Two Families of LCD BCH Codes

Shuxing Li, Chengju Li, Cunsheng Ding, *Senior Member, IEEE*, and Hao Liu

***Abstract*— Historically, LCD cyclic codes were referred to as reversible cyclic codes, which had applications in data storage. Due to a newly discovered application in cryptography, there has been renewed interest in LCD codes. In this paper, we explore two special families of LCD cyclic codes, which are both BCH codes. The dimensions and the minimum distances of these LCD BCH codes are investigated.**

***Index Terms*— BCH codes, LCD codes, linear codes, reversible BCH codes.**

I. Introduction

Let GF(q) be a finite field of size q. An $[n, k, d]$ linear code $\mathcal{C}$ over GF(q) is a linear subspace of GF$(q)^n$ with dimension k and minimum distance d. A linear code $\mathcal{C}$ over GF(q) is called an *LCD code (linear code with complementary dual)* [26] if $\mathcal{C} \cap \mathcal{C}^{\perp} = \{\mathbf{0}\}$, where $\mathcal{C}^{\perp}$ denotes the dual code of $\mathcal{C}$ and is defined by

$$\mathcal{C}^{\perp} = \left\{ \begin{array}{l} (b_0, b_1, \ldots, b_{n-1}) \in \mathrm{GF}(q)^n : \\ \sum_{i=0}^{n-1} b_i c_i = 0 \quad \forall \ (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \end{array} \right\}.$$

An $[n, k, d]$ linear code $\mathcal{C}$ is said to be *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. By identifying each vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathrm{GF}(q)^n$ with

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathrm{GF}(q)[x]/(x^n - 1),$$

a linear code $\mathcal{C}$ of length n over GF(q) corresponds to a GF(q)-submodule of GF$(q)[x]/(x^n - 1)$. $\mathcal{C}$ is a cyclic code if and only if the corresponding submodule is an ideal of GF$(q)[x]/(x^n - 1)$. Note that every ideal of GF$(q)[x]/(x^n - 1)$ is principal. Then there is a monic polynomial $g(x)$ of the smallest degree such that $\mathcal{C} = \langle g(x) \rangle$ and $g(x) \mid (x^n - 1)$. In addition, $g(x)$ is unique and called the *generator polynomial*, and $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity-check polynomial* of $\mathcal{C}$.

Let $f(x) \in \mathrm{GF}(q)[x]$ be a monic polynomial with degree l and $f(0) \neq 0$, then the reciprocal polynomial of f is defined to be $f(0)^{-1} x^l f(x^{-1})$. f is called self-reciprocal if $f(x)$ is equal to its reciprocal. A cyclic code $\mathcal{C}$ with generator polynomial $g(x)$ is called *reversible* if $g(x)$ is self-reciprocal. The reversibility implies if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, then $(c_{n-1}, c_{n-2}, \ldots, c_0) \in \mathcal{C}$. We have the following lemma, showing that LCD cyclic codes and reversible cyclic codes are the same thing.

Lemma 1 [32], [21, Th. 4]: Let $\mathcal{C}$ be a cyclic code over GF(q) *with generator polynomial $g(x)$. Then the following statements are equivalent.*

1) *$\mathcal{C}$ is an LCD code.*
2) *$g(x)$ is self-reciprocal, i.e., $\mathcal{C}$ is a reversible cyclic codes.*
3) *β^{-1} is a root of $g(x)$ for every root β of $g(x)$.*

LCD cyclic codes were first studied by Massey for data storage applications [25], under the name of *reversible codes*. Massey showed that some LCD cyclic codes are BCH codes, and made a comparison between LCD codes and non-LCD codes [25]. He also demonstrated that asymptotically good LCD codes exist [26]. Yang and Massey gave a necessary and sufficient condition for a cyclic code to have a complementary dual [32]. Using the hull dimension spectra of linear codes, Sendrier showed that LCD codes meet the asymptotic Gilbert-Varshamov bound [30]. Esmaeili and Yari analysed LCD codes that are quasi-cyclic [17]. Muttoo and Lal constructed an LCD cyclic code over GF(q) [28]. Tzeng and Hartmann proved that the minimum distance of a class of LCD cyclic codes is greater than the BCH bound [31]. Dougherty, Kim, Ozkaya, Sok and Solé developed a linear programming bound on the largest size of an LCD code of given length and minimum distance [16]. Carlet and Guilley investigated an application of LCD codes against side-channel attacks, and presented several constructions of LCD codes [9]. There are two well known classes of LCD cyclic codes [24, p. 206], which are Melas's double-error correcting binary codes with parameters $[2^m - 1, 2^m - 2m - 1, d \geq 5]$ and Zetterberg's double-error correcting binary codes of length $2^{\ell} + 1$. A well-rounded treatment of LCD cyclic codes was given in [21]. In addition, Boonniyoma and Jitman gave a study on linear codes with Hermitian complementary dual [8].

The objective of this paper is to investigate basic parameters of two families of LCD primitive BCH codes, including their dimensions and minimum distances. More specifically, in Theorems 18, 22, 35 and 42, we determine the dimensions of LCD BCH codes $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ and $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ with $\delta = uq^{\lceil m/2 \rceil} + 1$

Manuscript received June 30, 2016; revised January 23, 2017 and May 24, 2017; accepted June 14, 2017. Date of publication July 4, 2017; date of current version August 16, 2017. C. Li was supported in part by the Shanghai Sailing Program under Grant 17YF1404300 and in part by the NSFC-Zhejiang Joint Fund for the Integration of Industrialization and Informatization under Grant U1509219. C. Ding was supported by the Hong Kong Research Grants Council under Grant 16301114.

S. Li is with the Department of Mathematics, The Hong Kong University of Science and Technology, Hong Kong (e-mail: lsxlsxlsx1987@gmail.com).

C. Li is with the Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai 200062, China (e-mail: lichengju1987@163.com).

C. Ding and H. Liu are with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong (e-mail: cding@ust.hk; hliuar@connect.ust.hk).

Communicated by C. Xing, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2017.2723363

if q is odd, and with $\delta = uq^{\lceil m/2 \rceil}/2 + 1$ if q is even, where $m \geq 4$ and $1 \leq u \leq q-1$. In Theorems 26 and 45, we determine the dimensions of LCD BCH codes $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ and $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ when it has designed distance $q^t - 1$, where $1 \leq t \leq \lceil m/2 \rceil$. In Theorem 49, we determine the dimensions of LCD BCH codes $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$, with $2 \leq \delta \leq q^{(m+1)/2}$ when m is odd, and with $2 \leq \delta \leq 2q^{m/2}$ when m is even. In Theorem 53, we determine the dimensions of LCD BCH codes $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$, with q being odd, $m \geq 4$, $\delta = uq^{\lceil m/2 \rceil} + 1$ and $1 \leq u \leq q-1$. In Theorem 56, we derive lower and upper bounds on the dimension of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$, where $\delta = q^{\lambda}$ and $\frac{m}{2} \leq \lambda \leq m-1$. In Theorem 57 and Corollaries 58 and 59, we determine the minimum distance of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ in some special cases. In Theorems 62, 63 and 64, we determine the parameters of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ when δ is small. According to the tables of best known linear codes (referred to as the *Database* later) maintained by Markus Grassl at http://www.codetables.de/ and the tables of best cyclic codes documented in [13], some of the codes presented in this paper are optimal in the sense that given the length and dimension, the minimum distance is the largest possible.

II. q-Cyclotomic Cosets and BCH Codes

In this section, we introduce q-cyclotomic cosets and their coset leaders, which will play a crucial role in our analysis of LCD codes. Moreover, we give a brief review on BCH codes.

A. q-Cyclotomic Cosets

To deal with cyclic codes of length n over GF(q), we need to study the canonical factorization of $x^n - 1$ over GF(q). To this end, we are going to introduce q-cyclotomic cosets modulo n. Note that $x^n - 1$ has no repeated factors over GF(q) if and only if $\gcd(n,q) = 1$. Throughout this paper, we assume that $\gcd(n,q) = 1$.

Let $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ denote the ring of integers modulo n. For each $s \in \mathbb{Z}_n$, the *q-cyclotomic coset of s modulo n* is defined by

$$C_s = \{s, sq, sq^2, \cdots, sq^{\ell_s - 1}\} \bmod n \subseteq \mathbb{Z}_n, \qquad (1)$$

where ℓ_s is the smallest positive integer such that $q^{\ell_s} s \equiv s \pmod{n}$. Therefore, ℓ_s is the size of the q-cyclotomic coset C_s. We use $cl(s)$ to denote the coset leader of C_s, which is the smallest integer belonging to C_s. Note that the subscript of C_s is regarded as an integer modulo n. Thus, we have $C_{-s} = C_{n-s}$.

B. BCH Codes

Let n be a positive integer with $\gcd(n,q) = 1$ and let m be the smallest positive integer such that $q^m \equiv 1 \pmod{n}$. Let α be a generator of GF(q^m)* and put $\beta = \alpha^{\frac{q^m-1}{n}}$. Then β is a primitive n-th root of unity. For $0 \leq i \leq n-1$, let $m_i(x)$ denote the minimal polynomial of β^i over GF(q). We use $i \bmod n$ to denote the unique integer in the set $\{0, 1, \ldots, n-1\}$, which is congruent to i modulo n. Thus, we have $m_i(x) := m_{i \bmod n}(x)$. Next, we are going to introduce the BCH codes.

Definition 2: For an integer $\delta \geq 2$, define

$$g_{(q,n,\delta,b)}(x) = \mathrm{lcm}(m_b(x), m_{b+1}(x), \cdots, m_{b+\delta-2}(x)),$$

where lcm *denotes the least common multiple of these polynomials. Let $\mathcal{C}_{(q,n,\delta,b)}$ be the cyclic code of length n with generator polynomial $g_{(q,n,\delta,b)}(x)$. Then $\mathcal{C}_{(q,n,\delta,b)}$ is called a BCH code with* designed distance δ.

The famous *BCH bound* implies that the minimum distance of $\mathcal{C}_{(q,n,\delta,b)}$ is greater than or equal to the designed distance δ. We call $\mathcal{C}_{(q,n,\delta,b)}$ a *narrow-sense BCH code* if $b = 1$. When $n = q^m - 1$, $\mathcal{C}_{(q,n,\delta,b)}$ is called a *primitive BCH code*.

So far, we have very limited knowledge of BCH codes, as the dimension and minimum distance of BCH codes are in general open. The narrow-sense primitive BCH codes form the most well-studied subclass of BCH codes, which have been investigated in a series of papers in the literature, including [1], [3], [4], [6], [7], [10]–[12], [14], [15], [20], [23], [24], and [33]. The reader is referred to [15] for a recent survey on known results of narrow-sense primitive BCH codes and to [22] for some new results on narrow-sense nonprimitive BCH codes. As pointed out by Charpin in [11], it is very difficult to determine the minimum distance of BCH codes. However, in some special cases, the minimum distance is known.

Lemma 3 [5, p. 247]: For a narrow-sense BCH code $\mathcal{C}_{(q,n,\delta,1)}$ over GF(q) of length n with designed distance δ, its minimum distance $d = \delta$ if δ divides n.

The following corollary is a generalization of Lemma 3 and will be employed later.

Corollary 4: Let $\mathcal{C}_{(q,n,\delta,b)}$ be the BCH code over GF(q) of length n with designed distance δ. Then its minimum distance $d = \delta$ if δ divides $\gcd(n, b-1)$.

Proof: Write

$$c(x) = \frac{x^n - 1}{x^{n/\delta} - 1} = x^{(\delta-1)\frac{n}{\delta}} + \cdots + x^{\frac{n}{\delta}} + 1.$$

Since $\delta \mid (b-1)$, we have $c(\beta^j) = 0$ for each $b \leq j \leq b+\delta-2$ and $\delta \nmid j$, where β is a primitive n-th root of unity. It then follows that $c(x) \in \mathcal{C}_{(q,n,\delta,b)}$. It is clear that the Hamming weight of $c(x)$ is equal to δ. □

III. Two Families of LCD Primitive BCH Codes

In this section, we introduce two families of LCD primitive BCH codes, whose parameters will be analyzed subsequently. From now on, we always assume that $n = q^m - 1$, and use $\bar{n}$ (respectively, $\bar{m}$) to denote $\lceil \frac{n}{2} \rceil$ (respectively, $\lceil \frac{m}{2} \rceil$).

For each integer δ with $2 \leq \delta \leq \lfloor \frac{n+1}{2} \rfloor$, define

$$g(x) = \begin{cases} \mathrm{lcm}\Big(x+1, g_{(q,n,\delta,\frac{n}{2}+1)}(x), g_{\left(q,n,\delta,\frac{n}{2}-(\delta-1)\right)}(x)\Big), \\ \qquad\qquad\qquad \text{if } n \text{ is even;} \\ \mathrm{lcm}\Big(g_{(q,n,\delta,\frac{n+1}{2})}(x), g_{\left(q,n,\delta,\frac{n+1}{2}-(\delta-1)\right)}(x)\Big), \\ \qquad\qquad\qquad \text{if } n \text{ is odd.} \end{cases} \qquad (2)$$

It can be verified that

$$g(x) = \begin{cases} g_{\left(q,n,2\delta,\frac{n}{2}-(\delta-1)\right)}(x), & \text{if } n \text{ is even;} \\ g_{\left(q,n,2\delta-1,\frac{n+1}{2}-(\delta-1)\right)}(x), & \text{if } n \text{ is odd.} \end{cases} \qquad (3)$$

Let $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ (resp. $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$) be the BCH code of length n with the generator polynomial $g_{\left(q,n,2\delta,\frac{n}{2}-(\delta-1)\right)}(x)$ (resp. $g_{\left(q,n,2\delta-1,\frac{n+1}{2}-(\delta-1)\right)}(x)$). Note that $2 \leq \delta \leq \lfloor\frac{n+1}{2}\rfloor$ ensures $g(x) \neq x^n - 1$. Thus, $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)} \neq \{\mathbf{0}\}$ and $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)} \neq \{\mathbf{0}\}$. It is easy to check that $g_{\left(q,n,2\delta,\frac{n}{2}-\delta+1\right)}(x)$ and $g_{\left(q,n,2\delta-1,\frac{n+1}{2}-\delta+1\right)}(x)$ are self-reciprocal. Therefore, it follows from Lemma 1 that $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ and $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ are LCD BCH codes.

For each $2 \leq \delta < \lfloor\frac{n+1}{2}\rfloor$, define

$$\tilde{g}_{(q,n,2\delta,n-\delta+1)}(x) = \operatorname{lcm}(g_{(q,n,\delta,1)}(x), g_{(q,n,\delta,n-\delta+1)}(x)).$$

Let $\tilde{\mathcal{C}}_{(q,n,2\delta,n-\delta+1)}$ denote the cyclic code of length n with generator polynomial $\tilde{g}_{(q,n,2\delta,n-\delta+1)}(x)$. By Lemma 1, $\tilde{\mathcal{C}}_{(q,n,2\delta,n-\delta+1)}$ is an LCD cyclic code. For the minimum distance d of $\tilde{\mathcal{C}}_{(q,n,2\delta,n-\delta+1)}$, it was shown in [31] that

$$\begin{cases} d = \delta & \text{if } \delta \mid n, \\ d \geq \delta + 1 & \text{otherwise.} \end{cases}$$

Moreover, if we consider the even-like subcode of $\tilde{\mathcal{C}}_{(q,n,2\delta,n-\delta+1)}$, namely, the code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ with length n and generator polynomial

$$g_{(q,n,2\delta,n-\delta+1)}(x) = (x-1)\tilde{g}_{(q,n,2\delta,n-\delta+1)}(x),$$

its minimum distance is at least 2δ by the BCH bound. Hence, a potentially great improvement on the minimum distance is expected by considering the even-like subcode of $\tilde{\mathcal{C}}_{(q,n,2\delta,n-\delta+1)}$. This intuition motivates us to study the code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$, which is an LCD BCH code.

We remark that the two families of codes above are closely related. In fact, when q is odd, $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ and $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ are monomially equivalent [19, p. 24]. Let α be the primitive element of $\mathrm{GF}(q^m)$. Note that $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ has generator polynomial $g_{\left(q,n,2\delta,\frac{n}{2}-\delta+1\right)}(x)$. The parity-check matrix of $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ consists of rows with the form

$$\begin{aligned}(1, \alpha^{\frac{n}{2}+j}, \alpha^{2(\frac{n}{2}+j)}, \alpha^{3(\frac{n}{2}+j)}, \ldots, \alpha^{(n-2)(\frac{n}{2}+j)}, \alpha^{(n-1)(\frac{n}{2}+j)}) \\ = (1, -\alpha^{j}, \alpha^{2j}, -\alpha^{3j}, \ldots, \alpha^{(n-2)j}, -\alpha^{(n-1)j})\end{aligned}$$

where $-\delta+1 \leq j \leq \delta-1$. Meanwhile, the code $C_{(q,n,2\delta,n-\delta+1)}$ has generator polynomial $g_{(q,n,2\delta,n-\delta+1)}(x)$. The parity check matrix of $C_{(q,n,2\delta,n-\delta+1)}$ consists of rows with the form

$$(1, \alpha^{j}, \alpha^{2j}, \alpha^{3j}, \ldots, \alpha^{(n-2)j}, \alpha^{(n-1)j})$$

where $-\delta+1 \leq j \leq \delta-1$. Hence, the parity-check matrix of $C_{(q,n,2\delta,n-\delta+1)}$ can be obtained from that of $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$, by multiplying -1 to some columns. Thus, $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ and $C_{(q,n,2\delta,n-\delta+1)}$ are monomially equivalent when q is odd. Consequently, they have the same parameters, including the dimension and minimum distance. It is worthwhile to note that this equivalence does not hold in general for even q.

IV. Parameters of the Primitive Narrow-Sense BCH Codes $\mathcal{C}_{(q,n,\delta,1)}$

In this section, we always assume that u is an integer with $1 \leq u \leq q-1$ and use notation as in Equation (1).

Lemma 5 [1, Lemmas 8 and 9], [12, Th. 3]: Let $m \geq 2$. Then we have the following.

