

A Class of Narrow-Sense BCH Codes

Shixin Zhu, Zhonghua Sun, and Xiaoshan Kai

Abstract

BCH codes are an important class of cyclic codes which have applications in satellite communications, DVDs, disk drives, and two-dimensional bar codes. Although BCH codes have been widely studied, their parameters are known for only a few special classes. Recently, Ding et al. made some new progress in BCH codes. However, we still have very limited knowledge on the dimension of BCH codes, not to mention the weight distribution of BCH codes. In this paper, we generalize the results on BCH codes from several previous papers.

- (i) The dimension of narrow-sense BCH codes of length $\frac{q^m-1}{\lambda}$ with designed distance $2 \leq \delta \leq \frac{q^{[(m+1)/2]}-1}{\lambda} + 1$ is settled, where λ is any factor of $q-1$.
- (ii) The weight distributions of two classes of narrow-sense BCH codes of length $\frac{q^m-1}{2}$ with designed distance $\delta = \frac{(q-1)q^{m-1}-q^{[(m-1)/2]}-1}{2}$ and $\delta = \frac{(q-1)q^{m-1}-q^{[(m+1)/2]}-1}{2}$ are determined.
- (iii) The weight distribution of a class of BCH codes of length $\frac{q^m-1}{q-1}$ is determined.

In particular, a subclass of this class of BCH codes is optimal with respect to the Griesmer bound. Some optimal linear codes obtained from this class of BCH codes are characterized.

Keywords: Cyclic codes, BCH codes, Weight distribution

I. INTRODUCTION

A. Backgrounds

Let q be a prime power and \mathbb{F}_q be the finite field with q elements. Let n, k be positive integers with $1 \leq k \leq n$. An $[n, k]$ linear code \mathcal{C} is a subspace of the vector space \mathbb{F}_q^n with dimension k . If this linear code \mathcal{C} is, in addition, closed under the cyclic shift, i.e., $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathcal{C}$ for any $(c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$, then \mathcal{C} is called a cyclic code. Each vector $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$, and a code is identified with the set of polynomial representations of its codewords. A linear code \mathcal{C} of length n over \mathbb{F}_q is cyclic if and only if \mathcal{C} is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$. It is well known that every ideal of $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ is principal. Hence, there is a monic divisor $g(x)$ of $x^n - 1$ such that $\mathcal{C} = \langle g(x) \rangle$. The polynomial $g(x)$ is called the generator polynomial of \mathcal{C} , and $h(x) = \frac{x^n-1}{g(x)}$ is called the parity-check polynomial of \mathcal{C} . If $h(x)$ has t irreducible factors over \mathbb{F}_q , we say such a cyclic code \mathcal{C} has t nonzeros.

Suppose n is a positive integer with $\gcd(n, q) = 1$. Let $m = \text{ord}_n(q)$, i.e., the multiplicative order of q modulo n is m , and α be a primitive element in \mathbb{F}_{q^m} . Assume that $q^m - 1 = n\lambda$ and $\theta = \alpha^\lambda$, then θ is a primitive n -th root of unity. For each $0 \leq i \leq n-1$, let $m_i(x)$ be the minimum polynomial of θ^i over \mathbb{F}_q . A cyclic code of length n over \mathbb{F}_q is called a BCH code with designed distance δ if its generator polynomial is of the form

$$\text{lcm}(m_b(x), m_{b+1}(x), \dots, m_{b+\delta-2}(x)),$$

where lcm denotes the least common multiple of the polynomials, $2 \leq \delta \leq n$ and $b \geq 0$. Denote such a BCH code with designed distance δ by $\mathcal{C}_{(q,m,\lambda,\delta,b)}$. If $b = 1$ it is called a narrow-sense BCH code and we denote it by $\mathcal{C}_{(q,m,\lambda,\delta)}$. Clearly, $\mathcal{C}_{(q,m,\lambda,\delta+1,0)} \subseteq \mathcal{C}_{(q,m,\lambda,\delta)}$. We denote $\mathcal{C}_{(q,m,\lambda+1,0)}$ by $\hat{\mathcal{C}}_{(q,m,\lambda,\delta)}$.

BCH codes were invented by Hocquenghem [18], and independently by Bose and Ray-Chaudhuri [5]. One of the key features of BCH codes is a precise control over the number of symbol errors correctable by the code. Another advantage of BCH codes is that they have efficient encoding and decoding algorithms. Due to BCH codes have such good properties, they are widely used in DVDs, solid-state drives, compact disc players, disk drives, two-dimensional bar codes and satellite communications.

The authors are with the School of Mathematics, Hefei University of Technology, Hefei 230009, China. Their research is supported by the National Natural Science Foundation of China under Grants 61772168 and 61572168. Emails: zhushixin@hfut.edu.cn; sunzhonghuas@163.com; kxs6@sina.com.

TABLE I: KNOWN RESULTS ON DIMENSION OF $\mathcal{C}_{(q,m,\lambda,\delta)}$

λ	δ	Reference
$\lambda = 1$	$\delta = q^t$	[39]
	$\delta = q^{m-2} + 1$	[9]
	$2 \leq \delta \leq q^{\lfloor m/2 \rfloor} + 1;$ $q^{m/2} + 2 \leq \delta \leq 2q^{m/2} + 1, m \text{ even}$	[48]
	$2 \leq \delta \leq q^{\lfloor m/2 \rfloor + 1}$	[29]
$\lambda = q - 1$	$2 \leq \delta \leq q^{m/2}, m \text{ even}$	[28]
	$2 \leq \delta \leq q^{(m+1)/2}, m \text{ odd}$	[29]
$\lambda = q^\ell - 1,$ $m = 2\ell$	$3 \leq \delta \leq q^{\lfloor (\ell-1)/2 \rfloor} + 2$	[28]
	$2 \leq \delta \leq q^{\lfloor (\ell+1)/2 \rfloor} + 1$	[29]
	$2 \leq \delta \leq 2q^{\ell/2} + 3, \ell \text{ even};$ $2 \leq \delta \leq 2q^{(\ell+1)/2} + 2q, \ell \text{ odd.}$	[33]

B. Known Results

BCH codes have been extensively studied in the literature ([1], [2], [4]–[11], [14], [16], [18]–[29], [33]–[40], [42], [45]–[48]). Nonetheless, their parameters are known for only a few special classes. As pointed out by Charpin [6], the dimension and minimum distance of BCH codes are difficult to determine in general. The dimensions of the BCH codes $\mathcal{C}_{(q,m,\lambda,\delta)}$ were investigated in a lot of papers. We roughly list them in the Table I. Besides the results in Table I, for $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$ and $2 \leq \delta \leq \frac{nq^{\lfloor m/2 \rfloor}}{q^m - 1}$, the dimension of $\mathcal{C}_{(q,m,\lambda,\delta)}$ was settled by Aly et al. [3]. Recently, the dimensions of some BCH codes $\mathcal{C}_{(q,m,\lambda,\delta,b)}$ with $b \neq 0, 1$ were settled in [28], [29], [35].

The exact minimum distance of BCH codes has been studied in many literatures ([7], [9]–[11], [14], [20], [23], [34], [36]). The reader is referred to [9] for a recent summary of various results on minimum distance of BCH codes. In general, the problem of determining the weight distribution of BCH codes is very difficult, and it is known for only a few special classes. Not much work has been done on determining the weight distribution of BCH codes. We list them in the following two cases.

- (i) Case 1: $\lambda = 1$. For $\delta = (q-1)q^{m-1} - q^{\lfloor (m-1)/2 \rfloor} - 1$ and $\delta = (q-1)q^{m-1} - q^{\lfloor (m+1)/2 \rfloor} - 1$, when $q = 2$, the weight distribution of $\mathcal{C}_{(q,m,\lambda,\delta)}$ was settled by Kasami [23]; when q is a prime, the weight distribution of $\mathcal{C}_{(q,m,\lambda,\delta)}$ and $\widehat{\mathcal{C}}_{(q,m,\lambda,\delta)}$ was settled by Ding et al. [11]. For $\delta = q^3 - q^2 - q - 2$ and $m = 3$, the weight distribution of $\mathcal{C}_{(q,m,\lambda,\delta)}$ was determined by Yan [45]. Recently, For $\delta = q^m - q^{m-1} - q^i - 1$, where $\frac{m-2}{2} \leq i \leq m - \lfloor \frac{m}{3} \rfloor - 1$, the weight distribution of $\widehat{\mathcal{C}}_{(q,m,\lambda,\delta_i)}$ was determined by Li [34].
- (ii) Case 2: $\lambda = 2$ and $q = 3$. For $\delta_i = 3^{m-1} - 1 - \frac{3^{\lfloor (m+2i-3)/2 \rfloor} - 1}{2}$, where $1 \leq i \leq 2$, the weight distribution of $\mathcal{C}_{(q,m,\lambda,\delta_i)}$ and $\widehat{\mathcal{C}}_{(q,m,\lambda,\delta_i)}$ was settled by Li et al. [36].

C. The contribution of the present paper

The objective of this paper is to study narrow-sense BCH codes over \mathbb{F}_q of length $\frac{q^m-1}{\lambda}$, where λ is a positive factor of $q-1$. The main contributions are the following:

- (i) For $2 \leq \delta \leq \frac{q^{\lfloor (m+1)/2 \rfloor} - 1}{\lambda} + 1$, the dimension of the BCH code $\mathcal{C}_{(q,m,\lambda,\delta)}$ is completely determined. These results generalize those from [28], [29].
- (ii) For $\lambda = 2$ and $\delta_i = \frac{(q-1)q^{m-1} - q^{\lfloor (m+2i-3)/2 \rfloor} - 1}{2}$ with $i = 1, 2$, we give a trace representation for the codewords in $\mathcal{C}_{(q,m,2,\delta_i)}$ and $\widehat{\mathcal{C}}_{(q,m,2,\delta_i)}$. By using exponential sums, the weight distribution of the BCH code $\mathcal{C}_{(q,m,\lambda,\delta_i)}$ and $\widehat{\mathcal{C}}_{(q,m,\lambda,\delta_i)}$ is settled. These results generalize those from [36].
- (iii) For $m = a(q-1) + 1$ or $a(q-1) + 2$ for some integer $a \geq 1$, the first largest q -cyclotomic coset leader modulo $\frac{q^m-1}{q-1}$ is determined, and then the weight distribution of a class of BCH codes of length $\frac{q^m-1}{q-1}$ is determined.

The paper is organized as follows. In Section II, we give some background and recall some basic results on character sums. By using cyclotomic cosets, the dimension of this class of narrow-sense BCH codes is determined in Section III. In Section IV, we find a trace representation for the codewords in $\mathcal{C}_{(q,m,2,\delta_i)}$ and $\widehat{\mathcal{C}}_{(q,m,2,\delta_i)}$, where $\delta_i = \frac{(q-1)q^{m-1} - q^{\lfloor (m+2i-3)/2 \rfloor} - 1}{2}$ with $i = 1, 2$. In addition, by using exponential sums and the theory of quadratic forms over finite fields, the weight distributions of $\mathcal{C}_{(q,m,2,\delta_i)}$ and $\widehat{\mathcal{C}}_{(q,m,2,\delta_i)}$ are determined. Moreover, the weight distribution of a class of BCH codes of length $\frac{q^m-1}{q-1}$ is also determined. Furthermore, a subclass of such BCH

codes meeting the Griesmer bound is presented. Compared with the table of the best known linear codes maintained by Markus Grassl at <http://www.codetables.de/>, which is called the Database later in this paper, these two classes of BCH codes are sometimes among the best linear codes known. Finally, the conclusion of the paper is given in Section V.

II. PRELIMINARIES

Throughout this paper, let λ be a positive divisor of $q-1$ and $n = \frac{q^m-1}{\lambda}$, where $m \geq 2$ is a positive integer. Clearly, $\gcd(n, q) = 1$ and $\text{ord}_n(q) = m$.

Let α be a primitive element of \mathbb{F}_{q^m} and put $\theta = \alpha^\lambda$, then θ is a primitive n -th root of unity. For any $0 \leq i \leq n-1$, the q -cyclotomic coset of i modulo n is defined as $\mathbb{C}_i = \{iq^j \pmod{n} : 0 \leq j \leq l_i - 1\}$, where l_i is the least positive integer such that $iq^{l_i} \equiv i \pmod{n}$ and is the size of \mathbb{C}_i . Obviously, $l_i \mid m$. The smallest element in \mathbb{C}_i is called the coset leader of \mathbb{C}_i . For every $2 \leq \delta \leq n$ and $b \geq 0$, we define

$$g_{(q,m,\lambda,\delta,b)}(x) = \prod_{z \in \mathcal{D}} (x - \theta^z), \quad \text{where } \mathcal{D} = \bigcup_{j=0}^{\delta-2} \mathbb{C}_{b+j}.$$

Obviously, $g_{(q,m,\lambda,\delta,b)}$ is the generator polynomial of $\mathcal{C}_{(q,m,\lambda,\delta,b)}$. If $b = 1$, the dimension of $\mathcal{C}_{(q,m,\lambda,\delta)}$ is

$$\dim(\mathcal{C}_{(q,m,\lambda,\delta)}) = n - \left| \bigcup_{i=1}^{\delta-1} \mathbb{C}_i \right|.$$

Moreover, $\dim(\widehat{\mathcal{C}}_{(q,m,\lambda,\delta)}) = \dim(\mathcal{C}_{(q,m,\lambda,\delta)}) - 1$. The following is the well known BCH bound.

Lemma 1. [40, Ch. 7, Th. 8] *The minimum distance of $\mathcal{C}_{(q,m,\lambda,\delta,b)}$ is at least δ .*

Let p be the characteristic of \mathbb{F}_q , then q is a power of p . Let $\text{Tr}_q^{q^m}$ be the trace mapping from \mathbb{F}_{q^m} to \mathbb{F}_q and $\zeta_p = e^{\frac{2\pi i}{p}}$, where m is a positive integer. For any given $a \in \mathbb{F}_q$, the function $\chi_a(x) = \zeta_p^{\text{Tr}_p^q(ax)}$ is an additive character of \mathbb{F}_q . The character χ_1 is called the canonical character of \mathbb{F}_q . Let β be a fixed primitive element of \mathbb{F}_q . For each $0 \leq j \leq q-2$, the function ψ_j with $\psi_j(\beta^k) = \zeta_p^{jk}$ for $0 \leq k \leq q-2$ defines a multiplicative character of \mathbb{F}_q , and every multiplicative character of \mathbb{F}_q can be defined in this way. The character ψ_0 is called the trivial multiplicative character of \mathbb{F}_q . When q is odd, the character $\psi_{\frac{q-1}{2}}$ is called the quadratic character of \mathbb{F}_q , and is usually denoted by η . Let ψ be a multiplicative character and χ an additive character of \mathbb{F}_q . Then the Gaussian sum $G(\psi, \chi)$ is defined by $G(\psi, \chi) = \sum_{x \in \mathbb{F}_q^*} \psi(x)\chi(x)$. From now on we shall denote the Gaussian sum $G(\eta, \chi_1)$ over \mathbb{F}_q by G_q . The explicit value of G_q is known.

Lemma 2. [32, Theorems 5.15, 5.33] *Let $q = p^s$, where p is an odd prime and s is a positive integer. Then*

$$G_q = \begin{cases} (-1)^{s-1} \sqrt{q} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{s-1} (\sqrt{-1})^s \sqrt{q} & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

and for each $a \in \mathbb{F}_q^*$,

$$\sum_{x \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^q(ax^2)} = \eta(a)G_q - 1,$$

where η is the quadratic character of \mathbb{F}_q .

We recall the following trace representation of cyclic codes, which is a direct consequence of Delsarte's Theorem [13].

Lemma 3. [36, Proposition 18] *Let q be a prime power and $m = \text{ord}_n(q)$. Let θ be a primitive n -th root of unity in \mathbb{F}_{q^m} and C be a cyclic code of length n over \mathbb{F}_q . Suppose C has t nonzeros and let $\theta^{i_1}, \theta^{i_2}, \dots, \theta^{i_t}$ be the t roots of its parity-check polynomial which are not conjugate with each other. Denote the size of the q -cyclotomic coset \mathbb{C}_{i_j} to be m_j , $1 \leq j \leq t$. Then C has the following trace representation*

$$C = \{c(a_1, a_2, \dots, a_t) : a_j \in \mathbb{F}_{q^{m_j}}, 1 \leq j \leq t\},$$

where $c(a_1, a_2, \dots, a_t) = \left(\sum_{j=1}^t \text{Tr}_q^{q^{m_j}}(a_j \theta^{-\ell i_j}) \right)_{\ell=0}^{n-1}$.

We give a brief introduction to the theory of quadratic forms over finite fields, which is used to calculate the weight distribution of BCH codes. Quadratic forms have been well studied ([15], [30], [31], [44], [49]). The form is called a quadratic form over \mathbb{F}_q if is a homogeneous polynomial of degree two in the form

$$Q(x_1, x_2, \dots, x_m) = \sum_{1 \leq i \leq j \leq m} a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{F}_q.$$

If q is odd, for a quadratic form $Q(x_1, x_2, \dots, x_m)$ in m variables over \mathbb{F}_q , there exists a symmetric matrix A of order m over \mathbb{F}_q such that $Q(x) = \mathbf{x}A\mathbf{x}'$, where $\mathbf{x} = (x_0, x_1, \dots, x_{m-1}) \in \mathbb{F}_q^m$ and \mathbf{x}' denotes the transpose of \mathbf{x} . Let $r = \text{rank } A$, then there exists $M \in \text{GL}_m(\mathbb{F}_q)$ such that $B = MAM'$ is a diagonal matrix and $B = \text{diag}(a_1, a_2, \dots, a_r, 0, \dots, 0)$, where $a_i \in \mathbb{F}_q^*$. Let $\nabla = a_1 a_2 \cdots a_r$ and assume that $\nabla = 1$ when $r = 0$. Let η be the quadratic character of \mathbb{F}_q , then $\eta(\nabla)$ is an invariant of M under the conjugate action of $M \in \text{GL}_m(\mathbb{F}_q)$. We identify \mathbb{F}_q^m with the m -dimensional \mathbb{F}_q -vector space. The following results are useful in the sequel.

