Narrow-Sense BCH Codes over GF(q) with Length \( n = \frac{q^m-1}{q-1} \)

Shuxing Li, Cunsheng Ding, Maosheng Xiong, and Gennian Ge

Abstract

Cyclic codes over finite fields are widely employed in communication systems, storage devices and consumer electronics, as they have efficient encoding and decoding algorithms. BCH codes, as a special subclass of cyclic codes, are in most cases among the best cyclic codes. A subclass of good BCH codes are the narrow-sense BCH codes over GF(q) with length \( n = (q^m-1)/(q-1) \). Little is known about this class of BCH codes when \( q > 2 \). The objective of this paper is to study some of the codes within this class. In particular, the dimension, the minimum distance, and the weight distribution of some ternary BCH codes with length \( n = (3^m-1)/2 \) are determined in this paper. A class of ternary BCH codes meeting the Griesmer bound is identified. An application of some of the BCH codes in secret sharing is also investigated.

Index Terms

BCH codes, cyclic codes, linear codes, quadratic forms, secret sharing, weight distribution.

I. INTRODUCTION

Throughout this paper, let \( q \) be a power of a prime \( p \). A linear \([n,k,d]\) code \( C \) over GF(q) is a \( k \)-dimensional subspace of GF(q)^n with minimum Hamming distance \( d \). A linear code \( C \) of length \( n \) over GF(q) is called cyclic if \((c_0,c_1,\cdots,c_{n-1}) \in C \) implies \((c_{n-1},c_0,c_1,\cdots,c_{n-2}) \in C \). Cyclic codes over GF(q) can also be viewed as ideals in the quotient ring GF(q)[x]/(x^n - 1).

By identifying any vector \((c_0,c_1,\cdots,c_{n-1}) \in GF(q)^n \) with
\[
c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in GF(q)[x]/(x^n - 1),
\]
any linear code \( C \) of length \( n \) over GF(q) corresponds to a subset of the quotient ring GF(q)[x]/(x^n - 1). A linear code \( C \) is cyclic if and only if the corresponding subset in GF(q)[x]/(x^n - 1) is an ideal of the ring GF(q)[x]/(x^n - 1).

Note that every ideal of GF(q)[x]/(x^n - 1) is principal. Let \( C = \langle g(x) \rangle \) be a cyclic code, where \( g(x) \) is monic and has the smallest degree among all the generators of \( C \). Then \( g(x) \) is unique and called the generator polynomial, and \( h(x) = (x^n - 1)/g(x) \) is referred to as the parity-check polynomial of \( C \). In this paper, we consider only cyclic codes of length \( n \) over GF(q), where \( \gcd(n,q) = 1 \), which implies that the generator polynomial of the code does not have repeated roots.

Let \( n \) be a positive integer. Let \( m = \text{ord}_n(q) \), that is, \( m \) is the smallest positive integer such that \( n|q^m - 1 \). Let \( \alpha \) be a generator of GF\((q^m)^*, \) which is the multiplicative group of GF\((q^m), \) and put \( \beta = \alpha^{q^m - 1}/n \).

The research of C. Ding was supported by the Hong Kong Research Grants Council, under Grant No. 16300415. The research of M. Xiong was supported by RGC grant numbers 606211 and 609513 from Hong Kong. The research of G. Ge was supported by the National Natural Science Foundation of China under Grant Nos. 61171198 and 11431003, the Importation and Development of High-Caliber Talents Project of Beijing Municipal Institutions, and the Scientific and Technological Innovation Capacity Enhancement Program of Beijing Municipal Institutions.

S. Li is with the Department of Mathematics, Zhejiang University, Hangzhou 310027, Zhejiang, China (e-mail: sxli@zju.edu.cn).
C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (email: cding@ust.hk).
M. Xiong is with the Department of Mathematics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong (e-mail: mamxiong@ust.hk).
G. Ge is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China (e-mail: gnge@zju.edu.cn). He is also with Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing, 100048, China.
Then $\beta$ is a primitive $n$-th root of unity in $\text{GF}(q^m)$. For any $i$ with $1 \leq i \leq q^m - 2$, let $m_i(x)$ denote the monic minimal polynomial of $\beta^i$ over $\text{GF}(q)$. For any $2 \leq \delta < n$, define

$$g_{(n,q,m,\delta)}(x) = \text{lcm}(m_1(x), m_2(x), \ldots, m_{\delta-1}(x)),$$

where lcm denotes the least common multiple of these minimal polynomials. Moreover, we define

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

Let $C_{(n,q,m,\delta)}$ and $\tilde{C}_{(n,q,m,\delta)}$ denote the cyclic code of length $n$ with generator polynomial $g_{(n,q,m,\delta)}(x)$ and $\tilde{g}_{(n,q,m,\delta)}(x)$, respectively. Then $C_{(n,q,m,\delta)}$ is called a narrow-sense BCH code with designed distance $\delta$, and $\tilde{C}_{(n,q,m,\delta)}$ is the even-like subcode of $C_{(n,q,m,\delta)}$. Clearly, we have

$$\dim(\tilde{C}_{(n,q,m,\delta)}) = \dim(C_{(n,q,m,\delta)}) - 1.$$ 

By definition, $g_{(n,q,m,\delta)}(x)$ has $\delta - 1$ consecutive roots $\beta^i$ for all $1 \leq i \leq \delta - 1$, and $\tilde{g}_{(n,q,m,\delta)}(x)$ has $\delta$ consecutive roots $\beta^i$ for all $0 \leq i \leq \delta - 1$. It then follows from the BCH bound that the minimum distance of $C_{(n,q,m,\delta)}$ and $\tilde{C}_{(n,q,m,\delta)}$ is at least $\delta$ and $\delta + 1$, respectively. Due to this fact, $\delta$ is called the designed distance of the code $C_{(n,q,m,\delta)}$.

It is well known that the codes $C_{(n,q,m,\delta)}$ and $C_{(n,q,m,\delta')}$ may be identical for two different $\delta$ and $\delta'$. Hence, a BCH code may have many designed distances. The largest designed distance of $C_{(n,q,m,\delta)}$ is called the Bose distance and denoted by $d_B$, which is at least the designed distance of the code. By definition, the Bose distance of a BCH code serves as a lower bound on the minimum distance of the code. It is thus meaningful to determine the Bose distance, if the minimum distance cannot be found out.

The cyclic codes $C_{(n,q,m,\delta)}$ are treated in almost every book on coding theory. When $n = q^m - 1$, the codes $C_{(n,q,m,\delta)}$ and $\tilde{C}_{(n,q,m,\delta)}$ are called narrow-sense primitive BCH codes, which have been studied in a series of literatures [2], [3], [4], [5], [6], [2], [11], [13], [15], [16], [17], [22], [23], [25], [27], [28]. In particular, for a recent summary on the results of narrow-sense primitive BCH codes, the reader is referred to [13]. When $n = (q^m - 1)/(q - 1)$, the codes $C_{(n,q,m,\delta)}$ and $\tilde{C}_{(n,q,m,\delta)}$ are referred to as narrow-sense projective BCH codes, which are not studied in the literature when $q > 2$.

The objective of this paper is to study the parameters of special classes of narrow-sense projective BCH codes. Various methods, including cyclotomic cosets, locator polynomials, nondecreasing sequence decompositions and exponential sums related to quadratic forms over finite fields are used to obtain the dimension, Bose distance, minimum distance and weight distribution of several families of narrow-sense projective BCH codes. A class of ternary BCH codes meeting the Griesmer bound is identified. An application of some of the BCH codes presented in this paper is also investigated.

As will be shown, some narrow-sense projective BCH codes have optimal parameters. To investigate the optimality of some of the codes studied in this paper, we compare them with tables of the best known linear codes maintained by Markus Grassl at [http://www.codetables.de](http://www.codetables.de) which is called the Database later in this paper. In some cases, we will also use the tables of best cyclic codes given in the monograph [12] as benchmarks.

II. Preliminaries

In this section, we present some necessary background concerning cyclotomic cosets, coset leaders, nondecreasing sequence decompositions, quadratic forms over finite fields and exponential sums. Some known results about BCH codes are also recalled.
A. Cyclotomic cosets

To deal with cyclic codes of length \( n \) over \( GF(q) \), we have to study the canonical factorization of \( x^n - 1 \) over \( GF(q) \). To this end, we need to introduce \( q \)-cyclotomic cosets modulo \( n \).

Recall that \( \mathbb{Z}_n \) denotes the ring of integers modulo \( n \). Let \( s \) be an integer with \( 0 \leq s < n \). The \( q \)-cyclotomic coset of \( s \) modulo \( n \) is defined by

\[
C_s = \{s, sq, sq^2, \cdots, sq^{\ell_s-1}\} \mod n \subseteq \mathbb{Z}_n,
\]

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

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

Namely, the \( q \)-cyclotomic cosets modulo \( n \) form a partition of \( \mathbb{Z}_n \).

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

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

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

\[x^n - 1 = \prod_{s \in \Gamma_{(n,q)}} m_s(x), \tag{3}\]

which is the factorization of \( x^n - 1 \) into irreducible factors over \( GF(q) \). Thus, for any cyclic code

\[C = \langle g(x) \rangle \subseteq GF(q)[x]/(x^n - 1),\]

the generator polynomial \( g(x) \) must be the product of several \( m_s(x) \)'s. Hence, the degree of \( g(x) \) and thus the dimension of \( C \) are determined by the sizes of cyclotomic cosets associated with \( g(x) \).

Below, we present some useful results concerning cyclotomic cosets. For the size of cyclotomic cosets, we have the following lemma.

**Lemma 1.** [14, Theorem 4.1.4] The size \( \ell_s \) of each \( q \)-cyclotomic coset \( C_s \) is a divisor of \( \text{ord}_n(q) \), which is the size \( \ell_1 \) of \( C_1 \).

The following lemma says when \( s \) is small, the size of \( q \)-cyclotomic coset \( C_s \subset \mathbb{Z}_n \) is always equal to \( \text{ord}_n(q) \).

**Lemma 2.** [2, Lemma 8] Let \( n \) be a positive integer such that \( \gcd(n,q) = 1 \) and \( q^{\lfloor m/2 \rfloor} < n \leq q^m - 1 \), where \( m = \text{ord}_n(q) \). Then the \( q \)-cyclotomic coset \( C_s \) has cardinality \( m \) for all \( s \) in the range \( 1 \leq s \leq nq^{\lfloor m/2 \rfloor}/(q^m - 1) \).

As a direct consequence, we can easily know the dimension of certain BCH codes.

**Theorem 3.** [2, Theorem 10] Let \( n \) be a positive integer such that \( \gcd(n,q) = 1 \) and \( q^{\lfloor m/2 \rfloor} < n \leq q^m - 1 \), where \( m = \text{ord}_n(q) \). Then the narrow-sense BCH code of length \( n \) and designed distance \( \delta \) in the range \( 2 \leq \delta \leq \min\{nq^{\lfloor m/2 \rfloor}/(q^m - 1), n\} \) has dimension

\[k = n - m[(\delta - 1)(1 - 1/q)].\]
B. Nondecreasing sequence decompositions and coset leaders

As is well known, the Bose distance of a narrow-sense BCH code over GF($q$) with length $n$ is necessarily a coset leader of a $q$-cyclotomic coset in $\mathbb{Z}_m$. There have been some interesting results on coset leaders of $q$-cyclotomic cosets when $n = q^m - 1$ ([13], [22], [27]). Particularly, in [27], the concept of nondecreasing sequence decompositions was proposed and its close relation with coset leaders modulo $q^m - 1$ was discussed. In this subsection, we show that this concept is also helpful in determining some special $q$-cyclotomic coset leaders modulo $\frac{q^m - 1}{q-1}$. Here we always assume that $q > 2$ is a prime power.

