IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received June 18, 2019, accepted August 14, 2019, date of publication August 26, 2019, date of current version September 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2937544

Negacyclic Codes of Length $2^m p^n$ Over Finite Fields

JING HUANG
School of Mathematics, South China University of Technology, Guangzhou 510641, China
e-mail: jhuangmath@foxmail.com

ABSTRACT Let F_q be a finite field of odd order q. Let m be a positive integer such that $X^{2^m}+1$ factors completely into degree-one factors in $F_{q^2}[X]$. The polynomial generators of all negacyclic codes of length $2^m p^n$ over F_q are obtained, where p is an odd prime coprime to q.

INDEX TERMS Negacyclic code, irreducible factorization, polynomial generator.

I. INTRODUCTION

Negacyclic codes were initiated in the early 1960's ([3], [4]), which have been extendedly studied for their theoretical importance and practical applications. The issues of algebraic structures for negacyclic codes, self-dual and self-orthogonal negacyclic codes have been attractive research topics (e.g. see [6]–[19]).

In [19], Dinh obtained the polynomial generators of all self-dual negacyclic codes of length $2p^s$ over F_{p^m}. Bakshi and Raka in [1] determined the polynomial generators of all negacyclic codes of length 2^n over an odd characteristic finite field; they also exhibited all self-dual negacyclic codes of the same length. In [13], Chen et al. obtained the polynomial generators of all negacyclic codes of length $\ell^t p^s$ over F_{p^m}, where ℓ is a prime number different from the characteristic p.

Let F_q be a finite field of odd order q and let N be 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 $F_q[X]$. In other words, the polynomial generators of all negacyclic codes of length N over F_q can be given by the q-cyclotomic cosets modulo $2N$. Noting those facts, Bakshi and Raka in [1] described the polynomial generators of negacyclic codes of length 2^n over F_q by means of recognizing the q-cyclotomic cosets modulo 2^{n+1} which are corresponding to the irreducible factors of $X^{2^n}+1$. In the subsequent paper [2], the authors studied self-dual and self-orthogonal negacyclic codes of length $2p^n$ over F_q, where p is an odd prime coprime to q. They proceed by first determining the q-cyclotomic cosets modulo $4p^n$, which give the irreducible factorization of $X^{4p^n}-1$ over F_q.

Let m be a positive integer such that $X^{2^m}+1$ factors completely into degree-one factors in $F_{q^2}[X]$. In this paper, we study negacyclic codes of length $2^m p^n$ over F_q, where p is an odd prime coprime to q and n is a positive integer. The polynomial generators of all negacyclic codes of length $2^m p^n$ over F_q are explicitly expressed. This extends the results given by Bakshi and Raka [2] which considered the case $m=1$. We propose a new approach to obtain the irreducible factorization of $X^{2^m p^n}+1$ over F_q. In brief, we get the irreducible factorization of $X^{2^m p^n}+1$ over F_q by analyzing the irreducible factors of $X^{2^m p^n}+1$ over F_{q^2}; we derive the irreducible factorization of $X^{2^m p^n}+1$ over F_{q^2} from the irreducible factorization of $X^{p^n}-1$ over F_{q^2}, which is accomplished by determining the q^2-cyclotomic cosets modulo p^n. We mention that, $m=2$ also valid under our hypothesis. That is, one can obtain all self-dual and self-orthogonal negacyclic codes of length $4p^n$ over F_q by our results.

The rest sections of this paper are organized as follows. In Section 2, the necessary notations and known results are presented. All distinct q^2-cyclotomic cosets modulo p^n are also provided in this section. In Section 3, we determine the polynomial generators of all negacyclic codes of length $2^m p^n$ over F_q. We conclude this paper with Section 4.

II. PRELIMINARIES

Let F_q be a finite field of odd order q. We denote by F_q^* the multiplicative group of non-zero elements of F_q. For $\beta\in F_q^*$ we denote by $\mathrm{ord}(\beta)$ the order of β in the group F_q^*; then $\mathrm{ord}(\beta)$ is a divisor of $q-1$, and β is called a *primitive* $\mathrm{ord}(\beta)$*th*

The associate editor coordinating the review of this article and approving it for publication was Xueqin Jiang.

root of unity. It is well known that F_q^* is generated by a primitive $(q-1)$th root ξ of unity, in symbols $F_q^* = \langle \xi \rangle$.

Assume that n is a positive integer and p is an odd prime coprime to q. Let $\mathbf{Z}_{p^n} = \{[b]_{p^n} \mid b \text{ is an integer}\}$ be the ring consisting of all residue classes modulo p^n and $\mathbf{Z}_{p^n}^*$ the unit group of the ring; it is known that $\mathbf{Z}_{p^n}^*$ is a cyclic group. We denote by $\langle q \rangle$, the cyclic subgroup of $\mathbf{Z}_{p^n}^*$ generated by $[q]_{p^n}$. Let $\langle q \rangle$ act on $\mathbf{Z}_{p^n}$ by the following rule:

$$q^i \cdot [b]_{p^n} = [bq^i]_{p^n}, \quad \text{for any integer } i \text{ and } [b]_{p^n} \in \mathbf{Z}_{p^n}.$$

For any integer t, the orbit of $[t]_{p^n}$ under the given action,

$$C_t = \{t, tq, tq^2, \cdots tq^{n_t - 1}\},$$

is called the *q-cyclotomic coset of t mod p^n*. Here the elements in the brace are calculated modulo p^n and n_t is the cardinality of the orbit C_t. It is readily seen that n_t is equal to the multiplicative order of q modulo $\frac{p^n}{\gcd(p^n,t)}$.

