

Two classes of narrow-sense BCH codes and their duals

Xiaoqiang Wang, Jiaojiao Wang, Chengju Li*, 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 the duals of BCH codes. Recently, a new concept called dually-BCH code was introduced to investigate the duals of BCH codes and the lower bounds on their minimum distances in [12]. For a prime power q and an integer $m \geq 4$, let $n = \frac{q^m-1}{q+1}$ (m even), or $n = \frac{q^m-1}{q-1}$ ($q > 2$). 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 [12]. Lower bounds on the minimum distances of their dual codes are developed for $n = \frac{q^m-1}{q+1}$ (m even). As byproducts, we present the largest coset leader δ_1 modulo n being of two types, which proves a conjecture in [28] and partially solves an open problem in [21]. We also investigate the parameters of the narrow-sense BCH codes of length n with design distance δ_1 . The BCH codes presented in this paper have good parameters in general.

Index Terms

The work of Chengju Li was supported by the National Natural Science Foundation of China (12071138), Shanghai Rising-Star Program (22QA1403200), the open research fund of National Mobile Communications Research Laboratory of Southeast University (2022D05), and the Shanghai Trusted Industry Internet Software Collaborative Innovation Center.

Corresponding author*.

Xiaoqiang Wang is with Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China (E-mail: waxiqq@163.com).

Jiaojiao Wang is with Data Science and Information Technology Research Center, Tsinghua-Berkeley Shenzhen Institute, Tsinghua Shenzhen International Graduate School, Shenzhen, China. (E-mail: wjj22@mails.tsinghua.edu.cn).

Chengju Li is the Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai, 200062, China; and is also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (E-mail: cjli@sei.ecnu.edu.cn).

Yansheng Wu is with School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (E-mail: yanshengwu@njupt.edu.cn).

BCH code, cyclic code, dually-BCH code, dual code.

I. INTRODUCTION

Let $\text{GF}(q)$ 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 $[n, k, d]$ linear code C over the finite field $\text{GF}(q)$ is a k -dimensional linear subspace of $\text{GF}(q)^n$ with minimum (Hamming) distance d . The dual code of C , denoted by C^\perp , is defined by

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

where $\mathbf{b}\mathbf{c}^T$ is the standard inner product of two vector \mathbf{b} and \mathbf{c} . If the code C is closed under the cyclic shift, i.e., if $(c_0, c_1, c_2, \dots, c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, c_2, \dots, c_{n-2}) \in C$, then C is called a *cyclic code*. By identifying any vector $(c_0, c_1, \dots, c_{n-1}) \in \text{GF}(q)^n$ corresponds to a polynomial

$$c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1} \in \text{GF}(q)[x]/(x^n - 1),$$

then any cyclic code C of length n over $\text{GF}(q)$ corresponds to a subset of the quotient ring $\text{GF}(q)[x]/(x^n - 1)$. Since every ideal of $\text{GF}(q)[x]/(x^n - 1)$ 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 $[n, k, d]$ linear code over $\text{GF}(q)$ is said to be *distance-optimal* (respectively, *dimension-optimal* and *length-optimal*) if there does not exist $[n, k, d' \geq d + 1]$ (respectively, $[n, k' \geq k + 1, d]$ and $[n' \leq n - 1, k, d]$) linear code over $\text{GF}(q)$. A code is called 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 $\ell = \text{ord}_n(q)$ be the order of q modulo n , and let α be a generator of the group $\text{GF}(q^\ell)^*$. Put $\gamma = \alpha^{(q^\ell - 1)/n}$, then γ is a primitive n -th root of unity in the finite field $\text{GF}(q^\ell)$. For any i with $0 \leq i \leq q^\ell - 2$, let $m_i(x)$ denote the minimal polynomial of γ^i over $\text{GF}(q)$. For any δ with $2 \leq \delta \leq n$, let

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

where b is an integer and lcm denotes the least common multiple of these minimal polynomials. Let $C_{(q,n,\delta,b)}$ denote the cyclic code of length n with generator polynomial $g_{(q,n,\delta,b)}$, then $C_{(q,n,\delta,b)}$ is called a BCH code with *designed distance* δ . If $b = 1$, then $C_{(q,n,\delta,1)}$ is called a *narrow-sense*

BCH code. In this case, for convenience we will use $C_{(q,n,\delta)}$ in the sequel. A BCH code is called *dually-BCH code* if both the BCH code and its dual are a BCH code with respect to an n -th primitive root of unity γ . This concept was introduced in [12] to investigate the duals of BCH codes and the lower bounds on their minimum distances.

BCH codes were invented in 1959 by Hocquenghem [16], and independently in 1960 Bose and Ray-Chaudhuri [5]. They were extended to BCH codes over finite fields by Gorenstein and Zierler in 1961 [13]. 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 cyclic codes with interesting properties and applications and are usually among the best cyclic codes. The reader is referred to, for example, [1], [2], [6], [9], [10], [11], [20], [22], [23], [31], [32] for more information.

In [28], let $m \geq 6$ be even, the authors described the largest coset leader δ_1 modulo $n = \frac{q^m-1}{q+1}$ for $q = 2, 3$ and studied the parameters of the narrow-sense BCH codes with design distance δ_1 . In addition, the authors gave a conjecture on the largest coset leader modulo $n = \frac{q^m-1}{q+1}$ for $q > 3$. In [12], the authors obtained a sufficient and necessary condition for the code $C_{(q, \frac{q^m-1}{q+1}, \delta)}$ being a dually-BCH code in the ternary case, while the case $q \geq 4$ is still open.

Below we always assume that $m \geq 4$ is an integer and q is a prime power, m is even if $n = \frac{q^m-1}{q+1}$ and $q > 2$ if $n = \frac{q^m-1}{q-1}$. The main objective of this paper is to 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, where $n = \frac{q^m-1}{q+1}$. This paper generalizes some results in [12] when $n = \frac{q^m-1}{q+1}$. As byproducts, we present the largest coset leader δ_1 modulo n , which proves a conjecture in [28] and partially solves an open problem in [21]. We also investigate the parameters of the narrow-sense BCH codes of length n with designed distance δ_1 , where $n = \frac{q^m-1}{q+1}$. 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 [14], and the best known cyclic codes maintained in [7], 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 $n = \frac{q^m-1}{q+1}$. 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.
- α is a primitive element of $\text{GF}(q^m)$ and $\beta = \alpha^n$ is a primitive n -th root of unity, where $n \mid q^m - 1$.
- $m_i(x)$ denotes the minimal polynomial of β^i over $\text{GF}(q)$.
- $g_{(q,n,\delta)} = \text{lcm}(m_1(x), m_2(x), \dots, m_{\delta-1}(x))$ denotes the least common multiple of these minimal polynomials.
- $C_{(q,n,\delta)}$ denotes the BCH code with generator polynomial $g_{(q,n,\delta)}$.
- $T = \{0 \leq i \leq n-1 : g(\beta^i) = 0\}$ is the defining set of $C_{(q,n,\delta)}$ with respect to β .
- $T^{-1} = \{n-i : i \in T\}$.
- T^\perp is the defining set of the dual code $C_{(q,n,\delta)}^\perp$ with respect to β .
- $\lceil x \rceil$ denotes the smallest integer larger than or equal to x .
- $\lfloor x \rfloor$ denotes the largest integer less than or equal to x .
- \bar{x}_t denotes $x \pmod{t}$ and $0 \leq \bar{x}_t \leq t-1$, where t is a positive integer.

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 expansion of a and b , respectively. Write $\bar{a} = (a_{m-1}, a_{m-2}, \dots, a_0)_q$ and $\bar{b} = (b_{m-1}, b_{m-2}, \dots, b_0)_q$. Define $\bar{a} > \bar{b}$ if $a_{m-1} > b_{m-1}$ or there exists an integer $0 \leq i \leq m-2$ 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 $\bar{a} > \bar{b}$.*

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

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

where ℓ_s is the smallest positive integer such that $s \equiv sq^{\ell_s} \pmod{n}$, and is the size of the q -cyclotomic coset. The smallest integer in C_s is called the *coset leader* of C_s . The following lemma on coset leaders modulo $q^m - 1$ will play an important role in proving the conjecture documented in [28].

Lemma 2. *The first three largest q -cyclotomic coset leaders modulo $n = q^m - 1$ are given as follows:*

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

The following lemma is given in [12], which is useful to give a characterization of $C_{(q, \frac{q^m-1}{q-1}, \delta)}$ being a dually-BCH code for $q \geq 3$.

Lemma 3. *For $2 \leq \delta < n$, let $I(\delta)$ be the integer such that $\{0, 1, 2, \dots, I(\delta) - 1\} \subseteq T^\perp$ and $I(\delta) \notin T^\perp$. Then we have $I(\delta) = \frac{q^{m-t}-1}{q-1}$ if $\frac{q^t-1}{q-1} < \delta \leq \frac{q^{t+1}-1}{q-1}$ ($1 \leq t \leq m-2$) and $I(\delta) = 1$ if $\frac{q^{m-1}-1}{q-1} < \delta < n$.*

III. BCH CODES 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 $C_{(q,n,\delta)}$ is a BCH code with designed distance δ , i.e., the defining set with respect to β is $T = C_1 \cup C_2 \cup \dots \cup C_{\delta-1}$, where $2 \leq \delta \leq n$ and $\beta = \alpha^{q+1}$. It then follows that $T^\perp = Z_n \setminus T^{-1}$ is the defining set of the dual code $C_{(q,n,\delta)}^\perp$ with respect to β , where $T^{-1} = \{n-i : i \in T\}$. It is clear that $0 \in T^\perp$. In this section, we give the largest coset leader δ_1 modulo n and study the parameters of the BCH code $C_{(q,n,\delta_1)}$. We also derive a sufficient and necessary condition for $C_{(q,n,\delta)}$ being a dually-BCH code and develop the lower bounds on the minimum distance of $C_{(q,n,\delta)}^\perp$, where $2 \leq \delta \leq n$.

