The Dual Codes of Several Classes of BCH Codes

Binkai Gong, Cunsheng Ding, *Senior Member, IEEE*, and Chengju Li

***Abstract*—As a special subclass of cyclic codes, BCH codes have wide applications in communication and storage systems. A BCH code of length n over $\mathbb{F}_q$ is always relative to an n-th primitive root of unity β in an extension field of $\mathbb{F}_q$, and is called a dually-BCH code if its dual is also a BCH code relative to the same β. The question as to whether a BCH code is a dually-BCH code is in general very hard to answer. In this paper, an answer to this question for primitive narrow-sense BCH codes and projective narrow-sense ternary BCH codes is given. Sufficient and necessary conditions in terms of the designed distances δ will be presented to ensure that these BCH codes are dually-BCH codes. In addition, the parameters of the primitive narrow-sense BCH codes and their dual codes are investigated. Some lower bounds on minimum distances of the dual codes of primitive and projective narrow-sense BCH codes are developed. Especially for binary primitive narrow-sense BCH codes, the new bounds on the minimum distances of the dual codes improve the classical Sidel'nikov bound, and are also better than the Carlitz and Uchiyama bound for large designed distances δ. The question as to what subclasses of cyclic codes are BCH codes is also answered to some extent. As a byproduct, the parameters of some subclasses of cyclic codes are also investigated.**

***Index Terms*—BCH code, cyclic code, linear code.**

I. Introduction

THROUGHOUT this paper, let $\mathbb{F}_q$ denote the finite field of order q, where q is a power of a prime p. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum (Hamming) distance d. The (Euclidean) dual code of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined by

$$\mathcal{C}^\perp = \{\mathbf{b} \in \mathbb{F}_q^n : \mathbf{b}\mathbf{c}^T = 0 \ \forall \ \mathbf{c} \in \mathcal{C}\},$$

where $\mathbf{b}\mathbf{c}^T$ denotes the standard inner product of the two vectors $\mathbf{b}$ and $\mathbf{c}$.

A linear code $\mathcal{C}$ is said to be cyclic if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. By identifying each vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ with

$$c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]/\langle x^n - 1\rangle,$$

a code $\mathcal{C}$ of length n over $\mathbb{F}_q$ corresponds to a subset of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Then $\mathcal{C}$ is a cyclic code if and only if the corresponding subset is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Note that every ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is principal. Then there is a monic polynomial $g(x)$ of the smallest degree such that $\mathcal{C} = \langle g(x)\rangle$ and $g(x) \mid (x^n - 1)$. Then $g(x)$ is called the generator polynomial and $h(x) = (x^n - 1)/g(x)$ is referred to as the check polynomial of $\mathcal{C}$.

We always assume that $\gcd(n, q) = 1$ in this paper. Denote $m = \mathrm{ord}_n(q)$, i.e., m is the smallest positive integer such that $q^m \equiv 1 \pmod{n}$. Let α be a primitive element of $\mathbb{F}_{q^m}$ and put $\beta = \alpha^{\frac{q^m-1}{n}}$. Then β is a primitive n-th root of unity. The set $T = \{0 \le i \le n-1 : g(\beta^i) = 0\}$ is referred to as the defining set of $\mathcal{C}$ with respect to β. It is clear that the generator polynomial of the cyclic code $\mathcal{C}$ can be derived from its defining set and the corresponding β. Thus the code is determined once the defining set and β are given. Denote $T^{-1} = \{n - t : i \in T\}$. Then the defining set of the dual code $\mathcal{C}^\perp$ with respect to β is $\mathbb{Z}_n \setminus T^{-1}$.

For an integer b and an integer δ with $2 \le \delta \le n$, define

$$g_{(q,n,\delta,b)}(x) = \mathrm{lcm}\Big(\mathbb{M}_{\beta^b}(x), \mathbb{M}_{\beta^{b+1}}(x), \ldots, \mathbb{M}_{\beta^{b+\delta-2}}(x)\Big), \quad (1)$$

where $\mathbb{M}_{\beta^i}(x)$ denotes the minimal polynomial of β^i over $\mathbb{F}_q$ and lcm denotes the least common multiple of these polynomials. Let $\mathcal{C}_{(q,n,\delta,b)}$ denote the cyclic code of length n over $\mathbb{F}_q$ 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 with respect to β. We call $\mathcal{C}_{(q,n,\delta,b)}$ a narrow-sense BCH code if $b = 1$ and for convenience we will use $\mathcal{C}_{(q,n,\delta)}$ in the sequel. When $n = \frac{q^m-1}{q-1}$, $\mathcal{C}_{(q,n,\delta,b)}$ is called a projective BCH code. It follows from the BCH bound for cyclic codes that the minimum distance of $\mathcal{C}_{(q,n,\delta,b)}$ is greater than or equal to the designed distance δ.

A cyclic code $\mathcal{C}$ over $\mathbb{F}_q$ with length n is called a BCH code if there are an n-th primitive root of unity β in $\mathbb{F}_{q^m}$, an integer δ with $2 \le \delta \le n+1$, and an integer b such that the generator polynomial of $\mathcal{C}$ can be expressed as the polynomial $g_{(q,n,\delta,b)}(x)$ in (1). BCH codes form a subclass of cyclic codes, and are very attractive in both theory and practice. Consequently, the following question is quite interesting.

Question 1: When is a cyclic code a BCH code?

By definition, if the generator polynomial of a cyclic code is irreducible, then the cyclic code is a BCH code with designed distance 2. However, Question 1 is hard to answer in general. Our interest in this question comes from the fact that the largest designed distance (called the Bose distance) of a BCH code may be a very tight estimation of the minimum distance of the BCH code. If we are able to prove that a cyclic code $\mathcal{C}$

Manuscript received June 22, 2021; accepted October 29, 2021. Date of publication November 8, 2021; date of current version January 20, 2022. The work of Binkai Gong and Chengju Li was supported in part by the National Natural Science Foundation of China under Grant 12071138 and in part by the Shanghai Chenguang Program under Grant 18CG22. The work of Cunsheng Ding was supported by the Hong Kong Research Grants Council under Grant 16302121. *(Corresponding author: Chengju Li.)*

Binkai Gong and Chengju Li are with the Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai 200062, China, and also with the State Key Laboratory of Cryptology, Beijing 100878, China (e-mail: 51205902050@stu.ecnu.edu.cn; cjli@sei.ecnu.edu.cn).

Cunsheng Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong (e-mail: cding@ust.hk).

Communicated by G. Matthews, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2021.3125933

is a BCH code with designed distance δ, we will know that $\mathcal{C}$ has minimum distance at least δ. We will answer Question 1 for some subclasses of cyclic codes in Section III.

It is well-known that the dual codes of cyclic codes are also cyclic. Then we have the following question.

Question 2: When is the dual code of a BCH code still a BCH code?

This is a very hard question in general, although it may be answered for some special BCH codes. If the dual of a BCH code is still a BCH code, then the BCH bound may be a tight lower bound on the minimum distance of the dual code. This explains why we are interested in Question 2. Since Question 2 is very hard to answer, we are interested in the following question:

Question 3: When is the dual code of a BCH code over $\mathbb{F}_q$ with respect to an n-th primitive root of unity β still a BCH code with respect to β?

If the dual of a BCH code $\mathcal{C}$ over $\mathbb{F}_q$ with respect to an n-th primitive root of unity β is still a BCH code with respect to β, we call $\mathcal{C}$ a *dually-BCH code*. If a cyclic code $\mathcal{C}$ is a dually-BCH code, by definition $\mathcal{C}^{\perp}$ must be a BCH code. If a cyclic code $\mathcal{C}$ is not a dually-BCH code, $\mathcal{C}^{\perp}$ could still be a BCH code. Hence, Question 3 is in general easier than Question 2.

We are very much interested in dually-BCH codes, as the BCH bound may give a very tight lower bound on the minimum distance of their dual codes and binary BCH codes of length between 7 and 125 are always the best cyclic codes except two special cases [8, Appendix A]. This is the main motivation of this paper. In the past 55 years, a lot of progress on the study of BCH cyclic codes has been made, but little is known about the minimum distances of the duals of BCH codes. We refer the reader to [2]–[4], [6], [7], [9], [10], [13], [15]–[18], [20], [21], [23], [24] and references therein for known results on BCH codes.

In this paper, we will answer Question 1 for some subclasses of cyclic codes. In addition, we will answer Question 3 for the codes $\mathcal{C}_{(q,q^m-1,\delta)}$ and $\mathcal{C}_{(3,\frac{3^m-1}{2},\delta)}$, where $2 \leq \delta \leq n$. Sufficient and necessary conditions in terms of the designed distance δ are given to ensure that these codes are dually-BCH codes. In addition, we will investigate the parameters of these narrow-sense dually-BCH codes and their dual codes. Some lower bounds on the minimum distances of $\mathcal{C}^{\perp}_{(q,q^m-1,\delta)}$ and $\mathcal{C}^{\perp}_{(q,(q^m-1)/(q-1),\delta)}$ are developed. Especially for the binary codes $\mathcal{C}_{(2,2^m-1,\delta)}$, our new bounds on the minimum distances of the dual codes improve the classical Sidel'nikov bound, and are also better than the Carlitz and Uchiyama bound for large designed distances δ.

In this paper, the tables of best known linear codes, maintained at http://www.codetables.de/, are referred to as the *Database*. All examples of codes presented in this paper are computed by Magma.

II. Preliminaries

In this section, we introduce some results on coset leaders and BCH codes, which will be employed later. For more information on BCH codes, we refer the reader to [22] and [5].

A. Coset Leaders

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

$$C_s = \{s, sq, sq^2, \ldots, sq^{l_s-1}\} \bmod n \subseteq \mathbb{Z}_n,$$

where l_s is the smallest positive integer such that $s \equiv sq^{l_s} \pmod{n}$, and is the size of the q-cyclotomic coset. The smallest integer in C_s is called the coset leader of C_s. Let $\Gamma_{(n,q)}$ be the set of all the coset leaders. We have then $C_s \cap C_t = \phi$ for any two distinct elements s and t in $\Gamma_{(n,q)}$, and

$$\bigcup_{s \in \Gamma_{(n,q)}} C_s = \mathbb{Z}_n.$$

Hence, the distinct q-cyclotomic cosets modulo n partition $\mathbb{Z}_n$.

For an integer i with $0 \leq i \leq q^m - 1$, let

$$i = i_{m-1}q^{m-1} + i_{m-2}q^{m-2} + \cdots + i_1 q + i_0$$

be the q-adic expansion of i, where $0 \leq i_j \leq q-1$ for $0 \leq j \leq m-1$. We will also write $i = (i_{m-1}, i_{m-2}, \ldots, i_1, i_0)_q$ and call it the q-adic expansion of i in the sequel. It is easy to obtain the q-cyclotomic coset leaders from the q-adic expansion when $n = q^m - 1$. The following two lemmas on coset leaders modulo $n = q^m - 1$ and $n = (q^m - 1)/(q - 1)$ will play an important role in the sequel.

