Two Classes of Narrow-Sense BCH Codes and Their Duals

Xiaoqiang Wang, Jiaojiao Wang, Chengju Li, and Yansheng Wu

Abstract—BCH codes and their dual codes are two special subclasses of cyclic codes and are the best linear codes in many cases. A lot of progress on the study of BCH cyclic codes has been made, but little is known about the minimum distances of duals of BCH codes. Recently, a concept called dually-BCH code was introduced to investigate the duals of BCH codes and the lower bounds on their minimum distances in Gong et al., (2022). For a prime power \( q \) and an integer \( m \geq 4 \), let \( n = \frac{q^m-1}{q-1} \) (\( mn \) even), or \( n = \frac{q^m-1}{q^2-1} \) (\( q \) > 2). In this paper, some sufficient and necessary conditions in terms of the designed distance will be given to ensure that the narrow-sense BCH codes of length \( n \) are dually-BCH codes, which extended the results in Gong et al., and necessary conditions in terms of the designed distance will be given to ensure that the narrow-sense BCH codes of length \( n \) are dually-BCH codes, which extended the results in Gong et al., (2022). Lower bounds on the minimum distances of their dual codes are developed for \( n = \frac{q^m-1}{q-1} \) (\( mn \) even). As byproducts, we present the largest cost vector \( \delta_1 \) modulo \( n \) being of two types, which proves a conjecture in Wu et al., (2019) and partially solves an open problem in Li et al., (2017). We also investigate the parameters of narrow-sense BCH codes of length \( n \) with design distance \( \delta_1 \). The BCH codes presented in this paper have good parameters in general.

Index Terms—BCH code, cyclic code, dually-BCH code, dual code.

I. INTRODUCTION

Let \( GF(q) \) be the finite field with \( q \) elements, where \( q \) is a prime power. Let \( n, k \) be two positive integers such that \( k \leq n \). An \( [n, k, d]_q \) linear code \( C \) over the finite field \( GF(q) \) is a \( k \)-dimensional linear subspace of \( GF(q)^n \) with minimum (Hamming) distance \( d \). The dual code of \( C \), denoted by \( C^\perp \), is defined by

\[
C^\perp = \{ \mathbf{b} \in GF(q)^n : \mathbf{b} \mathbf{c}^T = 0 \text{ for all } \mathbf{c} \in C \},
\]

where \( \mathbf{b} \mathbf{c}^T \) is the standard inner product of two vectors \( \mathbf{b} \) and \( \mathbf{c} \). If the code \( C \) is closed under the cyclic shift, i.e., if \( (c_0, c_1, c_2, \ldots, c_{n-1}) \in C \) implies \( (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C \), then \( C \) is called a cyclic code. By identifying any vector \( (c_0, c_1, \ldots, c_{n-1}) \in GF(q)^n \) corresponds to a polynomial \( c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in GF(q)[x]/(x^n - 1) \), it is clear that any cyclic code \( C \) of length \( n \) over \( GF(q) \) corresponds to a subset of the quotient ring \( GF(q)[x]/(x^n - 1) \). Since every ideal of \( GF(q)[x]/(x^n - 1) \) must be principal, \( C \) can be expressed as \( C = \langle g(x) \rangle \), where \( g(x) \) is a monic polynomial with the smallest degree and is called the generator polynomial. Let \( h(x) = (x^n - 1)/g(x) \), then \( h(x) \) is referred to as the check polynomial of \( C \). The zeros of \( g(x) \) and \( h(x) \) are called zeros and non-zeros of \( C \).

An \([n, k, d]_q \) linear code over \( GF(q) \) is said to be distance-optimal (respectively, dimension-optimal and length-optimal) if there does not exist \([n, k', d'] \geq d + 1 \) (respectively, \([n, k'= k+1, d] \) and \([n' \leq n - 1, k, d] \) linear code over \( GF(q) \). A code is called an optimal code if it is length-optimal, or dimension-optimal, or distance-optimal, or meets a bound for linear codes.

Let \( n \) be a positive integer with \( \gcd(n, q) = 1 \). Let \( \ell = \ord_q(n) \) be the order of \( q \) modulo \( n \), and let \( \alpha \) be a generator of the group \( GF(q^\ell)^* \). Put \( \gamma = \alpha^{(q^\ell-1)/n} \), then \( \gamma \) is a primitive \( n \)-th root of unity in the finite field \( GF(q^\ell) \). For any \( i \) with \( 0 \leq i < q^\ell - 2 \), let \( m_i(x) \) denote the minimal polynomial of \( \gamma^i \) over \( GF(q) \). For any \( \delta \) with \( 2 \leq \delta \leq n \), let

\[
g(\delta, b) = \text{lcm}(m_0(x), m_{b+1}(x), \ldots, m_{b+\delta-2}(x)),
\]

where \( b \) is an integer and \( \text{lcm} \) denotes the least common multiple of these minimal polynomials. Let \( C(\delta, b) \) denote the cyclic code of length \( n \) with generator polynomial \( g(\delta, b) \), then \( C(\delta, b) \) is called a BCH code with designed distance \( \delta \). If \( n = q^\ell - 1 \) and \( n = q^\ell + 1 \), then \( C(\delta, b) \) is called a primitive \( BCH \) code and antiprimitive \( BCH \) code, respectively. If \( b = 1 \), then \( C(\delta, 1) \) is called a narrow-sense \( BCH \) code. In this case, for convenience we will use \( C(\delta) \) in the sequel.

BCH codes were invented in 1959 by Hocquenghem [12], and independently in 1960 by Bose and Ray-Chaudhuri [3]. They were extended to BCH codes over finite fields by Gorenstein and Zierler in 1961 [10]. In the past several decades, BCH codes have been widely studied and are treated in almost every book on coding theory since they are a special class of codes.
of cyclic codes with interesting properties and applications and are usually among the best cyclic codes. BCH codes with dual-containing properties under certain inner product can be used to construct quantum codes, the reader is referred to [18] and [23] and references therein.

It is very hard to determine the minimum distance of BCH codes in general. So far, we have very limited knowledge about the minimum distance of BCH codes. Among all types of BCH codes, narrow-sense primitive BCH codes are the most extensively studied. The reader is referred to, for example, [1], [2], [4], [7], [8], [15], [16], [21], and [22] for information. Antiprimitive BCH codes are another family of interesting codes. In [13], [16], and [20], the authors determined a necessary and sufficient condition for \( a \) being a coset leader modulo \( q^m + 1 \) in some ranges. Liu et al. in [17] considered the first five largest coset leaders modulo \( q^m + 1 \) for \( q = 2 \) and \( m \) being some special positive integers, and Yan et al. in [20] studied the first three largest coset leaders modulo \( q^m + 1 \) for \( q \) being an odd prime power and \( m \) being odd. Based on these results, they obtained the parameters of antiprimitive BCH codes for the design distance in some ranges. For further information on BCH codes of the other lengths, the reader is referred to [6] for a summary of various results of BCH codes before 2016.

A BCH code is called \( \text{dually-BCH code} \) if both the BCH code and its dual are BCH codes with respect to an \( n \)-th primitive root of unity \( \gamma \). This concept was introduced in [9] to investigate the duals of BCH codes and the lower bounds on their minimum distances. Up to now, all the results about the dually-BCH codes are focused on the narrow-sense BCH codes, and we list these results in Table I. Below we always assume that \( m \geq 4 \) is an integer and \( q \) is a prime power, \( m \) is even if \( n = q^m - 1 \) and \( q > 2 \) if \( n = q^m - 1 \) and \( q > 2 \) unless otherwise stated. In [19], let \( m \geq 6 \) be even, the authors described the largest coset leader \( \delta_1 \) modulo \( n = q^m - 1 \) for \( q = 2, 3 \) and studied the parameters of the narrow-sense BCH codes with design distance \( \delta_1 \). In addition, the authors gave a conjecture on the largest coset leader modulo \( n = q^m - 1 \) for \( q > 3 \). In [14], the authors showed the largest coset leader \( \delta_1 \) modulo \( n = q^m - 1 \) for \( q = 3 \), while the case \( q \geq 4 \) is still open. In [9], the authors obtained a sufficient and necessary condition for the code \( C_d \) being a dually-BCH code in the ternary case when the length of \( C_d \) is \( n = q^m - 1 \) and showed the case \( q \geq 4 \) as an open problem. The main objective of this paper is to solve some open problems in [9], [14], and [19], and give several sufficient and necessary conditions in terms of the designed distance to ensure that the BCH codes with length \( n \) are dually-BCH codes, and develop lower bounds on the minimum distances of the dual codes for some BCH codes.

Specifically, this paper gives the sufficient and necessary condition for the code \( C_d \) being a dually-BCH code when \( n = q^m - 1 \), which solved the case \( q \geq 4 \) in [9]. As byproducts, we present the largest coset leader \( \delta_1 \) modulo \( n \), which proves a conjecture in [19] and partially solves an open problem in [14]. We also investigate the parameters of the narrow-sense BCH codes of length \( n \) with designed distance \( \delta_1 \), where \( n = q^m - 1 \). To investigate the optimality of the codes studied in this paper, we compare them with the tables of the best known linear codes maintained in [11], and the best known cyclic codes maintained in [5], and some of the proposed codes are optimal or almost optimal.

The rest of this paper is organized as follows. Section II contains some preliminaries. Sections III and IV give the sufficient and necessary conditions in terms of the designed distance to ensure that the BCH codes with length \( n \) are dually-BCH codes and develop lower bounds on the minimum distances of the dual codes for \( n = q^m - 1 \). Section V concludes the paper.

II. PRELIMINARIES

In this section, we introduce some basic concepts and known results on BCH codes, which will be used later. Starting from now on, we adopt the following notation unless otherwise stated:

- \( \text{GF}(q) \) is the finite field with \( q \) elements.
- \( \alpha \) is a primitive element of \( \text{GF}(q^m) \) and \( \beta = \alpha^{q^m - 1} \) is a primitive \( n \)-th root of unity, where \( n \mid q^m - 1 \).
- \( m_1(x) \) denotes the minimal polynomial of \( \beta^i \) over \( \text{GF}(q) \).
- \( g_S = \text{lcm}(m_1(x), m_2(x), \ldots, m_{S-1}(x)) \) denotes the least common multiple of these minimal polynomials.
- \( C_d \) denotes the BCH code with generator polynomial \( g_S \) and length \( n \).
- \( T = \{0 \leq i \leq n - 1 : g(\beta^i) = 0\} \) is the defining set of \( C_d \) with respect to \( \beta \).
- \( T^1 = \{n - i : i \in T\} \).
- \( T^\perp \) is the defining set of the dual code \( C_d^\perp \) with respect to \( \beta \).
- \( \lfloor x \rfloor \) denotes the smallest integer larger than or equal to \( x \).
- \( \overline{x} \) denotes the largest integer less than or equal to \( x \).
- \( \overline{t_i} \) denotes \( x \) (mod \( t \)) and \( 0 \leq \overline{t_i} \leq t - 1 \), where \( t \) is a positive integer.
- \( [u, v] \) means all integers \( i \) with \( u \leq i \leq v \).

For two positive integers \( 0 < a, b < q^m - 1 \), let \( a = \sum_{i=0}^{m-1} a_i q^i \) and \( b = \sum_{i=0}^{m-1} b_i q^i \) be the \( q \)-adic expansions of \( a \) and \( b \), respectively. Write \( \overline{a} = (a_{m-1}, a_{m-2}, \ldots, a_0) \) and \( \overline{b} = (b_{m-1}, b_{m-2}, \ldots, b_0) \). Define \( \overline{a} > \overline{b} \) if \( a_{m-1} > b_{m-1} \) or there exists an integer \( 0 \leq i < m - 2 \) such that \( a_i > b_i \) and \( a_j = b_j \) for \( j \in [i + 1, m - 1] \). Then we have the following result.

**Lemma 1:** Let \( a, b \) be given as above. Then \( a > b \) if and only if \( \overline{a} > \overline{b} \).

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

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

where \( \ell_s \) is the smallest positive integer such that \( s \equiv sq^{\ell_s} \) (mod \( n \)), and is the size of the \( q \)-cyclotomic coset. The smallest integer in \( C_s \) is called the coset leader of \( C_s \). The following lemmas on coset leaders will play an important role in proving the conjecture documented in [19].

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
Lemma 2 [8]: The first three largest $q$-cycloctic coset leaders modulo $n = q^m - 1$ are given as follows:
\[ \delta_1 = (q - 1)q^{m-1} - 1, \quad \delta_2 = (q - 1)q^{m-1} - q^{\frac{m-1}{2}} - 1, \]
\[ \delta_3 = (q - 1)q^{m-1} - q^{\frac{m-1}{2}} + 1. \]

Lemma 3 [18]: Let $h$ be a positive integer and let $q$ be a prime power such that $(q + 1) \mid h$. Let $n = \frac{q^m - 1}{q+1}$, then $h$ is a coset leader modulo $q^m - 1$ if and only if $h \equiv 1 \pmod{q+1}$ is a coset leader modulo $n$.

