Journal of Algebraic Systems
Vol. 7, No. 2, (2020), pp 291-300

SOME NEW CONSTRUCTIONS OF LINEAR CODES INCLUDING A WIDE FAMILY OF MDS CODES

A. RAFIEEPOUR AND M. MAZROOEI*

Abstract. Let $\mathbb{Z}_p$ be the finite field of integers modulo p, where $p > 3$ is a prime integer. This paper presents new constructions of linear codes over $\mathbb{Z}_p$. Based on our construction, linear codes of length $p-1$, including a wide family of MDS codes, and codes of length $(p-1)^2$ are constructed. We shall discuss the parameters of the codes defined while describing a generator matrix for the first family.

1. Introduction

Linear codes are an interesting area in data transmission for two reasons. First, they provide a mechanism to transmit data over a noisy channel while ensuring the data's integrity and second, they can be used to protect data against unwanted readers, by using them for encryption. Linear codes, and ideas behind some of the good constructions, have also found many exciting applications such as in complexity theory, cryptography, pseudorandomness and explicit combinatorial constructions, see for example [18, 19, 11, 3].

Linear codes are constructed over symbols from a group [22, 23], a ring [12, 15, 9, 20, 10] or a field [21, 2, 7, 1, 5, 16], while they have a wide range of parameters (block or constraint lenght, dimension, rate, distance, etc).

One of the important goals in coding theory is to maximize the minimum distance d for given alphabet size and number of codewords. This

MSC(2010): Primary: 94B05; Secondary: 65T50.
Keywords: Linear code, MDS code.
Received: 27 April 2018, Accepted: 21 June 2019.
*Corresponding author.

increases the number of errors that can be detected or corrected, making the transmision more reliable. The well-known Singleton Bound [17] says that for codes C of lenght n over any alphabet of size m,

$$d(C) \leq n - log_m(|C|) + 1.$$

Codes meeting this bound are called *Maximum Distance Separable* codes (MDS codes, for short). For a linear $[n, k, d]$-code, de Boer [6] defined $s(C) = n - k + 1 - d$ as the *Singleton defect*, the Singleton Bound ensures that $s(C)$ is always non-negative. Therefore, a linear code C is MDS when $s(C) = 0$, while he called a code C *almost MDS* (AMDS, for short) when $s(C) = 1$. Unlike MDS codes, the dual code of an AMDS code is not necessarily AMDS, codes in which $s(C) = s(C^{\perp}) = 1$ is called *near MDS* (NMDS) codes [8].

Due to the fact of the importance of linear codes, a wide range of works are gone in this context, many authors have studied construction methods of linear codes. In [7], boolean functions are employed to construct binary linear codes, while in [3], construction of linear codes over $GF(p^h)$ using perfect nonlinear functions is discussed. Beyond, someone can find other constrution methods for linear codes in [2] and [17]. In the meantime, some authors focused on the construction methodes of MDS, AMDS and NMDS codes, see [21, 15, 1, 16, 14, 5, 17].

This paper is organized to present some new construction methods of linear codes over the Galois field $\mathbb{Z}_p$, $p > 3$ a prime, which leads to construct interesting families of MDS codes. For this, the paper is structured as follows. In Section 2, we recall some preliminaries which are needed to follow the paper. Section 3 deals with our approach to construct a class of linear codes of length $p - 1$ over the field $\mathbb{Z}_p$, while we will study the structure of the constructed codes. In Section 4, the minimum distance of the codes introduced in Section 3 will be discussed. Specially, we give a sufficient condition for the codes to be MDS. In the last section, we will generalize the process in Section 3 to construct two-dimentional codes of length $(p - 1)^2$ and discuss about the dimension and the distance of them.

2. Preliminaries

Let q be a prime power and F_q denotes the Galois field of size q. A linear code C of length n over the field F_q is just a vector subspace of $(F_q)^n$, the vector space of all n-tuples over F_q. If the dimension of C, denoted by $\dim(C)$, is k then C will be called an $[n, k]_q$-linear code. In this case, the $(k \times n)$-matrix G whose rows form a basis for C is called a generator matrix of the code C. The encoding procedure of a linear

code can be easily done by its generator matrix. It sufficies to encode an input vector x of length k by the codeword $c = xG$.

