On Some Bounds of Minimum Distances of Cyclic Codes over Finite Fields

研究生：林俊佑

中華民國 105 年 6 月
ON SOME BOUNDS OF MINIMUM DISTANCES OF CYCLIC CODES OVER FINITE FIELDS

CHUN-YOU LIN

Abstract. After reviewed the theory of cyclic codes over finite fields, we study some results on lower bounds of minimum distance of cyclic codes. We also give several examples to illustrate these lower bounds.

Keywords. Cyclic Code, Bound on the Minimum Distance.

CONTENTS

1. Introduction 1
2. Cyclic codes over finite fields 2
3. On bounds of minimum distance of cyclic codes 7
4. Some examples 13
References 18

1. INTRODUCTION

In this master thesis, we first review the theory of cyclic codes over finite fields. Then follow the line of van Lint and Wilson [2], we give detailed proofs for the BCH bounds and the HT bound of minimum distance of cyclic codes. Further, we discuss the generalization of the BCH bound developed by Roos([4],[5]). Finally, we construct some examples to illustrate these lower bounds discussed above.

In the final section, we construct some examples for which the above three bounds were evaluated and compared with each other. Among these examples, the first step is to find the defining set of the given cyclic code. Then, for the BCH bound, if one found the defining set contained certain consecutive set, then the minimum distance is greater or equal to the length of this consecutive set plus one. For the HT bound, one needs several consecutive sets with specific condition. For the Roos bound, one starts with a set of roots of unity A, if B is any set of roots of unity satisfies certain condition, then one obtains a lower bound of the minimum distance of the cyclic codes with defining set AB.

Date: 2016.6.24.
2. Cyclic codes over finite fields

Let \( \mathbb{F}_q \) be the finite field of \( q \) elements and \( \mathbb{F}_q^n \) be the set of all vectors of length \( n \) with entries in \( \mathbb{F}_q \).

A linear code \( C \) of length \( n \) over \( \mathbb{F}_q \) is a subspace of \( \mathbb{F}_q^n \).

**Definition 1.** A code \( C \) is cyclic if it is linear and if every element \( (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C \) whenever \( (c_0, c_1, \ldots, c_{n-1}) \in C \).

**Example 2.1.** The following codes are cyclic code

1. three trivial codes \( \{0\} \), \( \{\lambda \cdot 1 : \lambda \in \mathbb{F}_q\} \), \( \mathbb{F}_q^n \).
2. the \([4,2,2]\)-linear code over \( \mathbb{F}_3 \)
   \( \{(0,0,0,0) \ (1,0,1,0) \ (0,1,0,1) \ (2,0,2,0) \ (0,2,0,2) \ (1,1,1,1) \ (2,2,2,2) \ (1,2,1,2) \ (2,1,2,1)\} \).
3. the \([3,1,3]\)-linear code over \( \mathbb{F}_7 \)
   \( \{(0,0,0) \ (1,2,4) \ (2,4,1) \ (4,1,2) \ (3,6,5) \ (5,3,6) \ (6,5,3)\} \).

In order to convert the combinatorial structure of cyclic codes into an algebraic one, we consider the following correspondence:

\[
\phi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]/(x^n - 1),
\]

\[
(c_0, c_1, \ldots, c_{n-1}) \longrightarrow c_0 + c_1x + \cdots + c_{n-1}x^{n-1}
\]

Then \( \phi \) is an \( \mathbb{F}_q \)-linear transformation of vector spaces over \( \mathbb{F}_q \). From now on, we will sometimes identify \( \mathbb{F}_q^n \) with \( \mathbb{F}_q[x]/(x^n - 1) \), and a vector \( (u_0, u_1, \ldots, u_{n-1}) \) with the polynomial \( u(x) = \sum_{i=0}^{n-1} u_ix^i \). We know that \( \mathbb{F}_q[x]/(x^n - 1) \) is a ring (but not a field unless \( n = 1 \)). Thus, there is a multiplicative operation besides the addition in \( \mathbb{F}_q^n \).

**Theorem 2.1.** Let \( \phi \) be the linear map in (1). Then a nonempty subset \( C \) of \( \mathbb{F}_q^n \) is a cyclic code if and only if \( \phi(C) \) is an ideal of \( \mathbb{F}_q[x]/(x^n - 1) \).

**Proof.** Suppose that \( \phi(C) \) is an ideal of \( \mathbb{F}_q[x]/(x^n - 1) \). Then, for any \( \alpha, \beta \in \mathbb{F}_q \subset \mathbb{F}_q[x]/(x^n - 1) \) and \( a, b \in C \), we have \( \alpha \phi(a), \beta \phi(b) \in \phi(C) \) by definition of ideal. Thus by definition of ideal, \( \alpha \phi(a) + \beta \phi(b) \) is an element of \( \phi(C) \); i.e., \( \phi(aa + bb) \in \phi(C) \), hence \( aa + bb \) is a codeword of \( C \). This shows that \( C \) is a linear code.

Now let \( c = (c_0, c_1, \ldots, c_{n-1}) \) be a codeword of \( C \). The polynomial

\[
\phi(c) = c_0 + c_1x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}
\]

is an element of \( \phi(C) \). Since \( \phi(C) \) is an ideal, the element

\[
x\phi(c) = c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}x^n
\]

\[
= c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}
\]

is in \( \phi(C) \); i.e., \( (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \) is a codeword of \( C \). This means that \( C \) is cyclic.
Conversely, suppose that $C$ is a cyclic code. Then it is clear that definition of ideal is satisfied for $\phi(C)$. For any polynomial $f(x) = f_0 + f_1x + \cdots + f_{n-2}x^{n-2} + f_{n-1}x^{n-1} = \phi(f_0, f_1, \ldots, f_{n-1})$ of $\phi(C)$ with $(f_0, f_1, \ldots, f_{n-1}) \in C$, the polynomial $xf(x) = f_{n-1} + f_0x + f_1x^2 + \cdots + f_{n-2}x^{n-1}$ is also an element of $\phi(C)$ since $C$ is cyclic. Thus, $x^2f(x) = x(xf(x))$ is an element of $\phi(C)$. By induction, we know that $x^if(x)$ belongs to $\phi(C)$ for all $i \geq 0$. Since $C$ is a linear code and $\phi$ is a linear transformation, $\phi(C)$ is a linear space over $\mathbb{F}_q$. Hence, for any $g(x) = g_0 + g_1x + \cdots + g_{n-1}x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1)$, the polynomial
\[
g(x)f(x) = \sum_{i=0}^{n-1} g_i(x^i f(x))
\]
is an element of $\phi(C)$. Therefore, $\phi(C)$ is an ideal of $\mathbb{F}_q[x]/(x^n - 1)$ since definition of ideal is also satisfied.

**Example 2.2.**

1. The trivial cyclic code $\{0\}$ corresponds to the ideal $\{0\}$ and $\mathbb{F}_q^n$ corresponds to $\mathbb{F}_q[x]/(x^n - 1)$.
2. The code $C = \{(0, 0, 0, 0), (2, 1, 2, 1), (1, 2, 1, 2)\}$ is a ternary cyclic code. The corresponding ideal in $\mathbb{F}_3[x]/(x^4 - 1)$ is $\phi(C) = \{0, 2 + x + 2x^2 + x^3, 1 + 2x + x^2 + 2x^3\}$.
3. The ideal $\{0, 1 + x + x^2, 2 + 2x + 2x^2\}$ in $\mathbb{F}_3[x]/(x^3 - 1)$.

**Proposition 2.2.** $\mathbb{F}_q[x]/(x^n - 1)$ is a principal ideal ring.

**Proof.** The zero ideal is obviously principal. We choose a nonzero polynomial $g(x)$ of a nonzero ideal $I$ with the lowest degree. For any polynomial $f(x)$ in $I$, we have
\[
f(x) = s(x)g(x) + r(x)
\]
for some polynomials $s(x), r(x) \in \mathbb{F}_q[x]$ with $\deg r(x) < \deg g(x)$. This forces $r(x) = 0$, since $r(x) = f(x) - s(x)g(x) \in I$ and $g(x)$ has the lowest degree among the nonzero polynomials of $I$. Hence, $I = \langle g(x) \rangle$, so $\mathbb{F}_q[x]/(x^n - 1)$ is a principal ideal ring.

