SOME NEW CONSTRUCTIONS OF ISODUAL AND LCD CODES OVER FINITE FIELDS

Fatma-Zohra Benahmed
University M’Hamed Bougara of Boumerdes
Faculty of Sciences, Boumerdes, Algeria

Kenza Guenda and Aicha Batoul*
University of Science and Technology: Houari Boumediene
Faculty of Mathematics, Algiers, 16411, Algeria

Thomas Aaron Gulliver
Department of Electrical and Computer Engineering
University of Victoria
Victoria, BC V8W 2Y2, Canada

(Communicated by Sihem Mesnager)

Abstract. This paper presents some new constructions of LCD, isodual, self-dual and LCD-isodual codes based on the structure of repeated-root constacyclic codes. We first characterize repeated-root constacyclic codes in terms of their generator polynomials and lengths. Then we provide simple conditions on the existence of repeated-root codes which are either self-dual negacyclic or LCD cyclic and negacyclic. This leads to the construction of LCD, self-dual, isodual, and LCD-isodual cyclic and negacyclic codes.

Repeated-root constacyclic codes were first studied by Berman [6] and Falkner et al. [14]. Since then several authors have studied these codes. Dinh determined the generator polynomials of constacyclic codes over \( \mathbb{F}_q \) of lengths \( 3p^r \) and \( 6p^r \) in [12] and [13], respectively. These results have been extended to more general lengths by Bakshi [2] and Chen et al. [10] who gave the generator polynomials of all constacyclic codes of lengths \( 2^l p^r \) and \( lp^r \) with \( l \) prime, respectively. Linear code with complementary dual (LCD) were introduced by Massey [26, 23]. They provide an optimum linear coding solution for the two-user binary adder channel. Further, it has been shown that asymptotically good LCD codes exist [23]. Li et al. and Guenda [21, 16] investigated LCD BCH codes. Carlet et al. [9] gave a general construction of LCD codes from arbitrary linear codes. Isodual codes are codes which are equivalent to their dual. These codes are related to isodual lattices construction [1]. Recently, Batoul et al. [4, 5] constructed classes of isodual codes from an important class of linear codes, namely the class of constacyclic codes.

In this paper, we construct new LCD, isodual and self-dual codes. Some of these codes are both isodual and LCD, and so are called LCD-isodual codes. These constructions are based on the structure of repeated-root constacyclic codes. We first characterize these codes in terms of their generator polynomials and lengths.

2010 Mathematics Subject Classification: Primary: 58F15, 58F17; Secondary: 53C35.
Key words and phrases: Repeated-root constacyclic codes, negacyclic codes, self-dual codes, LCD codes, isodual codes, LCD-isodual codes.

* Corresponding author: Aicha Batoul.
Then we provide simple conditions on the existence of repeated-root codes which are either self-dual negacyclic, or LCD, isodual cyclic and negacyclic. This leads to constructions of LCD, self-dual, isodual and LCD-isodual cyclic and negacyclic codes.

The remainder of this paper is organized as follows. Some preliminary results are given in Section 2. In Section 3, the structure of the generator polynomials of constacyclic codes of length $2^a mp^r$ with $0 \leq a$ is given using the generator polynomials of constacyclic codes of length $m$. Further, we provide conditions on the existence of LCD repeated-root cyclic and negacyclic codes. In Section 4, we present the structure of constacyclic codes of lengths $mp^r$ and $2^a mp^r$ over $\mathbb{F}_{p^r}$, and constructions are given for self-dual, LCD and LCD-isodual codes from duadic codes where $p$ is prime (odd or even). The minimum distance of these codes is also examined. In Section 5, the structure of the generator polynomials of constacyclic codes of length $2^a mp^r$ for $a \geq 1$ is presented using primitive $2^a$th roots of unity. The case when constacyclic codes are equivalent to cyclic codes is considered. Further, conditions on the existence of self-dual negacyclic codes of length $2^a mp^r$ over $\mathbb{F}_{p^r}$ are given and LCD-isodual cyclic and negacyclic codes are constructed. Finally, Section 6 provides some conclusions and a suggestion for future work.

1. Preliminaries

Let $p$ be a prime number and $\mathbb{F}_q$ the finite field with $q = p^s$ elements. An $[n, k]$ linear code $C$ over $\mathbb{F}_{p^r}$ is a $k$-dimensional subspace of $\mathbb{F}_{p^r}^n$. For $\lambda$ in $\mathbb{F}_q^*$, a linear code $C$ of length $n$ over $\mathbb{F}_q$ is said to be $\lambda$-constacyclic if it satisfies

$$\begin{align*}
(\lambda c_{n-1}, c_0, \ldots, c_{n-2}) &\in C, \text{ whenever } (c_0, c_1, \ldots, c_{n-1}) \in C.
\end{align*}$$

When $\lambda = 1$, respectively $\lambda = -1$, the code is called cyclic, respectively negacyclic. The Euclidean dual code $C^\perp$ of $C$ is defined as

$$C^\perp = \{(x_0, \ldots, x_{n-1}) \in \mathbb{F}_q^n, \sum_{i=0}^{n-1} x_i y_i = 0, \forall (y_0, \ldots, y_{n-1}) \in C\}.$$  

If $C = C^\perp$, then $C$ is self-dual. Note that the dual of a $\lambda$-constacyclic code is a $\lambda^{-1}$-constacyclic code.

A monomial linear transformation of $\mathbb{F}_q^n$ is an $\mathbb{F}_q$-linear transformation $\tau$ such that there exist scalars $\lambda_1, \ldots, \lambda_n$ in $\mathbb{F}_q^*$ and a permutation $\sigma \in S_n$ (the group of permutations of the set $\{1, 2, \ldots, n\}$) such that for all $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$, we have

$$\tau(x_1, \ldots, x_n) = (\lambda_1 x_{\sigma(1)}, \lambda_2 x_{\sigma(2)}, \ldots, \lambda_n x_{\sigma(n)}).$$  

(1)

When all the $\lambda_i$ in (1) are equal to 1, the monomial permutation is simply called a permutation. Two linear codes $C$ and $C'$ of length $n$ are equivalent if there exists a monomial transformation of $\mathbb{F}_q^n$ such that $\tau(C) = C'$. If $C$ is equivalent to $C^\perp$, then $C$ is called an isodual code. A linear code with a complementary dual (LCD) code is defined to be a linear code $C$ whose dual $C^\perp$ satisfies $C \cap C^\perp = \{0\}$. When a code is both isodual and LCD, it is called an LCD-isodual code.

For a monic polynomial $f(x) = a_0 + a_1 x + \ldots + a_r x^r$ in $\mathbb{F}_q[x]$ with $a_0 \neq 0$ and degree $r$, the reciprocal polynomial of $f(x)$ is

$$f^r(x) = x^r f(x^{-1}) = (a_r + a_{r-1} x + \ldots + a_0 x^r).$$  

(2)
If a polynomial $f(x) = af^*(x)$ for some $a \in \mathbb{F}_q^*$, then $f(x)$ is called self-reciprocal. We can easily verify the following equalities for polynomials.

(3) \( (f(x))^* = af(x) \) and \( (fg(x))^* = bf(x)^*g(x)^* \), for some $a$ and $b \in \mathbb{F}_q^*$.

Usually we do not care about the constant $a$ in the equality $f(x) = af^*(x)$, and we write $f(x) = f^*(x)$.

2. Repeated-root LCD constacyclic codes of length $mp^r$ over $\mathbb{F}_{p^s}$

It is well known that every $\lambda$-constacyclic code is generated by a unique polynomial of least degree which divides $x^n - \lambda$. Such a polynomial is called the generator of the code. This section presents the structure of constacyclic codes of lengths $mp^r$ over $\mathbb{F}_q$ where $(m, p) = 1$. Further, we give conditions on the existence of LCD constacyclic codes. We begin with an important lemma which will be used later.