Lemma 4. [30, Lemma 1] *Let q be an odd prime power and $Q(x)$ be a quadratic form in m variables of rank r over \mathbb{F}_q . Then*

$$\sum_{x \in \mathbb{F}_q^m} \zeta_p^{\text{Tr}_p^q(Q(x))} = \begin{cases} \pm q^{m-\frac{r}{2}} & \text{if } q \equiv 1 \pmod{4}, \\ \pm (\sqrt{-1})^r q^{m-\frac{r}{2}} & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

The following identity holds (see [36, Lemma 9]):

$$\sum_{x \in \mathbb{F}_q^m} \zeta_p^{\text{Tr}_p^q(yQ(x))} = \eta(y^r) \sum_{x \in \mathbb{F}_q^m} \zeta_p^{\text{Tr}_p^q(Q(x))}, \quad \forall y \in \mathbb{F}_q^*,$$

where η is the quadratic character of \mathbb{F}_q .

III. THE DIMENSION OF BCH CODE OF LENGTH $n = \frac{q^m-1}{\lambda}$

In this section, we will determine the dimension of the BCH codes $\mathcal{C}_{(q,m,\lambda,\delta)}$ for $\delta - 1 \leq \frac{q^{\lfloor \frac{m+1}{2} \rfloor} - 1}{\lambda}$. Recall

$$\dim(\mathcal{C}_{(q,m,\lambda,\delta)}) = n - \left| \bigcup_{i=1}^{\delta-1} \mathbb{C}_i \right|.$$

Let $\Gamma_1 = \{i : 1 \leq i \leq \delta - 1 \text{ and } i \not\equiv 0 \pmod{q}\}$. Then $\dim(\mathcal{C}_{(q,m,\lambda,\delta)}) = n - \left| \bigcup_{i \in \Gamma_1} \mathbb{C}_i \right|$, since if $i \equiv 0 \pmod{q}$ there exists an integer j with $1 \leq j < i$ such that $\mathbb{C}_j = \mathbb{C}_i$. Let Γ_2 denote the set of coset leaders in Γ_1 and Γ_3 the set of non coset leader in Γ_1 . Then $\Gamma_1 = \Gamma_2 \cup \Gamma_3$. Note that if $i \in \Gamma_3$, there is an integer $1 \leq j < i$ such that $j \in \mathbb{C}_i$ and j is a coset leader of \mathbb{C}_i . That is, for every $i \in \Gamma_3$, there exists an integer $j \in \Gamma_2$ such that $\mathbb{C}_i = \mathbb{C}_j$. It follows that

$$\begin{aligned} \dim(\mathcal{C}_{(q,m,\lambda,\delta)}) &= n - \sum_{i \in \Gamma_2} |\mathbb{C}_i| \\ &= n - \sum_{i \in \Gamma_1} |\mathbb{C}_i| + \sum_{i \in \Gamma_3} |\mathbb{C}_i|. \end{aligned}$$

Hence, to determine the dimension of the code $\mathcal{C}_{(q,m,\lambda,\delta)}$, we need to find out the coset leader of \mathbb{C}_i and its cardinality for each $i \in \Gamma_1$.

The following result given in [3] will be useful for determining coset leaders when δ is small.

Lemma 5. [3, Lemmas 8, 9] *Let n be an integer with $q^{\lfloor \frac{m}{2} \rfloor} < n \leq q^m - 1$, where $m = \text{ord}_n(q)$. Then the q -cyclotomic coset \mathbb{C}_i has cardinality m for all i in the range $1 \leq i \leq \frac{nq^{\lfloor \frac{m}{2} \rfloor}}{q^m - 1}$. Moreover, the following assert holds: every i with $i \not\equiv 0 \pmod{q}$ in this range is a q -cyclotomic coset leader modulo n .*

When m is odd, by Lemma 5, we have the following conclusion.

Theorem 1. *Let $m \geq 3$ be odd. For every integer δ with $1 \leq \delta - 1 \leq \frac{q^{\frac{m+1}{2}} - 1}{\lambda}$, $\mathcal{C}_{(q,m,\lambda,\delta)}$ has length $n = \frac{q^m - 1}{\lambda}$, minimum distance $d \geq \delta$ and dimension $n - m \left\lfloor \frac{(\delta-1)(q-1)}{q} \right\rfloor$.*

Now we consider the dimension of $\mathcal{C}_{(q,m,\lambda,\delta)}$ when $m = 2h \geq 4$ and $\delta - 1 \leq \frac{q^{h+1} - 1}{\lambda}$. When $\lambda = 1$, the following result was prove in [3], [29], [46], [48].

Lemma 6. Let $m = 2h \geq 4$. Let i be an integer with $1 \leq i \leq \frac{q^{h+1}-1}{\lambda}$ and $i \not\equiv 0 \pmod{q}$. Let $f(a, b, c) = aq^h + \frac{b(q^h-1)}{\lambda} + c$, where a, b, c are integers. Then i is not a q -cyclotomic coset leader modulo n if and only if $i \in \Delta_0 \cup \Delta_1 \cup \Delta_2$, where

$$\begin{aligned}\Delta_0 &= \left\{ f(a, 0, c) : 1 \leq c < a \leq \frac{q-1}{\lambda} \right\}, \\ \Delta_1 &= \left\{ f(a, b, c) : 1 \leq c \leq a < \frac{q-1}{\lambda}, 1 \leq b < \lambda \right\}, \\ \Delta_2 &= \left\{ f(a, b, a+1) : 0 \leq a < \frac{q-1}{\lambda}, \frac{\lambda}{2} < b < \lambda \right\}.\end{aligned}$$

Proof: We claim that an integer $1 \leq i < n$ is not the coset leader in the q -cyclotomic coset of i modulo n if and only if λi is not the coset leader in the q -cyclotomic coset of λi modulo λn . In fact, i is not a coset leader if and only if there exists an integer j with $1 \leq j < i$ such that $i \equiv jq^s \pmod{n}$, for some integer s . Note that $i \equiv jq^s \pmod{n}$ is equivalent to $\lambda i \equiv \lambda jq^s \pmod{\lambda n}$. Hence, the above assert holds.

We divide λ into two cases to prove our result.

- (i) If $\lambda = 1$, an integer i with $1 \leq i \leq q^{h+1} - 1$ and $i \not\equiv 0 \pmod{q}$ is not a coset leader if and only if $i = aq^h + c$, where $1 \leq c < a \leq q - 1$, which has been proven in [29].
- (ii) If $\lambda \geq 2$, an integer i with $1 \leq i \leq \frac{q^{h+1}-1}{\lambda}$ and $i \not\equiv 0 \pmod{q}$ is not the coset leader in the q -cyclotomic coset of i modulo n if and only if λi is not the coset leader in the q -cyclotomic coset of λi modulo λn . From Case (i), $\lambda i = i_h q^h + i_0$ for integers $1 \leq i_0 < i_h \leq q - 1$.
 - (a) If $\lambda \mid i_h$, then $\lambda \mid i_0$. Suppose $i_h = \lambda a$ and $i_0 = \lambda c$. Then, $i = aq^h + c$, where $1 \leq c < a \leq \frac{q-1}{\lambda}$. That is, $i \in \Delta_0$.
 - (b) If $\lambda \nmid i_h$, there exist integers a, b such that $i_h = \lambda a + b$, where $1 \leq b < \lambda$ and $0 \leq a < \frac{q-1}{\lambda}$. Note that $i_0 + i_h \equiv 0 \pmod{\lambda}$, thus, $i_0 = \lambda c - b$, where $c \geq 1$. Notice that $i_h - i_0 = \lambda(a - c) + 2b > 0$. We claim $a - c \geq -1$. Otherwise, $i_h - i_0 \leq 2(b - \lambda) < 0$. We continue our discussions by distinguishing the following two subcases.
 - If $a - c \geq 0$, i.e., $1 \leq c \leq a$, then $i \in \Delta_1$.
 - If $a - c = -1$, then $i_h - i_0 = 2b - \lambda > 0$. It gives $\frac{\lambda}{2} < b < \lambda$. Hence, $i = aq^h + \frac{b(q^h-1)}{\lambda} + a + 1$, where $0 \leq a < \frac{q-1}{\lambda}$ and $\frac{\lambda}{2} < b < \lambda$. That is, $i \in \Delta_2$.

The result follows. ■

Note that

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

Define $\Delta = \{c(q^h+1) : 1 \leq c \leq \frac{q-1}{\lambda}\}$ when λ is odd. Otherwise,

$$\Delta = \left\{ \frac{c(q^h+1)}{2} : 1 \leq c \leq \frac{2(q-1)}{\lambda} \right\}.$$

We have the following conclusion.

Lemma 7. Let Δ be defined as above. Let $m = 2h \geq 4$, and i be an integer with $1 \leq i \leq \frac{q^{h+1}-1}{\lambda}$. Then $|\mathbb{C}_i| = h$ if and only if $i \in \Delta$.

Proof: Clearly, $|\mathbb{C}_i|$ divides m . Notice that $iq^\ell < n$ for each $1 \leq \ell \leq h-1$. Hence, $|\mathbb{C}_i| = h$ if and only if

$$iq^h \equiv i \pmod{n} \iff \lambda i \equiv 0 \pmod{q^h+1}. \quad (2)$$

- (i) If λ is odd, from (1), $\gcd(\lambda, q^h+1) = 1$. It follows from (2) that

$$iq^h \equiv i \pmod{n} \iff i \equiv 0 \pmod{q^h+1}.$$

- (ii) If λ is even, from (1), $\gcd(\lambda, q^h+1) = 2$. It follows from (2) that

$$iq^h \equiv i \pmod{n} \iff i \equiv 0 \pmod{(q^h+1)/2}.$$

The result follows. ■

Combining with Lemmas 6 and 7, we have the following conclusion.

Theorem 2. *Let $m = 2h \geq 4$. Let i be an integer with $1 \leq i \leq \frac{q^{h+1}-1}{\lambda}$ and $i \not\equiv 0 \pmod{q}$. Then i is not a q -cyclotomic coset leader modulo n if and only if $i \in \Delta_0 \cup \Delta_1 \cup \Delta_2$, where Δ_0, Δ_1 and Δ_2 are defined as Lemma 6. Moreover,*

$$|\mathbb{C}_i| = \begin{cases} h & \text{if } i \in \Delta, \\ m & \text{otherwise,} \end{cases}$$

where Δ is defined as above.

Proof: The first statement of this theorem comes from Lemma 6. We now prove that all cosets have only two possible sizes. For every integer i with $1 \leq i \leq \frac{q^{h+1}-1}{\lambda}$, it is clear that $iq^\ell < n$ for all $1 \leq \ell \leq h-1$. This gives that $|\mathbb{C}_i| \geq h$. Notice that $|\mathbb{C}_i|$ divides m , we have $|\mathbb{C}_i| = m$ or h . According to Lemma 7, the result follows. ■

The following corollary can be deduced from Theorem 2.

Corollary 1. *Let $m = 2h \geq 4$, then*

- (i) *if $\lambda \geq 3$ is odd, the smallest i with $i \not\equiv 0 \pmod{q}$ that is not a q -cyclotomic coset leader modulo n is $\frac{(\lambda+1)q^h + \lambda - 1}{2\lambda}$,*
- (ii) *if $\lambda = 2$, the smallest i with $i \not\equiv 0 \pmod{q}$ that is not a q -cyclotomic coset leader modulo n is $\frac{3q^h + 1}{2}$;*
- (iii) *if $\lambda \geq 4$ is even, the smallest i with $i \not\equiv 0 \pmod{q}$ that is not a q -cyclotomic coset leader modulo n is $\frac{(\lambda+2)q^h + \lambda - 2}{2\lambda}$.*

Proof: Recall Δ_i defined as Lemma 6. Let $\min(\Delta_i)$ denote the smallest number in Δ_i for $i = 0, 1, 2$. It is easy to check that $f(a, b, c)$ has the following properties. If $a > a'$, then $f(a, b, c) > f(a', b', c')$ for all $0 \leq b, b' < \lambda$ and $1 \leq c, c' \leq q-1$. If $b > b'$, then $f(a, b, c) > f(a, b', c')$ for all $1 \leq c, c' \leq q-1$. Hence, if $\Delta_i \neq \emptyset$, we have $\min(\Delta_0) = f(2, 0, 1)$, $\min(\Delta_1) = f(1, 1, 1)$ and $\min(\Delta_2) = f(0, \lceil \frac{\lambda+1}{2} \rceil, 1)$. This gives that the smallest i with $i \not\equiv 0 \pmod{q}$ that is not a coset leader is $\min(\Delta_2)$ if $\lambda \geq 3$. Hence, the results of Cases (i) and (iii) are follow.

If $\lambda = 2$ and $q > 3$, then $\Delta_1 \neq \emptyset$ and $\Delta_2 = \emptyset$. It follows that the smallest i with $i \not\equiv 0 \pmod{q}$ that is not a coset leader is $\min(\Delta_1)$. If $\lambda = 2$ and $q = 3$, then $\Delta_0 = \Delta_1 = \Delta_2 = \emptyset$. That is, every integer $i \leq \frac{3^{h+1}-1}{2}$ with $i \not\equiv 0 \pmod{3}$ is a coset leader. Notice that $\frac{(3^{h+1}+1)3^{h-1}}{2} \equiv \frac{3^{h-1}+1}{2} \pmod{n}$, we have that $\frac{3^{h+1}+1}{2}$ is not a coset leader. The proof is completed. ■

For $\lambda = 1$, the result that the smallest i with $i \not\equiv 0 \pmod{q}$ that is not a q -cyclotomic coset leader modulo n is $2q^h + 1$ was shown in [46]. Moreover, for $\delta \leq q^{h+1} - 1$, the dimension of $\mathcal{C}_{(q,m,\lambda,\delta)}$ was determined in [29]. For $\lambda = q-1$, if $\delta \leq q^h$, the dimension of $\mathcal{C}_{(q,m,\lambda,\delta)}$ was determine in [28]. Theorem 3 is a generalization of the results in [28]. With the conclusions on cyclotomic cosets in Theorem 2, we determine the dimension of $\mathcal{C}_{(q,m,\lambda,\delta)}$ with $\lambda \geq 2$ as follows.

Theorem 3. *Let $m = 2h \geq 4$. For every integer δ with $1 \leq \delta - 1 \leq \frac{q^{h+1}-1}{\lambda}$, let $\delta - 1 = \sum_{j=0}^h \delta_j q^j$ and $\bar{\delta} = \left\lceil \frac{(\delta-1)(q-1)}{q} \right\rceil$, where $0 \leq \delta_j \leq q-1$. Then $\mathcal{C}_{(q,m,\lambda,\delta)}$ has length $n = \frac{q^m-1}{\lambda}$, minimum distance $d \geq \delta$ and dimension k , where*

- (i) *if $\delta \leq q^h + 1$, define $\varepsilon = \left\lceil \frac{(\delta-2)\lambda}{q^h-1} \right\rceil$, then*

$$k = \begin{cases} n - m\bar{\delta} & \text{if } \varepsilon < \left\lfloor \frac{\lambda}{2} \right\rfloor, \\ n - m\bar{\delta} + m\left(\varepsilon - \frac{\lambda-1}{2}\right) & \text{if } \left\lfloor \frac{\lambda}{2} \right\rfloor \leq \varepsilon < \lambda, \\ n - m\bar{\delta} + m\left(\frac{\lambda-1}{2}\right) & \text{if } \varepsilon = \lambda. \end{cases}$$

(ii) if $\delta \geq q^h + 2$ and $\delta_h < \frac{q-1}{\lambda}$, define $\vartheta = \left\lfloor \frac{(\delta - 2 - \delta_h q^h)\lambda}{q^h - 1} \right\rfloor$, then

$$k = \begin{cases} n - m\bar{\delta} + m \frac{\lambda\delta_h^2 + 2(\delta_0 - \delta_h) + 1}{2} & \text{if } \delta \leq \delta_h q^h + \delta_h, \\ n - m\bar{\delta} + m \frac{\lambda\delta_h^2}{2} & \text{if } \delta_h q^h + \delta_h < \delta \leq \delta_h q^h + \frac{q^h - 1}{\lambda} + 1, \\ n - m\bar{\delta} + m \frac{\lambda\delta_h^2}{2} + m[(\vartheta - 1)\delta_h + \delta_0 - \frac{\vartheta(q-1)}{\lambda}] & \\ \text{if } \delta_h q^h + \frac{\vartheta(q^h - 1)}{\lambda} + 1 < \delta \leq \delta_h q^h + \frac{\vartheta(q^h - 1)}{\lambda} + \delta_h + 1 \text{ and } 1 \leq \vartheta \leq \frac{\lambda}{2}, \\ n - m\bar{\delta} + m \frac{\lambda\delta_h^2}{2} + m[(\vartheta - 1)\delta_h + \delta_0 - \frac{\vartheta(q-1)}{\lambda}] + m(\vartheta - \frac{\lambda+1}{2}) & \\ \text{if } \delta_h q^h + \frac{\vartheta(q^h - 1)}{\lambda} + 1 < \delta \leq \delta_h q^h + \frac{\vartheta(q^h - 1)}{\lambda} + \delta_h + 1 \text{ and } \vartheta > \frac{\lambda}{2}, \\ n - m\bar{\delta} + m \frac{\lambda\delta_h^2}{2} + m\vartheta\delta_h & \\ \text{if } \delta_h q^h + \frac{\vartheta(q^h - 1)}{\lambda} + \delta_h + 1 < \delta \text{ and } 1 \leq \vartheta < \frac{\lambda}{2}, \\ n - m\bar{\delta} + m \frac{\lambda\delta_h^2}{2} + m\vartheta\delta_h + m(\vartheta - \frac{\lambda-1}{2}) & \\ \text{if } \delta_h q^h + \frac{\vartheta(q^h - 1)}{\lambda} + \delta_h + 1 < \delta \text{ and } \vartheta \geq \frac{\lambda}{2}. \end{cases}$$

(iii) if $\delta \geq q^h + 2$ and $\delta_h = \frac{q-1}{\lambda}$, then

$$k = \begin{cases} n - m\bar{\delta} + m \frac{\lambda\delta_h^2 + 2(\delta_0 - \delta_h) + 1}{2} & \text{if } \delta \leq \delta_h q^h + \delta_h, \\ n - m\bar{\delta} + m \frac{\lambda\delta_h^2}{2} & \text{if } \delta > \delta_h q^h + \delta_h. \end{cases}$$

Proof: The lower bound on the minimum distance comes from Lemma 1. For every integer δ with $1 \leq \delta - 1 \leq \frac{q^{h+1} - 1}{\lambda}$, it follows from Theorem 2 that $|\mathbb{C}_i| = m$ except for $i \in \Delta$, and $i \in \Gamma_1$ is a coset leader except for $i \in \Delta_0 \cup \Delta_1 \cup \Delta_2$. Hence, the dimension of the BCH code $\mathcal{C}_{(q,m,\lambda,\delta)}$ is

$$k = n - m|\Gamma_1| + \frac{m}{2}|\Gamma_1 \cap \Delta| + m \sum_{j=0}^2 |\Gamma_1 \cap \Delta_j|, \quad (3)$$

where Γ_1 , Δ , Δ_0 , Δ_1 and Δ_2 are defined as above. It is easy to see that $|\Gamma_1| = \bar{\delta}$. To determine the dimension, we just need to calculate the values of $|\Gamma_1 \cap \Delta|$ and $|\Gamma_1 \cap \Delta_j|$ for $j = 0, 1, 2$, respectively.

