The Bose and Minimum Distance of a Class of BCH Codes

Cunsheng Ding, *Senior Member, IEEE*, Xiaoni Du, and Zhengchun Zhou

***Abstract*— Cyclic codes are an interesting class of linear codes due to their efficient encoding and decoding algorithms. Bose-Ray-Chaudhuri-Hocquenghem (BCH) codes form a subclass of cyclic codes and are very important in both theory and practice as they have good error-correcting capability and are widely used in communication systems, storage devices, and consumer electronics. However, the dimension and minimum distance of BCH codes are not known in general. The objective of this paper is to determine the Bose and minimum distances of a class of narrow-sense primitive BCH codes.**

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

I. Introduction

THROUGHOUT this paper, let p be a prime and let q be a power of p. An $[n,k,d]$ 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 $(c_0, c_1, \cdots, c_{n-1}) \in \mathrm{GF}(q)^n$ 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 $m \geq 1$ be a positive integer and let $n = q^m - 1$. Let α be a generator of GF$(q^m)^*$. For any i with $1 \leq i \leq q^m - 2$, let $m_i(x)$ denote the minimal polynomial of α^i over GF(q). For any $2 \leq \delta < n = q^m - 1$, 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. 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 Bose-Ray-Chaudhuri-Hocquenghem (BCH) code* with *design distance* δ. It is well known that the codes $\mathcal{C}_{(q,m,\delta)}$ and $\mathcal{C}_{(q,m,\delta')}$ may be equal 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 codes $\mathcal{C}_{(q,m,\delta)}$ are treated in every book 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 we conclude that BCH codes are neither well-understood nor well-studied.

In the 1990's, there were a few papers on narrow-sense primitive BCH codes [1], [2], [5], [12]. However, in the last eighteen years, little progress on the study of these codes has been made. As pointed out by Charpin in [6], it is a well-known hard problem to determine the minimum distance of narrow-sense BCH codes.

The objective of this paper is to determine the Bose distance and the minimum distance of the codes $\mathcal{C}_{(q,m,\delta)}$ with design distance $\delta = q^t + h$, where $1 \leq t \leq m-2$ and $0 \leq h \leq \lfloor (q^t-1)/q^{m-t} \rfloor + 1$.

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

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.

Manuscript received May 9, 2014; revised October 19, 2014; accepted February 6, 2015. Date of publication March 9, 2015; date of current version April 17, 2015. C. Ding's work was supported by the Research Grants Council, University Grants Committee, Hong Kong, under Project 601013. X. Du's work was supported by the National Natural Science Foundation of China under Project 61202395 and Project 61462077 and in part by the Program for New Century Excellent Talents in University under Grant NCET-12-0620. Z. Zhou's work was supported in part by the Natural Science Foundation of China under Project 61201243 and in part by the Sichuan Provincial Youth Science and Technology Fund under Grant 2015JQO004.

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

X. Du is with the College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China (e-mail: ymldxn@126.com).

Z. Zhou is with the School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China (e-mail: zzc@home.swjtu.edu.cn).

Communicated by J. Lahtonen, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2015.2409838

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 [7, 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 equal to $q - \delta$.

When δ is small enough, the dimension k of the code $\mathcal{C}_{(q,m,\delta)}$ is given in the following theorem [12].

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

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

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

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

When $t \geq m/2$ and $\delta = q^t$, we have the following theorem due to Mann [10].

Theorem 2: Let $\delta = q^t$, where $m/2 \leq t \leq m - 2$, and let $r = m - t$. Then the dimension k of the code $\mathcal{C}_{(q,m,\delta)}$ is given by

$$k = \varphi(m) - (q-1)^2 \sum_{i=0}^{r-2} (r - i - 1)\varphi(m - r - i - 2),$$

where $\varphi(m)$ is determined by the following linear recurrence

$$\varphi(m) = q\varphi(m-1) - (q-1)\varphi(m - r - 1), \quad m > r$$

with the initial conditions

$$\varphi(i) = q^i \text{ for } 0 \leq i < r, \quad \text{and } \varphi(r) = q^r - 1.$$

Theorem 2 can be employed to compute the dimension of the code recursively in the case that $t \geq m/2$ and $\delta = q^t$. Further recurrence formulas may be found in [3].