**Proposition 2.3.** Let $C$ be a a cyclic code of length $n$, so there is a corresponding nonzero ideal $\phi(C)$ in the ring $R = \mathbb{F}_q[x]/(x^n - 1)$.

(a) There is a unique monic polynomial $g(x)$ of minimal degree in $\phi(C)$.
(b) $\phi(C) = \langle g(x) \rangle$, i.e., $g(x)$ is a generator polynomial of $\phi(C)$.
(c) $g(x)$ is a factor of $x^n - 1$.
(d) Any $c(x) \in \phi(C)$ can be written uniquely as $c(x) = f(x)g(x)$ in $\mathbb{F}_q[x]$, where $f(x) \in \mathbb{F}_q[x]$ has less than $n - r$, where $r = \deg g(x)$. The dimension of $C$ is $n - r$. 

□
(e) If \( g(x) = g_0 + g_1 x + \cdots + g_r x^r \), then \( C \) is generated by the rows of the generator matrix

\[
G = \begin{bmatrix}
g_0 & g_1 & g_2 & \cdots & g_r & 0 \\
g_0 & g_1 & \cdots & g_r - 1 & g_r \\
0 & g_0 & \cdots & \cdots & g_r
\end{bmatrix}
\]

Proof.

(a) Suppose \( f(x), g(x) \in \phi(C) \) both are monic with the minimal degree \( r \). Then \( f(x) - g(x) \in \phi(C) \) has lower degree, which is a contradiction unless \( f(x) = g(x) \).

(b) Suppose \( c(x) \in \phi(C) \). Write \( c(x) = q(x)g(x) + r(x) \) in \( R \), where \( \deg r(x) < r \). But \( r(x) = c(x) - q(x)g(x) \in \phi(C) \) since the code is linear, so \( r(x) = 0 \). Therefore, \( c(x) \in g(x) \).

(c) Write \( x^n - 1 = h(x)g(x) + r(x) \) in \( F[x] \), where \( \deg r(x) < r \). In \( R \), this says \( r(x) = h(x)g(x) \in \phi(C) \), a contradiction unless \( r(x) = 0 \).

(d) (e) From (b), any \( c(x) \in \phi(C) \), \( \deg c(x) < n \), is equal to \( q(x)g(x) \) in \( R \). Thus

\[
c(x) = q(x)g(x) + e(x)(x^n - 1) \text{ in } F[x]
\]

where \( \deg f(x) \leq n - r - 1 \). Thus the code consists of multiples of \( g(x) \) by polynomials of degree \( \leq n - r - 1 \), evaluated in \( F[x] \). There are \( n - r \) linearly independent multiples of \( g(x) \), namely, \( g(x), xg(x), \ldots, x^{n-r-1}g(x) \). The corresponding vectors are the rows of \( G \). Thus the code has dimension \( n - r \).

Let \( C \) be a cyclic code with generator polynomial \( g(x) \). By Proposition 2.3, \( g(x) \) divides \( x^n - 1 \). Then \( h(x) := (x^n - 1)/g(x) \) is called the check polynomial of \( C \), and

\[
H = \begin{bmatrix}
0 & h_{n-r} & \cdots & h_1 & h_0 \\
h_{n-r} & h_{n-r-1} & \cdots & h_1 & h_0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
h_{n-r} & h_{n-r-1} & \cdots & h_0 & 0
\end{bmatrix}
\]

is a parity-check matrix of \( C \).

If \( G \) is a generator matrix for a cyclic code \( C \), and \( H \) is a parity check matrix for \( C \), then \( HG^T = 0 \) or \( GH^T = 0 \).

**Example 2.3.** Consider the \( x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1) \) over \( F_2 \). The polynomial \( g(x) = (x - 1)(x^3 + x + 1) = x^4 + x^3 + x + 1 \) generates a cyclic (7,4) code. The elements

\[
x^2g(x) = (1110100), \ xg(x) = (0111010), \ g(x) = (0011101),
\]
can be taken as basis vectors, and therefore $G$ can be taken as the generator matrix. This code is the dual space of the ideal generated by $h(x) = (x^7 - 1)/g(x) = x^3 + x^2 + 1$.

\[x^3h(x) = (1101000), \quad x^2h(x) = (0110100), \quad xh(x) = (0011010, \quad h(x) = (0001101)\]

\[H = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}\]

Definition 2. Let $n$ be co-prime to $q$. The cyclotomic coset of $q$ modulo $n$ containing $i$ is defined by

\[C_i = \{(i \cdot q^j \mod n) : j = 0, 1, \ldots \}.\]

A subset $\{i_1, \ldots, i_{\ell}\}$ of $\mathbb{Z}_n$ is called a complete set of representatives of cyclotomic cosets of $q$ modulo $n$ if $C_{i_1}, \ldots, C_{i_{\ell}}$ are distinct and $\bigcup_{j=1}^{\ell} C_{i_j} = \mathbb{Z}_n$.

Example 2.4. Consider the cyclotomic cosets of 5 modulo 24:

- $C_0 = \{0\}$
- $C_1 = \{1, 5\}$
- $C_2 = \{2, 10\}$
- $C_3 = \{3, 15\}$
- $C_4 = \{4, 20\}$
- $C_6 = \{6\}$
- $C_7 = \{7, 11\}$
- $C_8 = \{8, 16\}$
- $C_9 = \{9, 21\}$
- $C_{12} = \{12\}$
- $C_{13} = \{13, 17\}$
- $C_{14} = \{14, 22\}$
- $C_{18} = \{18\}$
- $C_{19} = \{19, 23\}$

The set $\{0, 1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14, 18, 19\}$ is a complete set of representatives of cyclotomic cosets of 5 modulo 24.

Theorem 2.4. Let $\alpha$ be a primitive element of $\mathbb{F}_{q^m}$. Then the minimal polynomial of $\alpha^i$ with respect to $\mathbb{F}_q$ is

\[M^{(i)}(x) := \prod_{j \in C_i} (x - \alpha^j),\]

where $C_i$ is the unique cyclotomic coset of $q$ modulo $q^m - 1$ containing $i$.

Proof. Step 1: It is clear that $\alpha^i$ is a root of $M^{(i)}(x)$ as $i \in C_i$.

Step 2: Let $M^{(i)}(x) = a_0 + a_1x + \cdots + a_rx^r$, where $a_k \in \mathbb{F}_{q^m}$ and $r = |C_i|$. Raising each coefficient to its $q$th power, we obtain

\[a_0^q + a_1^q x + \cdots + a_r^q x^r = \prod_{j \in C_i} (x - \alpha^{qj}) = \prod_{j \in C_i} (x - \alpha^j) = \prod_{j \in C_i} (x - \alpha^j) = M^{(i)}(x).\]
In order to determine the factorization of the definition of the minimal polynomial, the polynomials and hence all the roots of $x$ for some $q$. Let $F$ cyclotomic cosets of $q$ modulo $q$ for all $0 < q < n$. This implies that all the roots of $x$ are elements of $F$. Hence, $M(i)(x)$ has no multiple roots. Now let $f(x) = F(q)$ and $f(a^i) = 0$. Put $f(x) = f_0 + f_1x + \cdots + f_nx^n$ for some $f_k \in F$. Then, for any $j \in C_i$, there exists an integer $l$ such that $j \equiv iq^l \pmod{q^m - 1}$. Hence,

$$f(a^j) = f(a^{iq^l}) = f_0 + f_1a^{iq^l} + \cdots + f_na^{nq^l} = f_0^{q^l} + f_1^{q^l}a^{iq^l} + \cdots + f_n^{q^l}a^{nq^l}
= (f_0 + f_1a^i + \cdots + f_na^{ni})q^l = f(a^i)^{q^l} = 0$$

This implies that $M(i)(x)$ is a divisor of $f(x)$. The above three steps show that $M(i)(x)$ is the minimal polynomial of $a^i$.

