LCD Cyclic Codes Over Finite Fields

Chengju Li, Cunsheng Ding, and Shuxing Li

***Abstract*— In addition to their applications in data storage, communications systems, and consumer electronics, linear complementary dual (LCD) codes—a class of linear codes—have been employed in cryptography recently. LCD cyclic codes were referred to as reversible cyclic codes in the literature. The objective of this paper is to construct several families of reversible cyclic codes over finite fields and analyze their parameters. The LCD cyclic codes presented in this paper have very good parameters in general, and contain many optimal codes. A well rounded treatment of reversible cyclic codes is also given in this paper.**

***Index Terms*— BCH codes, cyclic codes, linear codes, linear complementary dual (LCD) codes, reversible codes.**

I. Introduction

THROUGHOUT this paper, let q be a power of a prime p. An $[n, k, d]$ code $\mathcal{C}$ over GF(q) is a k-dimensional subspace of GF(q)^n with minimum (Hamming) distance d. Let $\mathcal{C}$ be an $[n, k]$ linear code over GF(q). Its dual code, denoted by $\mathcal{C}^\perp$, is defined by

$$\mathcal{C}^\perp = \{\mathbf{b} \in \mathrm{GF}(q)^n : \mathbf{b}\mathbf{c}^T = 0 \ \forall \ \mathbf{c} \in \mathcal{C}\},$$

where $\mathbf{b}\mathbf{c}^T$ denotes the standard inner product of the two vectors $\mathbf{b}$ and $\mathbf{c}$. A linear code is called an *LCD code (linear code with complementary dual)* if $\mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\}$, which is equivalent to $\mathcal{C} \oplus \mathcal{C}^\perp = \mathrm{GF}(q)^n$.

A linear $[n, k]$ code $\mathcal{C}$ over GF(q) is called *cyclic* if $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in \mathcal{C}$. By identifying any vector $(c_0, c_1, \cdots, c_{n-1}) \in \mathrm{GF}(q)^n$ with

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

any code $\mathcal{C}$ of length n over GF(q) corresponds to a subset of the quotient ring GF(q)$[x]/(x^n - 1)$. A linear code $\mathcal{C}$ is cyclic if and only if the corresponding subset in GF(q)$[x]/(x^n - 1)$ is an ideal of the ring GF(q)$[x]/(x^n - 1)$.

Note that every ideal of GF(q)$[x]/(x^n - 1)$ is principal. Let $\mathcal{C} = \langle g(x) \rangle$ be a cyclic code, where $g(x)$ is monic and has the smallest degree among all the generators of $\mathcal{C}$. Then $g(x)$ is unique and called the *generator polynomial,* and $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity-check polynomial* of $\mathcal{C}$.

Linear complementary dual (LCD) cyclic codes over finite fields were called *reversible codes* and studied by Massey [12]. Massey showed that some LCD cyclic codes over finite fields are BCH codes, and made a comparison between LCD codes and non-LCD codes [12]. He also demonstrated that asymptotically good LCD codes exist [13]. Yang and Massey gave a necessary and sufficient condition for a cyclic code to have a complementary dual [18]. Using the hull dimension spectra of linear codes, Sendrier showed that LCD codes meet the asymptotic Gilbert-Varshamov bound [16]. Esmaeili and Yari analysed 1-generator LCD quasi-cyclic codes [9]. Muttoo and Lal constructed a reversible code over GF(q) [15]. Tzeng and Hartmann proved that the minimum distance of a class of reversible cyclic codes is greater than the BCH bound [17]. Dougherty, Kim, Özkaya, Sok and Solè developed a linear programming bound on the largest size of an LCD code of given length and minimum distance [8]. Güneri, Özkaya, and Solè studied quasi-cyclic complementary dual codes [10]. Carlet and Guilley investigated an application of LCD codes against side-channel attacks, and presented several constructions of LCD codes [3]. LCD codes can be used in a direct-sum-masking technique for the prevention of side-channel attacks (see [3] for detail).

The objective of this paper is to construct several families of LCD cyclic codes over finite fields and analyse their parameters. The dimensions of these codes are determined and the minimum distances of some of the codes are settled and lower bounds on the minimum distance of other codes are given. Many codes are optimal in the sense that they have the best possible parameters. We will also give a well rounded treatment of LCD cyclic codes in general.

We will compare some of the codes presented in this paper with the tables of best known linear codes (referred to as the *Database* later) maintained by Markus Grassl at http://www.codetables.de.

II. q-Cyclotomic Cosets Modulo n and Auxiliaries

To deal with cyclic codes of length n over GF(q), we have to study the canonical factorization of $x^n - 1$ over GF(q). To this end, we need 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 $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$, denoting the ring of integers modulo n. For any $s \in \mathbb{Z}_n$, the *q-cyclotomic coset*

Manuscript received July 7, 2016; revised December 5, 2016; accepted February 11, 2017. Date of publication February 22, 2017; date of current version June 14, 2017. C. Li was supported by the Shanghai Sailing Program under Grant 17YF1404300. C. Ding was supported by The Hong Kong Research Grants Council under Project 16301114.

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

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

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

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

Digital Object Identifier 10.1109/TIT.2017.2672961

of s modulo n is defined by

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

where ℓ_s is the smallest positive integer such that $s \equiv sq^{\ell_s} \pmod n$, 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 $C_s \cap C_t = \emptyset$ for any two distinct elements s and t in $\Gamma_{(n,q)}$, and

$$\bigcup_{s \in \Gamma_{(n,q)}} C_s = \mathbb{Z}_n. \tag{1}$$

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

Let $m = \mathrm{ord}_n(q)$, and let α be a generator of $\mathrm{GF}(q^m)^*$, which denotes the multiplicative group of $\mathrm{GF}(q^m)$. Put $\beta = \alpha^{(q^m-1)/n}$. Then β is a primitive n-th root of unity in $\mathrm{GF}(q^m)$. The minimal polynomial $\mathrm{m}_s(x)$ of β^s over $\mathrm{GF}(q)$ is the monic polynomial of the smallest degree over $\mathrm{GF}(q)$ with β^s as a zero. It is now straightforward to prove that this polynomial is given by

$$\mathrm{m}_s(x) = \prod_{i \in C_s} (x - \beta^i) \in \mathrm{GF}(q)[x], \tag{2}$$

which is irreducible over $\mathrm{GF}(q)$. It then follows from (1) that

$$x^n - 1 = \prod_{s \in \Gamma_{(n,q)}} \mathrm{m}_s(x) \tag{3}$$

which is the factorization of $x^n - 1$ into irreducible factors over $\mathrm{GF}(q)$. This canonical factorization of $x^n - 1$ over $\mathrm{GF}(q)$ is crucial for the study of cyclic codes.

The following result will be useful and is not hard to prove [11, Th. 4.1.4].

Lemma 1: The size ℓ_s of each q-cyclotomic coset C_s is a divisor of $\mathrm{ord}_n(q)$, which is the size ℓ_1 of C_1.

The following lemma was proved in [1] and contains results in [4] as special cases.

Lemma 2: Let n be a positive integer such that $q^{\lfloor m/2 \rfloor} < n \le q^m - 1$, where $m = \mathrm{ord}_n(q)$. Then the q-cyclotomic coset $C_s = \{sq^j \bmod n : 0 \le j \le m-1\}$ has cardinality m for all s in the range $1 \le s \le nq^{\lceil m/2 \rceil}/(q^m - 1)$. In addition, every s with $s \not\equiv 0 \pmod q$ in this range is a coset leader.

Later in this paper, we will need the following fundamental result on elementary number theory.

Lemma 3: Let $h \ge 1$ and let $a > 1$ be an integer. Then

$$\gcd(a^\ell + 1, a^h - 1) = \begin{cases} 1 & \text{if } \frac{h}{\gcd(\ell,h)} \text{ is odd and } a \text{ is even,} \\ 2 & \text{if } \frac{h}{\gcd(\ell,h)} \text{ is odd and } a \text{ is odd,} \\ a^{\gcd(\ell,h)} + 1 & \text{if } \frac{h}{\gcd(\ell,h)} \text{ is even.} \end{cases}$$

III. Characterisations of LCD Cyclic Codes Over Finite Fields

Let $f(x) = f_h x^h + f_{h-1} x^{h-1} + \cdots + f_1 x + f_0$ be a polynomial over $\mathrm{GF}(q)$ with $f_h \ne 0$ and $f_0 \ne 0$. The reciprocal $f^*(x)$ of $f(x)$ is defined by

$$f^*(x) = f_0^{-1} x^h f(x^{-1}).$$

A polynomial is self-reciprocal if it coincides with its reciprocal.

A code $\mathcal{C}$ is called *reversible* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies that $(c_{n-1}, c_{n-2}, \ldots, c_0) \in \mathcal{C}$. The conclusions of the following theorem are known in the literature (see [18], [14, p. 206]), and are easy to prove. We will employ some of them later.

Theorem 4: ([18], [14, p. 206]): Let $\mathcal{C}$ be a cyclic code of length n over $\mathrm{GF}(q)$ with generator polynomial $g(x)$. Then the following statements are equivalent.

- *$\mathcal{C}$ is an LCD code.*
- *$g(x)$ is self-reciprocal.*
- *β^{-1} is a root of $g(x)$ for every root β of $g(x)$ over the splitting field of $g(x)$.*

Furthermore, if -1 is a power of q mod n, then every cyclic code over $\mathrm{GF}(q)$ of length n is reversible.

Proof: The conclusion of the last part is known [14, p. 206]. But we would present the following proof, which provides hints for studying LCD cyclic codes in the next section.

