J. Algebra Comb. Discrete Appl.
7(1) • 21–33

Received: 30 June 2019
Accepted: 12 October 2019

Journal of Algebra Combinatorics Discrete Structures and Applications

A class of constacyclic codes containing formally self-dual and isodual codes

Research Article

Manjit Singh

Abstract: In this paper, we investigate a class of constacyclic codes which contains isodual codes and formally self-dual codes. Further, we introduce a recursive approach to obtain the explicit factorization of $x^{2^m\ell^n} - \mu_k \in \mathbb{F}_q[x]$, where n, m are positive integers and μ_k is an element of order ℓ^k in $\mathbb{F}_q$. Moreover, we give many examples of interesting isodual and formally self-dual constacyclic codes.

2010 MSC: 12E05, 94B05, 11T71

Keywords: Constacyclic codes, Weight distributions, Isodual codes, Formally self-dual codes

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and n be a positive integer. An $[n, k]_q$-linear code C is a k-dimensional subspace of $\mathbb{F}_q^n$. Usually, elements of C are referred to as codewords. The Hamming weight of a vector $c \in \mathbb{F}_q^n$, denoted by $wt(c)$, is the number of nonzero coordinate entries in c. The Hamming distance between two vectors c and c' in $\mathbb{F}_q^n$ is defined as $d(c, c') = wt(c - c')$. The minimum distance $d_H(C)$ of a code C is the smallest distance between distinct codewords of the code C, i.e. $d_H(C) = \min\{d(c, c') : c, c' \in C\}$. For a linear code C, the minimum distance $d = d_H(C)$ is the same as the minimum weight of nonzero codewords of C.

Let A_i denote the number of codewords with Hamming weight i in C, where $0 \le i \le n$. The sequence $(A_0, A_1, \ldots, A_n)$ is called the weight distribution of the code C. A linear code possessing minimum weight d has no nonzero codeword of weight less than d except zero codeword, that is, $A_i = 0$ for all $1 \le i \le d-1$ and $A_0 = 1$. The weight distribution is an important research object in coding theory. However, the problem of determining the weight distribution of linear codes is, in general, notoriously difficult. There are extremely few linear codes for which the weight distribution is known (see for example [7], [11], [17], [18] and the references therein).

Manjit Singh; Department of Mathematics, Deenbandhu Chhotu Ram University of Science and Technology, Murthal-131039, Sonepat, India (email: manjitsingh.math@gmail.com).

http://dx.doi.org/10.13069/jacodesmath.645018

ISSN 2148-838X

For an $[n,k]_q$-linear code C, the dual code $C^\perp$ is also a linear code of length n and dimension $n-k$ over $\mathbb{F}_q$. The code C is self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$. The length n of a self-dual code is even and dimension is $n/2$. Further, if q is odd, then there is no self-dual cyclic code of length 2^n over $\mathbb{F}_q$ and, if q is even, then there is a unique self-dual cyclic code of dimension 2^{n-1} of length 2^n (see [16, Section 5]). Blackford [4] obtained the necessary and sufficient conditions for the existence of simple-root self-dual negacyclic codes. Bakshi and Raka [3] obtained all the self-dual negacyclic codes of length 2^n over $\mathbb{F}_{p^m}$, where p is an odd prime and integer $m \geq 1$. Dinh [8, Corollary 3.3] characterized all repeated-root self-dual negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$. Remarkably note that constacyclic codes, except negacyclic codes or binary cyclic codes, do not include an important class of codes, that is, self-dual codes, however these codes contain formally self-dual and isodual codes.

A linear code C is called isodual if C is equivalent to its dual code $C^\perp$. A code C is called formally self-dual (f.s.d.) code if C and $C^\perp$ have the same weight distribution. Automatically, self-dual codes are isodual codes and isodual codes are formally self-dual codes. Huffman and Pless [9] studied formally self-dual binary codes, however little work is known about formally self-dual codes over non-binary fields. These codes are important due to their applications in lattices [2], designs [10], code based cryptography, particularly in determining a minimal access set [14] and coding theory [5].

In this paper, motivated by the numerous practical applications of isodual codes and formally self-dual codes, we investigate a class of isodual and formally self-dual constacyclic codes which are permutation and monomially equivalent to each other. Further, we study the form of codewords, generator polynomials and the weight distribution of a class of μ_k- irreducible constacyclic codes of length $2\ell^n$ over $\mathbb{F}_q$, where ℓ is odd prime such that $\ell^k|(q-1)$ and μ_k is an element of order ℓ^k in $\mathbb{F}_q^* \setminus \{1,-1\}$. This paper also presents a recursive factorization of $x^{2^m\ell^n} - \mu_k \in \mathbb{F}_q[x]$, where integer $m \geq 1$.

The structure of the paper is as follows: Some background of constacyclic codes, the necessary notation and some known results are to be used presented in Section 2. In Section 3, the explicit factorization of $x^{2\ell^n} - \mu_k$ over $\mathbb{F}_q$ is obtained. Further, we introduce a recursive factorization of $x^{2^m\ell^n} - \mu_k$. The form of codewords of all irreducible μ_k-constacyclic codes of length ℓ^n and $2\ell^n$ are also obtained. Moreover, the weight distributions of these codes are determined by simply observing the weight of each message word. In Section 4, we construct a family of isodual and hence formally self-dual codes of length $2\ell^n$ over $\mathbb{F}_q$ in a very special case. In the end of this section, we illustrate a class of isodual codes and formally self-dual codes by means of some examples.

2. Preliminaries

Throughout this paper $\mathbb{F}_q$ denotes a finite field with q elements, where q is a power of a prime. For a fixed $\mu \in \mathbb{F}_q^*$, where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, a linear code C of length n over $\mathbb{F}_q$ is called a μ-constacyclic code if

$$(c_1, c_2, \ldots, c_{n-1}, \mu c_0) \in C \text{ for each } (c_0, c_1, c_2, \ldots, c_{n-1}) \in C.$$

The code C is called cyclic if $\mu = 1$ and negacyclic if $\mu = -1$. If $\gcd(n,q) = 1$, a μ-constacyclic code of length n is called simple-root code; otherwise it is called repeated-root code. Identifying the vector $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ with the polynomial $a_0x^{n-1} + a_1x^{n-2} + \cdots + a_{n-1} \in \mathbb{F}_q[x]$, a simple-root μ-constacyclic code C can be represented as an ideal of the quotient ring $\mathbb{F}_q[x]/\langle x^n - \mu\rangle$. Each ideal in $\mathbb{F}_q[x]/\langle x^n - \mu\rangle$ is of the form $\langle g(x)\rangle$, where $g(x)$ is a monic divisor of $x^n - \mu$ in $\mathbb{F}_q[x]$. The polynomial $g(x)$ is known as the generator polynomial of the code C. A μ-constacyclic code C is called irreducible or minimal over $\mathbb{F}_q$ if $h(x) = (x^n - \mu)/g(x)$ is an irreducible polynomial over $\mathbb{F}_q$, where the polynomial $h(x)$ is known as the parity check polynomial of the code C. The structure of constacyclic codes have been extensively studied and can be found in [1, 3, 5–8, 11].