1) *When m is odd, for $1 \leq j \leq q^{(m+1)/2}$, $|C_j| = |C_{-j}| = m$. For $1 \leq j \leq q^{(m+1)/2}$, j is a coset leader of a q-cyclotomic coset if and only if $q \nmid j$.*
2) *When m is even, $|C_{q^{m/2}+1}| = |C_{-q^{m/2}-1}| = \frac{m}{2}$ and $|C_j| = |C_{-j}| = m$ for $1 \leq j \leq 2q^{m/2}$, $j \neq q^{m/2}+1$. For $1 \leq j \leq 2q^{m/2}$, j is a coset leader of a q-cyclotomic coset if and only if $q \nmid j$.*

We present the size of each cyclotomic coset C_j and characterize all coset leaders j satisfying $1 \leq j \leq uq^{\bar{m}}$ in the following proposition, where $m \geq 5$ is an odd integer.

Proposition 6: Let $m \geq 5$ be an odd integer and let j be an integer with $1 \leq j \leq uq^{\bar{m}}$ and $q \nmid j$, where $1 \leq u \leq q-1$. Then the following holds.

1) $|C_j| = m$,
2) *j is a coset leader of the cyclotomic coset C_j except $j \in J_1 \cup J_2$, where*

$$J_1 = \left\{ j_{\bar{m}}q^{\bar{m}} + j_1q + j_0 : \begin{array}{r} 1 \leq j_{\bar{m}} \leq u-1, \\ 0 \leq j_1 < j_{\bar{m}}, \\ 1 \leq j_0 \leq q-1 \end{array} \right\} \tag{4}$$

and

$$J_2 = \left\{ \begin{array}{l} j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + j_0 : \\ 1 \leq j_{\bar{m}} \leq u-1, \\ 1 \leq j_{\bar{m}-1} \leq q-1, \\ 1 \leq j_0 \leq j_{\bar{m}} \end{array} \right\}. \tag{5}$$

3) $|J_1 \cup J_2| = (u^2-u)(q-1)$.

Proof: For each j with $1 \leq j \leq uq^{\bar{m}}$, let $\ell = |C_j|$. Since m is odd, we have $1 \leq \ell \leq \frac{m}{3}$ if $\ell < m$. For $m \geq 9$, one can check that

$$j < jq^{\ell} < n \text{ for all } 1 \leq j \leq uq^{\bar{m}},$$

which means that

$$jq^{\ell} \equiv j \pmod{n}$$

does not hold for each $\ell < m$. Thus we have $|C_j| = m$ if $m \geq 9$.

For $m \in \{5, 7\}$, if $|C_j| < m$, then $|C_j| = 1$. Therefore, $qj \equiv j \bmod n$, which means that $j \equiv 0 \bmod \frac{q^m-1}{q-1}$. This is impossible as $j < \frac{q^m-1}{q-1}$. Hence, $|C_j| = m$.

Below we characterize all coset leaders j satisfying $1 \leq j \leq uq^{\bar{m}}$. To this end, we have to find all integers j satisfying $j \in C_i$, i.e.,

$$jq^{\ell} \bmod n = i \tag{6}$$

for some integer ℓ with $1 \leq \ell \leq m-1$ and some integer $i < j$. Let i and j be two integers with $q \nmid i, q \nmid j$, and $i < j \leq uq^{\bar{m}}$. By Lemma 5, j is a coset leader if $1 \leq j \leq q^{\bar{m}}$ and $q \nmid j$, so we can further assume that $j \geq q^{\bar{m}}+1$. Then we have the two q-adic expansions

$$i = i_{\bar{m}}q^{\bar{m}} + i_{\bar{m}-1}q^{\bar{m}-1} + \cdots + i_1q + i_0$$

and

$$j = j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + \cdots + j_1q + j_0,$$

where $1 \le i_0, j_0 \le q-1$, $1 \le j_{\bar{m}} \le u-1$, and $0 \le i_{\bar{m}} \le j_{\bar{m}}$.

Case 1: When $1 \le \ell \le \bar{m}-2$, it is easy to check that $i < jq^{\ell} < n$, so (6) does not hold.

Case 2: When $\ell = \bar{m}-1$, we have

$$jq^{\ell} = j_{\bar{m}}q^{m} + j_{\bar{m}-1}q^{m-1} + \cdots + j_1 q^{\bar{m}} + j_0 q^{\bar{m}-1}$$

by noting that $\bar{m} = \frac{m+1}{2}$. Then

$$jq^{\ell} \bmod n = j_{\bar{m}-1}q^{m-1} + \cdots + j_2 q^{\bar{m}+1} + j_1 q^{\bar{m}} + j_0 q^{\bar{m}-1} + j_{\bar{m}}.$$

By (6), we obtain

$$\begin{cases} j_{\bar{m}} = i_0, \\ j_{\bar{m}-1} = j_{\bar{m}-2} = \cdots = j_2 = i_{\bar{m}-2} = i_{\bar{m}-3} = \cdots = i_1 = 0, \\ j_1 = i_{\bar{m}}, \\ j_0 = i_{\bar{m}-1}. \end{cases} \tag{7}$$

Thus $j = j_{\bar{m}}q^{\bar{m}} + j_1 q + j_0$.

Notice that $i < j$. Then $i_{\bar{m}} \le j_{\bar{m}}$. We assert that the equality $i_{\bar{m}} = j_{\bar{m}}$ does not hold. Otherwise, it follows from (7) and $i < j$ that $i_{\bar{m}-1} \le j_{\bar{m}-1} = 0$ and $j_0 = i_{\bar{m}-1} = 0$, which is a contradiction. We then deduce that $0 \le j_1 = i_{\bar{m}} < j_{\bar{m}} \le u-1$. Write

$$J_1 = \left\{ j_{\bar{m}}q^{\bar{m}} + j_1 q + j_0 : \begin{array}{l} 1 \le j_{\bar{m}} \le u-1, \\ 0 \le j_1 < j_{\bar{m}}, \\ 1 \le j_0 \le q-1 \end{array} \right\}.$$

Then when $\ell = \bar{m}-1$, (6) holds if and only if $j \in J_1$.

Case 3: When $\ell = \bar{m}$, we have

$$jq^{\ell} = j_{\bar{m}}q^{m+1} + j_{\bar{m}-1}q^{m} + \cdots + j_1 q^{\bar{m}+1} + j_0 q^{\bar{m}}.$$

Then

$$jq^{\ell} \bmod n = j_{\bar{m}-2}q^{m-1} + \cdots + j_1 q^{\bar{m}+1} + j_0 q^{\bar{m}} + j_{\bar{m}} q + j_{\bar{m}-1}.$$

By (6), we obtain

$$\begin{cases} j_{\bar{m}} = i_1, \\ j_{\bar{m}-1} = i_0, \\ j_{\bar{m}-2} = \cdots = j_2 = j_1 = i_{\bar{m}-1} = i_{\bar{m}-2} = \cdots = i_2 = 0, \\ j_0 = i_{\bar{m}}. \end{cases} \tag{8}$$

Thus $j = j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + j_0$.

Case 3.1: If $i_{\bar{m}} < j_{\bar{m}}$, it then follows from (8) that (6) holds if and only if $j \in J_{21}$, where

$$J_{21} = \left\{ j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + j_0 : \begin{array}{l} 1 \le j_{\bar{m}} \le u-1, \\ 1 \le j_{\bar{m}-1} \le q-1, \\ 1 \le j_0 < j_{\bar{m}} \end{array} \right\}.$$

Case 3.2: If $i_{\bar{m}} = j_{\bar{m}}$ and $j_{\bar{m}-1} > 0$, it then follows from (8) that (6) holds if and only if $j \in J_{22}$, where

$$J_{22} = \left\{ j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + j_0 : \begin{array}{l} 1 \le j_{\bar{m}} \le u-1, \\ 1 \le j_{\bar{m}-1} \le q-1, \\ j_0 = j_{\bar{m}} \ge 1 \end{array} \right\}.$$

Case 3.3: If $i_{\bar{m}} = j_{\bar{m}}$, $j_{\bar{m}-1} = 0$, then $i_0 = j_{\bar{m}-1} = 0$. This is a contradiction to the assumption that $1 \le i_0 \le q-1$.

Write

$$\begin{aligned} J_2 &= J_{21} \cup J_{22} \\ &= \left\{ j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + j_0 : \begin{array}{l} 1 \le j_{\bar{m}} \le u-1, \\ 1 \le j_{\bar{m}-1} \le q-1, \\ 1 \le j_0 \le j_{\bar{m}} \end{array} \right\}. \end{aligned}$$

Then when $\ell = \bar{m}$, (6) holds if and only if $j \in J_2$.

Case 4: When $\bar{m}+1 \le \ell \le m-1$, let $\ell = \bar{m} + \epsilon$, where $1 \le \epsilon \le \bar{m}-2$. Then

$$jq^{\ell} = \\ j_{\bar{m}}q^{2\bar{m}+\epsilon} + \cdots + j_{\bar{m}-\epsilon-1}q^{m} + j_{\bar{m}-\epsilon-2}q^{m-1} + \cdots + j_0 q^{\bar{m}+\epsilon}$$

and

$$\begin{aligned} &jq^{\ell} \bmod n \\ &= j_{\bar{m}-\epsilon-2}q^{m-1} + \cdots + j_0 q^{\bar{m}+\epsilon} + j_{\bar{m}}q^{\epsilon+1} + \cdots + j_{\bar{m}-\epsilon-1}. \end{aligned}$$

Note that $j_0 \ge 1$. Then $jq^{\ell} \bmod n > i$, which implies that (6) is impossible in this case.

Combining Cases 1, 2, 3, and 4, we obtain the conclusion on the characterization of coset leaders. Note that $|J_1| = |J_2| = \frac{u(u-1)}{2}(q-1)$. Since $J_1 \cap J_2 = \emptyset$, we have

$$|J_1 \cup J_2| = (u^2 - u)(q-1).$$

□

Employing Proposition 6, we obtain the dimension of certain narrow-sense primitive BCH code.

Theorem 7: Let $m \ge 5$ be an odd integer and $\delta = uq^{\frac{m+1}{2}} + 1$, where $1 \le u \le q-1$. Then the code $\mathcal{C}_{(q,n,\delta,1)}$ has length n, dimension

$$k = q^{m} - 1 - (uq^{\frac{m-1}{2}} - u^2 + u)(q-1)m,$$

and minimum distance $d \ge \delta$. Furthermore, the generator polynomial is given by

$$g_{(q,n,\delta,1)}(x) = \prod_{\substack{1 \le j \le uq^{\frac{m+1}{2}} \\ q \nmid j,\, j \notin J_1 \cup J_2}} m_j(x),$$

where J_1 and J_2 are defined in Proposition 6.

Proof: The desired conclusions follow from Proposition 6 and the BCH bound immediately. □

Example 8:

1) *When $(q, m, u) = (2, 5, 1)$ in the theorem above, the code $\mathcal{C}_{(q,n,\delta,1)}$ has parameters* $[31, 11, 11]$. *According to the Database, it is an optimal code in the sense that the minimum distance of each binary linear code with length* 31 *and dimension* 11 *is no larger than* 11.
2) *When $(q, m, u) = (2, 7, 1)$ in the above theorem, the code $\mathcal{C}_{(q,n,\delta,1)}$ has parameters* $[127, 71, 19]$, *which are the best known parameters for linear codes according to the Database.*

The following proposition gives the size of each cyclotomic coset C_j and characterizes all coset leaders j satisfying $1 \le j \le uq^{\bar{m}}$, where $m \ge 2$ is an even integer.

Proposition 9: Let $m \ge 2$ be an even integer and let j be an integer with $1 \le j \le uq^{\bar{m}}$ and $q \nmid j$, where $1 \le u \le q-1$. Then the following holds.

1) *$|C_j| = m$, except $|C_{v(q^{\bar{m}}+1)}| = \bar{m}$, where $1 \leq v \leq u-1$.*
2) *j is a coset leader of the cyclotomic coset C_j except $j \in J$, where*

$$J = \{j_{\bar{m}}q^{\bar{m}} + j_0 : 1 \leq j_0 < j_{\bar{m}} \leq u-1\}. \tag{9}$$

3) *$|J| = \frac{(u-1)(u-2)}{2}$.*

Proof: Let i and j be two integers with $q \nmid i, q \nmid j$, and $i < j \leq uq^{\bar{m}}$. Suppose that $j \in C_i$. Then there exists some integer ℓ with $1 \leq \ell \leq m-1$ such that

$$jq^{\ell} \bmod n = i. \tag{10}$$

By Lemma 5, j is a coset leader if $1 \leq j \leq 2q^{\bar{m}}$ and $q \nmid j$, so we can further assume that $j \geq 2q^{\bar{m}} + 1$. Then we have the two q-adic expansions

$$i = i_{\bar{m}}q^{\bar{m}} + i_{\bar{m}-1}q^{\bar{m}-1} + \cdots + i_1q + i_0$$

and

$$j = j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + \cdots + j_1q + j_0,$$

where $1 \leq i_0, j_0 \leq q-1$, $2 \leq j_{\bar{m}} \leq u-1$, and $0 \leq i_{\bar{m}} \leq j_{\bar{m}}$.

Case 1: When $1 \leq \ell \leq \bar{m}-1$, it is easy to check that $i < jq^{\ell} < n$, so (10) does not hold.

Case 2: When $\ell = \bar{m}$, we have

$$jq^{\ell} = j_{\bar{m}}q^{m} + j_{\bar{m}-1}q^{m-1} + \cdots + j_1q^{\bar{m}+1} + j_0q^{\bar{m}}.$$

Then

$$jq^{\ell} \bmod n = j_{\bar{m}-1}q^{m-1} + \cdots + j_1q^{\bar{m}+1} + j_0q^{\bar{m}} + j_{\bar{m}}.$$

By (10), we obtain

$$\begin{cases} j_{\bar{m}} = i_0, \\ j_{\bar{m}-1} = j_{\bar{m}-2} = \cdots = j_1 = i_{\bar{m}-1} = i_{\bar{m}-2} \cdots = i_1 = 0, \\ j_0 = i_{\bar{m}}. \end{cases} \tag{11}$$

Thus $j = j_{\bar{m}}q^{\bar{m}} + j_0$.

Case 2.1: If $i_{\bar{m}} < j_{\bar{m}}$, it then follows from (11) that (10) holds if and only if $j \in J$, where

$$J = \{j_{\bar{m}}q^{\bar{m}} + j_0 : 1 \leq j_0 < j_{\bar{m}} \leq u-1\}.$$

Case 2.2: If $i_{\bar{m}} = j_{\bar{m}}$, since $i_{\bar{m}-1} = \cdots = i_1 = 0$, we have $i_0 < j_0$. Then

$$i_0 < j_0 = i_{\bar{m}} = j_{\bar{m}} = i_0,$$

which is a contradiction. Thus (10) does not hold.

Case 3: When $\bar{m}+1 \leq \ell \leq m-1$, let $\ell = \bar{m} + \epsilon$, where $1 \leq \epsilon \leq \bar{m}-1$. Then

$$jq^{\ell} = j_{\bar{m}}q^{2\bar{m}+\epsilon} + \cdots + j_{\bar{m}-\epsilon}q^{m} + j_{\bar{m}-\epsilon-1}q^{m-1} + \cdots + j_0q^{\bar{m}+\epsilon}.$$

Then

$$jq^{\ell} \bmod n = j_{\bar{m}-\epsilon-1}q^{m-1} + \cdots + j_1q^{\bar{m}+\epsilon+1} + j_0q^{\bar{m}+\epsilon} \\ + j_{\bar{m}}q^{\epsilon} + j_{\bar{m}-1}q^{\epsilon-1} + \cdots + j_{\bar{m}-\epsilon}.$$

Note that $j_0 \geq 1$. Then $jq^{\ell} \bmod n > i$, which implies that (10) is impossible in this case.

Summarizing all the discussions in Cases 1, 2, and 3, we get the desired conclusion of 2). It is easy to see that

$$jq^{\ell} \bmod n > j$$

in both Cases 1 and 3. In Case 2, we have $C_j = \bar{m}$ if and only if $j = j_{\bar{m}}q^{\bar{m}} + j_0$ and $j_0 = j_{\bar{m}}$. Then we proved 1). It is clear that $|J| = \frac{(u-1)(u-2)}{2}$. This completes the proof. □

Employing Proposition 9, we can obtain the dimension of certain narrow-sense primitive BCH code.

Theorem 10: Let $m \geq 2$ be an even integer and $\delta = uq^{\frac{m}{2}} + 1$, where $1 \leq u \leq q-1$. Then the code $\mathcal{C}_{(q,n,\delta,1)}$ has length n, dimension

$$k = q^m - 1 - uq^{\frac{m}{2}-1}(q-1)m + \frac{(u-1)^2}{2}m,$$

and minimum distance $d \geq \delta$. When $u = 1$, we have $d = \delta$. Furthermore, the generator polynomial is given by

$$g_{(q,n,\delta,1)}(x) = \prod_{\substack{1 \leq j \leq uq^{\frac{m}{2}} \\ q \nmid j, j \notin J}} m_j(x),$$

where J is defined in Proposition 9.

Proof: When $u = 1$, it is clear that $\delta | n$. The desired conclusions then follow from Lemma 3, Proposition 9 and the BCH bound. □

Example 11:
1) *When $(q, m, u) = (2, 4, 1)$ in the above theorem, the code $\mathcal{C}_{(q,n,\delta,1)}$ has parameters $[15, 7, 5]$. According to the Database, it is an optimal code in the sense that the minimum distance of each binary linear code with length 15 and dimension 7 is no larger than 5.*
2) *When $(q, m, u) = (3, 4, 1)$, $(3, 4, 2)$ in the above theorem, the code $\mathcal{C}_{(q,n,\delta,1)}$ has parameters $[80, 56, 10]$, and $[80, 34, 20]$, respectively. The former has the best known parameters for linear codes according to the Database.*

V. PARAMETERS OF LCD BCH CODE $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ WHEN q IS ODD

In this section, we always assume that q is odd and use notation as in Equation (1). Unless otherwise stated, u is an integer with $1 \leq u \leq q-1$. The following proposition will be used later.