Let C_a denote the q-cyclotomic class modulo n that contains a, where $0 \le a \le n-1$. By assumption, $q^\ell \equiv -1 \pmod n$ for some positive integer ℓ. Then $a \equiv -aq^\ell \pmod n$. We deduce that $-a \in C_a$. Hence every irreducible factor of $x^n - 1$ is self-reciprocal. It follows that every cyclic code over $\mathrm{GF}(q)$ of length n is reversible. □

Massey showed that reversible cyclic codes are those which have self-reciprocal generator polynomials [12]. It then follows from Theorem 4 that a cyclic code is LCD if and only if it is reversible.

IV. A Construction of All Reversible Cyclic Codes Over GF(q)

The goal in this section is to give an exact count of reversible cyclic codes of length $q^m - 1$ for odd primes m. Recall the q-cyclotomic cosets C_a modulo n and the irreducible polynomials defined in Section II. It is straightforward that $-a = n - a \in C_a$ if and only if $a(1 + q^j) \equiv 0 \pmod n$ for some integer j. The following two lemmas are straightforward.

Lemma 5: The irreducible polynomial $\mathrm{m}_a(x)$ is self-reciprocal if and only if $n - a \in C_a$.

Lemma 6: The least common multiple $\mathrm{lcm}(\mathrm{m}_a(x), \mathrm{m}_{n-a}(x))$ is self-reciprocal for every $a \in \mathbb{Z}_n$.

By Lemma 5, we have that

$$\mathrm{lcm}(\mathrm{m}_a(x), \mathrm{m}_{n-a}(x)) = \begin{cases} \mathrm{m}_a(x) & \text{if } n - a \in C_a, \\ \mathrm{m}_a(x)\mathrm{m}_{n-a}(x) & \text{otherwise.} \end{cases}$$

Let

$$\Pi_{(n,q)} = \Gamma_{(n,q)} \setminus \{\max\{a, \mathrm{Ld}(n-a)\} : a \in \Gamma_{(n,q)}, n - a \notin C_a\},$$

where $\mathrm{Ld}(i)$ denotes the coset leader of C_i. Then $\{C_a \cup C_{n-a} : a \in \Pi_{(q,n)}\}$ is a partition of $\mathbb{Z}_n$.

The following conclusion follows directly from Lemmas 5, 6, and Theorem 4.

Theorem 7: The total number of reversible cyclic codes over $\mathrm{GF}(q)$ of length n is equal to $2^{|\Pi_{(q,n)}|} - 1$.

Every reversible cyclic code over GF(q) *of length* n *is generated by a polynomial*

$$g(x) = \prod_{a \in S} \operatorname{lcm}\left(\mathrm{m}_a(x), \mathrm{m}_{n-a}(x)\right),$$

where S *is a nonempty subset of* $\Pi_{(q,n)}$.

Example 8: Let $(n, q) = (15, 2)$. *There are the following* 2*-cyclotomic classes*

$$\begin{aligned} C_0 &= \{0\}, \\ C_1 &= \{1, 2, 4, 8\}, \\ C_3 &= \{3, 6, 9, 12\}, \\ C_5 &= \{5, 10\}, \\ C_7 &= \{7, 11, 13, 14\}. \end{aligned}$$

We have also

$$x^{15} - 1 = \mathrm{m}_0(x)\mathrm{m}_1(x)\mathrm{m}_3(x)\mathrm{m}_5(x)\mathrm{m}_7(x),$$

where

$$\begin{aligned} \mathrm{m}_0(x) &= x + 1, \\ \mathrm{m}_1(x) &= x^4 + x + 1, \\ \mathrm{m}_3(x) &= x^4 + x^3 + x^2 + x + 1, \\ \mathrm{m}_5(x) &= x^2 + x + 1, \\ \mathrm{m}_7(x) &= x^4 + x^3 + 1. \end{aligned}$$

Note that all $\mathrm{m}_i(x)$ *are self-reciprocal except* $\mathrm{m}_1(x)$ *and* $\mathrm{m}_7(x)$. *In this case,*

$$\Gamma_{(n,q)} = \{0, 1, 3, 5, 7\}.$$

But

$$\Pi_{(n,q)} = \{0, 1, 3, 5\}.$$

Hence, there are 15 reversible binary cyclic codes of length 15.

Corollary 9: Let q *be an even prime power and* $n = q^m - 1$. *If* m *is odd, then the only self-reciprocal irreducible divisor of* $x^n - 1$ *over* GF(q) *is* $x - 1$. *If* m *is an odd prime, then the total number of reversible cyclic codes of length* n *over* GF(q) *is equal to* $2^{\frac{q^m+(m-1)q}{2m}} - 1$.

Proof: Since m is odd and q is even, it then follows from Lemma 3 that $\gcd(q^j + 1, q^m - 1) = 1$ for all j with $0 \le j \le m - 1$. Hence $a(1 + q^j) \equiv 0 \pmod n$ if and only if $a = 0$, where $a \in \mathbb{Z}_n$. We then deduce that the only self-reciprocal irreducible divisor of $x^n - 1$ over GF(q) is $x - 1$.

Since m is a prime, the length of q-cyclotomic cosets module n is either 1 or m. Since $\gcd(q - 1, q^m - 1) = q - 1$, there are exactly $q - 1$ elements in $\mathbb{Z}_n$, i.e, $\{i\frac{q^m-1}{q-1} \mid 0 \le i \le q - 2\}$, such that the corresponding q-cyclotomic cosets have length 1. Note that $0 \in \mathbb{Z}_n$ corresponds to $x - 1$, which is the only self-reciprocal irreducible divisor of $x^n - 1$ over GF(q). Thus, we have

$$|\Pi_{(q,n)}| = \frac{q^m - 1 - (q - 1)}{2m} + \frac{q - 2}{2} + 1 = \frac{q^m + (m - 1)q}{2m}.$$

Hence, in this case, the total number of reversible cyclic codes of length n over GF(q) is $2^{\frac{q^m+(m-1)q}{2m}} - 1$. □

Corollary 10: Let q *be an odd prime power and* $n = q^m - 1$. *If* m *is odd, then the only self-reciprocal irreducible divisor of* $x^n - 1$ *over* GF(q) *are* $x - 1$ *and* $x + 1$. *If* m *is an odd prime, then the total number of reversible cyclic codes of length* n *over* GF(q) *is equal to* $2^{\frac{q^m+(m-1)q+m}{2m}} - 1$.

Proof: Since m is odd and q is odd, by Lemma 3 we have $\gcd(q^j + 1, q^m - 1) = 2$ for all j with $0 \le j \le m - 1$. Hence $a(1 + q^j) \equiv 0 \pmod n$ if and only if $a = 0$ or $a = n/2$, where $a \in \mathbb{Z}_n$. We then deduce that the only self-reciprocal irreducible divisors of $x^n - 1$ over GF(q) are $x \pm 1$.

Since m is a prime, the length of q-cyclotomic cosets module n is either 1 or m. Since $\gcd(q - 1, q^m - 1) = q - 1$, there are exactly $q - 1$ elements in $\mathbb{Z}_n$, i.e, $\{i\frac{q^m-1}{q-1} \mid 0 \le i \le q - 2\}$, such that the corresponding q-cyclotomic cosets have length 1. Note that $0 \in \mathbb{Z}_n$ and $\frac{q^m-1}{2} \in \mathbb{Z}_n$ correspond to $x - 1$ and $x + 1$, which are the only self-reciprocal irreducible divisors of $x^n - 1$ over GF(q). Thus, we have

$$|\Pi_{(q,n)}| = \frac{q^m - 1 - (q - 1)}{2m} + \frac{q - 3}{2} + 2 = \frac{q^m + (m - 1)q + m}{2m}.$$

Hence, in this case, the total number of reversible cyclic codes of length n over GF(q) is $2^{\frac{q^m+(m-1)q+m}{2m}} - 1$. □

V. BCH Codes

Let n be a positive integer, and let $m = \mathrm{ord}_n(q)$. Let α be a generator of GF$(q^m)^*$, and put $\beta = \alpha^{(q^m-1)/n}$. Then β is a primitive n-th root of unity.

For any i with $0 \le i \le n - 1$, let $\mathrm{m}_i(x)$ denote the minimal polynomial of β^i over GF(q). For any $2 \le \delta \le n$, define

$$g_{(q,n,\delta,b)}(x) = \operatorname{lcm}(\mathrm{m}_b(x), \mathrm{m}_{b+1}(x), \cdots, \mathrm{m}_{b+\delta-2}(x)), \quad (4)$$

where b is an integer, lcm denotes the least common multiple of these minimal polynomials, and the addition in the subscript $b+i$ of $\mathrm{m}_{b+i}(x)$ always means the integer addition modulo n. Let $\mathcal{C}_{(q,n,\delta,b)}$ denote the cyclic code of length n with generator polynomial $g_{(q,n,\delta,b)}(x)$. The δ is called a *designed distance* of $\mathcal{C}_{(q,n,\delta,b)}$. The *Bose distance*, denoted δ_B, of a BCH code is the largest designed distance of the code. The BCH bound says that

$$d \ge \delta_B \ge \delta$$

for the code $\mathcal{C}_{(q,n,\delta,b)}$. Thus, determining the Bose distance may improve the lower bound on the minimum distance of $\mathcal{C}_{(q,n,\delta,b)}$.

When $b = 1$, the set $\mathcal{C}_{(q,n,\delta,b)}$ is called a *narrow-sense BCH code* with *designed distance* δ. If $n = q^m - 1$, $\mathcal{C}_{(q,n,\delta,b)}$ is called a *primitive BCH code*.

The following theorem was proved in [1] and contains results in [4] as special cases.