Lemma 4. *Let h be a positive integer and let q be a prime power such that $(q+1) \mid h$. Then h is a coset leader modulo $q^m - 1$ if and only if $\frac{h}{q+1}$ is a coset leader modulo n .*

Proof. We first assume that h is a coset leader modulo $q^m - 1$. If $\frac{h}{q+1}$ is not a coset leader modulo n , then there would be an integer ℓ with $1 \leq \ell \leq m-1$ such that

$$\frac{h}{q+1} q^\ell \bmod n < \frac{h}{q+1},$$

which implies that

$$h q^\ell \bmod q^m - 1 < h.$$

This leads to a contradiction. Hence, $\frac{h}{q+1}$ is a coset leader modulo n . With the same argument, we can see that h is a coset leader modulo $q^m - 1$ if $\frac{h}{q+1}$ is a coset leader modulo n . The proof is then completed. \square

Lemma 5. Let δ_1 be the largest coset leader modulo n , then

$$\delta_1 = \begin{cases} \frac{(q-1)q^{m-1}-q^{\frac{m-2}{2}}-1}{q+1}, & \text{if } m \equiv 2 \pmod{4}, \\ \frac{(q-1)q^{m-1}-q^{\frac{m}{2}}-1}{q+1}, & \text{if } m \equiv 0 \pmod{4}. \end{cases}$$

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 $(q+1) \mid (q^{m-1}+1)$ and $(q+1) \mid (q^{\frac{m}{2}-1}+1)$ by noting that $m \equiv 0 \pmod{4}$. Then

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

which implies that $(q+1) \mid (q+1)q^{m-1} - (2q^{m-1} + q^{\frac{m}{2}} + 1) = (q-1)q^{m-1} - q^{\frac{m}{2}} - 1$. Recall that $(q-1)q^{m-1} - q^{\frac{m}{2}} - 1$ is a coset leader modulo $q^m - 1$ from Lemma 2. It then follows from Lemma 4 that $\frac{(q-1)q^{m-1}-q^{\frac{m}{2}}-1}{q+1}$ is a coset leader modulo n .

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

$$((q+1)\delta' q^\ell \bmod q^m - 1) \geq (q+1)\delta'.$$

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

$$(q+1)\delta' = (q-1)q^{m-1} - 1 \text{ or } (q+1)\delta' = (q-1)q^{m-1} - q^{\frac{m-2}{2}} - 1. \quad (1)$$

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

A conjecture on the largest coset leader modulo n was given in [28] 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 $C_{(q,n,\delta_1)}$.

Lemma 6. Let δ_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 $|C_{\delta}| = \ell$, then

$$\frac{q^m-1}{q+1} \mid \left(\frac{(q-1)q^{m-1}-q^{\frac{m}{2}}-1}{q+1} \right) (q^\ell - 1),$$

which is equivalent to

$$q^m - 1 \mid \left((q-1)q^{m-1} - q^{\frac{m}{2}} - 1 \right) (q^\ell - 1).$$

It then follows from Lemma 2 that $\ell = m$. \square

The following theorem gives the information on the parameters of the BCH code $C_{(q,n,\delta_1)}$, where $n = \frac{q^m-1}{q+1}$.

Theorem 7. *When $m \equiv 2 \pmod{4}$, then the BCH code $C_{(q,n,\delta_1)}$ has parameters*

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

When $m \equiv 0 \pmod{4}$, then the BCH code $C_{(q,n,\delta_1)}$ has parameters

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

Proof. It is straightforward from Lemmas 5 and 6. \square

We inform the reader that Theorem 7 generalizes the results in [28, Theorems 14 and 17], where the only the binary and ternary cases were involved. In this sense, the results documented in [28] 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.*

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

All the four codes are almost optimal according to the tables of best codes known in [14] when the equality holds. These results are verified by Magma programs.

To present a sufficient and necessary condition for $C_{(q,n,\delta)}$ 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 $\frac{q^l+1}{q+1}$, $\frac{q^t-1}{q+1}$, $\frac{\sum_{i=0}^{m-1} q^i}{q+1}$, $\frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1}$ and $\frac{q^m - q^{m-1} - q^{m-2} - 1}{q+1}$ are coset leaders 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

$$\overline{q^m - q^{m-1} - q^{m-2} - 1} = (q-2, q-2, q-1, q-1, \dots, q-1)_q.$$

By Lemma 1, we see that $q^m - q^{m-1} - q^{m-2} - 1$ is a coset leader modulo $q^m - 1$. The desired conclusion then follows from Lemma 4. \square

Lemma 10. *Let δ_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 $2 \leq \delta \leq \frac{q^{\frac{m}{2}-1} + 1}{q+1}$.
- (2) $\delta_1 \in T^\perp$ is a coset leader modulo n if $m \equiv 2 \pmod{4}$, $m \geq 6$ and $2 \leq \delta \leq \frac{q^{\frac{m}{2}} + 1}{q+1}$.

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

Lemma 11. *Let q be an odd prime power. Then $\frac{(q-1)q^3 - q^2 - q - 2}{q+1}$ is the second largest coset leader modulo $\frac{q^4 - 1}{q+1}$.*

Proof. It is easy to see that

$$\overline{(q-1)q^3 - q^2 - q - 2} = (q-2, q-2, q-2, q-2)_q,$$

so $(q-1)q^3 - q^2 - q - 2$ is a coset leader modulo $q^4 - 1$. From Lemma 4, 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 $\frac{(q-1)q^3 - q^2 - q - 2}{q+1}$ is the second largest coset leader modulo $\frac{q^4 - 1}{q+1}$. If there exists a coset leader δ' 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 ℓ with $1 \leq \ell \leq m-1$, we have $(\delta' q^\ell \bmod \frac{q^m - 1}{q+1}) \geq \delta'$, which implies that

$$((q+1)\delta' q^\ell \bmod q^m - 1) \geq (q+1)\delta'.$$

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 $q^4 - 1$ are $(q-2, q-1, q-1, q-1)_q$, $(q-2, q-1, q-2, q-1)_q$, $(q-2, q-2, q-1, q-1)_q$, $(q-2, q-2, q-2, q-1)_q$ and $(q-2, q-2, q-2, q-2)_q$, respectively. Then the first five largest coset leaders modulo $q^4 - 1$ are $(q-1)q^3 - 1$, $(q-1)q^3 - q - 1$, $(q-1)q^3 - q^2 - 1$, $(q-1)q^3 - q^2 - q - 1$ and

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

$$(q+1)\delta' = (q-1)q^3 - q - 1, \text{ or } (q+1)\delta' = (q-1)q^3 - q^2 - 1, \text{ or } (q+1)\delta' = (q-1)q^3 - q^2 - q - 1. \quad (2)$$

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

Lemma 12. *Let $q > 2$ be a prime power and $m \geq 4$ be even. Let δ_1 be given as in Lemma 5. Then the following hold.*

- (1) $\frac{(q-1)q^3 - q^2 - q - 2}{q+1} \in T^\perp$ is a coset leader modulo n if $m = 4$ and $2 \leq \delta \leq q^2 + 1$.
- (2) $\frac{\sum_{i=0}^{m-1} q^i}{q+1} \in T^\perp$ is a coset leader modulo n if $2 \leq \delta \leq \frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1}$.
- (3) $2 \notin T^\perp$ is a coset leader modulo n if $\frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1} < \delta \leq \delta_1$.

Proof. From Lemma 4 and Lemma 11, it is easy to get that $\frac{(q-1)q^3 - q^2 - q - 2}{q+1}$, $\frac{\sum_{i=0}^{m-1} q^i}{q+1}$, and 2 are coset leaders modulo n .

When $m = 4$ and $2 \leq \delta \leq q^2 + 1$, it follows from Lemma 9 that $\frac{q^3 + q^2 + q + 1}{q+1} = q^2 + 1$ is a coset leader modulo $\frac{q^4 - 1}{q+1}$. This means that $q^2 + 1 \notin T$ in this case. Hence,

$$\frac{(q-1)q^3 - q^2 - q - 2}{q+1} = n - (q^2 + 1) \notin T^{-1} \text{ and } \frac{(q-1)q^3 - q^2 - q - 2}{q+1} \in Z_n \setminus T^{-1} = T^\perp.$$

When $2 \leq \delta \leq \frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1}$, we see from Lemma 9 that $\frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1}$ is a coset leader modulo n . Then $\frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1} \notin T$. Hence,

$$\frac{\sum_{i=0}^{m-1} q^i}{q+1} = n - \frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1} \notin T^{-1} \text{ and } \frac{\sum_{i=0}^{m-1} q^i}{q+1} \in Z_n \setminus T^{-1} = T^\perp.$$

When $\frac{(q-2)(\sum_{i=0}^{m-1} q^i)}{q+1} < \delta \leq \delta_1$, it is easy to see that

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

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 -cyclotomic coset modulo n . Then we have $n - 2 \in T$, i.e., $2 \in T^{-1}$. Hence, $2 \notin T^\perp = Z_n \setminus T^{-1}$. \square

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 $\frac{\sum_{i=0}^{m-5} 2^i}{3}$.*

Proof. Let $M = 2^8 + 2^6 + 2^5 + 2^4 + 2^2 + 2 + 1 = (0, 1, 0, 1, 1, 1, 0, 1, 1, 1)_2$ if $m = 10$, and

$$\begin{aligned} M &= 2^{m-2} + \sum_{i=0}^1 (2^{m-4-4i} + 2^{m-5-4i} + 2^{m-6-4i}) + \sum_{i=0}^{\frac{m-13}{3}} (2^{m-12-3i} + 2^{m-13-3i}) \\ &= (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, \underline{0, 1, 1}, \underline{0, 1, 1}, \dots, \underline{0, 1, 1})_2 \end{aligned}$$

if $m \equiv 1 \pmod{3}$ and $m \neq 10$, and

$$M = \begin{cases} \sum_{i=0}^{\frac{m-2}{2}} 2^{2i} = (0, 1, 0, 1, \dots, 0, 1)_2, & \text{if } m \equiv 0 \pmod{3}, \\ \sum_{i=1}^{\frac{m-2}{2}} 2^{2i} + 2 + 1 = (\underline{0, 1, 0, 1}, \dots, \underline{0, 1, 1, 1})_2, & \text{if } m \equiv 2 \pmod{3}. \end{cases}$$

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 4, $\frac{M}{3}$ is a coset leader modulo n .

Since $\frac{M}{3} > \frac{2^{m-2}-1}{3}$, we have $M \notin T$. If $m = 10$, then

$$\frac{2^3(2^6 + 2^4 + 1)}{3} = n - M \notin T^{-1} \text{ and } \frac{2^6 + 2^2 + 1}{3} \in Z_n \setminus T^{-1} = T^\perp$$

since $\frac{2^6 + 2^2 + 1}{3}$ and $\frac{2^6 + 2^4 + 1}{3}$ are in the same coset modulo n . If $m \equiv 1 \pmod{3}$ and $m \neq 10$, then

$$\frac{2^2(2^{m-3} + 2^{m-5} + 2^{m-9} + \sum_{i=0}^{\frac{m-13}{3}} 2^{3i})}{3} = n - M \notin T^{-1} \text{ and}$$

$$\frac{2^{m-4} + \sum_{i=0}^{\frac{m-13}{3}} 2^{3i+5} + 2^2 + 1}{3} \in Z_n \setminus T^{-1} = T^\perp$$

since $\frac{2^{m-3} + 2^{m-5} + 2^{m-9} + \sum_{i=0}^{\frac{m-13}{3}} 2^{3i}}{3}$ and $\frac{2^{m-4} + \sum_{i=0}^{\frac{m-13}{3}} 2^{3i+5} + 2^2 + 1}{3}$ are in the same coset modulo n .