**Lemma 2.1.** [19, Lemma 3.3] Let $q = p^s$ be a prime power, then for all $\lambda$ in $\mathbb{F}_q^*$ there exists $\lambda_0$ in $\mathbb{F}_q^*$ such that $\lambda = \lambda_0^p$ for $r$ in $\mathbb{N}$.

Since $\mathbb{F}_{p^r}$ has characteristic $p$, by Lemma 2.1 the polynomial $x^{mp^r} - \lambda$ can be factored as

(4) \( x^{mp^r} - \lambda = x^{mp^r} - \lambda_0^p = (x^m - \lambda_0)^{p^r} \),

where the polynomial $x^m - \lambda_0$ is a monic square-free polynomial. Hence from [11, Proposition 2.7], it factors uniquely as a product of pairwise coprime monic irreducible polynomials $f_1(x), \ldots, f_t(x)$. Thus from (4), we obtain the following factorization

(5) \( x^{mp^r} - \lambda_0^p = f_1(x)^{p^r} \ldots f_t(x)^{p^r} \).

Denote the factors $f_i$ in the factorization of $x^m - \lambda_0$ which are self-reciprocal by $g_1, \ldots, g_s$ and the remaining $f_i$ grouped in pairs by $h_1, h_1^t, \ldots, h_t, h_t^r$. Then we have

(6) \( x^n - \lambda = g_1^r(x) \ldots g_s^r(x)h_1^{pr}(x)h_1^{*pr}(x) \ldots h_t^{pr}(x)h_t^{*pr}(x) \).

From (6), a $\lambda$-constacyclic code $C$ of length $n = mp^r$ over $\mathbb{F}_{p^r}$ is generated by a polynomial of the form

(7) \( G(x) = g_1^{a_1}(x) \ldots g_s^{a_s}(x)h_1^{b_1}(x)h_1^{*c_1}(x) \ldots h_t^{b_t}(x)h_t^{*c_t}(x) \)

where $g_i(x)$ and $h_j(x)$ are the polynomials in (6) and $0 \leq a_i, b_j, c_k \leq p^r$. Denote by $\overline{C}$ the linear code with generator $g(x) = g_1(x) \ldots g_s(x)h_1(x)h_1^*(x) \ldots h_t(x)h_t^*(x)$, where $g_i$ and $h_j$ are the simple factors of $G$ given in (7). Then $\overline{C}$ is called the simple root code of $C$. From (4), if $C$ is a $\lambda$–constacyclic then $\overline{C}$ is a $\lambda_0$–constacyclic simple root code.

From [13], we have that if $\lambda \neq \pm 1$ then a $\lambda$-constacyclic code is an LCD code over $\mathbb{F}_q$. Hence in this section, we study $\lambda$-constacyclic LCD codes for $\lambda \in \{\pm 1\}$ and provide conditions on the existence of LCD cyclic and negacyclic codes of length $mp^r$ over $\mathbb{F}_{p^r}$. The following lemma is required to characterize LCD cyclic and negacyclic repeated-root codes. It was proven for cyclic codes in [26] and the proof for negacyclic codes is similar and so is omitted.

**Lemma 2.2.** If $g(x)$ is the generator polynomial of a $q$-ary cyclic, respectively negacyclic, code $C$ of length $n$, then $C$ is an LCD code if and only if $g(x)$ is self-reciprocal and all the monic irreducible factors of $g(x)$ have the same multiplicity in $g(x)$ and in $x^n - \lambda$ for $\lambda \in \{-1, 1\}$. 
Pang et al. [24, Theorem 3.1] gave the following result for cyclic codes. Using Lemma 2.2, it can be extended to negacyclic codes.

**Theorem 2.3.** Let $p^s$ be a prime power and $n = mp^r$ with $\gcd(m, p) = 1$. Then a cyclic LCD or negacyclic LCD code $C$ of length $n$ over $\F_{p^r}$ is generated by

$$g(x) = g_1^{a_1}(x) \cdots g_s^{a_s}(x)h_1^{b_1}(x)h_1^{s_1}(x) \cdots h_t^{b_t}(x)h_t^{s_t}(x),$$

where $a_i, b_j \in \{0, p^r\}$, and for all $1 \leq i \leq s, 1 \leq j \leq t$.

From Theorem 2.3 and a proof similar to that of [24, Theorem 4.1], we obtain the following result.

**Theorem 2.4.** Let $C$ be a cyclic or negacyclic code $C$ of length $n = mp^r$ over $\F_{p^r}$. Then $C$ is an LCD code if and only if the corresponding simple root code $\overline{C}$ is an LCD code. Further, $C$ has parameters $[n, p^r k, d]$ if and only if $\overline{C}$ has parameters $[m, k, d]$.

Next we provide a characterization of LCD cyclic and negacylic codes using their parameters. For this we need some facts concerning the defining sets of cyclic and negacyclic codes. Recall that the order of an element $a$ in the multiplicative group $\F_q^*$ is the smallest integer $t$ such that $a^t = 1$ in $\F_q^*$ and denote $t = \text{ord}_q(a)$. Let $n$ and $i$ be integers such that $0 \leq i < n$. The $q$-cyclotomic coset of $i$ modulo $n$ is the set

$$C_n(i) = \{i, iq, \ldots, iq^{l-1} \mod n\},$$

where $l$ is the smallest positive integer such that $iq^l \equiv i \mod n$.

The minimal polynomial of $\beta^i$ over $\F_q$ is

$$M_{\beta^i}(x) = \prod_{j \in C_n(i)} (x - \beta^j),$$

where $\beta$ is a primitive $n$-th root of unity in a suitable extension field of $\F_q$. A cyclic code $C$ of length $n$ over $\F_q$ and generator polynomial $f$ is uniquely determined by its defining set $T = \{0 \leq i < m \mid f(\beta^i) = 0\}$. Hence the defining set of a cyclic code over $\F_{p^r}$ is the union of some $p^r$-cyclotomic cosets. A similar definition holds for negacyclic codes. The roots of $x^n + 1$ are $\delta^{2i+1}$, $0 \leq i \leq n - 1$, where $\delta$ is a primitive $2n$-th root of unity in some extension field of $\F_q$. Let $\theta = \beta^2$ which is a primitive $n$-th root of unity, and $O_{2n}$ be the set of odd integers from 1 to $2n - 1$. The defining set of a negacyclic code $C$ of length $n$ and generator polynomial $g$ is the set $T = \{i \in O_{2n} : g(\delta^i) = 0\}$.

**Theorem 2.5.** Let $q$ be a power of an odd prime $p$ and $n = mp^r$ a positive integer such that $m$ is an odd integer. Assume that for $\lambda \in \{\pm 1\}$ we have $x^{mp^r} - \lambda = f_1(x)^{p^r} \cdots f_l(x)^{p^r}$. Then if $\text{ord}_{m}(q)$ is even then there exist cyclic LCD, respectively negacyclic LCD, codes of length $n$ over $\F_{p^r}$ generated by

$$\prod_{i=0}^{l} f_i^{t_i}(x),$$

where $t_i \in \{0, p^r\}$ and $I = \{i, 0 \leq i \leq l; \ C_m(i) = C_m(-i)\}$, respectively $I = \{i \in O_{2n}; \ C_m(i) = C_m(-i)\}$.
Proof. Cyclic and negacyclic codes of length $n$ are generated by polynomials of the form
\[ \prod_{i=0}^{l} f_i^t(x). \]
From [18], $\text{ord}_m(p^r)$ is even if and only if there exists $0 \leq i \leq l$ such that $C_m(i) = C_m(-i)$. This is true if and only if $f_i(x) = f_i^t(x)$ and if and only if $f_i^t(x) = f_i^t(x)$ where $t_i \in \{0, p^r\}$. Then if the $i$ which satisfy this property are in $I$, respectively in $O_{2n}$, the result follows.

For the construction of isodual codes we need the following result which was proven for cyclic codes but is also true for negacyclic codes if $\text{gcd}(n,p) \neq 1$ or $\text{gcd}(n,p) = 1$.

