Parameters of Several Classes of BCH Codes

Cunsheng Ding, *Senior Member, IEEE*

***Abstract*— Because of their efficient encoding and decoding algorithms, cyclic codes—an interesting class of linear codes—are widely used in communication systems, storage devices, and consumer electronics. BCH codes form a special class of cyclic codes, and are usually among the best cyclic codes. A subclass of good BCH codes is the narrow-sense primitive BCH codes. However, the dimension and minimum distance of these codes are not known in general. The main objective of this paper is to study the dimension and minimum distances of a subclass of the narrow-sense primitive BCH codes with design distance $\delta = (q-\ell_0)q^{m-\ell_1-1}-1$ for certain pairs (ℓ_0, ℓ_1), where $0 \le \ell_0 \le q-2$ and $0 \le \ell_1 \le m-1$. The parameters of other related classes of BCH codes are also investigated, and some open problems are proposed in this paper.**

***Index Terms*— BCH codes, cyclic codes, linear codes.**

I. Introduction

THROUGHOUT this paper, let q be a power of a prime p. A linear $[n, k, d]$ code $\mathcal{C}$ over GF(q) is a k-dimensional subspace of GF$(q)^n$ with minimum (Hamming) distance d.

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

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

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

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

Let $m > 1$ be a positive integer and let $n = q^m - 1$. Let α be a generator of GF$(q^m)^*$, which is the multiplicative group of the finite field GF(q^m). For any i with $1 \le i \le q^m - 2$, let $m_i(x)$ denote the minimal polynomial of α^i over GF(q). For any $2 \le \delta < n = q^m - 1$, define

$$g_{(q,m,\delta)}(x) = \mathrm{lcm}(m_1(x), m_2(x), \cdots, m_{\delta-1}(x)),$$

where lcm denotes the least common multiple of these minimal polynomials $m_i(x)$. Let $\mathcal{C}_{(q,m,\delta)}$ denote the cyclic code of length n with generator polynomial $g_{(q,m,\delta)}(x)$. This code $\mathcal{C}_{(q,m,\delta)}$ is called the *narrow-sense primitive BCH code* with *design distance* δ. By definition, the generator polynomial $g_{(q,m,\delta)}(x)$ of the BCH code $\mathcal{C}_{(q,m,\delta)}$ has $\delta - 1$ consecutive roots α^i for all $1 \le i \le \delta - 1$. Hence, by the BCH bound [15, Th. 5.1.1], the minimum distance of the code $\mathcal{C}_{(q,m,\delta)}$ is at least δ. This is why δ is called the design distance of the code $\mathcal{C}_{(q,m,\delta)}$. Binary BCH codes were discovered around 1960 by Hocquenghem [14] and independently by Bose and Ray-Chaudhuri [6], [7], and were generalized to all finite fields by Gorenstein and Zierler [13].

It is well known that the codes $\mathcal{C}_{(q,m,\delta)}$ and $\mathcal{C}_{(q,m,\delta')}$ may be identical for two different δ and δ'. The largest design distance of a BCH code is called the *Bose distance* of the code and is denoted by d_B.

The cyclic codes $\mathcal{C}_{(q,m,\delta)}$ are treated in most books on coding theory. However, the following questions about the codes $\mathcal{C}_{(q,m,\delta)}$ are still open in general.

1) What is the dimension of $\mathcal{C}_{(q,m,\delta)}$?
2) What is the Bose distance (i.e., the maximum design distance) of $\mathcal{C}_{(q,m,\delta)}$?
3) What is the minimum distance d (i.e., the minimum weight) of $\mathcal{C}_{(q,m,\delta)}$?

The dimension of $\mathcal{C}_{(q,m,\delta)}$ is known when δ is small, and is open in general. There are lower bounds on the dimension of $\mathcal{C}_{(q,m,\delta)}$, which are very bad in many cases. The minimum distance d of $\mathcal{C}_{(q,m,\delta)}$ is known only in a few cases. Only when δ is very small or when $\mathcal{C}_{(q,m,\delta)}$ is the Reed-Solomon code, both the dimension and minimum distance of $\mathcal{C}_{(q,m,\delta)}$ are known. Hence, we have very limited knowledge of the narrow-sense primitive BCH codes, not to mention BCH codes in general. Thus, BCH codes are far from being well understood and studied.

In the 1990's, there were a few papers on the narrow-sense primitive BCH codes [2], [3], [9], [20]. However, in the last eighteen years, little progress on the study of these codes has been made. As pointed out by Charpin in [10], it is a well-known hard problem to determine the minimum distance of narrow-sense BCH codes.

The major objective of this paper is to determine the dimension and minimum distance of the codes $\mathcal{C}_{(q,m,\delta)}$ with design distance $\delta = (q-\ell_0)q^{m-\ell_1-1} - 1$ for certain pairs of (ℓ_0, ℓ_1), where $0 \le \ell_0 \le q-2$ and $0 \le \ell_1 \le m-1$. The parameters of other related classes of BCH codes will also be investigated. A number of open problems about the narrow-sense primitive BCH codes will be proposed.

To investigate the optimality of the BCH codes studied in this paper, we compare them with the tables of best linear codes known maintained by Markus Grassl at http://www.codetables.de, which is called the

Manuscript received April 14, 2015; revised August 9, 2015; accepted August 10, 2015. Date of publication August 19, 2015; date of current version September 11, 2015. C. Ding was supported by the Research Grants Council, Hong Kong, under Project 16301114.

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

Communicated by C. Xing, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2015.2470251

0018-9448 © 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Database subsequently. We will also compare these BCH codes with the tables of best cyclic codes documented in the monograph [11].

II. Known Results About the Codes $\mathcal{C}_{(q,m,\delta)}$

In order to give a well-rounded treatment of the codes $\mathcal{C}_{(q,m,\delta)}$, we summarize known results on the dimension and minimum distance of the codes in this section.

A. Known Results on the Dimension of $\mathcal{C}_{(q,m,\delta)}$

In general, for the dimension k of the code $\mathcal{C}_{(q,m,\delta)}$ we have the following lower bounds [15, p. 170]:

1) $k \geq q^m - 1 - m(\delta - 1)$, and
2) $k \geq q^m - 1 - m(\delta - 1)/2$ if $q = 2$ and δ is odd.

When δ is getting large, these two bounds are very bad as they become very small or even negative.

When $m = 1$, the code $\mathcal{C}_{(q,m,\delta)}$ is a Reed-Solomon code and its dimension is known.

When δ is small enough, the dimension k of the code $\mathcal{C}_{(q,m,\delta)}$ is given in the following theorem [20].

Theorem 1: Let δ_q and δ_0 be the unique integers such that $\delta - 1 = \delta_q q + \delta_0$, where $0 \leq \delta_0 < q$.

If $\delta - 1 \leq q^{\lceil m/2 \rceil}$, then the dimension k of the code $\mathcal{C}_{(q,m,\delta)}$ is given by

$$k = q^m - 1 - m(\delta_q(q-1) + \delta_0).$$

Let $T = 2q^{m/2} - 1$ for even m. If m is even and $q^{m/2} + 1 \leq \delta - 1 \leq T + 1$, then the dimension k of the code $\mathcal{C}_{(q,m,\delta)}$ is given by

$$k = q^m - 1 - m(\delta_q(q-1) + \delta_0) + \frac{m}{2}.$$

In the special case $\delta = q^t$, Mann derived the following result [18].

Theorem 2: The dimension k of the code $\mathcal{C}_{(q,m,q^t)}$ is equal to

$$q^m - 1 - \sum_{i=1}^{\lfloor \frac{m}{r+1} \rfloor} (-1)^{i-1} \frac{m(q-1)^i}{i} \binom{m - ir - 1}{i - 1} q^{m-i(r+1)}, \tag{1}$$

where $r = m - t$.

A rent result is the following [12].