**Theorem 2.5.** Let $n$ be a positive integer with $\gcd(q, n) = 1$. Suppose that $m$ is a positive integer satisfying $n \mid (q^m - 1)$. Let $\alpha$ be a primitive element of $F_q$ and let $M(i)(x)$ be the minimal polynomial of $\alpha^i$ with respect to $F_q$. Let $\{s_1, \ldots, s_l\}$ be a complete set of representatives of cyclotomic cosets of $q$ modulo $n$. Then the polynomial $x^n - 1$ has the factorization into monic irreducible polynomial over $F_q$:

$$x^n - 1 = \prod_{i=1}^l M((q^m - 1)s_i/n)(x).$$

**Proof.** Put $r = (q^m - 1)/n$. Then $\alpha^r$ is a primitive $n$th root of unity, and hence all the roots of $x^n - 1$ are $1, \alpha^r, \alpha^{2r}, \ldots, \alpha^{(n-1)r}$. Thus, by the definition of the minimal polynomial, the polynomials $M((i)r)(x)$ are divisors of $x^n - 1$, for all $0 \leq i \leq n - 1$. It is clear that we have

$$x^n - 1 = \text{lcm}(M(0)(x), M(r)(x), M(2r)(x), \ldots, M((n-1)r)(x)).$$

In order to determine the factorization of $x^n - 1$, it suffices to determine all the distinct polynomials among $M(0)(x)$, $M(r)(x)$, $M(2r)(x)$, $\ldots$, $M((n-1)r)(x)$. We know that $M((i)r)(x) = M((j)r)(x)$ if and only if $i$ and $j$ are in the same cyclotomic coset of $q$ modulo $n$, i.e., $i$ and $j$ are in the same cyclotomic coset of $q$ modulo $n$. This implies that all the distinct polynomials among $M(0)(x)$, $M(r)(x)$, $M(2r)(x)$, $\ldots$, $M((n-1)r)(x)$ are $M(s_1r)(x)$, $M(s_2r)(x)$, $\ldots$, $M(s_lr)(x)$. The proof is completed.

**Example 2.5.** For $n = 9, q = 2$

$$C_0 = \{0\}, C_1 = \{1, 2, 4, 5, 7, 8\}, C_2 = \{3, 6\}.$$
Thus \( m = 6 \), and \( x^9 - 1 \) splits into linear factors over \( \mathbb{F}_{2^6} \). Then
\[
x^9 + 1 = M^{(0)}(x)M^{(1)}(x)M^{(3)}(x)
\]
where \( M^{(0)}(x) = x + 1, M^{(1)}(x) = x^6 + x^3 + 1, M^{(3)}(x) = x^2 + x + 1 \).

3. On bounds of minimum distance of cyclic codes

In the 1960s, the well-known bound was first established by Bose, Ray-Chaudhuri and Hocquenghem (BCH). It was further generalized to HT bound by Hartmann and Tzeng (HT) \[4\]. Then, Roos \[5\], van Lint and Wilson \[2\] later extended it by using A, B sets construction and shifting method.

**Definition 3.** Let \( A = \{\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_m}\} \) be a set of \( n \)th roots of unity in \( \mathbb{F}_{q^m} \),
\[
H_A := \begin{bmatrix}
1 & \alpha^{i_1} & \alpha^{2i_1} & \ldots & \alpha^{(n-1)i_1} \\
1 & \alpha^{i_2} & \alpha^{2i_2} & \ldots & \alpha^{(n-1)i_2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{i_m} & \alpha^{2i_m} & \ldots & \alpha^{(n-1)i_m}
\end{bmatrix}
\]
Then \( H_A \) is a parity check matrix for the cyclic code \( C_A \) over \( \mathbb{F}_q \) having \( A \) as a defining set. Let \( d_A \) be the minimum distance of \( C_A \). Let \( C_A^* \) be the cyclic code over \( \mathbb{F}_{q^m} \) with \( H_A \) as parity check matrix and denote its minimum distance by \( d_A^* \). Then \( C_A^* \) contains \( C_A \) as a subcode and hence \( d_A \geq d_A^* \).

Let \( g(x) \) be a generator polynomial of \( C_A \). If \( A = \{\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{n-k}} \mid g(\alpha^{i_j}) = 0, j = 1, 2, \ldots, n - k\} \),
where \( \alpha \) is a primitive \( n \)th roots of unity, then we shall say that \( A \) is a *defining set* for \( C_A \).

A set \( A = \{\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_l}\} \) will be called a *consecutive set* of length \( l \) if a primitive \( n \)th root of unity \( \beta \) and an exponent \( i \) exist such that \( A = \{\beta^i, \beta^{i+1}, \ldots, \beta^{i+l-1}\} \).

**Theorem 3.1.** Let \( C \) be a linear code and \( H \) be a parity check matrix for \( C \). Then
(1) \( C \) has distance \( \geq d \) if and only if any \( d - 1 \) columns of \( H \) are linearly independent.
(2) \( C \) has distance \( \leq d \) if and only if \( H \) has \( d \) columns that are linearly dependent.

**Proof.** See \[1\], Theorem 4.5.6.

**Corollary 3.2.** Let \( C \) be a linear code and let \( H \) be a parity check matrix for \( C \). Then the following statements are equivalent:
(1) \( C \) has distance \( d \);
(2) any \( d - 1 \) columns of \( H \) are linearly independent and \( H \) has \( d \) columns that are linearly dependent.
Theorem 3.3. (BCH bound)

If $A$ is a defining set for a cyclic code and contains a consecutive set of length $\delta - 1$, then $d_A \geq \delta$.

Proof. We form the $m$ by $n$ matrix $H_A$:

$$H_A := \begin{bmatrix}
1 & \alpha^{i_1} & \alpha^{2i_1} & \cdots & \alpha^{(n-1)i_1} \\
1 & \alpha^{i_2} & \alpha^{2i_2} & \cdots & \alpha^{(n-1)i_2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{i_m} & \alpha^{2i_m} & \cdots & \alpha^{(n-1)i_m}
\end{bmatrix}$$

A word $c$ in $C_A$ iff $cH_A^T = 0$. The $m$ rows of $H_A$ are not necessarily independent. Consider any $\delta - 1$ columns of $H_A$ and let $\alpha^{i_1}, \ldots, \alpha^{i_m}$ be the top elements in these columns. The determinant of the submatrix of $H_A$ is a Vandermonde determinant with value $\alpha^{i_1 + \cdots + i_m} \prod_{j>k}(\alpha^{i_j} - \alpha^{i_k}) \neq 0$, since $\alpha$ is a primitive $n$th root of unity. Therefore, by Theorem 3.1, any $\delta - 1$ columns of $H_A$ are linearly independent and hence a codeword $c \neq 0$ has weight $\geq \delta$. \hfill \Box

If $M$ is a matrix with $n$ columns and $J \subseteq \{1, 2, \ldots, n\}$, then $M_J$ is the submatrix of $M$ consisting of the columns indexed by elements of $J$. Often $J$ will be the support of a codeword $c$, that is, $J = \{j \mid c_j \neq 0, 1 \leq j \leq n\}$.

Lemma 3.4. If $\beta$ is a primitive $n$th root of unity and $|J| = \delta - 1$, then $M(\beta^1, \beta^{i+1}, \ldots, \beta^{i+\delta-2})_J$ has rank $\delta - 1$.

Proof. See [3]. \hfill \Box

Example 3.1. Take $n = 26, g = 3$ and let $C$ be the cyclic code with generator polynomial $g(x) = m_1(x)m_2(x)m_4(x)m_5(x)m_7(x)$. The zeros of $g(x)$ are $\alpha^i$, with $i \in C_1 \cup C_2 \cup C_4 \cup C_5 \cup C_7$, where $C_1 = \{1, 3, 9\}, C_2 = \{2, 6, 18\}, C_4 = \{4, 10, 12\}, C_5 = \{5, 15, 19\}, C_7 = \{7, 11, 21\}$. Clearly $\{1, 2, 3, 4, 5, 6, 7\} \subset C_1 \cup C_2 \cup C_4 \cup C_5 \cup C_7$. Hence the BCH bound is $d \geq 8$.

To prove HT bound, we start with a lemma.