We prove the conclusion on the dimension only for the case that $\delta_h q^h + \frac{\vartheta(q^h - 1)}{\lambda} + 1 < \delta \leq \delta_h q^h + \frac{\vartheta(q^h - 1)}{\lambda} + \delta_h + 1$ and $\vartheta > \frac{\lambda}{2}$, where $\delta_h < \frac{q-1}{\lambda}$, $\lambda \geq 2$ is even integer. The proofs of the other cases are similar, and details are omitted here.

Let $\Gamma = \{i : 1 \leq i \leq \delta_h q^h, \text{ and } i \not\equiv 0 \pmod{q}\}$ and $\Gamma' = \{i : \delta_h q^h + 1 \leq i \leq \delta - 1, \text{ and } i \not\equiv 0 \pmod{q}\}$, then $\Gamma_1 = \Gamma \cup \Gamma'$. It follows from (3) that

$$k = n - m\bar{\delta} + \frac{m}{2}|\Gamma \cap \Delta| + m \sum_{j=0}^2 |\Gamma \cap \Delta_j| + \frac{m}{2}|\Gamma' \cap \Delta| + m \sum_{j=0}^2 |\Gamma' \cap \Delta_j|.$$

It is easy to check the following results are established.

$$\Gamma \cap \Delta = \left\{ \frac{c(q^h + 1)}{2} : 1 \leq c \leq 2\delta_h - 1 \right\},$$

$$\Gamma \cap \Delta_0 = \{f(a, 0, c) : 1 \leq c < a \leq \delta_h - 1\},$$

$$\Gamma \cap \Delta_1 = \{f(a, b, c) : 1 \leq c \leq a \leq \delta_h - 1, 1 \leq b < \lambda\},$$

and

$$\Gamma \cap \Delta_2 = \left\{ f(a, b, a + 1) : 0 \leq a \leq \delta_h - 1, \frac{\lambda}{2} < b < \lambda \right\},$$

where $f(a, b, c)$ is defined as Lemma 6. It follows that

$$k = n - m\bar{\delta} + m \left(\frac{\lambda\delta_h^2 - 2\delta_h + 1}{2} \right) + \frac{m}{2} |\Gamma' \cap \Delta| + m \sum_{i=0}^2 |\Gamma' \cap \Delta_i|.$$

For $\delta_h q^h + \frac{\vartheta(q^h-1)}{\lambda} + 1 < \delta \leq \delta_h q^h + \frac{\vartheta(q^h-1)}{\lambda} + \delta_h + 1$ and $\vartheta > \frac{\lambda}{2}$, we have

$$\delta - 1 = \delta_h q^h + \frac{\vartheta(q-1)}{\lambda} [q^{h-1} + \dots + q] + \delta_0,$$

where $\frac{\vartheta(q-1)}{\lambda} + 1 \leq \delta_0 \leq \frac{\vartheta(q-1)}{\lambda} + \delta_h$. Clearly,

$$\Gamma' \cap \Delta = \left\{ \delta_h(q^h + 1), \frac{(2\delta_h + 1)(q^h + 1)}{2} \right\},$$

$$\Gamma' \cap \Delta_0 = \{f(\delta_h, 0, c) : 1 \leq c < \delta_h\},$$

$$\Gamma' \cap \Delta_1 = \{f(\delta_h, b, c) : 1 \leq c \leq \delta_h, 1 \leq b \leq \vartheta - 1\}$$

$$\cup \left\{ f(\delta_h, \vartheta, c) : 1 \leq c \leq \delta_0 - \frac{\vartheta(q-1)}{\lambda} \right\}.$$

and

$$\Gamma' \cap \Delta_2 = \left\{ f(\delta_h, b, \delta_h + 1) : \frac{\lambda + 2}{2} \leq b \leq \vartheta - 1 \right\}.$$

It follows that

$$k = n - m\bar{\delta} + m \frac{\lambda\delta_h^2}{2} + m \left[(\vartheta - 1)\delta_h + \delta_0 - \frac{\vartheta(q-1)}{\lambda} \right] + m \left(\vartheta - \frac{\lambda + 1}{2} \right).$$

The result follows. \blacksquare

IV. THE WEIGHT DISTRIBUTION OF TWO CLASSES OF BCH CODES

In this section, we study the weight distribution of BCH codes of length $n = \frac{q^m - 1}{\lambda}$, where $m \geq 2$ is an integer. Our main task is to find a trace representation for the codewords in this class of BCH codes. For this reason, we need to find the first few largest q -cyclotomic coset leaders modulo n .

When $\lambda = 1$, the first few largest q -cyclotomic coset leaders modulo n were determined in [11] and [34]. When $\lambda = 2$ and $q = 3$, the first few largest q -cyclotomic coset leaders modulo n were determined in [36]. It seems to be a hard problem to determine the first few largest q -cyclotomic coset leaders modulo n for all q, m and λ . We only deal with the cases $\lambda = 2$ and $\lambda = q - 1$.

For every integer i with $0 \leq i \leq n - 1$, the q -adic expansion of i is defined by $\sum_{\ell=0}^{m-1} i_\ell q^\ell$, where $0 \leq i_\ell \leq q - 1$. We will study the properties of the cyclotomic cosets by using q -adic expansion in the following paper. Let $[a]_n$ be the smallest non-negative integer such that $a \equiv [a]_n \pmod{n}$.

Lemma 8. *Let $1 \leq i \leq n - 1$ be an integer. Denote the q -adic expansion of i by $\sum_{\ell=0}^{m-1} i_\ell q^\ell$. If i is a q -cyclotomic coset leader modulo n , then $0 \leq i_{m-1} \leq \frac{q-1}{\lambda} - 1$ and $i_\ell \geq i_{m-1}$ for all $0 \leq \ell \leq m - 2$.*

Proof: Note that $n = \frac{q-1}{\lambda} \sum_{\ell=0}^{m-1} q^\ell$. From $i \leq n - 1$, there exists an index v with $0 \leq v \leq m - 1$ such that $i_v \leq \frac{q-1}{\lambda} - 1$. If $v = m - 1$, then $i_{m-1} \leq \frac{q-1}{\lambda} - 1$. If $v \leq m - 2$, we have

$$[iq^{m-1-v}]_n = \sum_{\ell=0}^v i_\ell q^{m-1-v+\ell} + \sum_{\ell=v+1}^{m-1} i_\ell q^{\ell-v-1}.$$

From $i \leq [iq^{m-1-v}]_n$, we deduce $i_{m-1} \leq i_v \leq \frac{q-1}{\lambda} - 1$.

We now prove $i_\ell \geq i_{m-1}$ for all $0 \leq \ell \leq m - 2$. If there is an index u such that $i_u < i_{m-1}$, then $[iq^{m-1-u}]_n < i$, which contradicts the fact that i is a coset leader. \blacksquare

A. The weight distribution of BCH codes of length $(q^m - 1)/2$

Throughout this subsection, let q be an odd prime power and $m \geq 2$ be an integer. We will find the first few largest q -cyclotomic coset leaders modulo $n = \frac{q^m - 1}{2}$. Let δ_i denote the i -th largest coset leader, then δ_1 , δ_2 and δ_3 are explicitly given in [36] when $q = 3$.

Lemma 9. *The largest q -cyclotomic coset leader modulo $n = \frac{q^m - 1}{2}$ is*

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

Furthermore, $|\mathbb{C}_{\delta_1}| = m$ when m is odd and $|\mathbb{C}_{\delta_1}| = \frac{m}{2}$ when m is even.

Proof: When $q = 3$, δ_1 was determined in [36]. Now assume $q \geq 5$, we distinguish two cases for even and odd m .

Case 1. $m \geq 3$ is odd. It is easy to see that

$$\mathbb{C}_{\delta_1} = \left\{ \frac{q^m - 1 - q^{\ell-1} - q^{\ell + \frac{m-1}{2}}}{2} : 1 \leq \ell \leq \frac{m-1}{2} \right\} \cup \left\{ \frac{q^m - 1 - q^{\ell-1} - q^{\ell - \frac{m+1}{2}}}{2} : \frac{m+1}{2} \leq \ell \leq m \right\},$$

and the q -adic expansion of δ_1 is

$$\left(\frac{q-3}{2} \right) q^{m-1} + (q-1) \sum_{i=\frac{m-1}{2}}^{m-2} q^i + \left(\frac{q-1}{2} \right) \sum_{i=0}^{\frac{m-3}{2}} q^i.$$

Hence, $|\mathbb{C}_{\delta_1}| = m$ and δ_1 is the smallest integer in \mathbb{C}_{δ_1} . We will prove that δ_1 is the largest integer in the set of all coset leaders. Suppose there exists an integer s with $\delta_1 < s < n$ is a q -cyclotomic coset leader modulo n , by Lemma 8, the q -adic expansion of s must be of the form

$$\left(\frac{q-3}{2} \right) q^{m-1} + (q-1) \sum_{i=\frac{m-1}{2}}^{m-2} q^i + \sum_{i=0}^{\frac{m-3}{2}} s_i q^i,$$

where $s_i \geq \frac{q-3}{2}$ and $\sum_{i=0}^{\frac{m-3}{2}} s_i q^i > \left(\frac{q-1}{2} \right) \sum_{i=0}^{\frac{m-3}{2}} q^i$.

When $m = 3$, we have $\frac{q+1}{2} \leq s_0 \leq (q-1)$. Moreover,

$$[sq^2]_n = \left(s_0 - \frac{q+1}{2} \right) q^2 + (q-1)q + \frac{q-1}{2}.$$

It follows that $[sq^2]_n \leq \delta_1 < s$, and so we arrive at a contradiction. Now consider the case $m \geq 5$ in the following.

Case 1.1. There exists an index v such that $s_v = \frac{q-3}{2}$. From $s > \delta_1$, we obtain $0 \leq v \leq \frac{m-5}{2}$, and

$$[sq^{m-1-v}]_n = \sum_{i=0}^v s_i q^{i+m-1-v} + \left(\frac{q-3}{2} \right) q^{m-2-v} + (q-1) \sum_{i=\frac{m-1}{2}}^{m-2} q^{i-1-v} + \sum_{i=v+1}^{\frac{m-3}{2}} s_i q^{i-v-1}.$$

Note that $m-2-v \geq \frac{m+1}{2}$, we have $[sq^{m-1-v}]_n < s$, which gives a contradiction.

Case 1.2. There exists an index v with $0 \leq v \leq \frac{m-3}{2}$ such that $\frac{q-1}{2} < s_v < q-1$. Then

$$[sq^{m-1-v}]_n = \sum_{i=0}^v \left(s_i - \frac{q-1}{2} \right) q^{i+m-1-v} - q^{m-2-v} + \left(\frac{q-1}{2} \right) \sum_{i=\frac{m-1}{2}}^{m-2} q^{i-1-v} + \sum_{i=v+1}^{\frac{m-3}{2}} \left(s_i - \frac{q-1}{2} \right) q^{i-1-v} \leq \left(\frac{q-3}{2} \right) q^{m-1} + \left(\frac{q-1}{2} \right) \sum_{i=0}^{m-2} q^i < \delta_1.$$

Hence, $[sq^{m-1-v}]_n < s$, a contradiction.

Case 1.3. There exists an index v with $1 \leq v \leq \frac{m-3}{2}$ such that $s_v = \frac{q-1}{2}$ and $s_{v-1} = q-1$. Similar to Case 1.2, we have $[sq^{m-1-v}]_n < s$, a contradiction.

Summarizing the discussions above, we just need to prove that for $s = \left(\frac{q-3}{2}\right)q^{m-1} + (q-1)\sum_{i=v}^{m-2} q^i + \left(\frac{q-1}{2}\right)\sum_{i=0}^{v-1} q^i$, there exists an integer $i \in \mathbb{C}_s$ such that $i < s$, where $0 \leq v \leq \frac{m-3}{2}$. At this point,

$$\begin{aligned} [sq^{m-1-v}]_n &= \frac{q^m - 1 - q^{m-1} - q^{m-2-v}}{2} \\ &\leq \frac{q^m - 1 - q^{m-1} - q^{\frac{m+1}{2}}}{2} < \delta_1 < s. \end{aligned}$$

This gives a contradiction.

Collecting all the conclusions above, we conclude that δ_1 is the largest coset leader for the case that m is odd.

Case 2. $m \geq 2$ is even. It is easy to see that

$$\mathbb{C}_{\delta_1} = \left\{ \frac{q^m - 1 - q^{\ell-1} - q^{\ell+\frac{m}{2}-1}}{2} : 1 \leq \ell \leq \frac{m}{2} \right\}.$$

Clearly, $|\mathbb{C}_{\delta_1}| = \frac{m}{2}$ and δ_1 is the coset leader of \mathbb{C}_{δ_1} . Similarly as in the case that m is odd, one can prove that δ_1 is the largest coset leader for the case that m is even. Details are omitted here.

This completes the proof. \blacksquare

Similarly, we can calculate the second and the third largest q -cyclotomic coset leaders modulo $\frac{q^m-1}{2}$.

Lemma 10. *The second largest q -cyclotomic coset leader modulo $n = \frac{q^m-1}{2}$ is*

$$\delta_2 = \frac{q^m - 1 - q^{m-1} - q^{\lfloor \frac{m+1}{2} \rfloor}}{2}$$

and $|\mathbb{C}_{\delta_2}| = m$.

Proof: When $q = 3$, δ_2 was determined in [36]. Now consider the case $q \geq 5$. The proof is divided into the following two cases according to the parity of m .

Case 1. $m \geq 3$ is odd. It is easy to see that

$$\begin{aligned} \mathbb{C}_{\delta_2} &= \left\{ \frac{q^m - 1 - q^{\ell-1} - q^{\ell+\frac{m+1}{2}}}{2} : 1 \leq \ell \leq \frac{m-3}{2} \right\} \\ &\cup \left\{ \frac{q^m - 1 - q^{\ell-1} - q^{\ell-\frac{m-1}{2}}}{2} : \frac{m-1}{2} \leq \ell \leq m \right\}, \end{aligned}$$

and the q -adic expansion of δ_2 is

$$\left(\frac{q-3}{2}\right)q^{m-1} + (q-1)\sum_{i=\frac{m+1}{2}}^{m-2} q^i + \left(\frac{q-1}{2}\right)\sum_{i=0}^{\frac{m-1}{2}} q^i.$$

Therefore, $|\mathbb{C}_{\delta_2}| = m$ and δ_2 is the smallest integer in \mathbb{C}_{δ_2} . Suppose there exists an integer s with $\delta_2 < s < \delta_1$ is a q -cyclotomic coset leader modulo n , by Lemma 8, the q -adic expansion of s must be of the form

$$\left(\frac{q-3}{2}\right)q^{m-1} + (q-1)\sum_{i=\frac{m+1}{2}}^{m-2} q^i + \sum_{i=0}^{\frac{m-1}{2}} s_i q^i,$$

where $\frac{q-3}{2} \leq s_i \leq q-1$ and

$$\left(\frac{q-1}{2}\right)\sum_{i=0}^{\frac{m-1}{2}} q^i < \sum_{i=0}^{\frac{m-1}{2}} s_i q^i < (q-1)q^{\frac{m-1}{2}} + \left(\frac{q-1}{2}\right)\sum_{i=0}^{\frac{m-3}{2}} q^i. \quad (4)$$

We continue our discussions by distinguishing the following three cases.

Case 1.1. $s_{\frac{m-1}{2}} = \frac{q-1}{2}$. From (4), there exists an index ι with $0 \leq \iota \leq \frac{m-3}{2}$ such that $s_\iota > \frac{q-1}{2}$. Let v be the largest index such that $s_v > \frac{q-1}{2}$. Similar to the proof of Case 1.2 in Lemma 9, we have $[sq^{m-2-v}]_n < s$, which contradicts the fact that s is a coset leader.

Case 1.2. $\frac{q-1}{2} < s_{\frac{m-1}{2}} < q-1$. Similar to Case 1.2 in Lemma 9, we have $[sq^{\frac{m-1}{2}}]_n < s$, a contradiction.

Case 1.3. $s_{\frac{m-1}{2}} = q-1$. From (4), there exists an index ι with $0 \leq \iota \leq \frac{m-3}{2}$ such that $s_\iota < \frac{q-1}{2}$. Let v be the largest index such that $s_v < \frac{q-1}{2}$. Similar to Lemma 9, one can prove that $[sq^{m-1-v}]_n < s$. Hence, s cannot be a coset leader.

