Existence Conditions for Self-Orthogonal Negacyclic Codes over Finite Fields*

Liren Lin[1], Bocong Chen[2], Hongwei Liu[1]

[1]School of Mathematics and Statistics, Central China Normal University, Wuhan, Hubei, 430079, China
[2]School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637616, Singapore

Abstract

In this paper, we obtain necessary and sufficient conditions for the nonexistence of nonzero self-orthogonal negacyclic codes over a finite field, of length relatively prime to the characteristic of the underlying field.

Keywords: Cyclic code, negacyclic code, self-orthogonal code, cyclotomic coset.

2010 Mathematics Subject Classification: 11T71; 94B15

1 Introduction

The issues concerning existence conditions, algebraic structures and enumerations for self-dual codes have been hot research topics in the theory of error-correcting codes (e.g. see [1], [2]-[10], [14], [16]). As a natural generalization of self-dual codes, self-orthogonal codes also have received a lot of attention.

In [6], Fu and Feng gave characterizations for self-orthogonal abelian codes in the group algebra FG, where F is a finite field with characteristic p and G is a finite abelian group with cyclic Sylow p-subgroup. In [1], assuming that p is an odd prime, Bakshi and Rake obtained a nonexistence condition for nonzero self-orthogonal negacyclic codes of length $2p^n$ over a finite field, where the characteristic of the base field is coprime to $2p$.

In [13], Pless linked self-orthogonal and self-dual cyclic codes with the class of duadic codes, and presented some conditions for the nonexistence of nonzero self-orthogonal cyclic codes. Recently, Kathuria and Raka [11] pointed out that [13, Theorem 8] is incorrect, and tried to obtain necessary and sufficient

*E-Mail addresses: lirenlin86@yahoo.com (L. Lin), bocong_chen@yahoo.com (B. Chen), hwliu@mail.ccnu.edu.cn (H. Liu).

conditions for the nonexistence of nonzero self-orthogonal cyclic codes over a finite field, of length relatively prime to the characteristic of the underlying field. Unfortunately, one of the main results in [11], [11, Theorem 2], is not true in general.

In this paper, we first fix the error in [11, Theorem 2]. We then exhibit necessary and sufficient conditions for the nonexistence of nonzero self-orthogonal negacyclic codes over a finite field F_q, of length relatively prime to the characteristic of F_q (see Theorem 3.5 in Section 3). It should be noted that, if nonzero self-orthogonal negacyclic codes of a given length do not exist, neither do nonzero self-orthogonal cyclic codes of the same length.

The remaining sections of this paper are organized as follows. The necessary notations and known results are provided in Section 2. In Section 3, we first give corrections to [11, Theorem 2], then we derive necessary and sufficient conditions for the nonexistence of nonzero self-orthogonal negacyclic codes.

2 Preliminaries

Let F_q be the finite field with q elements and F_q^* the multiplicative group of F_q consisting of all nonzero elements of F_q. For $\beta \in F_q^*$ we denote by $\mathrm{ord}(\beta)$ the order of β in the group F_q^*. We then know that $\mathrm{ord}(\beta)$ is a divisor of $q-1$, and β is called a *primitive* $\mathrm{ord}(\beta)$*th root of unity*.

Let N be a positive integer coprime to q and F_q^N the F_q-vector space of N-tuples. A *linear code* C of length N over F_q is an F_q-subspace of F_q^N. Let λ be a nonzero element in F_q. A linear code C of length N over F_q is called λ-*constacyclic* if $(\lambda c_{N-1}, c_0, \cdots, c_{N-2}) \in C$ for every $(c_0, c_1, \cdots, c_{N-1}) \in C$. Note that for λ =1 (respectively, $\lambda = -1$), λ-constacyclic codes are cyclic codes (respectively, negacyclic codes).