Also, when $\delta = q^t$, Mann derived the following result [10].

Theorem 3: 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 $r = m - t$.

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. As will be seen later, 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, it was conjectured that $d \leq d_B + 4$ for the narrow-sense primitive BCH codes [6]. 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 [9, 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 following result is due to Kasami and Lin [8].

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 [11].

Theorem 6: Suppose a narrow-sense primitive BCH code over GF(q) *with Bose distance δ has $d = \delta$, and $\delta + 1$ is divisible by p, the characteristic of* GF(q). *Then the narrow-sense primitive BCH code over* 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 [4, p. 247].

Theorem 7: Let $\mathcal{C}$ be a narrow-sense BCH code of length n with design distance δ over 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 $\mathcal{C}_{(q,m,\delta)}$ [9, 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 Parameters of $\mathcal{C}_{(q,m,\delta)}$ Are Known

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

- When $(\delta, q) = (3, 2)$, $\mathcal{C}_{(q,m,\delta)}$ 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 $(\delta, q) = (5, 2)$, $\mathcal{C}_{(q,m,\delta)}$ has parameters $[2^m - 1, 2^m - 1 - 2m, 5]$ and generator polynomial

$$\begin{aligned} g_{(2,m,5)}(x) &= \mathrm{lcm}(m_1(x), m_2(x), m_3(x), m_4(x)) \\ &= m_1(x)m_3(x), \end{aligned}$$

where $m \geq 4$.
- When $(\delta, q) = (7, 2)$, $\mathcal{C}_{(q,m,\delta)}$ has parameters $[2^m - 1, 2^m - 1 - 3m, 7]$ and generator polynomial

$m_1(x)m_3(x)m_5(x)$ due to a similar reduction, where $m \geq 5$.

- When $(\delta, q) = (9, 2)$, the code $\mathcal{C}_{(q,m,\delta)}$ has parameters $[2^m - 1, 2^m - 1 - 4m, 9]$ and generator polynomial $m_1(x)m_3(x)m_5(x)m_7(x)$ due to a similar reduction, where $m \geq 7$.
- When $(\delta, q) = (3, 3)$, the code $\mathcal{C}_{(q,m,\delta)}$ 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 $1 \leq \delta < 9$ 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 $\delta \geq 11$.

III. New Results on This Class of BCH Codes With $\delta = q^t + 1$

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

$$C_i = \{iq^j \bmod n : 0 \leq j < \ell_i\},$$

where ℓ_i is the smallest positive integer such that $q^{\ell_i} i \equiv i \pmod{n}$, and is called the *size* of C_i. The smallest integer in C_i is called the *coset leader* of C_i. Let $\Delta_j = \bigcup_{i=1}^{j-1} C_i$ for any $j \geq 2$.

A. The Dimensions of the Codes $\mathcal{C}_{(q,m,q^{m-2}+1)}$

The dimension of the code $\mathcal{C}_{(q,m,q^{m-2}+1)}$ is given in (1), which looks complex. The following theorem gives an alternative formula for the dimension of the code $\mathcal{C}_{(q,m,q^{m-2}+1)}$.

