Journal of Mathematical Research with Applications
May, 2016, Vol. 36, No. 3, pp. 275–284
DOI:10.3770/j.issn:2095-2651.2016.03.004
Http://jmre.dlut.edu.cn

Repeated-Root Self-Dual Negacyclic Codes over Finite Fields

Xiuli LI[1,2]
1. *School of Mathematics and Physics, Qingdao University of Science and Technology, Shandong* 266000*, P. R. China;*
2. *College of Information Science and Engineering, Ocean University of China, Shandong* 266000*, P. R. China*

Abstract Let F_q be a finite field with $q = p^m$, where p is an odd prime. In this paper, we study the repeated-root self-dual negacyclic codes over F_q. The enumeration of such codes is investigated. We obtain all the self-dual negacyclic codes of length $2^a p^r$ over F_q, $a \geq 1$. The construction of self-dual negacyclic codes of length $2^a bp^r$ over F_q is also provided, where $\gcd(2, b) = \gcd(b, p) = 1$ and $a \geq 1$.

Keywords constacyclic codes; negacyclic codes; self-dual codes; generator polynomials

MR(2010) Subject Classification 11T71

1. Introduction

The class of constacyclic codes plays a significant role in the theory of error correcting codes. These include cyclic and negacyclic codes, which have been well studied since 1950's. Constacyclic codes can be efficiently encoded using shift registers, which explains their preferred role in engineering.

Definition 1.1 *Let F_q be the Galois field with q elements. For $\lambda \in F_q^*$, a subset C of F_q^n is called a λ-constacyclic code of length n if*

(1) C is a subspace of F_q^n;

(2) if $c = (c_0, c_1, \ldots, c_{n-1})$ is a codeword of C, then $T_\lambda(c) = (\lambda c_{n-1}, c_0, \ldots, c_{n-2})$ is also a codeword in C.

T_λ is called λ-constacyclic shift. When $\lambda = 1$, λ-constacyclic codes are cyclic codes. When $\lambda = -1$, λ-constacyclic codes are negacyclic codes.

If n is coprime to the characteristic of F_q, a λ-constacyclic code of length n over F_q is called simple-root λ-constacyclic code; otherwise it is called repeated-root λ-constacyclic code. Simple-root λ-constacyclic codes of a given length over finite fields have been studied extensively by several authors [1–9]. Sharma et al. [7,8] studied simple-root cyclic codes of prime power length

Received May 5, 2015; Accepted January 13, 2016
Supported by Reward Fund for Outstanding Young and Middle-Aged Scientists of Shandong Province (Grant No. BS2011DX011) and Qingdao Postdoctoral Fund (Grant No. 861605040007).
E-mail address: lixiuli2004@tom.com

over a finite field. Repeated-root λ-constacyclic codes, although, are known to be asymptotically bad, nevertheless, are optimal in a few cases, which have motivated the researchers to further study these codes.

If $q = 2^m$, then the negacyclic codes are just cyclic codes. Self-dual cyclic codes have been studied in [10–12]. Jia et al. [10] showed that self-dual cyclic codes of length n over F_q exist if and only if n is even and $q = 2^m$ with m a positive integer. Thus we assume that q is an odd prime power while considering negacyclic codes.

Bakshi and Raka [13] explicitly determined all the simple root self-dual negacyclic codes of length $2p^n$, $n \geq 1$, over F_q where p is an odd prime coprime to q. Bakshi and Raka [14] obtained all the simple root self-dual negacyclic codes of length 2^n over F_q. Dinh [15] provided the self-dual negacyclic codes of length $2p^s$ over F_{p^m}. In this paper, self-dual negacyclic codes are considered in a more general domain than in [14] and [15]. We study the repeated-root self-dual negacyclic codes of length $n'p^r$ over the finite field F_{p^m} with p an odd prime such that $\gcd(n', p) = 1$. The rest of this paper is organized as follows. In Section 2, the conditions for the existence of self-dual negcyclic codes are given. We also give a characterization of the generator polynomials of self-dual negacyclic codes. In Section 3, we provide the enumeration formula for the self-dual negcyclic codes of length $n = 2^a p^r$, $a \geq 1$, $r \geq 0$. In Section 4, the construction of self-dual negacyclic codes of length $n = 2^a b p^r$ over F_q such that $\gcd(2, b) = \gcd(b, p) = 1$ and $a \geq 1$ is presented.