We denote by $\mathrm{ord}_p(q) = f$, the multiplicative order of q in $\mathbf{Z}_p^*$. Write

$$q^f = 1 + p^d z, \quad p \nmid z, \ d \geq 1.$$

For any integer ℓ, $1 \leq \ell \leq n$, we set

$$\lambda(\ell) := fp^{\max(\ell - d, 0)}.$$

One knows that $\mathrm{ord}_{p^\ell}(q) = \lambda(\ell)$ (e.g. see [2] or [23]). Put $\delta(\ell) = \frac{\phi(p^\ell)}{\lambda(\ell)}$, where ϕ denotes the Euler's phi-function. Let g be a generator of the cyclic group $\mathbf{Z}_{p^n}^*$. By [23, Theorem 1], $C_0 = \{0\}$, and

$$C_{p^{n-\ell}g^k} = \{p^{n-\ell}g^k, p^{n-\ell}g^k q, \cdots, p^{n-\ell}g^k q^{\lambda(\ell)-1}\},$$

with $0 \leq k \leq \delta(\ell) - 1$ and $1 \leq \ell \leq n$, consist all the distinct q-cyclotomic cosets modulo p^n. For simplify, we write $C_{\rho_0} = \{0\}$ and C_{ρ_k}, $1 \leq k \leq h$ to denote all the distinct q-cyclotomic cosets modulo p^n; it is easy to see that $h = \sum_{\ell=1}^n \delta(\ell)$.

Take η to be a primitive p^nth root of unity (maybe in an extension of F_q), and denote by $M_{\rho_k}(X)$, the minimal polynomial of η^{ρ_k} over F_q, $0 \leq k \leq h$. It is well known that (e.g. see [20, Theorem 4.1.1]):

$$X^{p^n} - 1 = (X-1)M_{\rho_1}(X)M_{\rho_2}(X)\cdots M_{\rho_h}(X), \quad \text{(II.1)}$$

with

$$M_{\rho_k}(X) = \prod_{u \in C_{\rho_k}} (X - \eta^u), \quad 1 \leq k \leq h,$$

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

We point out that, $C_0 = \{0\}$ and

$$C_{-p^{n-\ell}g^k} = \{-p^{n-\ell}g^k, -p^{n-\ell}g^k q, \cdots, -p^{n-\ell}g^k q^{\lambda(\ell)-1}\},$$

with $0 \leq k \leq \delta(\ell) - 1$ and $1 \leq \ell \leq n$, also consist all the distinct q-cyclotomic cosets modulo p^n, where the elements in the brace are calculated modulo p^n. Hence,

$$X^{p^n} - 1 = (X-1)M_{-\rho_1}(X)M_{-\rho_2}(X)\cdots M_{-\rho_h}(X),$$

also gives the monic irreducible factorization of $X^{p^n} - 1$ over F_q.

In this paper, we need to obtain all the distinct q^2-cyclotomic cosets modulo p^n according to the above given q-cyclotomic cosets modulo p^n. It requires to consider two subcases. First, if f is odd, namely $\lambda(\ell) = \mathrm{ord}_{p^\ell}(q)$ is odd for each $1 \leq \ell \leq n$, then $\mathrm{ord}_{p^\ell}(q) = \mathrm{ord}_{p^\ell}(q^2)$, which means that the cyclic subgroup generated by $[q]_{p^\ell}$ in $\mathbf{Z}_{p^\ell}^*$ is equal to the cyclic subgroup generated by $[q^2]_{p^\ell}$, i.e. $\langle q \rangle = \langle q^2 \rangle$ in $\mathbf{Z}_{p^\ell}^*$. In particular, $\langle q \rangle = \langle q^2 \rangle$ in $\mathbf{Z}_{p^n}^*$. By the definition of q^2-cyclotomic cosets, $C_{\rho_0} = \{0\}$ and C_{ρ_k}, $1 \leq k \leq h$, consist all the distinct q^2-cyclotomic cosets modulo p^n. It follows that Formula (II.1) also gives the irreducible factorization of $X^{p^n} - 1$ in $F_{q^2}[X]$. If f is even, we deduce that $\mathrm{ord}_{p^\ell}(q^2) = \frac{\lambda(\ell)}{2}$ for all $1 \leq \ell \leq n$. It is straightforward to verify that $D_0 = \{0\}$,

$$D_{p^{n-\ell}g^j} = \{p^{n-\ell}g^j, p^{n-\ell}g^j \cdot q^2, \cdots, p^{n-\ell}g^j \cdot q^{2(\frac{\lambda(\ell)}{2} - 1)}\},$$

and

$$D_{p^{n-\ell}g^j q} = \{p^{n-\ell}g^j q, p^{n-\ell}g^j q \cdot q^2, \cdots, p^{n-\ell}g^j q \cdot q^{2(\frac{\lambda(\ell)}{2} - 1)}\},$$

where $0 \leq j \leq \delta(\ell) - 1$, $1 \leq \ell \leq n$, consist all the distinct q^2-cyclotomic cosets modulo p^n. Observe that