Proposition 2.6. [5, Proposition 3.1] Let $C$ be a cyclic, respectively negacyclic, code of length $n$ over $\mathbb{F}_q$ generated by $g(x)$, and $\gamma \in \mathbb{F}_q^*$ such that $\gamma^n = 1$. Then the following results hold.

(i) $C$ is equivalent to the cyclic, respectively negacyclic, code generated by $g^\ast(x)$.
(ii) $C$ is equivalent to the cyclic, respectively negacyclic, code generated by $g(\gamma x)$.

3. Repeated-root LCD and self-dual codes from duadic codes over $\mathbb{F}_{p^r}$

In this section we present the structure of constacyclic codes and give constructions of self-dual, LCD and LCD-isodual codes of lengths $mp^r$ and $2mp^r$ over $\mathbb{F}_{p^r}$ from duadic codes where $p$ is prime and $m$ is a positive odd integer such that $(m, p) = 1$.

3.1. Repeated-root LCD cyclic codes of length $mp^r$ from duadic cyclic codes.

Let $C$ be a cyclic code over $\mathbb{F}_{p^r}$ of length $m$ generated by $f(x)$ and $b$ be an integer such that $(b, m) = 1$. The function $\mu_b$ defined on $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ by $\mu_b(i) \equiv ib \mod m$ is a permutation of the coordinate positions $\{0, 1, 2, \ldots, m-1\}$ and is called a multiplier. Multipliers also act on polynomials and this gives the following ring automorphism

\[ \mu_b : \mathbb{F}_{p^r}[x]/(x^m - 1) \rightarrow \mathbb{F}_{p^r}[x]/(x^m - 1) \]
\[ f(x) \rightarrow \mu_b(f(x)) = f(x^b). \]

Let $S_1$ and $S_2$ be unions of cyclotomic cosets modulo $m$ such that $S_1 \cap S_2 = \emptyset$, $S_1 \cup S_2 = \mathbb{Z}_m \setminus \{0\}$, and $\mu_b S_1 \mod n = S_{(i+1) \mod 2}$. Then the triple $\mu_b$, $S_1$, $S_2$ is called a splitting modulo $m$. The odd-like duadic codes $D_1$ and $D_2$ are the cyclic codes over $\mathbb{F}_{p^r}$ with defining sets $S_1$ and $S_2$ and generator polynomials $f_1(x) = \prod_{i \in S_1} (x - \beta^i)$ and $f_2(x) = \prod_{i \in S_2} (x - \beta^i)$, respectively, where $\beta$ is a primitive $m$-th root of unity. The even-like duadic codes $C_1$ and $C_2$ are the cyclic codes over $\mathbb{F}_{p^r}$ with defining sets $\{0\} \cup S_1$ and $\{0\} \cup S_2$, respectively. The codes $D_i$ and $C_i$ have the property

\[ \mu_b(D_i) = D_{(i+1) \mod 2} \quad \text{and} \quad \mu_b(C_i) = C_{(i+1) \mod 2}. \]

From (9) and the fact that the multiplier $\mu_b$ is a permutation acting on the coordinate of the codes, we obtain that the odd-like duadic codes, respectively the even-like duadic codes, are equivalent. In this paper, the notation $p^r \equiv 0 \mod m$. 

\[ \text{(8)} \]
\[ \mu_b : \mathbb{F}_{p^r}[x]/(x^m - 1) \rightarrow \mathbb{F}_{p^r}[x]/(x^m - 1) \]
\[ f(x) \rightarrow \mu_b(f(x)) = f(x^b). \]
means that $p^s$ is a quadratic residue modulo $m$ where $p$ is a prime number and $m$ an integer such that $\gcd(p, m) = 1$. The following result gives some properties of duadic codes.

**Theorem 3.1.** [20] Duadic codes of length $m$ over $\mathbb{F}_{p^r}$ exist if and only if $p^s = \square \mod m$, i.e. if $m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ is the prime factorization of the odd integer $m$ where $s_j > 0$. Then duadic codes of length $m$ over $\mathbb{F}_{p^r}$ exist if and only if $p^r = \square \mod p_j$, $j \in \{1, 2, \ldots, k\}$. If $d_0$ is the minimum odd-like weight, then

(i) $d_0^2 \geq m$,

(ii) $d_0^2 - d_0 + 1 \geq m$ if the splitting is given by $\mu_{-1}$.

Next, we recall some results concerning the splitting.

**Proposition 3.2.** [5, Proposition 2] Let $\mathbb{F}_{p^r}$ be a finite field and $m$ a positive odd integer such that $(m, p) = 1$ and $p^s = \square \mod m$. Then there exists a pair of odd-like duadic codes over $\mathbb{F}_{p^r}$, $D_1$ and $D_2$ generated by $f_1(x)$ and $f_2(x)$, respectively, such that $x^m - 1 = (x - 1) f_1(x) f_2(x)$ and

(i) if the splitting is given by $\mu_{-1}$, then $f_1^*(x) = f_2(x)$ and $f_2^*(x) = f_1(x)$,

(ii) if the splitting is not given by $\mu_{-1}$, then $f_1^*(x) = f_1(x)$ and $f_2^*(x) = f_2(x)$.

We now give constructions of LCD cyclic codes using the generator polynomials of odd-like duadic codes over $\mathbb{F}_{p^r}$ of length $m$.

**Theorem 3.3.** Suppose there exists a pair of odd-like duadic codes $D_i = \langle f_i(x) \rangle$ of odd length $m$ with odd-like minimum distance $d$, then we have the following results.

(i) If the splitting modulo $m$ is not given by $\mu_{-1}$, then the cyclic codes of length $mp^r$ over $\mathbb{F}_{p^r}$ generated by

$$f_i^{p^r}(x), \ (x - 1)p^r f_i^{p^r}(x), \ i \in \{1, 2\},$$

are LCD codes over $\mathbb{F}_{p^r}$ with parameters $[mp^r, p^r \left(\frac{m+1}{2}\right), d]$, respectively $[mp^r, p^r \left(\frac{m-1}{2}\right), d']$, respectively $[mp^r, p^r \left(\frac{m-1}{2}\right), d' \geq d]$.

(ii) If $p$ is odd and the splitting is given by $\mu_{-1}$, then the cyclic code generated by

$$(x^{mp^r} - 1),$$

is a $[2mp^r, mp^r, 2]$ LCD-isodual code over $\mathbb{F}_{p^r}$.

**Proof.** For part (i), if the splitting modulo $m$ is not given by $\mu_{-1}$, then from Proposition 3.2 we have $f_1^*(x) = f_1(x)$ and $f_2^*(x) = f_2(x)$, so $(f_i^{p^r}(x))^* = f_i^{p^r}(x)$ and $(x - 1)p^r f_i^{p^r}(x))^* = (x - 1)p^r f_i^{p^r}(x)$ for $i \in \{1, 2\}$. Then by Lemma 2.2, the cyclic codes generated by

$$f_i^{p^r}(x), \ (x - 1)p^r f_i^{p^r}(x), \ i \in \{1, 2\},$$

are LCD codes of length $mp^r$ over $\mathbb{F}_{p^r}$. Further, the dimensions of these codes are obtained from the degree of the generator polynomial and the minimum distance in the first case is obtained from Theorem 2.3. The upper bound on the minimum distance in the second case comes from the fact that these codes contain the odd-like duadic codes $D_i$ which have minimum distance $d$.