Theorem 3: Let $m \geq 4$. Then the dimension of the BCH code $\mathcal{C}_{(q,\, m,\, q^{m-2}+1)}$ is equal to

$$\left(\frac{q - 1 - \sqrt{q^2 + 2q - 3}}{2} \right)^m + \left(\frac{q - 1 + \sqrt{q^2 + 2q - 3}}{2} \right)^m.$$

B. Known Results on the Minimum Distance of $\mathcal{C}_{(q,m,\delta)}$

According to the BCH bound, the minimum distance d of the code $\mathcal{C}_{(q,m,\delta)}$ satisfies

$$d \geq d_B \geq \delta,$$

where d_B denotes the Bose distance of the code $\mathcal{C}_{(q,m,\delta)}$. In some cases the difference $d - \delta$ is very small or zero. In many cases the difference $d - \delta$ is very large and in such cases the design distance does not give much information on the minimum distance d, but the Bose distance d_B may be very close to the minimum distance. In fact, we have the following conjecture [10].

Charpin's Conjecture: The minimum distance $d \leq d_B + 4$ for the narrow-sense primitive BCH codes.

In view of this conjecture, it is very useful to determine the Bose distance for the narrow-sense primitive BCH codes.

Given a design distance δ, it is a difficult problem to determine the Bose distance d_B, not to mention the minimum distance d. However, in some special cases the minimum distance d is known. Below we summarize known results regarding the minimum distance of BCH codes.

The first result on the minimum distance is the following [17, p. 260].

Theorem 4: For any h with $1 \leq h \leq m-1$, a primitive BCH code of length $n = q^m - 1$ and design distance $\delta = q^h - 1$ has minimum distance $d = q^h - 1$.

The next result is due to Kasami and Lin [16]

Theorem 5: For binary primitive BCH codes of length $n = 2^m - 1$ and Bose distance $d_B = 2^{m-1-s} - 2^{m-1-s-i} - 1$ with $1 \leq i \leq m - s - 2$ and $0 \leq s \leq m - 2i$, we have $d = d_B$.

The following result was developed by Peterson [19].

Theorem 6: Suppose a narrow-sense primitive BCH code over $\mathrm{GF}(q)$ with Bose distance δ has $d = \delta$, and $\delta + 1$ is divisible by p, the characteristic of $\mathrm{GF}(q)$. Then the narrow-sense primitive BCH code over $\mathrm{GF}(q)$ with Bose distance $d_B = (\delta + 1)q^{m-h} - 1$, where $h \geq \delta$, has minimum distance d_B.

A proof of the following theorem can be found in [5, p. 247].

Theorem 7: Let $\mathcal{C}$ be a narrow-sense BCH code of length n with design distance δ over $\mathrm{GF}(q)$. If δ divides n, then the minimum distance $d = \delta$.

The following result is sometimes useful in determining the minimum distance of the codes $\mathcal{C}_{(q,m,\delta)}$ [17, p. 259].

Theorem 8: The narrow-sense primitive binary BCH code $\mathcal{C}_{(2,m,\delta)}$ with design distance $\delta = 2t + 1$ has minimum distance $d = \delta$, provided that

- $\sum_{i=0}^{t+1} \binom{2^m - 1}{i} > 2^{mt}$ *or*
- $m > 1 + \log_2((t+1)!)$.

C. Cases When Both the Dimension and Minimum Distance of $\mathcal{C}_{(q,m,\delta)}$ Are Known

Both the dimension and minimum distance of the Reed-Solomon code $\mathcal{C}_{(q,1,\delta)}$ are known. In addition we have the following cases.

- When $\delta = 3$ and $q = 2$, $\mathcal{C}_{(q,m,\delta)}$ is the binary Hamming code with parameters $[2^m - 1, 2^m - 1 - m, 3]$ and generator polynomial $m_1(x)$, where $m \geq 3$.
- When $\delta = 5$ and $q = 2$, $\mathcal{C}_{(q,m,\delta)}$ has parameters $[2^m - 1, 2^m - 1 - 2m, 5]$ and generator polynomial $m_1(x)m_3(x)$, where $m \geq 4$.
- When $\delta = 7$ and $q = 2$, the code $\mathcal{C}_{(q,m,\delta)}$ has parameters $[2^m - 1, 2^m - 1 - 3m, 7]$ and generator polynomial $m_1(x)m_3(x)m_5(x)$, where $m \geq 5$.
- When $\delta = 3$ and $q = 3$, $\mathcal{C}_{(q,m,\delta)}$ has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ and generator polynomial $m_1(x)m_2(x)$, where $m \geq 3$.

In all these cases, the conclusion on the dimension of $\mathcal{C}_{(q,m,\delta)}$ follows from Theorem 1 and that on the minimum distance comes from the BCH bound and Theorem 8. When $1 \le \delta < 9$ and q is odd, it is possible to find out both the dimension and minimum distance of the code $\mathcal{C}_{(q,m,\delta)}$. However, it looks hard to determine both the dimension and minimum distance of the code when $\delta \ge 11$.

The following was recently proved in [12].

Theorem 9: Let $m \ge 4$, t be any integer with $1 \le t \le m-2$, and let h be any integer with $0 \le h \le \lfloor (q^t-1)/q^{m-t} \rfloor + 1$. The code $\mathcal{C}_{(q,m,q^t+h)}$ has parameters $[q^m-1, k, d]$, where

$$d \ge d_B = \left\lfloor \frac{n-1}{q^{m-t}-1} \right\rfloor + 1$$

and the dimension k is given in

- *Theorem 1 when $t \le \lceil m/2 \rceil$;*
- *Theorem 2 when $t > \lceil m/2 \rceil$; and*
- *also Theorem 3 when $t = m-2$.*

If $t \equiv 0 \pmod{m-t}$, the minimum distance d of the code $\mathcal{C}_{(q,m,q^t+h)}$ is given by

$$d = d_B = \frac{q^m-1}{q^{m-t}-1}.$$

If $m \equiv 0 \pmod{2t}$, then

$$d = d_B = \delta = q^t + 1.$$

III. The BCH Codes With $\delta = (q-\ell_0)q^{m-\ell_1-1} - 1$, Where $0 \le \ell_0 \le q-2$ and $0 \le \ell_1 \le m-1$

The *q-cyclotomic coset* modulo n containing i is defined by

$$C_i = \{iq^j \bmod n : 0 \le j < \ell_j\},$$

where ℓ_j is the smallest positive integer such that $q^{\ell_j} i \equiv i \pmod{n}$, and is called the *size* of C_i. The smallest integer in C_i is called the *coset leader* of C_i.

Throughout this section, let

$$\delta = (q-\ell_0)q^{m-\ell_1-1} - 1, \tag{2}$$

where $0 \le \ell_0 \le q-2$ and $0 \le \ell_1 \le m-1$. We investigate the parameters of the code $\mathcal{C}_{(q,m,\delta)}$ in this section.

A. The Codes $\mathcal{C}_{(q,m,\delta)}$ in Some General Cases

Theorem 10: The code $\mathcal{C}_{(q,m,\delta)}$ has length $n = q^m - 1$, minimum weight $d = (q-\ell_0)q^{m-\ell_1-1} - 1$ and dimension

$$k \ge \sum_{i=0}^{\ell} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{i - jq + m - 1}{i - jq}, \tag{3}$$

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

Proof: In order to prove this theorem, we need to introduce the punctured generalized Reed-Muller codes first. Let q be a prime power as before. For any integer $j = \sum_{i=0}^{m-1} j_i q^i$, where $0 \le j_i \le q-1$ for all $0 \le i \le m-1$ and m is a positive integer, we define

$$\omega_q(j) = \sum_{i=0}^{m-1} j_i, \tag{4}$$

where the sum is taken over the ring of integers.