Similarly, we have

$$\begin{cases} \frac{\sum_{i=0}^{\frac{m-2}{2}} 2^{2i}}{3} \in Z_n \setminus T^{-1} = T^\perp, & \text{if } m \equiv 0 \pmod{3}, \\ \frac{\sum_{i=0}^{\frac{m-4}{2}} 2^{2i}}{3} \in Z_n \setminus T^{-1} = T^\perp, & \text{if } m \equiv 2 \pmod{3}. \end{cases}$$

Let

$$L = \begin{cases} 2^6 + 2^2 + 1, & \text{if } m = 10, \\ \sum_{i=0}^{\frac{m-2}{2}} 2^{2i}, & \text{if } m \equiv 0 \pmod{3}, \\ 2^{m-4} + \sum_{i=0}^{\frac{m-13}{3}} 2^{3i} + 2^2 + 1, & \text{if } m \equiv 1 \pmod{3} \text{ and } m \neq 10, \\ \sum_{i=0}^{\frac{m-4}{2}} 2^{2i}, & \text{if } m \equiv 2 \pmod{3}. \end{cases}$$

It is easy to check that L is a coset leader modulo $2^m - 1$. From Lemma 4, $\frac{L}{3}$ is a coset leader modulo n . It is obvious that $\frac{L}{3} > \frac{\sum_{i=0}^{m-5} 2^i}{3}$. The desired conclusion then follows. \square

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 $\{0, 1, 2, \dots, I(\delta) - 1\} \subseteq T^\perp$ and $I(\delta) \notin T^\perp$. Then we have $I(\delta) = \frac{q^{m-t}-1}{q+1}$ if $\frac{q^t-1}{q+1} < \delta \leq \frac{q^{t+1}+2q^t-1}{q+1}$.

Proof. When $\frac{q^t-1}{q+1} < \delta \leq \frac{q^{t+1}+2q^t-1}{q+1}$, it is straightforward to see that

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

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

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

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

and the sequence of $(q+1) \cdot q^t u + q^t - 1$ is

$$\underbrace{(i_{m-1}, i_{m-2}, \dots, i_t)}_{m-t}, \underbrace{(q-1, \dots, q-1)}_t,$$

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 cyclotomic 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 that

$$\text{CL} \left(\frac{(q+1) \cdot q^t u + q^t - 1}{q+1} \right) \geq \frac{q^{t+1} + 2q^t - 1}{q+1} > \delta - 1,$$

where $\text{CL} \left(\frac{(q+1) \cdot q^t u + q^t - 1}{q+1} \right)$ denotes the coset leader of the 2-cyclotomic coset modulo n containing $\frac{(q+1) \cdot q^t u + q^t - 1}{q+1}$. Consequently, $\frac{(q+1) \cdot q^t u + q^t - 1}{q+1} \notin T$ and $\frac{q^{m-t}-1}{q+1} - u \notin T^{-1}$. This leads to $i = \frac{q^{m-t}-1}{q+1} - u \in T^\perp$. It then follows that $I(\delta) = \frac{q^{m-t}-1}{q+1}$ for any δ with $\frac{q^t-1}{q+1} < \delta \leq \frac{q^{t+1}+2q^t-1}{q+1}$. The proof is then completed. \square

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

Proof. From the BCH bound, in order to obtain the desired result, we only need to show that $\{0, 1, 2, \dots, \frac{q^{m-1}+2q^{m-2}-1}{q+1} - 1\} \subseteq T^\perp$.

It is clear that $0 \in T^\perp$. For every integer i with $1 \leq i \leq \frac{q^{m-1}+2q^{m-2}-1}{q+1} - 1$, we have $i = \frac{q^{m-1}+2q^{m-2}-1}{q+1} - u$, where $1 \leq u \leq \frac{q^{m-1}+2q^{m-2}-1}{q+1} - 1$. Since $q+1 \mid q^{m-1} + 2q^{m-2} - 1$ and $q+1 \mid q^m - 1$, if there exist $0 < t \leq q-1$ and $0 \leq i \leq m-1$ such that

$$q^{m-1} + 2q^{m-2} - 1 - u(q+1) \equiv tq^i \pmod{q^m - 1},$$

then $q+1 \mid tq^i$, which is impossible. Hence,

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

where $\text{CL}\left(\frac{q^{m-1} + 2q^{m-2} - 1 - u(q+1)}{q+1}\right)$ denotes the coset leader of the 2-cyclotomic coset modulo n containing $\frac{q^{m-1} + 2q^{m-2} - 1 - u(q+1)}{q+1}$. Consequently, $\frac{q^{m-1} + 2q^{m-2} - 1 - u(q+1)}{q+1} \notin T$ and $\frac{q^{m-1} + 2q^{m-2} - 1}{q+1} - u \notin T^{-1}$. This leads to $i = \frac{q^{m-1} + 2q^{m-2} - 1}{q+1} - u \in T^\perp$. From the BCH bound, the desired conclusion then follows. \square

Let $2 \leq \delta' \leq \delta'' \leq n$, it is clear that $C_{(q,n,\delta'')} \subseteq C_{(q,n,\delta')}$. Then we have $C_{(q,n,\delta'')}^\perp \supseteq C_{(q,n,\delta')}^\perp$, which implies that $d(C_{(q,n,\delta'')}^\perp) \leq d(C_{(q,n,\delta')}^\perp)$. 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 $C_{(q,n,\delta)}^\perp$.

Theorem 16. Let $2 \leq \delta \leq n$, $0 \leq t \leq m-2$ and $d^\perp(\delta)$ be the minimum distance of $C_{(q,n,\delta)}^\perp$. Let $q=2$, then we have $d^\perp(\delta) \geq \frac{2^{m-t}-1}{3} + 1$ if $\frac{2^t-1}{3} < \delta \leq \frac{2^{t+2}-1}{3}$. Let $q > 2$ be a prime power, then we have

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

It is very hard to determine the minimum distance of $C_{(q,n,\delta)}^\perp$ 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 minimum distance of the lower bound of $C_{(3,20,2)}^\perp$ is 11. By Magma, the true minimum distance of $C_{(3,20,2)}^\perp$ is 12.

Example 18. Let $\delta = 2$, $q = 2$ and $m = 6$. In theorem 16, the minimum distance of the lower bound of $C_{(2,21,2)}^\perp$ is 6. By Magma, the true minimum distance of $C_{(2,21,2)}^\perp$ is 8.

We now give the sufficient and necessary condition for $C_{(q,n,\delta)}$ 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 $C_{(q,n,\delta)}$ is a dually-BCH code if and only if $\delta_1 + 1 \leq \delta \leq n$, where δ_1 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 $n-1 \in T^{-1}$. Furthermore, we have $0 \in T^\perp$, which means that C_0 must be the initial cyclotomic coset of T^\perp . In other words, there must be an integer $J \geq 1$ such that $T^\perp = C_0 \cup C_1 \cup \dots \cup C_{J-1}$ if $C_{(q,n,\delta)}$ is a dually-BCH code.

When $\delta_1 + 1 \leq \delta \leq n$, it is easily seen that $T^\perp = \{0\}$ and $C_{(q,n,\delta)}^\perp$ is a BCH code with respect to β since δ_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 three cases.

Case 1: $2 \leq \delta \leq 3$. From Lemma 10 and $0 \in T^\perp$, we know that $T^\perp = C_0 \cup C_1 \cup \dots \cup C_{\delta_1} = Z_n$ if $C_{(2,n,\delta)}^\perp$ is a BCH code, which leads to $C_{(2,n,\delta)} = \{0\}$. It is obvious that $C_{(2,n,\delta)} \neq \{0\}$, which is a contradiction.

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

$$2^{m-2} + 2^{m-4} + \sum_{i=0}^{m-6} 2^i = (0, 1, 0, 1, 0, \underbrace{1, \dots, 1}_{m-5})_2$$

is a coset leader modulo $2^m - 1$. From Lemma 4, we know that $\frac{2^{m-2} + 2^{m-4} + \sum_{i=0}^{m-6} 2^i}{3}$ is a coset leader modulo $\frac{2^m-1}{3}$. Obviously, $21 = (0, \dots, 0, 1, 0, 1, 0, 1)_2$ is a coset leader modulo $2^m - 1$, then 7 is a coset leader modulo $\frac{2^m-1}{3}$ from Lemma 4. Since $7 \cdot 2^{m-5} \notin T$, we have

$$\frac{2^{m-2} + 2^{m-4} + \sum_{i=0}^{m-6} 2^i}{3} = n - 7 \cdot 2^{m-5} \notin T^{-1} \text{ and } \frac{2^{m-2} + 2^{m-4} + \sum_{i=0}^{m-6} 2^i}{3} \in Z_n \setminus T^{-1} = T^\perp.$$

It is easy to check that

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

It then follows that there is no integer $J \geq 1$ such that $T^\perp = C_0 \cup C_1 \cup \dots \cup C_{J-1}$, i.e., $C_{(q,n,\delta)}^\perp$ is not a BCH code with respect to β .

Case 3: $7 < \delta \leq \frac{2^{m-2}-1}{3}$. It is clear that $5 = \frac{2^3+2^2+2+1}{3} \in T$, then

$$\frac{2^4(\sum_{i=0}^{m-5} 2^i)}{3} = n - 5 \in T^{-1} \text{ and } \frac{\sum_{i=0}^{m-5} 2^i}{3} \in Z_n \setminus T^{-1} \notin T^\perp.$$

From Lemma 13, there is no integer $J \geq 1$ such that $T^\perp = C_0 \cup C_1 \cup \dots \cup C_{J-1}$, i.e., $C_{(q,n,\delta)}^\perp$ is not a BCH code with respect to β .

Case 4: $\frac{2^{m-2}-1}{3} < \delta \leq \delta_1$. Since $1 \notin T^\perp$, we have $C_{(2,n,\delta)}^\perp = \{0\}$ if $C_{(2,n,\delta)}^\perp$ is a BCH code with respect to β . However, the dimension of $C_{(2,n,\delta)}$ is $\dim(C_{(2,n,\delta)}) \leq n - |C_{\delta_1}| < n$, which is contradictory to $\dim(C_{(2,n,\delta)}) + \dim(C_{(2,n,\delta)}^\perp) = n$.