Lemma 1: [11] The first three largest q-cyclotomic coset leaders modulo $n = q^m - 1$ are give as follows:

$$\delta_1 = (q-1)q^{m-1} - 1, \delta_2 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m-1}{2} \rfloor},$$
$$\delta_3 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m+1}{2} \rfloor}.$$

Lemma 2: [18] Let $q = 3$ and $m \geq 2$. The first largest coset leader modulo $n = (q^m - 1)/(q - 1)$ is

$$\delta_1 = q^{m-1} - 1 - \frac{q^{\lfloor (m-1)/2 \rfloor} - 1}{q - 1}.$$

B. Some Lemmas on BCH Codes

Charpin pointed out in [5] that it is a well-known hard problem to determine the minimum distance of BCH codes. So far, we have very limited knowledge of BCH codes, as the dimension and minimum distance of BCH codes are in general open. The following lemmas about the dimensions and minimum distances of primitive BCH codes and their dual codes will be employed later.

Lemma 3: [21] The dimension k of $\mathcal{C}_{(q,q^m-1,q^t)}$ is equal to

$$q^m - 1 - \sum_{i=1}^{\lfloor \frac{m}{r+1} \rfloor} \frac{(-1)^{i-1} m (q-1)^i}{i} \binom{m - ir - 1}{i - 1} q^{m - i(r+1)},$$

where $r = m - t$.

Lemma 4: [22] For any t with $1 \leq t \leq m - 1$, a primitive narrow-sense BCH code of length $n = q^m - 1$ and design distance $\delta = q^t - 1$ has minimum distance $d = q^t - 1$.

Lemma 5 (Carlitz-Uchiyama Bound, See [22]): Let $\mathcal{C}$ be a binary BCH code of length $2^m - 1$ and designed distance $2s+1$. Then $\mathcal{C}^\perp$ has minimum distance

$$d^\perp \geq 2^{m-1} - (s-1)2^{\frac{m}{2}}.$$

Lemma 6 (Sidel'nikov Bound, See [22]): Let $\mathcal{C}$ be a binary BCH code of length $2^m - 1$ and designed distance $2s+1$. Then $\mathcal{C}^\perp$ has minimum distance

$$d^\perp \geq 2^{m-1-\lfloor \log_2(2s-1) \rfloor}.$$

III. When Is a Cyclic Code a BCH Code?

We follow the notation introduced in Section I, and will give an answer to Question 1 for some special cyclic codes. Recall that $\gcd(n,q) = 1$, $m = \mathrm{ord}_n(q)$, $\beta = \alpha^{(q^m-1)/n}$ and α is a primitive element of $\mathbb{F}_{q^m}$. The following result is straightforward.

Theorem 7: Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_q$ with length n and generator polynomial $g(x)$. If $g(x)$ is irreducible over $\mathbb{F}_q$, then $\mathcal{C}$ is a BCH code with designed distance 2.

Theorem 8: Let $\mathcal{C}$ be the cyclic code over $\mathbb{F}_q$ with length n and generator polynomial $g(x) = \mathbb{M}_{\beta^i}(x)\mathbb{M}_{\beta^j}(x)$, where i and j are not in the same q-cyclotomic coset modulo n. Then $\mathcal{C}$ is a BCH code if and only if there exists an integer ℓ with $0 \leq \ell \leq m-1$ such that $\gcd(i - jq^\ell, n) = 1$.

Proof: Note that every n-th primitive root of unity β' must be of the form $\beta' = \beta^u$ with $\gcd(u,n) = 1$. By definition, $\mathcal{C}$ is a BCH code with designed distance 3 with respect to β' if and only if $ui - ujq^\ell \equiv \pm 1 \pmod{n}$ for an integer ℓ with $0 \leq \ell \leq m-1$, which holds if and only if $i - jq^\ell \equiv \pm u^{-1} \pmod{n}$ for an integer ℓ with $0 \leq \ell \leq m-1$. The desired conclusions then follow. ■

As a corollary of Theorem 8, we have the following.

Corollary 9: Let $\mathcal{C}$ be the cyclic code over $\mathbb{F}_q$ with length n and generator polynomial $g(x) = \mathbb{M}_{\beta^i}(x)\mathbb{M}_{\beta^j}(x)$, where i and j are not in the same q-cyclotomic coset modulo n. If n is a prime, then $\mathcal{C}$ is a BCH code.

Corollary 9 shows that cyclic codes of prime lengths are very interesting. The following is also a corollary of Theorem 8.

Corollary 10: Let $\mathcal{C}(j)$ be the cyclic code over $\mathbb{F}_q$ with length n and generator polynomial $g_j(x) = (x-1)\mathbb{M}_{\beta^j}(x)$, where $1 \leq j < n$. Then $\mathcal{C}(j)$ is a BCH code with designed distance 3 if and only if $\gcd(j,n) = 1$.

If $\gcd(j,n) = 1$, then $\mathcal{C}(j)$ has parameters $[n, n-m-1, d]$ with $d \geq 3$, and is permutation-equivalent to $C(1)$.

Proof: The conclusion of the first part follows from Theorem 8. We now prove the second conclusion. Since $\gcd(j,n) = 1$, $j(q^\ell - 1) \equiv 0 \pmod{n}$ for some ℓ with $1 \leq \ell \leq m$ if and only if $\ell = m$. Hence, the q-cyclotomic class C_j modulo n has size m. Consequently, the dimension of $\mathcal{C}(j)$ equals $n-(m+1)$. The conclusion of the first part and the BCH bound show that the minimum distance $d(\mathcal{C}(j)) \geq 3$. By Delsarte's theorem,

$$\mathcal{C}(j) = \{(\mathrm{Tr}_{q^m/q}(a\beta^{-ji}) + b)_{i=0}^{n-1} : a \in \mathbb{F}_{q^m},\ b \in \mathbb{F}_q\},$$

where $\mathrm{Tr}_{q^m/q}(x)$ denotes the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Clearly, $\pi_j(x) := xj \bmod n$ is a permutation of $\mathbb{Z}_n$, as $\gcd(j,n) = 1$. It is easily seen that $\pi_j(\mathcal{C}(1)) = \mathcal{C}(j)$. This completes the proof. ■

TABLE I

$\mathcal{C}(1)$ and $\mathcal{C}(1)^\perp$

q	$\mathcal{C}(1)$	Record code	$\mathcal{C}(1)^\perp$	Record code
2	$[15,10,4]$	$[15,10,4]$	$[15,5,7]$	$[15,5,7]$
2	$[17,8,6]$	$[17,8,6]$	$[17,9,5]$	$[17,9,5]$
2	$[31,25,4]$	$[31,25,4]$	$[31,6,15]$	$[31,6,15]$
2	$[33,22,6]$	$[33,22,6]$	$[33,11,11]$	$[33,11,11]$
3	$[26,22,3]$	$[26,22,3]$	$[26,4,17]$	$[26,4,17]$
3	$[28,21,4]$	$[28,21,4]$	$[28,7,12]$	$[28,7,12]$
3	$[80,75,3]$	$[80,75,3]$	$[80,5,53]$	$[80,5,53]$
3	$[82,73,4]$	$[82,73,5]$	$[82,9,44]$	$[82,9,48]$

TABLE II

$\mathcal{C}'((n-2)/2)$ and $\mathcal{C}'((n-2)/2)^\perp$

q	$\mathcal{C}'((n-2)/2)$	Record code	$\mathcal{C}'((n-2)/2)^\perp$	Record code
3	$[26,22,3]$	$[26,22,3]$	$[26,4,17]$	$[26,4,17]$
3	$[28,21,4]$	$[28,21,4]$	$[28,7,12]$	$[28,7,12]$
3	$[80,75,3]$	$[80,75,3]$	$[80,5,53]$	$[80,5,53]$
3	$[82,73,4]$	$[82,73,5]$	$[82,9,44]$	$[82,9,48]$
5	$[24,21,3]$	$[24,21,3]$	$[24,3,19]$	$[24,3,19]$
5	$[26,21,4]$	$[26,21,4]$	$[26,5,16]$	$[26,5,17]$

We remark that the lower bound that $d(\mathcal{C}(j)) \geq 3$ given in Corollary 10 is very general and is tight in certain cases. Such cyclic codes $\mathcal{C}(j)$ with generator polynomial $g_j(x) = (x-1)\mathbb{M}_{\beta^j}(x)$ have very good parameters in general, where $1 \leq j < n$ and $\gcd(j,n) = 1$, as they are BCH codes. Table I documents examples of $\mathcal{C}(1)$ and $\mathcal{C}(1)^\perp$, where the record linear code with same length and dimension is from the Database.

Similarly, we can prove the following.

Corollary 11: Let q be odd and let n be even. Let $\mathcal{C}'(j)$ be the cyclic code over $\mathbb{F}_q$ with length n and generator polynomial $g'_j(x) = (x+1)\mathbb{M}_{\beta^j}(x)$, where $1 \leq j < n$ and $j \neq n/2$. Then $\mathcal{C}'(j)$ is a BCH code if and only if there is an integer u such that $\gcd(u,n) = 1$ and $j = u(n \pm 2)/2 \bmod n$.

If there is an integer u such that $\gcd(u,n) = 1$ and $j = u(n \pm 2)/2 \bmod n$, then $\mathcal{C}'(j)$ has parameters $[n, n-m-1, d]$ with $d \geq 3$.

The cyclic codes $\mathcal{C}'((n \pm 2)/2)$ documented in Corollary 11 are very good in general, as they are BCH codes. Table II documents examples of $\mathcal{C}'((n-2)/2)$ and $\mathcal{C}'((n-2)/2)^\perp$, where the record linear code with same length and dimension is from the Database.

Theorem 12: Let $\mathcal{C}(0,i,j)$ denote the cyclic code over $\mathbb{F}_q$ with length n and generator polynomial $g_{(0,i,j)}(x) = (x-1)\mathbb{M}_{\beta^i}(x)\mathbb{M}_{\beta^j}(x)$, where i and j are not in the same q-cyclotomic coset modulo n and $\{i,j\} \subset \mathbb{Z}_n \setminus \{0\}$. Then $\mathcal{C}(0,i,j)$ is a BCH code if and only if one of the following sets of conditions is satisfied:

(a) $\gcd(i,n) = 1$ and $j = 2i \bmod n$;
(b) $\gcd(j,n) = 1$ and $i = 2j \bmod n$;
(c) $\gcd(i,n) = \gcd(j,n) = 1$ and $i + j \equiv 0 \pmod{n}$.

Proof: Let $\beta' = \beta^u$ with $\gcd(u,n) = 1$. Note that $u \times 0 = 0$. Then $\mathcal{C}(0,i,j)$ is a BCH code with designed distance

TABLE III

$\mathcal{C}(0,2,4)$ AND $\mathcal{C}(0,2,4)^{\perp}$

q	$\mathcal{C}(0,2,4)$	Record code	$\mathcal{C}(0,2,4)^{\perp}$	Record code
4	$[15,10,4]$	$[15,10,4]$	$[15,5,7]$	$[15,5,7]$
4	$[17,8,6]$	$[17,8,8]$	$[17,9,5]$	$[17,9,5]$
4	$[63,56,4]$	$[63,56,4]$	$[63,7,31]$	$[63,7,43]$
4	$[65,52,6]$	$[65,52,7]$	$[65,13,25]$	$[65,13,33]$

TABLE IV

$\mathcal{C}(0,1,n-1)$ AND $\mathcal{C}(0,1,n-1)^{\perp}$

q	$\mathcal{C}(0,1,n-1)$	Record code	$\mathcal{C}(0,1,n-1)^{\perp}$	Record code
2	$[15,6,6]$	$[15,6,6]$	$[15,9,4]$	$[15,9,4]$
2	$[17,8,6]$	$[17,8,6]$	$[17,9,5]$	$[17,9,5]$
2	$[31,20,6]$	$[31,20,6]$	$[31,11,10]$	$[31,11,11]$
2	$[33,22,6]$	$[33,22,6]$	$[33,11,11]$	$[33,11,11]$
3	$[26,19,4]$	$[26,19,5]$	$[26,7,12]$	$[26,7,14]$
3	$[28,21,4]$	$[28,21,4]$	$[28,7,12]$	$[28,7,12]$
3	$[80,71,4]$	$[80,71,5]$	$[80,9,42]$	$[80,9,47]$
3	$[82,73,4]$	$[82,73,5]$	$[82,9,44]$	$[82,9,48]$

4 with respect to β' if and only if one of the following sets of conditions is satisfied:

(1) $ui \equiv 1 \pmod{n}$ and $uj \equiv 2 \pmod{n}$;
(2) $ui \equiv 2 \pmod{n}$ and $uj \equiv 1 \pmod{n}$;
(3) $ui \equiv 1 \pmod{n}$ and $uj \equiv -1 \pmod{n}$;
(4) $ui \equiv -1 \pmod{n}$ and $uj \equiv 1 \pmod{n}$;
(5) $ui \equiv -1 \pmod{n}$ and $uj \equiv -2 \pmod{n}$;
(6) $ui \equiv -2 \pmod{n}$ and $uj \equiv -1 \pmod{n}$.

