Pair of primitive elements with prescribed traces over finite fields

R. K. Sharma & Anju Gupta

To cite this article: R. K. Sharma & Anju Gupta (2019): Pair of primitive elements with prescribed traces over finite fields, Communications in Algebra, DOI: 10.1080/00927872.2018.1503283

To link to this article: https://doi.org/10.1080/00927872.2018.1503283

Published online: 17 Jan 2019.
Pair of primitive elements with prescribed traces over finite fields

R. K. Sharma and Anju Gupta
Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, India

Abstract
In this article, we establish a sufficient condition for the existence of a primitive element \( \alpha \in \mathbb{F}_{q^n} \) such that for any matrix \( \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2,3}(\mathbb{F}_q) \) of rank 2, the element \( (a \alpha^2 + b \alpha + c)/(d \alpha + e) \) is a primitive element of \( \mathbb{F}_{q^n} \), and \( \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \mu, \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^{-1}) = \nu \) for any prescribed \( \mu, \nu \in \mathbb{F}_q \), where \( q = 2^k \) for some positive integer \( k \). We establish existence of such elements for all pairs \( (q, n) \) \( (n \geq 7) \) except for finitely many pairs.

1. Introduction
Throughout the article, \( \mathbb{F}_q \) 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 cyclic multiplicative group \( \mathbb{F}_q^\times \) of \( \mathbb{F}_q \) is known as a primitive element of \( \mathbb{F}_q \). Any field \( \mathbb{F}_q \) contains \( \phi(q-1) \) primitive elements, where \( \phi \) is the Euler’s phi-function. A nonzero element \( \alpha \in \mathbb{F}_q^\times \) is primitive if and only if its minimal polynomial \( m_\alpha(x) \) over \( \mathbb{F}_q \) is primitive, that is, an irreducible polynomial of degree \( n \) and order \( q^n-1 \). For \( \alpha \in \mathbb{F}_{q^n} \), the trace, \( \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \), of \( \alpha \) is defined by \( \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{n-1}} \). The existence of a primitive polynomial with one or more of its coefficients prescribed has become an active area of research. Cohen [10] has completely resolved the problem of existence of a primitive element of \( \mathbb{F}_{q^n} \) with prescribed trace over \( \mathbb{F}_q \), that is, with the coefficient of \( x^{n-1} \) in \( m_\alpha(x) \) prescribed. Chou and Cohen [4] completely resolved the problem of the existence of a primitive element \( \alpha \) such that \( \alpha \) and \( \alpha^{-1} \) both have trace zero over \( \mathbb{F}_q \). The cases, when traces of \( \alpha \) and \( \alpha^{-1} \) are not both zero, are considered in [6].

We recall that a pair of the form \( (\alpha, f(\alpha)) \in \mathbb{F}_q \times \mathbb{F}_q \), for any rational function \( f(\alpha) \in \mathbb{F}_q(\alpha) \), is called a primitive pair in \( \mathbb{F}_q \) if both \( \alpha \) and \( f(\alpha) \) are primitive elements of \( \mathbb{F}_q \). A lot of work has been done in this direction. In 1985, Cohen [5] proved the existence of a primitive pair of the form \( (\alpha, \alpha + 1) \) in \( \mathbb{F}_q \), with \( q > 3, q \not\equiv 7 \mod 12 \) and \( q \not\equiv 1 \mod 60 \). Later, Cohen and Huczynska [9] 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 \( \alpha \) and \( \alpha^{-1} \) are primitive normal over \( \mathbb{F}_q \) except when \( (q, n) \) is one of the pairs \( (2, 3), (2, 4), (3, 4), (4, 3), (5, 4) \).

In 2012, Wang et al. [15] gave a sufficient condition for the existence of a primitive pair \( (\alpha, \alpha + \alpha^{-1}) \) for the case \( 2|q \). Liao et al. [14] generalized their results to the case when \( q \) is any prime power. In 2014, Cohen [7] completed the existence results obtained by Wang et al. [15] for
finite fields of characteristic 2. In [10], Cohen proved that if \( n \geq 2 \) is a natural number then for every \( a \in \mathbb{F}_q \), \( \mathbb{F}_{q^n} \) contains a primitive element \( \alpha \) such that \( Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = a \) except when \( a = 0 \) if \( n = 2 \) or \( (q, n) = (4, 3) \). In 2014, Cao and Wang [3] proved that for all \( q \) and \( n \geq 29, \mathbb{F}_{q^n} \) contains an element \( \alpha \) such that \( \alpha + \alpha^{-1} \) is primitive, and \( Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = a, Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^{-1}) = b \) for any pair of prescribed elements \( a, b \in \mathbb{F}_{q^n}^* \).