Lemma 3.5. Let $M = [m_1, m_2, \ldots, m_n]$ be a matrix over a field $K$ such that no $k-1$ columns of $M$ are linearly dependent, and let $x_1, x_2, \ldots, x_n$ be a sequence of elements of $K$ in which no element of $K$ occurs more than $k-1$ times. Then in the matrix

$$M' := \begin{bmatrix}
m_1 & m_2 & \cdots & m_n \\
x_1m_1 & x_2m_2 & \cdots & x_nm_n
\end{bmatrix}$$

any $k$ columns are linearly independent.

Proof. Suppose $M'$ contains $k$ columns which are linearly dependent. Without loss of generality, we may assume that these are the first $k$
columns. Then there exist elements \( \lambda_1, \lambda_2, \ldots, \lambda_n \in K \) (not all zero) such that
\[
\sum_{i=1}^{k} \lambda_i m_i = \sum_{i=1}^{k} \lambda_i x_i m_i = 0.
\]
Hence,
\[
\sum_{i=1}^{k-1} \lambda_i (x_i - x_k) m_i = 0.
\]
Since any \( k - 1 \) columns of \( M \) are linearly independent this implies that \( \lambda_i(x_i - x_k) \neq 0 \) for \( 1 \leq i \leq k - 1 \). However, \( \lambda_i \neq 0 \) for \( 1 \leq i \leq k \); this also follows from the fact that no \( k - 1 \) columns of \( M \) are linearly dependent. Hence we obtain \( x_1 = x_2 = \cdots = x_k \), which contradicts our hypothesis. \( \square \)

For each divisor \( i \) of \( n \) we define the cyclic code \( C_{N^i} \) as follow: Put \( N^i := \{ \alpha^i | \alpha \in N \} \) and \( n = in' \). Then, if \( i > 1 \), it is clear that the cyclic code \( C_{N^i} \) is degenerate, because its check polynomial divides \( x^{n'} - 1 \); it consists of the \( i \)-fold repetition of the words in the cyclic code of length \( n' \) having \( N^i \) as defining set of zeros. The latter code will be denoted as \( C_{N^i} \), and the corresponding code over \( \mathbb{F}_{q^m} \) as \( C_{N^i}^{*} \).

**Theorem 3.6.** Let \( N \) be a nonempty subset of \( n \)th roots of unity in \( \mathbb{F}_{q^m} \) such that \( d_N^* < n \), and let \( \beta \) be a \( n \)th root of unity of order \( i \). Then \( d_{N \cup \beta N}^* \geq d_N^* \), and equality will occur if and only if \( C_{N^i}^{*} \) has minimum distance \( d_N^* \).

**Proof.** The inequality \( d_{N \cup \beta N}^* \geq d_N^* \) is a obvious consequence of the inclusion \( N \subset N \cup \beta N \). Equality occurs if and only if the code \( C_{N \cup \beta N}^* \) contains a word of weight \( d_N^* \), i.e., if and only if the matrix \( H_{N \cup \beta N} \) contains \( d_N^* \) columns which are linearly dependent over the field \( \mathbb{F}_{q^m} \).

Therefore, let us assume that \( C_{N \cup \beta N}^* \) contains a word \( c = (c_1, c_2, \ldots, c_n) \) of weight \( d_N^* \). Without loss of generality we may assume that \( c_n \neq 0 \). Now Lemma 1 implies that \( c_k \) can be nonzero only if \( \beta^k = \beta^n = 1 \). Hence, \( c_k \neq 0 \) implies that \( i \) divides \( k \). So \( C_{N^i}^{*} \) has minimum distance \( d_N^* \) in this case.

Conversely, if \( C_{N^i}^{*} \) has minimum distance \( d_N^* \), then there exists a word \( c = (c_1, c_2, \ldots, c_n) \in C_{N^i}^{*} \) such that \( c_k \neq 0 \) holds only if \( i \mid k \). Hence \( \beta^k = 1 \) if \( c_k \neq 0 \), and consequently, one also has \( c \in C_{N \cup \beta N}^* \).

Hence \( d_{N \cup \beta N}^* = d_N^* \). \( \square \)

**Example 3.2.** Take \( n = 21, q = 2 \) and \( N = \{ \alpha, \alpha^2 \} \), where \( \alpha \) is a primitive element in \( \mathbb{F}_{64} \). The decomposition of \( x^{21} - 1 \) in irreducible factors is as follow:
\[
x^{21} - 1 = (x + 1)(x^2 + x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)
\begin{align*}
&= (x^6 + x^4 + x^2 + 1)(x^6 + x^5 + x^4 + x^2 + 1)
\end{align*}
\]
Suppose that $\alpha^6 + \alpha^4 + \alpha^2 + \alpha + 1 = 0$, $\beta = \alpha^3$, for some $j$, $o(\beta) = i$ and $N' = N \cup \beta N$. If $o(\beta) = 21$, then $N'^i = \{1\}$, hence $C_{N'}^\perp$ is the zero code, whence $d^*_{N'} \geq d^*_N = 2$. If $o(\beta) = 7$, then $N'^i = \{\alpha^7, \alpha^{14}\}$. The minimal polynomial of $\alpha^7$ is $m_7(x) = x^2 + x + 1$. This is the generator polynomial of $C_{N'}^\perp$, which has length 3. Hence $C_{N'}^\perp$ has minimum distance. So then yields that $d^*_{N'} = d^*_N$ is the case. If $o(\beta) = 3$, then $N'^i = \{\alpha^3, \alpha^6\}$. The minimal polynomial of $\alpha^3$ is $m_3(x) = x^3 + x^2 + 1$. It is also the generator polynomial of $C_{N'}^\perp$, which has length 7. So is $d^*_{N'} = d^*_N$.

**Corollary 3.7.** If $o(\beta) > n/d^*_N$, then $d^*_{N \cup \beta N} > d^*_N$.

**Proof.** Let $o(\beta) = i$ and $n = in'$. Then $n' < d^*_N$. Since the code $C_{N'}$ has length $n'$ its minimum distance cannot be $d^*_N$. Hence above Theorem implies the result.

**Theorem 3.8.** (HT bound) Let $b, i_1, i_2, c_1, c_2 \in \mathbb{Z}$ and $N$ be a subset of $n$th roots of unity in $\mathbb{F}_{q^n}$. If $N = \{\alpha^{b+i_1c_1+i_2c_2} | 0 \leq i_1 \leq \delta - 2, 0 \leq i_2 \leq s\}$, where $\delta \geq 2$, $(n, c_1) = 1$ and $(n, c_2) < \delta$. Then $d^*_N \geq \delta + s$.

**Proof.** Use induction on $s$. Let us assume that $s \geq 0$ and that $d^*_N \geq \delta + s$ for the set $N$ described in the theorem. Note that $\beta = \alpha^{c_2}$ has order $n/(n, c_2)$, which exceeds $n/(\delta + s)$ since $(n, c_2) < \delta$. Hence Corollary 3.7 can be applied to yield $d^*_{N \cup \alpha^{c_2} N} \geq \delta + s + 1$. Since $N \cup \alpha^{c_2} N = \{\alpha^{b+i_1c_1+i_2c_2} | 0 \leq i_1 \leq \delta - 2, 0 \leq i_2 \leq s + 1\}$, this proves the theorem.

To prove Roos bound, we start with a Theorem.

**Theorem 3.9.** Let

$$H_A := \begin{bmatrix} \alpha_1^1 & \alpha_1^2 & \cdots & \alpha_1^n \\ \alpha_2^1 & \alpha_2^2 & \cdots & \alpha_2^n \\ \vdots & \cdots & \cdots & \cdots \\ \alpha_m^1 & \alpha_m^2 & \cdots & \alpha_m^n \end{bmatrix}$$

be the parity check matrix for a cyclic code $C$ with minimum distance $d_A$ and $\alpha$ is a primitive $n$th root of unity in $\mathbb{F}_{q^n}$. The $m \times n$ matrix $H_B$, and it’s columns $\beta_i = (\beta_{i1}, \beta_{i2}, \ldots, \beta_{in})$ from the set $B$, for all $i$, $1 \leq i \leq n$.