Theorem 11: Let n *be a positive integer such that* $q^{\lfloor m/2 \rfloor} < n \le q^m - 1$, *where* $m = \mathrm{ord}_n(q)$. *Then the narrow-sense BCH code* $\mathcal{C}_{(q,n,\delta,1)}$ *of length* n *and designed distance* δ, *where* $2 \le \delta \le \min\{\lfloor nq^{\lceil m/2 \rceil}/(q^m - 1) \rfloor, n\}$, *has dimension*

$$k = n - m\lceil (\delta - 1)(1 - 1/q) \rceil.$$

Although BCH codes are not asymptotically good, they are among the best linear codes when the length of the codes is

not very large [5, Appendix A]. So far, we have very limited knowledge of BCH codes, as the dimension and minimum distance of BCH codes are in general open, in spite of some recent progress [6], [7]. It is surprising that only two papers on BCH codes of length $q^\ell + 1$ have been published in the literature.

Theorem 11 gives indeed the dimension of some BCH codes, but has the following limitations:

- It applies only to narrow-sense BCH codes with small designed distances. Note that most BCH codes are not narrow-sense codes.
- It is useful only when n is close to $q^m - 1$. For example, it is not useful at all when $n = q^{\lfloor m/2 \rfloor} + 1$.

The following three theorems follow directly from Theorem 4 and the definition of BCH codes, and can be viewed as corollaries of Theorem 4. We will make use of them directly later.

Theorem 12: The BCH code $\mathcal{C}_{(q,n,\delta,b)}$ is reversible when $b = -t$ and the designed distance is $\delta = 2t + 2$ for any nonnegative integer t.

Theorem 13: The BCH code $\mathcal{C}_{(q,n,\delta,b)}$ is reversible when n is odd, $b = (n - t)/2$ and the designed distance is $\delta = t + 2$ for any odd integer t with $1 \le t \le n - 2$.

Theorem 14: The BCH code $\mathcal{C}_{(q,n,\delta,b)}$ is reversible when n is even, $b = (n-2t)/2$ and the designed distance is $\delta = 2t+2$ for any integer t with $0 \le t \le n/2$.

For all the reversible BCH codes described in Theorems 12, 13, and 14, we have obviously the BCH bound on the minimum distance $d \ge \delta$. Little is known about their dimensions. Determining the dimension is a very hard problem in general. We will settle the dimension for some of them in some special cases later.

VI. Some Reversible BCH Codes of Length $q^\ell + 1$ Over GF(q) and Their Parameters

It follows from Theorem 4 that every cyclic code of length $n = q^\ell + 1$ over GF(q) is reversible. Little has been done so far for cyclic codes of length $n = q^\ell + 1$ over GF(q). Only a few papers on such codes are available in the literature. This is because the structure of the q-cyclotomic cosets modulo n is extremely complex. However, we mention that Zetterberg's double-error correcting binary codes have length $2^\ell + 1$ [14, p. 206].

In this section, we will determine the dimensions of a few families of such reversible cyclic codes and improve the BCH bound on their minimum distances by making use of the reversibility. Throughout this section, let $m = 2\ell$ and $n = q^\ell + 1$.

A. A Basic Result on q-Cyclotomic Cosets Modulo n

The following is a basic result and will be employed very often.

Lemma 15: $\mathrm{ord}_n(q) = 2\ell = m$.

Proof: Let h be the least positive integer with $q^h \equiv 1 \pmod n$. Then $q^\ell + 1$ divides $q^h - 1$. The desired conclusion then follows from Lemma 3. □

The following lemma will play an important role in this section.

Lemma 16: Let $\ell \ge 2$. Then every positive integer $a \le q^{\lfloor (\ell-1)/2 \rfloor} + 1$ and $a \not\equiv 0 \pmod q$ is a coset leader and $|C_a| = 2\ell$, and all the remaining positive integers in this range are not coset leaders. In particular, these C_a's are pairwise disjoint for all such a's.

Proof: We prove the conclusions of this lemma only for the case that ℓ is odd, and omit the proof of the conclusions for ℓ being even, which is similar.

Let ℓ be odd from now on. Define $h = \lfloor (\ell - 1)/2 \rfloor = (\ell - 1)/2$. We have then $\ell = 2h + 1$. Recall that $n = q^\ell + 1 = q^{2h+1} + 1$. We first prove that $a := q^h + 1$ is a coset leader and $|C_a| = m = 2\ell$. It can be verified that

$$aq^j \bmod n = \begin{cases} aq^j & \text{if } 1 \le j \le h, \\ (q^{h+1} - 1)q^{j-(h+1)} & \text{if } h + 1 \le j \le 2h, \\ n - (q^h + 1)q^{j-(2h+1)} & \text{if } 2h + 1 \le j \le 3h, \\ n - q^{2h} - q^h & \text{if } j = 3h + 1, \\ n + q^{j-(3h+2)} - q^{j-(2h+1)} & \text{if } 3h + 2 \le j \le 4h + 1. \end{cases}$$

One can then easily check that $aq^j \bmod n > a$ for all j with $1 \le j \le m - 1 = 2\ell - 1 = 4h + 1$. We then deduce that a is a coset leader and $|C_a| = m = 2\ell$.

Let a be an integer with $a \not\equiv 0 \pmod q$ and $1 \le a \le q^h - 1$. Then a can be uniquely expressed as

$$a = \sum_{u=0}^{t} a_u q^{i_u}, \tag{5}$$

where

$$\begin{cases} 0 \le t \le h - 1, \\ i_0 = 0, \\ 1 \le i_1 < i_2 < \cdots < i_t \le h - 1, \\ 1 \le a_i \le q - 1 \text{ for all } i \text{ with } 0 \le i \le t. \end{cases} \tag{6}$$

It then follows that

$$1 \le i_{k_2} - i_{k_1} \le h - 2 \text{ for all } k_2 > k_1 \ge 1 \tag{7}$$

and

$$1 \le i_k - i_0 \le h - 1 \text{ for all } k \ge 1. \tag{8}$$

We now prove that $aq^j \bmod n > a$ for all j with $1 \le j \le 4h + 1$ by distinguishing the following four cases.

Case I ($1 \le j \le h + 1$): In this case, we have clearly that $aq^j \bmod n = aq^j > a$.

Case II ($h + 2 \le j \le 2h$): If $j + i_k \le 2h$ for all k with $1 \le k \le t$, we have then $aq^j \bmod n = aq^j > a$. Otherwise, let k be the smallest integer such that $j + i_k \ge 2h + 1$. We have then $1 \le k \le t$, as $i_0 + j = j \le 2h$. By assumption, we have

$$j + i_u < 2h + 1 \text{ for } u \le k - 1$$

and

$$j + i_u \ge 2h + 1 \text{ for } u \ge k.$$

In this case, we have

$$aq^j \bmod n = \sum_{u=0}^{k-1} a_u q^{i_u+j} - \sum_{u=k}^{t} a_u q^{i_u+j-2h-1}. \quad (9)$$

Notice that

$$2h \geq i_{k-1}+j-(i_t+j-2h-1)=2h+1-(i_t-i_{k-1}) \geq h+2.$$

We see that the right-hand side of (9) is less than n and larger than a.

Case III ($2h+1 \leq j \leq 3h$):

In this case, we have

$$aq^j \equiv -\sum_{u=0}^{t} a_u q^{i_u+j-2h-1} \bmod n.$$

Note that

$$0 \leq i_t + j - 2h - 1 \leq 2h - 2.$$

We get that

$$\begin{aligned} aq^j \bmod n &= q^{2h+1} + 1 - \sum_{u=0}^{t} a_u q^{i_u+j-2h-1} \\ &\geq q^{2h+1} + 1 - (q-1) \sum_{u=2h-t-2}^{2h-2} q^u \\ &= q^{2h+1} - q^{2h-1} + 1 + q^{2h-t-2} \\ &> q^h + 1 \\ &> a. \end{aligned}$$

Case IV ($3h+1 \leq j \leq 4h+1$):

Put $\bar{h} = j - 2h - 1$. Then $h \leq \bar{h} \leq 2h$. In this case, we have

$$aq^j \equiv -\sum_{u=0}^{t} a_u q^{i_u+\bar{h}} \pmod n.$$

If $i_u + \bar{h} \leq 2h$ for all u with $1 \leq u \leq t$, then

$$\begin{aligned} aq^j \bmod n &= q^{2h+1} + 1 - \sum_{u=0}^{t} a_u q^{i_u+\bar{h}} \\ &\geq q^{2h+1} + 1 - (q-1) \sum_{u=2h-t}^{2h} q^u \\ &= 1 + q^{2h-t} \\ &\geq q^{h+1} + 1 \\ &> a. \end{aligned}$$

Otherwise, let k be the smallest integer such that $i_k + \bar{h} \geq 2h+1$. We have then $1 \leq k \leq t$, as $i_0 + \bar{h} = \bar{h} \leq 2h$. Define

$$T_1 = \sum_{u=0}^{k-1} a_u q^{i_u+\bar{h}}$$

and

$$T_2 = \sum_{u=k}^{t} a_u q^{i_u+\bar{h}-(2h+1)} \geq a_k \geq 1.$$

We have then

$$aq^j \equiv -T_1 + T_2 \pmod n.$$

Observe that

$$i_t + \bar{h} - (2h+1) = i_t + j - (4h+2) \leq h - 2$$

and

$$i_0 + \bar{h} = j - (2h+1) \geq h.$$

We conclude that $a_0 q^{i_0+\bar{h}} > T_2$. As a result, $-T_1 + T_2 < 0$. We obtain that

$$\begin{aligned} aq^j \bmod n &= n - T_1 + T_2 \\ &= n - \sum_{u=0}^{k-1} a_u q^{i_u+\bar{h}} + T_2 \\ &\geq n - (q-1) \sum_{u=2h-k+1}^{2h} q^u + T_2 \\ &= q^{2h-k+1} + 1 + T_2 \\ &\geq q^{2h-k+1} + 1 + 1 \\ &\geq q^{h+2} + 2 \\ &> a. \end{aligned}$$

Summarizing all the discussions above, we obtain the desired conclusions. □

B. Reversible BCH Codes Over GF(q) *of Length* $n = q^\ell + 1$

Since $n = q^\ell + 1$ by assumption, the BCH codes $\mathcal{C}_{(q,m,\delta,b)}$ are reversible, and have the BCH bound $d \geq \delta$ for their minimum distances. For some of these BCH codes, we have the following bound, which is much better when δ is getting large.