In [2], Anju and Sharma defined a rational expression \( \lambda_A(x) \in \mathbb{F}_{q^n}(x) \) by
\[
\lambda_A(x) = \frac{ax^2 + bx + c}{dx + e},
\]
for any matrix \( A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2 \times 3}(\mathbb{F}_{q^n}) \) of rank 2, and a subset \( \mathcal{M}_{q^n} \) of \( M_{2 \times 3}(\mathbb{F}_{q^n}) \) given by
\[
\mathcal{M}_{q^n} = \left\{ A = [a_{ij}] \in M_{2 \times 3}(\mathbb{F}_{q^n}) \mid a_{21} = 0, \text{ Rank}(A) = 2 \text{ and if } \lambda_A(x) = \beta x \text{ or } \beta x^2 \text{ for } \beta \in \mathbb{F}_{q^n} \text{ then } \beta = 1 \right\}.
\]

In the same paper, they proved the existence of a primitive pair of the form \( (\alpha, \lambda_A(\alpha)) \) in \( \mathbb{F}_{q^n} \), for each matrix \( A \in \mathcal{M}_{q^n} \) whenever \( k \neq 1, 2, 4 \). In this article, we study the existence of primitive pairs \( (\alpha, \lambda_A(\alpha)) \in \mathbb{F}_{q^n} \) \( (n \geq 7), q = 2^k \), with the more demanding conditions that \( Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \mu, Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^{-1}) = \nu \) for any prescribed \( \mu, \nu \in \mathbb{F}_q \).

Precisely, we prove following main result.

**Theorem 1.1.** Let \( q = 2^k \) for some positive integer \( k \), and \( n \geq 7 \) be an integer. Suppose \( A \in \mathcal{M}_{q^n} \). Then for every \( \mu, \nu \in \mathbb{F}_q \) there exists a primitive pair \( (\alpha, \lambda_A(\alpha)) \in \mathbb{F}_{q^n} \) such that \( Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \mu, Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^{-1}) = \nu \) unless \((q, n)\) is one of the pairs \((2, 24), (2, 20), (2, 18), (2, 16), (2, 15), (2, 14), (2, 12), (2, 11), (2, 10), (2, 9), (2, 8), (2, 7), (4, 12), (4, 11), (4, 10), (4, 9), (4, 8), (4, 7), (8, 10), (8, 8), (8, 7), (16, 9), (16, 8), (16, 7), (32, 8)\).

### 2. Preliminaries

Throughout the section, \( q \) is an arbitrary prime power. For \( r | (q - 1) \), an element \( \xi \in \mathbb{F}_q^* \) is called \( r \)-free if \( \xi = \beta^s \) for any \( s | r \), and \( \beta \in \mathbb{F}_q \) implies \( s = 1 \). Hence an element \( \alpha \in \mathbb{F}_q^* \) is primitive if and only if it is \((q - 1)\)-free. Next, we define character of a finite abelian group.

**Definition 1.** A homomorphism \( \chi \) of a finite abelian group \( G \) into the multiplicative group \( U \) of complex numbers of absolute value 1 is called a character of \( G \). The set of all characters of \( G \) is denoted by \( \hat{G} \), and forms a group under multiplication. Also \( G \cong \hat{G} \). Furthermore, the character \( \chi_1 \) defined by \( \chi_1(g) = 1 \) 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 \( \mathbb{F}_{q^n}^* \) are called multiplicative characters. Every nontrivial additive character \( \psi \) of a finite field \( \mathbb{F}_q \) lifts to an additive character \( \tilde{\psi} \) of \( \mathbb{F}_{q^n}, n \geq 1 \), by \( \tilde{\psi}(x) = \psi(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)) \) for every \( x \in \mathbb{F}_{q^n} \). 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 \( \hat{\mathbb{F}_q^*} \cong \hat{\mathbb{F}_q} \), we have that \( \hat{\mathbb{F}_q^*} \) is cyclic. For any \( r | (q - 1) \), \( \chi_r \) denotes a multiplicative character of order \( r \), which are \( \phi(r) \) in number. Following Cohen and Huczynska [9, 8], it can be shown that for any \( m | (q - 1) \)
\[
\rho_m : \chi \mapsto \theta(m) \sum_{r|m} \frac{\mu(r)}{\phi(r)} \sum_{\chi_r} \chi_r(x),
\]
where $\theta(m) := \frac{\varphi(m)}{m}$, $\mu$ is the Möbius function and the internal sum runs over all multiplicative characters $\chi_r$ of order $r$, gives an expression of the characteristic function for the subset of $m$-free elements of $\mathbb{F}_q^*$. An expression of the characteristic function for the set of elements in $\mathbb{F}_q^n$ with $\text{Tr}_{\mathbb{F}_q^n}[x] = t \in \mathbb{F}_q$ is given by

$$\tau_t(x) = \frac{1}{q} \sum_{\psi \in \mathbb{F}_q} \psi(\text{Tr}_{\mathbb{F}_q^n}(x) - t).$$

Further, every additive character $\psi$ of $\mathbb{F}_q$ can be obtained by $\psi(x) = \psi_0(ux)$, where $\psi_0$ is the canonical additive character of $\mathbb{F}_q$ and $u$ is any element of $\mathbb{F}_q$. Thus

$$\tau_t(x) = \frac{1}{q} \sum_{u \in \mathbb{F}_q} \psi_0(\text{Tr}_{\mathbb{F}_q^n}(ux) - ut) = \frac{1}{q} \sum_{u \in \mathbb{F}_q} \psi_0(ux)\psi_0(-ut).$$

Now, we give some lemmas which will be used in our main results.