The following lemma is given in [9], which is useful to give a characterization of $C_\delta$ being a dually-BCH code for $q \geq 3$ and $n = \frac{q^m - 1}{q+1}$.

Lemma 4 [9]: For $2 \leq \delta < n$, let $I(\delta)$ be the integer such that \( \{0, 1, 2, \ldots, |I(\delta)| - 1\} \subseteq T^\bot \setminus \{0\}$ and $I(\delta) \not\subseteq T^\bot$. Then we have $I(\delta) = \frac{q^m - 1}{q+1} - \delta < \frac{q^m - 1}{q+1} - 1$ (1) and $I(\delta) = 1$ if $\frac{q^m - 1}{q+1} < \delta < n$.

### III. BCH Code of Length $n = \frac{q^m - 1}{q+1}$ and Its Dual

Throughout this section, we always assume that $n = \frac{q^m - 1}{q+1}$, where $m \geq 4$ is even. Recall that $C_\delta$ is a BCH code with designed distance $\delta$ and length $n$, i.e., the defining set with respect to $\beta$ is $T = C_1 \cup C_2 \cup \ldots \cup C_{\delta-1}$, where $2 \leq \delta \leq n$ and $\beta = \alpha^{q+1}$. It then follows that $T^\bot = \{ n - i : i \in T \}$.

It is clear that $0 \in T^\bot$ and $n - 1 \not\in T^\bot$. Thus $T^\bot$ must be of the form

\[ T^\bot = C_0 \cup C_1 \cup \ldots \cup C_{j-1} \]

for some $j \geq 1$ if $C_{\delta}^\bot$ is a BCH code with respect to $\beta$. Otherwise, $T^\bot$ cannot be written as a union of cycloctic cosets of consecutive integers. This is the key idea to derive a sufficient and necessary condition for $C_\delta$ being a dually-BCH code. The lower bounds on the minimum distance of $C_{\delta}^\bot$ will be presented. To this end, we begin to determine the largest coset leader $\delta_1$ modulo $n$ and its cardinality.

Lemma 5: Let $\delta_1$ be the largest coset leader modulo $n$, then
\[ \delta_1 = \begin{cases} (q-1)q^{m-1} - q^{\frac{m-1}{2}} - 1 & \text{if } m \equiv 2 \pmod{4}, \\ (q-1)q^{m-1} - \frac{m-1}{2} & \text{if } m \equiv 0 \pmod{4}. \end{cases} \]

Proof: We prove the desired conclusion only for the case $m \equiv 0 \pmod{4}$, and omit the proof for the case $m \equiv 2 \pmod{4}$, which is similar.

It is easy to check that (1) is impossible since $\delta \equiv 0 \pmod{4}$.

We now assert that $\frac{q^m - 1}{q+1} - q^{\frac{m-1}{2}} - 1$ is the largest coset leader modulo $n$.

We now assert that $\frac{q^m - 1}{q+1} - q^{\frac{m-1}{2}} - 1$ is the largest coset leader modulo $n$. If there exists a coset leader $\delta'$ modulo $n$ such that $\frac{q^m - 1}{q+1} < \delta' < \frac{q^m - 1}{q+1}$, then for any positive integer $\ell$ with $1 \leq \ell \leq m - 1$, we have
\[ \ell \delta' \pmod{q^m - 1} \geq (q + 1)\delta'. \]

Hence, $(q + 1)\delta'$ is a coset leader modulo $q^m - 1$. From Lemma 2, we know that
\[ (q+1)\delta' = (q+1)q^{m-1} - 1 \]
\[ (q+1)\delta' = (q+1)q^{m-1} - q^{\frac{m-1}{2}} - 1. \]

It is easy to check that (1) is impossible since $\delta'$ is an integer. The desired conclusion then follows.

A conjecture on the largest coset leader modulo $n$ was given in [19] for $q > 3$. In Lemma 5, we answered this problem. We are now ready to determine $|C_{\delta_1}|$ that is useful to determine the dimension of the BCH code $C_{\delta_1}$.

Lemma 6: Let $\delta_1$ be given as in Lemma 5, then $|C_{\delta_1}| = m$ if $m \equiv 0 \pmod{4}$ and $|C_{\delta_1}| = \frac{m}{2}$ if $m \equiv 2 \pmod{4}$.

Proof: We prove the desired conclusion only for the case $m \equiv 0 \pmod{4}$, and omit the proof for the case $m \equiv 2 \pmod{4}$, which is similar.

Let $|C_{\delta_1}| = \ell$, then
\[ \frac{q^m - 1}{q+1} - (q-1)q^{m-1} - q^{\frac{m-1}{2}} - 1 \]
\[ \frac{q^m - 1}{q+1} - (q-1)q^{m-1} - q^{\frac{m-1}{2}} - 1 \]

which is equivalent to
\[ q^m - 1 - (q-1)q^{m-1} - q^{\frac{m-1}{2}} - 1 \]

Hence, (1) is impossible since $\delta'$ is an integer. The desired conclusion then follows.
It then follows from Lemma 2 that $\ell = m$.

The following theorem gives the information on the parameters of the BCH code $C_{\ell}$.

**Theorem 7:** When $m = 2 \pmod{4}$, then the BCH code $C_{\ell}$ has parameters

$$\left[\frac{q^m - 1}{q+1}, m+1, d \geq \frac{(q-1)q^{m-1} - q^{m-2} - 1}{q+1}\right].$$

When $m = 0 \pmod{4}$, then the BCH code $C_{\ell}$ has parameters

$$\left[\frac{q^m - 1}{q+1}, m+1, d \geq \frac{(q-1)q^{m-1} - q^{m-2} - 1}{q+1}\right].$$

**Proof:** It is straightforward from Lemmas 5 and 6.

We inform the reader that Theorem 7 generalizes the results in [19, Theorems 14 and 17], where only the binary and ternary cases were involved. In this sense, the results discussed in [19] can be seen as a special case of Theorem 7. The following example shows that the lower bounds given in Theorem 7 are very good.

**Example 8:** We have the following examples for the code of Theorem 7.

1. Let $q = 2$, $m = 6$ and $\delta = 9$, then the code $C_9$ has parameters $[21, 4, 9]$.
2. Let $q = 3$, $m = 4$ and $\delta = 11$, then the code $C_{11}$ has parameters $[20, 5, 11]$.
3. Let $q = 4$, $m = 4$ and $\delta = 35$, then the code $C_{35}$ has parameters $[51, 5, 35]$.
4. Let $q = 5$, $m = 4$ and $\delta = 79$, then the code $C_{79}$ has parameters $[104, 5, 79]$.

All the four codes are almost optimal according to the tables of best codes known in [11] under the equality holds. These results are verified by Magma programs.

To present a sufficient and necessary condition for $C_\ell$ being a dually-BCH code, the following several lemmas will be needed later.

**Lemma 9:** Let $t \geq 2$ be even, $m \geq 4$ even and $l$ odd. Then

$$\frac{q^m - q^{m-1} - q^{m-2} - 1}{q+1}$$

is a coset leader modulo $n$.

**Proof:** We only prove the desired conclusion for the case that $\frac{q^m - q^{m-1} - q^{m-2} - 1}{q+1}$ is a coset leader modulo $n$, and omit the proofs of other cases, which are similar.

It is easy to check that $(q + 1) \mid (q^m - q^{m-1} - q^{m-2} - 1)$, and

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

By Lemma 1, we see that $q^m - q^{m-1} - q^{m-2} - 1$ is not the second largest coset leader modulo $n$. The desired conclusion then follows from Lemma 9.

**Lemma 10:** Let $\delta_1$ be given as in Lemma 5. Then we have

1. $\delta_1 \in T^\perp$ is a coset leader modulo $n$ if $m \equiv 0 \pmod{4}$, $m \geq 8$ and $2 \leq \delta \leq \frac{q^m + 1}{q+1}$.
2. $\delta_1 \in T^\perp$ is a coset leader modulo $n$ if $m \equiv 2 \pmod{4}$, $m \geq 6$ and $2 \leq \delta \leq \frac{q^m + 1}{q+1}$.

**Proof:** For the first case, recall from Lemma 9 that $\frac{q^m + 1}{q+1}$ is a coset leader modulo $n$. This means that $\frac{q^{m+1}+1}{q+1} \notin T^\perp$ if $2 \leq \delta \leq \frac{q^{m+1}+1}{q+1}$. Hence, $\delta_1 = n - \frac{q^m + 1}{q+1} \notin T^{-1}$, i.e., $\delta_1 \in \mathbb{Z}_nT^{-1} = T^\perp$. It is similar to give the proof for the second case, and we omit the details.

**Lemma 11:** Let $q$ be an odd prime power. Then $\frac{q-1}{q^4 - q^2 - q - 2}$ is the second largest coset leader modulo $\frac{q^4 - 1}{q+1}$.

**Proof:** It is easy to see that

$$\frac{(q-1)q^3 - q^2 - q - 2}{q+1} = (q - 2, q - 2, q - 2, q - 2, q - 2)_{q^4 - 1},$$

so $(q-1)q^3 - q^2 - q - 2$ is a coset leader modulo $q^4 - 1$. From Lemma 3, we know that $\frac{(q-1)q^3 - q^2 - q - 2}{q+1}$ is a coset leader modulo $\frac{q^4 - 1}{q+1}$.

We now assert that $(q-1)q^3 - q^2 - q - 2$ is the second largest coset leader modulo $\frac{q^4 - 1}{q+1}$ if there exists a coset leader $\delta'$ modulo $n$ such that $\frac{(q-1)q^3 - q^2 - q - 2}{q+1} < \delta' < \frac{(q-1)q^3 - 1}{q+1}$, then for any positive integer $\ell$ with $1 \leq \ell \leq m - 1$, we have

$$((q + 1)\delta' \ell \pmod{q^m - 1}) \geq (q + 1)\delta'.$$

Hence, $(q + 1)\delta'$ is a coset leader modulo $q^m - 1$.

From Lemma 1, we know that the sequences of first five largest coset leaders modulo $q^m - 1$ are $(q - 2, q - 1, q - 1, q - 1, q - 1, q - 2, q - 2, q - 2, q - 2)$, $(q - 2, q - 1, q - 2, q - 1, q - 1, q - 2, q - 2, q - 2, q - 2)$, respectively. Then the first five largest coset leaders modulo $q^m - 1$ are $(q - 2, q - 1, q - 2, q - 1, q - 1, q - 2, q - 2, q - 2, q - 2)$, $(q - 2, q - 1, q - 2, q - 1, q - 1, q - 2, q - 2, q - 2, q - 2)$, $(q - 2, q - 1, q - 2, q - 1, q - 1, q - 2, q - 2, q - 2, q - 2)$, $(q - 2, q - 1, q - 2, q - 1, q - 1, q - 2, q - 2, q - 2, q - 2)$.

Since $(q - 2)q^2 - q^2 - q - 2 < \delta' < (q - 1)q^3 - 1$, if $(q - 1)q^3 - q^2 - q - 2$ is not the second largest coset leader, we have

$$(q + 1)\delta' = (q - 1)q^3 - q - 1, (q + 1)\delta' = (q - 1)q^3 - q^2 - 1, (q + 1)\delta' = (q - 1)q^3 - q^2 - 1.$$

It is easy to check that (2) is impossible since $\delta'$ is an integer. The desired conclusion then follows.

**Lemma 12:** Let $q > 2$ be a prime power and $m \geq 4$ be even. Let $\delta_1$ be given as in Lemma 5. Then the following hold.

1. $\frac{(q-1)q^3 - q^2 - q - 2}{q+1}$ is a coset leader modulo $n$ if $m = 4$ and $2 \leq \delta \leq q^2 + 1$.
2. $\frac{(q-1)q^3 - 1}{q+1} \in T^\perp$ is a coset leader modulo $n$ if $2 \leq \delta \leq \frac{(q-1)q^3 - 1}{q+1}$.
3. $\frac{2}{q+1}$ is a coset leader modulo $n$ if $\frac{(q-2)(q^m - 1)}{q+1} < \delta \leq \delta_1$.

**Proof:** From Lemma 3 and Lemma 11, it is easy to get that $\frac{(q-1)q^3 - q^2 - q - 2}{q+1}$, $\frac{(q-1)q^3 - 1}{q+1}$ and $2$ are coset leaders modulo $n$.