Summarizing all the conclusion above, we obtain that δ_2 is the second largest coset leader for the case that m is odd.

Case 2. $m \geq 2$ is even. It is easy to see that

$$\mathbb{C}_{\delta_2} = \left\{ \frac{q^m - 1 - q^{\ell-1} - q^{\ell + \frac{m}{2}}}{2} : 1 \leq \ell \leq \frac{m-2}{2} \right\} \cup \left\{ \frac{q^m - 1 - q^{\ell-1} - q^{\ell - \frac{m}{2}}}{2} : \frac{m}{2} \leq \ell \leq m \right\}.$$

Hence, $|\mathbb{C}_{\delta_2}| = m$ and δ_2 is the coset leader in \mathbb{C}_{δ_2} . Similarly as in the case that m is odd, one can prove that δ_2 is the second largest coset leader for the case that m is even. Details are omitted here.

The desired result follows. \blacksquare

Lemma 11. *Let $m \geq 6$. Then the third largest q -cyclotomic coset leader modulo $n = \frac{q^m-1}{2}$ is*

$$\delta_3 = \frac{q^m - 1 - q^{m-1} - q^{\lfloor \frac{m+3}{2} \rfloor}}{2}.$$

In addition, $|\mathbb{C}_{\delta_3}| = m$.

Proof: When $q = 3$, δ_3 was determined in [36] for $m \geq 9$. We can verify that δ_3 is the third largest coset leader for the case that $6 \leq m \leq 8$. Now consider the case $q \geq 5$. The proof is divided into the following two cases.

Case 1. $m \geq 7$ is odd. We have

$$\mathbb{C}_{\delta_3} = \left\{ \frac{q^m - 1 - q^{\ell-1} - q^{\ell + \frac{m+3}{2}}}{2} : 1 \leq \ell \leq \frac{m-5}{2} \right\} \cup \left\{ \frac{q^m - 1 - q^{\ell-1} - q^{\ell - \frac{m-3}{2}}}{2} : \frac{m-3}{2} \leq \ell \leq m \right\}$$

and the q -adic expansion of δ_3 is

$$\left(\frac{q-3}{2}\right)q^{m-1} + (q-1) \sum_{i=\frac{m+3}{2}}^{m-2} q^i + \left(\frac{q-1}{2}\right) \sum_{i=0}^{\frac{m+1}{2}} q^i.$$

Therefore, $|\mathbb{C}_{\delta_3}| = m$ and δ_3 is the coset leader in \mathbb{C}_{δ_3} . Suppose there exists an integer s with $\delta_3 < s < \delta_2$ is a q -cyclotomic coset leader modulo n , by Lemma 8, the q -adic expansion of s must be of the form

$$\left(\frac{q-3}{2}\right)q^{m-1} + (q-1) \sum_{i=\frac{m+3}{2}}^{m-2} q^i + \sum_{i=0}^{\frac{m+1}{2}} s_i q^i,$$

where $\frac{q-3}{2} \leq s_i \leq q-1$ and

$$\left(\frac{q-1}{2}\right) \sum_{i=0}^{\frac{m+1}{2}} q^i < \sum_{i=0}^{\frac{m+1}{2}} s_i q^i < (q-1)q^{\frac{m+1}{2}} + \left(\frac{q-1}{2}\right) \sum_{i=0}^{\frac{m-1}{2}} q^i. \quad (5)$$

Similar to Lemma 10, we can prove that the following Cases 1.1 and 1.2 are hold.

Case 1.1. $s_{\frac{m+1}{2}} = \frac{q-1}{2}$. Let v be the largest index such that $s_v > \frac{q-1}{2}$, then $[sq^{m-2-v}]_n < s$, which gives a contradiction.

Case 1.2. $\frac{q-1}{2} < s_{\frac{m+1}{2}} < q-1$. Then $[sq^{\frac{m-3}{2}}]_n < s$, we obtains a contradiction.

Case 1.3. $s_{\frac{m+1}{2}} = q-1$. From (5), there exists an index ι with $0 \leq \iota \leq \frac{m-1}{2}$ such that $s_\iota = \frac{q-3}{2}$. Let v be the largest index such that $s_v = \frac{q-3}{2}$. It follows that $s_i = \frac{q-1}{2}$ for all $v+1 \leq i \leq \frac{m-1}{2}$. Then,

$$\begin{aligned} [sq^{m-1-v}]_n &= \sum_{i=0}^v s_i q^{m-1-v+i} + \left(\frac{q-3}{2}\right) q^{m-2-v} \\ &+ (q-1) \sum_{i=\frac{m+1}{2}}^{m-2} q^{i-1-v} + \left(\frac{q-1}{2}\right) \sum_{i=v+1}^{\frac{m-1}{2}} q^{i-1-v}. \end{aligned}$$

If $v \leq \frac{m-3}{2}$, we deduce $[sq^{m-1-v}]_n < s$ since $m-2-v \geq v+1$. If $v = \frac{m-1}{2}$, we continue our discussions of this case by distinguishing the following cases.

Case 1.3.1. If there exists an index v with $1 \leq v \leq \frac{m-3}{2}$ such that $s_v < q-1$, we have $[sq^{\frac{m-1}{2}}]_n < s$, a contradiction.

Case 1.3.2. If $s_{\frac{m-1}{2}} = \frac{q-3}{2}$ and $s_i = q-1$ for all $1 \leq i \leq \frac{m-3}{2}$, we have $[sq^{\frac{m-3}{2}}]_n < s$ since $m-2 > \frac{m+1}{2}$.

Summarizing all the conclusion above, we obtain that δ_3 is the third largest coset leader for the case that m is odd.

Case 2. $m \geq 6$ is even. It is easy to see that

$$\begin{aligned} \mathbb{C}_{\delta_3} &= \left\{ \frac{q^m - 1 - q^{\ell-1} - q^{\ell + \frac{m+2}{2}}}{2} : 1 \leq \ell \leq \frac{m-4}{2} \right\} \\ \cup &\left\{ \frac{q^m - 1 - q^{\ell-1} - q^{\ell - \frac{m-2}{2}}}{2} : \frac{m-2}{2} \leq \ell \leq m \right\} \end{aligned}$$

Obviously, $|\mathbb{C}_{\delta_3}| = m$ and δ_3 is the coset leader in \mathbb{C}_{δ_3} . Similarly as in the case that m is odd, one can prove that δ_3 is the third largest coset leader for the case that m is even. Details are omitted here.

The desired result follows. \blacksquare

Based on the lemmas above, we can calculate the weight distribution of BCH code $\mathcal{C}_{(q,m,2,\delta_i)}$ and $\widehat{\mathcal{C}}_{(q,m,2,\delta_i)}$ as follows.

Theorem 4. *The BCH code $\widehat{\mathcal{C}}_{(q,m,2,\delta_1)}$ has parameters $[\frac{q^m-1}{2}, k, d]$, where*

- (i) if m is odd, then $k = m$ and $d = \frac{(q-1)q^{m-1}}{2}$.
- (ii) if m is even, then $k = \frac{m}{2}$ and $d = \frac{(q-1)(q^{m-1} + q^{k-1})}{2}$.

In addition, $\widehat{\mathcal{C}}_{(q,m,2,\delta_1)}$ has only one nonzero weight, and meets the Griesmer bound.

Proof: Let α be a primitive element of \mathbb{F}_{q^m} , then α^2 is a primitive n -th root of unity in \mathbb{F}_{q^m} . From Lemma 9, the code $\widehat{\mathcal{C}}_{(q,m,2,\delta_1)}$ has one nonzero and $\alpha^{2\delta_1}$ is a root of its parity-check polynomial. The dimension of $\widehat{\mathcal{C}}_{(q,m,2,\delta_1)}$ follows from Lemma 9.

Case 1. m is odd. Notice that $\gcd(2\delta_1, q-1) = \gcd(2, q-1) = 2$, and $\gcd(2\delta_1, \frac{q^m-1}{q-1}) = \gcd(q^{\frac{m-1}{2}} + 1, \frac{q^m-1}{q-1}) = \gcd(q^{\frac{m-1}{2}} + 1, q^{m-1}) = 1$. From Theorem 11 in [41], the result follows.

Case 2. m is even. Let $h = \frac{m}{2}$ and $\tau = q^{m-1} + q^{h-1}$, then $-2\delta_1 \equiv \tau \pmod{q^m - 1}$. By Lemma 3,

$$\widehat{\mathcal{C}}_{(q,m,2,\delta_1)} = \left\{ \left(\text{Tr}_q^{q^h} (a\alpha^{\tau\ell}) \right)_{\ell=0}^{n-1} : a \in \mathbb{F}_{q^h} \right\}.$$

Let $\beta = \alpha^{(q^h+1)}$. Since $\text{Tr}_q^{q^h} (a\alpha^{\tau\ell}) = \text{Tr}_q^{q^h} (a^q \alpha^{q\tau\ell})$, it follows that $\widehat{\mathcal{C}}_{(q,m,2,\delta_1)}$ has the same weight distribution with the following code

$$\left\{ c(a) = \left(\text{Tr}_q^{q^h} (a\beta^\ell) \right)_{\ell=0}^{n-1} : a \in \mathbb{F}_{q^h} \right\}.$$

Let $n' = q^h - 1$ and

$$C' = \left\{ c'(a) = \left(\text{Tr}_q^{q^h} (a\beta^\ell) \right)_{\ell=0}^{n'-1} : a \in \mathbb{F}_{q^h} \right\}.$$

Clearly,

$$\begin{aligned} w(c'(a)) &= n' - \left| \left\{ \ell : \text{Tr}_q^{q^h}(a\beta^\ell) = 0, 0 \leq \ell \leq n' - 1 \right\} \right| \\ &= n' - \left| \left\{ x \in \mathbb{F}_q^* : \text{Tr}_q^{q^h}(ax) = 0 \right\} \right|. \end{aligned}$$

Hence, C' is a $[q^h - 1, h, q^h - q^{h-1}]$ one-weight code over \mathbb{F}_q . It is easy to check that

$$c(a) = \overbrace{c'(a) \parallel \cdots \parallel c'(a)}^{(q^h+1)/2},$$

where \parallel denotes the concatenation of vectors. Hence, $\widehat{C}_{(q,m,2,\delta_1)}$ is a $[n, h, \frac{(q-1)(q^{m-1}+q^{h-1})}{2}]$ one-weight code over \mathbb{F}_q .

Let C be a linear code of length n over \mathbb{F}_q with dimension k and minimum distance d . Recall the Griesmer bound (see [17]) for C is $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$, where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x . It is easy to check that $\widehat{C}_{(q,m,2,\delta_1)}$ meets the Griesmer bound, and hence is optimal. \blacksquare

Remark 1. *It is well known that all one-weight code with dual weight at least 2 have been completely characterized by Wolfmann [43]. Moreover, a set of characterizations for the one-weight irreducible cyclic codes was introduced by Vega [41]. Hence, the result of Theorem 4 is not new. However, we show that this class of BCH code is also one-weight code.*

In the following theorem, we calculate the weight distribution of BCH code $\mathcal{C}_{(q,m,2,\delta_1)}$.

Theorem 5. *The BCH code $\mathcal{C}_{(q,m,2,\delta_1)}$ has parameters $[\frac{q^m-1}{2}, k, \delta_1]$, where*

- (i) *if m is odd, then $k = m + 1$ and $\mathcal{C}_{(q,m,2,\delta_1)}$ is a four-weight code. In addition, the weight distribution of $\mathcal{C}_{(q,m,2,\delta_1)}$ is listed in Table II.*
- (ii) *if m is even, then $k = \frac{m}{2} + 1$ and $\mathcal{C}_{(q,m,2,\delta_1)}$ is a three-weight code if $m \geq 4$. In addition, the weight distribution of $\mathcal{C}_{(q,m,2,\delta_1)}$ is listed in Table III.*

Proof: Let α be a primitive element of \mathbb{F}_{q^m} , then α^2 is a primitive n -th root of unity in \mathbb{F}_{q^m} . From Lemma 9, the code $\mathcal{C}_{(q,m,2,\delta_1)}$ has two nonzeros, and 1 and $\alpha^{2\delta_1}$ are two non-conjugate roots of its parity-check polynomial. The dimension of $\mathcal{C}_{(q,m,2,\delta_1)}$ follows from Lemma 9.

Case 1. m is odd. Let $\tau = q^{m-1} + q^{\frac{m-1}{2}}$. From Lemmas 3 and 9,

$$\mathcal{C}_{(q,m,2,\delta_1)} = \left\{ \left(\text{Tr}_q^{q^m}(a\alpha^{\tau\ell}) + b \right)_{\ell=0}^{n-1} : a \in \mathbb{F}_{q^m}, b \in \mathbb{F}_q \right\}.$$

Note that $\gcd(\tau, q^m - 1) = \gcd(q^{\frac{m-1}{2}} + 1, q^m - 1) = \gcd(q^{\frac{m-1}{2}} + 1, q - 1) = 2$. Hence, $\mathcal{C}_{(q,m,2,\delta_1)}$ has the same weight distribution with the following code

$$\left\{ c(a, b) = \left(\text{Tr}_q^{q^m}(a\alpha^{2\ell}) + b \right)_{\ell=0}^{n-1} : a \in \mathbb{F}_{q^m}, b \in \mathbb{F}_q \right\}.$$

If $a = 0$, then $w(c(a, b)) = \frac{q^m-1}{2}$ for each $b \in \mathbb{F}_q^*$. If $b = 0$, from Theorem 4, $w(c(a, b)) = \frac{(q-1)q^{m-1}}{2}$ for each $a \in \mathbb{F}_{q^m}^*$. If $a \neq 0$ and $b \neq 0$, then

$$\begin{aligned} w(c(a, b)) &= n - \sum_{\ell=0}^{n-1} \frac{1}{q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(y \text{Tr}_q^{q^m}(a\alpha^{2\ell}) + yb)} \\ &= n - \frac{1}{q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(yb)} \sum_{\ell=0}^{n-1} \zeta_p^{\text{Tr}_p^q(ay\alpha^{2\ell})} \\ &= \frac{(q-1)n}{q} - \frac{1}{q} \sum_{y \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^q(yb)} \sum_{\ell=0}^{n-1} \zeta_p^{\text{Tr}_p^q(ay\alpha^{2\ell})}. \end{aligned}$$

Note that

$$\begin{aligned} \sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\text{Tr}_p^{q^m}(axy^2)} &= \sum_{\ell=0}^{2n-1} \zeta_p^{\text{Tr}_p^{q^m}(ay\alpha^{2\ell})} \\ &= \sum_{\ell=0}^{n-1} \left[\zeta_p^{\text{Tr}_p^{q^m}(ay\alpha^{2\ell})} + \zeta_p^{\text{Tr}_p^{q^m}(ay\alpha^{2(\ell+n)})} \right] \end{aligned} \quad (6)$$

and $\text{ord}(\alpha) = 2n$, thus,

$$\sum_{\ell=0}^{n-1} \zeta_p^{\text{Tr}_p^{q^m}(ay\alpha^{2\ell})} = \frac{1}{2} \sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\text{Tr}_p^{q^m}(axy^2)}.$$

It follows that

$$w(c(a, b)) = \frac{(q-1)n}{q} - \frac{1}{2q} \sum_{y \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^q(yb)} \sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\text{Tr}_p^{q^m}(axy^2)}.$$

From Lemma 2,

$$\sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\text{Tr}_p^{q^m}(axy^2)} = \eta(ay)G_{q^m} - 1.$$

where η is the quadratic character of \mathbb{F}_{q^m} . We define a function $\eta'(y) = \eta(y)$, $y \in \mathbb{F}_q$. Since m is odd, η' is the quadratic character of \mathbb{F}_q . Hence,

$$\begin{aligned} w(c(a, b)) &= \frac{(q-1)n}{q} - \frac{1}{2q} \sum_{y \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^q(yb)} (\eta(ay)G_{q^m} - 1) \\ &= \frac{(q-1)n}{q} - \frac{1}{2q} - \frac{\eta(a)G_{q^m}}{2q} \sum_{y \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^q(yb)} \eta(y). \end{aligned}$$

Note that

$$\begin{aligned} \sum_{y \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^q(yb)} \eta(y) &= \sum_{y \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^q(yb)} \eta'(y) \\ &= \eta'(b^{-1})G_q = \eta(b)G_q, \end{aligned}$$

$$\text{we have } w(c(a, b)) = \frac{q^m - q^{m-1} - 1}{2} - \frac{\eta(ab)G_q G_{q^m}}{2q}.$$

Assume $s = [\mathbb{F}_q : \mathbb{F}_p]$, from Lemma 2, if $p \equiv 1 \pmod{4}$, then $w(c(a, b)) = \frac{q^m - q^{m-1} - \eta(ab)q^{\frac{m-1}{2}} - 1}{2}$. If $p \equiv 3 \pmod{4}$, then

$$w(c(a, b)) = \frac{q^m - q^{m-1} - \eta(ab)(-1)^{\frac{(m+1)s}{2}} q^{\frac{m-1}{2}} - 1}{2}.$$

Let $n_\varepsilon = |\{(a, b) \in \mathbb{F}_{q^m}^* \times \mathbb{F}_q^* : \eta(ab) = \varepsilon\}|$, where $\varepsilon = 1$ or -1 , it is easy to check that $n_1 = n_{-1} = \frac{(q-1)(q^m-1)}{2}$. The weight distribution then follows.

Case 2. m is even. Similar to Case 1, $\mathcal{C}_{(q, m, 2, \delta_1)}$ has the same weight distribution with the following code

$$\left\{ c(a, b) = \left(\text{Tr}_q^{q^h}(a\beta^\ell) + b \right)_{\ell=0}^{n-1} : a \in \mathbb{F}_{q^h}, b \in \mathbb{F}_q \right\},$$

where $h = \frac{m}{2}$ and $\beta = \alpha^{(q^h+1)}$.