Theorem 9: Let $m \geq 4$. Then the dimension k of the BCH code $\mathcal{C}_{(q,m,q^{m-2}+1)}$ is equal to

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

Proof: For the design distance $\delta = q^{m-2} + 1$, $\tilde{\delta} = q^{m-2}$ is also a design distance of this code $\mathcal{C}_{(q,m,\delta)}$. According to Theorem 2, the dimension k is given by

$$k = \varphi(m) - (q-1)^2\varphi(m-4), \tag{2}$$

where

$$\varphi(m) = q\varphi(m-1) - (q-1)\varphi(m-3) \tag{3}$$

with the initial conditions

$$\varphi(0) = 1,\ \varphi(1) = q,\ \varphi(2) = q^2 - 1.$$

To prove the explicit formula for the dimension of this code, we need to solve the linear recurrence relation of (3). To this end, we solve the following equation

$$x^3 - qx^2 + q - 1 = 0,$$

over the field of complex numbers, which has the following three distinct roots

$$x_1 = 1,\ x_2 = \frac{q-1-\sqrt{q^2+2q-3}}{2},$$
$$x_3 = \frac{q-1+\sqrt{q^2+2q-3}}{2}.$$

Thus, we can assume that $\varphi(m) = \ell + ux_2^m + vx_3^m$ for some constants ℓ, u and v in the field of complex numbers. Solving the following system of equations

$$\begin{cases}\varphi(0) = \ell + u + v = 1,\\ \varphi(1) = \ell + ux_2 + vx_3 = q,\\ \varphi(2) = \ell + ux_2^2 + vx_3^2 = q^2 - 1,\end{cases} \tag{4}$$

we obtain

$$\begin{cases}u(x_2 - 1) + v(x_3 - 1) = q - 1,\\ u(x_2^2 - 1) + v(x_3^2 - 1) = q^2 - 2,\end{cases}$$

which is the same as

$$\begin{cases}u\frac{q-3-\sqrt{q^2+2q-3}}{2} + v\frac{q-3+\sqrt{q^2+2q-3}}{2} = q - 1,\\ u\frac{q^2-3-(q-1)\sqrt{q^2+2q-3}}{2} + v\frac{q^2-3+(q-1)\sqrt{q^2+2q-3}}{2} = q^2 - 2.\end{cases} \tag{5}$$

Solving then (5), we obtain that

$$u = \frac{q^2+2q-3-(q+1)\sqrt{q^2+2q-3}}{2(q^2+2q-3)}$$

and

$$v = \frac{q^2+2q-3+(q+1)\sqrt{q^2+2q-3}}{2(q^2+2q-3)}.$$

It then follows from the first equation in (4) that $\ell = 0$. Hence

$$\varphi(m) = ux_2^m + vx_3^m.$$

From (2), we then obtain

$$\begin{aligned}k &= \varphi(m) - (q-1)^2\varphi(m-4)\\ &= ux_2^{m-4}(x_2^4 - (q-1)^2) + vx_3^{m-4}(x_3^4 - (q-1)^2)\\ &= \left(\frac{q-1-\sqrt{q^2+2q-3}}{2}\right)^m\\ &\quad + \left(\frac{q-1+\sqrt{q^2+2q-3}}{2}\right)^m.\end{aligned}$$

This completes the proof of the conclusion on the dimension of this code. □

As a corollary of Theorem 9, we have the following two results.

Corollary 10: When $q = 2$, the dimension of the BCH code $\mathcal{C}_{(q,m,q^{m-2}+1)}$ is given by

$$k = \left(\frac{1+\sqrt{5}}{2}\right)^m + \left(\frac{1-\sqrt{5}}{2}\right)^m$$

for any $m \geq 4$.

Corollary 11: When $q = 3$, the dimension of the BCH code $\mathcal{C}_{(q,m,q^{m-2}+1)}$ is given by

$$k = \left(1-\sqrt{3}\right)^m + \left(1+\sqrt{3}\right)^m$$

for any $m \geq 4$.

B. The Bose and Minimum Distance of the Class of Codes $\mathcal{C}_{(q,m,q^t+h)}$ With $0 \le h \le \lfloor (q^t-1)/q^{m-t} \rfloor + 1$

Given the design distance δ, determining the Bose distance of the code $\mathcal{C}_{(q,m,\delta)}$ is a difficult problem in general. However, this problem may be solvable for special types of δ. The next lemma demonstrates this.

