NEW BOUNDS ON THE MINIMUM DISTANCE OF CYCLIC CODES

SAN LING AND BUKET ÖZKAYA*

School of Physical and Mathematical Sciences
Nanyang Technological University
21 Nanyang Link, Singapore 637371

(Communicated by Sihem Mesnager)

Abstract. Two bounds on the minimum distance of cyclic codes are proposed. The first one generalizes the Roos bound by embedding the given cyclic code into a cyclic product code. The second bound also uses a second cyclic code, namely the non-zero-locator code, but is not directly related to cyclic product codes and it generalizes a special case of the Roos bound.

1. Introduction

Estimating the minimum distance of a given linear code is one of the major problems of coding theory. Cyclic codes have attracted the attention of many researchers in the field for more than 50 years due to their nice structure, which allows a fast encoding via shift registers as well as a study of their minimum distance in algebraic terms. They have also given rise to many classes of codes generalizing them (e.g., quasi-cyclic codes), but the research on cyclic codes is never out of fashion since they provide the base to the theory of all their generalizations.

Several bounds on the minimum distance are derived from the zero set of the given cyclic code. The first and maybe the most famous one was obtained by Bose and Chaudhuri ([1]) and by Hocquenghem ([4]). The so-called BCH bound looks for the biggest subset of consecutive elements in the zero set. An extension of the BCH bound was formulated by Hartmann and Tzeng in [3], where consecutive sets of consecutive elements are searched to estimate the minimum distance. In a sense, the HT bound can be considered as a two-directional BCH bound. The Roos bound ([6, 7]) generalizes this idea further by allowing gaps in both directions of consecutive element search in the zero set.

Recently, Zeh and Bezzateev presented a new method for estimating the minimum distance of cyclic codes in [8], which also generalizes the BCH bound. Their idea is to use a second cyclic code, namely the non-zero-locator code, which fills the gaps in the zero set of the given cyclic code, and then the derived minimum distance code is expressed in terms of the parameters of this second cyclic code. In [9], two extensions of the HT bound were derived by two different techniques. The first bound uses properties of cyclic product codes ([2, 5]), whereas the second bound is again obtained through some non-zero-locator code.

2010 Mathematics Subject Classification: Primary: 94B15, 94B65; Secondary: 11T71.
Key words and phrases: Cyclic codes, product code, minimum distance bound, Roos bound.
The authors are supported by NTU Research Grant M4080456.
* Corresponding author.
In this paper, we aim at generalizing the Roos bound by using the cyclic product code method first, and then once more with the non-zero-locator code method. We present two new lower bounds on the minimum distance of a given cyclic code, which contain the aforementioned results in [8] and [9] as special cases. We discuss the performance of the new results using examples.

This paper is organized as follows. In Section 2, we provide some background on cyclic codes and the main contributions in [8] and [9]. In Section 3, we present our results and explain how the previous minimum distance bounds are improved. Moreover, we provide a few numerical examples and we also compare these new bounds with each other.

2. Preliminaries

Let $\mathbb{F}_q$ denote the finite field with $q$ elements, where $q$ is a prime power, and let $n$ be a positive integer with $\gcd(n,q) = 1$. A linear code $C$ of length $n$ over $\mathbb{F}_q$ is called a cyclic code if it is invariant under the cyclic shift of codewords, i.e., $(c_0,\ldots,c_{n-1}) \in C$ implies $(c_{n-1},c_0,\ldots,c_{n-2}) \in C$. A $q$-ary cyclic code of length $n$, dimension $k$ and minimum distance $d$ will be denoted by $C(n,k,d;q)$.

