On the existence of some specific elements in finite fields of characteristic 2

Peipei Wang\textsuperscript{a}, Xiwang Cao\textsuperscript{a,b,c,}, Rongquan Feng\textsuperscript{d}

\textsuperscript{a} School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China
\textsuperscript{b} School of Mathematical Sciences, LMIB of Ministry of Education, Beijing University of Aeronautics and Astronautics, Beijing 100191, China
\textsuperscript{c} State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100049, China
\textsuperscript{d} School of Mathematical Sciences, Peking University, Beijing 100871, China

\textbf{Article history:}
Received 31 August 2011
Revised 12 April 2012
Accepted 16 April 2012
Available online 21 April 2012
Communicated by D. Panario

\textbf{MSC:}
11T23
11T71

\textbf{Keywords:}
Finite fields
Primitive element
Normal element
Exponential sums
Characters

\textbf{Abstract}
Let $q$ be a power of 2, $n$ be a positive integer, and let $\mathbb{F}_{q^n}$ be the finite field with $q^n$ elements. In this paper, we consider the existence of some specific elements in $\mathbb{F}_{q^n}$. The main results obtained in this paper are listed as follows:

1. There is an element $\xi$ in $\mathbb{F}_{q^n}$ such that both $\xi$ and $\xi + \xi^{-1}$ are primitive elements of $\mathbb{F}_{q^n}$ if $q = 2^s$, and $n$ is an odd number no less than 13 and $s > 4$.

2. For $q = 2^s$, and any odd $n$, there is an element $\xi$ in $\mathbb{F}_{q^n}$ such that $\xi$ is a primitive normal element and $\xi + \xi^{-1}$ is a primitive element of $\mathbb{F}_{q^n}$ if either $n|(q-1)$, and $n \geq 33$, or $n \nmid (q-1)$, and $n \geq 30$, $s \geq 6$.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

Let $\mathbb{F}_q$ be the finite field with $q$ elements of characteristic $p$, and $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$. For every positive integer $n$, let $\mathbb{F}_{q^n}$ be the extension field of $\mathbb{F}_q$ of degree $n$. Then $\mathbb{F}_q^*$ is a cyclic group of order $q^n - 1$. The generators of $\mathbb{F}_{q^n}$ are called primitive elements of $\mathbb{F}_{q^n}$ [20]. There are $\varphi(q^n - 1)$ primitive elements of $\mathbb{F}_{q^n}$, where $\varphi$ is the Euler phi-function. A primitive polynomial
of degree \( n \geq 1 \) is a minimal polynomial over \( \mathbb{F}_q \) of a primitive element of \( \mathbb{F}_{q^n} \). Many researchers are engaged in studying primitive polynomials, such as Cohen, Fan and Han in [7,11,12] and so on. A normal basis of \( \mathbb{F}_{q^n} \) regarded as a vector space over \( \mathbb{F}_q \) is a basis of the form \( \{ \alpha, \alpha^q, \ldots, \alpha^{q^{n-1}} \} \), and the corresponding element \( \alpha \) is called a normal element of \( \mathbb{F}_{q^n} \). If \( \alpha \) is also a primitive element, then \( \alpha \) is called a primitive normal element.

In 1850, Eisenstein [10] conjectured the following normal basis theorem for finite fields, and in 1888, Hensel [17] gave the first complete proof of it.

**Theorem 1.1 (The normal basis theorem).** There is a normal basis for any finite Galois extension of finite fields.

Primitive elements and normal elements over finite fields are widely used in many fields, such as codes, cryptography and computer algebra, etc. The combination of primitivity and normality was first studied by Carlitz [1]. He proved that there are at most finitely many pairs \( (\mathbb{F}_{q^n}, \mathbb{F}_q) \) of finite fields (with \( \mathbb{F}_{q^n} \) being an extension of \( \mathbb{F}_q \)) without a primitive and normal element over \( \mathbb{F}_q \). Davenport [8] proved that there exist primitive normal elements over \( \mathbb{F}_q \) when \( q \) is a prime. Lenstra and Schoof [19] affirmatively settled the existence of primitive normal elements for all finite fields \( \mathbb{F} \) and all finite extensions over \( \mathbb{F} \).

**Theorem 1.2 (Primitive normal basis theorem).** (See [19].) For any prime power \( q \) and positive integer \( n \), there is a primitive normal basis in \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_q \).

Coding Theory [21] motivated the study of primitive elements with prescribed trace, see also [6, 17,22,23]. Recall that the \((\mathbb{F}_{q^n}, \mathbb{F}_q)\)-trace, denoted by \( \text{Tr}(\alpha) \), is defined as

\[
\text{Tr}(\alpha) := \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) := \sum_{i=0}^{n-1} \alpha^{q^i}.
\]

(1.1)

Cohen [6] proved that if \( n \geq 3 \), and \((q,n) \neq (4,3)\), for every \( a \in \mathbb{F}_q \), there exists a primitive element \( \alpha \in \mathbb{F}_{q^n} \) such that \( \text{Tr}(\alpha) = a \). Moreover, if \( n = 2 \) or \((q,n) = (4,3)\), for every nonzero \( a \in \mathbb{F}_q \), there exists a primitive element \( \alpha \in \mathbb{F}_{q^n} \) such that \( \text{Tr}(\alpha) = a \).

Considering primitive elements with nonzero trace, some existence results were independently proved by Jungnickel and Vanstone [18] when \( n \geq 3 \): existence was settled for every nonzero \( a \in \mathbb{F}_q \) whenever \( n \geq 3 \), whereas for \( n = 2 \) it was shown that there are at most 143 exceptional values for \( q \).

The case of nonzero trace and \( q = 2 \) had been handled already by Moreno [22]. Cohen [4,5] settled the existence of primitive and normal elements \( \alpha \) over \( \mathbb{F}_q \) such that \( \text{Tr}(\alpha) = a \), where \( a \in \mathbb{F}_q^* \).

