Cyclic and negacyclic codes of length 2^m over finite fields*

Guanghui Zhang[1], Xiaokun Zhu[2]

[1]School of Mathematical Sciences, Luoyang Normal University, Luoyang, Henan, 471022, China

[2]Editorial Department of Journal of Central China Normal University, Central China Normal University, Wuhan, Hubei, 430079, China

Abstract

Let F_q be a finite field of odd order q. In this note the generator polynomials and the numbers of all self-dual and self-orthogonal cyclic and negacyclic codes of length 2^m over F_q are precisely characterized.

Keywords: Cyclic code, negacyclic code, self-dual code, self-orthogonal code.

2010 Mathematics Subject Classification: 94B15; 94B05.

1 Introduction

Self-dual and self-orthogonal cyclic and negacyclic codes over finite fields play a very significant role in the theory of error-correcting codes. A great deal of effort has been devoted to them from either a theoretical or a practical point of view (e.g. see [2], [4]-[6], [9]-[11], [16],[17]).

It is known that self-dual cyclic codes of length n over F_q exist if and only if n and q are both even ([9], [10]). In [15], Pless linked self-orthogonal and self-dual cyclic codes with the class of duadic codes. Kathuria and Raka [12] showed a necessary and sufficient condition for the nonexistence of self-orthogonal cyclic codes over a finite field, of which the lengths are coprime to the characteristic of the underlying field. Lin, Liu and Chen [14] obtained a necessary and sufficient condition under which nonzero self-orthogonal negacyclic codes over finite fields do not exist.

*E-mail address: zghui2012@126.com (G. Zhang).

Dinh [7] explicitly determined repeated-root self-dual negacyclic codes of length $2p^s$ over F_{p^m}. All self-dual cyclic and negacyclic codes of length $3p^s$ over F_{p^m} were obtained concretely in [8]. Bakshi and Rake [2] obtained the self-dual and self-orthogonal negacyclic codes of length $2\ell^n$ over F_q, where ℓ is an odd prime different from the characteristic of F_q.

Let F_q be a finite field of odd order q and N a positive integer coprime to q. Any negacyclic code of length N over F_q is identified with exactly one ideal in the quotient algebra $F_q[X]/\langle X^N+1\rangle$. Since every ideal in $F_q[X]/\langle X^N+1\rangle$ can be generated by a monic divisor of X^N+1, it follows that the irreducible factorization of X^N+1 in $F_q[X]$ determines all negacyclic codes of length N over F_q.

Obviously, $(X^N+1)(X^N-1)=X^{2N}-1$. We know that the irreducible factors of $X^{2N}-1$ over F_q can be described by the q-cyclotomic cosets modulo $2N$. One can recognize the irreducible factors of $X^{2N}-1$ in $F_q[X]$ which are corresponding to the irreducible factors of X^N+1. In other words, the generator polynomials of all negacyclic codes of length N over F_q can be given by the q-cyclotomic cosets modulo $2N$. Using these facts, Bakshi and Raka in [1] characterized all self-dual negacyclic codes of length 2^m over F_q according to the q-cyclotomic cosets modulo 2^{m+1}.

In this note we study self-dual and self-orthogonal cyclic and negacyclic codes of length 2^m over F_q. Explicit expressions for the generator polynomials and the numbers of these codes are obtained. Further, the algebraic structures of codes mentioned above are exactly clear. In contrast to the proof in [1], the methods proposed in this paper are more succinct and intuitive. Based on the explicit irreducible factorization of $X^{2^m}\pm 1$ over F_q ([3, Theorem 1] and [13, Theorem 3.75]), we obtain our results without the need of cyclotomic cosets. Moreover, one can easily get the dimension of each code, since the degree of each irreducible factor of $X^{2^m}\pm 1$ over F_q is explicitly determined.

2 Preliminaries

Throughout this paper, F_q denotes the finite field of odd order q. 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. For a nonzero element λ 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 $(c_0, c_1, \cdots, c_{N-1}) \in C$. If $\lambda = 1$, λ-constacyclic codes are known as cyclic codes and if $\lambda = -1$, λ-constacyclic codes are known as negacyclic codes.