Lemma 12: Let $\delta = q^t + 1$. The Bose distance d_B of the code $\mathcal{C}_{(q,m,\delta)}$ is given by

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

Proof: We divide the proof of the conclusion into two cases: Case A in which $t \le m/2$ and Case B in which $t > m/2$. As before, we define

$$\Delta_\delta = \bigcup_{i=1}^{\delta-1} C_i.$$

In Case A, we have $t \le m/2$ and then

$$\delta_B := \left\lfloor \frac{n-1}{q^{m-t}-1} \right\rfloor + 1 = q^t + \left\lfloor \frac{q^t-2}{q^{m-t}-1} \right\rfloor + 1 = q^t + 1.$$

Hence, in this case we only need to prove that $\delta \notin \Delta_\delta$.

For any i with $0 \le i \le m-1$, define $J_i = \delta q^i \bmod n$. When $t + i < m$, we have

$$J_i = q^{t+i} + q^i \ge q^t + 1 = \delta.$$

When $t + i \ge m$, we have $i \ge m - t \ge m/2$. On the other hand, $t + i \le m + m/2$. Consequently,

$$J_i = q^{(t+i) \bmod m} + q^i \ge q^{m/2} + 1 \ge \delta.$$

Hence $J_i \notin \Delta_\delta$ for all i with $0 \le i \le m-1$. It then follows that $d_B = \delta_B = \delta$ in Case A.

In Case B, by definition $t > m/2$. We have then $t > m - t$. Thus, there are two unique integers u and v such that

$$t = u(m-t) + v,$$

where $u \ge 1$ and $0 \le v < m - t$. It then follows that

$$\begin{aligned}\delta_B &:= \left\lfloor \frac{n-1}{q^{m-t}-1} \right\rfloor + 1 \\ &= q^t + q^v\left(\frac{q^{(m-t)u}-1}{q^{m-t}-1}\right) + \left\lfloor \frac{q^v-2}{q^{m-t}-1} \right\rfloor + 1 \\ &= \begin{cases} q^t + q^v\left(\frac{q^{(m-t)u}-1}{q^{m-t}-1}\right) + 1 & \text{if } 1 \le v < m-t, \\ q^t + \frac{q^{(m-t)u}-1}{q^{m-t}-1} & \text{if } v = 0. \end{cases}\end{aligned}$$

Case B is further divided into two subcases. In the first subcase (called Subcase B.1 later), we assume that $v = 0$. Since $t > m/2$, we have $u \ge 2$ and $t = (m-t)u$. In this subcase,

$$\delta_B = q^{(m-t)u} + q^{(m-t)(u-1)} + \ldots + q^{m-t} + 1.$$

We now prove that $d_B = \delta_B$ in Subcase B.1. To this end, we first prove that every integer i with $\delta \le i \le \delta_B - 1$ belongs to Δ_δ.

Note that $\delta = q^t + 1 = q^{(m-t)u} + 1$ and

$$\delta q^{m-t} \bmod n = 1 + q^{m-t} < \delta.$$

It then follows that $\delta \in \Delta_\delta$. This means that

$$\Delta_{\delta+1} = \Delta_\delta. \tag{6}$$

We now prove that

$$\Delta_{q^{(m-t)u}+q^{(m-t)(u-1)}+1} = \Delta_\delta. \tag{7}$$

Let $j = q^{(m-t)u} + j_0$ with $1 \le j_0 \le q^{(m-t)(u-1)}$. We have then

$$jq^{m-t} \bmod n = 1 + j_0 q^{m-t} \le \delta.$$

The desired conclusion then follows from (6).