Theorem 17: Let $n = q^\ell + 1$ and $m = 2\ell$. Then the code $\mathcal{C}_{(q,n,\delta,0)}$ has minimum distance $d \geq 2(\delta - 1)$.

Proof: Let $\beta = \alpha^{q^\ell - 1}$, where α is a generator of GF$(q^m)^*$. By definition, the generator polynomial $g_{(q,n,\delta,0)}(x)$ of this code defined in (4) has the roots β^i for all i in the set

$$\{0, 1, 2, \cdots, \delta - 2\}.$$

It follows from Theorem 4 that this code is reversible. As a result, the polynomial $g_{(q,n,\delta,0)}(x)$ has the roots β^i for all i in the set

$$\{n - (\delta - 2), \cdots, n-2, n-1, 0, 1, 2, \cdots, \delta - 2\}.$$

Again by the BCH bound, we deduce that $d \geq 2(\delta - 1)$. □

Given this much improved lower bound on the minimum distance of the codes $\mathcal{C}_{(q,n,\delta,0)}$, we would like to determine the dimension of these codes. Unfortunately, Lemma 2 and Theorem 11 are useless in this case because

$$\left\lfloor nq^{\lceil m/2 \rceil}/(q^m - 1) \right\rfloor = 1.$$

The lower bound on the minimum distance of the reversible BCH code $\mathcal{C}_{(q,n,\delta,0)}$ is quite tight according to experimental data. However, the determination of the dimension of this code is in general very difficult. We will settle the dimension of this code in a number of special cases in this section.

The main result of this subsection is documented in the following theorem.

Theorem 18: For any integer δ with $3 \le \delta \le q^{\lfloor(\ell-1)/2\rfloor}+3$, the reversible code $\mathcal{C}_{(q,n,\delta,0)}$ has parameters

$$\left[q^\ell+1,\ q^\ell-2\ell\left(\delta-2-\left\lfloor\frac{\delta-2}{q}\right\rfloor\right),\ d\ge 2(\delta-1)\right]$$

and generator polynomial

$$(x-1)\prod_{1\le a\le\delta-2,\ a\not\equiv 0 \pmod q} \mathrm{m}_a(x),$$

where $\mathrm{m}_a(x)$ is the minimal polynomial of β^a over $\mathrm{GF}(q)$ and β is the n-th root of unity in $\mathrm{GF}(q^m)$.

Proof: Note that $0 \le \delta-2 \le q^{\lfloor(\ell-1)/2\rfloor}+1$. By Lemma 16, every integer a with $1 \le a \le \delta-2$ and $a \not\equiv 0 \pmod q$ is a coset leader and all the remaining integers in this range are not coset leaders. The total number of integers a such that $1 \le a \le \delta-2$ and $a \equiv 0 \pmod q$ is equal to $\lfloor(\delta-2)/q\rfloor$. The conclusions on the dimension and generator polynomial then follow from Lemma 16 and the definition of BCH codes. The lower bound on the minimum distance comes from Theorem 17. □

As a special case of Theorem 18, we have the following corollaries.

Corollary 19: Let $q=2$. We have the following.

- *Let $\ell \ge 3$. The reversible code $\mathcal{C}_{(2,n,4,0)}$ has parameters $[2^\ell+1, 2^\ell-2\ell, 6]$ and generator polynomial $(x-1)\mathrm{m}_1(x)$.*
- *Let $\ell \ge 5$. The reversible code $\mathcal{C}_{(2,n,6,0)}$ has parameters $[2^\ell+1, 2^\ell-4\ell, d \ge 10]$ and generator polynomial $(x-1)\mathrm{m}_1(x)\mathrm{m}_3(x)$.*
- *Let $\ell \ge 6$. The reversible code $\mathcal{C}_{(2,n,8,0)}$ has parameters $[2^\ell+1, 2^\ell-6\ell, d \ge 14]$ and generator polynomial $(x-1)\mathrm{m}_1(x)\mathrm{m}_3(x)\mathrm{m}_5(x)$.*
- *Let $\ell \ge 7$. The reversible code $\mathcal{C}_{(2,n,10,0)}$ has parameters $[2^\ell+1, 2^\ell-8\ell, d \ge 18]$ and generator polynomial $(x-1)\mathrm{m}_1(x)\mathrm{m}_3(x)\mathrm{m}_5(x)\mathrm{m}_7(x)$.*

Example 20: We have the following examples for the codes of Corollary 19.

- *When $\ell \in \{3,4,5,6\}$, $\mathcal{C}_{(2,n,4,0)}$ has parameters $[9,2,6]$, $[17,8,6]$, $[32,22,6]$, and $[65,52,6]$, respectively, which are the best possible for cyclic codes* [5, pp. 246, 247, 250, and 261]. *All these codes are optimal linear codes according to the Database.*
- *When $\ell \in \{5,6,7\}$, $\mathcal{C}_{(2,n,6,0)}$ has parameters $[32,12,10]$, $[65,40,10]$, and $[129,100,10]$, respectively, which are the best possible for cyclic codes* [5, pp. 250 and 261].
- *When $\ell \in \{6,7,8\}$, $\mathcal{C}_{(2,n,8,0)}$ has parameters $[65,28,14]$, $[129,86,14]$, and $[257,208,14]$, respectively. The first one is the best possible for cyclic codes* [5, p. 261].

Corollary 21: Let $q=3$. We then have the following statements.

- *Let $\ell \ge 3$. The reversible code $\mathcal{C}_{(3,n,3,0)}$ has parameters $[3^\ell+1, 3^\ell-2\ell, d \ge 4]$ and generator polynomial $(x-1)\mathrm{m}_1(x)$.*
- *Let $\ell \ge 3$. The reversible code $\mathcal{C}_{(3,n,5,0)}$ has parameters $[3^\ell+1, 3^\ell-4\ell, d \ge 8]$ and generator polynomial $(x-1)\mathrm{m}_1(x)\mathrm{m}_2(x)$.*
- *Let $\ell \ge 6$. The reversible code $\mathcal{C}_{(3,n,6,0)}$ has parameters $[3^\ell+1, 3^\ell-6\ell, d \ge 10]$ and generator polynomial $(x-1)\mathrm{m}_1(x)\mathrm{m}_2(x)\mathrm{m}_4(x)$.*

Example 22: We have the following examples of the codes of Corollary 21.

- *When $\ell \in \{3,4\}$, $\mathcal{C}_{(3,n,3,0)}$ has parameters $[28,21,4]$, $[82,73,4]$, respectively. The former has the best possible parameters for cyclic codes* [5, p. 301].
- *When $\ell \in \{3,4\}$, $\mathcal{C}_{(3,n,5,0)}$ has parameters $[28,15,8]$ and $[82,65,8]$, respectively. The former has the best possible parameters for cyclic codes* [5, p. 301].
- *When $\ell \in \{3,4\}$, $\mathcal{C}_{(3,n,6,0)}$ has parameters $[28,9,10]$ and $[82,57,10]$, respectively. The first one is the best possible for cyclic codes* [5, p. 301]. *The latter has the same parameters as the best known code in the Database.*

Conjecture 23: The following conjectures are supported by experimental data.

- *The code $\mathcal{C}_{(3,n,3,0)}$ of Corollary 21 has minimum distance $d=4$.*
- *The code $\mathcal{C}_{(3,n,5,0)}$ of Corollary 21 has minimum distance $d=8$.*

VII. Reversible Cyclic Codes of Length $n = q^m-1$ Over $\mathrm{GF}(q)$

Throughout this section, let $n = q^m-1$ for a positive integer m, and let α be a generator of $\mathrm{GF}(q^m)^*$. Our task in this section is to construct reversible cyclic codes with some known cyclic codes. Our idea is to construct reversible cyclic codes with some known families of cyclic codes $\mathcal{C}$, which are not reversible. Given a cyclic code $\mathcal{C}$, we wish to find out conditions under which the even-like subcode of $\mathcal{C}\cap\mathcal{C}^\perp$ or the code $\mathcal{C}\cap\mathcal{C}^\perp$ is reversible, where the even-like subcode of $\mathcal{C}\cap\mathcal{C}^\perp$ is defined as

$$\{c(x) \in \mathcal{C}\cap\mathcal{C}^\perp : c(1)=0\}.$$

A known class of reversible cyclic codes are the Melas's double-error correcting binary codes with parameters $[2^m-1, 2^m-2m, d\ge 5]$ [14, p. 206].

We now employ the punctured generalised Reed-Muller codes to construct reversible cyclic codes with the construction idea above. To this end, we need to do some preparations.

For any i with $0 \le i \le n-1$, define $\omega_q(i) = \sum_{j=0}^{m-1} i_j$, where $i = \sum_{j=0}^{m-1} i_j q^j$ is the q-adic expansion of i and each $0 \le i_j \le q-1$. We define

$$I_{(q,n,t)} = \{1 \le i \le n-1 : 1 \le \omega_q(j) \le t\} \tag{10}$$

and

$$-I_{(q,n,t)} = \{n-a : a \in I_{(q,n,t)}\},$$

where $t \ge 1$.