We define

$$AB := \begin{bmatrix} \beta_{11}\alpha_1^1 & \beta_{12}\alpha_1^2 & \cdots & \beta_{1n}\alpha_1^n \\ \beta_{21}\alpha_2^1 & \beta_{22}\alpha_2^2 & \cdots & \beta_{2n}\alpha_2^n \\ \vdots & \cdots & \cdots & \cdots \\ \beta_{m1}\alpha_m^1 & \beta_{m2}\alpha_m^2 & \cdots & \beta_{mn}\alpha_m^n \end{bmatrix}$$

If $d_A \geq 2$ and every $m \times (m + d_A - 2)$ submatrix of $H_B$ has full rank, then $d_{AB} \geq d_A + m - 1$. 

Proof. Assume that $d_{AB} < d_A + m - 1$. Then there exist $d_A + m - 2$ columns of the matrix $AB$ which are linearly dependent over the field $\mathbb{F}_{q^m}$. Then denote the $i$th column of $AB$ as $a'_i$ and let $\{a'_i \mid i \in I\}$ be such a set of $d_A + m - 2$ columns. Then there exist elements $\lambda_i$ (not all zero) in $\mathbb{F}_{q^m}$ such that $\sum_{i \in I} \lambda_i a'_i = 0$.

This implies
\[
\sum_{i \in I} \lambda_i \beta_i a'_i = 0, \quad 1 \geq r \geq m.
\]

Consider the submatrix of $B$ consisting of the columns $\beta_i, i \in I$. This submatrix has size $m \times (d_A + m - 2)$, and by the hypothesis, it will contain a $m \times m$ submatrix which has full rank. Let $J$ be an $m$-subset of $I$ such that the columns $\beta_j, j \in J$, form such a nonsingular square submatrix of $B$, and let $\Delta(J)$ denote the determinant of this matrix. For $j \in J$ and $i \in I$, let $\Delta_{ij}(J)$ denote the determinant by replacing column $\beta_j$ in $\Delta(J)$ by $\beta_i$.

Multiplication of both members of (2) by the cofactor of the element $x_{rj}$ in the determinant $\Delta(J)$, and then taking the sum over $r$ yields the following identity:
\[
\sum_{i \in I} \lambda_i \Delta_{ij}(J) a_i = 0, \quad j \in J.
\]

It is clear that $\Delta_{ij}(J)$ vanishes if $i \in J \setminus j$. Hence the sum in (3) contains at most $(d_A + m - 2) - (m_1) = d_A - 1$ nonzero terms. However, since any $d_A - 1$ columns in the matrix $A$ are linearly independent, it follows that every term in this sum must vanish. So we have
\[
\lambda_i \Delta_{ij}(J) = 0, \quad i \in I, \quad j \in J.
\]

Now take $i = j \in J$ in (4). This gives $\lambda_j = 0$ for each $j \in J$. Therefore, at most $d_A - 2$ of the elements $\lambda_i$ are nonzero. Using again that any $d_A - 2$ columns in the matrix $A$ are linearly independent we deduce from (2) that
\[
\lambda_i \beta_i = 0, \quad i \in I, \quad r = 1, 2, \ldots, m.
\]

We assumed that some $\lambda_i$ is nonzero. From (5) it follows that the corresponding column $\beta_i$ in $B$ must vanish elementwise. This is a contradiction. Thus we have shown that $d_{AB} \geq d_A + m - 1$. \hfill \Box

Theorem 3.10. (Roos bound) Let $A$ be a subset of $n$th roots of unity in $\mathbb{F}_{q^m}$ then the $m \times n$ matrix over $\mathbb{F}_{q^m}$ whose $i$th row equals $(\alpha_{1i}^1, \alpha_{2i}^2, \ldots, \alpha_{ni}^n)$ will be denoted as $H_A$. Then $H_A$ is a parity check matrix for the cyclic code $C_A$ over $\mathbb{F}_q$ and $d_A$ be the minimum distance of $C_A$. Let $B$ be any subset of $n$th roots of unity in the field $\mathbb{F}_{q^m}$. If there exists a consecutive set $\overline{B}$ containing $B$ such that $|\overline{B}| \leq |B| + d_A - 2$, then the code with defining set $AB$ has minimum distance $d_{AB} \geq |B| + d_A - 1$.  


Proof. Since $A$ is nonempty, $d_A \geq 2$. If every $|B| \times (|B| + d_A - 2)$ submatrix in the matrix $H_B$ has full rank. It’s obvious to know $H_B$ is a submatrix of $H_{\overline{B}}$, and that in the matrix $H_{\overline{B}}$ every $|\overline{B}| \times |\overline{B}|$ submatrix is nonsingular (the determinant of this submatrix is of Vandermonde type). So every $|B| \times |\overline{B}|$ submatrix of $H_B$ has full rank. Since $|\overline{B}| \leq |B| + d_A - 2$ this implies that also every $|B| \times |B| + d_A - 2$ submatrix of $H_B$ has full rank. Then the proof is complete. □

If $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$ are vectors, then we define the product $a \ast b = (a_1b_1, a_2b_2, \ldots, a_nb_n)$. For an $m \times m$ matrix $A$ with entries $a_{ij}$ ($1 \leq i \leq m, 1 \leq j \leq n$) and a matrix $B$ with columns $b_1, b_2, \ldots, b_n$, we define

$$A \ast B := \begin{bmatrix} a_{11}b_1 & a_{12}b_2 & \cdots & a_{1n}b_n \\ a_{21}b_1 & a_{22}b_2 & \cdots & a_{2n}b_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}b_1 & a_{m2}b_2 & \cdots & a_{mn}b_n \end{bmatrix}$$

that is, $A \ast B$ is a matrix that has as rows all the products $a \ast b$, where $s$ is a row of $A$ and $b$ is a row of $B$.

Next theorem is useful to find minimum distance.

**Theorem 3.11.** If a linear combination, with nonzero coefficients, of columns of $A \ast B$ is 0, then

$$\text{rank}(A) + \text{rank}(B) \leq n.$$

**Proof.** See [2], Theorem 4. □

**Corollary 3.12.** Let $A$ and $B$ be matrices with entries from a field $\mathbb{F}$, and let $A \ast B$ be a parity check matrix for the code $C$ over $\mathbb{F}$. If $I$ is the support of a codeword in $C$, then

$$\text{rank}(A_I) + \text{rank}(B_I) \leq |I|.$$

In particular, $C$ has minimum distance $\geq \delta$ if $\text{rank}(A_I)+\text{rank}(B_I) > |I|$ for every subset $I$ of $\{1, 2, \ldots, n\}$ for which $|I| < \delta$.

This theorem also provides another proof for Roos bound. Let $A$ and $B$ be the sets mentioned in the theorem. Then we have

$$\text{rank}(M(A)_I) = \begin{cases} |I|, & \text{if } |I| < d_A \\ \geq d_A - 1, & \text{if } |I| \geq d_A. \end{cases}$$

From Corollary 3.4 and the condition on $B$ and $\overline{B}$, we find

$$\text{rank}(M(B)_I) = \begin{cases} 1, & \text{for } |I| < d_A \\ |I| - d_A + 2, & \text{for } d_A \leq |I| \leq |B| + d_A - 2. \end{cases}$$

Therefore,

$$\text{rank}(M(A)_I) + \text{rank}(M(B)_I) \geq |I|, \text{ for } |I| \leq |B| + d_A - 2.$$
4. Some examples

**Example 4.1.** Let $n = 14, q = 3$, $g(x) = m_2(x)m_7(x)$. Here $R = \{\alpha^i \mid 2, 4, 6, 7, 8, 10, 12\}$. Then by Theorem 3.3., we have $d \geq 4$. In fact, the minimum distance is 4.

**Example 4.2.** Let $n = 16, q = 3$, $g(x) = m_1(x)m_5(x)m_8(x)$. Here $R = \{\alpha^i \mid 1, 3, 5, 7, 8, 9, 11, 13, 15\}$. Then by Theorem 3.3., we have $d \geq 4$. Actually the minimum distance is 5.

**Example 4.3.** Let $n = 25, q = 3$, $g(x) = m_1(x)$. Here $R = \{\alpha^i \mid 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$. Then by Theorem 3.3., we have $d \geq 5$. The minimum distance is equal 5.