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

Theorem 20. Let $n = \frac{q^m - 1}{q + 1}$, where $q > 2$ is a prime power and $m \geq 4$ is even. Let δ_1 be given in Lemma 5. Then the following statements hold.

(1) If $m = 4$, then $C_{(q,n,\delta)}$ is a dually-BCH code if and only if

$$\delta = 2, \delta_1 \leq \delta \leq n.$$

(2) If $m \neq 4$, then $C_{(q,n,\delta)}$ 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 $C_{(q,n,\delta)}^\perp$ is a BCH code with respect to β . It remains to show that whether $C_{(q,n,\delta)}^\perp$ is a BCH code with respect to β for $2 \leq \delta \leq \delta_1$. We have the following four cases.

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

$$n - q^{m-2} = \frac{q^m - q^{m-1} - q^{m-2} - 1}{q + 1} \in T^{-1}.$$

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

If $m = 4$, then $\delta' = \delta_1$, i.e., $T^{-1} = C_{\delta_1}$. Hence, $T^\perp = Z_n \setminus T^{-1} = C_0 \cup C_1 \cup \dots \cup C_{\delta_1-1}$. This means that $C_{(2,n,\delta)}^\perp = C_{(2,n,\delta_1+1,0)}$ is a BCH code with the designed distance $\delta_1 + 1$ with respect to β .

If $m \neq 4$, then $\delta' < \delta_1$. Since δ' and δ_1 are not in the same coset, then $\delta_1 \notin T^{-1}$, i.e., $\delta_1 \in Z_n \setminus T^{-1} = T^\perp$. It then follows $T^\perp = C_0 \cup C_1 \cup \dots \cup C_{\delta_1} = Z_n$ if $C_{(2,n,\delta)}^\perp$ is a BCH code. This means that $C_{(2,n,\delta)} = \{0\}$ 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

$$T^\perp \supseteq C_0 \cup C_1 \cup \dots \cup C_{\frac{(q-1)q^3 - q^2 - q - 2}{q+1}}$$

if $C_{(2,n,\delta)}^\perp$ is a BCH code. From Lemma 11, we know that the dimension of $C_{(2,n,\delta)}^\perp$ is

$$\dim(C_{(2,n,\delta)}^\perp) \geq \frac{q^4 - 1}{q + 1} - |C_{\delta_1}| - |C_0| = \frac{q^4 - 1}{q + 1} - 5 \quad (3)$$

since $|C_{\delta_1}| = 4$. It is easy to check that $|C_1| = |C_2| = 4$, then $\dim(C_{(2,n,\delta)}) \geq |C_2| + |C_3| \geq 8$. From

(3), we know that $\dim(C_{(2,n,\delta)}) = \frac{q^4 - 1}{q + 1} - \dim(C_{(q,n,\delta)}^\perp) \leq 5$ and this leads to a contradiction.

Hence, $C_{(q,n,\delta)}^\perp$ is not a BCH code.

If $m \neq 4$, from Lemma 10 and $0 \in T^\perp$, we know that $T^\perp = C_0 \cup C_1 \cup \dots \cup C_{\delta_1} = \mathbb{Z}_n$ if $C_{(2,n,\delta)}^\perp$ is a BCH code, which leads to $C_{(2,n,\delta)} = \{\mathbf{0}\}$. It is obvious that $C_{(2,n,\delta)} \neq \{\mathbf{0}\}$, 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

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

Hence, $\frac{q^{m-2}-1}{q+1} = n - \frac{(q^m - q^{m-2})}{q+1} \in T^{-1}$ and $\frac{q^{m-2}-1}{q+1} \notin T^\perp = \mathbb{Z}_n \setminus T^{-1}$. From Lemma 12, we know that $\frac{\sum_{i=0}^{m-1} q^i}{q+1} \in T^\perp$ is the coset leader modulo n . It is clear that $\frac{q^{m-2}-1}{q+1} < \frac{\sum_{i=0}^{m-1} q^i}{q+1}$. It then follows that there is no integer $J \geq 1$ such that $T^\perp = C_0 \cup C_1 \cup \dots \cup C_{J-1}$, i.e., $C_{(q,n,\delta)}^\perp$ is not a BCH code with respect to β .

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., $n - \delta_1 \in \mathbb{Z}_n \setminus T^{-1} = T^\perp$. Obviously, we have

$$n - \delta_1 = \frac{q^{m-1} + q^{\frac{m}{2}}}{q+1} = \frac{q^{\frac{m}{2}}(q^{\frac{m}{2}-1} + 1)}{q+1} \in C_{\frac{q^{\frac{m}{2}-1} + 1}{q+1}}$$

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

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

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

IV. BCH CODES 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, we first consider the parameters of the BCH code $C_{(q,n,\delta_1)}$, and then show a sufficient and necessary condition for $C_{(q,n,\delta)}$ being a dually-BCH code, where $2 \leq \delta \leq n$ and δ_1 is the largest coset leader modulo n . It is clear that the defining set of $C_{(q,n,\delta)}$ with respect to β is $T = C_1 \cup C_2 \cup \dots \cup C_{\delta-1}$. As before, denote by T^\perp the defining set of the dual code $C_{(q,n,\delta)}^\perp$ with respect to β . Then $T^\perp = \mathbb{Z}_n \setminus T^{-1}$ and $0 \in T^\perp$.

Lemma 21. Let $q \geq 3$ be a prime power and $m \geq 4$ an integer. Let $q-1 = mt_1 + t_2$, where $t_1 \geq 0$ and $m > t_2 \geq 0$. Assume that $\Upsilon = \{\lceil \frac{mt}{q-1} \rceil - 1, \gamma = 1, 2, \dots, t_2\}$ if $t_2 \neq 0$. Let

$$\sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} \rceil - 1} = a_{m-1}q^{m-1} + a_{m-2}q^{m-2} + \dots + a_1q + a_0.$$

If $t_2 = 0$, then $a_i = \frac{q-1}{m}$ for all $i \in [0, m-1]$. If $t_2 \neq 0$, then $a_i = \lceil \frac{q-1}{m} \rceil$ if $i \in \Upsilon$, $a_i = \lfloor \frac{q-1}{m} \rfloor$ if $i \in [0, m-1] \setminus \Upsilon$ and $\sum_{i=0}^{m-1} a_i = q-1$.

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 $a_0 = a_1 = \dots = a_{m-1} = \frac{q-1}{m}$. 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 $\lceil \frac{mt}{q-1} \rceil$ for $t \in [1, q-1]$. There are four cases.

Case 1: $t \in [1, it_1 + u_i]$. It is clear that

$$\left\lceil \frac{mt}{q-1} - 1 \right\rceil \leq \left\lceil \frac{m(it_1 + u_i)}{q-1} - 1 \right\rceil.$$

Since $mt_1 = q-1 - t_2$ and $mu_i = it_2 - v_i$, we obtain

$$\left\lceil i-1 + \frac{mu_i - it_2}{q-1} \right\rceil = \left\lceil i-1 - \frac{v_i}{q-1} \right\rceil = i-1.$$

In this case, we have $\lceil \frac{mt}{q-1} - 1 \rceil \leq i-1$.

Case 2: $t \in [it_1 + u_i + 1, (i+1)t_1 + u_i]$. 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

$$\left\lceil \frac{mt}{q-1} - 1 \right\rceil = \left\lceil i-1 + \frac{mu_i + mg - it_2}{q-1} \right\rceil = \left\lceil i-1 + \frac{mg - v_i}{q-1} \right\rceil.$$

It is clear that $0 < mg - v_i < q-1$, then $\lceil \frac{mt}{q-1} - 1 \rceil = i$.

Case 3: $t = it_1 + u_i + t_1 + 1$. From $mt_1 = q-1 - t_2$ and $mu_i = it_2 - v_i$, we have

$$\frac{mt}{q-1} = i + \frac{t_1m + m - v_i}{q-1},$$

Then $\lceil \frac{mt}{q-1} - 1 \rceil = i$ if $m - v_i \leq t_2$, and $\lceil \frac{mt}{q-1} - 1 \rceil = i+1$ if $m - v_i > t_2$.

Case 4: $t \in [it_1 + u + t_1 + 2, q-1]$. Similar as above, it is easy to get that

$$\left\lceil \frac{mt}{q-1} - 1 \right\rceil \geq i+1.$$

From above four cases, we know that

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

When i runs over $[0, m-1]$, note that $t_1 = \lfloor \frac{q-1}{m} \rfloor$ and $t_1 + 1 = \lceil \frac{q-1}{m} \rceil$, it is easy to get that

$$a_i = \begin{cases} \lceil \frac{q-1}{m} \rceil, & \text{if } 0 < m - v_i \leq t_2, \\ \lfloor \frac{q-1}{m} \rfloor, & \text{if } t_2 < m - v_i \end{cases}$$

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

$$\frac{m(u_i + 1)}{t_2} - 1 \leq i < \frac{m(u_i + 1)}{t_2},$$

which implies that $i = \lceil \frac{m(u_i + 1)}{t_2} - 1 \rceil$. This means that $a_i = \lceil \frac{q-1}{m} \rceil$ if and only if $i \in \Upsilon$. The desired conclusion then follows. \square

Lemma 22. Let $t_2 \neq 0$ and $N_\gamma^\xi = \lceil \frac{m\gamma}{t_2} - 1 \rceil - \lceil \frac{m(\gamma - \xi)}{t_2} - 1 \rceil$, where $1 \leq \xi \leq t_2$ and $1 \leq \gamma \leq t_2$. Then the following statements hold.

1. If $t_2 \mid m$, then $N_i^\xi = N_j^\xi$, where $1 \leq i, j \leq t_2$.
2. If $t_2 \nmid m$, then $N_\gamma^\xi - N_{t_2}^\xi = 0$ or 1. Moreover, there exists $1 \leq \xi_0 \leq t_2$ such that $N_\gamma^{\xi_0} = N_{t_2}^{\xi_0}$.

