Chin. Ann. Math.
37B(2), 2016, 259–266
DOI: 10.1007/s11401-016-0949-5

Chinese Annals of Mathematics, Series B

On the Existence for Some Special Primitive Elements in Finite Fields*

Qunying LIAO[1] Jiyou LI[2] Keli PU[3]

Abstract Let $\mathbf{F}_q$ be a finite field of characteristic p. In this paper, by using the index sum method the authors obtain a sufficient condition for the existence of a primitive element $\alpha \in \mathbf{F}_{q^n}$ such that $\alpha + \alpha^{-1}$ is also primitive or $\alpha + \alpha^{-1}$ is primitive and α is a normal element of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.

Keywords Finite field, Primitive element, Normal basis
2000 MR Subject Classification 11T30

1 Introduction and Background

Let $\mathbf{F}_q$ be a finite field of characteristic p and order q. Let $n \geq 2$ and $\mathbf{F}_{q^n}$ be a fixed n-extension of $\mathbf{F}_q$. An element $\alpha \in \mathbf{F}_{q^n}$ is called normal over $\mathbf{F}_q$ if $\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$, called a normal basis. Normal bases are important in efficient arithmetic computation for finite fields and have many applications in coding theory and cryptography (see [16–17]). The basic facts on normal bases of finite fields are collected in the book [16].

An element $\alpha \in \mathbf{F}_{q^n}$ is called primitive if it is a generator of the multiplicative group $\mathbf{F}_{q^n}^*$. It is a central problem in computational number theory to construct a primitive element in a finite field. However, even determining a primitive element in a finite field is hard. Primitive elements over finite fields are discussed by Carlitz [1], Davenport [10], et al., and are widely used in cryptography system, coding theory and design theory.

An element is called primitive normal if it is both primitive and normal. The normal basis generated by a primitive normal element is called a primitive normal basis. For any $\alpha \in \mathbf{F}_{q^n}$, $f(x) \in \mathbf{F}_q[x]$ represents the monic minimal polynomial of α over $\mathbf{F}_q$. $f(x)$ is said to be a primitive or normal polynomial over $\mathbf{F}_q$ if α is primitive or normal respectively. $f(x)$ is called a primitive normal polynomial over $\mathbf{F}_q$ when α is a primitive normal element over $\mathbf{F}_q$.

The combination of primitivity and normality was first studied by Carlitz [1]. By using properties for the additive character of $\mathbb{F}_{q^n}$, he proved that there are at most finitely many pairs

Manuscript received March 23, 2013. Revised January 4, 2015.
[1]College of Mathematics and Software Science, Sichuan Normal University, Chengdu 610066, China. E-mail: qunyingliao@sicnu.edu.cn
[2]Department of Mathematics, Shanghai Jiao Tong University, Shanghai 200240, China. E-mail: lijiyou@sjtu.edu.cn
[3]Corresponding author. Department of Mathematics and Finance Economics, Aba Teachers College, Aba 623000, Sichuan, China. E-mail: pp180896@163.com
*The first author is supported by the National Natural Science Foundation of China (No. 11401408), the Natural Science Foundation of Sichuan Province (No. 14ZA0034) and the Sichuan Normal University Key Project Foundation (No. 13ZDL06). The second author is supported by the National Natural Science Foundation of China (No. 11001170) and the Natural Science Foundation of Shanghai Municipal (No. 13ZR1422500).

(q, n) of finite fields, for which there does not exist an element in $\mathbb{F}_{q^n}$ that is both primitive and normal over $\mathbb{F}_q$. He also proved in [1–2] that for all sufficiently large q^n, there exists a primitive normal elements of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$. In the case where the cardinality q is prime, the existence of a primitive normal element was proved by Davenport [10]. For the general case, by improving the method of Carlitz and Davenport, which handles all but finitely many pairs (q, n), Lenstra and Schoof [15] affirmatively settled the existence of primitive normal elements for all finite fields extensions $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and proved the following well-known primitive normal basis theorem.

Theorem 1.1 (see [15]) *For any $n \geq 1$ and any prime power q, there is a primitive normal element in $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.*

For a different proof of this theorem, see Cohen and Huczynska [8]. Cohen and Hachenberger [7] strengthened the primitive normal basis theorem of Lenstra and Schoof [15] and the theorem of Cohen on primitive elements with prescribed trace (see [6]). It established the conjecture of Morgan and Mullen [18], who, by means of a computer search, verified the existence of such elements for the cases in which $q \leq 97$ and $n \leq 6$, n being the degree of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$. Apart from two pairs (q, n), Cohen and Hachenberger [7] settled the conjecture purely theoretically and proved the following theorem.