Lemma 24: If $1 \le t \le \lceil(q-1)m/2\rceil - 1$, then $I_{(q,n,t)} \cap (-I_{(q,n,t)}) = \emptyset$.

Proof: Note that

$$n = q^m-1 = \sum_{i=0}^{m-1}(q-1)q^i.$$

Hence, we have $\omega_q(i)+\omega_q(n-i) = m(q-1)$ for all $i \in \mathbb{Z}_n$.

By this identity, if $i \in \mathbb{Z}_n$ and $\omega_q(i) \le \lceil (q-1)m/2 \rceil - 1$, then $\omega_q(n-i) > \lceil (q-1)m/2 \rceil - 1$. The desired conclusion then follows. □

Let $\ell = \ell_1(q-1) + \ell_0 < q(m-1)$, where $\ell_0 < q-1$. The ℓ-th order *punctured generalized Reed-Muller code* $\mathcal{R}_q(\ell, m)^*$ over GF(q) is the cyclic code of length $n = q^m - 1$ with generator polynomial

$$g_R(x) := \prod_{\substack{1 \le j \le n-1 \\ \omega_q(j) < (q-1)m - \ell}} (x - \alpha^j), \tag{11}$$

where α is a generator of GF$(q^m)^*$. It is easily seen that $g_R(x)$ is a polynomial over GF(q).

By definition, we have

$$(q-1)m - \ell = (m - \ell_1 - 1)(q-1) + (q - 1 - \ell_0).$$

Let h be the smallest integer with $\omega_q(h) = (q-1)m - \ell$. Then

$$\begin{aligned} h &= (q - 1 - \ell_0) q^{m-\ell_1-1} + \sum_{i=0}^{m-\ell_1-2} (q-1) q^i \\ &= (q - \ell_0) q^{m-\ell_1-1} - 1. \end{aligned}$$

By the construction of the code $\mathcal{R}_q(\ell, m)^*$, every integer u with $0 < u < h$ satisfies $\omega_q(u) < (q-1)m - \ell$. Hence, the elements $\alpha^1, \alpha^2, \ldots, \alpha^{h-1}$ are all roots of the generator polynomial $g_R(x)$ of (11). Consequently, the minimum distance of $\mathcal{R}_q(\ell, m)^*$ is at least h. It was proved in [2, Th. 5.4.1] that the minimum distance of $\mathcal{R}_q(\ell, m)^*$ equals h and the dimension of the code $\mathcal{R}_q(\ell, m)^*$ is equal to

$$\sum_{i=0}^{\ell} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{i - jq + m - 1}{i - jq}. \tag{12}$$

Let $g_R^*(x)$ denote the reciprocal of $g_R(x)$ defined above. Set

$$g(x) = (x-1)\mathrm{lcm}(g_R(x), g_R^*(x)).$$

Let $\mathcal{R}_{(q,m,\ell)}$ denote the cyclic code of length n over GF(q) with generator polynomial $g(x)$. We have then the following theorem.

Theorem 25: If $q(m-1) - 2 \ge \ell \ge 1 + (q-1)m - \lceil (q-1)m/2 \rceil$, then the code $\mathcal{R}_{(q,m,\ell)}$ is reversible and has minimum distance

$$d \ge 2((q - \ell_0) q^{m-\ell_1-1} - 1)$$

and dimension

$$2 \sum_{i=0}^{\ell} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{i - jq + m - 1}{i - jq} - q^m. \tag{13}$$

Proof: When $q(m-1) - 2 \ge \ell \ge 1 + (q-1)m - \lceil (q-1)m/2 \rceil$, it follows from Lemma 24 that $g_R(x)$ and $g_R^*(x)$ have no common roots. Consequently, $g(x) = (x-1) g_R(x) g_R^*(x)$. Therefore,

$$\deg(g(x)) = 2 \deg(g_R(x)) + 1.$$

The desired conclusion on the dimension of the code then follows from the dimension of $\mathcal{R}_q(\ell, m)^*$, which was given in (12). In this case, $g(x)$ has the roots α^i for all i in the set

$$\{n - (h-1), n - (h-2), \cdots, n-2, n-1, \\ 0, 1, 2, \cdots, h-2, h-1\}.$$

The desired conclusion on the minimum distance then follows from the BCH bound. □

The first part of Theorem 25 can be simplified into the following.

Theorem 26: When $q = 2$ and $m - 2 \ge \ell \ge m - \lfloor (m-2)/2 \rfloor$, the code $\mathcal{R}_{(q,m,\ell)}$ is a reversible cyclic code and has parameters

$$\left[2^m - 1,\ 2^m - 2 \sum_{j=0}^{m-1-\ell} \binom{m}{j},\ d \ge 2(2^{m-\ell} - 1) \right].$$

Example 27: Let $m = 5$ and let α be a generator of GF$(2^5)^*$ *with $\alpha^5 + \alpha^2 + 1 = 0$. Then $\mathcal{R}_{(2,5,3)}$ has parameters* $[31, 20, 6]$*, and generator polynomial*

$$g(x) = x^{11} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1.$$

$\mathcal{R}_{(2,5,3)}$ has the best possible parameters for cyclic codes [5, p. 250]*. Its dual code has parameters* $[31, 11, 10]$*, while the best binary cyclic code of length* 31 *and dimension* 11 *has minimum distance* 11 [5, p. 250].

Example 28: Let $m = 6$ and let α be a generator of GF$(2^6)^*$ *with $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$. Then $\mathcal{R}_{(2,6,4)}$ has parameters* $[63, 50, 6]$*, and generator polynomial*

$$g(x) = x^{13} + x^9 + x^7 + x^6 + x^4 + 1.$$

$\mathcal{R}_{(2,6,4)}$ has the best possible parameters for cyclic codes [5, p. 260]*. Its dual code has parameters* $[63, 13, 24]$*, and is the best possible linear code* [5, p. 258].

Example 29: Let $m = 6$ and let α be a generator of GF$(2^6)^*$ *with $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$. Then $\mathcal{R}_{(2,6,3)}$ has parameters* $[63, 20, 14]$*, and generator polynomial*

$$\begin{aligned} g(x) = {} & x^{43} + x^{42} + x^{40} + x^{37} + x^{36} + x^{35} + x^{34} + x^{33} \\ & + x^{29} + x^{25} + x^{22} + x^{21} + x^{18} + x^{14} + x^{10} + x^9 \\ & + x^8 + x^7 + x^6 + x^3 + x + 1. \end{aligned}$$

Its dual code has parameters $[63, 43, 6]$*, which are the best possible parameters* [5, p. 260].

Note that the punctured generalized Reed-Muller codes $\mathcal{R}_q(\ell, m)^*$ are in general not BCH codes. So are the reversible codes $\mathcal{R}_{(q,m,\ell)}$. The following problem is open and interesting.

Open Problem 30: Is it true that the minimum distance $d = 2((q-\ell_0)q^{m-\ell_1-1} - 1)$ for the codes $\mathcal{R}_{(q,m,\ell)}$ of Theorem 25?

VIII. Two Classes of Reversible BCH Cyclic Codes of Length $(q^m - 1)/(q-1)$ Over GF(q)

In this section, we construct a class of reversible cyclic codes from a family of projective BCH codes. Throughout this section, $n = (q^m - 1)/(q-1)$ and $q \ge 3$. We first do some preparations.

Let $\delta \ge 2$ be a positive integer. Define

$$J_{(q,n,\delta)} = \cup_{1 \le i \le \delta - 1} C_i$$

and

$$-J_{(q,n,\delta)} = \{n - a : a \in J_{(q,n,\delta)}\}.$$

We will need the following conclusion.

Lemma 31: Let $\delta = q^e$, where $e = \lfloor (m-1)/2 \rfloor$. Then $J_{(q,n,\delta)} \cap (-J_{(q,n,\delta)}) = \emptyset$.

Proof: Suppose on the contrary that $J_{(q,n,\delta)} \cap (-J_{(q,n,\delta)}) \neq \emptyset$. Then there exist a, $1 \leq i \leq \delta - 1$ and $1 \leq j \leq \delta - 1$ such that

$$a \in C_i \cap (-C_j),$$

which implies that

$$a \equiv iq^{\ell_1} \equiv -jq^{\ell_2} \pmod{n},$$

where $0 \leq \ell_1 \leq m-1$ and $0 \leq \ell_2 \leq m-1$. Without loss of generality, assume that $\ell_2 \geq \ell_1$. Then

$$i + jq^{\ell_2 - \ell_1} \equiv 0 \pmod{n}.$$

Let $\ell = \ell_2 - \ell_1$. Then $0 \leq \ell \leq m-1$. We can further assume that $\ell \leq \lceil (m-1)/2 \rceil$. Otherwise, we have

$$iq^{m-\ell} + j \equiv 0 \pmod{n},$$

where $m - \ell \leq \lceil (m-1)/2 \rceil$.

Since $\ell \leq \lceil (m-1)/2 \rceil$ by assumption and

$$1 \leq i \leq \delta - 1 = q^{\lfloor (m-1)/2 \rfloor} - 1 \quad \text{and}$$
$$1 \leq j \leq \delta - 1 = q^{\lfloor (m-1)/2 \rfloor} - 1,$$

one can verify that

$$0 < i + jq^{\ell} < n,$$

which shows that $i + jq^{\ell} \not\equiv 0 \pmod{n}$. This contradiction proves the lemma. □

One of the main results of this section is the following.