Let ℓ be defined as in this theorem. The ℓ-th order *punctured generalized Reed-Muller code* $\mathcal{R}_q(\ell, m)^*$ over GF(q) is the cyclic code of length $n = q^m - 1$ with generator polynomial

$$g_R(x) := \prod_{\substack{1 \le j \le n-1 \\ \omega_q(j) < (q-1)m - \ell}} (x - \alpha^j), \tag{5}$$

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

By definition, we have

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

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

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

By the construction of the code $\mathcal{R}_q(\ell, m)^*$, every integer u with $0 < u < h$ satisfies $\omega_q(u) < (q-1)m - \ell$. Hence, the elements $\alpha^1, \alpha^2, \ldots, \alpha^{h-1}$ are all roots of the generator polynomial $g_R(x)$ of (5). It then follows from the definition of the code $\mathcal{C}_{(q,m,\delta)}$ that $\mathcal{C}_{(q,m,\delta)}$ contains the punctured generalized Reed-Muller code $\mathcal{R}_q(\ell, m)^*$ as a subcode. By the BCH bound, the minimum weight d of the code $\mathcal{C}_{(q,m,\delta)}$ is at least $(q-\ell_0)q^{m-\ell_1-1} - 1$, which is exactly the minimum weight of the code $\mathcal{R}_q(\ell, m)^*$ [1, Th. 5.5.2]. The desired conclusion on the minimum weight of the code $\mathcal{C}_{(q,m,\delta)}$ then follows.

It was proved in [1, Th. 5.4.1] that the dimension of the code $\mathcal{R}_q(\ell, m)^*$ is equal to

$$\sum_{i=0}^{\ell} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{i - jq + m - 1}{i - jq}. \tag{6}$$

The lower bound of (3) on the dimension of the code $\mathcal{C}_{(q,m,\delta)}$ then follows. This completes the proof of this theorem. □

Example 1: Let $(q,m) = (3,3)$ and let $(\ell_0, \ell_1) = (1,1)$. Let α be a generator of GF$(3^3)^*$ *with $\alpha^3 + 2\alpha + 1 = 0$. Then $\ell = 3$ and $\delta = 5$. The two codes $\mathcal{C}_{(3,3,5)}$ and $\mathcal{R}_3(3,3)^*$ are identical, and have parameters* $[26, 17, 5]$.

Example 2: Let $(q,m) = (3,3)$ and let $(\ell_0, \ell_1) = (0,1)$. Let α be a generator of GF$(3^3)^*$ *with $\alpha^3 + 2\alpha + 1 = 0$. Then $\ell = 2$ and $\delta = 8$. The two codes $\mathcal{C}_{(3,3,8)}$ and $\mathcal{R}_3(2,3)^*$ have parameters* $[26, 11, 8]$ *and* $[26, 10, 8]$, *respectively.*

Example 3: Let $(q,m) = (3,4)$ and let $(\ell_0, \ell_1) = (1,1)$. Let α be a generator of GF$(3^4)^*$ *with $\alpha^4 + 2\alpha^3 + 2 = 0$. Then $\ell = 3$ and $\delta = 17$. The two codes $\mathcal{C}_{(3,4,17)}$ and $\mathcal{R}_3(3,3)^*$ have parameters* $[80, 38, 17]$ *and* $[80, 31, 17]$, *respectively.*

When $(\ell_0, \ell_1) = (1,0)$, $\ell = 1$. In this special case, the equality in (3) holds. In general, the dimension k of the code $\mathcal{C}_{(q,m,\delta)}$ is more than the lower bound of (3). Thus, the BCH code $\mathcal{C}_{(q,m,\delta)}$ is in general much better than the corresponding punctured generalized Reed-Muller code $\mathcal{R}_q(\ell, m)^*$ whose dimension is equal to the lower bound of (3).

We would like to determine the dimension of $\mathcal{C}_{(q,m,\delta)}$. This can be done for certain cases.

Theorem 11: If $\delta - 1 \le q^{\lceil m/2 \rceil}$, then the code $\mathcal{C}_{(q,m,\delta)}$ has length $n = q^m - 1$, minimum weight $d = (q-\ell_0)q^{m-\ell_1-1} - 1$

and dimension

$$k = q^m - 1 - m\left((q-1)\left[(q-\ell_0)q^{m-\ell_1-2}-1\right]+q-2\right). \tag{7}$$

Proof: According to (2), we have

$$\begin{aligned}\delta - 1 &= (q-\ell_0)q^{m-\ell_1-1} - 2\\ &= [(q-\ell_0)q^{m-\ell_1-2} - 1]q + q - 2.\end{aligned}$$

The desired conclusion on the dimension then follows from Theorem 1. The minimum distance d was already determined in Theorem 10. □

The following result follows similarly from Theorems 1 and 10.

Theorem 12: If m is even and

$$q^{m/2} + 2 \le \delta \le 2q^{m/2} + 1,$$

then the code $\mathcal{C}_{(q,m,\delta)}$ has length $n = q^m - 1$, minimum weight $d = (q-\ell_0)q^{m-\ell_1-1} - 1$ and dimension

$$q^m - 1 - m\left((q-1)\left[(q-\ell_0)q^{m-\ell_1-2}-1\right]+q-2\right) + \frac{m}{2}.$$

B. The Codes $\mathcal{C}_{(q,m,\delta)}$ in the Case That $\ell = 1$

Recall that $\ell = \ell_1(q-1) + \ell_0$, where $0 \le \ell_0 \le q-1$. Hence in this case we have

$$(\ell_1, \ell_0) = \begin{cases}(1,0) & \text{if } q = 2,\\ (0,1) & \text{if } q > 2,\end{cases}$$

and

$$\begin{aligned}\delta &= (q-1)q^{m-1} - 1\\ &= (q-2)q^{m-1} + (q-1)\sum_{i=0}^{m-2} q^i.\end{aligned} \tag{8}$$

Our main result of this subsection is the following.

Theorem 13: The two cyclic codes $\mathcal{C}_{(q,m,(q-1)q^{m-1}-1)}$ and $\mathcal{R}_q(1,m)^*$ are identical, and have parameters $[q^m-1, m+1, (q-1)q^{m-1}-1]$.

Proof: It is well known that $\mathcal{R}_q(1,m)^*$ has parameters $[q^m-1, m+1, (q-1)q^{m-1}-1]$. Note that $\mathcal{C}_{(q,m,\delta)}$ contains $\mathcal{R}_q(1,m)^*$ as a subcode. We need only to prove that $\mathcal{C}_{(q,m,\delta)}$ has dimension $m+1$.

Let C_i denote the q-cyclotomic coset modulo n containing i for any i with $0 \le i \le n-1$, where $n = q^m - 1$. We need to prove that the set $\cup_{i=1}^{\delta-1} C_i$ has exactly $n-(m+1)$ elements. Equivalently, we need to prove that the following three statements are true:

(P1) $\cup_{i=1}^{\delta} C_i = \{1, 2, 3, \ldots, n-1\}$.
(P2) $|C_\delta| = m$.
(P3) $\delta \notin \cup_{i=1}^{\delta-1} C_i$.

We first prove that Property P1 holds. Note that every integer i with $1 \le i \le n-1$ has the following q-adic expression

$$i = i_0 q^{e_0} + i_1 q^{e_1} + \ldots + i_t q^{e_t} \tag{9}$$

where $0 \le e_0 < e_1 < \ldots < e_t \le m-1$, $1 \le i_j \le q-1$, and t is an integer with $0 \le t \le m-1$.

Observe that

$$i = q^{e_0}(i_0 + i_1 q^{e_1-e_0} + \ldots + i_t q^{e_t-e_0}).$$

We know that i and $i_0 + i_1 q^{e_1-e_0} + \ldots + i_t q^{e_t-e_0}$ are in the same q-cyclotomic coset modulo n. Hence we need only to consider the case that $e_0 = 0$ in the expression of (9). If $e_t \le m-2$ or $i_t < q-1$ then $i \le \delta$ and $i \in \cup_{j=1}^{\delta} C_j$. Therefore, it suffices to consider only the case that $i_t = q-1$ and $e_t = m-1$ in the expression of (9).