It is easily verified that both (1) and (5) are the same as (a), both (2) and (6) are the same as (b), and both (3) and (4) are the same as (c). This completes the proof. ∎

As a corollary of Theorem 11, we have the following results.

Corollary 13: Let $\mathcal{C}(0,i,j)$ denote the cyclic code over $\mathbb{F}_q$ with length n and generator polynomial $g_{(0,i,j)}(x) = (x-1)\mathbb{M}_{\beta^i}(x)\mathbb{M}_{\beta^j}(x)$, where i and j are not in the same q-cyclotomic coset modulo n and $\{i,j\} \subset \mathbb{Z}_n \setminus \{0\}$. If $\gcd(i,n) = 1$ and $j = 2i \bmod n$, then $\mathcal{C}(0,i,j)$ has parameters $[n, n-(\deg(\mathbb{M}_{\beta^j}(x)) + m + 1), d]$ with $d \geq 4$, where $\deg(\mathbb{M}_{\beta^j}(x)) = m$ provided that n is odd.

The cyclic codes documented in Corollary 13 have very good parameters in general, as they are BCH codes. Table III documents examples of $\mathcal{C}(0,2,4)$ and $\mathcal{C}(0,2,4)^{\perp}$ over $\mathbb{F}_4$, where the record linear code with same length and dimension is from the Database.

Corollary 14: Let $\mathcal{C}(0,i,n-i)$ denote the cyclic code over $\mathbb{F}_q$ with length n and generator polynomial $g_{(0,i,n-i)}(x) = (x-1)\mathbb{M}_{\beta^i}(x)\mathbb{M}_{\beta^{n-i}}(x)$, where i and $n-i$ are not in the same q-cyclotomic coset modulo n and $1 \leq i < n$. If $\gcd(i,n) = 1$, then $\mathcal{C}(0,i,n-i)$ has parameters $[n, n-(2m+1), d]$ with $d \geq 4$.

The cyclic codes documented in Corollary 14 have very good parameters in general, as they are BCH codes. Table IV documents examples of $\mathcal{C}(0,1,n-1)$ and $\mathcal{C}(0,1,n-1)^{\perp}$ over $\mathbb{F}_q$, where the record linear code with same length and dimension is from the Database.

If the generator polynomial $g(x)$ of a cyclic code $\mathcal{C}$ over $\mathbb{F}_q$ is the product of more distinct irreducible polynomials over $\mathbb{F}_q$ in general, it is harder to answer Question 1 for $\mathcal{C}$. The reader is cordially invited to answer Question 1 for other special subclasses of cyclic codes.

IV. Dual Codes of Binary Narrow-Sense BCH Codes of Length $2^m - 1$

In this section, we always assume that $n = 2^m - 1$, where $m \geq 2$. We follow the notation introduced in Section I. In this case, $\beta = \alpha$, which is a primitive element of $\mathbb{F}_{2^m}$. Let $\mathcal{C}_{(2,n,\delta)}$ be the primitive narrow-sense binary BCH code with designed distance δ, i.e., the defining set of $\mathcal{C}_{(2,n,\delta)}$ with respect to β is $T = C_1 \cup C_2 \cup \cdots \cup C_{\delta-1}$, where $2 \leq \delta \leq n$. Denote by $T^{\perp}$ the defining set of the dual code $\mathcal{C}_{(2,n,\delta)}^{\perp}$ with respect to β. It is clear that $T^{\perp} = \mathbb{Z}_n \setminus T^{-1}$ and $0 \in T^{\perp}$. We aim to investigate the parameters of the dual code $\mathcal{C}_{(2,n,\delta)}^{\perp}$ and present a characterization of $\mathcal{C}_{(2,n,\delta)}^{\perp}$ being a dually-BCH code. To this end, we will need the following lemma later.

Lemma 15: For $4 \leq \delta < 2^{m-1} - 2^{\lfloor \frac{m-1}{2} \rfloor}$, let $I(\delta) \geq 2$ be the integer such that $\{0,1,2,\ldots,I(\delta)-1\} \subseteq T^{\perp}$ and $I(\delta) \notin T^{\perp}$. Then we have $I(\delta) = 2^{m-t} - 1$ if $2^t \leq \delta < 2^{t+1}$ $(2 \leq t \leq m-3)$ and $I(\delta) = 3$ if $2^{m-2} \leq \delta < 2^{m-1} - 2^{\lfloor \frac{m-1}{2} \rfloor}$.

Proof: When $2^t \leq \delta < 2^{t+1}$ $(2 \leq t \leq m-3)$, it is easy to see that

$$2^m - 2^{m-t} = 2^{m-t}(2^t - 1) \in C_{2^t-1} \subseteq T.$$

Thus $2^{m-t} - 1 = n - (2^m - 2^{m-t}) \in T^{-1}$ and $2^{m-t} - 1 \notin T^{\perp} = \mathbb{Z}_n \setminus T^{-1}$.

Next we need to show that $\{0,1,2,\ldots,2^{m-t}-2\} \subseteq T^{\perp}$. It is clear that $0 \in T^{\perp}$. For every integer i with $1 \leq i \leq 2^{m-t} - 2$, we have $i = 2^{m-t} - u$, where $2 \leq u \leq 2^{m-t} - 1$. Note that

$$((u-1)2^t + 2^t - 1)2^{m-t} \equiv 2^m - 1 - 2^{m-t} + u \pmod{n}.$$

Thus $(u-1)2^t + 2^t - 1 \in C_{2^m-1-2^{m-t}+u} = C_{n-i}$. In addition, we have

$$(u-1)2^t + 2^t - 1 = (\underbrace{i_{m-1}, i_{m-2}, \ldots, i_t}_{m-t}, \underbrace{1, \ldots, 1}_{t})_2,$$

where $(i_{m-1}, i_{m-2}, \ldots, i_t) \neq (0,0,\ldots,0)$, i.e.,

$$Z = |\{i_j = 0 : t \leq j \leq m-1\}| \leq m - t - 1.$$

Note that

$$2^{t+1} - 2 = (\underbrace{0, \ldots, 0}_{m-t-1}, \underbrace{1, \ldots, 1}_{t}, 0)_2.$$

It then follows that

$$\mathrm{CL}(2^m - 1 - 2^{m-t} + u) > 2^{t+1} - 2 \geq \delta - 1,$$

where $\mathrm{CL}(2^m - 1 - 2^{m-t} + u)$ denotes the coset leader of the 2-cyclotomic coset containing $2^m - 1 - 2^{m-t} + u$. Hence $2^m - 1 - 2^{m-t} + u \notin T$ and $2^{m-t} - u \notin T^{-1}$. This leads to $i = 2^{m-t} - u \in T^{\perp}$. Consequently, we have $I(\delta) = 2^{m-t} - 1$.

When $2^{m-2} \leq \delta < 2^{m-1} - 2^{\lfloor \frac{m-1}{2} \rfloor}$, the desired conclusion can be similarly proved. We omit the details of the proof of this part here. ∎

TABLE V

$\mathcal{C}_{(2,n,\delta)}^{\perp}$ FOR $2 \le m \le 5$

m	δ	Is $\mathcal{C}_{(2,n,\delta)}$ dually-BCH?		m	δ	Is $\mathcal{C}_{(2,n,\delta)}$ dually-BCH?
2	$\delta = 2,3$	Yes		5	$2 \le \delta \le 3$	Yes
3	$2 \le \delta \le 7$	Yes			$4 \le \delta \le 5$	No
4	$2 \le \delta \le 3$	Yes			$6 \le \delta \le 7$	Yes
	$4 \le \delta \le 5$	No			$8 \le \delta \le 11$	No
	$6 \le \delta \le 15$	Yes			$12 \le \delta \le 31$	Yes

Proposition 16:

1) Let $m \ge 4$ be even. Then $\frac{2^m-1}{3} \in T^{\perp}$ is a coset leader modulo n if $4 \le \delta \le \frac{2^m-1}{3}$ and $2^{\frac{m}{2}}+1 \in T^{\perp}$ is a coset leader modulo n if $\frac{2^m-1}{3} < \delta < 2^{m-1} - 2^{\frac{m}{2}-1}$.
2) Let $m \ge 5$ be odd. Then $\frac{2^m+1}{3} \in T^{\perp}$ is a coset leader modulo n if $4 \le \delta \le \frac{2^{m-1}-1}{3}$ and $2^{\frac{m-1}{2}}+1 \in T^{\perp}$ is a coset leader modulo n if $\frac{2^{m-1}-1}{3} < \delta < 2^{m-1} - 2^{\frac{m-1}{2}}$.

Proof: We prove only the desired conclusions for the even m case, as the desired conclusions for the odd m case can be similarly proved. It is clear that $\frac{2^m-1}{3} = (0,1,0,1,\ldots,0,1)_2$ is the 2-cyclotomic coset leader of $C_{\frac{2(2^m-1)}{3}}$. Note that $n - \frac{2^m-1}{3} = \frac{2(2^m-1)}{3} = (1,0,1,0,\ldots,1,0)_2$. If $4 \le \delta \le \frac{2^m-1}{3}$, then we have

$$\mathrm{CL}\left(n - \frac{2^m-1}{3}\right) = \frac{2^m-1}{3} > \frac{2^m-1}{3} - 1 \ge \delta - 1.$$

Thus $n - \frac{2^m-1}{3} \notin T$ and $\frac{2^m-1}{3} \in T^{\perp}$.