Proof. If $t_2 \mid m$, the desired conclusion follows from the definition of N_γ^ξ , directly. Next, we give the proof for the case $t_2 \nmid m$. By the definition of N_γ^ξ , it is easy to get that

$$\frac{m\xi_0}{t_2} - 1 = \frac{m\gamma}{t_2} - 1 - \left(\frac{m(\gamma - \xi)}{t_2} \right) < N_\gamma^\xi < \frac{m\gamma}{t_2} - \left(\frac{m(\gamma - \xi)}{t_2} - 1 \right) = \frac{m\xi_0}{t_2} + 1.$$

Similarly, we have

$$\frac{m\xi}{t_2} - 1 < N_{t_2}^\xi < \frac{m\xi}{t_2}.$$

Then $N_\gamma^\xi - N_{t_2}^\xi = 0$ or 1. When $\xi = t_2$ we have $N_\gamma^\xi = N_{t_2}^{\xi_0} = m$, then there must exist $\xi_0 \in [1, t_2]$ such that $N_\gamma^{\xi_0} = N_{t_2}^{\xi_0}$. The proof is then completed. \square

Lemma 23. Let $q \geq 3$ be a prime power and $m \geq 4$ be an integer. Then $\theta = q^{m-1} - 1 - \frac{(\sum_{t=1}^{q-2} q^{\lceil \frac{mt}{q-1} - 1 \rceil - q + 2})}{q-1}$ is a coset leader modulo n .

Proof. Note that

$$\theta q^i \pmod{n} \geq \theta \Leftrightarrow \theta(q-1)q^i \pmod{q^m-1} \geq \theta(q-1) \quad (4)$$

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

$$\theta = q^{m-1} - 1 - \frac{(\sum_{t=1}^{q-2} q^{\lceil \frac{mt}{q-1} \rceil - 1} - q + 2)}{q-1} = \frac{q^m - \sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} \rceil - 1} - 1}{q-1}.$$

Then by Lemma 21 we have

$$\theta(q-1) = q^m - a_{m-1}q^{m-1} - a_{m-2}q^{m-2} - \cdots - a_1q - a_0 - 1 \quad (5)$$

and

$$\begin{aligned} \theta(q-1)q^i \pmod{q^m-1} &= q^m - a_{m-i-1}q^{m-1} - \cdots - a_1q^{i+1} - a_0q^i - \\ &\quad a_{m-1}q^{i-1} - \cdots - a_{m+1-i}q - a_{m-i} - 1. \end{aligned} \quad (6)$$

For the sake of narrative, we denote $\theta' = (q-1)\theta$. If $m|(q-1)$, 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 θ is a coset leader modulo n . If $m \nmid (q-1)$, we have the following three cases.

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

Case 2: $i \in \Upsilon$ and $t_2|m$. Put $1 \leq h \leq m$. From Lemma 21, we know that

$$a_{h-1} = \begin{cases} \lceil \frac{q-1}{m} \rceil, & \text{if } \frac{m}{t_2} | h, \\ \lfloor \frac{q-1}{m} \rfloor, & \text{if } \frac{m}{t_2} \nmid h. \end{cases}$$

Let $h_1 = (\overline{h-i})_m$, then $a_h = a_{h_1}$. Hence, the sequences of

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

and

$$(a_{m-i-1}, a_{m-i-2}, \cdots, a_{m+1-i}, a_{m-i})_q$$

are the same. From (5) and (6), we have $\theta'q^i \pmod{q^m-1} = \theta'$.

Case 3: $i \in \Upsilon$ and $t_2 \nmid m$. From Lemma 21, let $0 \leq h \leq m-1$, we know that $a_h = \lceil \frac{q-1}{m} \rceil$ if and only if $h = \lceil \frac{m(t_2-l)}{t_2} - 1 \rceil$ and $a_h = \lfloor \frac{q-1}{m} \rfloor$ for the other values of h , where $l \in [0, t_2-1]$. It is easy to check that

$$m-1 - \left\lceil \frac{m(t_2-l)}{t_2} - 1 \right\rceil = m-1 - \left\lceil m-1 - \frac{ml}{t_2} \right\rceil = \left\lfloor \frac{ml}{t_2} \right\rfloor.$$

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

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

can be expressed as

$$\underbrace{(ab, \dots, b, a, b, \dots, b, a, \dots, a, \dots, b, a, b, \dots, b)}_{\lfloor \frac{m}{t_2} \rfloor - 1} \underbrace{\dots}_{\lfloor \frac{2m}{t_2} \rfloor - 1} \dots \underbrace{\dots}_{\lfloor \frac{m(t_2-1)}{t_2} \rfloor - 1}.$$

Since $i \in \Upsilon$, we can assume that $m-1-i = \lceil \frac{m\gamma_1}{t_2} - 1 \rceil$, where $\gamma_1 \in [1, t_2-1]$. Moreover, we have

$$\left\lceil \frac{m\gamma_1}{t_2} - 1 \right\rceil - \left\lceil \frac{m(\gamma_1 + l)}{t_2} - 1 \right\rceil \leq \left\lfloor \frac{ml}{t_2} \right\rfloor.$$

Then the sequence of

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

can be expressed as

$$\underbrace{(ab, \dots, b, a, b, \dots, b, a, \dots, a, \dots, b, a, b, \dots, b)}_{\leq \lfloor \frac{m}{t_2} \rfloor - 1} \underbrace{\dots}_{\leq \lfloor \frac{2m}{t_2} \rfloor - 1} \dots \underbrace{\dots}_{\leq \lfloor \frac{m(t_2-1)}{t_2} \rfloor - 1}.$$

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 θ is a coset leader modulo n from (4). This completes the proof. \square

Let

$$M = q^m - \sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} \rceil - 1} - 1 + \mu(q-1) \quad (7)$$

and $0 < \mu < \frac{\sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} \rceil - 1}}{q-1}$. By the definition of μ , we know that μ can be expressed as

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

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

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

By Lemma 21, we have

$$M = q^m - (a_{m-1} - b_{m-2})q^{m-1} - (a_{m-2} + b_{m-2} - b_{m-3})q^{m-2} - \dots - (a_1 + b_1 - b_0)q - a_0 - b_0 - 1. \quad (8)$$

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 $b_{m-2} > 0$, $0 \leq a_0 + b_0 < q$ and $0 \leq a_i + b_i - b_{i-1} < q$ for $i \in [1, m-2]$, then M is not a coset leader modulo $q^m - 1$.*

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

$$b_{m-2} + a_{m-2} - b_{m-3} = a_{m-1} + a_{m-2} - b_{m-3} \leq 2\lceil \frac{q-1}{m} \rceil - b_{m-3} \leq \frac{q+1}{2} \leq q-1.$$

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 $a_{m-1} = \lceil \frac{q-1}{m} \rceil$. Let

$$a = a_{m-1} - b_{m-2}, \quad (9)$$

then $0 < a < \lceil \frac{q-1}{m} \rceil$. 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 $Mq^{i_0} \pmod{q^m - 1} < M$.

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

$$\begin{cases} a_{m-2} + b_{m-2} - b_{m-3} \leq a, \\ a_{m-3} + b_{m-3} - b_{m-4} \leq a, \\ \vdots \\ a_1 + b_1 - b_0 \leq a, \end{cases} \quad (10)$$

then by (9) and (10) we have

$$a_{m-1} + a_{m-2} + \dots + a_2 + a_1 - b_0 \leq (m-1)a,$$

i.e.,

$$a_{m-1} + a_{m-2} + \dots + a_2 + a_1 + a_0 - a_0 - b_0 \leq (m-1)a. \quad (11)$$

Since $\sum_{i=0}^{m-1} a_i = q - 1$ and $a < \lceil \frac{q-1}{m} \rceil$, from (11) we have

$$b_0 + a_0 \geq q - 1 - (m - 1)a > a.$$

From (8) we know that $Mq^{m-1} \pmod{q^m - 1} < M$. The desired conclusion then follows. \square

Lemma 25. *Let the notation be given as above. If $b_{m-2} = 0$, $0 \leq a_0 + b_0 < q$ and $0 \leq a_i + b_i - b_{i-1} < q$ for $i \in [1, m-2]$, then M is not a coset leader modulo $q^m - 1$.*

Proof. If M is a coset leader modulo $q^m - 1$, then $M \leq Mq^i \pmod{q^m - 1}$ for $i \in [1, m-1]$.

From Lemma 21 and the definition of M , we have

$$\begin{cases} a_{m-2} - b_{m-3} \leq \lceil \frac{q-1}{m} \rceil, \\ b_{m-3} + a_{m-3} - b_{m-4} \leq \lceil \frac{q-1}{m} \rceil, \\ \vdots \\ b_1 + a_1 - b_0 \leq \lceil \frac{q-1}{m} \rceil, \\ a_0 + b_0 \leq \lceil \frac{q-1}{m} \rceil. \end{cases} \quad (12)$$

If $m \mid (q-1)$, we have $\lceil \frac{q-1}{m} \rceil = \frac{q-1}{m}$. Then from (12) and $a_i = \frac{q-1}{m}$ for all $i \in [0, m-1]$, we have

$$b_0 = b_1 = \dots = b_{m-3} = 0.$$

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 $m \nmid (q-1)$. In this case, we have $\lceil \frac{q-1}{m} \rceil - \lfloor \frac{q-1}{m} \rfloor = 1$. By Lemma 21, we know that $a_0 = \lfloor \frac{q-1}{m} \rfloor$. Then $b_0 = 0$ or $b_0 = 1$.

Case 1: $b_0 = 1$. Recall that

$$M = q^m - (a_{m-1} - b_{m-2})q^{m-1} - (b_{m-2} + a_{m-2} - b_{m-3})q^{m-2} - \dots - (b_1 + a_1 - b_0)q - a_0 - b_0 - 1. \quad (13)$$

Then

$$\begin{aligned} q^{m-1}M \pmod{q^m - 1} &= q^m - (b_0 + a_0)q^{m-1} - (a_{m-1} - b_{m-2})q^{m-2} - \dots - (b_2 + a_2 - b_1)q \\ &\quad - (b_1 + a_1 - b_0) - 1. \end{aligned} \quad (14)$$

If $M \leq q^{m-1}M$, by comparing (13) and (14), we know that

$$a_{m-1} = a_{m-2} = \dots = a_1 = \left\lceil \frac{q-1}{m} \right\rceil \text{ and } b_0 = b_1 = \dots = b_{m-3} = 0$$

since $b_{m-2} = 0$ and $\lceil \frac{q-1}{m} \rceil \leq a_i \leq \lfloor \frac{q-1}{m} \rfloor$. Then we obtain that $\mu = 0$, which is contradictory to $\mu > 0$. Hence, we have $M > q^{m-1}M \pmod{q^m - 1}$.

