J. Algebra Comb. Discrete Appl.
10(3) • 149–159

Received: 14 February 2022
Accepted: 27 January 2023

Journal of Algebra Combinatorics Discrete Structures and Applications

On the parameters of a class of narrow sense primitive BCH codes

Research Article

El Mahdi Mouloua, M. Najmeddine

Abstract: The last few decades have seen an increase in the determination of the parameters of the primitive BCH codes. Indeed, BCH codes are powerful in terms of encoding and decoding. They are applied in several fields such as: satellite communications, cryptography, compact disk drives etc, and have good structural properties. Nevertheless, the dimension and the minimum distance of those codes are not known in general. In this paper, we present a class of narrow sense primitive BCH codes of designed distance $\delta_4 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m+3}{2} \rfloor}$. Also, we investigate their Bose distance and dimension.

2010 MSC: 11T71, 94B15

Keywords: BCH codes, Cyclic codes, Bose distance, Cyclotomic cosets, Minimum distance

1. Introduction

In coding theory, cyclic codes are considered as an important class of codes. They include a special subclass, discovered by **B**ose and **R**ay-**C**haudhuri in 1960 [12], and independently by **H**ocquenghem in 1959 [2], known as BCH codes. Indeed, BCH codes have a good error-correcting capability. In many cases, BCH codes are the best linear codes, but the exact dimension and minimum weight are considered unsolved[11].

Recent results on the determination of the parameters of narrow sense primitive BCH codes can be found in [1, 3–8, 10, 14].

Let $\mathbb{F}_q$ be the finite field of q elements, such that q is a prime power. We recall that an $[n, k, d]$ linear code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$, where d is its Hamming minimum distance, and n is its length. An $[n, k]$ code C is cyclic if it is linear and if any cyclic shift of a codeword is also a

E. Mouloua, (Corresponding Author); Department of mathematics, ENSAM–Meknes, Moulay Ismail university, Morocco (email: e.mouloua@edu.umi.ac.ma).
M. Najmeddine; Department of mathematics, ENSAM–Meknes, Moulay Ismail university, Morocco (email: m.najmeddine@umi.ac.ma)

codeword, i.e., whenever $\left(c_0, c_1, \ldots, c_{n-1}\right)$ is in C then so is $\left(c_{n-1}, c_0, \ldots, c_{n-2}\right)$. More information about cyclic codes can be found in [16] page 121. We identify a vector $\left(c_0, \ldots, c_{n-1}\right) \in \mathbb{F}_q^n$ with the polynomial $c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ in the ring $R_n = \dfrac{\mathbb{F}_q[X]}{< x^n - 1 >}$. Thus, we can view an $[n, k]$ cyclic code as a principal ideal of the ring R_n (see [16]). If C is not trivial there exists a unique monic polynomial g that generates the code C, g is called the (standard) generator polynomial of the code C, and g divides the polynomial $x^n - 1$. The polynomial h defined by $h(x) = \dfrac{x^n - 1}{g(x)}$ is called the (parity) check polynomial and gives information on the dual of the cyclic code C. Let δ be an integer in $\{0, \ldots, n-1\}$, and α be a primitive n^{th} root of unity. For any integer i such that $0 \leqslant i \leqslant n-1$, let $M^{(i)}(x)$ denote the minimal ploynomial of α^i. A cyclic code C is said to be a BCH code of designed distance δ, if for some integer $b \geqslant 0$ its generator polynomial noted $g_{(q,m,\delta)}(x)$ is given by :

$$g_{(q,m,\delta)}(x) = lcm\left(M^{(b)}(x), M^{(b+1)}(x), \ldots, M^{(b+\delta-2)}(x)\right),$$

where lcm is the least common multiple of these minimal polynomials. Therefore, $g_{(q,m,\delta)}$ is the lowest degree monic polynomial over $\mathbb{F}_q$ having $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ as zeros, and a word c is in the code if and only if $c(\alpha^b) = c(\alpha^{b+1}) = \ldots = c(\alpha^{b+\delta-2}) = 0$. In the case $b = 1$, we obtain the so called narrow sense BCH codes. The BCH codes of length $n = q^m - 1$ are called the primitive BCH codes. The largest designed distance is called the Bose distance and denoted by d_B. For more results on the Bose distance of BCH codes see [6]. Let $\tilde{g}_{(q,m,\delta)}(x) = (x-1)g_{(q,m,\delta)}(x)$.