Suppose $\underline{v} = (v_{n-1}, v_{n-2}, \ldots, v_0)$ is a sequence of length $n$ with each component $v_i$ satisfying $0 \leq v_i \leq q - 1$. The sequence $\underline{v}$ is called a nondecreasing sequence (NDS) if $v_{i+1} \leq v_i$ for $0 \leq i \leq n - 1$. Any sequence has a unique nondecreasing sequence decomposition as a concatenation $V_1V_2\ldots V_r$ where the $V_i$’s are NDSs and $r$ is minimal. Let $\underline{v} = (v_{l-1}, \ldots, v_0)$ and $\underline{w} = (w_{k-1}, \ldots, w_0)$ be two NDSs. We say $\underline{v} = \underline{w}$ if $l = k$ and $v_{l-1-i} = w_{k-1-i}$ for $0 \leq i \leq l - 1$. We say $\underline{v} \geq \underline{w}$ if either $l > k$ and $v_{l-1-i} = w_{k-1-i}$ for $0 \leq i \leq k - 1$ or there is an integer $0 \leq j \leq \min\{l, k\} - 1$ such that $v_{l-1-j} > w_{k-1-j}$ and $v_{l-1-i} = w_{k-1-i}$ for $0 \leq i \leq j - 1$. For two sequences of the same length with the NDS decomposition given by $\underline{v} = V_1V_2\ldots V_r$ and $\underline{w} = W_1W_2\ldots W_s$, we say $\underline{v} = \underline{w}$ if $\underline{v}$ and $\underline{w}$ are identical. We say $\underline{v} \geq \underline{w}$ if there is an integer $0 \leq j \leq \min\{r, s\} - 1$ such that $V_{r-1-j} > W_{s-1-j}$ and $V_{r-1-i} = W_{s-1-i}$ for $0 \leq i \leq j - 1$. We remark that the notion “$\underline{v} \geq \underline{w}$” described above is consistent with the natural inequality $\sum_i v_i q^i \geq \sum_i w_i q^i$ of the corresponding integers.

Given a positive integer $s$, we may assume that $0 < s < n$. Suppose the unique $q$-ary expansion of $s$ is $\sum_{i=0}^{m-1} s_i q^i$, where $0 \leq s_i \leq q - 1$. This defines the sequence $\underline{s} = (s_{m-1}, s_{m-2}, \ldots, s_0)$. Denote by $E(s)$ the NDS decomposition of $\underline{s}$. Conversely, let $V_1V_2\ldots V_r$ be the NDS decomposition of $\underline{s}$. Then define

$$E^{-1}(V_1V_2\ldots V_r) = s.$$

The coset leader of $C_s$ modulo $n$ is denoted by $s^*$.

When $n = q^m - 1$ and $\underline{s} = (s_{m-1}, s_{m-2}, \ldots, s_0)$, noting that $\underline{\pi} = (q - 1, q - 1, \ldots, q - 1)$, it is clear that the sequence $q^i s$ corresponding to $q^i s \mod n$ is

$$q^i s = (s_{m-1-i}, \ldots, s_0, s_{m-1}, \ldots, s_{m-i}), \quad 1 \leq i \leq m - 1.$$  

That is, when $n = q^m - 1$, multiplying a power of $q$ simply corresponds to a cyclic shift of the original sequence $\underline{s}$. This key fact is fundamental for the important results presented in [27]. When $n = \frac{q^m - 1}{q-1}$, the situation is more complicated: while (4) is still true, however, when $q^i s \geq \underline{\pi}$, noting that $\underline{\pi} = (1, 1, \ldots, 1)$, we need to subtract $q^i s$ by some multiples of $(1, 1, \ldots, 1)$ so that the resulting sequence lies in between $\underline{0}$ and $\underline{\pi}$. With this observation, we can translate easily some results of [27] into the new context, where the modulus is $n = \frac{q^m - 1}{q-1}$. From now on, we always concern $q$-cyclotomic cosets modulo $n = \frac{q^m - 1}{q-1}$.

**Lemma 4.** Let $0 \leq s \leq \frac{q^m - 1}{q-1} - 1$ be an integer such that the components of $\underline{s}$ are either 0 or 1. Suppose $E(s) = V_1V_2\ldots V_r$. Then we have the following.

i) $E(s^*) = V_jV_{j+1}\ldots V_rV_1\ldots V_{j-1}$ for some $j$ where $V_i \geq V_{i+1}$ for any $1 \leq i \leq r$.

ii) If $V_1 = V_2 = \cdots = V_r$ or $V_1 = V_2 = \cdots = V_j < V_k$ for all $k > j$, then $s = s^*$.

iii) If $r = 1$, then $s = s^*$.

**Proof:** Since $\underline{\pi} = (1, 1, \ldots, 1)$ and the components of $\underline{s}$ are either 0 or 1, the components of $q^i s$ are also either 0 or 1. Thus $0 < q^i s < \underline{\pi}$ for any $i$. Therefore the process of subtracting $q^i s$ by multiples of $\underline{\pi}$ is not involved. The proof is exactly the same as that of [27, Theorem 2.2] for $n = q^m - 1$.

Let $\underline{v} = (v_{l-1}, v_{l-2}, \ldots, v_0)$ be an NDS. Define the truncating operator $T_k$ as

$$T_k(\underline{v}) = (v_{l-1}, v_{l-2}, \ldots, v_{l-k}), \quad 1 \leq k \leq l.$$

We now define the successor operator $S$ in the way that $S(\underline{v})$ is the smallest NDS that is larger than $\underline{v}$. In particular, if $v_0 \leq q - 1$, we have

$$S(\underline{v}) = (v_{l-1}, v_{l-2}, \ldots, v_0 + 1),$$
which corresponds to the successor of the integer \( \sum_{i=0}^{l-1} v_i q^i \). The following lemma provides information about the coset leaders modulo \( \frac{q^m - 1}{q - 1} \) in a special case.

**Lemma 5.** Let \( 0 \leq s \leq \frac{q^m - 1}{q - 1} - 1 \) be an integer. Suppose \( E(s) = V_1 V_2 \ldots V_r \), where \( V_1 > V_2 \). Suppose \( V_1 \) has length \( l \) and has components either 0 or 1. Let \( M(s) \) be the smallest coset leader greater than or equal to \( s \). Write \( m = al + b \), where \( 0 \leq b \leq l - 1 \). If \( b = 0 \), we have

\[
M(s) = E^{-1}(V_1 V_2 \ldots V_1).
\]

If \( 1 \leq b \leq l - 1 \), we have

\[
M(s) \geq E^{-1}(V_1 V_2 \ldots V_1 S(T_b(V_1))).
\]

In particular, if the last component of \( S(T_b(V_1)) \) is 1, then the equality holds.

**Proof:** The proof is the same as that of [27, Theorem 2.5] for \( n = q^m - 1 \), because in (4) no subtracting of \((1,1,\ldots,1)\) from \( q^i \) is involved.

---

**C. Gauss and exponential sums related to quadratic forms**

In this subsection, we recall some properties of Gauss sums and exponential sums related to quadratic forms over finite fields. Instead of presenting a detailed account, we refer readers to [18, Chapter 5] for basic properties of Gauss sums and to [18, Chapter 6] and [19] for definitions and basic properties of quadratic forms over finite fields. Here, we only list two lemmas which will be used later in the paper.

**Definition 1.** Let \( \chi \) be a multiplicative character over \( \text{GF}(q) \) and \( \text{Tr} \) be the trace function from \( \text{GF}(q) \) to \( \text{GF}(p) \). The Gauss sum \( G(\chi) \) is defined to be

\[
G(\chi) = \sum_{x \in \text{GF}(q)} \chi(x) \zeta_p^{\text{Tr}(x)},
\]

where \( \zeta_p := \exp(2\pi \sqrt{-1}/p) \) is a \( p \)-th complex root of unity.

**Lemma 6.** [18, Theorem 5.15] Let \( q = p^s \) and \( \eta \) be the quadratic character of \( \text{GF}(q) \) (hence \( p \) is odd). Then the quadratic Gauss sum satisfies

\[
G(\eta) = \begin{cases} 
(-1)^{s-1} \sqrt{q} & \text{if } p \equiv 1 \mod 4, \\
(-1)^{s-1}(\sqrt{-1})^s \sqrt{q} & \text{if } p \equiv 3 \mod 4.
\end{cases}
\]

If \( \eta \) is the quadratic character of \( \text{GF}(q) \) and \( G(\eta) \) is the quadratic Gauss sum, the following identity holds:

\[
\sum_{x \in \text{GF}(q)^*} \zeta_p^{\text{Tr}(ax^2)} = \frac{\eta(a)G(\eta) - 1}{2}, \quad \forall a \in \text{GF}(q)^*.
\]  

**Lemma 7.** [19, Lemma 1] Let \( q \) be an odd prime power and \( Q(x) \) be a quadratic form from \( \text{GF}(q^m) \) to \( \text{GF}(q) \) with rank \( r \). Then

\[
\sum_{x \in \text{GF}(q^m)} \zeta_p^{\text{Tr}_p^m(Q(x))} = \begin{cases} 
\pm q^{m-r/2} & \text{if } q \equiv 1 \mod 4, \\
\pm (\sqrt{-1})^r q^{m-r/2} & \text{if } q \equiv 3 \mod 4.
\end{cases}
\]
D. Some known results concerning BCH codes

We first review the definition of the locator polynomial of a vector. It has been observed that locator polynomials are very useful in the study of BCH codes [3], [4].

**Definition 2.** Let $c = (c_0, c_1, \ldots, c_{n-1}) \in \text{GF}(q)^n$ be a vector with nonzero components $c_1, c_2, \ldots, c_w$. Then

\[ X_1 = \beta^i_1, \ldots, X_w = \beta^i_w \]

are called the locators of $c$. The locator polynomial of $c$ is

\[ \sigma(z) = \prod_{i=1}^{w} (1 - X_i z) = \sum_{i=0}^{w} \sigma_i z^i, \]

where $\sigma_0 = 1$. The coefficients $\sigma_i$ are the elementary symmetric functions of $X_i$:

\[
\begin{align*}
\sigma_1 &= -(X_1 + \cdots + X_w), \\
\sigma_2 &= X_1X_2 + X_1X_3 + \cdots + X_{w-1}X_w, \\
& \vdots \\
\sigma_w &= (-1)^w X_1 \cdots X_w.
\end{align*}
\]

The following lemma describes a condition for a polynomial over $\text{GF}(q)$ being a locator polynomial of a codeword in a BCH code. Indeed, this lemma suggests a way to find a codeword in a BCH code with prescribed weight, in which the locator polynomial is used.