For any two vectors $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ in $\mathbb{F}_q^n$, the (Euclidean) inner product or dot product of $\mathbf{a}$ and $\mathbf{b}$ is defined as follows:

$$\mathbf{a}\cdot\mathbf{b}=\sum_{i=1}^{n}a_ib_i\in\mathbb{F}_q,\text{ where }a_i,b_i\in\mathbb{F}_q\text{ for each }i=1,2,\ldots,n.$$

The two vectors $\mathbf{a}$ and $\mathbf{b}$ are said to be orthogonal if $\mathbf{a}\cdot\mathbf{b}=0$. The dual code of C, denoted by $C^{\perp}$, is defined as

$$C^{\perp}=\{\mathbf{b}\in\mathbb{F}_q^n:\mathbf{a}\cdot\mathbf{b}=0\text{ for all }\mathbf{a}\in C\}.$$

For any polynomial $f(x)=\sum_{i=0}^{r}a_ix^{r-i}$, where $a_0\neq 0$, over $\mathbb{F}_q$, the reciprocal polynomial of $f(x)$, denoted by $f^*(x)$, is given by:

$$f^*(x)=x^rf(x^{-1})=\sum_{i=0}^{r}a_ix^i.$$

For a μ-constacyclic $[n,k]_q$-code C with parity check polynomial $h(x)$ of degree k over $\mathbb{F}_q$, the generator polynomial of $C^{\perp}$ is given by $h^*(x)$ over $\mathbb{F}_q$. Note that $h^*(x)$ divides $x^n-\mu^{-1}$ over $\mathbb{F}_q$ if and only if $h(x)$ divides $x^n-\mu$ over $\mathbb{F}_q$.

Lemma 2.1. *[8, Proposition 2.2] The dual of μ-constacyclic code is a μ^{-1}-constacyclic code.*

Remark 2.2. *The dual code $C^{\perp}$ of a cyclic (negacyclic) code C is a cyclic (negacyclic) code, however, from Lemma 2.1, we notice that the dual code of μ-constacyclic code is not a μ-constacyclic code for every $\mu\in\mathbb{F}_q^*\setminus\{1,-1\}$.*

Definition 2.3 (see [13])**.** *Two (n,M)-codes, where M is the size of the code, over $\mathbb{F}_q$ are equivalent if one can be obtained from the other by a combination of operations of the following type:*

(i) permutation of the n digits of the codewords;

(ii) multiplication of the symbols appearing in a fixed position by a nonzero scalar.

Lemma 2.4. *[13, p.72] Equivalent linear codes have the same length, dimension and distance.*

The following result contains a criterion on irreducible non-linear binomials over $\mathbb{F}_q$, which was given by Serret in 1866.

Lemma 2.5. *[12, Theorem 3.75] Let $t\geq 2$ be an integer and $a\in\mathbb{F}_q^*$. Then the binomial x^t-a is irreducible in $\mathbb{F}_q[x]$ if and only if the following two conditions are satisfied:*

(i) each prime factor of t divides the order e of a in $\mathbb{F}_q^*$, but does not divide $(q-1)/e$;

(ii) $q\equiv 1 \pmod 4$ if $t\equiv 0 \pmod 4$.

For this section and the rest of this work, we set the following notation: Let ℓ be a prime such that $\gcd(\ell,q)=1$ and $v=\max\{k:\ell^k|(q-1)\}$. Obviously, $v=0$ if and only if $\ell\nmid(q-1)$. Let μ_k be a primitive ℓ^kth root of unity in $\mathbb{F}_q^*$ with $\mu_0=1$.

For a fixed k, where $1\leq k\leq v$, we rephrase the factorization of $x^{\ell^n}-\mu_k$ over $\mathbb{F}_q$ in the following form:

Lemma 2.6. *[6, Theorem 4.1(ii)] Let n be a positive integer, $\gcd(q,\ell)=1$, $r=\min\{n,v-k\}$, $1\leq k\leq v$, and $v\geq 2$ if $\ell=2$. Then the irreducible factorization of $x^{\ell^n}-\mu_k$ is given by*

$$x^{\ell^n}-\mu_k=\prod_{i=1}^{\ell^r}(x^{\ell^{n-r}}-\mu_{k+r}^{\ell^k i+1}),$$

where μ_{k+r} is an element of order ℓ^{k+r} in $\mathbb{F}_q^*$.

In particular, by taking $\ell = 2$ in Lemma 2.6, a factorization of $x^{2^n} - \mu_k$ into the product of 2^r factors is given as follows:

Lemma 2.7. *Let n be a positive integer, q be odd prime power, $r = \min\{n, v-k\}$ and $1 \leq k \leq v$. Then a factorization of $x^{2^n} - \mu_k$ over $\mathbb{F}_q$ is given by:*

$$x^{2^n} - \mu_k = \prod_{i=1}^{2^r} (x^{2^{n-r}} - \mu_{k+r}^{2^k i+1}),$$

where μ_{k+r} is an element of order 2^{k+r} in $\mathbb{F}_q^*$. Further, if $v \geq 2$, the factorization is irreducible over $\mathbb{F}_q$, and if $v = 1$, the irreducible factorization of $x^{2^n} - \mu_v$ is given in Lemma [16, Lemma 2.6].

In order to give a detailed explanation of our examples, we consider the following notions and results given in [15].

Let $\mathcal{S}_q = \{a^2 : a \in \mathbb{F}_q^*\}$ and $\mathcal{O}_q = \{a \in \mathbb{F}_q^* : |a| \text{ is odd}\}$, where $|a|$ denotes the order of $a \in \mathbb{F}_q^*$. Readily note that $\mathcal{O}_q$ and $\mathcal{S}_q$ are subgroups of the multiplicative group $\mathbb{F}_q^*$ of the nonzero elements of $\mathbb{F}_q$ satisfying $\mathcal{O}_q \subseteq \mathcal{S}_q$. Remarkably note that $q \equiv 3 \pmod 4$ if and only if $\mathcal{O}_q = \mathcal{S}_q$.

Lemma 2.8. *[15, Theorem 4.2] Let q and t be odd primes such that $q = 2t+1$. Then $\mathcal{S}_q$ is generated by 4.*

Lemma 2.9. *[15, Theorem 4.4] Let q and t be odd primes such that $q = 4t+1$. Then the following holds:*

(i) $\mathcal{O}_q = \langle t \rangle = \{t^i : 0 \leq i \leq t-1\}$.

(ii) $\mathcal{S}_q = \langle 4 \rangle$ *and* $\mathcal{O}_q = \langle 16 \rangle$ *for* $q > 13$.

3. A class of irreducible constacyclic codes

This section studies a class of μ_k- irreducible constacyclic code over $\mathbb{F}_q$. The weight distribution of this class of codes is followed by the form of codewords without putting much effort.