Consider the principal ideal $I = \langle x^m-1 \rangle$ of $\mathbb{F}_q[x]$ and define the residue class ring $R := \mathbb{F}_q[x]/I$. To an element $\bar{a} \in \mathbb{F}_q^n$, we can associate an element of $R$ via the following isomorphism:

$$\phi : \mathbb{F}_q^n \rightarrow R$$

$$\bar{a} = (a_0,\ldots,a_{n-1}) \mapsto a(x) := a_0 + a_1x + \cdots + a_{n-1}x^{n-1}. $$

Observe that the cyclic shift on $\mathbb{F}_q^n$ corresponds to multiplication by $x$ in $R$. Hence, a $q$-ary cyclic code of length $n$ can be viewed as an ideal in $R$. Since every ideal in $R$ is principal, there exists a unique monic polynomial $g(x)$ of degree $n-k$ such that $C = \langle g(x) \rangle$, i.e., each codeword $c(x) \in C$ must be of the form $c(x) = a(x)g(x)$ where $\deg(a(x)) < k$. The polynomial $g(x)$ is called the generator polynomial of the cyclic code $C$ and $g(x)|x^n-1$.

Let $\alpha$ be a primitive $n$'th root of unity over $\mathbb{F}_q$. The set of roots of the generator polynomial

$$N := \{\alpha^i : g(\alpha^i) = 0\}$$

is called the zero set of $C$. The set $N$ is said to be a consecutive set of zeros if there exist integers $f,m$ and $\delta$ with $\delta \geq 2$, $m \neq 0$ such that

$$N = \{\alpha^{f+jm} : 0 \leq j \leq \delta - 2\}. $$

We now recall the Roos bound on the minimum distance of a given cyclic code. Let $C_N$ be the cyclic code of length $n$ over $\mathbb{F}_q$ with a given zero set $N$. Let $d_N$ denote the minimum distance of $C_N$. For the proof of the result below, we refer to [7, Theorem 2].

**Theorem 2.1 (Roos bound).** Let $N$ and $M$ be nonempty sets of $n$'th roots of unity over $\mathbb{F}_q$. If there exists a consecutive set $\bar{M}$ containing $M$ such that $|\bar{M}| \leq |M| + d_N - 2$, then we have $d_{MN} \geq |M| + d_N - 1$ where $MN = \bigcup_{\lambda \in M} \lambda N$.

If $N$ is consecutive like in (2), then we obtain the following by using the fact $d_N = |N| + 1$. 

---

*Advances in Mathematics of Communications*  Volume X, No. X (200X), X–XX
Corollary 1. [7, Corollary 1] If \( N \) is a consecutive set, then the existence of a consecutive set \( M \) containing \( M \) and satisfying \( |M| < |M| + |N| \) implies \( d_{MN} \geq |M| + |N| \).

In particular, the case \( M = \{1\} \) yields the BCH bound and by taking \( M = M \) we obtain the HT bound ([8, Theorem 2]). If \( M = M_1 M_2 \cdots M_r \), where each \( M_j \) is consecutive for \( 1 \leq j \leq r \), then we get the generalized HT bound ([3, Theorem 3],[6, Theorem 2]).

In [8], Zeh and Bezzateev derived a generalization of the BCH bound, which improves the HT bound in many cases. Their technique relates another cyclic code to a given cyclic code. This second cyclic code is called the non-zero-locator code and it is defined as follows.

Definition 2.2. Let a \( q \)-ary cyclic code \( C(n, k, d; q) \) be given. Let \( \gcd(n, n_\ell) = 1 \) and let \( F_q(n) \) be the extension field of \( F_q \) containing the \( n_\ell \)'th roots of unity (i.e., the splitting field of the polynomial \( x^{n_\ell} - 1 \)). Let \( \alpha \) and \( \beta \) be primitive \( n \)'th and \( n_\ell \)'th roots of unity, respectively. Then \( L(n_\ell, k_\ell, d_\ell; q_\ell) \) is a non-zero-locator code of \( C \) if there exist integers \( f_1, f_2, m_1, m_2 \) and \( \delta \) with \( \delta \geq 2, m_1 \neq 0, m_2 \neq 0 \) such that

\[
\gcd(n, m_1) = \gcd(n_\ell, m_2) = 1 \quad \text{and} \quad \forall \delta \neq c(x) \in C \quad \text{and} \quad \forall \delta \neq a(x) \in L,
\]

the following holds:

\[
(3) \quad \sum_{j=0}^{\infty} c(\alpha^{f_1+jm_1})a(\beta^{f_2+jm_2})x^j \equiv 0 \pmod{x^{\delta-1}}.
\]

Note that \( f_2 = 0 \) and \( m_1 = m_2 = 1 \) in [8, Definition 2]. Their method looks for the “longest” sequence

\[
c(\alpha) a(\beta), c(\alpha^{f_1+m_1}) a(\beta^{f_2+m_2}), \ldots, c(\alpha^{f_1+(\delta-2)m_1}) a(\beta^{f_2+(\delta-2)m_2}),
\]

and they obtain the following bound on the minimum distance, which is expressed in terms of the parameters of the associated non-zero-locator code.

