Available online at http://scik.org
Commun. Math. Biol. Neurosci. 2025, 2025:68
https://doi.org/10.28919/cmbn/9267
ISSN: 2052-2541

REVERSIBLE (BISYMMETRIC) SELF-DUAL CODES OVER FINITE FIELDS WITH CHARACTERISTIC TWO AND THEIR APPLICATIONS TO DNA CODES

VIRA HARI KRISNAWATI, ABDUL ROUF ALGHOFARI, ARDI NUR HIDAYAT*

Department of Mathematics, Faculty of Mathematics and Natural Sciences,
University of Brawijaya, Malang 65145, Indonesia

Abstract. Some recent studies reveal the development of reversible (bisymmetric) self-dual codes over fields of order 2 and 4. In this paper, we give new methods of constructing reversible (bisymmetric) self-dual codes over finite fields with characteristic two. This approach is motivated by the well-known reversible (bisymmetric) self-dual codes over finite fields of order two. We first investigated some properties of a reversible (bisymmetric) self-dual code over finite fields with characteristic two. Next, we developed a method to construct a new reversible (bisymmetric) self-dual code over finite fields with characteristic two. Additionally, we found an optimal reversible (bisymmetric) self-dual code over finite fields with characteristic two, and this method is applied to construct DNA codes.

Keywords: linear code; reversible self-dual code; bisymmetric self-dual code; DNA code.
2020 AMS Subject Classification: 94B05, 94B60, 15B99, 92D20.

1. INTRODUCTION

Coding theory was first introduced by Shannon in 1948 [1]. The concept of error-correcting codes in coding theory is explored using linear codes. Error-correcting codes have a close

*Corresponding author
E-mail address: ardinurhidayat@student.ub.ac.id
Received March 28, 2025

relationship with cryptography [2]. One type of linear code in error-correcting codes is the self-dual code. Golay first introduced the self-dual code in 1949 [3]. Some researchers have utilized this code in the field of cryptography, as seen in [4, 5].

Conceptually, self-dual codes have been developed by some researchers using algebraic properties of finite fields. In 1970, Gleason discussed the properties of codes over a field of order 2 and 3 [6]. Pless proposed a generalization of the extended Golay code over a field of order 3 in 1972 [7]. In 1981, Leon classified self-dual codes of length 24 over a field of order 3 [8]. In 1987, Pless discussed the properties of self-dual codes over a field of order 7 [9]. Dougherty investigated self-dual codes over a field of order 2 associated with finite projective planes [10] in 1998. Next, in 2003, Gaborit studied self-dual codes over a field of order 4, 5, 7, and 9 [11]. In 2009, Kim discussed and constructed self-dual codes over a field of order $q \equiv 3 \mod 4$ [12]. In 2018, Shi investigated orthogonal matrices as a basis for algorithms and methods for developing self-dual codes over arbitrary finite fields [13].

In 1964, Massey introduced the concept of reversible codes [14]. In error-correcting codes, reversible codes facilitate error correction by enabling lossless information recovery [15]. In 1970, Tzeng explored certain classes of reversible codes and investigated their minimum distance. These codes have shown significant potential for applications in data storage and retrieval systems, as they provide enhanced reliability by correcting up to two errors, which is crucial for maintaining data integrity in high-density storage [16]. In 1986, Muttoo discussed reversible codes over fields of order q and developed these codes. These codes were structured with information symbols, providing a mechanism for efficient error detection and correction [17]. In 1995, Takishima demonstrated that reversible codes offer strong error correction capabilities and enable efficient data transmission [18]. Bhasin, in 2013, applied reversible codes as a cryptographic tool to detect hardware Trojan horse virus attacks [19]. Later, in 2016, Jin discussed an optimal reversible code construction. In error-correcting, an optimal code is a code that meets an upper bound, ensuring maximum efficiency in detecting and correcting errors [20].

In biology, reversible and self-dual codes have been applied to construct DNA codes [21, 22, 23, 24]. DNA codes are sequences over the alphabet $\{\mathbf{A}, \mathbf{T}, \mathbf{G}, \mathbf{C}\}$, representing the four nucleotides: Adenine (**A**), Thymine (**T**), Guanine (**G**), and Cytosine (**C**). These codes must satisfy specific constraints such as Watson-Crick complementarity, where A pairs with T and G pairs with C, ensuring stability and error correction in DNA-based data storage and molecular computing. Reversible and self-dual codes provide a robust framework for constructing DNA codes by ensuring that each codeword's reverse complement is also a codeword, enhancing error correction and preserving genetic information integrity.

Moreover, various researchers developed construction studies that combine the concept of reversible and self-dual code. The concept was introduced by Kim in 2020 [25]. The article explores how reversible self-dual codes are connected to persymmetric matrices. In 2021, Kim showed that the properties of the generator matrix of reversible self-dual codes over a field of order two were also applied to codes over a field of order four [26]. The research resulted in an optimal code. Then, in 2024, some researchers developed constructions of reversible self-dual codes over arbitrary finite fields using alternative methods unrelated to persymmetric matrices [27, 28]. The concept of a persymmetric matrix is generally employed for building reversible self-dual codes over fields of order 2 and 4. It can be observed that the construction of reversible self-dual code over a field of order 2 and 4 involves fields with characteristic two. Therefore, in this paper, we develop reversible self-dual codes over finite fields with characteristic two in general. Meanwhile, in 2024, Kim developed a code construction over a field of order 2, associated with bisymmetric matrices, called bisymmetric self-dual code [29]. Furthermore, building on advancements in the code, we also construct a bisymmetric self-dual code over arbitrary fields with characteristic two.

Based on concepts analogous to those derived from relevant articles, the research methodology is outlined below. First, we examine the properties of reversible (bisymmetric) self-dual codes over a field with characteristic two. After that, we analyze the construction of new reversible (bisymmetric) self-dual codes over finite fields with characteristic two using known reversible (bisymmetric) self-dual codes. Finally, an updated generator matrix of the reversible (bisymmetric) self-dual code over a field with characteristic two will be constructed. There are four sections in this article. In the second section, we provide some literature reviews. We present some properties of a reversible (bisymmetric) self-dual code over a field with characteristic two. We also construct a new reversible self-dual code over a field with characteristic two in the third section. Furthermore, we perform computations of a bisymmetric self-dual code. Then, we compare their parameters with the data provided in Grassl [30]. Additionally, these codes are applied to construct DNA codes. Later, in the final section, we give the conclusion of this article.

2. Preliminaries

Let $q \geq 2$ and n be a natural number. We denote a finite field of order q by F_q. A finite field F_q has the characteristic n if $nx = 0$ holds for every $x \in F_q$. A code $\mathscr{C}$ of length n over a finite field F_q is called a linear code if $\mathscr{C}$ is a subspace of F_q^n. Each element of $\mathscr{C}$ is known as a codeword. The dual code of $\mathscr{C}$, denoted as $\mathscr{C}^{\perp}$, is defined as:

$$\mathscr{C}^{\perp} = \left\{ \mathbf{u} \in {F_q}^n | \mathbf{u} \cdot \mathbf{z} = 0 \text{ for all } \mathbf{z} \in \mathscr{C} \right\}.$$

We define $\mathscr{C}$ as a self-dual code if $\mathscr{C}^{\perp}$ is identical to $\mathscr{C}$. The Hamming weight of a codeword $\mathbf{a}$, represented as $wt(\mathbf{a})$, is defined as the count of non-zero symbols in the codeword. The Hamming distance between two codewords $\mathbf{a}$ and $\mathbf{b}$ is defined as $wt(\mathbf{a} - \mathbf{b})$. The minimum distance of a code, represented by $d(\mathscr{C})$, is defined as $d(\mathscr{C}) = \min \{ d(\mathbf{a}, \mathbf{b}) \, | \mathbf{a}, \mathbf{b} \in \mathscr{C}, \, \mathbf{a} \neq \mathbf{b} \}$. For a linear code $\mathscr{C}$ over F_q with length n, dimension k, and minimum distance d, the code is referred to as an $[n,k,d]_q$ code. The $[n,k,d]_q$ code with the minimum distance $d = n - k + 1$ is called a maximum distance separable (MDS) code. An MDS code is optimal because it meets the singleton bound [31].