If \( \xi \) is a primitive element over \( \mathbb{F}_{q^n} \), then \( \xi^{-1} \) is also a primitive element over \( \mathbb{F}_{q^n} \). Wan [25] studied the existence of \( \alpha \) satisfying that \( \mathbb{F}_{q^n} = \mathbb{F}(\alpha) \) and the multiplicative group \( \mathbb{F}_{q^n}^* \) is generated by the line \( \mathbb{F}_q + \alpha \). Chou and Cohen [2] resolved completely the question of whether there is a primitive element \( \xi \in \mathbb{F}_{q^n} \) such that both \( \xi \) and \( \xi^{-1} \) have zero trace over \( \mathbb{F}_q \). He and Han [16] studied primitive elements in the form of \( \alpha + \alpha^{-1} \) over finite fields. In 2006, Tian and Qi [24] proved that if \( n > 32 \), then there exists a primitive element \( \xi \) of \( \mathbb{F}_{q^n} \) satisfying that \( \xi \) and \( \xi^{-1} \) are normal elements of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_q \). Dong and Cao [9] settled the following question: if \( \alpha \in \mathbb{F}_{q^n}^* \) is a primitive element, for \( x \in \mathbb{F}_{q^n}^* \), \( \alpha + x \) is still a primitive element.

Let \( n \) and \( k \) be positive integers such that \( r = nk + 1 \) is a prime, not dividing \( q \), and \( K \) the unique subgroup of order \( k \) of the multiplicative group of \( \mathbb{Z}_r = \mathbb{Z}/r\mathbb{Z} \). For any primitive \( r \)-th root \( \beta \) of unity in \( \mathbb{F}_{q^n}^* \), the element

\[
\alpha = \sum_{a \in K} \beta^a
\]
is called a Gauss period of type \((n; k)\) over \(\mathbb{F}_q\). It is easy to see that \(\alpha \in \mathbb{F}_q^*\). It is known that a Gauss period of type \((n; k)\) over \(\mathbb{F}_q\) generates a normal basis for \(\mathbb{F}_{q^n}\) over \(\mathbb{F}_q\) if and only if \(\gcd(e; n) = 1\), where \(e\) denotes the index of \(q\) modulo \(nk + 1\), see Wasserman [27], Gao et al. [13].

Gauss periods of type \((n; 2)\) (i.e., \(\alpha = \beta + \beta^{-1}\)) over \(\mathbb{F}_2\) also have other remarkable properties. Gao and Vanstone [14] proved that they can be exponentiated in \(O(n^2)\) bit operations. This is faster than any known algorithm for exponentiation of an arbitrary element in \(\mathbb{F}_{2n}\) by a factor of \(\log \log n\). The orders of Gauss periods of type \((n; 2)\) over \(\mathbb{F}_2\) were also computed for \(n < 1200\) [15]. The experimental results in their paper show that Gauss periods have high multiplicative order, and in fact are often primitive elements over \(\mathbb{F}_2\). This is useful in cryptosystems where a fixed element needs to be raised to many large powers.

The motivation of the presented paper is to investigate the existence of Gauss periods of type \((n; 2)\). Before we state our results, let us introduce several symbols that will emerge in our results.

\[ U_1 = \{(q, n) \mid \text{there exists } \xi \in \mathbb{F}_{q^n} \text{ such that both } \xi \text{ and } \xi + \xi^{-1} \text{ are primitive}\}, \]

\[ U_2 = \{(q, n) \mid \text{there exists } \xi \in \mathbb{F}_{q^n} \text{ such that both } \xi \text{ and } \xi + \xi^{-1} \text{ are primitive and } \xi \text{ is normal}\}. \]

In this paper, the following results are obtained.

1. Let \(q = 2^s\), and \(n\) odd. Then one has \((q, n) \in U_1\) when \(s > 4\), and \(n \geq 13\).
2. Let \(q = 2^s\), and \(n\) odd. Then one has \((q, n) \in U_2\) when \(n|(q - 1)\), and \(n \geq 33\).
3. Let \(q = 2^s\), and \(n\) odd. Then one has \((q, n) \in U_2\) when \(n|(q - 1)\), and \(n \geq 30\), \(s \geq 6\).

The paper is organized as follows. In Section 2, the relevant knowledge about the estimation of exponential sums over finite fields is introduced, and then in Sections 3 and 4 the main results are proved.

2. Preliminaries

In this part we will introduce some definitions and results which will be used in this paper.

**Definition 2.1.** Let \(G\) be a finite abelian group (written multiplicatively) of order \(|G|\) with identity element \(1_G\). A character \(\lambda\) of \(G\) is a homomorphism from \(G\) into the multiplicative group \(U\) of complex numbers of absolute value 1, that is, a mapping from \(G\) into \(U\) with

\[ \lambda(g_1 g_2) = \lambda(g_1) \lambda(g_2), \quad \text{for all } g_1, g_2 \in G. \]

We note that \(\lambda(g)\lambda(g^{-1}) = \lambda(gg^{-1}) = \lambda(1_G) = 1\), and so \(\lambda(g^{-1}) = \lambda(g)^{-1} = \overline{\lambda(g)}\) for every \(g \in G\), where the bar denotes complex conjugation. With each character \(\lambda\) of \(G\) there is associated the conjugate character \(\overline{\lambda}\) defined by \(\overline{\lambda}(g) = \overline{\lambda(g)}\) for all \(g \in G\).

In finite field \(\mathbb{F}_q\), there are two finite abelian groups that are of significance, namely, the additive group and the multiplicative group of the field. Therefore, we will have to make an important distinction between the characters pertaining to these two group structures.

Consider first the additive group of \(\mathbb{F}_q\). Let \(p\) be the characteristic of \(\mathbb{F}_q\). Then the prime field contained in \(\mathbb{F}_q\) is \(\mathbb{F}_p\), which we identify with \(\mathbb{Z}/(p)\). Let \(\Tr: \mathbb{F}_q \to \mathbb{F}_p\) be the absolute trace function from \(\mathbb{F}_q\) to \(\mathbb{F}_p\). Then the function \(\chi_1(x) = \exp(2\pi i \Tr(x)/p)\), for \(x \in \mathbb{F}_q\) is an additive character of \(\mathbb{F}_q\). The character \(\chi_1\) is called the canonical additive character of \(\mathbb{F}_q\). Moreover, every additive character can be obtained by \(\chi_c(x) = \chi_1(cx), \quad (x \in \mathbb{F}_q)\) for any \(c \in \mathbb{F}_q\). Taking \(c = 0\), we obtain the trivial character \(\chi_0\). Further, let \(\chi' = \chi(\Tr g)\) denote the lift of \(\chi\) to \(\mathbb{F}_{q^n}\).