Now we assume that

$$i = i_0 + i_1 q^{e_1} + \ldots + i_{t-1} q^{e_{t-1}} + (q-1)q^{m-1}, \tag{10}$$

where $1 \le e_1 < \ldots < e_{t-1} \le m-2$ and $1 \le i_j < q$.

We now consider the integer i of (10), and distinguish between the following two cases.

Case 1: $i_0 = i_1 = \ldots = i_{t-1} = q-1$: In this case, we have

$$i = (q-1)(1 + q^{e_1} + \ldots + q^{e_{t-1}} + q^{m-1}).$$

Since $i < n$, there must exist an integer h such that

$$i = (q-1)\left(1 + q^{e_1} + \ldots + q^{e_{h-1}} + \sum_{j=e_h}^{m-1} q^j\right),$$

where $e_{h-1} \le e_h - 2$. We have then

$$i \times q^{m-e_h} \bmod n = r_i,$$

where

$$r_i = (q-1)\left(\sum_{j=0}^{m-e_h} q^j + \sum_{j=1}^{h-1} q^{m-e_h+e_j}\right).$$

Since $m - e_h + e_{h-1} \le m-2$, we obtain $r_i < \delta$. Hence $i \in \cup_{j=1}^{\delta} C_j$.

Case 2: At least one of the elements in $\{i_0, i_1, \ldots, i_{t-1}\}$ is less than $q-1$: Note that Case 2 cannot happen if $q = 2$. Hence in Case 2, we must have $q > 2$.

Let h be the largest index such that $i_h < q-1$. Then we have

$$i \times q^{m-e_{h+1}} \bmod n = r_i,$$

where

$$\begin{aligned}r_i = (q-1)&\left(\sum_{j=h+1}^{t-1} q^{e_j-e_{h+1}} + q^{m-1-e_{h+1}}\right)\\ &+ i_0 q^{m-e_{h+1}} + \sum_{j=1}^{h} i_j q^{m-e_{h+1}+e_j}.\end{aligned}$$

Notice that $i_h \le q-2$ and $m - e_{h+1} + e_h \le m-1$. We have $r_i \le \delta$. It then follows that

$$i \in C_{r_i} \subset \cup_{j=1}^{\delta} C_j.$$

Summarizing the conclusions in the foregoing two cases proves Property P1.

It is easy to verify that

$$C_\delta = \{n - q^{m-1}, n - q^{m-2}, \ldots, n-q, n-1\}.$$

Hence, Propery P2 holds and δ is the coset leader of C_δ.

Since δ is the coset leader of C_δ, we know Property P3 is true. This completes the proof of the conclusion on the dimension of the code $\mathcal{C}_{(q,m,\delta)}$. □

Theorem 13 says that $\mathcal{R}_q(1,m)^*$ is a BCH code. In general, the punctured generalized Reed-Muller code $\mathcal{R}_q(\ell,m)^*$ is not a BCH code.

Example 4: Let $(q,m)=(3,3)$ *and let* $(\ell_0,\ell_1)=(1,0)$. *Let* α *be a generator of* $\mathrm{GF}(3^3)^*$ *with* $\alpha^3+2\alpha+1=0$. *Then* $\ell=1$ *and* $\delta=17$. *The two codes* $\mathcal{C}_{(3,3,17)}$ *and* $\mathcal{R}_3(1,3)^*$ *are the same, and have parameters* $[26,4,17]$.

It is noticed that the code $\mathcal{C}_{(q,m,(q-1)q^{m-1}-1)}$ is optimal, as its parameters meet the Griesmer bound.

C. The Codes $\mathcal{C}_{(q,m,\delta)}$ in the Case That $\ell = h(q-1)$, Where $1 \le h \le m-1$

Recall that $\ell=\ell_1(q-1)+\ell_0$, where $0\le\ell_0\le q-1$. Hence in this case we have $(\ell_1,\ell_0)=(h,0)$ and $\delta=q^{m-h}-1$.

The parameters of the code $\mathcal{C}_{(q,m,\delta)}$ in this case can be determined and are given as follows.

Theorem 14: For any h *with* $1\le h\le m-1$, $\mathcal{C}_{(q,m,q^{m-h}-1)}$ *has minimum distance* $d=q^{m-h}-1$ *and dimension*

$$m+q^m-1-\sum_{i=1}^{\lfloor \frac{m}{h+1}\rfloor}(-1)^{i-1}\frac{m(q-1)^i}{i}\binom{m-ih-1}{i-1}q^{m-i(h+1)}.$$

Proof: Recall that $\delta=q^{m-h}-1$. Obviously, $q^h\delta=n-(q^h-1)$. It is then easily verified that

$$C_\delta=\Big\{n-(q^{h+i}-q^i):i=1,2,\ldots,m-h\Big\}\cup\Big\{q^i-q^{(h+i) \bmod m}:i=m-h+1,\ldots,m\Big\}.$$

We now prove that $|C_\delta|=m$. First of all, for any two distinct i and j in $\{1,2,\ldots,m-h\}$, we have

$$n-(q^{h+i}-q^i)\ne n-(q^{h+j}-q^j).$$

Secondly, we have

$$\Big\{q^i-q^{(h+i) \bmod m}:i=m-h+1,\ldots,m\Big\}=\Big\{(q^{m-h}-1)q^i:i=1,2,\ldots,h\Big\}.$$

This set has clearly cardinality h.

It is obvious that

$$n=q^m-1=(q-1)(q^{m-1}+q^{m-2}+\ldots+q+1)$$

and

$$(q^h-1)q^i=(q-1)\sum_{\ell=0}^{h-1}q^{i+\ell},$$

$$(q^{m-h}-1)q^j=(q-1)\sum_{\ell=0}^{m-h-1}q^{j+\ell}.$$

We then deduce that

$$n-(q^h-1)q^i\ne(q^{m-h}-1)q^j$$

for any $1\le i\le m-h$ and $1\le j\le h$. Thus, $|C_\delta|=m$.

TABLE I

PARAMETERS OF $\mathcal{C}_{(q,m,q^{m-h}-1)}$ AND $\mathcal{R}_q(h(q-1),m)^*$

n	k_1	k_2	d	q	m	h
31	16	16	7	2	5	2
31	26	26	3	2	5	3
63	24	22	15	2	6	2
63	45	42	7	2	6	3
63	57	57	3	2	6	4
127	36	29	31	2	7	2
127	78	64	15	2	7	3
127	106	99	7	2	7	4
26	23	23	2	3	3	2
80	60	50	8	3	4	2
242	157	96	26	3	5	2
242	217	192	8	3	5	3
255	211	150	15	4	4	2
1023	788	357	63	4	5	2

Furthermore, one can check that δ is the coset leader of C_δ. It then follows that $\delta\notin\cup_{j=1}^{\delta-1}C_j$. We then conclude that the difference between the dimensions of the two codes $\mathcal{C}_{(q,m,\delta+1)}$ and $\mathcal{C}_{(q,m,\delta)}$ is m. The desired conclusion on the dimension of the code $\mathcal{C}_{(q,m,\delta)}$ follows from the dimension of the code $\mathcal{C}_{(q,m,\delta+1)}$, which was given in Theorem 2. □

The two codes $\mathcal{C}_{(q,m,\delta)}$ and $\mathcal{R}_q(\ell,m)^*$ have the same minimum distance δ, and the former contains the latter as a subcode. In the case that $\ell=h(q-1)$, the dimension of $\mathcal{C}_{(q,m,\delta)}$ is given in (11) and that of $\mathcal{R}_q(\ell,m)^*$ is described in (6). However, it is hard to compare the two dimensions as the two dimension formulas look quite complex. In order to compare the two codes, we computed the parameters of some examples of the two codes and put them in Table I, where k_1 and k_2 are the dimensions of $\mathcal{C}_{(q,m,\delta)}$ and $\mathcal{R}_q(\ell,m)^*$, respectively. In most cases, $\mathcal{C}_{(q,m,\delta)}$ is much better than $\mathcal{R}_q(\ell,m)^*$ as the dimension of the former is much more than that of the latter. Some of the codes $\mathcal{C}_{(q,m,q^{m-h}-1)}$ are optimal, others are the best cyclic codes and almost optimal according to the tables in [11].