A matrix G is called a generator matrix for the linear code $\mathscr{C}$ if its rows form a basis for $\mathscr{C}$. Linear code $\mathscr{C}$ of length n and dimension k with generator matrix G which can be stated as

$$\mathscr{C} = \left\{ \mathbf{z}G | \mathbf{z} \in {F_q}^k \right\}.$$

If $\mathscr{C}$ is self-dual, then $GG^T = O$. The standard generator matrix of $[n,k,d]_q$ code is defined by $G = (I_k|X)$, with G as a matrix of size $k \times n$ and I_k as the identity matrix of size $k \times k$. $G = (I_k|X)$ is generator standard of self-dual code if $XX^T = -I_k$ [13]. Next, some definitions related to reversible code are provided.

Definition 2.1. [17] *A linear code $\mathscr{C}$ of length n digit is said to be a reversible code if for all*

$$\mathbf{c} = (c_1, c_2, \cdots, c_n) \in \mathscr{C}$$

there is $\mathbf{c}^r = (c_n, c_{n-1}, \cdots, c_1) \in \mathscr{C}$.

Definition 2.2. [25] *A reversible code* $\mathscr{C}$ *is said to be a reversible self-dual code if* $\mathscr{C}$ *is a self-dual code.*

Next, we recall some definitions of special matrices needed to generate reversible self-dual codes over a field with characteristic two. Let $K = (k_{i,j})_{m\times n}$. Then, the transpose of matrix K is $K^T = (k_{j,i})_{n\times m}$, and the flip transpose of matrix K is $K^F = (k_{n-j+1,m-i+1})_{n\times m}$, and $K^r = (k_{m,n-j+1})_{m\times n}$ is the column reversed matrix of K. The matrix K is called persymmetric if $K = K^F$. We say K is a bisymmetric matrix if $K = K^F = K^T$. Therefore, if K is bisymmetric, then K is persymmetric and symmetric.

Let X, Y be a square matrix of size $n\times n$ and I be the identity matrix of size $n\times n$. The following properties of the flip transpose of the matrix are straightforward:

(1) $I^r = (I^r)^T = (I^r)^F$,
(2) $(I^r)^2 = I$,
(3) $X^r = XI^r$,
(4) $X^F = I^r X^T I^r$,
(5) $(X^F)^F = X$,
(6) $(X^F)^T = (X^T)^F$,
(7) $(X+Y)^F = X^F + Y^F$,
(8) $(XY)^F = Y^F X^F$.

Moreover, a self-dual code related to bisymmetric matrices is defined as follows.

Definition 2.3. [29] *A self-dual code* $\mathscr{C}$ *with the standard generator matrix* $G = (I_n|X)$ *is called a bisymmetric self-dual code if the matrix* X *is bisymmetric.*

3. Main Result

Here, we begin by investigating the properties of a reversible self-dual code over a finite field with characteristic two. We denote a finite field with characteristic two by $\mathscr{F}$, a reversible self-dual code by RSD code, and a bisymmetric self-dual code by BSD code.

3.1. Some Properties of Reversible (Bisymmetric) Self-dual Codes over $\mathscr{F}$.

Lemma 3.1. *If* $\mathbf{z} \in \mathscr{F}^{2n}$, *then*

$$\mathbf{z}^F \mathbf{z} = \mathbf{z}^T (\mathbf{z}^F)^T = 0.$$

Proof. $\mathbf{z}^F \mathbf{z} = \mathbf{z}^T (\mathbf{z}^F)^T = \sum_{i=1}^{2n} z_i z_{2n-i+1} = 2\sum_{i=1}^{n} z_i z_{2n-i+1} = 0.$ □

Lemma 3.2. *For a square matrix X over $\mathscr{F}$, the following conditions hold.*

(1) X is persymmetric if and only if X^r is symmetric.

(2) X is bisymmetric if and only if X^r is bisymmetric.

Proof. (1) Suppose X is persymmetric. Then $X = X^F$. By using some properties of the flip transpose of matrix X, we obtain,

$$X = X^F \Longleftrightarrow XI_n = I_n^r X^T I_n^r \Longleftrightarrow XI_n^r = I_n^r X^T \Longleftrightarrow X^r = (X^r)^T.$$

Therefore, X^r is symmetric. In a similar way, the opposite direction can be proven.

(2) Suppose X is bisymmetric. Thus, we have X, which is persymmetric. Based on (1) and some properties of the flip transpose of matrix X, we get,

$XI_n^r = I_n^r X^T \Longleftrightarrow I_n^r X I_n^r = I_n^r I_n^r X^T \Longleftrightarrow I_n^r X I_n^r I_n^r = I_n^r I_n^r X^T I_n^r \Longleftrightarrow X^r = (X^r)^F.$

Thus, X^r is persymmetric. Because $X^r = (X^r)^T = (X^r)^F$, X^r is bisymmetric. Using the same method, the reverse can be proven.

□

Lemma 3.3. *For a self-dual code $\mathscr{C}$ over $\mathscr{F}$ with the generator matrix $G = (I_n \,|\, X)$, $\mathscr{C}$ is reversible if and only if it meets at least one of the following conditions:*

(1) X is persymmetric.

(2) X^r is symmetric.

Proof. Since $\mathscr{C}$ is reversible, it implies that

$$\begin{aligned} & G(G^r)^T = O, \\ \Longrightarrow \quad & \left(I_n \,\middle|\, X\right)\left(X^r \,\middle|\, I_n^r\right)^T = O, \\ \Longrightarrow \quad & \left(I_n^r X^T + X I_n^r\right) = O, \end{aligned}$$

The expression $I_n^r X^T + X I_n^r = O$ holds if $I_n^r X^T = X I_n^r$, implying that $(X^r)^T = X^r$. Thus, condition (2) is satisfied. Then, based on condition 1 it is also satisfied by Lemma 3.2. The reverse case can be shown similarly. $\square$

Example 3.1. *Given an RSD code C over* $F_4 = \{u + va | a^2 = a + 1, u, v \in F_2\}$. *The generator matrix of C is as follows.*

$$(I_2|X) = \left(\begin{array}{cc|cc} 1 & 0 & a+1 & a \\ 0 & 1 & a & a+1 \end{array}\right),$$

where $XX^T = I_2$. *Here, X is persymmetric* $X = X^F$. *Moreover, the matrix* $X^r = \begin{pmatrix} a & a+1 \\ a+1 & a \end{pmatrix}$ *is symmetric.*

Based on Definition 2.3 and Lemma 3.3, the BSD code is closely related to RSD code, as in the corollary below.

Corollary 3.1. *If* $\mathscr{C}$ *is a bisymmetric self-dual code over* $\mathscr{F}$, *then* $\mathscr{C}$ *is a reversible self-dual.*

The existence of an RSD code over $\mathscr{F}$ is established in the following proposition.