When $m = 4$ and $2 \leq \delta \leq q^2 + 1$, it follows from Lemma 9 that $\frac{q^4 + q^2 + 1}{q+1} = q^2 + 1$ is a coset leader modulo $\frac{q^4 - 1}{q+1}$. This
means that $q^2 + 1 \not\equiv T$ in this case. Hence,
\[
(q-1)q^3 - q^2 - q - 2 = n - (q^2 + 1) \not\equiv T^{-1} \quad \text{and}
\]
\[
(q-1)^2 - q^2 - q - 2 = n - (q^2 + 1) \not\equiv T^{-1} \quad \text{and}
\]
\[
\sum_{i=0}^{m-1} q^i = n - \frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1} \not\equiv T^{-1} \quad \text{and}
\]
\[
\sum_{i=0}^{m-1} q^i \in Z_n \setminus T^{-1} = T^\perp.
\]

When $2 \leq \delta \leq \frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1}$, we see from Lemma 9 that
\[
(q-2)(\sum_{i=0}^{m-1} q^i) \not\equiv T.\]

Hence,
\[
\sum_{i=0}^{m-1} q^i = n - \frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1} \not\equiv T^{-1} \quad \text{and}
\]
\[
\sum_{i=0}^{m-1} q^i \in Z_n \setminus T^{-1} = T^\perp.
\]

When $\frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1} < \delta \leq 1$, it is easy to see that
\[
(q-2)q^{m-1} - 2q^{m-2} - 1 < \frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1}.
\]

Then
\[
\frac{(q-2)q^{m-1} - 2q^{m-2} - 1}{q+1} = \frac{q^m - 1}{q+1} - 2q^{m-2} \in T.
\]

Note that $n - 2q^{m-2}$ and $n - 2$ are in the same $q$-cyclic coset modulo $n$. Then we have $n - 2 \in T$, i.e., $2 \in T^{-1}$. Hence, $2 \not\equiv T^{-1} = Z_n \setminus T^\perp$.

Lemma 13: Let $q = 2$ and $m \geq 8$ be even. When $7 < \delta \leq \frac{2^{m-2}-1}{3}$, there is a coset leader belonging to $T^\perp$. Moreover, the coset leader is larger than $\frac{2^{m-5}+1}{3}$.

Proof: Let $M = 2^6 + 2^5 + 2^4 + 2^2 + 2 = (0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$ if $m = 10$, and
\[
M = 2^{m-2} + \sum_{i=0}^{m-13} (2^{m-4-4i} + 2^{m-5-4i} + 2^{m-6-4i})
\]
\[
+ \sum_{i=0}^{m-13} (2^{m-12-3i} + 2^{m-13-3i})
\]
\[
= (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)
\]
if $m \equiv 1$ (mod 3) and $m \neq 10$, and
\[
M = \begin{cases} 
\sum_{i=0}^{m-2} 2^{2i} = (0, 1, 0, 1, 1, 0, 1, 1, 1) & \text{if } m \equiv 0 \text{ (mod 3),} \\
\sum_{i=1}^{m-2} 2^{2i} + 2 = (0, 1, 0, 1, 1, 0, 1, 1, 1) & \text{if } m \equiv 2 \text{ (mod 3).}
\end{cases}
\]

It is easy to see that $M$ is a coset leader modulo $2^{m-1}$. By the definition of $M$, we know that $3 \mid M$. Then from Lemma 3, $M$ is a coset leader modulo $n$.

Since $\frac{2^3}{q+1} > \frac{2^{m-5}+1}{3}$, we have $M \not\equiv T$. If $m = 10$, then
\[
\frac{2^6 + 2^4 + 1}{3} = n - M \not\equiv T^{-1} \quad \text{and}
\]
\[
\frac{2^6 + 2^4 + 1}{3} \in Z_n \setminus T^{-1} = T^\perp.
\]

Since $\frac{2^6 + 2^2 + 1}{3}$ and $\frac{2^6 + 2^4 + 1}{3}$ are in the same coset modulo $n$. If $m \equiv 1$ (mod 3) and $m \neq 10$, then
\[
\frac{2^6 + 2^4 + 1}{3} = n - M \not\equiv T^{-1} \quad \text{and}
\]
\[
\frac{2^6 + 2^2 + 1}{3} \in Z_n \setminus T^{-1} = T^\perp.
\]

Since $(2^m-3 + 2^m-5 + 2^m-9 + \sum_{i=0}^{m-13} 2^{3i})/3$ and $(2^m+4 + \sum_{i=0}^{m-13} 2^{3i+5} + 2^2 + 1)/3$ are in the same coset modulo $n$. Similarly, we have
\[
\begin{cases} 
\frac{\sum_{i=0}^{m-2} 2^{2i}}{3} \in Z_n \setminus T^{-1} = T^\perp & \text{if } m \equiv 0 \text{ (mod 3),} \\
\frac{\sum_{i=0}^{m-2} 2^{2i}}{3} \in Z_n \setminus T^{-1} = T^\perp & \text{if } m \equiv 2 \text{ (mod 3).}
\end{cases}
\]

Let
\[
L = \begin{cases} 
2^6 + 2^2 + 1 & \text{if } m = 10, \\
\frac{\sum_{i=0}^{m-2} 2^{2i}}{3} & \text{if } m \equiv 0 \text{ (mod 3),} \\
\frac{\sum_{i=0}^{m-2} 2^{2i}}{3} & \text{if } m \equiv 2 \text{ (mod 3).}
\end{cases}
\]

It is easy to check that $L$ is a coset leader modulo $2^m - 1$. From Lemma 3, $L$ is a coset leader modulo $n$. It is obvious that $\frac{L}{q+1} > \frac{2^{m-5}+1}{3}$. The desired conclusion then follows.

Lemma 14: Let $q$ be a prime power and $2 \leq t \leq m - 2$ be even. For $2 \leq \delta < n$, let $I(\delta) \geq 1$ be the integer such that
\[
\{0, 1, 2, \ldots, I(\delta) - 1\} \subseteq T^\perp \quad \text{and} \quad I(\delta) \notin T^\perp.
\]
Then we have
\[
I(\delta) = q^{m-1} \cdot q^{m-t} - 1 \quad \text{if } \frac{q^m - q^{m-t}}{q+1} \in C_{q+1} \subseteq T.
\]

Therefore,
\[
\frac{q^{m-t} - 1}{q+1} \equiv q^m - q^{m-t} + (q+1)u \text{ (mod } q^m - 1 \text{)}
\]
and the sequence of $(q+1) \cdot q^t u + q^t - 1$ is
\[
\frac{(i_{m-1}, i_{m-2}, \ldots, i_t, q - 1, \ldots, q - 1)}{q+1}.
\]

where $i_t = i_{t+1} = 1$ if $u = 1$ and there are at least two $t+1 \leq j \leq m - 1$ such that $i_j \neq 0$ if $u > 1$. It follows that the coset leader of the cyclic coset of $(q+1) \cdot q^t u + q^t - 1$ modulo $q^m - 1$ is larger than or equal to $q^{t+1} + 2q^t - 1$. Then we obtain
\[
CL \left( \frac{(q+1) \cdot q^t u + q^t - 1}{q+1} \right) > \frac{q^{t+1} + 2q^t - 1}{q+1} > \delta - 1,
\]
where \( \text{CL} \left( \frac{(q+1)q'u+q'-1}{q+1} \right) \) denotes the coset leader of the \( q \)-cyclotomic coset modulo \( n \) containing \( \frac{(q+1)q'u+q'-1}{q+1} \). Consequently, \( \frac{(q+1)q'u+q'-1}{q+1} \notin T \) and \( \frac{m-1}{q+1} - u \notin T^t \). This leads to \( i = \frac{m-1}{q+1} - u \in T^t \). It then follows that \( \delta = \frac{q^{m-1}}{q+1} \) for any \( \delta \leq \frac{q^{m-1}}{q+1} < \delta \leq \frac{q^{m-1}+2q'-1}{q+1} \). The proof is then completed.

**Lemma 15:** Let \( q \) be a prime power and \( 2 \leq \delta \leq q-1 \). Let \( d^\perp(\delta) \) be the minimum distance of \( C_\delta^+ \). Then \( d^\perp(\delta) \geq \frac{2^{m-t} - 1}{3} + 1 \).

**Proof:** From the BCH bound, in order to obtain the desired result, we only need to show that \( \{0, 1, 2, \ldots, q^{m-1}+2q'-2-1\} \subseteq T^t \).

It is clear that \( 0 \in T^t \). For every integer \( i \) with \( 1 \leq i \leq q^{m-1}+2q'-2-1 \), we have \( i = \frac{q^{m-1}+2q'-2-1}{q+1} - u \), where \( 1 \leq u \leq q^{m-1}+2q'-2-1 \). Since \( (q+1) | \frac{q^{m-1}+2q'-2-1}{q+1} \) and \( (q+1) \mid \frac{q^{m-1}}{q+1} \), if there exist \( 0 < t < q-1 \) and \( 0 \leq i \leq m-1 \) such that \( q^{m-1}+2q'-2-1 - u(q+1) \equiv tq^i \pmod{q^{m-1}} \), then \( (q+1) | tq^i \), which is impossible.

\[
\text{CL} \left( \frac{q^{m-1}+2q'-2-1}{q+1} \right) > q-1 > \delta,
\]

where \( \text{CL} \left( \frac{q^{m-1}+2q'-2-1}{q+1} \right) \) denotes the coset leader of the \( q \)-cyclotomic coset modulo \( n \) containing \( \frac{q^{m-1}+2q'-2-1}{q+1} - u(q+1) \). Consequently, \( \frac{q^{m-1}+2q'-2-1}{q+1} - u \notin T^t \) and \( \frac{q^{m-1}+2q'-2-1}{q+1} - u \notin T^t \). This leads to \( i = \frac{m-1}{q+1} - u \in T^t \). The desired conclusion then follows from the BCH bound.

Let \( 2 \leq \delta' \leq \delta^t \leq n \), it is clear that \( \mathcal{C}_{\delta'} \subseteq \mathcal{C}_\delta \). Then we have \( \mathcal{C}_{\delta'} \supseteq \mathcal{C}_\delta \), which implies that \( d(\mathcal{C}_{\delta'}) \leq d(\mathcal{C}_\delta) \). From Lemma 14, Lemma 15 and the BCH bound for cyclic codes, it is easy to get the minimum distance of the lower bound of \( \mathcal{C}_\delta^+ \).

**Theorem 16:** Let \( 2 \leq \delta \leq n \), \( 0 \leq t \leq m-2 \) and \( d^\perp(\delta) \) be the minimum distance of \( C_\delta^+ \), where \( m \) and \( t \) are even. Let \( q = 2 \), then we have

\[
d^\perp(\delta) \geq \frac{2^{m-t} - 1}{3} + 1
\]

if \( \frac{2^{t-1}}{3} \leq \delta \leq \frac{3^{t+3}}{3} \). Let \( q > 2 \) be a prime power, then we have

\[
d^\perp(\delta) \geq \begin{cases} 
\frac{q^{m-1}+2q'-2-1}{q+1} + 1 & \text{if } 2 \leq \delta \leq q-1, \\
\frac{q^{m-1}}{q+1} + 1 & \text{if } \frac{q^{m-1}}{q+1} < \delta \leq \frac{q^{m-1}+2q'-1}{q+1}, \\
\frac{q^{m-2}-1}{q+1} + 1 & \text{if } \frac{q^{m-2}-1}{q+1} < \delta \leq \frac{q^{m-2}+1}{q+1}, \\
2 & \text{if } \frac{q^{m-3}+2q'-2-1}{q+1} < \delta \leq \frac{q^{m-1}}{q+1}.
\end{cases}
\]

It is very hard to determine the minimum distance of \( C_\delta^+ \) in general. The following examples show that the lower bounds in Theorem 16 are good in some cases.

**Example 17:** Let \( \delta = 2, q = 3 \) and \( m = 4 \). In Theorem 16, the lower bound on the minimum distance of \( C_2^+ \) is 12. By Magma, the true minimum distance of \( C_2^+ \) is 12.

**Example 18:** Let \( \delta = 2, q = 2 \) and \( m = 6 \). In Theorem 16, the lower bound on the minimum distance of \( C_2^+ \) is 6. By Magma, the true minimum distance of \( C_2^+ \) is 8.

We now give a sufficient and necessary condition for \( C_\delta \) being a dually-BCH code. The cases \( q = 2 \) and \( q \neq 2 \) will be treated separately.

**Theorem 19:** Let \( n = \frac{q^{m-1}}{q+1} \), where \( q = 2 \) and \( m \geq 4 \) is even. Then \( C_\delta \) is a dually-BCH code if and only if there exist \( \frac{d}{2} \leq \delta \leq n \), where \( \delta \) is given in Lemma 5.

**Proof:** We only prove the desired conclusion for the case \( m \equiv 0 \pmod{4} \), and omit the proof of the case \( m \equiv 2 \pmod{4} \), which is similar.

By definition, we have \( 0 \notin T \) and \( 1 \in T \), then \( 0 \notin T^{-1} \) and \( n - 1 \notin T^{-1} \). Furthermore, we have \( 0 \in T^{-1} \), which means that \( C_0 \) must be the initial cyclotomic coset of \( T^{-1} \). In other words, there must be an integer \( J \geq 1 \) such that \( T^{-1} = C_0 \cup C_1 \cup \cdots \cup C_{J-1} \) if \( C_\delta \) is a BCH code.

When \( \delta + 1 \leq \delta \leq n \), it is easily seen that \( T^{-1} = \{0\} \) and \( C_\delta^+ \) is a BCH code with respect to \( \beta \) since \( \delta + 1 \) is the largest coset leader modulo \( n \).

It remains to prove the desired conclusion for \( 2 \leq \delta \leq \delta + 1 \). If \( m = 4 \), there is nothing to prove since \( \delta + 1 = 1 \). When \( m > 4 \), we have the following four cases.