$$C_{p^{n-\ell}g^j} = D_{p^{n-\ell}g^j} \bigcup D_{p^{n-\ell}g^j q},$$

for each $0 \leq j \leq \delta(\ell) - 1$ and $1 \leq \ell \leq n$. For simplify let $D_{\rho_0} = \{0\}$, D_{ρ_k} and $D_{\rho_k q}$, $1 \leq k \leq h$ such that $C_{\rho_k} = D_{\rho_k} \bigcup D_{\rho_k q}$, denote all the distinct q^2-cyclotomic cosets modulo p^n. By [20, Theorem 4.1.1] again, we have that $X^{p^n} - 1$ factors into

$$(X-1)N_{\rho_1}(X)N_{\rho_1 q}(X)N_{\rho_2}(X)N_{\rho_2 q}(X)\cdots N_{\rho_h}(X)N_{\rho_h q}(X),$$

with

$$N_{\rho_k}(X) = \prod_{u \in D_{\rho_k}} (X - \eta^u)$$

and

$$N_{\rho_k q}(X) = \prod_{u \in D_{\rho_k q}} (X - \eta^u), \quad 1 \leq k \leq h,$$

all being monic irreducible in $F_{q^2}[X]$.

In the rest of this section, we recall some basic concepts and results from negacyclic codes over F_q. Let N be a positive integer. Any non-empty subset C of F_q^N is called a *code* of length N. If the code C is an F_q-linear subspace of F_q^N, then C is called a *linear code*. A linear code C of length N over F_q is said to be *negacyclic* if for any code word $(c_0, c_1, \cdots, c_{N-1}) \in C$ we have that $(-c_{N-1}, c_0, c_1, \cdots, c_{N-2}) \in C$.

Any element of the quotient algebra $F_q[X]/\langle X^N + 1 \rangle$ is uniquely represented by a polynomial $a_0 + a_1 X + \cdots + a_{N-1}X^{N-1}$ of degree less than N, hence it can be identified with a word $(a_0, a_1, \cdots, a_{N-1})$ of length N over F_q. In this way, any negacyclic code C of length N over F_q is identified with exactly one ideal of the quotient algebra $F_q[X]/\langle X^N + 1 \rangle$, which is generated uniquely by a monic divisor $g(X)$

of X^N+1. In this case, $g(X)$ is called a *polynomial generator* of C. Specifically, the irreducible factorization of X^N+1 in $F_q[X]$ determines all negacyclic codes of length N over F_q.

For any negacyclic code C of length N over F_q, its *dual code* $C^\perp$ is defined as $C^\perp = \{u \in {F_q}^N \mid u \cdot v = 0,$ 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 $C^\perp = C$. It turns out that the dual of a negacyclic code is again a negacyclic code.

III. NEGACYCLIC CODES OF LENGTH $2^m p^n$ OVER F_q

Let F_q be a finite field of odd order q and $F_q^* = \langle \xi \rangle$ as before. We first adopt the following notations.

Notation 1: Let p be an odd prime coprime with q and n a positive integer. Write $q-1 = 2^s c$ with c being an odd positive integer. We assume further that m is a positive integer such that $X^{2^m}+1$ factors completely into degree-one factors in $F_{q^2}[X]$.

Suppose that $f(X)$ is a polynomial with leading coefficient $a_n \neq 0$; we denote by $\hat{f}(X)$, the monic polynomial such that $\hat{f}(X) = a_n^{-1} f(X)$.

In this section, the polynomial generators of all negacyclic codes of length $2^m p^n$ over F_q are obtained. As mentioned in the introductory section, Bakshi and Raka determined the polynomial generators of all negacyclic codes of length $2p^n$ over F_q. Note that X^2+1 always factors completely in $F_{q^2}[X]$. In this sense, our results give a natural generalization of the results of [1].

We continue the discussion of negacyclic codes of length $2^m p^n$ over F_q with two subsections. In the first subsection, we give the polynomial generators of all negacyclic codes of length $2^m p^n$ over F_q under the condition $s \geq 2$, i.e. $4 \mid (q-1)$; then in the second subsection, we give the polynomial generators of all negacyclic codes of length $2^m p^n$ over F_q under the condition $s = 1$, i.e. $4 \nmid (q-1)$.

A. NEGACYCLIC CODES OF LENGTH $2^m p^n$ OVER F_q WITH $4 \mid (q-1)$

As mentioned above, in this subsection, we assume that $q-1 = 2^s c$ with c being odd and $s \geq 2$. Take $\alpha = \xi^c$. Then $\langle \alpha \rangle$ is the Sylow 2-subgroup of F_q^*. Since p is odd, it is clear that the following map gives an isomorphism of group:

$$\begin{aligned} \theta : \quad \langle \alpha \rangle &\longrightarrow \langle \alpha \rangle \\ x &\mapsto x^{p^n}. \end{aligned} \tag{III.1}$$

One knows that the irreducible decomposition of $X^{2^m}+1$ over F_q is given by:

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

where $\vartheta = \xi^{2^{s-m-1}c}$ is a primitive 2^{m+1}th root of unity for $m < s$. We just mention that, the fact $X^{2^{m-s+1}} - \alpha^j$ with $2 \nmid j$ is irreducible in $F_q[X]$, is a direct consequence of ([22, Theorem 3.75] or [24, Theorem 10.7]). By our hypothesis $X^{2^m}+1$ factors completely into degree-one factors in $F_{q^2}[X]$, we get $m \leq s$.