Throughout this paper, we adopt the following notation : $n = q^m - 1$, $\delta_4 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m+3}{2} \rfloor}$, and $C_{(q,m,\delta)}$ denotes the narrow sense primitive BCH code of designed distance δ with generator polynomial $g_{(q,m,\delta)}$, and $\tilde{C}_{(q,m,\delta)}$ denotes the primitive BCH code with generator polynomial $\tilde{g}_{(q,m,\delta)}(x)$. According to authors in [4], the code $\tilde{C}_{(q,m,\delta)}$ is a primitive code of designed distance $\delta + 1$, and since $dim(\tilde{C}_{(q,m,\delta)}) = n - deg(\tilde{C}_{(q,m,\delta)})$, we have $dim(\tilde{C}_{(q,m,\delta)}) = dim(C_{(q,m,\delta)}) - 1$. Let A_i be the number of codewords with Hamming weight i, the polynomial $1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$ is called the weight enumerator of the code $C_{(q,m,\delta)}$.
The set $A_1, A_2, \ldots, A_n$ is called the weight distribution of the code $C_{(q,m,\delta)}$. Inspired by the results of [4], we prove that δ_4 is the fourth largest coset leader, and we study the parameters of the code $C_{(q,m,\delta_4)}$. According to [5], author determined the first largest coset leader denoted by $\delta_1 = (q-1)q^{m-1} - 1$ and examined the parameters of the code $C_{(q,m,\delta_1)}$. Later, authors in [4] determined the second and the third largest coset leaders modulo n, denoted respectively $\delta_2 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m-1}{2} \rfloor}$ and $\delta_3 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m+1}{2} \rfloor}$ and studied the parameters of $C_{(q,m,\delta_2)}$ and $C_{(q,m,\delta_3)}$. With their weight distributions. The remainder of this paper is organized as follows. In section 2, preliminaries and notations are introduced. Section 3 is devoted to the exploration of the parameters of the codes $C_{(q,m,\delta_4)}$ and $\tilde{C}_{(q,m,\delta_4)}$. Section 4 concludes the paper.

2. Notation and basic concepts

In order to present the most recent results and apply them to investigate the dimension and the Bose distance of our class of narrow sense primitive BCH codes, we present some auxiliary results on cyclotomic cosets. More details on cyclotomic cosets and code constructions can be found in [9].

Definition 2.1 ([16], page 122)**.** *The $q-$coset modulo n containing an element t is defined by $C_t = \{t, tq, tq^2, \ldots, tq^{l_t - 1}\}$, where l_t is the smallest integer such that $tq^{l_t} \equiv t \pmod{n}$.*

The smallest integer in C_t is called the coset leader of C_t. We denote by $\Gamma_{(q,m)}$ the set of all coset leaders modulo n.

In [14], the authors give a general formula for computing the dimension of narrow sense primitive BCH code.

Proposition 2.2 ([14], Proposition 2.1)**.** *The dimension of the code $C_{(q,m,\delta)}$ is equal to* $1+\sum_{\substack{r\geqslant\delta\\ r\in\Gamma_{(q,m)}}}|C_r|$.

Cyclotomic cosets can be used to determine the Bose distance of narrow sense primitive BCH codes. The following proposition gives the connection between d_B and coset leaders. For more details about the proof we refer the readers to [13] page 3.

Proposition 2.3 ([13], Proposition 4, page 3)**.** *The Bose distance of the code $C_{(q,m,\delta)}$ is a coset leader of a q-cyclotomic coset modulo n. Furthermore if δ is a coset leader, then $d_B=\delta$.*

Next, we present some lemmas, that we will need later.

Lemma 2.4 ([1], Lemma 2.1)**.** *Let a and b be two positive distinct integers less than or equal to n. Let $\sum_{j=0}^{m-1} a_jq^j$ and $\sum_{j=0}^{m-1} b_jq^j$ be the $q-$adic expansions of a and b respectively. Set*

$$k=min\left\{i\in\mathbb{N}:0\leq i\leq m-1, a_{m-1-i}\neq b_{m-1-i}\right\}.$$

Then we have $a>b$ if and only if $a_{m-1-k}>b_{m-1-k}$.

Lemma 2.5. *For non-negative integers a and j with $0\leqslant a\leqslant n-1$ such that $a=\sum_{i=0}^{m-1}a_iq^i$ and $1\leqslant j\leqslant m-1$ we have*

$$\left[q^ja\right]_n=\left(a_{m-(j+1)},a_{m-(j+2)},a_{m-(j+3)},\dots,a_{m-j+2},a_{m-j+1},a_{m-j}\right),$$

where $[c]_n=(c_{m-1},c_{m-2},\dots,c_1,c_0)$ if $c=c_0+c_1q+\cdots+c_{m-2}q^{m-2}+c_{m-1}q^{m-1}$ (mod n).

Proof. Since

$$\begin{aligned} a &= a_0+a_1q+a_2q^2+\cdots+a_{m-(j+2)}q^{m-(j+2)}+a_{m-(j+1)}q^{m-(j+1)}+\\ & a_{m-j}q^{m-j}+a_{m-j+1}q^{m-j+1}+a_{m-j+2}q^{m-j+2}+\cdots+a_{m-1}q^{m-1},\end{aligned}$$

for all $1\leqslant j\leqslant m-1$,

$$\begin{aligned} q^ja &= a_0q^j+a_1q^{j+1}+a_2q^{j+2}+\cdots+a_{m-(j+2)}q^{m-2}+a_{m-(j+1)}q^{m-1}+\\ & a_{m-j}+a_{m-j+1}q+a_{m-j+2}q^2+\cdots+a_{m-1}q^{m-1+j} \pmod{n}.\end{aligned}$$

Hence, $\left[q^ja\right]_n=\left(a_{m-(j+1)},a_{m-(j+2)},a_{m-(j+3)},\dots,a_{m-j+2},a_{m-j+1},a_{m-j}\right)$. □

Lemma 2.6 ([4], Lemma 5, Lemma 7, Lemma 12)**.** *Let*

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

Then we have :

1. *δ_1 is the first largest $q-$cyclotomic coset modulo n and $|C_{\delta_1}|=m$.*
2. *δ_2 is the second largest $q-$cyclotomic coset modulo n. Furthermore*

$$\begin{cases}\left|C_{\delta_2}\right| = m & \textit{if}\quad m\quad \textit{is odd,}\\ \left|C_{\delta_2}\right| = \dfrac{m}{2} & \textit{if}\quad m\quad \textit{is even.}\end{cases}$$

3. For $m \geqslant 4$, δ_3 is the third largest $q-$cyclotomic coset modulo n and $\left|C_{\delta_3}\right| = m$.

Below we give an overview about the recent results on the parameters of the codes $C_{(q,m,\delta_1)}$, $C_{(q,m,\delta_2)}$ and $C_{(q,m,\delta_3)}$.