Theorem 1.2 (see [7]) *For any $n \geq 1$, any prime power q and any nonzero element c in $\mathbf{F}_q$, there exists a primitive normal element $\alpha \in \mathbf{F}_{q^n}$ over $\mathbf{F}_q$ such that* $\mathrm{Tr}(\alpha) = c$, *where* Tr *is the trace map from $\mathbf{F}_{q^n}$ to $\mathbf{F}_q$.*

In recent years, some further improvements of the primitive normal basis theorem are given (see [11–13]).

It is also interesting to note that Chou and Cohen [3] resolved completely the question whether there exists a primitive element $\alpha \in \mathbf{F}_{q^n}$ such that both α and its reciprocal α^{-1} have zero trace over $\mathbf{F}_q$. Trivially, there was no such element when $n < 5$, and they established the existence for all pairs (q, n) $(n \geq 5)$ except $(4, 5), (2, 6)$ and $(3, 6)$. In recent years, Fan and Cohen, et al. [9, 19] further proved that for any prime power q and any integer $n \geq 2$, there is an element $\alpha \in \mathbf{F}_{q^n}$ such that both α and α^{-1} are primitive normal over $\mathbf{F}_q$ except when (q, n) is one of the pairs $(2, 3)$–$(2, 4)$, $(3, 4)$, $(4, 3)$ and $(5, 4)$. Equivalently, with the same exceptions, there is always a primitive polynomial $p(x)$ of degree n over $\mathbf{F}_q$ whose coefficients of x and of x^{n-1} are both zero. Their method employed Kloosterman sums and a sieving technique.

For convenience, throughout this paper we denote $\omega(n)$ to be the number of distinct prime factors of the integer $n > 1$.

In 2006, Tian and Qi [19] proved that there exists 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 $n \geq 32$. Recently, Wang, et al. [21] gave a sufficient condition on the existence of α such that α and $\alpha + \alpha^{-1}$ are both primitive or primitive normal for the case $2 \mid q$. In the present paper, by using the index sum method we generalize their results to the case that q is any prime power and prove the following main results.

Theorem 1.3 *Let q, n be positive integers such that* $\gcd(n, q) = 1$ *and $q^{\frac{n}{2}} > 2^{2\omega(q^n-1)}$, and then there exists $\alpha \in \mathbf{F}_q^n$ such that α and $\alpha + \alpha^{-1}$ are both primitive, where $\omega(q^n - 1)$ is the number of distinct prime divisors of $q^n - 1$.*

Corollary 1.1 *Let q and n be positive integers such that* $\gcd(n, q) = 1$. *If $n \geq 13$ and $t \geq 4$, then $(q, n) \in U_1$.*

Theorem 1.4 *Let q and n be positive integers such that $\gcd(n,q)=1$. Suppose that $\Omega=\Phi_q(x^n-1)$, and $q^{\frac{n}{2}}>2^{2\omega(q^n-1)+\Omega}$, so then there exists $\alpha\in\mathbf{F}_q^n$ such that α is primitive normal and $\alpha+\alpha^{-1}$ is primitive, where $\Omega=\Phi_q(x^n-1)$ is the Euler function of the polynomial x^n-1.*

2 Preliminaries

In this section, some necessary definitions and lemmas are given.

Definition 2.1 (see [4]) *Let $r>1$ be a positive integer and suppose $r\mid q-1$. We call $\alpha\in\mathbf{F}_q^*$ an r-free element if $\gcd\left(r,\frac{q-1}{\mathrm{ord}_q(\alpha)}\right)=1$.*

Lemma 2.1 (see [5]) *Let $\alpha\in\mathbf{F}_q^*$, and $r>1$ be a positive integer such that $r\mid q-1$. Then*

$$\sum_{d\mid r}\frac{\mu(d)}{\phi(d)}\sum_{\mathrm{ord}(\chi)=d}\chi(\alpha)=\begin{cases}\dfrac{r}{\phi(r)}, & \alpha \text{ is } r\text{-free},\\ 0, & \text{otherwise},\end{cases}\tag{2.1}$$

where ϕ is the Euler totient function, μ is the Möbius function and $\mathrm{ord}(\chi)$ is the order of the multiplicative character χ of $\mathbf{F}_q$.