For any λ-constacyclic code C of length N over F_q, the *Euclidean 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 is a cyclic code and the dual of a negacyclic code is a negacyclic code (e.g. see [7, 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 it is denoted by $C = \langle g(X) \rangle$. 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 $h(X) = \frac{X^N - \lambda}{g(X)}$. It is known that its dual code $C^{\perp}$ has generator polynomial $h^*(X)$, where $h^*(X) = h(0)^{-1} X^{\deg h} h(\frac{1}{X})$ 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 focus on cyclic and negacyclic codes of length 2^m over the finite field F_q. The following lemmas characterize all cyclic and negacyclic codes of this length over F_q according to the cases $q \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$, respectively. If $q \equiv 3 \pmod 4$, we adopt the notation $2^a \parallel (q+1)$, which means $2^a \mid (q+1)$ but $2^{a+1} \nmid (q+1)$. The following result was presented in [3, Theorem 1].

Lemma 2.1. Assume that $q \equiv 3 \pmod 4$. Set $G_1 = \{0\}$; recursively define

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

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

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

If $1 \le m \le a-1$, then

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

if $m \ge a$, then

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

If $1 \le m \le a$, then

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

if $m \geq a+1$, then

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

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

On the other hand, if $q \equiv 1 \pmod 4$, we write $q-1 = 2^s c$ with $\gcd(2,c)=1$. The next result was presented in [13, Theorem 3.75, Page 124].

Lemma 2.2. *Assume that $q \equiv 1 \pmod 4$, then the irreducible decomposition of $X^{2^m}+1$ over F_q is given by:*

$$X^{2^m}+1 = \begin{cases} \prod\limits_{\substack{i=1,\\ 2\nmid i}}^{2^s} (X^{2^{m-s+1}}-\delta^i), & \text{if } m \geq s; \\ \prod\limits_{\substack{j=1,\\ 2\nmid j}}^{2^{m+1}} (X-\vartheta^j), & \text{if } m < s, \end{cases}$$

where δ is a primitive 2^s-th root of unity in F_q for $m \geq s$ and ϑ is a primitive 2^{m+1}-th root of unity in F_q for $m < s$.

The irreducible decomposition of $X^{2^m}-1$ over F_q is given by:

$$X^{2^m}-1 = \begin{cases} \prod\limits_{k=0}^{2^m-1} (X-\eta^k), & \text{if } m \leq s; \\ \prod\limits_{k=0}^{2^s-1} (X-\zeta^k) \prod\limits_{j=1}^{m-s} \prod\limits_{\substack{i=1\\ 2\nmid i}}^{2^s-1} (X^{2^j}-\zeta^i), & \text{if } m \geq s+1. \end{cases}$$

where η is a primitive 2^m-th root of unity in F_q for $m \leq s$ and ζ is a primitive 2^s-th root of unity in F_q for $m \geq s+1$.

3 Main Results

Let F_q be a finite field of odd order q as before. In this section, we determine the algebraic structures of all self-dual and self-orthogonal cyclic and negacyclic codes of length 2^m over F_q. We first begin with self-orthogonal negacyclic codes under the condition $4 \nmid q-1$.

Before giving our result, we adopt the following notations. According to

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

as in Lemma 2.1, we put

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

Therefore, the cardinality of G_a^+ is equal to 2^{a-2}.

Theorem 3.1. *With the notations introduced in Lemma 2.1, the following statements hold.*

(i) *If $m \geq a$, then there are precisely $3^{2^{a-2}}$ self-orthogonal negacyclic codes of length 2^m over F_q generated by:*

$$\prod_{g \in G_a^+} (X^{2^{m-a+1}} - 2gX^{2^{m-a}} - 1)^{\tau_g} (X^{2^{m-a+1}} + 2gX^{2^{m-a}} - 1)^{\sigma_g},$$

where $\tau_g, \sigma_g \in \{0,1\}$ and $\tau_g + \sigma_g \geq 1$.

(ii) *If $m < a$, then there does not exist non-zero self-orthogonal negacyclic codes of length 2^m over F_q.*

Proof. Suppose $C = \langle g(X) \rangle$ is a self-orthogonal negacyclic code of length 2^m over F_q with generator polynomial $g(X)$.

