Existence of primitive normal elements has become an active area of research because of applications in coding theory, cryptography, etc. In [3,4], Carlitz showed that for sufficiently large q^n, the field $\mathbb{F}_{q^n}$ contains a primitive element that generates a primitive normal basis over $\mathbb{F}_q$. Davenport [11] proved the existence of a primitive normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ when q is a prime. Lenstra and Schoof [15] completely resolved the question of the existence of primitive normal elements for all field extensions $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Cohen and Huczynska [9] gave the first computer-free proof of the result of Lenstra and Schoof.

In general, for any primitive element $\alpha \in \mathbb{F}_q$, $f(\alpha)$ (where f is any rational function) need not be primitive in $\mathbb{F}_q$, for example, if we take the polynomial function $f(x) = x+1$ over the field $\mathbb{F}_2$ of order 2 then 1 is the only primitive element of $\mathbb{F}_2$, but $f(1) = 0$, which is not primitive. But for $f(x) = \frac{1}{x}$, $f(\alpha)$ is primitive in $\mathbb{F}_q$ whenever α is primitive. We call $(\alpha, f(\alpha))$ a *primitive pair* if both α and $f(\alpha)$ are primitive. Many researchers have worked in this direction. In 1985, Cohen [7] showed that a finite field $\mathbb{F}_q$, with $q > 3$, $q \not\equiv 7(mod\ 12)$ and $q \not\equiv 1(mod\ 60)$ contains two consecutive primitive elements. Tian and Qi [20] showed the existence of a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that both α and α^{-1} are normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, when $n \geq 32$. Later, Cohen and Huczynska [10] proved that for any prime power q and any integer $n \geq 2$, there exists an element $\alpha \in \mathbb{F}_{q^n}$ such that both α and α^{-1} are primitive normal over $\mathbb{F}_q$ except when (q, n) is one of the pairs $(2, 3)$, $(2, 4)$, $(3, 4)$, $(4, 3)$, $(5, 4)$. Chou and Cohen [6] completely resolved the question whether there exists a primitive element α such that α and α^{-1} both have trace zero over $\mathbb{F}_q$. In 2014, Kapetanakis [14] extended the result of Cohen and Huczynska [10] by proving the existence of a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that both α and $(a\alpha + b)/(c\alpha + d)$ produce a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, for every q, n, with a few exceptions, and for every a, b, c, $d \in \mathbb{F}_q$. He and Han [12] studied primitive elements of the form $\alpha + \alpha^{-1}$ over finite fields. In 2012, Wang et al. [21] gave a sufficient condition for the existence of α such that α and $\alpha + \alpha^{-1}$ are both primitive, and also a sufficient condition for the existence of a normal element α such that α and $\alpha + \alpha^{-1}$ are both primitive for the case $2|q$. Liao et al. [16] generalized their results to the case when q is any prime power. In 2014, Cohen [8] completed the existence results obtained by Wang et al. [21] for finite fields of characteristic 2. In this article, we extend results of Wang et al. and of Cohen.

Corresponding to every matrix $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_q)$, we define a rational expression $\lambda_A(x) \in \mathbb{F}_q(x)$ and a subset $\mathfrak{M}_q$ of $M_{2\times 3}(\mathbb{F}_q)$ given by

$$\lambda_A(x) = \frac{ax^2+bx+c}{dx+e},$$

and

$$\mathfrak{M}_q = \{A = [a_{ij}] \in M_{2\times 3}(\mathbb{F}_q) \mid a_{21} = 0,\ Rank(A) = 2 \text{ and } \\ \text{if } \lambda_A(x) = \beta x \text{ or } \beta x^2 \text{ for } \beta \in \mathbb{F}_q \text{ then } \beta = 1\}.$$

For each matrix $A \in \mathfrak{M}_q$, we study the existence of a primitive element $\alpha \in \mathbb{F}_q$ such that $\lambda_A(\alpha)$ is also a primitive element of $\mathbb{F}_q$ as well as for each matrix $A \in \mathfrak{M}_{q^n}$, a primitive normal element α of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that $\lambda_A(\alpha)$ is also a primitive element of $\mathbb{F}_{q^n}$. Observe that for $q = p^k$, where p is an odd prime, there exists at least one matrix $A = \begin{pmatrix} 1 & p-2 & 1 \\ 0 & 0 & 1 \end{pmatrix} \in \mathfrak{M}_q$, for which $\lambda_A(\alpha)$ can't be primitive for any $\alpha \in \mathbb{F}_q$. Hence we will consider only fields of characteristic 2. Let $\mathfrak{P}$ be the set of q' ($q' = 2^v$ for any positive integer v) such that for each $A \in \mathfrak{M}_{q'}$, $\mathbb{F}_{q'}$ contains a primitive pair $(\alpha, \lambda_A(\alpha))$, and $\mathfrak{N}$ be the set of (q', m') such that for each $A \in \mathfrak{M}_{q'^{m'}}$, $\mathbb{F}_{q'^{m'}}$ contains a primitive pair $(\alpha, \lambda_A(\alpha))$ with α normal over $\mathbb{F}_{q'}$.

In this article, we have proved the following two main results:

Theorem 1.1. *Let $q = 2^k$ for some positive integer k and $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in \mathfrak{M}_q$. Then there exists a primitive element $\alpha \in \mathbb{F}_q$ such that $\lambda_A(\alpha)$ is also primitive except for $k = 1,\ 2,\ 4$. That is, if $k \in \mathbb{N}\backslash\{1, 2, 4\}$ then $q = 2^k \in \mathfrak{P}$.*

Theorem 1.2. *Let $\mathbb{F}_{q^n}$ be an extension of $\mathbb{F}_q$ of degree $n \geq 2$, where $q = 2^k$. Also suppose that $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_q)$ is of rank 2 such that if $\lambda_A(x) = \beta x$ or βx^2 for some $\beta \in \mathbb{F}_q$ then $\beta = 1$. Then $\mathbb{F}_{q^n}$ contains a primitive pair $(\alpha, \lambda_A(\alpha))$ with α normal over $\mathbb{F}_q$ unless (q, n) is one of the pairs $(2, 2)$, $(2, 3)$, $(2, 4)$, $(2, 6)$, $(2, 8)$, $(2, 9)$, $(2, 10)$, $(2, 11)$, $(2, 12)$, $(2, 14)$, $(2, 15)$, $(2, 16)$, $(2, 18)$, $(2, 20)$, $(2, 24)$, $(4, 2)$, $(4, 3)$, $(4, 4)$, $(4, 5)$, $(4, 6)$, $(4, 7)$, $(4, 8)$, $(4, 9)$, $(4, 10)$, $(4, 12)$, $(8, 2)$, $(8, 3)$, $(8, 4)$, $(8, 7)$, $(16, 2)$, $(16, 3)$, $(16, 4)$, $(16, 5)$, $(16, 6)$, $(32, 2)$, $(64, 2)$.*

2. Preliminaries

In this section, we give some necessary definitions, preliminary notations and results which will be used in the paper. Throughout the section, q is an arbitrary prime power. For any positive integer $m > 1$, and any $g \in \mathbb{F}_q[x]$, $\omega(m)$ and $\Omega_q(g)$ are used to denote the number of prime divisors of m, and the number of monic irreducible divisors of g respectively. Also $W(m)$ and $W(g)$ denote the number of square free divisors of m and g respectively.

Definition 1. Let $e|q-1$. Then $\xi \in \mathbb{F}_q^*$ is said to be *e-free* if $\xi = \gamma^d$ for any $d|e$, and $\gamma \in \mathbb{F}_q$, implies $d = 1$. Hence an element $\alpha \in \mathbb{F}_q^*$ is primitive if and only if it is $(q-1)$-free.

For any $\beta \in \mathbb{F}_{q^n}$ and $f(x) = \sum_{i=1}^{t} f_i x^i \in \mathbb{F}_q[x]$, if we define an action of $\mathbb{F}_q[x]$ over $\mathbb{F}_{q^n}$ by

$$f \ o \ \beta = \sum_{i=1}^{t} f_i \beta^{q^i}$$

then the additive group of $\mathbb{F}_{q^n}$ becomes an $\mathbb{F}_q[x]$-module.

Definition 2. For $\beta \in \mathbb{F}_{q^n}$, the unique monic polynomial g of the least degree dividing $x^n - 1$ is said to be $\mathbb{F}_q$-*order* of β if $g \ o \ \beta = 0$, and is denoted by $Ord(\beta)$.

If $Ord(\beta)$ is g then $\beta = h \ o \ v$ for some $v \in \mathbb{F}_{q^n}$, where $h = \frac{x^n-1}{g}$.

In an analogy to the definition of an e-free element for any $e|q^n - 1$, we can also define an M-free element for any $M|x^n - 1$.

Definition 3. Let $M|x^n - 1$. Then $\beta \in \mathbb{F}_{q^n}^*$ is said to be *M-free* if for any $h|M$ and $v \in \mathbb{F}_{q^n}$, $\beta = h \ o \ v$ implies $h = 1$. Hence an element of $\mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if and only if it is $(x^n - 1)$-free.

Next, we give definition of a character of a finite abelian group and some results in this context.

Definition 4. Let G be a finite abelian group. A *character* χ of G is a homomorphism from G into the multiplicative group U of complex numbers of absolute value 1. The set of all characters of G is denoted by $\widehat{G}$, and forms a group under multiplication, which is isomorphic to G. Furthermore, the character χ_1, where $\chi_1(g) = 1$ for all $g \in G$ is the *trivial character* of G.

For a finite field $\mathbb{F}_q$, the characters of the additive group $\mathbb{F}_q$ are called *additive characters* and the characters of $\mathbb{F}_q^*$ are called *multiplicative characters.* Multiplicative characters are extended to zero using the rule,

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

Since $\widehat{\mathbb{F}_q^*} \cong \mathbb{F}_q^*$, we have that $\widehat{\mathbb{F}_q^*}$ is cyclic. Let χ_d denote a multiplicative character of order d for any $d|q-1$, which are $\phi(d)$ in number. Following Cohen and Huczynska [9,10], it can be shown that for any $m|q-1$,

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

where $\theta(m) := \frac{\phi(m)}{m}$, μ is Möbius function and the internal sum runs over all multiplicative characters χ_d of order d, gives an expression of the characteristic function for the subset of m-free elements of $\mathbb{F}_q^*$. Further, for any $\psi \in \widehat{\mathbb{F}_{q^n}}$, $f \in \mathbb{F}_q[x]$, and $\beta \in \mathbb{F}_{q^n}$, if we define an action of $\mathbb{F}_q[x]$ over $\widehat{\mathbb{F}_{q^n}}$ by

$$\psi \ o \ f(\beta) = \psi(f \ o \ \beta)$$

then $\widehat{\mathbb{F}_{q^n}}$ becomes an $\mathbb{F}_q[x]$-module.

Definition 5. $\mathbb{F}_q$-*order* of any typical additive character ψ_g of $\mathbb{F}_{q^n}$ is defined to be a unique monic polynomial g of the least degree dividing $x^n - 1$ such that $\psi_g \ o \ g$ is the trivial character in $\mathbb{F}_{q^n}$.