Theorem 2.7 ([5], theorem 13, page 5325)**.** *The two cyclic codes $C_{(q,m,\delta_1)}$ and $R_q(1,m)^*$ are identical, and have parameters $[q^m-1, m+1, (q-1)q^{m-1}-1]$ where $R_q(1,m)^*$ is the first order punctured generalized Reed-Muller code of length n.*

According to authors in [16], a linear code C of length n over $\mathbb{F}_q$ and minimum distance at least d is called optimal, if it has $B_q(n,d)$ codewords, where $B_q(n,d)$ is the largest number of codewords in the code C. There are other perspectives on optimizing a code, for more information readers can refer to [16] page 53.

According to authors in [5], the code $C_{(q,m,\delta_1)}$ is optimal. The main results about the parameters of the codes $C_{(q,m,\delta_2)}$, $\tilde{C}_{(q,m,\delta_2)}$, $C_{(q,m,\delta_3)}$, and $\tilde{C}_{(q,m,\delta_3)}$ are given in [4], and according to them we have the following theorems :

Theorem 2.8 ([4], theorem 8, page 243)**.** *The code $\tilde{C}_{(q,m,\delta_2)}$ has parameters $[n,\tilde{k},\tilde{d}]$, where $n = q^m - 1$, $\delta_2 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m-1}{2} \rfloor}$, $\tilde{d} \geqslant \delta_2 + 1$ and*

$$\tilde{k} = \begin{cases} 2m & \text{for odd } m, \\ \dfrac{3m}{2} & \text{for even } m. \end{cases}$$

In particular,

a- For $q = 2$ and m any integer, $\tilde{d} = \delta_2 + 1$.

b- For q an odd prime, $\tilde{d} = \delta_2 + 1$.
The weight distribution in the case a, b are given [4].

Theorem 2.9 ([4], theorem 11, page 250)**.** *Let $m \geqslant 2$ be an integer. The code $C_{(q,m,\delta_2)}$ has parameters $[n,k,d]$, where $n = q^m - 1$, $\delta_2 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m-1}{2} \rfloor}$, $d \geqslant \delta_2$ and*

$$k = \begin{cases} 2m+1 & \text{for odd } m, \\ \dfrac{3m}{2}+1 & \text{for even } m. \end{cases}$$

Furthermore, $d = \delta_2$ if q is prime.

According to authors in [4], the codes $C_{(q,m,\delta_2)}$ and $\tilde{C}_{(q,m,\delta_2)}$ are sometimes optimal, and sometimes have the same parameters as the best known linear codes in the tables of the best known linear codes maintained by Markus Grassl at http://www.codetables.de.

Theorem 2.10 ([4], theorem 13, page 251)**.** *Let $m \geqslant 4$. The code $\tilde{C}_{(q,m,\delta_3)}$ has parameters $[n,\tilde{k},\tilde{d}]$, where $n = q^m - 1$, $\delta_3 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m+1}{2} \rfloor}$, $\tilde{d} \geqslant \delta_3 + 1$ and*

$$\tilde{k} = \begin{cases} 3m & \text{for odd } m, \\ \dfrac{5m}{2} & \text{for even } m. \end{cases}$$

In particular,

a- When $q = 2$ for any integer m, $\tilde{d} = \delta_3 + 1$.

b- If q is an odd prime, and $m \geqslant 4$ is even then $\tilde{d} = \delta_3 + 1$.

c- If q is an odd prime, and $m \geqslant 5$ is odd then $\tilde{d} = \delta_3 + 1$.
The weight distributions in the cases a, b, c and d are given in [4].

Theorem 2.11 ([4], theorem 15, page 254)**.** *Let $m \geqslant 4$. The code $C_{(q,m,\delta_3)}$ has parameters $[n, k, d]$, where $n = q^m - 1$, $\delta_3 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m+1}{2} \rfloor}$, $d \geqslant \delta_3$ and*

$$k = \begin{cases} 3m + 1 & \text{for odd } m, \\ \dfrac{5m}{2} + 1 & \text{for even } m. \end{cases}$$

According to authors in [4], the codes $C_{(q,m,\delta_3)}$ and $\tilde{C}_{(q,m,\delta_3)}$ are sometimes optimal, and sometimes have the same parameters as the best known linear codes in the tables of the best linear known codes maintained by Markus Grassl at http://www.codetables.de.