TABLE II: THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{(q,m,2,\delta_1)}$ WHEN m IS ODD

Weight	Frequency
0	1
$\frac{q^m - q^{m-1} - q^{\frac{m-1}{2}} - 1}{2}$	$\frac{(q-1)(q^m - 1)}{2}$
$\frac{q^m - q^{m-1}}{2}$	$q^m - 1$
$\frac{q^m - q^{m-1} + q^{\frac{m-1}{2}} - 1}{2}$	$\frac{(q-1)(q^m - 1)}{2}$
$\frac{q^{m-1} - 1}{2}$	$q - 1$

TABLE III: THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{(q,m,2,\delta_1)}$ WHEN m IS EVEN

Weight	Frequency
0	1
$\frac{q^m - q^{m-1} - q^{\frac{m}{2}} - 1}{2}$	$(q-1)\left(q^{\frac{m}{2}} - 1\right)$
$\frac{(q-1)(q^{m-1} + q^{\frac{m}{2}} - 1)}{2}$	$q^{\frac{m}{2}} - 1$
$\frac{q^{m-1} - 1}{2}$	$q - 1$

If $a = 0$, we have $w(c(a, b)) = \frac{q^m - 1}{2}$ for each $b \in \mathbb{F}_q^*$. If $b = 0$, it follows from Theorem 4 that $w(c(a, b)) = \frac{(q-1)(q^{m-1} + q^{h-1})}{2}$ for each $a \in \mathbb{F}_{q^h}^*$. If $a \neq 0$ and $b \neq 0$, then

$$\begin{aligned}
w(c(a, b)) &= n - \sum_{\ell=0}^{n-1} \frac{1}{q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(y \text{Tr}_q^{q^h}(a\beta^\ell) + yb)} \\
&= n - \frac{1}{q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(yb)} \sum_{\ell=0}^{n-1} \zeta_p^{\text{Tr}_p^{q^h}(ay\beta^\ell)} \\
&= n - \frac{1}{q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(yb)} \sum_{\ell_2=0}^{q^h-2} \sum_{\ell_1=0}^{\frac{q^h-1}{2}} \zeta_p^{\text{Tr}_p^{q^h}(ay\beta^{[(q^h-1)\ell_1 + \ell_2]})}.
\end{aligned}$$

Note that $\text{ord}(\beta) = q^h - 1$, we have

$$\begin{aligned}
w(c(a, b)) &= n - \frac{q^h + 1}{2q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(yb)} \sum_{\ell_2=0}^{q^h-2} \zeta_p^{\text{Tr}_p^{q^h}(ay\beta^{\ell_2})} \\
&= n - \frac{q^h + 1}{2q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(yb)} \sum_{x \in \mathbb{F}_{q^h}^*} \zeta_p^{\text{Tr}_p^{q^h}(ayx)} \\
&= n - \frac{q^h + 1}{2q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(yb)} \sum_{x \in \mathbb{F}_{q^h}} \zeta_p^{\text{Tr}_p^{q^h}(ayx)}
\end{aligned}$$

By using the orthogonality relations for additive characters, we have

$$w(c(a, b)) = n - \frac{q^h + 1}{2q} q^h = \frac{q^m - q^{m-1} - q^{h-1} - 1}{2}.$$

This completes the proof. ■

Example 1. When $(q, m) = (3, 3)$, the BCH code $\mathcal{C}_{(q,m,2,\delta_1)}$ is a $[13, 4, 7]$ code over \mathbb{F}_3 with weight enumerator $1 + 26z^7 + 26z^9 + 26z^{10} + 2z^{13}$. It has the same parameters with the best known linear code in the Database.

Example 2. When $(q, m) = (5, 3)$, the BCH code $\mathcal{C}_{(q,m,2,\delta_1)}$ is a $[62, 4, 47]$ code over \mathbb{F}_5 with weight enumerator $1 + 248z^{47} + 124z^{50} + 248z^{52} + 4z^{62}$. The best known linear code over \mathbb{F}_5 with length 62 and dimension 4 has minimum distance 48.

Let $m \geq 3$ be odd and α be a primitive element of \mathbb{F}_{q^m} , then α^2 is a primitive n -th root of unity in \mathbb{F}_{q^m} . From Lemmas 9 and 10, the code $\widehat{\mathcal{C}}_{(q,m,2,\delta_2)}$ has two nonzeros, and $\alpha^{2\delta_1}$ and $\alpha^{2\delta_2}$ are two non-conjugate roots of its parity-check polynomial. Let $\rho_1 = q^{m-1} + q^{\frac{m-1}{2}}$ and $\rho_2 = q^{m-1} + q^{\frac{m+1}{2}}$. By Lemma 3,

$$\widehat{\mathcal{C}}_{(q,m,2,\delta_2)} = \left\{ \left(\text{Tr}_q^{q^m} (a\alpha^{\ell\rho_1} + b\alpha^{\ell\rho_2}) \right)_{\ell=0}^{n-1} : a, b \in \mathbb{F}_{q^m} \right\}.$$

Note that $\text{Tr}_q^{q^m} (a\alpha^{\ell\rho_1}) = \text{Tr}_q^{q^m} (a q^{\frac{m+1}{2}} \alpha^{q^{\frac{m+1}{2}} \ell \rho_1})$ and $q^{\frac{m+1}{2}} \rho_1 \equiv q^{\frac{m-1}{2}} + 1 \pmod{q^m - 1}$, we have

$$\text{Tr}_q^{q^m} (a\alpha^{\ell\rho_1}) = \text{Tr}_q^{q^m} (a q^{\frac{m+1}{2}} \alpha^{(q^{\frac{m-1}{2}} + 1)\ell}).$$

Similarly, we have $\text{Tr}_q^{q^m} (b\alpha^{\ell\rho_2}) = \text{Tr}_q^{q^m} (b q^{\frac{m-1}{2}} \alpha^{(q^{\frac{m-3}{2}} + 1)\ell})$. Hence, $\widehat{\mathcal{C}}_{(q,m,2,\delta_2)}$ has the same weight distribution with the following code $\mathcal{V}_1 = \{v_1(a, b) : a, b \in \mathbb{F}_{q^m}\}$, where

$$v_1(a, b) = \left(\text{Tr}_q^{q^m} (a\alpha^{(q^{\frac{m-1}{2}} + 1)\ell} + b\alpha^{(q^{\frac{m-3}{2}} + 1)\ell}) \right)_{\ell=0}^{n-1}.$$

Clearly, $w(v_1(a, b)) = 0$ for $(a, b) = (0, 0)$. If $(a, b) \in \mathbb{F}_{q^m}^2 \setminus \{(0, 0)\}$, then

$$w(v_1(a, b)) = n - \sum_{\ell=0}^{n-1} \frac{1}{q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q (y \text{Tr}_q^{q^m} (a\alpha^{(q^{\frac{m-1}{2}} + 1)\ell} + b\alpha^{(q^{\frac{m-3}{2}} + 1)\ell})}.$$

Note that both $q^{\frac{m-1}{2}} + 1$ and $q^{\frac{m-3}{2}} + 1$ are even integers, then we have

$$\begin{aligned} & \sum_{\ell=0}^{2n-1} \zeta_p^{\text{Tr}_p^q (y \text{Tr}_q^{q^m} (a\alpha^{(q^{\frac{m-1}{2}} + 1)\ell} + b\alpha^{(q^{\frac{m-3}{2}} + 1)\ell})} \\ &= 2 \sum_{\ell=0}^{n-1} \zeta_p^{\text{Tr}_p^q (y \text{Tr}_q^{q^m} (a\alpha^{(q^{\frac{m-1}{2}} + 1)\ell} + b\alpha^{(q^{\frac{m-3}{2}} + 1)\ell})}. \end{aligned}$$

It follows that

$$\begin{aligned} w(v_1(a, b)) &= n - \frac{1}{2q} \sum_{y \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\text{Tr}_p^q (y Q_{a,b}(x))} \\ &= n - \frac{q^m - 1}{2q} - \frac{1}{2q} \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\text{Tr}_p^q (y Q_{a,b}(x))} \\ &= \frac{(q-1)n}{q} - \frac{1}{2q} \sum_{y \in \mathbb{F}_q^*} \left(\sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\text{Tr}_p^q (y Q_{a,b}(x))} - 1 \right) \\ &= \frac{(q-1)q^{m-1}}{2} - \frac{1}{2q} \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\text{Tr}_p^q (y Q_{a,b}(x))}, \end{aligned}$$

where $Q_{a,b}(x) = \text{Tr}_q^{q^m} (ax^{q^{\frac{m-1}{2}} + 1} + bx^{q^{\frac{m-3}{2}} + 1})$.

Clearly, $Q_{a,b}(x)$ is a quadratic form in m variables over \mathbb{F}_q , and

$$Q_{a,b}(x+y) - Q_{a,b}(x) - Q_{a,b}(y) = \text{Tr}_q^{q^m} (g_{a,b}(x) \cdot y),$$

where

$$g_{a,b}(x) = b^q \frac{m+3}{2} x^{q^{\frac{m+3}{2}}} + a^q \frac{m+1}{2} x^{q^{\frac{m+1}{2}}} + ax^{q^{\frac{m-1}{2}}} + bx^{q^{\frac{m-3}{2}}}.$$

Assume the rank of $Q_{a,b}(x)$ is $r_{a,b}$, then $r_{a,b} = r$ if and only if $g_{a,b}(x) = 0$ has q^{m-r} solutions in \mathbb{F}_{q^m} . The number of solutions of the above equation equals the number of solutions of the following equation

$$b^q \frac{m+3}{2} x^{q^3} + a^q \frac{m+1}{2} x^{q^2} + ax^q + bx = 0,$$

which has at most q^3 solutions. Thus, we have the following result.

Lemma 12. For $(a, b) \in \mathbb{F}_{q^m}^2 \setminus \{(0, 0)\}$, let $r_{a,b}$ be the rank of $Q_{a,b}(x)$.

- (i) If $m = 3$, the possible values of $r_{a,b}$ are m , $m - 1$ and $m - 2$.
- (ii) If $m \geq 5$ is odd, the possible values of $r_{a,b}$ are m , $m - 1$, $m - 2$ and $m - 3$.

By Lemma 4, we have

$$w(v_1(a, b)) = \frac{(q-1)q^{m-1}}{2} - \frac{T(a, b)}{2q} \sum_{y \in \mathbb{F}_q^*} \eta(y^{r_{a,b}}), \quad (7)$$

where $T(a, b) = \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\text{Tr}_p^q(Q_{a,b}(x))}$. In order to determine the value distribution of $T(a, b)$, we need the following results on moments of $T(a, b)$.

Lemma 13. Let m be odd and $T(a, b)$ be defined as above, and let $S(a, b) = \sum_{y \in \mathbb{F}_q^*} T(ay, by)$.

- (i) $\sum_{a, b \in \mathbb{F}_{q^m}} T(a, b) = q^{2m}$.
- (ii) If $q \equiv 3 \pmod{4}$, then $\sum_{a, b \in \mathbb{F}_{q^m}} T(a, b)^2 = q^{2m}$. If $q \equiv 1 \pmod{4}$, then

$$\sum_{a, b \in \mathbb{F}_{q^m}} T(a, b)^2 = (2q^m - 1)q^{2m}.$$

- (iii) $\sum_{a, b \in \mathbb{F}_{q^m}} T(a, b)^3 = [q^m + q^{m-1} - 1]q^{2m+1}$.
- (iv) $\sum_{a, b \in \mathbb{F}_{q^m}} S(a, b)^2 = (q-1)^2 q^{3m}$.

Proof: (i) The identity is trivially true.

(ii) We observe that

$$\begin{aligned} \sum_{a, b \in \mathbb{F}_{q^m}} T(a, b)^2 &= \sum_{a, b \in \mathbb{F}_{q^m}} \sum_{x, y \in \mathbb{F}_{q^m}} \zeta_p^{\text{Tr}_p^q(Q_{a,b}(x) + Q_{a,b}(y))} \\ &= \sum_{x, y \in \mathbb{F}_{q^m}} \sum_{a \in \mathbb{F}_{q^m}} \zeta_p^{\text{Tr}_p^q(a f_m(x, y))} \sum_{b \in \mathbb{F}_{q^m}} \zeta_p^{\text{Tr}_p^q(b f_{m-2}(x, y))} \\ &= A \cdot q^{2m}, \end{aligned}$$

where $f_i(x, y) = x^{q^{\frac{i-1}{2}}+1} + y^{q^{\frac{i-1}{2}}+1}$ for every positive odd i and A denotes the number of the pair $(x, y) \in \mathbb{F}_{q^m}^2$, which is a solution of the following system of equations:

$$\begin{cases} x^{q^{\frac{m-1}{2}}+1} + y^{q^{\frac{m-1}{2}}+1} = 0, \\ x^{q^{\frac{m-3}{2}}+1} + y^{q^{\frac{m-3}{2}}+1} = 0. \end{cases}$$

Clearly, $(0, 0)$ is a solution of the above system of equations. If $y \neq 0$, the system above is equivalent to

$$\begin{cases} \left(\frac{x}{y}\right)^{q^{\frac{m-1}{2}}+1} = -1, \\ \left(\frac{x}{y}\right)^{q^{\frac{m-3}{2}}+1} = -1. \end{cases} \quad (8)$$

Let B be the number of pair $(x, y) \in \mathbb{F}_{q^m}^2$, which is a solution of the system of equations (8). Clearly, $A = B + 1$. Thus, it suffices to determine the value of B .

Now assume the system of equations (8) has a solution (x, y) . Note that $\gcd(2(q^{\frac{m-1}{2}}+1), 2(q^{\frac{m-3}{2}}+1)) = 4$, from (8), $\text{ord}(\frac{x}{y})$ divides 4. We claim $\text{ord}(\frac{x}{y}) = 4$. Otherwise, we have $1 = (\frac{x}{y})^{q^{\frac{m-1}{2}}+1} = -1$, which is impossible. Thus, if the system of equations (8) has solutions, then $q^{\frac{m-1}{2}}+1 \equiv q^{\frac{m-3}{2}}+1 \equiv 2 \pmod{4}$, which deduces $q \equiv 1 \pmod{4}$. Now assume $q \equiv 1 \pmod{4}$, then the system (8) is equivalent to $(\frac{x}{y})^2 = -1$. Thus, $B = 2(q^m - 1)$. Note that $B = 0$ if $q \equiv 3 \pmod{4}$. The result follows.

(iii) Similar to (ii), we have

$$\sum_{a, b \in \mathbb{F}_{q^m}} T(a, b)^3 = M \cdot q^{2m},$$

where M is the number of triple $(x, y, z) \in \mathbb{F}_{q^m}^3$, which is a solution of the following system of equations:

$$\begin{cases} x^{q^{\frac{m-1}{2}+1}} + y^{q^{\frac{m-1}{2}+1}} + z^{q^{\frac{m-1}{2}+1}} = 0, \\ x^{q^{\frac{m-3}{2}+1}} + y^{q^{\frac{m-3}{2}+1}} + z^{q^{\frac{m-3}{2}+1}} = 0. \end{cases}$$

From (ii), the number of triples $(x, y, 0) \in \mathbb{F}_{q^m}^3$ which are solutions of the above system of equations is equal to A . If $z \neq 0$, the above system is equivalent to

$$\begin{cases} \left(\frac{x}{z}\right)^{q^{\frac{m-1}{2}+1}} + \left(\frac{y}{z}\right)^{q^{\frac{m-1}{2}+1}} + 1 = 0, \\ \left(\frac{x}{z}\right)^{q^{\frac{m-3}{2}+1}} + \left(\frac{y}{z}\right)^{q^{\frac{m-3}{2}+1}} + 1 = 0. \end{cases} \quad (9)$$

Assume the above system of equations has a solution $(x, y, z) \in \mathbb{F}_{q^m}^3$. Raising to the q -th power both sides of (10), we have

$$\left(\frac{x}{z}\right)^{q^{\frac{m-1}{2}+q}} + \left(\frac{y}{z}\right)^{q^{\frac{m-1}{2}+q}} + 1 = 0. \quad (11)$$

Taking the difference between (11) and (9), we obtain

$$\left(\frac{x}{z}\right)^{q^{\frac{m-1}{2}+1}} \left[\left(\frac{x}{z}\right)^{q-1} - 1\right] + \left(\frac{y}{z}\right)^{q^{\frac{m-1}{2}+1}} \left[\left(\frac{y}{z}\right)^{q-1} - 1\right] = 0. \quad (12)$$

From (12), if one of $\frac{x}{z}, \frac{y}{z}$ is in \mathbb{F}_q , then the other must also be in \mathbb{F}_q . We claim both $\frac{x}{z}$ and $\frac{y}{z}$ are in \mathbb{F}_q . Otherwise, we will give a contradiction. On the one hand, it follows from (12) that

$$\left(\frac{x}{y}\right)^{q^{\frac{m-1}{2}+1}} = \frac{z^{q-1} - y^{q-1}}{x^{q-1} - z^{q-1}}.$$

On the other hand, notice that both $\frac{x}{z}$ and $\frac{y}{z}$ are in \mathbb{F}_{q^m} . Raising to the $q^{\frac{m+3}{2}}$ -th power both sides of (9) and (10), we have

$$\begin{cases} \left(\frac{x}{z}\right)^{q^{\frac{m+3}{2}+1}} + \left(\frac{y}{z}\right)^{q^{\frac{m+3}{2}+1}} + 1 = 0, \\ \left(\frac{x}{z}\right)^{q^{\frac{m+3}{2}+q}} + \left(\frac{y}{z}\right)^{q^{\frac{m+3}{2}+q}} + 1 = 0, \end{cases}$$

which deduces

$$\left(\frac{x}{z}\right)^{q^{\frac{m+3}{2}+1}} \left[\left(\frac{x}{z}\right)^{q-1} - 1\right] + \left(\frac{y}{z}\right)^{q^{\frac{m+3}{2}+1}} \left[\left(\frac{y}{z}\right)^{q-1} - 1\right] = 0.$$

This gives that

$$\left(\frac{x}{y}\right)^{q^{\frac{m+3}{2}+1}} = \frac{z^{q-1} - y^{q-1}}{x^{q-1} - z^{q-1}}.$$

Therefore, $\left(\frac{x}{y}\right)^{q^{\frac{m-1}{2}+1}} = \left(\frac{x}{y}\right)^{q^{\frac{m+3}{2}+1}}$. It follows that

$$\left(\frac{x}{y}\right)^{q^{\frac{m+3}{2}-q^{\frac{m-1}{2}}}} = 1,$$

since $\frac{x}{y} \notin \mathbb{F}_q$. Notice that $\frac{x}{y} \in \mathbb{F}_{q^m}$ and $\gcd(q^{\frac{m+3}{2}} - q^{\frac{m-1}{2}}, q^m - 1) = q - 1$, we obtain $\left(\frac{x}{y}\right)^{q-1} = 1$. Now we assume $x = \sigma y$, where $\sigma \in \mathbb{F}_q^*$. Taking it into the equations (9) and (10), we have

$$\begin{cases} (\sigma^2 + 1) \left(\frac{y}{z}\right)^{q^{\frac{m-1}{2}+1}} + 1 = 0, \\ (\sigma^2 + 1) \left(\frac{y}{z}\right)^{q^{\frac{m-3}{2}+1}} + 1 = 0. \end{cases}$$

Obviously, both $\sigma^2 + 1$ and $\frac{y}{z}$ are nonzero elements. Hence, $\left(\frac{y}{z}\right)^{q^{\frac{m-1}{2}+1}} = \left(\frac{y}{z}\right)^{q^{\frac{m-3}{2}+1}}$. Note that $\frac{y}{z} \in \mathbb{F}_{q^m}$, it follows that $\left(\frac{y}{z}\right)^{q-1} = 1$, which contradicts the fact that $\frac{y}{z} \notin \mathbb{F}_q$. Therefore, the equations (9) and (10) have a solution $(x, y, z) \in \mathbb{F}_{q^m}^3$, then both $\frac{x}{z}$ and $\frac{y}{z}$ are in \mathbb{F}_q . Let $D = |\{(x, y) \in \mathbb{F}_q^2 : x^2 + y^2 + 1 = 0\}|$, then the number of triples $(x, y, z) \in \mathbb{F}_{q^m}^3$ which are solutions of (9) and (10) is equal to $(q^m - 1)D$.