Proposition 3.1. *For every code of even length, there exists an RSD code over* $\mathscr{F}$.

Proof. Consider that, $(I_n|I_n^r)$ generates a trivial RSD code over $\mathscr{F}$ of length $2n$. This holds Lemma 3.3 because $(I_n^r)^F = I_n^r$ and $(I_n^r)(I_n^r)^T = I_n$. $\square$

Next, an RSD code can be constructed by extending the previously known RSD code based on the properties below.

3.2. Construction of a Reversible (Bisymmetric) Self-dual Code over $\mathscr{F}$.

Theorem 3.1. *Suppose that* $G_1 = (I_n|M)$ *is a generator matrix of an RSD code* $\mathscr{C}_1$ *over* $\mathscr{F}$ *of length* $2n$ *and* $\mathbf{z}$ *is an eigenvector of* M^r *with eigenvalue 1. The following matrix* $G_2 = (I_{n+1}|N)$, *where*

$$N = \left(\begin{array}{c|c} \mathbf{z} & M+L \\ \hline k & \mathbf{z}^F \end{array}\right)$$

is a generator matrix of a RSD code $\mathscr{C}_2$ *of length* $2n+2$ *digits, the vector* $\mathbf{z}$*,* k *and the matrix* L *are given under the following case.*

(1) *If* $k=0$*,* $\mathbf{z}^T\mathbf{z}=1$ *and* $L=\mathbf{z}\mathbf{z}^F$*.*

(2) *If* $k\neq 0, k^2=1+\mathbf{z}^T\mathbf{z}$*,* $\mathbf{z}^T\mathbf{z}\neq 0$*, and* $L=(k+1)^{-1}\mathbf{z}\mathbf{z}^F$*.*

Proof. We prove that, $G_2=(I_{n+1}|N)$ is a generator matrix of RSD code $\mathscr{C}_2$. First, we have to show that $\mathscr{C}_2$ is self-dual code. Thus,

$$
\begin{aligned}
N(N)^T &= \left(\begin{array}{c|c} \mathbf{z} & M+L \\ \hline k & \mathbf{z}^F \end{array}\right)\left(\begin{array}{c|c} \mathbf{z}^T & k \\ \hline M^T+L^T & (\mathbf{z}^F)^T \end{array}\right) \\
&= \left(\begin{array}{c|c} \mathbf{z}\mathbf{z}^T+(M+L)(M^T+L^T) & k\mathbf{z}+(M+L)(\mathbf{z}^F)^T \\ \hline k\mathbf{z}^T+\mathbf{z}^F(M^T+L^T) & k^2+\mathbf{z}^F(\mathbf{z}^F)^T \end{array}\right) \\
&= I_{n+1}.
\end{aligned}
$$

Then, we need to verify that the following equations are true.

$$\mathbf{z}\mathbf{z}^T+(M+L)(M^T+L^T)=I_n, \tag{3.1}$$

$$k\mathbf{z}+(M+L)(\mathbf{z}^F)^T=O_{n\times 1}, \tag{3.2}$$

$$k\mathbf{z}^T+\mathbf{z}^F(M^T+L^T)=O_{1\times n}, \tag{3.3}$$

$$k^2+\mathbf{z}^F(\mathbf{z}^F)^T=1. \tag{3.4}$$

Based on the given assumptions, it follows that $MM^T=I_n$. Additionally, since $\mathbf{z}$ is an eigenvector of M^r with eigenvalue 1, it is clear that $\mathbf{z}=M^r\mathbf{z}$. By using some properties of the flip transpose of the matrix and direct computations, we obtain that

$$M(\mathbf{z}^F)^T=M(I_n^r\mathbf{z})=M^r\mathbf{z}=\mathbf{z} \tag{3.5}$$

consequently, we have

$$\mathbf{z}^F M^T=(M(\mathbf{z}^F)^T)^T=\mathbf{z}^T.$$

Next, we verify equations (3.1), (3.2), (3.3), and (3.4) for each case.

For case (i), $k=0$, $\mathbf{z}^T\mathbf{z}=1$ and $L=\mathbf{z}\mathbf{z}^F$. Thus, by equation (3.5), we get

$$ML^T = M(\mathbf{z}\mathbf{z}^F)^T = M(\mathbf{z}^F)^T)\mathbf{z}^T = \mathbf{z}\mathbf{z}^T, \tag{3.6}$$

$$LM^T = (ML)^T = \mathbf{z}\mathbf{z}^T, \tag{3.7}$$

$$LL^T = \mathbf{z}\mathbf{z}^F(\mathbf{z}\mathbf{z}^F)^T = \mathbf{z}(\mathbf{z}^T\mathbf{z})^F\mathbf{z}^T = \mathbf{z}\mathbf{z}^T, \tag{3.8}$$

$$L(\mathbf{z}^F)^T = \mathbf{z}\mathbf{z}^F(\mathbf{z}^F)^T = \mathbf{z}(\mathbf{z}^F(\mathbf{z}^F)^T) = \mathbf{z}, \tag{3.9}$$

$$\mathbf{z}^F L^T = (L(\mathbf{z}^F)^T)^T = \mathbf{z}^T. \tag{3.10}$$

By equation (3.6), (3.7), (3.8), (3.9), and (3.10), we have

$$\begin{aligned}
\mathbf{z}\mathbf{z}^T + (M+L)(M^T+L^T) =& \mathbf{z}\mathbf{z}^T + MM^T + LM^T + ML^T + LL^T \\
=& \mathbf{z}\mathbf{z}^T + I_n + \mathbf{z}\mathbf{z}^T + \mathbf{z}\mathbf{z}^T + \mathbf{z}\mathbf{z}^T \\
=& I_n, \\
k\mathbf{z} + (M+L)(\mathbf{z}^F)^T =& M(\mathbf{z}^F)^T + L(\mathbf{z}^F)^T = \mathbf{z} + \mathbf{z} = O_{n\times 1}, \\
k\mathbf{z}^T + \mathbf{z}^F(M^T+L^T) =& \mathbf{z}^F(M^T) + \mathbf{z}^F(L^T) = \mathbf{z}^T + \mathbf{z}^T = O_{1\times n}, \\
k^2 + \mathbf{z}^F(\mathbf{z}^F)^T =& 0 + (\mathbf{z}^T\mathbf{z})^F = 1.
\end{aligned}$$

Hence, equations (3.1), (3.2), (3.3), and (3.4) are true.

For case (ii), $k \neq 0, k^2 = 1 + \mathbf{z}^T\mathbf{z}$, $\mathbf{z}^T\mathbf{z} \neq 0$, *and* $L = (k+1)^{-1}\mathbf{z}\mathbf{z}^F$. Thus, by equation (3.5), we get

$$ML^T = M((k+1)^{-1}\mathbf{z}\mathbf{z}^F)^T = (k+1)^{-1}M(\mathbf{z}^F)^T)\mathbf{z}^T = (k+1)^{-1}\mathbf{z}\mathbf{z}^T, \tag{3.11}$$

$$LM^T = (ML)^T = (k+1)^{-1}\mathbf{z}\mathbf{z}^T, \tag{3.12}$$

$$LL^T = (k+1)^{-2}\mathbf{z}\mathbf{z}^F(\mathbf{z}\mathbf{z}^F)^T = (k+1)^{-2}\mathbf{z}(k+1)^2\mathbf{z}^T = \mathbf{z}\mathbf{z}^T, \tag{3.13}$$