Let $\alpha\in\mathbf{F}_{q^n}$ and d be a positive integer. Define

$$P(d,\alpha)=\frac{\mu(d)}{\phi(d)}\sum_{\chi_d}\chi_d(\alpha),\quad P(\alpha)=\frac{\phi(q^n-1)}{q^n-1}\sum_{d\mid q^n-1}P(d,\alpha),$$

where $\sum\limits_{\chi_d}$ ranges over all multiplicative characters of $\mathbf{F}_{q^n}$ of order d. Thus (2.1) implies

$$P(\alpha)=\begin{cases}1, & \alpha \text{ is a primitive element},\\ 0, & \text{otherwise}.\end{cases}\tag{2.2}$$

Lemma 2.2 (see [14]) *Suppose that χ is a multiplicative character of $\mathbf{F}_q$ with $\mathrm{ord}(\chi)>1$. Then $\sum\limits_{x\in\mathbf{F}_q^*}\chi(x+x^{-1})\le 2q^{\frac{1}{2}}$.*

Now for any $g(x)\in\mathbf{F}_q[x]$, $g(x)\diamond\alpha=g(\sigma)(\alpha)$, $\sigma:\alpha\mapsto\alpha^q$. Then $\alpha\in\mathbf{F}_{q^n}$ if and only if $(x^n-1)\diamond\alpha=0$. The unique monic polynomial in $\mathbf{F}_q[x]$ generating this annihilator as an ideal is called the order of α, denoted by $\mathrm{ord}_q(\alpha)$. Clearly, $\alpha\in\mathbf{F}_{q^n}\Leftrightarrow\mathrm{ord}_q(\alpha)\mid x^n-1$.

Definition 2.2 (see [14]) *Let $\alpha\in\mathbf{F}_{q^n}$ and $f(x)\in\mathbf{F}_q[x]$ with $f(x)\mid(x^n-1)$. We call α an $f(x)$-free element if $\gcd\left(f(x),\frac{x^n-1}{\mathrm{ord}_q(\alpha)}\right)=1$.*

By this definition, $\alpha\in\mathbf{F}_{q^n}$ is a normal element over $\mathbf{F}_q$ if and only if α is (x^n-1)-free.

Lemma 2.3 (see [15]) *Let $f(x)\in\mathbf{F}_q[x]$ and $f(x)\mid x^n-1,\alpha\in\mathbf{F}_{q^n}$. Then*

$$\sum_{g\mid f}\frac{\mu(g)}{\Phi_q(g)}\sum_{\lambda_g}\lambda_g(\alpha)=\begin{cases}\dfrac{q^{\deg f}}{\Phi_q(g)}, & \alpha \text{ is } f(x)\text{-free},\\ 0, & \text{otherwise},\end{cases}$$

where $\Phi_q(g)=\sharp\left(\frac{\mathbf{F}_q[x]}{f(x)}\right)^*$ and λ_g is an additive character with $\mathrm{ord}_q g(x)$.

Similarly, for a monic polynomial $g(x) \in \mathbf{F}_q[x]$, let $\Omega_q(g(x))$ be the number of distinct monic irreducible divisors of $g(x)$ in $\mathbf{F}_q[x]$. Define $R(g,\alpha) = \frac{\mu(g)}{\Phi_q(g)} \sum\limits_{\lambda_g} \lambda_g(\alpha)$ and

$$R(\alpha) = \frac{\Phi_q(x^n-1)}{q^n} \sum_{g(x)|x^n-1} R(g,\alpha).$$

Similarly,

$$R(\alpha) = \begin{cases} 1, & \alpha \text{ is a mormal element,} \\ 0, & \text{otherwise.} \end{cases} \tag{2.3}$$

Lemma 2.4 (see [15]) *Let $n > 1$, $l > 1$ be integers and Λ be a set of primes $\le l$. Set $L = \prod\limits_{r\in\Lambda} r$. Assume that every prime factor $r < l$ of n is contained in Λ. Then*

$$\omega(n) \le \frac{\log n - \log L}{\log l} + |\Lambda|.$$

Let m be a positive integer and p_m be the m-th prime. Later we will take $l = p_m$, and then Λ is the set of primes no more than p_m, and $|\Lambda| = m$, so we have the following inequality instead of

$$\omega(N) \le \frac{\log N - \sum\limits_{i=1}^{m} \log p_i}{\log p_m} + m. \tag{2.4}$$

For our proof, we need the Weil's character sum estimate in the following form (see [20]).