**Lemma 8.** [21, Ch. 9, Lemma 4] Let

\[ \sigma(z) = \sum_{i=0}^{w} \sigma_i z^i \]

be a polynomial over $\text{GF}(q)$. Then $\sigma(z)$ is the locator polynomial of a codeword $c$ with only 0 and 1 components belonging to $C_{n,q,m,\delta}$ if and only if the following two conditions hold.

i) The zeroes of $\sigma(z)$ are distinct $n$-th roots of unity.

ii) $\sigma_i = 0$ for all $1 \leq i \leq \delta - 1$ with $p \nmid i$, where $p$ is the characteristic of $\text{GF}(q)$.

The following lemma says in some cases, the minimum distance equals the designed distance.

**Lemma 9.** [6] Theorem 4.3.13] For a BCH code $C_{n,q,m,\delta}$, if $\delta \mid n$, then the minimum distance $d = \delta$.

### III. The narrow-sense projective BCH codes with large dimensions

For the rest of this paper, we will always assume that $n = \frac{q^m - 1}{q - 1}$. Therefore, we have $\text{ord}_n(q) = m$. We use $\alpha$ to denote a primitive element of $\text{GF}(q^m)$ and $\beta = \alpha^{q-1}$. $C_{(q,m,\delta)}$ and $\widetilde{C}_{(q,m,\delta)}$ are the narrow-sense projective BCH codes $C_{(\frac{q^m - 1}{q-1},q,m,\delta)}$ and $\widetilde{C}_{(\frac{q^m - 1}{q-1},q,m,\delta)}$ respectively. In this section, we consider the narrow-sense projective BCH codes with few zeroes, and thus with large dimensions.

The narrow-sense projective BCH code with designed distance 2 has only one zero. The parameters of these codes are known.

**Theorem 10.** The code $C_{(n,q,m,2)}$ has parameters $[(q^m - 1)/(q - 1), (q^m - 1)/(q - 1) - m, d]$, where

\[
d = \begin{cases} 
3 & \text{if } \gcd(m, q - 1) = 1, \\
2 & \text{if } \gcd(m, q - 1) \neq 1.
\end{cases}
\]

**Proof:** The dimension follows from the fact that $|C_1| = m$. Since $C_{(n,q,m,2)}$ has only one zero $\beta$, its parity check matrix is

\[ H = (1, \beta, \ldots, \beta^{n-1}), \]
where the \(i\)-th column is a vector in \(\text{GF}(q)^m\) corresponding to \(\beta^{i-1}\). When \(\gcd(n,q-1) = \gcd(m,q-1) = 1\), it is easy to verify that every two columns of \(H\) are linearly independent. Thus, the code \(C_{(n,q,m,2)}\) is simply the Hamming code and \(d = 3\). When \(\gcd(m,q-1) \neq 1\), we can find two columns of \(H\) which are linearly dependent. This implies that \(d = 2\).

**Theorem 11.** The code \(\tilde{C}_{(n,q,m,2)}\) has parameters \([(q^m - 1)/(q - 1), (q^m - 1)/(q - 1) - m - 1, d], \) where \(d \in \{3, 4\}\).

**Proof:** \(\tilde{C}_{(n,q,m,2)}\) is the even-like subcode of \(C_{(n,q,m,2)}\) with dimension \((q^m - 1)/(q - 1) - m - 1\). The minimum distance \(2 \leq d \leq 4\), where the lower bound follows from the BCH bound and the upper bound follows from the sphere packing bound. Note that the parity check matrix is

\[
\tilde{H} = \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
& H
\end{pmatrix},
\]

where \(H\) is the parity check matrix of the code \(C_{(n,q,m,2)}\) in Theorem 10. It is easy to show that the column rank of \(\tilde{H}\) is greater than 2. Thus, we have \(d \in \{3, 4\}\).

For the narrow-sense projective BCH codes with designed distance 3, the parameters can be determined in some cases, and are described in the next theorem.

**Theorem 12.** Let \(q \geq 3\). The code \(C_{(n,q,m,3)}\) has parameters \([(q^m - 1)/(q - 1), (q^m - 1)/(q - 1) - 2m, d], \) where \(d = 3\) in the following cases:

i) \(q \equiv 1 \mod 3\) and \(3 \mid m\),

ii) \(q \equiv 2 \mod 3\) and \(2 \mid m\),

and \(d \leq 4\) in the following cases:

iii) \(q \equiv 1 \mod 4\) and \(4 \mid m\),

iv) \(q \equiv 3 \mod 4\) and \(2 \mid m\).

In particular, if \(q = 3\) and \(2 \mid m\), we have \(d = 4\).

**Proof:** The dimension follows from the fact that \(|C_1| = |C_2| = m\). For the minimum distance, we will only prove the case where \(d \leq 4\). The case for \(d = 3\) is analogous. To show \(d \leq 4\), we are going to find a codeword \(c \in C_{(n,q,m,3)}\) with weight 4. By Lemma 8, it suffices to find a locator polynomial \(\sigma(z) = \sum_{i=0}^{4} \sigma_i z^i\) of \(c\), where all roots of \(\sigma(z)\) belong to the cyclic group \(\langle \beta \rangle\) and \(\sigma_1 = \sigma_2 = 0\). By Definition 2 that is to find \(X_1, X_2, X_3, X_4 \in \langle \beta \rangle\), such that

\[
\begin{cases}
X_1 + X_2 + X_3 + X_4 = 0, \\
X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 = 0.
\end{cases}
\]

Condition iii) or Condition iv) implies that \(4 \mid \frac{q^m - 1}{q - 1}\) and \(-1 \in \langle \beta \rangle\). Thus, we can choose \(X_1 = 1, X_2 = -1, X_3 = \beta^{\frac{q^m - 1}{q - 1}}, X_4 = -\beta^{\frac{q^m - 1}{q - 1}}\), such that \(X_1, X_2, X_3, X_4 \in \langle \beta \rangle\) and the two equations above hold. Namely, we find a codeword \(c \in \tilde{C}_{(n,q,m,3)}\) with weight 4, whose components are 0 or 1. Thus, we have \(d \leq 4\).

In particular, if \(q = 3\), we have \(3 \in C_1\), which implies the Bose distance \(d_B \geq 4\). On the other hand, when \(q = 3\) and \(2 \mid m\), we have \(d \leq 4\). Noting that \(4 \geq d \geq d_B \geq 4\), we have \(d = 4\).

Let \(q \geq 3\). For the minimum distance of the code \(C_{(n,q,m,3)}\), numerical experiments show that \(d = 4\) when \(q = 3\) and \(d \in \{3, 4\}\) when \(q > 3\). Theoretically, the BCH bound and the sphere packing bound imply that \(4 \leq d \leq 6\) when \(q = 3\) and \(3 \leq d \leq 6\) when \(q > 3\). As shown in Theorem 12, we can exclude the possibility of \(d \in \{5, 6\}\) in some cases using locator polynomials. However, we are not sure if this technique can be applied to the remaining cases since this approach can only find the codeword whose components are either 0 or 1.
IV. THE NARROW-SENSE PROJECTIVE BCH CODES WITH SMALL DIMENSIONS

In this section, we study narrow-sense projective BCH codes with small dimensions. Our task is to find the first few largest coset leaders modulo \( n = (q^m - 1)/(q - 1) \). Note that the Bose distance of a narrow-sense BCH code must be a coset leader. The knowledge of these coset leaders provides information on the Bose distance and dimension of narrow-sense BCH codes whose zeroes include all roots of \( x^n - 1 \) except those corresponding to the first few largest coset leaders. We denote the first (resp. second) largest coset leader modulo \( n \) by \( \delta_1 \) (resp. \( \delta_2 \)). It looks to be a hard problem to determine \( \delta_1 \) and \( \delta_2 \) for all \( q > 2 \).

For the rest of this section, we assume that \( q = 3 \) and deal with only the case \( q = 3 \).

A. THE TWO COSET LEADERS \( \delta_1 \) AND \( \delta_2 \)

**Lemma 13.** Let \( q = 3 \) and \( m \geq 2 \). The first largest coset leader modulo \( n = (q^m - 1)/(q - 1) \) is

\[
\delta_1 = q^{m-1} - 1 - \frac{q^{(m-1)/2} - 1}{q - 1}
\]

and

\[|C_{\delta_1}| = \begin{cases} m & \text{if } m \text{ is odd,} \\ \frac{m}{2} & \text{if } m \text{ is even.} \end{cases}\]

The second largest coset leader modulo \( n \) is

\[
\delta_2 = q^{m-1} - 1 - \frac{q^{(m+1)/2} - 1}{q - 1}
\]

and \( |C_{\delta_2}| = m \).

**Proof:** When \( m \in \{2, 3\} \), the desired conclusions can be verified directly. Below, we consider the case that \( m \geq 4 \). Suppose \( 0 < \delta < n \) is a coset leader of the form \( \overline{\delta} = (a_{m-1}, a_{m-2}, \ldots, a_0) \). We first observe that \( a_{m-1} = 0 \). This is because suppose otherwise, since \( \delta < n \), we have \( a_{m-1} = 1 \) and there is a component \( a_i \) such that \( a_i = 0 \). We may take a cyclic shift \( \frac{q}{\delta} \) for some \( j \) (see (4)) so that \( a_i = 0 \) becomes the first component, thus \( \frac{q}{\delta} \overline{\delta} < \overline{\delta} \), a contradiction to the assumption that \( \delta \) is a coset leader.

Next we assume that the coset leader \( \delta \) is of the form \( \overline{\delta} = (0, 2, a_{m-3}, \ldots, a_0) \). By the same argument as before, \( 00 \) and \( 01 \) cannot appear in the sequence \( \overline{\delta} \). Moreover, if \( 12 \) appears, by taking a suitable cyclic shift we have \( \frac{q}{\delta} \overline{\delta} = (1, 2, \ldots, 0, 2, \ldots) \) for some \( j \). It is easy to see that

\[
0 < \frac{q}{\delta} \overline{\delta} - \overline{n} = (1, 2, \ldots, 0, 2, \ldots) - (1, 1, \ldots, 1) = (0, b_{m-1}, \ldots, b_0) = \overline{v},
\]

where \( 0 \leq b_{m-1} \leq 1 \), hence \( \overline{v} < \overline{\delta} \), a contradiction to the assumption that \( \delta \) is a coset leader. So \( 12 \) does not appear in \( \overline{\delta} \).

Thirdly, let

\[
\overline{\delta} = (0, 2, \ldots, 2, 1, \ldots, 1),
\]

(6)
where \( u + v + 1 = m \). We can check that the sequences corresponding to \( q^i \delta \mod n \) are given by

\[
\overline{q^i \delta} = (1, \ldots, 1, 0, 2, \ldots, 2), \quad \text{where} \quad u - 1 \quad \text{and} \quad v + 1
\]

\[
\overline{q^i \delta} = (1, \ldots, 1, 0, 2, \ldots, 2, 1, \ldots), \quad 2 \leq i \leq u - 1,
\]

\[
\overline{q^i \delta} = (0, 2, \ldots, 2, 1, \ldots),
\]

\[
\overline{q^i \delta} = \left(0, \underbrace{2, \ldots, 2}_{u-1}, \underbrace{1, \ldots, 1}_{v+1}\right), \quad 1 \leq i \leq v - 1.
\]

Therefore, the \( \delta \) of the form (6) is a coset leader modulo \( n \) if and only if \( u \leq v + 1 \), that is, \( u \leq \frac{m}{2} \).