For $m = s$, we take a primitive 2^{s+1}th root of unity $\beta \in F_{q^2}$ such that $\beta^2 = \alpha$, then $X^2 - \alpha^j = (X-\beta^j)(X+\beta^j)$ for each $1 \leq j \leq 2^s$ with $2 \nmid j$. In $F_{q^2}[X]$, we have

$$X^{2^s p^n}+1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^s} (X^{p^n} - \beta^j)(X^{p^n} + \beta^j).$$

At this point we deduce that there exists a unique element γ in the Sylow 2-subgroup of $F_{q^2}^*$ such that $\gamma^{p^n}\beta = 1$. In the next lemma, we proceed by first giving the irreducible factorization of $X^{2^m p^n}+1$ in $F_{q^2}[X]$. Then, we recognize the irreducible factors of $X^{2^m p^n}+1$ over F_q by analyzing the irreducible factors of $X^{2^m p^n}+1$ over F_{q^2}.

Lemma 2: With respect to the above notations, we have that

(i) *If $m < s$, then the irreducible decomposition of $X^{2^m p^n}+1$ over F_q is given by:*

$$X^{2^m p^n}+1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^{m+1}} \prod_{k=0}^{h} \hat{M}_{\rho_k}(\lambda_1^j X);$$

(ii) *if $m = s$ and f is odd, then the irreducible decomposition of $X^{2^m p^n}+1$ over F_q is given by:*

$$X^{2^m p^n}+1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^s} \prod_{k=0}^{h} \hat{M}_{\rho_k}(\lambda_2^j X^2);$$

(iii) *if $m = s$ and f is even, then the irreducible decomposition of $X^{2^m p^n}+1$ over F_q is given by:*

$$X^{2^m p^n}+1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^s} (X^2 - \lambda_2^{-j}) \cdot \prod_{\substack{j=1,\\ 2\nmid j}}^{2^s} \prod_{k=1}^{h} \left(H_k^j(X) K_k^j(X) \right).$$

where λ_1 is a unique element in the Sylow 2-subgroup of F_q^* such that $\lambda_1^{p^n} \xi^{2^{s-m-1}c} = 1$ while $s > m$, λ_2 is a unique element in the Sylow 2-subgroup of F_q^* such that $\lambda_2^{p^n}\alpha = 1$, $H_k^j(X) = \hat{N}_{\rho_k}(\gamma^j X)\hat{N}_{\rho_k q}(-\gamma^j X)$ and $K_k^j(X) = \hat{N}_{\rho_k q}(\gamma^j X)\hat{N}_{\rho_k}(-\gamma^j X)$.

Proof: (i). Since $X^{2^m}+1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^{m+1}} (X - \vartheta^j)$, then

$$X^{2^m p^n}+1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^{m+1}} (X^{p^n} - \vartheta^j), \tag{III.2}$$

where $\vartheta = \xi^{2^{s-m-1}c}$ is a primitive 2^{m+1}th root of unity in F_q. It suffices to determine the irreducible factors of each term on the right hand side of Formula (III.2). We know that

$C_{\rho_0} = \{0\}$, $C_{\rho_1}, C_{\rho_2}, \cdots, C_{\rho_h}$ are all the distinct q-cyclotomic cosets modulo p^n, then

$$X^{p^n} - 1 = \prod_{k=0}^{h} M_{\rho_k}(X),$$

gives the irreducible factorization of $X^{p^n} - 1$ over F_q. Since p is odd and $\mathrm{ord}(\vartheta) = 2^{m+1}$, then $\vartheta \in \langle \xi^{p^n} \rangle$. This implies that there exists a unique element λ_1 in the Sylow 2-subgroup of F_q^* such that $\lambda_1^{p^n}\vartheta = 1$. We have the following F_q-algebra isomorphism:

$$\varphi : \quad F_q[X]/\langle X^{p^n} - 1\rangle \longrightarrow F_q[X]/\langle X^{p^n} - \vartheta^j\rangle,$$

which maps $f(X) + \langle X^{p^n} - 1\rangle$ to $f(\lambda_1^j X) + \langle X^{p^n} - \vartheta^j\rangle$. Hence,

$$X^{p^n} - \vartheta^j = \vartheta^j \prod_{k=0}^{h} M_{\rho_k}(\lambda_1^j X),$$

gives the irreducible factorization of $X^{p^n} - \vartheta^j$ in $F_q[X]$. Therefore,

$$X^{2^m p^n} + 1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^{m+1}} \prod_{k=0}^{h} \hat{M}_{\rho_k}(\lambda_1^j X),$$

with all the factors on the right hand side being irreducible over F_q. This completes the proof of (i).

Recall that $X^{2^s} + 1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^s} (X^2 - \alpha^j)$, where $\alpha = \xi^c$ is a primitive 2^sth root of unity in F_q. We take a primitive 2^{s+1}th root of unity $\beta \in F_{q^2}$ such that $\beta^2 = \alpha$, then $X^2 - \alpha^j = (X - \beta^j)(X + \beta^j)$ for each $1 \le j \le 2^s$ with $\gcd(2, j) = 1$. In $F_{q^2}[X]$, we have

$$X^{2^s p^n} + 1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^s} (X^{p^n} - \beta^j)(X^{p^n} + \beta^j).$$