Case 2: $b_0 = 0$. From (12), we know that $b_1 = 0$ or $b_1 = 1$. If $b_1 = 0$, then from (12) 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 Υ is defined in Lemma 21. If $i_1 \in \Upsilon$, then we have $b_{i_1-1} = 0$, $b_{i_1} = 1$ and $a_{i_1} = \lceil \frac{q-1}{m} \rceil$, which is contradictory to $a_{i_1} + b_{i_1} - b_{i_1-1} \leq \lceil \frac{q-1}{m} \rceil$. Hence, we obtain that $i_1 \in [0, m-1] \setminus \Upsilon$. This means that there is $\gamma_2 \in [0, t_2-1]$ satisfying $\lceil \frac{\gamma_2 m}{t_2} - 1 \rceil < i_1 < \lceil \frac{(\gamma_2+1)m}{t_2} - 1 \rceil$. For the sake of narrative, we assume that $b_{m-1} = b_{-1} = 0$ in the following of this proof.

Subcase 1: $\lceil \frac{\gamma_2 m}{t_2} - 1 \rceil < i_1 < \lceil \frac{(\gamma_2+1)m}{t_2} - 1 \rceil - 1$. Let $\xi = m - i_1 - 1 + \lceil \frac{\gamma_2 m}{t_2} - 1 \rceil$. It is clear that M and $q^{m-i_1-1}M$ can be expressed as

$$\begin{aligned} M = & q^m - (a_{m-1} - b_{m-2})q^{m-1} - (a_{m-2} + b_{m-2} - b_{m-3})q^{m-2} - \cdots - (b_\xi + a_\xi - b_{\xi-1})q^\xi - \cdots \\ & - (b_1 + a_1 - b_0)q - a_0 - b_0 - 1, \end{aligned} \quad (15)$$

and

$$\begin{aligned} q^{m-i_1-1}M \pmod{q^m - 1} = & q^m - (a_{i_1} + b_{i_1} - b_{i_1-1})q^{m-1} - (a_{i_1-1} + b_{i_1-1} - b_{i_1-2})q^{m-2} - \cdots \\ & - (a_{\lceil \frac{(\gamma_2-1)t_2 m+m}{t_2} - 1 \rceil} + b_{\lceil \frac{(\gamma_2-1)t_2 m+m}{t_2} - 1 \rceil} - b_{\lceil \frac{(\gamma_2-1)t_2 m+m}{t_2} - 2 \rceil})q^\xi \\ & - \cdots - (b_{i_1} + a_{i_1} - b_{i_1-1})q - (b_{i_1-1} + a_{i_1-1} - b_{i_1-2}) - 1. \end{aligned} \quad (16)$$

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

$$\left\lceil \frac{q-1}{m} \right\rceil = a_{i_1} + b_{i_1} - b_{i_1-1} = a_{m-1} - b_{m-2}.$$

It is clear that

$$m-1 - \left(m - i_1 - 1 + \left\lceil \frac{\gamma_2 m}{t_2} - 1 \right\rceil \right) = i_1 - \left\lceil \frac{\gamma_2 m}{t_2} - 1 \right\rceil \leq N_{\gamma_2+1}^1 - 2 \leq N_{t_2}^1 - 1.$$

Then

$$a_{m-2} = a_{m-3} = \cdots = a_{\xi+1} = \left\lfloor \frac{q-1}{m} \right\rfloor \text{ and } a_{i_1} = a_{i_1-1} = \cdots = a_{\lceil \frac{\gamma_2 m}{t_2} \rceil} = \left\lfloor \frac{q-1}{m} \right\rfloor$$

since $0 \leq N_{\gamma_2+1}^1 - N_{t_2}^1 \leq 1$ and $\lceil \frac{\gamma_2 m}{t_2} - 1 \rceil < i_1 < \lceil \frac{(\gamma_2+1)m}{t_2} - 1 \rceil - 1$. If there exists $l_1 \in [2, m-2-\xi]$ such that

$$a_{m-l_1-1} + b_{m-l_1-1} - b_{m-l_1-2} > a_{i_1-l_1} + b_{i_1-l_1} - b_{i_1-l_1-1}, \quad (17)$$

let l_2 be the least integer in the range $[2, m-2-\xi]$ such that (17) holds, then we have $b_{m-l_2-1} > 0$ and

$$a_{m-1-l_3} + b_{m-1-l_3} - b_{m-2-l_3} \leq a_{i_1-l_3} + b_{i_1-l_3} - b_{i_1-l_3-1} \quad (18)$$

for all $0 \leq l_3 < l_2$. If all of the equals in (18) hold, since $b_{m-2} = 0$ and $b_{i_1-l} = 0$ for all $l \in [1, i_1 - 1]$, we know that $b_{m-3} = b_{m-4} = \dots = b_{m-l_2-1} = 0$, which is contradictive with $b_{m-l_2-1} > 0$. Then at least one of equals in (18) does not hold, we obtain that $q^{m-i_1-1}M \pmod{q^m-1} < M$ from (15) and (16).

If there does not exist $l_1 \in [2, m-2-\xi]$ such that (17) holds, then we have

$$\begin{cases} \lfloor \frac{q-1}{m} \rfloor = a_{i_1-1} + b_{i_1-1} - b_{i_1-2} \geq b_{m-2} + a_{m-2} - b_{m-3}, \\ \lfloor \frac{q-1}{m} \rfloor = a_{i_1-2} + b_{i_1-2} - b_{i_1-3} \geq b_{m-3} + a_{m-3} - b_{m-4}, \\ \vdots \\ \lfloor \frac{q-1}{m} \rfloor = a_{\lceil \frac{\gamma_2 m}{t_2} \rceil} + b_{\lceil \frac{\gamma_2 m}{t_2} \rceil} - b_{\lceil \frac{\gamma_2 m}{t_2} \rceil - 1} \geq b_{\xi+1} + a_{\xi+1} - b_{\xi}. \end{cases} \quad (19)$$

If there is one of equals in (19) that does not hold, then $q^{m-i_1-1}M \pmod{q^m-1} < M$ from (15) and (16).

If all the equals in (19) holds, then $b_{m-3} = b_{m-4} = \dots = b_{\xi} = 0$. Hence,

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

It is clear that $a_{\lceil \frac{(\gamma_2-1)m+m}{t_2} \rceil - 1} + b_{\lceil \frac{(\gamma_2-1)m+m}{t_2} \rceil - 1} - b_{\lceil \frac{(\gamma_2-1)m+m}{t_2} \rceil - 2} = \lceil \frac{q-1}{m} \rceil$ since $a_{\lceil \frac{(\gamma_2-1)m+m}{t_2} \rceil - 1} = \lceil \frac{q-1}{m} \rceil$ and $b_{\lceil \frac{(\gamma_2-1)m+m}{t_2} \rceil - 1} = b_{\lceil \frac{(\gamma_2-1)m+m}{t_2} \rceil - 2} = 0$. Then $q^{m-i_1-1}M \pmod{q^m-1} < M$ from (15) and (16).

Subcase 2: $i_1 = \lceil \frac{(\gamma_2+1)m}{t_2} \rceil - 1$. From Lemma 22, there exists $\xi \in [1, t_2]$ such that $N_{\gamma_2}^{\xi} = N_{t_2}^{\xi}$. Assume that $\xi_1 \in [1, t_2]$ is the minimum value such that $N_{\gamma_2}^{\xi_1} = N_{t_2}^{\xi_1}$.

If there exists $l \in [2, i_1 - \lceil \frac{(\gamma_2-\xi_1)m}{t_2} \rceil - 1]$ such that $a_{m-1-l} + b_{m-1-l} - b_{m-2-l} > a_{\overline{(i_1-l)}_m} + b_{\overline{(i_1-l)}_m} - b_{\overline{(i_1-l-1)}_m}$, similar to the discuss of (17) and (18), then there is $1 \leq l_4 < l$ such that $a_{m-1-l_4} + b_{m-1-l_4} - b_{m-2-l_4} < a_{\overline{(i_1-l_4)}_m} + b_{\overline{(i_1-l_4)}_m} - b_{\overline{(i_1-l_4-1)}_m}$. Hence, we obtain $q^{m-i_1-1}M \pmod{q^m-1} < M$.

If there does not exist $l \in [2, i_1 - \lceil \frac{(\gamma_2-\xi_1)m}{t_2} \rceil - 1]$ such that $a_{m-1-l} + b_{m-1-l} - b_{m-2-l} > a_{\overline{(i_1-l)}_m} + b_{\overline{(i_1-l)}_m} - b_{\overline{(i_1-l-1)}_m}$, then we have

$$a_{\overline{(i_1-l)}_m} + b_{\overline{(i_1-l)}_m} - b_{\overline{(i_1-l-1)}_m} \geq a_{m-1-l} + b_{m-1-l} - b_{m-2-l} \quad (20)$$

for all $l \in [2, i_1 - \lceil \frac{(\gamma_2-\xi_1)m}{t_2} \rceil - 1]$. If one of equals in (20) does not hold, then $q^{m-i_1-1}M \pmod{q^m-1} < M$.

If all the equals in (20) holds, then $b_{m-3} = b_{m-4} = \dots = b_\eta = 0$, where $\eta = m - 1 - i_1 + \lceil \frac{(\gamma_2 - \xi_1)m}{t_2} \rceil$. Hence,

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

Since $a_{\lceil \frac{(\gamma_2 - \xi_1 - 1)t_2^{m+m}}{t_2} - 1 \rceil} = \lceil \frac{q-1}{m} \rceil$ and $b_{\lceil \frac{(\gamma_2 - \xi_1 - 1)t_2^{m+m}}{t_2} - 1 \rceil} = b_{\lceil \frac{(\gamma_2 - \xi_1 - 1)t_2^{m+m}}{t_2} - 2 \rceil} = 0$, we have

$$a_{\lceil \frac{(\gamma_2 - \xi_1 - 1)t_2^{m+m}}{t_2} - 1 \rceil} + b_{\lceil \frac{(\gamma_2 - \xi_1 - 1)t_2^{m+m}}{t_2} - 1 \rceil} - b_{\lceil \frac{(\gamma_2 - \xi_1 - 1)t_2^{m+m}}{t_2} - 2 \rceil} = \left\lfloor \frac{q-1}{m} \right\rfloor,$$

then

$$a_{\eta+1} + b_{\eta+1} - b_\eta < a_{\lceil \frac{(\gamma_2 - \xi_1 - 1)t_2^{m+m}}{t_2} - 1 \rceil} + b_{\lceil \frac{(\gamma_2 - \xi_1 - 1)t_2^{m+m}}{t_2} - 1 \rceil} - b_{\lceil \frac{(\gamma_2 - \xi_1 - 1)t_2^{m+m}}{t_2} - 2 \rceil}.$$