2. Self-dual negacyclic codes

Let F_q be the Galois field with q elements. Let $F_q[x]$ denote the polynomials in the indeterminate x with coefficients in F_q. In the following part of this paper we always assume that $q = p^m$ with p an odd prime except specific explanation. For $\lambda \in F_q^*$, let $R = F_q[x]/\langle x^n - \lambda\rangle$, where $\langle x^n - \lambda\rangle$ denotes the ideal generated by $x^n - \lambda$ in $F_q[x]$.

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $F_q[x]/\langle x^n - \lambda\rangle$, $xc(x)$ corresponds to a λ-constacyclic shift of $c(x)$. The following facts are well known and straightforward.

Proposition 2.1 ([16]) *A linear code C of length n is λ-constacyclic over F_q if and only if C is an ideal of $F_q[x]/\langle x^n - \lambda\rangle$. Moreover, $F_q[x]/\langle x^n - \lambda\rangle$ is a principal ideal ring, whose ideals are generated by monic factors of $x^n - \lambda$.*

Proposition 2.2 ([16]) *The dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.*

In particular, the dual of a negacyclic code is also a nagacyclic code.

For any linear code C of length n over F_q, the dual $C^{\perp}$ is defined as $C^{\perp} = \{u \in F_q^n \mid u \cdot v = 0, \forall v \in C\}$, where $u \cdot v$ denotes the standard inner product of u and v in F_q^n. The code is called self-dual if $C = C^{\perp}$.

For any polynomial $f(x) = \sum_{i=0}^{r} a_i x^i$ of degree r ($a_r \neq 0$) over F_q, let $\overleftarrow{f(x)}$ denote a polynomial given by

$$\overleftarrow{f(x)} = x^r f\left(x^{-1}\right) = \sum_{i=0}^{r} a_{r-i} x^i.$$

Furthermore, if $a_0 \neq 0$, then let $f^*(x) = a_0^{-1}\overleftarrow{f(x)}$, $f^*(x)$ is called the reciprocal polynomial of $f(x)$. It is clear that $(f(x)g(x))^* = f^*(x)g^*(x)$ for polynomials $f(x), g(x) \in F_q[x]$. In particular, if a polynomial is equal to its reciprocal polynomial over F_q, then it is called self-reciprocal over F_q.

Let C be a q-ary negacyclic code of length n generated by $g(x)$ which is monic. Then $g(x)|(x^n+1)$. Let the annihilator of C, denoted by $\mathrm{ann}(C)$ be the set

$$\mathrm{ann}(C) = \{f(x) \in F_q[x]/\langle x^n+1\rangle : f(x)g(x) \equiv 0 \bmod (x^n+1)\}.$$

Put $h(x) = \frac{x^n+1}{g(x)}$. Clearly $\mathrm{ann}(C)$ is an ideal in $F_q[x]$ generated by $h(x)$. $h(x)$ is the check polynomial of C. The dimension of C is $\deg(h(x))$.

Suppose that $h(x) = \sum_{i=0}^{k} b_i x^i$. Notice that $b_k = 1$ and $b_0 \neq 0$. Then $h^*(x)$ is a generator polynomial of $C^{\perp}$. It is known that the dual code $C^{\perp}$ is generated by $h^*(x)$ (see [15]). Thus the following proposition holds.

Proposition 2.3 *A negacyclic code C of length n is self-dual if and only if $g(x) = h^*(x)$, where $g(x)$ is the generator polynomial of C, $h(x)$ is the check polynomial of $C^{\perp}$ and $h^*(x)$ is the reciprocal polynomial of $h(x)$.*

Clearly, self-dual codes of odd length over F_q do not exist. Suppose that C is a self-dual negacyclic code of length n over F_q. Then n must be even and $\deg(g(x)) = \deg(h(x)) = \frac{n}{2}$.

Each negacyclic code over F_q is uniquely determined by its generator polynomial, a monic divisor of x^n+1 over F_q. Notice that $q = p^m$ with p an odd prime. In order to describe the generator polynomials of $\left[n, \frac{n}{2}\right]_q$ self-dual negacyclic codes, we need to know the factorization of x^n+1 over F_q. Write $n = n'p^r$ with $\gcd(n', p) = 1$, r is a nonnegative integer. Then n' is even and $x^n+1 = (x^{n'}+1)^{p^r}$.