3. Parameters of the code $C_{(q,m,\delta_4)}$

In order to investigate the parameters of $C_{(q,m,\delta_4)}$, we need the following two lemmas:

Lemma 3.1. *δ_4 is a coset leader in the $q-$cyclotomic coset C_{δ_4} and C_{δ_4} has cardinality m.*

Proof. To prove the lemma, we need to distinguish two cases :

- **Case** 1, m is odd. Then,

$$\delta_4 = (q-1)q^{m-1} - 1 - q^{\frac{m+3}{2}} = n - q^{m-1} - q^{\frac{m+3}{2}} = n - q^{\frac{m+3}{2}}\left(1 + q^{\frac{m-5}{2}}\right)$$

Now, let us determine C_{δ_4}

$$\begin{aligned}
\delta_4 &= n - q^{\frac{m+3}{2}}(1 + q^{\frac{m-5}{2}})\ , \ (\text{mod } n). \\
\delta_4 q &= n - qq^{\frac{m+3}{2}}(1 + q^{\frac{m-5}{2}})\ , \ (\text{mod } n). \\
&= n - (1 + q^{\frac{m+5}{2}})\ , \ (\text{mod } n). \\
\delta_4 q^2 &= n - q(1 + q^{\frac{m+5}{2}})\ , \ (\text{mod } n). \\
&\vdots \\
\delta_4 q^{\frac{m-5}{2}} &= n - q^{\frac{m-7}{2}}(1 + q^{\frac{m+5}{2}})\ , \ (\text{mod } n). \\
\delta_4 q^{\frac{m-3}{2}} &= n - q^{\frac{m-5}{2}}(1 + q^{\frac{m+5}{2}})\ , \ (\text{mod } n). \\
&= n - (1 + q^{\frac{m-5}{2}})\ , \ (\text{mod } n). \\
\delta_4 q^{\frac{m-1}{2}} &= n - q(1 + q^{\frac{m-5}{2}}), \ (\text{mod } n). \\
&\vdots \\
\delta_4 q^{m-3} &= n - q^{\frac{m-3}{2}}(1 + q^{\frac{m-5}{2}})\ , \ (\text{mod } n). \\
\delta_4 q^{m-2} &= n - q^{\frac{m-1}{2}}(1 + q^{\frac{m-5}{2}})\ , \ (\text{mod } n). \\
\delta_4 q^{m-1} &= n - q^{\frac{m+1}{2}}(1 + q^{\frac{m-5}{2}})\ , \ (\text{mod } n).
\end{aligned}$$

If i and j are two distinct integers in the set $\left\{0,1,\dots,\dfrac{m-7}{2}\right\}$, then we have $n-q^{i}(1+q^{\frac{m+5}{2}})=(q-1)q^{m-1}+\cdots+(q-2)q^{i}+\cdots+(q-2)q^{i+\frac{m+5}{2}}+\cdots+(q-1)q+(q-1)$ and $n-q^{j}(1+q^{\frac{m+5}{2}})=(q-1)q^{m-1}+\cdots+(q-2)q^{j}+\cdots+(q-2)q^{j+\frac{m+5}{2}}+\cdots+(q-1)q+(q-1)$.
It is clear, by lemma [2.4], we have $n-q^{i}(1+q^{\frac{m+5}{2}})\neq n-q^{j}(1+q^{\frac{m+5}{2}})$.
By the same reasoning when i and j are two distinct integers in the set $\{0,\dots,\frac{m+3}{2}\}$, we have that $n-q^{i}(1+q^{\frac{m-5}{2}})\neq n-q^{j}(1+q^{\frac{m-5}{2}})$. Thus
$C_{\delta_4}=\left\{n-q^{i}\left(1+q^{\frac{m+5}{2}}\right):i=0,1,\dots,\dfrac{m-7}{2}\right\}\bigcup\left\{n-q^{i}\left(1+q^{\frac{m-5}{2}}\right):i=0,\dots,\dfrac{m+3}{2}\right\}.$
It is clear that $\left|C_{\delta_4}\right|=m$.
Observe that δ_4 is the smallest integer in C_{δ_4}. Indeed, in the set $\left\{n-q^{i}\left(1+q^{\frac{m-5}{2}}\right):i=0,\dots,\dfrac{m+3}{2}\right\}$, δ_4 is the smallest integer. Let's compare δ_4 with $n-q^{\frac{m-7}{2}}(1+q^{\frac{m+5}{2}})$. We have

$$\delta_4-\left(n-q^{\frac{m-7}{2}}(1+q^{\frac{m+5}{2}})\right)=q^{\frac{m-7}{2}}-q^{\frac{m+3}{2}}<0.$$

Thus δ_4 is a coset leader modulo n.

- **Case** 2, m is even. Then,

$$\delta_4=(q-1)q^{m-1}-1-q^{\frac{m+2}{2}}=n-q^{m-1}-q^{\frac{m+2}{2}}=n-q^{\frac{m+2}{2}}\left(1+q^{\frac{m-4}{2}}\right).$$

Let's determine C_{δ_4}.

$$\begin{aligned}
\delta_4 &= n-q^{\frac{m+2}{2}}\left(1+q^{\frac{m-4}{2}}\right), \pmod{n}.\\
\delta_4 q &= n-qq^{\frac{m+2}{2}}\left(1+q^{\frac{m-4}{2}}\right), \pmod{n}.\\
&= n-\left(1+q^{\frac{m+4}{2}}\right), \pmod{n}.\\
\delta_4 q^{2} &= n-q\left(1+q^{\frac{m+4}{2}}\right), \pmod{n}.\\
&\vdots\\
\delta_4 q^{\frac{m-8}{2}} &= n-q^{\frac{m-10}{2}}\left(1+q^{\frac{m+4}{2}}\right), \pmod{n}.\\
\delta_4 q^{\frac{m-6}{2}} &= n-q^{\frac{m-8}{2}}\left(1+q^{\frac{m+4}{2}}\right), \pmod{n}.\\
\delta_4 q^{\frac{m-4}{2}} &= n-q^{\frac{m-6}{2}}\left(1+q^{\frac{m+4}{2}}\right), \pmod{n}.\\
\delta_4 q^{\frac{m-2}{2}} &= n-q^{\frac{m-4}{2}}\left(1+q^{\frac{m+4}{2}}\right), \pmod{n}.\\
&= n-\left(1+q^{\frac{m-4}{2}}\right), \pmod{n}.\\
\delta_4 q^{\frac{m}{2}} &= n-q\left(1+q^{\frac{m-4}{2}}\right), \pmod{n}.\\
&\vdots\\
\delta_4 q^{m-1} &= n-q^{\frac{m}{2}}\left(1+q^{\frac{m-4}{2}}\right), \pmod{n}.
\end{aligned}$$