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. \square

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 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.,

$$\begin{cases} a_{m-2} + b_{m-2} - b_{m-3} \geq 0, \\ \vdots \\ a_{i_2+1} + b_{i_2+1} - b_{i_2} \geq 0, \\ a_{i_2} + b_{i_2} - b_{i_2-1} \geq q, \end{cases} \quad (21)$$

then $b_{i_2-1} \leq \sum_{j=i_2}^{m-2} a_j + b_{m-2} - q \leq \sum_{j=i_2}^{m-2} a_j + a_{m-1} - q < 0$, 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 Ψ 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 $i_4 = \max\{i : i \in \Psi\}$. 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 (21), 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

$$\begin{cases} a_{m-2} + b_{m-2} - b_{m-3} \geq 0, \\ \vdots \\ a_{i_4+1+b_{i_4}+1} - b_{i_4} \geq 0, \\ a_{i_4} + b_{i_4} - b_{i_4-1} = -1, \\ a_{i_4-1} + b_{i_4-1} - b_{i_4-2} \geq q. \end{cases}$$

Then we have $b_{i_4-2} \leq -q + \sum_{i=i_4-1}^{m-2} a_i + 1 \leq -q + \sum_{i=i_4-1}^{m-1} a_i \leq -1 < 0$, 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

$$M = (q - a_{m-1} + b_{m-2})q^{m-1} + (b_{m-3} - a_{m-2} - b_{m-2})q^{m-2} + \cdots + (b_0 - a_1 - b_1)q - a_0 - b_0 - 1. \quad (22)$$

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

$$\begin{aligned} q^{m-i_4-1}M \pmod{q^m - 1} = & (b_{i_4-1} - a_{i_4} - b_{i_4})q^{m-1} + (b_{i_4-2} - a_{i_4-1} - b_{i_4-1})q^{m-2} + \cdots + \\ & (-a_0 - b_0)q^{m-i_4-1} + (q - a_{m-1} + b_{m-2})q^{m-i_4-2} + \\ & \cdots + (b_{i_4} - a_{i_4+1} - b_{i_4+1}) \end{aligned} \quad (23)$$

if $i_4 \neq m-2$ and

$$\begin{aligned} q^{m-i_4-1}M \pmod{q^m - 1} = & (b_{i_4-1} - a_{i_4} - b_{i_4})q^{m-1} + (b_{i_4-2} - a_{i_4-1} - b_{i_4-1})q^{m-2} + \cdots + \\ & (-a_0 - b_0)q^{m-i_4-1} + (-a_{m-1} + b_{m-2}) \end{aligned}$$

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

$$b_{i_4-1} = q - 1, b_{i_4} = 0, a_{i_4} = \lfloor \frac{q-1}{m} \rfloor, b_{m-2} = 0 \text{ and } m \nmid (q-1) \quad (24)$$

since $a_{m-1} = \lceil \frac{q-1}{m} \rceil$. Then there exists a positive integer γ_3 such that $\lceil \frac{(\gamma_3-1)m}{t_2} - 1 \rceil < i_4 < \lceil \frac{\gamma_3 m}{t_2} - 1 \rceil$. Let $1 \leq s \leq i_4$ and

$$D_{(m-1-s)} = (b_{i_4-s-1} - a_{i_4-s} - b_{i_4-s}) - (b_{m-s-2} - b_{m-s-1} - a_{m-s-1}).$$

Clearly, from (24) we know that

$$\begin{aligned} D_{(m-2)} &= (b_{i_4-2} - a_{i_4-1} - b_{i_4-1}) - (b_{m-3} - b_{m-2} - a_{m-2}) \\ &= b_{i_4-2} - (q-1) - b_{m-3} - a_{i_4-1} + a_{m-2}. \end{aligned}$$

From Lemma 21, it is obvious that

$$-a_{i_4-1} + a_{m-2} \in \{-1, 0, 1\}. \quad (25)$$

If $a_{m-2} - a_{i_4-1} = 1$, then we have $a_{i_4-1} = \lfloor \frac{q-1}{m} \rfloor$ and $a_{m-2} = \lceil \frac{q-1}{m} \rceil$. Since $a_{i_4} = a_{i_4-1} = \lfloor \frac{q-1}{m} \rfloor$ and $a_{m-1} = a_{m-2} = \lceil \frac{q-1}{m} \rceil$, we obtain that $N_{\gamma_3}^1 \geq 3$ and $N_{t_2}^1 = 1$, which is contradictory to Lemma 22. Then from (25) 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 (24), we obtain that

$$b_{i_4-2} = q-1, b_{m-3} = 0 \text{ and } a_{m-2} - a_{i_4-1} = 0. \quad (26)$$

With a similar analysis on $D_{(m-2)}$, we obtain $D_{(m-3)} \leq 0$. If $D_{(m-3)} < 0$, then $q^{m-i_4-1}M \pmod{q^m-1} < M$.

If $D_{(m-3)} = 0$, combined with (26) 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

$$\begin{cases} b_{i_4-1} = b_{i_4-2} = \cdots = b_0 = q-1, \\ b_{m-2} = b_{m-3} = \cdots = b_{m-i_4-1} = 0, \\ \vdots \\ a_{m-2} - a_{i_4-1} = a_{m-3} - a_{i_4-2} = a_{m-i_4} - a_1 = 0. \end{cases} \quad (27)$$

If (27) holds, then

$$\begin{aligned} D_{(m-i_4-1)} &= -(b_0 + a_0) - (b_{m-i_4-2} - b_{m-i_4-1} - a_{m-i_4-1}) \\ &= -(q-1) - \lfloor \frac{q-1}{m} \rfloor - b_{m-i_4-2} + a_{m-i_4-1} \leq -(q-2) < 0. \end{aligned}$$

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. \square

Proposition 27. *Let $q \geq 3$ be a prime power and $m \geq 4$ be an integer. Then $\delta_1 = \theta$ is the largest coset leader modulo n , where θ is given in Lemma 23.*

Proof. If δ is a coset leader modulo n , then $(q-1)\delta$ must be a coset leader modulo q^m-1 since

$$\theta q^i \pmod{n} \geq \theta \Leftrightarrow \theta(q-1)q^i \pmod{q^m-1} \geq \theta(q-1)$$

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, δ is not a coset leader modulo n if $\delta > \delta_1$, i.e., δ_1 is the largest coset leader modulo n . The desired results then follows. \square

Lemma 28. *Let δ_1 be given as in Proposition 27, then $|C_{\delta_1}| = \frac{m}{\gcd(m, q-1)}$.*

Proof. It is known that $\text{ord}_n(q) = m$, then $|C_{\delta_1}|$ is a divisor of m . Assume that $|C_{\delta_1}| = h$, then

$$n \mid \delta_1(q^h - 1). \quad (28)$$

By definition, δ_1 can be written as

$$\delta_1 = n - \frac{\sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} - 1 \rceil}}{q-1}.$$

Then (28) holds if and only if $\frac{q^m-1}{q^h-1} \mid \sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} - 1 \rceil}$, i.e.,

$$q^{m-h} + q^{m-2h} + \dots + q^{m-(i-1)h} + 1 \mid \sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} - 1 \rceil},$$

where $i = \frac{m}{h}$. It is easy to check that

$$\sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} - 1 \rceil} = \left(\sum_{i_0=0}^{\gcd(q-1, m)-1} q^{\frac{mi_0}{\gcd(q-1, m)}} \right) \left(\sum_{i_1=1}^{\frac{(q-1)}{\gcd(m, q-1)}} q^{\lceil \frac{mt}{q-1} - 1 \rceil} \right).$$

In addition,

$$q^{m-h} + q^{m-2h} + \dots + q^{m-(i-1)h} + 1 = \sum_{i=0}^{\gcd(q-1, m)-1} q^{\frac{mi}{\gcd(q-1, m)}}$$

if $h = \frac{m}{\gcd(q-1, m)}$. Hence, (28) holds if $h = \frac{m}{\gcd(q-1, m)}$. This means that

$$|C_{\delta_1}| = h \leq \frac{m}{\gcd(q-1, m)}. \quad (29)$$

We now prove that $h \geq \frac{m}{\gcd(q-1, m)}$. Assume that there exists a positive integer Q such that

$$Q(q^{m-h} + q^{m-2h} + \dots + q^{m-(i-1)h} + 1) = \sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} - 1 \rceil}. \quad (30)$$

Let $Q = a_i q^i + a_{i-1} q^{i-1} + \dots + a_1 q + a_0$ and $a_i + a_{i-1} + \dots + a_0 = r$. If (30) holds, then $\frac{rm}{h} = q-1$, which implies that $rm = h(q-1)$. Hence, we have

$$r \cdot \frac{m}{\gcd(m, q-1)} = h \cdot \frac{q-1}{\gcd(m, q-1)}.$$

Since

$$\gcd\left(\frac{m}{\gcd(m, q-1)}, \frac{q-1}{\gcd(m, q-1)}\right) = 1,$$

we obtain that $\frac{m}{\gcd(m, q-1)} \mid h$. Hence, from (29) we have $|C_{\delta_1}| = \frac{m}{\gcd(q-1, m)}$. The desired conclusion then follows. \square

Remark 29. When $q = 3$, δ_1 and $|C_{\delta_1}|$ have been given in [22, Lemma 17]. Let $m \geq q$, $b \equiv m-1 \pmod{q-1}$. When $b = 0$, $b = 1$ or $b = q-2$, δ_1 and $|C_{\delta_1}|$ have been given in [35, Lemma 16]. We general 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 $C_{(q, n, \delta_1)}$ has parameters

$$\left[\frac{q^m - 1}{q - 1}, \frac{m}{\gcd(m, q-1)} + 1, d \geq q^{m-1} - 1 - \frac{\sum_{t=1}^{q-2} q^{\lceil \frac{mt}{q-1} \rceil - 1} - q + 2}{q - 1} \right].$$

Example 31. Let $(q, m) = (3, 4)$. Then the code $C_{(q, n, \delta_1)}$ in Theorem 19 has parameters $[40, 3, \geq 25]$. This code is the best cyclic code according to [7, P. 305] when the equality holds.

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

Lemma 32. Let δ' be the coset leader of $C_{n-\delta_1}$ modulo n . Then the following hold.