Proposition 12: Let q be odd and $m \geq 2$. Then we have the following.

1) *$|C_{\bar{n}+i}| = |C_i| = |C_{-i}| = |C_{\bar{n}-i}|$.*
2) *$|C_{\bar{n}+qi}| = |C_{\bar{n}+i}|$ and $|C_{\bar{n}-qi}| = |C_{\bar{n}-i}|$.*
3) *$C_i = C_j$ if and only if $C_{\bar{n}+i} = C_{\bar{n}+j}$.*
4) *$C_i = C_j$ if and only if $C_{\bar{n}-i} = C_{\bar{n}-j}$.*

Proof: The proofs of 1) and 2) are obvious. Note that q is odd. It is clear that

$$\frac{n}{2} \pm i \equiv (\frac{n}{2} \pm j)q^{\ell} \pmod{n},$$

is equivalent to

$$i \equiv jq^{\ell} \pmod{n}$$

for each ℓ with $0 \leq \ell \leq m-1$. Then the conclusions of 3) and 4) follow. □

Let $1 \leq u \leq q-1$ be an integer. Define

$$J^{+}_{(q,n,u)} = \bigcup_{1 \leq j \leq uq^{\bar{m}}} C_{\bar{n}+j} \text{ and } J^{-}_{(q,n,u)} = \bigcup_{1 \leq j \leq uq^{\bar{m}}} C_{\bar{n}-j},$$

where q is odd. It can be deduced from Proposition 12 that $C_{\bar{n}+i} \neq C_{\bar{n}+j}$ and $C_{\bar{n}-i} \neq C_{\bar{n}-j}$ if and only if $C_i \neq C_j$. The following corollary then follows from Propositions 6 and 9 directly.

Corollary 13: Let q be odd and let j be an integer with $1 \leq j \leq uq^{\bar{m}}$.

1) *If $m \geq 5$ is odd, then $|C_{\bar{n}+j}| = |C_{\bar{n}-j}| = m$ and*

$$|J^{+}_{(q,n,u)}| = |J^{-}_{(q,n,u)}| = (uq^{\bar{m}-1} - u^2 + u)(q-1)m.$$

2) *If $m \geq 2$ is even, then $|C_{\bar{n}+j}| = |C_{\bar{n}-j}| = m$ except $j = \upsilon(q^{\bar{m}}+1)$ with $|C_{\bar{n}+\upsilon(q^{\bar{m}}+1)}| = |C_{\bar{n}-\upsilon(q^{\bar{m}}+1)}| = \frac{m}{2}$, where $\upsilon = 1, 2, \ldots, u-1$. In this case,*

$$|J^{+}_{(q,n,u)}| = |J^{-}_{(q,n,u)}| = uq^{\bar{m}-1}(q-1)m - \frac{(u-1)^2}{2}m.$$

Theorem 14: Let $m \geq 2$ be an integer and $\delta = uq^{\bar{m}} + 1$.

1) *If $m \geq 5$ is odd, then $\mathcal{C}_{(q,n,\delta,\frac{n}{2}+1)}$ and $\mathcal{C}_{(q,n,\delta,\frac{n}{2}-(\delta-1))}$ both have length n, dimension*

$$k = q^m - 1 - (uq^{\frac{m-1}{2}} - u^2 + u)(q-1)m,$$

and minimum distance $d \geq \delta$. In addition, the generator polynomials are given by

$$g_{(q,n,\delta,\frac{n}{2}+1)}(x) = \prod_{\substack{1 \leq j \leq uq^{\frac{m+1}{2}} \\ q \nmid j,\, j \notin J_1 \cup J_2}} m_{\frac{n}{2}+j}(x)$$

and

$$g_{(q,n,\delta,\frac{n}{2}-(\delta-1))}(x) = \prod_{\substack{1 \leq j \leq uq^{\frac{m+1}{2}} \\ q \nmid j,\, j \notin J_1 \cup J_2}} m_{\frac{n}{2}-j}(x),$$

where J_1 and J_2 are defined in Proposition 6.

2) *If $m \geq 2$ is even, then $\mathcal{C}_{(q,n,\delta,\frac{n}{2}+1)}$ and $\mathcal{C}_{(q,n,\delta,\frac{n}{2}-(\delta-1))}$ both have length n, dimension*

$$q^m - 1 - uq^{\frac{m}{2}-1}(q-1)m + \frac{(u-1)^2}{2}m,$$

and minimum distance $d \geq \delta$. In addition, the generator polynomials are given by

$$g_{(q,n,\delta,\frac{n}{2}+1)}(x) = \prod_{\substack{1 \leq j \leq uq^{\frac{m}{2}} \\ q \nmid j,\, j \notin J}} m_{\frac{n}{2}+j}(x)$$

and

$$g_{(q,n,\delta,\frac{n}{2}-(\delta-1))}(x) = \prod_{\substack{1 \leq j \leq uq^{\frac{m}{2}} \\ q \nmid j,\, j \notin J}} m_{\frac{n}{2}-j}(x),$$

where J is defined in Proposition 9.

Proof: The proof follows from Corollary 13 and the BCH bound, and is omitted here. □

Example 15:

1) *When $(q, m, u) = (3, 5, 1), (3, 5, 2)$ in the above theorem, the code $\mathcal{C}_{(q,n,\delta,1)}$ has parameters $[242, 152, d \geq 28]$ and $[242, 82, d \geq 55]$, respectively.*
2) *When $(q, m, u) = (4, 4, 1), (4, 4, 2), (4, 4, 3)$ in the above theorem, the code $\mathcal{C}_{(q,n,\delta,1)}$ has parameters $[255, 207, d \geq 17]$, $[242, 161, d \geq 33]$, and $[242, 119, d \geq 49]$, respectively.*

A. Parameters of $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ When m is Odd

The following proposition plays an important role in determining the dimension of the BCH code $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ when $m \geq 5$ is odd and $\delta = uq^{\frac{m+1}{2}} + 1$, where $1 \leq u \leq q-1$.

Proposition 16: For odd $m \geq 5$, we have

$$J^{+}_{(q,n,u)} \cap J^{-}_{(q,n,u)} = \bigcup_{l \in \mathcal{J}_O} (C_{\bar{n}+l} \cup C_{\bar{n}-l}),$$

where the union is disjoint and

$$\mathcal{J}_O = \left\{ \begin{array}{r} l_{\bar{m}}q^{\bar{m}} + l_{\bar{m}-1}q^{\bar{m}-1} + q^{\bar{m}-1} - q + l_0 : \\ 0 \leq l_{\bar{m}} \leq u-1, \\ 0 \leq l_{\bar{m}-1} \leq q-2, \\ q-u \leq l_0 \leq q-1 \end{array} \right\}.$$

Moreover,

$$|J^{+}_{(q,n,u)} \cap J^{-}_{(q,n,u)}| = 2u^2(q-1)m.$$

Proof: We are going to find the integers i and j with $1 \leq i \leq uq^{\bar{m}}$ and $1 \leq j \leq uq^{\bar{m}}$ such that

$$C_{\bar{n}+i} = C_{\bar{n}-j}.$$

This is equivalent to

$$\bar{n}+i \equiv (\bar{n}-j)q^{\ell} \pmod{n} \text{ and } i + jq^{\ell} \equiv 0 \pmod{n} \quad (12)$$

for some $1 \leq \ell \leq m-1$.

By Proposition 12, we can further assume that $q \nmid i$ and $q \nmid j$. Then we have the q-adic expansions

$$i = i_{\bar{m}}q^{\bar{m}} + i_{\bar{m}-1}q^{\bar{m}-1} + \cdots + i_1 q + i_0$$

and

$$j = j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + \cdots + j_1 q + j_0,$$

where $0 \leq i_{\bar{m}}, j_{\bar{m}} \leq u-1$, $1 \leq i_0, j_0 \leq q-1$, and $0 \leq i_k, j_k \leq q-1$ for all k with $1 \leq k \leq \bar{m}-1$.

Case 1: When $1 \leq \ell \leq \bar{m}-2$, it is easy to check that $0 < i + jq^{\ell} < n$ by noticing that $j_{\bar{m}} \leq u-1 < q-1$, so $i + jq^{\ell} \equiv 0 \pmod{n}$ does not hold.

Case 2: When $\ell = \bar{m}-1$, it can be verified that $i + jq^{\ell} \equiv \Delta \pmod{n}$, where

$$\begin{aligned}\Delta = {} & j_{\bar{m}-1}q^{m-1} + \cdots + j_2 q^{\bar{m}+1} + (j_1 + i_{\bar{m}})q^{\bar{m}} \\ & + (j_0 + i_{\bar{m}-1})q^{\bar{m}-1} + i_{\bar{m}-2}q^{\bar{m}-2} + \cdots + i_1 q + (i_0 + j_{\bar{m}}).\end{aligned}$$

It is clear that $0 < \Delta < 2n$. It then follows from (12) that $\Delta = n$. Thus

$$\begin{aligned} j_{\bar{m}-1} = \cdots = j_2 = j_1 + i_{\bar{m}} = j_0 + i_{\bar{m}-1} \\ = i_{\bar{m}-2} = \cdots = i_1 = i_0 + j_{\bar{m}} = q-1. \end{aligned}$$

Then

$$i = i_{\bar{m}}q^{\bar{m}} + i_{\bar{m}-1}q^{\bar{m}-1} + (q-1)(q^{\bar{m}-2} + \cdots + q^2 + q) + i_0,$$

where

$$0 \leq i_{\bar{m}} \leq u-1, \; 0 \leq i_{\bar{m}-1} \leq q-2, \text{ and } q-u \leq i_0 \leq q-1.$$

Hence, there exists exactly one integer j with $1 \leq j \leq uq^{\bar{m}}$, such that

$$C_{\bar{n}+i} = C_{\bar{n}-j},$$

if and only if i has the above form. Therefore,

$$J^{+}_{(q,n,u)} \cap J^{-}_{(q,n,u)} \supset \bigcup_{l \in \mathcal{J}_O} C_{\bar{n}+l}.$$

Case 3: When $\ell = \bar{m}$, we have $i + jq^{\ell} \equiv \Delta \pmod{n}$, where

$$\Delta = j_{\bar{m}-2}q^{m-1} + \cdots + j_1 q^{\bar{m}+1} + (j_0 + i_{\bar{m}})q^{\bar{m}} \\ + i_{\bar{m}-1}q^{\bar{m}-1} + \cdots + i_2 q^2 + (j_{\bar{m}} + i_1)q + (j_{\bar{m}-1} + i_0).$$

Notice that $0 < \Delta < 2n$. If $\Delta \equiv 0 \pmod{n}$, then $\Delta = n$ and

$$j_{\bar{m}-2} = \cdots = j_1 = j_0 + i_{\bar{m}} = i_{\bar{m}-1} = \cdots = i_2 \\ = j_{\bar{m}} + i_1 = j_{\bar{m}-1} + i_0 = q-1.$$

Thus

$$j = j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + (q-1)(q^{\bar{m}-2} + \cdots + q^2 + q) + j_0,$$

where

$$0 \le j_{\bar{m}} \le u-1,\ 0 \le j_{\bar{m}-1} \le q-2, \text{ and } q-u \le j_0 \le q-1.$$

Hence, there exists exactly one integer i with $1 \le i \le uq^{\bar{m}}$, such that

$$C_{\bar{n}+i} = C_{\bar{n}-j},$$

if and only if j has the above form. Therefore,

$$J^{+}_{(q,n,u)} \cap J^{-}_{(q,n,u)} \supset \bigcup_{l \in \mathcal{J}_O} C_{\bar{n}-l}.$$

Case 4: When $\bar{m}+1 \le \ell \le m-1$, write $\ell = \bar{m} + \epsilon$, where $1 \le \epsilon \le \bar{m}-2$. Then $i + jq^{\ell} \equiv \Delta \pmod{n}$, where

$$\Delta = j_{\bar{m}-\epsilon-2}q^{m-1} + \cdots + j_0 q^{\bar{m}+\epsilon} + i_{\bar{m}}q^{\bar{m}} \\ + i_{\bar{m}-1}q^{\bar{m}-1} + \cdots + i_{\epsilon+2}q^{\epsilon+2} \\ + (i_{\epsilon+1} + j_{\bar{m}})q^{\epsilon+1} + \cdots + (i_1 + j_{\bar{m}-\epsilon})q + (i_0 + j_{\bar{m}-\epsilon-1}).$$

It is easy to see that the coefficient of $q^{\bar{m}}$ in the q-adic expansion of Δ is less than $q-1$. Thus we have $0 < \Delta < n$, which means that (12) is impossible.

Note that Cases 1, 2, 3, and 4 contain all possible pairs (i, j), such that $1 \le i, j \le uq^{\bar{m}}$ and $C_{\bar{n}+i} = C_{\bar{n}-j}$. Thus, we have $J^{+}_{(q,n,u)} \cap J^{-}_{(q,n,u)} = \bigcup_{l \in \mathcal{J}_O}(C_{\bar{n}+l} \cup C_{\bar{n}-l})$. Next, we are going to show that this union is disjoint. By Proposition 6, each $l \in \mathcal{J}_O$ is a coset leader and $|C_{\bar{n}+l}| = |C_{\bar{n}-l}| = m$. Hence, by Proposition 12, we have $C_{\bar{n}+l} \ne C_{\bar{n}+l'}$ and $C_{\bar{n}-l} \ne C_{\bar{n}-l'}$ for distinct $l, l' \in \mathcal{J}_O$. In addition, suppose $C_{\bar{n}+l} = C_{\bar{n}-l'}$. If $l \in \mathcal{J}_O$, by the arguments in Case 2, we have

$$l' = l'_{\bar{m}}q^{\bar{m}} + (q-1)(q^{\bar{m}-1} + \cdots + q^2) + l'_1 q + l'_0,$$

where

$$0 \le l'_{\bar{m}} \le u-1, q-u \le l'_1 \le q-1, 1 \le l'_0 \le q-1.$$

Hence, $l' \notin \mathcal{J}_O$. Similarly, if $l' \in \mathcal{J}_O$, by the arguments in Case 3, we must have $l \notin \mathcal{J}_O$. Therefore, the union $\bigcup_{l \in \mathcal{J}_O}(C_{\bar{n}+l} \cup C_{\bar{n}-l})$ is disjoint and $|J^{+}_{(q,n,u)} \cap J^{-}_{(q,n,u)}| = 2m|\mathcal{J}_O| = 2u^2(q-1)m$. □

Remark 17: Let $m \ge 5$ be an odd integer. Let $1 \le i, j \le uq^{\bar{m}}$ be two integers with q-adic expansions

$$i = i_{\bar{m}}q^{\bar{m}} + i_{\bar{m}-1}q^{\bar{m}-1} + \cdots + i_1 q + i_0$$

and

$$j = j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + \cdots + j_1 q + j_0.$$

The proof of Proposition 16 shows that there exists a unique $1 \le j \le uq^{\bar{m}}$, such that

$$i + jq^{\ell} \equiv 0 \pmod{n}$$

for some $1 \le \ell \le m-1$, if and only if one of the following holds:

- *$i \in \mathcal{J}_O, j \notin J_1 \cup J_2 \cup \mathcal{J}_O$ with*

$$j_{\bar{m}-1} = \cdots = j_2 = j_1 + i_{\bar{m}} = j_0 + i_{\bar{m}-1} \\ = i_{\bar{m}-2} = \cdots = i_1 = i_0 + j_{\bar{m}} = q-1.$$

- *$i \notin J_1 \cup J_2 \cup \mathcal{J}_O, j \in \mathcal{J}_O$ with*

$$j_{\bar{m}-2} = \cdots = j_1 = j_0 + i_{\bar{m}} = i_{\bar{m}-1} = \cdots = i_2 \\ = j_{\bar{m}} + i_1 = j_{\bar{m}-1} + i_0 = q-1.$$

We remark that this result does not depend on the parity of q and n. Namely, the above result is true when q is odd, n is even or q is even, n is odd.

The following result gives the dimension of the LCD code $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ when $m \ge 5$ is odd and $\delta = uq^{\frac{m+1}{2}} + 1$, where $1 \le u \le q-1$.

Theorem 18: Let $m \ge 5$ be an odd integer, q odd, and $\delta = uq^{\frac{m+1}{2}} + 1$, where $1 \le u \le q-1$. Then $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ has length n, dimension

$$k = q^m - 2 - 2(uq^{\frac{m-1}{2}} - 2u^2 + u)(q-1)m,$$

and minimum distance $d \ge 2\delta$. In addition, the generator polynomial is given by

$$g(x) = (x+1) \prod_{\substack{1 \le l \le uq^{\frac{m+1}{2}} \\ q \nmid l, l \notin J_1 \cup J_2 \cup \mathcal{J}_O}} m_{\frac{n}{2}+l}(x) m_{\frac{n}{2}-l}(x), \qquad (13)$$

where J_1, J_2 are defined in Proposition 6 and $\mathcal{J}_O$ is defined in Proposition 16.

Proof: Let $1 \le i, j \le uq^{\frac{m+1}{2}}$ be two integers satisfying $C_{\frac{n}{2}+i} = C_{\frac{n}{2}-j}$. By Remark 17, we must have either $i \in \mathcal{J}_O$, $j \notin J_1 \cup J_2 \cup \mathcal{J}_O$ or $j \in \mathcal{J}_O$, $i \notin J_1 \cup J_2 \cup \mathcal{J}_O$. Together with Theorem 14, we can see that the generator polynomial is given by (13), and its degree is equal to $1 + 2(uq^{\frac{m-1}{2}} - 2u^2 + u)(q-1)m$. Hence, the dimension follows easily. The minimum distance $d \ge 2\delta$ follows from the BCH bound. □

Example 19: When $(q, m, u) = (3, 7, 1), (3, 7, 2)$ in the above theorem, the code $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ has parameters $[2186, 1457, d \ge 164]$, and $[2186, 841, d \ge 326]$, respectively.