Let C be a λ-constacyclic code of length N over F_q. The *dual code of* C is defined as $C^\perp = \{u \in F_q^N \mid u \cdot v = 0, \text{for any } v \in C\}$, where $u \cdot v$ denotes the standard Euclidean inner product of u and v in F_q^N. The code C is said to be *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if $C = C^\perp$. It turns out that the dual of a λ-constacyclic code is a λ^{-1}-constacyclic code; specifically, the dual of a cyclic code (respectively, negacyclic code) is a cyclic code (respectively, negacyclic code) (e.g. see [4, Proposition 2.2.]).

We know that any λ-constacyclic code C of length N over F_q is identified with exactly one ideal of the quotient algebra $F_q[X]/\langle X^N - \lambda\rangle$, which is generated uniquely by a monic divisor $g(X)$ of $X^N - \lambda$. In this case, $g(X)$ is called the *generator polynomial* of C and we write $C = \langle g(X)\rangle$. In particular, the irreducible factorization of $X^N - \lambda$ in $F_q[X]$ determines all λ-constacyclic codes of length N over F_q.

Assume that $C = \langle g(X)\rangle$ is a λ-constacyclic code of length N over F_q, where $g(X)$ is the generator polynomial of C. Let $h(X) = \frac{X^N - \lambda}{g(X)}$ and let $\deg h(X)$ be the degree of $h(X)$. It is known that its dual code $C^\perp$ has generator polynomial

$h^*(X)$, where $h^*(X) = h(0)^{-1}X^{\deg h(X)}h(\frac{1}{X})$ is called the *reciprocal polynomial* of $h(X)$. Note that $h^*(X)$ is a monic polynomial and it divides $X^N - \lambda^{-1}$. If a polynomial is equal to its reciprocal polynomial, then it is called *self-reciprocal*.

In this paper, we only focus on cyclic and negacyclic codes over finite fields. It is known that the irreducible factors of $X^N - 1$ in $F_q[X]$ can be described by *q-cyclotomic cosets*. For any integer t, the *q-cyclotomic coset* C_t *of* t *modulo* N is defined by

$$C_t = \{t \cdot q^j \pmod N \,|\, j = 0, 1, \cdots\}.$$

Let $\{0, i_1, \cdots, i_h\}$ be a *complete set of representatives* of all q-cyclotomic cosets modulo N; this means that $\{0, i_1, \cdots, i_h\}$ is a subset of $\{0, 1, \cdots, N-1\}$, $C_{i_0} = \{0\}, C_{i_1}, C_{i_2}, \cdots, C_{i_h}$ are distinct and $\bigcup_{k=0}^{h} C_{i_k} = \{0, 1, \cdots, N-1\}$.

Take η to be a primitive Nth root of unity (maybe in an extension of F_q), and denote by $M_{i_j}(X)$, the minimal polynomial of η^{i_j} over F_q, for each $0 \le j \le h$. It is well known that (e.g. see [7, Theorem 4.1.1])

$$X^N - 1 = (X-1)M_{i_1}(X)M_{i_2}(X)\cdots M_{i_h}(X)$$

with

$$M_{i_k}(X) = \prod_{j \in C_{i_k}} (X - \eta^j), \qquad k = 1, \cdots, h$$

all being monic irreducible in $F_q[X]$.

Write

$$X^N - 1 = f_1(X)f_2(X)\cdots f_u(X)h_1(X)h_1^*(X)h_2(X)h_2^*(X)\cdots h_v(X)h_v^*(X)$$

where $f_i(X)$, $1 \le i \le u$, are monic irreducible self-reciprocal polynomials over F_q while $h_j(X)$ and its reciprocal polynomial $h_j^*(X)$ are both monic irreducible polynomials over F_q.