First of all, by using the same notation introduced in Lemma 2.6, let $C_{k,i}$ denote a μ_k-constacyclic $[\ell^n, \ell^{n-r}]_q$ code with the parity check polynomial $h_{k,i}(x) = x^{\ell^{n-r}} - \mu_{k+r}^{\ell^k i+1}$. Then the generator polynomial $g_{k,i}(x)$ of $C_{k,i}$ is given by:

$$g_{k,i}(x) = \frac{x^{\ell^n} - \mu_k}{x^{\ell^{n-r}} - \mu_{k+r}^{\ell^k i+1}}.$$

Theorem 3.1. *Let n be a positive integer, ℓ be a prime such that $\gcd(\ell, q) = 1$, $\ell^k | (q-1)$ for $1 \leq k \leq v$ and $r = \min\{n, v-k\}$. Then the generator polynomial of $C_{k,i}$ is given by:*

$$g_{k,i}(x) = \sum_{u=0}^{\ell^r - 1} \mu_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(\ell^r - u - 1)}.$$

Further, if $\mathbf{a} = (a_0, a_1, \ldots, a_{\ell^{n-r}-1}) \in \mathbb{F}_q^{\ell^{n-r}}$ be any message word, then

$$C_{k,i} = \{(\mathbf{a}, \mathbf{a}\mu_{k+r}^{\ell^k i+1}, \cdots, \mathbf{a}\mu_{k+r}^{(\ell^k i+1)(\ell^r - 1)})\}.$$

Proof. Let $r = \min\{n, v-k\}$ and $1 \leq k \leq v$. Since $\mu_k = \mu_{k+r}^{(\ell^k i+1)\ell^r}$ for $1 \leq i \leq \ell^r$, so

$$x^{\ell^n} - \mu_k = (x^{\ell^{n-r}})^{\ell^r} - \mu_{k+r}^{(\ell^k i+1)\ell^r} = (x^{\ell^{n-r}} - \mu_{k+r}^{\ell^k i+1})\Big(\sum_{u=0}^{\ell^r-1} \mu_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(\ell^r - u - 1)}\Big).$$

Therefore, the generator polynomial $g_{k,i}(x)$ of a μ_k-constacyclic $[\ell^n, \ell^{n-r}]_q$ code $C_{k,i}$ is given by:

$$g_{k,i}(x) = \frac{x^{\ell^n} - \mu_k}{x^{\ell^{n-r}} - \mu_{k+r}^{\ell^k i+1}} = \sum_{u=0}^{\ell^r-1} \mu_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(\ell^r-u-1)}.$$

Let $\mathbf{a} = (a_0, a_1, \cdots, a_{\ell^{n-r}-1}) \in \mathbb{F}_q^{\ell^{n-r}}$ be any message word. Then the corresponding message polynomial can be expressed as

$$\mathbf{a}(x) = \sum_{j=0}^{\ell^{n-r}-1} a_j x^{\ell^{n-r}-j-1}.$$

Therefore, the code polynomial of $C_{k,i}$ is given as follows:

$$\begin{aligned} \mathbf{a}(x)g_{k,i}(x) &= \left(\sum_{j=0}^{\ell^{n-r}-1} a_j x^{\ell^{n-r}-j-1}\right)\left(\sum_{u=0}^{\ell^r-1} \mu_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(\ell^r-u-1)}\right) \\ &= \sum_{u=0}^{\ell^r-1} \mu_{k+r}^{(\ell^k i+1)u} \left(\sum_{j=0}^{\ell^{n-r}-1} a_j x^{\ell^{n-r}-j-1}\right) x^{\ell^{n-r}(\ell^r-u-1)} \\ &= \sum_{u=0}^{\ell^r-1} \sum_{j=0}^{\ell^{n-r}-1} a_j \mu_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(\ell^r-u)-j-1}. \end{aligned}$$

Further, the uth component of codeword $(c_0^*, c_1^*, \cdots, c_{\ell^r-1}^*)$ is

$$c_u^* = (a_0\mu_{k+r}^{(\ell^k i+1)u}, a_1\mu_{k+r}^{(\ell^k i+1)u}, \cdots, a_{\ell^{n-r}-1}\mu_{k+r}^{(\ell^k i+1)u}).$$

By using notation $\mathbf{a}\theta$ for the vector $(a_0\theta, a_1\theta, \cdots, a_{\ell^{n-r}-1}\theta)$, where $\theta \in \mathbb{F}_q^*$, the code $C_{k,i}$ is given by:

$$C_{k,i} = \{(\mathbf{a}, \mathbf{a}\mu_{k+r}^{\ell^k i+1}, \cdots, \mathbf{a}\mu_{k+r}^{(\ell^k i+1)(\ell^r-1)}) : \mathbf{a} \in \mathbb{F}_q^{\ell^{n-r}}\}.$$

This completes the proof. □

Remark 3.2. *By Lemma 2.5, $x^{\ell^{n-r}} - \mu_{k+r}^{\ell^k i+1}$ is an irreducible factor of $x^{\ell^n} - \mu_k$ over $\mathbb{F}_q$ for every $1 \le i \le \ell^r$ provided that $v \ge 2$ if $\ell = 2$. Let us consider the exceptional case $v = 1$ if $\ell = 2$. Then $k = 1$, $i = 1$ and hence $g_{k,i} = 1$. Thus, the code $C_{k,i}$ becomes the whole space $\mathbb{F}_q^{2^n}$, a trivial negacyclic code. For any $n \ge 2$, $x^{2^n}+1$ is reducible over $\mathbb{F}_q$, where $q \equiv 3 \pmod 4$. Therefore, there are non-trivial negacyclic equivalent codes of length 2^n. These negacyclic codes of length 2^n over $\mathbb{F}_q$ and their weight distribution have been studied in [17, Theorem 4.6].*

Lemma 3.3. *For any $1 \le i, j \le \ell^r$, $C_{k,i}$ is equivalent to $C_{k,j}$.*

Proof. There are ℓ^r irreducible codes $C_{k,i}$ for $1 \le i \le \ell^r$ for each fixed k, where $1 \le k \le v$ and $r = \min\{n, v-k\}$. For every pair (i, j), where $1 \le i \le j \le \ell^r$, there exists a unique $l = j - i \pmod{\ell^r}$ such that $\mu_{k+r}^{\ell^k j+1} = \mu_r^l \mu_{k+r}^{\ell^k i+1}$. Using the form of codewords of $C_{k,i}$ and $C_{k,j}$ given in Theorem 3.1, it follows that $C_{k,j} = \mu_r^{j-i} C_{k,i}$. Thus, the code $C_{k,j}$ can be obtained form the code $C_{k,i}$ by multiplying μ_r^{j-i} and hence they are equivalent. □

By Lemma 3.3, in particular, the code $C_{k,i}$ is equivalent to C_{k,ℓ^r}. For convenience point of view, we denote C_{k,ℓ^r} by C_k.

Theorem 3.4. *By using the assumptions of Theorem 3.1, the weight distribution of μ_k-constacyclic $[\ell^n, \ell^{n-r}]_q$ code C_k is*

$$A_{\ell^r j} = \binom{\ell^{n-r}}{j}(q-1)^j \ \ \textit{for} \ \ 0 \leq j \leq \ell^{n-r}.$$

Proof. Direct from Theorem 3.1. □

Keeping in mind the previous notation, we now present the following result, which will be important in order to study of isodual and formally self-dual constacyclic codes that we are interested in.