Thus,
$C_{\delta_4} = \left\{ n - q^i(1 + q^{\frac{m-4}{2}}) : i = 0, 1, \ldots, \frac{m+2}{2} \right\} \bigcup \left\{ n - q^i(1 + q^{\frac{m+4}{2}}) : i = 0, \ldots, \frac{m-6}{2} \right\}.$

It is clear that $\left| C_{\delta_4} \right| = m$.

Observe that δ_4 is the smallest integer in the set $\left\{ n - q^i \left(1 + q^{\frac{m-4}{2}} \right) : i = 0, \ldots, \frac{m+2}{2} \right\}$.

Let's compare δ_4 with $n - q^{\frac{m-6}{2}}(1 + q^{\frac{m+4}{2}})$. We have

$$\delta_4 - (n - q^{\frac{m-6}{2}}(1 + q^{\frac{m+4}{2}})) = q^{\frac{m-6}{2}} - q^{\frac{m+2}{2}} < 0.$$

Thus δ_4 is a coset leader modulo n. □

Now we verify that δ_4 is the fourth largest coset leader modulo n.

Lemma 3.2. *For $m \geqslant 11$, δ_4 is the fourth largest coset leader modulo n.*

Proof. To prove the lemma, we need to distinguish two cases :

○ **Case** 1, m is odd. Then,
$\delta_4 = (q-1)q^{m-1} - 1 - q^{\frac{m+3}{2}}$. We verify that there is no coset leader between δ_3 and δ_4. Set $s = \frac{m-1}{2}$. Then,

$$\begin{aligned} \delta_4 &= (q-1)q^{m-1} - 1 - q^{\frac{m+3}{2}} \\ &= q^m - 1 - q^{m-1} - q^{s+2} \\ &= (q-1)(q^{m-1} + q^{m-2} + \cdots + q + 1) - q^{m-1} - q^{s+2} \\ &= (q-2)q^{m-1} + (q-1)q^{m-2} + \cdots + (q-2)q^{s+2} + (q-1)q^{s+1} + \\ & (q-1)q^s + (q-1)q^{s-1} + \cdots + (q-1)q + (q-1). \end{aligned}$$

With the same argument we have

$$\begin{aligned} \delta_3 &= (q-1)q^{m-1} - 1 - q^{\frac{m+1}{2}} \\ &= q^m - 1 - q^{m-1} - q^{s+1} \\ &= (q-2)q^{m-1} + (q-1)q^{m-2} + \cdots + (q-1)q^{s+2} + (q-2)q^{s+1} + \\ & (q-1)q^s + (q-1)q^{s-1} + \cdots + (q-1)q + (q-1). \end{aligned}$$

Hence

$$\begin{aligned} \delta_3 - \delta_4 &= (q-1)q^{s+2} + (q-2)q^{s+1} - (q-2)q^{s+2} - (q-1)q^{s+1} \\ &= q^{s+2} - q^{s+1} \\ &= q^{s+1}(q-1). \end{aligned}$$

Since $q^{s+1}(q-1) - 1 = (q-2)q^{s+1} + (q-1)q^s + \cdots + (q-1)$, any $i \in \left\{ 1, \ldots, q^{s+1}(q-1) - 1 \right\}$ can be written as $i = i_{s+1}q^{s+1} + i_s q^s + \cdots + i_1 q + i_0$, where $0 \leqslant i_{s+1} \leqslant q-2$ and $0 \leqslant i_l \leqslant q-1$; $l \in \{0, \ldots, s\}$. Let $K_i := \delta_3 - i$ for all $i \in \{1, \ldots, q^{s+1}(q-1) - 1\}$. We are able to give the $q-$adic expansion of K_i and analyze it. Indeed, we have

$$\begin{aligned} K_i &= (q-2)q^{m-1} + (q-1)q^{m-2} + \cdots + (q-1)q^{s+2} + (q-2)q^{s+1} + (q-1)q^s + (q-1)q^{s-1} + \\ & \cdots + (q-1)q - i_{s+1}q^{s+1} - i_s q^s - i_{s-1}q^{s-1} - \ldots - i_1 q - i_0. \end{aligned}$$

Therefore,

$$\begin{aligned} K_i &= (q-2)q^{m-1} + (q-1)q^{m-2} + \cdots + (q-1)q^{s+2} + (q-2-i_{s+1})q^{s+1} + \\ &\quad (q-1-i_s)q^s + (q-1-i_{s-1})q^{s-1} + \cdots + (q-1-i_1)q + (q-1-i_0). \end{aligned}$$

Now we need to verify that K_i cannot be a coset leader. To this end, we consider two subcases as follows.