Further, there are $\Phi_q(g)$ characters ψ_g, where $\Phi_q(g) = |(\mathbb{F}_q[x]/g\mathbb{F}_q[x])^*|$ is the analogue of Euler's phi-function on $\mathbb{F}_q[x]$.

In an analogy to the above, for any $g|x^n - 1$, an expression of the characteristic function for the set of g-free elements in $\mathbb{F}_{q^n}$ is given by,

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

where $\Theta(g) := \frac{\Phi_q(g)}{q^{deg(g)}}$, the internal sum runs over additive characters ψ_h of $\mathbb{F}_q$-order h, and μ' is the analogue of the Möbius function, which is defined by the rule,

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

We shall need the following results for our main results.

Lemma 2.1. *[17, Theorem 5.4] If χ is any non-trivial character of a finite abelian group G, and β is a non-trivial element of G then*

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

Lemma 2.2. *[17, Theorem 5.11] Let χ be a non-trivial multiplicative character, and ψ be a non-trivial additive character of $\mathbb{F}_q$. Then*

$$|\sum_{\alpha \in \mathbb{F}_q^*} \chi(\alpha)\psi(\alpha)| = q^{1/2}.$$

Lemma 2.3. *[17, Theorem 5.41] Let χ be a multiplicative character of $\mathbb{F}_q$ of order $r > 1$, and let $f \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree such that $f(x)$ is not of the form $g(x)^r$, where $g(x) \in \mathbb{F}_q[x]$ with degree at least 1. Suppose d is the number of distinct roots of f in its splitting field over $\mathbb{F}_q$. Then for every $a \in \mathbb{F}_q$, we have*

$$|\sum_{c\in\mathbb{F}_q} \chi(af(c))| \leq (d-1)q^{1/2}.$$

Lemma 2.4. *[5] Let χ be a non-trivial multiplicative character of order r and ψ be a non-trivial additive character of $\mathbb{F}_{q^n}$. Let f, g be rational functions in $\mathbb{F}_{q^n}(x)$ such that $f \neq yh^r$, for any $y \in \mathbb{F}_{q^n}$ and $h \in \mathbb{F}_{q^n}(x)$, and $g \neq h^p - h + y$, for any $y \in \mathbb{F}_{q^n}$ and $h \in \mathbb{F}_{q^n}(x)$. Then*

$$\Big|\sum_{x\in\mathbb{F}_{q^n}\setminus S} \chi(f(x))\psi(g(x))\Big| \leq (\deg(g)_\infty + m + m' - m'' - 2)q^{n/2},$$

where S is the set of poles of f and g, $(g)_\infty$ is the pole divisor of g, m is the number of distinct zeros and finite poles of f in $\bar{\mathbb{F}}_q$ (algebraic closure of $\mathbb{F}_q$), m' is the number of distinct poles of g (including ∞) and m'' is the number of finite poles of f that are poles or zeros of g.

3. Existence of primitive pairs $(\alpha, \lambda_A(\alpha))$ in $\mathbb{F}_q$

In this section, we show the existence of primitive pairs $(\alpha, \lambda_A(\alpha))$ in $\mathbb{F}_q$, which is precisely our main result, Theorem 1.1. We begin by proving a series of results.

Let $q = 2^k$, for some positive integer k, $A \in \mathfrak{M}_q$ and e_1, $e_2 | q-1$. Let $N_A(e_1, e_2)$ be the number of $\alpha \in \mathbb{F}_q$ such that α is e_1-free and $\lambda_A(\alpha)$ is e_2-free. Hence we need to show that $N_A(q-1, q-1) > 0$.

Lemma 3.1. *Let $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in \mathfrak{M}_q$ be such that $\lambda_A(x) = x$ or x^2 and l divides $q-1$. Then $N_A(l,l) > 0$.*

Proof. Proof is obvious, hence omitted.

Lemma 3.2. *Let $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in \mathfrak{M}_q$ with $d \neq 0$ be such that $\lambda_A(x) \neq \beta x, \beta x^2$ for any $\beta \in \mathbb{F}_q$, and l_1, l_2 divide $q-1$. If $q^{1/2} > 3W(l_1)W(l_2)$ then $N_A(l_1, l_2) > 0$.*

Proof. By definition,

$$N_A(l_1, l_2) = \sum_{\alpha\neq\frac{-e}{d}} \rho_{l_1}(\alpha)\rho_{l_2}(\lambda_A(\alpha)), \tag{1}$$

where the sum runs over $\alpha \in \mathbb{F}_q$ except $\alpha = -\frac{e}{d}$. Now (1) gives

$$N_A(l_1, l_2) = \theta(l_1)\theta(l_2) \sum_{d_1|l_1,\ d_2|l_2} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\chi_{d_1}, \chi_{d_2}} \boldsymbol{\chi}_A(\chi_{d_1}, \chi_{d_2}) \tag{2}$$

where, $\boldsymbol{\chi}_A(\chi_{d_1}, \chi_{d_2}) = \sum_{\alpha \neq \frac{-e}{d}} \chi_{d_1}(\alpha)\chi_{d_2}(\lambda_A(\alpha))$. As we know that, there exist $n_i \in \{0, 1, 2, \cdots, q-2\}$ such that $\chi_{d_i}(x) = \chi_{q-1}(x^{n_i})$ for $i = 1,\ 2$. Hence

$$\begin{aligned}\boldsymbol{\chi}_A(\chi_{d_1}, \chi_{d_2}) &= \sum_{\alpha \neq \frac{e}{d}} \chi_{q-1}(\alpha^{n_1}(a\alpha^2 + b\alpha + c)^{n_2}(d\alpha + e)^{q-n_2-1}) \\ &= \sum_{\alpha \neq \frac{e}{d}} \chi_{q-1}(F(\alpha)),\end{aligned}$$

where $F(x) = x^{n_1}(ax^2 + bx + c)^{n_2}(dx + e)^{q-n_2-1} \in \mathbb{F}_q[x]$ for some $0 \leq n_1, n_2 \leq q-2$.

We show that if $(\chi_{d_1}, \chi_{d_2}) \neq (\chi_1, \chi_1)$ then

$$|\boldsymbol{\chi}_A(\chi_{d_1}, \chi_{d_2})| \leq 3q^{1/2}.$$

If $F(x) \neq yH^{q-1}$ for any $y \in \mathbb{F}_q$ and $H \in \mathbb{F}_q[x]$ then using Lemma 2.3

$$|\boldsymbol{\chi}_A| \leq (4-1)q^{1/2} = 3q^{1/2}.$$

Now if $F = yH^{q-1}$ for some $y \in \mathbb{F}_q$ and $H \in \mathbb{F}_q[x]$ then $n_1 = n_2 = 0$. To see this let us assume that

$$x^{n_1}(ax^2 + bx + c)^{n_2}(dx + e)^{q-1-n_2} = yH^{q-1}, \tag{3}$$

for some $y \in \mathbb{F}_q$ and $H \in \mathbb{F}_q[x]$. Now (3)$\Rightarrow (dx + e)^{q-1-n_2} | H^{q-1}$, hence we get

$$x^{n_1}(ax^2 + bx + c)^{n_2} = y(dx + e)^{n_2} H'^{\,q-1} \tag{4}$$

where $H'(x) = H(x)/(dx + e) \in \mathbb{F}_q[x]$. Comparing powers of x on both the sides of (4), we get $n_1 + n_2 \geq k_1(q-1) \Rightarrow k_1 \leq 1$, where k_1 is the degree of the polynomial $H'(x)$. Hence $H'(x) = (a'x + b')^{k_1}$ for some $a',\ b' \in \mathbb{F}_q$ and $k_1 = 0$ or 1. Thus, the following cases arise:

Case 1. $a \neq 0$, $e \neq 0$.

Let us suppose that $n_1 > 0$. Then (4) gives

$$(ax^2 + bx + c)^{n_2} = y(dx + e)^{n_2} x^{q-1-n_1} B(x)^{q-1}, \tag{5}$$

where $B(x) = H'(x)/x \in \mathbb{F}_q[x]$ is a constant polynomial. Hence from (5), we see that $c = 0$, putting this back in (5), we get $x^{n_2}(ax + b)^{n_2} = y(dx + e)^{n_2} x^{q-1-n_1} B(x)^{q-1}$, which is possible only if $\gcd(dx+e, ax+b) = x + e/d$ and $q-1 = n_1 + n_2$. In this case, we get $\lambda_A(x) = \frac{a}{d}x$, which is not possible. Hence $n_1 = 0$ and from (4), we get $(ax^2+bx+c)^{n_2} = y(dx+e)^{n_2}H'^{\,q-1}$. Again comparing degrees, we get $k_1 = 0$, and hence $n_2 = 0$.

Case 2. $a \neq 0$, and $e = 0$.

In this case (4) becomes

$$x^{n_1}(ax^2+bx+c)^{n_2} = y'x^{n_2}H'^{\,q-1}, \tag{6}$$

where $y' = yd^{n_2} \in \mathbb{F}_q$.

From (6), we see that $x^{n_1} | x^{n_2}(a'x+b')^{k_1(q-1)} \Rightarrow$ either $n_1 = 0$ or $n_1 \leq n_2$ or $b' = 0$. If $n_1 = 0$ then a comparison of degrees of x on both the sides of (6) gives $k_1 = 0$ and hence $n_2 = 0$.

So let us assume that $n_1 > 0$, and $n_1 \leq n_2$. Then from (6), we get

$$(ax^2+bx+c)^{n_2} = y'x^{n_2-n_1}(a'x+b')^{k_1(q-1)}, \tag{7}$$

$\Rightarrow (a'x+b')^{k_1(q-1)} | (ax^2+bx+c)^{n_2} \Rightarrow$ either $k_1 = 0$ or $ax^2+bx+c = (a''x+b'')^2$, for some a'' and $b'' \in \mathbb{F}_q$. If $k_1 = 0$ then $n_1 = n_2 = 0$ from (7). So let us assume that $k_1 = 1$. Then (7) gives that $(a''x+b'')^{2n_2-(q-1)} = y'a'(a'')^{-1}x^{n_2-n_1}$, which is possible only if either $n_1 = n_2$ and $2n_2 = q-1$ or $b'' = 0$. But $q-1 \neq 2n_2$ since $q-1$ is odd. So $b'' = 0$ and hence $b = c = 0$. But in this case we get that $\lambda_A(x) = \frac{a}{d}x$. Now if $b' = 0$ then from (7), we get either $n_1 = n_2 = k_1 = 0$ or $b = c = 0$. If $b = c = 0$ then $\lambda_A(x) = \frac{a}{d}x$, and hence $n_1 = n_2 = 0$.