D. The Codes $\mathcal{C}_{(q,m,\delta)}$ in the Case That $\ell = 2$

The cases that $(q,\ell)=(2,2)$ and $(q,\ell)=(3,2)$ are covered by the results in Section III-C. Therefore, we need to consider only the case that $q\ge4$. In this case, we have $(\ell_0,\ell_1)=(2,0)$ and thus

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

We have the following conjectured parameters of the code $\mathcal{C}_{(q,m,(q-2)q^{m-1}-1)}$.

Conjecture 1: Let $q\ge4$ *and* $\ell=2$. *Then* $\mathcal{C}_{(q,m,(q-2)q^{m-1}-1)}$ *has parameters*

$$\Big[q^m-1,\ 2^m+m,\quad (q-2)q^{m-1}-1\Big].$$

Example 5: Let $(q,m)=(4,3)$ *and let* $\ell=2$. *The two codes* $\mathcal{C}_{(4,3,31)}$ *and* $\mathcal{R}_4(2,3)^*$ *have parameters* $[63,11,31]$ *and* $[63,10,31]$, *respectively.*

Example 6: Let $(q,m)=(3,4)$ *and let* $\ell=2$. *The two codes* $\mathcal{C}_{(3,4,26)}$ *and* $\mathcal{R}_3(2,4)^*$ *have parameters* $[80,20,26]$ *and* $[80,15,26]$, *respectively.*

Note that the code $\mathcal{R}_q(2,m)^*$ has parameters

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

If Conjecture 1 is true, one would see a huge difference between the dimensions of the two codes $\mathcal{C}_{(q,m,\delta)}$ and $\mathcal{R}_q(2,m)^*$. The former is exponential in m, while the latter is polynomial in m. Both dimensions are independent of q, which is a little amazing.

It can be proved that $\delta = (q-2)q^{m-1}-1$ is a coset leader and $|C_\delta| = m$. Let

$$\gamma = (q-2)\frac{q^m-1}{q-1}.$$

Clearly, $C_\gamma = \{\gamma\}$. Hence, γ is also a coset leader. It can be proved that every integer i with $\delta < i < \gamma$ cannot be a coset leader. Hence, the dimension of the code in the following conjecture is also true if Conjecture 1 is true.

Conjecture 2: Let $q \geq 4$. Then the code $\mathcal{C}_{(q,m,(q-2)(q^m-1)/(q-1))}$ has parameters

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

Example 7: Let $(q,m) = (4,3)$. Then $\gamma = 42$. The cyclic code $\mathcal{C}_{(4,3,42)}$ has parameters $[63, 8, 42]$. *This code is optimal according to the Database. The record code in the Database has the same parameters, but is not cyclic.*

Example 8: Let $(q,m) = (5,2)$ and let α be the generator of $\mathrm{GF}(5^2)^*$ *with $\alpha^2 + 4\alpha + 2 = 0$. Then $\gamma = 18$. The code $\mathcal{C}_{(5,2,18)}$ has parameters* $[24, 4, 18]$ *and parity-check polynomial*

$$h(x) = x^4 + 3x^3 + 3x^2 + 4x + 4.$$

This code is optimal according to the Database, where the record code is not known to be cyclic.

Example 9: Let $(q,m) = (5,3)$ and let α be the generator of $\mathrm{GF}(5^3)^*$ *with $\alpha^3 + 3\alpha + 3 = 0$. Then $\gamma = 93$. The code $\mathcal{C}_{(5,3,93)}$ has parameters* $[124, 8, 93]$ *and parity-check polynomial*

$$h(x) = x^8 + 2x^7 + x^6 + 2x^4 + 4x^2 + 4x + 1.$$

This code is optimal according to the Database, where the record code is not known to be cyclic.

IV. Some Other Classes of BCH Codes

In this section, we study the parameters of several other families of BCH codes. Some of them are related to the BCH codes discussed in the previous sections.

A. The Codes $\mathcal{C}_{(q,\,m,\,q^{m-h}-2)}$

Let h be any integer with $1 \leq h \leq m-1$, and let $\delta = q^{m-h}-1$. The codes $\mathcal{C}_{(q,m,\delta)}$ were dealt with in Section III-C. Clearly, $\mathcal{C}_{(q,m,\delta-1)}$ contains $\mathcal{C}_{(q,m,\delta)}$ as a subcode. Our objective of this section is to obtain parameters of the code $\mathcal{C}_{(q,m,\delta-1)}$ with the parameters of the code $\mathcal{C}_{(q,m,\delta)}$ developed in Section III-C.

The parameters of the code $\mathcal{C}_{(q,m,\delta-1)}$ are given as follows.

Theorem 15: For any h with $1 \leq h \leq m-1$ and $q > 2$, the code $\mathcal{C}_{(q,m,q^{m-h}-2)}$ has minimum distance d with $q^{m-h}-2 \leq d \leq q^{m-h}-1$ and dimension

$$2m + q^m - 1 - \sum_{i=1}^{\lfloor \frac{m}{h+1} \rfloor} (-1)^{i-1} \frac{m(q-1)^i}{i} \binom{m-ih-1}{i-1} q^{m-i(h+1)}.$$

Proof: The lower bound on the minimum distance d of the code $\mathcal{C}_{(q,m,\delta-1)}$ follows from the BCH bound, and the upper bound on d comes from the fact that $\mathcal{C}_{(q,m,\delta)}$ is a subcode of $\mathcal{C}_{(q,m,\delta-1)}$.

We now prove the conclusion on the dimension k of the code $\mathcal{C}_{(q,m,\delta-1)}$. Let $\gamma = \delta - 1 = q^{m-h}-2$. Obviously, $q^h\gamma = n - (2q^h - 1)$. It is then easily verified that

$$C_\gamma = \left\{n - (2q^{h+i} - q^i) : i = 0, 1, \ldots, m-h-1\right\} \cup \left\{q^i - 2q^{(h+i) \bmod m} : i = m-h, \ldots, m-1\right\}.$$

It is now time to prove that $|C_\gamma| = m$. First of all, for any two distinct i and j in $\{0, 1, \ldots, m-h-1\}$, we have

$$n - (2q^{h+i} - q^i) \neq n - (2q^{h+j} - q^j).$$

Secondly, we have

$$\left\{q^i - 2q^{(h+i) \bmod m} : i = m-h, m-h+1, \ldots, m-1\right\} = \left\{(q^{m-h}-2)q^i : i = 0, 1, \ldots, h-1\right\},$$

which has clearly cardinality h, as $q > 2$.

Notice that $q > 2$ and $1 \leq h \leq m-1$. We then deduce that

$$n - (2q^h - 1)q^i \neq (q^{m-h}-2)q^j$$

for any $0 \leq i \leq m-h-1$ and $0 \leq j \leq h-1$. Thus, $|C_\gamma| = m$. Furthermore, one can check that γ is the coset leader of C_γ.