**Lemma 2.1.** [11, Theorem 5.5] Let $f(x) \in \mathbb{F}_q(x)$ be a rational function. Write $f(x) = \prod_{i=1}^{k} f_i(x)^{n_i}$, where $f_i(x) \in \mathbb{F}_q[x]$ are irreducible polynomials and $n_i$ are nonzero integers. Let $\chi$ be a multiplicative character of $\mathbb{F}_q$. Suppose that the rational function $f(x)$ is not of the form $h(x)^{\text{ord}(\chi)}$ in $\mathbb{F}_q(x)$, where $\text{ord}(\chi)$ is the smallest integer $r$ such that $\chi^r = \chi_1$. Then we have

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq \left( \sum_{j=1}^{k} \deg(f_j) - 1 \right) q^{1/2}.$$

**Lemma 2.2.** [11, Theorem 5.6] Let $f(x), g(x) \in \mathbb{F}_q^n(x)$ be rational functions. Write $f(x) = \prod_{i=1}^{k} f_i(x)^{n_i}$, where $f_i(x) \in \mathbb{F}_q^n[x]$ are irreducible polynomials and $n_i$ are nonzero integers. Let $\chi$ be a multiplicative character of $\mathbb{F}_q^n$, and let $\psi$ be a non-trivial additive character of $\mathbb{F}_q^n$. Suppose that $g(x)$ is not of the form $r(x)^{\text{ord}(\chi)} - r(x)$ in $\mathbb{F}_q^n(x)$. Then

$$\left| \sum_{x \in \mathbb{F}_q^n} \chi(f(x))\psi(g(x)) \right| \leq (n_1 + n_2 + n_3 + n_4 - 1)q^{n/2},$$

where $n_1 = \sum_{j=1}^{s} \deg(f_j)$, $n_2 = \max(\deg(g), 0)$, $n_3$ is the degree of the denominator of $g(x)$ and $n_4$ is the sum of degrees of those irreducible polynomials dividing the denominator of $g$, but distinct from $f_j(x)$ ($j = 1, ..., s$).

Throughout the rest of the article, we shall use the notation $\omega(m)$ for the number of distinct prime divisors of $m$, for any integer $m>1$. Also the number of square free divisors of $m$ is denoted by $W(m)$, that is, $W(m) = 2^{\omega(m)}$.

### 3. Main result

Let $q = 2^k$, for some positive integer $k$ and $A \in \mathbb{N}_{q^*}$. In this section, we show the existence of primitive pairs $(\alpha, \lambda_A(\alpha))$ in $\mathbb{F}_q^n$ for each $A \in \mathbb{N}_{q^*}$, such that $\text{Tr}_{\mathbb{F}_q^n}[\mathbb{F}_q^n(\alpha) = \mu]$, $\text{Tr}_{\mathbb{F}_q^n}[\mathbb{F}_q^n(\alpha^{-1})] = \nu$ for any prescribed $\mu, \nu \in \mathbb{F}_q$. Let $e_1$, $e_2$, $(q^n-1)$ and $N_{A,q,n}(e_1, e_2, \mu, \nu)$ be the number of $\alpha \in \mathbb{F}_q^n$, such that $\alpha$ is $e_1$-free and $\lambda_A(\alpha)$ is $e_2$-free, and $\text{Tr}_{\mathbb{F}_q^n}[\mathbb{F}_q^n(\alpha) = \mu]$, $\text{Tr}_{\mathbb{F}_q^n}[\mathbb{F}_q^n(\alpha^{-1})] = \nu$. Hence we need to show that $N_{A,q,n}(q^n-1, q^n-1, \mu, \nu)>0$, for all $A \in \mathbb{N}_{q^*}$ and $\mu, \nu \in \mathbb{F}_q$. Let $P$ be the set of $(q, n)$ such that $N_{A,q,n}(q^n-1, q^n-1, \mu, \nu)>0$ for all $A \in \mathbb{N}_{q^*}$ and $\mu, \nu \in \mathbb{F}_q$. 


Lemma 3.1. Let $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in \mathbb{M}_q$ be such that $\lambda_A(x) = x$ or $x^2$. Then $N_{A,q,n}(q^n-1, q^n-1, \mu, \nu) > 0$ except when $(q, n) = (2, 6), (4, 5)$.