Suppose $C = \langle g(X) \rangle$ is a nonzero cyclic code of length N over F_q with generator polynomial $g(X)$. We can assume that

$$g(X) = f_1(X)^{\tau_1}\cdots f_u(X)^{\tau_u}h_1(X)^{\sigma_1}h_1^*(X)^{\omega_1}\cdots h_v(X)^{\sigma_v}h_v^*(X)^{\omega_v}$$

where each $\tau_i, \sigma_j, \omega_k$ is equal to 0 or 1. Then

$$h(X) = f_1(X)^{1-\tau_1}\cdots f_u(X)^{1-\tau_u}h_1(X)^{1-\sigma_1}h_1^*(X)^{1-\omega_1}\cdots h_v(X)^{1-\sigma_v}h_v^*(X)^{1-\omega_v}.$$

Hence

$$h^*(X) = f_1(X)^{1-\tau_1}\cdots f_u(X)^{1-\tau_u}h_1(X)^{1-\omega_1}h_1^*(X)^{1-\sigma_1}\cdots h_v(X)^{1-\omega_v}h_v^*(X)^{1-\sigma_v}.$$

We know that C is self-orthogonal if and only if $h^*(X) \mid g(X)$, i.e.,

$$\begin{cases} 1 \le 2\tau_i, & \text{for each } 1 \le i \le u, \\ 1 \le \sigma_j + \omega_j, & \text{for each } 1 \le j \le v. \end{cases} \tag{2.1}$$

In this case, $C = \langle f_1(X)f_2(X)\cdots f_u(X)h_1(X)^{\sigma_1}h_1^*(X)^{\omega_1}\cdots h_v(X)^{\sigma_v}h_v^*(X)^{\omega_v}\rangle$, where $\sigma_j + \omega_j \ge 1$ for all j. In the light of the above discussion we have the following result.

Remark 2.1. *The following statements are equivalent:*

(i) Nonzero self-orthogonal cyclic codes of length N over F_q do not exist.

(ii) All the monic irreducible factors of $X^N - 1$ over F_q are self-reciprocal.

(iii) There exists an integer i such that $q^i \equiv -1 \pmod{N}$.

(iv) The q-cyclotomic coset modulo N containing 1 is equal to the q-cyclotomic coset modulo N containing -1, i.e. $C_1 = C_{-1}$.

Note that the equivalence of (i) *and* (iv) *appeared previously in [11, Lemma 1].*

An argument similar to the one above shows that, nonzero self-orthogonal negacyclic codes of length N over F_q do not exist if and only if all the monic irreducible factors of $X^N + 1$ over F_q are self-reciprocal.

Observe that $X^N + 1$ divides $X^{2N} - 1$ in $F_q[X]$. Assume that $\gcd(2N, q) = 1$. Let D_1 be the q-cyclotomic coset modulo $2N$ containing 1 and let ζ be a primitive $2N$th root of unity in some extension field of F_q. Since $\zeta^N = -1$, it follows that $\prod_{j \in D_1}(X - \zeta^j)$ is a monic irreducible factor of $X^N + 1$ over F_q. By Remark 2.1, we have the following result.

Remark 2.2. *Assume that* $\gcd(2N, q) = 1$. *The following statements are equivalent:*

(i) Nonzero self-orthogonal negacyclic codes of length N over F_q do not exist.

(ii) All the monic irreducible factors of $X^N + 1$ over F_q are self-reciprocal.

(iii) All the monic irreducible factors of $X^{2N} - 1$ over F_q are self-reciprocal.

Finally, we reproduce the irreducible factorization of $X^{2^\ell} - 1$ and $X^{2^\ell} + 1$ in $F_q[X]$, where ℓ is a positive integer and $q \equiv 3 \pmod{4}$. The irreducible factorization of $X^{2^\ell} - 1$ and $X^{2^\ell} + 1$ in $F_q[X]$ have been characterized precisely in [3]. We should mention that, though [3, Theorem 1] and [3, Corollary 4] are proved for a prime field F_p with $p \equiv 3 \pmod{4}$, one can check in the same way as in [3] that it also holds for the present case that q is a power of a prime and $q \equiv 3 \pmod{4}$.

Note that $4 \,|\, (q + 1)$ in the present case, hence there is a unique integer $a \geq 2$ such that $2^a \| (q + 1)$, where the notation $2^a \| (q + 1)$ means $2^a \,|\, (q + 1)$ but $2^{a+1} \nmid (q + 1)$. We reformulate the result as follows.