- *Case* 1 : $q = 2$. In this case, we have :

  $$K_i = 2^{m-2} + \cdots + 2^{s+2} + (1-i_s)2^s + \cdots + (1-i_1)2 + (1-i_0).$$

  Where $i_0 \in \{0, 1\}$.

  - $i_0 = 1$. Then $\frac{K_i}{2}$ and K_i are in the same $q-$cyclotomic coset modulo n, and since $K_i > \frac{K_i}{2}$, K_i cannot be a coset leader.
  - $i_0 = 0$. Then,

    $$K_i = 2^{m-2} + 2^{m-3} + \cdots + 2^{s+2} + (1-i_s)2^s + (1-i_{s-1})2^{s-1} + \cdots + (1-i_1)\,2 + 1.$$

    Since $i \neq 0$, one of the $i_l's$ must be nonzero. Let l denote the largest one such that $i_l = 1$. Thus, we have :

    $$\begin{aligned} K_i &= 0 \times 2^{m-1} + 2^{m-2} + 2^{m-3} + \cdots + 2^{s+2} + 0 \times 2^{s+1} + 2^s + \\ &\quad \cdots + 2^{l+1} + 0 \times 2^l + (1-i_{l-1})2^{l-1} + \cdots + (1-i_1)2 + 1. \\ 2^{m-1-l}K_i &= 0 \times 2^{m-l-2} + 2^{m-l-3} + 2^{m-l-4} + \cdots + 2^{s+1} + \cdots + 2^{s-(l-1)} + \\ &\quad 2^{s-(l+1)} + \cdots + 2 + 1 + 0 \times 2^{m-1} + (1-i_{l-1})2^{m-2} + \\ &\quad \cdots + (1-i_1)2^{m-l} + 2^{m-l-1}. \\ &= 0 \times 2^{m-1} + (1-i_{l-1})2^{m-2} + \cdots + (1-i_1)\,2^{m-l} + 2^{m-l-1} + \\ &\quad 0 \times 2^{m-l-2} + 2^{m-l-3} + 2^{m-l-4} + \cdots + 2^{s+2} + 2^{s+1} + \cdots + \\ &\quad 2^{s-(l-1)} + 0 \times 2^{s-l} + 2^{s-(l+1)} + \cdots + 2 + 1. \end{aligned}$$

    Using lemma [2.4], we confirm that $2^{m-1-l}K_i < K_i$. Hence, K_i cannot be a coset leader. In all cases there is no coset leader between δ_4 and δ_3.

- *Case* 2 : $q > 2$. Then,

  $$\begin{aligned} K_i &= (q-2)q^{m-1} + (q-1)q^{m-2} + \cdots + (q-1)q^{s+2} + \left(q-2-i_{s+1}\right)q^{s+1} + \\ &\quad (q-1-i_s)\,q^s + \left(q-1-i_{s-1}\right)q^{s-1} + \cdots + (q-1-i_1)\,q + (q-1-i_0)\,. \end{aligned}$$

  - If $i_{s+1} \geqslant 1$, then we verify that $q^{m-1-(s+1)}K_i < K_i$.
    By lemma [2.5] we have $\left[q^{m-2-s}K_i\right]_n = ((q-2-i_{s+1}); (q-1-i_s); (q-1-i_{s-1}); \ldots; (q-1-i_1); (q-1-i_0); 0; (q-2); (q-1); \ldots; (q-1))$.
    Since $1 \leqslant i_{s+1} \leqslant q-2$, $q-2-i_{s+1} < q-2$, and by lemma [2.4], K_i cannot be a coset leader.
  - If $i_l \geqslant 2$ for some l with $l \in \{0, \ldots, s\}$, let $K_i = (q-2)q^{m-1} + (q-1)q^{m-2} + \cdots + (q-1)q^{s+2} + (q-2-i_{s+1})q^{s+1} + (q-1-i_s)q^s + (q-1-i_{s-1})q^{s-1} + \ldots + (q-1-i_l)q^l + \ldots + (q-1-i_1)q + (q-1-i_0)$.
    $[q^{m-1-l}K_i]_n = ((q-1-i_l); (q-1-i_{l-1}); (q-1-i_{l-2}); \ldots; (q-1-i_1); (q-1-i_0); 0; (q-2); (q-1); \ldots; (q-1); (q-2-i_{s+1}); (q-1-i_s); \ldots; (q-1-i_{l-1}))$.
    Since $i_l \geqslant 2$, $q-1-i_l \leqslant q-3 < q-2$, and by lemma [2.4], K_i cannot be a coset leader.

– We now assume that $i_l \in \{0,1\}$ for all $0 \leqslant l \leqslant s-1$ and $i_{s+1} = 0$. Since $i \geqslant 1$, at least one of the $i_l's$ must be 1. Let l denote the largest one such that $i_l = 1$. Then we have :