Proof. As $q^n-1$ is odd, $x^2$ is primitive if $x$ is primitive. Hence the problem is reduced to the problem of existence of a primitive element $\alpha$ such that $Tr_{\mathbb{F}_q[\alpha]}(x) = \mu$ and $Tr_{\mathbb{F}_q[\alpha]}(x^{-1}) = \nu$. Thus, by Theorem 1.1 of [6], we get that the result is true except when $(q, n) = (2, 6), (4, 5)$.

Lemma 3.2. Let $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in \mathbb{M}_q$ be such that $\lambda_A(x) \neq \lambda x, \lambda x^2$ for any $\lambda \in \mathbb{F}_q$, and $l_1, l_2 | (q^n-1)$. If $q^{n/2-2} > 5W(l_1)W(l_2)$ then $N_{A,q,n}(l_1, l_2, \mu, \nu) > 0$ for all $\mu, \nu \in \mathbb{F}_q$.

Proof. By definition

$$N_{A,q,n}(l_1, l_2, \mu, \nu) = \sum_{\alpha \in \mathbb{F}_q} \rho_{l_1}(\alpha) \rho_{l_2}(\lambda_A(\alpha)) \tau_\mu(\alpha) \tau_\nu(\alpha^{-1}),$$

where $S = \{ \alpha \in \mathbb{F}_q | a\alpha^2 + b\alpha + c = 0 \text{ or } d\alpha + e = 0 \text{ or } \alpha = 0 \}$. Now (2) gives

$$N_{A,q,n}(l_1, l_2, \mu, \nu) = \theta(\alpha_{l_1}) \theta(\alpha_{l_2}) \sum_{d_1, d_2 | l_1, l_2} \mu(d_1) \mu(d_2) \sum_{l_{d_1}, l_{d_2}} \chi_A(l_{d_1}, l_{d_2}, \mu, \nu)$$

where, $\chi_A(l_{d_1}, l_{d_2}, \mu, \nu) = \sum_{u,v \in \mathbb{F}_q} \psi_0(-\mu u - \nu v) \sum_{x \in \mathbb{F}_q, x = S} \chi_{d_1}(x) \chi_{d_2}(\lambda_A(\alpha)) \hat{\psi}_0(ux + vx^{-1})$. As $\chi_{d_1}(x) = \chi_{q^{-d_1}}(x^{q^n})$ for some $n_i \in \{0, 1, 2, \ldots, q^n-2\}$, we get

$$\chi_A(l_{d_1}, l_{d_2}, \mu, \nu) = \sum_{u,v \in \mathbb{F}_q} \psi_0(-\mu u - \nu v) \sum_{x \in \mathbb{F}_q, x = S} \chi_{q^{-d_1}}(ax^2 + bx + c)^{n_1}(dx + e)^{-n_2} \hat{\psi}_0(ux + vx^{-1})$$

$$= \sum_{u,v \in \mathbb{F}_q} \psi_0(-\mu u - \nu v) \sum_{x \in \mathbb{F}_q, x = S} \chi_{q^{-d_1}}(f(x)) \hat{\psi}_0(g(x)),$$

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

If $g(x) \neq H^{n_1}_x - h$ for any $h \in \mathbb{F}_q(x)$ then using Lemma 2.2, we get

$$|\chi_A(l_{d_1}, l_{d_2}, \mu, \nu)| \leq 5q^{n/2+2}.$$

Next assume $g(x) = H^{n_1}_x - h$ for any $h = \frac{h_1(x)}{h_2(x)} \in \mathbb{F}_q(x)$, where $h_1$ and $h_2$ are co-prime polynomials over $\mathbb{F}_q$. Then we get

$$(ux^2 + v)H^{n_1}_{d_2} = (H^{n_1}_{d_2} - H^{n_1}_{d_2} - h_1)x.$$

This gives that $h_1(x)(H^{n_1}_{d_2} - H^{n_1}_{d_2} - h_1)x$, but gcd$(H^{n_1}_{d_2}, H^{n_1}_{d_2} - h_1) = 1$. Hence $h_1(x)|x$, which is possible only if $h_2$ is constant. Hence from (4), we get

$$ux^2 + v = y^{-1}(H^{n_1}_{d_2} - y^{n_1} - h_1)x,$$

where $y = h_2$. Now (5) is possible only if $v = 0$. Putting this back in (5), we get $ux = y^{-1}(H^{n_1}_{d_2} - y^{n_1} - h_1)$, which is possible only if $u = 0$ and $h_1$ is a constant. If additionally $f(x) \neq H^{n_1}_x - h$ for any $H \in \mathbb{F}_q(x)$ then using Lemma 2.1