(i) If $m \geq a$, by Lemma 2.1 we have

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

For any $a_g(X) = X^{2^{m-a+1}} - 2gX^{2^{m-a}} - 1, \quad g \in G_a$, we get $a_g^*(X) = X^{2^{m-a+1}} + 2gX^{2^{m-a}} - 1$. It is clear that $a_g^*(X) \neq a_g(X)$. This means all the irreducible factors of $X^{2^m} + 1$ in $F_q[X]$ are not self-reciprocal. Note that g is always paired with $-g$ in G_a. We have

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

Without loss of generality, we can assume that

$$g(X) = \prod_{g \in G_a^+} (X^{2^{m-a+1}} - 2gX^{2^{m-a}} - 1)^{\tau_g} (X^{2^{m-a+1}} + 2gX^{2^{m-a}} - 1)^{\sigma_g},$$

where $\tau_g, \sigma_g \in \{0,1\}$. Therefore

$$\begin{aligned} h(X) &= \frac{X^{2^m+1}}{g(X)} \\ &= \prod_{g \in G_a^+} (X^{2^{m-a+1}} - 2gX^{2^{m-a}} - 1)^{1-\tau_g} \\ &\quad \cdot (X^{2^{m-a+1}} + 2gX^{2^{m-a}} - 1)^{1-\sigma_g}. \end{aligned}$$

Thus,

$$h^*(X) = \prod_{g\in G_a^+} (X^{2^{m-a+1}} + 2gX^{2^{m-a}} - 1)^{1-\tau_g} \cdot (X^{2^{m-a+1}} - 2gX^{2^{m-a}} - 1)^{1-\sigma_g}.$$

Since $C \subseteq C^\perp$, then $h^*(X) \mid g(X)$. This is possible if and only if $1 - \sigma_g \leq \tau_g$ for every $g \in G_a^+$, namely $\tau_g + \sigma_g \geq 1$ and $\tau_g, \sigma_g \in \{0,1\}$ for each $g \in G_a^+$.

As g runs over the set G_a^+, there exist $3^{2^{a-2}}$ distinct self-orthogonal negacyclic codes of length 2^m over F_q and

$$C = \Big\langle \prod_{g\in G_a^+} (X^{2^{m-a+1}} - 2gX^{2^{m-a}} - 1)^{\tau_g} (X^{2^{m-a+1}} + 2gX^{2^{m-a}} - 1)^{\sigma_g} \Big\rangle,$$

where $\tau_g, \sigma_g \in \{0,1\}, \tau_g + \sigma_g \geq 1$.

(ii) If $m < a$, By Lemma 2.1, the irreducible factorization of $X^{2^m} + 1$ over F_q is given by

$$X^{2^m} + 1 = \prod_{g\in G_m} (X^2 - 2gX + 1),$$

Working the same as in the proof of part (i), we find that for any $g \in G_m$, $(X^2 - 2gX + 1)^* = X^2 - 2gX + 1$. This implies that all the irreducible factors of $X^{2^m} + 1$ in $F_q[X]$ are self-reciprocal. We deduce that, in this case, non-zero self-orthogonal negacyclic codes do not exist. □

Next we investigate self-orthogonal negacyclic codes of length 2^m over F_q under the condition $4 \mid q - 1$.

Theorem 3.2. *With the notations of Lemma 2.2, we have that*

(i) *If $m \geq s$, then there are precisely $3^{2^{s-2}}$ self-orthogonal negacyclic codes of length 2^m over F_q generated by:*

$$\prod_{\substack{i=1,\\ 2\nmid i}}^{2^{s-1}} (X^{2^{m-s+1}} - \delta^i)^{\tau_i} (X^{2^{m-s+1}} - \delta^{-i})^{\sigma_i},$$

where $\sigma_i, \tau_i \in \{0,1\}$ and $\tau_i + \sigma_i \geq 1$.