Finally, let \( \delta \) be a coset leader of the form \( \overline{\delta} = (0, 2, a_{m-3}, \ldots, a_0) \) but not of the form (6). From what we have proved, \( \overline{\delta} \) must be of the form

\[
\overline{\delta} = (0, 2, \ldots, 2, 1, \ldots, 1, 0, 2, \ldots, 2, 1, \ldots) = (0, 2, \ldots, 2, 1, \ldots). \quad \text{where} \quad t \geq 2 \quad \text{and} \quad u_1 \leq u_i \quad \text{for all} \quad 2 \leq i \leq u.
\]

In particular, we have \( u_1 \leq u_2 \) and \( u_1 + u_2 + 2 \leq m \), which implies that \( u_1 \leq \frac{m}{2} - 1 \).

From the arguments above, it is easy to see that the largest two coset leaders \( \delta_1 \) and \( \delta_2 \) are given below:

When \( m \geq 4 \) is even: \( \overline{\delta_1} = (0, 2, \ldots, 2, 1, \ldots) \), \( \overline{\delta_2} = (0, 2, \ldots, 2, 1, \ldots) \).

When \( m \geq 4 \) is odd: \( \overline{\delta_1} = (0, 2, \ldots, 2, 1, \ldots) \), \( \overline{\delta_2} = (0, 2, \ldots, 2, 1, \ldots) \).

It is easily seen that this corresponds to

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

Since \( q^\frac{m}{2} \delta_1 \equiv \delta_1 \pmod{n} \) when \( m \) is even. We have

\[
|\mathcal{C}_\delta| = \begin{cases} \frac{m}{2} & \text{if} \ m \text{ is odd}, \\ m & \text{if} \ m \text{ is even}. \end{cases}
\]

It is easily verified that

\[
\delta_2 = q^{m-1} - 1 - \frac{q^{\lfloor (m+1)/2 \rfloor} - 1}{q - 1}.
\]

It can also be showed that \( |\mathcal{C}_{\delta_2}| = m \). This completes the proof of Lemma 13.
B. Some other coset leaders \( \delta_i \)

Recall that \( q = 3 \). Let \( \delta_i \) denote the \( i \)-th largest coset leader modulo \( n = (q^m - 1)/(q - 1) \). In this section, we point out that some of the coset leaders \( \delta_i \) can also be determined in the case \( q = 3 \).

Let \( \delta \) be a coset leader of the form

\[
\overline{\delta} = (0, 2, \ldots, 2, 1, \ldots, 1, \ldots, 0, 2, \ldots, 2, 1, \ldots, 1).
\]

where \( \sum_{i=1}^{t} (u_i + v_i + 1) = m \). Moreover,

\[
q\delta = (1, \ldots, 1, 0, 2, \ldots, 2, 1, \ldots, 1, 0, 2, \ldots, 2).
\]

Clearly, \( \delta \) is a coset leader only if \( u_1 \leq u_2 \leq \cdots \leq u_t \) and \( u_1 \leq v_i + 1 \) for any \( 1 \leq i \leq t \). In particular, if \( t \geq 2 \), then \( u_1 + v_1 + u_2 + v_2 + 2 \leq m \) which implies that \( u_1 \leq \frac{m}{4} \). Consequently, for \( 1 \leq i \leq \lfloor \frac{m}{4} \rfloor \), \( \delta_i \) must be of the form

\[
\overline{\delta}_i = (0, 2, \ldots, 2, 1, \ldots, 1, \ldots, 0, 2, \ldots, 2, 1, \ldots, 1, \ldots, 0, 2, \ldots, 2).
\]

where \( \lfloor \frac{m}{4} \rfloor - i \). Therefore

\[
\delta_i = q^{m-1} - 1 - \frac{q^{\lfloor \frac{m}{2} - 1 \rfloor} - 1}{q^{1}}, \quad 1 \leq i \leq \lfloor \frac{m}{4} \rfloor.
\]

We can see the condition \( q = 3 \) plays an essential role since the resulting value after multiplying a power of 3 is predictable. However, for the case \( q > 3 \), we do not have a similar result.

C. The ternary codes \( C_{(n,q,m,\delta_1)} \) and \( \bar{C}_{(n,q,m,\delta_1)} \)

Now we study the ternary codes \( C_{(n,q,m,\delta_1)} \) and \( \bar{C}_{(n,q,m,\delta_1)} \). Recall again that \( q = 3 \).

Theorem 14. Let \( m \geq 3 \) and \( q = 3 \). Then the ternary code \( C_{(n,q,m,\delta_1)} \) has parameters

\[
\left[ \frac{q^m - 1}{q - 1}, k, \delta_1 \right],
\]

where

\[
k = \begin{cases} 
m + 1 & \text{if } m \text{ is odd}, \\
\frac{m+2}{2} & \text{if } m \text{ is even}.
\end{cases}
\]

In addition, \( C_{(n,q,m,\delta_1)} \) is a three-weight code if \( m \geq 4 \) is even, and a four-weight code if \( m \geq 3 \) is odd. The weight distribution of \( C_{(n,q,m,\delta_1)} \) is listed in Table 7 and Table 14.

Proof: We consider only the case that \( m \geq 3 \) is odd. The case that \( m \geq 4 \) is even can be treated in the same way. The conclusion on the dimension of the code follows from Lemma 13. Note that

\[
\frac{3^m - 1}{2} - \delta_1 = \frac{3^{m-1} + 3^{m-1} - 1}{2}.
\]

By Delsarte’s Theorem [10],

\[
C_{(n,q,m,\delta_1)} = \{ \bar{c}(a,b) : a \in GF(3^m), b \in GF(3) \},
\]

where

\[
\bar{c}(a,b) = \left( \text{Tr}_{3}^{3^m} \left( a\alpha^{i(3^{m-1} + 3^{m-1} - 1)} + b \right) \right)^{n-1}.
\]

Here \( \alpha \) is a generator of \( GF(3^m)^* \). Since \( \gcd(3^{m-1} + 3^{m-1}, 3^m - 1) = 2 \), it is equivalent to studying the weight distribution of the code whose codewords are given by

\[
c(a,b) = \left( \text{Tr}_{3}^{3^m} \left( a\alpha^{j} + b \right) \right)^{n-1}, \quad a \in GF(3^m), b \in GF(3).
\]
we obtain the weight distribution for the case that

Here \( \zeta_3 \) is the quadratic character and \( \zeta_3 = \frac{-1 + \sqrt{-3}}{2} \) is the 3rd complex root of unity. By (5) we obtain

\[
w(c(a,b)) = \frac{2}{3} n - \frac{1}{6} \sum_{x \in \mathbb{GF}(3)^*} \zeta_3^b \left( \eta(ax)G(\eta) - 1 \right)
\]

where \( \eta \) is the quadratic character and \( G(\eta) \) is the quadratic Gauss sum over \( \mathbb{GF}(3^m) \).

Since \( m \) is odd, \( \eta(-1) = -1 \). Using the values of \( G(\eta) \) from Lemma 6, we find that if \( a \neq 0 \) and \( b = 0 \), \( w(c(a,b)) \) takes the value \( 3^{m-1} \) for \( 3^m - 1 \) times, and if \( a = 0 \) and \( b \neq 0 \), the weight \( w(c(a,b)) \) takes the value \( 3^{m-1} - \frac{1+(-1)^{m+1/2}(m+1/2)}{2} \) for \( 3^m - 1 \) times, respectively. Therefore, we obtain the weight distribution for the case that \( m \geq 3 \) is odd.

**Example 1.** Let \((q,m) = (3,4)\). Then the code \( C_{(n,q,m,d)} \) of Theorem 14 has parameters \([40,3,25]\), and weight enumerator \( 1 + 16z^{25} + 8z^{30} + 2z^{40} \). This code is the best cyclic code according to [12, p. 305].

TABLE I

| Weight | Frequency |
|--------|-----------|
| 0      | 1         |
| \(3^m-1 - \frac{3^{m+1}}{2} + 3^{m/2} + 1\) | \(2(3^{m/2} - 1)\) |
| \(3^m-1 + 3^{m/2} - 1\) | \(3^{m/2} - 1\) |
| \(\frac{3^{m-1}}{2}\) | 2         |

TABLE II

| Weight | Frequency |
|--------|-----------|
| 0      | 1         |
| \(3^m-1\) | \(3^m - 1\) |
| \(3^m-1 - \frac{1+(-1)^{m+1/2}(m+1/2)}{2}\) | \(3^m - 1\) |
| \(3^m-1 - \frac{1+(-1)^{m+1/2}(m+1/2)}{2}\) | \(3^m - 1\) |
| \(\frac{3^{m-1}}{2}\) | 2         |
Example 2. Let \((q,m) = (3,5)\). Then the code \(C_{(n,q,m,\delta_1)}\) of Theorem [14] has parameters \([121,6,76]\), and weight enumerator \(1 + 242z^{76} + 242z^{81} + 242z^{85} + 2z^{121}\).

Theorem 15. Let \(m \geq 3\) and \(q = 3\). Then the ternary code \(\tilde{C}_{(n,q,m,\delta_1)}\) has parameters
\[
\left\lfloor \frac{q^m - 1}{q - 1}, k, d \right\rfloor,
\]
where
\[
k = \begin{cases} m & \text{if } m \text{ is odd}, \\ \frac{m}{2} & \text{if } m \text{ is even}, \end{cases}
\]
and
\[
d = \begin{cases} 3^{m-1} & \text{if } m \text{ is odd}, \\ 3^{m-1} + 3^{\frac{m}{2}} - 1 & \text{if } m \text{ is even}. \end{cases}
\]
In addition, \(\tilde{C}_{(n,q,m,\delta_1)}\) is a one-weight code.

Proof: By Delsarte’s Theorem [10],
\[
\tilde{C}_{(n,q,m,\delta_1)} = \{c(a) : a \in GF(3^m)\},
\]
where
\[
c(a) = \left( \text{Tr}_3 3^m \left( aq^{(3^{m-1} + 3^{\frac{m-1}{2}})} \right) \right)_{j=0}^{n-1}.
\]
Note that \(\tilde{C}_{(n,q,m,\delta_1)}\) is simply a subcode of \(C_{(n,q,m,\delta_1)}\). The weight distribution easily follows from Theorem [14].

It can be easily verified that the code \(\tilde{C}_{(n,q,m,\delta_1)}\) of Theorem [15] meets the Griesmer bound for linear codes, and is thus optimal. When \(m\) is even, the parameters of the code \(\tilde{C}_{(n,q,m,\delta_1)}\) may be new. When \(m\) is odd, the parameters of the code \(\tilde{C}_{(n,q,m,\delta_1)}\) are not new, as the ternary simplex code should be equivalent to the simplex code over \(GF(3)\). In the case that \(m\) is odd, the contribution of this theorem is the proof of the fact that the ternary simplex code is actually equivalent to the ternary narrow-sense projective \(BCH\) code. It is known that the simplex code over \(GF(q)\) is permutation equivalent to a cyclic code if \(\gcd(m,q-1) = 1\). However, it is in general open if the simplex code over \(GF(q)\) is equivalent to a \(BCH\) code when \(\gcd(m,q-1) = 1\).