B. Parameters of $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ When m is Even

To investigate the parameters of the LCD BCH code $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ when $m \ge 2$ is even, we will need the following conclusion.

Proposition 20: Let $m \ge 2$ be an even number. Suppose

$$\begin{cases} 1 \le u \le \frac{q-1}{2} & \text{if } m = 2, \\ 1 \le u \le q-1 & \text{if } m \ge 4. \end{cases}$$

Then we have

$$J^{+}_{(q,n,u)} \cap J^{-}_{(q,n,u)} = \bigcup_{l\in\mathcal{J}_E} C_{\bar{n}-l},$$

where the union is disjoint and

$$\mathcal{J}_E = \left\{ \begin{array}{l} l_{\bar{m}}q^{\bar{m}} + q^{\bar{m}} - q + l_0 : \\ 0 \le l_{\bar{m}} \le u-1 \text{ and } q-u \le l_0 \le q-1 \end{array} \right\}.$$

Moreover,

$$|J^{+}_{(q,n,u)} \cap J^{-}_{(q,n,u)}| = u^2 m.$$

Proof: We are going to find all the integers i and j with $1 \le i \le uq^{\bar{m}}$ and $1 \le j \le uq^{\bar{m}}$ such that

$$C_{\bar{n}+i} = C_{\bar{n}-j}.$$

This is equivalent to

$$\bar{n} + i \equiv (\bar{n} - j)q^{\ell} \pmod{n} \text{ and } i + jq^{\ell} \equiv 0 \pmod{n}$$

for some $1 \le \ell \le m-1$.

By Proposition 12, we can assume that $q \nmid i$ and $q \nmid j$. For $i, j \le uq^{\bar{m}}$, let

$$i = i_{\bar{m}}q^{\bar{m}} + i_{\bar{m}-1}q^{\bar{m}-1} + \cdots + i_1 q + i_0$$

and

$$j = j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + \cdots + j_1 q + j_0,$$

where $0 \le i_{\bar{m}}, j_{\bar{m}} \le u-1$, $1 \le i_0, j_0 \le q-1$, and $0 \le i_k, j_k \le q-1$ for all $1 \le k \le \bar{m}-1$.

Case 1: When $1 \le \ell \le \bar{m}-1$, we can easily see that $0 < i + jq^{\ell} < n$ as $j_{\bar{m}} \le u-1 < q-1$, which implies that $i + jq^{\ell} \equiv 0 \pmod{n}$ does not hold.

Case 2: When $\ell = \bar{m}$, it can be verified that

$$i + jq^{\ell} \equiv \Delta \pmod{n},$$

where

$$\Delta = j_{\bar{m}-1}q^{m-1} + \cdots + j_1 q^{\bar{m}+1} + (j_0 + i_{\bar{m}})q^{\bar{m}} + i_{\bar{m}-1}q^{\bar{m}-1} + \cdots + i_1 q + (i_0 + j_{\bar{m}}).$$

Notice that $0 < \Delta < 2n$. If $\Delta \equiv 0 \pmod{n}$, then $\Delta = n$ and

$$j_{\bar{m}-1} = \cdots = j_1 = j_0 + i_{\bar{m}} = i_{\bar{m}-1} = \cdots = i_1 = i_0 + j_{\bar{m}} = q-1.$$

Thus

$$j = j_{\bar{m}}q^{\bar{m}} + (q-1)(q^{\bar{m}-1} + q^{\bar{m}-2} + \cdots + q) + j_0,$$

where

$$0 \le j_{\bar{m}} \le u-1 \text{ and } q-u \le j_0 \le q-1.$$

Hence, there exists exactly one integer i with $1 \le i \le uq^{\bar{m}}$, such that

$$C_{\bar{n}+i} = C_{\bar{n}-j},$$

if and only if j has the above form. Therefore,

$$J^{+}_{(q,n,u)} \cap J^{-}_{(q,n,u)} \supset \bigcup_{l\in\mathcal{J}_E} C_{\bar{n}-l}.$$

Case 3: When $\bar{m}+1 \le \ell \le m-1$, let $\ell = \bar{m} + \epsilon$, where $1 \le \epsilon \le \bar{m}-1$. Then one can check that $i + jq^{\ell} \equiv \Delta \pmod{n}$, where

$$\Delta = j_{\bar{m}-\epsilon-1}q^{m-1} + \cdots + j_0 q^{\bar{m}+\epsilon} + i_{\bar{m}}q^{\bar{m}} + \cdots + i_{\epsilon+1}q^{\epsilon+1} + (i_{\epsilon} + j_{\bar{m}})q^{\epsilon} + \cdots + (i_0 + j_{\bar{m}-\epsilon}).$$

Note that the coefficient of $q^{\bar{m}}$ in the q-adic expansion of Δ is equal to $i_{\bar{m}} \le u-1 < q-1$. Then $0 < \Delta < n$, which means that

$$(i + jq^{\ell}) \bmod n = \Delta \not\equiv 0 \pmod{n}.$$

Note that Cases 1, 2 and 3 contain all possible pairs (i, j), such that $1 \le i, j \le uq^{\bar{m}}$ and $C_{\bar{n}+i} = C_{\bar{n}-j}$. Thus, $J^{+}_{(q,n,u)} \cap J^{-}_{(q,n,u)} = \bigcup_{l\in\mathcal{J}_E} C_{\bar{n}-l}$. By Proposition 9, each $l \in \mathcal{J}_E$ is a coset leader and $|C_{\bar{n}-l}| = m$. In particular, when $m = 2$, we need $1 \le u \le \frac{q-1}{2}$ to ensure that each $l \in \mathcal{J}_E$ is a coset leader and $|C_{\bar{n}-l}| = m$. Hence, by Proposition 12, we have $C_{\bar{n}-l} \ne C_{\bar{n}-l'}$ for distinct $l, l' \in \mathcal{J}_E$. Therefore, the union $\bigcup_{l\in\mathcal{J}_E} C_{\bar{n}-l}$ is disjoint and $|J^{+}_{(q,n,u)} \cap J^{-}_{(q,n,u)}| = m|\mathcal{J}_E| = u^2 m$. □

Remark 21: Let $m \ge 2$ be an even number. Suppose

$$\begin{cases} 1 \le u \le \frac{q-1}{2} & \text{if } m = 2, \\ 1 \le u \le q-1 & \text{if } m \ge 4. \end{cases}$$

Let $1 \le i, j \le uq^{\bar{m}}$ be two integers with q-adic expansions

$$i = i_{\bar{m}}q^{\bar{m}} + i_{\bar{m}-1}q^{\bar{m}-1} + \cdots + i_1 q + i_0$$

and

$$j = j_{\bar{m}}q^{\bar{m}} + j_{\bar{m}-1}q^{\bar{m}-1} + \cdots + j_1 q + j_0.$$

The proof of Proposition 20 shows that for $1 \le j \le uq^{\bar{m}}$, there exists a unique $1 \le i \le uq^{\bar{m}}$, such that

$$i + jq^{\ell} \equiv 0 \pmod{n}$$

for some $1 \le \ell \le m-1$, if and only if $i, j \in \mathcal{J}_E$ with

$$j_{\bar{m}-1} = \cdots = j_1 = j_0 + i_{\bar{m}} = i_{\bar{m}-1} = \cdots = i_1 = i_0 + j_{\bar{m}} = q-1.$$

We remark that this result does not depend on the parity of q and n. Namely, the above result is true when q is odd, n is even or q is even, n is odd.

Theorem 22: Let q be odd and $m \ge 2$ be even. Let $\delta = uq^{\frac{m}{2}} + 1$, where

$$\begin{cases} 1 \le u \le \frac{q-1}{2} & \text{if } m = 2, \\ 1 \le u \le q-1 & \text{if } m \ge 4. \end{cases}$$

Then $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ has length n, dimension

$$k = q^m - 2 - 2uq^{\frac{m}{2}-1}(q-1)m + (2u^2 - 2u + 1)m,$$

and minimum distance $d \ge 2\delta$. In addition, the generator polynomial is given by

$$g(x) = (x+1) \prod_{\substack{1\le l\le uq^{\frac{m}{2}} \\ q\nmid l,\, l\notin J}} m_{\frac{n}{2}+l}(x) \prod_{\substack{1\le l\le uq^{\frac{m}{2}} \\ q\nmid l,\, l\notin J\cup\mathcal{J}_E}} m_{\frac{n}{2}-l}(x),$$

where J is defined in Proposition 9 and $\mathcal{J}_E$ is defined in Proposition 20, respectively.

Proof: By Remark 21, if for $1 \le i, j \le u\delta^{\frac{m}{2}}$, $C_{\bar{n}+i} = C_{\bar{n}-j}$, then $i, j \in \mathcal{J}_E$. Note that $J \cap \mathcal{J}_E = \emptyset$. The dimension and the generator polynomial follow from Theorem 14 and Proposition 20. The minimum distance $d \ge 2\delta$ follows from the BCH bound. □

Example 23: When $(q, m, u) = (5, 2, 1)$ *in the above theorem, the code* $\mathcal{C}_{(5,24,12,7)}$ *has parameters* $[24, 9, 12]$*, which are the best known parameters for linear codes according to the Database.*

Corollary 24: Let $u = 1$ *and* $\delta = q^{\frac{m}{2}} + 1$*, where* $q \equiv 3 \pmod 4$ *and* $m \equiv 2 \pmod 4$*. Then the true minimum distance of the code* $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ *presented in Theorem 22 is equal to* 2δ*.*

Proof: Note that $b = \frac{n}{2} - \delta + 1$. It is easy to check that $2\delta \mid \gcd(n, b-1)$ in this case. The conclusion then follows from Corollary 4. □

Example 25: When $(q, m, u) = (7, 2, 1)$ *in the above corollary, the code* $\mathcal{C}_{(7,48,16,17)}$ *has parameters* $[48, 25, 16]$*, which are the best known parameters for linear codes according to the Database.*

C. Parameters of $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ *With Designed Distance* $q^t - 1$*, Where* $1 \le t \le \bar{m}$

The dimension of the LCD code $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ is described in the following theorem when $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ has designed distance $2\delta = q^t - 1$ for an integer t with $1 \le t \le \bar{m}$.

Theorem 26: Let q *be odd and* $m \ge 2$*. Suppose* $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ *has designed distance* $2\delta = q^t - 1$*, where* $1 \le t \le \bar{m}$*. Then* $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ *has length n, dimension*

$$k = q^m - 2 - (q^t - q^{t-1} - 2)m$$

and minimum distance $d \ge q^t - 1$*.*

Proof: Set $\delta = \frac{q^t-1}{2}$. Recall that the generator polynomial of the code $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ is $g_{(q,n,2\delta,\frac{n}{2}-(\delta-1))}(x)$, we have

$$\deg(g_{(q,n,2\delta,\frac{n}{2}-(\delta-1))}(x)) = 1 + \left|\left(\bigcup\nolimits_{1\le j\le\delta-1} C_{\bar{n}+j}\right) \bigcap \left(\bigcup\nolimits_{1\le j\le\delta-1} C_{\bar{n}-j}\right)\right|.$$

It follows from Propositions 16 and 20 that

$$\left(\bigcup_{1\le j\le\delta-1} C_{\bar{n}+j}\right) \bigcap \left(\bigcup_{1\le j\le\delta-1} C_{\bar{n}-j}\right) = \emptyset \qquad (14)$$

for each integer m with $m \ge 2$ and $m \ne 3$. Using Remark 17, it can be checked that (14) also holds for $m = 3$. It then follows from Lemma 5 that

$$\deg(g_{(q,n,2\delta,\frac{n}{2}-(\delta-1))}(x)) = (q^t - q^{t-1} - 2)m + 1 \text{ for } 1 \le t \le \bar{m}.$$

Thus, the dimension is obtained. Moreover, $d \ge q^t - 1$ follows from the BCH bound. □

Example 27:

1) *When* $(q, m, t) = (3, 5, 1), (3, 5, 2), (3, 5, 3)$ *in the above theorem, the code* $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ *has parameters* $[242, 241, 2]$, $[242, 221, 8]$, *and* $[242, 161, 26]$*, respectively. All of them are the best known parameters for linear codes according to the Database.*
2) *When* $(q, m, t) = (3, 4, 1), (3, 4, 3)$ *in the above theorem, the code* $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ *has parameters* $[80, 79, 2]$ *and* $[80, 63, 8]$*, respectively. Both of them are the best known parameters for linear codes according to the Database.*

In the above theorem, each triple (q, m, t) satisfying $(q, m) \in \{(3, 2), (3, 3), (3, 4), (3, 5), (5, 2), (7, 2)\}$ and $1 \le t \le \bar{m}$ has been tested in numerical experiments and the experimental results suggest the following conjecture.

Conjecture 28: The code $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ *in Theorem 26 has true minimum distance* $q^t - 1$*.*

VI. Parameters of LCD BCH Code $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ When q is Even

In this section, we always assume that q is even and use notation as in Equation (1). Unless otherwise stated, u is an integer with $1 \le u \le q-1$. The following proposition will be used later.

Proposition 29: Let q *be even and* $m \ge 2$*. Then we have the following.*

1) $|C_{\bar{n}+i}| = |C_{2i+1}|$ *and* $|C_{\bar{n}-i}| = |C_{2i-1}|$*.*
2) $C_{2i+1} = C_{2j+1}$ *if and only if* $C_{\bar{n}+i} = C_{\bar{n}+j}$*.*
3) $C_{2i-1} = C_{2j-1}$ *if and only if* $C_{\bar{n}-i} = C_{\bar{n}-j}$*.*

Proof: The proof of 1) is trivial. Since q is even and $\gcd(2, n) = 1$, it is clear that

$$\frac{n+1}{2} \pm i \equiv (\frac{n+1}{2} \pm j)q^\ell \pmod n,$$

which is equivalent to

$$2i \pm 1 \equiv (2j \pm 1)q^\ell \pmod n$$

for each ℓ with $0 \le \ell \le m-1$. Conclusions 2) and 3) then follow. □

Let $1 \le u \le q-1$ be an integer. Define

$$\tilde{J}^+_{(q,n,u)} = \bigcup_{0\le j\le uq^{\bar{m}}/2-1} C_{\bar{n}+j} \text{ and } \tilde{J}^-_{(q,n,u)} = \bigcup_{1\le j\le uq^{\bar{m}}/2} C_{\bar{n}-j},$$

where q is even.

A. Parameters of $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ *When m is Odd*

In this subsection, we always assume that $m \ge 5$ and m is odd. It can be deduced from Proposition 29 that $C_{\bar{n}+i} \ne C_{\bar{n}+j}$ if and only if $C_{2i+1} \ne C_{2j+1}$ (resp. $C_{\bar{n}-i} \ne C_{\bar{n}-j}$ if and only if $C_{2i-1} \ne C_{2j-1}$). Let J_1 and J_2 be the sets of integers that are not coset leaders, which are given by (4) and (5). Note that $1 \le 2j+1 \le uq^{\bar{m}} - 1$ if $0 \le j \le uq^{\bar{m}}/2 - 1$ and $1 \le 2j-1 \le uq^{\bar{m}} - 1$ if $1 \le j \le uq^{\bar{m}}/2$. Therefore, we have

$$|\tilde{J}^+_{(q,n,u)}| = |\tilde{J}^-_{(q,n,u)}| = |\bigcup_{\substack{1\le l\le uq^{\bar{m}}-1 \\ l \text{ odd}}} C_l|.$$

By Proposition 6, we have $|C_l| = m$ for each $1 \le l \le uq^{\bar{m}} - 1$. When $m \ge 5$, by the definition of J_1 and J_2 in Proposition 6, if $j \in J_1 \cup J_2$, then $|C_j \cap (J_1 \cup J_2)| = 1$. Thus, we have

$$\begin{aligned}|\tilde{J}^+_{(q,n,u)}| &= |\tilde{J}^-_{(q,n,u)}| \\ &= m|\{1 \le l \le uq^{\bar{m}} - 1 : l \text{ is an odd coset leader}\}| \\ &\quad + m|\{1 \le l \le uq^{\bar{m}} - 1 : l \in J_1 \cup J_2 \\ &\qquad \text{is odd and } cl(l) \text{ is even}\}|.\end{aligned}$$

Define

$$\lambda_1 := \lambda_1(u, \bar{m}) = |\{1 \le \tilde{j} \le uq^{\bar{m}} - 1 : \tilde{j} \text{ is an odd coset leader}\}| \tag{15}$$

and

$$\lambda_2 := \lambda_2(u, \bar{m}) = |\{1 \le \tilde{j} \le uq^{\bar{m}} - 1 : \tilde{j} \in J_1 \cup J_2 \text{ is odd, } cl(\tilde{j}) \text{ is even}\}|. \tag{16}$$

It then follows that

$$|\tilde{J}^+_{(q,n,u)}| = |\tilde{J}^-_{(q,n,u)}| = (\lambda_1 + \lambda_2)m. \tag{17}$$

Lemma 30: Let q be even and $m \ge 5$ be odd. Then the following holds.

1)
$$\lambda_1 = \begin{cases} uq^{\bar{m}}/2 - (u^2 - u)q/4 - u^2(q-1)/4, & \text{if } u \text{ is even;} \\ uq^{\bar{m}}/2 - (u^2 - u)q/4 - (u^2 - 1)(q-1)/4, & \text{if } u \text{ is odd.} \end{cases}$$

2)
$$\lambda_2 = \begin{cases} ((u^2 - u)q - u^2)/4, & \text{if } u \text{ is even;} \\ (u^2 - 1)(q-1)/4, & \text{if } u \text{ is odd.} \end{cases}$$

Proof: Notice that q is even. It then follows from Proposition 6 and (15) that

$$\lambda_1 = uq^{\bar{m}}/2 - |\{\tilde{j} \in J_1 : \tilde{j} \text{ is odd}\}| - |\{\tilde{j} \in J_2 : \tilde{j} \text{ is odd}\}|.$$

By (4) and (5), it is easy to see that

$$\begin{aligned} &|\{\tilde{j} \in J_1 : \tilde{j} \text{ is odd}\}| \\ &= \left| \left\{ j_{\bar{m}} q^{\bar{m}} + j_1 q + j_0 : \begin{array}{r} 1 \le j_{\bar{m}} \le u - 1, \\ 0 \le j_1 < j_{\bar{m}}, \\ 1 \le \text{ odd } j_0 \le q - 1 \end{array} \right\} \right| \\ &= (u^2 - u)q/4 \end{aligned}$$

and

$$|\{\tilde{j} \in J_2 : \tilde{j} \text{ is odd}\}| = \begin{cases} u^2(q-1)/4, & \text{if } u \text{ is even;} \\ (u^2 - 1)(q-1)/4, & \text{if } u \text{ is odd.} \end{cases}$$

Then we prove the conclusion on λ_1.