Lemma 2.5 (see [20]) *Let $f_1(T)$ and $f_2(T)$ be two monic pairwise prime polynomials in $\mathbf{F}_q[T]$ whose largest square-free divisors have degree d_1 and d_2 respectively. Let χ_1 and χ_2 be two multiplicative nontrivial characters of the finite field $\mathbf{F}_q$. Assume that none of $f_i(T)$ is of the form $g(T)^{\mathrm{ord}\chi_i}$ for $i = 1, 2$, where $g(T) \in \mathbf{F}_q[T]$ with degree at least 1. Then we have $\big|\sum\limits_{a\in\mathbf{F}_q} \chi_1(f_1(a))\chi_2(f_2(a))\big| \le (d_1+d_2-1)\sqrt{q}$.*

3 Proofs of the Main Results

Proof of Theorem 1.3 Denote $\mathcal{P}$ to be the set of primitive elements of $\mathbb{F}_{q^n}$ and $\mathcal{N}$ to be the set of normal elements of $\mathbb{F}_{q^n}$ over $\mathbf{F}_q$. Define $U_1 = \{(q,n) \,|\, \alpha, \alpha+\alpha^{-1} \in \mathcal{P}\}$, $U_2 = \{(q,n) \,|\, \alpha, \alpha+\alpha^{-1} \in \mathcal{P} \text{ and } \alpha \in \mathcal{N}\}$. By Definition 2.1 and (2.2) one has

$$\begin{aligned} |U_1| &= \sum_{\alpha\in\mathbf{F}_{q^n}^*} P(\alpha)P(\alpha+\alpha^{-1}) \\ &= \Big(\frac{\phi(q^n-1)}{q^n-1}\Big)^2 \sum_{\alpha\in\mathbf{F}_{q^n}^*} \sum_{d,h|q^n-1} P(d,\alpha)P(h,\alpha+\alpha^{-1}) \\ &= \Big(\frac{\phi(q^n-1)}{q^n-1}\Big)^2 (A_1+A_2+A_3+A_4), \end{aligned}$$

where $A_1 = \sum\limits_{\alpha\in\mathbf{F}_{q^n}^*} P(1,\alpha)P(1,\alpha+\alpha^{-1})$, $A_2 = \sum\limits_{\alpha\in\mathbf{F}_{q^n}^*} \sum\limits_{1\ne d|q^n-1} P(d,\alpha)P(1,\alpha+\alpha^{-1})$, $A_3 = \sum\limits_{\alpha\in\mathbf{F}_{q^n}^*} \sum\limits_{1\ne h|q^n-1} P(1,\alpha)P(h,\alpha+\alpha^{-1})$ and $A_4 = \sum\limits_{\alpha\in\mathbf{F}_{q^n}^*} \sum\limits_{1\ne d,h|q^n-1} P(d,\alpha)P(h,\alpha+\alpha^{-1})$. It is clear that

$$A_1 = \sum_{\alpha\in\mathbf{F}_{q^n}^*} \frac{\mu(1)}{\phi(1)} \sum_{\chi_1} \chi_1(\alpha) \sum_{\chi_1} \chi_1(\alpha+\alpha^{-1}) = \sum_{\alpha\in\mathbf{F}_{q^n}^*} 1 = q^n - 1 \tag{3.1}$$

and

$$\begin{aligned}|A_2| &= \Big|\sum_{\alpha\in\mathbf{F}_{q^n}^*}\frac{\mu(1)}{\phi(1)}\sum_{\chi_1}\chi_1(\alpha+\alpha^{-1})\sum_{1\neq d|q^n-1}\frac{\mu(d)}{\phi(d)}\sum_{\chi_d}\chi_d(\alpha)\Big|\\ &= \Big|\sum_{\alpha\in\mathbf{F}_{q^n}^*}\sum_{1\neq d|q^n-1}\frac{\mu(d)}{\phi(d)}\sum_{\chi_d}\chi_d(\alpha)\Big|\\ &\leq \sum_{1\neq d|q^n-1}\frac{1}{\phi(d)}\sum_{\chi_d}\Big|\sum_{\alpha\in\mathbf{F}_{q^n}^*}\chi_d(\alpha)\Big|.\end{aligned}$$