Lemma 2.3. Assume that $q \equiv 3 \pmod{4}$. Set $G_1 = \{0\}$; recursively define

$$G_i = \left\{ \pm \left(\tfrac{g+1}{2}\right)^{\frac{q+1}{4}} \,\middle|\, g \in G_{i-1} \right\},$$

for $i = 2, 3, \cdots, a - 1$; and set

$$G_a = \left\{ \pm \left(\tfrac{g-1}{2}\right)^{\frac{q+1}{4}} \,\middle|\, g \in G_{a-1} \right\}.$$

If $1 \leq \ell \leq a-1$, then

$$X^{2^\ell}+1 = \prod_{g \in G_\ell} (X^2 - 2gX + 1);$$

if $\ell \geq a$, then

$$X^{2^\ell}+1 = \prod_{g \in G_a} (X^{2^{\ell-a+1}} - 2gX^{2^{\ell-a}} - 1).$$

If $1 \leq \ell \leq a$, then

$$X^{2^\ell}-1 = (X-1)(X+1)\prod_{i=1}^{\ell-1}\prod_{g \in G_i} (X^2 - 2gX + 1);$$

if $\ell \geq a+1$, then

$$X^{2^\ell}-1 = (X-1)(X+1)\prod_{\substack{g \in G_i,\\ 1 \leq i \leq a-1}} (X^2-2gX+1) \prod_{\substack{g \in G_a,\\ 0 \leq j \leq (\ell-a-1)}} (X^{2^{j+1}} - 2gX^{2^j} - 1).$$

All the factors in the above products are irreducible over F_q.

3 Main Results

Let F_q be the finite field with q elements. Let ℓ be a positive integer and $n' > 1$ an odd positive integer. Write $n' = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$, where p_j are distinct odd primes and λ_j are positive integers for $1 \leq j \leq r$.

In the first subsection, after providing a counterexample of [11, Theorem 2], we give corrections to this result. We then derive necessary and sufficient conditions for the nonexistence of nonzero self-orthogonal negacyclic codes in subsection 3.2.

3.1 Nonexistence conditions for self-orthogonal cyclic codes

In [11, Theorem 2], it asserts that: *Let $n = 2^{\lambda_0} p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$, where $\lambda_0 \geq 2$, p_j are distinct odd primes and λ_j are positive integers for $1 \leq j \leq r$. Non-trivial self-orthogonal cyclic codes of length n over F_q with $\gcd(n,q) = 1$ do not exist if and only if $\lambda_0 = 2$ or 3; $q \equiv 3 \pmod 4$ if $\lambda_0 = 2$, $q \equiv 7 \pmod 8$ if $\lambda_0 = 3$ and $\mathrm{ord}_{p_j}(q)$ is even but not divisible by 4 for each j, $1 \leq j \leq r$.*

This result is not true in general. For example take $\lambda_0 = 4$, $p_1 = 7$, $\lambda_1 = 1$ and $q = 31$. In other words, consider cyclic codes of length $2^4 \cdot 7 = 112$ over F_{31}. The 31-cyclotomic coset containing 1 modulo 112 is given by:

$$C_1 = \{1, 31, 65, 111, 81, 47\} = C_{111} = C_{-1}.$$

This implies that non-trivial self-orthogonal cyclic codes of length 112 over F_{31} do not exist, but $\lambda_0 = 4 > 3$. We mention that the statement in the proof of

[11, Theorem 2], $\mathrm{ord}_{2^{\lambda_0}}(q) = 2^{\lambda_0-2}$ for $\lambda_0 \geq 3$, is incorrect. (It is easy to check that $\mathrm{ord}_{2^4}(31) = 2$ and $2 \neq 2^{4-2}$.)

In this subsection, we fix the error in [11, Theorem 2] and give a necessary and sufficient condition under which nonzero self-orthogonal cyclic codes over F_q do not exist.

We begin with the following special case, i.e. cyclic codes of length 2^ℓ over F_q.