Theorem 3.5. *Let q, ℓ, r and k be as before, and additionally, let ℓ be odd. Then*

$$x^{2\ell^n} - \mu_k = \prod_{i=1}^{\ell^r}(x^{\ell^{n-r}} \pm \theta_{k+r}^{\ell^k i+1}),$$

where θ_{k+r} is an element of order ℓ^{k+r} and $\theta_k^2 = \mu_k$.

Proof. For each $1 \leq k \leq v$, the order of μ_k is ℓ^k. Clearly ℓ^k is odd and $\mu_k^{\ell^k+1} = \mu_k$. Let $\theta_k = \mu_k^{(\ell^k+1)/2}$ for $1 \leq k \leq v$. Then the order of θ_k is ℓ^k and $\theta_k^2 = \mu_k$. It follows that $x^{2\ell^n} - \mu_k = x^{2\ell^k} - \theta_k^2 = (x^{\ell^k} - \theta_k)(x^{\ell^k} + \theta_k)$. By Lemma 2.6, the factorization of $x^{\ell^n} - \theta_k$ over $\mathbb{F}_q$ is given by:

$$x^{\ell^n} - \theta_k \ = \prod_{i=1}^{\ell^r}(x^{\ell^{n-r}} - \theta_{k+r}^{\ell^k i+1}).$$

By changing x to $-x$ in the above factorization of $x^{\ell^n} - \theta_k$, we obtain the factorization of $x^{\ell^n} + \theta_k$ over $\mathbb{F}_q$ as follows:

$$x^{\ell^n} + \theta_k \ = \prod_{i=1}^{\ell^r}(x^{\ell^{n-r}} + \theta_{k+r}^{\ell^k i+1}).$$

This completes the proof. □

Theorem 3.6. *Let q, ℓ, r, k ℓ be as in Theorem 3.5, and additionally, let m be a positive integer. Then a recursive factorization of $x^{2^m\ell^n} - \mu_k$ over $\mathbb{F}_q$ is given by*

$$x^{2^m\ell^n} - \mu_k = \prod_{i=1}^{\ell^r}(x^{2^{m-1}\ell^{n-r}} \pm \theta_{k+r}^{\ell^k i+1}),$$

where θ_{k+r} is an element of order ℓ^{k+r} and $\theta_k^2 = \mu_k$.

Proof. The required form of factorization follows directly by using the substitution x to $x^{2^{m-1}}$ in Theorem 3.5. By Lemma 2.5, binomials $x^{2^{m-1}\ell^n} \pm \theta_{k+r}^{\ell^k i+1}$ is reducible over $\mathbb{F}_q$ if and only if $\mp\theta_{k+r}^{\ell^k i+1} \in \mathcal{S}_q$, where $\mathcal{S}_q$ is the set of all square elements in $\mathbb{F}_q^*$. □

For each $1 \leq k \leq v$, in view of Theorem 3.5, there are $2\ell^r$ distinct irreducible factors of $x^{2\ell^n} - \mu_k$ over $\mathbb{F}_q$. Let $C'_{k,i}$ and $C''_{k,i}$ be μ_k-constacyclic $[2\ell^n, \ell^{n-r}]_q$ codes such that $C'_{k,i} = \langle g'_{k,i}(x)\rangle$ and $C''_{k,i} = \langle g''_{k,i}(x)\rangle$, where $1 \leq i \leq \ell^r$, $1 \leq k \leq v$ and

$$g'_{k,i}(x) = \frac{x^{2\ell^n} - \mu_k}{x^{\ell^{n-r}} - \theta_{k+r}^{\ell^k i+1}} = \left(\frac{x^{\ell^n} - \theta_k}{x^{\ell^{n-r}} - \theta_{k+r}^{\ell^k i+1}}\right)(x^{\ell^n} + \theta_k)$$

and

$$g''_{k,i}(x) = \frac{x^{2\ell^n} - \mu_k}{x^{\ell^{n-r}} + \theta_{k+r}^{\ell^k i+1}} = \left(\frac{x^{\ell^n} + \theta_k}{x^{\ell^{n-r}} + \theta_{k+r}^{\ell^k i+1}}\right)(x^{\ell^n} - \theta_k).$$

Theorem 3.7. *Let ℓ be a prime. $1 \le i \le \ell^r$ and $1 \le k \le v$. Then the generator polynomial $g'_{k,i}(x)$ of $C'_{k,i}$ is given by*

$$g'_{k,i}(x) = \sum_{u=0}^{\ell^r-1} \theta_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(\ell^r-u-1)}(x^{\ell^n}+\theta_k).$$

Further, if $\mathbf{a} \in \mathbb{F}_q^{\ell^{n-r}}$ is any message word, then

$$C'_{k,i} = \{(\mathbf{a}, \mathbf{a}\theta_{k+r}^{\ell^k i+1}, \cdots, \mathbf{a}\theta_{k+r}^{(\ell^k i+1)(2\ell^r-1)})\}.$$

Proof. Using the argument of Theorem 3.1, we obtain

$$x^{\ell^n} - \theta_k \;=\; (x^{\ell^{n-r}} - \theta_{k+r}^{\ell^k i+1})\Big(\sum_{u=0}^{\ell^r-1} \theta_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(\ell^r-u-1)}\Big).$$

It follows that

$$\begin{aligned} x^{2\ell^n} - \mu_k &= (x^{\ell^n}-\theta_k)(x^{\ell^n}+\theta_k) \\ &= (x^{\ell^{n-r}} - \theta_{k+r}^{\ell^k i+1})\Big(\sum_{u=0}^{\ell^r-1} \theta_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(\ell^r-u-1)}\Big)\big(x^{\ell^n}+\theta_k\big) \\ &= (x^{\ell^{n-r}} - \theta_{k+r}^{\ell^k i+1})\Big(\sum_{u=0}^{2\ell^r-1} \theta_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(2\ell^r-u-1)}\Big). \end{aligned}$$

Thus the generator polynomial $g'_{k,i}(x)$ of a μ_k-constacyclic $[2\ell^n, \ell^{n-r}]_q$ code $C'_{k,i}$ is

$$g'_{k,i}(x) = \frac{x^{2\ell^n}-\mu_k}{x^{\ell^{n-r}} - \theta_{k+r}^{\ell^k i+1}} = \sum_{u=0}^{2\ell^r-1} \theta_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(2\ell^r-u-1)}.$$

Let $\mathbf{a} = (a_0, a_1, \cdots, a_{\ell^{n-r}-1}) \in \mathbb{F}_q^{\ell^{n-r}}$ be any message word. Then the corresponding message polynomial can be expressed as $\mathbf{a}(x) = \sum_{j=0}^{\ell^{n-r}-1} a_j x^{\ell^{n-r}-j-1}$. It follows that the code polynomial of $C'_{k,i}$ is

$$\begin{aligned} \mathbf{a}(x)g'_{k,i}(x) &= \left(\sum_{j=0}^{\ell^{n-r}-1} a_j x^{\ell^{n-r}-j-1}\right)\left(\sum_{u=0}^{2\ell^r-1} \theta_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(2\ell^r-u-1)}\right) \\ &= \sum_{u=0}^{\ell^r-1} \theta_{k+r}^{(\ell^k i+1)u} \left(\sum_{j=0}^{\ell^{n-r}-1} a_j x^{\ell^{n-r}-j-1}\right) x^{\ell^{n-r}(2\ell^r-u-1)} \\ &= \sum_{u=0}^{2\ell^r-1} \sum_{j=0}^{\ell^{n-r}-1} a_j \theta_{k+r}^{(\ell^k i+1)u} x^{\ell^{n-r}(2\ell^r-u)-j-1}. \end{aligned}$$