It is also easy to see that $2^{\frac{m}{2}}+1 = (\underbrace{0,\ldots,0}_{\frac{m}{2}-1},1,\underbrace{0,\ldots,0}_{\frac{m}{2}-1},1)_2$ is the 2-cyclotomic coset leader of $C_{2^{\frac{m}{2}}+1}$. In addition, we have $n - (2^{\frac{m}{2}}+1) = 2^m - 2^{\frac{m}{2}} - 2 = (\underbrace{1,\ldots,1}_{\frac{m}{2}-1},0,\underbrace{1,\ldots,1}_{\frac{m}{2}-1},0)_2$. Then

$$\begin{aligned}\mathrm{CL}\left(n-(2^{\frac{m}{2}}-1)\right) &= (0,\underbrace{1,\ldots,1}_{\frac{m}{2}-1},0,\underbrace{1,\ldots,1}_{\frac{m}{2}-1})_2\\ &= 2^{m-1} - 2^{\frac{m}{2}-1} - 1.\end{aligned}$$

For $\frac{2^m-1}{3} < \delta < 2^{m-1} - 2^{\frac{m}{2}-1}$, we have

$$\mathrm{CL}\left(n-(2^{\frac{m}{2}}-1)\right) > 2^{m-1} - 2^{\frac{m}{2}-1} - 2 \ge \delta - 1.$$

It then follows that $n - (2^{\frac{m}{2}}+1) \notin T$ and $2^{\frac{m}{2}}+1 \in T^{\perp}$. This completes the proof. ■

For $2 \le m \le 5$, Table V documents if $\mathcal{C}_{(2,n,\delta)}$ is a dually-BCH code. For $m \ge 6$, the following theorem gives a sufficient and necessary condition for $\mathcal{C}_{(2,n,\delta)}$ being a dually-BCH code, where $2 \le \delta \le n$.

Theorem 17: Let $m \ge 6$. Then $\mathcal{C}_{(2,n,\delta)}$ is a dually-BCH code if and only if

$$\delta = 2, 3, \text{ or } 2^{m-1} - 2^{\lfloor \frac{m-1}{2} \rfloor} \le \delta \le n.$$

Proof: Let β be the n-th primitive root of unity for defining $\mathcal{C}_{(2,n,\delta)}$ and let T denote the defining set of this code with respect to β. It is clear that $0 \notin T$ and $1 \in T$, so $0 \notin T^{-1}$ and $n-1 \in T^{-1}$. Furthermore, we have $0 \in T^{\perp}$ and $n-1 \notin T^{\perp}$, which means that C_0 must be the initial cyclotomic coset of $T^{\perp}$. In other words, there must be an integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$ if $\mathcal{C}_{(2,n,\delta)}$ is a dually-BCH code.

When $\delta = 2, 3$, the defining set of $\mathcal{C}_{(2,n,\delta)}$ is equal to $T = C_1$. In this case, $T^{-1} = C_{2^{m-1}-1}$. Note that $\delta_1 := 2^{m-1}-1$ is the largest coset leader modulo n by Lemma 1. Consequently, $T^{\perp} = \mathbb{Z}_n \setminus T^{-1} = C_0 \cup C_1 \cup \cdots \cup C_{2^{m-1}-2}$ and $\mathcal{C}_{(2,n,\delta)}^{\perp} = \mathcal{C}_{(2,n,2^{m-1},0)}$, which is a BCH code with the designed distance 2^{m-1} with respect to β.

By Lemma 1, $\delta_2 := 2^{m-1} - 2^{\lfloor \frac{m-1}{2} \rfloor}$ is the second largest coset leader modulo n. When $\delta_2 \le \delta \le n$, we will show that $T^{\perp} = C_0$ or $T^{\perp} = C_0 \cup C_1$. If $\delta_1 + 1 \le \delta \le n$, it is easy to see that $T^{\perp} = \{0\}$. In this subcase, $\mathcal{C}_{(2,n,\delta)}^{\perp} = \mathcal{C}_{(2,n,2,0)}$ with respect to β. If $\delta_2 + 1 \le \delta \le \delta_1$, then

$$T^{\perp} = \mathbb{Z}_n \setminus T^{-1} = (\mathbb{Z}_n \setminus T)^{-1} = (C_0 \cup C_{\delta_1})^{-1} = C_0 \cup C_1.$$

In this subcase, $\mathcal{C}_{(2,n,\delta)}^{\perp} = \mathcal{C}_{(2,n,3,0)}$ with respect to β.

Finally, we need to show that $\mathcal{C}_{(2,n,\delta)}^{\perp}$ is not a BCH code with respect to β when $4 \le \delta < 2^{m-1} - 2^{\lfloor \frac{m-1}{2} \rfloor}$ for $m \ge 6$. It suffices to show that there is no integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$.

When $m \ge 6$ is even, we have the following two cases.

- If $4 \le \delta \le \frac{2^m-1}{3}$, it follows from Proposition 16 that $\frac{2^m-1}{3} \in T^{\perp}$ is the coset leader of $C_{\frac{2^m-1}{3}}$. Note that $\frac{2^m-1}{3} - I_{\max} = \frac{2^m}{12} + \frac{2}{3} > 0$, where
$$I_{\max} := \max\{I(\delta) : 4 \le \delta \le \frac{2^m-1}{3}\} = 2^{m-2} - 1$$
by Lemma 15. As a result, there is no integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$, i.e., $\mathcal{C}_{(2,n,\delta)}^{\perp}$ is not a BCH code with respect to β.
- If $\frac{2^m-1}{3} < \delta < 2^{m-1} - 2^{\frac{m}{2}-1}$, it follows from Proposition 16 that $2^{\frac{m}{2}}+1 \in T^{\perp}$ is the coset leader of $C_{2^{\frac{m}{2}}+1}$. Note that $2^{\frac{m}{2}}+1 > 3$. It then follows from Lemma 15 that there is no integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$, i.e., $\mathcal{C}_{(2,n,\delta)}^{\perp}$ is not a BCH code with respect to β.

When $m \ge 7$ is odd, we also have the following two cases.

- If $4 \le \delta \le \frac{2^{m-1}-1}{3}$, Proposition 16 tells us that $\frac{2^m+1}{3} \in T^{\perp}$ is the coset leader of $C_{\frac{2^m+1}{3}}$. Note that $\frac{2^m+1}{3} > (2^{m-2}-1) = I_{\max}$ by Lemma 15. Consequently, there is no integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$, i.e., $\mathcal{C}_{(2,n,\delta)}^{\perp}$ is not a BCH code with respect to β.
- If $\frac{2^{m-1}-1}{3} < \delta < 2^{m-1} - 2^{\frac{m-1}{2}}$, Proposition 16 informs us that $2^{\frac{m-1}{2}}+1 \in T^{\perp}$ is the coset leader of $C_{2^{\frac{m-1}{2}}+1}$. Note that $2^{\frac{m-1}{2}}+1 > 7$ if $m > 5$. It then follows from

TABLE VI
THE CODES OF $\mathcal{C}_{(2,127,\delta)}$ AND $\mathcal{C}^{\perp}_{(2,127,\delta)}$

δ	k	d	$k^{\perp}$	$d^{\perp}$	Is $\mathcal{C}_{(2,127,\delta)}$ dually-BCH?	Optimality of $\mathcal{C}_{(2,127,\delta)}$	Optimality of $\mathcal{C}^{\perp}_{(2,127,\delta)}$
$2 \sim 3$	120	3	7	64	Yes	Yes	Yes
$4 \sim 5$	113	5	14	56	No	Yes	Yes
$6 \sim 7$	106	7	21	48	No	Best known	Best known
$8 \sim 9$	99	9	28	44	No	Best known	Best known
$10 \sim 11$	92	11	35	32	No	Best known	No
$12 \sim 13$	85	13	42	32	No	Best known	Best known
$14 \sim 15$	78	15	49	28	No	Best known	Best known
$16 \sim 19$	71	19	56	22	No	Best known	No
$20 \sim 21$	64	21	63	22	No	Best known	Best known
$22 \sim 23$	57	23	70	16	No	No	No
$24 \sim 27$	50	27	77	16	No	Best known	Best known
$28 \sim 29$	43	31	84	14	No	Best known	Best known
$30 \sim 31$	36	31	91	12	No	No	Best known
$32 \sim 43$	29	43	98	10	No	Best known	Best known
$44 \sim 47$	22	47	105	8	No	Best known	Yes
$48 \sim 55$	15	55	112	6	No	Best known	Yes
$56 \sim 63$	8	63	119	4	Yes	Yes	Yes
$64 \sim 127$	1	127	126	2	Yes	Yes	Yes

Lemma 15 that there is no integer $J \geq 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$, i.e., $\mathcal{C}^{\perp}_{(2,n,\delta)}$ is not a BCH code with respect to β.

Collecting all discussions above proves the desired conclusions. ■

Example 1: For $m = 7$, we have $n = 127$. The parameters of $\mathcal{C}_{(2,127,\delta)}$ and $\mathcal{C}^{\perp}_{(2,127,\delta)}$ are presented in Table VI, where the codes are optimal or best known according to the Database [14].

The following theorem gives the parameters or their bounds of the codes $\mathcal{C}_{(2,n,\delta)}$ and $\mathcal{C}^{\perp}_{(2,n,\delta)}$, where $n = 2^m - 1$ and $m \geq 6$. Specially, lower bounds on minimum distances of the dual codes $\mathcal{C}^{\perp}_{(2,n,\delta)}$ are presented.

Theorem 18: Let $[n, k, d]$ and $[n, k^{\perp}, d^{\perp}]$ be the parameters of $\mathcal{C}_{(2,n,\delta)}$ and $\mathcal{C}^{\perp}_{(2,n,\delta)}$, respectively, where $n = 2^m - 1$ and $m \geq 6$. Denote

$$k_t = 2^m - 1 - \sum_{i=1}^{\lfloor \frac{m}{r+1} \rfloor} (-1)^{i-1} \frac{m}{i} \binom{m - ir - 1}{i - 1} 2^{m-i(r+1)},$$

where $r = m - t$.

1) For $\delta = 2, 3$, we have

$$k = 2^m - 1 - m, \; d = 3, \quad \text{and} \quad k^{\perp} = m, \; d^{\perp} = 2^{m-1}.$$

2) Assume that $4 \leq \delta < 2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1}$.

- For $2^t \leq \delta < 2^{t+1}$ with $2 \leq t \leq m - 3$, we have

$$k_{t+1} < k \leq k_t, \; d \geq \delta, \quad \text{and}$$
$$q^m - 1 - k_t \leq k^{\perp} < q^m - 1 - k_{t+1}, \; d^{\perp} \geq 2^{m-t}.$$

- For $2^{m-2} \leq \delta < 2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1}$, we have

$$k_{m-1} < k \leq k_{m-2}, \; d \geq \delta, \quad \text{and}$$
$$q^m - 1 - k_{m-2} \leq k^{\perp} < q^m - 1 - k_{m-1}, \; d^{\perp} \geq 4.$$

3) For $2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1} \leq \delta < 2^{m-1}$, we have

$$k = m + 1, \; d = 2^{m-1} - 1 \quad \text{and}$$
$$k^{\perp} = 2^m - m - 2, \; d^{\perp} \geq 4.$$

Proof: For $\delta = 2, 3$, it follows from the proof of Theorem 17 that the defining sets of $\mathcal{C}_{(2,n,\delta)}$ and $\mathcal{C}^{\perp}_{(2,n,\delta)}$ are

$$T = C_1 \quad \text{and} \quad T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{2^{m-1}-2},$$

respectively. Then we have $k = 2^m - 1 - m$ and $k^{\perp} = m$. It is easy to see from Lemma 4 that $d = 3$. Note that $C_{n-1} = C_{\delta_1}$. Then $\mathcal{C}^{\perp}_{(2,n,\delta)}$ is an irreducible primitive cyclic code with check polynomial $\mathbb{M}_{\delta_1}(x)$, where $\mathbb{M}_{\delta_1}(x)$ is the minimal polynomial of α^{δ_1} over $\mathbb{F}_2$. Then the minimum distance of $\mathcal{C}^{\perp}_{(2,n,\delta)}$ is equal to $d^{\perp} = 2^{m-1}$, which is also documented in [11] and [12].