Theorem 2.3. [8, Theorem 2] Given a cyclic code \( C(n, k, d; q) \), let \( L(n_\ell, k_\ell, d_\ell; q_\ell) \) be its associated non-zero-locator code with \( \gcd(n, n_\ell) = 1 \) and let the integer \( \delta \) be as in Definition 2.2. Then

\[
d \geq \left\lfloor \frac{\delta}{d_\ell} \right\rfloor.
\]

Given two \( q \)-ary cyclic codes \( C_1(n_1, k_1, d_1; q) \) and \( C_2(n_2, k_2, d_2; q) \), the cyclic product code \( C_1 \otimes C_2(n_1 n_2, k_1 k_2, d_1 d_2; q) \) contains all the Kronecker products \( \vec{c}_1 \otimes \vec{c}_2 \) as codewords, where \( \vec{c}_1 \in C_1 \) and \( \vec{c}_2 \in C_2 \). If the codewords of \( C_1 \otimes C_2 \) are written as arrays of size \( n_1 \times n_2 \), then the rows of each array are codewords in \( C_1 \) and the columns are codewords in \( C_2 \). Cyclic product codes were introduced by Burton and Weldon in [2], where it was shown that a given cyclic product code of length \( n_1 n_2 \) is equivalent to a cyclic code if \( \gcd(n_1, n_2) = 1 \) ([2, Theorem 1]). If \( C_1 = \langle g_1(x) \rangle \) and \( C_2 = \langle g_2(x) \rangle \) with \( an_1 + bn_2 = 1 \) for some integers \( a \) and \( b \), then the generator polynomial of their product is \( \gcd(g_1(x^{bn_2})g_2(x^{an_1}), x^{n_1 n_2} - 1) \) (see [2, Theorem 3]). Therefore, the zero set of the cyclic product code is determined by the zero sets of \( C_1 \) and \( C_2 \). Let \( N_1 \) and \( N_2 \) denote the zero sets of \( C_1 \) and \( C_2 \), respectively. We set \( \Omega_1 \) and \( \Omega_2 \) as the sets of all \( n_1 \)'th and \( n_2 \)'th roots of unity, respectively. Then, the zero set \( N \) of the cyclic product code \( C_1 \otimes C_2 \) is given as ([5, Theorem 3]):

\[
N = \{ \alpha \cdot \beta : (\alpha, \beta) \in (N_1, N_2) \cup (N_1, \Omega_2 - N_2) \cup (\Omega_1 - N_1, N_2) \}.
\]
Zeh et al. provided two generalizations of the HT bound in [9], in a similar way that the bound given in Theorem 2.3 generalizes the BCH bound, but they used $q$-ary non-zero-locator codes in their results. The first minimum distance bound they derived uses the notion of cyclic product codes in its proof, whereas the proof of the second generalization is more involved and close to the proof of Theorem 2.3, yielding a stronger bound than the first one. We sum up and reformulate the results of Zeh et al. in our notation below.