D. The ternary codes \(\tilde{C}_{(n,3,m,\delta_2)}\) and \(C_{(n,3,m,\delta_2)}\)

The determination of the weight distributions of the ternary codes \(\tilde{C}_{(n,3,m,\delta_2)}\) and \(C_{(n,3,m,\delta_2)}\) depends heavily on the theory of quadratic forms over finite fields. We first do some preparations below.

For reasons which will be explained later, let \(m \geq 3\) be an odd integer. For \(a,b \in GF(3^m)\), define the quadratic form
\[
Q(x) = \text{Tr}_3 3^m \left( ax^\frac{m-1}{2} + bx^\frac{m-3}{2} + 1 \right).
\]
Let \(r_{a,b}\) be the rank of the quadratic form above.

Lemma 16. Let \(m\) be odd, \(a,b \in GF(3^m)\) and \((a,b) \neq (0,0)\). The quadratic form
\[
Q(x) = \text{Tr}_3 3^m \left( ax^\frac{m-1}{2} + bx^\frac{m-3}{2} + 1 \right)
\]
has rank \(r_{a,b} \in \{m, m-1, m-2, m-3\}\).
Lemma 17. For the $S$ of the equation above equals the number of solutions of the following one:

Recall that the equation

has $3^r$ solutions $x \in \text{GF}(3^m)$ if and only if the rank of $Q(x)$ equals $m - r$. Note that the number of solutions of the equation above equals the number of solutions of the following one:

This has at most 27 solutions, thus $r \leq 3$ and $r_{a,b} \in \{m, m-1, m-2, m-3\}$. For $a, b \in \text{GF}(3^m)$, define

Denote by $r_{a,b}$ the rank of the quadratic form $Q(x) = \text{Tr}_3^m \left( ax^{3^r} + bx^{-1} \right)$ and denote by $\eta_0$ the quadratic character over GF(3). Then

We will need the following lemma concerning power moment identities.

Lemma 17. For the $S(a,b)$ defined above, we have the following:

- i) $\sum_{a,b \in \text{GF}(3^m)} S(a,b) = 2 \times 3^{2m}$.
- ii) $\sum_{a,b \in \text{GF}(3^m)} S(a,b)^2 = 4 \times 3^{3m}$.
- iii) $\sum_{a,b \in \text{GF}(3^m)} S(a,b)^3 = 32 \times 3^{3m} - 24 \times 3^{2m}$.
- iv) $\sum_{a,b \in \text{GF}(3^m)} T(a,b)^2 = 3^{2m}$.

Proof: i) The identity is trivially true.

ii) Define $N_2$ to be the number of pairs $(u,v) \in \text{GF}(3)^* \times \text{GF}(3)^*$ and $(x,y) \in \text{GF}(3^m) \times \text{GF}(3^m)$, which satisfy the following two equations:

It is easy to see that $\sum_{a,b \in \text{GF}(3^m)} S(a,b)^2 = 3^{2m} N_2$. Thus, it suffices to determine $N_2$.

When $x = y = 0$, we have four choices of the pair $(u,v)$. When $x \neq 0$ and $y \neq 0$, the system above is equivalent to

\[
\begin{cases}
(u)_{m-1}^{m-1} + v y_{m-1}^{m-1} = 0, \\
(u)_{m-1}^{m-1} + v y_{m-1}^{m-1} = 0.
\end{cases}
\]
Notice that \( \gcd(3^{m-1} + 1, 3^n - 1) = \gcd(3^{m-1} + 1, 3^m - 1) = 2 \). We see that \(-\frac{x}{y} \in \GF(3)\) must be a square. Namely, \(-\frac{x}{y} = 1\). Thus, we have two choices for the pair \((u, v)\). Meanwhile, \(\frac{x}{y} = \pm 1\) are precisely all solutions to the following system of equations:

\[
\begin{cases}
(x/y)^{3^{m-1} + 1} = 1, \\
(x/y)^{3^{m-3} + 1} = 1.
\end{cases}
\]

Thus, we have \(2(3^n - 1)\) choices for the pair \((x, y)\). To sum up, we have \(4(3^n - 1)\) choices for the pairs \((u, v)\) and \((x, y)\) when \(x \neq 0\) and \(y \neq 0\). In total, we have \(N_2 = 4 + 4(3^n - 1) = 4 \times 3^n\).

iii) Define \(N_3\) to be the number of triples \((u, v, w) \in \GF(3)^* \times \GF(3)^* \times \GF(3)^*\) and \((x, y, z) \in \GF(3^n) \times \GF(3^n) \times \GF(3^n)\), which satisfy the following two equations:

\[
\begin{cases}
u x^{3^{m-1} - 1} + v y^{3^{m-1} - 1} + w z^{3^{m-1} - 1} = 0, \\
u x^{3^{m-3} - 1} + v y^{3^{m-3} - 1} + w z^{3^{m-3} - 1} = 0.
\end{cases}
\]

It is easy to see that \(\sum_{a, b \in \GF(3^n)} S(a, b)^3 = 3^{2m}N_3\). Thus, it suffices to determine \(N_3\).

When \(x = y = z = 0\), we have eight choices of the triple \((u, v, w)\). When exactly one of \(x, y, z\) equals 0, we can use the result of ii). For instance, if \(x = 0\), then \(u \in \{1, 2\}\) and the system degenerates to

\[
\begin{cases}
v y^{3^{m-1} - 1} + w z^{3^{m-1} - 1} = 0, \\
v y^{3^{m-3} - 1} + w z^{3^{m-3} - 1} = 0.
\end{cases}
\]

By ii), we have \(4(3^n - 1)\) choices for the pairs \((v, w)\) and \((y, z)\). Thus, we have \(8(3^n - 1)\) choices for the triples \((u, v, w)\) and \((0, y, z)\). In total, when exactly one of \(x, y, z\) equals 0, we have \(24(3^n - 1)\) choices.

When \(x, y, z\) are all nonzero, we have

\[
\begin{align*}
u \left(\frac{x}{z}\right)^{3^{m-1} - 1} + v \left(\frac{y}{z}\right)^{3^{m-1} - 1} + w & = 0, \quad (8) \\
u \left(\frac{x}{z}\right)^{3^{m-3} - 1} + v \left(\frac{y}{z}\right)^{3^{m-3} - 1} + w & = 0. \quad (9)
\end{align*}
\]

It follows from (8) and (9) that

\[
\left(\frac{x}{y}\right)^{3^{m-3} - 1} + 1 = -\frac{v(y^2 - z^2)}{u(x^2 - z^2)}, \quad (10)
\]

Raising to the third power both sides of (9), we obtain

\[
\begin{align*}
u \left(\frac{x}{z}\right)^{3^{m-1} - 3} + v \left(\frac{y}{z}\right)^{3^{m-1} - 3} + w & = 0. \quad (11)
\end{align*}
\]

Combining (11) and (8) we get

\[
\left(\frac{x}{y}\right)^{3^{m-1} - 1} = -\frac{v(y^2 - z^2)}{u(x^2 - z^2)}. \quad (12)
\]

By (10) and (12), we have \(\left(\frac{x}{y}\right)^{3^{m-3} - 1} = \left(\frac{x}{y}\right)^{3^{m-1} - 1} = 1\), which is equivalent to \(\left(\frac{x}{y}\right)^8 = 1\). Since \(\gcd(8, 3^n - 1) = 2\), we have \(\left(\frac{x}{y}\right)^2 = 1\). By the symmetry of \(x, y, z\), we also conclude that \(\left(\frac{x}{z}\right)^2 = 1\) and \(\left(\frac{x}{y}\right)^2 = 1\). Hence, the original system degenerates to

\[
u + v + w = 0, \quad u, v, w \in \GF(3)^*.
\]

It is easy to verify that there are two choices of the triple \((u, v, w)\) and \(4(3^n - 1)\) choices of the triple \((x, y, z)\). In total, there are \(8(3^n - 1)\) choices when \(x, y, z\) are all nonzero. Hence, \(N_3 = 8 + 24(3^n - 1) + 8(3^n - 1) = 32 \times 3^n - 24\).

iv) The proof is very similar to that of ii), and thus omitted here.
For $j \in \{0, 2\}$, define

$$n_j = \left| \{ (a, b) \in GF(3^m) \times GF(3^m) : T(a, b) = \pm 3^{\frac{m+j}{2}} \sqrt{-1} \} \right|.$$ 

For $j \in \{1, 3\}$ and $\varepsilon = \pm 1$, define

$$n_{\varepsilon,j} = \left| \{ (a, b) \in GF(3^m) \times GF(3^m) : T(a, b) = \varepsilon 3^{\frac{m+j}{2}} \} \right|.$$ 

Under the assumption $n_{1,3} = 0$, which will be verified later (see the proof of Theorem [19] below), we obtain the value distribution of $T(a, b)$ and $S(a, b)$.

**Lemma 18.** Let $m \geq 3$ be an odd integer. Assume that $n_{1,3} = 0$.

(i). The value distribution of $T(a, b)$ is as follows:

| Rank $r_{a,b}$ | Value $T(a, b)$ | Multiplicity |
|-----------------|-----------------|--------------|
| $m$             | $3^{\frac{m}{2}} \sqrt{-1}$ | $(3^{m-1})(8 \times 3^{m-9} \times 3^{m-1} + 9)$/8 |
| $m$             | $-3^{\frac{m}{2}} \sqrt{-1}$ | $(3^{m-1})(8 \times 3^{m-9} \times 3^{m-1} + 9)$/8 |
| $m-1$           | $3^{\frac{m+1}{2}}$ | $(3^{m-1}+\frac{m+1}{2})(3^{m-1})$ |
| $m-1$           | $-3^{\frac{m+1}{2}}$ | $(3^{m-1}-\frac{m+1}{2})(3^{m-1})$ |
| $m-2$           | $3^{\frac{m}{2}+1} \sqrt{-1}$ | $(3^{m-1})(3^{m-1}+1)$/8 |
| $m-2$           | $-3^{\frac{m}{2}+1} \sqrt{-1}$ | $(3^{m-1})(3^{m-1}+1)$/8 |
| 0               | $3^m$           | 1 |

(ii). The value distribution of $S(a, b)$ is as follows:

| Rank $r_{a,b}$ | Value $S(a, b)$ | Multiplicity |
|-----------------|-----------------|--------------|
| $m, m-2$        | 0               | $(3^m - 3^{m-1} + 1)(3^m - 1)$ |
| $m-1$           | $2 \times 3^{\frac{m+1}{2}}$ | $(3^{m-1}+\frac{m+1}{2})(3^{m-1})$ |
| $m-1$           | $-2 \times 3^{\frac{m+1}{2}}$ | $(3^{m-1}-\frac{m+1}{2})(3^{m-1})$ |
| 0               | $2 \times 3^m$  | 1 |

**Proof:** From the moment identities in Lemma [17] we have

\[
\begin{align*}
n_0 + n_2 + n_{1,1} + n_{-1,1} + n_{1,3} + n_{-1,3} &= 3^{2m} - 1, \\
n_{1,1} - n_{-1,1} + 3(n_{1,3} - n_{-1,3}) &= 3^{\frac{m+1}{2}} (3^m - 1), \\
n_{1,1} + n_{-1,1} + 9(n_{1,3} + n_{-1,3}) &= 3^{m-1} (3^m - 1), \\
n_{1,1} - n_{-1,1} + 27(n_{1,3} - n_{-1,3}) &= 3^{\frac{m+1}{2}} (3^m - 1), \\
-n_0 + 3(n_{1,1} + n_{-1,1}) - 9n_2 + 27(n_{1,3} + n_{-1,3}) &= 0.
\end{align*}
\]

Combining $n_{1,3} = 0$, we can easily derive the value distribution of $T(a, b)$. The value distribution of $S(a, b)$ is a direct consequence since $S(a, b) = 0$ if $r_{a,b} \in \{m, m-2\}$ and $S(a, b) = 2T(a, b)$ if $r_{a,b} \in \{m-1, m-3\}$. 

\[\blacksquare\]
Theorem 19. Let $m \geq 3$ and $q = 3$. Then the ternary code $\tilde{C}_{(n,q,m,3^2)}$ has parameters
$$[q^m-1, q-1, k, d],$$
where
$$k = \begin{cases} 2m & \text{if } m \text{ is odd,} \\ \frac{3m}{2} & \text{if } m \text{ is even,} \end{cases}$$
and $d = 3^{m-1} - 3^{\frac{m+1}{2}}$. Moreover, the weight distribution is presented in Table III when $m$ is even and in Table IV when $m$ is odd.