For part (ii), assume that there is a splitting modulo $m$. From [18, Proposition 4.1] we obtain the decomposition

$$x^{2mp^r} - 1 = (x - 1)p^r (x + 1)p^r f_1^{p^r}(x) f_2^{p^r}(x) f_1^{p^r}(-x) f_2^{p^r}(-x).$$
Since the splitting is given by $\mu_{-1}$, from Proposition 3.2 we have $f_1^*(x) = f_2^*(x)$. Then $((x - 1)^p f_1^*(x) f_j^p(x)) = (x - 1)^p f_1^*(x) f_j^p(x)$, and from Lemma 2.2 the cyclic code $C$ of length $2mp^r$ generated by this polynomial is LCD. We also obtain that the dual of $C$ is generated by $(x + 1)^p f_1^*(x) f_j^p(x)$. From Proposition 2.6, the dual code is equivalent to the code generated by $(x - 1)^p f_1^p(x) f_j^p(x)$, so the code is LCD-isodual. The degree of the generator is $mp^r$, and hence the dimension is $2mp^r - mp^r$. Since the weight of the generator is 2, the minimum distance is 2.

3.2. Self-dual and LCD-isodual codes from duadic cyclic codes over $\mathbb{F}_{2^s}$. Let $q = 2^s$, $s \in \mathbb{N}^*$ and $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ be the prime factorization of the odd integer $m$. Then $2^s = \square \text{mod} \ m$, and $D_i = \langle f_i(x) \rangle$, $1 \leq i \leq 2$, be odd-like duadic codes over $\mathbb{F}_{2^s}$ with minimum distance $d$. Then for $1 \leq i \leq 2$, the cyclic codes generated by

$$g_i(x) = (x - 1)^{2^{s-1}} f_i^{2^s}(x),$$

are self-dual $[2^s m, 2^{s-1} m, \geq d]$ codes or isodual $[2^s m, 2^{s-1} m, \geq d]$ codes.

Theorem 3.4. Let $n = 2^s m$ with $m$ an odd integer, $a \geq 1$, $s$ an integer such that $2^s = \square \text{mod} \ m$, and $D_i = \langle f_i(x) \rangle$, $1 \leq i \leq 2$, be odd-like duadic codes over $\mathbb{F}_{2^s}$, with minimum distance $d$. Then if $f_i^*(x) = f_j^*(x)$ for $i \neq j$, we obtain

$$C_i^\perp = \langle h_i^*(x) \rangle = \langle (x - 1)^{2^{s-1}} (f_j^{2^s}(x))^* \rangle = \langle (x - 1)^{2^{s-1}} (f_j^{2^s}(x)) \rangle = C_i^\perp = \langle (x - 1)^{2^{s-1}} f_j^{2^s}(x) \rangle = C_i,$$

and therefore $C_i$ is self-dual. If $f_i^*(x) = f_j^*(x)$ for $i \in \{1, 2\}$, then

$$C_i^\perp = \langle h_i^*(x) \rangle = \langle (x - 1)^{2^{s-1}} (f_j^{2^s}(x))^* \rangle = \langle (x - 1)^{2^{s-1}} (f_j^{2^s}(x)) \rangle = C_j,$$

which is an equivalent to $C_i$ from (9). Hence $C_i$ is an isodual code. The bound on the minimum distance for both cases is a consequence of the fact that these codes contain the odd-like duadic codes.

Example 3.5. For $n = 14$, $x^{14} - 1 = (x - 1)^2 (x^3 + x + 1)^2 (x^3 + x^2 + 1)^2$ over $\mathbb{F}_2$. Since $ord_7(2) = 3$ is odd, $x^3 + x + 1$ is the reciprocal polynomial of $x^3 + x^2 + 1$. Then $C_1 = \langle (x - 1)(x^3 + x + 1) \rangle$, and $C_2 = \langle (x - 1)(x^3 + x^2 + 1) \rangle$, are $[14, 7, 4]$ self-dual codes over $\mathbb{F}_2$, and these codes are optimal [15].

The following result presents a case where the cyclic isodual codes constructed from duadic codes have the same minimum distance.
Theorem 3.6. Let $n = 2m$ where $m$ is an odd integer such that $2 = \square \mod m$ and $D_i = \langle f_i(x) \rangle$, $1 \leq i \leq 2$, are the odd-like duadic codes over $\mathbb{F}_2$. Then the cyclic codes generated by $g_i(x) = (x - 1)f_i^2(x)$, $1 \leq i \leq 2$, are self-dual or isodual codes with minimum distance $d = d_{C_i}$ where $C_i = \langle (x - 1)f_i \rangle$.

Proof. The result regarding cyclic codes follows from Theorem 3.4 so we need only prove that the minimum distances are equal. From [25], we have that the binary code generated by $g_i(x)$ is equivalent to the Plotkin sum of $D_i$ and $C_i = \langle (x - 1)f_i \rangle$. From the McEliece bound [20, Theorem 4.513], we obtain that $d = \min\{2d_{D_i}, d_{C_i}\} = d_{C_i}$. \hfill $\square$

3.3. Repeated-root LCD-isodual negacyclic codes of length $2mp^r$ from duadic negacyclic codes. Negacyclic codes of odd length are equivalent to cyclic codes [11], so in this subsection we consider negacyclic codes of even length. Assume that $p$ is an odd prime number, and let $S_1$ and $S_2$ be unions of $p$-cyclotomic cosets modulo $4m$ such that $S_1 \cap S_2 = X$, $S_1 \cup S_2 \subseteq \mathbb{F}_4m$ and $\mu_4S_1 \mod 4m = S_{(i+1) \mod 2}$. A $p^s$-splitting is of type I if $X = \emptyset$ and of type II if $X = \{m, 3m\}$. A negacyclic code $C$ of length $2m$ over $\mathbb{F}_{p^s}$ is duadic if such a splitting exists and the defining set is one of the subsets $S_1$, $S_2$, $S_1 \cup X$ or $S_2 \cup X$. Similar to the cyclic code case we have two pairs of duadic codes, two odd-like duadic codes $D_i$ and two even-like duadic codes $C_i$, $i \in \{1, 2\}$. Further, (9) holds for the codes $D_i$ and $C_i$, $i \in \{1, 2\}$. For more details on negacyclic duadic codes, see [7].

Remark 3.7. If $q \equiv 3 \mod 4$, then every multiplier leaves the set $\{m, 3m\}$ and in this case the polynomial $x^2 + 1$ is irreducible over $\mathbb{F}_{p^s}$.

If $b$ gives a splitting of type I then we have $x^{2m} + 1 = g_1(x)g_2(x)$ for some $g_1(x)$, $g_2(x)$ in $\mathbb{F}_{p^s}$ such that $\mu_4(g_1(x)) = g_2(x)$ and $\mu_4(g_2(x)) = g_1(x)$. If $b$ gives a splitting of type II, then we have $x^{2m} + 1 = (x^2 + 1)g_1(x)g_2(x)$ for some $g_1(x)$, $g_2(x)$ in $\mathbb{F}_{p^s}$ such that $\mu_4(g_1(x)) = g_2(x)$ and $\mu_4(g_2(x)) = g_1(x)$.

Proposition 3.8. Assume there exist duadic negacyclic codes over $\mathbb{F}_{p^s}$ of type I generated by $g_1(x)$ and $g_2(x)$ such that $x^{2m} + 1 = g_1(x)g_2(x)$ or of type II generated by $g_1(x)$, $g_2(x)$, $(x^2 + 1)g_1(x)$ and $(x^2 + 1)g_2(x)$ such that $x^{2m} + 1 = (x^2 + 1)g_1(x)g_2(x)$. Then we have the following results.

(i) If the splitting is given by $\mu_1$, then $g_1^2(x) = g_2(x)$ and $g_2^2(x) = g_1(x)$.

(ii) If the splitting is not given by $\mu_1$, then $g_1^2(x) = g_1(x)$ and $g_2^2(x) = g_2(x)$.

(iii) If $d$ is the minimum distance of $D_i$, then

(a) $d \geq \sqrt{m}$, and

(b) if the splitting is given by $\mu_1$, then $d^2 - d + 1 \geq m$.

Proof. The proof for parts (i) and (ii) is similar to that of Proposition 3.2. The proof of part (iii) is (8) in [7, Theorem 11]. \hfill $\square$

Now, Proposition 3.8 and a proof similar to that for part i of Theorem 3.3 gives the following.