$$\begin{aligned}
K_i &= (q-2)q^{m-1} + (q-1)q^{m-2} + \cdots + (q-1)q^{s+2} + (q-2)q^{s+1} + \\
&\quad (q-1)q^{s} + (q-1)q^{s-1} + \cdots + (q-1)q^{l+1} + (q-2)q^{l} + \\
&\quad (q-1-i_{l-1})q^{l-1} + \cdots + (q-1-i_1)q + (q-1-i_0) \\
q^{m-1-l}K_i &= (q-2)q^{m-2-l} + (q-1)q^{m-3-l} + \cdots + (q-1)q^{s+1-l} + (q-1)q^{s-l} + \\
&\quad (q-1)q^{s-(l+1)} + \cdots + (q-1) + (q-2)q^{m-1} + (q-1-i_{l-1})q^{m-2} \\
&\quad + \cdots + (q-1-i_1)q^{m-l} + (q-1-i_0)q^{m-1-l} \\
q^{m-1-l}K_i &= (q-2)q^{m-1} + \left(q-1-i_{l-1}\right)q^{m-2} + \cdots + \left(q-1-i_1\right)q^{m-l} + \\
&\quad \left(q-1-i_0\right)q^{m-1-l} + (q-2)q^{m-2-l} + (q-1)q^{m-3-l} + \cdots + (q-1)q^{s} + \\
&\quad \cdots + (q-1)q^{s-(l-1)} + (q-1)q^{s-l} + (q-1)q^{s-(l+1)} + \cdots + (q-1).
\end{aligned}$$

By lemma [2.4], K_i cannot be a coset leader.

– **Case** 2, m is even. Then,
$\delta_4 = (q-1)q^{m-1} - 1 - q^{\frac{m+2}{2}}$. We verify that there is no coset leader between δ_3 and δ_4.
Set $s = \frac{m-2}{2}$. Then,

$$\begin{aligned}
\delta_4 &= (q-1)q^{m-1} - 1 - q^{s+2} \\
&= q^{m} - 1 - q^{m-1} - q^{s+2} \\
&= (q-1)(q^{m-1} + q^{m-2} + \cdots + q + 1) - q^{m-1} - q^{s+2} \\
&= (q-2)q^{m-1} + (q-1)q^{m-2} + \cdots + (q-2)q^{s+2} + (q-1)q^{s+1} + \\
&\quad (q-1)q^{s} + (q-1)q^{s-1} + \cdots + (q-1)q + (q-1)
\end{aligned}$$

With the same argument we have :

$$\begin{aligned}
\delta_3 &= (q-1)q^{m-1} - 1 - q^{\frac{m}{2}} \\
&= q^{m} - 1 - q^{m-1} - q^{s+1} \\
&= (q-2)q^{m-1} + (q-1)q^{m-2} + \cdots + (q-1)q^{s+2} + (q-2)q^{s+1} + \\
&\quad (q-1)q^{s} + (q-1)q^{s-1} + \cdots + (q-1)q + (q-1)
\end{aligned}$$

It is similar to the odd case that we follow the same steps for the remainder of the proof.

□

Now we are able to investigate the parameters of the code $C_{(q,m,\delta_4)}$ and the code $\tilde{C}_{(q,m,\delta_4)}$:

Theorem 3.3. *Let $m \geqslant 11$. The code $\tilde{C}_{(q,m,\delta_4)}$ has parameters $[n,k,d]$, where $n = q^m - 1$, $d \geqslant \delta_4 + 1$ and*

$$k = \begin{cases} 4m & \text{if } m \text{ is odd,} \\ \dfrac{7m}{2} & \text{if } m \text{ is even.} \end{cases}$$

Proof. For the value of the dimension we apply the proposition [2.2]. Finally the BCH bound ensures the bound on the minimum distance. □

Corollary 3.4. *For an odd integer m, $m \geqslant 11$, the code $\tilde{C}_{(2,m,\delta_4)}$ has parameters $[n,k,d]$, where $n = 2^m - 1$, $k = 4m$ and $d = 2^{m-1} - 2^{\frac{m+3}{2}}$.*

Weight w	**Number of words of weight** w
0	1
$2^{m-1}+2^{\frac{m-1}{2}}$	$\left(2^{m-1}-2^{\frac{m-1}{2}}\right)\left(151\times 2^{2m-3}+25\times 2^{m}+2^{5}\right)\frac{2^{m-1}}{45}$
$2^{m-1}-2^{\frac{m-1}{2}}$	$(2^{m-1}+2^{\frac{m-1}{2}})(151\times 2^{2m-3}+25\times 2^{m}+2^{5})(\frac{2^{m}-1}{45})$
$2^{m-1}+2^{\frac{m+1}{2}}$	$(2^{m-2}-2^{\frac{m-1}{2}})(23\times 2^{m-5}+1)(2^{m-1}-1)(\frac{2^{m}-1}{9})$
$2^{m-1}-2^{\frac{m+1}{2}}$	$(2^{m-2}+2^{\frac{m-1}{2}})(23\times 2^{m-5}+1)(2^{m-1}-1)(\frac{2^{m}-1}{9})$
$2^{m-1}+2^{\frac{m+3}{2}}$	$(2^{m-6}-2^{\frac{m-7}{2}})(2^{m-3}-1)(\frac{2^{m}-1}{45})$
$2^{m-1}-2^{\frac{m+3}{2}}$	$(2^{m-6}+2^{\frac{m-7}{2}})(2^{m-3}-1)(\frac{2^{m}-1}{45})$
2^{m-1}	$2^{4m}-1-\sum_{j\neq 0,2^{m-1}} A_j$

Table 1. Weight distribution of the code $\tilde{C}_{(2,m,\delta_4)}$

Proof. Since m is odd, and $m \geqslant 11$. Then the dimension of the code $\tilde{C}_{(2,m,\delta_4)}$ is $4m$. According to Kassami in [15] theorem 16 page 24, the code $\tilde{C}_{(2,m,\delta_4)}$ is the same as the code defined under [15] lemma 9 page 15, which has the weight distribution shown in table 1. And since there is a codeword with weight δ_4. Then, the minimum distance of the code $\tilde{C}_{(2,m,\delta_4)}$ is exactly δ_4. □

According to author in [15] page 24. The dual code of the code $\tilde{C}_{(2,m,\delta_4)}$ is a subcode of the dual code of the code $\tilde{C}_{(2,m,\delta_4)}$, which has minimum distance 7.