Proof: The conclusion on the dimension of the code follows from Lemma 13. Note that
$$\tilde{C}_{(n,q,m,3^2)} = \{c_1(a,b) : a, b \in GF(3^m)\},$$
where
$$c_1(a,b) = \left( \text{Tr}_{3}^m \left( a\beta^{3^{m-1} \cdot 3^{\frac{m-1}{2}}j} + b\beta^{3^{m-1} \cdot 3^{\frac{m+1}{2}}j} \right) \right)^{n-1},$$
for any $a, b \in GF(3^m)$, $a \neq 0$. Then the weight distribution of $\tilde{C}_{(n,q,m,3^2)}$ is reduced to that of the code $C$ consisting of the codewords
$$c_2(a,b) = \left( \text{Tr}_{3}^m \left( a\alpha^{3^{\frac{m+1}{2}}j} + b\alpha^{3^{\frac{m-1}{2}}+1}j \right) \right)^{n-1}, a \in GF(3^m), b \in GF(3^m).$$
We remark that the weight distribution of $C$ has been derived in [20, Theorem 2]. Hence the weight distribution of $\tilde{C}_{(n,q,m,3^2)}$ is obtained and presented in Table III. It is also known that the minimum distance is $d = 3^{m-1} - 3^{\frac{m+1}{2}}$.

When $m$ is odd, we need some extra work. For $a, b \in GF(3^m)$, define
$$c_3(a,b) = \left( \text{Tr}_{3}^m \left( a\alpha^{3^{\frac{m-1}{2}}j} + b\alpha^{3^{\frac{m+1}{2}}+1}j \right) \right)^{n-1}.$$ 
It is equivalent to considering the code
$$C' = \{c_3(a,b) : a, b \in GF(3^m)\}.$$ 
A routine computation shows that
$$w(c_3(a,b)) = 3^{m-1} - \frac{1}{6}S(a,b).$$
Hence we obtain the weight distribution of $\tilde{C}_{(n,q,m,3^2)}$ (see Table IV) directly from the value distribution of $S(a,b)$ in Lemma 18 provided that $n_{1.3} = 0$.

We finally prove that $n_{1.3} = 0$. This is because $n_{1.3}$ is the frequency of codewords of $\tilde{C}_{(n,q,m,3^2)}$ which attain the weight $3^{m-1} - 3^{\frac{m+1}{2}}$. However, $\tilde{C}_{(n,q,m,3^2)}$ is a subcode of $C_{(n,q,m,3^2)}$, whose minimum distance satisfies $d \geq \delta_2 = 3^{m-1} - 1 - \frac{3^{\frac{m+1}{2}}-1}{2} > 3^{m-1} - 3^{\frac{m+1}{2}}$. Therefore $n_{1.3} = 0$. This concludes the proof of Theorem 19.

Example 3. Let $(q,m) = (3,4)$. Then the code $\tilde{C}_{(n,q,m,3^2)}$ of Theorem 19 has parameters $[40,6,24]$, and weight enumerator $1 + 300z^{24} + 240z^{27} + 168z^{30} + 20z^{36}$. This is the best cyclic code and optimal according to [12, p. 305].
TABLE III
THE WEIGHT DISTRIBUTION OF $\tilde{C}_{(n,q,m,\delta_2)}$ WHEN $m \geq 4$ IS EVEN

| Weight          | Frequency                                      |
|-----------------|------------------------------------------------|
| $0$             | $1$                                            |
| $3^{m-1} - 3^{\frac{m}{2}} - 1$ | $\frac{3(3^{\frac{m}{2}} - 1)(3^{\frac{m}{2}} + 1)^2}{8}$ |
| $3^{m-1}$       | $3^{\frac{m}{2}} - 1(3^m - 1)$                |
| $3^{m-1} + 3^{\frac{m}{2}} - 1$ | $\frac{3(3^{\frac{m}{2}} - 1)(3^{m-1} + 1)}{4}$ |

TABLE IV
THE WEIGHT DISTRIBUTION OF $\tilde{C}_{(n,q,m,\delta_2)}$ WHEN $m \geq 3$ IS ODD

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

Example 4. Let $(q,m) = (3,5)$. Then the code $\tilde{C}_{(n,q,m,\delta_2)}$ of Theorem 19 has parameters $[121,10,72]$, and weight enumerator $1 + 10890z^{72} + 39446z^{81} + 8712z^{90}$. This code has the same parameters as the best ternary linear code known in the Database.

Theorem 20. Let $m \geq 3$ and $q = 3$. Then the ternary code $C_{(n,q,m,\delta_2)}$ has parameters
$$\left[ \frac{q^m - 1}{q - 1}, k, \delta_2 \right],$$
where
$$k = \begin{cases} 
2m + 1 & \text{if } m \text{ is odd}, \\
\frac{3m + 2}{2} & \text{if } m \text{ is even}.
\end{cases}$$

In addition, the weight distribution is presented in Table V when $m$ is even and in Table VI when $m$ is odd.

proof: The conclusion on the dimension of the code follows from Lemma 13. Note that
$$C_{(n,q,m,\delta_2)} = \{ c_1(a,b,c) : a,b \in GF(3^m), c \in GF(3) \},$$
where
$$c_1(a,b,c) = \left( \text{Tr}_3^{3m} \left( a\beta^{3^{m-1}+3^j} + b\beta^{3^{m-1}+3^j} \right) + c \right)_{j=0}^{n-1}.$$ 

Here $\beta = \alpha^2$ and $\alpha$ is a generator of $GF(3^m)^*$. 

When $m$ is even, for $a,b\in GF(3^m)$, define
$$c_2(a,b,c) = \left( \text{Tr}_3^{3m} \left( a\alpha^{3^{\frac{m}{2}}+1}j + b\alpha^{3^{\frac{m}{2}}+1} \right) + c \right)_{j=0}^{n-1}.$$ 

Here $\beta = \alpha^2$ and $\alpha$ is a generator of $GF(3^m)^*$. 


The determination of the weight distribution of $C_{(n,q,m,δ_2)}$ is reduced to that of the code
\[ C = \left\{ c_2(a,b,c) : a \in \text{GF}(3^m), b \in \text{GF}(3^m), c \in \text{GF}(3) \right\}. \]

A routine computation shows that
\[
w(c_2(a,b,c)) = 3^{m-1} + \frac{1}{2}(δ_{0,c} - 1) - \frac{1}{6} \sum_{y \in \text{GF}(3)} \zeta_3^{cy} U(ya,yb)
\]
\[
= 3^{m-1} + \frac{1}{2}(δ_{0,c} - 1) - \frac{1}{6} \sum_{y \in \text{GF}(3)} \zeta_3^{cy} (-1)^{r'_{a,b}} U(a,b),
\]

where
\[
U(a,b) = \sum_{x \in \text{GF}(3^m)} \zeta_3^{Tr_3^m(ax^{3^m+1} + bx^{3^m-1} + 1)},
\]
\[
δ_{0,c} = \begin{cases} 
1 & \text{if } c = 0, \\
0 & \text{if } c \neq 0,
\end{cases}
\]

and $r'_{a,b}$ is the rank of the quadratic form $Tr_3^m(ax^{3^m+1} + bx^{3^m-1} + 1)$. Thanks to [20, Theorem 1], the value distribution of $U(a,b)$ is already known which is presented in the following table:

| Rank $r'_{a,b}$ | Value $U(a,b)$ | Multiplicity |
|------------------|----------------|--------------|
| $m$              | $3^\frac{m}{2}$ | $\frac{3(3^m-1)(3^m+1)^2}{8}$ |
| $m$              | $-3^\frac{m}{2}$ | $\frac{3(3^m-1)(3^m+1)}{4}$ |
| $m-1$            | $3^{\frac{m-1}{2}}i$ | $\frac{3^{m-1}(3^m-1)}{2}$ |
| $m-1$            | $-3^{\frac{m-1}{2}}i$ | $\frac{3^{m-1}(3^m-1)}{2}$ |
| $m-2$            | $-3^{\frac{m-1}{2}}$ | $\frac{(3^{m-1}-1)(3^m-1)}{8}$ |
| $0$              | $3^m$          | $1$          |

It is easy to see that the weight distribution of $C$ and $C_{(n,q,m,δ_2)}$ (see Table V) follows directly from the value distribution of $U(a,b)$ when $m$ is even. For example, according to the table above, when $r'_{a,b} = m$, $U(a,b)$ takes the value $3^\frac{m}{2}$ for $\frac{3(3^m-1)(3^m+1)^2}{8}$ times. Thus, if $c = 0$, $w(c_2(a,b,c))$ takes the value $3^{m-1} - 3^\frac{m}{2} - 1$ for $\frac{3(3^m-1)(3^m+1)^2}{8}$ times, and if $c = 1$ or $2$, $w(c_2(a,b,c))$ takes the value $3^{m-1} + \frac{1}{2}(3^\frac{m}{2} - 1)$ for $\frac{3(3^m-1)(3^m+1)^2}{4}$ times.