$$L(\mathbf{z}^F)^T = (k+1)^{-1}\mathbf{z}\mathbf{z}^F(\mathbf{z}^F)^T = (k+1)^{-1}\mathbf{z}(\mathbf{z}^F(\mathbf{z}^F)^T) = (k+1)\mathbf{z}, \tag{3.14}$$

$$\mathbf{z}^F L^T = (L(\mathbf{z}^F)^T)^T = (k+1)\mathbf{z}^T. \tag{3.15}$$

By equation (3.11), (3.12), (3.13), (3.14), and (3.15) we have,

$$\mathbf{z}\mathbf{z}^T + (M+L)(M^T+L^T) = I_n,$$

$$\begin{aligned} k\mathbf{z}+(M+L)(\mathbf{z}^F)^T &= k\mathbf{z}+M(\mathbf{z}^F)^T+L(\mathbf{z}^F)^T = k\mathbf{z}+\mathbf{z}+(k+1)\mathbf{z} = O_{n\times 1}, \\ k\mathbf{z}^T+\mathbf{z}^F(M^T+L^T) &= k\mathbf{z}^T+\mathbf{z}^F(M^T)+\mathbf{z}^F(L^T) = k\mathbf{z}^T+\mathbf{z}^T+(k+1)\mathbf{z}^T = O_{1\times n}, \\ k^2+\mathbf{z}^F(\mathbf{z}^F)^T &= 1. \end{aligned}$$

According to two cases, equations (3.1), (3.2), (3.3), and (3.4) are true. Therefore, $\mathscr{C}_2$ is self-dual code. Based on Lemma 3.3 M is persymmetric, so we have to show that N is persymmetric or $N^F = N$.

$$\begin{aligned} (N)^F &= \left(\begin{array}{c|c} \mathbf{z} & M+L \\ \hline k & \mathbf{z}^F \end{array}\right)^F \\ &= \left(\begin{array}{c|c} (\mathbf{z}^F)^F & M^F+L^F \\ \hline k^F & \mathbf{z}^F \end{array}\right) \\ &= \left(\begin{array}{c|c} \mathbf{z} & M+L^F \\ \hline k & \mathbf{z}^F \end{array}\right). \end{aligned}$$

Thus, N is persymmetric if L is persymmetric. Note that for two cases, by definition of flip transpose $(\mathbf{z}\mathbf{z}^F)^F = (\mathbf{z}\mathbf{z}^F)^F$ and $((k+1)^{-1}\mathbf{z}\mathbf{z}^F)^F = (k+1)^{-1}(\mathbf{z}\mathbf{z}^F)^F$. Therefore, L is persymmetric, implying N is persymmetric. □

According to Theorem 3.1, the minimum distance of the code can be determined as shown in Proposition 3.2 below.

Proposition 3.2. *If* $G = (I_{n+1}|N)$, *where*

$$N = \left(\begin{array}{c|c} \mathbf{z} & M+L \\ \hline k & \mathbf{z}^F \end{array}\right)$$

is a generator matrix of an RSD code $\mathscr{C}$ *of length* $2n+2$ *digits over* $\mathscr{F}$, *then*

$$d(\mathscr{C}) = 1+\min\{wt(k)+wt(\mathbf{z}), \min\{wt(\mathbf{y}^{(i)}\},$$

where $\mathbf{y}^{(i)}$ *is the* i^{th}*-row vector of G, generated after eliminating the first* $n+1$ *digits for* $i = 1,2\cdots n$.

Proof. Note that for all $\mathbf{c} \in \mathscr{C}$ can be generated from $\mathbf{w} \in \mathscr{F}^{n+1}$. Therefore, we need to examine the following two cases.

(1) If the first n digit of $\mathbf{w}$ are zero and the last digit of $\mathbf{w}$ is non-zero, $\mathbf{w} = (\mathbf{0}|t)$. Then $\mathbf{c} \in \mathscr{C}$ is $\mathbf{c} = (\mathbf{0}|t|tk|t\mathbf{z}^F)$. Thus, we find that $wt(c) = 1 + wt(k) + wt(\mathbf{z}^F)$. Because $wt(\mathbf{z}^F) = wt(\mathbf{z})$, then $wt(\mathbf{c})= 1 + wt(k) + wt(\mathbf{z})$.

(2) If the i^{th}-digit of $\mathbf{w}$ is non-zero and other digit are zero with $i = 1, \cdots, n$. In this case, several conditions will be considered, as follows.

   (a) If the first digit of $\mathbf{w}$ is non-zero, $\mathbf{w} = (t|\mathbf{0})$. Then we get $\mathbf{c} \in \mathscr{C}$ is $\mathbf{c} = (t|\mathbf{0}|t\mathbf{z}|t(\mathbf{M}+\mathbf{L}))$. Then $wt(\mathbf{c}) = 1 + wt(\mathbf{y}^{(1)})$, where $\mathbf{y}^{(1)}$ is the first row vector of G is obtained by removing the first $n+1$ digits.

   (b) If the i^{th}-digit of $\mathbf{w}$ is non-zero with $i = 2, 3...., n$, $\mathbf{w} = (\mathbf{0}|t|\mathbf{0})$. Thus, we get $\mathbf{c} \in \mathscr{C}$ is $\mathbf{c} = (\mathbf{0}|t|t\mathbf{z}|t(\mathbf{M}+\mathbf{L})|\mathbf{0})$. Then $wt(\mathbf{c}) = 1 + wt(\mathbf{y}^{i)})$, where $\mathbf{y}^{(i)}$ is the i^{th}-row vector of G, generated after eliminating the first $n+1$ digits.

   Therefore, $\min wt(\mathbf{c}) = 1 + \min\{wt(\mathbf{y}^{(i)}\}$ with $i = 1, 2, \cdots, n$.

According to the 2 cases above, $d(\mathscr{C})$ = 1+min$\{wt(k) + wt(\mathbf{z}), \min\{wt(\mathbf{y}^{(i)})\}\}$. □

Example 3.2. *Given an RSD code $\mathscr{C}_1$ of length 4 over $F_4 = \{u + va | a^2 = a + 1, u, v \in F_2\}$. The generator matrix of $\mathscr{C}_1$ is*

$$G = (I_2|M) = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right).$$

To construct a new code $\mathscr{C}_2$ with a length of 6 digits as stated in Theorem 3.1, we can calculate the eigenvectors of the matrix M^r that satisfy the assumptions in Theorem 3.1. Therefore, the resulting eigenvector is as follows.

$$\mathbf{z} = \begin{pmatrix} a \\ a+1 \end{pmatrix}$$

Thus,

$$M + L = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & a+1 \\ a & 1 \end{pmatrix} = \begin{pmatrix} 0 & a+1 \\ a & 0 \end{pmatrix}.$$

Finally, if we choose $k = 0$ then the generator matrix of $\mathscr{C}_2$ is

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & a & 0 & a+1 \\ 0 & 1 & 0 & a+1 & a & 0 \\ 0 & 0 & 1 & 0 & a+1 & a \end{pmatrix}.$$

Moreover, if we encode $\mathscr{C}_2$ using the matrix G_2 and obtain codewords from $\mathscr{C}_2$, then by calculating its minimum distance, we find that $d(\mathscr{C}_2) = 3$. Let $\mathbf{y}^{(i)}$ be the vector of the i^{th} row of G_2 with i=1,2. Consider that, $wt(\mathbf{y}^{(1)} = wt(\mathbf{y}^{(2)}) = wt(\mathbf{z}) = 2$, and $d(\mathscr{C}_2) = 1 + \min\{wt(0) + wt(\mathbf{z}), \min\{wt(\mathbf{r}^i)\}\} = 3$. This shows that Proposition 3.2 is satisfied.