If $x^{n'}+1 = p(x)q(x)$, then $x^{n'}+1 = (x^{n'}+1)^* = p^*(x)q^*(x)$. Thus for any irreducible polynomial dividing $x^{n'}+1$ over F_q, its reciprocal polynomial also divides $x^{n'}+1$ over F_q and is also irreducible over F_q. Since $\gcd(n', p) = 1$, the polynomial $x^{n'}+1$ can be factorized into distinct irreducible polynomials as follows

$$x^{n'}+1 = f_1(x)\cdots f_s(x)h_1(x)h_1^*(x)\cdots h_t(x)h_t^*(x),$$

where $f_i(x)$ $(1 \le i \le s)$ are monic irreducible self-reciprocal polynomials over F_q while $h_j(x)$ and its reciprocal polynomial $h_j^*(x)$ $(1 \le j \le t)$ are both monic irreducible polynomials over F_q. We say that $h_j(x)$ and $h_j^*(x)$ form a reciprocal polynomial pair. Therefore

$$x^n+1 = f_1(x)^{p^r}\cdots f_s(x)^{p^r} h_1(x)^{p^r} h_1^*(x)^{p^r}\cdots h_t(x)^{p^r} h_t^*(x)^{p^r}. \tag{2.1}$$

Note that s and t both depend on n and q. We regard them as two functions of the pair (n, q). As in [10], we give the following notation.

Definition 2.4 *Define $s(n,q)$ to be the number of self-reciprocal polynomials in the factorization of $x^{n'}+1$ over F_q, and $t(n,q)$ be the number of reciprocal polynomial pairs in the factorization of $x^{n'}+1$ over F_q.*

We can describe the generator polynomials for the self-dual negacyclic codes as soon as we know the factorization of x^n+1 over F_q.

Theorem 2.5 *Let x^n+1 be factorized as in (2.1). A negacyclic code C of length n is self-dual over F_q if and only if $s(n,q)=0$ and its generator polynomial is of the form*

$$h_1(x)^{\beta_1}h_1^*(x)^{p^r-\beta_1}\cdots h_t(x)^{\beta_t}h_t^*(x)^{p^r-\beta_t}, \tag{2.2}$$

where $t=t(n,q)$ and $0\le\beta_i\le p^r$ for each $1\le i\le t$.

Proof Let C be a negacyclic code of length n over F_q and $g(x)$ be its generator polynomial. We need to show that C is self-dual if and only if $g(x)$ is of the form as in (2.2).

Let $s=s(n,q)$ and $t=t(n,q)$. Since the generator polynomial $g(x)$ of C is monic and divides x^n+1, we may assume that

$$g(x)=f_1(x)^{\alpha_1}\cdots f_s(x)^{\alpha_s}h_1(x)^{\beta_1}h_1^*(x)^{\gamma_1}\cdots h_t(x)^{\beta_t}h_t^*(x)^{\gamma_t},$$

where $0\le\alpha_i\le p^r$ for each $1\le i\le s$, and $0\le\beta_j,\gamma_j\le p^r$ for each $1\le j\le t$. Then the check polynomial of C is

$$h(x)=f_1(x)^{p^r-\alpha_1}\cdots f_s(x)^{p^r-\alpha_s}h_1(x)^{p^r-\beta_1}h_1^*(x)^{p^r-\gamma_1}\cdots h_t(x)^{p^r-\beta_t}h_t^*(x)^{p^r-\gamma_t}.$$

Hence

$$h^*(x)=f_1(x)^{p^r-\alpha_1}\cdots f_s(x)^{p^r-\alpha_s}h_1^*(x)^{p^r-\beta_1}h_1(x)^{p^r-\gamma_1}\cdots h_t^*(x)^{p^r-\beta_t}h_t(x)^{p^r-\gamma_t}.$$

By Proposition 2.3, C is self-dual if and only if $g(x)=h^*(x)$. Thus

$$\begin{cases}\alpha_i=p^r-\alpha_i, & 1\le i\le s;\\ \gamma_j=p^r-\beta_j, & 1\le j\le t.\end{cases}$$

Since p is odd, so $\alpha_i=p^r-\alpha_i$ does not hold for any i, $1\le i\le s$. Thus C is self-dual if and only if $s=0$ and its generator polynomial $g(x)$ is of the form as in (2.2). $\Box$

Corollary 2.6 *Let x^n+1 be factorized over F_q as in (2.1) with $s=s(n,q)=0$. Then the number of $[n,\frac{n}{2}]_q$ self-dual negacyclic codes is exactly $(p^r+1)^{t(n,q)}$.*

We may give all the self-dual negacyclic codes of length n over F_q following the factorization of $x^{n'}+1$ over F_q.