When $m$ is odd, for $a,b \in \text{GF}(3^m)$ and $c \in \text{GF}(3)$, define
\[
c_3(a,b,c) = \left( \text{Tr}_3^m(a\alpha^{(3^\frac{m-1}{2}+1)j} + b\alpha^{(3^\frac{m-1}{2} + 1)j}) + c \right)_{j=0}^{n-1}.
\]

It suffices to consider the code
\[ C' = \left\{ c_3(a,b,c) : a,b \in \text{GF}(3^m), c \in \text{GF}(3) \right\}. \]

A routine computation shows that
\[
w(c_3(a,b,c)) = 3^{m-1} + \frac{1}{2}(δ_{0,c} - 1) - \frac{1}{6} \sum_{y \in \text{GF}(3)} \zeta_3^{cy} (-1)^{r'_{a,b}} T(a,b),
\]
TABLE V
THE WEIGHT DISTRIBUTION OF $C_{(n,q,m,\delta_2)}$ WHEN $m \geq 4$ IS EVEN

| Weight | Frequency |
|--------|-----------|
| $0$    | $1$       |
| $3^n - 3^{n-1}$ | $(3^n - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2}$ | $(3^n - 3^{n-2} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 1$ | $(3^n - 3^{n-2} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3}$ | $(3^n - 3^{n-1} - 3^{n-2} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 1$ | $(3^n - 3^{n-1} - 3^{n-2} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4}$ | $(3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4} - 1$ | $(3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4} - 3^{n-5}$ | $(3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4} - 3^{n-5} - 1$ | $(3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4} - 1)/2$ |

TABLE VI
THE WEIGHT DISTRIBUTION OF $C_{(n,q,m,\delta_2)}$ WHEN $m \geq 3$ IS ODD

| Weight | Frequency |
|--------|-----------|
| $0$    | $1$       |
| $3^n - 3^{n-1} - 3^{n-2}$ | $(3^n - 3^{n-2} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3}$ | $(3^n - 3^{n-1} - 3^{n-2} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 1$ | $(3^n - 3^{n-1} - 3^{n-2} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4}$ | $(3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4} - 1$ | $(3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4} - 3^{n-5}$ | $(3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4} - 1)/2$ |
| $3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4} - 3^{n-5} - 1$ | $(3^n - 3^{n-1} - 3^{n-2} - 3^{n-3} - 3^{n-4} - 1)/2$ |

where $T(a,b)$ and $r_{a,b}$ are the same as the ones in Lemma 18. Employing the value distribution of $T(a,b)$ in Lemma 18, we obtain the weight distribution of $C_{(n,q,m,\delta_2)}$ (see Table VI) directly when $m$ is odd. This completes the proof of Theorem 20.

Example 5. Let $(q,m) = (3,4)$. Then the code $C_{(n,q,m,\delta_2)}$ of Theorem 20 has parameters $[40,7,22]$, and weight enumerator

$$1 + 280z^{22} + 300z^{24} + 336z^{25} + 240z^{27} + 600z^{28} + 168z^{30} + 240z^{31} + 20z^{36} + 2z^{40}.$$ 

According to [12], p. 305, this is the best ternary cyclic code, and has the same parameters as the best ternary linear code in the Database. Note that for any ternary linear code with parameters $[40,7,d]$, we have $d \leq 23$.

Example 6. Let $(q,m) = (3,5)$. Then the code $C_{(n,q,m,\delta_2)}$ of Theorem 20 has parameters $[121,11,67]$, and
weight enumerator
\[ 1 + 2420z^{67} + 10890z^{72} + 54450z^{76} + 39446z^{81} + 58806z^{85} + 8712z^{90} + 2420z^{94} + 2z^{121}. \]

The best ternary linear code known in the Database has parameters \([121,11,68]\), which is not cyclic.

V. SOME NARROW-SENSE PROJECTIVE BCH CODES WITH SPECIAL DESIGNED DISTANCES

In this section, we focus on narrow-sense projective BCH codes of length \(n = \frac{q^m-1}{q-1}\) with special designed distances. As stated in Section III some information about coset leaders modulo \(\frac{q^m-1}{q-1}\) can be obtained via the NDS decomposition. Note that for a narrow-sense BCH code, its Bose distance must be a coset leader. Therefore, we can obtain the Bose distance if the designed distance is of certain special form.

**Theorem 21.** Let \(2 \leq \delta \leq n\) be an integer. Suppose \(E(\delta) = V_1V_2 \ldots V_r\).

i) Suppose \(\delta\) has only 0 and 1 as components. If \(V_1 = V_2 = \cdots = V_r\) or \(V_1 > V_2 = \cdots = V_j < V_k\) for all \(j < k \leq r\), then \(C(n,q,m,\delta)\) has Bose distance \(d_B = \delta\).

ii) Suppose \(V_1\) has length \(1\) and has components either 0 or 1. Let \(V_1 > V_2\) and \(m = al + b\), where \(0 \leq b \leq l - 1\).

(a) If \(b = 0\), then \(C(n,q,m,\delta)\) has Bose distance

\[ d_B = E^{-1}(V_1V_1 \ldots V_1). \]

(b) If \(1 \leq b \leq l - 1\), then \(C(n,q,m,\delta)\) has Bose distance

\[ d_B \geq E^{-1}(V_1V_1 \ldots V_1 S(T_b(V_1))). \]

In particular, if the last component of \(S(T_b(V_1))\) is 1, then the equality holds.

**Proof:** These results are immediate consequences of Lemma 4 and Lemma 5. □

The theorem above is very powerful in determining the Bose distance of \(C(n,q,m,\delta)\) for some special \(\delta\). In the following, we give several examples.

**Example 7.** For \(q = 3\), \(m = 6\) and \(\delta = 110\), consider the code \(C(364,3,6,110)\). Note that

\[ \bar{\delta} = (0,1,1,0,0,2) = V_1V_2, \]

where \(V_1 = (0,1,1)\) and \(V_2 = (0,0,2)\). Since \(V_1 > V_2\), by ii) of Theorem 21 the Bose distance

\[ d_B = E^{-1}(V_1V_1) = E^{-1}(0,1,1,0,1,1) = 112. \]

Indeed, the smallest coset leader no less than \(\delta = 110\) is just 112, where \(C_{112} = \{112,280,336\}\).

**Example 8.** For \(q = 3\), \(m = 5\) and \(\delta = 29\), consider the code \(C(121,3,5,29)\). Note that

\[ \bar{\delta} = (0,1,0,0,2) = V_1V_2, \]

where \(V_1 = (0,1)\) and \(V_2 = (0,0,2)\). Since \(V_1 > V_2\), by ii) of Theorem 21 the Bose distance

\[ d_B = E^{-1}(V_1V_1 S(T_1(V_1))) = E^{-1}(0,1,0,1,1) = 31. \]

Indeed, the smallest coset leader no less than \(\delta = 29\) is just 31, where \(C_{31} = \{31,37,91,93,111\}\).

**Example 9.** For \(q = 7\), \(m = 5\) and \(\delta = 393\), consider the code \(C(2801,7,5,393)\). Note that

\[ \bar{\delta} = (0,1,1,0,1) = V_1V_2, \]
where $V_1 = (0, 1, 1)$ and $V_2 = (0, 1)$. Since $V_1 > V_2$, by ii) of Theorem 21 the Bose distance

$$d_B \geq E^{-1}(V_1S(T_2(V_1))) = E^{-1}(0, 1, 1, 0, 2) = 394.$$ 

Indeed, the smallest coset leader no less than $\delta = 393$ is just 394, where $C_{394} = \{394, 694, 2057, 2500, 2758\}$. Hence, we have the Bose distance $d_B = 394$.

Below, we consider two special classes of designed distances. First, we consider BCH codes with designed distances $q^i - 1$, where $1 \leq i \leq m - 1$.

**Theorem 22.** For $1 \leq i \leq m - 1$, $C_{(n,q,m,\frac{q^i - 1}{q - 1})}$ has Bose distance $d_B = \frac{q^i - 1}{q - 1}$. Furthermore, if $1 \leq i \leq \lceil \frac{m}{2} \rceil$, then the code $C_{(n,q,m,\frac{q^i - 1}{q - 1})}$ has parameters

$$\left[ \frac{q^m - 1}{q - 1}, \frac{q^m - 1}{q - 1} - m(q^i - 1), d \right],$$

where $d \geq \frac{q^i - 1}{q - 1}$. In particular, if $i \mid m$, then $d = \frac{q^i - 1}{q - 1}$.

**Proof:** Note that

$$\frac{q^i - 1}{q - 1} = \left( \underbrace{0, \ldots, 0}_{m-i}, 1, \ldots, 1 \right).$$

By i) of Theorem 21 $\frac{q^i - 1}{q - 1}$ is a coset leader. Then we have $d_B = \frac{q^i - 1}{q - 1}$. When $1 \leq i \leq \lceil \frac{m}{2} \rceil$, the conclusion on dimensions follows from Theorem 3. If $i \mid m$, by Lemma 9 we have $d = \frac{q^i - 1}{q - 1}$. □

Based on the theorem above and numerical experiments, we have the following conjecture.

**Conjecture 1.** The code $C_{(n,q,m,\frac{q^i - 1}{q - 1})}$ has minimum distance $d = (q^i - 1)/(q - 1)$, where $1 \leq i \leq m - 1$.

Note that Theorem 22 says the conjecture is true when $i \mid m$. Next, we consider BCH codes with designed distances $q^i + l$, where $1 \leq i \leq \lceil \frac{m}{2} \rceil - 1$ and $1 \leq l \leq q - 1$.

**Theorem 23.** For $1 \leq i \leq \lceil \frac{m}{2} \rceil - 1$ and $1 \leq l \leq q - 1$, $C_{(n,q,m,q^i + l)}$ has Bose distance $d_B = q^i + l$. Furthermore, the code $C_{(n,q,m,q^i + l)}$ has parameters

$$\left[ \frac{q^m - 1}{q - 1}, \frac{q^m - 1}{q - 1} - m \left( (q^i + l - 1) \left( \frac{1}{q} \right) \right), d \right],$$

where $d \geq q^i + l$. In particular, if $(q^i + l) \mid n$, then $d = q^i + l$.

**Proof:** The conclusion on the dimension follows from Theorem 3. For $1 \leq i \leq \lceil \frac{m}{2} \rceil - 1$ and $1 \leq l \leq q - 1$, let $\delta = q^i + l$. To prove that the Bose distance is equal to $\delta$, it suffices to show that $\delta$ is a coset leader. Note that

$$\overrightarrow{\delta} = (0, \ldots, 0, 1, 0, \ldots, 0, 1).$$

We are going to show that $\delta$ is a coset leader by analyzing $\overrightarrow{\delta}$. Direct computation shows that for $1 \leq i \leq m - 2$, $q^i \delta > \overrightarrow{\delta}$. Moreover,

$$\overrightarrow{q^{m-1} \delta} = \begin{cases} (1,0,\ldots,0,1,0,\ldots,0) & \text{if } l = 1, \\ (0,q-l,\ldots,q-l,q-l+1,q-l,\ldots,q-l,q-l+1) & \text{if } 2 \leq l \leq q-1, \end{cases}$$

\begin{align*}
&
\overrightarrow{m-i-1} \overrightarrow{i-1} \\
&
\overrightarrow{m-i-1} \overrightarrow{i-2}
\end{align*}
which implies that $q^{n-1}\delta \geq \delta$. Consequently, $\delta$ is a coset leader modulo $n$. In addition, if $(q^i+l) \mid n$, by Lemma 9 we have $d = q^i + l$.

**Example 10.** Let $(q,m) = (3,3)$. Then the code $C_{(n,q,m,q+1)}$ has parameters $[13,7,4]$. The optimal linear code in the Database has parameters $[13,7,5]$, which is not cyclic.

**Example 11.** Let $(q,m) = (3,4)$. Then the code $C_{(n,q,m,q+1)}$ has parameters $[40,32,4]$, and is the best ternary cyclic code according to [12] p. 306. The optimal linear code in the Database has parameters $[40,32,5]$, which is not cyclic.

**Example 12.** Let $(q,m) = (3,4)$. Then the code $C_{(n,q,m,q+2)}$ has parameters $[40,28,5]$. The best linear code in the Database has parameters $[40,28,6]$, which is not cyclic.

**Example 13.** Let $(q,m) = (3,5)$. Then the code $C_{(n,q,m,q+2)}$ has parameters $[121,106,6]$. The best linear code in the Database has the same parameters, and is not cyclic.