Characters of the multiplicative group \(\mathbb{F}_q^*\) of \(\mathbb{F}_q\) are called multiplicative characters of \(\mathbb{F}_q\). Since \(\mathbb{F}_q^*\) is a cyclic group of order \(q - 1\), its characters can be easily determined: Let \(g\) be a fixed primitive element of \(\mathbb{F}_q\), for each \(j = 0, 1, \ldots, q - 2\), the function \(\psi_j\) with
Lemma 2.6. This annihilator as an ideal is called the annihilator of \( F_q \), and every multiplicative character of \( F_q \) is obtained in this way. No matter what \( g \) is, the character \( \psi \) will always represent the trivial multiplicative character, which satisfies \( \psi(c) = 1 \) for all \( c \in F_q^* \). It is clear that the group of multiplicative characters of \( F_q \) is cyclic of order \( q - 1 \) with identity element \( \psi_0 \).

For every \( \xi \in F_q^* \), denote by \( \text{ord}_q(\xi) \) the multiplicative order of \( \xi \) in \( F_q^* \).

Definition 2.2. Let \( r > 1 \) be a positive integer, and \( r | (q - 1) \). The element \( \xi \in F_q^* \) is called an \( r \)-free element if \( \gcd(r, (q - 1)/\text{ord}_q(\xi)) = 1 \).

From the definition above, we know that \( \xi \) is a primitive element if and only if \( \xi \) is a \((q - 1)\)-free element.

Lemma 2.3. (See [3].) Let \( \xi \in F_q^* \), and let \( r > 1 \) be a positive integer with \( r | (q - 1) \). Then we have

\[
\sum_{d|r} \frac{\mu(d)}{\varphi(d)} \sum_{\psi_d(\xi)} = \begin{cases} \frac{r}{\varphi(r)}, & \text{if } \xi \text{ is an } r\text{-free element,} \\ 0, & \text{otherwise,} \end{cases}
\]

where \( \mu \) is the Möbius function, and \( \varphi \) is the Euler function. The first sum runs over all positive divisors of \( r \), and the inner sum ranges over all multiplicative characters \( \psi_d \) of order \( d \).

Let \( \sigma : \xi \mapsto \xi^q \), \( \xi \in F_q^* \), and \( g(x) \in F_q[x] \). Define the operator “\( \sigma \)” as \( g(x) \circ \xi = g(\sigma) \xi \). Obviously, we have \( \xi \in F_q^* \iff \sigma^r(\xi) = \xi \iff (x^r - 1) \circ \xi = 0 \). The unique monic polynomial in \( F_q[x] \) generating this annihilator as an ideal is called the polynomial order of \( \xi \), and is denoted by \( \text{Ord}_q(\xi) \). Then we have \( \xi \in F_q^* \) if and only if \( \text{Ord}_q(\xi) | (x^n - 1) \).

Similarly to Definition 2.1, we have the following definition.

Definition 2.4. Let \( \xi \in F_q^* \), \( f(x) \in F_q[x] \) with \( f(x)/(x^n - 1) \), \( \xi \) is called an \( f(x) \)-free element if \( \gcd(f(x), (x^n - 1)/\text{ord}_q(\xi)) = 1 \).

From the definition, we get that \( \xi \in F_q^* \) is a normal element over \( F_q \) if and only if \( \xi \) is an \((x^n - 1)\)-free element.

Let \( \hat{F}_q^* \) denote the set of additive characters of \( F_q^* \). For \( \xi \in F_q^* \), \( \chi \in \hat{F}_q^* \), and \( f(x) \in F_q[x] \), define

\[
f(x) \circ \chi(\xi) = \chi(f(x) \circ \xi) = \chi(f(\sigma)\xi) =: \chi_f(\xi).
\]

Obviously, for every \( \chi \in \hat{F}_q^* \), the annihilator of \( \chi \) in \( F_q[x] \) is also the nonzero principal ideal in \( F_q[x] \).

Definition 2.5. Let \( \chi \in \hat{F}_q^* \). Then the annihilator of \( \chi \) in \( F_q[x] \) is an ideal in \( F_q[x] \), we define the monic generator of the ideal, hence unique, as the polynomial order of \( \chi \), and denote it by \( \text{Ord}_q(\chi) \).

Lemma 2.6. (See [19].) Let \( f(x) \in F_q[x] \), and \( f(x)/(x^n - 1) \), \( \xi \in F_q^* \), then we have

\[
\sum_{g|f} \frac{\mu'(g)}{\Phi_q(g)} \sum_{\chi_g(\xi)} = \begin{cases} \frac{q^{\deg f}}{\Phi_q(f)}, & \text{if } \xi \text{ is a } f(x)\text{-free element,} \\ 0, & \text{otherwise,} \end{cases}
\]

where \( \mu' \) is the Möbius function in \( F_q[x] \), and analogously to the Euler function, \( \Phi_q(g) \) is defined by \( \Phi_q(g) = \sharp(F_q[x]/gF_q[x])^* \), i.e., the number of invertible elements in the ring \( F_q[x]/gF_q[x] \), here we use the symbol \( \sharp \) to denote the cardinality of a set. The first sum runs over all monic divisors of \( f(x) \), and the inner sum ranges over all additive characters of order \( g(x) \). It is clear that there are \( \Phi_q(g) \) characters \( \chi_g \) of order \( g(x) \).
The following two lemmas on the estimation of exponential sums are essential in the proof of our main results.

**Lemma 2.7.** (See [6].) Let \( \psi \) be a multiplicative character of \( \mathbb{F}_q^* \) and \( \text{ord}(\psi) > 1 \). Then one has

\[
\left| \sum_{x \in \mathbb{F}_q^*} \psi(x + x^{-1}) \right| \leq 2q^{\frac{1}{2}}. \tag{2.1}
\]