For every fixed δ in the range $4 \leq \delta < 2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1}$, there is an integer t_0 such that $2 \leq t_0 \leq m - 2$ and $2^{t_0} \leq \delta < 2^{t_0+1}$, which means that

$$\mathcal{C}_{(2,n,2^{t_0+1})} \subseteq \mathcal{C}_{(2,n,\delta)} \subseteq \mathcal{C}_{(2,n,2^{t_0})}.$$

The desired conclusion on the dimensions of $\mathcal{C}_{(2,n,\delta)}$ and $\mathcal{C}^{\perp}_{(2,n,\delta)}$ then follows from Lemma 3. Moreover, the lower bound on the minimum distance d comes from the BCH bound. It is clear that $\mathcal{C}^{\perp}_{(2,n,\delta)}$ is a subcode of $\mathcal{C}^{\perp}_{(2,n,I(\delta))}$, where $I(\delta)$ is given in Lemma 15. We then obtain the desired conclusion on $d^{\perp}$.

When $2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1} \leq \delta < 2^{m-1}$, from the proof of Theorem 17 we have $T^{\perp} = C_0 \cup C_1$. Then $k = m + 1$ and $k^{\perp} = 2^m - m - 2$. In addition, $d = 2^{m-1} - 1$ is documented in [11]. Note that $C_1 = C_2$ and $T^{\perp} = C_0 \cup C_1 \cup C_2$. Then $d^{\perp} \geq 4$. ■

It should be remarked that Theorem 18 improves the classical Sidel'nikov bound documented in Lemma 6. For $\delta = 2s + 1$, there is an integer t such that $2^t < 2s + 1 < 2^{t+1}$

TABLE VII

LOWER BOUNDS ON MINIMUM DISTANCES OF $\mathcal{C}^{\perp}_{(2,63,\delta)}$

δ(odd)	$d^{\perp} \ge$			$d^{\perp}$
	Sidel'nikov bound	Carlitz-Uchiyama bound	Theorem 18	
3	32	32	32	32
5	16	24	16	24
7	8	16	16	16
9	8	8	8	14
11	4	0	8	14
13	4	< 0	8	12
15	4	< 0	8	8
17	4	< 0	4	8
$19 \sim 21$	2	< 0	4	8
23	2	< 0	4	6
$25 \sim 31$	2	< 0	4	4

and $2^t - 2 < 2s - 1 < 2^{t+1} - 2$. Moreover, we have

$$2^{m-1-\lfloor \log_2(2s-1) \rfloor} \le 2^{m-1-\lfloor \log_2(2^t-2) \rfloor} = 2^{m-t}.$$

It then follows that the lower bound on $d^{\perp}$ given in Theorem 18 is tighter than the Sidel'nikov bound (see Table VII for comparison). It is clear that Carlitz-Uchiyama bound given in Lemma 5 is useless when $\delta > 2^{\frac{m}{2}} + 3$ since the bound is negative. Therefore, the bound on $d^{\perp}$ given in Theorem 18 is larger than the Carlitz-Uchiyama bound when $\delta > 2^{\frac{m}{2}} + 3$.

Corollary 19: For $\delta = 2^t - 1$ $(2 \le t \le m-1)$, we have

$$k = k_t + m,\ d = 2^t - 1, \quad \text{and}$$
$$k^{\perp} = 2^m - 1 - k_t - m,\ d^{\perp} \ge 2^{m-t+1},$$

where k_t was given in Theorem 18.

Proof: For $\delta = 2^t - 1$, we have $T = C_1 \cup C_2 \cup \cdots \cup C_{2^t-2}$. It is clear that $2^t - 1$ is a coset leader and $|C_{2^t-1}| = m$. It then follows from Lemmas 3 and 4 that $k = k_t + m$ and $d = 2^t - 1$. Thus $k^{\perp} = 2^m - 1 - k_t - m$. Moreover, $d^{\perp} \ge 2^{m-t+1}$ follows from the proof of Theorem 18. ■

V. DUAL CODES OF BCH CODES OF LENGTH $q^m - 1$

In this section, we always assume that $n = q^m - 1$, where $q \ge 3$ and $m \ge 2$. We follow the notation introduced in Section I. In this case, $\beta = \alpha$, which is a primitive element of $\mathbb{F}_{q^m}$. Let $\mathcal{C}_{(q,n,\delta)}$ be the primitive narrow-sense BCH code over $\mathbb{F}_q$ with designed distance δ, i.e., the defining set of $\mathcal{C}_{(q,n,\delta)}$ with respect to the n-th primitive root β is $T = C_1 \cup C_2 \cup \cdots \cup C_{\delta-1}$, where $2 \le \delta \le n$. Denote by $T^{\perp}$ the defining set of the dual code $\mathcal{C}^{\perp}_{(q,n,\delta)}$ with respect to β. It is clear that $T^{\perp} = \mathbb{Z}_n \setminus T^{-1}$ and $0 \in T^{\perp}$. Our task in this section is to investigate the parameters of the dual code $\mathcal{C}^{\perp}_{(q,n,\delta)}$ and present a characterization of $\mathcal{C}^{\perp}_{(q,n,\delta)}$ being a dually-BCH code. As will be seen later, the case $q \ge 3$ is more complicated than the case $q = 2$, and should be treated separately.

The following lemma will be employed later.

Lemma 20: For $3 \le \delta < (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}$, let $I(\delta) \ge 2$ be the integer such that $\{0, 1, 2, \ldots, I(\delta) - 1\} \subseteq T^{\perp}$ and $I(\delta) \notin T^{\perp}$. Then we have

$$I(\delta) = \begin{cases} q^{m-t} - a, & \text{if } aq^t \le \delta \le (a+1)q^t - 1 \\ & (1 \le t \le m-2, 1 \le a < q-1); \\ q^{m-t} - q + 1, & \text{if } (q-1)q^t \le \delta \le q^{t+1} - q + 1 \\ & (1 \le t \le m-2); \\ q - a, & \text{if } aq^{m-1} \le \delta \le (a+1)q^{m-1} - 1 \\ & (1 \le a < q-2); \\ 2, & \text{if } (q-2)q^{m-1} \le \delta < \\ & (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}; \\ (b+1)q^{m-t} - 1 & \text{if } \delta = q^t - b \\ & (1 \le t \le m-1, 1 \le b \le q-2, \\ & q^t - b \ge 3). \end{cases}$$

Proof: When $aq^t \le \delta \le (a+1)q^t - 1$ $(1 \le t \le m-2, 1 \le a < q-1)$, it is easy to see that

$$q^m - q^{m-t} + a - 1 \equiv q^{m-t}(aq^t - 1) \in C_{aq^t-1} \subseteq T.$$

Thus $q^{m-t} - a = n - (q^m - q^{m-t} + a - 1) \in T^{-1}$ and $q^{m-t} - a \notin T^{\perp} = \mathbb{Z}_n \setminus T^{-1}$.

Now we are going to show that $\{0, 1, 2, \ldots, q^{m-t} - a - 1\} \subseteq T^{\perp}$. It is clear that $0 \in T^{\perp}$. For every integer i with $1 \le i \le q^{m-t} - a - 1$, we have $i = q^{m-t} - a - u$, where $1 \le u \le q^{m-t} - a - 1$. Note that

$$q^{m-t}(aq^t - 1 + uq^t) \equiv q^m - q^{m-t} + a + u - 1 \pmod{n}.$$

Thus $aq^t - 1 + uq^t \in C_{q^m - q^{m-t} + a + u - 1} = C_{n-i}$. In addition, we have

$$aq^t - 1 + uq^t = (a + u - 1)q^t + q^t - 1$$
$$= (\underbrace{i_{m-1}, i_{m-2}, \ldots, i_{t+1}}_{m-t-1}, i_t, \underbrace{q-1, \ldots, q-1}_{t})_q.$$

Note that

$$(a+1)q^t - 2 = (\underbrace{0, \ldots, 0}_{m-t-1}, a, \underbrace{q-1, \ldots, q-1, q-2}_{t})_q.$$

Denote

$$Z = |\{i_j = 0 : t+1 \le j \le m-1\}|.$$

If $Z < m-t-1$, then there is some integer $t+1 \le j_0 \le m-1$ such that $i_{j_0} \neq 0$. It is clear that

$$\mathrm{CL}(q^m - q^{m-t} + a + u - 1) > (a+1)q^t - 2 \ge \delta - 1. \quad (2)$$

If $Z = m-t-1$, then $a \le a+u-1 \le q-1$ and Equation (2) also holds. Hence $q^m - q^{m-t} + a + u - 1 \notin T$ and $q^{m-t} - a - u \notin T^{-1}$. This leads to $i = q^{m-t} - a - u \in T^{\perp}$. Thus we have $I(\delta) = q^{m-t} - a$.

For the following four cases of δ,

- $(q-1)q^t \le \delta \le q^{t+1} - q + 1$ $(1 \le t \le m-2)$,
- $aq^{m-1} \le \delta \le (a+1)q^{m-1} - 1$ $(1 \le a < q-2)$,
- $(q-2)q^{m-1} \le \delta < (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}$,
- $\delta = q^t - b$ $(1 \le t \le m-1, 1 \le b \le q-2, q^t - b \ge 3)$,

we can similarly prove the desired results and omit the details here. ■

Proposition 21: Let $n = q^m - 1$, where $q \ge 3$ and $m \ge 2$. Then the following hold:

1) $\frac{(q-2)(q^m-1)}{q-1} \in T^{\perp}$ is a coset leader modulo n if $3 \le \delta \le \frac{q^m-1}{q-1}$.
2) $q^{\lfloor \frac{m}{2} \rfloor} + 1 \in T^{\perp}$ is a coset leader modulo n if $\frac{q^m-1}{q-1} < \delta < (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}$.

Proof: Obviously, $\frac{(q-2)(q^m-1)}{q-1} = (\underbrace{q-2, \ldots, q-2}_{m})_q$. Hence, $\frac{(q-2)(q^m-1)}{q-1}$ is the q-cyclotomic coset leader of $C_{\frac{(q-2)(q^m-1)}{q-1}}$. Note that

$$n - \frac{(q-2)(q^m-1)}{q-1} = \frac{q^m-1}{q-1} = (1, \ldots, 1)_q.$$

If $3 \le \delta \le \frac{q^m-1}{q-1}$, then we have

$$\mathrm{CL}\left(n - \frac{(q-2)(q^m-1)}{q-1}\right) = \frac{q^m-1}{q-1} > \frac{q^m-1}{q-1} - 1 \ge \delta - 1.$$

Consequently, $n - \frac{(q-2)(q^m-1)}{q-1} \notin T$ and $\frac{(q-2)(q^m-1)}{q-1} \notin T^{-1}$. This leads to $\frac{(q-2)(q^m-1)}{q-1} \in T^{\perp}$.