$$|\chi_A| \leq 3q^{n/2+2}.$$

Assume $f = H^{n_1}_x - h$ for some $H \in \mathbb{F}_q(x)$. Let $H(x) = \frac{H_1(x)}{H_2(x)}$ for any $H_1(x), H_2(x) \in \mathbb{F}_q[x]$ with gcd$(H_1(x), H_2(x)) = 1$. Then
Lemma 3.4. Let \( l \) denote \( qn \) if \( n \) is odd but not \( l \). Assume \( \chi_{r,l} \) from the proof of \([2, \text{Lemma } 3.2, \text{Lemma } 3.3]\) that \( \chi_{r,l} \) is a constant. Hence \( x_{n_1}^{n_2} (ax^2 + bx + c)^{n_1} = (dx + e)^{n_2} H_1(x)^{n_1} \Rightarrow H_2(x)^{n_1} x_{n_1}^{n_2} (ax^2 + bx + c)^{n_1} = (dx + e)^{n_2} H_1(x)^{n_2} \Rightarrow H_2(x)^{n_1} (dx + e)^{n_2} H_1(x)^{n_1} \).

But \( \gcd(H_1(x), H_2(x)) = 1 \). Hence \( H_2(x)^{n_1} (dx + e)^{n_2} \), which is possible only if \( H_2(x) \) is a constant. Hence \( x_{n_1}^{n_2} (ax^2 + bx + c)^{n_1} = y^{n_1-1} (dx + e)^{n_2} H_1(x)^{n_1} \) where \( y' = H_2(x) \in \mathbb{F}_q \). Now it follows from the proof of \([2, \text{Lemma } 3.2, \text{Lemma } 3.3]\) that \( n_1 = n_2 = 0 \). Hence if \( (\chi_{d_1}, \chi_{d_2}, u, v) \neq (\chi_1, \chi_1, 0, 0) \) then

\[
|\mathcal{A}(\chi_{d_1}, \chi_{d_2}, \mu, v)| \leq 5q^{n/2+2}.
\]

Using this in (3), we get

\[
N_{A,q,n}(l_1, l_2, \mu, \nu) \geq \frac{\theta(l_1)\theta(l_2)}{q^2} \left( q^n - 4 - 5q^{n/2+2} (W(l_1)W(l_2) - 1) \right).
\]

From (6), we see that \( N_{A,q,n}(l_1, l_2, \mu, \nu) > 0 \) if \( q^{n/2-2} > 4q^{-n/2-2} + 5(W(l_1)W(l_2) - 1) \), i.e., if \( q^{n/2-2} > 5W(l_1)W(l_2) \).

Hence from the Lemmas 3.1 and 3.2, we see that \( (q, n) \in P \) if

\[
q^{n/2-2} > 5W(q^n - 1)^2.
\]

Next we obtain an extension of the sieving Lemma 3.7 of \([7]\). The proof is similar to that of Proposition 5.2 of \([13]\), hence omitted.

**Lemma 3.3.** Let \( l \mid (q^n - 1) \) and \( p_1, \ldots, p_s \) be all the primes dividing \( q^n - 1 \) but not \( l \). Then for any \( \mu, \nu \in \mathbb{F}_q \)

\[
N_{A,q,n}(l^n - 1, l^n - 1, \mu, \nu) \geq \sum_{i=1}^{s} N_{A,q,n}(l^n - 1, l^n - 1, \mu, \nu) + \sum_{i=1}^{s} N_{A,q,n}(l^n - 1, l^n - 1, \mu, \nu) - (s-1)N_{A,q,n}(l^n - 1, \mu, \nu).
\]

In the next Lemma, we give upper bounds for the absolute values of \( N_{A,q,n}(l^n - 1, \mu, \nu) - 0 \) and \( N_{A,q,n}(l^n - 1, \mu, \nu) - 0 \).

**Lemma 3.4.** Let \( l \mid (q^n - 1) \) and \( r \) any prime dividing \( q^n - 1 \) but not \( l \). Then

\[
|N_{A,q,n}(l^n - 1, \mu, \nu) - 0| \leq \frac{4 \theta(l)^2 \theta(r)}{q} W(l)^2 q^{n/2+2}.
\]

Also

\[
|N_{A,q,n}(l^n - 1, \mu, \nu) - 0| \leq \frac{4 \theta(l)^2 \theta(r)}{q} W(l)^2 q^{n/2+2}.
\]

**Proof.** Proof follows on the lines of \([12, \text{Lemma } 3.2]\), hence omitted.

Next Lemma gives an improved criterion for \( (q, n) \) to be a member of \( P \).