The dual code of an $[n,k]_q$-linear code C is the $[n,n-k]$-linear code defined by

$$C^{\perp} = \{x \in (F_q)^n \mid < x, c >= 0,\ \forall c \in C\},$$

where $< x, c >= \sum_{i=1}^{n} x_i c_i$. A generator matrix H of $C^{\perp}$ is called a parity-check matrix of the code C. This means that a word $c \in (F_q)^n$ is a codeword of C iff the syndrome of c, which is defined as the vector-matrix product cH^t, is zero. One of the most efficient decoding algorithms of linear codes, called syndrome decoding, is described by calculating the syndrome of words, See [17].

The (Hamming) distance between any words $x, y \in (F_q)^n$, denoted by $d(x,y)$, is the number of those positions i whose $x_i \neq y_i$. The minimum distance of a linear code C is defined as

$$d(C) = \min\{d(x,y) \mid x, y \in C,\ x \neq y\}.$$

It can be easily checked that $d(C) = \min\{wt(x) \mid x \in C,\ x \neq 0\}$, where $wt(x)$ is the number of non-zero components of the word x.

Theorem 2.1. *([17]) Let H be a parity-check matrix for an $[n,k]_q$-linear code C. Then every set of $s-1$ columns of H are linearly independent (over F_q) iff C has minimum distance at least s.*

It follows from the theorem that a linear code C with a parity-check matrix H has minimum distance (exactly) d if and only if every set of $d-1$ columns of H are linearly independent, and some set of d columns are linearly dependent. Hence this theorem could be used to determine the minimum distance of a linear code, given a parity check matrix.

3. $\mathfrak{V}$-codes

Throughout this section, $p > 3$ is a prime, $n = p - 1$ and $\mathfrak{n} = \{1, 2, \ldots, n\}$.

Definition 3.1. For a non-empty subset $A \subseteq \mathfrak{n}$, the $\mathfrak{V}$-code C_A is the vector subspace of $(\mathbb{Z}_p)^n$ defined by

$$C_A = \{(c_1, \ldots, c_n) \in (\mathbb{Z}_p)^n \mid \sum_{i=1}^{n} c_i i^a = 0,\ \forall a \in A\}.$$

Note that a $\mathfrak{V}$-code C_A, $A \subseteq \mathfrak{n}$, is just the space of the solutions of the system of linear equations

$$\sum_{i\in\mathfrak{n}} i^a x_i = 0, \ (a \in A),$$

over the Galois field $\mathbb{Z}_p$ with unknowns $x_1, \ldots, x_n$. Since the matrix of this system, i.e the matrix $(i^a)_{i\in\mathfrak{n},\ a\in A}$, is of Vandermond's type, we have $\dim(C_A) = n - |A|$.

According to the definition of $\mathfrak{V}$-codes, it is clrear that the matrix H_A whose rows are the vectors $(1, 2^a, \ldots, n^a)$, $a \in A$, is a parity-check matrix for the code C_A. Next, we are going to describe the generator matrix of the code C_A. For this, we need the following simple lemma.

Lemma 3.2. *Let F be a finite field of order q and $F^\times$ denotes the multiplicative group of F. For an integer k, if $q-1 \nmid k$ then $\sum_{i\in F^\times} i^k = 0$.*

Proof. Let $F^k = \{a^k \mid a \in F\}$ and assume that b is a generator for the cyclic group $F^\times$. Then $b^k F^k = F^k$. Now, we have

$$b^k \sum_{i\in F^\times} i^k = \sum_{i\in F^\times} b^k i^k = \sum_{i\in F^\times} i^k,$$

showing that $(b^k - 1)\sum_{i\in F^\times} i^k = 0$. Since $q - 1 \nmid k$, $b^k \neq 1$. Therefore, we should have $\sum_{i\in F^\times} i^k = 0$, as desired. □

Lemma 3.3. *Let $A \subseteq \mathfrak{n}$. Then there exists $B \subseteq \mathfrak{n}$ such that $C_A^\perp = C_B$.*

Proof. Let $B = \mathfrak{n} \setminus \{n - a \mid a \in A\}$. We claim that $C_A^\perp = C_B$. First, note that the vectors $(1^b, 2^b, \ldots, n^b)$, $b \in B$, form a basis of $C_B^\perp$. We show that $(1^b, 2^b, \ldots, n^b) \in C_A$ for all $b \in B$. Let $a \in A$ and $b \in B$. There are two cases.