Lemma 3.1. *Assume that the notation as given above. Nonzero self-orthogonal cyclic codes of length 2^ℓ over F_q with $\gcd(2, q) = 1$ do not exist if and only if one of the following two statements holds:*

(i) $\ell = 1$.

(ii) $q \equiv 3 \pmod 4$ *and* $2 \leq \ell \leq a$, *where a is the positive integer with $2^a \| (q+1)$.*

Proof. Assume that nonzero self-orthogonal cyclic codes of length 2^ℓ over F_q with $\gcd(2, q) = 1$ do not exist. If $\ell = 1$, then there is nothing to prove. Hence, we may assume that $\ell \geq 2$. It follows from Remark 2.1 that there is an integer i such that $q^i \equiv -1 \pmod{2^\ell}$, which implies $4 \nmid (q-1)$. By Remark 2.1 again, all the monic irreducible factors of $X^{2^\ell} - 1$ over F_q are self-reciprocal. From Lemma 2.3, it is easy to see that $2 \leq \ell \leq a$, where a is the positive integer with $2^a \| (q+1)$.

Now, suppose that (i) or (ii) is satisfied. We know from Remark 2.1 that nonzero self-orthogonal cyclic codes of length 2^ℓ over F_q with $\gcd(2, q) = 1$ do not exist if and only if all the monic irreducible factors of $X^{2^\ell} - 1$ over F_q are self-reciprocal. The result then follows directly from Lemma 2.3. □

The following lemma has been presented in [11, Theorem 1].

Lemma 3.2. *Let $n' = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$, where p_j are distinct odd primes and λ_j are positive integers for $1 \leq j \leq r$. We assume that $\lambda_0 = 0$ or 1. Nonzero self-orthogonal cyclic codes of length $2^{\lambda_0} n'$ over F_q with $\gcd(2^{\lambda_0} n', q) = 1$ do not exist if and only if $\mathrm{ord}_{p_j}(q)$ is even and the highest power of 2 dividing $\mathrm{ord}_{p_j}(q)$ is the same for each j, $1 \leq j \leq r$.*

We adopt the following notation. For each $1 \leq j \leq r$, let $\mathrm{ord}_{p_j^{\lambda_j}}(q) = 2^{a_j} y_j$, where y_j is an odd positive integer. It has already been pointed out in [11], $2^{a_j} \| \mathrm{ord}_{p_j^{\lambda_j}}(q)$ if and only if $2^{a_j} \| \mathrm{ord}_{p_j}(q)$, and $\mathrm{ord}_{n'}(q) = 2^{a_0} z$, where $n' = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$, $a_0 = \max\{a_1, a_2, \cdots, a_r\}$ and $z = \mathrm{lcm}(y_1, y_2, \cdots, y_r)$. We have the following result.

Theorem 3.3. *With respect to the above notations, we further assume that $\ell \geq 2$ and $\gcd(2n', q) = 1$. Then there does not exist any nonzero self-orthogonal cyclic code of length $2^\ell n'$ over F_q if and only if both the following two conditions hold:*

(i) $q \equiv 3 \pmod 4$ *and* $2 \le \ell \le a$, *where* a *is the positive integer with* $2^a \| (q+1)$.

(ii) $\mathrm{ord}_{p_j}(q)$ *is even but not divisible by* 4 *for each* j, $1 \le j \le r$.

Proof. Suppose that there does not exist any nonzero self-orthogonal cyclic code of length $2^\ell n'$ over F_q. By Remark 2.1, all the monic irreducible factors of $X^{2^\ell n'} - 1$ over F_q are self-reciprocal. It is readily seen that $X^{2^\ell} - 1 \mid X^{2^\ell n'} - 1$ and $(X^{2^\ell} - 1)^* = X^{2^\ell} - 1$. It follows from Remark 2.1 again that all the monic irreducible factors of $X^{2^\ell} - 1$ over F_q are self-reciprocal. By Lemma 3.1, we obtain the statement (i) of the theorem.

