International Journal of Mathematics And its Applications
Volume 5, Issue 2–B (2017), 265–268.
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of Mathematics And its Applications

On Special Primitive Elements over Finite Fields

Research Article

Anju[1] and Meenu Khatkar[1]*

1 Department of Mathematics, Indian Institute of Technology Delhi, Hauz Khas, New Delhi, India.

Abstract: Let $\mathbb{F}_{q^n}$ be an extension of the field $\mathbb{F}_q$ of degree n, where $q = p^k$ for some prime p and positive integer k. In this article, we establish a sufficient condition for the existence of a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that $\alpha^2 + \alpha + 1$ is also primitive and $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a$ for any $a \in \mathbb{F}_q$.

MSC: 12E20, 11T23.

Keywords: Finite Fields, Primitive Element, Characters.

1. Introduction

Let $\mathbb{F}_q$ 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. The multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is cyclic and its generators are called *primitive elements* of $\mathbb{F}_q$. Any field $\mathbb{F}_q$ has $\phi(q-1)$ primitive elements, where ϕ is the Euler's phi-function. For $\alpha \in \mathbb{F}_{q^n}$, the *trace* $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)$ of α is defined by $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^n-1}$.

In 1985, Cohen [5] considered the problem of existence of two consecutive primitive elements in $\mathbb{F}_q$. Chou and Cohen [4] completely resolved the question of the existence of a primitive element α such that α and α^{-1} both have trace zero over $\mathbb{F}_q$. He and Han [8] studied primitive elements of the form $\alpha + \alpha^{-1}$ over finite fields. In 2012, Wang et al. [11] established a sufficient condition for the existence of α such that α and $\alpha + \alpha^{-1}$ are both primitive for the case $2|q$. Liao et al. [9] generalized their results to the case when q is any prime power. In 2014, Cao and Wang [2] proved that for all q and $n \geq 29$, $\mathbb{F}_{q^n}$ contains an element α such that $\alpha + \alpha^{-1}$ ia also 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 $a, b \in \mathbb{F}_q^*$.

In this article, we consider the existence of a primitive pair $(\alpha, \alpha^2 + \alpha + 1)$ in $\mathbb{F}_{q^n}$ with $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a$ for any prescribed $a \in \mathbb{F}_q^*$.

2. Preliminaries

We denote the number of prime divisors of m by $\omega(m)$, for any positive integer $m > 1$. For the basics on the character groups of the additive group and the multiplicative group of finite fields, the reader is referred to [10].

* E-mail: meenukhatkar@gmail.com

Definition 2.1. *An element $\alpha \in \mathbb{F}_q^*$ is called e-free, for any $e|q-1$, if $\alpha = \gamma^d$ 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.*

Since $\widehat{\mathbb{F}_q^*}$ is cyclic, for any $d|q-1$, $\mathbb{F}_q^*$ has $\phi(d)$ multiplicative characters χ_d of order d. Following Cohen and Huczynska [6, 7], it can be shown that for any $m|q-1$, an expression of the characteristic function for the subset of m-free elements of $\mathbb{F}_q^*$ is given by

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

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.

If ψ is a nontrivial additive character of a finite field $\mathbb{F}_q$ then ψ lifts to an additive character $\hat{\psi}$ of $\mathbb{F}_{q^n}$, $n \geq 1$, by setting: $\hat{\psi}(\alpha) = \psi(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha))$ for every $\alpha \in \mathbb{F}_{q^n}$.

An expression of the characteristic function for the set of elements in $\mathbb{F}_{q^n}$ with $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a \in \mathbb{F}_q$ is given by,

$$T_a : \alpha \mapsto \frac{1}{q} \sum_{\psi \in \widehat{\mathbb{F}_q}} \psi(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) - a).$$

For every $\alpha \in \mathbb{F}_{q^n}$, we have that

$$T_a(\alpha) = \frac{1}{q} \sum_{\psi \in \widehat{\mathbb{F}_q}} \psi(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) - a).$$

Every additive character $\psi \in \widehat{\mathbb{F}_q}$ can be obtained by $\psi(\alpha) = \psi_g(u\alpha)$, where ψ_g is the canonical additive character of $\mathbb{F}_q$ and u is any element of $\mathbb{F}_q$. Hence

$$\begin{aligned} T_a(\alpha) &= \frac{1}{q} \sum_{u \in \mathbb{F}_q} \psi_g(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(u\alpha) - ua) \\ &= \frac{1}{q} \sum_{u \in \mathbb{F}_q} \hat{\psi}_g(u\alpha)\psi_g(-ua). \end{aligned} \tag{1}$$

Next, we give some Lemmas, which are useful for our main results.