If $d\neq 1$, then $\big|\sum_{\alpha\in\mathbf{F}_{q^n}^*}\chi_d(\alpha)\big|=0$ and thus

$$|A_2|=0. \tag{3.2}$$

Similar to A_2, one shows that $|A_3|\leq\sum_{1\neq h|q^n-1}\frac{1}{\phi(h)}\sum_{\chi_h}\big|\sum_{\alpha\in\mathbf{F}_{q^n}^*}\chi_h(\alpha+\alpha^{-1})\big|$. From Lemma 2.2, we have $|A_3|\leq\sum_{1\neq h|q^n-1}\frac{1}{\phi(h)}\sum_{\chi_h}2q^{\frac{n}{2}}=\sum_{1\neq h|q^n-1}\frac{2q^{\frac{n}{2}}}{\phi(h)}\sum_{\chi_h}1$, namely,

$$|A_3|\leq 2q^{\frac{n}{2}}\sum_{1\neq h|q^n-1}\frac{1}{\phi(h)}\phi(h)=2q^{\frac{n}{2}}(2^{\omega(q^n-1)}-1). \tag{3.3}$$

Now we compute A_4:

$$\begin{aligned}|A_4| &= \Big|\sum_{\alpha\in\mathbf{F}_{q^n}^*}\sum_{1\neq d,h|q^n-1}P(d,\alpha)P(h,\alpha+\alpha^{-1})\Big|\\ &= \Big|\sum_{1\neq d,h|q^n-1}\frac{\mu(d)\mu(h)}{\phi(d)\phi(h)}\sum_{\chi_d,\chi_h}\sum_{\alpha\in\mathbf{F}_{q^n}^*}\chi_d(\alpha)\chi_h(\alpha+\alpha^{-1})\Big|\\ &\leq \sum_{1\neq d=h|q^n-1}\frac{1}{\phi(d)\phi(h)}\sum_{\chi_d,\chi_h}\Big|\sum_{\alpha\in\mathbf{F}_{q^n}^*}\chi_d(\alpha)\chi_h(\alpha+\alpha^{-1})\Big|\\ &= \sum_{1\neq d,h|q^n-1}\frac{1}{\phi(d)\phi(h)}\sum_{\chi_d=\chi_h}\Big|\sum_{\alpha\in\mathbf{F}_{q^n}^*}\chi_d(\alpha^2+1)\Big|\\ &\quad+\sum_{1\neq d,h|q^n-1}\frac{1}{\phi(d)\phi(h)}\sum_{\chi_d\neq\chi_h}\Big|\sum_{\alpha\in\mathbf{F}_{q^n}^*}\chi_d\chi_h^{-1}(\alpha)\chi_h(\alpha^2+1)\Big|\\ &\leq \sum_{1\neq d,h|q^n-1}\frac{1}{\phi(d)\phi(h)}\sum_{\chi_d=\chi_h}q^{\frac{n}{2}}+\sum_{1\neq d,h|q^n-1}\frac{1}{\phi(d)\phi(h)}\sum_{\chi_d\neq\chi_h}2q^{\frac{n}{2}}.\end{aligned}$$

The last inequality follows from Lemma 2.5 and thus

$$|A_4|\leq\sum_{1\neq d|q^n-1}\frac{q^{\frac{n}{2}}}{\phi(d)\phi(h)}\sum_{\chi_d}1+\sum_{1\neq d,h|q^n-1}\frac{1}{\phi(d)\phi(h)}\sum_{\chi_d\neq\chi_h}2q^{\frac{n}{2}}\leq q^{\frac{n}{2}}(2^{\omega(q^n-1)}-1)^2. \tag{3.4}$$

From (3.1)–(3.4) we now have $\big||U_1|-\frac{(\phi(q^n-1))^2}{q^n-1}\big|\leq\big(\frac{\phi(q^n-1)}{q^n-1}\big)^2\big(2q^{\frac{n}{2}}(2^{\omega(q^n-1)}-1)+q^{\frac{n}{2}}(2^{\omega(q^n-1)}-1)^2\big)$. In order to have $|U_1|>0$, it is sufficient to have $q^n-1>2q^{\frac{n}{2}}(2^{\omega(q^n-1)}-1)+q^{\frac{n}{2}}(2^{\omega(q^n-1)}-1)^2$), namely, $q^{\frac{n}{2}}-\frac{1}{q^{\frac{n}{2}}}>2^{2\omega(q^n-1)}-2^{2+\omega(q^n-1)}-1$, and it is sufficient to have $q^{\frac{n}{2}}>2^{2\omega(q^n-1)}$ as desired. The proof is complete.