**Lemma 2.8.** (See Wan [26].) Let \( f_i(x) \) be polynomials in \( \mathbb{F}_q[x] \), \( 1 \leq i \leq l \). Let \( D_1 \) be the degree of the squarefree part of \( \prod_{i=1}^l f_i(x) \). Let \( f_{i+1}(x) \) be a rational function in \( \mathbb{F}_q(x) \). For each \( 1 \leq i \leq l \), let \( \psi_i \) be a multiplicative character of \( \mathbb{F}_q \). Define

\[
S(\chi, \psi) = \sum_{a \in \mathbb{F}_q} \psi_1(f_1(a)) \cdots \psi_l(f_l(a)) \chi(f_{i+1}(a)), \tag{2.2}
\]

where the sum is over all \( a \in \mathbb{F}_q \) such that \( f_{i+1}(a) \) is defined. Define the degree of a rational function as the degree of its numerator minus the degree of its denominator. Let \( D_2 = 0 \) if \( \text{deg}(f_{i+1}) \leq 0 \) and \( D_2 = \text{deg}(f_{i+1}) + 1 \) if \( \text{deg}(f_{i+1}) > 0 \). Let \( D_3 \) be the degree of the denominator of \( f_{i+1}(x) \) and \( D_4 \) be the degree of the squarefree part of the \( \prod_{i=1}^{l-1} f_i(x) \). Suppose that \( \chi \) is non-trivial and \( f_{i+1}(x) \) is not of the form \( r(x)^p - r(x) + c \) in \( \mathbb{F}_q(x) \). Then, we have the estimate

\[
|S(\chi, \psi)| \leq (D_1 + D_2 + D_3 + D_4 - 2)\sqrt{q}. \tag{2.3}
\]

Now, let’s introduce some further number-theoretic notations. For an integer \( N \geq 1 \), let \( \omega(N) \) be the number of distinct prime divisors of \( N \). Analogously, for a monic polynomial \( g(x) \in \mathbb{F}_q[x] \), let \( \Omega_q(g(x)) \) be the number of distinct irreducible divisors of \( g(x) \) in \( \mathbb{F}_q[x] \).

**Lemma 2.9.** (See [19].) Let \( N > 1, l > 1 \) be integers and \( \Lambda \) be a set of primes \( \leq l \). Set \( L = \prod_{r \in \Lambda} r \). Assume that every prime factor \( r < l \) of \( N \) is contained in \( \Lambda \). Then

\[
\omega(N) \leq \frac{\log N - \log L}{\log l} + \sharp(\Lambda). \tag{2.4}
\]

Let \( m \) be a positive integer and \( p_m \) be the \( m \)-th prime. Setting \( l = p_m \), \( \Lambda \) be the set of primes no greater than \( p_m \), and \( \sharp(\Lambda) = m \), we have the following inequality instead of (2.4):

\[
\omega(N) \leq \frac{\log N - \sum_{i=1}^m \log p_i}{\log p_m} + m. \tag{2.5}
\]

**Lemma 2.10.** (See [19].) Let \( q \) be a prime power and \( n \) a positive integer. Let \( T(x) = x^n - 1 \) and \( \Omega = \Omega_q(T(x)) \). Then we have \( \Omega \leq \lfloor n + \gcd(n, q - 1) \rfloor / 2 \). In particular, \( \Omega \leq n \) and \( \Omega = n \) if and only if \( n | (q - 1) \). Moreover \( \Omega \leq \frac{3q}{4} n \), if \( q - 1 \) is not divisible by \( n \).

By Lemmas 2.3 and 2.6, we construct two characteristic polynomials to verify the primitivity and normality of an element respectively.

Let \( \xi \in \mathbb{F}_{q^n} \) and \( d \) be a positive integer. Define

\[
P(d, \xi) = \frac{\mu(d)}{\varphi(d)} \sum_{\psi \mid d} \psi_d(\xi), \quad \text{and} \quad P(\xi) = \frac{\varphi(q^n - 1)}{q^n - 1} \sum_{d | (q^n - 1)} P(d, \xi),
\]
Theorem 3.1.

3. The case of \( \psi_d \) and \( \psi_h \) are trivial or not: 

where \( \mu \) is the Möbius function, \( \phi \) is the Euler function, \( \sum_{\psi_d} \) ranges over all multiplicative characters of \( \mathbb{F}_{q^n} \) having order exactly \( d \), and \( \sum_{d|(q^n-1)} \) runs over all positive divisors of \( q^n - 1 \). Obviously from Lemma 2.3, one has 

\[
P(\xi) = \begin{cases} 
1, & \text{if } \xi \text{ is a primitive element}, \\
0, & \text{otherwise}.
\end{cases}
\]

Similarly, let \( G \in \mathbb{F}_q[x] \) be monic and dividing \( (x^n - 1) \), \( \xi \in \mathbb{F}_{q^n} \). Define 

\[
R(G, \xi) = \frac{\mu'(G)}{\Phi_q(G)} \sum_{G} \chi_G(\xi), \quad \text{and} \quad R(\xi) = \frac{\Phi_q(x^n - 1)}{q^n} \sum_{G|(x^n-1)} R(G, \xi),
\]

where \( \mu' \) is the Möbius function, \( \sum_{\chi_G} \) ranges over all additive characters of \( \mathbb{F}_{q^n} \) having order exactly \( G(\xi) \), and \( \sum_{G|(x^n-1)} \) runs over all monic divisors of \( x^n - 1 \) in \( \mathbb{F}_q[x] \). Then by Lemma 2.6 we get 

\[
R(\xi) = \begin{cases} 
1, & \text{if } \xi \text{ is a normal element}, \\
0, & \text{otherwise}.
\end{cases}
\]

For the sake of brevity, we define the notations: 
\[ L = \frac{\phi(q^n-1)}{q^n-1}, \quad M = \frac{\Phi_q(x^n-1)}{q^n}. \]

### 3. The case of \( (q, n) \in U_1 \)

Now we present a sufficient condition for the existence of element \( \xi \) such that both \( \xi \) and \( \xi + \xi^{-1} \) are primitive in \( \mathbb{F}_{q^n} \); that is, a sufficient condition for the pair of \( (q, n) \) such that \( (q, n) \in U_1 \).

**Theorem 3.1.** Let \( q = 2^i \) and \( n \) be a positive integer, \( \gcd(n, q) = 1 \), let \( \omega = \omega(q^n - 1) \). If \( q^\frac{n}{2} > 2^{2\omega} \), then \( (q, n) \in U_1 \).