In the following proposition, we discuss the existence of an MDS code over $\mathscr{F}$ generated using a method in Theorem 3.1.

Proposition 3.3. *Let $G = (I_{n+1}|N)$, where*

$$N = \left(\begin{array}{c|c} \mathbf{z} & M+L \\ \hline k & \mathbf{z}^F \end{array}\right)$$

be a generator matrices of an RSD code $\mathscr{C}$ over $\mathscr{F}$. If $k \neq 0$ and $wt(\mathbf{z}) = \min\{wt(\mathbf{y}^i)\} = n$, with $\mathbf{y}^{(i)}$ is the i^{th}-row vector of G with $i = 1, 2, 3..., n$, then $\mathscr{C}$ is an MDS code.

We obtained the development of RSD codes in Theorem 3.1. Based on Corollary 3.1, the next theorem will address the construction of BSD codes.

Theorem 3.2. *Let $[I_{2n}|M]$ be a generator matrix of a BSD code of length $4n$ over $\mathscr{F}$. The matrix $G = (I_{2n+2}|N)$, where*

$$N = \left(\begin{array}{c|c|c} \alpha & \mathbf{z}^T & \beta \\ \hline \mathbf{z} & M+L & (\mathbf{z}^F)^T \\ \hline \beta & \mathbf{z}^F & \alpha \end{array}\right)$$

constructs a BSD code of length $4n+4$ over $\mathscr{F}$ for the matrix L, $\alpha, \beta \in \mathscr{F}$, and the column vector $\mathbf{z} \in \mathscr{F}^{2n}$ that satisfy one of the following cases.

(1) $\beta = \alpha + 1$, *$\mathbf{z}$ is an eigenvector of M^r, $L = O$, and* $\mathbf{z}^T = \mathbf{z}^F$.
(2) $\alpha = \beta = 1$, *$\mathbf{z}$ is an eigenvector of M^r, $L = \mathbf{z}\mathbf{z}^T + (\mathbf{z}^F)^T\mathbf{z}^F$, and* $\mathbf{z}^T\mathbf{z} = 1$.
(3) $\alpha = \beta = 0$, *$\mathbf{z}$ is an eigenvector of M, $L = \mathbf{z}\mathbf{z}^T + (\mathbf{z}^F)^T\mathbf{z}^F$, and* $\mathbf{z}^T\mathbf{z} = 1$.

Proof. According to the assumption, we have $MM^T = MM = I_{2n}$ and the matrix L is bisymmetric which satisfy all cases. Thus, it can be easily shown that N is bisymmetric. Thus, we need to verify that

$$NN = \left(\begin{array}{c|c|c} \alpha^2+\mathbf{z}^T\mathbf{z}+\beta^2 & \alpha\mathbf{z}^T+\mathbf{z}^T(M+L)+\beta\mathbf{z}^F & \mathbf{z}^T(\mathbf{z}^F)^T \\ \hline \alpha\mathbf{z}+(M+L)\mathbf{z}+\beta(\mathbf{z}^F)^T & \mathbf{z}\mathbf{z}^T+(M+L)^2+(\mathbf{z}^F)^T\mathbf{z}^F & \beta\mathbf{z}+(M+L)(\mathbf{z}^F)^T+\alpha(\mathbf{z}^F)^T \\ \hline \mathbf{z}^F\mathbf{z} & \beta\mathbf{z}^T+\mathbf{z}^F(M+L)+\alpha\mathbf{z}^F & \beta^2+\mathbf{z}^F(\mathbf{z}^F)^T+\alpha^2 \end{array}\right)$$
$$=I_{2n+2}.$$

First, we have to show that the following equations hold:

$$\alpha^2+\mathbf{z}^T\mathbf{z}+\beta^2 = 1, \tag{3.16}$$

$$\alpha\mathbf{z}^T+\mathbf{z}^T(M+L)+\beta\mathbf{z}^F = O_{1\times 2n}, \tag{3.17}$$

$$\mathbf{z}^T(\mathbf{z}^F)^T = 0, \tag{3.18}$$

$$\alpha\mathbf{z}+(M+L)\mathbf{z}+\beta(\mathbf{z}^F)^T = O_{2n\times 1}, \tag{3.19}$$

$$\mathbf{z}\mathbf{z}^T+(M+L)^2+(\mathbf{z}^F)^T\mathbf{z}^F = I_{2n}, \tag{3.20}$$

$$\beta\mathbf{z}+(M+L)(\mathbf{z}^F)^T+\alpha(\mathbf{z}^F)^T = O_{2n\times 1}, \tag{3.21}$$

$$\mathbf{z}^F\mathbf{z} = 0, \tag{3.22}$$

$$\beta\mathbf{z}^T+\mathbf{z}^F(M+L)+\alpha\mathbf{z}^F = O_{1\times 2n}, \tag{3.23}$$

$$\beta^2+\mathbf{z}^F(\mathbf{z}^F)^T+\alpha^2 = 1. \tag{3.24}$$

Based on Lemma 3.1, equations (3.18) and (3.22) are clearly satisfied. Next, we show that the other equations are satisfied for each case.

Case (i) Since $\mathbf{z}$ is an eigenvector of M^r, we have $M^r\mathbf{z} = \mathbf{z}, \Longleftrightarrow M(\mathbf{z}^F)^T = \mathbf{z} \Longleftrightarrow \mathbf{z}^T M = \mathbf{z}^F$. Since $\mathbf{z}^T = \mathbf{z}^F$, by Lemma 3.2 $\mathbf{z}^T\mathbf{z} = 0$. Therefore, we obtain

$$\alpha^2+\mathbf{z}^T\mathbf{z}+\beta^2 = \alpha^2+(\alpha+1)^2 = 1,$$

$$\alpha\mathbf{z}^T+\mathbf{z}^T(M+L)+\beta\mathbf{z}^F = \alpha\mathbf{z}^T+(\beta+1)\mathbf{z}^F = O_{1\times 2n},$$

$$\alpha\mathbf{z}+(M+L)\mathbf{z}+\beta(\mathbf{z}^F)^T = (\alpha\mathbf{z}^T+\mathbf{z}^T(M+L)+\beta\mathbf{z}^F)^T = O_{2n\times 1},$$

$$\mathbf{z}\mathbf{z}^T+(M+L)^2+(\mathbf{z}^F)^T\mathbf{z}^F = M^2 = I_{2n},$$

$$\beta \mathbf{z}+(M+L)(\mathbf{z}^F)^T+\alpha(\mathbf{z}^F)^T =(\alpha \mathbf{z}^T+\mathbf{z}^T(M+L)+\beta \mathbf{z}^F)^F = O_{2n\times 1},$$

$$\beta \mathbf{z}^T+\mathbf{z}^F(M+L)+\alpha \mathbf{z}^F =(\beta \mathbf{z}+(M+L)(\mathbf{z}^F)^T+\alpha(\mathbf{z}^F)^T)^T = O_{1\times 2n},$$

$$\beta^2+\mathbf{z}^F(\mathbf{z}^F)^T+\alpha^2 =(\alpha+1)^2+\alpha^2 = 1.$$

Hence, equations (3.16), (3.17), (3.18), (3.19), (3.20), (3.21), (3.22), (3.23), and (3.24) are satisfied. The other cases are verified similarly. □

The minimum distance of the constructed code is determined in the following proposition using Theorem 3.2.