Proof of Corollary 1.1 By (2.4) we have

$$\omega(q^n-1) \le \frac{\log(q^n-1)-\sum\limits_{i=1}^{m}\log p_i}{\log p_m}+m < \frac{n\log q-\sum\limits_{i=1}^{m}\log p_i}{\log p_m}+m.$$

From $q^{\frac{n}{2}} > 2^{2\omega(q^n-1)}$ we have

$$\frac{n\log q}{\log 16}-\frac{n\log q}{\log p_m} > m-\frac{\sum\limits_{i=1}^{m}\log p_i}{\log p_m}. \tag{3.5}$$

If the left of (3.5) is positive, we have $\frac{1}{\log 16}-\frac{1}{\log p_m}>0$, i.e., $m\ge 7$. So we can choose a suitable m with $m\ge 7$. Thus we complete the proof of Corollary 1.1.

Example 3.1 Let $p=3$, when $q<32$, that is, $t\le 3$. We can find the (q,n) such that $(q,n)\in U_1$.

$t=$	1	2	3
$n\ge$	7	4	5

Proof of Theorem 1.4 Similarly, by (2.3) one has

$$\begin{aligned}|U_2| &= \sum_{\alpha\in\mathbf{F}_{q^n}^*} P(\alpha)P(\alpha+\alpha^{-1})R(\alpha)\\ &= \Big(\frac{\phi(q^n-1)}{q^n-1}\Big)^2\frac{\phi_q(x^n-1)}{q^n}\Big)\sum_{\alpha\in\mathbf{F}_{q^n}^*}\sum_{d,h|q^n-1}\sum_{g|(x^n-1)}P(d,\alpha)P(h,\alpha+\alpha^{-1})R(g,\alpha)\\ &= \Big(\frac{\phi(q^n-1)}{q^n-1}\Big)^2\frac{\phi_q(x^n-1)}{q^n}\Big)(D_1+D_2+D_3+D_4+D_5+D_6),\end{aligned}$$

where

$$\begin{aligned}D_1 &= \sum_{\alpha\in\mathbf{F}_{q^n}^*}P(1,\alpha)P(1,\alpha+\alpha^{-1})R(1,\alpha)\\ D_2 &= \sum_{\alpha\in\mathbf{F}_{q^n}^*}\sum_{1\ne d|q^n-1}P(d,\alpha)P(1,\alpha+\alpha^{-1})R(1,\alpha),\\ D_3 &= \sum_{\alpha\in\mathbf{F}_{q^n}^*}\sum_{1\ne h|q^n-1}P(1,\alpha)P(h,\alpha+\alpha^{-1})R(1,\alpha),\\ D_4 &= \sum_{\alpha\in\mathbf{F}_{q^n}^*}\sum_{1\ne d,h|q^n-1}P(d,\alpha)P(h,\alpha+\alpha^{-1})R(1,\alpha),\\ D_5 &= \sum_{\alpha\in\mathbf{F}_{q^n}^*}\sum_{1\ne g|x^n-1}P(1,\alpha)P(1,\alpha+\alpha^{-1})R(g,\alpha),\\ D_6 &= \sum_{\alpha\in\mathbf{F}_{q^n}^*}\sum_{1\ne d,h|q^n-1}\sum_{1\ne g|x^n-1}P(d,\alpha)P(h,\alpha+\alpha^{-1})R(g,\alpha).\end{aligned}$$