Define

$$\mathrm{CL}_1 = \{cl(\tilde{j}) : \tilde{j} \in J_1\} \text{ and } \mathrm{CL}_2 = \{cl(\tilde{j}) : \tilde{j} \in J_2\}.$$

By Proposition 6, we have

$$\mathrm{CL}_1 = \left\{ j_1 q^{\bar{m}} + j_0 q^{\bar{m}-1} + j_{\bar{m}} : \begin{array}{r} 1 \le j_{\bar{m}} \le u - 1, \\ 0 \le j_1 < j_{\bar{m}}, \\ 1 \le j_0 \le q - 1 \end{array} \right\}$$

and

$$\mathrm{CL}_2 = \left\{ j_0 q^{\bar{m}} + j_{\bar{m}} q + j_{\bar{m}-1} : \begin{array}{r} 1 \le j_{\bar{m}} \le u - 1, \\ 1 \le j_{\bar{m}-1} \le q - 1, \\ 1 \le j_0 \le j_{\bar{m}} \end{array} \right\}.$$

It then follows from (16) that

$$\begin{aligned} \lambda_2 = &|\{\tilde{j} \in J_1 : j_0 \text{ is odd and } j_{\bar{m}} \text{ is even}\}| \\ &+ |\{\tilde{j} \in J_2 : j_0 \text{ is odd and } j_{\bar{m}-1} \text{ is even}\}|. \end{aligned}$$

One can easily check that

$$\lambda_2 = \begin{cases} ((u^2 - u)q - u^2)/4, & \text{if } u \text{ is even;} \\ (u^2 - 1)(q-1)/4, & \text{if } u \text{ is odd.} \end{cases}$$

This completes the proof. □

The following proposition follows from Lemma 30 and (17) directly.

Proposition 31: Let $m \ge 5$ be odd. Then

$$|\tilde{J}^+_{(q,n,u)}| = |\tilde{J}^-_{(q,n,u)}| = \begin{cases} (uq^{\bar{m}}/2 - u^2q/4)m, & \text{if } u \text{ is even;} \\ \left(uq^{\bar{m}}/2 - (u^2 - u)q/4\right)m, & \text{if } u \text{ is odd.} \end{cases}$$

Theorem 32: Let $m \ge 5$ be an odd integer, q even, and $\delta = uq^{\frac{m+1}{2}}/2 + 1$.

1) *If u is even, then $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2})}$ and $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2}-(\delta-1))}$ both have length n, dimension*

$$q^m - 1 - (uq^{\frac{m+1}{2}}/2 - u^2q/4)m,$$

and minimum distance $d \ge \delta$.

2) *If u is odd, then $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2})}$ and $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2}-(\delta-1))}$ both have length n, dimension*

$$k = q^m - 1 - \left(uq^{\frac{m+1}{2}}/2 - (u^2 - u)q/4\right)m,$$

and minimum distance $d \ge \delta$.

Proof: The desired conclusions follow from Proposition 31 and the BCH bound directly. □

Example 33:

1) *When $(q, m, u) = (2, 7, 1)$ in the above theorem, the code $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2})}$ (or $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2}-(\delta-1))}$) has parameters $[127, 71, 19]$, which are the best known parameters for linear codes according to the Database.*
2) *When $(q, m, u) = (4, 5, 1), (4, 5, 2), (4, 5, 3)$ in the above theorem, the code $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2})}$ (or $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2}-(\delta-1))}$) has parameters $[1023, 863, d \ge 33]$, $[1023, 723, d \ge 65]$, and $[1023, 573, d \ge 97]$, respectively.*

The following conclusion will be employed to determine the dimension of the code $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ when $m \ge 5$ is odd.

Proposition 34: For odd $m \ge 5$, we have

$$\tilde{J}^+_{(q,n,u)} \cap \tilde{J}^-_{(q,n,u)} = \bigcup_{l \in \tilde{\mathcal{J}}_O} C_{\bar{n}+(l-1)/2} \cup C_{\bar{n}-(l+1)/2},$$

where the union is disjoint and

$$\tilde{\mathcal{J}}_O = \left\{ \begin{array}{r} l_{\bar{m}} q^{\bar{m}} + l_{\bar{m}-1} q^{\bar{m}-1} + q^{\bar{m}-1} - q + l_0 : \\ 0 \le l_{\bar{m}} \le u - 1, \\ 0 \le \text{ even } l_{\bar{m}-1} \le q - 2, \\ q - u \le \text{ odd } l_0 \le q - 1 \end{array} \right\}.$$

Moreover,

$$|\tilde{J}^+_{(q,n,u)} \cap \tilde{J}^-_{(q,n,u)}| = \begin{cases} \frac{u^2qm}{2}, & \text{if } u \text{ is even;} \\ \frac{u(u+1)qm}{2}, & \text{if } u \text{ is odd.} \end{cases}$$

Proof: We are going to find the integers i and j with $1 \le i \le uq^{\bar{m}}$ and $1 \le j \le uq^{\bar{m}}$ such that

$$C_{\bar{n}+i} = C_{\bar{n}-j}.$$

This is equivalent to

$$(2i+1)+(2j-1)q^{\ell} \equiv 0 \pmod{n}$$

for some $1 \le \ell \le m-1$. Recall that in Remark 17, for $m \ge 5$ being odd, the integers $1 \le i_1, j_1 \le uq^{\bar{m}}$ satisfying

$$i_1 + j_1 q^{\ell} \equiv 0 \pmod{n}$$

have been characterized. Using this result, we can further characterize the odd integers i_1 and j_1 satisfying $i_1 = 2i+1$, $j_1 = 2j-1$ such that

$$C_{\bar{n}+(i_1-1)/2} = C_{\bar{n}-(j_1+1)/2}.$$

The remaining part of the proof follows from Remark 17 with a straightforward calculation. □

Theorem 35: Let $m \ge 5$ be an odd integer, q even, and $\delta = uq^{\frac{m+1}{2}}/2+1$. Then $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ has length n, dimension

$$k = q^m - 1 - (uq^{\frac{m+1}{2}} - u^2 q)m,$$

and minimum distance $d \ge 2\delta - 1$.

Proof: The desired conclusion follows from Theorem 32, Proposition 34, and the BCH bound. □

Example 36:

1) *When $(q,m,u) = (2,7,1)$ in the above theorem, the code $\mathcal{C}_{(2,127,17,56)}$ has parameters* $[127, 29, 37]$.
2) *When $(q,m,u) = (4,5,1), (4,5,2), (4,5,3)$ in the above theorem, the code $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ has parameters* $[1023, 723, d \ge 65]$, $[1023, 463, d \ge 129]$, *and* $[1023, 243, d \ge 193]$, *respectively.*

B. Parameters of $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ When m is Even

It has been seen from Proposition 29 that $C_{\bar{n}+i} \ne C_{\bar{n}+j}$ if and only if $C_{2i+1} \ne C_{2j+1}$ (resp. $C_{\bar{n}-i} \ne C_{\bar{n}-j}$ if and only if $C_{2i-1} \ne C_{2j-1}$). Let J be the set of integers that are not coset leaders, which are given by (9). Note that $1 \le 2j+1 \le uq^{\bar{m}}-1$ if $0 \le j \le uq^{\bar{m}}/2-1$ and $1 \le 2j-1 \le uq^{\bar{m}}-1$ if $1 \le j \le uq^{\bar{m}}/2$. Using the same arguments at the beginning of previous subsection, we can see that

$$|\tilde{J}^{+}_{(q,n,u)}| = |\tilde{J}^{-}_{(q,n,u)}| = \theta_1 m + \theta_2 m/2 + \theta_3 m, \tag{18}$$

where

$$\theta_1 = |\{1 \le \tilde{j} \le uq^{\bar{m}}-1 : \tilde{j} \text{ an odd coset leader } \& \ |C_{\tilde{j}}| = m\}|, \tag{19}$$

$$\theta_2 = |\{1 \le \tilde{j} \le uq^{\bar{m}}-1 : \tilde{j} \text{ an odd coset leader } \& \ |C_{\tilde{j}}| = \frac{m}{2}\}|, \tag{20}$$

and

$$\theta_3 = |\{1 \le \tilde{j} \le uq^{\bar{m}}-1 : \tilde{j} \in J \text{ is odd}, cl(\tilde{j}) \text{ is even}\}|. \tag{21}$$

Lemma 37: Let q be even and $m \ge 2$ be even. Then we have the following.

1)
$$\theta_1 = \begin{cases} uq^{\bar{m}}/2 - u^2/4, & \textit{if } u \textit{ is even;} \\ uq^{\bar{m}}/2 - (u^2-1)/4, & \textit{if } u \textit{ is odd.} \end{cases}$$

2)
$$\theta_2 = \begin{cases} u/2, & \textit{if } u \textit{ is even;} \\ (u-1)/2, & \textit{if } u \textit{ is odd.} \end{cases}$$

3)
$$\theta_3 = \begin{cases} u(u-2)/8, & \textit{if } u \textit{ is even;} \\ (u^2-1)/8, & \textit{if } u \textit{ is odd.} \end{cases}$$

Proof: Notice that q is even. It then follows from Proposition 9, (19), and (20) that

$$\theta_1 = uq^{\bar{m}}/2 - \theta_2 - |\{\tilde{j} \in J : \tilde{j} \text{ is odd}\}|.$$

By (9), it is easy to see that

$$\begin{aligned} &|\{\tilde{j} \in J : \tilde{j} \text{ is odd}\}| \\ &\quad = |\{j_{\bar{m}} q^{\bar{m}} + j_0 : 1 \le j_0 < j_{\bar{m}} \le u-1, j_0 \text{ odd }\}| \\ &\quad = \begin{cases} u(u-2)/4, & \text{if } u \text{ is even,} \\ (u-1)^2/4, & \text{if } u \text{ is odd.} \end{cases} \end{aligned}$$

In addition, it follows from Proposition 9 that

$$\theta_2 = |\{v(q^{\bar{m}}+1) : 1 \le \text{ odd } v \le u-1| = \begin{cases} u/2, & \text{if } u \text{ even;} \\ (u-1)/2, & \text{if } u \text{ odd.} \end{cases}$$

Then we get the conclusions on θ_1 and θ_2.

Define

$$\mathrm{CL} = \{cl(\tilde{j}) : \tilde{j} \in J\}.$$

It follows from Proposition 9 that

$$\mathrm{CL} = \{j_0 q^{\bar{m}} + j_{\bar{m}} : j_0 + 1 \le j_{\bar{m}} \le u-1, 1 \le j_0 \le u-1\}.$$

Then we can deduce from (21) that

$$\theta_3 = |\{j_0 q^{\bar{m}} + j_{\bar{m}} : 1 \le j_0 < j_{\bar{m}} \le u-1, j_0 \text{ odd}, j_{\bar{m}} \text{ even}\}|.$$

It can be easily verified that

$$\theta_3 = \begin{cases} u(u-2)/8, & \text{if } u \text{ is even;} \\ (u^2-1)/8, & \text{if } u \text{ is odd.} \end{cases}$$

This completes the proof. □

The following results follow from Lemma 37 and (18) directly.

Proposition 38: Let $m \ge 2$ be even. Then

$$|\tilde{J}^{+}_{(q,n,u)}| = |\tilde{J}^{-}_{(q,n,u)}| = \begin{cases} \left(uq^{\bar{m}} - u^2/4\right)\frac{m}{2}, & \textit{if } u \textit{ is even;} \\ \left(uq^{\bar{m}} - (u-1)^2/4\right)\frac{m}{2}, & \textit{if } u \textit{ is odd.} \end{cases}$$

Theorem 39: Let $m \ge 2$ be an even integer, q even, and $\delta = uq^{\frac{m}{2}}/2+1$.

1) *If u is even, then $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2})}$ and $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2}-(\delta-1))}$ both have length n, dimension*
$$k = q^m - 1 - \left(uq^{\frac{m}{2}} - u^2/4\right)\frac{m}{2},$$
and minimum distance $d \ge \delta$.
2) *If u is odd, then $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2})}$ and $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2}-(\delta-1))}$ both have lenth n, dimension*
$$k = q^m - 1 - \left(uq^{\frac{m}{2}} - (u-1)^2/4\right)\frac{m}{2},$$
and minimum distance $d \ge \delta$.

Proof: The desired conclusions follow from Proposition 38 and the BCH bound directly. □

Example 40:

1) *When* $(q,m,u)=(2,6,1)$ *in the above theorem, the code* $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2})}$ *(or* $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2}-(\delta-1))}$*) has parameters* $[63,39,9]$*, which are the best known parameters for linear codes according to the Database and the best possible cyclic codes according to* [13, p. 260].
2) *When* $(q,m,u) = (4,4,1),(4,4,2),(4,4,3)$*, the code* $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2})}$ *(or* $\mathcal{C}_{(q,n,\delta,\frac{n+1}{2}-(\delta-1))}$*) has parameters* $[255,223,d\geq 9]$, $[255,193,d\geq 17]$, *and* $[255,161,d\geq 25]$*, respectively.*

The following conclusion will be employed to investigate the parameters of the code $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ when $m\geq 2$ is even.

Proposition 41: Let $m\geq 2$ *be an even integer and* q *be even. Suppose*

$$\begin{cases} 1\leq u\leq \frac{q}{2} & \textit{if } m=2,\\ 1\leq u\leq q-1 & \textit{if } m\geq 4. \end{cases}$$

Then we have

$$\tilde{J}^{+}_{(q,n,u)}\cap \tilde{J}^{-}_{(q,n,u)}=\bigcup_{l\in\tilde{\mathcal{J}}_E} C_{\bar{n}-(l+1)/2},$$

where the union is disjoint and

$$\tilde{\mathcal{J}}_E=\left\{\begin{array}{l} j_{\bar{m}}q^{\bar{m}}+q^{\bar{m}}-q+j_0: \\ 0\leq \text{ even } j_{\bar{m}}\leq u-1,\\ q-u\leq \text{ odd } j_0\leq q-1 \end{array}\right\}.$$

Moreover,

$$|\tilde{J}^{+}_{(q,n,u)}\cap \tilde{J}^{-}_{(q,n,u)}|=\begin{cases} u^2m/4, & \textit{if } u \textit{ is even;}\\ (u+1)^2m/4, & \textit{if } u \textit{ is odd.}\end{cases}$$

Proof: We are going to find all the integers i and j with $1\leq i\leq uq^{\bar{m}}$ and $1\leq j\leq uq^{\bar{m}}$ such that

$$C_{\bar{n}+i}=C_{\bar{n}-j}.$$

This is equivalent to

$$(2i+1)+(2j-1)q^{\ell}\equiv 0 \pmod{n}$$

for some $1\leq \ell\leq m-1$. Recall that in Remark 21, for $m\geq 2$ being even, the integers $1\leq i_1, j_1\leq uq^{\bar{m}}$ satisfying

$$i_1+j_1q^{\ell}\equiv 0 \pmod{n}$$

have been characterized. Using this result, we can further characterize the odd integers i_1 and i_2 satisfying $i_1=2i+1$, $j_1=2j-1$ such that

$$C_{\bar{n}+(i_1-1)/2}=C_{\bar{n}-(j_1+1)/2}.$$

As a consequence, we have $\tilde{J}^{+}_{(q,n,u)}\cap\tilde{J}^{-}_{(q,n,u)}=\bigcup_{l\in\tilde{\mathcal{J}}_E}C_{\bar{n}-(l+1)/2}$. By Proposition 9, each $l\in\tilde{\mathcal{J}}_E$ is a coset leader and $|C_{\bar{n}-l}|=m$. In particular, when $m=2$, we need $1\leq u\leq\frac{q}{2}$ to ensure that each $l\in\tilde{\mathcal{J}}_E$ is a coset leader and $|C_{\bar{n}-l}|=m$. The remaining part of the proof follows from Remark 21 by employing a straightforward calculation. □

Theorem 42: Let $m\geq 2$ *be an even integer,* q *even, and* $\delta=uq^{\frac{m}{2}}/2+1$*. Suppose*

$$\begin{cases} 1\leq u\leq \frac{q}{2} & \textit{if } m=2\\ 1\leq u\leq q-1 & \textit{if } m\geq 4 \end{cases}$$

1) *If* u *is even, then* $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ *has length* n*, dimension*
$$k=q^m-1-(uq^{\frac{m}{2}}-u^2/2)m,$$
and minimum distance $d\geq 2\delta-1$.
2) *If* u *is odd, then* $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ *has length* n*, dimension*
$$k=q^m-1-(uq^{\frac{m}{2}}-(u^2+1)/2)m,$$
and minimum distance $d\geq 2\delta-1$.

Proof: The desired conclusion follows from Theorem 39, Proposition 41, and the BCH bound. □

Example 43:

1) *When* $(q,m,u)=(2,4,1)$ *in the above theorem, the code* $C_{(2,15,5,6)}$ *has parameters* $[15,3,5]$*, which are the best possible parameters for cyclic codes* [13, pp. 247].
2) *When* $(q,m,u) = (4,4,1),(4,4,2),(4,4,3)$ *in the above theorem, the code* $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ *has parameters* $[255,195,17]$, $[255,135,d\geq 33]$, *and* $[255,83,d\geq 49]$*, respectively.*

Corollary 44: When $u=1$ *and* $\delta=q^{\frac{m}{2}}/2+1$*, the true minimum distance of the code* $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ *presented in Theorem 42 is equal to* $2\delta-1$.