Proposition 3.4. *If* $G = (I_{2n+2}|N)$, *where*

$$N = \left(\begin{array}{c|c|c} \alpha & \mathbf{z}^T & \beta \\ \hline \mathbf{z} & M+L & (\mathbf{z}^F)^T \\ \hline \beta & \mathbf{z}^F & \alpha \end{array}\right)$$

is a generator matrix of a BSD code $\mathscr{C}$ *of length* $4n+4$ *digits over* $\mathscr{F}$, *then* $d(\mathscr{C}) = 1+\min\{wt(\alpha)+wt(\beta)+wt(\mathbf{z}), \min\{wt(\mathbf{y}^{(i)}\}$ *where* $\mathbf{y}^{(i)}$ *is the* i^{th}*-row vector of G, obtained by removing the first* $2n+2$ *digits for* $i = 2,3\cdots 2n+1$.

Proof. The proof is similar to the proof of Proposition 3.2 □

Next, we show the subsistence of an MDS code for the BSD code over finite fields with characteristic two by employing the method outlined in the definition of an MDS code and Proposition 3.4.

Proposition 3.5. *Let* $G = (I_{2n+2}|N)$, *where*

$$N = \left(\begin{array}{c|c|c} \alpha & \mathbf{z}^T & \beta \\ \hline \mathbf{z} & M+L & (\mathbf{z}^F)^T \\ \hline \beta & \mathbf{z}^F & \alpha \end{array}\right)$$

be a generator matrix of a BSD code $\mathscr{C}$ *of length* $4n+4$ *digits over* $\mathscr{F}$. *If* $\alpha,\beta \neq 0$, $wt(\mathbf{z}) = n$ *and* $wt(\mathbf{y}^{(i)}) = 2n+2$ *where* $\mathbf{y}^{(i)}$ *is the* i^{th}*-row vector of G, obtained by removing the first* $2n+2$ *digits for* $i = 2,3\cdots 2n+1$, *then* $\mathscr{C}$ *is an MDS code.*

The following example illustrates Theorem 3.2 and Proposition 3.5.

Example 3.3. *Let* $\mathscr{C}_1$ *be a BSD code with parameter* $[4,2,2]_4$*, where* $F_4 = \{u+va | a^2 = a+1, u,v \in F_2\}$*. The generator matrix of* $\mathscr{C}_1$ *is*

$$G_1 = (I_2|M) = \left(\begin{array}{cc|cc} 1 & 0 & a & a+1 \\ 0 & 1 & a+1 & a \end{array}\right).$$

We can apply the construction method described in Theorem 3.2. Choose $\alpha = a, \beta = a+1$*. Thus, we compute, according to case (i), that the eigenvector of* M^r *is* $\mathbf{z} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$*. Therefore, we obtain a BSD [8,4,5] code* $\mathscr{C}_2$ *over* F_4 *with generator matrix*

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & a & 1 & 1 & a+1 \\ 0 & 1 & 0 & 0 & 1 & a & a+1 & 1 \\ 0 & 0 & 1 & 0 & 1 & a+1 & a & 1 \\ 0 & 0 & 0 & 1 & a+1 & 1 & 1 & a \end{pmatrix}.$$

The code is MDS.

3.3. Computational Result of Bisymmetric Self-dual Code over F_4.

In this section, we develop a BSD code over $F_4 = \{u+va | a^2 = a+1, u,v \in F_2\}$, using the method in the previous section. First, we present a BSD code $\mathscr{C}_1$ of length 8 to generate a BSD code $\mathscr{C}_4$ of length 20.

- A generator matrix of $[8,4,5]_4$ code $\mathscr{C}_1$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & a & 1 & 1 & a+1 \\ 0 & 1 & 0 & 0 & 1 & a & a+1 & 1 \\ 0 & 0 & 1 & 0 & 1 & a+1 & a & 1 \\ 0 & 0 & 0 & 1 & a+1 & 1 & 1 & a \end{pmatrix}.$$

- A generator matrix of $[12,6,7]_4$ code $\mathscr{C}_2$

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & a+1 & 1 & 1 & 1 & 1 & a \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & a & 1 & 1 & a+1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & a & a+1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & a+1 & a & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & a+1 & 1 & 1 & a & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & a & 1 & 1 & 1 & 1 & a+1
\end{pmatrix}$$

- A generator matrix of $[16,8,9]_4$ code $\mathscr{C}_3$

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & a+1 & a & a & a & a & a & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & a+1 & a & a+1 & a+1 & a+1 & a+1 & a & a \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & a & a+1 & a & 1 & 1 & a+1 & a+1 & a \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & a & a+1 & 1 & a & a+1 & 1 & a+1 & a \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & a & a+1 & 1 & a+1 & a & 1 & a+1 & a \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & a & a+1 & a+1 & 1 & 1 & a & a+1 & a \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & a & a & a+1 & a+1 & a+1 & a+1 & a & a+1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & a & a & a & a & a & a+1 & 1
\end{pmatrix}$$

- A generator matrix of $[20,10,11]_4$ code $\mathscr{C}_4$

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a+1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & a \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & a+1 & a & a & a & a & a & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & a+1 & a & a+1 & a+1 & a+1 & a+1 & a & a & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & a & a+1 & a & 1 & 1 & a+1 & a+1 & a & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & a & a+1 & 1 & a & a+1 & 1 & a+1 & a & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & a & a+1 & 1 & a+1 & a & 1 & a+1 & a & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & a & a+1 & a+1 & 1 & 1 & a & a+1 & a & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & a & a & a+1 & a+1 & a+1 & a+1 & a & a+1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & a & a & a & a & a & a & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & a & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & a+1
\end{pmatrix}$$

We demonstrate a transformation of BSD codes with applying Theorem 3.2 in Table 1. Based on [30], we have obtained new codes over F_4 with improved parameters and all three codes are MDS (optimal) codes. The MDS codes are derived from Proposition 3.5 with $\alpha,\beta \neq 0$.

TABLE 1. Construction of code $\mathscr{C}_4$

Length	**Case**	$\mathbf{z}^T$	**Constant**	$d(\mathscr{C})$
8	-	-	-	5
12	i)	1111	$\alpha = a+1$	7
16	ii)	$(a+1)aaaaa$	$\alpha = 1$	9
20	i)	11111111	$\alpha = a+1$	11

3.4. The Application of Bisymmetric Self-dual Codes to DNA Codes.

In this section, DNA codes will be constructed using BSD codes over $F_4 = \{u+va | a^2 = a+1, u,v \in F_2\}$ and $F_{4^n} = F_4 + y_1F_4 + \ldots + y_nF_4$. Let $D = \{\mathbf{A},\mathbf{T},\mathbf{G},\mathbf{C}\}$ be a set of DNA alphabets of order 4. We define a bijective mapping f as follows.

$$f : F_4 \longrightarrow D,$$

with $f(0) = \mathbf{C}, f(1) = \mathbf{G}, f(a) = \mathbf{T}$ and, $f(a+1) = \mathbf{A}$. Next, a DNA code of length $2n$ $\mathscr{D}$, can be constructed from a BSD code of length $2n$ $\mathscr{C}$ with the following bijective mapping.

$$f_1 : \mathscr{C} \longrightarrow \mathscr{D},$$

with $f_1(\mathbf{c} = (c_1c_2,\cdots c_{2n})) = (f(c_1)f(c_2)\cdots f(c_{2n}))$. Then, we apply Proposition 3.5 to construct an MDS DNA code. Let $\mathscr{C}_1$ be a BSD code of length $4n+4$ with a generator matrix G as in Proposition 3.5. The code $\mathscr{C}_1 \subseteq F_4^{4n+4}$ is obtained by performing the following encoding.