(ii). Now we prove the case $m = s$ and f is odd. Since f is odd, then $C_{\rho_0} = \{0\}$, $C_{\rho_1}, C_{\rho_2}, \cdots, C_{\rho_h}$ are all the distinct q^2-cyclotomic cosets modulo p^n. Hence, for each $1 \le j \le 2^s$ with $\gcd(2, j) = 1$,

$$X^{p^n} - \beta^j = \beta^j \prod_{k=0}^{h} M_{\rho_k}(\gamma^j X),$$

where $\gamma \in F_{q^2}^*$ such that $\gamma^{p^n}\beta = 1$. Similarly,

$$X^{p^n} + \beta^j = -\beta^j \prod_{k=0}^{h} M_{\rho_k}(-\gamma^j X).$$

It is clear that γ is a primitive 2^{s+1}th root of unity in F_{q^2} and we have the following monic irreducible factorization of $X^{2^m p^n} + 1$ in $F_{q^2}[X]$:

$$X^{2^m p^n} + 1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^s} \Big(\prod_{k=0}^{h} \hat{M}_{\rho_k}(\gamma^j X)\hat{M}_{\rho_k}(-\gamma^j X) \Big).$$

On the other hand, note that $\gamma^{2p^n} = \beta^{-2} = \alpha^{-1}$; we take $\lambda_2 \in F_{q^2}$ such that $\gamma^2 = \lambda_2$. This gives $\lambda_2 \in F_q$ and $\lambda_2^{p^n}\alpha = 1$. Therefore, for each $1 \le j \le 2^s$ with $\gcd(2, j) = 1$,

$$X^{p^n} - \alpha^j = \alpha^j \prod_{k=0}^{h} M_{\rho_k}(\lambda_2^j X),$$

is the irreducible factorization of $X^{p^n} - \alpha^j$ in $F_q[X]$. We get that

$$X^{2p^n} - \alpha^j = \alpha^j \prod_{k=0}^{h} M_{\rho_k}(\lambda_2^j X^2).$$

Hence,

$$X^{2^m p^n} + 1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^s} (X^{2p^n} - \alpha^j) = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^s} \prod_{k=0}^{h} \hat{M}_{\rho_k}(\lambda_2^j X^2). \quad \text{(III.3)}$$

We claim that Formula (III.3) gives the irreducible factorization of $X^{2^m p^n} + 1$ over F_q. Observe that $\lambda_2^{p^n} = \alpha^{-1} = \beta^{-2} = \gamma^{2p^n}$, then $\lambda_2 = \gamma^2$. Obviously, $C_{2\rho_0} = \{0\}$, $C_{2\rho_1}, C_{2\rho_2}, \cdots, C_{2\rho_h}$ also consist all the distinct q-cyclotomic cosets modulo p^n. Then $X^{p^n} - 1 = \prod_{k=0}^{h} M_{2\rho_k}(X)$ gives the irreducible factorization. This leads to

$$X^{2^m p^n} + 1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^s} \prod_{k=0}^{h} \hat{M}_{2\rho_k}(\lambda_2^j X^2).$$

We deduce that

$$\hat{M}_{\rho_k}(\gamma^j X)\hat{M}_{\rho_k}(-\gamma^j X) = \hat{M}_{2\rho_k}(\lambda_2^j X^2).$$

It is straightforward to verify that

$$\hat{M}_{\rho_k}(\gamma^j X) \in F_{q^2}[X], \quad \hat{M}_{\rho_k}(-\gamma^j X) \in F_{q^2}[X],$$

and

$$\hat{M}_{\rho_k}(\gamma^j X) \notin F_q[X], \quad \hat{M}_{\rho_k}(-\gamma^j X) \notin F_q[X].$$

This forces $\hat{M}_{2\rho_k}(\lambda_2^j X^2)$ to be a monic irreducible polynomials in $F_q[X]$. We get that

$$X^{2^m p^n} + 1 = \prod_{\substack{j=1,\\ 2\nmid j}}^{2^s} \prod_{k=0}^{h} \hat{M}_{\rho_k}(\lambda_2^j X^2),$$

is a monic irreducible factorization of $X^{2^m p^n} + 1$ over F_q.

(iii). Finally, we are left to prove the case $m = s$ and f is even. As indicated in Section 2, all the distinct q^2-cyclotomic cosets modulo p^n are given by $D_{\rho_0} = \{0\}$, D_{ρ_j} and $D_{\rho_j q}$ for $1 \le j \le h$. Hence, $X^{p^n} - 1$ has the irreducible factorization over F_{q^2} as follows:

$$X^{p^n} - 1 = (X - 1) \prod_{j=1}^{h} \big(N_{\rho_j}(X) N_{\rho_j q}(X)\big),$$

where $N_{\rho_j}(X)=\prod_{k\in D_{\rho_j}}(X-\eta^k)$ and $N_{\rho_j q}(X)=\prod_{k\in D_{\rho_j q}}(X-\eta^k)$ with η being a primitive p^nth root of unity in some extension field of F_q. Then

$$X^{p^n}-\beta^j=\beta^j(\gamma^jX-1)\prod_{k=1}^{h}\left(N_{\rho_k}(\gamma^jX)N_{\rho_k q}(\gamma^jX)\right),$$

$$X^{p^n}+\beta^i=-\beta^i(-\gamma^jX-1)\prod_{k=1}^{h}\left(N_{\rho_k}(-\gamma^jX)N_{\rho_k q}(-\gamma^jX)\right).$$