Example 2.7 Let $q=3$, $n=60=n'\cdot 3$ such that $n'=20=2^2\cdot 5$. We have

$$\begin{aligned}x^{20}+1=&(x^2+x+2)(x^2+2x+2)(x^4+x^2+x+1)(x^4+x^2+2x+1)\\&(x^4+x^3+x^2+1)(x^4+2x^3+x^2+1).\end{aligned}$$

There are three reciprocal polynomial pairs:

$$(x^2+x+2) \text{ and } (x^2+2x+2);$$

$$(x^4+x^2+x+1) \text{ and } (x^4+x^3+x^2+1);$$

$$(x^4+x^2+2x+1) \text{ and } (x^4+2x^3+x^2+1).$$

Thus $t(60,3)=3$ and there are 4^3 self-dual negacyclic codes of length 60 over F_3. The generator polynomials are

$$(x^2+x+2)^{\beta_1}(x^2+2x+2)^{3-\beta_1}(x^4+x^2+x+1)^{\beta_2}(x^4+x^3+x^2+1)^{3-\beta_2}$$
$$(x^4+x^2+2x+1)^{\beta_3}(x^4+2x^3+x^2+1)^{3-\beta_3},$$

where $0\le\beta_i\le 3$, $1\le i\le 3$.

Blackford [3] gave the necessary and sufficient conditions for the existence of self-dual negacyclic codes over F_q.

Theorem 2.8 ([3]) *If $n=2^ab$ for some odd integer b, $a\ge 1$. Then self-dual negacyclic codes over F_q of length n exist if and only if $q\not\equiv -1 \pmod{2^{a+1}}$. Thus let n be a positive integer and factorize it as $n=n'p^r=2^abp^r$, where $a\ge 1$, b is an odd integer and $\gcd(b,p)=1$. Since bp^r is odd, then self-dual negacyclic codes over F_q of length n exist if and only if $q\not\equiv -1 \pmod{2^{a+1}}$.*

For convenience, we adopt a notation : $2^e \parallel m$ means $2^e|m$ but $2^{e+1} \not| m$, where e and m are positive integers.

Example 2.9 (1) For $q=3$, $2^2\parallel 4$. From Theorem 2.8 it follows that there exist self-dual negacyclic codes over F_3 of length $n=n'p^r=2^ab3^r$, where $a\ge 1$, b is an odd integer with $\gcd(b,3)=1$ if and only if $a\ge 2$.

(2) For $q=5$, $2^1\parallel 6$. From Theorem 2.8 it follows that there exist self-dual negacyclic codes over F_5 of length $n=n'p^r=2^ab5^r$, where $a\ge 1$, b is an odd integer with $\gcd(b,5)=1$ if and only if $a\ge 1$.

(3) For $q=7$, $2^3\parallel 8$. From Theorem 2.8 it follows that there exist self-dual negacyclic codes over F_7 of length $n=n'p^r=2^ab7^r$, where $a\ge 1$, b is an odd integer with $\gcd(b,7)=1$ if and only if $a\ge 3$.

(4) For $q=9$, $2^1\parallel 10$. From Theorem 2.8 it follows that there exist self-dual negacyclic codes over F_9 of length $n=n'p^r=2^ab3^r$, where $a\ge 1$, b is an odd integer with $\gcd(b,3)=1$ if and only if $a\ge 1$.

The following 4 tables list the numbers of self-dual negacyclic codes over F_q of lengths n' up to 448,144,576 and 224 for $q=3,5,7,9$, respectively. We use MAGMA software to perform factorization. Notice that $t(n,q)=t(n',q)$ under the hypotheses.

$n'=2^ab$	4	8	16	32	64	20	40	80	160	320	28	56	112	224	448
a	2	3	4	5	6	2	3	4	5	6	2	3	4	5	6
b	1	1	1	1	1	5	5	5	5	5	7	7	7	7	7
$t(n',q)$	1	1	1	1	1	3	5	5	5	5	3	3	3	3	3

Table 1 $q=3$, $n=n'3^r=2^ab3^r$, $a\ge 2$, $r\ge 0$, $\gcd(2,b)=\gcd(b,3)=1$. The number of self-dual negacyclic codes over F_3 of length n is $(3^r+1)^{t(n',q)}$.

$n'=2^ab$	2	4	8	16	6	12	24	48	14	28	56	112	18	36	72	144
a	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
b	1	1	1	1	3	3	3	3	7	7	7	7	9	9	9	9
$t(n',q)$	1	1	1	1	2	3	3	3	2	3	3	3	3	5	5	5

Table 2 $q=5$, $n=n'5^r=2^ab5^r$, $a\geq 1$, $r\geq 0$, $\gcd(2,b)=\gcd(b,5)=1$. The number of self-dual negacyclic codes over F_5 of length n is $(5^r+1)^{t(n',q)}$.