Theorem 32: Let δ be an integer with $2 \leq \delta \leq q^{\lfloor (m-1)/2 \rfloor}$. Then the BCH code $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ is reversible and has length $n = (q^m - 1)/(q-1)$, dimension

$$k = n - 1 - 2m \left\lceil \frac{(\delta - 1)(q-1)}{q} \right\rceil,$$

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

Proof: Let $g_u(x)$ denote the generator polynomial of the BCH code $\mathcal{C}_{(q,n,\delta,1)}$. It follows from Lemma 2 that

$$\deg(g_u(x)) = m \left\lceil \frac{(\delta - 1)(q-1)}{q} \right\rceil.$$

Hence, $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ is reversible. By definition, $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ has generator polynomial

$$g(x) = \operatorname{lcm}(x-1, g_u(x), g_u^*(x)),$$

where $g_u^*(x)$ is the reciprocal of $g_u(x)$. Notice that $2 \leq \delta \leq q^{\lfloor (m-1)/2 \rfloor}$. By Lemma 31, we deduce that

$$g(x) = (x-1) g_u(x) g_u^*(x).$$

The conclusion on the dimension of $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ then follows. The lower bound on the minimum distance comes from the BCH bound. □

Example 33: The following are examples of the code of Theorem 32.

- *When $(q,m,\delta) = (3,4,2)$, $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ has parameters* $[40, 31, 4]$.
- *When $(q,m,\delta) = (3,4,3)$, $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ has parameters* $[40, 23, 8]$, *which are the best possible for cyclic codes* [5, p. 306].
- *When $(q,m,\delta) = (5,3,2)$, $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ has parameters* $[31, 24, 5]$, *which are the best parameters for linear codes according to the Database.*
- *When $(q,m,\delta) = (5,3,3)$, $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ has parameters* $[31, 18, 8]$.
- *When $(q,m,\delta) = (5,3,4)$, $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ has parameters* $[31, 12, 12]$.
- *When $(q,m,\delta) = (5,3,5)$, $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ has parameters* $[31, 6, 19]$.
- *When $(q,m,\delta) = (4,4,3)$, $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ has parameters* $[85, 68, 6]$.

Lemma 34: Let m be a positive even integer and $\delta = q^{m/2}$. Define $\ell = (q^{m/2} - 1)/(q-1)$. Then $s\ell$ is a coset leader for each $1 \leq s \leq q-1$, $|C_{s\ell}| = m$ and $C_{s\ell} = -C_{s\ell}$. In addition,

$$J_{(q,n,\delta)} \cap (-J_{(q,n,\delta)}) = \bigcup_{1 \leq s \leq q-1} C_{s\ell}.$$

Proof: Let m be even and $\bar{m} = m/2$. Recall that

$$n = \frac{q^m - 1}{q-1} \text{ and } \ell = \frac{q^{\bar{m}} - 1}{q-1}$$

We first prove that $s\ell$ is a coset leader and $|C_{s\ell}| = m$ for each s with $1 \leq s \leq q-1$. To this end, we consider $s\ell q^k \bmod n$ by distinguishing the following three cases.

Case I: When $1 \leq k \leq \bar{m} - 1$, it is obvious that

$$s\ell q^k = s \frac{q^{\bar{m}+k} - q^k}{q-1} < n.$$

As a result, $s\ell q^k \bmod n = s\ell q^k > s\ell$.

Case II: When $k = \bar{m}$, $s\ell q^k \bmod n = n - s\ell > s\ell$.

Case III: When $\bar{m} + 1 \leq k \leq m-1$, we have

$$\begin{aligned} s\ell q^k &\equiv s \left(\sum_{i=0}^{k-1-\bar{m}} q^i + \sum_{j=k}^{m-1} q^j \right) \pmod{n} \\ &\equiv -s \sum_{i=k-\bar{m}}^{k-1} q^i \pmod{n}. \end{aligned}$$

It then follows that

$$\begin{aligned} s\ell q^k \bmod n &= n - s \sum_{i=k-\bar{m}}^{k-1} q^i \\ &= \frac{q^m - 1 - s(q^{\bar{m}} - 1) q^{k-\bar{m}}}{q-1} \\ &> s\ell. \end{aligned}$$

Collecting the conclusions in Cases I, II and III yields the desired conclusions on $s\ell$ above. We now proceed to prove the rest of the conclusions of this lemma.

Let a and b be two coset leaders in $J_{(q,n,\delta)}$ such that $C_a = -C_b$. Then there exists a j with $0 \leq j \leq m-1$ such that

$$a + bq^j \equiv 0 \pmod{n}. \tag{14}$$

By assumption, $a \not\equiv 0 \pmod{q}$, $b \not\equiv 0 \pmod{q}$, and

$$1 \leq a \leq q^{\bar{m}} - 1, \quad 1 \leq b \leq q^{\bar{m}} - 1.$$

Let

$$a=\sum_{i=0}^{\bar{m}-1}a_iq^i \quad \text{and} \quad b=\sum_{i=0}^{\bar{m}-1}b_iq^i,$$

where $0\le a_i\le q-1$, $0\le b_i\le q-1$, $a_0\neq 0$ and $b_0\neq 0$.

Below we continue our proof by considering the following three cases.

Case 1: If $j\le \bar{m}-1$, then $\bar{m}+j-1\le m-2$. Consequently,

$$0<a+bq^j=\sum_{i=\bar{m}}^{\bar{m}-1+j}b_{i-j}q^i+\sum_{i=j}^{\bar{m}-1}(a_i+b_{i-j})q^i+\sum_{i=0}^{j-1}a_iq^i<n.$$

This means that

$$a+bq^j \bmod n=a+bq^j\neq 0,$$

which is contrary to (14).

Case 2: If $j=\bar{m}$, then

$$\begin{aligned}bq^j&=\sum_{i=1}^{\bar{m}}b_{\bar{m}-i}q^{m-i}\\&\equiv\sum_{i=2}^{\bar{m}}(b_{\bar{m}-i}-b_{\bar{m}-1})q^{m-i}-b_{\bar{m}-1}\sum_{i=0}^{\bar{m}-1}q^i \pmod n.\end{aligned}$$

We then obtain

$$a+bq^j\equiv T \pmod n,$$

where

$$T=\sum_{i=2}^{\bar{m}}(b_{\bar{m}-i}-b_{\bar{m}-1})q^{m-i}+\sum_{i=0}^{\bar{m}-1}(a_i-b_{\bar{m}-1})q^i.$$

Note that the highest power of q in the expression of T is at most $m-2$. We know that $-n<T<n$. It then follows from (14) that all the coefficients in the expression of T are zero. This implies that

$$a_0=a_1=\cdots=a_{\bar{m}-1}=b_0=b_1=\cdots=b_{\bar{m}-1}.$$

Recall that $a_0\neq 0$ and $b_0\neq 0$. We then deduce that $a=b=s\ell$ for some s with $1\le s\le q-1$. Furthermore, $C_{s\ell}=-C_{s\ell}$.

Case 3: If $\bar{m}+1\le j\le m-1$, then

$$\begin{aligned}bq^j&\equiv\sum_{h=0}^{j-\bar{m}-1}b_{m-j+h}q^h+\sum_{h=j}^{m-1}b_{h-j}q^h \pmod n\\&\equiv\sum_{k=j}^{m-2}(b_{k-j}-b_{m-j-1})q^k-b_{m-j-1}\sum_{h=j-\bar{m}}^{j-1}q^h\\&\quad+\sum_{h=0}^{j-\bar{m}-1}(b_{m-j+h}-b_{m-j-1})q^h \pmod n. \qquad (15)\end{aligned}$$

Case 3.1: If $b_{k-j}-b_{m-j-1}=0$ for all k with $j\le k\le m-2$, then

$$b_0=b_1=\cdots=b_{m-j-1}\neq 0.$$

It then follows from (15) that

$$\begin{aligned}bq^j \bmod n&=n-b_{m-j-1}\sum_{h=j-\bar{m}}^{j-1}q^h\\&\quad+\sum_{h=0}^{j-\bar{m}-1}(b_{m-j+h}-b_{m-j-1})q^h.\end{aligned}$$

Note that $\bar{m}\le j-1\le m-2$ and $1\le a\le q^{\bar{m}}-1$. We arrive at

$$0<a+(bq^j \bmod n)<n,$$

which means that

$$a+bq^j\not\equiv 0 \pmod n.$$

This is contrary to (14).

Case 3.2: If $b_{k-j}-b_{m-j-1}\neq 0$ for some k with $j\le k\le m-2$, let k be the largest such one.

Case 3.2.1: If $b_{k-j}-b_{m-j-1}<0$, it follows from (15) that

$$\begin{aligned}bq^j \bmod n&=n+\sum_{h=j}^{k}(b_{h-j}-b_{m-j-1})q^h-b_{m-j-1}\sum_{h=j-\bar{m}}^{j-1}q^h\\&\quad+\sum_{h=0}^{j-\bar{m}-1}(b_{m-j+h}-b_{m-j-1})q^h.\end{aligned}$$

Recall that $j\le k\le m-2$ and $1\le a\le q^{\bar{m}}-1$. We deduce that

$$0<a+(bq^j \bmod n)<n,$$

which shows that

$$a+bq^j\not\equiv 0 \pmod n.$$

This is contrary to (14).

Case 3.2.2: If $b_{k-j}-b_{m-j-1}>0$, it follows from (15) that

$$\begin{aligned}bq^j \bmod n&=\sum_{h=j}^{k}(b_{h-j}-b_{m-j-1})q^h-b_{m-j-1}\sum_{h=j-\bar{m}}^{j-1}q^h\\&\quad+\sum_{h=0}^{j-\bar{m}-1}(b_{m-j+h}-b_{m-j-1})q^h.\end{aligned}$$

Recall that $\bar{m}\le k\le m-2$ and $1\le a\le q^{\bar{m}}-1$. We conclude that

$$0<a+(bq^j \bmod n)<n,$$

which implies that

$$a+bq^j\not\equiv 0 \pmod n.$$

This is contrary to (14).