Theorem 3.9. Assume there exist duadic negacyclic codes of type I $D_i = \langle g_i(x) \rangle$, $1 \leq i \leq 2$, of length $2m$ and minimum distance $d_1$ such that $x^{2m} + 1 = g_1(x)g_2(x)$, or there exist duadic negacyclic codes of type II, $D_i = \langle g_i(x) \rangle$, with minimum distance $d_2$ and $C_i = \langle (x^2 + 1)g_i(x) \rangle$ $1 \leq i \leq 2$, of length $2m$, such that $x^{2m} + 1 = (x^2 + 1)g_1(x)g_2(x)$. Then we have $d_1 = d_2$. Further, among all possible $d_1$ and $d_2$, the one that is bigger is the minimum distance of a duadic code $D_i$.
1) $g_1(x)g_2(x)$. If the splitting modulo $4m$ is not given by $\mu_{-1}$, then for $i \in \{1, 2\}$ the negacyclic codes over $\mathbb{F}_{p^{r_i}}$ of type I generated by
\[ g_{i}^{p^{r_i}}(x), \text{ for } i \in \{1, 2\}, \]
are $[2mp^r, mp^r, d_1]$ LCD-isodual codes over $\mathbb{F}_{p^r}$. Further, the corresponding negacyclic codes of length $2mp^r$ over $\mathbb{F}_{p^r}$ of type II generated by
\[ g_{i}^{p^{r_i}}(x), (x^2 + 1)^{p^{r_i}}g_{i}^{p^{r_i}}(x), \text{ for } i \in \{1, 2\}, \]
are LCD codes over $\mathbb{F}_{p^r}$ with parameters $[2mp^r, (m + 1)p^r, \geq d_2]$ and $[2mp^r, (m - 1)p^r, \geq d_2]$, respectively.

The following result from [7] gives a necessary and sufficient condition for the existence of a splitting of $4m$ given by $\mu_{2m+1}$.

**Lemma 3.10.** If $m$ is an odd prime power such that $(m, p) = 1$ and $p \equiv 3 \mod 4$, then $\mu_{2m+1}$ gives a splitting of $4m$ of type II if and only if $\text{ord}_{4m}(p)$ is even, in which case
\[ x^{2m} + 1 = (x^2 + 1)g(x)g(-x). \]

This result is used to prove the following proposition.

**Proposition 3.11.** If $m$ is an odd prime power such that $(m, p) = 1$, $p \equiv 3 \mod 4$ and $\text{ord}_{4m}(p)$ is even, then there exist LCD negacyclic codes of length $2mp^r$ over $\mathbb{F}_{p^r}$.

**Proof.** If $m$ is an odd prime power such that $(m, p) = 1$, $p \equiv 3 \mod 4$, and $\text{ord}_{4m}(p)$ is even, then by Lemma 3.10, there exists a polynomial $g(x) \in \mathbb{F}_{p^r}$ such that $x^{2m} + 1 = (x^2 + 1)g(x)g(-x)$. Since the splitting is not given by $\mu_{-1}$, by Proposition 3.8 the polynomials $g(x)$ and $g(-x)$ are self-reciprocal. Then from Lemma 2.2, the negacyclic codes generated by $g(x)^{p^r}, g(-x)^{p^r}, (x^2 + 1)^{p^r}g(x)^{p^r}$ and $(x^2 + 1)^{p^r}g(-x)^{p^r}$ are LCD codes of length $2mp^r$ over $\mathbb{F}_{p^r}$. \hfill $\square$

4. **Repeated-root constacyclic codes of length $2^am p^r$ over $\mathbb{F}_{p^r}$**

In this section, we give the structure of repeated-root constacyclic codes over $\mathbb{F}_q$, $q = p^s$, of length $2^am p^r$, $a \geq 1$, and provide conditions on when constacyclic codes are equivalent to cyclic codes. For this, we require the following lemma.

**Lemma 4.1.** [4, Lemma 3.2] Let $q$ be an odd prime power, $a \geq 1$ an integer and $\alpha$ a primitive $2^a$th root of unity in $\mathbb{F}_q^*$. Then the following results hold.

(i) There exist a primitive $2^a$th root of unity in $\mathbb{F}_q^*$ if and only if $q \equiv 1 \mod 2^a$.

(ii) $\alpha^{2^i}$ is a primitive $2^{a-i}$th root of unity in $\mathbb{F}_q^*$ for all $i \leq a$.

(iii) $\alpha^{2^m}$ is a primitive $2^a$th root of unity in $\mathbb{F}_q^*$ for all odd integers $m$.

(iv) $\prod_{k=1}^{2^a} \alpha^k = -1$.

**Proposition 4.2.** Let $q$ be a power of an odd prime $p$ and $n = 2^am p^r$ a positive integer with $m$ an odd integer and $(m, p) = 1$, $a \geq 1$. Then if $\mathbb{F}_q^*$ contains a primitive $2^a$th root of unity $\alpha$ and the $f_i(x)$, $0 \leq i \leq l$, are the monic irreducible factors of $x^m - 1$ in $\mathbb{F}_q[x]$, we have that
\[ x^{2^am} - 1 = \prod_{k=1}^{2^a} \left( \prod_{i=0}^{l} f_i(\alpha^{-k}x) \right). \]
Further, all cyclic codes of length \( n = 2^a mp^r \) are generated by \( \prod_{k=1}^{2^a} (\prod_{i=0}^{l} f_i^j (\alpha^{-k} x)) \) where \( 0 \leq j_i \leq p^r \).

**Proof.** The proof of (10) is omitted since it is the same as for [4, Proposition 3.3] with \( (x-1) \) replaced by \( f_0(x) \). The proof of the second statement follows from the fact that a cyclic code of length \( n = 2^a mp^r \) is generated by a factor of the polynomial \( (x^{2^a mp^r} - 1) = (x^{2^m - 1})^{p^r} \), and the result follows from (10). \( \Box \)

We now give the main result of this section.

**Theorem 4.3.** Let \( q \) be a power of an odd prime \( p \) and \( m \) an odd integer such that \( (m,p) = 1 \). Let \( \lambda \) and \( \delta \) be elements of the multiplicative group \( \mathbb{F}_q^* \) such that \( \delta^m = \lambda \). If \( \delta = \beta^{2^a} \) in \( \mathbb{F}_q^* \), then the following hold.

(i) The \( \lambda \)-constacyclic codes of length \( 2^a mp^r \) over \( \mathbb{F}_q \) are equivalent to cyclic codes of length \( 2^a mp^r \) over \( \mathbb{F}_q \).

(ii) If \( q \equiv 1 \mod 2^{a+1} \), then \( -\lambda \)-constacyclic codes of length \( 2^a mp^r \) over \( \mathbb{F}_q \) are equivalent to cyclic codes of length \( 2^a mp^r \) over \( \mathbb{F}_q \).

**Proof.** For part (i), let \( \lambda \in \mathbb{F}_q^* \) such that there exists \( \delta \in \mathbb{F}_q^* \) with \( \delta^m = \lambda \) and \( \delta = \beta^{2^a} \) in \( \mathbb{F}_q \). Then \( \lambda = \beta^{2^a m} \) and by Lemma 4.1 there exist \( \beta_0 \in \mathbb{F}_q^* \) such that \( \beta = \beta_0^{2^a m} \). Then \( \lambda = \beta_0^{2^a mp^r} \), and then by [3, Proposition 3.2], \( \lambda \)-constacyclic codes of length \( 2^a mp^r \) over \( \mathbb{F}_q \) are equivalent to cyclic codes over \( \mathbb{F}_q \). For part (ii), since \( q \equiv 1 \mod 2^{a+1} \), from Lemma 4.1 there exists a primitive \( 2^{a+1} \)-root of unity \( \alpha \in \mathbb{F}_q^* \). Thus \( \alpha^{2^a} = -1 \), and \( -\lambda = (-1)^{mp^r} \lambda = (\alpha^{2^a})^{mp^r} \beta_0^{2^a mp^r} = (\alpha \beta_0)^{2^a mp^r} \). Then by [3, Proposition 3.2], \( -\lambda \)-constacyclic codes of length \( 2^a mp^r \) over \( \mathbb{F}_q \) are equivalent to cyclic codes over \( \mathbb{F}_q \). \( \Box \)

**Corollary 4.4.** Let \( \lambda = \beta_0^{2^a mp^r} \), \( \alpha \) a primitive \( 2^a \)th root of unity in \( \mathbb{F}_q^* \), and \( C \) a \( \lambda \)-constacyclic code of length \( 2^a mp^r \). We then have that

\[
C = \left\langle \prod_{k=1}^{2^a} \left( \prod_{i=0}^{l} f_i^j (\beta_0^{-1} \alpha^{-k} x) \right) \rightangle,
\]

where \( 0 \leq j_i \leq p^r \).