$$E : F_4^{2n+2} \longrightarrow F_4^{4n+4}$$
$$\mathbf{x} \longmapsto E(\mathbf{x}) = \mathbf{x}G.$$

So, we get an MDS DNA code of length $4n+4$ $\mathscr{D}_1$, the following bijective mapping.

$$h : \mathscr{C}_1 \longrightarrow \mathscr{D}_1$$
$$\mathbf{c}_1 \longmapsto h(\mathbf{c}_1) = h(E(\mathbf{x})) = f(x_1g_{1,1} + \cdots + x_{2n+2}g_{2n+2,1}) \cdots f(x_1g_{1,4n+4} + \cdots + x_{2n+2}g_{2n+2,4n+4}),$$

where $\mathbf{x} \in F_4^{2n+2}$. Meanwhile, we define the following bijective mapping from the field F_{4^n} to the set of DNA $D = \{\mathbf{A},\mathbf{T},\mathbf{G},\mathbf{C}\}$ to construct DNA codes over the field F_{4^n}.

$$\theta : F_{4^n} \longrightarrow D,$$

with $\theta(a_1 + b_1 a_2 + b_2 a_3 + \cdots + b_{n-1} a_n) = f(a_1 + a_2 + \cdots a_n)$, where $a_1, a_2, \cdots, a_n \in F_4$. Next, using Proposition 3.5, the MDS DNA code of length $4n+4$ $\mathscr{D}_2$, can be constructed from the BSD code over F_{4^n}. Let $\mathscr{C}_2$ be a BSD of length $4n+4$code over F_{4^n} with generator matrix G^*. The code $\mathscr{C}_1 \subseteq F_{4^n}^{4n+4}$ is generated through the encoding function E_1 as follows.

$$E_1 : F_{4^n}^{2n+2} \longrightarrow F_{4^n}^{4n+4}$$

$$\mathbf{x} \longmapsto E_1(\mathbf{x}) = \mathbf{x}G^*.$$

Then, the MDS DNA code $\mathscr{D}_2$ is obtained through the following bijective mapping.

$$h_1 : \mathscr{C}_2 \longrightarrow \mathscr{D}_2,$$

with $h(\mathbf{c}_1) = h_1(E_1(\mathbf{x})) = \theta\left(x_1 g^*_{1,1} + \cdots + x_{2n+2} g^*_{2n+2,1}\right) \cdots \theta\left(x_1 g^*_{1,4n+4} + \cdots + x_{2n+2} g^*_{2n+2,4n+4}\right)$, where $\mathbf{x} \in F_{4^n}^{2n+2}$.

Example 3.4. *Given a BSD code of length* 8 *over* $F_4 = \{u + va | a^2 = a+1, u, v \in F_2\}$ $\mathscr{C}$. *The generator matrix of* $\mathscr{C}$ *is as follows.*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & a & 1 & 1 & a+1 \\ 0 & 1 & 0 & 0 & 1 & a & a+1 & 1 \\ 0 & 0 & 1 & 0 & 1 & a+1 & a & 1 \\ 0 & 0 & 0 & 1 & a+1 & 1 & 1 & a \end{pmatrix}.$$

According to Example 3.3, $\mathscr{C}$ *is an MDS code. Thus, we can construct an MDS DNA code* $\mathscr{D}$ *using the following bijective mapping.*

$$h : \mathscr{C} \longrightarrow \mathscr{D}_1$$

$$\mathbf{c} \longmapsto h(\mathbf{c}_1) = h(E(\mathbf{x})) = f\left(x_1 g_{1,1} + \cdots + x_4 g_{4,1}\right) \cdots f\left(x_1 g_{1,8} + \cdots + x_4 g_{4,8}\right),$$

where E is an encoding map from $F_4^{\,4}$ *to* $F_4^{\,8}$. *The elements of the MDS DNA code* $\mathscr{D}$ *are presented in the following table.*

TABLE 2. Element of an MDS code $\mathscr{D}$

CCCCCCCC	*CCTCTTCT*	*CCCGAGGT*	*CCTGGAGC*	*CCCTTTTC*	*CCTTCCTT*	*CCCAGAAT*	*CCTAAGAC*
GCCCTGGA	*GCTCCAGG*	*GCCGGTTG*	*GCTGACTA*	*GCCTCAAA*	*GCTTTGAG*	*GCCAACCG*	*GCTAGTCA*
TCCCCTTT	*TCTCTCTC*	*TCCGAAAC*	*TCTGGGAT*	*TCCTTCCT*	*TCTTCTCC*	*TCCAGGGC*	*TCTAAAGT*
ACCCTAAG	*ACTCCGAA*	*ACCGGCCA*	*ACTGATCG*	*ACCTCGGG*	*ACTTTAGA*	*ACCAATTA*	*ACTAGCTG*
CGCCGTAG	*CGTCACAA*	*CGCGCACA*	*CGTGTGCG*	*CGCTACGG*	*CGTTGTGA*	*CGCATGTA*	*CGTACATG*
GGCCAACC	*GGTCGGCT*	*GGCGTCGT*	*GGTGCTGC*	*GGCTGGTC*	*GGTTAATT*	*GGCACTAT*	*GGTATCAC*
TGCCGCGA	*TGTCATGG*	*TGCGCGTG*	*TGTGTATA*	*TGCTATAA*	*TGTTGCAG*	*TGCATACG*	*TGTACGCA*
AGCCAGTT	*AGTCGATC*	*AGCGTTAC*	*AGTGCCAT*	*AGCTGACT*	*AGTTAGCC*	*AGCACCGC*	*AGTATTGT*
CTCCTCTT	*CTTCCTTC*	*CTCGGGAC*	*CTTGAAAT*	*CTCTCTCT*	*CTTTTCCC*	*CTCAAAGC*	*CTTAGGGT*
GTCCCGAG	*GTTCTAAA*	*GTCGATCA*	*GTTGGCCG*	*GTCTTAGG*	*GTTTCGGA*	*GTCAGCTA*	*GTTAATTG*
TTCCTTCC	*TTTCCCCT*	*TTCGGAGT*	*TTTGAGGC*	*TTCTCCTC*	*TTTTTTTT*	*TTCAAGAT*	*TTTAGAAC*
ATCCCAGA	*ATTCTGGG*	*ATCGACTG*	*ATTGGTTA*	*ATCTTGAA*	*ATTTCAAG*	*ATCAGTCG*	*ATTAACCA*
CACCATGA	*CATCGCGG*	*CACGTATG*	*CATGCGTA*	*CACTGCAA*	*CATTATAG*	*CACACGCG*	*CATATACA*
GACCGATT	*GATCAGTC*	*GACGCCAC*	*GATGTTAT*	*GACTAGCT*	*GATTGACC*	*GACATTGC*	*GATACCGT*
TACCACAG	*TATCGTAA*	*TACGTGCA*	*TATGCACG*	*TACTGTGG*	*TATTACGA*	*TACACATA*	*TATATGTG*
AACCGGCC	*AATCAACT*	*AACGCTGT*	*AATGTCGC*	*AACTAATC*	*AATTGGTT*	*AACATCAT*	*AATACTAC*

4. CONCLUSIONS

In this study, we have investigated some properties of reversible (bisymmetric) self-dual codes over finite fields with characteristic two. We have also proposed a method for constructing reversible (bisymmetric) self-dual codes over finite fields with characteristic two, based on code extension. We construct bisymmetric self-dual codes over finite fields with improved parameters and also discover MDS codes using this method. We applied bisymmetric self-dual codes over the fields F_4 and F_{4^n} to form a DNA code using a bijective mapping. However, this construction method can be applied only to fields with characteristic two. Therefore, future research can develop other algebraic structures. Additionally, applications of reversible (bisymmetric) self-dual codes on $\mathscr{F}$ can also be explored.