**Proof.** Let \( N_1(q, n) \) denote the number of \( \xi \) satisfying that both \( \xi \) and \( \xi + \xi^{-1} \) are primitive elements over \( \mathbb{F}_{q^n} \). Then we have \( N_1(q, n) > 0 \) if and only if \( (q, n) \in U_1 \). According to the definition of the characteristic polynomial \( P(\xi) \) above, we obtain 

\[
N_1(q, n) = \sum_{\xi \in \mathbb{F}_{q^n}^*} P(\xi)P(\xi + \xi^{-1}) 
= L^2 \sum_{\xi \in \mathbb{F}_{q^n}^*} \sum_{d|(q^n-1)} P(d, \xi)P(h, \xi + \xi^{-1}).
\]

Below we divide the calculation of \( N_1(q, n) \) into the following four cases (see Table 1) according to the multiplicative characters \( \psi_d \) and \( \psi_h \) are trivial or not:

<table>
<thead>
<tr>
<th>Case</th>
<th>The partial sum</th>
<th>Case</th>
<th>The partial sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1(1). ( d = 1 ) and ( h = 1 )</td>
<td>( N_{11}(q, n) )</td>
<td>1(2). ( d \neq 1 ) and ( h = 1 )</td>
<td>( N_{121}(q, n) )</td>
</tr>
<tr>
<td>1(3). ( d = 1 ) and ( h \neq 1 )</td>
<td>( N_{113}(q, n) )</td>
<td>1(4). ( d \neq 1 ) and ( h \neq 1 )</td>
<td>( N_{141}(q, n) )</td>
</tr>
</tbody>
</table>
Case 1(1). $d = 1$ and $h = 1$. In this case, we have

$$N_{1(1)}(q, n) = L^2 \sum_{\xi \in \mathbb{F}_{q^n}^*} P(1, \xi) P(1, \xi + \xi^{-1}) = L^2 (q^n - 1) = \frac{(\varphi(q^n - 1))^2}{q^n - 1}.$$  

Case 1(2). $d \neq 1$ and $h = 1$. In this case, we have

$$N_{1(2)}(q, n) = L^2 \sum_{\xi \in \mathbb{F}_{q^n}^*} P(d, \xi) P(1, \xi + \xi^{-1})$$

$$= \sum_{1 < d | (q^n - 1)} \frac{\mu(d)}{\varphi(d)} \sum_{\psi_d} \sum_{\xi \in \mathbb{F}_{q^n}^*} \psi_d(\xi).$$

Since $\psi_d$ is a multiplicative character of order $d > 1$, we know that

$$N_{1(2)}(q, n) = \sum_{1 < d | (q^n - 1)} \frac{\mu(d)}{\varphi(d)} \sum_{\psi_d} \sum_{\xi \in \mathbb{F}_{q^n}^*} \psi_d(\xi) = 0.$$  

Case 1(3). $d = 1$ and $h \neq 1$. In this case, we have

$$N_{1(3)}(q, n) = L^2 \sum_{\xi \in \mathbb{F}_{q^n}^*} P(1, \xi) P(h, \xi + \xi^{-1})$$

$$= L^2 \sum_{1 < h | (q^n - 1)} \frac{\mu(h)}{\varphi(h)} \sum_{\psi_h} \sum_{\xi \in \mathbb{F}_{q^n}^*} \psi_h(\xi + \xi^{-1}).$$

Similar to the computing of $N_{1(2)}(q, n)$, one has

$$\left| N_{1(3)}(q, n) \right| \leq L^2 \sum_{1 < h | (q^n - 1)} \frac{1}{\varphi(h)} \sum_{\psi_h} \left| \sum_{\xi \in \mathbb{F}_{q^n}^*} \psi_h(\xi + \xi^{-1}) \right|,$$

since $|\mu(h)| \leq 1$, $\sum_{\psi_h} 1 = 2^\omega - 1$, $\sum_{\psi_h} \psi_h = \varphi(h)$ and due to Lemma 2.7, one has

$$\left| N_{1(3)}(q, n) \right| \leq L^2 \sum_{1 < h | (q^n - 1)} \frac{1}{\varphi(h)} \sum_{\psi_h} 2q^n$$

$$= 2L^2 q^n (2^\omega - 1).$$  

Case 1(4). $d \neq 1$ and $h \neq 1$. Now we have

$$N_{1(4)}(q, n) = L^2 \sum_{\xi \in \mathbb{F}_{q^n}^*} P(d, \xi) P(h, \xi + \xi^{-1})$$

$$= L^2 \sum_{1 < d, h | (q^n - 1)} \frac{\mu(d) \mu(h)}{\varphi(d) \varphi(h)} \sum_{\psi_d, \psi_h} \sum_{\xi \in \mathbb{F}_{q^n}^*} \psi_d(\xi) \psi_h(\xi + \xi^{-1}).$$
Thus

\[ |N_{1(4)}(q, n)| \leq L^2 \sum_{1<d,h|(q^n-1)} \frac{1}{\varphi(d)\varphi(h)} \left| \sum_{\xi \in \mathbb{F}_q^n} \psi_d(\xi) \psi_h(\xi + \xi^{-1}) \right|. \]

For the exponential sum \( \sum_{\xi \in \mathbb{F}_q^n} \psi_d(\xi) \psi_h(\xi + \xi^{-1}) \) over \( \mathbb{F}_q \) of characteristic 2, we have the following transformation:

\[
\sum_{\xi \in \mathbb{F}_q^n} \psi_d(\xi) \psi_h(\xi + \xi^{-1}) = \sum_{\xi \in \mathbb{F}_q^n} \psi_d(\xi) \psi_h(\xi^2 + 1) \psi_h(\xi)
\]

\[
= \sum_{\xi \in \mathbb{F}_q^n} (\psi_d \psi_h(\xi)) \psi_h^2(\xi + 1)
\]

\[
= \sum_{\xi \in \mathbb{F}_q^n} \psi_1(\xi) \psi_2(\xi + 1),
\]

where \( \psi_1 = \psi_d \psi_h \), and \( \psi_2 = \psi_h^2 \). From a known result regarding Jacobi sums [20], we have

\[
\left| \sum_{\xi \in \mathbb{F}_q^n} \psi_d(\xi) \psi_h(\xi + \xi^{-1}) \right| = \left| \sum_{\xi \in \mathbb{F}_q^n} \psi_1(\xi) \psi_2(\xi + 1) \right| \leq q^n.
\]

So we have

\[
|N_{1(4)}(q, n)| \leq L^2 (2^{2\omega} - 1)^2 q^n.
\]