When $\frac{q^m-1}{q-1} < \delta < (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}$, we prove the desired conclusion only for the even m case, as the desired conclusion for the odd m case can be similarly proved. It is straightforward that

$$q^{\lfloor \frac{m}{2} \rfloor} + 1 = q^{\frac{m}{2}} + 1 \in T^{\perp} = (\underbrace{0, \ldots, 0}_{\frac{m}{2}-1}, 1, \underbrace{0, \ldots, 0}_{\frac{m}{2}-1}, 1)_q.$$

Hence, $q^{\frac{m}{2}} + 1$ is the q-cyclotomic coset leader of $C_{q^{\frac{m}{2}}+1}$. Note that

$$\begin{aligned} n - (q^{\frac{m}{2}} + 1) &= q^m - q^{\frac{m}{2}} - 2 \\ &= (\underbrace{q-1, \ldots, q-1}_{\frac{m}{2}-1}, q-2, \underbrace{q-1, \ldots, q-1}_{\frac{m}{2}-1}, q-2)_q. \quad (3) \end{aligned}$$

If $\frac{q^m-1}{q-1} < \delta < (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}$, then by (3) we have

$$\begin{aligned} \mathrm{CL}\left(n - (q^{\frac{m}{2}} + 1)\right) &= (q-1)q^{m-1} - q^{\frac{m}{2}-1} - 1 \\ &> (q-1)q^{m-1} - q^{\frac{m}{2}-1} - 2 \\ &\ge \delta - 1. \end{aligned}$$

Thus $n - (q^{\frac{m}{2}} + 1) \notin T$ and $(q^{\frac{m}{2}} + 1) \notin T^{-1}$. This leads to $q^{\frac{m}{2}} + 1 \in T^{\perp}$. The proof is then completed. ■

The following theorem gives a sufficient and necessary condition for $\mathcal{C}_{(q,n,\delta)}$ being a dually-BCH code, where $2 \le \delta \le n$.

Theorem 22: Let $q \ge 3$ and $m \ge 2$. Then $\mathcal{C}_{(q,n,\delta)}$ is a dually-BCH code if and only if

$$\delta = 2 \;\text{ or }\; (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor} \le \delta \le n.$$

Proof: It is clear that $0 \notin T$ and $1 \in T$, so $0 \notin T^{-1}$ and $n-1 \in T^{-1}$. Furthermore, we have $0 \in T^{\perp}$ and $n-1 \notin T^{\perp}$. As a result, C_0 must be the initial cyclotomic coset of $T^{\perp}$. Consequently, there must be an integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$ if $\mathcal{C}_{(q,n,\delta)}^{\perp}$ is a BCH code with respect to β.

When $\delta = 2$, the defining set of $\mathcal{C}_{(q,n,\delta)}$ with respect to β is equal to $T = C_1$. Then it is clear that $T^{-1} = C_{(q-1)q^m-1}$. Recall that $\delta_1 := (q-1)q^m - 1$ is the largest coset leader modulo n. Thus $T^{\perp} = \mathbb{Z}_n \setminus T^{-1} = C_0 \cup C_1 \cup \cdots \cup C_{(q-1)q^m-2}$ and $\mathcal{C}_{(q,n,\delta)}^{\perp}$ is a BCH code with respect to β.

Recall that $\delta_2 = q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}$. When $q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor} \le \delta < n$, we will show that $T^{\perp} = C_0$ or $T^{\perp} = C_0 \cup C_1$. If $\delta_1 + 1 \le \delta \le n$, it is easy to see that $T^{\perp} = \{0\}$. If $\delta_2 + 1 \le \delta \le \delta_1$, then

$$T^{\perp} = \mathbb{Z}_n \setminus T^{-1} = (\mathbb{Z}_n \setminus T)^{-1} = (C_0 \cup C_{\delta_1})^{-1} = C_0 \cup C_1.$$

Hence, $\mathcal{C}_{(q,n,\delta)}^{\perp}$ is a BCH code with respect to β.

Finally, we will show that $\mathcal{C}_{(q,n,\delta)}^{\perp}$ is not a BCH code with respect to β when $3 \le \delta < (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}$. It suffices to prove that there is no integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$.

When $3 \le \delta \le \frac{q^m-1}{q-1}$, it follows from Proposition 21 that $\frac{(q-2)(q^m-1)}{q-1} \in T^{\perp}$ is a coset leader modulo n. Write $I_{\max} = \max\{I(\delta) : 3 \le \delta \le \frac{q^m-1}{q-1}\}$. It then follows from Lemma 20 that $I_{\max} = I(3) = (q-2)q^{m-1} - 1$. It is clear that

$$\frac{(q-2)(q^m-1)}{q-1} > I_{\max}.$$

Consequently, there is no integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$, i.e., $\mathcal{C}_{(q,n,\delta)}^{\perp}$ is not a BCH code with respect to β.

When $\frac{q^m-1}{q-1} < \delta < (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}$, it follows from Proposition 21 that $q^{\lfloor \frac{m}{2} \rfloor} + 1 \in T^{\perp}$ is the coset leader of $C_{q^{\lfloor \frac{m}{2} \rfloor}+1}$. Write $I'_{\max} = \max\{I(\delta) : \frac{q^m-1}{q-1} < \delta < (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}\}$. It then follows from Lemma 20 that $I'_{\max} = q-1$. Note that $q^{\lfloor \frac{m}{2} \rfloor} + 1 > I'_{\max}$. Therefore, there is no integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$, i.e., $\mathcal{C}_{(q,n,\delta)}^{\perp}$ is not a BCH code with respect to β. Summarising all discussions above, we obtain the desired conclusion. ■

The following theorem gives information on the codes $\mathcal{C}_{(q,n,\delta)}$ and $\mathcal{C}_{(2,n,\delta)}^{\perp}$, where $n = q^m - 1$ and $m \ge 2$. In fact, the dimensions of the codes $\mathcal{C}_{(q,n,\delta)}$ were determined explicitly in [1] and [19] when $2 \le \delta \le q^{\lceil \frac{m}{2} \rceil + 1}$.

Theorem 23: Let $[n, k, d]$ and $[n, k^{\perp}, d^{\perp}]$ denote the parameters of $\mathcal{C}_{(q,n,\delta)}$ and $\mathcal{C}_{(q,n,\delta)}^{\perp}$, respectively, where

TABLE VIII
THE CODES $\mathcal{C}_{(3,26,\delta)}$ AND $\mathcal{C}^{\perp}_{(3,26,\delta)}$

δ	k	d	$k^{\perp}$	$d^{\perp}$	Is $\mathcal{C}$ dually-BCH?	Optimality of $\mathcal{C}$	Optimality of $\mathcal{C}^{\perp}$
2	23	2	3	18	Yes	Yes	Yes
$3 \sim 4$	20	4	6	15	No	Yes	Yes
5	17	5	9	9	No	No	No
$6 \sim 7$	14	7	12	9	No	Best known	Best known
8	11	8	15	6	No	No	No
$9 \sim 13$	8	13	18	6	No	Yes	Yes
14	7	14	19	5	No	Yes	Yes
$15 \sim 17$	4	17	22	3	Yes	Yes	Yes
$18 \sim 26$	1	26	25	2	Yes	Yes	Yes

$n = q^m - 1$ and $q \geq 3$. Let $r = m - s$ and

$$k_s = q^m - 1 - \sum_{i=1}^{\lfloor \frac{m}{r+1} \rfloor} \frac{(-1)^{i-1} m (q-1)^i}{i} \binom{m - ir - 1}{i - 1} q^{m - i(r+1)}.$$

1) When $\delta = 2$, we have

$$k = q^m - 1 - m,\ d = 2, \text{ and } k^{\perp} = m,\ d = q^m - q^{m-1}.$$

2) When $3 \leq \delta < (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}$, there is an integer $s \geq 0$ such that $q^s \leq \delta < q^{s+1}$, and we have

$$k_{s+1} < k \leq k_s,\ d \geq \delta, \quad \text{and}$$
$$q^m - 1 - k_s \leq k^{\perp} < q^m - 1 - k_{s+1},\ d^{\perp} \geq I(\delta) + 1,$$

where $I(\delta)$ is given in Lemma 20.

3) When $(q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor} \leq \delta < (q-1)q^{m-1}$, we have

$$k = m + 1,\ d = (q-1)q^{m-1} - 1, \quad \text{and}$$
$$k^{\perp} = q^m - m - 2,\ d^{\perp} \geq 3.$$

Proof: For $\delta = 2$, it follows from the proof of Theorem 22 that the defining sets of $\mathcal{C}_{(q,n,\delta)}$ and $\mathcal{C}^{\perp}_{(q,n,\delta)}$ with respect to β are

$$T = C_1 \quad \text{and} \quad T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{(q-1)q^m - 2},$$

respectively. Then we have $k = q^m - 1 - m$ and $k^{\perp} = m$. In this case, $\mathcal{C}^{\perp}_{(q,n,\delta)}$ is an irreducible primitive cyclic code with check polynomial $\mathbb{M}_{\beta_1^{\delta}}(x)$ as $C_{n-1} = C_{\delta_1}$, where $\mathbb{M}_{\beta_1^{\delta}}(x)$ is the minimal polynomial of β^{δ_1} over $\mathbb{F}_q$. Then the minimum distance of $\mathcal{C}^{\perp}_{(q,n,\delta)}$ is equal to $d^{\perp} = q^m - q^{m-1}$ and its weight enumerator is $1 + (q^m - 1)x^{q^m - q^{m-1}}$, which are also documented in [11] and [12]. It then follows from the MacWilliams identity that $d = 2$.

For every fixed δ in the range $3 \leq \delta < (q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor}$, there is an integer $s \geq 0$ such that $q^s \leq \delta < q^{s+1}$, which leads to

$$\mathcal{C}_{(q,n,q^{s+1})} \subseteq \mathcal{C}_{(q,n,\delta)} \subseteq \mathcal{C}_{(q,n,q^s)}.$$

The desired conclusion on the dimensions of $\mathcal{C}_{(q,n,\delta)}$ and $\mathcal{C}^{\perp}_{(q,n,\delta)}$ then follows from Lemma 3. Moreover, the lower bound on the minimum distance d comes from the BCH bound and Theorem 22. It is clear that $\mathcal{C}^{\perp}_{(q,n,\delta)}$ is a subcode of $\mathcal{C}^{\perp}_{(q,n,I(\delta))}$, where $I(\delta)$ is given in Lemma 20. We then obtain the desired conclusion on $d^{\perp}$.

When $(q-1)q^{m-1} - q^{\lfloor \frac{m-1}{2} \rfloor} \leq \delta < (q-1)q^{m-1}$, we have $T^{\perp} = C_0 \cup C_1$. Then $k = m + 1$ and $k^{\perp} = q^m - m - 2$. In addition, $d = (q-1)q^{m-1} - 1$ is documented in [11], and $d^{\perp} \geq 3$. ■

Example 2: For $q = 3, m = 3$, we have $n = 26$. The parameters of $\mathcal{C}_{(3,26,\delta)}$ and $\mathcal{C}^{\perp}_{(3,26,\delta)}$ are presented in Table VIII, where the codes are optimal or the best known according to the Database [14].

Corollary 24: For $\delta = q^s - 1$ ($1 \leq s \leq m - 1$ and $q^s \geq 4$), we have

$$k = k_s + m,\ d = q^s - 1, \quad \text{and}$$
$$k^{\perp} = q^m - 1 - k_s - m,\ d^{\perp} \geq 2q^{m-s},$$

where k_s is given in Theorem 23.