Observe that $X^{n'} - 1 \mid X^{2^\ell n'} - 1$. Similar reasoning then shows $\mathrm{ord}_{p_j}(q)$ is even by Lemma 3.2. Hence, we are left to verify that $a_j = 1$, for each $1 \le j \le r$. Assume not. Suppose $a_k \ge 2$ for some $1 \le k \le r$. It follows from Remark 2.1 that $C_1 = C_{-1}$, where C_1 and C_{-1} denote the q-cyclotomic cosets modulo $2^\ell n'$ containing 1 and -1, respectively. Then there is some integer i such that $q^i \equiv -1 \pmod{2^\ell n'}$. Obviously, $q^{2i} \equiv 1 \pmod{p_k^{\lambda_k}}$. From $\mathrm{ord}_{p_k^{\lambda_k}}(q) = 2^{a_k} y_k$, it follows that $2^{a_k} y_k \mid 2i$ and then i is even. This leads to $q^i \equiv 1 \pmod 4$, a contradiction.

Assume now that both conditions (i) and (ii) hold. By Remark 2.1, we need to show that there is an integer i such that $q^i \equiv -1 \pmod{2^\ell n'}$. Since $\mathrm{ord}_{p_j}(q)$ is even but not divisible by 4, then $a_j = 1$ for each $1 \le j \le r$ and $q^{y_j} \equiv -1 \pmod{p_j^{\lambda_j}}$. This implies that $q^z \equiv -1 \pmod{p_j^{\lambda_j}}$. Therefore, $q^z \equiv -1 \pmod{n'}$. By the conditions $2^a \| (q+1)$ and $2 \le \ell \le a$, we have $2^\ell \mid (q+1)$, i.e. $q \equiv -1 \pmod{2^\ell}$. It follows that $q^z \equiv -1 \pmod{2^\ell}$, since z is an odd positive integer. Hence $q^z \equiv -1 \pmod{2^\ell n'}$. This completes the proof. □

3.2 Nonexistence conditions for self-orthogonal negacyclic codes

In this subsection, we focus on the nonexistence conditions for nonzero self-orthogonal negacyclic codes.

The following proposition concerns self-orthogonal negacyclic codes of odd length. It is well known that negacyclic codes of odd length are scalar equivalent to cyclic codes of the same length under the following map:

$$F_q[X]/\langle X^{n'} - 1\rangle \longrightarrow F_q[X]/\langle X^{n'} + 1\rangle$$

$$a(X) \mapsto a(-X).$$

By Lemma 3.2, we have the following result.

Proposition 3.4. *Let* $n' = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$, *where* p_j *are distinct odd primes and* λ_j *are positive integers for* $1 \le j \le r$. *Nonzero self-orthogonal negacyclic codes of length* n' *over* F_q *with* $\gcd(n', q) = 1$ *do not exist if and only if* $\mathrm{ord}_{p_j}(q)$ *is even and the highest power of* 2 *dividing* $\mathrm{ord}_{p_j}(q)$ *is the same for all* j, $1 \le j \le r$.

Let p be an odd prime such that $\gcd(2p, q) = 1$. As mentioned in the introductory section, Bakshi and Raka showed that if $q \equiv 3 \pmod 4$ and the multiplicative order of q modulo p is even but not divisible by 4, then nonzero self-orthogonal negacyclic codes of length $2p^n$ over F_q do not exist. ([1, Theorem 6(iii)]). More generally, we have the following result.

Theorem 3.5. *Let $n' = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$, where p_j are distinct odd primes and λ_j are positive integers for $1 \leq j \leq r$. Let ℓ be any positive integer, and assume that $\gcd(2n', q) = 1$. Then there does not exist any nonzero self-orthogonal negacyclic code of length $2^\ell n'$ over F_q if and only if both the following two conditions hold:*

(i) $q \equiv 3 \pmod 4$ *and* $1 \leq \ell \leq a - 1$, *where a is the positive integer with* $2^a \| (q + 1)$.