(ii) *If $m < s$, then there are precisely $3^{2^{m-1}}$ self-orthogonal negacyclic codes of length 2^m over F_q generated by:*

$$\prod_{\substack{j=1,\\ 2\nmid j}}^{2^m} (X - \vartheta^j)^{\tau_j} (X - \vartheta^{-j})^{\sigma_j},$$

where $\sigma_j, \tau_j \in \{0,1\}$ and $\tau_j + \sigma_j \geq 1$.

Proof. Suppose $C = \langle g(X) \rangle$ is a self-orthogonal negacyclic code of length 2^m over F_q.

(i) Assuming that $m \geq s$, we put $a_i(X) = X^{2^{m-s+1}} - \delta^i$ with $1 \leq i \leq 2^s$ and $2 \nmid i$. Then $a_i^*(X) = X^{2^{m-s+1}} - \delta^{-i} = X^{2^{m-s+1}} - \delta^{2^s-i}$. Hence, $a_i^*(X) = a_i(X)$ if and only if $i = 2^{s-1}$, this is a contradiction. From Lemma 2.2, we get all the irreducible factors of $X^{2^m} + 1$ in $F_q[X]$ are not self-reciprocal. Therefore, we can write

$$X^{2^m} + 1 = \prod_{\substack{i=1, \\ 2 \nmid i}}^{2^{s-1}} (X^{2^{m-s+1}} - \delta^i)(X^{2^{m-s+1}} - \delta^{-i}).$$

This gives that

$$g(X) = \prod_{\substack{i=1, \\ 2 \nmid i}}^{2^{s-1}} (X^{2^{m-s+1}} - \delta^i)^{\tau_i}(X^{2^{m-s+1}} - \delta^{-i})^{\sigma_i}, \quad \sigma_i, \tau_i \in \{0, 1\}.$$

Hence,

$$h^*(X) = \prod_{\substack{i=1, \\ 2 \nmid i}}^{2^{s-1}} (X^{2^{m-s+1}} - \delta^{-i})^{1-\tau_i}(X^{2^{m-s+1}} - \delta^i)^{1-\sigma_i}.$$

Since $C \subseteq C^{\perp}$, we have $\sigma_i + \tau_i \geq 1$ for each $1 \leq i \leq 2^{s-1}, 2 \nmid i$.

As a consequence, there exist $3^{2^{s-1}}$ distinct self-orthogonal negacyclic codes of length 2^m over F_q and

$$C = \left\langle \prod_{\substack{i=1, \\ 2 \nmid i}}^{2^{s-1}} (X^{2^{m-s+1}} - \delta^i)^{\tau_i}(X^{2^{m-s+1}} - \delta^{-i})^{\sigma_i} \right\rangle,$$

where $\tau_i + \sigma_i \geq 1$ and $\tau_i, \sigma_i \in \{0, 1\}$.

(ii) If $m < s$, working the same as in the proof of part (i), we put $b_j(X) = X - \vartheta^j$. Then $b_j^*(X) = X - \vartheta^{-j} = X - \vartheta^{2^{m+1}-j}$. Hence, we assume that

$$g(X) = \prod_{\substack{j=1, \\ 2 \nmid j}}^{2^m} (X - \vartheta^j)^{\tau_j}(X - \vartheta^{-j})^{\sigma_j}, \quad \tau_i, \sigma_i \in \{0, 1\}.$$

Thus,

$$h^*(X) = \prod_{\substack{j=1, \\ 2 \nmid j}}^{2^m} (X - \vartheta^{-j})^{1-\tau_j}(X - \vartheta^j)^{1-\sigma_j}.$$

As $C \subseteq C^{\perp}$, we have $\tau_j + \sigma_j \geq 1$, and $\tau_j, \sigma_j \in \{0,1\}$.

Also, one can check that there exist $3^{2^{m-1}}$ distinct self-orthogonal negacyclic codes of length 2^m over F_q and

$$C = \Big\langle \prod_{\substack{j=1, \\ 2 \nmid j}}^{2^m} (X - \vartheta^j)^{\tau_j} (X - \vartheta^{-j})^{\sigma_j} \Big\rangle,$$

where $\sigma_j, \tau_j \in \{0,1\}$ and $\tau_j + \sigma_j \geq 1$.