Proof: For $\delta = q^s - 1$, we have $T = C_1 \cup C_2 \cup \cdots \cup C_{q^s - 2}$. It is clear that $q^s - 1$ is a coset leader and $|C_{q^s - 1}| = m$. It then follows from Lemmas 3 and 4 that $k = k_s + m$ and $d = q^s - 1$. Thus $k^{\perp} = q^m - 1 - k_s - m$. Moreover, $d^{\perp} \geq 2q^{m-s}$ follows from Theorem 23. ■

VI. DUAL CODES OF BCH CODES OF LENGTH $\frac{q^m - 1}{q - 1}$

In this section, we always assume that $q \geq 3$ and $n = \frac{q^m - 1}{q - 1}$, where $m \geq 3$ is an integer. We follow the notation specified in Section I, where α is a primitive element of $\mathbb{F}_{q^m}$ and $\beta = \alpha^{q-1}$. Consider the projective narrow-sense BCH code $\mathcal{C}_{(q,n,\delta)}$ whose defining set with respect to β is $T = C_1 \cup C_2 \cup \cdots \cup C_{\delta - 1}$, where $2 \leq \delta \leq n$. As before, denote by $T^{\perp}$ the defining set of the dual code $\mathcal{C}^{\perp}_{(q,n,\delta)}$ with respect to β. It is clear that $T^{\perp} = \mathbb{Z}_n \setminus T^{-1}$ and $0 \in T^{\perp}$.

The dimension of the dual code $\mathcal{C}^{\perp}_{(q,n,\delta)}$ was known in many cases and is documented in the next few theorems.

Theorem 25: [16, Theorem 27] Let $m \geq 4$ be even and $2 \leq \delta \leq q^{m/2}$. Define

$$\epsilon = \left\lfloor \frac{(\delta - 2)(q - 1)}{q^{m/2} - 1} \right\rfloor.$$

Then $\mathcal{C}^{\perp}_{(q,n,\delta)}$ has dimension

$$k^{\perp} = \begin{cases} m \left\lceil \frac{(\delta-1)(q-1)}{q} \right\rceil - (2\epsilon - (q-2))\frac{m}{2}, & \text{if } \epsilon \geq \lfloor \frac{q-1}{2} \rfloor; \\ m \left\lceil (\delta - 1)(q - 1)/q \right\rceil, & \text{if } \epsilon < \lfloor \frac{q-1}{2} \rfloor. \end{cases}$$

Theorem 26: [19] Let $m \geq 5$ be an odd integer. Set $h = (m-1)/2$. For $\delta = \ell q^h + 1$ with $1 \leq \ell \leq q-1$, the dimension of $\mathcal{C}^{\perp}_{(q,n,\delta)}$ is given by

$$k^{\perp} = \begin{cases} m\left(\delta_{Nq} - \ell(\ell-1)\right) \text{ if } \ell \leq \lfloor \frac{q}{2} \rfloor; \\ m\left(\delta_{Nq} - \ell(\ell-1) + 2\ell - q\right) \text{ if } \lfloor \frac{q}{2} \rfloor + 1 \leq \ell \leq q-1; \\ m\left(\delta_{Nq} - \ell(\ell-1) + 2\ell - 2\right) \text{ if } \ell = q, \end{cases}$$

where $\delta_{Nq} = \delta - 1 - \lfloor \frac{\delta-1}{q} \rfloor$.

Although the dimension of $\mathcal{C}^{\perp}_{(q,n,\delta)}$ is known in many cases, little is known about the minimum distance of this code. One of our tasks in this section is to develop lower bounds on the minimum distance of $\mathcal{C}^{\perp}_{(q,n,\delta)}$. Another task is to present a characterization of the ternary code $\mathcal{C}_{(3,n,\delta)}$ being dually-BCH. To this end, we need the lemma below.

Lemma 27: For $2 \leq \delta < n$, let $I(\delta) \geq 2$ be the integer such that $\{0, 1, 2, \ldots, I(\delta) - 1\} \subseteq T^{\perp}$ and $I(\delta) \notin T^{\perp}$. Then we have $I(\delta) = \frac{q^{m-t}-1}{q-1}$ if $\frac{q^t-1}{q-1} < \delta \leq \frac{q^{t+1}-1}{q-1}$ $(1 \leq t \leq m-2)$ and $I(\delta) = 1$ if $\frac{q^{m-1}-1}{q-1} < \delta < n$.

Proof: When $\frac{q^t-1}{q-1} < \delta \leq \frac{q^{t+1}-1}{q-1}$, it is easy to see that $q^t - 1$ is a coset leader modulo $q^m - 1$. We then assert that $\frac{q^t-1}{q-1}$ is a coset leader modulo n. On the contrary, suppose that $\frac{q^t-1}{q-1}$ is not a coset leader modulo n, then there would be an integer ℓ with $1 \leq \ell \leq m$ such that

$$\begin{aligned} \frac{q^t-1}{q-1} q^{\ell} \bmod n &< \frac{q^t-1}{q-1} \quad \Leftrightarrow \\ (q^t-1)q^{\ell} \bmod (q-1)n &< q^t - 1. \end{aligned} \tag{4}$$

This means that $q^t - 1$ is not a coset leader modulo $q^m - 1$ and leads to a contradiction.

It is straightforward to see that

$$\frac{q^m - q^{m-t}}{q-1} = \frac{q^t-1}{q-1} q^{m-t} \in C_{\frac{q^t-1}{q-1}} \subseteq T.$$

Therefore, $\frac{q^{m-t}-1}{q-1} = n - \frac{q^m - q^{m-t}}{q-1} \in T^{-1}$ and $\frac{q^{m-t}-1}{q-1} \notin T^{\perp} = \mathbb{Z}_n \setminus T^{-1}$.

We are ready to show that $\{0, 1, 2, \ldots, \frac{q^{m-t}-1}{q-1} - 1\} \subseteq T^{\perp}$. It is clear that $0 \in T^{\perp}$. For every integer i with $1 \leq i \leq \frac{q^{m-t}-1}{q-1} - 1$, we have $i = \frac{q^{m-t}-1}{q-1} - u$, where $1 \leq u \leq \frac{q^{m-t}-1}{q-1} - 1$. Note that

$$((q-1)q^t u + q^t - 1)q^{m-t} \equiv q^m - q^{m-t} + (q-1)u \pmod{q^m - 1}$$

and

$$(q-1)q^t u + q^t - 1 = (\underbrace{i_{m-1}, i_{m-2}, \ldots, i_t}_{m-t}, \underbrace{q-1, \ldots, q-1}_{t})_q,$$

where $i_t = q-1$ if $u = 1$ and $i_j \neq 0$ for $t+1 \leq j \leq m-1$ if $u > 1$. It follows that the coset leader of the cyclotomic coset of $(q-1)q^t u + q^t - 1$ modulo $q^m - 1$ is larger than or equal to $q^{t+1} - 1$. Then we obtain from (4) that

$$\mathrm{CL}\left(\frac{q^t - 1 + (q-1)q^t u}{q-1}\right) \geq \frac{q^{t+1}-1}{q-1} > \delta - 1.$$

Consequently, $\frac{q^m - q^{m-t} + (q-1)u}{q-1} \notin T$ and $\frac{q^{m-t}-1}{q-1} - u \notin T^{-1}$. This leads to $i = \frac{q^{m-t}-1}{q-1} - u \in T^{\perp}$. It then follows that $I(\delta) = \frac{q^{m-t}-1}{q-1}$ for any δ with $\frac{q^t-1}{q-1} < \delta \leq \frac{q^{t+1}-1}{q-1}$ $(1 \leq t \leq m-2)$.

When $\frac{q^{m-1}-1}{q-1} < \delta < \frac{q^m-1}{q-1}$, we can similarly prove the desired result and hence omit the details. The proof is then completed. ■

TABLE IX

LOWER BOUNDS ON MINIMUM DISTANCES OF $\mathcal{C}^{\perp}_{(3,40,\delta)}$

δ	$d^{\perp}$	$d^{\perp} \geq$
4	18	14
9	8	5
13	6	5
14	4	2
40	2	2

Although the dimension of $\mathcal{C}^{\perp}_{(q,n,\delta)}$ is known in many cases, little is known about the minimum distance of this code. One of the main contributions of this paper is the following theorem, which documents very good lower bounds on the minimum distance of the code $\mathcal{C}^{\perp}_{(q,n,\delta)}$.

Theorem 28: Let $d^{\perp}(\delta)$ be the minimum distance of $\mathcal{C}^{\perp}_{(q,n,\delta)}$. Then we have

$$d^{\perp}(\delta) \geq \begin{cases} \frac{q^{m-t}-1}{q-1} + 1, & \text{if } \frac{q^t-1}{q-1} < \delta \leq \frac{q^{t+1}-1}{q-1} \ (1 \leq t \leq m-2); \\ 2, & \text{if } \frac{q^{m-1}-1}{q-1} < \delta < n. \end{cases}$$

Proof: The desired conclusions then follow from Lemma 27 and the BCH bound for cyclic codes. ■

Theorems 25, 26 and 28 give a lot of information on the parameters of the code $\mathcal{C}^{\perp}_{(q,n,\delta)}$. It would be very hard to determine the minimum distance of $\mathcal{C}^{\perp}_{(q,n,\delta)}$. However, the following example shows that the lower bounds in Theorem 28 are very good.

Example 3: When $q = 3$ and $m = 4$, we have $n = 40$. The minimum distances and their lower bounds of the dual codes $\mathcal{C}^{\perp}_{(3,40,\delta)}$ are listed in Table IX, where $\delta \in \{4, 9, 13, 14, 40\}$.

Proposition 29: Let $q = 3$. Then the following hold.

1) When m is even, $\frac{3^m-1}{4} \in T^{\perp}$ is a coset leader modulo n if $2 \leq \delta \leq \frac{3^m-1}{4}$ and $\frac{3^{\frac{m}{2}}+1}{2} \in T^{\perp}$ is a coset leader modulo n if $\frac{3^m-1}{4} < \delta \leq 3^{m-1} - \frac{3^{\frac{m}{2}-1}+1}{2}$.
2) When m is odd, we have the following.
   - $\frac{3^m+1}{4} \in T^{\perp}$ is a coset leader modulo n if $2 \leq \delta \leq \frac{3^{m-1}-1}{4}$,
   - $\frac{3^{m-1}-1}{4} \in T^{\perp}$ is a coset leader modulo n if $\frac{3^{m-1}-1}{4} < \delta \leq \frac{3^m+1}{4}$,
   - $\frac{3^{\frac{m-1}{2}}+1}{2} \in T^{\perp}$ is a coset leader modulo n if $\frac{3^m+1}{4} < \delta \leq 3^{m-1} - \frac{3^{\frac{m-1}{2}}+1}{2}$.