**Theorem 2.4.** [9, Theorems 5 and 6] Let $C(n,k,d;q)$ and $L(n_\ell,k_\ell,d_\ell;q)$ be two $q$-ary cyclic codes such that $\gcd(n,n_\ell) = 1$. Let $\alpha$ and $\beta$ be primitive $n$'th and $n_\ell$'th roots of unity, respectively. Suppose that there exist integers $f_1,f_2,m_1,m_2,\delta$ and $\nu$ satisfying $\delta \geq 2, \nu > 0, m_1 \neq 0, m_2 \neq 0$ and $\gcd(n,m_1) = \gcd(n_\ell,m_2) = 1$. If $\forall 0 \neq c(x) \in C$ and $\forall 0 \neq a(x) \in L$, the following holds:

i. $\sum_{j=0}^{\infty} c(\alpha^{f_1+jm_1+k})a(\beta^{f_2+jm_2+k})x^j \equiv 0 \mod x^{\delta-1}, \ \forall k = 0, \ldots, \nu$, then

$$d \geq \left\lceil \frac{\delta + \nu}{d_\ell} \right\rceil.$$ 

ii. $\sum_{j=0}^{\infty} c(\alpha^{f_1+jm_1+k})a(\beta^{f_2+jm_2})x^j \equiv 0 \mod x^{\delta-1}, \ \forall k = 0, \ldots, \nu$, then we have

$$d \geq \left\lceil \frac{\delta}{d_\ell} + \nu \right\rceil.$$ 

In the next section, we state and prove two generalizations of the Roos bound for cyclic codes in a similar manner, which will also contain the minimum distance bounds given in Theorems 2.3 and 2.4 above as their special cases.

### 3. Generalized Roos bounds

After the preparation in Section 2, the following result is immediate.

**Theorem 3.1.** Let $C(n,k,d;q)$ and $L(n_\ell,k_\ell,d_\ell;q_\ell)$ be two cyclic codes such that $\gcd(n,n_\ell) = 1$. If $C = \langle g(x) \rangle$, then there exists a cyclic code $C'(n,k',d';q_\ell)$ such that $C' = \langle g(x) \rangle$ over $\mathbb{F}_{q_\ell}$. Assume that the cyclic product code $C' \otimes L$ over $\mathbb{F}_{q_\ell}$ has a zero set $MN$, where $M$ and $N$ satisfy the conditions in Theorem 2.1. If $d_N = \delta$ and $|M| = t + 1$, then we have

$$d \geq \left\lceil \frac{\delta + t}{d_\ell} \right\rceil.$$ 

**Proof.** The cyclic product code $C' \otimes L$ is equivalent to a cyclic code over $\mathbb{F}_{q_\ell}$ since $\gcd(n,n_\ell) = 1$. Note that if the codewords of $C' \otimes L$ are written as arrays of size $n \times n_\ell$, then the columns of each array are codewords in $L$ and the rows are codewords in the $\mathbb{F}_{q_\ell}$-linear code $C'$, which has length $n$ and contains $C$ as a subfield subcode. Hence, we have $d \geq d'$. Applying the Roos bound on $C' \otimes L$ yields $d' \cdot d_\ell \geq \delta + t$ and the result follows. \hfill $\Box$

**Remark 1.** In particular, if both $N$ and $M$ are consecutive and $q = q_\ell$, then we obtain the bound given in Theorem 2.4 i. If furthermore $M = \{1\}$ (i.e., $t = 0$), then we get the statement of Theorem 2.3.
Example 1. Consider the binary cyclic code $C$ of length 31 with the zero set $N_1 = \{\alpha^i : i = 1, 2, 4, 5, 8, 9, 10, 11, 13, 15, 16, 18, 20, 21, 22, 23, 26, 27, 29, 30\}$, where $\alpha$ is a fixed 31'st root of unity satisfying $\alpha^5 + \alpha^2 + 1 = 0$ and $d = 10$. Let $L$ be the binary cyclic code of length 5 with the zero set $N_2 = \{\beta^0 = 1\}$, where $\beta$ is a fixed 5'th root of unity with $\beta^3 + \beta^3 + \beta^2 + \beta + 1 = 0$ and $d_\ell = 2$. Theorem 3.1 gives $d \geq 9$, whereas the Roos and HT bounds estimate $d \geq 7$ and the BCH bound estimates $d \geq 5$.

For the second generalization, we require more assumptions for the statement and the proof is more involved.