**Case 1:** \( 2 \leq \delta \leq 3 \). From Lemma 10 and \( 0 \in T^{-1} \), we know that \( T^{-1} = C_0 \cup C_1 \cup \cdots \cup C_{J-1} \). From \( C_\delta \) is a BCH code, which leads to \( C_\delta = \{0\} \). It is obvious that \( C_\delta \neq \{0\} \), which is a contradiction.

**Case 2:** \( 2 \leq \delta \leq 7 \). It is clear that there exists \( 2 \leq t \leq m - 4 \) such that \( \frac{2^{t-1}}{3} \leq \delta \leq \frac{2^{t-1}+2}{3} \) if \( 3 < \delta \leq 7 \). It is easily seen that

\[
2^{m-2} + 2^{m-4} + \sum_{i=0}^{m-6} 2^i = (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)_{2^{m-5}} \in Z_n \setminus T^{-1} = T^t.
\]

It is easy to check that

\[
I_{\max} := \max \left\{ I(\delta) : 3 < \delta \leq \frac{2^{m-2} - 1}{3} \right\} = I(1) \geq \frac{2^{m-2} - 1}{3} = \frac{2^{m-2} + 2^{m-4} + \sum_{i=0}^{m-6} 2^i}{3}.
\]

It then follows that there is no integer \( J \geq 1 \) such that \( T^{-1} = C_0 \cup C_1 \cup \cdots \cup C_{J-1} \), i.e., \( C_\delta^+ \) is not a BCH code with respect to \( \beta \).
Case 3: $7 < \delta \leq \frac{2^{m-2} - 1}{3}$. It is clear that $5 = \frac{2^4 + 2^2 + 2 + 1}{3} \in T$, then

\[2^4 \left( \sum_{i=0}^{m-5} 2^i \right) \frac{3}{3} = n - 5 \in T^{-1} \text{ and } \sum_{i=0}^{m-5} 2^i \in Z_n \setminus T^{-1} \not\in T^\perp.
\]

From Lemma 13, there is no integer $J \geq 1$ such that $T^\perp = C_0 \cup C_1 \cup \cdots \cup C_{J-1}$, i.e., $C^\perp_5$ is not a BCH code with respect to $\beta$.

Case 4: $\frac{2^{m-2} - 1}{q+1} < \delta \leq \delta_1$. Since $1 \notin T^\perp$, we have $C_5^\perp = \{0\}$ if $C_5^\perp$ is a BCH code with respect to $\beta$. However, the dimension of $C_5$ is $\dim(C_5) \leq n - |C^\perp_5| < n$, which is contradictory to $\dim(C_5^\perp) + \dim(C^\perp_5) = n$.

Combining all the cases above, the desired conclusion then follows.

**Theorem 20:** Let $n = \frac{q^{m-1}}{q+1}$, where $q > 2$ is a prime power and $m \geq 4$ is even. Let $\delta_1$ be given in Lemma 5. Then the following statements hold.

1. If $m = 4$, then $C_5$ is a dually-BCH code if and only if $\delta = 2$, $\delta_1 \leq \delta \leq n$.
2. If $m \neq 4$, then $C_5$ is a dually-BCH code if and only if $\delta_1 + 1 \leq \delta \leq n$.

**Proof:** We only prove the conclusion of this lemma for the case that $m \equiv 0 \pmod{4}$, and omit the proof of the conclusion for $m \equiv 2 \pmod{4}$, which is similar.

With an analysis similar as Theorem 19, when $\delta_1 + 1 \leq \delta \leq n$, we know that $T^\perp = \{0\}$ and $C^\perp_5$ is a BCH code with respect to $\beta$. It remains to show that whether $C^\perp_5$ is a BCH code with respect to $\beta$ for $2 \leq \delta \leq \delta_1$. We have the following four cases.

Case 1: $\delta = 2$. The defining set of $C_3$ with respect to $\beta$ is $T = C_1$. Since $q^{m-2} \in T$, we have

\[n - q^{m-2} = q^m - q^{m-1} - q^{m-2} - 1 = T^{-1}.
\]

Let $\delta' = \frac{q^m - q^{m-1} - q^{m-2} - 1}{q+1}$. From Lemma 9, we know that $\delta'$ is a coset leader modulo $n$. Hence, we obtain $T = C^\perp_5$.

If $m = 4$, then $\delta' = \delta_1$, i.e., $T^{-1} = C^\perp_5$. Hence, $T^\perp = Z_n \setminus \{0\} \cup C_1 \cup C_2 \cup \cdots \cup C_{5-1}$. This means that $C^\perp_5 = C^\perp_{\delta_1+1,0}$ is a BCH code with the designed distance $\delta_1+1$ with respect to $\beta$.

If $m \neq 4$, then $\delta' < \delta_1$. Since $\delta'$ and $\delta_1$ are not in the same coset, then $\delta_1 \notin T^\perp$, i.e., $\delta_1 \in Z_n \setminus T^{-1} = T^\perp$. It then follows $T^\perp = C_0 \cup C_1 \cup C_2 \cup \cdots \cup C_{\delta_1-1}$. If $C^\perp_5$ is a BCH code. This means that $C_5^\perp = \{0\}$ and leads to a contradiction.

Case 2: $3 \leq \delta \leq q + 1$. If $m = 4$, from Lemma 12 and 0 $\in T^\perp$, we know that

\[T^\perp = C_0 \cup C_1 \cup \cdots \cup C_3 \cup C_1^{q-1}\frac{q^4 - 1}{q + 1} - a_1 q + a_0.
\]

if $C^\perp_5$ is a BCH code. From Lemma 11, we know that the dimension of $C^\perp_5$ is

\[\dim(C^\perp_5) \geq \frac{q^4 - 1}{q + 1} - |C_1| - |C_2| = \frac{q^4 - 1}{q + 1} - 5.
\]

since $|C_2| = 4$. It is easy to check that $|C_1| = |C_2| = 4$, then dim($C^\perp_5$) $\geq |C_2| + |C_3| \geq 8$. From (3), we know that dim($C^\perp_5$) $\geq \frac{q^4 - 1}{q + 1} - 5$ and this leads to a contradiction. Hence, $C^\perp_5$ is not a BCH code.

If $m \neq 4$, from Lemma 10 and 0 $\in T^\perp$, we know that $T^\perp = C_0 \cup C_1 \cup \cdots \cup C_{\delta_1-1}$ is a BCH code, which leads to $C_5^\perp = \{0\}$, which is a contradiction.

Case 3: $q + 1 < \delta \leq \frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1}$. Since $q - 1 < \delta$, we have $q - 1 \in T$. Then

\[q^m - q^{m-2} = q^m - q^{m-2} = q^m - q^{m-2} = q^m - (q^{m-2} + 1) \in T.
\]

Hence,

\[\frac{q^m - q^{m-2}}{q+1} = \frac{q^m - q^{m-2}}{q+1} = \frac{q^m - q^{m-2}}{q+1} \in T^{-1} \text{ and } \frac{q^m - q^{m-2}}{q+1} \not\in T^\perp = Z_n \setminus T^{-1}.
\]

From Lemma 12, we know that $\frac{q^m - q^{m-2}}{q+1} \not\in T^{-1}$ is the coset leader modulo $n$. It is clear that $\frac{q^m - q^{m-2}}{q+1} \not\in T^{-1}$ is a BCH code with respect to $\beta$.

Case 4: $\frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1} < \delta \leq \delta_1$. It is clear that $\delta_1 \notin T$, which implies that $n - \delta_1 \notin T^{-1}$, i.e., $n - \delta_1 \in Z_n \setminus T^{-1} = T^\perp$. Obviously, we have

\[n - \delta_1 = \frac{q^{m-1} + q^m}{q+1} = \frac{q^{m-1} + q^m}{q+1} \in C_\frac{q^m - 1}{q+1}.
\]

since $\frac{q^m - 1}{q+1}$ is a coset leader modulo $n$ from Lemma 9. From Lemma 12, we know that $2 \notin C^\perp_5$. Then $T^\perp = C_0 \cup C_1$ if $C^\perp_5$ is a BCH code. If $m \neq 4$, it is obvious that $C_\frac{q^m - 1}{q+1} \not\in C_0 \cup C_1$.

Hence, $C^\perp_5$ is not a BCH code.

If $m = 4$, we obtain that $\delta = \delta_1$. It is clear that $T = C_1 \cup C_2 \cup \cdots \cup C_{\delta_1-1}$ and $T^\perp = C_0 \cup C_1$. This means that $C^\perp_5 = C_{2,0}$ is a BCH code with the designed distance 2 with respect to $\beta$.

Combining all the cases above, the desired conclusion then follows.

**IV. BCH CODE OF LENGTH $n = \frac{q^{m-1}}{q+1}$ AND ITS DUAL**

Throughout this section, we always assume that $n = \frac{q^{m-1}}{q+1}$, where $q \geq 3$ is a prime power and $m \geq 4$ is an integer. In accordance with the notation specified in Section II, the defining set of $C_5$ with respect to $\beta$ is $T = C_1 \cup C_2 \cup \cdots \cup C_{\delta-1}$. As before, denote by $T^\perp$ the defining set of the dual code $C^\perp_5$ with respect to $\beta$. Then $T^\perp = Z_n \setminus T^{-1}$.

It is clear that $0 \notin T^\perp$ and $n - 1 \notin T^\perp$. In this section, we also begin to present the largest coset leader $\delta_1$ modulo $n$, and then show a sufficient and necessary condition for $C^\perp_5$ being a dually-BCH code. As we will see, it is very difficult to determine $\delta_1$ in this case. To this end, we introduce Lemmas 21-26 and Proposition 27 in the following.

**Lemma 21:** Let $q \geq 3$ be a prime power and $m \geq 4$ be an integer. Let $q - 1 = mt_1 + t_2$ and $s = m \frac{t_1}{t_2}$, where $t_1 \geq 0$ and $m > t_2 \geq 0$. Assume that $T = \{[\gamma s - 1], \gamma = 1, 2, \ldots, t_2\}$ if $t_2 \neq 0$. Let

\[\sum_{i=1}^{q-1} q^{\frac{m_i - 1}{q+1}} = a_m - a_{m-1} q^{m-1} + a_{m-2} q^{m-2} + \cdots + a_1 q + a_0.
\]
It is clear that \( \sum_{i=0}^{m-2} a_i = q - 1 \). Moreover, if \( t_2 = 0 \), then \( a_i = \frac{q-1}{m} \) for all \( i \in [0, m-1] \). If \( t_2 \neq 0 \), then \( a_i = \frac{q-1}{m} \) if \( i \in \mathbb{Y} \), and \( a_i = \frac{q-1}{m} \) if \( i \in [0, m-1] \setminus \mathbb{Y} \).

**Proof:** We only prove the lemma for the case that \( q-1 \geq m \). The case \( q-1 < m \) can be shown similarly and we omit the details.

If \( t_2 = 0 \), it is clear that \( a_0 = a_1 = \cdots = a_{m-1} = \frac{q-1}{m} \). The desired conclusion then follows. If \( t_2 \neq 0 \), let \( it_2 = mu_i + v_i \), where \( i \in [0, m-1] \), \( 0 \leq u_i \leq t_2 - 1 \) and \( 0 \leq v_i < m \). To determine the value of \( a_i \) for \( i \in [0, m-1] \), we need to consider the possible values of \( \left\lfloor \frac{mt}{q-1} \right\rfloor \) for \( t \in [1, q-1] \). There are four cases.

**Case 1:** \( t \in [1, it_1 + u_i] \). It is clear that
\[
\left\lfloor \frac{mt}{q-1} \right\rfloor \leq \left\lfloor \frac{m(it_1 + u_i)}{q-1} \right\rfloor - 1.
\]

Since \( mt_1 = q - 1 - t_2 \) and \( mu_i = it_2 - v_i \), we obtain
\[
\left\lfloor \frac{mt}{q-1} \right\rfloor \leq \left\lfloor \frac{m(it_1 + u_i)}{q-1} \right\rfloor - 1 = i - 1.
\]

In this case, we have \( \left\lfloor \frac{mt}{q-1} \right\rfloor \leq i - 1 \).

**Case 2:** \( t \in [it_1 + u_i + 1, (i+1)t_1 + 1] \). It is clear that \( t \) can be expressed as \( t = it_1 + u_i + g \), where \( 1 \leq g < t_1 \). Since \( mt_1 = q - 1 - t_2 \) and \( mu_i = it_2 - v_i \), we have
\[
\left\lfloor \frac{mt}{q-1} \right\rfloor = \left\lfloor \frac{i + 1 - \frac{mu_i + mg - it_2}{q-1}}{q-1} \right\rfloor = i + 1 - \frac{mg - v_i}{q-1}.
\]

It is clear that \( 0 < mg - v_i < q-1 \), then \( \left\lfloor \frac{mt}{q-1} \right\rfloor = i \).

**Case 3:** \( t \in [it_1 + u_i + 1 + (i+1)t_1 + 1] \). From \( mt_1 = q - 1 - t_2 \) and \( mu_i = it_2 - v_i \), we have
\[
\left\lfloor \frac{mt}{q-1} \right\rfloor = i + 1 - \frac{tm_1 + m - v_i}{q-1}.
\]

Then \( \left\lfloor \frac{mt}{q-1} \right\rfloor \geq i + 1 \) if \( m - v_i > t_2 \).