**Example 4.4.** Let $n = 22, q = 7$, $g(x) = m_2(x)m_{11}(x)$. Here $R = \{\alpha^i \mid 2, 4, 6, 8, 10, 11, 12, 14, 16, 18, 20\}$. Then by Theorem 3.3., we have $d \geq 4$. The minimum distance is equal 5.

**Example 4.5.** Take $n = 35, q = 3$, and let $C$ be the cyclic code with generator polynomial $g(x) = m_1(x)m_2(x)$. The zeros of $g(x)$ are $\alpha^i$, with $i \in C_1 \cup C_2$, where $C_1 = \{1, 3, 4, 9, 12, 13, 16, 17, 27, 29, 33, 46\}$, $C_2 = \{2, 6, 8, 18, 19, 22, 23, 24, 26, 31, 32, 34\}$. Clearly $\{12, 13, 17, 18, 22, 23\} \subset C_1 \cup C_2$. Hence, by Theorem 3.8., with $b = 12, c_1 = 1, c_2 = 5, \delta = 3, s = 2$ yields that $d \geq 5$.

**Example 4.6.** Let $n = 40, q = 3$, $g(x) = m_1(x)m_2(x)m_3(x)m_5(x)m_7(x)m_{11}(x)m_{13}(x)m_{20}(x)m_{22}(x)$. The zeros of $g(x)$ are $\alpha^i$, with $i \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_7 \cup C_{11} \cup C_{13} \cup C_{20} \cup C_{22}$, where $C_1 = \{1, 3, 9, 27\}$, $C_2 = \{2, 6, 14, 18\}$, $C_3 = \{4, 12, 28, 36\}$, $C_4 = \{5, 15\}$, $C_7 = \{7, 21, 23, 29\}$, $C_{11} = \{11, 17, 19, 33\}$, $C_{13} = \{13, 31, 37, 39\}$, $C_{20} = \{20\}$, $C_{22} = \{22, 26, 34, 38\}$. Clearly $\{5, 6, 7, 12, 13, 14, 19, 20, 21, 26, 27, 28\} \subset C_1 \cup C_2 \cup C_4 \cup C_5 \cup C_7 \cup C_{11} \cup C_{13} \cup C_{20} \cup C_{22}$. By Theorem 3.8. with $b = 5, c_1 = 1, c_2 = 7, \delta = 4, s = 3$ yields that $d \geq 7$.

**Example 4.7.** Let $n = 39, q = 5$, $g(x) = m_1(x)m_3(x)m_4(x)m_6(x)m_{12}(x)m_{14}(x)m_{23}(x)$. The zeros of $g(x)$ are $\alpha^i$, with $i \in C_1 \cup C_3 \cup C_4 \cup C_6 \cup C_{12} \cup C_{14} \cup C_{23}$, where $C_1 = \{1, 5, 8, 25\}$, $C_3 = \{3, 15, 24, 36\}$, $C_4 = \{4, 20, 22, 32\}$, $C_6 = \{6, 9, 30, 33\}$, $C_{12} = \{12, 18, 21, 27\}$, $C_{14} = \{14, 31, 34, 38\}$, $C_{23} = \{23, 28, 29, 37\}$. Clearly $\{4, 5, 6, 20, 21, 22, 26, 37, 38\} \subset C_1 \cup C_3 \cup C_4 \cup C_6 \cup C_{12} \cup C_{14} \cup C_{23}$. By Theorem 3.8. with $b = 4, c_1 = 1, c_2 = 16, \delta = 4, s = 2$ yields that $d \geq 6$.

**Example 4.8.** Let $n = 45, q = 7$, $g(x) = m_0(x)m_1(x)m_2(x)m_5(x)m_9(x)m_{10}(x)m_{30}(x)$. The zeros of $g(x)$ are $\alpha^i$, with $i \in C_0 \cup C_1 \cup C_2 \cup C_5 \cup C_9 \cup C_{10} \cup C_{30}$, where $C_0 = \{0\}$, $C_1 = \{1, 4, 7, 13, 16, 19, 22, 28, 31, 34, 37, 43\}$, $C_2 = \{2, 8, 11, 14, 17, 23, 26, 29, 32, 38, 41, 44\}$, $C_5 = \{5, 20, 35\}$, $C_9 = \{9, 18, 27, 36\}$, $C_{10} = \{10, 25, 40\}$, $C_{30} = \{30\}$. Clearly $\{7, 8, 9, 18, 19, 20, 29, 30, 31, 40, 41, 42\} \subset C_0 \cup C_1 \cup C_2 \cup C_5 \cup C_9 \cup C_{10} \cup C_{30}$. By Theorem 3.8. with $b = 7, c_1 = 1, c_2 = 11, \delta = 4, s = 3$ yields that $d \geq 7$. 


Example 4.9. Take $n = 32$, $q = 3$, and let $C$ be the cyclic code with generator polynomial $g(x) = m_1(x)m_2(x)m_3(x)m_4(x)m_5(x)m_6(x)$. So the zeros of $g(x)$ are $\alpha^i$ with $i \in C_1 \cup C_2 \cup C_3 \cup C_5 \cup C_{10}$, where

$C_1 = \{1, 3, 9, 11, 17, 19, 25, 27\}$

$C_2 = \{2, 6, 18, 22\}$

$C_3 = \{5, 7, 13, 15, 21, 23, 29, 31\}$

$C_{10} = \{10, 14, 26, 30\}$.

Note that $C$ has the following consecutive sets of zeros:

$\{\alpha^i | i = 1, 2, 3\}, \{\alpha^i | i = 5, 6, 7\}, \{\alpha^i | i = 9, 10, 11\}, \{\alpha^i | i = 13, 14, 15\}, \{\alpha^i | i = 17, 18, 19\}, \{\alpha^i | i = 21, 22, 23\}, \{\alpha^i | i = 25, 26, 27\}, \{\alpha^i | i = 29, 30, 31\}$.

Take $N = \{\alpha^i | i = 2, 3\}$ and $M = \{\beta^j | j = 0, 1\}$ with $\beta = \alpha^7$. Then the elements of $MN$ are zeros of $C$. Since $d_N = 3$ and $2 \leq |M| + d_N - 2$, by Theorem 3.10., we have $d_{MN} \geq 2 + 3 - 1 = 4$. Hence the minimum distance of $C$ is at least 4.

Example 4.10. Take $n = 31$, $q = 5$, and let $C$ be the cyclic code with generator polynomial $g(x) = m_1(x)m_2(x)m_3(x)m_4(x)m_5(x)m_6(x)m_7(x)m_8(x)m_9(x)m_{11}(x)$. So the zeros of $g(x)$ are $\alpha^i$ with $i \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_6 \cup C_8 \cup C_{11}$, where

$C_1 = \{1, 5, 25\}$

$C_2 = \{2, 10, 19\}$

$C_3 = \{3, 13, 15\}$

$C_4 = \{4, 7, 20\}$

$C_6 = \{6, 26, 30\}$

$C_8 = \{8, 9, 14\}$

$C_{11} = \{11, 24, 27\}$

Note that $C$ has the following consecutive sets of zeros:

$\{\alpha^i | i = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}, \{\alpha^i | i = 13, 14, 15\}, \{\alpha^i | i = 19, 20\}$,

$\{\alpha^i | i = 24, 25, 26, 27\}$.

Take $N = \{\alpha^i | i = 2, 3\}$ and $M = \{\beta^j | j = 0, 1, 3\}$ with $\beta = \alpha^8$. Then the elements of $MN$ are zeros of $C$. Since $d_N = 3$ and $4 \leq |M| + d_N - 2$, by Theorem 3.10., we have $d_{MN} \geq 3 + 3 - 1 = 5$. Hence the minimum distance of $C$ is at least 5.