We now conclude that the difference between the dimensions of the two codes $\mathcal{C}_{(q,m,\delta)}$ and $\mathcal{C}_{(q,m,\delta-1)}$ is m. The desired conclusion on the dimension of the code $\mathcal{C}_{(q,m,\delta-1)}$ then follows from the dimension of the code $\mathcal{C}_{(q,m,\delta)}$, which was given in Theorem 14. □

Example 10: Let $(q,m,h) = (3,3,1)$. Then the code $\mathcal{C}_{(3,3,7)}$ has parameters $[26, 14, 7]$, *which has the same parameters as the best linear code in the Database. The upper bound on the minimum distance of any ternary code with length 26 and dimension 14 is 8. This code $\mathcal{C}_{(3,3,7)}$ is the best possible cyclic code [11].*

Example 11: Let $(q,m,h) = (3,4,2)$. Then the code $\mathcal{C}_{(3,4,7)}$ has parameters $[80, 64, 7]$. *The best known ternary linear code of length 80 and dimension 64 has minimum distance* 8 *according to the Database.*

In view that the difference between the upper bound and the lower bound on the minimum distance of the code $\mathcal{C}_{(q,m,\delta-1)}$ is only one, it may not be important to determine the exact minimum distance of the code. Nevertheless, we state the following conjecture.

Conjecture 3: For the code $\mathcal{C}_{(q,m,\delta-1)}$ in Theorem 15, we have $d = q^{m-h}-2$.

B. The BCH Codes $\mathcal{C}_{(q,m,q^{(m+1)/2}+q+2)}$ and $\mathcal{C}_{(q,m,q^{(m+1)/2}+q+3)}$

Throughout this section, let $m \geq 3$ be odd and let $q > 2$. Define $\delta = q^{(m+1)/2} + q + 2$. The parameters of the code $\mathcal{C}_{(q,m,q^{(m+1)/2}+q+2)}$ are described in the following theorem.

Theorem 16: For odd $m \geq 3$ and $q > 2$, $\mathcal{C}_{(q,m,q^{(m+1)/2}+q+2)}$ has parameters $[q^m-1, k, d]$, where

$$k = \begin{cases} q^3 - 1 - 3(q-1)q^{(m-1)/2} - 1 & \text{if } m = 3 \\ q^m - 1 - m(q-1)q^{(m-1)/2} - m & \text{if } m > 3 \end{cases}$$

and

$$d \geq d_B = q^{(m+1)/2} + q + 2.$$

Proof: We first determine the Bose distance of the code $\mathcal{C}_{(q,m,q^{(m+1)/2}+q+2)}$. Let $\delta = q^{(m+1)/2} + q + 2$. We prove that δ is the coset leader of $C_{q^{(m+1)/2}+q+2}$. Note that

$$\delta q^{(m-1)/2} \bmod n = (q+2)q^{(m-1)/2} + 1$$

and $q \geq 3$. It can be verified that

$$\begin{aligned} C_\delta = &\left\{((q+2)q^{(m-1)/2}+1)q^i : i = 0, 1, \ldots, \frac{m-3}{2}\right\} \\ &\cup \left\{2q^{m-1} + q^{(m-1)/2} + 1\right\} \\ &\cup \left\{(2+q+q^{(m+1)/2})q^i : i = 0, 1, \ldots, \frac{m-3}{2}\right\}. \end{aligned}$$

It is then easily seen that δ is the smallest integer in $\mathcal{C}_\delta$ and $|C_\delta| = m$. Whence, $d_B = \delta = q^{(m+1)/2} + q + 2$.

It is now time to find out the dimension k of the code $\mathcal{C}_{(q,m,q^{(m+1)/2}+q+2)}$. Our idea of settling this problem is to make use of the dimension of the code $\mathcal{C}_{(q,m,q^{(m+1)/2}+1)}$, which is equal to

$$q^m - 1 - m(q-1)q^{(m-1)/2} \tag{11}$$

according to Theorem 1. To proceed in this direction, we will prove that all the integers i with $q^{(m+1)/2} + 1 \leq i \leq q^{(m+1)/2} + q$ cannot be coset leaders.

Let $\gamma_i = q^{(m+1)/2} + i$ for any integer i. We have

$$\gamma_i q^{(m-1)/2} \bmod n = iq^{(m-1)/2} + 1 \leq q^{(m+1)/2} + i = \gamma_i$$

for all i with $1 \leq i \leq q$. Whence, γ_i is not a coset leader for all i with $1 \leq i \leq q$.

Now we prove that γ_{q+1} is a coset leader. Observing that

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

one can verify that

$$\begin{aligned} C_{\gamma_{q+1}} = &\left\{((q+1)q^{(m-1)/2}+1)q^i : i = 0, 1, \ldots, \frac{m-3}{2}\right\} \\ &\cup \left\{q^{m-1} + q^{(m-1)/2} + 1\right\} \\ &\cup \left\{(1+q+q^{(m+1)/2})q^i : i = 0, 1, \ldots, \frac{m-3}{2}\right\}. \end{aligned}$$

It can be checked that γ_{q+1} is the smallest integer in $C_{\gamma_{q+1}}$. In addition, we have

$$|C_{\gamma_{q+1}}| = \begin{cases} 1 & \text{if } m = 3, \\ m & \text{if } m > 3. \end{cases}$$

We now deduce that the difference between the dimension of $\mathcal{C}_{(q,m,q^{(m+1)/2}+1)}$ and that of $\mathcal{C}_{(q,m,q^{(m+1)/2}+q+2)}$ is $|C_{\gamma_{q+1}}|$. The desired conclusion on the dimension of $\mathcal{C}_{(q,m,q^{(m+1)/2}+q+2)}$ then follows from the dimension of $\mathcal{C}_{(q,m,q^{(m+1)/2}+1)}$, which was given in (11). □

It is noticed that Theorem 16 is not covered by Theorem 9.

Example 12: Let $(q, m) = (4, 3)$. *Then* $\delta = 22$. *The code* $\mathcal{C}_{(4,3,22)}$ *has parameters* $[63, 26, 22]$. *This code has the same parameters as the best code in the Database, which is not cyclic.*

Example 13: Let $(q, m) = (3, 3)$ *and let* α *be the generator of* $\mathrm{GF}(3^3)^*$ *with* $\alpha^3 + 2\alpha + 1 = 0$. *Then* $\delta = 14$. *The code* $\mathcal{C}_{(3,3,14)}$ *has parameters* $[26, 7, 14]$ *and parity-check polynomial*

$$x^7 + x^6 + 2x^4 + x^2 + 1.$$

This code is optimal according to the Database, while the optimal code in the Database is not cyclic.

Example 14: Let $(q, m) = (5, 3)$ *and let* α *be the generator of* $\mathrm{GF}(5^3)^*$ *with* $\alpha^3 + 3\alpha + 3 = 0$. *Then* $\delta = 32$. *The code* $\mathcal{C}_{(5,3,32)}$ *has parameters* $[124, 63, 32]$. *This code has the same parameters as the best code in the Database, which is not cyclic.*

Conjecture 4: For the code $\mathcal{C}_{(q,m,q^{(m+1)/2}+q+2)}$ *in Theorem 16, we have* $d = \delta = q^{(m+1)/2} + q + 2$.

Theorem 17: For odd $m \geq 7$, *the binary code* $\mathcal{C}_{(2,m,2^{(m+1)/2}+5)}$ *has parameters*

$$[2^m - 1, 2^m - 1 - m(2^{(m-1)/2} + 1), d],$$

where

$$d \geq d_B = 2^{(m+1)/2} + 5.$$

Proof: The proof of this theorem is similar to that of Theorem 16. Note that $2^{(m+1)/2} + 4$ is not a coset leader. The only additional part in the proof is to prove that $2^{(m+1)/2} + 5$ is a coset leader, which can be done in a similar way. We omit the details of the proof. □

Example 15: Let $(q, m) = (2, 7)$. *Then* $\delta = 21$. *The code* $\mathcal{C}_{(2,7,21)}$ *has parameters* $[127, 64, 21]$, *and has the same parameters as the best code in the Database.*

Theorem 18: For odd $m \geq 3$ *and* $q > 3$, $\mathcal{C}_{(q,m,q^{(m+1)/2}+q+3)}$ *has parameters* $[q^m - 1, k, d]$, *where*

$$k = \begin{cases} q^3 - 1 - 3(q-1)q^{(m-1)/2} - 4 & \text{if } m = 3 \\ q^m - 1 - m(q-1)q^{(m-1)/2} - 2m & \text{if } m > 3 \end{cases}$$

and

$$d \geq d_B = q^{(m+1)/2} + q + 3.$$

Proof: One can similarly prove that $q^{(m+1)/2} + q + 3$ is a coset leader of $C_{q^{(m+1)/2}+q+3}$. Then the proof of Theorem 16 can then be extended into a proof of this theorem. The details are omitted here. □

Below we consider the code $\mathcal{C}_{(q,m,\delta)}$ for even m.