Proof: Note that $b=\frac{n+1}{2}-\delta+1$. It is easy to check that $(2\delta-1)\mid\gcd(n,b-1)$ in this case. The desired result then follows from Corollary 4. □

C. Parameters of $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ *With Designed Distance* q^t-1*, Where* $1\leq t\leq\bar{m}$

When q is even, the parameters of the LCD code $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ are described in the following theorem if it has designed distance $2\delta-1=q^t-1$ for an integer t with $1\leq t\leq\bar{m}$.

Theorem 45: Let q *be even,* $m\geq 2$ *and* $m\neq 3$*. Suppose that* $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ *has designed distance* $2\delta-1=q^t-1$*, where* $1\leq t\leq\bar{m}$*. Then* $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ *has length* n*, dimension*

$$k=\begin{cases} q^m-1-(q^{\frac{m+1}{2}}-q)m & \textit{if } m\geq 5 \textit{ is odd and } t=\frac{m+1}{2},\\ q^m-1-(q^t-2)m & \textit{otherwise,}\end{cases}$$

and minimum distance $d\geq q^t-1$.

Proof: Set $\delta=\frac{q^t}{2}$. Recall that the generator polynomial of the code $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ is $g_{(q,n,2\delta-1,\frac{n+1}{2}-(\delta-1))}(x)$. By Lemma 5, we have

$$\begin{aligned}&\deg(g_{(q,n,2\delta-1,\frac{n+1}{2}-(\delta-1))}(x))\\ &\quad=(q^t-2)m-\left|\left(\bigcup_{1\leq j\leq\delta-1}C_{\bar{n}+j}\right)\bigcap\left(\bigcup_{0\leq j\leq\delta-2}C_{\bar{n}-j}\right)\right|.\end{aligned}$$

When $m \geq 5$ is odd, the integers $1 \leq i_1, j_1 \leq uq^{\bar{m}}$ satisfying

$$i_1 + j_1 q^{\ell} \equiv 0 \pmod{n}$$

have been characterized in Remark 17. Using this result, we can show that

$$\left(\bigcup_{0\leq j\leq\delta-2} C_{\bar{n}+j}\right) \bigcap \left(\bigcup_{1\leq j\leq\delta-1} C_{\bar{n}-j}\right) = \begin{cases} \bigcup_{j\in J'}(C_{\bar{n}+(j-1)/2} \cup C_{\bar{n}-(j+1)/2}) & \text{if } t = \frac{m+1}{2}, \\ \emptyset & \text{if } 1 \leq t \leq \frac{m-1}{2}, \end{cases}$$

where $J' = \{j_{\bar{m}-1}q^{\bar{m}-1} + q^{\bar{m}-1} - 1 : 2 \leq \text{ even } j_{\bar{m}-1} \leq q-2\}$.

When $m \geq 2$ is even, by Proposition 29, for $1 \leq t \leq \frac{m}{2}$, we have

$$\left(\bigcup_{0\leq j\leq\delta-2} C_{\bar{n}+j}\right) \bigcap \left(\bigcup_{1\leq j\leq\delta-1} C_{\bar{n}-j}\right) = \emptyset.$$

Therefore, we have

$$\left|\left(\bigcup_{0\leq j\leq\delta-2} C_{\bar{n}+j}\right) \bigcap \left(\bigcup_{1\leq j\leq\delta-1} C_{\bar{n}-j}\right)\right| = \begin{cases} (\frac{q}{2}-1)2m & \text{if } m \geq 5 \text{ is odd and } t = \frac{m+1}{2}, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, the dimension is obtained. Moreover, the minimum distance $d \geq q^t - 1$ follows from the BCH bound. □

We remark that the minimum distance of the code $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ given in Theorem 45 may be larger than $q^t - 1$.

Example 46: 1) *When* $(q, m, t) = (2, 7, 2), (2, 7, 3), (2, 7, 4)$ *in the above theorem,* $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ *has parameters* $[127, 113, 5]$*,* $[127, 85, 11]$*, and* $[127, 29, 37]$ *with designed distance* 3*,* 7*, and* 15*, respectively.*

2) *When* $(q, m, t) = (2, 6, 2), (2, 6, 3)$ *in the above theorem, the code* $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ *has parameters* $[63, 51, 3]$*, and* $[63, 27, 7]$.

VII. PARAMETERS OF LCD BCH CODE $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$

In this section, we investigate the parameters of the LCD BCH code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$. We use notation as in Equation (1).

A. The Dimension of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ When δ is Relatively Small

Every positive integer s with $0 \leq s \leq n$ has a unique q-adic expansion as $s = \sum_{i=0}^{m-1} s_i q^i$, where $0 \leq s_i \leq q-1$. The q-adic expansion sequence of $s = \sum_{i=0}^{m-1} s_i q^i$ is denoted by $\overline{s} = (s_{m-1}, s_{m-2}, \ldots, s_0)$. Below, we simply call the q-adic expansion sequence of s as the sequence of s, whenever this causes no confusion. The weight of $\overline{s}$ is defined to be the number of nonzero entries among the entries s_i of $\overline{s}$ and denoted by $wt(\overline{s})$. Define the support of $\overline{s}$ as

$$\mathrm{supp}(\overline{s}) = \{0 \leq i \leq m-1 : s_i \neq 0\}.$$

For the sake of simplicity, we use the notation

$$\overline{s} = (0, \ldots, 0, \underset{j_1}{a}, \ldots, \underset{j_2}{a}, \underset{j_2-1}{b}, \underset{j_2-2}{c}, \ldots, c)$$

to represent a sequence $\overline{s} = (s_{m-1}, s_{m-2}, \ldots, s_0)$ with $s_i = 0$ for $j_1 + 1 \leq i \leq m-1$, $s_i = a$ for $j_2 \leq i \leq j_1$, $s_i = b$ for $i = j_2 - 1$ and $s_i = c$ for $0 \leq i \leq j_2 - 2$. This kind of notation will be used below and can be interpreted in a similar way.

Lemma 47: Let $m \geq 2$*. Then the following holds.*

1) *When* m *is odd, for* $1 \leq i, j \leq q^{(m+1)/2}$*,* $-j \in C_i$ *if and only if*

$$\begin{cases} \overline{i} = (0, \ldots, 0, \underset{\frac{m-1}{2}}{q-1}, \ldots, \underset{1}{q-1}, u), \\ \overline{j} = (0, \ldots, 0, \underset{\frac{m-1}{2}}{q-1-u}, \underset{\frac{m-3}{2}}{q-1}, \ldots, q-1), \end{cases}$$

or

$$\begin{cases} \overline{i} = (0, \ldots, 0, \underset{\frac{m-1}{2}}{q-1-u}, \underset{\frac{m-3}{2}}{q-1}, \ldots, q-1), \\ \overline{j} = (0, \ldots, 0, \underset{\frac{m-1}{2}}{q-1}, \ldots, \underset{1}{q-1}, u), \end{cases}$$

where $0 \leq u \leq q-1$.

2) *When* m *is even and* $q > 2$*, for* $1 \leq i, j \leq 2q^{m/2}$*,* $-j \in C_i$ *if and only if*

$$\begin{cases} \overline{i} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, \underset{\frac{m}{2}-1}{q-1}, \ldots, q-1, q-2), \\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, \underset{\frac{m}{2}-1}{q-1}, \ldots, q-1, q-2), \end{cases}$$

or

$$\begin{cases} \overline{i} = (0, \ldots, 0, \underset{\frac{m}{2}-1}{q-1}, \ldots, \underset{1}{q-1}, q-2), \\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, \underset{\frac{m}{2}-1}{q-1}, \ldots, q-1), \end{cases}$$

or

$$\begin{cases} \overline{i} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, \underset{\frac{m}{2}-1}{q-1}, \ldots, q-1), \\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}-1}{q-1}, \ldots, \underset{1}{q-1}, q-2), \end{cases}$$

or

$$\begin{cases} \overline{i} = (0, \ldots, 0, \underset{\frac{m}{2}-1}{q-1}, \ldots, q-1), \\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}-1}{q-1}, \ldots, q-1). \end{cases}$$

3) *When* m *is even and* $q = 2$*, for* $1 \leq i, j \leq 2^{(m/2)+1}$*,* $-j \in C_i$ *if and only if*

$$\begin{cases} \overline{i} = (0, \ldots, 0, \underset{\frac{m}{2}-2}{1}, \ldots, 1), \\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, \ldots, 1), \end{cases}$$

or

$$\begin{cases} \overline{i} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, \ldots, 1), \\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}-2}{1}, \ldots, 1), \end{cases}$$

or

$$\begin{cases}\overline{i} = (0, \ldots, 0, \underset{\frac{m}{2}-1}{1}, \ldots, 1),\\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}-1}{1}, \ldots, 1),\end{cases}$$

or

$$\begin{cases}\overline{i} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, 0, 1, \ldots, 1),\\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, \ldots, 1, 0, 1),\end{cases}$$

or

$$\begin{cases}\overline{i} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, \ldots, 1, 0, 1),\\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, 0, 1, \ldots, 1).\end{cases}$$

Proof: 1) If $-j \in C_i$, then there exists an l with $0 \le l \le m-1$, such that $q^l i + j \equiv 0 \pmod{n}$. Hence,

$$\overline{q^l i + j} = (q-1, q-1, \ldots, q-1).$$

Since $m = wt(\overline{q^l i + j}) \le wt(\overline{i}) + wt(\overline{j}) \le m+1$, we have $\{wt(\overline{i}), wt(\overline{j})\} = \{\frac{m-1}{2}, \frac{m+1}{2}\}$ or $\{wt(\overline{i}), wt(\overline{j})\} = \{\frac{m+1}{2}\}$. If $\{wt(\overline{i}), wt(\overline{j})\} = \{\frac{m-1}{2}, \frac{m+1}{2}\}$, then clearly, $\text{supp}(\overline{q^l i}) \cap \text{supp}(\overline{j}) = \emptyset$. Otherwise, if $\text{supp}(\overline{q^l i}) \cap \text{supp}(\overline{j}) \neq \emptyset$, there is at least one entry in $\overline{q^l i + j}$, which is not $q-1$. Hence, $\overline{q^l i}$ and $\overline{j}$ must have the following two forms

$$\overline{q^l i} = (\underset{m-1}{q-1}, \ldots, \underset{\frac{m+1}{2}}{q-1}, 0, \ldots, 0),\ \overline{j} = (0, \ldots, 0, \underset{\frac{m-1}{2}}{q-1}, \ldots, q-1),$$

or

$$\overline{q^l i} = (\underset{m-1}{q-1}, \ldots, \underset{\frac{m-1}{2}}{q-1}, 0, \ldots, 0),\ \overline{j} = (0, \ldots, 0, \underset{\frac{m-3}{2}}{q-1}, \ldots, q-1),$$

If $\{wt(\overline{i}), wt(\overline{j})\} = \{\frac{m+1}{2}\}$, then clearly, $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\overline{j})| \ge 1$. If $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\overline{j})| > 1$, then there is at least one entry in $\overline{q^l i + j}$, which is not $q-1$. Hence, $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\overline{j})| = 1$. Therefore, $\overline{q^l i}$ and $\overline{j}$ must have the following $2q-4$ forms

$$\begin{cases}\overline{q^l i} = (\underset{m-1}{q-1}, \ldots, q-1, \underset{\frac{m+1}{2}}{u}, 0, \ldots, 0),\\ \overline{j} = (0, \ldots, 0, \underset{\frac{m-1}{2}}{q-1-u}, \underset{\frac{m-3}{2}}{q-1}, \ldots, q-1),\end{cases}$$

or

$$\begin{cases}\overline{q^l i} = (\underset{m-1}{q-1}, \ldots, q-1, \underset{\frac{m+1}{2}}{\ }\underset{\frac{m-1}{2}}{0}, \ldots, 0, u),\\ \overline{j} = (0, \ldots, 0, \underset{\frac{m-1}{2}}{q-1}, \ldots, q-1, q-1-u),\end{cases}$$

where $1 \le u \le q-2$. Therefore, the conclusion follows.

2) If $-j \in C_i$, then there exists an l with $0 \le l \le m-1$, such that $q^l i + j \equiv 0 \pmod{n}$. Hence,

$$\overline{q^l i + j} = (q-1, q-1, \ldots, q-1).$$

Since $m = wt(\overline{q^l i + j}) \le wt(\overline{i}) + wt(\overline{j}) \le m+2$, we must have

$$\{wt(\overline{i}), wt(\overline{j})\} = \begin{cases}\{\frac{m}{2}+1\}, \text{ or}\\ \{\frac{m}{2}, \frac{m}{2}+1\}, \text{ or}\\ \{\frac{m}{2}-1, \frac{m}{2}+1\}, \text{ or}\\ \{\frac{m}{2}\}.\end{cases}$$

If $\{wt(\overline{i}), wt(\overline{j})\} = \{\frac{m}{2}+1\}$, then $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\overline{j})| = 2$. Hence, $\overline{q^l i}$ and $\overline{j}$ must have the following form

$$\begin{cases}\overline{q^l i} = (\underset{m-1}{q-1}, \ldots, \underset{\frac{m}{2}+1}{q-1}, \underset{\frac{m}{2}}{q-2}, \underset{\frac{m}{2}-1}{0}, \ldots, 0, 1),\\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, \underset{\frac{m}{2}-1}{q-1}, \ldots, q-1, q-2).\end{cases}$$

If $\{wt(\overline{i}), wt(\overline{j})\} = \{\frac{m}{2}, \frac{m}{2}+1\}$, then $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\overline{j})| = 1$. Hence, $\overline{q^l i}$ and $\overline{j}$ must have the following two forms

$$\begin{cases}\overline{q^l i} = (\underset{m-1}{q-1}, \ldots, \underset{\frac{m}{2}+1}{q-1}, \underset{\frac{m}{2}}{q-2}, 0, \ldots, 0),\\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}}{1}, \underset{\frac{m}{2}-1}{q-1}, \ldots, q-1),\end{cases}$$

or

$$\begin{cases}\overline{q^l i} = (\underset{m-1}{q-1}, \ldots, \underset{\frac{m}{2}}{q-1}, \underset{\frac{m}{2}-1}{0}, \ldots, 0, 1),\\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}-1}{q-1}, \ldots, \underset{1}{q-1}, q-2).\end{cases}$$

If $\{wt(\overline{i}), wt(\overline{j})\} = \{\frac{m}{2}-1, \frac{m}{2}+1\}$, then $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\overline{j})| = 0$. Hence, there is at least one entry in $\overline{(q^l i + j)}$ which is not equal to $q-1$. If $\{wt(\overline{i}), wt(\overline{j})\} = \{\frac{m}{2}\}$, then $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\overline{j})| = 0$. Hence, $\overline{q^l i}$ and $\overline{j}$ must have the following form

$$\begin{cases}\overline{i} = (\underset{m-1}{q-1}, \ldots, \underset{\frac{m}{2}}{q-1}, 0, \ldots, 0),\\ \overline{j} = (0, \ldots, 0, \underset{\frac{m}{2}-1}{q-1}, \ldots, q-1).\end{cases}$$

Therefore, the conclusion follows.

3) The proof is similar to that of 2) and is omitted here. □

As a consequence, we have the following proposition.

Proposition 48: Let $m \ge 2$.

1) *Suppose m is odd. Then*

$$|\{(cl(i), cl(j)) : -j \in C_i, 1 \le i, j \le l\}| = \begin{cases}0 & \text{if } 1 \le l \le q^{(m+1)/2} - q,\\ 2h & \text{if } l = q^{(m+1)/2} - q + h,\ 1 \le h \le q-2,\\ 2(q-1) & \text{if } q^{(m+1)/2} - 1 \le l \le q^{(m+1)/2}.\end{cases}$$

2) *Suppose m is even and $q > 2$. Then*

$$|\{(cl(i), cl(j)) : -j \in C_i, 1 \le i, j \le l\}| = \begin{cases}0 & \text{if } 1 \le l \le q^{m/2} - 2,\\ 1 & \text{if } q^{m/2} - 1 \le l \le 2q^{m/2} - 3,\\ 2 & \text{if } l = 2q^{m/2} - 2,\\ 4 & \text{if } 2q^{m/2} - 1 \le l \le 2q^{m/2}.\end{cases}$$

3) *Suppose $m \geq 4$ is even and $q = 2$. Then*

$$\begin{aligned}&|\{(cl(i), cl(j)) : -j \in C_i, 1 \leq i, j \leq l\}|\\ &= \begin{cases} 0 & \textit{if } 1 \leq l \leq 2^{m/2} - 2,\\ 1 & \textit{if } 2^{m/2} - 1 \leq l \leq 2^{(m/2)+1} - 4,\\ 3 & \textit{if } 2^{(m/2)+1} - 3 \leq l \leq 2^{(m/2)+1} - 2,\\ 5 & \textit{if } 2^{(m/2)+1} - 1 \leq l \leq 2^{(m/2)+1}.\end{cases}\end{aligned}$$

Combining Lemma 5 and Proposition 48, we have the following theorem.

Theorem 49: Let $m \geq 2$. Let δ be an integer satisfying

$$\begin{cases} 2 \leq \delta \leq q^{(m+1)/2} + 1 & \textit{if } m \textit{ is odd},\\ 2 \leq \delta \leq 2q^{m/2} + 1 & \textit{if } m \textit{ is even}.\end{cases}$$

Let δ_q and δ_0 be the unique integers such that $\delta - 1 = \delta_q q + \delta_0$, where $0 \leq \delta_0 < q$. Then $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ has parameters $[q^m - 1, k, d \geq 2\delta]$, in which the dimension k is given below.