We get the irreducible factors of $X^{2^mp^n}+1$ in $F_{q^2}[X]$: $X^{2^mp^n}+1$ factors into

$$\prod_{\substack{j=1,\\ 2\nmid j}}^{2^s}\left((X-\gamma^{-j})(X+\gamma^{-j})\right)$$

$$\cdot\prod_{\substack{j=1,\\ 2\nmid j}}^{2^s}\prod_{k=1}^{h}\left(\hat{N}_{\rho_k}(\gamma^jX)\hat{N}_{\rho_k q}(\gamma^jX)\hat{N}_{\rho_k}(-\gamma^jX)\hat{N}_{\rho_k q}(-\gamma^jX)\right).$$

Obviously, $(X-\gamma^{-j})(X+\gamma^{-j})=X^2-\lambda_2^{-j}$. By $\gamma^q=-\gamma$, we deduce that

$$\hat{N}_{\rho_k}(\gamma^jX)\hat{N}_{\rho_k q}(-\gamma^jX)\in F_q[X]$$

and

$$\hat{N}_{\rho_k q}(\gamma^jX)\hat{N}_{\rho_k}(-\gamma^jX)\in F_q[X].$$

We get the desired result. ■

The following theorem gives the polynomial generators of all negacyclic codes of length 2^mp^n over F_q with $4\mid(q-1)$. Let ε_i, ε_i^j and ϵ_i^j be equal to 0 or 1 when i,j range over the subscripts and superscripts respectively.

Theorem 3: Notations as in Lemma 2. Then all the negacyclic codes of length 2^mp^n over F_q with $4\mid(q-1)$ are given by:

(i) *if $m<s$,*

$$\left\langle\prod_{\substack{j=1,\\ 2\nmid j}}^{2^{m+1}}\prod_{k=0}^{h}\hat{M}_{\rho_k}(\lambda_1^jX)^{\varepsilon_k^j}\right\rangle;$$

(ii) *if $m=s$ and f is odd,*

$$\left\langle\prod_{\substack{j=1,\\ 2\nmid j}}^{2^s}\prod_{k=0}^{h}\hat{M}_{\rho_k}(\lambda_2^jX^2)^{\varepsilon_k^j}\right\rangle;$$

(iii) *if $m=s$ and f is even,*

$$\left\langle\prod_{\substack{j=1,\\ 2\nmid i}}^{2^s}(X^2-\lambda_2^{-j})^{\varepsilon_j}\cdot\prod_{\substack{j=1,\\ 2\nmid j}}^{2^s}\prod_{k=1}^{h}\left(H_k^j(X)^{\varepsilon_k^j}K_k^j(X)^{\epsilon_k^j}\right)\right\rangle.$$

B. NEGACYCLIC CODES OF LENGTH $4p^n$ OVER F_q WITH $4\nmid(q-1)$

Let F_q be a finite field of odd order q and $F_q^*=\langle\xi\rangle$ as before. Recall that $q-1=2^sc$, where c is an odd positive integer. In the previous subsection, we have given the polynomial generators of all negacyclic codes of length 2^mp^n over F_q with $s\geq 2$. In this subsection, we continue to give the polynomial generators of all negacyclic codes of length 2^mp^n over F_q with $s=1$, i.e. $4\nmid(q-1)$; we further assume that $2^a\,||\,(q+1)$, where the notation $2^a\|(q+1)$ means $2^a\mid(q+1)$ but $2^{a+1}\nmid(q+1)$. It is readily seen that $a\geq 2$.

Let e be a positive integer. It is remarkable that, the irreducible factorization of $X^{2^e}+1$ over F_q has been characterized precisely (see [5, Theorem 1] or [13, Remark 2.2]). We reproduce it here. Set $U_1=\{0\}$; recursively define

$$U_i=\left\{\pm\left(\frac{u+1}{2}\right)^{\frac{q+1}{4}}\,\middle|\,u\in U_{i-1}\right\},$$

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

$$U_a=\left\{\pm\left(\frac{u-1}{2}\right)^{\frac{q+1}{4}}\,\middle|\,u\in U_{a-1}\right\}.$$

Then

$$X^{2^e}+1=\begin{cases}\prod_{u\in U_e}(X^2-2uX+1), & \text{if } e\leq a-1;\\ \prod_{u\in U_a}(X^{2^{e-a+1}}-2uX^{2^{e-a}}-1), & \text{if } e\geq a.\end{cases}$$

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

It is plain that $m\leq a$ by our hypothesis $X^{2^m}+1$ factors completely into degree-one factors in $F_{q^2}[X]$. If $m<a$, then $X^{2^m}+1=\prod_{u\in U_m}(X^2-2uX+1)$ is the irreducible factorization over F_q. Let β_u be a primitive 2^{m+1}th root of unity in F_{q^2} such that $X^2-2uX+1=(X-\beta_u)(X-\beta_u^{-1})$, then

$$X^{2^mp^n}+1=\prod_{u\in U_m}(X^{p^n}-\beta_u)(X^{p^n}-\beta_u^{-1}).$$

We take $\gamma_u\in F_{q^2}$ such that $\gamma_u^{p^n}\beta_u=1$. Note that $\beta_u^q=\beta_u^{-1}$, which implies $\gamma_u^q=\gamma_u^{-1}$.

Lemma 4: Notations as given above.

If $m<a$ and f is odd, then the irreducible factorization of $X^{2^mp^n}+1$ over F_q is given as follows:

$$X^{2^mp^n}+1=\prod_{u\in U_m}\prod_{j=0}^{h}I_j^u(X),$$

where $I_j^u(X)=\hat{M}_{\rho_j}(\gamma_uX)\hat{M}_{\rho_j}(\gamma_u^{-1}X)$.