If $u = 2$, the proof of the desired conclusion in Subcase B.1 is completed. If $u \ge 3$, we then prove that

$$\Delta_{q^{(m-t)u}+q^{(m-t)(u-1)}+q^{(m-t)(u-2)}+1} = \Delta_\delta.$$

Let

$$j = q^{(m-t)u} + q^{(m-t)(u-1)} + j_0,$$

where $1 \le j_0 \le q^{(m-t)(u-2)}$. We have then

$$\begin{aligned} jq^{2(m-t)} \bmod n &= 1 + q^{m-t} + j_0 q^{2(m-t)} \\ &< q^{(m-t)u} + q^{(m-t)(u-1)} + 1. \end{aligned}$$

The desired conclusion then follows from (7).

If $u = 3$, the proof of the desired conclusion is completed. If $u \ge 4$, we continue this process until we prove that $\{\delta, \delta+1, \ldots, \delta_B - 1\} \subset \Delta_\delta$.

To finish the proof of the desired conclusion in Subcase B.1, we need to prove that $\delta_B \notin \Delta_\delta$. This is indeed true as the q-cyclotomic coset modulo n containing δ_B is given by

$$C_{\delta_B} = \{q^j \delta_B : 0 \le j \le m - t - 1\}.$$

Hence δ_B must be the coset leader of C_{δ_B}. To summarize, we have $d_B = \delta_B$ in Subcase B.1.

In the second subcase (called Subcase B.2 later), we assume that $1 \le v < m - t$ and have

$$\delta_B = q^{(m-t)u+v} + q^{(m-t)(u-1)+v} + \ldots + q^{(m-t)+v} + q^v + 1.$$

The proof of the conclusion that $d_B = \delta_B$ in Subcase B.2 is similar and is omitted here. □

The proof of Lemma 12 showed that the Bose distance d_B is equal to the design distance $\delta = q^t + 1$ when $t \le m/2$.

The main result of this paper is the following.

Theorem 13: When $m \ge 4$, the code $\mathcal{C}_{(q,m,q^t+1)}$ 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 3 when $t > \lceil m/2 \rceil$; and*
- *also Theorem 9 when $t = m - 2$.*

If $t \equiv 0 \pmod{m-t}$, the minimum distance d of the code $\mathcal{C}_{(q,m,q^t+1)}$ is given by

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

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

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

Proof: The lower bound on d follows from Lemma 12 and the BCH bound.

When $m \equiv 0 \pmod{m - t}$, it was shown in the proof of Lemma 12 that the Bose distance d_B is given by

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

which divides the length n of this code. It then follows from Theorem 7 that $d = d_B$.

When $m \equiv 0 \pmod{2t}$, we have $t \le m/2$. The proof of Lemma 12 shows that $d_B = \delta$. It follows from $m \equiv 0 \pmod{2t}$ that δ divides n. It then follows from Theorem 7 that $d = \delta$. □

As a corollary of Theorem 13, we have the following.

Corollary 14: When $m \ge 4$, $q = 2$ and $\delta = 2^{m-2} + 1$, the code $\mathcal{C}_{(2,m,2^{m-2}+1)}$ has parameters $[2^m - 1, k, d]$, where the dimension k is given in Corollary 10 and

$$d \ge \frac{2^m + 1}{3}$$

if m is odd; and

$$d = \frac{2^m - 1}{3}$$

if m is even.

We have the following conjecture on the code $\mathcal{C}_{(2,m,2^{m-2}+1)}$.

Conjecture 1: Let m be odd. Then the minimum distance d of the binary cyclic code $\mathcal{C}_{(2,m,2^{m-2}+1)}$ is given by

$$d = \frac{2^m + 1}{3}.$$

To prove this conjecture, we may find a codeword of $\mathcal{C}_{(2,m,2^{m-2}+1)}$ with weight $(2^m + 1)/3$. Experimental data indicates that the generating idempotent of $\mathcal{C}_{(2,m,2^{m-2}+1)}$ has weight

$$d_B = \frac{2^m + 1}{3}.$$

But we were not able to prove this. The reader is cordially invited to attack this open problem.