Theorem 19: For even $m \geq 2$, *the binary code* $\mathcal{C}_{(2,m,2^{m/2}+3)}$ *has parameters*

$$\left[2^m - 1,\ 2^m - 1 - m2^{(m-2)/2} - m/2,\ d\right],$$

where

$$d \geq d_B = 2^{m/2} + 3.$$

Proof: Since the proof of this theorem is similar to that of some previous theorems in this section, we only provide a sketch of the proof here. Let $\delta = 2^{m/2} + 3$.

One can similarly prove the following:

1) $2^{m/2}+1$ is the coset leader of $\mathcal{C}_{2^{m/2}+1}$ and $|\mathcal{C}_{2^{m/2}+1}| = m/2$.
2) $2^{m/2}+2$ is not the coset leader of $\mathcal{C}_{2^{m/2}+2}$.
3) $2^{m/2}+3$ is the coset leader of $\mathcal{C}_{2^{m/2}+3}$.

We now deduce that $d_B = \delta = 2^{m/2}+3$ and

$$\dim(\mathcal{C}_{(2,m,2^{m/2}+3)}) = \dim(\mathcal{C}_{(2,m,2^{m/2}+1)}) - \frac{m}{2}.$$

By Theorem 1, we have

$$\dim(\mathcal{C}_{(2,m,2^{m/2}+1)}) = 2^m - 1 - m2^{(m-2)/2}.$$

The desired conclusion on the dimension of $\mathcal{C}_{(2,m,2^{m/2}+3)}$ then follows. □

Examples of the codes in Theorem 19 are given below.

Example 16: The code $\mathcal{C}_{(2,4,7)}$ has parameters $[15, 5, 7]$*, where $d = d_B = \delta = 7$, which is optimal. The code $\mathcal{C}_{(2,6,11)}$ has parameters* $[63, 36, 11]$*, where $d = d_B = \delta = 11$, which is the best possible cyclic code and has the same parameters as the best known code in the Database. The code $\mathcal{C}_{(2,8,19)}$ has parameters* $[255, 187, 19]$*, where $d = d_B = \delta = 19$, which has the same parameters as the best known code in the Database.*

Conjecture 5: For the code $\mathcal{C}_{(2,m,2^{m/2}+3)}$ in Theorem 19, we have $d = d_B = 2^{m/2}+3$.

Theorem 20: For $q > 3$ and even $m \geq 2$, the code $\mathcal{C}_{(q,m,q^{m/2}+3)}$ has parameters

$$\left[q^m - 1,\ q^m - 1 - m(q-1)q^{(m-2)/2} - 3m/2,\ d\right],$$

where

$$d \geq d_B = q^{m/2} + 3.$$

Proof: For the same reason, we only provide a sketch of the proof here. Let $\delta = q^{m/2}+3$.

Similarly, one can prove the following statements:

1) $q^{m/2}+1$ is the coset leader of $\mathcal{C}_{q^{m/2}+1}$ and $|\mathcal{C}_{q^{m/2}+1}| = m/2$.
2) $q^{m/2}+2$ is the coset leader of $\mathcal{C}_{q^{m/2}+2}$ and $|\mathcal{C}_{q^{m/2}+2}| = m$.
3) $q^{m/2}+3$ is the coset leader of $\mathcal{C}_{q^{m/2}+3}$.

We then deduce that $d_B = \delta = q^{m/2}+3$ and

$$\dim(\mathcal{C}_{(q,m,q^{m/2}+3)}) = \dim(\mathcal{C}_{(q,m,q^{m/2}+1)}) - \frac{3m}{2}.$$

By Theorem 1, we have

$$\dim(\mathcal{C}_{(q,m,q^{m/2}+1)}) = q^m - 1 - m(q-1)q^{(m-2)/2}.$$

The desired conclusion on the dimension of $\mathcal{C}_{(q,m,q^{m/2}+3)}$ then follows. □

Examples of the codes in Theorem 20 are given below.

Example 17: The code $\mathcal{C}_{(4,2,7)}$ has parameters $[15, 6, 7]$*, where $d = d_B = \delta = 7$, while the best code in the Database has parameters* $[15, 6, 8]$*, which is not cyclic. The code $\mathcal{C}_{(4,4,19)}$ has parameters* $[255, 201, 19]$*, where $d = d_B = \delta = 19$, while the best code in the Database has parameters* $[255, 201, 20]$*, which is not cyclic. The code $\mathcal{C}_{(5,2,8)}$ has parameters* $[24, 13, 8]$*, where $d = d_B = \delta = 8$, which has the same parameters as the best code in the Database.*

Conjecture 6: For the code $\mathcal{C}_{(q,m,q^{m/2}+3)}$ in Theorem 20, we have $d = d_B = q^{m/2}+3$.

Theorem 21: For even $m \geq 6$, the binary code $\mathcal{C}_{(2,m,2^{(m+2)/2}+5)}$ has parameters

$$\left[2^m - 1,\ 2^m - 1 - m2^{m/2} + m/2,\ d\right],$$

where

$$d \geq d_B = 2^{(m+2)/2} + 5.$$

Proof: We only provide a sketch of the proof here. Let $\delta = 2^{(m+2)/2}+5$.

One can similar prove the following:

1) $2^{(m+2)/2}+i$ is not the coset leader of $\mathcal{C}_{2^{(m+2)/2}+i}$ for all i with $1 \leq i \leq 4$.
2) $2^{(m+2)/2}+5$ is the coset leader of $\mathcal{C}_{2^{(m+2)/2}+5}$.

We now deduce that $d_B = \delta = 2^{(m+2)/2}+5$ and

$$\begin{aligned}\dim(\mathcal{C}_{(2,m,2^{(m+2)/2}+5)}) &= \dim(\mathcal{C}_{(2,m,2^{(m+2)/2}+1)}) \\ &= 2^m - 1 - m2^{m/2} + m/2,\end{aligned}$$

where the last equality follows from Theorem 1. □

Examples of the codes in Theorem 21 are given below.

Example 18: The code $\mathcal{C}_{(2,6,21)}$ has parameters $[63, 18, 21]$*, where $d = d_B = \delta = 21$, which is the best possible cyclic code and has the same parameters as the best known code in the Database. The code $\mathcal{C}_{(2,8,37)}$ has parameters* $[255, 131, 37]$*, where $d = d_B = \delta = 37$, which has the same parameters as the best known code in the Database.*

Conjecture 7: For the code $\mathcal{C}_{(2,m,2^{(m+2)/2}+5)}$ in Theorem 21, we have $d = d_B = 2^{(m+2)/2}+5$.

It is noticed that Theorems 19, 20, and 21 are not coved by Theorem 9.

Theorem 22: For $q > 3$ and even $m \geq 2$, the code $\mathcal{C}_{(q,m,2q^{m/2}+3)}$ has parameters

$$\left[q^m - 1,\ q^m - 1 - 2m(q-1)q^{(m-2)/2},\ d\right],$$

where

$$d \geq d_B = 2q^{m/2} + 3.$$

Proof: For the same reason, we only provide a sketch of the proof here. Let $\delta = 2q^{m/2}+3$.