**Theorem 3.5.** Let \( l \mid (q^n - 1) \) and \( \{p_1, p_2, \ldots, p_s\} \) be the collection of all the primes dividing \( q^n - 1 \), but not \( l \). Assume \( \delta = 1 - 2 \sum_{i=1}^{s} \frac{1}{p_i} \) and \( \Delta = \frac{2\delta - 1}{\delta} + 2 \). Also assume \( \delta > 0 \). If

\[
q^{n/2-2} > 5W(l)^2 \Delta
\]

Then \( (q, n) \in P \).
then

\[(q, n) \in P.\]

**Proof.** Proof is similar to that of Theorem 3.4 of [12]. \qed

### 3.1. Computations

Clearly, \((q, 1) \notin P\) as in that case \(\text{Tr}_{F_q/F_p}(\alpha) = \alpha, \text{Tr}_{F_q/F_p}(\alpha^{-1}) = \alpha^{-1}\). Hence for \((q, 1)\) to be in \(P\) every pair \((\alpha, \lambda_A(\alpha))\) in \(F_q\) must be primitive, which is not possible as \((0, \lambda_A(0))\) is not a primitive pair in \(F_q\).

Also for \(n = 2, 3, 4\), there does not exist any primitive element in \(F_{q^n}\) such that \(\text{Tr}_{F_{q^n}/F_q}(\alpha) = \text{Tr}_{F_{q^n}/F_q}(\alpha^{-1}) = 0\). As if there exists such a primitive element then in its minimal polynomial coefficients of \(\alpha^{n-1}\) and \(\alpha\) are both zero. For example, let \(\alpha\) be such a primitive element in \(F_{q^n}\). Then for \(n = 2\) its minimal polynomial is of the form \(\alpha^2 + u\) over \(F_q\). Hence, order of \(\alpha\) is a divisor of \(2(q-1)\). Similarly, for \(n = 3\), its order is a divisor of \(3(q-1)\) and for \(n = 4\), its order is a divisor of \(2(q^2-1)\). Thus, we assume that \(n \geq 5\). In this article, we consider the cases \(n \geq 7\). The cases \(n = 5, 6\) have been tried using extensive computation. It appears they require altogether a different approach, and hence are left as open problems.

In this section, we use \(\omega\) to denote \(\omega(q^n-1)\) and \(R\) to denote the value on the right hand side of (9).

**Lemma 3.6.** If \(m > 5 \cdot 4 \times 10^{39}\) is odd, then \(W(m) < m^{1/5}\).

**Proof.** If \(m > 5 \cdot 4 \times 10^{39}\) then \(m^{1/5} > 2^{26}\). Hence if \(\omega(m) \leq 26\) then \(W(m) < m^{1/5}\). So assume \(\omega(m) > 26\). Set \(m = m_1 m_2\), where prime divisors of \(m_1\) are the smallest 26 primes dividing \(q^n-1\) and that of \(m_2\) are the remaining \(\omega(m) - 26\) prime divisors of \(q^n-1\). So \(m_1 > 3 \cdot 5 \cdot 1039\) and \(m_2 > 107 \cdot 109 \cdots \omega(m)\)th odd prime. Then, \(W(m) = 2^{\omega(m)} W(m_1) W(m_2)\). Since \(m_1 > 5 \cdot 4 \times 10^{39}\), \(W(m_1) = 2^{26} < m_1^{1/5}\). Also \(W(m_2) \leq m_2^{1/5}\), as if \(p'\) is any prime dividing \(m_2\) then \(p'^{1/5} > 2\). So \(W(m) < m_1^{1/5} m_2^{1/5} < m^{1/5}\). \qed

**Theorem 3.7.** Suppose \(q = 2^k\) for some positive integer \(k\), and \(n \geq 27\). Then \((q, n) \in P\).

**Proof.** If \(q \geq 32\) and \(n \geq 27\) then \(q^n-1 > 5 \cdot 4 \times 10^{39}\). Hence, by Lemma 3.6, \(W(q^n-1) < q^{n/5}\). Using this in (7), we see that \((q, n) \in P\) if \(q^{n/10} > 2\), which is true for \(q \geq 32\) and \(n \geq 27\). Now suppose that \(2 \leq q \leq 16\). Also let \(n(q)\) be the least positive integer such that \(q^{n(q)} > 5 \cdot 4 \times 10^{39}\). Then, \(n(16) = 33, n(8) = 44, n(4) = 66\) and \(n(2) = 132\). For \(n \geq n(q)\), we see that \(q^{n/10} > 2\). For \(q = 2, 4, 8, 16, 27 \leq n < n(q)\), factorizing \(q^n-1\), we see that (7) is satisfied except for \(q = 2\) and \(n = 36, 30, 28\). For these, we see that (9) is satisfied by appropriate choices of \(l\) (see Table 1). \qed

**Theorem 3.8.** Let \(q = 2^k\) for some positive integer \(k\), and \(7 \leq n \leq 26\) be an integer. Then for every \(\mu, \nu \in F_q\) there exists a primitive pair \((\alpha, \lambda_A(\alpha))\) in \(F_q\) such that \(\text{Tr}_{F_q/F_p}(\alpha) = \mu, \text{Tr}_{F_q/F_p}(\alpha^{-1}) = \nu\) if \((q, n)\) is not one of the pairs \((2, 24), (2, 20), (2, 18), (2, 16), (2, 15), (2, 14), (2, 12), (2, 11), (2, 10), (2, 9), (2, 8), (2, 7), (4, 12), (4, 11), (4, 10), (4, 9), (4, 8), (4, 7), (8, 10), (8, 8), (8, 7), (16, 9), (16, 8), (16, 7), (32, 8)\).