If $m<a$ and f is even, then the irreducible factorization of $X^{2^mp^n}+1$ over F_q is given as follows:

$$X^{2^mp^n}+1=\prod_{u\in U_m}(X^2-2uX+1)\cdot\prod_{u\in U_m}\prod_{j=1}^{h}S_j^u(X)T_j^u(X),$$

where $S_j^u(X)=\hat{N}_{\rho_j}(\gamma_uX)\hat{N}_{\rho_j q}(\gamma_u^{-1}X)$ and $T_j^u(X)=\hat{N}_{\rho_j}(\gamma_u^{-1}X)\hat{N}_{\rho_j q}(\gamma_uX)$.

Proof: Since f is odd, then $C_{\rho_0} = \{0\}$, C_{ρ_1}, $C_{\rho_2}, \cdots, C_{\rho_h}$ are all the distinct q^2-cyclotomic cosets modulo p^n. Hence

$$X^{p^n} - \beta_u = \beta_u \prod_{j=0}^{h} M_{\rho_j}(\gamma_u X),$$

$$X^{p^n} - \beta_u^{-1} = \beta_u^{-1} \prod_{j=0}^{h} M_{\rho_j}(\gamma_u^{-1} X).$$

It follows that

$$X^{2^m p^n} + 1 = \prod_{u \in U_m} (X^{p^n} - \beta_u)(X^{p^n} - \beta_u^{-1})$$
$$= \prod_{u \in U_m} \prod_{j=0}^{h} \hat{M}_{\rho_j}(\gamma_u X)\hat{M}_{\rho_j}(\gamma_u^{-1} X).$$

By $\gamma_u^q = \gamma_u^{-1}$, one can show that $I_j^u(X) = \hat{M}_{\rho_j}(\gamma_u X)\hat{M}_{\rho_j}(\gamma_u^{-1} X)$ is a polynomial in $F_q[X]$. We obtain the desire result.

Similarly, we obtain the irreducible factorization of $X^{2^m p^n} + 1$ over F_q in case $m < a$ and f is even. ■

On the other hand, if $m = a$, then $X^{2^m} + 1 = \prod_{u \in U_a} (X^2 - 2uX - 1)$ is the irreducible factorization over F_q. Let ν_u be a root of $X^2 - 2uX - 1$. Clearly, ν_u is a primitive 2^{a+1}th root of unity in F_{q^2} such that $X^2 - 2uX - 1 = (X - \nu_u)(X + \nu_u^{-1})$. Therefore, in $F_{q^2}[X]$, we have

$$X^{2^m p^n} + 1 = \prod_{u \in U_a} (X^{p^n} - \nu_u)(X^{p^n} + \nu_u^{-1}).$$

Take $\theta_u \in F_{q^2}$ such that $\theta_u^{p^n} \nu_u = 1$. Note that $\nu_u^q = -\nu_u^{-1}$, which implies $\theta_u^q = -\theta_u^{-1}$.

Taking arguments similar to those used in Lemma 4, we have the following result.

Lemma 5: Notations as given above.

If $m = a$ and f is odd, then the irreducible factorization of $X^{2^m p^n} + 1$ over F_q is given as follows:

$$X^{2^m p^n} + 1 = \prod_{u \in U_a} \prod_{k=0}^{h} P_k^u(X),$$

where $P_k^u(X) = \hat{M}_{\rho_k}(\theta_u X)\hat{M}_{\rho_k}(-\theta_u^{-1} X)$.

If $m = a$ and f is even, then the irreducible factorization of $X^{2^m p^n} + 1$ over F_q is given as follows:

$$X^{2^m p^n} + 1 = \prod_{u \in U_a} (X^2 - 2uX - 1) \cdot \prod_{u \in U_a} \prod_{k=1}^{h} A_k^u(X) B_k^u(X),$$

where $A_k^u(X) = \hat{N}_{\rho_k}(\theta_u X)\hat{N}_{\rho_k q}(-\theta_u^{-1} X)$ and $B_k^u(X) = \hat{N}_{\rho_k q}(\theta_u X)\hat{N}_{\rho_k}(-\theta_u^{-1} X)$.

Combining Lemma 4 with Lemma 5, we obtain the polynomial generators of all negacyclic codes of length $2^m p^n$ over F_q with $4 \nmid (q-1)$.

Theorem 6: Notations as in Lemma 4 and Lemma 5. Let ε_i, ε_i^j and ϵ_i^j be equal to 0 or 1 when i, j range over the subscripts and superscripts respectively. Then the polynomial generators of all negacyclic codes of length $2^m p^n$ over F_q with $4 \nmid (q-1)$ are given by:

(i) *if $m < a$ and f is odd,*

$$\left\langle \prod_{u \in U_m} \prod_{k=0}^{h} I_k^u(X)^{\varepsilon_k^u} \right\rangle;$$

(ii) *if $m < a$ and f is even,*

$$\left\langle \prod_{u \in U_m} (X^2 - 2uX + 1)^{\varepsilon_u} \cdot \prod_{u \in U_m} \prod_{k=1}^{h} S_k^u(X)^{\epsilon_k^u} T_k^u(X)^{\varepsilon_k^u} \right\rangle;$$

(iii) *if $m = a$ and f is odd,*

$$\left\langle \prod_{u \in U_a} \prod_{j=0}^{h} P_j^u(X)^{\varepsilon_j^u} \right\rangle;$$

(iv) *if $m = a$ and f is even,*

$$\left\langle \prod_{u \in U_a} (X^2 - 2uX - 1)^{\varepsilon_u} \cdot \prod_{u \in U_a} \prod_{j=1}^{h} A_j^u(X)^{\varepsilon_j^u} B_j^u(X)^{\epsilon_j^u} \right\rangle.$$

IV. CONCLUSION

In this paper we determine the generator polynomials of all negacyclic codes of length $2^m p^n$ over F_q by assuming that $X^{2^m} + 1$ factors completely into degree-one factors in $F_{q^2}[X]$. It would be interest to find all self-dual or self-orthogonal negacyclic codes of length $2^m p^n$ over F_q in future works.