Further, the uth component of codeword $(c_0^{**}, c_1^{**}, \cdots, c_{\ell^r-1}^{**})$ is

$$c_u^{**} = (a_0\theta_{k+r}^{(\ell^k i+1)u}, a_1\theta_{k+r}^{(\ell^k i+1)u}, \cdots, a_{\ell^{n-r}-1}\theta_{k+r}^{(\ell^k i+1)u}).$$

If we denote $\mathbf{a}\theta = (a_0\theta, a_1\theta, \cdots, a_{\ell^{n-r}-1}\theta)$ for some $\theta \in \mathbb{F}_q^*$, then $c_u^{**} = \mathbf{a}\theta_{k+r}^{(\ell^k i+1)u}$ for each $0 \le u \le 2\ell^r - 1$. Therefore

$$C'_{k,i} = \{(\mathbf{a}, \mathbf{a}\theta_{k+r}^{\ell^k i+1}, \cdots, \mathbf{a}\theta_{k+r}^{(\ell^k i+1)(2\ell^r-1)}) : \mathbf{a} \in \mathbb{F}_q^{\ell^{n-r}}\}.$$

This completes the proof. □

Using the argument discussed in Lemma 3.3, observe that codes $C'_{k,i}$ and $C''_{k,i}$ are equivalent to codes C'_{k,ℓ^r} and C''_{k,ℓ^r} respectively. Denote C'_{k,ℓ^r} by C'_k, and C''_{k,ℓ^r} by C''_k.

Theorem 3.8. *With our notation and assumption, C'_k is equivalent to C''_k.*

Proof. Let $g'_k(x)$ and $g''_k(x)$ be generator polynomials of C'_k and C''_k respectively. Now the equivalence of these codes is asserted by the following identity:

$$g''_k(-x) = \frac{x^{2\ell^n} - \mu_k}{-x^{\ell^{n-r}} + \theta_{k+r}} = -\left(\frac{x^{2\ell^n} - \mu_k}{x^{\ell^{n-r}} - \theta_{k+r}}\right) = -g'_k(x).$$

□

Remark 3.9. *For each fixed $1 \le k \le v$ and $r = \min\{n, v-k\}$, there are $2\ell^r$ irreducible codes $C'_{k,i}$ and $C''_{k,i}$ for $1 \le i \le \ell^r$. By Theorem 3.8, these codes are equivalent to C'_k. By Lemma 2.4, since equivalent linear codes share the same weight distributions, so it is sufficient to determine the weight distribution of C'_k, a μ_k-constacyclic code of length $2\ell^n$ with the parity check polynomial $x^{\ell^{n-r}} - \theta_{k+r}$.*

Theorem 3.10. *Let ℓ be a prime, $r = \min\{n, v-k\}$ and $1 \le k \le v$. Then the weight distribution of μ_k-constacyclic $[2\ell^n, \ell^{n-r}]_q$ code C'_k is*

$$A_{2\ell^r j} = \binom{\ell^{n-r}}{j}(q-1)^j \ \ \textit{for} \ \ 0 \le j \le \ell^{n-r}.$$

Proof. From Theorem 3.7, the explicit form of codewords of C'_k is given by:

$$C'_k = \{(\mathbf{a}, \mathbf{a}\theta_{k+r}, \cdots, \mathbf{a}\theta_{k+r}^{2\ell^r-1}) : \mathbf{a} \in \mathbb{F}_q^{\ell^{n-r}}\}.$$

Now, the weight distribution of C'_k follows directly by using the above form of the code. □

In end of this section, we present two examples as follows.

Example 3.11. *With our notation, let $q = 163$, $\ell = 3$. Then $v = 4$, $1 \le k \le 3$ and $r = \min\{n, 4-k\} \ge 1$. Since $\mathcal{S}_q (= \mathcal{O}_q)$, a subgroup of order 81, has $\phi(3^i) = 3^{i-1} \cdot 2$ elements of order 3^i for $1 \le i \le 4$, and $4 \in \mathcal{S}_q$, so its order is either 9, 27 or 81. Using simple modular arithmetic, we obtain the order of 4 is 81. Thus one of the value of μ_4 is 4. Take $\mu_4 = -18 = 4^{61}$, $\mu_3 = 36 = 4^{21}$, $\mu_2 = 38 = 4^{63}$, $\mu_1 = 104 = 4^{27}$. It is important to note that the choice of μ_4 determines μ_i uniquely as follows $\mu_{4-i} = \mu_4^{3^i}$ for $0 \le i \le 3$, however if we choose μ_1 first, then μ_2 has more than one choices, for example if $\mu_1 = 104$, then $\mu_2 \in \{40, 38\}$. By Lemma 2.6, the factorization of $x^{3^n} - \mu_k$ is given by:*

$$x^{3^n} - \mu_k \ = \ \prod_{i=1}^{3^r} (x^{3^{n-r}} - \mu_{k+r}^{3^k i+1}).$$

In view of Table 1, the explicit factorization of $x^{81} - 38$ over $\mathbb{F}_{163}$ is given by:

$$\begin{aligned} x^{81} - 38 \ &= \ (x^9 + 32)(x^9 + 75)(x^9 + 79)(x^9 + 68)(x^9 - 24) \\ &\quad\ (x^9 + 66)(x^9 + 63)(x^9 - 51)(x^9 + 18). \end{aligned}$$

Further, by Theorem 3.4, the weight distribution of 38-constacyclic $[81, 9, 9]_{163}$ code C is

$$A_{9j} = \binom{9}{j}(162)^j \ \ \textit{for} \ \ 0 \le j \le 9.$$

Table 1. Parameters of the factorization $x^{3^n} - \mu_k$; $1 \leq k \leq 3$

n	k	$r = \min\{n, 4-k\}$	μ_k	*degree*	coefficients in $\mathbb{F}^*_{163}$
				3^{n-r}	$\{(-18)^{3^k i+1} : 1 \leq i \leq 3^r\}$
5	1	3	104	9	$\{(36)^i(-18) : 1 \leq i \leq 27\}$
5	2	2	38	27	$\{(38)^i(-18) : 1 \leq i \leq 9\}$
5	3	1	36	81	$\{(104)^i(-18) : 1 \leq i \leq 3\}$
4	1	3	104	3	$\{(36)^i(-18) : 1 \leq i \leq 27\}$
4	2	2	38	9	$\{(38)^i(-18) : 1 \leq i \leq 9\}$
4	3	1	36	27	$\{(104)^i(-18) : 1 \leq i \leq 3\}$
3	1	3	104	1	$\{(36)^i(-18) : 1 \leq i \leq 27\}$
3	2	2	38	3	$\{(38)^i(-18) : 1 \leq i \leq 9\}$
3	3	1	36	9	$\{(104)^i(-18) : 1 \leq i \leq 3\}$
2	1	2	104	3	$\{(36)^i(-18) : 1 \leq i \leq 9\}$
2	2	2	38	1	$\{(38)^i(-18) : 1 \leq i \leq 9\}$
2	3	1	36	3	$\{(104)^i(-18) : 1 \leq i \leq 3\}$
1	1	1	104	1	$\{(36)^i(-18) : 1 \leq i \leq 3\}$
1	2	1	38	1	$\{(38)^i(-18) : 1 \leq i \leq 3\}$
1	3	1	36	1	$\{(104)^i(-18) : 1 \leq i \leq 3\}$