$n'=2^ab$	8	16	32	64	24	48	96	192	40	80	160	320	72	144	288	576
a	3	4	5	6	3	4	5	6	3	4	5	6	3	4	5	6
b	1	1	1	1	3	3	3	3	5	5	5	5	9	9	9	9
$t(n',q)$	2	2	2	2	6	6	6	6	6	10	10	10	10	10	10	10

Table 3 $q=7$, $n=n'7^r=2^ab7^r$, $a\geq 3$, $r\geq 0$, $\gcd(2,b)=\gcd(b,7)=1$. The number of self-dual negacyclic codes over F_7 of length n is $(7^r+1)^{t(n',q)}$.

$n'=2^ab$	2	4	8	16	32	10	20	40	80	160	14	28	56	112	224
a	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
b	1	1	1	1	1	5	5	5	5	5	7	7	7	7	7
$t(n',q)$	1	2	2	2	2	3	3	10	10	10	3	6	6	6	6

Table 4 $q=9$, $n=n'3^r=2^ab3^r$, $a\geq 1$, $r\geq 0$, $\gcd(2,b)=\gcd(b,3)=1$. The number of self-dual negacyclic codes over F_9 of length n is $(3^r+1)^{t(n',q)}$.

3. Self-dual negacyclic codes of length 2^ap^r

Let F_q be the Galois field with q elements, $q=p^m$, and p is an odd prime. Let n be a positive integer such that $n=n'p^r=2^ap^r$ with $a\geq 1$.

For any $s\geq 0$, let $C_s=\{s,sq,sq^2,\ldots,sq^{m_s-1}\}$ denote the q-cyclotomic coset containing s modulo 2^{a+1}, where m_s is the least positive integer such that $sq^{m_s}\equiv s \pmod{2^{a+1}}$. Let α be a primitive 2^{a+1}-th root of unity in some extension field of F_q. It is well known that [16]

$$M_s(x)=\prod_{i\in C_s}(x-\alpha^i)$$

is the minimal polynomial of α^s over F_q and

$$x^{2^{a+1}}-1=\prod M_s(x)$$

gives the factorization of $x^{2^{a+1}}-1$ into irreducible factors over F_q, where s runs over a complete set of representatives from distinct q-cyclotomic cosets modulo 2^{a+1}. We choose α, a primitive 2^{a+1}-th root of unity satisfying $\alpha^{2^a}=-1$. Such a choice of α is possible.

Since $q=p^m$ is odd, we can write $q=1+2^dc$ or $-1+2^dc$ for some integers c, d, $d\geq 2$ and c odd, according as $q\equiv 1 \pmod 4$ or $q\equiv -1 \pmod 4$.

In [14], the authors provided the following theorems.

Theorem 3.1 ([14]) *Let $a \geq 1$, $q = 1 + 2^d c$, $d \geq 2$, c odd. Then*

$$x^{2^a} + 1 = \begin{cases} \prod_{i=0}^{2^{d-2}-1} M_{3^i}(x)M_{-3^i}(x), & \text{if } a \geq d; \\ \prod_{i=0}^{2^{a-1}-1} M_{3^i}(x)M_{-3^i}(x), & \text{if } a \leq d-1. \end{cases}$$

Theorem 3.2 ([14]) *Let $a \geq 1$, $q = -1 + 2^d c$, $d \geq 2$, c odd. Then*

$$x^{2^a} + 1 = \begin{cases} M_1(x)M_3(x)\cdots M_{3^{(2^{d-1}-1)}}(x), & \text{if } a \geq d \geq 3; \\ M_1(x)M_3(x)\cdots M_{3^{(2^{a-1}-1)}}(x), & \text{if } a \leq d-1,\ d \geq 3; \\ M_1(x)M_{-1}(x), & \text{if } a \geq 2,\ d = 2. \end{cases}$$

In the following we apply the above conclusions to the negacyclic codes of length $2^a p^r$ over F_q.

Theorem 3.3 *Suppose that $q = 1 + 2^d c$, $d \geq 2$, c odd. Then there exist self-dual negacyclic codes of length 2^a over F_q if and only if $a \geq 1$. Suppose that $q = -1 + 2^d c$, $d \geq 2$, c odd. Then there exist self-dual negacyclic codes of length 2^a over F_q if and only if $a \geq d$.*

Proof If $q = 1 + 2^d c$, $d \geq 2$, c odd, then $q + 1 = 2 + 2^d c = 2(1 + 2^{d-1}c)$. Since $1 + 2^{d-1}c$ is odd, then $2 \parallel (q + 1)$. If $q = -1 + 2^d c$, $d \geq 2$, c odd, then $q + 1 = 2^d c$. Since c is odd, then $2^d \parallel (q + 1)$. From Theorem 2.8 it follows the conclusion holds. □