**Theorem 3.2.** Let $C(n, k, d; q)$ and $L(n_f, k_f, d_\ell; q_\ell)$ be two cyclic codes such that $\gcd(n, n_f) = 1$. Let $\alpha$ and $\beta$ be primitive $n'$th and $n_f$'th roots of unity, respectively. Suppose that there exist integers $f_1, f_2, m_1, m_2$ and $\delta$ such that $\delta \geq 2, m_1 \neq 0, m_2 \neq 0$ and $\gcd(n, m_1) = \gcd(n_f, m_2) = 1$. Assume that $\forall 0 \neq c(x) \in C$ and $\forall 0 \neq a(x) \in L$, the following holds:

\[
(5) \quad \sum_{0 \leq j \leq t} c(\alpha^{f_1+jm_1+k})a(\beta^{f_2+jm_2})x^j \equiv 0 \mod x^\delta - 1, \quad \forall k = i_0, \ldots, i_t
\]

provided $0 \leq i_0 < i_1 < \cdots < i_t \leq n - 1$ and $i_t - i_0 + 1 < \left\lfloor \frac{\delta}{d_\ell} + t \right\rfloor$. Then we have

\[
d \geq \left\lfloor \frac{\delta}{d_\ell} + t \right\rfloor.
\]

**Proof.** Let $c(x) = \sum_{i \in Y} c_i x^i \in C$ and $a(x) = \sum_{m \in Z} a_m x^m \in L$ be two nonzero codewords with nonempty supports $Y \subseteq \{0, \ldots, n - 1\}$ and $Z \subseteq \{0, \ldots, n_f - 1\}$, respectively. Let $F_{q'}$ be the smallest extension of $F_q$ containing $\alpha$ and $\beta$ (i.e., $F_{q'} = F_q(\alpha, \beta)$). We combine the $t + 1$ series in (5) linearly, by multiplying each of them by some nonzero elements $\lambda_k \in F_{q'}$ and then summing them up:

\[
\sum_{k=i_0}^{i_t} \lambda_k \sum_{0 \leq j \leq t} c(\alpha^{f_1+jm_1+k})a(\beta^{f_2+jm_2})x^j
\]

\[
= \sum_{k=i_0}^{i_t} \lambda_k \sum_{j=0}^{\infty} \left( \sum_{i \in Y} c_i \alpha^{i(f_1+jm_1+k)} \right) a(\beta^{f_2+jm_2})x^j
\]

\[
= \sum_{k=i_0}^{i_t} \lambda_k \sum_{i \in Y} c_i \alpha^{i(f_1+k)} \sum_{j=0}^{\infty} \alpha^{jm_1} a(\beta^{f_2+jm_2})x^j
\]

\[
= \sum_{i \in Y} c_i \alpha^{if_1} \left( \sum_{k=i_0}^{i_t} \lambda_k \alpha^{ik} \right) \sum_{j=0}^{\infty} \alpha^{jm_1} a(\beta^{f_2+jm_2})x^j
\]

\[
= 0 \mod x^\delta - 1.
\]

We choose $\lambda_{i_0}, \ldots, \lambda_{i_t}$ such that $t$ terms are annihilated in the sum (6). Consider the following system of linear equations:
Note that Theorem 3.2 above generalizes Corollary 1, where $\gcd(Y, n) = 1$ (see Proposition 1 in the Appendix). Hence, the numerator is a nonzero polynomial; the statement follows from (6). We can rewrite (6) as:

$$
\sum_{i \in \mathcal{Y}} c_i \alpha_1 \beta_1 \left( \sum_{k=\bar{i}_t}^{\bar{i}_s} \lambda_k \alpha_1 \right) \sum_{j=0}^{\infty} \alpha_{ijm1} \beta_{m2} \gamma_i x^j
$$

where $\bar{i}_t, \ldots, \bar{i}_s \in \{0, \ldots, n-1\}$. Observe that we have $\alpha_i$ times a Vandermonde matrix on the left hand side. Hence, the system has a unique solution. Let $\mathcal{Y} = \mathcal{Y} - \{r_{i_0}, \ldots, r_{i_t-1}\}$ and note that, by replacing $\mathcal{Y}$ by $\mathcal{Y}$, (6) will not vanish as long as $i_t - i_0 + 1 < \frac{d}{d_t} + t$. We can rewrite (6) as:

$$
\sum_{i \in \mathcal{Y}} c_i \alpha_1 \beta_1 \left( \sum_{k=\bar{i}_t}^{\bar{i}_s} \lambda_k \alpha_1 \right) \sum_{j=0}^{\infty} \alpha_{ijm1} \beta_{m2} \gamma_i x^j
$$

where $\mathcal{Y}$ is an $n \times n$ matrix.