The weight distribution of C_k, where $A_j^{3^{n-r}} = \binom{3^{n-r}}{j}(162)^j$ for $0 \leq j \leq 3^{n-r}$

n	k	$r = 4-k$	μ_k	Weight	No. of codewords of weight i
				$i = 3^r j$	$A_i = A_j^{3^{n-r}}$
5	1	3	104	$27j$	A_j^9
5	2	2	38	$9j$	A_j^{27}
5	3	1	36	$3j$	A_j^{81}
4	1	3	104	$27j$	A_j^3
4	2	2	38	$9j$	A_j^9
4	3	1	36	$3j$	A_j^{27}
3	1	3	104	$27j$	A_j^1
3	2	2	38	$9j$	A_j^3
3	3	1	36	$3j$	A_j^9

Table 1 provides the weight distributions of all irreducible μ_k-constacyclic codes of length 3^n for $n = 3, 4, 5$ and $1 \leq k \leq 3$ over $\mathbb{F}_{163}$.

Example 3.12. *With our notation, let $q = 251$, $\ell = 5$. Then $v = 3$ and $r = \min\{n, 3-k\}$. The set of all square elements $\mathcal{S}_q$ contains 125 elements as follows: $\phi(125) = 100$ elements of order 125, $\phi(25) = 20$ elements of order 25, 4 elements of order 5 and one element of order 1. Since $4, 9 \in \mathcal{S}_q$ are of order 25 and 125 respectively. Take $\mu_3 = 9$, thereby $\mu_2 = \mu_3^5 = 64$ and $\mu_2^5 = \mu_1 = -32 = 219$. Now, $\mu_2 = 64$, $\mu_3 = 9$, $\theta_2 = 64^{13} = -8$ and $\theta_3 = 9^{13} = 88$. By Theorem 3.5, the factorization of $x^{2\cdot5^n} - \mu_k$ for $n \geq 1$ is given by:*

$$x^{2\cdot5^n} - \mu_k \;=\; \prod_{i=1}^{5^r}(x^{5^{n-r}} \pm \theta_{k+r}^{5^k i+1}).$$

Now for $n = 2$, $k = 2$, $r = 1$, $\mu_2 = 64$, $\theta_3 = 88$, the explicit factorization of $x^{50} - 64$ over $\mathbb{F}_{251}$ is given *by:*

$$\begin{aligned} x^{50}-64 &= \prod_{i=1}^{5}(x^5 \pm 88^{25i+1}) \\ &= (x^5+96)(x^5+55)(x^5-60)(x^5-3)(x^5-88) \\ &\quad (x^5-96)(x^5-55)(x^5+60)(x^5+3)(x^5+88). \end{aligned}$$

Also by Theorem 3.10, the weight distribution of 64*-constacyclic* $[50,5,10]_{251}$ *code is*

$$A_{10j} = \binom{5}{j}(250)^j \ \ for \ \ 0 \le j \le 5.$$

Further, by Theorem 3.6, a reducible factorization of $x^{100}-64$ *is given by:*

$$\begin{aligned} x^{100}-64 &= \prod_{i=1}^{5}(x^{10} \pm 88^{25i+1}) \\ &= (x^{10}+96)(x^{10}+55)(x^{10}-60)(x^{10}-3)(x^{10}-88) \\ &\quad (x^{10}-96)(x^{10}-55)(x^{10}+60)(x^{10}+3)(x^{10}+88). \end{aligned}$$

Since $-1 \notin \mathcal{S}_q$ *and* $88 \in \mathcal{S}_q$*, so there are* 5 *reducible binomials, for example* $x^{10}-88 = (x^5-3^{13})(x^5+3^{13}) = (x^5+29)(x^5-29)$*, and the remaining* 5 *are irreducible over* $\mathbb{F}_q$*. Moreover all binomials* $x^{10}-88^{25i+1}$ *for* $1 \le i \le 5$ *are reducible over* $\mathbb{F}_q$ *such as* $x^{10}-88^{25i+1} = (x^5-3^{13(25i+1)})(x^5+3^{13(25i+1)}) = (x^5+29^{25i+1})(x^5-29^{25i+1})$ *for* $1 \le i \le 5$*. This process can be carried forward for a reducible factorization of* $x^{200}-64$ *from the explicit factorization of* $x^{100}-64$ *with* 15 *irreducible factors over* $\mathbb{F}_q$*.*

4. Formally self-dual and isodual codes

A code is formally self-dual (f.s.d.) if the code and its dual have the same weight distribution. A code is isodual if it is equivalent to its dual. Since two equivalent codes have the same weight distribution, so the class of formally self-dual codes automatically contains the class of isodual codes, however, a formally self-dual code need not be isodual (see [9, p. 378]). In this section, we construct isodual and formally self-dual linear codes.

Theorem 4.1. *Let* ℓ *be an odd prime such that* $\ell|(q-1)$*, but* $\ell^2 \nmid (q-1)$ *and* n *be a positive integer. Let* η *be a primitive* ℓ*th root of unity in* $\mathbb{F}_q^*$*. Then there exists an element* $\theta = \eta^{(\ell+1)/2} \in \mathbb{F}_q^*$ *of the order* ℓ *such that* $x^{2\ell^n}-\eta = (x^{\ell^n}-\theta)(x^{\ell^n}+\theta)$*. If* $C_1 = \langle x^{\ell^n}+\theta)\rangle$ *and* $C_2 = \langle x^{\ell^n}-\theta)\rangle$*. Then* $C_1 = \{(\mathbf{a}, \theta\mathbf{a})\}$ *,* $C_1^{\perp} = \{(\theta\mathbf{a}, -\mathbf{a})\}$*,* $C_2 = \{(\mathbf{a}, -\theta\mathbf{a})$ *and* $C_2^{\perp} = \{(\theta\mathbf{a}, \mathbf{a})$ *where* $\mathbf{a} = (a_0, a_1, \ldots, a_{\ell^n-1}) \in \mathbb{F}_q^{\ell^n}$*. Further,* C_1 *and* C_2 *are isodual codes, and* C_i*,* $C_i^{\perp}$ *for* $i = 1, 2$ *are formally self-dual codes.*