Since \( N_1(q, n) = N_{1(1)}(q, n) + N_{1(2)}(q, n) + N_{1(3)}(q, n) + N_{1(4)}(q, n) \), from the above estimations, one has

\[
\left| N_1(q, n) - \frac{(\varphi(q^n - 1))^2}{q^n - 1} \right| \leq |N_{1(3)}(q, n)| + |N_{1(4)}(q, n)|
\]

\[
\leq L^2 [2q^n(2^{2\omega} - 1) + (2^{2\omega} - 1)^2 q^n].
\]

In order to get \( N_1(q, n) > 0 \), it is sufficient to have

\[
\frac{\varphi(q^n - 1)^2}{q^n - 1} > L^2 [2q^n(2^{2\omega} - 1) + (2^{2\omega} - 1)^2 q^n],
\]

which is equivalent to:

\[
q^n \frac{q^2 - 1}{q^n} > 2(2^{2\omega} - 1) + (2^{2\omega} - 1)^2.
\] (3.1)

Obviously, a sufficient condition for the validity of (3.1) is

\[
q^n > 2^{2\omega}.
\] (3.2)

In conclusion, if \( q^n > 2^{2\omega} \), then \( (q, n) \in U_1 \). \( \square \)
By (2.5) we get
\[ \omega(q^n - 1) \leq \frac{\log(q^n - 1) - \sum_{i=1}^{m} \log p_i}{\log p_m} + m < \frac{n \log q - \sum_{i=1}^{m} \log p_i}{\log p_m} + m. \] (3.3)

Now, (3.2) is equivalent to
\[ \omega < \frac{n \log q}{\log 16}. \] (3.4)

Thus by (3.3), we know that (3.4) holds true if
\[ \frac{n \log q}{\log 16} - \frac{n \log q}{\log p_m} > m - \sum_{i=1}^{m} \log p_i. \] (3.5)

If the left of (3.5) is positive, we have \( \frac{1}{\log 16} - \frac{1}{\log p_m} > 0 \), that is \( m \geq 7 \). So we can choose a suitable \( m \) with \( m \geq 7 \), and prove that most of \((q, n)\) satisfy (3.5). One of our main results is as follows.

**Theorem 3.2.** Let \( q = 2^s \) and let \( n \) be an odd positive integer. If \( n \geq 13 \), then \((q, n) \in U_1\).

**Proof.** Choose \( m = 15 \), then we can get that the left side of (3.5) is positive, so we have
\[ n > m - \frac{\sum_{i=1}^{m} \log p_i}{\log q} - \frac{\sum_{i=1}^{m} \log p_i}{\log p_m}. \] (3.6)

Since \( \sum_{i=1}^{m} \log p_i \leq m \log p_m \), we get that the right side of (3.6) is a decreasing function on \( q \). It is easy to check that when \( q = 32 \) and \( n \geq 13 \), the inequality (3.6) is true. That is, when \( q \geq 32 \) and \( n \geq 13 \), \((q, n) \in U_1\). \( \square \)

**Remark 1.** When \( q < 32 \), that is \( s < 5 \), by using the software Mathematica 4.1 we obtain the pairs of \((q, n)\) such that \((q, n) \in U_1\), the result is listed in Table 2.

### 4. The case of \((q, n) \in U_2\)

In this section, we present a sufficient condition for the existence of element \( \xi \) such that both \( \xi \) and \( \xi + \xi^{-1} \) are primitive in \( \mathbb{F}_{q^n} \) and \( \xi \) is again normal in \( \mathbb{F}_{q^n} \), that is, a sufficient condition for the pairs of \((q, n)\) such that \((q, n) \in U_2\).

**Theorem 4.1.** Let \( q = 2^s \) and \( n \) be a positive integer with \( \gcd(n, q) = 1 \), \( T = x^n - 1 \), \( \Omega = \Omega_q(T) \), \( \Phi(T) = \Phi_q(T) \), and \( \omega = \omega(q^n - 1) \). If \( q^n > 2^{2\omega + \Omega} \), then \((q, n) \in U_2\).

**Proof.** Let \( N_2(q, n) \) denote the number of \( \xi \) satisfying that both \( \xi \) and \( \xi + \xi^{-1} \) are primitive elements, and \( \xi \) is also a normal element of \( \mathbb{F}_{q^n} \). Then we have \( N_2(q, n) > 0 \) if and only if \((q, n) \in U_2\). According
Table 3
Cases of $N_{2}(q,n)$.

<table>
<thead>
<tr>
<th>Case</th>
<th>The partial sum</th>
<th>Case</th>
<th>The partial sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2(1). d = 1, h = 1, G = 1$</td>
<td>$N_{2(1)}(q,n)$</td>
<td>$2(2). d \neq 1, h = 1, G = 1$</td>
<td>$N_{2(2)}(q,n)$</td>
</tr>
<tr>
<td>$2(3). d = 1, h \neq 1, G = 1$</td>
<td>$N_{2(3)}(q,n)$</td>
<td>$2(4). d \neq 1, h \neq 1$ and $G = 1$</td>
<td>$N_{2(4)}(q,n)$</td>
</tr>
<tr>
<td>$2(5). d = 1, h = 1, G \neq 1$</td>
<td>$N_{2(5)}(q,n)$</td>
<td>$2(6). dh \neq 1, G \neq 1$</td>
<td>$N_{2(6)}(q,n)$</td>
</tr>
</tbody>
</table>

To the definition of the characteristic polynomial $P(\xi)$ and $R(\xi)$ above, we get that

$$N_{2}(q,n) = \sum_{\xi \in \mathbb{F}_{q^n}^*} P(\xi) P(\xi + \xi^{-1}) R(\xi)$$

$$= L^2 M \sum_{\xi \in \mathbb{F}_{q^n}^*} \sum_{d,h|(q^n-1)} \sum_{G|\mathbb{T}} P(d,\xi) P(h,\xi + \xi^{-1}) R(G,\xi).$$

Similarly to the proof of Theorem 3.1, we divide the calculation of $N_{2}(q,n)$ into the following six cases (see Table 3):

**Case 2(1).** When $d = 1, h = 1$ and $G = 1$, we have

$$N_{2(1)}(q,n) = L^2 M \sum_{\xi \in \mathbb{F}_{q^n}^*} P(1,\xi) P(1,\xi + \xi^{-1}) R(1,\xi)$$

$$= L^2 M \sum_{\xi \in \mathbb{F}_{q^n}^*} 1 = L^2 M (q^n - 1) = \frac{(\varphi(q^n - 1))^2}{q^n - 1} M.$$  

**Case 2(2).** When $d \neq 1, h = 1$ and $G = 1$, we have

$$N_{2(2)}(q,n) = L^2 M \sum_{\xi \in \mathbb{F}_{q^n}^*} \sum_{1 < d|(q^n-1)} P(d,\xi) P(1,\xi + \xi^{-1}) R(1,\xi) = MN_{1(2)}(q,n).$$

thus $N_{2(2)}(q,n) = 0$.