**Proof.** By Lemma 4.1, if \( q \equiv 1 \mod 2^a \), then there exists a primitive \( 2^a \)th root of unity \( \alpha \) in \( \mathbb{F}_q^* \). Thus by Proposition 4.2

\[
(x^{2^a mp^r} - 1) = (x^{2^m - 1})^{p^r} = \prod_{k=1}^{2^a} \left( \prod_{i=0}^{l} f_i^j (\alpha^{-k} x) \right),
\]

so then

\[
((\beta_0^{-1} x)^{2^a mp^r} - 1) = ((\beta_0^{-1} x)^{2^m - 1})^{p^r} = \prod_{k=1}^{2^a} \left( \prod_{i=0}^{l} f_i^j (\beta_0^{-1} \alpha^{-k} x) \right),
\]

and

\[
(x^{2^a mp^r} - \lambda) = \lambda((\beta_0^{-1} x)^{2^m - 1})^{p^r} = \prod_{k=1}^{2^a} \left( \prod_{i=0}^{l} f_i^j (\beta_0^{-1} \alpha^{-k} x) \right).
\]

Since a \( \lambda \)-constacyclic code of length \( 2^a mp^r \) is generated by a divisor of \( (x^{2^a mp^r} - \lambda) \), the result follows. \( \Box \)
4.1. Repeated-root self-dual negacyclic codes of length $2^a mp^r$ over $\mathbb{F}_{p^r}$. In this subsection, some results of [18] concerning conditions on the existence of self-dual codes are generalized. For this, we first need to give the structure of negacyclic codes over $\mathbb{F}_{p^r}$ of length $2^a mp^r$, $a \geq 1$. We begin with the following result.

Lemma 4.5. Let $q = p^s$ be an odd prime power such that $q \equiv 1 \mod 2^{a+1}$. Then there is a ring isomorphism between the ring $\mathbb{F}_q[x]/(x^{2^a mp^r} - 1)$ and the ring $\mathbb{F}_q[x]/(x^{2^a mp^r} + 1)$.

Proof. If $q \equiv 1 \mod 2^{a+1}$, then by Lemma 4.1 there exists a primitive $2^{a+1}$th root of unity $\alpha$ in $\mathbb{F}_q$. Therefore, $-1 = (-1)^{mp^r} = (\alpha^{2^a})^{mp^r}$ and so by [3, Proposition 3.2] negacyclic codes of length $2^a mp^r$ over $\mathbb{F}_q$ are equivalent to cyclic codes of length $2^a mp^r$ over $\mathbb{F}_q$.

Proposition 4.6. Let $q = p^s$ be an odd prime power such that $q \equiv 1 \mod 2^{a+1}$ and $n = 2^a mp^r$ with $m$ an odd integer such that $(m, p) = 1$. Then a negacyclic code of length $n$ over $\mathbb{F}_{p^r}$ with $q \equiv 1 \mod 2^{a+1}$ and $n = 2^a mp^r$ is a principal ideal of $\mathbb{F}_{p^r}[x]/(x^n + 1)$ generated by a polynomial of the form $\prod_{k=1}^{2^a} \prod_{i=0}^{r-1} f_i^r(\alpha^{-2^k i} x)$ where $0 \leq j_i \leq p^r$ and the $f_i(x)$ are monic irreducible factors of $x^m - 1$.

Proof. It suffices to find the factors of $x^{2^a mp^r} + 1$. Since $q \equiv 1 \mod 2^{a+1}$, from Lemma 4.1 there exists an $\alpha \in \mathbb{F}_q$ which is a primitive $2^{a+1}$th root of unity. Thus, $x^{2^a mp^r} + 1$ can be decomposed as $(x^{2^a mp^r} + 1)\prod_{k=1}^{2^a} \prod_{i=0}^{r-1} f_i^r(\alpha^{-2^k i} x) = (x^{2^a mp^r} + 1)\prod_{k=1}^{2^a} \prod_{i=0}^{r-1} f_i^r(\alpha^{-2^k i} x)$. The result then follows from the isomorphisms given in Lemma 4.5.

Theorem 4.7. Let $q = p^s$ be an odd prime power such that $q \equiv 1 \mod 2^{a+1}$, $n = 2^a mp^r$ an integer with $(m, p) = 1$, and $a \geq 1$. Then there exists a negacyclic self-dual code of length $2^a mp^r$ over $\mathbb{F}_{p^r}$ if and only if $ord_m(q)$ is odd.

Proof. Under the hypothesis on $q$ and $m$, we have from Proposition 4.6 that $x^{2^a mp^r} + 1 = \prod_{k=1}^{2^a} \prod_{i=0}^{r-1} f_i^r(\alpha^{-2^k i} x)$ where the $f_i(x)$ are the monic irreducible factors of $x^m - 1$ in $\mathbb{F}_{p^r}$. By [18, Lemma 3.6], $ord_m(q^s)$ is odd if and only if there is no cyclotomic class such that $C_m(i) = C_m(-i)$. From [18, Lemma 3.6], this is equivalent to saying that there are no nontrivial irreducible factors of $x^m - 1$ such that $f_i(x) = f_i^r(x)$. Then from Proposition 4.6, we have that $f_i(x) \neq f_i^r(x)$ for all $i \neq 0$ ($f_0(x) = (x - 1)$) is true if and only if $f_i(\alpha^k x) \neq f_i(\alpha^k x)^r$ is true for all $1 \leq k \leq 2^{a+1}$. Then by [19, Theorem 2.2], self-dual negacyclic codes exist.

4.2. Repeated-root isodual cyclic and negacyclic codes of length $2^a mp^r$ over $\mathbb{F}_{p^r}$. In this section we give constructions of isodual cyclic and negacyclic codes of length $2^a mp^r$ over $\mathbb{F}_{p^r}$.

Theorem 4.8. Let $q$ be a power of an odd prime $p$, $m$ an odd integer with $(m, q) = 1$, and $f_1(x), f_2(x)$ polynomials in $\mathbb{F}_q[x]$ such that

$$x^m - 1 = f_1(x)f_2(x).$$

Then we have the following results.

(i) If $q \equiv 1 \mod 2^{a}$ with $a \geq 1$ an integer, then the cyclic codes of length $2^a mp^r$ generated by

$$\prod_{k=1}^{2^a} f_i^r(\alpha^{-2^k i} x) \prod_{k=0}^{2^a-1} f_j^r(\alpha^{-2^k-1} x) \quad i, j \in \{1, 2\}, i \neq j,$$
Corollary 4.9. With the same assumptions as in Theorem 4.8, the cyclic codes generated by
\[ \prod_{k=0}^{2^{n-1}-1} f_i^p(\beta^{-4k-1}x) \prod_{k=0}^{2^{n-1}-1} f_j^p(\beta^{-4k-3}x) \quad i, j \in \{1, 2\}, i \neq j, \]
are isodual codes over \( \mathbb{F}_q \) where \( \beta \in \mathbb{F}_q^* \) is a primitive \( 2^n+1 \)th root of unity.