Example 4.11. Take $n = 40$, $q = 7$, and let $C$ be the cyclic code with generator polynomial $g(x) = m_1(x)m_2(x)m_3(x)m_4(x)m_5(x)m_6(x)m_{15}(x)m_{17}(x)$. So the zeros of $g(x)$ are $\alpha^i$ with $\alpha^i$ with $i \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_8 \cup C_{15} \cup C_{17}$, where

$C_1 = \{1, 7, 9, 23\}$

$C_2 = \{2, 6, 14, 18\}$

$C_3 = \{3, 21, 27, 29\}$

$C_4 = \{4, 12, 28, 36\}$

$C_8 = \{8, 16, 24, 32\}$

$C_{15} = \{15, 25\}$

$C_{17} = \{17, 31, 33, 39\}$.

Note that $C$ has the following consecutive sets of zeros:

$\{\alpha^i | i = 1, 2, 3, 4\}, \{\alpha^i | i = 6, 7, 8, 9\}, \{\alpha^i | i = 16, 17, 18\}, \{\alpha^i | i = 23, 24, 25\}$,

$\{\alpha^i | i = 27, 28, 29\}, \{\alpha^i | i = 31, 32, 33\}$.

Take $N = \{\alpha^i | i = 7, 8, 9\}$ and $M = \{\beta^j | j = 0, 1, 2, 3\}$ with $\beta = \alpha^8$. Then the elements of $MN$ are zeros of $C$. Since $d_N = 4$ and $4 \leq |M| + d_N - 2$, by Theorem 3.10., we have $d_{MN} \geq 4 + 4 - 1 = 7$. Hence the minimum distance of $C$ is at least 7.

Example 4.12. Take $n = 37$, $q = 11$, and let $C$ be the cyclic code with generator polynomial $g(x) = m_2(x)m_3(x)m_5(x)m_6(x)$. So the zeros of $g(x)$ are $\alpha^i$ with $i \in C_1 \cup C_2 \cup C_5 \cup C_{10}$, where
\[ C_2 = \{2, 15, 17, 20, 22, 35\}, \quad C_3 = \{3, 4, 7, 30, 33, 34\}, \quad C_5 = \{5, 13, 18, 19, 24, 32\}, \quad C_6 = \{6, 8, 14, 23, 29, 31\}. \]

Note that \( C \) has the following consecutive sets of zeros:
\[ \{\alpha^i | i = 2, 3, 4, 5, 6, 7, 8\}, \{\alpha^i | i = 13, 14, 15\}, \{\alpha^i | i = 17, 18, 19, 20\}, \{\alpha^i | i = 22, 23, 24\}, \{\alpha^i | i = 29, 30\}, \{\alpha^i | i = 31, 32, 33, 34, 35\}. \]

Take \( N = \{\alpha^i | i = 4, 5, 6\} \) and \( M = \{\beta^j | j = 0, 1, 2, 3\} \) with \( \beta = \alpha^9 \).

Then the elements of \( MN \) are zeros of \( C \). Since \( d_N = 4 \) and \( 4 \leq |M| + d_N - 2 \), by Theorem 3.10, we have \( d_{MN} \geq 4 + 4 - 1 = 7 \). Hence the minimum distance of \( C \) is at least 7.

**Example 4.13.** Let \( n = 80, q = 3 \), and \( C \) be the cyclic code with generator polynomial \( g(x) = m_2(x)m_4(x)m_5(x)m_{11}(x)m_{13}(x)m_{14}(x)m_{16}(x)m_{17}(x)m_{22}(x)m_{41}(x)m_{44}(x) \).

So the defining set \( R = \{\alpha^i | i = 2, 4, 5, 6, 11, 12, 13, 14, 15, 16, 17, 18, 19, 22, 25, 28, 31, 32, 33, 34, 35, 36, 37, 38, 39, 41, 42, 43, 44, 45, 46, 48, 49, 51, 52, 54, 55, 57, 58, 59, 64, 65, 66, 67, 68, 73, 75, 76\} \), where \( \alpha \) is a primitive 80th root of unity. Let \( A = \{\alpha^i | 1 \leq i \leq 46\} \cup \{\alpha^i | 48, 49\} \) \( B = \{\beta^j | j = -3, -1, 0\} \), where \( \beta = \alpha^5 \).

Then \( AB \subseteq R \). The set \( A \) contains 6 consecutive powers of \( \alpha \), and furthermore, it is a subset of a set of 9 consecutive powers of \( \alpha \), with the powers \( \alpha^{47} \) missing. So, from Corollary 3.4, we find

\[
\text{rank}(M(A)_I) = \begin{cases} 
|I|, & \text{for } 1 \leq |I| \leq 6 \\
6, & \text{for } 6 \leq |I| \leq 7 \\
|I| - 1, & \text{for } 7 \leq |I| \leq 9 
\end{cases}
\]

\[
\text{rank}(M(B)_I) = \begin{cases} 
|I|, & \text{for } 1 \leq |I| \leq 2 \\
2, & \text{for } 2 \leq |I| \leq 3 \\
3, & \text{for } |I| \geq 4 
\end{cases}
\]

By Corollary 3.12, we have \( d_R \geq 11 \).

**Example 4.14.** Let \( n = 124, q = 5 \), and \( C \) be the cyclic code with generator polynomial \( g(x) = m_2(x)m_3(x)m_5(x)m_{11}(x)m_{13}(x)m_{14}(x)m_{16}(x)m_{17}(x)m_{22}(x)m_{33}(x)m_{34}(x)m_{35}(x)m_{36}(x)m_{42}(x)m_{43}(x)m_{44}(x)m_{47}(x)m_{62}(x)m_{63}(x)m_{64}(x) \).

So the defining set \( R = \{\alpha^i | i = 1, 5, 6, 9, 11, 13, 21, 22, 23, 24, 25, 26, 27, 29, 30, 33, 34, 37, 38, 41, 42, 43, 44, 45, 46, 47, 54, 55, 57, 58, 59, 61, 62, 63, 64, 65, 66, 67, 72, 77, 79, 81, 82, 83, 86, 87, 91, 96, 101, 104, 105, 106, 108, 110, 111, 112, 115, 120\} \), where \( \alpha \) is a primitive 125th root of unity. Let \( A = \{\alpha^i | 21 \leq i \leq 27\} \cup \{\alpha^i | 29, 30\} \) \( B = \{\beta^j | j = 0, 1, 2\} \), where \( \beta = \alpha^{20} \).

Then \( AB \subseteq R \). The set \( A \) contains 7 consecutive powers of \( \alpha \), and furthermore, it is a subset of a set of 10 consecutive powers of \( \alpha \), with the powers \( \alpha^{28} \) missing. So, from Corollary 3.4, we find

\[
\text{rank}(M(A)_I) = \begin{cases} 
|I|, & \text{for } 1 \leq |I| \leq 7 \\
7, & \text{for } 7 \leq |I| \leq 8 \\
|I| - 1, & \text{for } 8 \leq |I| \leq 10 
\end{cases}
\]
\[ \text{rank}(M(B)_{ij}) = \begin{cases} |I|, & \text{for } 1 \leq |I| \leq 3 \\ 3, & \text{for } |I| \geq 4 \end{cases} \]

By Corollary 3.12., we have \( d_R \geq 12 \).

**Example 4.15.** Take \( n = 127, q = 2 \), and let \( C \) be the cyclic code with generator polynomial \( g(x) = m_1(x)m_3(x)m_5(x)m_7(x)m_9(x) m_{11}(x) m_{13}(x)m_{15}(x)m_{21}(x)m_{23}(x)m_{29}(x)m_{31}(x)m_{43}(x) m_{63}(x) \). So the zeros of \( g(x) \) are \( \alpha^i \) with \( i \in C_1 \cup C_3 \cup C_5 \cup C_7 \cup C_9 \cup C_{11} \cup C_{13} \cup C_{15} \cup C_{21} \cup C_{23} \cup C_{29} \cup C_{31} \cup C_{43} \cup C_{63} \), where

| \( C_1 \) | \{1, 2, 4, 8, 16, 32, 64\} |
| \( C_3 \) | \{3, 6, 12, 24, 48, 65, 96\} |
| \( C_5 \) | \{5, 10, 20, 33, 40, 66, 80\} |
| \( C_7 \) | \{7, 14, 28, 56, 67, 97, 112\} |
| \( C_9 \) | \{9, 17, 18, 34, 36, 68, 72\} |
| \( C_{11} \) | \{11, 22, 44, 49, 69, 88, 98\} |
| \( C_{13} \) | \{13, 26, 35, 52, 70, 81, 104\} |
| \( C_{15} \) | \{15, 30, 60, 71, 99, 113, 120\} |
| \( C_{21} \) | \{21, 37, 41, 42, 74, 82, 84\} |
| \( C_{23} \) | \{23, 46, 57, 75, 92, 101, 114\} |
| \( C_{29} \) | \{29, 39, 58, 78, 83, 105, 116\} |
| \( C_{31} \) | \{31, 62, 79, 103, 115, 121, 124\} |
| \( C_{43} \) | \{43, 45, 53, 85, 86, 90, 106\} |
| \( C_{63} \) | \{63, 95, 111, 119, 123, 125, 126\} |

Let \( A = \{\alpha^i | 119 \leq i \leq 121\} \cup \{\alpha^i | 123 \leq i \leq 126\} \) \( B = \{\beta^j | j = 0, 1, 3, 7\} \), where \( \beta = \alpha^9 \).