Case 1. $2 \leq a + b \leq 2p - 3$. Since $a + b \neq n$, $p - 1 \nmid a + b$. Thus, by lemma 3.2, we have $\sum_{i=1}^n i^{a+b} = 0$.

Case 2. $a + b = 2p - 2 = 2(p - 1)$. In this case, $a = b = p - 1$. Hence,

$$\sum_{i=1}^n i^{a+b} = \sum_{i=1}^n i^{2(p-1)} = \sum_{i=1}^n i^2.$$

Since $p - 1 \nmid 2$, lemma 3.2 shows that $\sum_{i=1}^n i^2 = 0$.

So the vector $(1^b, 2^b, \ldots, n^b) \in C_A$ for all $b \in B$. Thus, $C_B^\perp \subseteq C_A$. Since $\dim(C_B^\perp) = |B| = n - |A| = \dim(C_A)$, we have $C_B^\perp = C_A$, proving that $C_A^\perp = C_B$. □

Corollary 3.4. *Let $A \subseteq \mathfrak{n}$ and $B \subseteq \mathfrak{n}$ such that $C_A^{\perp} = C_B$. Then the matrix G_A whose rows are the vectors $(1, 2^b, \ldots, n^b)$, $b \in B$, is a generator matrix for C_A.*

Proof. By proposition 3.3, $C_A^{\perp} = C_B$ where $B = \mathfrak{n} \setminus \{n - a \mid a \in A\}$. Thus, the set $\{(1, 2^b, \ldots, n^b) \mid b \in B\}$ is a basis of $(C_A^{\perp})^{\perp} = C_A$, as desired. □

4. Minimum Distance of $\mathfrak{S}$-codes

In this section, we will show that there are a wide range of MDS codes in the family of $\mathfrak{V}$-codes. First, we need the following definition.

Definition 4.1. Let $A \subseteq \mathfrak{n}$ and $1 \leq d \leq n$. We say that A is an d-successive set if there exists some $a \in A$ in which $A = \{a, a+1, \ldots, a+d-1\}$.

Now, we introduce an interesting family of linear MDS codes.

Theorem 4.2. *Let $A \subseteq \mathfrak{n}$ and $1 \leq d \leq n$. If A is a d-successive set, then C_A is an MDS code.*

Proof. By hypothesis, there exists $a \in A$ such that $A = \{a, a+1, ..., a+d-1\}$. Since $\dim(C_A) = n - d$, It is enough to prove that there is no codeword of weight $t \leq d$ in C_A. This will be done by induction on d.

Let $d = 1$. Then $C_A = \{(x_1, \ldots, x_n) \mid \sum_{i=1}^{n} x_i i^a = 0\}$. If C_A has a codeword of weight 1, then we should have $i^a = 0 \pmod p$ for some $1 \leq i \leq n$, showing that $p \mid i$, a contradiction. Hence, the statement holds for $d = 1$.

Now, suppose that the statement is true for d and assume that $A = \{a, a+1, \ldots, a+d\}$ is a $(d+1)$-successive set. Since $C_A \subseteq C_{A\setminus\{a+d\}}$, by hypothesis induction, there is no codeword $c \in C_A$ with $wt(c) \leq d$. Now, assume that there exists $c \in C_A$ with exactly $d+1$ nonzero coordinates $c_{i_1}, c_{i_2}, ..., c_{i_{d+1}}$. This means that there is a nonzero solution for the system of linear equations

$$\sum_{j=1}^{d+1} x_j {i_j}^z = 0 \qquad (z \in A),$$

over the field $\mathbb{Z}_p$. The cofficients matrix of the system is $D = ({i_j}^z)$, $j = 1, \ldots, d+1$, $z \in A$. Let us compute the determinant of D.