Noticing the quadratic equation over \mathbb{F}_q has been studied by Wan, as an application of his results (see [44, Ch. 1, Th. 1.27]), we have $D = q - 1$ if $q \equiv 1 \pmod{4}$, and $D = q + 1$ if $q \equiv 3 \pmod{4}$. Note that $M = A + (q^m - 1)D$, the result follows.

The proof of (iv) is very similar to that of (ii), and thus is omitted here. \blacksquare

Let $m \geq 3$ be odd. According to Lemma 4, if $q \equiv 1 \pmod{4}$, for $\epsilon = \pm 1$ and $0 \leq i \leq 3$, we define that

$$N_{\epsilon,i} = \left\{ (a, b) \in \mathbb{F}_{q^m}^2 \setminus \{(0, 0)\} : T(a, b) = \epsilon q^{\frac{m+i}{2}} \right\}.$$

If $q \equiv 3 \pmod{4}$, for $\epsilon = \pm 1$ and $i \in \{0, 2\}$, we define that

$$N_{\epsilon,i} = \left\{ (a, b) \in \mathbb{F}_{q^m}^2 \setminus \{(0, 0)\} : T(a, b) = \epsilon q^{\frac{m+i}{2}} \sqrt{-1} \right\}.$$

For $i \in \{1, 3\}$, define

$$N_{\epsilon,i} = \left\{ (a, b) \in \mathbb{F}_{q^m}^2 \setminus \{(0, 0)\} : T(a, b) = \epsilon q^{\frac{m+i}{2}} \right\}.$$

And $n_{\epsilon,i} = |N_{\epsilon,i}|$.

Lemma 14. *Let $m \geq 3$ be odd, then the value distribution of $T(a, b)$ is listed in Table IV.*

Proof: We choose an element $\omega \in \mathbb{F}_q^*$ such that $\eta(\omega) = -1$, where η is the quadratic character of \mathbb{F}_q . When $i \in \{0, 2\}$, for any $(a, b) \in N_{1,i}$, from Lemma 4, we have $T(\omega a, \omega b) = -T(a, b)$, since $m - i$ is odd. Then the map $(a, b) \mapsto (\omega a, \omega b)$ gives a 1-to-1 correspondence from $N_{1,i}$ to $N_{-1,i}$. Thus, $n_{1,0} = n_{-1,0}$ and $n_{1,2} = n_{-1,2}$. It follows from Lemma 13 that

$$\begin{aligned} & \sum_{a,b \in \mathbb{F}_{q^m}} T(a, b) \\ &= q^m + (n_{1,1} - n_{-1,1})q^{\frac{m+1}{2}} + (n_{1,3} - n_{-1,3})q^{\frac{m+3}{2}} \\ &= q^{2m}, \\ & \sum_{a,b \in \mathbb{F}_{q^m}} T(a, b)^3 \\ &= q^{3m} + (n_{1,1} - n_{-1,1})q^{\frac{3m+3}{2}} + (n_{1,3} - n_{-1,3})q^{\frac{3m+9}{2}} \\ &= [q^m + q^{m-1} - 1]q^{2m+1}. \end{aligned}$$

It deduces that $n_{1,1} - n_{-1,1} = (q^m - 1)q^{\frac{m-1}{2}}$ and $n_{1,3} = n_{-1,3}$. If $n_{1,3} > 0$, from (7), we have

$$w(v_1(a, b)) = \frac{(q-1)q^{m-1}}{2} - \frac{(q-1)q^{\frac{m+1}{2}}}{2} < \delta_2 + 1.$$

However, from Lemma 1, the minimum distance of $\widehat{\mathcal{C}}_{(q,m,2,\delta_2)}$ is at least $\delta_2 + 1$. Hence, $n_{1,3} = 0$. That is, $n_{1,3} = n_{-1,3} = 0$. At this point, from (iv) of Lemma 13,

$$\begin{aligned} \sum_{a,b \in \mathbb{F}_{q^m}} S(a, b)^2 &= (q^2 - 1)[q^{2m} + (n_{1,1} + n_{-1,1})q^{m+1}] \\ &= (q^2 - 1)q^{3m}. \end{aligned}$$

Notice that if $q \equiv 1 \pmod{4}$,

$$\begin{aligned} & \sum_{a,b \in \mathbb{F}_{q^m}} T(a, b)^2 \\ &= q^{2m} + 2n_{1,0}q^m + (n_{1,1} + n_{-1,1})q^{m+1} + 2n_{1,2}q^{m+2} \\ &= (2q^m - 1)q^{2m}. \end{aligned}$$

If $q \equiv 3 \pmod{4}$, then

$$\begin{aligned} & \sum_{a,b \in \mathbb{F}_{q^m}} T(a, b)^2 \\ &= q^{2m} - 2n_{1,0}q^m + (n_{1,1} + n_{-1,1})q^{m+1} - 2n_{1,2}q^{m+2} \\ &= q^{2m}. \end{aligned}$$

TABLE IV: THE VALUE DISTRIBUTION OF $T(a, b)$

Rank $r_{a,b}$	Value $T(a, b)$	Multiplicity
m	$q^{\frac{m}{2}} \sqrt{(-1)^{\frac{q-1}{2}}}$	$\frac{(q^m-1)(q^{m+2}-q^{m+1}-q^m+q^2)}{2(q^2-1)}$
m	$-q^{\frac{m}{2}} \sqrt{(-1)^{\frac{q-1}{2}}}$	$\frac{(q^m-1)(q^{m+2}-q^{m+1}-q^m+q^2)}{2(q^2-1)}$
$m-1$	$q^{\frac{m+1}{2}}$	$\frac{(q^m-1)(q^{m-1}+q^{\frac{m-1}{2}})}{2}$
$m-1$	$-q^{\frac{m+1}{2}}$	$\frac{(q^m-1)(q^{m-1}-q^{\frac{m-1}{2}})}{2}$
$m-2$	$q^{\frac{m+2}{2}} \sqrt{(-1)^{\frac{q-1}{2}}}$	$\frac{(q^m-1)(q^{m-1}-1)}{2(q^2-1)}$
$m-2$	$-q^{\frac{m+2}{2}} \sqrt{(-1)^{\frac{q-1}{2}}}$	$\frac{(q^m-1)(q^{m-1}-1)}{2(q^2-1)}$
0	q^m	1

Moreover, $1 + 2n_{1,0} + n_{1,1} + n_{-1,1} + 2n_{1,2} = q^{2m}$. Simplifying the above equations leads to

$$\begin{cases} n_{1,1} - n_{-1,1} = (q^m - 1)q^{\frac{m-1}{2}}, \\ n_{1,1} + n_{-1,1} = (q^m - 1)q^{m-1}, \\ 2n_{1,0} + 2q^2n_{1,2} = (q^m - 1)q^m, \\ 2n_{1,0} + 2n_{1,2} = (q^m - 1)(q^m - q^{m-1} + 1). \end{cases}$$

The value distribution of $T(a, b)$ then follows. ■

Let $m \geq 2$ be even and α be a primitive element of \mathbb{F}_{q^m} , then α^2 is a primitive n -th root of unity in \mathbb{F}_{q^m} . From Lemmas 9 and 10, the code $\widehat{\mathcal{C}}_{(q,m,2,\delta_2)}$ has two nonzeros, and $\alpha^{2\delta_1}$ and $\alpha^{2\delta_2}$ are two non-conjugate roots of its parity-check polynomial. Let $h = \frac{m}{2}$, $\rho_1 = q^{m-1} + q^{h-1}$ and $\rho_2 = q^{m-1} + q^h$. By Lemma 3,

$$\widehat{\mathcal{C}}_{(q,m,2,\delta_2)} = \{c(a, b) : a \in \mathbb{F}_{q^h}, b \in \mathbb{F}_{q^m}\},$$

where

$$c(a, b) = \left(\text{Tr}_q^{q^h}(a\alpha^{\ell\rho_1}) + \text{Tr}_q^{q^m}(b\alpha^{\ell\rho_2}) \right)_{\ell=0}^{n-1}.$$

Since $\text{Tr}_q^{q^h}(a\alpha^{\ell\rho_1}) = \text{Tr}_q^{q^h}(a^q\alpha^{(q^h+1)\ell})$ and

$$\text{Tr}_q^{q^m}(b\alpha^{\ell\rho_2}) = \text{Tr}_q^{q^m}(b^{q^h}\alpha^{(q^{h-1}+1)\ell}),$$

it follows that $\widehat{\mathcal{C}}_{(q,m,2,\delta_2)}$ has the same weight distribution with the code

$$\mathcal{V}_2 = \{v_2(a, b) : a \in \mathbb{F}_{q^h}, b \in \mathbb{F}_{q^m}\},$$

where

$$v_2(a, b) = \left(\text{Tr}_q^{q^h}(a\alpha^{(q^h+1)\ell}) + \text{Tr}_q^{q^m}(b\alpha^{(q^{h-1}+1)\ell}) \right)_{\ell=0}^{n-1}.$$

Clearly, $w(v_2(a, b)) = 0$ for $(a, b) = (0, 0)$. If $(a, b) \in \mathbb{F}_{q^h} \times \mathbb{F}_{q^m} \setminus \{(0, 0)\}$, similar to the odd case $m \geq 3$, we have

$$\begin{aligned} w(v_2(a, b)) &= \frac{(q-1)q^{m-1}}{2} - \frac{1}{2q} \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\text{Tr}_p^q(y\overline{Q}_{a,b}(x))} \\ &= \frac{(q-1)q^{m-1}}{2} - \frac{\overline{T}(a, b)}{2q} \sum_{y \in \mathbb{F}_q^*} \eta(y^{r_{a,b}}), \end{aligned}$$

where $\overline{Q}_{a,b}(x) = \text{Tr}_q^{q^h}(ax^{q^h+1}) + \text{Tr}_q^{q^m}(bx^{q^{h-1}+1})$, $r_{a,b}$ is the rank of $\overline{Q}_{a,b}(x)$ and

$$\overline{T}(a, b) = \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\text{Tr}_p^q(\overline{Q}_{a,b}(x))}.$$

TABLE V: THE VALUE DISTRIBUTION OF $\overline{T}(a, b)$

Rank $r_{a,b}$	Value $\overline{T}(a, b)$	Multiplicity
m	$q^{\frac{m}{2}}$	$\frac{(q^m-1)(q^{\frac{m+2}{2}}+q)}{2(q+1)}$
m	$-q^{\frac{m}{2}}$	$\frac{(q^{\frac{m}{2}}-1)(q^{m+1}-2q^m+q)}{2(q-1)}$
$m-1$	$q^{\frac{m+1}{2}}\sqrt{(-1)^{\frac{q-1}{2}}}$	$\frac{(q^m-1)q^{\frac{m-2}{2}}}{2}$
$m-1$	$-q^{\frac{m+1}{2}}\sqrt{(-1)^{\frac{q-1}{2}}}$	$\frac{(q^m-1)q^{\frac{m-2}{2}}}{2}$
$m-2$	$-q^{\frac{m+2}{2}}$	$\frac{(q^m-1)(q^{\frac{m-2}{2}}-1)}{q^2-1}$
0	q^m	1

TABLE VI: THE WEIGHT DISTRIBUTION OF $\widehat{C}_{(q,m,2,\delta_2)}$ WHEN m IS ODD

Weight	Frequency
0	1
$\frac{(q-1)(q^{m-1}-q^{\frac{m-1}{2}})}{2}$	$\frac{(q^m-1)(q^{m-1}+q^{\frac{m-1}{2}})}{2}$
$\frac{(q-1)q^{m-1}}{2}$	$(q^m-1)(q^m-q^{m-1}+1)$
$\frac{(q-1)(q^{m-1}+q^{\frac{m-1}{2}})}{2}$	$\frac{(q^m-1)(q^{m-1}-q^{\frac{m-1}{2}})}{2}$

Clearly, in order to determine the weight of $v_2(a, b)$, it suffices to determine the value distribution of $\overline{T}(a, b)$. Fortunately, the value distribution of $\overline{T}(a, b)$ was determined in [31], and we list it in Table V.

Theorem 6. *The BCH code $\widehat{C}_{(q,m,2,\delta_2)}$ has parameters $[\frac{q^m-1}{2}, k, d]$, where*

- (i) *if m is odd, then $k = 2m$, $d = \frac{(q-1)(q^{m-1}-q^{\frac{m-1}{2}})}{2}$ and $\widehat{C}_{(q,m,2,\delta_2)}$ is a three-weight code. In addition, the weight distribution of $\widehat{C}_{(q,m,2,\delta_2)}$ is listed in Table VI.*
- (ii) *if m is even, then $k = \frac{3m}{2}$, $d = \frac{(q-1)(q^{m-1}-q^{\frac{m-2}{2}})}{2}$ and $\widehat{C}_{(q,m,2,\delta_2)}$ is a four-weight code for $m \geq 4$. In addition, the weight distribution of $\widehat{C}_{(q,m,2,\delta_2)}$ is listed in Table VII.*

Proof: We only prove the case that $m \geq 3$ is odd, and the even case is similar. If $r_{a,b}$ is odd, from (7), we have

$$w(v_1(a, b)) = \frac{(q-1)(q^m-1)}{2}.$$

Hence, the number of such codewords is equal to $n_{1,0} + n_{-1,0} + n_{1,2} + n_{-1,2}$. If $r_{a,b}$ is even, from (7), then $w(v_1(a, b)) = \frac{(q-1)q^{m-1}}{2} - \frac{(q-1)T(a,b)}{2q}$. By Lemma 14, the weight distribution of the code then follows. ■

It is observed that the weight of the BCH code in Theorem 6 has a common divisor $\frac{q-1}{2}$. Hence, we consider a punctured code of this class of BCH codes. Let $N = \frac{q^m-1}{q-1}$. If $m \geq 3$ is odd, we define $\mathcal{V}_3 = \{v_3(a, b) : a, b \in \mathbb{F}_{q^m}\}$,

TABLE VII: THE WEIGHT DISTRIBUTION OF $\widehat{C}_{(q,m,2,\delta_2)}$ WHEN m IS EVEN

Weight	Frequency
0	1
$\frac{(q-1)(q^{m-1}-q^{\frac{m-2}{2}})}{2}$	$\frac{(q^m-1)(q^{\frac{m}{2}+1}+q)}{2(q+1)}$
$\frac{(q-1)q^{m-1}}{2}$	$q^{\frac{m-2}{2}}(q^m-1)$
$\frac{(q-1)(q^{m-1}+q^{\frac{m-2}{2}})}{2}$	$\frac{(q^{\frac{m}{2}+1}-q)(q^m-2q^{m-1}+1)}{2(q-1)}$
$\frac{(q-1)(q^{m-1}+q^{\frac{m}{2}})}{2}$	$\frac{(q^m-1)(q^{\frac{m-2}{2}}-1)}{q^2-1}$

TABLE VIII: PUNCTURING CODE FROM $\widehat{\mathcal{C}}_{(q,m,2,\delta_2)}$ WHEN m IS ODD

Weight	Frequency
0	1
$q^{m-1} - q^{\frac{m-1}{2}}$	$\frac{(q^m-1)(q^{\frac{m-1}{2}} + q^{\frac{m-1}{2}})}{2}$
q^{m-1}	$(q^m - 1)(q^{\frac{m-1}{2}} - q^{\frac{m-1}{2}} + 1)$
$q^{m-1} + q^{\frac{m-1}{2}}$	$\frac{(q^m-1)(q^{\frac{m-1}{2}} - q^{\frac{m-1}{2}})}{2}$

TABLE IX: PUNCTURING CODE FROM $\widehat{\mathcal{C}}_{(q,m,2,\delta_2)}$ WHEN m IS EVEN

Weight	Frequency
0	1
$q^{m-1} - q^{\frac{m-2}{2}}$	$\frac{(q^m-1)(q^{\frac{m}{2}+1} + q)}{2(q+1)}$
q^{m-1}	$q^{\frac{m-2}{2}}(q^m - 1)$
$q^{m-1} + q^{\frac{m-2}{2}}$	$\frac{(q^{\frac{m}{2}+1} - q)(q^m - 2q^{\frac{m-1}{2}} + 1)}{2(q-1)}$
$q^{m-1} + q^{\frac{m}{2}}$	$\frac{(q^m-1)(q^{\frac{m-2}{2}} - 1)}{q^2 - 1}$

where

$$v_3(a, b) = \left(\text{Tr}_q^{q^m} (a\alpha^{\ell(q^{\frac{m-1}{2}} + 1)} + b\alpha^{\ell(q^{\frac{m-3}{2}} + 1)}) \right)_{\ell=0}^{N-1}.$$

If $m \geq 2$ is even, define

$$\mathcal{V}_3 = \left\{ v_3(a, b) : a \in \mathbb{F}_{q^{\frac{m}{2}}}, b \in \mathbb{F}_{q^m} \right\},$$

where

$$v_3(a, b) = \left(\text{Tr}_q^{q^{\frac{m}{2}}} (a\alpha^{\ell(q^{\frac{m}{2}} + 1)}) + \text{Tr}_q^{q^m} (b\alpha^{\ell(q^{\frac{m-2}{2}} + 1)}) \right)_{\ell=0}^{N-1}.$$

Let $\gamma = \alpha^N$, then γ is a primitive element of \mathbb{F}_q . Sequentially, $\gamma^{q^i+1} = \gamma^2$ for every positive integer i . Let $t = \frac{q-1}{2}$, we have

$$v_2(a, b) = v_3(a, b) \parallel \gamma^2 v_3(a, b) \parallel \cdots \parallel \gamma^{2(t-1)} v_3(a, b),$$

where $v_2(a, b)$ is defined as above and \parallel denotes the concatenation of vectors. Hence we obtain a punctured linear code \mathcal{V}_3 of the code \mathcal{V}_2 . By Theorem 6, we directly obtain the following result.