Case 3. $a = 0$, then (4) gives

$$x^{n_1}(bx+c)^{n_2} = yH'^{\,q-1}(dx+e)^{n_2}. \tag{8}$$

We compare degrees on both the sides of (8) and conclude that $n_1 \geq k_1(q-1) \Rightarrow k_1 = 0$ and $H'(x)$ is a constant. Now if $n_1 = 0$ then (8) is possible only if either $n_2 = 0$ or $dx+e | bx+c$, but in that case rank of A is 1. Hence $n_1 = n_2 = 0$. So let us assume that $n_1 > 0$. Then from (8) we see that $x^{n_1} | (dx+e)^{n_2}$, which is possible only if $e = 0$ and $n_1 \leq n_2$. Putting this in (8), we get $(bx+c)^{n_2} = yH'^{\,q-1}d^{n_2}x^{n_2-n_1}$. Thus, $n_1 = n_2 = 0$ or $c = 0$. But $n_1 > 0$, so $c = 0$. But in this case rank of A becomes 1. Hence $n_1 = n_2 = 0$.

Thus in all the cases, $(\chi_{d_1}, \chi_{d_2}) = (\chi_1, \chi_1)$.

Hence $|\boldsymbol{\chi}_A(\chi_{d_1}, \chi_{d_2})| \leq 3q^{1/2}$, when $(\chi_{d_1}, \chi_{d_2}) \neq (\chi_1, \chi_1)$. This, and (2) gives

$$N_A(l_1, l_2) \geq \theta(l_1)\theta(l_2)(q - 1 - 3q^{1/2}(W(l_1)W(l_2) - 1)). \tag{9}$$

Now $N_A(l_1, l_2) > 0$ if $q > 1 + 3q^{1/2}(W(l_1)W(l_2) - 1)$, that is, if $q^{1/2} > 3W(l_1)W(l_2)$. Hence the result follows.

Lemma 3.3. *Let* $A = \begin{pmatrix} a & b & c \\ 0 & 0 & e \end{pmatrix} \in \mathfrak{M}_q$ *be such that* $\lambda_A(x) \neq \beta x, \beta x^2$ *for any* $\beta \in \mathbb{F}_q$, *and* l_1, l_2 *divide* $q-1$. *If* $q^{1/2} > 3W(l_1)W(l_2)$ *then* $N_A(l_1, l_2) > 0$.

Proof. Here $d = 0$, therefore

$$N_A(l_1, l_2) = \theta(l_1)\theta(l_2) \sum_{d_1|l_1,\ d_2|l_2} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\chi_{d_1}, \chi_{d_2}} \boldsymbol{\chi}_A(\chi_{d_1}, \chi_{d_2}),$$

where $\boldsymbol{\chi}_A(\chi_{d_1}, \chi_{d_2}) = \sum_{\alpha \in \mathbb{F}_q} \chi_{d_1}(\alpha)\chi_{d_2}(\lambda_A(\alpha)) = \sum_{\alpha \in \mathbb{F}_q} \chi_{q-1}(F(\alpha))$.

In this case, $F(x) = x^{n_1}(\frac{a}{e}x^2 + \frac{b}{e}x + \frac{c}{e})^{n_2} \in \mathbb{F}_q[x]$ for some $n_1,\ n_2 \in \{1,\ 2, \ldots,\ q-2\}$.

Again if $F(x) \neq yH^{q-1}$ for any $y \in \mathbb{F}_q$ and $H \in \mathbb{F}_q[x]$ then using Lemma 2.3

$$|\boldsymbol{\chi}_A(\chi_{d_1}, \chi_{d_2})| \leq (3-1)q^{1/2} = 2q^{1/2}.$$

Now if $F = yH^{q-1}$ for some $y \in \mathbb{F}_q$ and $H \in \mathbb{F}_q[x]$ then $n_1 = n_2 = 0$. To see this, let us assume that $x^{n_1}(\frac{a}{e}x^2 + \frac{b}{e}x + \frac{c}{e})^{n_2} = yH^{q-1}$ for some $y \in \mathbb{F}_q$ and $H \in \mathbb{F}_q[x]$, which gives

$$x^{n_1}(ax^2 + bx + c)^{n_2} = y'H^{q-1}, \tag{10}$$

where $y' = (e)^{n_2}y \in \mathbb{F}_q$. From (10), we see that either $n_1 = n_2 = 0$, and H is a constant or $n_1 \neq 0$. If $n_1 \neq 0$ then $x^{n_1}|H^{q-1}$, hence $(ax^2 + bx + c)^{n_2} = y'x^{q-1-n_1}B(x)^{q-1}$, where $B(x) = H(x)/x \in \mathbb{F}_q[x]$. Now $x^{q-1-n_1}|(ax^2 + bx + c)^{n_2}$, which is possible only if $c = 0$. Hence from (10), we get $x^{n_1+n_2}(ax + b)^{n_2} = y'H(x)^{q-1}$. Further, if $a = 0$ then $\lambda_A(x) = \frac{b}{e}x$, a contradiction. So let us take $a \neq 0$. Then from the equation $x^{n_1+n_2}(ax + b)^{n_2} = y'H(x)^{q-1}$, we see that $(ax + b)^{n_2}|H(x)^{q-1}$, which is possible only if $n_2 = 0$ or $x^{n_1+n_2} = y'(ax+b)^{q-1-n_2}C(x)^{q-1}$ for $C(x) = H(x)/(ax+b) \in \mathbb{F}_q[x]$. If $x^{n_1+n_2} = y'(ax+b)^{q-1-n_2}C(x)^{q-1}$ then $b = 0$, and if $b = 0$ then $\lambda_A(x) = \frac{a}{e}x^2$, again a contradiction. Hence $n_2 = 0$. Putting $n_2 = 0$ in (10), we get $n_1 = 0$. Thus n_1 can't be nonzero. Putting $n_1 = 0$ in (10) and comparing degrees on its both sides, we get $2n_2 \geq k_1(q-1)$, where k_1 is the degree of $H(x)$. So $k_1 \leq 1$. If $k_1 = 0$, then looking at degrees of x on both the sides of (10), we have $n_2 = 0$. Therefore assume that $k_1 = 1$, that is, $H(x) = a'x + b'$ for some $a', b' \in \mathbb{F}_q$. Now if $n_2 > 0$ then (10) is possible only if $ax^2 + bx + c = y''(a'x + b')^2$ for some $y'' \in \mathbb{F}_q[x]$ and $q - 1 = 2n_2$, but $q-1$ is odd. Hence $n_2 = 0$ and $H(x)$ is a constant i.e. $k_1 = 0$.

Thus in all of the above cases $(\chi_{d_1}, \chi_{d_2}) = (\chi_1, \chi_1)$. So, $|\boldsymbol{\chi}_A(\chi_{d_1}, \chi_{d_2})| \leq 2q^{1/2} \leq 3q^{1/2}$, when $(\chi_{d_1}, \chi_{d_2}) \neq (\chi_1, \chi_1)$.

Now,

$$\begin{aligned} N_A(l_1, l_2) &\geq \theta(l_1)\theta(l_2)\Big\{q - 3q^{1/2} \sum_{\substack{d_1|l_1,\ d_2|l_2 \\ (d_1,d_2)\neq(1,1)}} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\chi_{d_1}, \chi_{d_2}} 1\Big\} \\ &= \theta(l_1)\theta(l_2)\Big\{q - 3q^{1/2}(W(l_1)W(l_2) - 1)\Big\}. \end{aligned} \tag{11}$$

Hence, $N_A(l_1, l_2) > 0$ if $q > 3q^{1/2}(W(l_1)W(l_2) - 1)$, that is, if $q^{1/2} > 3W(l_1)W(l_2)$.

We obtain an extension of the sieving Lemma 3.7 of [8]. The proof follows from the idea of Proposition 5.2 of [13], hence omitted.

Lemma 3.4. *Suppose $l|q-1$ and $\{p_1,\dots,p_s\}$ is the collection of all the primes dividing $q-1$ but not l. Then*

$$N_A(q-1,q-1) \geq \sum_{i=1}^{s} N_A(p_i l,l) + \sum_{i=1}^{s} N_A(l,p_i l) - (2s-1)N_A(l,l).$$

From Lemmas 3.1, 3.2, and 3.3, we observe that $N_A(q-1,q-1) > 0$, if $q^{1/2} > 3W(q-1)^2$. We further improve this condition.

Theorem 3.5. *Let $l|q-1$ and $\{p_1,\ p_2,\dots,p_s\}$ be the collection of all the primes dividing $q-1$, but not l. Suppose $\delta = 1 - 2\sum_{i=1}^{s}\frac{1}{p_i}$ and $\Delta = \frac{2s-1}{\delta} + 2$ and assume $\delta > 0$. If $q^{1/2} > 3W(l)^2\Delta$ then $q \in \mathfrak{P}$.*

Proof. Let $A \in \mathfrak{M}_q$ be arbitrary. If $\lambda_A(x) = x$ or x^2, then $N_A(q-1,q-1) > 0$ trivially. So let us assume that $\lambda_A(x) \neq x, x^2$. Now using (9), and (11) in Lemma 3.4, we get

$$\begin{aligned} N_A(q-1,q-1) \geq\ & 2\sum_{i=1}^{s}\theta(l)\theta(p_i l)\{q-1-3q^{1/2}(W(l)W(p_i l)-1)\} \\ & - (2s-1)\theta(l)^2\{q-1-3q^{1/2}(W(l)^2-1)\}. \end{aligned}$$

Using the facts $\theta(p_i l) = \theta(p_i)\theta(l)$ and $W(p_i l) = 2W(l)$, we get

$$\begin{aligned} N_A(q-1,q-1) \geq\ & 2\theta(l)^2\sum_{i=1}^{s}\theta(p_i)\{q-1-3q^{1/2}(2W(l)^2-1)\} \\ & - (2s-1)\theta(l)^2\{q-1-3q^{1/2}(W(l)^2-1)\}. \end{aligned}$$

Using $\delta = 2\sum_{i=1}^{s}\theta(p_i) - (2s-1)$, we get

$$\begin{aligned} N_A(q-1,q-1) \geq\ & 2\theta(l)^2\sum_{i=1}^{s}\theta(p_i)\{q-1-3q^{1/2}(2W(l)^2-1)\} \\ & + (\delta - 2\sum_{i=1}^{s}\theta(p_i))\theta(l)^2\{q-1-3q^{1/2}(W(l)^2-1)\}. \\ \Rightarrow N_A(q-1,q-1) \geq\ & q^{1/2}\delta\big[-3W(l)^2\theta(l)^2\frac{2\sum_{i=1}^{s}\theta(p_i)}{\delta} \\ & + \theta(l)^2\{q^{1/2}-q^{-1/2}-3(W(l)^2-1)\}\big]. \end{aligned}$$

Using $\frac{2\sum_{i=1}^{s}\theta(p_i)}{\delta} = \frac{2s-1}{\delta} + 1$, we get $N_A(q-1,q-1) \geq q^{1/2}\delta\big\{-3W(l)^2\theta(l)^2\left(\frac{2s-1}{\delta}+2\right) + \theta(l)^2(q^{1/2}-q^{-1/2}+3)\big\}$.