**Proof.** Here (7) is satisfied if \(k > \frac{4 \omega + 5}{n-1}\). If \(\omega \geq 321\) then

\[q^n > 3 \cdot 5 \cdots 2137 \cdot 2^{2k(\omega-321)},\]
which gives \( nk > 3006 + \frac{28}{3} \omega - 2996 \), that is, \( nk > \frac{28}{3} \omega + 12 \). But \( k > \frac{2\omega+12}{n} > \frac{4\omega+5}{n+4} \) for \( n \geq 7 \). Thus we may assume \( 51 \leq \omega \leq 320 \). Let \( l \) be the product of smallest 24 primes dividing \( q^n - 1 \). Then, \( s \leq 296 \). Now minimum value of \( \delta \) is obtained by taking \( s = 296 \) and replacing \( \{p_1, p_2, \ldots, p_s\} \) by the primes from 101 (25th odd prime) to 2131 (320th odd prime), that is, \( \delta > 0.003327 \) and \( R < 2.5000539 \times 10^{20} \). Hence (9) is satisfied if \( q > R^{2/(n-4)} \), that is (at worst \( n = 7 \)) if \( q > R^{2/3} \). Hence if \( q > 3.96856 \times 10^{13} \). So \( q > 1.550353 \times 10^{95} \) suffices. Now as \( \omega \geq 51, q^n > 5.31 \times 10^{95} \). Thus, \((q, n) \in P\) if \( \omega \geq 51 \).

Proceeding in the same way as above for the cases \( 27 \leq \omega \leq 50 \) with \( \omega(l) = 8 \), and \( 22 \leq \omega \leq 26 \) with \( \omega(l) = 5 \) we see that \((q, n) \in P\) in these cases too.

Hence, we may assume that \( \omega \geq 21 \). Proceeding as above, with \( \omega(l) = 5 \), we get \( R < 1071224 \). Hence (7) is satisfied for \( q > 10469 \) whenever \( n = 7 \), and \( q > 1034 \) whenever \( n \geq 8 \). From here onwards, we separate the cases \( n = 7 \) and \( n \geq 8 \).

**Case 1:** If \( n \geq 8 \) then with \( 18 \leq \omega \leq 21 \), (9) is satisfied if \( q > 1034 \), that is, if \( q^n > 1.306666 \times 10^{24} \). Since \( \omega \geq 18, q^n > 3.92916 \times 10^{24} \). Hence \((q, n) \in P\) for \( \omega \geq 18 \). For \( \omega = 17 \), proceeding as above with \( \omega(l) = 4 \), we see that (9) is satisfied. Hence, we may assume that \( 4 \leq \omega \leq 16 \). In this case, with \( \omega(l) = 4 \), we get \( \delta > 0.13927 \) and \( R < 213944.99777 \). Hence (9) is satisfied whenever \( q > 462 > 256 \) for \( n = 8 \); whenever \( q > 135 \) for \( n = 9 \); whenever \( q > 59 \) for \( n = 10 \); whenever \( q > 33 \) for \( n = 11 \); whenever \( q > 21 \) for \( n = 12 \); whenever \( q > 15 \) for \( n = 13, 14, 15 \); whenever \( q > 4 \) for \( 16 \leq n \leq 26 \). For these remaining values of \( q \) and \( n \), we factorize \( q^n - 1 \) and see that (9) is satisfied by these pairs \((q, n)\), for appropriate choices of \( l \), except the pairs \((2, 8), (4, 8), (8, 8), (16, 8), (32, 8), (2, 9), (4, 9), (16, 9), (2, 10), (4, 10), (8, 10), (2, 11), (4, 11), (2, 12), (4, 12), (2, 13), (2, 15), (2, 16), (2, 18), (2, 20), (2, 24)\) (refer to Table 1).

**Case 2:** If \( n = 7 \), we may assume that \( \omega \leq 21 \) and \( q \leq 10469 \). Let \( m = \frac{q^r - 1}{q-1} \). Let \( S \) be the set consisting of 7 and prime numbers which are congruent to 1 modulo 13, that is,
$S = \{7, 15, 29, 43, \ldots\}$. Then prime divisors of $m$ are in $S$. Moreover $\gcd(m, q-1) = 1$ or 7. Again let $P_r$ be the product of $r$ smallest odd primes, $Q_t$ be the product of $t$ smallest prime numbers from $S$, which are possible divisors of $m$, $s_1 = \omega(q-1)$, and $s_2 = \omega(m)$.