Proof. On substituting $v=1$, $r=0$, $k=1$, $\eta = \mu_{k+r} = \mu_1$ in Theorem 3.5, the factorization of $x^{2\ell^n}-\mu_k$ reduces in the following form:

$$x^{2\ell^n}-\eta = x^{2\ell^n}-\eta^{\ell+1} = (x^{\ell^n}-\theta)(x^{\ell^n}+\theta),$$

where $\theta = \eta^{(\ell+1)/2}$. Clearly the order of $\theta \in \mathbb{F}_q^*$ is ℓ. Further, by Theorem 3.7, we find the desired form of C_1 and C_2. Furthermore, $C_1^{\perp}$ is a η^{-1}-constacyclic code. Since $x^{2\ell^n}-\eta^{-1} = \frac{1}{\eta}(\theta x^{\ell^n}-1)(\theta x^{\ell^n}+1)$ and C_1 is generated by $x^{\ell^n}+\theta$, so $C_1^{\perp} = \langle \theta x^{\ell^n}-1\rangle = \langle x^{\ell^n}-\theta^{-1}\rangle$. Similarly $C_2^{\perp} = \langle \theta x^{\ell^n}+1\rangle = \langle x^{\ell^n}+\theta^{-1}\rangle$. Obviously, C_1, C_2, $C_1^{\perp}$ and $C_2^{\perp}$ are all equivalent via a permutation of coordinates and multiplying certain coordinates by constants. Since the relation of equivalence of codes is an equivalence relation, so C_1 is equivalent to $C_1^{\perp}$ and C_2 is equivalent to $C_2^{\perp}$. This proves that C_1 and C_2 are isodual codes. Further, by Theorem 3.10, the weight distribution of C_i and its dual $C_i^{\perp}$ is $A_{2j} = \binom{\ell}{j}(q-1)^j$, where $0 \le j \le \ell$ for $i = 1, 2$. Therefore C_1 and C_2 are formally self-dual codes. □

Remark 4.2. *In view of Theorem 3.5, $\theta_k \in \mathbb{F}_q^*$ presents one of the solution of the equation $x^2 = \mu_k$. Obviously, $-\theta_k$ is another solution of this equation. Since the order of θ_k is ℓ^k, then θ_k is a square element in $\mathbb{F}_q^*$. Note that -1 is a square in $\mathbb{F}_q$ if and only if $4|(q-1)$. In fact, the order of $-\theta_k$ is $2\ell^k$ when $q \equiv 3 \pmod 4$ and, ℓ^k when $q \equiv 1 \pmod 4$. From Theorem 3.6, a reducible factorization of $x^{4\ell^n} - \mu_k$ over $\mathbb{F}_q$ is given recursively as follows:*

$$x^{4\ell^n} - \mu_k = \prod_{i=1}^{\ell^r} (x^{2\ell^{n-r}} \pm \theta_{k+r}^{\ell^k i+1}).$$

(i) If $q \equiv 1 \pmod 4$, for each i, since $\pm\theta_{k+r}^{\ell^k i+1}$ is a square element of order ℓ^{k+r}, where r and k are as usual, and hence by applying Theorem 3.5, one has the explicit factorization of $x^{2\ell^{n-r}} \pm \theta_{k+r}^{\ell^k i+1}$ into the product of $2\ell^{r_1} + 2\ell^{r_1}$ irreducible factors over $\mathbb{F}_q$, where $r_1 = \min\{n-r, v-k\}$. In this case when $q \equiv 1 \pmod 8$, this process of factorization allows us to select the generator polynomials of isodual and formally self-dual codes of length $8\ell^n$ and dimension $4\ell^n$ over a finite field from the given factorization of $x^{8\ell^n} - \mu_k \in \mathbb{F}_q[x]$ (see Example 4.6).

(ii) If $q \equiv 3 \pmod 4$, then $-1 \notin \mathcal{S}_q$, and one of the element $\pm\theta_{k+r}^{\ell^k i+1}$ is a square element and hence either of the binomial $x^{2\ell^{n-r}} \pm \theta_{k+r}^{\ell^k i+1}$ can be expressed as a product of $2\ell^{r_1}$ irreducible factors over $\mathbb{F}_q$, where $r_1 = \min\{n-r, v-k\}$. In this case, the generator polynomials of isodual codes and formally self-dual codes are given by Theorem 4.1.

4.1. Worked examples

The following are examples of isodual codes and formally self-dual codes by means of Theorem 4.1 and Theorem 3.6.

Example 4.3. *For $q = 13$, we have $\ell = 3$, $v = 1$, $r = 0$. By Lemma 2.9, the order of 3 is 3 modulo 13, it follows that $\mu_1 = 3$ $\theta_1 = 9$. By Lemma 2.5, $x^3 - 3$ is an irreducible over $\mathbb{F}_{13}$. By Theorem 3.5, $x^6 - 3 = (x^3 - 9)(x^3 + 9)$. Let*

$$C_1 = \langle x^3 - 9 \rangle = \{(a_0, a_1, a_2, 4a_0, 4a_1, 4a_2) : a_0, a_1, a_2 \in \mathbb{F}_{13}\}.$$

Then $C_1^\perp$ is 9-constacyclic code and is given by:

$$C_1^\perp = \langle x^3 + 3 \rangle = \{(a_0, a_1, a_2, 3a_0, 3a_1, 3a_2) : a_0, a_1, a_2 \in \mathbb{F}_{13}\}.$$

The weight distribution of C_1 and $C_1^\perp$ is $A_{2j} = \binom{3}{j}(12)^j$ for $0 \le j \le 3$. Thus the weight distribution of this code is same as the weight of the code C_1. Denote by $C_2 = \langle x^3 + 9 \rangle$, $C_3 = \langle x^3 - 3 \rangle$ and $C_4 = \langle x^3 + 3 \rangle$. Then these codes are formally self-dual codes, while pairs (C_1, C_4) and (C_2, C_3) are of isodual codes.

Moreover, using Theorem 3.6, we obtain

$$x^{12} - 3 = (x^3 - 3)(x^3 + 3)(x^3 - 2)(x^3 + 2).$$

Now, let $C = \langle (x^3 + 10)(x^3 + 11) \rangle$, then $C^\perp = \langle (x^3 + 4)(x^3 + 6) \rangle$. Here C and $C^\perp$ are respectively, a 3-constacyclic $[12, 6, 3]_{13}$-code and a 9-constacyclic $[12, 6, 3]_{13}$-code. It is quite easy to see that these codes are equivalent and hence C is isodual.

Example 4.4. *For $q = 11$, we obtain $\ell = 5$, $v = 1$, $r = 0$. By Lemma 2.8, $\mu_1 \in \langle 4 \rangle$ is an element of order 5. All $\phi(5) = 4$ elements of order 5 are given in $\{3, 4, 5, 9\}$. Consider $\mu_1 = 3$. By Lemma 2.5, $x^5 - 3$ is irreducible and $x^{10} - 3$ is reducible over $\mathbb{F}_{11}$. Note that $x^{10} - 3 = x^{10} - 3^6 = (x^5 - 3^3)(x^5 + 3^3) = (x^5 - 5)(x^5 + 5)$. By Theorem 3.6, $x^{20} - 3 = (x^{10} - 5)(x^{10} + 5)$. Since $4^2 = 5$, so $\theta_1 = 4$, $x^{10} - 5 = (x^5 - 4)(x^5 + 4)$ and hence $x^{20} - 3 = (x^5 - 4)(x^5 + 4)(x^{10} - 6)$. Let $C = \langle x^5 + 5 \rangle = \{(\mathbf{a}, 5\mathbf{a}) : \mathbf{a} \in \mathbb{F}_{11}^5\}$.*

Then C is a 3-constacyclic code of length 10 over $\mathbb{F}_{11}$ with the parity check polynomial $x^5 - 5$. Then $C^{\perp} = \langle 5x^5 - 1 \rangle = \langle x^5 + 2 \rangle = \{(\mathbf{a}, 2\mathbf{a}) : \mathbf{a} \in \mathbb{F}_{11}^5\}$ is a 4-constacyclic code of length 10 over $\mathbb{F}_{11}$. Since $C^{\perp}$ is equivalent to C, so C is isodual and hence formally self-dual codes.