$$\begin{vmatrix} {i_1}^a & {i_2}^a & \ldots & {i_{d+1}}^a \\ {i_1}^{a+1} & {i_2}^{a+1} & \ldots & {i_{d+1}}^{a+1} \\ \vdots & \vdots & & \vdots \\ {i_1}^d & {i_2}^d & \ldots & {i_{d+1}}^d \end{vmatrix} =$$

$$i_1{}^a i_2{}^a \ldots i_{d+1}{}^a \begin{vmatrix} 1 & 1 & \ldots & 1 \\ i_1 & i_2 & \ldots & i_{d+1} \\ \vdots & \vdots & & \vdots \\ i_1{}^d & i_2{}^d & \ldots & i_{d+1}{}^d \end{vmatrix} =$$

$$i_1^a i_2^a \ldots i_{d+1}^a \prod_{1 \le r < s \le d+1} (i_s - i_r).$$

Now, it is clear that $\det(D) \neq 0 \pmod p$. Thus, the system of linear equations has unique zero solution, a contradiction. This completes the proof. □

Corollary 4.3. *Let $A \subseteq \mathfrak{n}$ contains a t-successive subset. Then $d(C_A) \geq t + 1$.*

5. Two-dimensional $\mathfrak{V}$-codes

In this section, we generalize the process described for constructing $\mathfrak{V}$-codes. As before, $p > 3$ is a prime number, $n = p - 1$ and $\mathfrak{n} = \{1, 2, \ldots, n\}$. Throughout this section, $\mathrm{Mat}_{r,s}(\mathbb{Z}_p)$ denotes the set of all $(r \times s)$-matrices over $\mathbb{Z}_p$. In the case of $r = s$, we simply use the notation $\mathrm{Mat}_r(\mathbb{Z}_p)$.

Definition 5.1. Let $\mathfrak{U} \subseteq \mathfrak{n} \times \mathfrak{n}$ be a non-empty set. we define the 2-dimensional $\mathfrak{V}$-code $C_{\mathfrak{U}}$ to be the set of all matrices $X = (x_{ij}) \in \mathrm{Mat}_n(\mathbb{Z}_p)$ whose $\sum_{i,j} x_{ij} i^a j^b = 0$ for all $(a, b) \in \mathfrak{U}$.

Note that, by definition, for any subset $\mathfrak{U} \subseteq \mathfrak{n} \times \mathfrak{n}$, we obtain a code whose elements are matrices, that can be viewed as vectors of length n^2, by reading them column by column.

A simple way of describing the 2-dimensional $\mathfrak{V}$-code $C_{\mathfrak{U}}$ is as follows. Let $\mathfrak{H}(\mathfrak{U})$ denote the matrix whose rows and columns are labeled by the pairs $(a, b) \in \mathfrak{U}$ and $(i, j) \in \mathfrak{n} \times \mathfrak{n}$ respectively and $\mathfrak{H}(\mathfrak{U})_{(a,b),(i,j)} = i^a j^b$. Then the code $C_{\mathfrak{U}}$ is just the set of all vectors $X \in (\mathbb{Z}_p)^{n^2}$ in which $\mathfrak{H}(\mathfrak{U})X^T = 0$.

For $\mathfrak{U} \subseteq \mathfrak{n} \times \mathfrak{n}$, let

$$\pi_1(\mathfrak{U}) = \{\alpha \in \mathfrak{n} \mid \exists \beta \in \mathfrak{n},\ (\alpha, \beta) \in \mathfrak{U}\},$$
$$\pi_2(\mathfrak{U}) = \{\beta \in \mathfrak{n} \mid \exists \alpha \in \mathfrak{n},\ (\alpha, \beta) \in \mathfrak{U}\}.$$

For any $\alpha \in \pi_1(\mathfrak{U})$, let $\psi(\alpha) = \{\beta \in \pi_2(\mathfrak{U}) \mid (\alpha, \beta) \in \mathfrak{U}\}$ and define the $(|\pi_1(\mathfrak{U})| \times n)$-matrix A_α to be the matrix whose rows and columns are labeled by the sets $\pi_1(\mathfrak{U})$ and $\mathfrak{n}$ respectively, and $(A_\alpha)_{ij} = \delta_{i\alpha} j^\alpha$, where δ is the Kronecker delta function. Beyond, define the $(|\pi_2(\mathfrak{U})| \times n)$-matrix B_α to be the matrix whose rows and columns are indexed

by the sets $\pi_2(\mathfrak{U})$ and $\mathfrak{n}$ respectively, and $(B_\alpha)_{ij} = \chi_{\psi(\alpha)}(i)j^i$, where $\chi_{\psi(\alpha)}(i)$ is 1 if $i \in \psi(\alpha)$ and is zero elsewhere.