The denominator of the rational expression (7) above is a nonzero polynomial (with constant term 1) of degree $|\mathcal{Y}| \cdot |Z|$. The numerator in (7) is a linear combination of $\prod_{(r,u) \neq (i,m)} (1 - \alpha^{rm1} \beta^{um2} x)$, where the polynomials in this product are pairwise distinct and therefore linearly independent since $\gcd(n, n_t) = \gcd(n, m_1) = \gcd(n_t, m_2) = 1$ (see Proposition 1 in the Appendix). Hence, the numerator is a nonzero polynomial of degree less than or equal to $|\mathcal{Y} + 1| |Z| - 1 = |\mathcal{Y} + 1| |Z| - 1$, which should be at least $\delta - 1$. In particular, for $|\mathcal{Y}| = d$ and $|Z| = d_t$, we obtain $|\mathcal{Y}| \leq d - t$ and the statement follows from $(d - t)d_t - 1 \leq \delta - 1$.

**Remark 2.** Note that Theorem 3.2 above generalizes Corollary 1, where $N$ is consecutive with $|N| = \delta - 1$ (hence $d_N = \delta$) and $M = \{\alpha^{i_0}, \ldots, \alpha^{i_t}\}$ with $\mathcal{M} = \prod_{r \in \mathcal{Y}\backslash \{i\}} \prod_{u \in \mathcal{Z}} (1 - \alpha^{rm1} \beta^{um2} x)$.
\{\alpha^0, \alpha^{i_0+1}, \ldots, \alpha^{i_t-1}, \alpha^{i_t}\}. The special case when \(M\) is consecutive (i.e., \(M = \bar{M}\)) and \(q = q_t\) corresponds to the bound in Theorem 2.4 ii. Moreover, if \(M = \{1\}\), we obtain Theorem 2.3.

**Example 2.** We consider the ternary cyclic code \(C\) of length 13 with the zero set \(N_1 = \{\alpha^i : i = 2, 4, 5, 6, 7, 8, 10, 11, 12\}\), where \(\alpha\) is a fixed 13'th root of unity satisfying \(\alpha^3 + \alpha^2 + \alpha - 1 = 0\). Let \(L \subseteq \mathbb{F}_3^4\) be the ternary cyclic code with the zero set \(N_2 = \{1, 3\}\), where \(\beta\) is a fixed 4'th root of unity so that \(\beta^2 + 1 = 0\) and \(d_\ell = 2\). Theorem 3.2 gives \(d \geq 7\), which is equal to the exact minimum distance of \(C\).

If \(N\) is a consecutive set in the first bound given in Theorem 3.1, then it is weaker than the second bound given in Theorem 3.2 in general. But if \(N\) is not consecutive, then this does not necessarily hold, as the following example shows.

**Example 3.** We now take the ternary cyclic code \(C\) of length 11 with the zero set \(N_1 = \{\alpha^i : i = 1, 2, 4, 5, 6, 10\}\), where \(\alpha\) is a fixed 11'th root of unity satisfying \(\alpha^5 + \alpha^4 - \alpha^3 + \alpha^2 - 1 = 0\). We choose the second cyclic code \(L \subseteq \mathbb{F}_3^4\) with the zeros \(N_2 = \{\beta^i : i = 2, 4\}\), where \(\beta\) is a fixed 4'th root of unity such that \(\beta^2 + 1 = 0\) and \(d_\ell = 2\). Theorem 3.1 yields \(d \geq 5\), where the actual minimum distance of \(C\) is equal to 5 and hence Theorem 3.1 gives a sharp estimate. On the other hand, Theorem 3.2 estimates \(d \geq 4\), as the BCH bound also does.