(ii) If \( q \equiv 1 \mod 2^{a+1} \) with \( a \geq 1 \) an integer, then the negacyclic codes of length \( 2^n mp^r \) generated by
\[ \prod_{k=0}^{2^{n-1}-1} f_i^p(\beta^{-4k-1}x) \prod_{k=0}^{2^{n-1}-1} f_j^p(\beta^{-4k-3}x) \quad i, j \in \{1, 2\}, i \neq j, \]
are isodual codes over \( \mathbb{F}_q \) where \( \beta \in \mathbb{F}_q^* \) is a primitive \( 2^n+1 \)th root of unity.

Proof. The proof follows from Proposition 2.6 and an argument similar to that for [4, Theorem 4.2] with \( x+1 \) replaced by \( f_1(x) \).

The following is a straightforward consequence of Theorem 4.8 and Lemma 2.2.

Corollary 4.9. With the same assumptions as in Theorem 4.8, the cyclic codes generated by
\[ \prod_{k=1}^{2^{n-1}-1} f_i^p(\alpha^{-2k}x) \prod_{k=1}^{2^{n-1}-1} f_j^p(\alpha^{-2k}x) \quad i, j \in \{1, 2\}, i \neq j, \]
and the negacyclic codes generated by
\[ \prod_{k=0}^{2^{n-1}-1} f_i^p(\beta^{-4k-1}x) \prod_{k=0}^{2^{n-1}-1} f_j^p(\beta^{-4k-3}x) \quad i, j \in \{1, 2\}, i \neq j, \]
are isodual codes of length \( 2^n mp^r \) over \( \mathbb{F}_q \).

Example 4.10. Since \( q = 17 \equiv 1 \mod 2^{3+1} \), from Lemma 4.1 there exists \( \alpha \in \mathbb{F}_{17}^* \) such that \( \alpha^{16} = 1 \), e.g. \( \alpha = 3 \), and \( m = 11 \) so that
\[ x^{11} - 1 = (x-1)(x^5 + 2x^4 + 4x^3 + x^2 + x + 4)(x^5 + 4x^4 + 4x^3 + 4x^2 + 3x + 4) = f_1(x)f_2(x), \]
with
\[ f_1(x) = (x-1)(x^5 + 2x^4 + 4x^3 + x^2 + x + 4), \]
and
\[ f_2(x) = (x^5 + 4x^4 + 4x^3 + 4x^2 + 3x + 4). \]
Then the negacyclic codes of length \( 2^3 \times 11 \times 17^r \) generated by
\[ \prod_{k=0}^{3} f_i^{17}(3^{4k-1}x) \prod_{k=0}^{3} f_j^{17}(3^{4k-3}x) \quad i, j \in \{1, 2\}, i \neq j, \]
are isodual codes over \( \mathbb{F}_{17} \).

In the following we give another construction of isodual cyclic and negacyclic codes of length \( 2^n mp^r \) over \( \mathbb{F}_q \).

Theorem 4.11. Let \( q \) be a power of an odd prime \( p \), \( m \) an odd integer with \( m \) \( \equiv 1 \) and \( f_1(x) \), \( f_2(x) \) polynomials in \( \mathbb{F}_q[x] \) such that \( x^m - 1 = f_1(x)f_2(x)f_3^*(x) \) and \( f_1(x) = f_1^*(x) \). Then we have the following.
(i) If \( q \equiv 1 \mod 2^a \) with \( a \geq 1 \) an integer, then the cyclic codes of length \( 2^n mp^r \) generated by
\[ \prod_{k=1}^{2^{n-1}} f_i^p(\alpha^{-2k}x) \prod_{k=1}^{2^n} f_j^p(\alpha^{-k}x), \]
and
\[ 2^{n-1} \prod_{k=1}^{2^n} f_1^{p^r}(\alpha^{-2k}x) \prod_{k=1}^{2^n} f_2^{p^r}(\alpha^{-k}x), \]
are isodual over \( \mathbb{F}_q \) where \( \alpha \in \mathbb{F}_q^* \) is a primitive 2\( a \)th root of unity.

(ii) If \( q \equiv 1 \mod 2^{a+1} \) with \( a \geq 1 \) an integer, then the negacyclic codes of length \( 2^n m p^r \) generated by
\[ 2^{n-1} \prod_{k=0}^{2^n-1} f_1^{p^r}(\beta^{-4k-1}x) \prod_{k=0}^{2^n-1} f_2^{p^r}(\beta^{-2k-1}x), \]
and
\[ 2^{n-1} \prod_{k=0}^{2^n-1} f_1^{p^r}(\beta^{-4k-1}x) \prod_{k=0}^{2^n-1} f_2^{p^r}(\beta^{-2k-1}x), \]
are isodual codes over \( \mathbb{F}_q \) where \( \beta \in \mathbb{F}_q^* \) is a primitive 2\( a+1 \)th root of unity.

Proof.

(i) By Lemma 4.1, if \( q \equiv 1 \mod 2^n \) then there exists a primitive 2\( a \)th root of unity \( \alpha \in \mathbb{F}_q^* \) such that \( \alpha^{2^n} = 1 \). Suppose \( x^{2^n} - 1 = f_1(x)f_2(x)f_3(x) \) so that
\[ (x^{2^n} - 1)^{p^r} = \prod_{k=1}^{2^n} f_1^{p^r}(\alpha^{-k}x)f_2^{p^r}(\alpha^{-k}x)f_3^{p^r}(\alpha^{-k}x). \]
We have \( (x^{2^n} - 1)^{p^r} = (x^{2^n-1} - 1)^{p^r}(x^{2^n+1} + 1)^{p^r} \), which gives that
\[ (x^{2^n} - 1)^{p^r} = \prod_{k=1}^{2^n} f_1^{p^r}(\alpha^{-k}x)f_2^{p^r}(\alpha^{-k}x)f_3^{p^r}(\alpha^{-k}x) \]
\[ = \prod_{k=1}^{2^n} f_1^{p^r}(\alpha^{-2k}x)f_2^{p^r}(\alpha^{-2k}x)f_3^{p^r}(\alpha^{-2k}x) \]
\[ \times \prod_{k=0}^{2^n-1} f_1^{p^r}(\alpha^{-2k-1}x)f_2^{p^r}(\alpha^{-2k-1}x)f_3^{p^r}(\alpha^{-2k-1}x). \]
If
\[ g(x) = \prod_{k=1}^{2^n-1} f_1^{p^r}(\alpha^{-2k}x) \prod_{k=1}^{2^n} f_2^{p^r}(\alpha^{-k}x), \]
then we have
\[ h(x) = - \prod_{k=0}^{2^n-1} f_1^{p^r}(\alpha^{-2k-1}x) \prod_{k=1}^{2^n} f_2^{p^r}(\alpha^{-k}x), \]
and \( h^*(x) = g(\alpha^{-1}x) \). By Proposition 2.6(i), the cyclic code \( C \) generated by \( g(x) \) is equivalent to the cyclic code generated by \( g(\alpha^{-1}x) \). By Proposition 2.6(ii), the cyclic code generated by \( g(\alpha^{-1}x) \) is equivalent to the cyclic code generated by \( g(\alpha^{-1}x) = (h(x))^* \). As the latter code is \( C^\perp \), \( C \) is isodual,
so the cyclic code generated by \( g(x) \) is isodual. The same result is obtained for the code generated by

\[
g(x) = \prod_{k=1}^{2^a-1} f_1^p(\alpha^{-2k}x) \prod_{k=1}^{2^a} f_2^p(\alpha^{-k}x).
\]

(ii) The proof is the same as that for cyclic codes. \( \square \)

**Example 4.12.** Since \( q = 17 \equiv 1 \mod 4 \), from Lemma 4.1 there exists \( \alpha \in \mathbb{F}_{17} \) such that \( \alpha^{16} = \alpha^{2^3+3} = 1 \), e.g. \( \alpha = 3 \), and \( m = 11 \). Hence

\[
x^{11} - 1 = (x - 1)(x^5 + 2x^4 + 4x^3 + x^2 + x + 4)(x^5 + 4x^4 + 4x^3 + 4x^2 + 3x + 4). = f_1(x)f_2(x)f_3(x),
\]

with

\[
f_1(x) = (x - 1),
\]

\[
f_2(x) = (x^5 + 2x^4 + 4x^3 + x^2 + x + 4),
\]

and

\[
f_3(x) = (x^5 + 4x^4 + 4x^3 + 4x^2 + 3x + 4).
\]

Then the negacyclic codes of length \( 2^{3} \times 11 \times 17^r \), \( r \geq 1 \) generated by

\[
\prod_{k=0}^{3} f_1^{17^r}(3^{4k-1}x) \prod_{k=0}^{7} f_2^{17^r}(3^{2k-1}x),
\]

and

\[
\prod_{k=0}^{3} f_1^{17^r}(3^{4k-1}x) \prod_{k=0}^{7} f_2^{17^r}(3^{2k-1}x),
\]

are isodual negacyclic codes over \( \mathbb{F}_{17} \).