1) *When m is odd,*

$$k = \begin{cases} q^m - 2 - 2m(\delta_q(q-1) + \delta_0)\\ \qquad\qquad \textit{if } \delta \leq q^{(m+1)/2} - q,\\ q^m - 2 - 2m(q^{(m-1)/2} - 1)(q - 1)\\ \textit{if } q^{(m+1)/2} - q + 1 \leq \delta \leq q^{(m+1)/2} + 1.\end{cases}$$

2) *When m is even and $q > 2$,*

$$k = \begin{cases} q^m - 2 - 2m(\delta_q(q-1) + \delta_0)\\ \qquad\qquad \textit{if } \delta \leq q^{m/2} - 1,\\ q^m - 2 - 2m(\delta_q(q-1) + \delta_0 - \frac{1}{2})\\ \qquad\qquad \textit{if } q^{m/2} \leq \delta \leq q^{m/2} + 1,\\ q^m - 2 - 2m(\delta_q(q-1) + \delta_0 - 1)\\ \qquad\qquad \textit{if } q^{m/2} + 2 \leq \delta \leq 2q^{m/2} - 2,\\ q^m - 2 - 2m(\delta_q(q-1) + \delta_0 - \frac{3}{2})\\ \qquad\qquad \textit{if } \delta = 2q^{m/2} - 1,\\ q^m - 2 - 2m(\delta_q(q-1) + \delta_0 - \frac{5}{2})\\ \qquad\qquad \textit{if } 2q^{m/2} \leq \delta \leq 2q^{m/2} + 1.\end{cases}$$

3) *When $m \geq 4$ is even and $q = 2$,*

$$k = \begin{cases} 2^m - 2 - 2m(\delta_q + \delta_0)\\ \qquad\qquad \textit{if } \delta \leq 2^{m/2} - 1 \textit{ and } m \geq 4,\\ 2^m - 2 - 2m(\delta_q + \delta_0 - \frac{1}{2})\\ \qquad\qquad \textit{if } 2^{m/2} \leq \delta \leq 2^{m/2} + 1 \textit{ and } m \geq 4,\\ 2^m - 2 - 2m(\delta_q + \delta_0 - 1)\\ \qquad \textit{if } 2^{m/2} + 2 \leq \delta \leq 2^{(m/2)+1} - 3 \textit{ and } m \geq 4,\\ 2^m - 2 - 2m(\delta_q + \delta_0 - 2)\\ \textit{if } 2^{(m/2)+1} - 2 \leq \delta \leq 2^{(m/2)+1} - 1 \textit{ and } m \geq 6,\\ 2^m - 2 - 2m(\delta_q + \delta_0 - 3)\\ \qquad \textit{if } 2^{(m/2)+1} \leq \delta \leq 2^{(m/2)+1} + 1 \textit{ and } m \geq 6.\end{cases}$$

In addition, the minimum distance d of the code satisfies $d \geq 2\delta$.

TABLE I

SOME OPTIMAL BINARY CODE $\mathcal{C}_{(2,n,\delta,n-\delta+1)}$ WITH $d = 2\delta$

m	δ
{5,6,7}	{3}
{8,9,10,11,12,13}	{3,5}
{14,15,17,17,18,19}	{3,5,7}
{20}	{3,5,7,9}

Proof: Let $\overline{g}_{(q,m,\delta)}(x)$ be the generator polynomial of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$. For the dimension of the code, we only prove 2) since the proofs of 1) and 3) are similar. By 2) of Lemma 5, the degree of $\overline{g}_{(q,m,\delta)}(x)$ equals

$$\begin{aligned}1 + 2m(\delta_q(q-1) + \delta_0) - \epsilon m&\\ - |\{(cl(i), cl(j)) : -j \in C_i, 1 \leq i, j \leq \delta - 1\}|m&,\end{aligned}$$

where

$$\epsilon = \begin{cases} 0 & \text{if } \delta \leq q^{m/2} + 1,\\ 1 & \text{if } \delta \geq q^{m/2} + 2.\end{cases}$$

With this conclusion on the degree of the generator polynomial and Proposition 48, we have

$$\begin{aligned}&\deg(\overline{g}_{(q,m,\delta)}(x))\\ &= \begin{cases} 1 + 2m(\delta_q(q-1) + \delta_0) \text{ if } \delta \leq q^{m/2} - 1,\\ 1 + 2m(\delta_q(q-1) + \delta_0 - \frac{1}{2}) \text{ if } q^{m/2} \leq \delta \leq q^{m/2} + 1,\\ 1 + 2m(\delta_q(q-1) + \delta_0 - 1) \text{ if } q^{m/2} + 2 \leq \delta \leq 2q^{m/2} - 2,\\ 1 + 2m(\delta_q(q-1) + \delta_0 - \frac{3}{2}) \text{ if } \delta = 2q^{m/2} - 1,\\ 1 + 2m(\delta_q(q-1) + \delta_0 - \frac{5}{2}) \text{ if } 2q^{m/2} \leq \delta \leq 2q^{m/2} + 1.\end{cases}\end{aligned}$$

Therefore, the conclusion on the dimension in 2) follows. Moreover, by the BCH bound, $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ has minimum distance $d \geq 2\delta$. □

Remark 50: For the code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$, if

$$\sum_{i=0}^{\delta} \binom{n}{i} (q-1)^i > q^{n-k}, \tag{22}$$

then $d \leq 2\delta$ by the sphere packing bound. Therefore, knowledge of the dimension of the code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ may provide more precise information on the minimum distance in some cases. As an illustration, we use Theorem 49 and the inequality (22) to get some binary codes $\mathcal{C}_{(2,n,\delta,n-\delta+1)}$ with $d = 2\delta$, which are listed in Table I. Note that the codes listed in Table I is optimal in the sense that given the length and dimension, the minimum distance is the largest possible. According to Inequality (22), increasing their minimum distances is impossible due to the sphere packing bound.

Remark 51: Theorem 49 gives the dimension of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ when δ is relatively small, in which δ is approximately the square root of the length n. In this case, the size of each cyclotomic coset containing i, where $-\delta \leq i \leq \delta$, follows form Lemma 5. Moreover, Lemma 47 characterizes all $1 \leq i, j \leq \delta$ satifying $-j \in C_i$. For a larger δ, the size of cyclotomic cosets, as well as the cases in which $-j \in C_i$, become much more complicated. Hence, from this viewpoint, it is difficult to extend the result of Theorem 49 to a larger δ.

Remark 52: Since when q is odd, $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ and $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ are monomially equivalent, Theorem 49 also gives the dimension of $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ for $2 \leq \delta \leq q^{(m+1)/2}$

when m is odd and for $2 \leq \delta \leq 2q^{m/2} + 1$ when m is even. Moreover, Theorem 26 is also a direct consequence of Theorem 49.

Due to the equivalence between $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ and $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ when q is even, the following theorem follows immediately from Theorems 18 and 22.

Theorem 53: Let q be odd and $\delta = uq^{\bar{m}} + 1$, where

$$\begin{cases} 1 \leq u \leq \frac{q-1}{2} & \text{if } m = 2, \\ 1 \leq u \leq q-1 & \text{if } m \geq 4. \end{cases}$$

1) *When $m \geq 5$ is an odd integer, the code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ has length n, dimension*

$$k = q^m - 2 - 2(uq^{\frac{m-1}{2}} - 2u^2 + u)(q-1)m,$$

and minimum distance $d \geq 2\delta$.

2) *When $m \geq 2$ is an even integer, the code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ has length n, dimension*

$$k = q^m - 2 - 2uq^{\frac{m}{2}-1}(q-1)m + (2u^2 - 2u + 1)m,$$

and minimum distance $d \geq 2\delta$.

B. The Dimension of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ When $\delta = q^\lambda$ and $\frac{m}{2} \leq \lambda \leq m-1$

In [23], the dimension of the narrow-sense primitive BCH code $\mathcal{C}_{(q,n,\delta,1)}$ with $\delta = q^\lambda$ was considered. The author derived two closed formulas concerning the dimension of such code. In this subsection, we use the idea in [23] to give an estimate of the dimension of the LCD BCH code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ with $\delta = q^\lambda$, where $\frac{m}{2} \leq \lambda \leq m-1$.

Let s and r be two positive integers. Given a sequence of length s and a fixed integer a with $0 \leq a \leq q-1$, we say that the sequence contains a straight run of length r with respect to a, if it has r consecutive entries formed by a. If we view the sequence as a circle where the first and last entry are glued together, we say that the sequence contains a circular run of length r with respect to a, if this circle has r consecutive entries formed by a. When the specific choice of the integer a does not matter, we simply say that the sequence has a straight or circular run of length r. Clearly, a straight run is also a circular run but the converse is not necessarily true. We use $l_r(s)$ to denote the number of sequences of length s, which contains a straight run of length r. Particularly, we define $l_r(0) = 0$. The following is a recursive formula of $l_r(s)$ which was presented in [23].

Result 54 [23, p. 155]: Let s and r be two nonnegative integers. Then

$$l_r(s) = \begin{cases} 0 \text{ if } 0 \leq s < r, \\ 1 \text{ if } s = r, \\ ql_r(s-1) + (q-1)(q^{s-r-1} - l_r(s-r-1)) \text{ if } s > r. \end{cases}$$

Throughout the rest of this section, we always assume that $\delta = q^\lambda$ and $\frac{m}{2} \leq \lambda \leq m-1$. Recall that the narrow-sense primitive BCH code $\mathcal{C}_{(q,n,\delta,1)}$ has generator polynomial $g_{(q,n,\delta,1)}(x)$. Set $r = m - \lambda$. Note that $\delta - 1$ corresponds to following sequence

$$\overline{\delta - 1} = (0, \ldots, 0, \underset{\lambda-1}{q-1}, q-1, \ldots, q-1).$$

The key observation in [23] is that for $1 \leq i \leq n-1$, α^i is a root of $g_{(q,n,\delta,1)}(x)$ if and only if the sequence of i has a circular run of length at least r with respect to 0. Similarly, note that $n - \delta + 1$ corresponds to the following sequence

$$\overline{n - \delta + 1} = (q-1, \ldots, q-1, \underset{\lambda-1}{0}, 0, \ldots, 0).$$

Therefore, for $1 \leq i \leq n-1$, α^i is a root of $g_{(q,n,\delta,n-\delta+1)}(x)$ if and only if the sequence of i has a circular run of length at least r with respect to $q-1$. The following proposition presents the degree of $g_{(q,n,\delta,1)}(x)$ and $g_{(q,n,\delta,n-\delta+1)}(x)$.

Result 55 [23, p. 155]: Set $r = m - \lambda$. Then

$$\deg(g_{(q,n,\delta,1)}(x)) = \deg(g_{(q,n,\delta,n-\delta+1)}(x)) = l_r(m) - 1$$
$$+ (q-1)^2 \sum_{u=0}^{r-2} (r-u-1)(q^{m-r-u-2} - l_r(m-r-u-2)).$$

We have the following estimation on the dimension of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$.

Theorem 56: Set $r = m - \lambda$. Then $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ has parameters $[q^m - 1, k, d \geq 2\delta]$, where

$$k \geq q^m - 2l_r(m) + 2l_r(m-r)$$
$$-2(q-1)^2 \sum_{u=0}^{r-2} (r-u-1)(q^{m-r-u-2} - l_r(m-r-u-2)),$$

and

$$k \leq q^m - 2l_r(m) + ml_r(m-r)$$
$$-2(q-1)^2 \sum_{u=0}^{r-2} (r-u-1)(q^{m-r-u-2} - l_r(m-r-u-2)).$$

Proof: Since $\lambda \geq \frac{m}{2}$, we have $m \geq 2r$. Define a set $N = \{1 \leq i \leq n-1 : g_{(q,n,\delta,1)}(\alpha^i) = g_{(q,n,\delta,n-\delta+1)}(\alpha^i) = 0\}$. Since $g_{(q,n,2\delta,n-\delta+1)}(x) = (x-1)\text{lcm}(g_{(q,n,\delta,1)}(x), g_{(q,n,\delta,n-\delta+1)}(x))$, we have

$$\deg(g_{(q,n,2\delta,n-\delta+1)}(x))$$
$$= \deg(g_{(q,n,\delta,1)}(x)) + \deg(g_{(q,n,\delta,n-\delta+1)}(x)) + 1 - |N|.$$

Since $\deg(g_{(q,n,\delta,1)}(x))$ and $\deg(g_{(q,n,\delta,n-\delta+1)}(x))$ are known by Result 55, it suffices to estimate the size of N. N contains the number $1 \leq i \leq n-1$, such that $\bar{i}$ contains two runs of length r with respect to 0 and $q-1$, where at most one of them is a circular run. Let N' be the set of integers $1 \leq i \leq n-2$ such that the first r entries of $\bar{i}$ is a straight run of length r with respect to 0 and the last $m-r$ entries contain a straight run of length r with respect to $q-1$. Clearly, we have $|N'| = l_r(m-r)$. Note that each element of N is a proper cyclic shift of an element of N'. Moreover, for each $i \in N'$, we have

$$2 \leq |\{q^j i \bmod n : 0 \leq j \leq m-1\}| \leq m,$$

which implies

$$2|N'| \leq |N| \leq m|N'|.$$

Thus, the conclusion follows from a direct computation. □

C. The Minimum Distance of LCD BCH Codes $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$

While it is difficult to determine the dimension of LCD BCH codes in general, it is more difficult to find out the minimum distance of LCD BCH codes. For the code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$, the BCH bound $d \geq 2\delta$ is usually very tight. But it would be better if we could determine the minimum distance exactly. In this section, we determine the minimum distance d of the code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ in some special cases.

Given a codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}_{(q,n,\delta,1)}$, we say c is reversible if $(c_{n-1}, c_{n-2}, \ldots, c_0) \in \mathcal{C}_{(q,n,\delta,1)}$. Namely, $c \in \mathcal{C}_{(q,n,\delta,1)}$ is reversible if and only if $c \in \tilde{\mathcal{C}}_{(q,n,2\delta,n-\delta+1)}$. The following theorem says that the reversible codeword in $\mathcal{C}_{(q,n,\delta,1)}$ provides some information on the minimum distance on $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$.

Theorem 57: Let $c(x) \in \mathcal{C}_{(q,n,\delta,1)}$ be a reversible codeword of weight w. If $c(1) \neq 0$, then $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ contains a codeword $(x-1)c(x)$ whose weight is at most $2w$. Therefore the minimum distance d of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ satisfies $d \leq 2w$. In particular, if the weight of $c(x)$ is δ, then the minimum distance $d = 2\delta$.

Proof: Since $c(x)$ is reversible and $c(1) \neq 0$, we have $(x-1)c(x) \in \mathcal{C}_{(q,n,2\delta,n-\delta+1)}$. The weight of $(x-1)c(x)$ is at most $2w$, which implies $d \leq 2w$. In particular, if $w = \delta$, together with the BCH bound, we have $d = 2\delta$. □

Let $c(x) = \sum_{i=0}^{n-1} c_i x^i$ be a codeword of a cyclic code $\mathcal{C}$ with length n. We can use the elements of $\mathrm{GF}(q^m)^*$ to index the coefficients of $c(x)$. Similarly, let $\overline{\mathcal{C}}$ be the extended cyclic code of $\mathcal{C}$ and let $\overline{c(x)} = \sum_{i=0}^{n} c_i x^i$ be a codeword of $\overline{\mathcal{C}}$ with length q^m. We can use the elements of $\mathrm{GF}(q^m)$ to index the coefficients of $\overline{c(x)}$. The support of $c(x)$ (resp. $\overline{c(x)}$) is defined to be the set of elements in $\mathrm{GF}(q^m)^*$ (resp. $\mathrm{GF}(q^m)$), which corresponds to the nonzero coefficients of $c(x)$ (resp. $\overline{c(x)}$).

Given a prime power q and an integer $0 \leq s \leq q^m - 1$, s has a unique q-adic expansion $s = \sum_{i=0}^{m-1} s_i q^i$. The q-weight of s is defined to be $wt_q(s) = \sum_{i=0}^{m-1} s_i$. Suppose H is a subset of $\mathrm{GF}(q)^*$. Then we use $H^{(-1)}$ to denote the subset $\{h^{-1} : h \in H\}$.

The following are two classes of LCD BCH codes whose minimum distances are known.

Corollary 58: For the LCD BCH code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$, we have $d = 2\delta$ if $\delta \mid n$.

Proof: It suffices to find a codeword $c(x)$ satisfying the condition in Theorem 57. If $\delta \mid n$, by the proof of [31, Theorem], $\mathcal{C}_{(q,n,\delta,1)}$ contains a reversible codeword $c(x)$ with weight δ, where $c(x) = \sum_{i=0}^{\delta-1} a_i x^{\frac{ni}{\delta}}$ and $c(1) \neq 0$. The desired conclusion then follows from Theorem 57. □

Corollary 59: Let $\delta = 2^r - 1$ and V be an m-dimensional vector space over $\mathrm{GF}(2)$. *Suppose $1 \leq r \leq \lfloor \frac{m}{2} \rfloor$. Then we can choose four r-dimensional subspaces of V, say H_i, $1 \leq i \leq 4$ of V, such that $H_1 \cap H_2 = \{0\}$ and $H_3 \cap H_4 = \{0\}$. If $((H_1 \cup H_2) \setminus \{0\})^{(-1)} = (H_3 \cup H_4) \setminus \{0\}$, then the LCD BCH code $\mathcal{C}_{(2,n,\delta,n-\delta+1)}$ has parameters $[2^m - 1, 2^m - 2 - 2m(2^{r-1} - 1), 2\delta]$.*

Proof: The dimension of $\mathcal{C}_{(2,n,\delta,n-\delta+1)}$ easily follows from Theorem 49. We are going to show that the minimum distance $d = 2\delta$. Define $\mathcal{C}_{(2,n,\delta,1)}$ (resp. $\mathcal{C}_{(2,n,\delta,n-\delta+1)}$) to be the BCH code with length $n = 2^m - 1$ and generator polynomial $g_{(2,n,\delta,1)}(x)$ (resp. $g_{(2,n,\delta,n-\delta+1)}(x)$). Let α be a primitive element of $\mathrm{GF}(2^m)$. We can assume the zeros of $\mathcal{C}_{(2,n,\delta,1)}$ (resp. $\mathcal{C}_{(2,n,\delta,n-\delta+1)}$) include the elements $\{\alpha^i : 1 \leq i \leq \delta - 1\}$ (resp. $\{\alpha^{-i} : 1 \leq i \leq \delta - 1\}$).