ACKNOWLEDGEMENT

We would like to thank you for the referee's fruitful suggestions, which improved the quality of the article.

CONFLICT OF INTERESTS

The authors declare that there is no conflict of interests.

REFERENCES

[1] C.E. Shannon, A Mathematical Theory of Communication, Bell Syst. Techn. J. 27 (1948), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

[2] N. Sendrier, Code-Based Cryptography: State of the Art and Perspectives, IEEE Secur. Priv. 15 (2017), 44–50. https://doi.org/10.1109/msp.2017.3151345.

[3] M.J.E. Golay, Notes on Digital Coding, Proc. IEEE 37 (1949), 657.

[4] S.T. Dougherty, S. Mesnager, P. Sole, Secret-Sharing Schemes Based on Self-Dual Codes, in: 2008 IEEE Information Theory Workshop, IEEE, Porto, Portugal, 2008: pp. 338–342. https://doi.org/10.1109/itw.2008.4578681.

[5] E. Nachmani, E. Marciano, L. Lugosch, et al. Deep Learning Methods for Improved Decoding of Linear Codes, IEEE J. Sel. Top. Signal Process. 12 (2018), 119–131. https://doi.org/10.1109/jstsp.2017.2788405.

[6] A.M. Gleason, Weight Polynomial of Selfdual Codes and the Macwilliams Identities, in: Actes Congres International des Mathematiciens, Gauthier-Villards, Vol. 3, pp. 211-215, 1971.

[7] V. Pless, Symmetry Codes over GF(3) and New Five-Designs, J. Comb. Theory, Ser. A 12 (1972), 119–142. https://doi.org/10.1016/0097-3165(72)90088-x.

[8] J. Leon, V. Pless, N. Sloane, On Ternary Self-Dual Codes of Length 24, IEEE Trans. Inf. Theory 27 (1981), 176–180. https://doi.org/10.1109/tit.1981.1056328.

[9] V. Pless, V. Tonchev, Self-dual codes overGF(7)(Corresp.), IEEE Trans. Inf. Theory 33 (1987), 723–727. https://doi.org/10.1109/tit.1987.1057345.

[10] S.T. Dougherty, Self-Dual Codes and Finite Projective Planes, Math. J. Okayama Univ. 40 (1998), 45–54.

[11] P. Gaborit, A. Otmani, Experimental Constructions of Self-Dual Codes, Finite Fields Their Appl. 9 (2003), 372–394. https://doi.org/10.1016/s1071-5797(03)00011-x.

[12] J.L. Kim, Y. Lee, Self-Dual Codes Using the Building-up Construction, in: 2009 IEEE International Symposium on Information Theory, IEEE, Seoul, South Korea, 2009: pp. 2400–2402. https://doi.org/10.1109/isit.2009.5206010.

[13] M. Shi, L. Sok, P. Solé, S. Çalkavur, Self-Dual Codes and Orthogonal Matrices over Large Finite Fields, Finite Fields Their Appl. 54 (2018), 297–314. https://doi.org/10.1016/j.ffa.2018.08.011.

[14] J.L. Massey, Reversible Codes, Inf. Control 7 (1964), 369–380. https://doi.org/10.1016/s0019-9958(64)90438-3.

[15] P.K. Kadbe, M.G. Waje, Error Detection in Fault-Tolerant Reversible Circuit Using Fredkin Gates, in: A. Kumar, S. Mozar, (eds) ICCCE 2021, Lecture Notes in Electrical Engineering, vol 828, Springer, Singapore, (2022). https://doi.org/10.1007/978-981-16-7985-8_58.

[16] K. Tzeng, C. Hartmann, On the Minimum Distance of Certain Reversible Cyclic Codes (Corresp.), IEEE Trans. Inf. Theory 16 (1970), 644–646. https://doi.org/10.1109/tit.1970.1054517.

[17] S.K. Muttoo, S. Lal, A Reversible Code over $GF(q)$, Kybernetika 22 (1986), 85–91. http://dml.cz/dmlcz/125543.

[18] Y. Takishima, M. Wada, H. Murakami, Reversible Variable Length Codes, IEEE Trans. Commun. 43 (1995), 158–162. https://doi.org/10.1109/26.380026.

[19] S. Bhasin, J.L. Danger, S. Guilley, X.T. Ngo, L. Sauvage, Hardware Trojan Horses in Cryptographic IP Cores, in: 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography, IEEE, Los Alamitos, CA, USA, 2013: pp. 15–29. https://doi.org/10.1109/fdtc.2013.15.

[20] L. Jin, Construction of MDS Codes with Complementary Duals, IEEE Trans. Inf. Theory 63 (2016), 2843–2847. https://doi.org/10.1109/tit.2016.2644660.

[21] F. Gursoy, E.S. Oztas, I. Siap, Reversible DNA Codes Using Skew Polynomial Rings, Appl. Algebra Eng. Commun. Comput. 28 (2017), 311–320. https://doi.org/10.1007/s00200-017-0325-z.

[22] S.T. Dougherty, A. Korban, S. Sahinkaya, D. Ustun, Construction of DNA Codes From Composite Matrices and a Bio-Inspired Optimization Algorithm, IEEE Trans. Inf. Theory 69 (2023), 1588–1603. https://doi.org/10.1109/tit.2022.3217518.

[23] A. Korban, S. Şahinkaya, D. Ustun, Reversible G^k-Codes with Applications to DNA Codes, Designs Codes Cryptogr. 90 (2022), 1679–1694. https://doi.org/10.1007/s10623-022-01067-7.

[24] O. Prakash, S. Patel, S. Yadav, Reversible Cyclic Codes over Some Finite Rings and Their Application to DNA Codes, Comput. Appl. Math. 40 (2021), 242. https://doi.org/10.1007/s40314-021-01635-y.

[25] H.J. Kim, W.-H. Choi, Y. Lee, Construction of Reversible Self-Dual Codes, Finite Fields Their Appl. 67 (2020), 101714. https://doi.org/10.1016/j.ffa.2020.101714.

[26] H.J. Kim, W.-H. Choi, Y. Lee, Designing DNA Codes from Reversible Self-Dual Codes over GF(4), Discrete Math. 344 (2021), 112159. https://doi.org/10.1016/j.disc.2020.112159.

[27] A.N. Hidayat, V.H. Krisnawati, A.R. Alghofari, Reversible Self-Dual Codes over Finite Field, Cauchy: J. Mat. Murni Apl. 9 (2024), 287–296. https://doi.org/10.18860/ca.v9i2.29116.

[28] B.S. Gopinadh, V. Marka, Reversible Codes in the Rosenbloom-Tsfasman Metric, AIMS Math. 9 (2024), 22927–22940. https://doi.org/10.3934/math.20241115.

[29] H.J. Kim, W.-H. Choi, Reversible Self-Dual Codes Over the Ring $F_2 + uF_2$, IEEE Access 12 (2024), 1117–1129. https://doi.org/10.1109/access.2023.3347408.

[30] M. Grassl, Bounds on the Minimum Distance of Linear Codes and Quantum Codes, https://www.codetables.de/BKLC/index.html. Accessed on 2024-12-1.

[31] S. Ling, C. Xing, Coding Theory: A First Course, Cambridge University Press, 2004. https://doi.org/10.1017/cbo9780511755279.