Summarizing all the conclusions in Cases 1, 2 and 3, we know that (14) holds if and only if

$$a=b=s\ell \text{ and } j=\frac{m}{2},$$

where $1\le s\le q-1$. This completes the proof of this lemma. □

Lemma 35: Let $m \geq 4$ be even and $n = (q^m - 1)/(q-1)$. Let a be an integer such that $q^{(m-2)/2} \leq a \leq q^{m/2}$ and $a \not\equiv 0 \pmod q$.

1) *When q is even, a is a coset leader with $|C_a| = m$ except that*

$$a = i + 1 + i\frac{q^{m/2} - q}{q-1},$$

where

$$i \in \left\{\frac{q}{2}, \frac{q}{2} + 1, \cdots, \frac{q}{2} + \frac{q-4}{2}\right\}.$$

2) *When $q = 3$, a must be a coset leader.*
When $q > 3$ is odd, a is a coset leader except that

$$a = i + 1 + i\frac{q^{m/2} - q}{q-1},$$

where

$$i \in \left\{\frac{q+1}{2}, \frac{q+1}{2} + 1, \cdots, \frac{q+1}{2} + \frac{q-5}{2}\right\}.$$

In addition, if q is odd and a is a coset leader, then $|C_a| = m$ except that

$$a = \frac{q^{m/2} + 1}{2}$$

with $|C_a| = m/2$.

Proof: Let $\bar{m} = m/2$. Let a be such that $q^{(m-2)/2} \leq a \leq q^{m/2}$ and $a \not\equiv 0 \pmod q$. Then the q-adic expansion of a is of the form

$$a = \sum_{i=0}^{\bar{m}-1} a_i q^i,$$

where $0 \leq a_i \leq q-1$, $a_0 \neq 0$ and $a_{\bar{m}-1} \neq 0$. Then

$$aq^j = \sum_{i=0}^{\bar{m}-1} a_i q^{i+j}$$

for all $j \geq 0$. To prove the desired conclusions of this lemma, we below consider $aq^j \bmod n$ for $1 \leq j \leq m-1$ by distinguishing the following three cases.

Case 1 ($1 \leq j \leq \bar{m} - 1$): In this case, $aq^j \bmod n = aq^j \bmod n > a$.

Case 2 ($j = \bar{m}$): In this case, we have

$$aq^j \equiv \sum_{i=\bar{m}}^{m-2} (a_{i-\bar{m}} - a_{\bar{m}-1}) q^i - a_{\bar{m}-1} \sum_{i=0}^{\bar{m}-1} q^i \pmod n. \quad (16)$$

We continue our discussions of Case 2 by distinguishing the following two subcases.

Case 2.1: In this subcase, we assume that $a_i - a_{\bar{m}-1} = 0$ for all i with $0 \leq i \leq \bar{m} - 2$. It then follows from (16) that

$$aq^j \bmod n = n - a_0\frac{q^{\bar{m}} - 1}{q-1} = \frac{q^m - 1 - a_0(q^{\bar{m}} - 1)}{q-1}$$
$$= \frac{(q^{\bar{m}} - 1)(q^{\bar{m}} + 1 - a_0)}{q-1} > a.$$

Case 2.2: In this subcase, let k be the largest such that $a_k - a_{\bar{m}-1} \neq 0$ and $0 \leq k \leq \bar{m} - 2$. It then follows from (16) that

$$aq^j \equiv \sum_{i=0}^{k} (a_i - a_{\bar{m}-1}) q^{\bar{m}+i} - a_{\bar{m}-1} \sum_{i=0}^{\bar{m}-1} q^i \pmod n. \quad (17)$$

Case 2.2.1: If $a_k - a_{\bar{m}-1} > 0$, it follows from (17) that

$$aq^j \bmod n = \sum_{i=0}^{k} (a_i - a_{\bar{m}-1}) q^{\bar{m}+i} - a_{\bar{m}-1} \sum_{i=0}^{\bar{m}-1} q^i. \quad (18)$$

When $k \geq 1$, we have that $\bar{m} + k \geq (m+2)/2$. It then follows from (18) that $aq^j \bmod n \geq q^{\bar{m}} > a$.

When $k = 0$, by assumption,

$$a_1 - a_{\bar{m}-1} = a_2 - a_{\bar{m}-1} = \cdots = a_{\bar{m}-2} - a_{\bar{m}-1} = 0$$

and

$$a_0 - a_{\bar{m}-1} > 0, \ a_0 \neq 0, \ a_{\bar{m}-1} \neq 0.$$

Consequently,

$$a_1 = a_2 = \cdots = a_{\bar{m}-2} = a_{\bar{m}-1}.$$

By (18), we obtain

$$aq^j \bmod n = (a_0 - a_{\bar{m}-1}) q^{\bar{m}} - a_{\bar{m}-1} \sum_{i=0}^{\bar{m}-1} q^i$$
$$= a_0 q^{\bar{m}} - a_1 \frac{q^{\bar{m}+1} - 1}{q-1}. \quad (19)$$

By definition and the discussions above, we get

$$a = a_0 + a_1 \frac{q^{\bar{m}} - q}{q-1}. \quad (20)$$

Combining (19) and (20), we arrive at

$$aq^j \bmod n - a = \left(a_0 - a_1\frac{q+1}{q-1}\right)(q^{\bar{m}} - 1). \quad (21)$$

If q is even, then $\gcd(q-1, q+1) = 1$. As a result,

$$a_0 - a_1\frac{q+1}{q-1} \neq 0. \quad (22)$$

In this case, it can be verified that the total number of pairs $(a_0, a_1) \in \{1, 2, \cdots, q-1\}^2$ such that $a_0 > a_1$ and

$$a_0 - a_1\frac{q+1}{q-1} < 0$$

is equal to $(q-2)/2$, and those pairs are $(i+1, i)$, where

$$i \in \left\{\frac{q}{2}, \frac{q}{2} + 1, \cdots, \frac{q}{2} + \frac{q-4}{2}\right\}. \quad (23)$$

Consequently, all the a's with $q^{(m-2)/2} \leq a \leq q^{m/2}$ and $a \not\equiv 0 \pmod q$ are coset leaders except that

$$a = (i+1) + i\frac{q^{\bar{m}} - q}{q-1},$$

where i satisfies (23).

If q is odd, then $\gcd(q-1, q+1) = 2$. The only pair $(a_0, a_1) \in \{1, 2, \cdots, q-1\}^2$ such that $a_0 > a_1$ and

$$a_0 - a_1 \frac{q+1}{q-1} = 0 \tag{24}$$

is $((q+1)/2, (q-1)/2)$. In this case,

$$a = \frac{q^{m/2}+1}{2}$$

and $aq^{\bar{m}} \bmod n = a$. It then follows from the conclusion of Case 1 that this a is a coset leader with $|C_a| = m/2$.

It can be verified that the total number of pairs $(a_0, a_1) \in \{1, 2, \cdots, q-1\}^2$ such that $a_0 > a_1$ and

$$a_0 - a_1 \frac{q+1}{q-1} < 0 \tag{25}$$

is equal to $(q-3)/2$, and those pairs are $(i+1, i)$, where

$$i \in \left\{ \frac{q+1}{2}, \frac{q+1}{2}+1, \cdots, \frac{q+1}{2}+\frac{q-5}{2} \right\}. \tag{26}$$

Consequently, all the a's with $q^{(m-2)/2} \le a \le q^{m/2}$ and $a \not\equiv 0 \pmod q$ are coset leaders except that

$$a = (i+1) + i\frac{q^{\bar{m}} - q}{q-1},$$

where i satisfies (26). This completes the discussions in Case 2.2.1.

Case 2.2.2: If $a_k - a_{\bar{m}-1} < 0$, it follows from (17) that

$$aq^j \bmod n = n + \sum_{i=0}^{k} (a_i - a_{\bar{m}-1}) q^{\bar{m}+i} - a_{\bar{m}-1} \sum_{i=0}^{\bar{m}-1} q^i. \tag{27}$$

Note that $\bar{m} + k \le m-2$. It then follows from (27) that

$$aq^j \bmod n \ge q^{\bar{m}} > a.$$

Case 3 ($\bar{m}+1 \le j \le m-1$): In this case, let $\bar{j} = j - (\bar{m}+1)$. Then $0 \le \bar{j} \le \bar{m} - 2$. Note that $(q^m - 1) \equiv 0 \pmod n$. One can check that

$$aq^j \equiv T \bmod n, \tag{28}$$

where

$$T = \sum_{u=0}^{\bar{j}} (a_{\bar{m}-1-\bar{j}+u} - a_{\bar{m}-\bar{j}-2}) q^u - a_{\bar{m}-\bar{j}-2} \sum_{u=\bar{j}+1}^{\bar{j}+\bar{m}} q^u + \sum_{u=\bar{j}+\bar{m}+1}^{m-2} (a_{u-(\bar{j}+\bar{m}+1)} - a_{\bar{m}-\bar{j}-2}) q^u.$$

Case 3.1: If $a_u - a_{\bar{m}-\bar{j}-2} = 0$ for all u with $0 \le u \le \bar{m} - \bar{j} - 3$, then

$$0 \ne a_0 = a_1 = \cdots = a_{\bar{m}-\bar{j}-2}.$$

In this case,

$$aq^j \bmod n = n + \sum_{u=0}^{\bar{j}} (a_{\bar{m}-1-\bar{j}+u} - a_{\bar{m}-\bar{j}-2}) q^u - a_{\bar{m}-\bar{j}-2} \sum_{u=\bar{j}+1}^{\bar{j}+\bar{m}} q^u.$$

Note that $\bar{m} + \bar{j} \le m-2$. We then deduce that

$$aq^j \bmod n \ge q^{\bar{m}} > a.$$

Case 3.2: If $a_u - a_{\bar{m}-\bar{j}-2} \ne 0$ for some u with $0 \le u \le \bar{m} - \bar{j} - 3$, let k be the largest such u. By definition,

$$0 \le k \le \bar{m} - \bar{j} - 3.$$

Case 3.2.1: If $a_k - a_{\bar{m}-\bar{j}-2} > 0$, then $T > 0$. Note that $k \ge \bar{m} + \bar{j} + 1 \ge \bar{m} + 1$. We have

$$aq^j \bmod n = T > a.$$

Case 3.2.2: If $a_k - a_{\bar{m}-\bar{j}-2} < 0$, then $T < 0$. Note that $k + \bar{m} + \bar{j} + 1 \le m-2$. We have

$$aq^j \bmod n = n - T > a.$$

Collecting all the conclusions in Cases 1, 2 and 3, we complete the proof of this lemma. □

Theorem 36: Let $m \ge 4$ be even and $2 \le \delta \le q^{m/2}$. Define

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

Then the BCH code $\mathcal{C}_{(q,n,\delta,1)}$ has length $n = (q^m-1)/(q-1)$, minimum distance $d \ge \delta$, and dimension

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

Proof: Let m be even. The lower bound on the minimum distance comes from the BCH bound. We prove the conclusion on the dimension only for the case that q is odd, and omit the proof of the conclusion for the other case, which is similar.