Similarly, one can prove the following statements:

1) $2q^{m/2}+1$ is not the coset leader of $\mathcal{C}_{2q^{m/2}+1}$.
2) $2q^{m/2}+2$ is the coset leader of $\mathcal{C}_{2q^{m/2}+2}$ and $|\mathcal{C}_{2q^{m/2}+2}| = m/2$.
3) $2q^{m/2}+3$ is the coset leader of $\mathcal{C}_{2q^{m/2}+3}$.

We then deduce that $d_B = \delta = 2q^{m/2}+3$ and

$$\dim(\mathcal{C}_{(q,m,2q^{m/2}+3)}) = \dim(\mathcal{C}_{(q,m,2q^{m/2}+1)}) - \frac{m}{2}.$$

By Theorem 1, we have

$$\dim(\mathcal{C}_{(q,m,2q^{m/2}+1)}) = q^m - 1 - 2m(q-1)q^{(m-2)/2} + m/2.$$

TABLE II
BCH CODES $\mathcal{C}_{(q,m,\delta)}$ DELT WITH IN THIS PAPER

m	q	δ	Thm.
Any	Any	$(q-\ell_0)q^{m-\ell_1-1}-1$	10, 11
Even	Any	$(q-\ell_0)q^{m-\ell_1-1}-1$	12
Any	Any	$(q-1)q^{m-1}-1$	13
Any	Any	$q^{m-h}-1$	14
Any	$q\geq 3$	$q^{m-h}-2$	15
Odd	$q>2$	$q^{(m+1)/2}+q+2$	16
Odd	$q=2$	$2^{(m+1)/2}+5$	17
Odd	$q>3$	$q^{(m+1)/2}+q+3$	18
Even	$q=2$	$2^{m/2}+3$	19
Even	$q>3$	$q^{m/2}+3$	20
Even	$q=2$	$2^{(m+2)/2}+5$	21
Even	$q>3$	$2q^{m/2}+3$	22

The desired conclusion on the dimension of $\mathcal{C}_{(q,m,2q^{m/2}+3)}$ then follows. □

Examples of the codes in Theorem 22 are given below.

Example 19: The code $\mathcal{C}_{(4,2,11)}$ has parameters $[15, 3, 11]$*, where $d = d_B = \delta = 11$, which is optimal. The code $\mathcal{C}_{(5,2,13)}$ has parameters* $[24, 8, 13]$*, where $d = d_B = \delta = 13$, which is optimal.*

V. SUMMARY AND CONCLUDING REMARKS

The contributions of this paper are the determination of the parameters or lower bounds on the parameters of the codes $\mathcal{C}_{(q,m,\delta)}$ documented in Sections III and IV. Table II is a summary of the narrow-sense primitive BCH codes treated in this paper. For some of these BCH codes, we were able to determine both their dimension and minimum distance. For others BCH codes, we found their dimension and Bose distance, and conjectured that the Bose distance is in fact the minimum distance. All the seven conjectures made in this paper are supported by Magma with a lot of experimental data. To prove the conjectured minimum distance, we face the difficulty in finding a specific codeword in the code having the conjectured minimum weight. The difficulty in settling the dimension of some BCH codes lies in the determination of all coset leaders less than δ and the sizes of their corresponding q-cyclotomic cosets or all coset leaders larger than δ and the sizes of their corresponding q-cyclotomic cosets. The reader is cordially invited to attack these conjectures.

Finally, we would inform the reader that the narrow-sense primitive BCH codes are among the best linear codes in many cases. We searched for all the narrow-sense primitive BCH codes over GF(2) and GF(3) of length up to 127 and 80, respectively. After comparing them with those in the Database and the tables in [11], we found that almost all of them are either optimal or almost optimal. This demonstrates the theoretical attractiveness of the class of narrow-sense primitive BCH codes. In addition, some BCH codes such as the Reed-Solomon codes are widely used in communication systems, data storage devices, and consumer electronics. This gives another strong motivation for researching into BCH codes.

ACKNOWLEDGEMENTS

The author is very grateful to the reviewers and the Associate Editor, Prof. Chaoping Xing, for their detailed comments and suggestions that improved the presentation and quality of this paper, and Dr. Pascale Charpin for proving helpful information on narrow-sense primitive BCH codes.

REFERENCES

[1] E. F. Assmus and J. D. Key, *Designs and Their Codes* (Cambridge Tracts in Mathematics), vol. 103. Cambridge, U.K.: Cambridge Univ. Press, 1992.
[2] D. Augot, P. Charpin, and N. Sendrier, "Studying the locator polynomials of minimum weight codewords of BCH codes," *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 960–973, May 1992.
[3] D. Augot and N. Sendrier, "Idempotents and the BCH bound," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 204–207, Jan. 1994.
[4] E. R. Berlekamp, "The enumeration of information symbols in BCH codes," *Bell Syst. Tech. J.*, vol. 46, no. 8, pp. 1861–1880, 1867.
[5] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann, *Error-Correcting Linear Codes: Classification by Isometry and Applications*. Berlin, Germany: Springer-Verlag, 2006.
[6] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Inf. Control*, vol. 3, pp. 68–79, Mar. 1960.
[7] R. C. Bose and D. K. Ray-Chaudhuri, "Further results on error correcting binary group codes," *Inf. Control*, vol. 3, no. 3, pp. 279–290, 1960.
[8] P. Charpin, "On a class of primitive BCH-codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 1, pp. 222–228, Jan. 1990.
[9] P. Charpin, "Weight distributions of cosets of two-error-correcting binary BCH codes, extended or not," *IEEE Trans. Inf. Theory*, vol. 40, no. 5, pp. 1425–1442, Sep. 1994.
[10] P. Charpin, "Open problems on cyclic codes," in *Handbook Coding Theory*, vol. 1, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, ch. 11, pp. 963–1063.
[11] C. Ding, *Codes From Difference Sets*. Singapore: World Scientific, 2015.
[12] 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.
[13] D. Gorenstein and N. Zierler, "A class of error-correcting codes in p^m symbols," *J. Soc. Ind. Appl. Math.*, vol. 9, no. 2, pp. 207–214, 1961.
[14] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, vol. 2, pp. 147–156, Sep. 1959.
[15] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[16] T. Kasami and S. Lin, "Some results on the minimum weight of primitive BCH codes (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 18, no. 6, pp. 824–825, Nov. 1972.
[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Mathematical Library). Amsterdam, The Netherlands: North Holland, 1977.
[18] H. B. Mann, "On the number of information symbols in Bose–Chaudhuri codes," *Inf. Control*, vol. 5, no. 2, pp. 153–162, 1962.
[19] W. W. Peterson, "Some new results on finite fields with applications to BCH codes," in *Combinatorial Mathematics and Its Applications*, R. C. Bose and T. A. Dowling, Eds. Chapel Hill, NC, USA: Univ. North Carolina Press, 1969, ch. 9.
[20] Y. Dianwu and H. Zhengming, "On the dimension and minimum distance of BCH codes over GF(q)," *J. Electron.*, vol. 13, no. 3, pp. 216–221, 1996.

Cunsheng Ding (M'98–SM'05) was born in 1962 in Shaanxi, China. He received the M.Sc. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xian, China; and the Ph.D. in 1997 from the University of Turku, Turku, Finland.

From 1988 to 1992 he was a Lecturer of Mathematics at Xidian University, China. Before joining the Hong Kong University of Science and Technology in 2000, where he is currently a Professor of Computer Science and Engineering, he was an Assistant Professor of Computer Science at the National University of Singapore.

His research fields are cryptography and coding theory. He has coauthored five research monographs, and served as a guest editor or editor for ten journals. Dr. Ding co-received the State Natural Science Award of China in 1989.