**Case 4:** \( t \in [it_1 + u_i + t_1 + 2, q-1] \). Similar as above, it is easy to get that
\[
\left\lfloor \frac{mt}{q-1} \right\rfloor \geq i + 1.
\]

From above four cases, we know that
\[
\begin{cases}
\left\lfloor \frac{mt}{q-1} \right\rfloor \leq i - 1 & \text{if } t \in [1, it_1 + u_i] \\
\left\lfloor \frac{mt}{q-1} \right\rfloor = i & \text{if } t \in [it_1 + u_i + 1, (i+1)t_1 + u_i], \text{ or } t = it_1 + u_i + t_1 + 1 \text{ and } m - v_i \leq t_2, \\
\left\lfloor \frac{mt}{q-1} \right\rfloor = i + 1 & \text{if } t = it_1 + u_i + t_1 + 1 \text{ and } m - v_i > t_2, \\
\left\lfloor \frac{mt}{q-1} \right\rfloor \geq i + 1 & \text{if } t \in [it_1 + u_i + t_1 + 2, q-1].
\end{cases}
\]

When \( i \) runs over \([0, m-1]\), note that \( t_1 = \left\lfloor \frac{q-1}{m} \right\rfloor \) and \( t_1 + 1 = \left\lfloor \frac{q-1}{m} \right\rfloor \), it is easy to get that
\[
a_i = \begin{cases}
\left\lfloor \frac{q-1}{m} \right\rfloor & \text{if } 0 < m - v_i \leq t_2, \\
\left\lfloor \frac{q-1}{m} \right\rfloor & \text{if } t_2 < m - v_i
\end{cases}
\]

since the number of \( t \) in the range \([it_1 + u_i + 1, (i+1)t_1 + u_i]\) is \( \left\lfloor \frac{q-1}{m} \right\rfloor \). Then \( a_i = \left\lfloor \frac{q-1}{m} \right\rfloor \) if and only if \( 0 < m - v_i \leq t_2 \). Since \( v_i = it_2 - mu_i \), we have \( a_i = \left\lfloor \frac{q-1}{m} \right\rfloor \) if and only if
\[
(u_i + 1)s - 1 \leq i < (u_i + 1)s,
\]

which implies that \( i = \left\lfloor (u_i + 1)s \right\rfloor - 1 \). This means that \( a_i = \left\lfloor \frac{q-1}{m} \right\rfloor \) if and only if \( i \in \mathbb{Y} \). The desired conclusion then follows.

**Lemma 22:** Let \( t_2 \neq 0 \) and \( N(\gamma, \epsilon) = \left\lfloor \gamma s \right\rfloor - \left\lfloor (\gamma - \epsilon)s \right\rfloor \), where \( 1 \leq \epsilon < t_2 \), \( s = \frac{m-1}{t_2} \) and \( 1 \leq \gamma \leq t_2 \). Then the following statements hold.

1. If \( t_2 \mid m \), then \( N(i, \epsilon) = N(j, \epsilon) \) where \( 1 \leq i, j \leq t_2 \).
2. If \( t_2 \nmid m \), then \( N(i, \epsilon) - N(j, \epsilon) = 0 \) or \( 1 \). Moreover, there exists \( 1 \leq \epsilon_0 \leq t_2 \) such that \( N(i, \epsilon_0) = N(t_2, \epsilon_0) \).

**Proof:** If \( t_2 \mid m \), the desired conclusion follows from the definition of \( N(\gamma, \epsilon) \) directly. Next, we give the proof for the case \( t_2 \nmid m \). By the definition of \( N(\gamma, \epsilon) \), it is easy to get that
\[
\epsilon s - 1 = \gamma s - 1 < \gamma s - (\gamma - \epsilon)s - 1 = \epsilon s + 1.
\]

Similarly, we have
\[
\epsilon s - 1 < N(t_2, \epsilon) < \epsilon s.
\]

Then \( N(i, \epsilon) - N(t_2, \epsilon) = 0 \) or \( 1 \). When \( \epsilon = t_2 \) we have \( N(i, \epsilon) = N(t_2, \epsilon) = m \), then there must exist \( \epsilon_0 \in [1, t_2] \) such that \( N(i, \epsilon_0) = N(t_2, \epsilon_0) \). The proof is then completed.

**Lemma 23:** Let \( q \geq 3 \) be a prime power and \( m \geq 4 \) be an integer. Then \( \theta q^m - 1 - \left( \sum_{i=1}^{m} q^{\left\lfloor \frac{mt}{q-1} \right\rfloor - q+2} \right) q^{-1} \) is a coset leader modulo \( n \).

**Proof:** Note that
\[
\theta q^i \pmod{n} \geq \theta (q-1) q^i \pmod{q^m-1} \geq \theta (q-1)
\]
for any \( 1 \leq i \leq m-1 \). Below we will prove that
\[
\theta (q-1) q^i \pmod{q^m-1} \geq \theta (q-1)
\]
holds for any \( 1 \leq i \leq m-1 \). It is clear that
\[
\theta = q^m - 1 - \left( \sum_{i=1}^{m-2} q^{\left\lfloor \frac{mt}{q-1} \right\rfloor - q+2} \right) q^{-1} = \frac{q^m - \sum_{i=1}^{m-2} q^{\left\lfloor \frac{mt}{q-1} \right\rfloor - 1} - 1}{q-1}.
\]

Then by Lemma 21 we have
\[
\theta (q-1) = q^m - a_{m-1} q^{m-1} - a_{m-2} q^{m-2} - \cdots - a_1 q - a_0 - 1
\]
where $\theta'(q-1)q^{i} \pmod{q^m-1} = q^{m} - a_{m-i}q^{m-1} - \cdots - a_1q^i + a_0q^i - a_{m-1}q - a_{m-i} - 1$. \hfill (6)

For the sake of narrative, we denote $\theta' = (q-1)\theta$. If $m \not| (q-1)$, from Lemma 21 we know that $a_i = \frac{q-1}{m}$ for all $i \in [0, m-1]$, then $\theta'q^{i} \pmod{q^m-1} = \theta'$. From (4), (5) and (6), we see that $\theta$ is a coset leader modulo $n$. If $m \not| (q-1)$, we have the following three cases.

**Case 1:** $i \in [1, m-1] \setminus Y$. From Lemma 21, we know that $a_i = \frac{q-1}{m}$. Then $\theta'q^{m-i-1} \pmod{q^m-1} > \theta'$ since $a_{m-1} = \frac{q-1}{m} = \frac{q-1}{m} + 1$.

**Case 2:** $i \in Y$ and $t_2 \not|m$. Put $1 \leq h \leq m$. From Lemma 21, we know that

$$a_{h-1} = \begin{cases} \left\lfloor \frac{q-1}{m} \right\rfloor & \text{if } s \mid h, \\ \left\lceil \frac{q-1}{m} \right\rceil & \text{if } s \nmid h, \end{cases}$$

where $s$ is given in Lemma 21. Let $a = \left\lfloor \frac{q-1}{m} \right\rfloor$ and $b = \left\lceil \frac{q-1}{m} \right\rceil$, then the sequences of

$$(a_{m-1}, a_{m-2}, \ldots, a_1, a_0)_q \quad \text{and} \quad (a_{m-i-1}, a_{m-i-2}, \ldots, a_{m-1}, a_{m-i})_q$$

can be expressed as

$$\begin{align*}
(a, b, \ldots, b, a, b, \ldots, a, b, a, \ldots, b)_q \\
\left\lfloor \frac{|s|-1}{2} \right\rfloor & \left\lfloor \frac{|s|-1}{2} \right\rfloor & \left\lfloor \frac{|s|-1}{2} \right\rfloor
\end{align*}$$

From (5) and (6), we know that $\theta'q^{i} \pmod{q^m-1} = \theta'$ for any $i \in Y$.

**Case 3:** $i \in Y$ and $t_2 \not|m$. From Lemma 21, let $0 \leq h \leq m-1$, we know that $a_i = \left\lfloor \frac{q-1}{m} \right\rfloor$ if and only if $h = \left\lfloor (t_2-l)s - 1 \right\rfloor$ and $a_i = \left\lceil \frac{q-1}{m} \right\rceil$ for the other values of $h$, where $l \in [0, t_2-1)$. It is easy to check that

$$m-1 - \left\lfloor (t_2-l)s - 1 \right\rfloor = m - 1 - \left\lfloor m-1 - ls \right\rfloor = \left\lfloor |s| \right\rfloor.$$  

Recall that $a = \left\lfloor \frac{q-1}{m} \right\rfloor$ and $b = \left\lceil \frac{q-1}{m} \right\rceil$, then the sequence of

$$(a_{m-1}, a_{m-2}, \ldots, a_1, a_0)\_q$$

can be expressed as

$$\begin{align*}
(a, b, \ldots, b, a, b, \ldots, a, a, b, a, \ldots, b)_q \\
\left\lfloor \frac{|s|-1}{2} \right\rfloor & \left\lfloor \frac{|s|-1}{2} \right\rceil & \left\lfloor \frac{|s|-1}{2} \right\rceil
\end{align*}$$

Since $i \in Y$, we can assume that $m - 1 - i = [\gamma_1s - 1]$, where $\gamma_1 \in [1, t_2-1]$. Moreover, we have

$$[\gamma_1s - 1] - ([\gamma_1 + 1]s - 1) \leq \left\lfloor |s| \right\rfloor.$$  

Then the sequence of

$$(a_{m-i-1}, a_{m-i-2}, \ldots, a_1, a_0, a_{m-1}, a_{m-2}, \ldots, a_{m-i})_q$$

can be expressed as

$$\begin{align*}
(a, b, \ldots, b, a, b, \ldots, b, a, b, \ldots, b)_q & \\
\left\lfloor \frac{|s|-1}{2} \right\rfloor & \left\lfloor \frac{|s|-1}{2} \right\rceil & \left\lfloor \frac{|s|-1}{2} \right\rceil
\end{align*}$$

Hence, from (5) and (6), we obtain $\theta'q^{i} \pmod{q^m-1} \geq \theta'$. From Cases 1, 2 and 3, we have $\theta'q^{i} \pmod{q^m-1} \geq \theta'$ for any $i \in [0, m-1]$. Then $\theta$ is a coset leader modulo $n$ from (4). This completes the proof. \hfill \blacksquare

Let

$$M = q^m - \sum_{i=1}^{q-1} q^\left\lfloor \frac{m+1}{q} \right\rceil - 1 + \mu(q-1)$$

and $0 < \mu < \sum_{i=1}^{q-1} \left\lfloor \frac{m+1}{q} \right\rceil - 1$. By the definition of $\mu$, we know that $\mu$ can be expressed as

$$\mu = b_{m-2}q^{m-2} + b_{m-3}q^{m-3} + \cdots + b_1q + b_0,$$

where $b_0, \ldots, b_{m-2} \in [0, q-1]$. Then

$$(q-1)\mu = (b_{m-2}q^{m-1} + (b_{m-3} - b_{m-2})q^{m-2} + \cdots + (b_1 - b_2)q^2 + (b_0 - b_1)q - b_0).$$

By Lemma 21, we have

$$M = q^m - (a_{m-1} - b_{m-2})q^{m-1} - (a_{m-2} + b_{m-2} - b_{m-3})q^{m-2} - \cdots - (a_1 + b_1 - b_0)q - a_0 - b_0 - 1.$$  

We next prove that $M$ is not a coset leader modulo $q^m - 1$ from the following three lemmas.

**Lemma 24:** Let the notation be given as above. If $b_{m-2} > 0$ and $0 \leq a_i + b_i - b_{i-1} < q$ for $i \in [1, m-2]$, then $M$ given in (8) is not a coset leader modulo $q^m - 1$.

Proof: If $b_{m-2} = a_{m-1}$, from Lemma 21, we know that

$$b_{m-2} + a_{m-2} - b_{m-3} = a_{m-1} + a_{m-2} - b_{m-3} < 2\left\lfloor \frac{q-1}{m} \right\rceil - b_{m-3} \leq \frac{q+1}{2} \leq q-1.$$

It is easy to see that the equality can not hold simultaneously. Hence, $M > (q-1)q^{m-1}$ from (8). By Lemma 2, we know that $M$ is not a coset leader modulo $q^m - 1$.

We now prove that $M$ is not a coset leader modulo $q^m - 1$ when $b_{m-2} < a_{m-1}$. From Lemma 21 we know that $a_{m-1} = \left\lfloor \frac{q-1}{m} \right\rceil$. Let

$$a = a_{m-1} - b_{m-2},$$

then $0 < a < \left\lfloor \frac{q-1}{m} \right\rceil$. If there exists a positive integer $i_0 \in [1, m-2]$ satisfying $a_{i_0} + b_{i_0} - b_{i_0-1} > a$, then $Mq^{i_0} \pmod{q^m-1} < M$, which means that $M$ is not a coset leader modulo $q^m - 1$.