Proof: We prove the desired conclusion only for the even m case, as the conclusion for the odd m case can be similarly proved. It is clear that $\frac{3^m-1}{2} = (1, \ldots, 1)_3$ is a coset leader modulo $3^m - 1$. It then follows from the proof of Lemma 27 that $\frac{3^m-1}{4}$ is a coset leader modulo n. If $2 \leq \delta \leq \frac{3^m-1}{4}$, then we have

$$\mathrm{CL}\left(n - \frac{3^m-1}{4}\right) = \frac{3^m-1}{4} > \frac{3^m-1}{4} - 1 \geq \delta - 1.$$

TABLE X

THE DUAL CODE $\mathcal{C}_{(3,n,\delta)}^{\perp}$

m	δ	Is $\mathcal{C}_{(3,n,\delta)}$ dually-BCH?		m	δ	Is $\mathcal{C}_{(3,n,\delta)}$ dually-BCH?
4	$2 \le \delta \le 25$	No		6	$2 \le \delta \le 238$	No
	$26 \le \delta \le 40$	Yes			$239 \le \delta \le 364$	Yes
5	$2 \le \delta \le 76$	No		7	$2 \le \delta \le 715$	No
	$77 \le \delta \le 121$	Yes			$716 \le \delta \le 1093$	Yes

Consequently, $n - \frac{3^m-1}{4} \notin T$ and $\frac{3^m-1}{4} \in T^{\perp}$. It is easy to see that

$$3^{\frac{m}{2}} + 1 = (\underbrace{0, \ldots, 0}_{\frac{m}{2}-1}, 1, \underbrace{0, \ldots, 0}_{\frac{m}{2}-1}, 1)_3$$

is a coset leader modulo $3^m - 1$, so $\frac{3^{\frac{m}{2}}+1}{2}$ is a coset leader modulo n. Note that

$$3^m - 3^{\frac{m}{2}} - 2 = (\underbrace{2, \ldots, 2}_{\frac{m}{2}-1}, 1, \underbrace{2, \ldots, 2}_{\frac{m}{2}-1}, 1)_3.$$

It is clear that the 3-cyclomotic coset leader of $3^m - 3^{\frac{m}{2}} - 2$ modulo $3^m - 1$ is

$$(1, \underbrace{2, \ldots, 2}_{\frac{m}{2}-1}, 1, \underbrace{2, \ldots, 2}_{\frac{m}{2}-1})_3 = 2 \cdot 3^{m-1} - 3^{\frac{m}{2}-1} - 1.$$

Then

$$\begin{aligned} \mathrm{CL}\left(n - \frac{3^{\frac{m}{2}}+1}{2}\right) &= \mathrm{CL}\left(\frac{3^m - 3^{\frac{m}{2}} - 2}{2}\right) \\ &= 3^{m-1} - \frac{3^{\frac{m}{2}-1}+1}{2}. \end{aligned}$$

For $\frac{3^m-1}{4} < \delta \le 3^{m-1} - \frac{3^{\frac{m}{2}-1}+1}{2}$, we have $\mathrm{CL}\left(n - \frac{3^{\frac{m}{2}}+1}{2}\right) > 3^{m-1} - \frac{3^{\frac{m}{2}-1}+1}{2} - 1 \ge \delta - 1$. It then follows that $n - \frac{3^{\frac{m}{2}}+1}{2} \notin T$ and $\frac{3^{\frac{m}{2}}+1}{2} \in T^{\perp}$. This completes the proof. ■

The following theorem gives a sufficient and necessary condition for $\mathcal{C}_{(3,n,\delta)}$ being a dually-BCH code, where $2 \le \delta \le n$.

Theorem 30: Let $n = \frac{3^m-1}{2}$ and $m \ge 4$. Then $\mathcal{C}_{(3,n,\delta)}$ is a dually-BCH code if and only if

$$3^{m-1} - \frac{3^{\lfloor \frac{m-1}{2} \rfloor}-1}{2} \le \delta \le n.$$

Proof: It is clear that $0 \notin T$ and $1 \in T$, so $0 \notin T^{-1}$ and $n-1 \in T^{-1}$. Furthermore, we have $0 \in T^{\perp}$ and $n-1 \notin T^{\perp}$, which means that C_0 must be the initial cyclotomic coset of $T^{\perp}$. In other words, there must be an integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$ if $\mathcal{C}_{(3,n,\delta)}$ is a dually-BCH code.

When $3^{m-1} - \frac{3^{\lfloor \frac{m-1}{2} \rfloor}-1}{2} \le \delta \le n$, we will show that $T^{\perp} = C_0$. Note that $\delta_1 = 3^{m-1} - \frac{3^{\lfloor \frac{m-1}{2} \rfloor}-1}{2} - 1$, where δ_1 is the largest coset leader modulo n and was given by Lemma 2. Then it is easy to see that $T^{\perp} = \{0\}$ and $\mathcal{C}_{(3,n,\delta)}^{\perp}$ is a BCH code with respect to β.

It remains to show that $\mathcal{C}_{(3,n,\delta)}^{\perp}$ is not a BCH code with respect to β when $2 \le \delta < 3^{m-1} - \frac{3^{\lfloor \frac{m-1}{2} \rfloor}-1}{2}$ for $m \ge 4$. To this end, we show that there is no integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$. We prove the conclusion only for the even m case, as the conclusion for the odd m case can be similarly proved. For even m, we have the following two subcases.

- If $2 \le \delta \le \frac{3^m-1}{4}$, it is easy to see from Proposition 29 that $\frac{3^m-1}{4} \in T^{\perp}$ is the coset leader of $C_{\frac{3^m-1}{4}}$. It follows from Lemma 27 that
$$\begin{aligned} I_{\max} &:= \max\{I(\delta) : 2 \le \delta \le \frac{3^m-1}{4}\} \\ &= I(2) = \frac{3^{m-1}-1}{2}. \end{aligned}$$
Note that $\frac{3^m-1}{4} - I(2) > 0$. It then follows that there is no integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$, i.e., $\mathcal{C}_{(3,n,\delta)}^{\perp}$ is not a BCH code with respect to β.
- If $\frac{3^m-1}{4} < \delta < 3^{m-1} - \frac{3^{\lfloor \frac{m-1}{2} \rfloor}-1}{2}$, it then follows from Proposition 29 that $\frac{3^{\frac{m}{2}}+1}{2} \in T^{\perp}$ is the coset leader of $C_{\frac{3^{\frac{m}{2}}+1}{2}}$. Note that $\frac{3^{\frac{m}{2}}+1}{2} > 1$. It then follows from Lemma 27 that there is no integer $J \ge 1$ such that $T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$, i.e., $\mathcal{C}_{(3,n,\delta)}^{\perp}$ is not a BCH code with respect to β.

This completes the proof. ■

By Theorem 30, the dual code $\mathcal{C}_{(3,n,\delta)}^{\perp}$ is not a BCH code with respect to β in most cases. When $m = 4, 5, 6, 7$, we give some examples of the dual code $\mathcal{C}_{(3,n,\delta)}^{\perp}$ in Table X.

Since Proposition 29 works only for the ternary case, Theorem 30 is restricted to the ternary code $\mathcal{C}_{(3,n,\delta)}$. It looks much harder to give a characterisation of $\mathcal{C}_{(q,n,\delta)}$ being dually-BCH for $q \ge 4$. The reader is cordially invited to solve this problem.

VII. Summary and Concluding Remarks

The main contributions of this paper are the following:

- The question as to what cyclic codes are BCH codes was answered for several subclasses of cyclic codes in Theorems 7, 8, and 12. The parameters of several classes of cyclic codes were studied in Corollaries 10, 11, 13, and 14.
- Sufficient and necessary conditions for $\mathcal{C}_{(q,q^m-1,\delta)}$ and $\mathcal{C}_{(3,\frac{3^m-1}{2},\delta)}$ being dually-BCH were developed (see Theorems 17, 22 and 30).
- The parameters of the primitive narrow-sense BCH codes and their duals were investigated in Theorems 18 and 23, Corollaries 19 and 24. Some lower bounds on the minimum distances of the dual codes of primitive and projective narrow-sense BCH codes were developed (see Theorems 18, 23, and 28). Especially for binary primitive

narrow-sense BCH codes, the bounds on minimum distances of the dual codes improve the classical Sidel'nikov bound, and are also better than the Carlitz-Uchiyama bound for large designed distances δ.

The question as to what cyclic codes are BCH codes is extremely hard to answer in general. It would be good if further progress regarding this question can be made. Little is known about the duals of BCH cyclic codes. The reader is cordially invited to study the duals of BCH codes.

Acknowledgment

The authors are very grateful to the reviewers and the Associate Editor, Prof. Gretchen Matthews, for their detailed comments and suggestions that highly improved the presentation and quality of this article.

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] 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.

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

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

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

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

[7] Y. Desaki, T. Fujiwara, and T. Kasami, "The weight distributions of extended binary primitive BCH codes of length 128," *IEEE Trans. Inf. Theory*, vol. 43, no. 4, pp. 1364–1371, Jul. 1997.

[8] C. Ding, *Codes From Difference Sets*. Singapore: World Scientific, 2014.

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

[10] 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.

[11] C. Ding, C. L. Fan, and Z. C. Zhou, "The dimension and minimum distance of two classes of primitive BCH codes," *Finite Fields Appl.*, vol. 45, pp. 237–263, May 2017.

[12] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," *Discrete Math.*, vol. 313, no. 4, pp. 434–446, 2013.

[13] Z. Du, C. Li, and S. Mesnager, "Constructions of self-orthogonal codes from hulls of BCH codes and their parameters," *IEEE Trans. Inf. Theory*, vol. 66, no. 11, pp. 6774–6785, Nov. 2020.

[14] M. Grassl, *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*. Accessed: May 16, 2021. [Online]. Available: http://www.codetables.de

[15] T. Kasami and S. Lin, "Some results on the minimum weight of BCH codes," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 6, pp. 824–825, Nov. 1972.

[16] 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.

[17] S. Li, "The minimum distance of some narrow-sense primitive BCH codes," *SIAM J. Discrete Math.*, vol. 31, no. 4, pp. 2530–2569, 2017.

[18] S. Li, C. Ding, M. Xiong, and G. Ge, "Narrow-sense BCH codes over $GF(q)$ with length $n = \frac{q^m-1}{q-1}$," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7219–7236, Nov. 2017.

[19] H. Liu, C. Ding, and C. Li, "Dimensions of three types of BCH codes over $GF(q)$," *Discrete Math.*, vol. 340, no. 8, pp. 1910–1927, Aug. 2017.

[20] Y. Liu, R. Li, Q. Fu, L. Lu, and Y. Rao, "Some binary BCH codes with length $n = 2^m + 1$," *Finite Fields Their Appl.*, vol. 55, pp. 109–133, Jan. 2019.

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

[22] F. J. MacWilliams and N. J. A. Sloane, *The Theory Error-Correcting Codes* (North-Holland Mathematical Library). Amsterdam, The Netherlands: North-Holland, 1977.

[23] S. Noguchi, X.-N. Lu, M. Jimbo, and Y. Miao, "BCH codes with minimum distance proportional to code length," *SIAM J. Discrete Math.*, vol. 35, no. 1, pp. 179–193, Feb. 2021.

[24] X. Shi, Q. Yue, and Y. Wu, "The dual-containing primitive BCH codes with the maximum designed distance and their applications to quantum codes," *Des., Codes Cryptogr.*, vol. 87, no. 9, pp. 2165–2183, Sep. 2019.

Binkai Gong is currently pursuing the master's degree with East China Normal University, Shanghai, China. His research interests include coding theory and cryptography.

Cunsheng Ding (Senior Member, IEEE) was born in Shaanxi, China, in 1962. He received the M.Sc. degree from the Northwestern Telecommunications Engineering Institute, Xi'an, China, in 1988, and the Ph.D. degree from the University of Turku, Turku, Finland, in 1997.

From 1988 to 1992, he was a Lecturer of mathematics with 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 with the National University of Singapore. He has coauthored five research monographs. His research interests include combinatorial designs, cryptography, and coding theory. He served as a guest editor or an editor for ten journals. He co-received the State Natural Science Award of China in 1989.

Chengju Li received the Ph.D. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2014. From March 2015 to February 2016, he was a Post-Doctoral Researcher with the Department of Mathematics, Korea Advanced Institute of Science and Technology, Daejeon, South Korea. From March 2016 to August 2016, he was a Post-Doctoral Researcher with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong. From July 2018 to September 2018, he visited the University of Paris VIII, Paris, France. He is currently a Professor with the Software Engineering Institute, East China Normal University, Shanghai, China. His research interests include exponential sums, coding theory, and cryptography.