(ii) $\mathrm{ord}_{p_j}(q)$ *is even but not divisible by* 4 *for each* j, $1 \leq j \leq r$.

Proof. Suppose that both (i) and (ii) are satisfied. Observe that $(X^{2^\ell n'} + 1)(X^{2^\ell n'} - 1) = X^{2^{\ell+1} n'} - 1$. By Theorem 3.3, there does not exist any nonzero self-orthogonal cyclic code of length $2^{\ell+1} n'$ over F_q, or equivalently, all monic irreducible factors of $X^{2^{\ell+1} n'} - 1$ over F_q are self-reciprocal. Hence, all irreducible factors of $X^{2^\ell n'} + 1$ over F_q are self-reciprocal. We deduce from Remark 2.2 that nonzero self-orthogonal negacyclic code of length $2^\ell n'$ over F_q do not exist.

Now, suppose that there does not exist any nonzero self-orthogonal negacyclic code of length $2^\ell n'$ over F_q. It follows from Remarks 2.2 and 2.1 that there does not exist any nonzero self-orthogonal cyclic code of length $2^{\ell+1} n'$ over F_q. By Theorem 3.3(ii), we get the desired result. □

Acknowledgements The authors would like to sincerely thank the referees for their very careful reading and many valuable comments that helped us improve this paper. This work is supported by NSFC (Grant No. 11171370), and self-determined research funds of CCNU from the colleges's basic research and operation of MOE (Grant No. CCNU14F01004). The research of Linren Lin is supported by Central China Normal University research grant number 2013YBYB43 (excellent doctorial dissertation cultivation grant). The research of Bocong Chen is also partially supported by Nanyang Technological University's research (Grant No. M4080456).

References

[1] G. K. Bakshi, M. Raka, Self-dual and self-orthogonal negacyclic codes of length $2p^n$ over a finite field, Finite Fields Appl., **19**(2013), 39-54.

[2] T. Blackford, Negacyclic duadic codes, Finite Fields Appl., **14**(2008), 930-943.

[3] I. F. Blake, S. Gao, R. C. Mullin, Explicit factorization of $X^{2^k}+1$ over F_p with prime $p \equiv 3 \pmod 4$, Appl. Algebra Engrg. Comm. Comput., **4**(1993), 89-94.

[4] H. Q. Dinh, Repeated-root constacyclic codes of length $2p^s$, Finite Fields Appl., **18**(2012) 133-143.

[5] H. Q. Dinh, Structure of repeated-root constacyclic codes of length $3p^s$ and their duals, Discrete Math., **313**(2013), 983-991.

[6] W. Fu, T. Feng, On self-orthogonal group ring codes, Designs, Codes and Crypt., **50**(2009), 203-214.

[7] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[8] W. C. Huffman, On the classification and enumeration of self-dual codes, Finite Fields Appl., **11**(2005), 451-490.

[9] Y. Jia, S. Ling, C. Xing, On self-dual cyclic codes over finite fields, IEEE Trans. Inform. Theory, **57**(2011), 2243-2251.

[10] X. Kai, S. Zhu, On cyclic self-dual codes, Appl. Algebra Engrg. Comm. Comput., **19**(2008), 509-525.

[11] L. Kathuria, M. Raka, Existence of cyclic self-orthogonal codes: A note on a result of Vera Pless, Adv. Math. Commun., **6**(2012), 499-503.

[12] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 2008.

[13] V. Pless, Cyclotomy and cyclic codes, the unreasonable effectiveness of number theory, in "Proc. Sympos. Appl. Math. (Orono, ME, 1991)," Amer. Math. Soc., **46**(1992), 91-104.

[14] N. J. A. Sloane, J. G. Thompson, Cyclic self-dual codes, IEEE Trans. Inform. Theory, **29**(1983), 364-367.

[15] Z. Wan, Lectures on Finite Fields and Galois Rings, World Scientific Publishing, 2003.

[16] W. Willems, A note on self-dual group codes, IEEE Trans. Inform. Theory, **48**(2002), 3107-3109.