Lemma 2.2 ([10, 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 2.3 ([3])**.** *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. Main Result

Let $N_{q^n}(m_1, m_2, a)$ be the number of $\alpha \in \mathbb{F}_{q^n}$, such that α is m_1 free and $\alpha^2+\alpha+1$ is m_2 free and $Tr(\alpha) = a$ for any $a \in \mathbb{F}_q$. Hence we need to show that $N_{q^n}(m_1, m_2, a) > 0$ for every $a \in \mathbb{F}_q$.

Theorem 3.1. *Let $q = p^k$ for some prime $p \neq 3$ and n be a positive integer and let $\omega = \omega(q^n - 1)$. If $q^{\frac{n}{2}-1} > 3 \cdot 2^{2\omega}$, then $N_{q^n}(m_1, m_2, a) > 0$ for every $a \in \mathbb{F}_q$.*

Proof. By definition

$$\begin{aligned}
N_{q^n}(q^n-1, q^n-1, a) &= \sum_{\alpha \in \mathbb{F}_{q^n}^*} \rho_{q^n-1}(\alpha)\rho_{q^n-1}(\alpha^2+\alpha+1)T_a(\alpha) \\
&= \frac{\theta(q^n-1)^2}{q} \sum_{\alpha \in \mathbb{F}_{q^n}^*} \sum_{d_1, d_2 | q^n-1} \frac{\mu(d_1)\mu(d_2)}{\phi(d_1)\phi(d_2)} \sum_{\chi_{d_1}, \chi_{d_2}} \chi_{d_1}(\alpha)\chi_{d_2}(\alpha^2+\alpha+1) \\
&\quad \sum_{v \in \mathbb{F}_q} \hat{\psi}_g(v\alpha)\psi_g(-va).
\end{aligned}$$

$$N_a(q^n-1, q^n-1, a) = \frac{\theta(q^n-1)^2}{q} \sum_{d_1, d_2 | q^n-1} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\chi_{d_1}, \chi_{d_2}} \boldsymbol{\chi}_a(\chi_{d_1}, \chi_{d_2}), \tag{2}$$

where

$$\boldsymbol{\chi}_a(\chi_{d_1}, \chi_{d_2}) = \sum_{v \in \mathbb{F}_q} \psi_g(-av) \sum_{\alpha \in \mathbb{F}_{q^n}^*} \chi_{d_1}(\alpha)\chi_{d_2}(\alpha^2+\alpha+1)\hat{\psi}_g(v\alpha).$$

As $\chi_{d_i}(x) = \chi_{q^n-1}(x^{n_i})$ for $i = 1,\ 2$, and some $n_i \in \{0, 1, 2, \cdots, q^n-2\}$, we have

$$\begin{aligned}
\boldsymbol{\chi}_a(\chi_{d_1}, \chi_{d_2}) &= \sum_{v \in \mathbb{F}_q} \psi_g(-av) \sum_{\alpha \in \mathbb{F}_{q^n}^*} \chi_{q^n-1}(\alpha^{n_1}(\alpha^2+\alpha+1)^{n_2})\hat{\psi}_g(v\alpha) \\
&= \sum_{v \in \mathbb{F}_q} \psi_g(-av) \sum_{\alpha \in \mathbb{F}_{q^n}^*} \chi_{q^n-1}(F(\alpha))\hat{\psi}_g(v\alpha),
\end{aligned}$$

where $F(x) = x^{n_1}(x^2+x+1)^{n_2} \in \mathbb{F}_{q^n}[x]$ for some $0 \le n_1, n_2 < q^n - 1$.