First let $q \equiv 1 \pmod{7}$. Then, $\omega = s_1 + s_2 - 1 \leq 21$. Since $q \leq 10469, s_1 \leq 6$. If $4 \leq s_1 \leq 6$, then $s_2 \leq 18$. Let $l$ be the product of smallest 4 primes dividing $q - 1$. Then, minimum value of $\delta$ is obtained by taking $s = 17$ and $\{p_1, p_2, \ldots, p_3\}$, the primes 13,17 and the primes between 29 to 547 (inclusive) from the set $S$. Hence $\delta > 0.4838$ and $R < 89869$. Thus, (9) is satisfied if $q > 2007$, that is, if $q^2 > 1.3116 \times 10^{23}$. But if $s_1 \geq 4$, then $q > 1155$, which gives $q \geq 2048$ and hence $(q, 7) \in P$.

Now we can assume that $1 \leq s_1 \leq 3$ and $s_2 \leq 21$. Proceeding as above with $l = q - 1$, we get $\delta > 0.7429$ and $R < 17440$. Thus (9) is satisfied if $q > 672$, that is, if $q_6 > 6.221335 \times 10^{19}$. As $q > Q_1^{1/6} - 1, s_2 \geq 9$ implies that $q > Q_1^{1/6} - 1 > 699$. Hence we may assume that $1 \leq s_2 \leq 8$. In this case, with $l = q - 1$, we get $\delta > 0.80327$ and $R < 5819$. Thus (9) is satisfied for $q > 323 > 256$.

Next we assume that $q \equiv 1 \pmod{7}$. Then $\omega = s_1 + s_2 \leq 21$. If $4 \leq s_1 \leq 6$ then $s_2 \leq 17$. Let $l$ be the product of smallest 4 primes dividing $q - 1$. Then, as in the previous cases, it follows that $\delta > 0.536$ and $R < 81366$. Thus (9) is true if $q > 1877$. Since $s_1 \geq 4, q > 3 \cdot 5 \cdot 11 \cdot 13 = 2145$. Hence, we may assume that $s_1 \leq 3$ and $s_2 \leq 21$. Again with $l = q - 1$ and $s = 21$, we get $\delta > 0.74005$ and $R < 18368.5319$. Thus (9) is satisfied if $q > 696$. Now if $s_2 \geq 9$ then $q > Q_1^{1/6} - 1 > 1234$. Hence, we may assume that $s_2 \leq 8$. Then, proceeding as above with $l = q - 1$, we get $R < 6679$. Thus (9) is satisfied for $q > 354 > 256$.

For $q \leq 256$, we factorize $q^2 - 1$ and observe that (9) is satisfied by $q = 256, 128, 64, 32$ for appropriate choices of $l$ (see Table 1). Hence the result follows.

Combining Theorem 3.7, and Theorem 3.8, we get main theorem of this paper Theorem 1.1.

Remark 1. Cohen [6] has proved that primitive pairs of the form $(x, x^{-1})$ with $Tr_{F_q/F_q}(x)$ and $Tr_{F_q(F_q^2)}(x^{-1})$ arbitrarily prescribed exist in $F_q^{\omega}$ for all the pairs $(q, n)$ except $(2, 6), (4, 5), (3, 6)$. For the pairs listed in Theorem 1.1, we have computationally verified the result using GAP 4r8 [1], for the pairs of the form $(x, x + x^{-1})$ and seen that for all the pairs $(q, n)$ except $(2, 6), (2, 8), (4, 5), F_q^{\omega}$ contains such primitive pairs.

From the above remark, we see that $(q, n) = (2, 8)$ is an actual exception as in that case for $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $F_q^{\omega}$ does not contain any primitive element $x$ such that $A(x)$ is also primitive and $Tr_{F_q(F_q^2)}(x) = 0$ and $Tr_{F_q(F_q^2)}(x^{-1}) = 1$.

For the remaining pairs listed in Theorem 1.1, we have computationally verified the result using GAP4r8 [1] and the code has run for sufficiently large time without throwing any exception. Accordingly, we formulate the following conjecture.

Conjecture 1. Let $q = 2^k$ for some positive integer $k$, and $n \geq 7$ be an integer. Suppose $A \in \mathfrak{W}_{F_q}$. Then for every $\mu, \nu \in F_q$ there exists a primitive pair $(x, A(x))$ in $F_q^{\omega}$ such that $Tr_{F_q(F_q^2)}(x) = \mu$, and $Tr_{F_q(F_q^2)}(x^{-1}) = \nu$ except when $(q, n) = (2, 8)$.

Acknowledgement

The authors would like to show their gratitude to Prof. S. D. Cohen for his valuable comments and suggestions in this direction.

Funding

The first author R. K. Sharma is thankful to MATRICS (DST-SERB), Project Grant No. MTR/2017/000736 for the support extended. This work has also been supported by CSIR, New Delhi, Govt. of India, Under Grant No. F.No. 09/086(1145)/2012-EMR-1.
References