Hence $N_A(q-1,q-1) > 0$ if $q^{1/2} - q^{-1/2} + 3 > 3W(l)^2\left(\frac{2s-1}{\delta} + 2\right)$, that is, if $q^{1/2} > 3W(l)^2\Delta$. So if $q^{1/2} > 3W(l)^2\Delta$ then for every $A \in \mathfrak{M}_q$, $\mathbb{F}_q$ contains a primitive pair $(\alpha, \lambda_A(\alpha))$ and hence $q \in \mathfrak{P}$.

3.1. $\mathbb{F}_q$ with primitive pairs $(\alpha, \lambda_A(\alpha))$

Lemma 3.6. *Suppose $q = 2^k$, where k is a positive integer. Then $q \in \mathfrak{P}$, for $k \geq 25$, and $k = 23,\ 22,\ 21,\ 19,\ 17$ and 13.*

Proof. From Lemma 3.2 and Lemma 3.3, we see that if $k > 4\omega(q-1) + 4$ then $q \in \mathfrak{P}$. If $\omega(q-1) \geq 16$, then

$$q > 3 \times 5 \times \ldots \times 59 \times 16^{\omega(q-1)-16}.$$

Thus $k > 70 + 4\omega(q-1) - 64$, that is, $k > 4\omega(q-1) + 6 > 4\omega(q-1) + 4$ and hence $q \in \mathfrak{P}$. Let $\omega(q-1) \leq 15$. Then $4\omega(q-1)+4 \leq 64$. If $k > 64$ then $q \in \mathfrak{P}$. Now let us take $k \leq 64$. By factorizing $q-1$ in each case, we see that $k > 4\omega(q-1) + 4$ for $25 \leq k \leq 64$ and $k = 23,\ 22,\ 21,\ 19,\ 17,\ 13$ except for $k = 36$ and 28, where equality occurs. For $k = 36$ and 28, $q^{1/2} > 3W(q-1)^2$ is satisfied.

A Mersenne prime is a prime of the form $2^k - 1$ for some positive integer k.

Lemma 3.7. *If $q - 1 \geq 7$ is a Mersenne prime then $q \in \mathfrak{P}$.*

Proof. If $q-1$ is a Mersenne prime, that is, if $k = 3,\ 5,\ 7,\ 13,\ 17,\ 19$ etc., then every element of $\mathbb{F}_q \backslash \{0\}$ other than 1 is a primitive element. Let $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in \mathfrak{M}_q$ be arbitrary. Then rank of A is 2. So at least one of a, b, c and one of d and e is nonzero. Hence $ax^2 + bx + c \neq 0$, and $dx + e \neq 0$. Since $|\mathbb{F}_q^*| > 5$, there exists some $\alpha \in \mathbb{F}_q \backslash \{0\}$ such that $a\alpha^2 + b\alpha + c \neq 0$, $d\alpha + e \neq 0$ and $a\alpha^2 + b\alpha + c \neq d\alpha + e$. Hence $2^k \in \mathfrak{P}$ for $k = 3,\ 5,\ 7,\ 13,\ 17,\ 19$ etc.

Also $q = 2^k \in \mathfrak{P}$, for $k = 24,\ 20,\ 18,\ 16,\ 15,\ 14,\ 11,\ 9$ as these satisfy sieving inequality in Theorem 3.5 (see Table 1 below). The remaining cases, $q = 2^k$ for $k = 1,\ 2,\ 4,\ 6,\ 8,\ 10,\ 12$, don't satisfy the sieving inequality given in Theorem 3.5.

We further observe that $2 \notin \mathfrak{P}$, as 1 is the only primitive element in $\mathbb{F}_2$ but $\lambda_A(1) = 0$, if exactly two of the entries a, b, c of the matrix A are nonzero. Also $2^k \notin \mathfrak{P}$ for $k = 2$, as $|\mathbb{F}_4^*| = 3$ and there exists at least one matrix for which $a\alpha^2 + b\alpha + c = 0$ for both the primitive elements of $\mathbb{F}_4$. Note that for $A = \begin{pmatrix} 0 & x^3 & x^2 \\ 0 & x^2 & x^3 \end{pmatrix} \in \mathfrak{M}_{16}$, where $x \in \mathbb{F}_{16}$ is a primitive element, $\lambda_A(\alpha)$ is not primitive for any primitive element α of $\mathbb{F}_{16}$. Thus $2^k \notin \mathfrak{P}$ for $k = 4$.

Table 1
Values of k with $2^k \in \mathfrak{P}$.

Sr. No.	k	l	s	δ	Δ	$q^{1/2} > 3 \cdot W(l)^2\Delta$
1	24	105	3	0.7202	8.9426	True
2	20	15	3	0.7048	9.0943	True
3	18	3	3	0.5816	10.597	True
4	16	3	3	0.4745	12.5375	True
5	15	1	3	0.6365	9.8555	True
6	14	3	2	0.9377	5.1994	True
7	11	1	2	0.8905	5.3689	True
8	9	1	2	0.6868	6.3681	True

We have verified computationally that $k = 1,\ 2,\ 4$ are the only exceptions such that $\mathbb{F}_{2^k}$ contains a primitive pair $(\alpha, \lambda_A(\alpha))$, for any positive integer $2 \le k \le 12$, and every $A \in \mathfrak{M}_{2^k}$.

Summarizing Lemmas 3.6, 3.7, Table 1, and above discussion, we complete the proof of Theorem 1.1.

4. Existence of primitive pairs $(\alpha, \lambda_A(\alpha))$ with α normal over $\mathbb{F}_q$

In this section, we show the existence of primitive pairs $(\alpha, \lambda_A(\alpha))$ in $\mathbb{F}_{q^n}$ with α normal over $\mathbb{F}_q$, which is precisely our main result Theorem 1.2. We begin by proving a series of results.

Let $\mathbb{F}_{q^n}$ be an extension of $\mathbb{F}_q$ of degree n, where $q = 2^k$ for some positive integer k, and $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in \mathfrak{M}_{q^n}$. For any divisors e_1, e_2 of $q^n - 1$, and g of $x^n - 1$, let $N_A(e_1, e_2, g)$ be the number of $\alpha \in \mathbb{F}_{q^n}$ such that α is e_1-free, $\lambda_A(\alpha)$ is e_2-free and α is g-free. Our purpose is to show that $N_A(q^n - 1, q^n - 1, x^n - 1) > 0$. If $n = 1$ then $(q, n) \in \mathfrak{N}$ if and only if $q^n \in \mathfrak{P}$. If $n = 2$ then any primitive element of $\mathbb{F}_{q^2}$ is normal over $\mathbb{F}_q$. Hence $(q, 2) \in \mathfrak{N}$ if and only if $q^2 \in \mathfrak{P}$. Therefore, we assume that $n \ge 3$.

Lemma 4.1. *Let* $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in \mathfrak{M}_{q^n}$ *be such that* $\lambda_A(x) = x$ *or* x^2. *Then* $N_A(q^n - 1, q^n - 1, x^n - 1) > 0$.

Proof. As $q^n - 1$ is odd, so if α is primitive then so is α^2. Hence the result follows from [15].

Lemma 4.2. *Let* $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in \mathfrak{M}_{q^n}$ *be such that* $\lambda_A(x) \ne \beta x,\ \beta x^2$ *for any* $\beta \in \mathbb{F}_{q^n}$, $l_1,\ l_2 | q^n - 1$ *and* $g | x^n - 1$. *Then*

$$N_A(l_1, l_2, g) \ge \theta(l_1)\theta(l_2)\Theta(g)\{q^n - 1 - 4q^{n/2}(W(l_1)W(l_2)W(g) - 1)\}, \tag{12}$$

that is, $N_A(l_1, l_2, g) > 0$, *if* $q^{n/2} > 4W(l_1)W(l_2)W(g)$.

Proof. Let us first assume that $d \neq 0$. Then by definition

$$N_A(l_1, l_2, g) = \sum_{\alpha \neq \frac{-e}{d}} \rho_{l_1}(\alpha)\rho_{l_2}(\lambda_A(\alpha))\kappa_g(\alpha)$$

$$= \theta(l_1)\theta(l_2)\Theta(g) \sum_{d_1|l_1,\ d_2|l_2, h|g} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \frac{\mu'(h)}{\Phi_q(h)} \sum_{\chi_{d_1}, \chi_{d_2}, \psi_h} \boldsymbol{\chi}'_A(\chi_{d_1}, \chi_{d_2}, \psi_h),$$

where

$$\boldsymbol{\chi}'_A(\chi_{d_1}, \chi_{d_2}, \psi_h) = \sum_{\alpha \neq \frac{-e}{d}} \chi_{d_1}(\alpha)\chi_{d_2}\left(\frac{a\alpha^2 + b\alpha + c}{d\alpha + e}\right)\psi_h(\alpha).$$

As $\chi_{d_i}(\alpha) = \chi(\alpha^{n_i})$ for $n_i \in \{0,\ 1,\ 2,\ \cdots, q^n - 2\}$, $i = 1,\ 2$ and $\psi_h(\alpha) = \psi_{x^n-1}(y_1\alpha)$ for some $y_1 \in \mathbb{F}_{q^n}$, we get

$$\boldsymbol{\chi}'_A(\chi_{d_1}, \chi_{d_2}, \psi_h) = \sum_{\alpha \neq \frac{-e}{d}} \chi_{q^n-1}(F(\alpha))\psi_{x^n-1}(G(\alpha)),$$

where $F(x) = x^{n_1}\left(\frac{ax^2+bx+c}{dx+e}\right)^{n_2}$ for $n_1,\ n_2 \in \{1,\ 2,\ \cdots,\ q^n - 2\}$, and $G(x) = y_1x \in \mathbb{F}_{q^n}(x)$. If $F \neq yH^{q^n-1}$ for any $y \in \mathbb{F}_{q^n}$ and $H \in \mathbb{F}_{q^n}(x)$ and also if $G \neq H^p - H + y$ for any $y \in \mathbb{F}_{q^n}$ and $H \in \mathbb{F}_{q^n}(x)$ then using Lemma 2.4, we get

$$|\boldsymbol{\chi}'_A(\chi_{d_1}, \chi_{d_2}, \psi_h)| \leq 4q^{n/2}.$$

Now if $F = yH^{q^n-1}$ for some $y \in \mathbb{F}_{q^n}$ and $H \in \mathbb{F}_{q^n}(x)$ then $n_1 = n_2 = 0$. To see this, assume that $H = \frac{H_1}{H_2}$, where H_1 and H_2 are coprime polynomials over $\mathbb{F}_{q^n}$. Then

$$x^{n_1}\left(\frac{ax^2 + bx + c}{dx + e}\right)^{n_2} = y\frac{{H_1}^{q^n-1}}{{H_2}^{q^n-1}}$$

$$\Rightarrow x^{n_1}{H_2}^{q^n-1}(ax^2 + bx + c)^{n_2} = y{H_1}^{q^n-1}(dx + e)^{n_2} \tag{13}$$

$$\Rightarrow\ {H_2}^{q^n-1}|(dx + e)^{n_2},$$

which is a contradiction unless H_2 is a constant as $n_2 < q^n - 1$.