Similar to the proof of Theorem 1.3, we have $|D_1|=q^n-1,\ |D_2|=0,\ |D_3|\le 2q^{\frac{n}{2}}(2^{\omega(q^n-1)}-1),\ |D_4|\le q^{\frac{n}{2}}(2^{\omega(q^n-1)}-1)^2$,

$$|D_5| = \Big|\sum_{\alpha\in\mathbf{F}_{q^n}^*}\frac{\mu(1)}{\phi(1)}\sum_{\chi_1}\chi_1(\alpha+\alpha^{-1})\frac{\mu(1)}{\phi(1)}\sum_{\chi_1}\chi_1(\alpha)\sum_{g|x^n-1}\sum_{\lambda_g}\lambda_g(\alpha)\Big|$$

$$
\begin{aligned}
&= \Big| \sum_{\alpha\in\mathbf{F}_{q^n}^*} \sum_{g|x^n-1} \frac{\mu(g)}{\phi(g)} \sum_{\lambda_g} \lambda_g(\alpha) \Big| \\
&= \Big| \sum_{g|x^n-1} \frac{\mu(g)}{\phi(g)} \sum_{\lambda_g} (-1) \Big| \\
&= \Big| \sum_{g|x^n-1} \frac{\mu(g)}{\phi(g)} \phi(g) \Big| \\
&\le 2^{\Omega} - 1
\end{aligned}
$$

and

$$
\begin{aligned}
|D_6| &= \Big| \sum_{\alpha\in\mathbf{F}_{q^n}^*} \sum_{1\neq d,h|q^n-1} \sum_{g|x^n-1} P(d,\alpha)P(h,\alpha+\alpha^{-1})R(g,\alpha) \Big| \\
&= \Big| \sum_{1\neq d,h|q^n-1} \frac{\mu(d)\mu(h)}{\phi(d)\phi(h)} \sum_{\alpha\in\mathbf{F}_{q^n}^*} \sum_{\chi_d,\chi_h} \chi_d(\alpha)\chi_h(\alpha+\alpha^{-1}) \sum_{1\neq g|x^n-1} \frac{\mu(g)}{\phi(g)} \sum_{\lambda_g} \lambda_g(\alpha) \Big| \\
&\le \Big| \sum_{\alpha\in\mathbf{F}_{q^n}^*} \sum_{1\neq g|x^n-1} \frac{\mu(g)}{\phi(g)} \sum_{\lambda_g} \lambda_g(\alpha) \Big| \Big(\sum_{1\neq d,h|q^n-1} \frac{1}{\phi(d)\phi(h)} \sum_{\chi_d=\chi_h} \Big| \sum_{\alpha\in\mathbf{F}_{q^n}^*} \chi_d(\alpha^2+1) \Big| \\
&\quad + \sum_{1\neq d,h|q^n-1} \frac{1}{\phi(d)\phi(h)} \sum_{\chi_d\neq\chi_h} \Big| \sum_{\alpha\in\mathbf{F}_{q^n}^*} \chi_d\chi_h^{-1}(\alpha)\chi_h(\alpha^2+1) \Big| \Big) \\
&\le \Big| \sum_{\alpha\in\mathbf{F}_{q^n}^*} \sum_{1\neq g|x^n-1} \frac{\mu(g)}{\phi(g)} \sum_{\lambda_g} \lambda_g(\alpha) \Big| \Big(\sum_{1\neq d,h|q^n-1} \frac{1}{\phi(d)\phi(h)} \sum_{\chi_d=\chi_h} q^{\frac{n}{2}} \\
&\quad + \sum_{1\neq d,h|q^n-1} \frac{1}{\phi(d)\phi(h)} \sum_{\chi_d\neq\chi_h} 2q^{\frac{n}{2}} \Big) \\
&\le (2^{\Omega}-1) q^{\frac{n}{2}} (2^{\omega(q^n-1)}-1)^2.
\end{aligned}
$$

Obviously, in order to get $|U_2| > 0$, it is sufficient to have $q^{\frac{n}{2}} > 2^{2\omega(q^n-1)+\Omega}$.

Thus we complete the proof of Theorem 1.4.

4 Concluding Remark

For the set U_i $(i = 1, 2)$, Wang, et al. considered the case that q is a power of 2. In this paper, we consider the general case and obtain the similar estimate. By the same proof of our main results, one can get a sufficient condition for the set $U_3 = \{(q,n) \,|\, \alpha, \alpha+\alpha^{-1} \in \mathcal{P} \cap \mathcal{N}\}$ to be not empty, which is left to readers.