□

Now we turn to determine all self-dual negacyclic codes of length 2^m over F_q. Also we have to distinguish the cases $q \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$.

Corollary 3.3. *Assume the notations given in Lemma 2.1.*

(i) *If $m \geq a$, then there are precisely $2^{2^{a-2}}$ self-dual negacyclic codes of length 2^m over F_q generated by:*

$$\prod_{g \in G_a^+} (X^{2^{m-a+1}} - 2gX^{2^{m-a}} - 1)^{\tau_g} (X^{2^{m-a+1}} + 2gX^{2^{m-a}} - 1)^{\sigma_g}, \quad (3.1)$$

where $\tau_g, \sigma_g \in \{0,1\}, \tau_g + \sigma_g = 1$.

(ii) *If $m < a$, then there does not exist self-dual negacyclic codes of length 2^m over F_q .*

Proof. Let $C = \langle g(X) \rangle$ be a self-dual negacyclic code of length 2^m over F_q.

(i) Working the same as in the proof of Theorem 3.1 (i), we just note that $C = C^{\perp}$ if and only if $h^*(X) = g(X)$.

(ii) It is a direct consequence of Theorem 3.1 (ii). □

Corollary 3.4. *Let the notations be the same as in Lemma 2.2.*

(i) *If $m \geq s$, then there are precisely $2^{2^{s-2}}$ self-dual negacyclic codes of length 2^m over F_q generated by:*

$$\prod_{\substack{i=1, \\ 2 \nmid i}}^{2^{s-1}} (X^{2^{m-s+1}} - \delta^i)^{\tau_i} (X^{2^{m-s+1}} - \delta^{-i})^{\sigma_i},$$

where $\sigma_i, \tau_i \in \{0,1\}$ and $\sigma_i + \tau_i = 1$.

(ii) *If $m < s$, then there are precisely $2^{2^{m-1}}$ self-dual negacyclic codes of length 2^m over F_q generated by:*

$$\prod_{\substack{j=1, \\ 2 \nmid j}}^{2^m} (X - \vartheta^j)^{\tau_j} (X - \vartheta^{-j})^{\sigma_j},$$

where $\sigma_j, \tau_j \in \{0,1\}$ and $\sigma_j + \tau_j = 1$.

As mentioned in the first section, self-dual cyclic code over a finite field exists if and only if the code length is even and the characteristic of the field is equal to two ([9],[10]). Therefore, there does not exist self-dual cyclic codes of length 2^m over F_q.

Proposition 3.5. *There do not exist self-dual cyclic codes of length 2^m over F_q.*

In the following, we focus on the generator polynomials of self-orthogonal cyclic codes of length 2^m over F_q. We first consider the case $4 \nmid q-1$.

Theorem 3.6. *Notations as defined in Lemma 2.1.*

(i) *If $m \geq a+1$, then there are precisely $3^{(m-a)2^{a-2}}$ self-orthogonal cyclic codes of length 2^m over F_q generated by:*

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

$$\cdot\prod_{j=1}^{m-a-1}\prod_{g\in G_a^+}(X^{2^{j+1}}-2gX^{2^j}-1)^{\tau_g^j}(X^{2^{j+1}}+2gX^{2^j}-1)^{\sigma_g^j},$$

where $\tau_g^j, \sigma_g^j \in \{0,1\}$ and $\tau_g^j+\sigma_g^j \geq 1$.

(ii) *If $m \leq a$, then there does not exist non-zero self-orthogonal cyclic codes of length 2^m over F_q .*

Proof. (i) If $m \geq a+1$, by Lemma 2.1 we know

$$\begin{aligned} X^{2^m}-1 &= (X-1)(X+1)\prod_{i=1}^{a-1}\prod_{g\in G_i}(X^2-2gX+1) \\ &\quad\cdot\prod_{\substack{g\in G_a,\\ 0\leq j\leq(m-a-1)}}(X^{2^{j+1}}-2gX^{2^j}-1). \end{aligned}$$

With this result the same method in Theorem 3.1 is applied to get our desired result.