Putting $H_2^{q^n-1} = y' \in \mathbb{F}_q$ in (13) we get,

$$x^{n_1}(ax^2 + bx + c)^{n_2} = yy'^{-1}{H_1}^{q^n-1}(dx + e)^{n_2}. \tag{14}$$

By a similar argument used in Lemma 3.2, we get $n_1 = n_2 = 0$. Additionally, if $y_1 \neq 0$, then we get

$$|\boldsymbol{\chi}'_A(\chi_{d_1}, \chi_{d_2}, \psi_h)| = |\sum_{\alpha \neq \frac{-e}{d}} \psi_{x^n-1}(y_1\alpha)| = 1.$$

Hence $|\boldsymbol{\chi}'_A(\chi_{d_1}, \chi_{d_2}, \psi_h)| \leq 4q^{n/2}$, when $(\chi_{d_1}, \chi_{d_2}, \psi_h) \neq (\chi_1, \chi_1, \psi_1)$, that is, $N_A(l_1, l_2, g) \geq \theta(l_1)\theta(l_2)\Theta(g)\{q^n - 1 - 4q^{n/2}(W(l_1)W(l_2)W(g) - 1)\}$.

Hence $N_A(l_1, l_2, g) > 0$, if $q^n > 1 + 4q^{n/2}(W(l_1)W(l_2)W(g) - 1)$, that is, if $q^{n/2} > 4W(l_1)W(l_2)W(g)$.

Now let us assume that $d = 0$. Then

$$\begin{aligned} N_A(l_1, l_2, g) &= \sum_{\alpha \in \mathbb{F}_{q^n}} \rho_{l_1}(\alpha)\rho_{l_2}\left(\frac{a\alpha^2 + b\alpha + c}{e}\right)\kappa_g(\alpha) \\ &= \theta(l_1)\theta(l_2)\Theta(g) \sum_{d_1|l_1,\ d_2|l_2, h|g} \frac{\mu(d_1)}{\phi(d_1)}\frac{\mu(d_2)}{\phi(d_2)}\frac{\mu'(h)}{\Phi(h)} \sum_{\chi_{d_1}, \chi_{d_2}, \psi_h} \boldsymbol{\chi}'_A(\chi_{d_1}, \chi_{d_2}, \psi_h), \end{aligned}$$

where,

$$\begin{aligned} \boldsymbol{\chi}'_A(\chi_{d_1}, \chi_{d_2}, \psi_h) &= \sum_{\alpha \in \mathbb{F}_{q^n}} \chi_{d_1}(\alpha)\chi_{d_2}\left(\frac{a\alpha^2 + b\alpha + c}{e}\right)\psi_h(\alpha) \\ &= \sum_{\alpha \in \mathbb{F}_{q^n}} \chi_{q^n-1}(F(\alpha))\psi_{x^n-1}(G(\alpha)), \end{aligned}$$

where $F(x) = x^{n_1}\left(\frac{ax^2+bx+c}{e}\right)^{n_2}$ for $n_1,\ n_2 \in \{1,\ 2,\ \cdots,\ q^n - 2\}$, and $G(x) = y_1 x \in \mathbb{F}_{q^n}(x)$ for $y_1 \in \mathbb{F}_{q^n}$. If $F \neq yH^{q^n-1}$ for any $y \in \mathbb{F}_{q^n}$, and $H \in \mathbb{F}_{q^n}(x)$ and $G \neq H^p - H + y$ for any $y \in \mathbb{F}_{q^n}$ and $H \in \mathbb{F}_{q^n}(x)$ then using Lemma 2.4, we get

$$|\boldsymbol{\chi}'_A(\chi_{d_1}, \chi_{d_2}, \psi_h)| \leq 3q^{n/2} \leq 4q^{n/2}.$$

Now let $F = yH^{q^n-1}$ for some $y \in \mathbb{F}_{q^n}$ and $H \in \mathbb{F}_{q^n}(x)$. In this case, since F is a polynomial over $\mathbb{F}_{q^n}$, H is also a polynomial over $\mathbb{F}_{q^n}$. Hence the above gives

$$x^{n_1}(ax^2 + bx + c)^{n_2} = yH^{q^n-1}e^{n_2} \tag{15}$$

for some $H(x) \in \mathbb{F}_q[x]$ and $y \in \mathbb{F}_{q^n}$. By the same arguments as in Lemma 3.3, we get $n_1 = n_2 = 0$. Further, if $y_1 \neq 0$ then we get

$$\boldsymbol{\chi}'_A(\chi_{d_1}, \chi_{d_2}, \psi_h) = \sum_{\alpha \in \mathbb{F}_{q^n}} \psi_{x^n-1}(y_1\alpha) = 0.$$

Hence $|\boldsymbol{\chi}'_A(\chi_{d_1}, \chi_{d_2}, \psi_h)| \leq 4q^{n/2}$ when $(\chi_{d_1}, \chi_{d_2}, \psi_h) \neq (\chi_1, \chi_1, \psi_1)$, that is,

$$N_A(l_1, l_2, g) \geq \theta(l_1)\theta(l_2)\Theta(g)\{q^n - 1 - 4q^{n/2}(W(l_1)W(l_2)W(g) - 1)\}. \tag{16}$$

Hence $N_A(l_1, l_2, g) > 0$ if $q^n > 1 + 4q^{n/2}(W(l_1)W(l_2)W(g) - 1)$, that is, if $q^{n/2} > 4W(l_1)W(l_2)W(g)$.

In the following Lemma, we give 'additive-multiplicative' sieve involving sieving with respect to primes in q^n-1 as well as irreducible polynomials dividing x^n-1. The proof follows from the idea of Proposition 5.2 of [13], hence omitted.

Lemma 4.3. *Suppose $l|q^n-1$ and $p_1,...,p_s$ are the remaining primes dividing q^n-1. Also suppose that $E|x^n-1$ and $P_1,...,P_t$ are the remaining irreducible polynomials dividing x^n-1. Then*

$$N_A(q^n-1,q^n-1,x^n-1) \geq \sum_{i=1}^{s} N_A(p_i l,l,E) + \sum_{i=1}^{s} N_A(l,p_i l,E) + \sum_{i=1}^{t} N_A(l,l,P_iE) - (2s+t-1)N_A(l,l,E).$$

From Lemmas 4.1, and 4.2, we observe that $N_A(q^n-1,q^n-1,x^n-1)>0$, if $q^{n/2} > 4W(q^n-1)^2W(x^n-1)$. We further improve this condition in the next theorem. Its proof is similar to that of Theorem 3.5, hence omitted.

Theorem 4.4. *Suppose $l|q^n-1$ and $p_1,...,p_s$ are the remaining primes dividing q^n-1. Also suppose that $E|x^n-1$ and $P_1,...,P_t$ are the remaining irreducible polynomials dividing x^n-1. Set $\delta = 1-2\sum_{i=1}^{s}\frac{1}{p_i} - \sum_{i=1}^{t}\frac{1}{q^{\deg(P_i)}}$ and $S=\frac{2s+t-1}{\delta}+2$. Assume $\delta>0$. Then one of the following holds*

1. $N_A(q^n-1,q^n-1,x^n-1)>0$ *trivially.*
2. $N_A(q^n-1,q^n-1,x^n-1) \geq \delta\theta(l)^2\Theta(E)\{q^n-1-4q^{n/2}S(W(l)^2W(E)-1)\}$.

Hence, if

$$q^{n/2} > 4SW(l)^2W(E) \tag{17}$$

then $(q,n)\in\mathfrak{N}$.

4.1. $\mathbb{F}_{q^n}$ with primitive pairs $(\alpha,\lambda_A(\alpha))$ such that α is normal over $\mathbb{F}_q$

In this section, we consider that $n=n'2^{\nu}$, where $\nu\geq 0$ is an integer and $\gcd(2,n')=1$. We divide our discussion into two parts, the one when $n'|q-1$ and the other when $n'\nmid q-1$. Throughout the rest of the section, let $\omega=\omega(q^n-1)$ and $l=q^n-1$ if not specified.

Case A. $n'|q-1$.

Recall the fact that if $n'|q-1$, $x^{n'}-1$ splits into a product of n' distinct linear factors over $\mathbb{F}_q$ [17, Theorem 2.47]. Hence the number of irreducible factors of $x^{n'}-1$ is n'. We use this fact to calculate S used in above lemmas.

Lemma 4.5. *[8, Lemma 6.2] Let m be an odd positive integer. Then $W(m) < 6.46m^{1/5}$.*

Lemma 4.6. *Let $q = 2^k$, for some positive integer k and $n'|q-1$. If $n' \geq 19$ then $(q,n) \in \mathfrak{N}$.*

Proof. Using Lemma 4.5, we get $W(q^n-1) \leq 6.46q^{n/5}$. From Theorem 4.4, by taking $E = 1$, we observe that, $(q,n) \in \mathfrak{N}$ if $q^{n/10} > 167S$. First suppose that $n' = q-1$, then $S = q^2 - 2q + 2 < q^2$, and the above inequality is satisfied if

$$q^{\frac{q-1}{10}-2} > 167. \tag{18}$$

We can see that (18) holds if $q \geq 64$. Now we consider the remaining case $q = 32$ and $n = 31$. For this (17), $q^{31/2} > 2^2 \times 2^{14} \times q^2$ is true. So $(32,31) \in \mathfrak{N}$. Now if $q \geq 64$ and $19 \leq n' \leq \frac{q-1}{3}$ then $S < \frac{q}{2}$. Hence $(q,n) \in \mathfrak{N}$ if $q^{n'/10-1} > 83.5$. Hence we observe that $q^{n'/10-1} > 83.5$ is true for $n' \geq 19$ and all $q = 2^k$ such that $n'|q-1$.

In the above lemma, we have considered the values of $n' \geq 19$. We discuss below the remaining values of n'.

1. $\boldsymbol{n' = 1}$. In this case, we have $n = 2^j$, for some $j \geq 2$.
   We need to check that
   $$q^{\frac{2^j}{2}} > 4(6.46)^2 q^{2\cdot\frac{2^j}{5}} W(E)S$$
   Let $E = x+1$, so that $\delta = 1$, $S = 1$.
   It remains to verify that
   $$q^{\frac{2^j}{10}} > 334.$$
   Observe that the above inequality holds for $q \geq 2^{21}$. Conversely, if it fails then necessarily $q^{2^j} \leq 2^{84}$. For the remaining pairs (q,n) (which are 40 in number), by calculating $\omega(q^n-1)$, we see that all the pairs except $(2,4)$, $(2,8)$, $(2,16)$, $(4,4)$, $(4,8)$, $(8,4)$, $(8,8)$, $(16,4)$, $(32,4)$, $(64,4)$, $(128,4)$, $(512,4)$ satisfy $q^{n/2} > 2^{2\omega(q^n-1)+3}$ and hence are in $\mathfrak{N}$.
   For these pairs, we refer to Table 2, and see that all pairs (q,n) except $(2,4)$, $(2,8)$, $(2,16)$, $(4,4)$, $(4,8)$, $(8,4)$, $(16,4)$ are in $\mathfrak{N}$.
2. $\boldsymbol{n' = 3}$. In this case $q = 2^{2m}$, for some $m \geq 1$ and $n = 3.2^j$ for some $j \geq 0$. Now by taking $E = 1$, (17) is true if
   $$2^{3m\cdot 2^{j+1}/10} > 167S.$$
   In this case $\delta = \frac{q-3}{q}$ and so $S = 2 + \frac{2q}{q-3}$. First assume $m \geq 2$, then $S < 9/2$, and the above inequality becomes $2^{\frac{3m2^{j+1}}{10}} > 83.5 \times 9$. Observe that the inequality holds

Table 2
(q, n) such that $n'|q-1$.