If for all $i \in [0, m-2]$, we have $a_i + b_i - b_{i-1} \leq a$, i.e.,

$$\begin{align*}
0 & \leq a_{m-2} + b_{m-2} - b_{m-3} \leq a, \\
0 & \leq a_{m-3} + b_{m-3} - b_{m-4} \leq a, \\
\vdots \\
0 & \leq a_1 + b_1 - b_0 \leq a,
\end{align*}$$  

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
then by (9) and (10) we have
\[
0 \leq a_{m-1} + a_{m-2} + \cdots + a_2 + a_1 - b_0 \leq (m - 1)a,
\]
i.e.,
\[
0 \leq a_{m-1} + a_{m-2} + \cdots + a_2 + a_1 - a_0 - b_0 \leq (m - 1)a.
\]
(11)
Since \(\sum_{i=0}^{m-1} a_i = q - 1\) and \(a < \left[\frac{q-1}{m}\right]\), from (11) we have
\[
a < q - 1 - (m - 1)a \leq b_0 + a_0 \leq q - 1.
\]
(12)
From (8) we know that \(Mq^{m-1} \mod q^m - 1 < M\). The desired conclusion then follows.

**Lemma 25:** Let the notation be given as above. If \(b_{m-2} = 0\) and \(0 \leq a_i + b_i - b_{i-1} < q\) for \(i \in [1, m-2]\), then \(M\) given in (8) is not a coset leader modulo \(q^m - 1\).

**Proof:** If \(M\) is a coset leader modulo \(q^m - 1\), then \(M \leq Mq^{m-1} \mod q^m - 1\) for \(i \in [1, m-1]\). From Lemma 21 and the definition of \(M\), we have
\[
\begin{align*}
\left\{ a_{m-2} - b_{m-3} & \leq \left[\frac{q-1}{m}\right], \\
 b_{m-3} + a_{m-3} - b_{m-4} & \leq \left[\frac{q-1}{m}\right], \\
 & \vdots \\
b_1 + a_1 - b_0 & \leq \left[\frac{q-1}{m}\right], \\
a_0 + b_0 & \leq \left[\frac{q-1}{m}\right].
\end{align*}
\]
(13)
If \(m\mid(q - 1)\), we have \(\left[\frac{q-1}{m}\right] = \frac{q-1}{m}\). Then from (13) and \(a_i = \frac{q-1}{m}\) for all \(i \in [0, m-1]\), we have
\[
b_0 = b_1 = \cdots = b_{m-3} = 0.
\]
Combining with \(b_{m-2} = 0\), we obtain that \(\mu = 0\), which is contradictory to \(\mu > 0\). Then \(M\) is not a coset leader modulo \(q^m - 1\).

In the following, we prove that \(M\) is not a coset leader modulo \(q^m - 1\) if \(m \nmid (q - 1)\). Since \(0 \leq a_i + b_i - b_{i-1}\), by the same way as we prove Lemma 24, we can obtain that \(0 \leq a_0 + b_0 < q - 1\). In this case, we have \(\left[\frac{q-1}{m}\right] - \left[\frac{q-1}{m}\right] = 1\). By Lemma 21, we know that \(a_0 = \left[\frac{q-1}{m}\right]\). Then \(b_0 = 0\) or \(b_0 = 1\).

**Case 1:** \(b_0 = 1\). Recall that
\[
M = q^m - (a_{m-1} - b_{m-2})q^{m-1} - (b_{m-2} + a_{m-2} - b_{m-3})q^{m-2} - \cdots - (b_1 + a_1 - b_0)q - a_0 - b_0 - 1.
\]
(14)
Then
\[
q^{m-1}M \mod q^m - 1 = q^m - (b_0 + a_0)q^{m-1} - (a_{m-1} - b_{m-2})q^{m-2} - \cdots - (b_2 + a_2 - b_1)q - (b_1 + a_1 - b_0) - 1.
\]
(15)
If \(M \leq q^{m-1}M\), by comparing (14) and (15), we know that
\[
a_{m-1} = a_{m-2} = \cdots = a_1 = \left[\frac{q-1}{m}\right] \quad \text{and} \\
b_0 = b_1 = \cdots = b_{m-3} = 0
\]
since \(b_{m-2} = 0\) and \(\left[\frac{q-1}{m}\right] \leq a_i \leq \left[\frac{q-1}{m}\right]\). Then we obtain that \(\mu = 0\), which is contradictory to \(\mu > 0\). Hence, we have \(M > q^{m-1}M \mod q^m - 1\).

**Case 2:** \(b_0 = 0\). From (13), we know that \(b_1 = 0\) or \(b_1 = 1\). If \(b_1 = 0\), then from (13) we know that \(b_2 = 0\) or \(b_2 = 1\). Continue this work, we can obtain that there exists \(i_1\) such that \(b_{i_1} = 1\) and \(b_{i_1 - l} = 0\), where \(i_1 \in [1, m-3]\) and \(l \in [1, i_1 - 1]\).

Recall that all the symbols are defined in Lemma 21. If \(i_1 \in \mathcal{Y}\), then we have \(b_{i_1 - 1} = 0\), \(b_1 = 1\) and \(a_{i_1} = \left[\frac{q-1}{m}\right]\), which is contradictory to \(a_{i_1} + b_{i_1} - b_{i_1 - 1} \leq \left[\frac{q-1}{m}\right]\). Hence, we obtain that \(i_1 \in [0, m-1] \setminus \mathcal{Y}\). This means that there is \(\gamma_2 \in [0, t_2 - 1]\) satisfying \(\left[\gamma_2s - 1\right] < i_1 < \left[(\gamma_2 + 1)s - 1\right]\). For the sake of narrative, we assume that \(b_{m-1} = b_{i_1 - 1} = 0\) in the following of this proof.

**Subcase 1:** If \(\left[\gamma_2s - 1\right] < i_1 < \left[(\gamma_2 + 1)s - 2\right]\). Let \(\xi = m - i_1 + 2 - \left[\gamma_2s\right]\) and \(\zeta = \left[(\gamma_2 - 1)s + 1\right]\). It is clear that \(M\) and \(q^{m-1} - 1\) can be expressed as
\[
M = q^m - (a_{m-1} - b_{m-2})q^{m-1} - (b_{m-2} + a_{m-2} - b_{m-3})q^{m-2} - \cdots - (b_1 + a_1 - b_0)q - a_0 - b_0 - 1,
\]
and
\[
q^{m-1}M \mod q^m - 1 = q^m - (a_{i_1} + b_{i_1} - b_{i_1 - 1})q^{m-2} - \cdots - (a_{i_1} + b_{i_1} - b_{i_1 - 1})q^\xi - \cdots - (b_1 + a_1 - b_0)q - a_0 - b_0 - 1.
\]
(16)
Since \(b_{m-2} = 0\), \(b_{i_1} = 1\) and \(b_{i_1 - l} = 0\) for \(l \in [1, i_1 - 1]\), we obtain that
\[
\left[\frac{q-1}{m}\right] = a_{i_1} + b_{i_1} - b_{i_1 - 1} = a_{m-1} - b_{m-2}.
\]
From Lemma 22, it is clear that
\[
m - 1 - (m - i_1 - 1 + \left[\gamma_2s - 1\right]) = i_1 - \left[\gamma_2s - 1\right] \leq N_{(\gamma_2+1),l} - 2 \leq N_{(l,t_2 - 1)} - 1.
\]
Then
\[
a_{m-2} = a_{m-3} = \cdots = a_{\xi + 1} = \left[\frac{q-1}{m}\right] \quad \text{and} \\
a_{i_1} = a_{i_1 - 1} = \cdots = a_{\gamma_2s} = \left[\frac{q-1}{m}\right]
\]
since \(0 \leq N_{(\gamma_2+1),l} - N_{(l,t_2 - 1)} \leq 1\) and \(\left[\gamma_2s - 1\right] < i_1 < \left[(\gamma_2 + 1)s - 2\right]\). If there exists \(l_1 \in [2, i_1 - \left[\gamma_2s\right]]\) such that
\[
a_{m-l_1+1} + b_{m-l_1+1} - b_{m-l_1-2} > a_{i_1 - l_1} + b_{i_1 - l_1} - b_{i_1 - l_1 - 1},
\]
(18)
let \(l_2\) be the least integer in the range \(l_1 \in [2, i_1 - \left[\gamma_2s\right]]\) such that (18) holds, then we have \(b_{m-l_2-1} > 0\) and
\[
a_{m-l_3} + b_{m-l_3} - b_{m-l_3} - b_{i_1 - l_3} - b_{i_1 - l_3 - 1} \leq a_{l_1 - l_3} + b_{l_1 - l_3} - b_{l_1 - l_3 - 1}
\]
(19)
for all \(0 \leq l_3 < l_2\). If all equalities for \(0 \leq l_3 < l_2\) in (19) hold, since \(b_{m-2} = 0\) and \(b_{i_1 - l} = 0\) for all \(l \in [1, i_1 - 1]\),
we know that $b_{m-3} = b_{m-4} = \cdots = b_{m-i_2-1} = 0$, which is contradictory with $b_{m-i_2-1} > 0$. Then at least one of equalities in (19) does not hold, we obtain that $q^{m-i_1-1}M \pmod{q^m-1} < M$ from (16) and (17).

If there does not exist $l_1 \in [2, i_1 - [\gamma_2 s]]$ such that (18) holds, then we have

$$
a_{i_1-1} + b_{i_1-1} - b_{i_1-2} \geq b_{m-2} + a_{m-2} - b_{m-3},
\quad a_{i_1-2} + b_{i_1-2} - b_{i_1-3} \geq b_{m-3} + a_{m-3} - b_{m-4},
\quad \vdots
\quad a_{[\gamma_2 s]} + b_{[\gamma_2 s]} - b_{[\gamma_2 s]-1} \geq b_{\xi+1} + a_{\xi+1} - b_{\xi},
$$

where $\xi = m-\xi_1-2 + [\gamma_2 s]$. If there exists one equality in (20) does not hold, then $q^{m-i_1-1}M \pmod{q^m-1} < M$ from (16) and (17).

Since $b_{i_1-l} = 0$ and $a_{i_1-l} = \lfloor \frac{q-1}{m} \rfloor$ for $l \in [1, i_1 - [\gamma_2 s]]$, we have $a_{i_1-l} + b_{i_1-l} - b_{i_1-1} = \lfloor \frac{q-1}{m} \rfloor$. If all equalities in (20) hold, then $b_{m-3} = b_{m-4} = \cdots = b_{\xi} = 0$. Hence,

$$a_{\xi} + b_{\xi} - b_{\xi-1} = \left\lceil \frac{q-1}{m} \right\rceil - b_{\xi-1} \leq \left\lfloor \frac{q-1}{m} \right\rfloor.$$

It is clear that $a_{\xi_1} + b_{\xi_1} - b_{\xi_1-1} = \left\lceil \frac{q-1}{m} \right\rceil$ since $a_{\xi_1} = \lfloor \frac{q-1}{m} \rfloor$ and $b_{\xi_1} = b_{\xi_1-1} = 0$. Then $q^{m-i_1-1}M \pmod{q^m-1} < M$ from (16) and (17).

Subcase 2: $i_1 = [(\gamma_2+1)s] - 2$. From Lemma 22, there exists $\xi \in [1, t_2]$ such that $N_{(\gamma_2+1, \xi)} = N((\xi_1, \xi_1))$ Assume that $\xi_1 \in [1, t_2]$ is the least integer such that $N((\xi_1, \xi_1)) = N((\xi_1, \xi_1))$. If there exists $l \in [2, i_1 - [(\gamma_2+1 - \xi_1)s]]$ such that $a_{m-1-l} + b_{m-1-l} - b_{m-2-l} > a_{(i_1-l)m} + b_{(i_1-l)m} - b_{(i_1-l-1)m}$, similar to the discussions of (18) and (19), then there is $1 \leq l_4 < l$ such that $a_{m-1-l_4} + b_{m-1-l_4} - b_{m-2-l_4} > a_{(i_4-l_4)m} + b_{(i_4-l_4)m} - b_{(i_4-l_4-1)m}$. Hence, we obtain $q^{m-i_1-1}M \pmod{q^m-1} < M$.

If there does not exist $l \in [2, i_1 - [(\gamma_2+1 - \xi_1)s]]$ such that $a_{m-1-l} + b_{m-1-l} - b_{m-2-l} > a_{(i_1-l)m} + b_{(i_1-l)m} - b_{(i_1-l-1)m}$, then we have

$$a_{(i_1-l)m} + b_{(i_1-l)m} - b_{(i_1-l-1)m} \geq a_{m-1-l} + b_{m-1-l} - b_{m-2-l} \tag{21}$$

for all $l \in [2, i_1 - [(\gamma_2+1 - \xi_1)s]]$. If there exists one equality in (21) does not hold, then $q^{m-i_1-1}M \pmod{q^m-1} < M$.