Now, consider the linear transformation

$$T_\alpha : \mathrm{Mat}_n(\mathbb{Z}_p) \to \mathrm{Mat}_{|\pi_1(\mathfrak{U})|,|\pi_2(\mathfrak{U})|}(\mathbb{Z}_p)$$

defined by $T_\alpha(X) = A_\alpha X B_\alpha^t$, where B_α^t denotes the transpose of the matrix B_α. Then, we will have

$$\begin{aligned} T_\alpha(X)_{ij} &= \sum_{k=1}^{n} (A_\alpha X)_{ik}(B_\alpha^t)_{kj} \\ &= \sum_{k=1}^{n} (\sum_{l=1}^{n} (A_\alpha)_{il} X_{lk})(B_\alpha)_{jk} \\ &= \sum_{k} \sum_{l} \delta_{i\alpha} l^\alpha X_{lk} \chi_{\psi(\alpha)}(j) k^j \\ &= \delta_{i\alpha} \chi_{\psi(\alpha)}(j) \sum_{k,l} X_{lk} l^\alpha k^j, \end{aligned}$$

for all $i \in \pi_1(\mathfrak{U})$, $j \in \pi_2(\mathfrak{U})$ and $X \in \mathrm{Mat}_n(\mathbb{Z}_p)$.

Now, for all $X \in \mathrm{Mat}_n(\mathbb{Z}_p)$, let $T(X) = \sum_{\alpha \in \pi_1(\mathfrak{U})} T_\alpha(X)$. Then, for all $i \in \pi_1(\mathfrak{U})$ and $j \in \pi_2(\mathfrak{U})$, we have

$$\begin{aligned} T(X)_{ij} &= \sum_{\alpha \in \pi_1(\mathfrak{U})} \delta_{i\alpha} \chi_{\psi(\alpha)}(j) (\sum_{k,l} X_{lk} l^\alpha k^j) \\ &= \chi_{\psi(\alpha)}(j) \sum_{k,l} X_{lk} l^i k^j \\ &= \begin{cases} 0 & (i,j) \notin \mathfrak{U} \\ \sum_{k,l} X_{lk} l^i k^j & (i,j) \in \mathfrak{U}. \end{cases} \end{aligned}$$

This implies the following lemma.

Lemma 5.2. *For $\mathfrak{U} \subseteq \mathfrak{n} \times \mathfrak{n}$, $X \in C_\mathfrak{U}$ iff $T(X) = 0$.*

Proof. Just note that $T(X) = 0$ iff for all $(i,j) \in \mathfrak{U}$, $\sum_{k,l} X_{lk} l^i k^j = 0$ iff $X \in C_\mathfrak{U}$. □

Theorem 5.3. *Let $\mathfrak{U} \subseteq \mathfrak{n} \times \mathfrak{n}$. Then*

$$n^2 - \sum_{\alpha \in \pi_1(\mathfrak{U})} |\psi(\alpha)| \leq \dim(C_\mathfrak{U}) \leq n^2 - |\pi_1(\mathfrak{U})||\pi_2(\mathfrak{U})|.$$

Proof. It's easy to see that $\mathrm{rank}(T_\alpha) = \mathrm{rank}(A_\alpha)\mathrm{rank}(B_\alpha) = |\psi(\alpha)|$. Since $T = \sum_{\alpha \in \pi_1(\mathfrak{U})} T_\alpha$, $\mathrm{rank}(T) \leq \sum_{\alpha \in \pi_1(\mathfrak{U})} \mathrm{rank}(T_\alpha) = \sum_{\alpha \in \pi_1(\mathfrak{U})} |\psi(\alpha)|$.