Sr. No.	(q, n)	l	s	E	t	S	$q^{n/2} > 4SW(l)^2W(E)$
1	(8,8)	15	4	$x+1$	0	18.1142	True
2	(32,4)	3	4	$x+1$	0	24.966	True
3	(64,4)	15	4	$x+1$	0	18.1142	True
4	(128,4)	15	4	$x+1$	0	10.226	True
5	(512,4)	15	6	$x+1$	0	32.96	True
6	(4096,3)	15	6	$x+1$	2	38.641	True
7	(1024,3)	21	4	$x+1$	2	14.2884	True
8	(256,3)	15	4	$x+1$	2	23.098	True
9	(64,3)	3	3	$x+1$	2	14.721	True
10	(64,6)	15	6	$x+1$	2	42.1111	True
11	(16,10)	15	5	x^5-1	0	17.327	True
12	(256,5)	15	5	x^5-1	0	17.327	True
13	(256,10)	165	6	x^5-1	0	16.451	True
14	(64,9)	21	4	x^9-1	0	10.08	True
15	(64,18)	q^n-1	0	x^9-1	0	1	True
16	(4096,9)	q^n-1	0	x^9-1	0	1	True
17	(16,15)	1155	7	$x^{15}-1$	0	21.141	True
18	(16,30)	q^n-1	0	$x^{15}-1$	0	1	True
19	(256,15)	q^n-1	0	$x^{15}-1$	0	1	True

for $j \geq 3$ when $m = 2,\ 3$, for $j \geq 2$ when $4 \leq m \leq 7$, for $j \geq 1$ when $8 \leq m \leq 15$, and for $j \geq 0$ when $m \geq 16$. Next assume $m = 1$, then $S < 10$ and $q^{n/10} > 167S$ is satisfied for $j \geq 5$. For the remaining pairs, we calculate $\omega(q^n - 1)$, and see that all the pairs except $(2^{12}, 3)$, $(2^{10}, 3)$, $(256, 3)$, $(64, 3)$, $(64, 6)$, $(16, 3)$, $(16, 6)$, $(4, 3)$, $(4, 6)$, $(4, 12)$ satisfy (17), which is equivalent to $q^{n/2} > 2^{2\omega+5}$ with $E = x^3 - 1$, hence are in $\mathfrak{N}$. For the remaining pairs, we refer to Table 2. Thus, the only pairs which fail the sieving inequality (17) are, $(4, 3)$, $(4, 6)$, $(4, 12)$, $(16, 3)$, $(16, 6)$.

3. If $\boldsymbol{n' = 5}$ then $q = 2^{4m}$ for some $m \geq 1$, and $n = 5 \cdot 2^j$ for some $j \geq 0$, that is, $q^n = 2^{5m \cdot 2^{j+2}}$ for some $j \geq 0$. In this case $S < 8$, with $E = 1$, so the inequality (17) reduces to $2^{m2^{j+1}} > 167 \times 8$, which holds for $j \geq 3$ whenever $m = 1$, for $j \geq 2$ whenever $m = 2$, for $j \geq 1$ whenever $m = 3, 4, 5$ and for $j \geq 0$ whenever $m \geq 6$. Also we see that (17), which is equivalent to $q^{n/2} > 2^{2\omega+7}$ for $E = x^5 - 1$, is satisfied by all the remaining pairs except $(16, 5)$, $(16, 10)$, $(256, 5)$, $(256, 10)$ for the exact value of $\omega(q^n - 1)$. From Table 2, we see that $(16, 10)$, $(256, 5)$, $(256, 10)$ are also in $\mathfrak{N}$. This leaves the remaining pair to be $(16, 5)$ only.
4. $\boldsymbol{n' = 7}$. In this case, $q = 2^{3m}$ for some $m \geq 1$ and $q^n = 8^{7m \cdot 2^j}$, where $n = 7 \cdot 2^j$ for some $j \geq 0$. Now let us take $E = 1$. Then $\delta = \frac{q-7}{q}$, $S = 2 + \frac{6q}{q-7} = 8 + \frac{42}{q-7} \leq 50$ and inequality (17) reduces to $2^{\frac{21m \cdot 2^j}{10}} > 8350$. This is true for $j \geq 3$ whenever $m = 1$, for $j \geq 2$ whenever $m = 2,\ 3$, for $j \geq 1$, whenever $m = 4,\ 5,\ 6$ and for $j \geq 0$, whenever $m \geq 7$. For the remaining pairs $(8, 7)$, $(8, 14)$, $(8, 28)$, $(64, 7)$, $(64, 14)$, $(512, 7)$, $(512, 14)$, $(2^{12}, 7)$, $(2^{15}, 7)$, $(2^{18}, 7)$, let us take $E = x + 1$. Then (17) is reduced to $q^{n/2} > 2^{2\omega+3} \cdot 22$, which is satisfied by all except $(8, 7)$.
5. If $\boldsymbol{n' = 9}$ then $q = 2^{6m}$ for some $m \geq 1$ and $q^n = 64^{9m \cdot 2^j}$ for some $j \geq 0$. Now (17) (with $E = 1$) reduces to the inequality,

$$q^{n/10} > 167S.$$

In this case, $\delta = \frac{q-9}{q}$, $S = 10 + \frac{72}{q-9} < 11.5$, which reduces the above inequality to $8^{\frac{9 \cdot 2^j m}{5}} > 1921$. This is satisfied for $j \geq 2$ if $m = 1$, for $j \geq 1$ if $m = 2$, and for $j \geq 0$ if $m \geq 3$. Hence, we are left with the cases $(64, 9)$, $(64, 18)$, $(4096, 9)$, all of which are in $\mathfrak{N}$ (see Table 2).

6. If $\boldsymbol{n' = 11}$ then $q = 2^{10m}$ for some $m \geq 1$ and $q^n = 2^{10m \cdot 11 \cdot 2^j}$, where $n = 10.2^j$, $j \geq 0$.
   If $E = 1$ then $\delta = \frac{q-11}{q}$, $S = 2 + \frac{10q}{q-11} = 12 + \frac{110}{q-11} < \frac{109}{9}$, which reduces (17) to $q^{\frac{n}{10}} = 2^{11m \cdot 2^j} > 2023$. The inequality is satisfied for all $j \geq 0$ and $m \geq 1$.
7. If $\boldsymbol{n' = 13}$ then $q = 2^{12m}$ for some $m \geq 1$ and $q^n = 2^{12m \cdot 13 \cdot 2^j}$, where $n = 13 \cdot 2^j$ for some $j \geq 0$.
   Let us take $E = 1$. Then $\delta = \frac{q-13}{q}$, $S = 2 + \frac{12q}{q-13} = 14 + \frac{156}{q-13} < \frac{29}{2}$ and the inequality (17) becomes $q^{\frac{n}{10}} > 2421.5$, which is satisfied for all $m \geq 1$, and $j \geq 0$. Hence (q, n) with $n' = 13|q - 1$ lie in $\mathfrak{N}$.
8. If $\boldsymbol{n' = 15}$ then $q = 2^{4m}$ for some $m \geq 1$ and $q^n = 2^{15m \cdot 2^{j+2}}$, where $n = 15 \cdot 2^j$ for some $j \geq 0$.
   In this case, with $E = 1$, $\delta = \frac{q-15}{q}$, $S = 2 + \frac{14q}{q-15} = 16 + \frac{210}{q-15} < 226$ and the inequality (17) becomes $q^{\frac{n}{10}} > 37742$, which is satisfied for $j \geq 2$ whenever $m = 1$, for $j \geq 1$ whenever $m = 2$, and for $j \geq 0$ whenever $m \geq 3$. For the remaining three pairs $(16, 15)$, $(16, 30)$, $(64, 15)$, the reader is referred to Table 2.
9. If $\boldsymbol{n' = 17}$ then $q = 2^{8m}$ for some $m \geq 1$ and $q^n = 2^{8m \cdot 17 \cdot 2^j}$, where $n = 17 \cdot 2^j$ for some $j \geq 0$.
   Now let us take $E = 1$. Then $\delta = \frac{q-17}{q}$, $S = 18 + \frac{272}{q-17} < \frac{39}{2}$ and the inequality (17) becomes $q^{\frac{n}{10}} > 3256.5$, which is satisfied for all $m \geq 1$, and $j \geq 0$. Hence all (q, n) with $n' = 17|q - 1$ lie in $\mathfrak{N}$.

From Lemma 4.6 and above discussion, we get the following result.

Theorem 4.7. *Let $q = 2^k$ and $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_q)$ be of rank 2 such that if $\lambda_A(x) = \beta x$ or βx^2 for some $\beta \in \mathbb{F}_q$, then $\beta = 1$. If $n'|q - 1$, then there exists a normal element α of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that α and $\lambda_A(\alpha)$ both are primitive unless (q, n) is one of the pairs* $(2, 2)$, $(2, 4)$, $(2, 8)$, $(2, 16)$, $(4, 2)$, $(4, 4)$, $(4, 8)$, $(8, 2)$, $(8, 4)$, $(16, 2)$, $(16, 4)$, $(32, 2)$, $(64, 2)$, $(4, 3)$, $(4, 6)$, $(4, 12)$, $(16, 6)$, $(16, 3)$, $(16, 5)$, $(8, 7)$.

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

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

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

Observe that $n\rho(q,n)=n'\rho(q,n')$. It is important to use the following upper bounds for $\rho(q,n)$.

Lemma 4.8. *[8, Lemma 7.1] Let n be odd, and $q=2^k$, for some positive integer k. Then*

1. $\rho(2,3)=1/3$; $\rho(2,5)=1/5$; $\rho(2,9)=2/9$; $\rho(2,21)=4/21$; *otherwise* $\rho(2,n)\le 1/6$.
2. $\rho(4,9)=1/3$; $\rho(4,45)=11/45$; *otherwise* $\rho(4,n)\le 1/5$.
3. $\rho(8,3)=\rho(8,21)=1/3$; *otherwise* $\rho(8,n)\le 1/5$.
4. *If* $q\ge 16$ *then* $\rho(q,n)\le 1/3$.

Lemma 4.9. *[8, Lemma 7.2] Suppose $q=2^k$, for some positive integer k and n is an integer such that n' does not divide $q-1$. If E is the product of irreducible factors of x^n-1 of degree less than u, then $S\le n'$.*

We now discuss the values of q for the Case B.