If $F(x) \neq yh^{q^n-1}$ for any $y \in \mathbb{F}_{q^n}$ and $h \in \mathbb{F}_{q^n}[x]$ then using Lemma 2.3,

$$|\boldsymbol{\chi}_a| \le 3q^{n/2+1}.$$

If $F = yh^{q^n-1}$ for some $y \in \mathbb{F}_{q^n}$ and $h \in \mathbb{F}_{q^n}[x]$ then

$$x^{n_1}(x^2+x+1)^{n_2} = yh(x)^{q^n-1}, \tag{3}$$

for some $y \in \mathbb{F}_{q^n}$ and $h \in \mathbb{F}_{q^n}[x]$. Now (3)$\Rightarrow$ $x^{n_1} | h^{q^n-1}$. Hence $n_1 = 0$ or

$$(x^2+x+1)^{n_2} = x^{q^n-1-n_1} y A^{(q^n-1)}, \tag{4}$$

where $A(x) = h(x)/x^{n_1} \in \mathbb{F}_{q^n}[x]$. Now if $n_1 = 0$ then we get $(x^2+x+1)^{n_2} = yh(x)^{q^n-1}$, which is possible only if $n_2 = 0$ and H is a constant. Now if $n_1 \neq 0$ then $x^{q^n-1-n_1}|(x^2+x+1)^{n_2}$, which is not possible. Hence $n_1 = n_2 = 0$.

Thus in this case $(\chi_{d_1}, \chi_{d_2}) = (\chi_1, \chi_1)$. Additionally if, $v \neq 0$ then using Lemma 2.2, we get

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

Hence $|\boldsymbol{\chi}_a(\chi_{d_1}, \chi_{d_2})| \leq 3q^{n/2+1}$, when $(\chi_{d_1}, \chi_{d_2}, v) \neq (\chi_1, \chi_1, 0)$. Thus, using (2) we get

$$N_{q^n}(q^n-1, q^n-1, a) \geq \frac{\theta(q^n-1)^2}{q}(q^n - 1 - 3q^{n/2+1}(2^{2\omega(q^n-1)} - 1)). \tag{5}$$

Hence $N_{q^n}(q^n-1, q^n-1, a) > 0$ if $q^{n/2} > q^{-n/2+1} + 3q(2^{2\omega(q^n-1)} - 1)$, i.e., if $q^{n/2-1} > 3 \cdot 2^{2\omega(q^n-1)}$. □

Lemma 3.2 ([1, Lemma 3.1])**.** *For any positive integer I, $2^{\omega(I)} < C(I)I^{1/5}$, where $C(I) < 11.25$.*

Corollary 3.3. *Let $q = p^k$ for some prime p and n be a positive integer. If $n \geq 96$ and $q \geq 2$, then $N_{q^n}(m_1, m_2, a) > 0$ for every $a \in \mathbb{F}_q$.*

Proof. By Lemma 3.2, $N_{q^n}(m_1, m_2, a) > 0$ if $q^{n/10-1} > 380$, which holds for all $n \geq 96$ and $q \geq 2$. Hence the result follows. □

References

[1] Anju and R.K.Sharma, *On primitive normal elements over finite fields*, Asian-European Journal of Mathematics, 11(2)(2018).

[2] X.Cao and P.Wang, *Primitive elements with prescribed trace*, Appl. Algebra Engrg. Comm. Comput., 25(5)(2017), 339-345.

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

[4] W.S.Chou and S.D.Cohen, *Primitive elements with zero traces*, Finite Fields Appl., 7(2001), 125141.

[5] S.D.Cohen, *Consecutive primitive roots in a finite field*, Proc. Amer. Math. Soc., 93(2)(1985), 189197.

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

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

[8] L.B.He and 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.

[9] Q.Liao, J.Li and K.Pu, *On the existence for some special primitive elements in finite fields*, Chin. Ann. Math., 37B(2016), 259266.

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

[11] P.P.Wang, X.W.Cao and R.Q.Feng, *On the existence of some specific elements in finite fields of characteristic 2*, Finite Fields Appl., 18(4)(2012), 800813.