Let q be odd. When $\epsilon \ge (q-1)/2$, it follows from Lemmas 2 and 35 that the total number of non-coset-leaders b with $(q^{m/2}+1)/2 \le b \le \delta - 1$ is equal to

$$\epsilon - \frac{q+1}{2} + 1 = \epsilon - \frac{q-1}{2}.$$

In this case, $\hat{a} := (q^{m/2}+1)/2 \le \delta - 1$. Hence, $\hat{a}$ is a coset leader with $|C_{\hat{a}}| = m/2$. It follows again from Lemmas 2 and 35 that the total number of coset leaders a with $1 \le a \le \delta - 1$ is equal to

$$\left\lceil \frac{(\delta-1)(q-1)}{q} \right\rceil - \left(\epsilon - \frac{q-1}{2} \right).$$

For all these coset leaders a we have $|C_a| = m$ except that $a = \hat{a}$. The desired conclusion on the dimension then follows.

When $\epsilon < (q-1)/2$, we have $\delta - 1 < (q^{m/2}+1)/2$, it follows from Lemmas 2 and 35, every integer a with $1 \le a \le \delta - 1$ and $a \not\equiv 0 \pmod q$ is a coset leader with $|C_a| = m$. The desired conclusion on the dimension then follows. □

Corollary 37: Let $m \ge 4$ be even and $\delta = q^{m/2}$. Then the code $\mathcal{C}_{(q,n,\delta,1)}$ has length $n = (q^m-1)/(q-1)$, dimension

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

and minimum distance $d \ge \delta + 1$.

Proof: The conclusion on the dimension follows from Theorem 36. The improvement on the lower bound of the

minimum distance is due to the fact that the Bose distance is $\delta+1$ in this case. □

Theorem 38: Let $m \geq 4$ be even and $2 \leq \delta \leq q^{m/2}$. Define

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

Then the BCH code $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ is reversible and has length $n = (q^m-1)/(q-1)$, minimum distance $d \geq 2\delta$, and dimension

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

Proof: Notice that the code $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ is reversible. The lower bound on the minimum distance comes from the BCH bound. Let $g_{(q,n,\delta,1)}(x)$ denote the generator polynomial of the code $\mathcal{C}_{(q,n,\delta,1)}$ of Theorem 36. It then follows from Theorem 36 that

$$\deg(g_{(q,n,\delta,1)}(x)) = \begin{cases} m\lceil(\delta-1)(q-1)/q\rceil-(2\epsilon-(q-2))\frac{m}{2} & \text{if } \epsilon \geq \lfloor\frac{q-1}{2}\rfloor, \\ m\lceil(\delta-1)(q-1)/q\rceil & \text{if } \epsilon < \lfloor\frac{q-1}{2}\rfloor. \end{cases}$$

By definition, the generator polynomial $g_{(q,n,2\delta,1-\delta)}(x)$ of $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ is given by

$$\begin{aligned} g_{(q,n,2\delta,1-\delta)}(x) &= \operatorname{lcm}(x-1, g_{(q,n,\delta,1)}(x), g^*_{(q,n,\delta,1)}(x)) \\ &= (x-1)\frac{g_{(q,n,\delta,1)}(x)g^*_{(q,n,\delta,1)}(x)}{\gcd(g_{(q,n,\delta,1)}(x), g^*_{(q,n,\delta,1)}(x))}, \end{aligned}$$

where $g^*_{(q,n,\delta,1)}(x)$ is the reciprocal of $g_{(q,n,\delta,1)}(x)$. Consequently,

$$\begin{aligned} \deg(g_{(q,n,2\delta,1-\delta)}(x)) = 1 &+ 2\deg(g_{(q,n,\delta,1)}(x)) \\ &- \deg(\gcd(g_{(q,n,\delta,1)}(x), g^*_{(q,n,\delta,1)}(x))). \end{aligned}$$

By Lemma 34, we have

$$\deg(\gcd(g_{(q,n,\delta,1)}(x), g^*_{(q,n,\delta,1)}(x))) = \bar{\epsilon}.$$

The desired conclusion on the dimension of $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ then follows. □

For the two parameters $\bar{\epsilon}$ and ϵ defined in Theorem 38, we have $\bar{\epsilon} = \epsilon$ except in a few cases where $\bar{\epsilon} = \epsilon + 1$.

Corollary 39: Let $m \geq 4$ be even and $\delta = q^{m/2}$. Then the reversible BCH code $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ has length $n = (q^m-1)/(q-1)$, dimension

$$k = n - 1 - 2mq^{(m-2)/2}(q-1) + (2q-3)m,$$

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

Proof: The conclusion on the dimension follows from Theorem 38. The improvement on the lower bound of the minimum distance is due to the fact that the Bose distance is $\delta+1$ in this case. □

Example 40: Let $(q,m,\delta) = (3,4,9)$. Then the code $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ has parameters [40, 3, 20].

Example 41: Let $(q,m,\delta) = (4,4,16)$. Then the code $\mathcal{C}_{(q,n,2\delta,1-\delta)}$ has parameters [85, 8, 34].

IX. Concluding Remarks

The main contributions of this paper are the following:

- The construction of all reversible cyclic codes over finite fields documented in Section IV.
- The construction of the family of reversible cyclic codes of length $n = q^\ell + 1$ over GF(q) and the analysis of their parameters (see Theorem 18).
- The analysis of the family of reversible cyclic codes of length $n = q^m - 1$ over GF(q) (see Theorem 25).
- The analysis of the family of reversible cyclic codes of length $n = (q^m-1)/(q-1)$ over GF(q) (see Theorem 38).

The dimensions of all these codes were settled. Lower bounds on the minimum distances of all the reversible cyclic codes were derived from the BCH bound. In most cases, we conjecture that the lower bounds are actually the minimum distances of the codes. However, it is extremely difficult to determine the minimum distance of these cyclic codes. The reader is cordially invited to settle the open problems and conjectures proposed in this paper.

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 Tracts Mathematics), vol. 103. Cambridge, U.K: Cambridge Univ. Press, 1992.
[3] C. Carlet and S. Guilley, "Complementary dual codes for counter-measures to side-channel attacks," in *Coding Theory and Applications* (CIM Series in Mathematical Sciences), vol. 3, E. R. Pinto Eds. Berlin, Germany: Springer Verlag, 2014, pp. 97–105.
[4] 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, Jul. 1996.
[5] C. Ding, *Codes From Difference Sets*. Singapore: World Scientific, 2015.
[6] C. Ding, "Parameters of several classes of BCH codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5322–5330, Oct. 2015.
[7] 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.
[8] S. T. Dougherty, J.-L. Kim, and B. Özkaya, L. Sok, and P. Solé. (Jun. 2015). "The combinatorics of LCD codes: Linear programming bound and orthogonal matrices." [Online]. Available: https://arxiv.org/abs/1506.01955
[9] M. Esmaeili and S. Yari, "On complementary-dual quasi-cyclic codes," *Finite Fields Appl.*, vol. 15, no. 3, pp. 375–386, Jun. 2009.
[10] C. Güneri, B. Özkaya, and P. Solé, "Quasi-cyclic complementary dual codes," *Finite Fields Appl.*, vol. 42, pp. 67–80, Nov. 2016.
[11] W. C. Huffman and V. Pless, *Fundamentals Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[12] J. L. Massey, "Reversible codes," *Inf. Control*, vol. 7, no. 3, pp. 369–380, Sep. 1964.
[13] J. L. Massey, "Linear codes with complementary duals," *Discrete Math.*, vols. 106–107, pp. 337–342, Sep. 1992.
[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory Error-Correcting Codes* (North-Holland Mathematical Library). Amsterdam, The Netherlands: North-Holland, 1977.
[15] S. K. Muttoo and S. Lal, "A reversible code over GF(q)," *Kybernetika*, vol. 22, no. 1, pp. 85–91, Jan. 1986.

[16] N. Sendrier, "Linear codes with complementary duals meet the Gilbert–Varshamov bound," *Discrete Math.*, vol. 285, nos. 1–3, pp. 345–347, Aug. 2004.
[17] K. Tzeng and C. Hartmann, "On the minimum distance of certain reversible cyclic codes (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 16, no. 5, pp. 644–646, Sep. 1970.
[18] 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, Mar. 1994.

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.

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.