**Case 2(3).** When $d = 1, h \neq 1$ and $G = 1$, we have

$$N_{2(3)}(q,n) = L^2 M \sum_{\xi \in \mathbb{F}_{q^n}^*} \sum_{1 < h|(q^n-1)} P(1,\xi) P(h,\xi + \xi^{-1}) R(1,\xi) = MN_{1(3)}(q,n),$$

so $|N_{2(3)}(q,n)| \leq 2L^2 M q^n 2^{\varphi(q^n - 1)}$.

**Case 2(4).** When $d \neq 1, h \neq 1$ and $G = 1$, we have

$$N_{2(4)}(q,n) = L^2 M \sum_{\xi \in \mathbb{F}_{q^n}^*} \sum_{1 < d,h|(q^n-1)} P(d,\xi) P(h,\xi + \xi^{-1}) R(1,\xi) = MN_{1(4)}(q,n),$$

thus $|N_{2(4)}(q,n)| \leq L^2 M (2^{\varphi(q^n - 1)}) 2 q^n$. 

Case 2(5). When \( d = 1, h = 1 \) and \( G \neq 1 \), we have

\[
N_{2(5)}(q, n) = L^2 M \sum_{\xi \in \mathbb{F}_q^n} \sum_{1 < G | T} P(1, \xi) P(1, \xi + \xi^{-1}) R(G, \xi)
\]

\[
= \sum_{\xi \in \mathbb{F}_q^n} \sum_{1 < G | T} R(G, \xi)
\]

\[
= \sum_{1 < G | T} \mu(G) \sum_{\chi \in \mathbb{F}_q^n} \chi G(\xi),
\]

by the properties of additive characters in finite fields, for \( G \neq 1 \), we have \( |\sum_{\xi \in \mathbb{F}_q^n} \chi G(\xi)| = 1 \). Since \( |\mu(G')| \leq 1 \), \( \sum_{|G| = 1} 2^{2^2} - 1 \), and \( \sum_{\chi} 1 = \Phi(G) \), one has

\[
|N_{2(5)}(q, n)| \leq L^2 M \sum_{G|T, G \neq 1} \frac{1}{\Phi(G)} \sum_{\chi \in \mathbb{F}_q^n} \chi G(\xi)
\]

\[
= L^2 M (2^{2^2} - 1).
\]

Case 2(6). When \( dh \neq 1 \) and \( G \neq 1 \), we have

\[
N_{2(6)}(q, n) = L^2 M \sum_{\xi \in \mathbb{F}_q^n} \sum_{1 < d, h | (q^n - 1)} \sum_{1 < G | T} P(d, \xi) P(h, \xi + \xi^{-1}) R(G, \xi)
\]

\[
= L^2 M \sum_{1 < d, h | (q^n - 1)} \sum_{1 < G | T} \frac{\mu(d) \mu(h) \mu(G)}{\varphi(d) \varphi(h) \Phi(G)} \sum_{\psi_d} \sum_{\psi_h} \sum_{\chi \in \mathbb{F}_q^n} \psi_d(\xi) \psi_h(\xi + \xi^{-1}) \chi G(\xi).
\]

Thus

\[
|N_{2(6)}(q, n)| \leq L^2 M \sum_{1 < d, h | (q^n - 1)} \sum_{1 < G | T} \frac{1}{\varphi(d) \varphi(h) \Phi(G)} \sum_{\psi_d} \sum_{\psi_h} \sum_{\chi \in \mathbb{F}_q^n} \psi_d(\xi) \psi_h(\xi + \xi^{-1}) \chi G(\xi),
\]

where

\[
\left| \sum_{\xi \in \mathbb{F}_q^n} \psi_d(\xi) \psi_h(\xi + \xi^{-1}) \chi G(\xi) \right| = \left| \sum_{\xi \in \mathbb{F}_q^n} \psi_d(\xi) \psi_h(\xi^2 + 1) \psi_h^{-1}(\xi) \chi G(\xi) \right|.
\]

(4.1)

By Lemma 2.8, we have \( \left| \sum_{\xi \in \mathbb{F}_q^n} \psi_d(\xi) \psi_h(\xi^2 + 1) \psi_h^{-1}(\xi) \chi G(\xi) \right| \leq q^2 \). Hence, \( |N_{2(6)}(q, n)| \leq L^2 M (2^{2^2} - 1)(2^2 - 1)q^2 \). Since

\[
N_2(q, n) = N_{2(1)}(q, n) + N_{2(2)}(q, n) + N_{2(3)}(q, n) + N_{2(4)}(q, n) + N_{2(5)}(q, n) + N_{2(6)}(q, n),
\]

we know that
\[
N_2(q, n) - \frac{(\varphi(q^n - 1))^2}{q^n - 1} \leq \left| N_{2(3)}(q, n) \right| + \left| N_{2(4)}(q, n) \right| + \left| N_{2(5)}(q, n) \right| + \left| N_{2(6)}(q, n) \right|
\leq L^2 M [2q^{\frac{\Omega}{2}} (2^{\omega'} - 1) + (2^{\omega'} - 1)^2 q^{\frac{n}{2}} + (2^{\Omega} - 1) + (2^{2\omega'} - 1)(2^{\Omega} - 1)q^{\frac{n}{2}}].
\]

If
\[
\frac{\varphi(q^n - 1)^2}{q^n - 1} M > L^2 M [2q^{\frac{\Omega}{2}} (2^{\omega'} - 1) + (2^{\omega'} - 1)^2 q^{n/2} + (2^{\Omega} - 1) + (2^{2\omega'} - 1)(2^{\Omega} - 1)q^{n/2}],
\]
then it is obvious that \( N_2(q, n) > 0 \). It is easily seen that (4.2) is equivalent to
\[
q^n/2 - 2^{\Omega} q^{n/2} > 2(2^{\omega'} - 1) + (2^{2\omega'} - 1)(2^{\Omega} - 1) + (2^{\omega'} - 1)^2.
\]