REFERENCES

[1] G. K. Bakshi and M. Raka, "A class of constacyclic codes over a finite field," *Finite Fields Appl.*, vol. 18, no. 2, pp. 362–377, Mar. 2012.

[2] G. K. Bakshi and M. Raka, "Self-dual and self-orthogonal negacyclic codes of length $2p^n$ over a finite field," *Finite Fields Appl.*, vol. 19, no. 1, pp. 39–54, Jan. 2013.

[3] E. R. Berlekamp, "Negacyclic codes for the Lee metric," in *Proc. Conf. Combinat. Math. Appl.*, Chapel Hill, NC, USA, 298-316, 1968.

[4] E. R. Berlekamp, *Algebraic Coding Theory (Revised edition)*. Laguna Hills, CA, USA: Aegean Park, 1984.

[5] I. F. Blake, S. Gao, and R. C. Mullin, "Explicit factorization of $x^{2^k} + 1$ over F p with prime p≡3 mod 4," *Appl. Algebra Engrg. Commun. Comput.*, vol. 4, no. 2, pp. 89–94, Jun. 1993.

[6] T. Blackford, "Negacyclic codes over Z4 of even length," *IEEE Trans. Inf. Theory*, vol. 6, no. 6, pp. 1417–1424, Jun. 2003.

[7] T. Blackford, "Negacyclic duadic codes," *Finite Fields Appl.*, vol. 14, no. 4, pp. 930–943, Nov. 2008.

[8] B. Chen, H. Q. Dinh, Y. Fan, and S. Ling, "Polyadic constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4895–4904, Sep. 2015.

[9] B. Chen, H. Q. Dinh, and H. Liu, "Repeated-root constacyclic codes of length ℓp^s and their duals," *Discrete Appl. Math.*, vol. 177, pp. 60–70, Nov. 2014.

[10] B. Chen, H. Q. Dinh, H. Liu, and L. Wang, "Constacyclic codes of length p^s over $F^{p^m} + uF^{p^m}$," *Finite Fields Appl.*, vol. 37, pp. 108–130, Jan. 2016.

[11] B. Chen, L. Lin, and H. Liu, "Constacyclic symbol-pair codes: Lower bounds and optimal constructions," *IEEE Trans. Inf. Theory*, vol. 63, no. 12, pp. 7661–7666, Dec. 2017.

[12] B. Chen, S. Ling, and G. Zhang, "Enumeration formulas for self-dual cyclic codes," *Finite Fields Appl.*, vol. 42, pp. 1–22, Nov. 2016.

[13] B. Chen, Y. Fan, L. Lin, and H. Liu, "Constacyclic codes over finite fields," *Finite Fields Appl.*, vol. 18, no. 6, pp. 1217–1231, Nov. 2012.

[14] B. Chen, L. Li, and R. Tuerhong, "Explicit factorization of $X^{2^m p^n} - 1$ over a finite field," *Finite Fields Appl.*, vol. 24, pp. 95–104, Nov. 2013.

[15] H. Q. Dinh and S. R. Lopez-Permouth, "Cyclic and negacyclic codes over finite chain rings," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1728–1744, Aug. 2004.
[16] H. Q. Dinh, "Complete distances of all negacyclic codes of length 2^s over Z_2a," *IEEE Trans. Inf. Theory*, vol. 53, no. 1 pp. 147–161, Jan. 2007.
[17] H. Q. Dinh, "On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions," *Finite Fields Appl.*, vol. 14, no. 1, pp. 22–40, Jan. 2008.
[18] H. Q. Dinh, "Constacylic codes of length p^s over $F^{p^m} + uF^{p^m}$," *J. Algebra*, vol. 324, pp. 940–950, Sep. 2010.
[19] H. Q. Dinh, "Repeated-root constacyclic codes of length $2p^s$," *Finite Fields Appl.*, vol. 18, no. 1, pp. 133–143, Jan. 2012.
[20] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[21] Y. Jia, S. Ling, and C. Xing, "On self-dual cyclic codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2243–2251, Apr. 2011.
[22] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
[23] A. Sharma, G. K. Bakshi, V. C. Dumir, and M. Raka, "Cyclotomic numbers and primitive idempotents in the ring GF(q)[x]/(x^{p^n}-1)," *Finite Fields Appl.*, vol. 10, pp. 653–673, Oct. 2004.
[24] Z. Wan, *Lectures on Finite Fields and Galois Rings*. Singapore: World Scientific, 2003.

JING HUANG received the B.Sc. degree in mathematics from Hubei Normal University, in 2013, and the M.Sc. and Ph.D. degrees in mathematics from Central China Normal University, in 2016 and 2019, respectively. She is currently with the School of Mathematics, South China University of Technology, Guangzhou, Guangdong, China. Her research interests include algebraic graph theory and algebraic coding theory.