**Acknowledgments**

The authors thank Seher Tutdere and Frederic Ezerman for their stimulating discussions which helped to improve the results in this paper. The computational support of Adama Asa Fahreza and Kevin Schires on the treatment of long binary arrays has decreased the huge amount of computational time to find the examples presented above. The authors also thank the anonymous reviewers for their useful comments. The authors are supported by NTU Research Grant M4080456.

**Appendix**

The following result was shown for the particular case \(m_1 = m_2 = 1\) in [8, Lemma 3].

**Proposition 1.** Let \(\alpha\) and \(\beta\) be primitive \(n\)'th and \(n_\ell\)'th roots of unity, respectively. If \(\gcd(n, n_\ell) = \gcd(n, m_1) = \gcd(n_\ell, m_2) = 1\), then the binomials \(1 - \alpha^{m_1} \beta^{m_2} x\) are pairwise distinct for \(i \in \{0, \ldots, n - 1\}\) and \(j \in \{0, \ldots, n_\ell - 1\}\).

**Proof.** Let \(F_{q^r}\) be the smallest extension field of \(F_q\) containing \(\alpha\) and \(\beta\) (i.e., \(r\) is the smallest positive integer satisfying \(n|q^r - 1\) and \(n_\ell|q^r - 1\)). If we set \(N = q^r - 1\), then let \(\gamma\) be a primitive element in \(F_{q^r}\) such that \(\alpha = \gamma^{N/n}\) and \(\beta = \gamma^{N/n_\ell}\).

We will prove the statement by contraposition. Assume that \(\alpha^{m_1} \beta^{m_2} = \alpha^{m_{1k}} \beta^{m_{2j}}\) for some \(i, k \in \{0, \ldots, n - 1\}\) and \(j, t \in \{0, \ldots, n_\ell - 1\}\) such that \(i \neq k\) and \(j \neq t\). Then

\[
\alpha^{m_1} \beta^{m_2} = \alpha^{m_{1k}} \beta^{m_{2t}} \iff \alpha^{(i-k)m_1} = \beta^{(j-t)m_2}
\]

\[
\iff \gamma^{\frac{N(i-k)m_1}{n}} = \gamma^{\frac{N(j-t)m_2}{n_\ell}}
\]

\[
\iff \gamma^{n_\ell (i-k)m_1 - n(j-t)m_2} = \lambda n_\ell, \text{ for some } \lambda \geq 0.
\]

\[
\iff \gcd(n, n_\ell m_1) > 1 \text{ and } \gcd(n_\ell, nm_2) > 1.
\]

\[\square\]
References

[1] R. C. Bose and D. K. R. Chaudhuri, On a class of error correcting binary group code, *Information and Control*, 3 (1960), 68–79.

[2] H. O. Burton and E. J. Weldon, Cyclic product codes, *IEEE Trans. Information Theory*, 11 (1965), 433–439.

[3] C. Hartmann and K. Tzeng, Generalizations of the BCH bound, *Information and Control*, 20 (1972), 489–498.

[4] A. Hocquenghem, Codes correcteurs d’erreurs, *Chiffres*, 2 (1959), 147–156.

[5] S. Lin and E. J. Weldon, Further results on cyclic product codes, *IEEE Trans. Information Theory*, 16 (1970), 452–459.

[6] C. Roos, A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound, *J. Combin. Theory Ser. A*, 33 (1982), 229–232.

[7] C. Roos, A new lower bound for the minimum distance of a cyclic code, *IEEE Trans. Inform. Theory*, 29 (1983), 330–332.

[8] A. Zeh and S. V. Bezzateev, A new bound on the minimum distance of cyclic codes using small-minimum-distance cyclic codes, *Des. Codes Cryptogr.*, 71 (2014), 229–246.

[9] A. Zeh, A. Wachter-Zeh, M. Gadouleau and S. V. Bezzateev, Generalizing bounds on the minimum distance of cyclic codes using cyclic product codes, *Proc. IEEE ISIT*, Istanbul, Turkey, 2013, 126–130.

Received December 2018; revised June 2019.

E-mail address: lingsan@ntu.edu.sg
E-mail address: buketozkaya@ntu.edu.sg