Lemma 4.10. *Let $q=2^k\ge 16$. If $n'\nmid q-1$ then there exists a normal element α of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that α and $\lambda_A(\alpha)$ are primitive in $\mathbb{F}_{q^n}$.*

Proof. Let E be the product of irreducible factors of x^n-1 of degree less than u. Then for $N_A(q^n-1,q^n-1,x^n-1)>0$, it suffices to show that $q^{n/2}>4(6.46)^2q^{2n/5}2^{n\rho(q,n)}S$, which is equivalent to $q^{n/60}>167n$. The inequality holds for $n\ge 229$. Next, assume that $n\le 228$, and $q^n\le 16^{228}<3.5\times 10^{274}$. But then $\omega\le 118$. Thus above inequality will be satisfied if $q^{5n/12}>n2^{2\omega+2}$. This holds when $n\ge 148$ and $q^n\ge 16^{148}$ with $\omega\le 118$. Now for the remaining cases we assume that $n\le 147$ and $q^n\le 16^{147}<1.02\times 10^{177}$. For this we get, $\omega\le 83$. Using this process repeatedly, we can assume that $n\le 39$ and $q^n\le 9.14\times 10^{46}$.

For the remaining pairs (q,n), which are 173 in numbers, we exactly evaluate $\omega=\omega(q^n-1)$, and test whether the condition $q^{n/2}>n2^{n/3+2\omega+2}$ is satisfied. This holds for all the pairs except for $(16,7)$, $(16,9)$, $(16,11)$, $(16,18)$, $(32,3)$, $(32,6)$, $(32,12)$, $(64,5)$, $(64,10)$, $(128,3)$.

These pairs satisfy (17), for appropriate choices of l and E (listed in Table 3). Hence all the pairs (q,n) with $q\ge 16$, and n such that $n'\nmid q-1$ are in $\mathfrak{N}$.

Lemma 4.11. *Let $q=8$. If $n'\nmid q-1$ then there exists a normal element α of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that α and $\lambda_A(\alpha)$ are primitive except for $(8,3)$.*

Proof. First suppose $n'=3$. Then $x^{n'}-1$ is a product of a linear and a quadratic factor over $\mathbb{F}_q$. Since $n\ge n'$, we first assume that $n'<n$, then $n=3\cdot 2^r$, $r\ge 1$. Let $E=1$. Then $\delta=1-\frac{1}{8}-\frac{1}{64}=\frac{55}{64}$ and $S=\frac{174}{55}<3.17$. From (17), for $N_A(q^n-1,q^n-1,x^n-1)$

Table 3
(q,n) such that $n' \nmid q-1$ (γ denotes a primitive element of $\mathbb{F}_4$).

Sr. No.	(q,n)	l	s	E	t	S	$q^{n/2} > 4SW(l)^2W(E)$
1	(16,7)	15	4	$x+1$	2	12.5821	True
2	(16,9)	15	6	$x+1$	4	67.2742	True
3	(16,11)	q^n-1	0	$x+1$	2	3.01	True
4	(16,18)	q^n-1	0	$x+1$	4	5.4306	True
5	(32,3)	7	2	1	2	7.618	True
6	(32,6)	21	4	1	2	14.8187	True
7	(32,12)	q^n-1	0	$x+1$	1	2	True
8	(64,5)	3	5	$x+1$	2	26.548	True
9	(64,10)	q^n-1	0	$x+1$	2	3.01	True
10	(128,3)	q^n-1	0	$x+1$	1	2	True
11	(8,6)	3	3	1	2	18	True
12	(8,12)	15	6	1	2	62.5497	True
13	(8,5)	7	2	1	2	8.2743	True
14	(8,10)	21	4	1	2	16.7759	True
15	(8,20)	q^n-1	0	$x+1$	1	2	True
16	(4,11)	3	3	$x+1$	2	9.9043	True
17	(4,13)	3	2	$x+1$	2	7.0076	True
18	(4,14)	15	4	$x+1$	2	12.9783	True
19	(4,15)	21	4	$(x+1)(x+\gamma)(x+\gamma^2)$	6	38.1815	True
20	(4,20)	165	4	$x+1$	2	15.9752	True
21	(4,21)	903	3	$x+1$	8	14.443	True
22	(4,22)	30705	3	$x+1$	2	9.0772	True
23	(4,25)	1023	4	$x+1$	4	14.7611	True
24	(4,30)	15015	6	$(x+1)(x+\gamma)(x+\gamma^2)$	6	39.1099	True
25	(2,36)	105	5	$(x^2+x+1)(x^6+x+1)$	1	17.9898	True
26	(2,72)	105	9	$(x^2+x+1)(x^6+x+1)$	1	38.3784	True
27	(2,21)	7	2	$x+1$	5	19.8971	True
28	(2,28)	3	5	$x+1$	2	56.727	True
29	(2,44)	15	5	$x+1$	1	13.3559	True
30	(2,60)	105	8	$x+1$	4	320	True
31	(2,22)	3	3	$x+1$	1	8.7675	True
32	(2,26)	3	2	$x+1$	1	6.006	True
33	(2,30)	21	4	$x+1$	4	39.062	True
34	(2,50)	1023	4	$x+1$	2	11.735	True
35	(2,13)	1	1	$x+1$	1	4.002	True
36	(2,17)	1	1	$x+1$	2	5.0239	True
37	(2,19)	1	1	$x+1$	1	4.01	True
38	(2,23)	1	2	$x+1$	2	7.228	True
39	(2,25)	31	2	$x+1$	2	7.3591	True
40	(2,27)	7	2	$x+1$	3	10.4878	True
41	(2,29)	233	2	$x+1$	1	6.0113	True
42	(2,33)	161	2	$x+1$	4	11.619	True
43	(2,35)	2201	2	$x+1$	5	13.919	True
44	(2,39)	553	2	$x+1$	4	11.3458	True
45	(2,45)	15841	3	$x+1$	7	24.651	True
46	(2,51)	721	3	$x+1$	7	18.5426	True
47	(2,55)	63457	3	$x+1$	4	11.641	True

to be greater than zero, it suffices to show that $8^{\frac{3\cdot 2^r}{10}} > 3.17 \times 167 = 529.39$. This holds for $r \geq 4$. Next suppose $1 \leq r \leq 3$, then $\omega(q^n-1) = 4r$. Now (17) holds if $8^{n/2} > 2^{8r+2} \times 3.17 = 3246.08$. This happens for $r = 3$. Hence it is true for all $r \geq 3$. Thus we are left with the cases $r = 1$, and 2. We discuss these in Table 3, and see that $(8,n) \in \mathfrak{N}$, for $n = 3 \cdot 2^r$, $r \geq 1$. Thus the only remaining case is $(8,3)$.

Next assume $n' = 21$. Then $x^{n'}-1$ is a product of 7 linear and 7 quadratic irreducible polynomials over $\mathbb{F}_q$. Let E be the product of the 7 linear factors. Then $\delta = 57/64 = 0.8906$, and $S < 8.74$. Now (17) reduces to $8^{n/10} > 167 \times 2^7 \times 8.74$, and it is satisfied for

$n \geq 84$. For $n = 21$ and 42, we find the factorization of $8^n - 1$, and test whether $8^{n/2} > 2^{2\omega+9}S$, where $\omega = \omega(8^n - 1)$, is satisfied. In fact, $\omega(8^{42} - 1) = 11$ and $\omega(8^{21} - 1) = 6$ for which the above inequality is easily satisfied. Thus $(8, n) \in \mathfrak{N}$, whenever $n' = 21$.

Now if $n' \neq 3,\ 21$, then by Lemma 4.8, $2^{n\rho(8,n)} \leq 8^{n/15}$. Hence (17) is equivalent to $8^{n/30} > 167n$, which is satisfied for $n \geq 146$. So we assume that $n \leq 145$. But then $\omega(8^n - 1) \leq 65$ and hence $8^{n/2} > n2^{2\omega+2+n/5}$ is true for $n \geq 107$. Repeating this process several times, we can assume that $n \leq 48$ and $\omega \leq 27$. For the remaining pairs (q, n), $\omega = \omega(8^n - 1)$ is evaluated exactly and tested to see whether $q^{n/2} > n2^{2\omega+2+n/5}$ is satisfied. This is satisfied for all (q, n) except the pairs $(8, 5)$, $(8, 10)$, $(8, 20)$. By taking appropriate choices of l and E (listed in Table 3) for each of these, we see that (17) is satisfied. Hence all of the pairs (q, n) with $q = 8$ and n such that $n' \nmid q - 1$ are in $\mathfrak{N}$ except the pair $(8, 3)$.

Lemma 4.12. *[8, Lemma 7.3] Suppose $m = 4^n - 1$, where n is odd. Then $W(m) < 6.04m^{1/6}$.*

Lemma 4.13. *Let $q = 4$. If $n' \nmid q - 1$ then there exists a normal element α of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that α and $\lambda_A(\alpha)$ are primitive unless (q, n) is one of the pairs* $(4, 5)$, $(4, 7)$, $(4, 9)$, $(4, 10)$.

Proof. Suppose $n' = 45$. Then $x^{n'} - 1$ is a product of 3 linear, 6 quadratic, 2 cubic and 4 sextic factors. Let E be the product of the three linear factors. Then $\delta = 0.5927$ and $S = 20.56$. Hence we deduce that (17) holds if $4^{n/10} > 2^3 \times 167 \times 20.56$, which in fact holds if $n \geq 90$. Now if $n = 45$ then $\omega(4^n - 1) = 11$ and (17) holds, as $4^{45/2} > 2^{2\omega+5} \times 20.56$. So $(4, 45) \in \mathfrak{N}$.

If $n' = 9$, $x^{n'} - 1$ is a product of 3 linear and 2 irreducible cubic factors. Let E be the product of the three linear factors. Then $\delta = \frac{31}{32}$ and $S < 3.033$. Hence (17) holds if $4^{n/10} > 167 \times 2^3 \times 3.033$ is true. The inequality is true for $n \geq 72$. Now if $n = 36$ then $\omega(4^n - 1) = 12$ and (17) holds, since $4^{36/2} > 2^{2\omega+5} \cdot 3.033$. Hence $(4, 36) \in \mathfrak{N}$. Suppose $n = 18$. Then $4^n - 1 = 3^3 \times 5 \times 7 \times 13 \times 19 \times 37 \times 73 \times 109$. Let us take $l = 105$ and E as before, so that $s = 5$, $t = 2$ and hence $\delta = 0.6098$, $S < 20.0388$. Then $4^9 > 2^2 \times 2^6 \times 2^3 \times 20.0388$. Thus $(4, 18) \in \mathfrak{N}$.

Hence the only remaining pair is $(4, 9)$.