Example 4.5. *For $q = 29$, we obtain $\ell = 7$, $v = 1$, $r = 0$. By Lemma 2.9, 7 is an element of order 7 modulo 29. Take $\mu_1 = 7$. By Lemma 2.5, $x^7 - 7$ is irreducible and $x^{14} - 7$ is reducible over $\mathbb{F}_{29}$. Note that $x^{14} - 7 = x^{14} - 7^8 = (x^7 - 7^4)(x^7 + 7^4) = (x^7 + 6)(x^7 - 6)$. Let $C = \langle x^7 - 6 \rangle = \{(\mathbf{a}, -6\mathbf{a}) : \mathbf{a} \in \mathbb{F}_{29}^7\}$. Then C is a 7-constacyclic code of length 14 over $\mathbb{F}_{29}$ with the parity check polynomial $x^7 + 6$. Then $C^{\perp} = \langle 6x^7 + 1 \rangle = \langle x^7 + 5 \rangle = \{(\mathbf{a}, 5\mathbf{a}) : \mathbf{a} \in \mathbb{F}_{29}^7\}$ is a 4-constacyclic code of length 14 over $\mathbb{F}_{29}$. Since $C^{\perp} = 4C$ and hence C is isodual and hence formally self-dual codes. By Theorem 3.6, $x^{28} - 7 = (x^{14} - 6)(x^{14} - 23) = (x^7 \pm 8)(x^7 \pm 9)$ and $x^{28} - 25 = (x^{14} - 5)(x^{14} + 5) = (x^7 \pm 11)(x^7 \pm 13)$. Now let $C_1 = \langle (x^7 - 8)(x^7 + 9) \rangle$,$C_1^{\perp} = \langle (x^7 - 11)(x^7 + 13) \rangle$,$C_2 = \langle (x^7 - 8)(x^7 - 9) \rangle$,$C_2^{\perp} = \langle (x^7 - 11)(x^7 - 13) \rangle$, $C_3 = \langle (x^7 + 8)(x^7 - 9) \rangle$, $C_3^{\perp} = \langle (x^7 + 11)(x^7 - 13) \rangle$ and $C_4 = \langle (x^7 + 8)(x^7 + 9) \rangle$, $C_4^{\perp} = \langle (x^7 + 11)(x^7 + 13) \rangle$ can be used for describing equivalent isodual and formally self-dual 23-constacyclic codes.*

Example 4.6. *For $q = 41$, we obtain $\ell = 5$, $v = 1$, $r = 0$. Note that 16 is an element of order 5 modulo 41. Take $\mu_1 = 16$, we have $\mu_1^{-1} = 18$. By Lemma 2.5, $x^5 - 16$ is irreducible and $x^{40} - 16$ is reducible over $\mathbb{F}_{41}$. The factorization of $x^{40} - 16$ over $\mathbb{F}_{41}$ is given by*

$$x^{40} - 16 = (x^5 \pm 17)(x^5 \pm 11)(x^5 \pm 10)(x^5 \pm 8).$$

Also

$$x^{40} - 18 = (x^5 \pm 12)(x^5 \pm 15)(x^5 \pm 4)(x^5 \pm 5).$$

Let $C = \langle f_1(x) f_2(x) g_1(x) g_2(x) \rangle$, where $f_i(x) = x^5 - \eta_i$ and $g_i(x) = x^5 + \eta_i$, where $\eta_i \in \{8, 10, 11, 17\}$ and $1 \leq i \leq 2$. Then C is a 16-constacyclic code of length 40 over $\mathbb{F}_{41}$ and Then

$$C^{\perp} = \left\langle \frac{x^{40} - 18}{f_1^*(x) f_2^*(x) g_1^*(x) g_2^*(x)} \right\rangle$$

is an 18-constacyclic code of length 40 over $\mathbb{F}_{41}$. This represents a class of isodual codes.

Acknowledgment: The author would like to sincerely thank the anonymous referees who gave many helpful comments and suggestions to create an improved version.

References

[1] N. Aydin, I. Siap, D. K. Ray–Chaudhuri, The structure of 1–generator quasi–twisted codes and new linear codes, Des. Codes Cryptogr. 24(3) (2001) 313–326.

[2] C. Bachoc, T. A. Gulliver, M. Harada, Isodual codes over $\mathbb{Z}_{2k}$ and isodual lattices, J. Algebra Combin. 12(3) (2000) 223–240.

[3] G. K. Bakshi, M. Raka, A class of constacyclic codes over a finite field, Finite Field Appl. 18(2) (2012) 362–377.

[4] T. Blackford, Negacyclic duadic codes, Finite Fields Appl. 14(4) (2008) 930–943.

[5] T. Blackford, Isodual constacyclic codes, Finite Fields Appl. 24 (2013) 29–44.

[6] B. Chen, Y. Fan, L. Lin, H. Liu, Constacyclic codes over finite fields, Finite Fields Appl. 18(6) (2012) 1217–1231.

[7] H. Q. Dinh, C. Li, Q. Yue, Recent progress on weight distributions of cyclic codes over finite fields, J. Algebra Comb. Discrete Struct. Appl. 2(1) (2015) 39–63.

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

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

[10] G. T. Kennedy, V. Pless, On designs and formally self–dual codes, Des. Codes Cryptogr. 4(1) (1994) 43–55.

[11] F. Li, Q. Yue, The primitive idempotents and weight distributions of irreducible constacyclic codes, Des. Codes Cryptogr. 86(4) (2018) 771–784.

[12] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, 1986.

[13] S. Ling, C. Xing, Coding Theory: A First Course, Cambridge University Press, 2004.

[14] J. L. Massey, Minimal codewords and secret sharing, Proc. 6th Joint Swedish–Russian Workshop on Information Theory, Mölle, Sweden, (1993) 276–279.

[15] M. Singh, Some subgroups of $\mathbb{F}_q^*$ and explicit factors of $x^{2^n d} - 1 \in \mathbb{F}_q[x]$, Transactions on Combinatorics (2019) doi: 10.22108/TOC.2019.114742.1612.

[16] M. Singh, S. Batra, Some special cyclic codes of length 2^n, J. Algebra Appl. 16(1) (2017) 17 pages.

[17] M. Singh, S. Batra, Weight distribution of a class of cyclic codes of length 2^n, J. Algebra Comb. Discrete Appl. 6(1) (2018) 1–11.

[18] X. Zhu, Q. Yue, L. Hu, Weight distributions of cyclic codes of length l^m, Finite Fields Appl. 31 (2015) 241–257.