In fact, the main difference between the proofs in [21] and the present paper is to compute $|A_4|$. In detail, the key is to estimate the value of $\Big| \sum_{\alpha\in\mathbb{F}_{q^n}^*} \chi_d(\alpha)\chi_h(\alpha+\alpha^{-1}) \Big|$. This can be reduced to the Jacobi sum $J(\chi_d\bar{\chi_h}, \chi_h)$ or $J((\chi_d\bar{\chi_h})^{\frac{1}{2}}, \chi_h)$ in the case $2 \mid q$, which can be bounded by using the techniques of Jacobi sums. In the case that q is odd, this approach does not work. In [21] the authors pointed out that similar results could be obtained through certain slight modification. To make it more exact, the difficulty of estimating the related exponential sums could be overcome to obtain similar results in finite fields with general characteristics. In this paper, we completely solve the problem and our proof looks briefer than that in [21] by using the Weil's character sum estimate (see [20]). With our method, all results in [21] for the case

$2 \mid q$ can be paralleled to the general case. For the time being, we omit it here and leave it to readers.

Acknowledgement The authors would like to thank the reviewers for some helpful suggestions.

References

[1] Carlitz, L., Primitive roots in finite fields, *Trans. Am. Math. Soc.*, **73**, 1952, 373–382.

[2] Carlitz, L., Some problems involving primitive roots in a finite field, *Proc. Nat. Acad. Sci. U. S. A.*, **38**, 1952, 314–318.

[3] Chou, W. S. and Cohen, S. D., Primitive elements with zero traces, *Finite Fields Appl.*, **7**, 2001, 125–141.

[4] Cohen, S. D., Primitive elements and polynomials: Existence results, *Lecture Notes in Pure and Appl.*, http:// www.researchgate.net/publication/265461791

[5] Cohen, S. D., Primitive roots in the quadratic extension of a finite field, *J. London Math Soc.*, **27**(2), 1983, 221–228.

[6] Cohen, S. D., Primitive elements and polynomials with arbitrary trace, *Discrete Math.*, **83**, 1990, 1–7.

[7] Cohen, S. D. and Hachenberger, D., Primitive normal bases with prescribed trace, *Applicable Algebra in Engineering Communication and Computing*, **9**, 1999, 383–403.

[8] Cohen, S. D. and Huczynska, S., Primitive free quartics with specified norm and trace, *Acta Arith.*, **109**(4), 2003, 359–385.

[9] Dahab, R., Hankerson, D., Hu, F., et al., Software multiplication using Gaussian normal bases, *IEEE Trans. Comput.*, **55**, 2006, 974–984.

[10] Davenport, H., Bases for finite fields, *J. London Math. Soc.*, **43**, 1968, 21–39.

[11] Fan, S. Q., Han, W. B., Feng, K. Q. and Zhang, X. Y., Primitive normal polynomials with the first two coefficients prescribed: A revised p-adic method, *Finite Fields Appl.*, **13**(3), 2007, 577–604.

[12] Fan, S. Q., Han, W. B. and Feng, K. Q., Primitive normal polynomials with multiple coefficients prescribed: An asymptotic result, *Finite Fields Appl.*, **13**(4), 2007, 1029–1044.

[13] Fan, S. Q., Primitive normal polynomials with the last half coefficients prescribed, *Finite Fields Appl.*, **15**(5), 2009, 604–614.

[14] He, L. B. and Han, W. B., Research on primitive elements in the form $\alpha + \alpha^{-1}$ over $\mathbf{F}_q$, *Journal of Information Engineering University*, **4**(2), 2003, 97–98 (in Chinese).

[15] Lenstra, H. W. Jr. and Schoof, R. J., Primitive normal bases for finite fields, *Math. Comp.*, **48**, 1987, 271–231.

[16] Lidl, R. and Niederreiter, H., Finite Fields, Cambridge University Press, Cambridge, 1987.

[17] Lidl, R. and Niederreiter, H., Finite Fields and Their Applications, 2nd edition, Cambrige University Press, Cambrige, 1994.

[18] Morgan, I. H. and Mullen, L. G., Primitive normal polynomials over finite fields, *Math. Comp.*, **63**, 1994, 759–765.

[19] Qi, W. F. and Tian, T., Primitive normal element and its inverse in finite fields, *Acta Mathematics Sinica* (Chinese Series), **49**(3), 2006, 657–668.

[20] Wan, D. Q., Generators and irreducible polynomials over finite fields, *Mathematics of Computation*, **66**, 1997, 1195–1212.

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