Theorem 3.4 *Let $n = n'p^r = 2^a p^r$, where $a \geq 1$, $r \geq 0$. Let d be the integer such that $2^d \parallel (q-1)$ while $q \equiv 1 \pmod 4$ or $2^d \parallel (q+1)$ while $q \equiv -1 \pmod 4$. And let $m = \min\{a-1, d-2\}$ when $q \equiv 1 \pmod 4$ or $q \equiv -1 \pmod 4$ and $a \geq d$. Then the number of self-dual negacyclic codes of length n over F_q is $(p^r + 1)^{2^m}$.*

Proof Suppose that $q = 1+2^d c$ and $a \geq 1$ or $q = -1+2^d c$ and $a \geq d$ such that $d \geq 2$ and c odd. By Theorem 2.8, there exist self-dual negacyclic codes of length 2^a over F_q. Thus $s(2^a, q) = 0$ and the irreducible polynomial factorization of $x^{2^a} + 1$ only contains distinct reciprocal polynomial pairs. From Theorems 3.1 and 3.2 it follows that

$$t(2^a, q) = \begin{cases} 2^{\min\{a-1,d-2\}}, & \text{if } q = 1 + 2^d c, d \geq 2, c \text{ odd}, a \geq 1; \\ 2^{d-2}, & \text{if } q = -1 + 2^d c, d \geq 2, c \text{ odd}, a \geq d. \end{cases}$$

Notice that $t(n, q) = t(2^a, q)$. From Corollary 2.6 and Theorem 3.3 it follows that the number of self-dual negacyclic codes of length n is

$$(p^r + 1)^{t(n,q)} = \begin{cases} (p^r + 1)^{2^{\min\{a-1,d-2\}}}, & \text{if } q = 1 + 2^d c, d \geq 2, c \text{ odd}, a \geq 1; \\ (p^r + 1)^{2^{d-2}}, & \text{if } q = -1 + 2^d c, d \geq 2, c \text{ odd}, a \geq d; \\ 0, & \text{otherwise.} \end{cases}$$

When $a \geq d$, $\min\{a - 1, d - 2\} = d - 2$. This completes the proof. □

Example 3.5 Suppose that $q = 9 = 3^2$. Then $q = 1 + 2^3$ and we may note $d = 3$. Let $n = n'3^r = 2^a 3^r$, where $a \geq 1$. Then the number of self-dual negacyclic codes of length n over

F_9 is

$$(3^r+1)^{t(n,9)} = \begin{cases} (3^r+1)^2, & \text{if } a \geq 2 \\ 3^r+1, & \text{if } a = 1. \end{cases}$$

In particular, for $n = 24 = 2^3 \cdot 3$ we have $a = 3$ and $r = 1$. Thus there are $4^2 = 16$ self-dual negacyclic codes of length 24 over F_9.

Furthermore, we may give the generator polynomials of the self-dual negacyclic codes of length $n = 2^a p^r$, $a \geq 1$.

Theorem 3.6 *Let $q = 1+2^d c$, $d \geq 2$, c odd. Let $n = 2^a p^r$, $a \geq 1$, $r \geq 0$ and $m = \min\{a-1, d-2\}$. Then the generator polynomials of the $(p^r+1)^{2^m}$ self-dual negacyclic codes of length n over F_q are precisely*

$$\prod_{i=0}^{2^m-1} M_{3^i}^{\beta_i}(x) M_{-3^i}^{p^r-\beta_i}(x)$$

where $0 \leq \beta_i \leq p^r$.

Proof Let $S = \{\pm 1, \pm 3, \pm 3^2, \ldots, \pm 3^{2^m-1}\}$. From Theorem 3.1 we have

$$x^{2^a} + 1 = \prod_{s \in S} M_s(x).$$

For any $s \in S$,

$$M_s(x) = \prod_{i \in C_s} (x - \alpha^i), \quad M_{-s}(x) = \prod_{i \in C_s} (x - \alpha^{-i}),$$

where α is the 2^{a+1}-th primitive root of unity over F_q satisfying $\alpha^{2^a} = -1$. We have

$$M_s^*(x) = \Big[\prod_{i \in C_s} (x - \alpha^i)\Big]^* = \prod_{i \in C_s} (x - \alpha^i)^* = \prod_{i \in C_s} (-x + \alpha^{-i}) = M_{-s}(x).$$

The last equation holds because $M_s(x)$ and $M_s^*(x)$ are all monic.