Hence,

$$\dim(C_{\mathfrak{U}}) = n^2 - \operatorname{rank}(T) \geq n^2 - \sum_{\alpha \in \pi_1(\mathfrak{U})} |\psi(\alpha)|.$$

On the other hand, $C_{\mathfrak{U}} \subseteq C_{\pi_1(\mathfrak{U}) \times \pi_2(\mathfrak{U})}$. Hence,

$$\dim C_{\mathfrak{U}}) \leq \dim(C_{\pi_1(\mathfrak{U}) \times \pi_2(\mathfrak{U})}).$$

Let $\mathfrak{C} \in \operatorname{Mat}_{|\pi_1(\mathfrak{U})| \times n}(\mathbb{Z}_p)$ and $\mathfrak{D} \in \operatorname{Mat}_{n \times |\pi_2(\mathfrak{U})|}(\mathbb{Z}_p)$ denote the matrices $(i^a)_{a,n}$ and $(j^b)_{b,j}$, $a \in \pi_1(\mathfrak{U})$, $b \in \pi_2(\mathfrak{U})$ and $1 \leq i, j \leq n$, respectively. As mentioned before, It is easy to see that the rank of the linear transform $S : \operatorname{Mat}_n(\mathbb{Z}_p) \to \operatorname{Mat}_{|\pi_1(\mathfrak{U})| \times |\pi_2(\mathfrak{U})|}(\mathbb{Z}_p)$, defined by $S(X) = \mathfrak{C}X\mathfrak{D}$ is equal to $\operatorname{rank}(\mathfrak{C})\operatorname{rank}(\mathfrak{D})$. This shows that the dimension of the kernel of S is $n^2 - \operatorname{rank}(\mathfrak{C})\operatorname{rank}(\mathfrak{D}) = n^2 - |\pi_1(\mathfrak{U})||\pi_2(\mathfrak{U})|$. Thus, the code $C_{\pi_1(\mathfrak{U}) \times \pi_2(\mathfrak{U})}$ has dimension $n^2 - |\pi_1(\mathfrak{U})||\pi_2(\mathfrak{U})|$. This implies that $\dim(C_{\mathfrak{U}}) \leq n^2 - |\pi_1(\mathfrak{U})||\pi_2(\mathfrak{U})|$, as claimed. □

Theorem 5.4. *For $\mathfrak{U} \subseteq \mathfrak{n} \times \mathfrak{n}$, we have*

$$\min\{d(C_{\pi_1(\mathfrak{U})}), d(C_{\pi_2(\mathfrak{U})})\} \leq d(C_{\mathfrak{U}}) \leq (\sum_{\alpha \in \pi_1(\mathfrak{U})} |\psi(\alpha)|) + 1.$$

Proof. By singleton bound, and thanks to theorem 5.3, we have $d(C) \leq (\sum_{\alpha \in \pi_1(\mathfrak{U})} |\psi(\alpha)|) + 1$.

Now, let $0 \neq X \in C_{\mathfrak{U}}$. Then, $\sum_{i,j} X_{ij} i^\alpha j^\beta = 0$ for all $(\alpha, \beta) \in \mathfrak{U}$. This means that, for $\alpha \in \pi_1(\mathfrak{U})$, $\sum_j (\sum_i i^\alpha x_{ij}) j^\beta = 0$ for all $\beta \in \psi(\alpha)$. Therefore, for each $\alpha \in \pi_1(\mathfrak{U})$, the vectote $w_\alpha = (\sum_i i^\alpha X_{i1}, \ldots, \sum_i i^\alpha X_{in})$ lies in the $\mathfrak{v}$-code $C_{\psi(\alpha)}$. Now, there are 2 cases.

Case 1. $w_\alpha = 0$ for all $\alpha \in \pi_1(\mathfrak{U})$. In this case, for any $1 \leq j \leq n$, the vector $v_j = (X_{1j}, \ldots, X_{nj}) \in C_{\pi_1(\mathfrak{U})}$. Since $0 \neq X$, there exists $1 \leq j \leq n$ such that $v_j \neq 0$. Thus, $\operatorname{wt}(v_j) \geq d(C_{\pi_1(\mathfrak{U})})$ which implies $wt(X) \geq d(C_{\pi_1(\mathfrak{U})})$.

Case 2. There exists $\alpha \in \pi_1(\mathfrak{U})$ such that $w_\alpha \neq 0$. Since $w_\alpha \in C_{\psi(\alpha)}$, $\operatorname{wt}(w_\alpha) \geq d(C_{\psi(\alpha)}) := d_\alpha$. This means that there are $1 \leq j_1, \ldots, j_{d_\alpha} \leq n$ such that $\sum_i i^\alpha X_{ij_r} \neq 0$, $r = 1, \ldots, d_\alpha$, which implies $\operatorname{wt}(X) \geq d_\alpha \geq d(C_{\pi_2(\mathfrak{U})})$.