Suppose $n' \neq 9, 45$; thus $\rho(q, n') \leq 1/5$. First assume that n is even. Then $n\rho(q, n) \leq n/10$, and hence $2^{n\rho(q,n)} \leq q^{n/20}$. For $(4, n) \in \mathfrak{N}$, it is sufficient to show that $4^{n/20} > 167n$. This holds when $n \geq 146$. Now let us take $n \leq 144$. Then $\omega \leq 47$. It suffices to show that $q^{n/2} > 2^{2\omega+\frac{n}{10}+2}n$, and it is true for $n \geq 116$. So let $n \leq 114$. Then $\omega \leq 39$, and the above inequality is true for $n \geq 98$. Therefore assume that $n \leq 96$, and hence $\omega \leq 34$. Continuing this way, we assume that $n \leq 64$.

For the remaining pairs, $\omega(4^n - 1)$ has been evaluated exactly and tested to see whether $4^{n/2} > 2^{2\omega+n/10+2}n$ is satisfied. All the pairs except $(4, 10)$, $(4, 14)$, $(4, 20)$, $(4, 22)$, $(4, 30)$ are in $\mathfrak{N}$.

Next suppose $n' \neq 9, 45$, is odd, then $n\rho(q,n) \leq n/5$. Using this and Lemma 4.12 in (17), we see that $(q,n) \in \mathfrak{N}$ if $q^{n/15} > 146n$, which is true for $n \geq 105$. Now we calculate $\omega = \omega(q^n - 1)$ for each pair (q,n) with $n \leq 103$, and see that (17), which is equivalent to $q^{n/2} > 2^{2\omega+2+n/5}n$, is satisfied for all except $(4,5)$, $(4,7)$, $(4,11)$, $(4,13)$, $(4,15)$, $(4,21)$, $(4,25)$. For the remaining pairs, we see that (17) is satisfied by taking appropriate choices of l and E (Table 3) except the pairs $(4,5)$, $(4,7)$, $(4,10)$.

Lemma 4.14. *[8, Lemma 7.5] Suppose n is odd, then $\omega(2^n - 1) < 3.76 \cdot 2^{n/7}$.*

Lemma 4.15. *Let $q = 2$. If $n' \nmid q - 1$ then there exists a normal element α of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that α and $\lambda_A(\alpha)$ are primitive unless (q,n) is one of the pairs $(2,6)$, $(2,12)$, $(2,24)$, $(2,10)$, $(2,20)$, $(2,9)$, $(2,18)$, $(2,14)$, $(2,11)$, $(2,15)$.*

Proof. Suppose $n' = 3$, then $x^{n'} - 1$ is the product of a linear factor and a quadratic factor. Let $E = x^{n'} - 1$. Then by (17) and Lemma 4.5, for $N_A(q^n - 1, q^n - 1, x^n - 1)$ to be greater than zero, it is sufficient to show that $2^{n/10} > 167 \times 4 = 668$. This holds for $n \geq 94$. Next assume that $n = 48$, then $\omega = 9$ and by (17), $(q,n) \in \mathfrak{N}$ if $2^{n/2-2\omega-4} = 4 > 1$, which is true. For the other cases (17) fails. Hence all the pairs except $(2,3)$, $(2,6)$, $(2,12)$, $(2,24)$ are in $\mathfrak{N}$.

Next suppose $n' = 5$, then $x^{n'} - 1$ is the product of a linear and an irreducible quartic factor. By (17), $(2,n) \in \mathfrak{N}$ if $2^{n/10} > 167 \times 4 = 668$ and this holds for $n \geq 95$. Now if $n = 80$ then $\omega(2^n - 1) = 9$, and (17) (with $E = x^5 - 1$) becomes $2^{40} > 2^2 \times 2^{18} \times 2^2$, which is true. For $n = 40$, $\omega = 7$, it is sufficient to show that $q^{n/2-2\omega-4} = 4 > 1$, which is true. For the pairs $(2,10)$, $(2,20)$, the sieving machinery fails.

Suppose $n' = 9$, then $x^9 - 1$ is a product of a linear, a quadratic and a sextic polynomial. If $E = 1$ then $\delta > 0.234$ and $S < 10.547$, and by (17) and Lemma 4.5, it is sufficient that $2^{n/10} > 167 \times 10.547 = 1761.349$. This inequality is true for $n \geq 144$. For the remaining values of n, we refer to Table 3, and see that $(2,72)$, $(2,36) \in \mathfrak{N}$. This leaves us with the pairs $(2,9)$ and $(2,18)$.

Next if $n' = 21$ then $x^{21} - 1$ is a product of a linear, a quadratic, two cubic and two sextic polynomials. Again by using Lemma 4.5 in (17), we see that $(2,n) \in \mathfrak{N}$ for $n \geq 168$. For $n = 84, 42$ and $E = x^{n'} - 1$, the factorization of $2^n - 1$, yields that $2^{n/2} > 2^{2\omega+2}W(E)S$, so that $(2,n) \in \mathfrak{N}$. Also $(2,21) \in \mathfrak{N}$ (explained in Table 3).

If $n' \neq 3, 5, 9, 21$ then $\rho(q,n') \leq 1/6$. Let $4 \mid n$. Then $2^{n\rho(q,n)} \leq 2^{n/24}$. Now (17) is equivalent to $2^{7n/120} > 167n$, which is true for $n \geq 268$. So let $n \leq 267$. But then $\omega \leq 44$, and hence (17), which is equivalent to $2^{n/2} > 2^{2+2\omega+n/24}$, is true for $n \geq 197$. So let $n \leq 196$. Repeating this, we can take $n \leq 126$. The condition $2^{n/2} > 2^{2\omega+2+n/24}n$ is satisfied for the remaining values of n except for $n = 28,\ 44,\ 60$. Table 3 shows that the pairs $(2,n)$ for $n = 28,\ 44,\ 60$ are also in $\mathfrak{N}$.

Now if $2 \mid n$ but $4 \nmid n$ then $n\rho(q,n) \leq \frac{n}{12}$. In this case, by using Lemma 4.12, (17) is reduced to $2^{n/12} > 146n$. This is satisfied for $n \geq 176$. Thus we assume that $n \leq 175$. For these values of n, we verify the condition $2^{n/2} > n2^{2\omega+n/12+2}$, using the exact value of

$\omega(2^n-1)$. This is satisfied for all except the pairs $(2,14)$, $(2,22)$, $(2,26)$, $(2,30)$, $(2,50)$. Out of these pairs, we can see through Table 3, that only $(2,14)$ remains.

If n is odd, then using Lemma 4.14 in (17), the sufficient condition becomes $2^{n/21} > 56.6n$, which is satisfied for $n \geq 295$. So take $n \leq 293$. For these cases the sufficient condition $2^{n/2} > 2^{2+2\omega+n/6}n$, is verified by using the exact value of ω. This holds for all except $(2,11)$, $(2,13)$, $(2,15)$, $(2,17)$, $(2,19)$, $(2,21)$, $(2,23)$, $(2,25)$, $(2,27)$, $(2,29)$, $(2,33)$, $(2,35)$, $(2,39)$, $(2,45)$, $(2,51)$, $(2,55)$.

For these pairs, we see that (17) is satisfied by taking appropriate choices of l and E except $(2,11)$ and $(2,15)$ (see Table 3).

Summarizing Lemmas 4.10, 4.11, 4.13 and 4.15, we get following Theorem.

Theorem 4.16. *Let $q = 2^k$ and $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_q)$ be of rank 2 such that if $\lambda_A(x) = \beta x$ or βx^2 for some $\beta \in \mathbb{F}_q$, then $\beta = 1$. If $n' \nmid q-1$, then there exists a normal element α of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that α and $\lambda_A(\alpha)$ are primitive unless (q,n) is one of the pairs* $(8,3)$, $(4,5)$, $(4,7)$, $(4,9)$, $(4,10)$, $(2,3)$, $(2,6)$, $(2,12)$, $(2,24)$, $(2,10)$, $(2,20)$, $(2,9)$, $(2,18)$, $(2,14)$, $(2,11)$, $(2,15)$.

Theorem 1.2 is now proved by combining Theorem 4.7 and Theorem 4.16.

In Table 3, γ denotes a primitive element of $\mathbb{F}_4$.

Acknowledgments

This work has been supported by CSIR, New Delhi, Govt. of India, under Grant F. No. 09/086(1145)/2012-EMR-1. The authors thank the referee for his valuable comments and suggestions.

References

[1] G.B. Agnew, R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone, An implementation for a fast public key cryptosystem, J. Cryptol. 3 (1991) 63–79.
[2] I.F. Blake, X.H. Gao, R.C. Mullin, S.A. Vanstone, T. Yaghoobian, Applications of Finite Fields, Kluwer Academic Publishers, Boston, Dordrecht, Lancaster, 1993.
[3] L. Carlitz, Primitive roots in a finite fields, Trans. Am. Math. Soc. 73 (3) (1952) 373–382.
[4] L. Carlitz, Some problems involving primitive roots in a finite field, Proc. Natl. Acad. Sci. USA 38 (4) (1952) 314–318.
[5] F.N. Castro, C.J. Moreno, Mixed exponential sums over finite fields, Proc. Am. Math. Soc. 128 (9) (2000) 2529–2537.
[6] W.S. Chou, S.D. Cohen, Primitive elements with zero traces, Finite Fields Appl. 7 (2001) 125–141.
[7] S.D. Cohen, Consecutive primitive roots in a finite field, Proc. Am. Math. Soc. 93 (2) (1985) 189–197.
[8] S.D. Cohen, Pair of primitive elements in fields of even order, Finite Fields Appl. 28 (2014) 22–42.
[9] S.D. Cohen, S. Huczynska, The primitive normal basis theorem – without a computer, J. Lond. Math. Soc. 67 (1) (2003) 41–56.
[10] S.D. Cohen, S. Huczynska, The strong primitive normal basis theorem, Acta Arith. 143 (4) (2010) 299–332.
[11] H. Davenport, Bases for finite fields, J. Lond. Math. Soc. 43 (1968) 21–39.

[12] 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.

[13] G. Kapetanakis, An extension of the (strong) primitive normal basis theorem, Appl. Algebra Eng. Commun. Comput. 25 (2013) 311–337.

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

[15] H.W. Lenstra Jr., R.J. Schoof, Primitive normal bases for finite fields, Math. Comput. 48 (1987) 217–231.

[16] Q. Liao, J. Li, K. Pu, On the existence for some special primitive elements in finite fields, Chin. Ann. Math. 37B (2016) 259–266.

[17] R. Lidl, H. Niederreiter, Finite Fields, 2nd edition, Cambridge University Press, Cambridge, 1997.

[18] J.L. Massey, J.K. Omura, Computational method and apparatus for finite field arithmetic, US Patent 4587627, May 6, 1986.

[19] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone, Computational method and apparatus for finite field multiplication, US Patent 4745568, May 17, 1988.

[20] T. Tian, W.F. Qi, Primitive normal element and its inverse in finite fields, Acta Math. Sin. 49 (3) (2006) 657–668.

[21] P.P. Wang, X.W. Cao, R.Q. Feng, On the existence of some specific elements in finite fields of characteristic 2, Finite Fields Appl. 18 (4) (2012) 800–813.