Thus

$$x^{2^a} + 1 = \prod_{i=0}^{2^m-1} M_{3^i}(x) M_{3^i}^*(x).$$

By Theorem 2.5, the conclusion holds. □

In the proof of Theorem 3.8, the following lemma plays an important role.

Lemma 3.7 ([14]) *Let $q = -1 + 2^d c$, $d \geq 2$, c odd. For any $a \geq d$, there exists some integer j, $0 \leq j \leq 2^{n+1-d} - 1$ such that*

$$3^{2^{d-2}} q^j \equiv -1 \pmod{2^{a+1}}.$$

Theorem 3.8 *Let $q = -1 + 2^d c$, $d \geq 2$, c odd. Let $n = 2^a p^r$, $a \geq d$, $r \geq 0$ and $m = \min\{a-1, d-2\}$. Then the generator polynomials of the $(p^r+1)^{2^m}$ self-dual negacyclic codes of length n over F_q are precisely*

$$\prod_{i=0}^{2^m-1} M_{3^i}^{\beta_i}(x) M_{-3^i}^{p^r-\beta_i}(x)$$

where $0 \le \beta_i \le p^r$.

Proof (1) Suppose that $d=2$, $a \ge 2$. Then $m=\min\{a-1,d-2\}=d-2=0$. We have $x^{2^a}+1=M_1(x)M_{-1}(x)$. As in Theorem 3.6 we have $M_{-1}(x)=M_1^*(x)$. Thus

$$x^{2^a}+1=M_1(x)M_1^*(x).$$

By Theorem 2.5, the conclusion holds.

(2) Suppose that $a \ge d \ge 3$. Then $m=\min\{a-1,d-2\}=d-2$. By Theorem 3.2,

$$x^{2^a}+1=M_1(x)M_3(x)\cdots M_{3^{(2^{d-1}-1)}}(x).$$

For any $i \in \{0,1,2,\ldots,2^{d-2}-1\}$,

$$M_{3^i}(x)=\prod_{s\in C_{3^i}}(x-\alpha^s),$$

where α is the 2^{a+1}-th primitive root of unity over F_q satisfying $\alpha^{2^a}=-1$. As in Theorem 3.6 we have $M_{3^i}^*(x)=M_{-3^i}(x)$.

By Lemma 3.7, there exists some integer j, $0 \le j \le 2^{n+1-d}-1$ such that

$$3^{2^{d-2}}q^j \equiv -1 \pmod{2^{a+1}}.$$

Thus $3^{i+2^{d-2}}q^j \equiv -3^i \pmod{2^{a+1}}$. So

$$M_{-3^i}(x)=M_{3^{i+2^{d-2}}}(x).$$

For any $i \in \{0,1,2,\ldots,2^{d-2}-1\}$. Then

$$x^{2^a}+1=\prod_{i=0}^{2^{d-2}-1}M_{3^i}(x)M_{3^{i+2^{d-2}}}(x)=\prod_{i=0}^{2^{d-2}-1}M_{3^i}(x)M_{-3^i}(x),$$

where $M_{-3^i}(x)=M_{3^i}^*(x)$. By Theorem 2.5, the conclusion holds. $\Box$

4. Construction of self-dual negacyclic codes of length 2^abp^r

Let F_q be the Galois field with q elements, $q=p^m$, and p is an odd prime. Let n be a positive integer such that $n=n'p^r=2^abp^r$, where $a \ge 1$, b is an odd integer and $\gcd(b,p)=1$. In this section we always suppose that $q \not\equiv -1 \pmod{2^{a+1}}$.

By Theorems 3.1 and 3.2, we have the following facts.

Theorem 4.1 *Let* $a \ge 1$, $q=1+2^dc$, $d \ge 2$, c *odd. Then*

$$x^{2^ab}+1=\begin{cases}\prod_{i=0}^{2^{d-2}-1}M_{3^i}(x^b)M_{-3^i}(x^b), & \text{if } a \ge d;\\ \prod_{i=0}^{2^{a-1}-1}M_{3^i}(x^b)M_{-3^i}(x^b), & \text{if } a \le d-1.\end{cases}$$

Theorem 4.2 *Let* $a \ge 1$, $q=-1+2^dc$, $d \ge 2$, c *odd. Then*

$$x^{2^ab}+1=\begin{cases}M_1(x^b)M_3(x^b)\cdots M_{3^{(2^{d-1}-1)}}(x^b), & \text{if } a \ge d \ge 3;\\ M_1(x^b)M_3(x^b)\cdots M_{3^{(2^{a-1}-1)}}(x^b), & \text{if } a \le d-1,\ d \ge 3;\\ M_1(x^b)M_{-1}(x^b), & \text{if } a \ge 2,\ d=2.\end{cases}$$

Suppose that $f(x) \in F_q[x]$ is a polynomial whose leading coefficient and constant term are non zero elements in F_q. It is easy to verify by definition that $[f(x^b)]^* = f^*(x^b)$. From Theorems 3.6 and 3.8 it follows the following facts.