Example 3.5. *Let $(q,m)=(2,11)$. Then $\delta_4=895$, and $\tilde{C}_{(q,m,\delta_4)}$ has parameters [2047, 44, 896], with the weight enumerator* $1+3574742979584z^{1056}+3805371558912z^{992}+164511003360z^{1088}+186445803808z^{960}+332260852z^{1152}+427192524z^{896}+9860355245375z^{1024}$.

Theorem 3.6. *Let $m \geqslant 11$. The code $C_{(q,m,\delta_4)}$ has parameters $[n,k,d]$, where $n=q^{m}-1$, $d \geqslant d_B$ such that $d_B=\delta_4$, and*

$$k=\begin{cases} 4m+1 & \text{if } m \text{ is odd,} \\ \dfrac{7m}{2}+1 & \text{if } m \text{ is even.} \end{cases}$$

Proof. For the value of the dimension we apply the proposition [2.2], and by proposition [2.3] we find that $d_B=\delta_4$ since $\delta_4 \in \Gamma_{(q,m)}$. Finally BCH bound ensures the bound on the minimum distance. □

Conclusion and further works

By this work we initiate our first reaserch in studying the parameters of narrow sense primitive BCH codes. Our idea in this work was inspired from the ideas proposed by authors in [4]. Thus we give a similar demonstration as the one proposed in [4] to find the fourth largest coset leader modulo $q^{m}-1$, and then investigate the parameters of the code $C_{(q,m;\delta_4)}$ and the code $\tilde{C}_{(q,m,\delta_4)}$. The investigation of the weight distribution of the code $\tilde{C}_{(2,m,\delta_4)}$ for odd $m \geqslant 11$ was presented by Tadao Kassami in [15]. In a future work we plan to study the weight distributions of the codes $C_{(q,m;\delta_4)}$ and $\tilde{C}_{(q,m,\delta_4)}$ by adopting the theory of quadratic forms over the finite field and the theory of association schemes. We also plan to attack some open problems proposed by Cunsheng Ding in [4] about the weight distribution of the extended codes $\tilde{C}_{(q,m,\delta_2)}$ and $\tilde{C}_{(q,m,\delta_3)}$.

Acknowledgment: The authors would like to thank the reviewers for their comments and suggestions that allowed us to correct several errors and improve the readability and quality of the article.

References

[1] A. Cherchem, A. Jamous, H. Lius, Y. Maouche, Some new results on dimension and Bose distance for various classes of BCH codes. Finite Fields Their Appl. 65 (2020).

[2] A. Hocquenghem, Codes correcteurs d'erreurs, Chiffres (Paris) 2 (1959) 147–156.

[3] B. Pang, S. Zhu, X. Kai, Five families of the narrow-sense primitive BCH codes over finite fields. Des. Codes Cryptogr. 89 (2021) 2679–2696.

[4] C. Ding, C. Fan, Z. Zhou, The dimension and minimum distance of two classes of primitive BCH codes, Finite Fields Appl. 340 (2017) 237–263.

[5] C. Ding, Parameters of several classes of BCH codes, IEEE Trans. Inform. Theory 61 (10) (2015) 5322–5330.

[6] C. Ding, X. Du, Z. Zhou, The Bose and minimum distance of a class of BCH codes, IEEE Trans. Inform. Theory 61 (5) (2015) 2351–2356.

[7] C. Li, P. Wu, and F. Liu, On two classes of primitive BCH codes and some related codes, IEEE Transactions on Information Theory, 65 (2019) 3830–3840.

[8] E. Mouloua, M. Najmeddine, O. Hassan, Around the parameters of primitive BCH codes, 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), 2022, pp. 1–7.

[9] G.G. La Guardia, M.M.S. Alves, On cyclotomic cosets and code constructions. Linear Algebra and its Applications, 488 (2016) 302–319.

[10] H. Liu, C. Ding, C. Li, Dimensions of three types of BCH codes over GF(q), Discrete Math. 340 (2017) 1910–1927.

[11] P. Charpin, Open problems on cyclic codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, vol. I, North-Holland, 1998, pp. 963–1063 (Chapter 11).

[12] R. Bose, D. Ray-Chaudhuri, On a class of error correcting binary group codes, Inf. Control 3 (1) (1960) 68–79.

[13] S. Li, C. Ding, M. Xiong, G. Ge, Narrow-sense BCH codes over GF(q) with length $n = \dfrac{q^m - 1}{q - 1}$, IEEE Trans. Inf. Theory 63 (11) (2017) 7219–7236.

[14] S. Li, The minimum distance of some narrow-sense primitive BCH codes, SIAM J. Discrete Math. 31 (2017) 2530–2569.

[15] T. Kasami, Weight distributions of Bose-Chaudhuri-Hocquenghem codes. Combinatorial Mathematics and Its Applications, 36 (1966).

[16] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes. Cambridge University Press, 2003.