Then \( AB \subseteq R \). The set \( A \) contains 4 consecutive powers of \( \alpha \), and furthermore, it is a subset of a set of 8 consecutive powers of \( \alpha \), with the powers \( \alpha^{122} \) missing. So, from Corollary 3.4. we find

\[ \text{rank}(M(A)_{ij}) = \begin{cases} |I|, & \text{for } 1 \leq |I| \leq 4 \\ 4, & \text{for } 4 \leq |I| \leq 5 \\ |I| - 1, & \text{for } 5 \leq |I| \leq 8 \end{cases} \]

\[ \text{rank}(M(B)_{ij}) = \begin{cases} |I|, & \text{for } 1 \leq |I| \leq 2 \\ 2, & \text{for } 2 \leq |I| \leq 3 \\ 3, & \text{for } 4 \leq |I| \leq 7 \\ 4, & \text{for } |I| \geq 8 \end{cases} \]

By Corollary 3.12., we have \( d_R \geq 11 \).

**Example 4.16.** Take \( n = 242, q = 3 \), and let \( C \) be the cyclic code with generator polynomial \( g(x) = m_1(x)m_2(x)m_4(x)m_5(x)m_{10}(x)m_{11}(x) m_{13}(x)m_{14}(x)m_{16}(x)m_{19}(x)m_{23}(x)m_{31}(x)m_{32}(x)m_{33}(x)m_{34}(x)m_{43}(x)m_{47}(x) m_{49}(x)m_{50}(x)m_{52}(x)m_{53}(x)m_{67}(x)m_{68}(x)m_{70}(x)m_{77}(x)m_{122}(x)m_{123}(x) m_{131}(x)m_{134}(x) \). So the zeros of \( g(x) \) are \( \alpha^i \) with \( i \in C_1 \cup C_2 \cup C_4 \cup C_5 \cup C_{10} \cup C_{11} \cup C_{13} \cup C_{14} \cup C_{16} \cup C_{19} \cup C_{23} \cup C_{31} \cup C_{32} \cup C_{35} \cup C_{44} \cup C_{47} \cup C_{49} \cup C_{50} \cup C_{52} \cup C_{53} \cup C_{67} \cup C_{68} \cup C_{70} \cup C_{77} \cup C_{122} \cup C_{125} \cup C_{131} \cup C_{134} \).
where
\[ C_1 = \{1, 3, 9, 27, 81\} \]
\[ C_2 = \{2, 6, 18, 54, 162\} \]
\[ C_4 = \{4, 12, 36, 82, 108\} \]
\[ C_5 = \{5, 15, 45, 135, 163\} \]
\[ C_{10} = \{10, 28, 30, 84, 90\} \]
\[ C_{11} = \{11, 33, 55, 99, 165\} \]
\[ C_{13} = \{13, 39, 85, 109, 117\} \]
\[ C_{14} = \{14, 42, 126, 136, 166\} \]
\[ C_{16} = \{16, 48, 86, 166, 196\} \]
\[ C_{19} = \{19, 29, 57, 87, 171\} \]
\[ C_{23} = \{23, 69, 137, 169, 207\} \]
\[ C_{31} = \{31, 37, 91, 93, 111\} \]
\[ C_{32} = \{32, 46, 96, 138, 172\} \]
\[ C_{35} = \{35, 73, 105, 173, 219\} \]
\[ C_{44} = \{44, 132, 154, 176, 220\} \]
\[ C_{47} = \{47, 59, 141, 177, 181\} \]
\[ C_{49} = \{49, 97, 113, 147, 199\} \]
\[ C_{50} = \{50, 140, 150, 78, 208\} \]
\[ C_{52} = \{52, 98, 156, 194, 226\} \]
\[ C_{53} = \{53, 159, 179, 221, 235\} \]
\[ C_{67} = \{67, 103, 115, 119, 201\} \]
\[ C_{68} = \{68, 128, 142, 184, 204\} \]
\[ C_{70} = \{70, 104, 146, 196, 210\} \]
\[ C_{77} = \{77, 143, 146, 196, 210\} \]
\[ C_{122} = \{122, 124, 130, 148, 202\} \]
\[ C_{125} = \{125, 133, 157, 203, 229\} \]
\[ C_{131} = \{131, 149, 151, 205, 211\} \]
\[ C_{134} = \{134, 160, 206, 230, 238\} . \]

Let \( A = \{\alpha^i | 10 \leq i \leq 16\} \cup \{\alpha^i | 18 \leq i \leq 19\} \) \( B = \{\beta^j | j = -3, 0, 1, 2\} \), where \( \beta = \alpha^{17} \).

Then \( AB \subseteq R \). The set \( A \) contains 7 consecutive powers of \( \alpha \), and furthermore, it is a subset of a set of 10 consecutive powers of \( \alpha \), with the powers \( \alpha^{17} \) missing. So, from Corollary 3.4. we find

\[
\text{rank}(M(A)_I) = \begin{cases} 
|I|, & \text{for } 1 \leq |I| \leq 7 \\
7, & \text{for } 7 \leq |I| \leq 8 \\
|I| - 1, & \text{for } 9 \leq |I| \leq 10 
\end{cases}
\]

\[
\text{rank}(M(B)_I) = \begin{cases} 
|I|, & \text{for } 1 \leq |I| \leq 3 \\
3, & \text{for } 3 \leq |I| \leq 5 \\
4, & \text{for } |I| \geq 6 
\end{cases}
\]

By Corollary 3.12., we have \( d_R \geq 13 \).

**Example 4.17.** Take \( n = 29 \), \( q = 7 \), and let \( C \) be the cyclic code with generator polynomial \( g(x) = m_2(x)m_4(x)m_8(x) \). Then the defining set
is $R = \{2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 21, 22, 26, 27, 28\}$.

By theorem, $d_{BCH} \geq 6$. Clearly $\{2, 3, 5, 6, 8, 9, 11, 12, 14, 15, 17, 18\} \subset R$. Hence HT bound, with $= 2, c_1 = 1, c_2 = 3, \delta = 3, s = 6$ yields that $d \geq 9$

Note that $C$ has the following consecutive sets of zeros:
$\{\alpha^i | i = 2, 3, 4, 5, 6\}, \{\alpha^i | i = 8, 9, 10\}, \{\alpha^i | i = 11, 12, 13, 14, 15\}$,
$\{\alpha^i | i = 17, 18, 19\}, \{\alpha^i | i = 26, 27, 28\}$.

Take $N = \{\alpha^i | i = 2, 3\}$ and $M = \{\beta^j | j = 0, 1, 2, 3, 4, 5\}$ with $\beta = \alpha^3$. Then the elements of $MN$ are zeros of $C$. Since $d_N = 3$ and $4 \leq |M| + d_N - 2$, by Theorem 3.10., we have $d_{MN} \geq 6 + 3 - 1 = 8$. Hence the minimum distance of $C$ is at least 8.

REFERENCES


CHUN-YOU LIN

DEPARTMENT OF MATHEMATICS, NATIONAL TAIWAN NORMAL UNIVERSITY, 88 SEC. 4, TING CHOU ROAD, TAIPEI 11677, TAIWAN

E-mail address: twroseal@hotmail.com