Theorem 4.3 *Let $q = 1 + 2^d c$, $d \geq 2$, c odd. Let $n = 2^a b p^r$, $a \geq 1$, $\gcd(2, b) = \gcd(b, p) = 1$, $r \geq 0$ and $m = \min\{a-1, d-2\}$. Then the generator polynomials of self-dual negacyclic codes of length n over F_q are given by*

$$\prod_{i=0}^{2^m-1} M_{3^i}^{\beta_i}(x^b) M_{-3^i}^{p^r-\beta_i}(x^b)$$

where $0 \leq \beta_i \leq p^r$.

Theorem 4.4 *Let $q = -1 + 2^d c$, $d \geq 2$, c odd. Let $n = 2^a b p^r$, $a \geq d$, $\gcd(2, b) = \gcd(b, p) = 1$, $r \geq 0$. Then the generator polynomials of self-dual negacyclic codes of length n over F_q are given by*

$$\prod_{i=0}^{2^{d-2}-1} M_{3^i}^{\beta_i}(x^b) M_{-3^i}^{p^r-\beta_i}(x^b)$$

where $0 \leq \beta_i \leq p^r$.

Acknowledgements We thank the referees for their time and comments.

References

[1] G. K. BAKSHI, M. RAKA. *Minimal cyclic codes of length $p^n q$.* Finite Fields Appl., 2003, **9**(4): 432–448.

[2] G. K. BAKSHI, M. RAKA, A. SHARMA. *Idempotent Generators of Irreducible Cyclic Codes.* Ramanujan Math. Soc., Mysore, 2008.

[3] T. BLACKFORD. *Negacyclic duadic codes.* Finite Fields Appl.. 2008, **14**(4): 930–943.

[4] H. Q. DINH, S. R. LÓPEZ-PERMOUTH. *Cyclic and negacyclic codes over finite chain rings.* IEEE Trans. Inform. Theory, 2004, **50**(8): 1728–1744.

[5] J. M. JENSEN. *A class of constacyclic codes.* IEEE Trans. Inform. Theory, 1994, **40**(3): 951–954.

[6] D. RADKOVA, A. J. VAN ZANTEN. *Constacyclic codes as invariant subspaces.* Linear Algebra Appl., 2009, **430**(2-3): 855–864.

[7] A. SHARMA, G. K. BAKSHI, V. C. DUMIR, et al. *Cyclotomic numbers and primitive idempotents in the ring $GF(q)[x]/(x^{p^n} - 1)$.* Finite Fields Appl., 2004, **10**(4): 653–673.

[8] A. SHARMA, G. K. BAKSHI, V. C. DUMIR, et al. *Irreducible cyclic codes of length 2^n.* Ars Combin., 2008, **86**: 133–146.

[9] A. SHARMA, G. K. BAKSHI, V. C. DUMIR, et al. *Weight distributions of irreducible cyclic codes of length 2^n.* Finite Fields Appl., 2007, **13**(4): 1086–1096.

[10] Yan JIA, San LING, Chaoping XING. *On self-dual cyclic codes over finite fields.* IEEE Trans. Inform. Theory, 2011, **57**(4): 2243–2251.

[11] Xiaoshan KAI, Shixin ZHU. *On cyclic self-dual codes.* Appl. Algebra Engrg. Comm. Comput., 2008, **19**(6): 509–525.

[12] C. S. NEDELOAIA. *Weight distributions of cyclic self-dual codes.* IEEE Trans. Inform. Theory, 2003, **49**(6): 1582–1591.

[13] G. K. BAKSHI, M. RAKA. *Self-dual and self-orthogonal negacyclic codes of length $2p^n$ over a finite field.* Finite Fields Appl., 2013, **19**: 39–54.

[14] G. K. BAKSHI, M. RAKA. *A class of constacyclic codes over a finite field.* Finite Fields Appl., 2012, **18**(2): 362–377.

[15] H. Q. DINH. *Repeated-root constacyclic codes of length $2p^s$.* Finite Fields Appl., 2012, **18**(1): 133–143.

[16] W. C. HUFFMAN, V. PLESS. *Fundamentals of Error-Correcting Codes.* Cambridge University Press, Cambridge, 2003.