Thus, the cases discusses above show that

$$d(C_{\mathfrak{U}}) \geq \min\{d(C_{\pi_1(\mathfrak{U})}), d(C_{\pi_2(\mathfrak{U})})\},$$

as desired. □

References

1. T. P. Berger and A. Ourivski, Construction of new MDS codes from Gabidulin codes, In *Proceedings of ACCT*, Kranevo, Bulgaria, (2009), 40–47.

2. M. Braun, Construction of linear codes with large minimum distance, *IEEE Trans. Inform. Theory*, **50**(8) (2004), 1687–1691.
3. C. Carlet, C. Ding and J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, *IEEE Trans. Inform. Theory*, **51**(6) (2005), 2089–2102.
4. C. Carlet, S. Mesnager, C. Tang and Y. Qi, Euclidean and Hermitian LCD MDS codes, *Des. Codes Cryptogr.*, **86**(11) (2018), 2605–2618.
5. B. Chen and H. Liu, New constructions of MDS codes with complementary duals, *IEEE Trans. Inform. Theory*, **64**(8) (2018), 5776–5782.
6. De Boer and A. Mario, Almost MDS codes, *Des. Codes Cryptogr.*, **9**(2) (1996), 143–155.
7. C. Ding, A construction of binary linear codes from Boolean functions, *Discrete Math.*, **339**(9) (2016), 2288–2303.
8. S. Dodunekov and I. Landgev, On near MDS codes, *J. Geom.*, **54**(1-2) (1995), 30–43.
9. S. T. Dougherty, J. L. Kim and H. Kulosman, MDS codes over finite principal ideal rings, *Des. Codes Cryptogr.*, **50**(1) (2009), 77–92.
10. M. El Oued and P. Sol , MDS convolutional codes over a finite ring, *IEEE Trans. Inform. Theory*, **59**(11) (2013), 7305–7313.
11. J. Feigenbaum, The use of coding theory in computational complexity, *Different Aspects of Coding Theory*, American Mathematical Soc (1995), 207–233.
12. K. Guenda and T. A. Gulliver, MDS and self-dual codes over rings, *Finite Fields Appl.*, **18**(6) (2012), 1061–1075.
13. L. F. Jin, Construction of MDS codes with complementary duals, *IEEE Trans. Inform. Theory*, **63**(5) (2017), 2843–2847.
14. L. F. Jin and C. P. Xing, New MDS self-dual codes from generalized Reed-Solomon codes, *IEEE Trans. Inform. Theory*, **63**(3) (2017), 1434–1438.
15. J. L. Kim and Y. Lee, Construction of MDS self-dual codes over Galois rings, *Des. Codes Cryptogr.*, **45**(2) (2007), 247–258.
16. J. Lacan and J. Fimes, Systematic MDS Erasure codes based on Vandermonde matrices, *IEEE Trans. Commun. Lett.*, **8**(9) (2004), 570–572.
17. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, Elsevier, 1977.
18. R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, *DSN Progress Report*, **114** (1978), 42–44.
19. R. Overbeck and N. Sendrier, Code-based cryptography, In Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, Post-Quantum Cryptography, Springer Berlin Heidelberg, 2009.
20. K. Shiromoto, Note on MDS codes over the integers modulo p^m, *Hokkaido Math. J.*, **29**(1) (2000), 149–157.
21. Y. Wu, A construction of systematic MDS codes with minimum repair bandwidth, *IEEE Trans. Inform. Theory*, **57**(6) (2011), 3738–3741.
22. A. A. Zain, Rajan and B. Sundar, Algebraic characterization of MDS group codes over cyclic groups, *IEEE Trans. Inform. Theory*, **41**(6) (1995), 2052–2056.
23. A. A. Zain, Rajan and B. Sundar, Quasideterminant characterization of MDS group codes over abelian groups, *Des. Codes Cryptogr.*, **13** (1998), 313–330.

Asiyeh Rafieepour
Department of Mathematical Sciences, University of Kashan, P.O. Box 87317-53153, Kashan, Iran.
Email: a.rafieepour@gmail.com

Majid Mazrooei
Department of Mathematical Sciences, University of Kashan, P.O. Box 87317-53153, Kashan, Iran.
Email: m.mazrooei@kashanu.ac.ir