- 1) $\delta_1 \in T^\perp$ 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 δ' be 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., $C_{\delta'} \not\subseteq T$, then $C_{n-\delta'} = C_{\delta_1} \not\subseteq T^{-1}$, $C_{\delta_1} \subseteq T^\perp$. If $\delta' < \delta \leq \delta_1$, i.e., $C_{\delta_1} \not\subseteq T$, then $C_{n-\delta_1} = C_{\delta'} \not\subseteq T^{-1}$ and $C_{\delta'} \subseteq T^\perp$. \square

Denote $m = r(q-1) + s$ and $v = \lceil \frac{(s-1)(q-1)}{s} \rceil$, where $r \geq 0$ and $0 \leq s \leq q-2$. Note that

$$\delta_1 = q^{m-1} - 1 - \frac{\sum_{t=1}^{q-2} q^{\lceil \frac{mt}{q-1} \rceil - 1} - q + 2}{q - 1} = \frac{q^m - \sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} \rceil - 1} - 1}{q - 1}.$$

Then

$$n - \delta_1 = \frac{\sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} \rceil - 1}}{q - 1}. \quad (31)$$

Let δ' and δ'' be the coset leaders of $C_{n-\delta_1}$ modulo n and $C_{(q-1)(n-\delta_1)}$ modulo $(q-1)n$, respectively. It is similar with (4), we have $(q-1) \mid \delta''$ and $\delta'' = \delta'(q-1)$. From (31) we have $(q-1)(n-\delta_1) = \sum_{t=1}^{q-1} q^{\lceil \frac{mt}{q-1} - 1 \rceil}$. From Lemma 21, one can see that the q -adic expansion of δ'' has the form $(\mathbf{0}_r, 1, \dots)_q$ if $r \geq 1$ and δ'' has the form $(\lfloor \frac{q-1}{m} \rfloor, \dots)_q$ if $r = 0$. where $\mathbf{0}_r = (\underbrace{0, 0, \dots, 0}_r)_q$. Then

$$\delta' = \frac{\delta''}{q-1} > \frac{q^{m-r-1} - 1}{q-1}. \quad (32)$$

With the preparations above, we now give a sufficient and necessary condition for $C_{(q,n,\delta)}$ 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 $C_{(q,n,\delta)}$ is a dually-BCH code if and only if $\delta_1 + 1 \leq \delta \leq n$, where δ_1 is given in Proposition 27.*

Proof. When $q = 3$, the result has been given in [12, Theorem 30], we only prove the result for $q > 3$ in the following.

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

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

Case 1: $2 \leq \delta \leq \frac{q^{r+1}-1}{q-1}$. It is easy to see that $m-r-1 \geq r+1$. Then from Equation (32) and Proposition 32 that $\delta_1 \in T^\perp$ is the coset leader of C_{δ_1} . It follows from Lemma 14 that

$$I_{\max} := \max \left\{ I(\delta) : 2 \leq \delta \leq \frac{q^{r+1}-1}{q-1} \right\} = I(2) = \frac{q^{m-1}-1}{q-1} = (0, \underbrace{1, \dots, 1}_{m-1})_q.$$

Note that $\delta_1 = q^{m-1} - 1 - \frac{\sum_{t=1}^{q-2} q^{\lceil \frac{mt}{q-1} - 1 \rceil}}{q-1} - q + 2$. 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 $T^\perp = C_0 \cup C_1 \cup \dots \cup C_{J-1}$, i.e., $C_{(q,n,\delta)}^\perp$ is not a BCH code with respect to β .

Case 2: If $\frac{q^{r+1}-1}{q-1} < \delta < q^{m-1} - \frac{\sum_{t=1}^{q-2} q^{\lceil \frac{mt}{q-1} - 1 \rceil} - q + 2}{q-1}$. It then follows from Proposition 32 that $\delta' \in T^\perp$ is the coset leader of $C_{\delta'}$. It follows from Lemma 14 that

$$I_{\max} := \max \left\{ I(\delta) : \frac{q^{r+1}-1}{q-1} < \delta < q^{m-1} - \frac{\sum_{t=1}^{q-2} q^{\lceil \frac{mt}{q-1} - 1 \rceil} - q + 2}{q-1} \right\} = \frac{q^{m-r-1}-1}{q-1}.$$

We deduce from Equation (32) that $\delta' > \frac{q^{m-r-1}-1}{q-1}$. It then follows from Lemma 14 that there is no integer $J \geq 1$ such that $T^\perp = C_0 \cup C_1 \cup \dots \cup C_{J-1}$, i.e., $C_{(q,n,\delta)}^\perp$ is not a BCH code with respect to β . \square

Remark 34. In [12], the authors gave the range of δ for BCH codes $C_{(3,n,\delta)}$ being dually-BCH codes and showed that it looks much harder to give a characterisation of $C_{(q,n,\delta)}$ being dually-BCH codes, where $q > 3$ is a prime power. Theorem 33 finished this work.

V. CONCLUSION

Let $n = \frac{q^m-1}{q+1}$ 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 $C_{(q,n,\delta)}$ 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 $n = \frac{q^m-1}{q+1}$. In this sense, we extended the results in [12].
- We determined the largest coset leader modulo $\frac{q^m-1}{q-1}$, which is very useful to completely solve Open Problem 45 in [21]. We also determined the largest coset leader modulo $\frac{q^m-1}{q+1}$, so the conjecture in [28] were proved.

REFERENCES

- [1] S. A. Aly, A. Klappenecker, P. K. Sarvepalli, On quantum and classical BCH codes, IEEE Trans. Inf. Theory 53 (3) (2007) 1183–1188.
- [2] D. Augot, N. Sendrier, Idempotents and the BCH bound, IEEE Trans. Inf. Theory 40 (1) (1994) 204–207.
- [3] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill Book, New York (1968).
- [4] E. R. Berlekamp, Negacyclic codes for the Lee metric, In: Proceedings of the Conference on Combinatorial Mathematics and Its Applications, pp. 298–316. University of North Carolina Press, Chapel Hill (1968).
- [5] R. C. Bose, D. K. Ray-Chaudhuri, On a class of error correcting binary group codes, Information and Control 3 (1962) 279–290.

- [6] P. Charpin, On a class of primitive BCH-codes, IEEE Trans. Inf. Theory 36 (1) (1990) 222–228.
- [7] C. Ding, Codes from Difference Sets, World Scientific, Singapore, 2015.
- [8] C. Ding, BCH codes in the past 55 years, The 7th international Workshop on Finite Fields Applications, Tianjin, China, 2016.
- [9] C. Ding, Parameters of several classes of BCH codes, IEEE Trans. Inf. Theory 61 (10) (2015) 5322–5330.
- [10] C. Ding, X. Du, Z. Zhou, The Bose and minimum distance of a class of BCH Codes, IEEE Trans. Inf. Theory 61 (5) (2015) 2351–2356.
- [11] C. Ding, C. Fan, Z. Zhou, The dimension and minimum distance of two classes of primitive BCH codes, Finite Fields Appl. 45 (2017) 237–263.
- [12] B. Gong, C. Ding, C. Li, The dual codes of several classes of BCH codes, IEEE Trans. Inf. Theory 68 (2) (2022) 953–964.
- [13] D. C. Gorenstein, N. Zierler, A class of error-correcting codes in p^m symbols, J. SIAM 9 (1961) 207–214.
- [14] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, Online available at <http://www.codetables.de>.
- [15] G. Guo, R. Li, Y. Liu, J. Wang, A family of negacyclic BCH codes of length $n = \frac{q^{2m}-1}{2}$, Crypto. Commun. 12 (2020) 187–203.
- [16] A. Hocquenghem, Codes correcteurs d’erreurs, Chiffres (Pairs) 2 (1959) 147–156.
- [17] X. Kai, S. Zhu, New quantum MDS codes from negacyclic codes, IEEE Trans. Inf. Theory 59 (2) (2013) 1193–1197.
- [18] X. Kai, S. Zhu, Y. Tang, Quantum negacyclic codes, Phys. Rev. A 88 (1) 012326 (2013).
- [19] A. Krishna, D. V. Sarwate, Pseudocyclic maximum-distance-separable codes, IEEE Trans. Inf. Theory 36 (4) (1990) 880–884.
- [20] C. Li, C. Ding, S. Li, LCD cyclic codes over finite fields, IEEE Trans. Inf. Theory 63 (7) (2017) 4344–4356.
- [21] S. Li, C. Ding, M. Xiong, G. Ge, Narrow-sense BCH codes over $\text{GF}(q)$ with length $n = \frac{q^m-1}{q-1}$, IEEE Trans. Inf. Theory 63 (11) (2007) 7219–7236.
- [22] S. Li, C. Li, C. Ding, H. Liu, Two families of LCD BCH codes, IEEE Trans. Inf. Theory 63 (9) (2017) 5699–5717.
- [23] H. Liu, C. Ding, C. Li, Dimensions of three types of BCH codes over $\text{GF}(q)$, Discrete Math. 340 (2017) 1910–1927.
- [24] Y. Liu, Y. Li, Q. Fu, L. Lu, Y. Rao, Some binary BCH codes with length $n = 2^m + 1$, Finite Fields Appl. 55 (2019) 109–133.
- [25] Y. Liu, R. Li, L. Guo, H. Song, Dimensions of nonbinary antiprimitive BCH codes and some conjectures, arXiv: 1712.06842v2.
- [26] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
- [27] B. Pang, S. Zhu, Z. Sun, On LCD Negacyclic Codes over Finite Fields, J. Syst. Sci. Complex 31 (2018) 1065–1077.
- [28] P. Wu, C. Li, W. Peng, On some cyclic codes of length $\frac{q^m-1}{q-1}$, Finite Fields Appl., 60 (2019) 101581.1–28
- [29] S.Y. El Rouayheb, C. N. Georgiades, E. Soljanin, A. Sprintson, Bounds on codes based on graph theory, IEEE Int. Symp. on Information Theory. Nice, France (2007) 1876–1879.
- [30] H. Yan, H. Liu, C. Li, S. Yang, Parameters of LCD BCH codes with two lengths, Adv. Math. Commun. 12 (3) (2018) 579–594.
- [31] D. Yue, Z. Feng, Minimum cyclotomic coset representatives and their applications to BCH codes and Goppa codes, IEEE Trans. Inf. Theory 46 (7) (2000) 2625–2628.
- [32] D. Yue, Z. Hu, On the dimension and minimum distance of BCH codes over $\text{GF}(q)$, J. Electron. 13 (3) (1996) 216–221.
- [33] H. Zhu, M. Shi, X. Wang, T. Helleseth, The q -ary antiprimitive BCH codes, IEEE Trans. Inf. Theory 68 (2022) 1683–1695.
- [34] S. Zhu, Z. Sun, P. Li, A class of negacyclic BCH codes and its application to quantum codes, Des. Codes. Crptogr. 86 (2018) 2139–2165.

- [35] S. Zhu, Z. Sun, X. Kai, A Class of Narrow-Sense BCH Codes. *IEEE Trans. Inf. Theory* 65 (2019) 4699–4714.