If all equalities in (21) hold simultaneously, then $b_{m-3} = b_{m-4} = \cdots = b_{\eta-1} = 0$, where $\eta = m-1-i_1 + [(\gamma_2+1 - \xi_1)s]$. Hence,

$$a_{\eta-1} + b_{\eta-1} - b_{\eta-2} = \left\lceil \frac{q-1}{m} \right\rceil + 0 - b_{\eta-2} \leq \left\lfloor \frac{q-1}{m} \right\rfloor .$$

Let $\varepsilon_2 = [((\gamma_2-\xi_1)\varepsilon_2+1)s-1]$. Since $a_{\varepsilon_2} = \lfloor \frac{q-1}{m} \rfloor$ and $b_{\varepsilon_2-1} = 0$, we have

$$a_{\varepsilon_2} + b_{\varepsilon_2} - b_{\varepsilon_2-1} = \left\lfloor \frac{q-1}{m} \right\rfloor ,$$

then

$$a_{\eta-1} + b_{\eta-1} - b_{\eta-2} < a_{\varepsilon_2} + b_{\varepsilon_2} - b_{\varepsilon_2-1} .$$

Hence, we obtain $q^{m-i_1-1}M \pmod{q^m-1} < M$. Hence, from Cases 1 and 2, we know that there always exists $i \in [1, m-1]$ such that $M \geq Mq^i \pmod{q^m-1}$. Hence, $M$ is not a coset leader modulo $q^m-1$. The desired conclusion then follows.

**Lemma 26:** Let the notation be given as above. If there exists $i \in [1, m-2]$ such that $a_i + b_i - b_{i-1} < 0$ or $a_i + b_i - b_{i-1} \geq q$, then $M$ given in (8) is not a coset leader modulo $q^m-1$.

**Proof:** If $a_i + b_i - b_{i-1} \geq 0$ for all $i \in [1, m-2]$ and there exists a positive integer $i_2 \in [1, m-2]$ such that $a_{i_2} + b_{i_2} - b_{i_2-1} \geq q$, i.e.,

$$a_{i_2} + b_{i_2} - b_{i_2-1} \geq q ,$$

then $b_{i_2-1} \leq \sum_{j=i_2}^{m-2} a_j + b_m - q \leq \sum_{j=i_2}^{m-2} a_j + a_m - q < 0$, which is impossible. Hence, there exists $i_3 \in [1, m-2]$ such that $a_{i_3} + b_{i_3} + b_{i_3-1} < 0$ if there exists $i_2 \in [1, m-2]$ such that $a_{i_2} + b_{i_2} - b_{i_2-1} \geq q$.

Let $\Psi$ be a subset of $[1, m-2]$ such that $b_i + a_i - b_{i-1} < 0$ if $i \in \Psi$ and $a_i + b_i - b_{i-1} \geq 0$ if $i \in [1, m-2] \setminus \Psi$. Let $i_5 = \max\{i : i \in \Psi\}$ If there exists $i$ such that $b_i + a_i - b_{i-1} \geq q$, we assume that $i_5 = \max\{i : a_i + b_i - b_{i-1} \geq q, i \in [1, m-2] \setminus \Psi\}$. If $i_5 > i_4$, with a similar analysis as (22), it is easy to get that $b_{i_4-1} < 0$, which is contradictory to $b_{i_4-1} \geq 0$.

If $b_{i_4} + a_{i_4} - b_{i_4-1} = -1$ and $i_5 = i_4 - 1$, we know that

$$a_{i_5} + b_{i_5} - b_{i_5-1} \geq a_{m-2} + b_m - q \geq 0 ,$$

then $b_{i_4-2} \leq \sum_{i=i_4-1}^{m-2} a_i + q \leq \sum_{i=i_4-1}^{m-2} a_i + a_m - q < 0$, which is contradictory to $b_{i_4-2} \geq 0$.

From above, in order to obtain the desired result, we only need to prove the case that $M$ is not a coset leader modulo $q^m-1$ if $b_{i_4} + a_{i_4} - b_{i_4-1} < -1$, or $i_5 \neq i_4 - 1$, or there does not exist $i \in [1, m-2]$ such that $b_i + a_i - b_{i-1} \geq q$. In these cases, it is clear that $M$ can be expressed as

$$M = (q - a_m - b_m)q^m + (b_m - a_m - b_m)q^m + \cdots + (b_0 - a_1 - b_1)q - a_0 - b_0 - 1 . \tag{23}$$

Then $q^{m-i_4-1}M \pmod{q^m-1}$ can be expressed as

$$q^{m-i_4-1}M \pmod{q^m-1} = (b_{i_4-1} - a_{i_4} - b_{i_4})q^m + \cdots + (b_0 - a_1 - b_1)q^m + \cdots + (b_i - a_{i+1} - b_{i+1}) . \tag{24}$$
If \( i_4 \neq m - 2 \) and
\[
q^{m-i_4-1}M \pmod{q^m - 1} = (b_{i_4-1} - a_{i_4} - b_{i_4})q^{m-1} + (b_{i_4-2} - a_{i_4} - b_{i_4-1})q^{m-2} + \cdots + (-a_0 - b_0)q^{m-i_4-1} + (-a_{m-1} + b_{m-2})
\]
if \( i_4 = m - 2 \). We only prove the case that \( M \) is not a coset leader modulo \( q^m - 1 \) if \( i_4 \neq m - 2 \). When \( i_4 = m - 2 \), the desired results can be shown similarly. We omit the details.

It is easy to see that \( b_{i_4-1} - b_{i_4} - a_{i_4} \leq q + b_{m-2} - a_{m-1} \).

If \( b_{i_4-1} - b_{i_4} - a_{i_4} < q + b_{m-2} - a_{m-1} \), then \( q^{m-i_4-1}M \pmod{q^m - 1} < M \).

If \( b_{i_4-1} - b_{i_4} - a_{i_4} = q + b_{m-2} - a_{m-1} \), it is clear that
\[
\begin{aligned}
b_{i_4-1} &= q - 1, \quad b_{i_4} = 0, \quad a_{i_4} = \left\lfloor \frac{q - 1}{m} \right\rfloor, \\
b_{m-2} &= 0 \quad \text{and} \quad m \nmid (q - 1)
\end{aligned}
\]
(25)
since \( a_{m-1} = \left\lfloor \frac{q - 1}{m} \right\rfloor \). There exists a positive integer \( \gamma_3 \) such that \( \left\lfloor (\gamma_3 - 1)s - 1 \right\rfloor \leq i_4 < \left\lfloor \gamma_3s - 1 \right\rfloor \). Let \( 1 \leq s \leq i_4 \) and
\[
D_{m-1-s} = (b_{i_4-s-1} - a_{i_4-s} - b_{i_4-s}) - (b_{m-3} - b_{m-2} - a_{m-2})
\]
Clearly, from (25) we know that
\[
D_{m-2} = (b_{i_4-2} - a_{i_4-1} - b_{i_4-1}) - (b_{m-3} - b_{m-2} - a_{m-2})
= b_{i_4-2} - (q - 1) - b_{m-3} - a_{m-1} - a_{m-2}.
\]
From Lemma 21, it is obvious that
\[
-a_{i_4-1} + a_{m-2} \in \{-1, 0, 1\}.
\]
(26)
If \( a_{m-2} - a_{i_4-1} = 1 \), then we have \( a_{i_4-1} = \left\lfloor \frac{q - 1}{m} \right\rfloor \) and \( a_{m-2} = \left\lceil \frac{q - 1}{m} \right\rceil \). Since \( a_{i_4} = a_{i_4-1} = \left\lfloor \frac{q - 1}{m} \right\rfloor \) and \( a_{m-1} = a_{m-2} = \left\lceil \frac{q - 1}{m} \right\rceil \), we obtain that \( N_{\gamma_3 (1)} \geq 3 \) and \( N_{(2,1)} = 1 \), which is contradictory to Lemma 22. Then from (26) we know that \( a_{m-2} - a_{i_4-1} \in \{-1, 0\} \). Hence, we obtain that \( D_{m-2} \leq 0 \). If \( D_{m-2} < 0 \), then \( q^{m-i_4-1}M \pmod{q^m - 1} < M \).

If \( D_{m-2} = 0 \), combined with (25), we obtain that
\[
\begin{aligned}
b_{i_4-2} &= q - 1, \\
b_{m-3} &= 0 \quad \text{and} \quad a_{m-2} - a_{i_4-1} = 0.
\end{aligned}
\]
(27)
With a similar analysis on \( D_{m-2} \), we obtain \( D_{m-3} \leq 0 \).

If \( D_{m-3} < 0 \), then \( q^{m-i_4-1}M \pmod{q^m - 1} \leq M \).

If \( D_{m-3} = 0 \), combined with (27) we obtain that \( b_{i_4-3} = q - 1, b_{m-4} = 0 \) and \( a_{m-3} - a_{i_4-2} = 0 \). Continue this work, we always have \( q^{m-i_4-1}M \pmod{q^m - 1} < M \), or
\[
\begin{aligned}
b_{i_4-1} &= b_{i_4-2} = \cdots = b_0 = q - 1, \\
b_{m-2} &= b_{m-3} = \cdots = b_{m-i_4-1} = 0, \\
&\vdots \\
& a_{m-2} - a_{i_4-1} = a_{m-3} - a_{i_4-2} = a_{m-i_4} = a_1 = 0.
\end{aligned}
\]
(28)
If (28) holds, then
\[
D_{m-i_4-1} = -(b_0 + a_0) - (b_{m-i_4-2} - b_{m-i_4-1} - a_{m-i_4-1}) = -(q - 1) - \left\lfloor \frac{q - 1}{m} \right\rfloor b_{m-i_4-2} + a_{m-i_4-1} - (q - 2) < 0.
\]

Hence, \( q^{m-i_4-1}M \pmod{q^m - 1} < M \). Combining with all the cases, we obtain that \( M \) is not a coset leader modulo \( q^m - 1 \). The desired conclusion then follows.

Proposition 27: Let \( q \geq 3 \) be a prime power and \( m \geq 4 \) be an integer. Then
\[
\delta_1 = \theta = q^m - 1 - \frac{\left( \sum_{i=1}^{q-2} q \left\lceil \frac{m}{m-1} \right\rceil - q + 2 \right)}{q - 1}
\]
is the largest coset leader modulo \( q^m - 1 \).

Proof: If \( \delta \) is a coset leader modulo \( n \), then \( (q-1)\delta \) must be a coset leader modulo \( q^m - 1 \) since
\[
delta q^m \pmod{n} \geq \delta \Leftrightarrow \delta(q-1)q^m \pmod{n} \geq \delta(q-1)
\]
for any \( 1 \leq i \leq m - 1 \). If \( \delta > \delta_1 \), we know that \( (q-1)\delta \) can be written as \( M \), where \( M \) is given in (7). From Lemmas 24-26, we obtain that \( M \) is not a coset leader modulo \( q^m - 1 \). Hence, \( \delta \) is not a coset leader modulo \( n \) if \( \delta > \delta_1 \). From Lemma 23, we know that \( \delta_1 \) is the largest coset leader modulo \( n \). The desired result then follows.

Lemma 28: Let \( \delta_1 \) be given as in Proposition 27, then \( |C_{\delta_1}| = m \frac{m}{\gcd(m,q-1)} \).

Proof: It is known that \( \mathord{n}(q) = m \), then \( |C_{\delta_1}| \) is a divisor of \( m \). Assume that \( |C_{\delta_1}| = h \), then
\[
n \mid \delta_1(q^h - 1).
\]
(29)
By definition, \( \delta_1 \) can be written as
\[
\delta_1 = n - \sum_{t=1}^{q-1} q \left\lceil \frac{m}{q^t - 1} \right\rceil.
\]
Then (29) holds if and only if \( q^{-1} + \sum_{t=1}^{q-1} q \left\lceil \frac{m}{q^t - 1} \right\rceil \), i.e.,
\[
(q^{m-h} + q^{m-2h} + \cdots + q^{m-(i-1)h} + 1) \mid \sum_{t=1}^{q-1} q \left\lceil \frac{m}{q^t - 1} \right\rceil,
\]
where \( i = \frac{m}{n} \). It is easy to check that
\[
\sum_{t=1}^{q-1} q \left\lceil \frac{m}{q^t - 1} \right\rceil = \left( \frac{\gcd(q-1,m)-1}{\gcd(q-1,m)} \right) \left( \sum_{i=1}^{\gcd(q-1,m)} q \left\lceil \frac{m}{q^i - 1} \right\rceil \right).
\]
In addition,
\[
q^{m-h} + q^{m-2h} + \cdots + q^{m-(i-1)h} + 1 = \sum_{t=0}^{\gcd(q-1,m)-1} q \gcd(q-1,m)
\]
if \( h = \frac{m}{\gcd(q-1,m)} \). Hence, (29) holds if \( h = \frac{m}{\gcd(q-1,m)} \). This means that
\[
|C_{\delta_1}| = h \leq \frac{m}{\gcd(q-1,m)}.
\]
(30)
We now prove that \( h \geq \frac{m}{\gcd(m,q-1)} \). Assume that there exists a positive integer \( Q \) such that
\[
Q(q^{m-h} + q^{m-2h} + \cdots + q^{m-(i-1)h} + 1) = \sum_{t=1}^{q-1} q \left\lceil \frac{m}{q^t - 1} \right\rceil.
\]
(31)
Let \( Q = a_t q^t + a_{t-1} q^{t-1} + \cdots + a_1 q + a_0 \) and \( a_t + a_{t-1} + \cdots + a_0 = r \). If (31) holds, then \( rm = h(q - 1) \). Hence, we have
\[
rm = h(q - 1).
\]
Since
\[
gcd\left(\frac{m}{gcd(m, q - 1)}, \frac{q - 1}{gcd(m, q - 1)}\right) = 1,
\]
we obtain that \( |C_{\delta_1}| = \frac{m}{gcd(m, q - 1)} \). Hence, from (30) we have \( |C_{\delta_1}| = \frac{m}{gcd(m, q - 1)} \). The desired conclusion then follows.