(ii) If $m \leq a$, we just note that the irreducible factors of $X^{2^m}-1$ F_q are self-reciprocal. □

Theorem 3.7. *Using the notations of Lemma 2.2, we have that*

(i) *If $m \geq s+1$, then there are precisely $3^{(m-s+2)2^{s-2}-1}$ self-orthogonal cyclic codes of length 2^m over F_q generated by:*

$$(X-1)(X+1)\prod_{k=1}^{2^{s-1}}(X-\zeta^k)^{\tau_k}(X-\zeta^{-k})^{\sigma_k}\prod_{j=1}^{m-s}\prod_{\substack{i=1\\ 2\nmid i}}^{2^{s-2}}(X^{2^j}-\zeta^i)^{v_i^j}(X^{2^j}-\zeta^{-i})^{\omega_i^j},$$

where $\tau_k+\sigma_k \geq 1, v_i^j+\omega_i^j \geq 1$, and $\tau_k, \sigma_k, v_i^j, \omega_i^j \in \{0,1\}$.

(ii) *If $m \leq s$, then there are precisely $3^{2^{m-1}-1}$ self-orthogonal cyclic codes of length 2^m over F_q generated by:*

$$(X-1)(X+1)\prod_{k=1}^{2^{m-1}-1}(X-\eta^k)^{\tau_k}(X-\eta^{-k})^{\sigma_k}, \tag{3.2}$$

where $\sigma_i, \tau_i \in \{0,1\}$ and $\tau_i + \sigma_k \geq 1$ for each $1 \leq k \leq 2^{m-1}-1$.

Proof. (i) If $m \geq s+1$, then the irreducible factorization of $X^{2^m}-1$ over F_q is given by

$$X^{2^m}-1 = \prod_{k=0}^{2^s-1}(X-\zeta^k)\prod_{j=1}^{m-s}\prod_{\substack{i=1\\ 2\nmid i}}^{2^s-1}(X^{2^j}-\zeta^i).$$

Then we can rewrite it as follows

$$X^{2^m}-1 = (X-1)(X+1)\prod_{k=1}^{2^{s-1}}(X-\zeta^k)(X-\zeta^{-k})\prod_{j=1}^{m-s}\prod_{\substack{i=1\\ 2\nmid i}}^{2^s-2}(X^{2^j}-\zeta^i)(X^{2^j}-\zeta^{-i}).$$

Thus the following proof is similar to that of Theorem 3.2.

(ii) Taking arguments similar to (i), we can get the desired result. □

Acknowledgements The authors are grateful to the anonymous referees for valuable comments and suggestions which help to create an improved version. The first author is supported by the Natural Science Foundation of China (Grant No. 11171370), the Youth Backbone Teacher Foundation of Henan's University (Grant No. 2013GGJS-152), and Science and Technology Development Program of Henan Province in 2014 (144300510051).

References

[1] G. K. Bakshi, M. Raka, A class of constacyclic codes over a finite field, Finite Fields Appl., **18**(2012), 362-377.

[2] 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.

[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] B. Chen, Y. Fan, L. Lin and H. Liu, Constacyclic codes over finite fields, Finite fields and Appl., **18**(2012), 1217-1231.

[5] B. Chen, L. Li and R. Tuerhong, Expliciting factorization of $x^{2^m p^n} - 1$ over a finite field, Finite fields and Appl., **24**(2013), 95-104.

[6] B. Chen, H. Q. Dinh, A note on isodual constacyclic codes, Finite fields and Appl., **29**(2014), 243-246.

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

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

[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] X. Kai, S. Zhu, On the distances of cyclic codes of length 2^e over Z_4, Discrete Math., **310**(2010), 12-20.

[12] 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.

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

[14] L. Lin, H. Liu, B. Chen, Existence conditions for self-orthogonal negacyclic codes over Finite Fields, Adv. Math. Commun. **9**(2015), 1-7.

[15] 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.

[16] S. Zhu, X. Kai, Dual and self-dual negacyclic codes of even length over Z_{2^a}, Discrete Math., **309**(2009), 2382-2391.

[17] S. Zhu, K. Qian, X. Kai, A note on negacyclic self-dual codes over Z_{2^a}, Discrete Math., **312**(2012), 3270-3275.