Theorem 7. Let \mathcal{V}_3 be defined as above. Then \mathcal{V}_3 has parameters $[\frac{q^m-1}{q-1}, k, d]$, where

- (i) if m is odd, then $k = 2m$, $d = q^{m-1} - q^{\frac{m-1}{2}}$ and \mathcal{V}_3 is a three-weight code. In addition, the weight distribution of \mathcal{V}_3 is listed in Table VIII.
- (ii) if m is even, then $k = \frac{3m}{2}$, $d = q^{m-1} - q^{\frac{m-2}{2}}$ and \mathcal{V}_3 is a four-weight code for $m \geq 4$. In addition, the weight distribution of \mathcal{V}_3 is listed in Table IX.

Example 3. When $(q, m) = (3, 3)$, the BCH code $\widehat{\mathcal{C}}_{(q,m,2,\delta_2)}$ is a $[13, 6, 6]$ code over \mathbb{F}_3 with weight enumerator $1 + 156z^6 + 494z^9 + 78z^{12}$. This code has the same parameters with the best known in the Database.

Example 4. When q is odd and $m = 2$, the linear code \mathcal{V}_3 is a $[q+1, 3, q-1]$ MDS code over \mathbb{F}_q with weight enumerator $1 + \frac{q(q^2-1)}{2}z^{w_1} + (q^2-1)z^{w_2} + \frac{q(q^2-2q+1)}{2}z^{w_3}$, where $w_1 = q-1$, $w_2 = q$, $w_3 = q+1$.

Example 5. When $(q, m) = (5, 3)$, the linear code \mathcal{V}_3 is a $[31, 6, 20]$ code over \mathbb{F}_5 with weight enumerator $1 + 1860z^{20} + 12524z^{25} + 1240z^{30}$. This code has the same parameters with the best known in the Database.

Theorem 8. The BCH code $\mathcal{C}_{(q,m,2,\delta_2)}$ has parameters $[\frac{q^m-1}{2}, k, \delta_2]$, where

TABLE X: THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{(q,m,2,\delta_2)}$ WHEN m IS ODD

Weight	Multiplicity
0	1
$\frac{q^m - q^{m-1} - q^{\frac{m+1}{2}} - 1}{2}$	$\frac{(q^m - 1)(q^{m-1} - 1)}{2(q+1)}$
$\frac{q^m - q^{m-1} - q^{\frac{m+1}{2}} + q^{\frac{m-1}{2}}}{2}$	$\frac{(q^m - 1)(q^{m-1} + q^{\frac{m-1}{2}})}{2}$
$\frac{q^m - q^{m-1} - q^{\frac{m-1}{2}} - 1}{2}$	$\frac{(q^m - 1)(q^{m+2} - q^m - q^{m-1} - q^{\frac{m+3}{2}} + q^{\frac{m-1}{2}} + q^2)}{2(q+1)}$
$\frac{q^m - q^{m-1}}{2}$	$(q^m - 1)(q^m - q^{m-1} + 1)$
$\frac{q^m - q^{m-1} + q^{\frac{m-1}{2}} - 1}{2}$	$\frac{(q^m - 1)(q^{m+2} - q^m - q^{m-1} + q^{\frac{m+3}{2}} - q^{\frac{m-1}{2}} + q^2)}{2(q+1)}$
$\frac{q^m - q^{m-1} + q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}}}{2}$	$\frac{(q^m - 1)(q^{m-1} - q^{\frac{m-1}{2}})}{2}$
$\frac{q^m - q^{m-1} + q^{\frac{m+1}{2}} - 1}{2}$	$\frac{(q^m - 1)(q^{m-1} - 1)}{2(q+1)}$
$\frac{q^m - 1}{2}$	$q - 1$

TABLE XI: THE WIGHT DISTRIBUTION OF $\mathcal{C}_{(q,m,2,\delta_2)}$ WHEN m IS EVEN

Weight	Multiplicity
0	1
$\frac{q^m - q^{m-1} - q^{\frac{m}{2}} - 1}{2}$	$\frac{(q^m - 1)(q^{\frac{m+2}{2}} + q^{\frac{m-2}{2}} - 2)}{2(q+1)}$
$\frac{q^m - q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}}{2}$	$\frac{(q^m - 1)(q^{\frac{m+2}{2}} + q)}{2(q+1)}$
$\frac{q^m - q^{m-1} - q^{\frac{m-2}{2}} - 1}{2}$	$\frac{(q^{\frac{m}{2}} - 1)(q^{m+1} - 2q^m + q)}{2}$
$\frac{q^m - q^{m-1}}{2}$	$(q^m - 1)q^{\frac{m-2}{2}}$
$\frac{q^m - q^{m-1} + q^{\frac{m-2}{2}} - 1}{2}$	$\frac{(q^m - 1)(q^{\frac{m+2}{2}} + q)(q-1)}{2(q+1)}$
$\frac{q^m - q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}}}{2}$	$\frac{(q^{\frac{m+2}{2}} - q)(q^m - 2q^{m-1} + 1)}{2(q-1)}$
$\frac{q^m - q^{m-1} + q^{\frac{m}{2}} - 1}{2}$	$\frac{(q^m - 1)(q^{\frac{m}{2}} - q^{\frac{m-2}{2}})}{2}$
$\frac{q^m - q^{m-1} + q^{\frac{m+2}{2}} - q^{\frac{m}{2}}}{2}$	$\frac{(q^m - 1)(q^{\frac{m-2}{2}} - 1)}{q^2 - 1}$
$\frac{q^m - 1}{2}$	$q - 1$

- (i) if m is odd, then $k = 2m + 1$ and the weight distribution of $\mathcal{C}_{(q,m,2,\delta_2)}$ is listed in Table X.
(ii) if m is even, then $k = \frac{3m}{2} + 1$ and the weight distribution of $\mathcal{C}_{(q,m,2,\delta_2)}$ is listed in Table XI.

Proof: Let α be a primitive element of \mathbb{F}_{q^m} , then α^2 is a primitive n -th root of unity in \mathbb{F}_{q^m} . From Lemmas 9 and 10, the code $\mathcal{C}_{(q,m,2,\delta_2)}$ has three nonzeros, and $1, \alpha^{2\delta_1}$ and $\alpha^{2\delta_2}$ are three non-conjugate roots of its parity-check polynomial. The dimension of $\mathcal{C}_{(q,m,2,\delta_2)}$ follows from Lemmas 9 and 10.

Case 1. m is odd. Similar to the above discussion, $\mathcal{C}_{(q,m,2,\delta_2)}$ has the same weight distribution with the code

$$\{v_4(a, b, c) : a, b \in \mathbb{F}_{q^m}, c \in \mathbb{F}_q\},$$

where

$$v_4(a, b, c) = \left(\text{Tr}_q^{q^m} (a\alpha^{(q^{\frac{m-1}{2}} + 1)\ell} + b\alpha^{(q^{\frac{m-3}{2}} + 1)\ell}) + c \right)_{\ell=0}^{n-1}.$$

When $c = 0$, the weight distribution of $v_4(a, b, c)$ is determined in Theorem 6. When $c \neq 0$, we have

$$\begin{aligned}
& w(v_4(a, b, c)) \\
&= n - \sum_{\ell=0}^{n-1} \frac{1}{q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(y \text{Tr}_q^m(a\alpha^{(q^{\frac{m-1}{2}}+1)\ell} + b\alpha^{(q^{\frac{m-3}{2}}+1)\ell}) + yc)} \\
&= n - \frac{1}{q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(yc)} \sum_{\ell=0}^{n-1} \zeta_p^{\text{Tr}_p^q(y \text{Tr}_q^m(a\alpha^{(q^{\frac{m-1}{2}}+1)\ell} + b\alpha^{(q^{\frac{m-3}{2}}+1)\ell}))} \\
&= n - \frac{1}{2q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(yc)} \sum_{\ell=0}^{2n-1} \zeta_p^{\text{Tr}_p^q(y \text{Tr}_q^m(a\alpha^{(q^{\frac{m-1}{2}}+1)\ell} + b\alpha^{(q^{\frac{m-3}{2}}+1)\ell}))} \\
&= n - \frac{1}{2q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(yc)} \sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\text{Tr}_p^q(yQ_{a,b}(x))} \\
&= n - \frac{1}{2q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}_p^q(yc)} \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\text{Tr}_p^q(yQ_{a,b}(x))} \\
&= \frac{q^m - q^{m-1} - 1}{2} - \frac{1}{2q} \sum_{y \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^q(yc)} \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\text{Tr}_p^q(yQ_{a,b}(x))},
\end{aligned}$$

where $Q_{a,b}(x) = \text{Tr}_q^m(ax^{q^{\frac{m-1}{2}}+1} + bx^{q^{\frac{m-3}{2}}+1})$. Let η be the quadratic character of \mathbb{F}_q , $r_{a,b}$ be the rank of $Q_{a,b}(x)$, and $T(a, b) = \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\text{Tr}_p^q(Q_{a,b}(x))}$. From Lemma 4,

$$\sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\text{Tr}_p^q(yQ_{a,b}(x))} = \eta(y^{r_{a,b}})T(a, b).$$

It follows that the weight of codeword $v_4(a, b, c)$ is

$$\frac{q^m - q^{m-1} - 1}{2} - \frac{T(a, b)}{2q} \sum_{y \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^q(yc)} \eta(y^{r_{a,b}}).$$

There are two cases.

If $r_{a,b}$ is even, then

$$w(v_4(a, b, c)) = \frac{q^m - q^{m-1} - 1}{2} + \frac{T(a, b)}{2q}.$$

If $r_{a,b}$ is odd, then

$$\begin{aligned}
w(v_4(a, b, c)) &= \frac{q^m - q^{m-1} - 1}{2} - \frac{T(a, b)}{2q} \sum_{y \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^q(yc)} \eta(y) \\
&= \frac{q^m - q^{m-1} - 1}{2} - \frac{\eta(c)T(a, b)G_q}{2q}.
\end{aligned}$$

Combining Lemmas 4 and 14, the desired conclusion on the weight distribution then follows.

Case 2. m is even. Similar to Case 1, $\mathcal{C}_{(q,m,2,\delta_2)}$ has the same weight distribution with the code

$$\left\{ v_5(a, b, c) : a \in \mathbb{F}_{q^{\frac{m}{2}}}, b \in \mathbb{F}_{q^m}, c \in \mathbb{F}_q \right\},$$

where

$$v_5(a, b, c) = \left(\text{Tr}_q^{\frac{m}{2}}(a\alpha^{(q^{\frac{m}{2}}+1)\ell}) + \text{Tr}_q^m(b\alpha^{(q^{\frac{m-2}{2}}+1)\ell}) + c \right)_{\ell=0}^{n-1}.$$

When $c = 0$, the weight distribution of $v_5(a, b, c)$ is determined in Theorem 6. When $c \neq 0$, similar to Case 1, the weight of codeword $v_5(a, b, c)$ is

$$\frac{q^m - q^{m-1} - 1}{2} - \frac{\overline{T}(a, b)}{2q} \sum_{y \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^q(yc)} \eta(y^{r_{a,b}}),$$

where $\overline{T}(a, b) = \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\text{Tr}_p^q(\overline{Q}_{a,b}(x))}$ and

$$\overline{Q}_{a,b}(x) = \text{Tr}_q^{q^{\frac{m}{2}}}(ax^{q^{\frac{m}{2}}+1}) + \text{Tr}_q^{q^m}(bx^{q^{\frac{m-2}{2}}+1}).$$

Thanks to [31], the value distribution of $\overline{T}(a, b)$ is already known which is presented in Table V. There are two cases.

If $r_{a,b}$ is even, then

$$w(v_5(a, b, c)) = \frac{q^m - q^{m-1} - 1}{2} + \frac{\overline{T}(a, b)}{2q}.$$

If $r_{a,b}$ is odd, then

$$w(v_5(a, b, c)) = \frac{q^m - q^{m-1} - 1}{2} - \frac{\eta(c)\overline{T}(a, b)G_q}{2q}.$$

Thus, the desired conclusion on the weight distribution then follows. \blacksquare

Example 6. When $(q, m) = (3, 3)$, the BCH code $\mathcal{C}_{(q,m,2,\delta_2)}$ is a $[13, 7, 4]$ code over \mathbb{F}_3 with weight enumerator $1 + 26z^4 + 156z^6 + 624z^7 + 494z^9 + 780z^{10} + 78z^{12} + 28z^{13}$. The best known linear code over \mathbb{F}_3 with length 13 and dimension 7 has minimum distance 5 in the Database.

Example 7. When $(q, m) = (3, 4)$, the BCH code $\mathcal{C}_{(q,m,2,\delta_2)}$ is a $[40, 7, 22]$ code over \mathbb{F}_3 with weight enumerator $1 + 280z^{22} + 300z^{24} + 336z^{25} + 240z^{27} + 600z^{28} + 168z^{30} + 240z^{31} + 20z^{36} + 2z^{40}$. This code has the same parameters with the best known in the Database.

B. The weight distribution of BCH codes of length $(q^m - 1)/(q - 1)$

In this subsection, we study the weight distribution of BCH codes of length $n = (q^m - 1)/(q - 1)$, where $m \geq q$.

Lemma 15. Let $q > 3$ and i be an integer with $1 \leq i \leq n - 1$. Denote the q -adic expansion of i by $\sum_{\ell=0}^{m-1} i_\ell q^\ell$. If i is a q -cyclotomic coset leader modulo n , then $i_{m-1} = 0$. Suppose $m - 1 = a(q - 1) + b$, where $a \geq 1$ and $0 \leq b \leq q - 2$ are integers. Let $\epsilon = a + 1$ when $b = q - 2$ and $\epsilon = a$ when $0 \leq b \leq q - 3$. If $i_\ell = q - 1$ for all $m - 1 - \epsilon \leq \ell \leq m - 2$, then $1 \leq i_{\ell-1} \leq i_\ell$ for all $1 \leq \ell \leq m - 2$.

Proof: The first statement of this lemma comes from Lemma 8. For every positive integer μ , if $i_\mu \neq 0$, we have $i_{\mu-1} \leq i_\mu$. Otherwise, we have $[iq^{m-1-\mu}]_n < i$, a contradiction. It follows that $(i_0, i_1, \dots, i_{m-1})$ must be of the form (I_0, I_1, \dots, I_v) , where v is some non-negative integer and

$$I_e = (\overbrace{1 \dots 1}^{n_{e,1}} \overbrace{2 \dots 2}^{n_{e,2}} \dots \overbrace{q-1 \dots q-1}^{n_{e,q-1}} 0), \quad n_{e,f} \geq 0,$$

for every $0 \leq e \leq v$. We now prove $v = 0$. Let $\kappa = \sum_{f=1}^{q-1} n_{0,f}$, from $[iq^{m-1-\kappa}]_n \geq i$, we have $n_{0,q-1} \geq n_{v,q-1}$. Similarly, we have $n_{e,q-1} \geq n_{v,q-1}$ for all $0 \leq e \leq v$. Note that

$$[iq]_n = 2 + \sum_{\ell=1}^{m-n_{v,q-1}-1} (i_{\ell-1} + 1)q^\ell + \sum_{m-n_{v,q-1}+1}^{m-1} q^\ell.$$

Denote the q -adic expansion of $[iq^{n_{v,q-1}}]_n$ by $\sum_{\ell=0}^{m-1} i'_\ell q^\ell$, then $(i'_0, i'_1, \dots, i'_{m-1})$ must be of the form $(I'_0, I'_1, \dots, I'_v)$, where

$$I'_0 = (\overbrace{1 \dots 1}^{n_{v,(q-1)}-1} \overbrace{2 \dots 2}^{n_{0,1}+1} \overbrace{3 \dots 3}^{n_{0,2}} \dots \overbrace{q-1 \dots q-1}^{n_{0,q-2}} 0),$$

$$I'_e = (\overbrace{1 \dots 1}^{n_{e-1,q-1}-1} \overbrace{2 \dots 2}^{n_{e,1}+1} \overbrace{3 \dots 3}^{n_{e,2}} \dots \overbrace{q-1 \dots q-1}^{n_{e,q-2}} 0),$$

for every $1 \leq e \leq v$. It follows that $n_{e,q-2} \geq n_{v,q-1}$ for all $0 \leq e \leq v$. By the same way, we have $n_{e,f} \geq n_{v,q-1}$ for all $0 \leq e \leq v$ and $2 \leq f \leq q - 2$, and $n_{e,1} \geq n_{v,q-1} - 1$ for all $0 \leq e \leq v$. Therefore,

$$\begin{aligned} m &= \sum_{e=0}^v \left(\sum_{f=1}^{q-1} n_{e,f} + 1 \right) \\ &\geq (v+1)(q-1)n_{v,q-1} \\ &\geq (v+1)(q-1)\epsilon, \end{aligned}$$

since $n_{v,q-1} \geq \epsilon$. If $v \geq 1$, we have $a(q-1) + b + 1 \geq 2(q-1)\epsilon$, a contradiction. \blacksquare

Lemma 16. *Let $q > 3$ be a prime power and $m \geq q$. Suppose $m - 1 = a(q-1) + b$, where $a \geq 1$, $0 \leq b \leq q-2$ are integers.*

(i) *If $b = 0$, i.e., $m = a(q-1) + 1$, then the first largest q -cyclotomic coset leader modulo $\frac{q^m-1}{q-1}$ is*

$$\delta = \frac{q^m - 1 - q^{m-1} - \sum_{\ell=1}^{q-2} q^{a\ell}}{q-1}$$

and $|\mathbb{C}_\delta| = m$.