**Corollary 4.13.** With the same assumptions as in Theorem 4.8, the negacyclic codes generated by

\[
\prod_{k=0}^{2^{a-1}-1} f_1^p(\alpha^{-4k-3}x) \prod_{k=0}^{2^{a-1}-1} f_2^p(\alpha^{-4k-3}x),
\]

and

\[
\prod_{k=0}^{2^{a-1}-1} f_1^p(\alpha^{-4k-1}x) \prod_{k=0}^{2^{a-1}-1} f_2^p(\alpha^{-4k-1}x),
\]

are isodual codes of length \( 2^a mp^r \) over \( \mathbb{F}_q \).

**Corollary 4.14.** Let \( q \) be an odd prime power such that \( m \) is an odd integer and \( f_1(x), f_2(x) \) be polynomials in \( \mathbb{F}_q[x] \) such that \( x^m - 1 = f_1(x)f_2(x)f_3(x) \) with \( f_3(x) = f_1(x) \). Then the negacyclic codes of length \( 2^a mp^s \) generated by

\[
\prod_{k=0}^{2^{a-1}-1} f_1^p(\alpha^{-4k-1}x) \prod_{k=0}^{2^{a-1}-1} f_2^p(\alpha^{-2k-1}x),
\]

and

\[
\prod_{k=0}^{2^{a-1}-1} f_1^p(\alpha^{-4k-3}x) \prod_{k=0}^{2^{a-1}-1} f_2^p(\alpha^{-2k-1}x),
\]

are isodual codes of length \( 2^a mp^r \) over \( \mathbb{F}_q \).

**Proof.** The results follow from Theorem 4.11. \( \square \)
5. Conclusion

This paper considered the structure of repeated-root constacyclic codes over finite fields. Necessary and sufficient conditions were given for the existence of LCD constacyclic and self-dual negacyclic codes. Further, new constructions of isodual, LCD and LCD-isodual constacyclic codes over finite fields were presented. It is well known [8] that LCD codes can be used to counter passive and active side-channel analysis attacks on embedded cryptosystems. Therefore, it would be interesting to investigate the use of LCD-isodual codes against these and other attacks.

Acknowledgments

The authors are greatly indebted to the editor and reviewers for their remarks and advice which allowed us to considerably improve the paper.

References

[1] C. Bachoc, T. A. Gulliver and M. Harada, Isodual codes over $\mathbb{Z}_{2^k}$ and isodual lattices, J. Algebra. Combin., 12 (2000), 223–240.
[2] G. K. Bakshi and M. Raka, A class of constacyclic codes over a finite field, Finite Fields Appl., 18 (2012), 362–377.
[3] A. Batoul, K. Guenda and T. A. Gulliver, Some constacyclic codes over finite chain rings, Adv. Math. Commun., 10 (2016), 683–694.
[4] A. Batoul, K. Guenda and T. A. Gulliver, Repeated-root isodual cyclic codes over finite fields, in Codes, Cryptology and Information Security (eds. S. El Hajji et al.), Lecture Notes in Computer Science, 9084, Springer, Cham, (2015), 119–132.
[5] A. Batoul, K. Guenda, T. A. Gulliver and N. Aydin, On isodual cyclic codes over finite chain rings, in Codes, Cryptology and Information Security (eds. S. El Hajji et al.), Lecture Notes in Computer Science, 10194, Springer, Cham, (2017), 176–194.
[6] S. D. Berman, Semisimple cyclic and abelian codes II, Cybernetics and Systems Analysis, 3 (1967), 17–23.
[7] T. Blackford, Negacyclic duadic codes, Finite Fields Appl., 14 (2008), 930–943.
[8] C. Carlet and S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, Adv. Math. Commun., 10 (2016), 131–150.
[9] C. Carlet, S. Mesnager, C. Tang, Y. Qi and R. Pellikaan, Linear codes over $\mathbb{F}_q$ equivalent to LCD codes for $q > 3$, IEEE Trans. Inform. Theory, 64 (2018), 3010–3017.
[10] B. Chen, Y. Fan, L. Lin and H. Liu, Constacyclic codes over finite fields, Finite Fields Appl., 18 (2012), 1217–1231.
[11] H. Q. Dinh and S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory, 50 (2004), 1728–1744.
[12] H. Q. Dinh, Structure of repeated-root constacyclic codes of length $3p^s$ and their duals, Discrete Math., 313 (2013), 983–991.
[13] H. Q. Dinh, Repeated-root cyclic and negacyclic codes of length $6p^s$ and their duals, Contemporary Mathematics, 609 (2014), 69–87.
[14] G. Falkner, B. Kowol, W. Heise and E. Zehendner, On the existence of cyclic optimal codes, Atti Sem. Mat. Fis. Univ. Modena, 28 (1979), 326–341.
[15] M. Grassl, Code tables: Bounds on the parameters of various types of codes, Available from: http://www.codetables.de.
[16] K. Guenda, Dimension and minimum distance of a class of BCH codes, Annales Des Sciences Mathématiques du Québec, 32 (2008), 57–62. Available from: http://www.labmath.uqam.ca/-annales/volumes/32-1/PDF/057-062.pdf.
[17] K. Guenda, New MDS self-dual codes over finite fields, Des., Codes and Crypt., 62 (2012), 31–42.
[18] K. Guenda and T. A. Gulliver, Self-dual repeated-root cyclic and negacyclic codes over finite fields, Proc. IEEE Int. Symp. Inform. Theory, (2012), 2904–2908.
[19] K. Guenda and T. A. Gulliver, Repeated-root constacyclic codes of length $mp^s$ over $\mathbb{F}_{p^r}+u\mathbb{F}_{p^r}+u^{-1}\mathbb{F}_{p^r}$, Journal of Algebra and Its Applications, 14 (2015), 1450081, 1–12.
[20] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, New York, USA, 2003.

[21] S. Li, C. Li, C. Ding and H. Liu, Two families of LCD BCH codes, *IEEE Trans. Inform. Theory*, 63 (2017), 5699–5717.

[22] (MR3724869) X. Liu, Y. Fan and H. Liu, Galois LCD codes over finite fields, *Finite Fields and Applications*, 49 (2018), 227–242.

[23] J. L. Massey, Linear codes with complementary duals, *Discr. Math.*, 106/107 (1992), 337–342.

[24] B. Pang, S. Zhu and J. Li, On LCD repeated-root cyclic codes over finite fields, *J. Appl. Math. Comput.*, 56 (2018), 625–635.

[25] J. H. Van Lint, Repeated-root cyclic codes, *IEEE Trans. Inform. Theory*, 37 (1991), 343–345.

[26] X. Yang and J. L. Massey, The condition for a cyclic code to have a complementary dual, *Discr. Math.*, 126 (1994), 391–393.

Received April 2018; revised August 2018.

E-mail address: zahraben4@gmail.com
E-mail address: ken.guenda@gmail.com
E-mail address: aic.batoul@gmail.com
E-mail address: agullive@ece.uvic.ca