In fact, we have the following more general conjecture on the code $\mathcal{C}_{(q,m,q^t+1)}$.

Conjecture 2: The minimum distance d of the cyclic code $\mathcal{C}_{(q,m,q^t+1)}$ is always equal to its Bose distance d_B, which is given in Lemma 12.

When $m - t$ divides t, this conjecture is true. However, the problem is still open in other cases. It would be nice if this conjecture can be proved or disproved. Reference [2] may be useful in attacking this conjecture.

It is easily seen that $\Delta_{q^t+1} = \Delta_{q^t+h}$ for any h with $0 \le h \le \lfloor (q^t - 1)/q^{m-t} \rfloor + 1$. Hence we have $\mathcal{C}_{(q,m,q^t+1)} = \mathcal{C}_{(q,m,q^t+h)}$ for any h with $0 \le h \le \lfloor (q^t - 1)/q^{m-t} \rfloor + 1$. Thus, all the conclusions about $\mathcal{C}_{(q,m,q^t+1)}$ stated in this paper are true for $\mathcal{C}_{(q,m,q^t+h)}$ for any h with $0 \le h \le \lfloor (q^t - 1)/q^{m-t} \rfloor + 1$.

TABLE I
EXAMPLES OF BINARY BCH CODES $\mathcal{C}_{(q,m,q^t+1)}$

n	k	$d = d_B$	δ	m	q	Optimality
15	11	3	3	4	2	Yes
15	7	5	5	4	2	Yes
31	26	3	3	5	2	Yes
31	21	5	5	5	2	Yes
31	11	11	9	5	2	Yes
63	57	3	3	6	2	Yes
63	51	5	5	6	2	Yes
63	39	9	9	6	2	Best known
63	18	21	17	6	2	Best known
127	120	3	3	7	2	Yes
127	113	5	5	7	2	Yes
127	99	9	9	7	2	Best known
127	71	19	17	7	2	Best known
127	29	43	33	7	2	Best known
255	247	3	3	8	2	Yes
255	239	5	5	8	2	Yes
255	223	9	9	8	2	Best known
255	191	17	17	8	2	Best known
255	131	37	33	8	2	Best known
255	47	85	65	8	2	Best known

TABLE II
EXAMPLES OF NONBINARY BCH CODES $\mathcal{C}_{(q,m,q^t+1)}$

n	k	$d = d_B$	δ	m	q	Optimality
26	20	4	4	3	3	Yes
80	72	10	4	4	3	Yes
80	56	10	10	4	3	Best known
242	232	4	4	5	3	Yes
242	212	10	10	5	3	Best known
63	51	5	5	3	4	Almost
255	239	5	5	4	4	Almost
255	191	17	17	4	4	Not best known
124	112	6	6	3	5	Best known

IV. Summary and Concluding Remarks

The main contribution of this paper is the Bose distance of the codes $\mathcal{C}_{(q,m,q^t+h)}$ given in Theorem 13, where $0 \le h \le \lfloor (q^t - 1)/q^{m-t} \rfloor + 1$. In the case that $m \equiv 0 \pmod{m - t}$, both the Bose and minimum distance of the codes are determined in this paper.

Although BCH codes are asymptotically bad, narrow-sense primitive binary BCH codes of length up to 257 are either optimal or the best known linear codes. Table I contains examples of the binary code $\mathcal{C}_{(q,m,\delta)}$. Table II consists of examples of nonbinary narrow-sense primitive BCH codes, which are optimal, or almost optimal, or the best known linear codes.

Lemma 12 shows that the Bose distance is sometimes much more than the design distance $\delta = q^t + 1$. This might explain why the codes $\mathcal{C}_{(q,m,\delta)}$ are either optimal or the best linear codes known.