(ii) *If $b = 1$, i.e., $m = a(q-1) + 2$, let $A = \lfloor \frac{q-1}{2} \rfloor$, then the first largest q -cyclotomic coset leader modulo $\frac{q^m-1}{q-1}$ is*

$$\delta = \frac{q^m - 1 - q^{m-1} - \sum_{\ell=1}^A q^{a\ell} - \sum_{\ell=A+1}^{q-2} q^{a\ell+1}}{q-1}.$$

Moreover, $|\mathbb{C}_\delta| = \frac{m}{2}$ when q is odd, and $|\mathbb{C}_\delta| = m$ when q is even.

(iii) *If $b = q-2$, i.e., $m = (a+1)(q-1)$, then the first largest q -cyclotomic coset leader modulo $\frac{q^m-1}{q-1}$ is*

$$\delta = \frac{q^m - 1 - q^{m-1} - \sum_{\ell=1}^{q-2} q^{(a+1)\ell-1}}{q-1}$$

and $|\mathbb{C}_\delta| = a+1$.

Proof: We just give the proof for Case (ii), since the proofs in the other cases are similar. Clearly, the q -adic expansion of δ is of the form

$$\sum_{i=1}^A \sum_{\ell=(i-1)a}^{ia-1} iq^\ell + \sum_{\ell=Aa}^{(A+1)a} (A+1)q^\ell + \sum_{i=A+2}^{q-1} \sum_{\ell=(i-1)a+1}^{ia} iq^\ell,$$

and it is easy to check that δ is a q -cyclotomic coset leader modulo n . Moreover, $|\mathbb{C}_\delta| = \frac{m}{2}$ if q is odd, and $|\mathbb{C}_\delta| = m$ if q is even.

We now prove that δ is the largest integer in the set of all coset leaders. Suppose there is an integer s with $\delta < s < n$ which is a q -cyclotomic coset leader modulo n and the q -adic expansion of s is $\sum_{\ell=0}^{m-1} s_\ell q^\ell$. By Lemma 15, $(s_0, s_1, \dots, s_{m-1})$ must be of the form

$$(\overbrace{1 \dots 1}^{n_1} \overbrace{2 \dots 2}^{n_2} \dots \overbrace{q-1 \dots q-1}^{n_{q-1}} 0),$$

where $n_{q-1} \geq a$, $n_\ell \geq n_{q-1}$ for $2 \leq \ell \leq q-2$, and $n_1 \geq n_{q-1} - 1$. Firstly, $n_{q-1} = a$. Otherwise,

$$\begin{aligned} m-1 &= \sum_{\ell=1}^{q-1} n_\ell \geq (q-1)n_{q-1} - 1 \\ &\geq a(q-1) + q-2 > m-1, \end{aligned}$$

a contradiction. Secondly, $n_\ell \leq a+1$ for all $2 \leq \ell \leq q-2$. Otherwise, there is an integer v such that $n_v = a+2$, then we have

$$[sq^{(q-v)a+2}]_n = \sum_{\ell=0}^a q^\ell + \sum_{i=2}^{q-1} \sum_{\ell=(i-1)a+1}^{ia} iq^\ell < \delta,$$

a contradiction. Thirdly, $n_1 \geq a$. Otherwise, suppose $n_1 = a-1$, then there are two integers $2 \leq u < v \leq q-2$ such that $n_u = n_v = a+1$. It is easy to check that

$$[sq^{(q-u)a+1}]_n < s,$$

a contradiction. Therefore, $n_0 = a$ and there is an integer v with $A+2 \leq v \leq q-2$ such that $n_v = a+1$. From $[sq^{(q-v)a+1}]_n \geq s$, we have $2v \leq q+1$, a contradiction.

Collecting all the conclusions above, we conclude that δ is the largest coset leader. \blacksquare

Based on Lemma 16, we calculate the weight distribution of BCH code $\widehat{\mathcal{C}}_{(q,m,q-1,\delta)}$ as follows.

Theorem 9. *Let $q > 3$ be a prime power and $m \geq q$. Suppose $m-1 = a(q-1) + b$, where $a \geq 1$ and $0 \leq b \leq q-2$ are integers.*

- (i) If $b = 0$ or $b = 1$ and q is even, then the BCH code $\widehat{\mathcal{C}}_{(q,m,q-1,\delta)}$ is a $[\frac{q^m-1}{q-1}, m, q^{m-1}]$ one-weight code.
(ii) If $b = 1$ and q is odd, then the BCH code $\widehat{\mathcal{C}}_{(q,m,q-1,\delta)}$ is a $[\frac{q^m-1}{q-1}, \frac{m}{2}, (q^{\frac{m}{2}} + 1)q^{\frac{m}{2}-1}]$ one-weight code.

Proof: We just give the proof for Case (ii), since the proofs in the other cases are similar. Let α be a primitive element of \mathbb{F}_{q^m} , then α^{q-1} is a primitive n -th root of unity in \mathbb{F}_{q^m} . From Lemma 16, the BCH code $\widehat{\mathcal{C}}_{(q,m,q-1,\delta)}$ has one nonzero and $\alpha^{(q-1)\delta}$ is a root of its parity-check polynomial. Let $\tau = q^{m-1} + \sum_{\ell=1}^{\frac{q-1}{2}} q^{a\ell} + \sum_{\ell=\frac{q+1}{2}}^{q-2} q^{a\ell+1}$, then $-(q-1)\delta \equiv \tau \pmod{q^m-1}$. By Lemma 3,

$$\widehat{\mathcal{C}}_{(q,m,q-1,\delta)} = \left\{ \left(\text{Tr}_q^{\frac{m}{2}}(a\alpha^{\tau\ell}) \right)_{\ell=0}^{n-1} : a \in \mathbb{F}_{q^{\frac{m}{2}}} \right\}.$$

Let $\beta = \alpha^{q^{\frac{m}{2}+1}}$. Since $\text{Tr}_q^{\frac{m}{2}}(a\alpha^{\tau\ell}) = \text{Tr}_q^{\frac{m}{2}}(a\beta^{q^{\frac{q-1}{2}}\ell})$ and $\gcd(q\tau, q^m-1) = \frac{(q-1)(q^{\frac{m}{2}+1})}{2}$, it follows that the BCH code $\widehat{\mathcal{C}}_{(q,m,q-1,\delta)}$ has the same weight distribution with the following code

$$\left\{ c(a) = \left(\text{Tr}_q^{\frac{m}{2}}(a\beta^{\frac{q-1}{2}\ell}) \right)_{\ell=0}^{n-1} : a \in \mathbb{F}_{q^{\frac{m}{2}}} \right\}.$$

Let $n' = \frac{2(q^{\frac{m}{2}-1})}{q-1}$ and

$$C' = \left\{ c'(a) = \left(\text{Tr}_q^{\frac{m}{2}}(a\beta^{\frac{q-1}{2}\ell}) \right)_{\ell=0}^{n'-1} : a \in \mathbb{F}_{q^{\frac{m}{2}}} \right\}.$$

Note that $\gcd(\frac{q^{\frac{m}{2}-1}}{q-1}, \frac{q-1}{2}) = 1$. From [12, Theorem 15], C' is a $[n', \frac{m}{2}, 2q^{\frac{m}{2}-1}]$ one-weight code over \mathbb{F}_q . It is easy to check that

$$c(a) = \overbrace{c'(a) \parallel \cdots \parallel c'(a)}^{n'}.$$

Hence, C is a $[n, \frac{m}{2}, (q^{\frac{m}{2}} + 1)q^{\frac{m}{2}-1}]$ one-weight code over \mathbb{F}_q . ■

V. CONCLUSION

The dimension of narrow-sense BCH codes of length $\frac{q^m-1}{\lambda}$ over \mathbb{F}_q has been obtained, where λ is a positive divisor of $q-1$. For the case $\lambda = 1$ and $q-1$, the dimension of $\mathcal{C}_{(q,m,\lambda,\delta)}$ was determined in [28], [29]. For the case $\lambda = q-1$ and m is even, the dimension of $\mathcal{C}_{(q,m,\lambda,\delta)}$ with designed distance δ with $2 \leq \delta \leq q^{\frac{m}{2}}$ was settled in [28]. We settled its dimension for all δ with $2 \leq \delta \leq \frac{q^{\frac{m}{2}}-1}{q-1}$. For $\lambda = 2$ and $q-1$, the weight distribution of $\mathcal{C}_{(q,m,\lambda,\delta)}$ was studied. We find the first few largest q -coset leaders modulo $n = \frac{q^m-1}{2}$ and a trace representation for the codewords in $\mathcal{C}_{(q,m,2,\delta_i)}$ and $\widehat{\mathcal{C}}_{(q,m,2,\delta_i)}$ for $i = 1, 2$. In addition, by using exponential sums and the theory of quadratic forms over finite fields, the weight distribution of $\mathcal{C}_{(q,m,2,\delta_i)}$ and $\widehat{\mathcal{C}}_{(q,m,2,\delta_i)}$ was determined. Moreover, the first largest q -coset leader modulo $\frac{q^m-1}{q-1}$ was determined for three special cases, and the weight distribution of a class of BCH codes of length $\frac{q^m-1}{q-1}$ was also determined. A class of BCH codes meeting the Griesmer bound has been given. These results generalized those from [28], [29], [36].

ACKNOWLEDGEMENTS

The authors wish to express their gratitude to Prof. Vladimir Sidorenko, the Associate Editor, and three anonymous reviewers who gave many helpful comments and suggestions to greatly improve the presentation of the paper.

REFERENCES

- [1] 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.
- [2] D. Augot and N. Sendrier, "Idempotents and the BCH bound," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 204–207, Jan. 1994.
- [3] 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.
- [4] E. R. Berlekamp, "The enumeration of information symbols in BCH codes," *Bell System Tech. J.*, vol. 46, no. 8, pp. 1861–1880, Oct. 1967.
- [5] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Information and control*, vol. 3, no. 1, pp. 68–79, 1960.
- [6] P. Charpin, "Open problems on cyclic codes," *Handbook of coding theory*, Elsevier, Amsterdam, pp. 963–1063, 1998.

- [7] P. Charpin, "On a class of primitive BCH codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 1, pp. 222–228, Jan. 1990.
- [8] P. Charpin, T. Helleseth, and V. A. Zinoviev, "The coset distribution of triple-error-correcting binary primitive BCH codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1727–1732, Apr. 2006.
- [9] 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.
- [10] C. Ding, "Parameters of several classes of BCH codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5322–5330, Oct. 2015.
- [11] C. Ding, C. Fan, and Z. Zhou, "The dimension and minimum distance of two classes of primitive BCH codes," *Finite Fields Appl.*, vol. 45, pp. 237–263, 2017.
- [12] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," *Discrete Math.* vol. 313, no. 4, pp. 434–446, 2013.
- [13] P. Delsarte, "On subfield subcodes of modified Reed-Solomon codes (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 21, no. 5, pp. 575–576, Sept. 1975.
- [14] 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.
- [15] K. Feng and J. Luo, "Weight distribution of some reducible cyclic codes," *Finite Fields Appl.*, vol. 14, no. 2, pp. 390–409, 2008.
- [16] T. Fujiwara, T. Takata, T. Kasami, and S. Lin, "An approximation to the weight distribution of binary primitive BCH codes with designed distances 9 and 11 (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 32, no. 5, pp. 706–709, Sept. 1986.
- [17] J. H. Griesmer, "A bound for error-correcting codes," *IBM J. Res.*, vol. 4, no. 5, pp. 532–542, Nov. 1960.
- [18] A. Hocquenghem, "Codes correcteurs derreurs," *Chiffres*, vol. 2, no. 2, pp. 147–156, 1959.
- [19] H. Helgert and R. Stinaff, "Shortened BCH codes (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 818–820, Nov. 1973.
- [20] G. van der Geer and M. van der Vlugt, "On generalized hamming weights of BCH codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 543–546, Mar. 1994.
- [21] I. Krasikov and S. Litsyn, "On the distance distributions of BCH codes and their duals," *Des. Codes Cryptogr.*, vol. 23, no. 2, pp. 223–232, 2001.
- [22] O. Keren and S. Litsyn, "More on the distance distribution of BCH codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 251–255, Jan. 1999.
- [23] T. Kasami, "Weight distributions of Bose-Chaudhuri-Hocquenghem codes," in: R.C. Bose, T.A. Dowlings (Eds.), *Combinatorial Mathematics and Applications*, Univ. North Carolina Press, Chapel Hill, NC, 1969, Ch.20.
- [24] T. Kasami, T. Fujiwara, and S. Lin, "An approximation of the weight distribution of binary linear codes," *IEEE Trans. Inf. Theory*, vol. 31, no. 6, pp. 769–780, Nov. 1985.
- [25] T. Kasami and S. Lin, "Some results on the minimum weight of primitive BCH codes," *IEEE Trans. Inf. Theory*, vol. 18, no. 6, pp. 824–825, Nov. 1972.
- [26] T. Kasami, S. Lin, and W. W. Peterson, "Linear codes which are invariant under the affine group and some results on minimum weights in BCH codes," *Electron. Commun. Japan*, vol. 50, no. 9, pp. 100–106, 1967.
- [27] T. Kasami and N. Tokura, "Some remarks on BCH bounds and minimum weights of binary primitive BCH codes," *IEEE Trans. Inf. Theory*, vol. 15, no. 3, pp. 408–413, May 1969.
- [28] 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.
- [29] H. Liu, C. Ding, and C. Li, "Dimensions of three types of BCH codes over $GF(q)$," *Discrete Mathematics*, vol. 240, no. 8, pp. 1910–1927, 2017.
- [30] J. Luo and K. Feng, "On the weight distributions of two classes of cyclic codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5332–5344, Dec. 2008.
- [31] J. Luo, Y. Tang, and H. Wang, "Exponential sums, cyclic codes and sequences: The odd characteristic Kasami case," 2009, arXiv:0902.4508.
- [32] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.
- [33] R. Li, Y. Liu, L. Guo, and H. Song, "Dimension of nonbinary antiprimitive BCH codes," 2017, arXiv:1712.06842.
- [34] S. Li, "The minimum distance of some narrow-sense primitive BCH codes," *SIAM Journal on Discrete Mathematics*, vol. 31, no. 4, pp. 2530–2569, 2017.
- [35] S. Li, C. Li, C. Ding, and H. Liu, "Two Families of LCD BCH Codes," *IEEE Trans. Inf. Theory*, vol. 63, no. 9, pp. 5699–5717, Sept. 2017.
- [36] 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.
- [37] S. Lin and E. J. Weldon, "Long BCH codes are bad," *Information and Control*, vol. 11, no. 4, pp. 445–451, 1967.
- [38] D. Mandelbaum, "Two applications of cyclotomic cosets to certain BCH codes (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 26, no. 6, pp. 737–738, Nov. 1980.
- [39] H. B. Mann, "On the number of information symbols in Bose-Chaudhuri codes," *Inf. Control*, vol. 5, no. 2, pp. 153–162, 1962.
- [40] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Pub. Co, 1977.
- [41] G. Vega, "Determining the number of one-weight cyclic codes when length and dimension are given," *International Workshop on the Arithmetic of Finite Fields*, Springer, Berlin, Heidelberg, 2007.
- [42] J. K. Wolf, "Adding two information symbols to certain nonbinary BCH codes and some applications," *Bell Labs Technical Journal*, vol. 48, no. 7, pp. 2405–2424, 1969.
- [43] J. Wolfmann, "Are 2-weight projective cyclic codes irreducible?" *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 733–737, Feb. 2005.
- [44] Z. Wan, *Geometry of classical groups over finite fields: Second edition*, Science Prss, Beijing/New York, 2002.
- [45] H. Yan, "A class of primitive BCH codes and their weight distribution," *AAECC*, DOI 10.1007/s00200-017-0320-4.
- [46] D. Yue, "The structure of cyclotomic cosets and its applications," *J. Sys. Sci. Math. Scis*, vol. 12, no. 1, pp. 15–20, 1992.
- [47] D. Yue and G. Feng, "Minimum cyclotomic coset representatives and their applications to BCH codes and Goppa codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2625–2628, 2000.
- [48] D. Yue and Z. Hu, "On the dimension and minimum distance of BCH codes over $GF(q)$," *J. of Electronics*, vol. 13, no. 3, pp. 216–221, 1996.
- [49] Z. Zhou and C. Ding, "A class of three-weight cyclic codes," *Finite Fields Appl.*, vol. 25, pp. 79–93, 2014.