Obviously, a sufficient condition for the validity of (4.3) is
\[
q^n/2 > 2^{2\omega' + \Omega}.
\]

In conclusion, if \( q^n/2 > 2^{2\omega' + \Omega} \), then \((q, n) \in U_2.\)

If \(\Omega \leq a n\) for a nonnegative number \(a\), then by Lemma 2.9, we know that (4.4) holds true if
\[
\left( \frac{n}{\log 4} - \frac{2n}{\log p_m} \right) \log q > 2m + na - 2 \sum_{i=1}^{m} \frac{\log p_i}{\log p_m},
\]
which is equivalent to
\[
\left( \frac{\log q}{\log 4} - \frac{2 \log q}{\log p_m} - a \right) n > 2m - 2 \sum_{i=1}^{m} \frac{\log p_i}{\log p_m}.
\]

If the left of (4.5) is positive, we have \( \frac{1}{\log 4} - \frac{2}{\log p_m} > 0 \), that is \( m \geq 7 \). So on the condition of \( m \geq 7 \), we can choose a suitable \( m \), and prove that most of \((q, n)\) satisfy (4.4).

By Lemma 2.10, we know that \(\Omega\) is decided by \( q - 1 \) being divisible by \( n \) or not. So we distinguish the following two cases:

Case a: When \( n \mid (q - 1) \), according to Lemma 2.10, we have \(\Omega = n\).
Case b: When \( n \nmid (q - 1) \), according to Lemma 2.10, we have \(\Omega \leq 3\frac{4}{3} n\).

Firstly, we consider Case a. In this case, we have

**Theorem 4.2.** Let \( q = 2^s \), and \( n \) be an odd positive integer with \( n \mid (q - 1) \). If \( n \geq 33 \), then \((q, n) \in U_2\).

**Proof.** Now \(\Omega = n\), that is, \( a = 1 \). Choose \( m = 32 \). Then from (4.5) we have
\[
\log q > \frac{1 + (2m - 2 \sum_{i=1}^{m} \frac{\log p_i}{\log p_m})/n}{\frac{1}{\log 4} - \frac{2}{\log p_m}}.
\]
Table 4
\[\begin{array}{c|c|c|c|c|c|c|c}
 n & 1 & 3 & 5 & 7 & 9 & 11 & 13 \\
 \hline
 s \geq & 80 & 30 & 20 & 16 & 13 & 12 & 11 \\
\end{array}\]
\[\begin{array}{c|c|c|c|c|c|c|c}
 n & 15 & 17 & 19 & 21 & 23 & 25 & 27 \\
 \hline
 s \geq & 10 & 99988888 & 8 & 8 & 8 & 8 & 8 \\
\end{array}\]

Table 5
\[\begin{array}{c|c|c}
 n \nmid (q-1), (q,n) \in U_2. \\
 \hline
 s = & 4 & 5 \\
 n \geq & 110 & 48 \\
\end{array}\]

By \( \sum_{i=1}^{m} \log p_i \leq m \log p_m \), and note that the right side of (4.7) is a decreasing function on \( n \). It is easy to check that when \( n = 33 \), \( q \) should be bigger than 120. Noticing \( q \) is a power of 2, when \( n \geq 33 \) and \( n \mid (q-1) \), then \( q \) is obviously larger than 120. Hence in this case \((q,n) \in U_2.\) \(\square\)

Remark 2. When \( n < 33 \), we give the range of \( s \) such that \((2^s, n) \in U_2\) in Table 4. Here we just need to consider the case of \( n \) being odd.

Now, let’s consider Case b. For this case, we have the following result.

Theorem 4.3. Let \( q = 2^s \) and \( n \) be odd with \( n \nmid (q-1) \). If \( n \geq 30 \) and \( s \geq 6 \), then \((q,n) \in U_2.\)

Proof. Now \( \Omega = 3/4 \), that is, \( a = 3/4 \) in (4.6). Choose \( m = 40 \). When \( q > 10 \), the left side of (4.6) is positive. By (4.6) we have

\[ n \geq \frac{2m - \frac{2 \sum_{i=1}^{m} \log p_i}{\log q} - \frac{2 \log q}{\log p_m} - \frac{3}{4}}{2 \log q}. \] (4.8)

Obviously the right side of (4.8) is a decreasing function on \( q \). It is clear that when \( q \geq 64 \), that is, \( s \geq 6 \), and \( n \geq 30 \), the inequality is true. So we have \((q,n) \in U_2\) if \( s \geq 6 \) and \( n \geq 30 \). \(\square\)

Remark 3. For positivity of the left side of (4.6), \( s \) must be bigger than 3. Now we give the range of \( n \) such that \((q,n) \in U_2\) when \( 3 < s < 6 \) in Table 5.

5. Conclusion remark

In this paper, we just discuss the case of finite fields with even characteristic. According to our results, for large enough \( q \) and \( n \), there are always some elements \( \xi \) in the finite field \( \mathbb{F}_{q^n} \), such that \( \xi \) is primitive (or primitive normal) and meanwhile \( \xi + \xi^{-1} \) is primitive. However, the aforementioned conclusion also holds for finite fields with odd characteristic. By some slightly modifications, one can obtain similar results. To say it more explicitly, one can overcome the difficulty of estimating the related exponential sums by using Wan’s lemma (Lemma 2.8 in this paper) and obtain similar results in finite fields with general characteristic. The reason that we just present here the results in finite fields of characteristic 2 instead of the general finite fields, is based on the fact that the finite fields of characteristic 2 have more applicative backgrounds, especially for the application of Gauss periods.

Furthermore, for \( q = 2^s \), and \( n \) is even, we can also use the results we obtained above. For example, let \( t \) be odd and \( n = 2t \). Then \( q^n = q^t \), where \( q' = 2^{t+1} \). In order to discuss \((q,n) \in U_i, i = 1, 2\), we just need to consider \((q', t)\).
Acknowledgments

The research of the present work was supported by the NNSF of China (Grant No. 10971250). The authors would like to express their grateful thankfulness to the anonymous referees for their careful reading of the manuscript of the presented paper and helpful comments. The authors also thank Professor Daqing Wan for the permission of using the unpublished (forthcoming) result in [26].

References