In general, the dual of a BCH code may not be a BCH code. The dual codes $\mathcal{C}^{\perp}_{(q,m,q^t+1)}$ are also optimal or the best linear codes known for certain lengths, as demonstrated in Table III. The dimension of the code $\mathcal{C}^{\perp}_{(q,m,q^t+1)}$ is $n - k$, where k is given in Theorem 9. But we still do not know the minimum distance $d^{\perp}$ of this code. For the special case that $t = m - 2$, we have the following conjecture.

TABLE III
EXAMPLES OF THE DUAL CODES $\mathcal{C}^{\perp}_{(q,\, m,\, q^t+1)}$

n	k	d	δ	m	q	Optimality
15	4	8	3	4	2	Yes
15	8	4	5	4	2	Yes
31	5	16	3	5	2	Yes
31	10	12	5	5	2	Yes
31	20	6	9	5	2	Yes
63	6	32	3	6	2	Yes
63	12	24	5	6	2	Yes
63	24	14	9	6	2	Best known
63	45	8	17	6	2	Yes
127	7	64	3	7	2	Yes
127	14	56	5	7	2	Yes
127	28	44	9	7	2	Best known
127	56	22	17	7	2	Not best known
127	98	10	33	7	2	Best known

Conjecture 3: The minimum distance $d^{\perp}$ *of the binary code* $\mathcal{C}^{\perp}_{(2,\, m,\, 2^{m-2}+1)}$ *is equal to* $2(m-2)$.

Acknowledgment

The authors are grateful to the reviewers and the Associate Editor, Dr. Jyrki Lahtonen, for their comments and suggestions that improved the presentation and quality of this paper, and to Dr. Pascale Charpin for proving information on known results on narrow-sense primitive BCH codes.

References

[1] D. Augot, P. Charpin, and N. Sendrier, "Studying the locator polynomials of minimum weight codewords of BCH codes," *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 960–973, May 1992.

[2] D. Augot and N. Sendrier, "Idempotents and the BCH bound," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 204–207, Jan. 1994.

[3] E. R. Berlekamp, "The enumeration of information symbols in BCH codes," *Bell Syst. Tech. J.*, vol. 46, no. 8, pp. 1861–1880, Oct. 1867.

[4] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann, *Error-Correcting Linear Codes*. Berlin, Germany: Springer-Verlag, 2006.

[5] P. Charpin, "On a class of primitive BCH-codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 1, pp. 222–228, Jan. 1990.

[6] P. Charpin, "Open problems on cyclic codes," in *Handbook of Coding Theory*, vol. 1, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, pp. 963–1063.

[7] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[8] 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.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes* (North-Holland Mathematical Library). Amsterdam, The Netherlands: North-Holland, 1977.

[10] H. B. Mann, "On the number of information symbols in Bose–Chaudhuri codes," *Inf. Control*, vol. 5, no. 2, pp. 153–162, Jun. 1962.

[11] 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.

[12] Y. Dianwu and H. Zhengming, "On the dimension and minimum distance of BCH codes over GF(q)," *J. Electron.*, vol. 13, no. 3, pp. 216–221, Jul. 1996.

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 four 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.

Xiaoni Du was born in Gansu in 1972. She received the M.S. degree from Lanzhou University in 2000 and the Ph.D. in Cryptography from Xidian University in 2008. She is currently a professor at Northwest Normal University. Her research interests include coding theory, cryptography and information security.

Zhengchun Zhou received the B.S. and M.S. degrees in mathematics and the Ph.D. degree in information security from Southwest Jiaotong University, Chengdu, China, in 2001, 2004, and 2010, respectively. From 2012 to 2013, he was a postdoctoral member in the Department of Computer Science and Engineering, the Hong Kong University of Science and Technology. From 2013 to 2014, he was a research associate in the Department of Computer Science and Engineering, the Hong Kong University of Science and Technology. Since 2001, he has been in the Department of Mathematics, Southwest Jiaotong University, where he is currently a professor. His research interests include sequence design and coding theory.

Dr. Zhou was the recipient of the National excellent Doctoral Dissertation award of China in 2013.