Based on Theorem 23 and the numerical experiments, we make the following conjecture on the minimum distance of $C_{(n,q,m,q+1)}$.

**Conjecture 2.** The code $C_{(n,q,m,q+1)}$ has minimum distance $d = q + 1$.

Note that Theorem 23 confirms the conjecture for the case that $m$ is even.

**VI. OPEN PROBLEMS AND CONCLUDING REMARKS**

Although BCH codes are introduced in almost every book on coding theory, a very small number of results about them are available in the literature (see [3], [4], [8], [9], [12] for information). In general, it is a hard problem to determine the dimension of a BCH code, and it is much harder to find its minimum distance.

The known results on BCH codes are almost entirely for the primitive length $n = q^m - 1$. To our knowledge, there are only a few papers on BCH codes with non-primitive lengths in the literature. This is because it is harder to deal with BCH codes with non-primitive lengths. This paper initializes the study of narrow-sense projective BCH codes with length $n = (q^m - 1)/(q - 1)$, and has the following contributions:

- The parameters of some narrow-sense projective BCH codes with large dimensions were determined in Section III.
- The parameters of some narrow-sense projective BCH ternary codes with small dimensions were settled in Section IV. Specifically, we determined the weight distributions of the ternary BCH codes $C_{(n,q,m,\delta_1)}, \tilde{C}_{(n,q,m,\delta_1)}, C_{(n,q,m,\delta_2)}$ and $\tilde{C}_{(n,q,m,\delta_2)}$ in Theorems 14, 15, 20 and 19 respectively. A class of optimal BCH ternary codes were identified.
- The parameters of some narrow-sense projective BCH codes with designed distances of special forms were settled in Section VI.

This paper only initialized the investigation of narrow-sense projective BCH codes over finite fields. There are many open problems on these codes. Below we mention a few open problems regarding these codes.

**Open Problem 1.** For $q = 3$, determine the parameters of $C_{(n,q,m,\delta_i)}$ and $\tilde{C}_{(n,q,m,\delta_i)}$ for $3 \leq i \leq |m/4|$.

For the case $q = 3$, we did find out $\delta_i$ for all $i$ with $3 \leq i \leq |m/4|$ in Section IV-B. The dimensions of $C_{(n,3,m,\delta_i)}$ and $\tilde{C}_{(n,3,m,\delta_i)}$ can thus be determined for $i$ with $3 \leq i \leq |m/4|$ recursively, given the dimensions of $C_{(n,3,m,\delta_2)}$ and $\tilde{C}_{(n,3,m,\delta_2)}$ computed earlier in this paper. Specifically, for $i \geq 1$ we have

$$\dim(C_{(n,3,m,\delta_i+1)}) = \dim(C_{(n,3,m,\delta_i)}) + |C_{\delta_i}|$$

and

$$\dim(\tilde{C}_{(n,3,m,\delta_i+1)}) = \dim(\tilde{C}_{(n,3,m,\delta_i)}) + |C_{\delta_i}|.$$

The remaining task is to compute the lengths of the cyclotomic cosets $C_{\delta_i}$. But it would be very hard to determine the minimum distances of the ternary BCH codes $C_{(n,3,m,\delta_i)}$ and $\tilde{C}_{(n,3,m,\delta_i)}$ for $i \geq 3$. 

The case that \( q \geq 4 \) is much more complicated. We have the following open problems for this case.

**Open Problem 2.** For \( q > 3 \), find out the largest coset leader \( \delta_1 \) and determine the parameters of \( C(n,q,m,\delta_1) \) and \( \tilde{C}(n,q,m,\delta_1) \).

We were able to find \( \delta_1 \) only for the case that \( m = \lambda(q-1) \) and \( q > 3 \). In this special case, we have

\[
\delta_1 = \frac{q^{\lambda-1} - 1}{q - 1} + \sum_{i=2}^{q-1} i q^{(i-1)\lambda-1}(q^{\lambda} - 1) / q - 1.
\]

(13)

Compared with the case \( q = 3 \), it is more difficult to prove that the value above is the largest coset leader. We were not able to determine the weight distribution of \( C(n,q,m,\delta_1) \) and \( \tilde{C}(n,q,m,\delta_1) \) for this special case that \( q \geq 4 \) and \( m = \lambda(q-1) \) due to the complicated expression of \( \delta_1 \) given in (13).

**Open Problem 3.** For \( q > 3 \), find out the second largest coset leader \( \delta_2 \) and determine the parameters of \( C(n,q,m,\delta_2) \) and \( \tilde{C}(n,q,m,\delta_2) \).

We were able to work out \( \delta_2 \) only for the case that \( m = \lambda(q-1) \) and \( q > 3 \). In this special case,

\[
\delta_2 = \frac{q^{\lambda-1} - 1}{q - 1} + \sum_{i=2}^{q-3} i q^{(i-1)\lambda-1}(q^{\lambda} - 1) / q - 1 + \sum_{i=2}^{q-3} i q^{(i-1)\lambda-1}(q^{\lambda} - 1) / q - 1 + q^{(q-2)\lambda}(q^{\lambda-1} - 1).
\]

(14)

Compared with the case \( q = 3 \), it is more difficult to prove that the value above is the second largest coset leader. We were not able to determine the weight distribution of \( C(n,q,m,\delta_2) \) and \( \tilde{C}(n,q,m,\delta_2) \) for this special case that \( q \geq 4 \) and \( m = \lambda(q-1) \), as the weight distributions of these codes may not be determined by exponential sums related to quadratic forms. Experimental data shows that \( C(n,q,m,\delta_2) \) has 25 nonzero weights when \((q,m) = (7,6)\).

The codes \( C(n,q,m,(q^i-1)/(q-1)) \) have also very good parameters according to experimental data. Hence, it is worthy to attack the following open problem.

**Open Problem 4.** Determine the dimension of \( C(n,q,m,(q^i-1)/(q-1)) \) for \( \left\lfloor \frac{m}{2} \right\rfloor < i \leq m-1 \).

It is possible to find the dimension of the code \( C(n,q,m,(q^m-1)/(q-1)) \). Experimental data shows that the dimension of this code is lower bounded by

\[
\left( \frac{p+m-2}{m-1} \right)^s + 1,
\]

where \( q = p^s \) and \( p \) is a prime. In general, the dimension of this code is much larger than the lower bound above.

In addition to the four open problems above, the reader is cordially invited to settle the two conjectures in Section V.

While primitive narrow-sense BCH codes contain many good linear codes \([12],[13]\), as shown by many examples in this paper, narrow-sense projective BCH codes also include many optimal linear codes. This fact provides us a strong motivation for studying narrow-sense projective BCH codes further.

Finally, we point out an application of some of the ternary codes of this paper in secret sharing. Any linear code over \( GF(q) \) can be employed to construct secret sharing schemes \([1],[7],[24],[26]\). In order to make such secret sharing scheme to have interesting access structures, we need a linear code \( C \) over \( GF(q) \) such that

\[
\frac{w_{\text{min}}}{w_{\text{max}}} > \frac{q-1}{q},
\]

(15)

where \( w_{\text{max}} \) and \( w_{\text{min}} \) denote the maximum and minimum nonzero weight in \( C \), respectively.

The ternary codes of Theorems 14 and 19 satisfy the inequality in (15) when \( m \geq 5 \), and the codes of Theorem 15 have only one nonzero weight and obviously satisfy the inequality in (15). Therefore, all the codes in Theorems 14 15 and 19 can be employed to obtain secret sharing schemes with interesting access structures using the framework documented in [1], [7], [24], [26].
REFERENCES

[1] R. Anderson, C. Ding, T. Helleseth and T. Klove, “How to build robust shared control systems,” Des. Codes Cryptogr., vol. 15, no. 2, pp 111–124, 1998.
[2] 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, 2007.
[3] D. Augot, P. Charpin and N. Sendrier, “Studying the locator polynomials of minimum weight codewords of BCH codes,” IEEE Trans. Inf. Theory, vol. 38, no. 3, pp. 960–973, 1992.
[4] D. Augot and N. Sendrier, “Idempotents and the BCH bound,” IEEE Trans. Inf. Theory, vol. 40, no. 1, pp. 204–207, 1994.
[5] E. R. Berlekamp, “The enumeration of information symbols in BCH codes,” Bell System Tech. J., vol. 46, no. 8, pp. 1861–1880, 1967.
[6] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert and A. Wassermann, Error-Correcting Linear Codes, Springer-Verlag, Berlin, 2006.
[7] C. Carlet, C. Ding and J. Yuan, “Linear codes from perfect nonlinear mappings and their secret sharing schemes,” IEEE Trans. Inf. Theory, vol. 51, no. 6, pp. 2089–2102, 2005.
[8] P. Charpin, “On a class of primitive BCH-codes,” IEEE Trans. Inf. Theory, vol. 36, no. 1, pp. 222–228, 1990.
[9] P. Charpin, “Open problems on cyclic codes,” In: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, vol. I, pp. 963–1063 (Chapter 11), Elsevier, Amsterdam, 1998.
[10] P. Delsarte, “On subfield subcodes of modified Reed-Solomon codes,” IEEE Trans. Inf. Theory, vol. 21, no. 5, pp. 575–576, 1975.
[11] Y. Dianwu and H. Zhengming, “On the dimension and minimum distance of BCH codes over GF(q), J. Electron., vol. 13, no. 3, pp. 216–221, Jul. 1996.
[12] C. Ding, Codes from Difference Sets, World Scientific, Singapore, 2015.
[13] 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, 2015.
[14] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
[15] 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, 1972.
[16] 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.
[17] T. Kasami and N. Tokura, “Some remarks on BCH bounds and minimum weights of binary primitive BCH codes”, IEEE Trans. Inf. Theory, vol. 15, pp. 408–413, 1969.
[18] R. Lidl and H. Niederreiter, Finite fields, Cambridge University Press, Cambridge, 1997.
[19] 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, 2008.
[20] J. Luo, Y. Tang and H. Wang, “Cyclic codes and sequences: the generalized Kasami case,” IEEE Trans. Inf. Theory, vol. 56, no. 5, pp. 2130–2142, 2010.
[21] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[22] D. M. Mandelbaum, “Two applications of cyclotomic cosets to certain BCH codes,” IEEE Trans. Inf. Theory, vol. 26, no. 6, pp. 737–738, 1980.
[23] H. B. Mann, “On the number of information symbols in Bose-Chaudhuri codes,” Information and Control, vol. 5, no. 2, pp. 153–162, 1962.
[24] J. L. Massey, “Minimal codewords and secret sharing,” in: Proc. 6th Joint Swedish-Russian Workshop on Information Theory, pp. 276–279, 1993.
[25] W. W. Peterson, “Some new results on finite fields with applications to BCH codes,” in: R. C. Bose and T. A. Dowling, Eds., Combinatorial Mathematics and Its Applications, Univ. North Carolina Press, Chapel Hill, NC, 1969.
[26] J. Yuan and C. Ding, “Secret sharing schemes from three classes of linear codes,” IEEE Trans. Inf. Theory, vol. 52, no. 1, pp. 206–212, 2006.
[27] 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.
[28] D. Yue and H. Zhu, “On the minimum distance of composite-length BCH codes,” IEEE Communications Letters, vol. 3, no. 9, pp. 269–271, 1999.