The BCH code $\mathcal{C}_{(2,n,\delta,1)}$ (resp. $\mathcal{C}_{(2,n,\delta,n-\delta+1)}$) contains the punctured Reed-Muller code $\mathrm{RM}^+(m-r,m)^*$ (resp. $\mathrm{RM}^-(m-r,m)^*$) as a subcode, in which $\mathrm{RM}^+(m-r,m)^*$ has zeros

$$\{\alpha^i : 0 < i < 2^m - 1, wt_2(i) < r\},$$

and $\mathrm{RM}^-(m-r,m)^*$ has zeros

$$\{\alpha^{-i} : 0 < i < 2^m - 1, wt_2(i) < r\}.$$

Let $c = (c_0, c_1, \ldots, c_{n-1})$ be a codeword of $\mathrm{RM}^+(m-r,m)^*$. Since $\mathrm{RM}^+(m-r,m)^*$ is a cyclic code, its coordinates can be indexed in the following way

$$c = (\underset{1}{c_0}, \underset{\alpha}{c_1}, \ldots, \underset{\alpha^{n-1}}{c_{n-1}}), \tag{23}$$

where $\sum_{j=0}^{n-1} c_j \alpha^{ij} = 0$ for each $1 \leq i \leq \delta - 1$. Similarly, suppose $c' = (c'_0, c'_1, \ldots, c'_{n-1})$ is a codeword of $\mathrm{RM}^-(m-r,m)^*$. Then, its coordinates can be indexed in the following way

$$c' = (\underset{1}{c'_0}, \underset{\alpha^{-1}}{c'_1}, \ldots, \underset{\alpha^{-(n-1)}}{c'_{n-1}}), \tag{24}$$

where $\sum_{j=0}^{n-1} c'_j \alpha^{-ij} = 0$ for each $1 \leq i \leq \delta - 1$.

By [2, Corollary 5.3.3], $\mathrm{RM}^+(m-r,m)^*$ contains two minimum weight codewords $c_1(x)$ and $c_2(x)$, such that the support of $c_1(x)$ and $c_2(x)$ are $H_1 \setminus \{0\}$ and $H_2 \setminus \{0\}$ respectively. Similarly, $\mathrm{RM}^-(m-r,m)^*$ contains two minimum weight codewords $c_3(x)$ and $c_4(x)$, such that the support of $c_3(x)$ and $c_4(x)$ are $H_3 \setminus \{0\}$ and $H_4 \setminus \{0\}$ respectively. Moreover, the coordinates of $c_1(x)$ and $c_2(x)$ are arranged in the way of (23) and the coordinates of $c_3(x)$ and $c_4(x)$ are arranged in the way of (24). Therefore,

$$c_1(x) + c_2(x) \in \mathrm{RM}^+(m-r,m)^* \subset \mathcal{C}_{(2,n,\delta,1)},$$

and

$$c_3(x) + c_4(x) \in \mathrm{RM}^-(m-r,m)^* \subset \mathcal{C}_{(2,n,\delta,n-\delta+1)}.$$

Since $((H_1 \cup H_2) \setminus \{0\})^{(-1)} = (H_3 \cup H_4) \setminus \{0\}$, by the arrangement of the coordinates of $c_i(x)$, $1 \leq i \leq 4$, the two codewords $c_1(x) + c_2(x)$ and $c_3(x) + c_4(x)$ coincide. Thus, we have $c_1(x) + c_2(x) \in \tilde{\mathcal{C}}_{(2,n,\delta,n-\delta+1)}$. Since $c_1(1) + c_2(1) = 0$, we have a codeword $c_1(x) + c_2(x) \in \mathcal{C}_{(2,n,\delta,n-\delta+1)}$ with weight 2δ. □

Example 60: Let $q = 2$, $m = 5$ and $\delta = 3$ in the above corollary. We are going to show that $\mathcal{C}_{(2,31,6,29)}$ has parameters $[31, 20, 6]$. *Note that the dimension of $\mathcal{C}_{(2,31,6,29)}$ easily follows from Theorem 49, it suffices to prove that the minimum distance is equal to* 6. *Let α be a primitive element of* $\mathrm{GF}(2^5)$ *and the minimal polynomial of α over* $\mathrm{GF}(2)$ *is* $x^5 + x^2 + 1$. *Then we have the following four* 2*-dimensional* *subspaces of* GF(2^5)*:*

$$\begin{aligned}H_1 &= \{0, \alpha, \alpha^2, \alpha^{19}\},\\ H_2 &= \{0, \alpha^8, \alpha^{12}, \alpha^{18}\},\\ H_3 &= \{0, \alpha^{12}, \alpha^{13}, \alpha^{30}\},\\ H_4 &= \{0, \alpha^{19}, \alpha^{23}, \alpha^{29}\}.\end{aligned}$$

Thus, we have $c_1(x)$ and $c_2(x)$ as codewords of $\mathcal{C}_{(2,31,3,1)}$, whose supports are $H_1 \setminus \{0\}$ and $H_2 \setminus \{0\}$. We have $c_3(x)$ and $c_4(x)$ as codewords of $\mathcal{C}_{(2,31,3,29)}$, whose supports are $H_3 \setminus \{0\}$ and $H_4 \setminus \{0\}$. Clearly, $((H_1 \cup H_2) \setminus \{0\})^{(-1)} = (H_3 \cup H_4) \setminus \{0\}$. Therefore, $c_1(x) + c_2(x)$ coincides with $c_3(x) + c_4(x)$, whose weight is six. Consequently, $c_1(x) + c_2(x) \in \mathcal{C}_{(2,31,6,29)}$ and the minimum distance of $\mathcal{C}_{(2,31,6,29)}$ equals 6*.*

Based on our numerical experiment, we have the following conjecture, which can be regarded as an analogy of [24, Ch. 9, Th. 5].

Conjecture 61: Let $\delta = q^\lambda - 1$, where $1 \le \lambda \le \lfloor m/2 \rfloor$. Then the code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ has minimum distance $d = 2\delta$.

D. Parameters of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ for Small δ

In this section, we determine the parameters of the code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ for a few small values of δ. With the help of Theorem 49 and Corollary 58, we can achieve this in some cases.

Recall that the Melas code over GF(q) is a cyclic code with length n and generator polynomial $m_{-1}(x)m_1(x)$ and was first studied by Melas for the case $q = 2$ [27]. The weight distribution of the Melas code has been obtained for $q = 2, 3$ [18], [29]. For $\delta = 2$, the code $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ is the even-like subcode of the Melas code. The following theorem is a direct consequence of Theorem 49 and Corollary 58.

Theorem 62: Suppose q is odd and $m \ge 2$, then $\mathcal{C}_{(q,n,4,n-1)}$ has parameters $[q^m - 1, q^m - 2 - 2m, 4]$.

When $\delta = 3$, we have the following result.

Theorem 63: 1) *When $q = 2$ and $m \ge 4$, $\mathcal{C}_{(q,n,6,n-2)}$ has parameters $[2^m - 1, 2^m - 2 - 2m, 6]$.*

2) *When $q^m \equiv 1 \pmod 3$ and $m \ge 4$, $\mathcal{C}_{(q,n,6,n-2)}$ has parameters $[q^m - 1, q^m - 2 - 4m, 6]$.*

Proof: 1) The dimension follows from Theorem 49. Applying the BCH and the sphere packing bound, we can see that the minimum distance is 6.

2) The dimension follows from Theorem 49. Since $q^m \equiv 1 \pmod 3$, we have $3 \mid n$. Therefore, by Corollary 58, the minimum distance is 6. □

Theorem 64: Suppose $m \ge 3$, then $\mathcal{C}_{(3,n,8,n-3)}$ has parameters $[3^m - 1, 3^m - 2 - 4m, d]$, where $d = 8$ if m is even and $d \ge 8$ if m is odd.

Proof: It follows from Theorem 49 that the dimension of this code is equal to $q^m - 2 - 4m$. By the BCH bound, the minimum distance of $\mathcal{C}_{(3,n,8,n-3)}$ is at least 8.

When m is even, 4 divides n. Hence, the minimum distance of $\mathcal{C}_{(3,n,8,n-3)}$ is equal to 8 according to Corollary 58. □

We have the following conjecture concerning the case $q = 3$.

Conjecture 65: When $q = 3$, $m \ge 3$ is odd and $\delta = 4$, $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ has minimum distance $d = 8$.

Example 66: Let $q = 3$, $m = 3$ and $\delta = 4$ in Theorem 64. Then $\mathcal{C}_{(3,26,8,n-3)}$ has parameters $[26, 13, 8]$. According to [13, p. 300, Table A.92]*, all known ternary linear codes with length* 26 *and dimension* 13 *have minimum distance at most* 8*. Hence, $\mathcal{C}_{(3,n,8,n-3)}$ has the same parameters as the best known linear code.*

VIII. Concluding Remarks

The main contributions of this paper are the following:

1) In Propositions 6 and 9, the characterization of the coset leaders of q-cyclotomic cosets C_j modulo $n = q^m - 1$, where $1 \le j \le (q-1)q^{\bar{m}}$. The size of these cyclotomic cosets was also computed.
2) In Theorems 18, 22, 35 and 42, the determination of the dimension of the LCD BCH codes $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ and $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ with $\delta = uq^{\bar{m}} + 1$ if q is odd and with $\delta = uq^{\bar{m}}/2 + 1$ if q is even, where $m \ge 4$ and $1 \le u \le q - 1$.
3) In Theorems 26 and 45, the determination of the dimension of the LCD BCH codes $\mathcal{C}_{(q,n,2\delta,\frac{n}{2}-\delta+1)}$ and $\mathcal{C}_{(q,n,2\delta-1,\frac{n+1}{2}-\delta+1)}$ when it has designed distance $q^t - 1$, where $1 \le t \le \bar{m}$.
4) In Theorem 49, the determination of the dimension of the LCD BCH codes $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$, with $2 \le \delta \le q^{(m+1)/2}$ when m is odd and with $2 \le \delta \le 2q^{m/2}$ when m is even.
5) In Theorem 53, the determination of the dimension of the LCD BCH codes $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$, with q being odd, $m \ge 4$, $\delta = uq^{\bar{m}} + 1$ and $1 \le u \le q - 1$.
6) In Theorem 56, the derivation of lower and upper bounds on the dimension of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$, where $\delta = q^\lambda$ and $\frac{m}{2} \le \lambda \le m - 1$.
7) In Theorem 57 and Corollaries 58 and 59, the determination of the minimum distance of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ in some special cases.
8) In Theorems 62, 63 and 64, the determination of the parameters of $\mathcal{C}_{(q,n,2\delta,n-\delta+1)}$ when δ is small.

For the two families of LCD BCH codes considered in this paper, we were able to determine their dimensions when δ is relatively small, which is approximately the square root of the length of the code. When δ goes larger, it is much more complicated to compute the size of cyclotomic cosets and to characterize the coset leaders. Hence, there seems no obvious way to extend our results to a larger δ.

Acknowledgements

The authors are very grateful to the reviewers and the Associate Editor, Prof. Chaoping Xing, for their detailed comments and suggestions that much improved the presentation and quality of this paper.

References

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical BCH codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1183–1188, Mar. 2007.

[2] E. F. Assmus and J. D. Key, *Designs and Their Codes*. Cambridge, U.K.: Cambridge Univ. Press, 1992.

[3] D. Augot, P. Charpin, and N. Sendrier, “Studying the locator polynomials of minimum weight codewords of BCH codes,” *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 960–973, May 1992.

[4] D. Augot and N. Sendrier, “Idempotents and the BCH bound,” *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 204–207, Jan. 1994.

[5] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann, *Error-Correcting Linear Codes: Classification by Isometry and Applications*. Berlin, Germany: Springer-Verlag, 2006.

[6] E. R. Berlekamp, *Algebraic Coding Theory: Revised Edition*. Hackensack, NJ, USA: World Scientific, 2015.

[7] E. R. Berlekamp, “The enumeration of information symbols in BCH codes,” *Bell Syst. Tech. J.*, vol. 46, no. 8, pp. 1861–1880, Oct. 1967.

[8] K. Boonniyom and S. Jitman. (May 2016). “Complementary dual subfield linear codes over finite fields.” [Online]. Available: https://arxiv.org/abs/1605.06827

[9] C. Carlet and S. Guilley, “Complementary dual codes for counter-measures to side-channel attacks,” *Adv. Math. Commun.*, vol. 10, no. 1, pp. 131–150, 2016.

[10] P. Charpin, “On a class of primitive BCH-codes,” *IEEE Trans. Inf. Theory*, vol. 36, no. 1, pp. 222–228, Jan. 1990.

[11] P. Charpin, “Open problems on cyclic codes,” in *Handbook of Coding Theory*, vol. 1, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, pp. 963–1063.

[12] Y. Dianwu and H. Zhengming, “On the dimension and minimum distance of BCH codes over GF(q),” *J. Electron.*, vol. 13, no. 3, pp. 216–221, 1996.

[13] C. Ding, *Codes From Difference Sets*. Singapore: World Scientific, 2015.

[14] C. Ding, “Parameters of several classes of BCH codes,” *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5322–5330, Oct. 2015.

[15] C. Ding, X. Du, and Z. Zhou, “The Bose and minimum distance of a class of BCH codes,” *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2351–2356, May 2015.

[16] S. T. Dougherty, J.-L. Kim, B. Özkaya, L. Sok, and P. Solé, “The combinatorics of LCD codes: Linear programming bound and orthogonal matrices,” *Int. J. Inf. Coding Theory*, vol. 4, nos. 2–3, pp. 116–128, Jan. 2017.

[17] M. Esmaeili and S. Yari, “On complementary-dual quasi-cyclic codes,” *Finite Fields Appl.*, vol. 15, no. 3, pp. 375–386, 2009.

[18] G. van der Geer, R. Schoof, and M. van der Vlugt, “Weight formulas for ternary Melas codes,” *Math. Comput.*, vol. 58, no. 198, pp. 781–792, 1992.

[19] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[20] T. Kasami and S. Lin, “Some results on the minimum weight of primitive BCH codes (Corresp.),” *IEEE Trans. Inf. Theory*, vol. 18, no. 6, pp. 824–825, Nov. 1972.

[21] C. Li, C. Ding, and S. Li, “LCD cyclic codes over finite fields,” *IEEE Trans. Inf. Theory*, vol. 63, no. 7, pp. 4344–4356, Jul. 2017.

[22] S. Li, C. Ding, M. Xiong, and G. Ge. (Nov. 2016). “Narrow-sense BCH codes over $GF(q)$ with length $n = \frac{q^{m-1}}{q-1}$.” [Online]. Available: https://arxiv.org/abs/1603.07009

[23] H. B. Mann, “On the number of information symbols in Bose–Chaudhuri codes,” *Inf. Control*, vol. 5, no. 2, pp. 153–162, 1962.

[24] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[25] J. L. Massey, “Reversible codes,” *Inf. Control*, vol. 7, no. 3, pp. 369–380, 1964.

[26] J. L. Massey, “Linear codes with complementary duals,” *Discrete Math.*, vols. 106–107, pp. 337–342, Sep. 1992.

[27] C. M. Melas, “A cyclic code for double error correction,” *IBM J. Res. Develop.*, vol. 4, no. 3, pp. 364–366, 1960.

[28] S. K. Muttoo and S. Lal, “A reversible code over $GF(q)$,” *Kybernetika*, vol. 22, no. 1, pp. 85–91, 1986.

[29] R. Schoof and M. van der Vlugt, “Hecke operators and the weight distributions of certain codes,” *J. Combinat. Theory A*, vol. 57, no. 2, pp. 163–186, 1991.

[30] N. Sendrier, “Linear codes with complementary duals meet the Gilbert–Varshamov bound,” *Discrete Math.*, vol. 285, nos. 1–3, pp. 345–347, 2004.

[31] K. Tzeng and C. Hartmann, “On the minimum distance of certain reversible cyclic codes,” *IEEE Trans. Inf. Theory*, vol. 16, no. 5, pp. 644–646, Sep. 1970.

[32] X. Yang and J. L. Massey, “The condition for a cyclic code to have a complementary dual,” *Discrete Math.*, vol. 126, nos. 1–3, pp. 391–393, 1994.

[33] D.-W. Yue and G.-Z. Feng, “Minimum cyclotomic coset representatives and their applications to BCH codes and Goppa codes,” *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2625–2628, Nov. 2000.

Shuxing Li received the Ph.D. degree in mathematics in 2016 from Zhejiang University, Hangzhou, Zhejiang, P. R. China. From November 2014 to July 2016, He was a research assistant at the Department of Mathematics, The Hong Kong University of Science and Technology, Hong Kong. He is now a postdoctoral fellow at the Department of Mathematics, Simon Fraser University, Burnaby, British Columbia, Canada. His research interests include algebraic coding theory, combinatorial design theory, algebraic combinatorics, and their interactions.

Chengju Li received the Ph.D. in 2014 from Nanjing University of Aeronautics and Astronautics, Nanjing, China. From March 2015 to February 2016, he was a postdoctoral researcher in the Department of Mathematics, Korea Advanced Institute of Science and Technology, Daejeon, Korea. From March 2016 to August 2016, he held a postdoctoral position in the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong. He is currently an associate professor at East China Normal University, China. His research interests include exponential sums and coding theory.

Cunsheng Ding (M’98–SM’05) was born in 1962 in Shaanxi, China. He received the M.Sc. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xian, China; and the Ph.D. in 1997 from the University of Turku, Turku, Finland.

From 1988 to 1992 he was a Lecturer of Mathematics at Xidian University, China. Before joining the Hong Kong University of Science and Technology in 2000, where he is currently a Professor of Computer Science and Engineering, he was an Assistant Professor of Computer Science at the National University of Singapore.

His research fields are combinatorial designs, cryptography and coding theory. He has coauthored four research monographs, and served as a guest editor or editor for ten journals. Dr. Ding co-received the State Natural Science Award of China in 1989.

Hao Liu received the B.Sc. degree in mathematics in 2014 from Tsinghua University, Beijing, P. R. China. He is currently a Ph.D. candidate at the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong, P. R. China. His research interests include coding theory and combinatorial designs.