Remark 29: When \( q = 3 \), \( \delta_1 \) and \( |C_{\delta_1}| \) have been given in [15, Lemma 17]. Let \( m \geq q, b = m - 1 \) (mod \( q - 1 \)). When \( b = 0 \), \( b = 1 \) or \( b = q - 2 \), \( \delta_1 \) and \( |C_{\delta_1}| \) have been given in [24, Lemma 16]. We generalize these results in Proposition 27 and Lemma 28.

From Proposition 27 and Lemma 28, one can get the following theorem.

Theorem 30: When \( m \geq 3 \) be an integer and \( q \geq 3 \) be a prime power, the BCH code \( C_{\delta_1} \) has parameters
\[
\left[ \frac{q^m - q}{q - 1}, \frac{m}{gcd(m, q - 1)} + 1 \right], \quad d \geq q^m - 1 - 1 - \frac{\sum_{t=1}^{q-2} q^t - 1 - q + 2}{q - 1}.
\]

Example 31: Let \( (q, m) = (3, 4) \). Then the code \( C_{\delta_1} \) in Theorem 19 has parameters \( [40, 3, \geq 25] \). This code is the best cyclic code according to [5, P. 305] when the equality holds.

In the following, we provide a sufficient and necessary condition for \( C_{\delta_1} \) being a dually-BCH code. We first give a key lemma.

Lemma 32: Let \( \delta' \) be the coset leader of \( C_n - \delta_1 \) modulo \( n \). Then the following hold.

1. \( \delta' \in T^{\perp} \) is a coset leader modulo \( n \) if \( 2 \leq \delta \leq \delta' \).
2. \( \delta' \in T^{\perp} \) is a coset leader modulo \( n \) if \( \delta' < \delta \leq \delta_1 \).

Proof: Since \( \delta' \) is the coset leader of \( C_n - \delta_1 \) modulo \( n \), we have \( C_n - \delta' = C_{\delta_1} \). If \( 2 \leq \delta \leq \delta' \), i.e., \( C_{\delta'} \nsubseteq T^{\perp} \), then \( C_n - \delta' = C_{\delta_1} \nsubseteq T^{\perp} \). If \( \delta' < \delta \leq \delta_1 \), i.e., \( C_{\delta_1} \nsubseteq T^{\perp} \), then \( C_n - \delta_1 = C_{\delta'} \nsubseteq T^{\perp} \) and \( C_{\delta'} \subseteq T^{\perp} \).

Denote \( m = r(q - 1) + s \) and \( n = \left\lceil \frac{(s-1)(q-1)}{s} \right\rceil \), where \( r \geq 0 \) and \( 0 \leq s \leq q - 2 \). Note that
\[
\delta_1 = q^m - 1 - \sum_{t=1}^{q-2} q^{t - 1} - q + 2.
\]
Then
\[
n - \delta_1 = \sum_{t=1}^{q-1} q^t - 1 - \frac{q^m - q - 1}{q - 1}.
\]  
(32)

Let \( \delta' \) and \( \delta'' \) be the coset leaders of \( C_n - \delta_1 \) modulo \( n \) and \( C_{\delta_1} \) modulo \( (q - 1)n \), respectively. It is similar with (4), we have \( (q - 1) | \delta'' \) and \( \delta'' = \delta'(q - 1) \). From (32) we have \( (q - 1)(n - \delta_1) = \sum_{t=1}^{q-1} q^t - 1 \). From Lemma 21, one can see that the \( q \)-adic expansion of \( \delta'' \) has the form \( (0, r, 1, \ldots)_q \) if \( r \geq 1 \) and \( \delta'' \) has the form \( (\frac{q-1}{q-1}, \ldots)_q \) if \( r = 0 \). where \( \theta_r = (0, 0, \ldots, 0)_q \).

\[
\delta' = \delta'' > \frac{q^m - 1}{q - 1}.
\]  
(33)

With the preparations above, we now give a sufficient and necessary condition for \( C_{\delta} \) being a dually-BCH code.

Theorem 33: Let \( n = \frac{q^m - 1}{q - 1} \), where \( q \geq 3 \) is a prime power and \( m \geq 4 \) is a positive integer. Then \( C_{\delta} \) is a dually-BCH code if and only if \( \delta_1 + 1 \leq \delta \leq \delta_1 \), where \( \delta_1 \) is given in Proposition 27.

Proof: When \( q = 3 \), the result has been given in [9, Theorem 30], we only prove the result for \( q > 3 \) in the following.

It is clear that \( 0 \notin T \) and \( 1 \notin T \), so \( 0 \notin T^{\perp} \) and \( n - 1 \notin T^{\perp} \). Furthermore, we have \( 0 \in T^{\perp} \) and \( n - 1 \notin T^{\perp} \), which means that \( C_0 \) must be the initial cyclotomic coset of \( T^{\perp} \). Consequently, there must be an integer \( J \geq 1 \) such that \( T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1} \) if \( C_{\delta} \) is a dually-BCH code.

When \( \delta_1 < \delta \leq \delta_1 \), it is easy to see that \( T^{\perp} = \{0\} \) and \( C_{\delta} \) is a BCH code with respect to \( \beta \). It remains to show that \( C_{\delta} \) is not a BCH code with respect to \( \beta \) when \( 2 \leq \delta \leq \delta_1 \). To this end, we show that there is no integer \( J \geq 1 \) such that \( T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1} \). Recall that \( m = r(q - 1) + s \), we have the following two cases.

Case 1: \( 2 \leq \delta \leq q^m - 1 \). It is easy to see that \( m - r - 1 = r + 1 \). Then from (33) and Proposition 32 that \( \delta_1 \in T^{\perp} \) is the coset leader of \( C_{\delta} \). It follows from Lemma 4 that
\[
I_{\max} := \max\left\{ I(\delta) : 2 \leq \delta \leq \frac{q^m - 1}{q - 1} \right\} = I(2) = \frac{q^m - 1}{q - 1} = (0, 1, \ldots, q)_q.
\]

Note that \( \delta_1 = q^{m-1} - 1 - \frac{\sum_{t=1}^{q-2} q^t - 1 - q + 2}{q - 1} \). It is easy to see that \( (q - 1) \delta_1 > q^{m-1} - 1 \) and \( \delta_1 > \frac{q^{m-1} - 1}{q - 1} \). It then follows that there is no integer \( J \geq 1 \) such that \( T^{\perp} = C_0 \cup C_1 \cup \cdots \cup C_{J-1} \), i.e., \( C_{\delta} \) is not a BCH code with respect to \( \beta \).

Case 2: \( \frac{q^{m-1} - 1}{q - 1} < \delta < q^{m-1} - 1 \). It then follows from Proposition 32 that \( \delta' \in T^{\perp} \) is the coset leader of \( C_{\delta} \). It follows from Lemma 4 that
\[
I_{\max} := \max\left\{ I(\delta) : \frac{q^{m-1} - 1}{q - 1} < \delta < q^{m-1} - 1 - \frac{\sum_{t=1}^{q-2} q^t - 1 - q + 2}{q - 1} \right\} = \frac{q^{m-1} - 1}{q - 1}.
\]

We deduce from (33) that \( \delta' > \frac{q^{m-1} - 1}{q - 1} \). It then follows from Lemma 4 that there is no integer \( J \geq 1 \) such that \( T^{\perp} = \{ \ldots \} \).
$C_0 \cup C_1 \cup \cdots \cup C_{q-1}$, i.e., $C_2^q$ is not a BCH code with respect to $\beta$.

**Remark 34:** In [9], let $q=3$, the authors gave the range of $\delta$ for BCH codes $C_\delta$ being dually-BCH codes. They showed that it looks much harder to give a characterisation of $C_\delta$ being dually-BCH codes, where $q>3$ is a prime power. Theorem 33 finished this work.

**V. Conclusion**

Let $n = \frac{q^{m-1}}{q^1+1}$ for $m \geq 4$ being even and $q$ being a prime power, or $n = \frac{q^{m-1}}{q^1}$ for $m \geq 4$ being a positive integer and $q$ being an odd prime power. The main contributions of this paper are the following:

- Sufficient and necessary conditions for BCH codes $C_\delta$ being dually-BCH codes were given, where $2 \leq \delta \leq n$. Lower bounds on the minimum distances of their dual codes are developed for $n = \frac{q^{m-1}}{q^1+1}$. In this sense, we extended the results in [9].
- We determined the largest coset leader modulo $\frac{q^{m-1}}{q^1+1}$, which is very useful to completely solve Open Problem 45 in [14]. We also determined the largest coset leader modulo $\frac{2^{m-1}}{q^1+1}$, so the conjecture in [19] were proved.

**Acknowledgment**

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

**References**

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, “On quantum and classical BCH codes,” IEEE Trans. Inf. Theory, vol. 53, no. 3, pp. 1183–1188, Mar. 2007.
[2] D. Augot and N. Sendrier, “Idempotents and the BCH bound,” IEEE Trans. Inf. Theory, vol. 40, no. 1, pp. 204–207, Jan. 1994.
[3] R. C. Bose and D. K. Ray-Chaudhuri, “On a class of error correcting binary group codes,” Inf. Control, vol. 3, pp. 279–290, Mar. 1960.
[4] P. Charpin, “On a class of primitive BCH-codes,” IEEE Trans. Inf. Theory, vol. 36, no. 1, pp. 222–228, Jan. 1990.
[5] C. Ding, Codes From Difference Sets, Singapore: World Scientific, 2015.
[6] C. Ding, “BCH codes in the past 55 years,” in Proc. 7th Int. Workshop Finite Fields Appl., Tianjin, China, 2016.
[7] C. Ding, X. Du, and Z. Zhou, “The Bose and minimum distance of a class of BCH codes,” IEEE Trans. Inf. Theory, vol. 61, no. 5, pp. 2351–2356, May 2015.
[8] C. Ding, C. Fan, and Z. Zhou, “The dimension and minimum distance of two classes of primitive BCH codes,” Finite Fields Their Appl., vol. 45, pp. 237–263, May 2017.
[9] B. Gong, C. Ding, and C. Li, “The dual codes of several classes of BCH codes,” IEEE Trans. Inf. Theory, vol. 68, no. 2, pp. 953–964, Feb. 2018.
[10] D. C. Gorenstein and N. Zierler, “A class of error-correcting codes in $p^n$ symbols,” J. Siam., vol. 9, no. 3, pp. 207–214, Jun. 1961.
[11] M. Grassl. Bounds on the Minimum Distance of Linear Codes and Quantum Codes. Accessed: May 16, 2023. [Online]. Available: http://www.codetables.de
[12] A. Hocquenghem, “Codes correcteurs d’erreurs,” Chiffres, vol. 2, pp. 147–156, Sep. 1959.
[13] 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.
[14] 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.
[15] 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, Sep. 2017.

**Xiaoxiang Wang** received the B.S. degree in mathematics from Hubei Normal University, Huangshi, China, in 2012, the M.S. degree in applied mathematics from Hubei University in 2015, and the Ph.D. degree in applied mathematics from Central China Normal University in 2019. From 2017 to 2018, he visited the Department of Mathematical Sciences, Kent State University, USA. From 2020 to 2021, he was a Post-Doctoral Fellow with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology. He is currently with Hubei University. His current research interests include coding theory and cryptography.

**Jiaojiao Wang** received the B.S. degree in mathematics from Hebei Normal University in 2019 and the M.S. degree in mathematics from Hubei University, China, in 2022. She is currently pursuing the Ph.D. degree with the Tsinghua-Berkeley Shenzhen Institute, under the supervision of Prof. Min Ye. Her current research interests include coding theory.

**Chengju Li** received the Ph.D. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2014. From March 2015 to February 2016, he was a Post-Doctoral Researcher with the Department of Mathematics, Korea Advanced Institute of Science and Technology, Daejeon, South Korea. From March 2016 to August 2016, he was a Post-Doctoral Researcher with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong. From July 2018 to September 2018, he visited Université Paris 8, Paris, France. He is currently a Professor with the Software Institute, East China Normal University, Shanghai, China. His current research interests include exponential sums, coding theory, and cryptography.

**Yansheng Wu** received the Ph.D. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2019. From September 2019 to August 2020, he was a Post-Doctoral Researcher with the Department of Mathematics, Ewha Womans University, Seoul, South Korea. Since October 2020, he has been with the School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, where he is currently a Professor appointed by the President. Since March 2023, he has been a Post-Doctoral Researcher with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong. His current research interests include coding theory and sequences.