CAUCHY: Jurnal Matematika Murni dan Aplikasi
Volume 9(2) (2024), Pages 287-296
p-ISSN: 2086-0382; e-ISSN: 2477-3344

Reversible Self-Dual Codes over Finite Field

Ardi Nur Hidayat, Vira Hari Krisnawati*, Abdul Rouf Alghofari

Department of Mathematic, Brawijaya University, Indonesia

Email: virahari@ub.ac.id

ABSTRACT

Reversible self-dual code is a linear code which combine the properties from self-dual code and reversible code. Previous research shows that reversible self-dual codes have only been developed over field of order 2 and order 4. In this article, we construct reversible self-dual code over any finite field of order q, F_q with natural number $q \geq 2$. We first examine and prove some of fundamental properties of reversible self-dual code over F_q. After a thorough analysis these, we obtain a new generator matrix of reversible self-dual code. A new generator matrix is derived from existing self-dual and reversible self-dual code over F_q. It will be shown that a new reversible self-dual over F_q can be constructs from one and more existing code by specific algebraic methods. Furthermore, using this construction, we determine the minimum distance of reversible self-dual code and ensuring its optimal performance in various applications.

Keywords: finite field; generator matrix; minimum distance; reversible self-dual code

INTRODUCTION

Coding theory is a branch of mathematics within the field of algebra. It was first introduced by Shannon in 1948 [1]. Coding theory employs concepts from linear algebra, specifically vector spaces, and combines them with concepts from algebraic structures such as rings, fields, and modules. In coding theory, message transmission and reception are performed using code. The code typically used is linear code. Linear code is a vector subspace over algebraic structures such as a finite field. Theoretical studies in linear code have advanced rapidly, one of them is dual code. Dual code is formed using the orthogonal complement of a linear code [2].

The relationship between dual code and linear code leads to the concept of self-dual code. Self-dual code was first introduced by Golay [3] in 1949. A self-dual code is a linear code in which each element is the same as the element of its dual code. Related to error correction in message, self-dual code can be applied in cryptography and machine learning [4].

Conceptually, self-dual codes have been extensively studied. Bouyuklieva and Harada [5] constructed self-dual codes over F_2. Then, Grassl and Gulliver [6] studied self-dual codes with optimal minimum distance. Subsequently, Grassl and Gulliver [7] further developed his previous research on self-dual codes over small fields. Park [8] classified

Submitted: September 12, 2024 Reviewed: September 23, 2024 Accepted: October 15, 2024
DOI: http://dx.doi.org/10.18860/ca.v9i2.29116

self-dual code. Shi et al. [9] examined self-dual code in connection with orthogonal matrices. In 2020, Sok [10] explicitly constructed self-dual code over F_2. In 2021 Kim and Choi [11] constructed self-dual code over finite fields of order q, specifically $q \equiv 1 \bmod 4$, using symmetric matrices and eigenvectors. Later in 2022, Choi and Kim [12] further generalized the construction of reversible self-dual code to any field of order q.

Besides the concept of self-dual code, the concept of reversible code has also developed. Reversible code was first introduced by Massey in 1964 [13]. This research discussed the basic concept of reversible code in the context of cryptography and digital communication. A reversible code is one where every element's reverse is always present within the code. In its development, some researchers have expanded the concept of reversible codes along with their applications. In 1995, Takishima et al. [14] showed that reversible code has good error correction capabilities and high transmission efficiency. Ngo et al. [15] used reversible code as a cipher to detect hardware Trojan horse virus attacks in 2013. In error correction code, reversible code enable error correction by allowing lossless information recovery, with techniques such as parity checking and Hamming codes effectively implemented in reversible circuits to improve communication reliability [16].

A code of length $2n$ with minimum distance d can detect up to $d-1$ errors and correct up to $\lfloor (d-1)/2 \rfloor$ errors. According to singleton bound, if the code is self-dual, the code can detect n errors and correct a maximum of $\lfloor n/2 \rfloor$ errors. Then, if the code is reversible, the code can detect $2n$ errors and correct n errors [2]. Since self-dual codes and reversible codes have strong error correction capabilities and can be applied across various areas, some researchers have investigated the properties and construction of self-dual and reversible code. In 2020, Kim et al. [17] explored reversible properties in self-dual code and introduced the concept of reversible self-dual code. This code is a self-dual code with reversible properties. Subsequently, reversible self-dual code was constructed using the concepts of persymmetric matrices. Later in 2021, Kim et al. [18] designed code over finite field of order 4.

Based on the analysis of the articles by Kim et al. [17] and [18] regarding the construction of reversible self-dual code, the properties provided cannot be applied to arbitrary finite fields. These properties only apply to code over fields of order two and four. However, according to Choi and Kim [11] and [12], self-dual code can be constructed from any finite field. Therefore, in this paper, the properties of reversible self-dual code over finite fields will be developed. These properties will be used to construct reversible self-dual code over finite fields. There are four sections in this article. In the second section, we provide a literature review and describe the research methodology. In the third section, we present results on the properties of reversible self-dual code over F_q and construct a new reversible self-dual code over F_q. The final section concludes the article.

METHODS

In this work, we study some relevant literature literatures. We first describe some terms in coding theory. Let n and $q \geq 2$ be natural number. A linear code C of length n and dimension k over finite field F_q is a subspace of F_q^n. An element of C is called a codeword. Let $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ and $\mathbf{y} = (y_1, y_2, \cdots, y_n)$ are vectors in F_q^n, we define inner product $\mathbf{x} \cdot \mathbf{y} = \sum_{j=0}^{n} x_j y_j$. A dual code of C is defined by

$$C^{\perp} = \{ \mathbf{x} \in F_q^n \mid \mathbf{x} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C \}.$$

Code C is called self-dual if $C = C^{\perp}$.

The weight of a codeword $\mathbf{c}$ is the count of non-zero symbols in the codeword, represented as $wt(\mathbf{c})$. The Hamming distance between two codewords $\mathbf{x}$ and $\mathbf{y}$ defined as $d(\mathbf{x} \cdot \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$. The minimum distance of a code, denoted as $d(C)$ is the smallest Hamming distance between any two distinct codewords in C. For a linear code 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. A linear code with minimum distance d can detect up to $d - 1$ errors and correct up to $\lfloor (d-1)/2 \rfloor$ errors.

A generator matrix for a linear code C is a matrix where a basis for C is formed by its rows. Therefore, each set of rows of the matrix $G$is linearly independent and spans C. Linear code C of length n and dimension k with generator matrix G which can be stated as $C = \{\mathbf{w}G \mid \mathbf{w} \in F_q^k\}$.

The standard generator matrix of $[n, k, d]_q$ code is defined by, $G = (I_n|A)$, with G is a matrix of size $k \times n$ and I_n is the identity matrix of size $n \times n$. The following theorem describes the properties of a generator matrix of a self-dual code.

Theorem 1 [1] Let $G = (I_n|A)$ is generator standar of linear code C over F_q. If C is self-dual code then $AA^T = -I_n$.

Next, we introduce the definition of reversible code and reversible self-dual code.

Definition 1 [18] Let C be a code with length n digit. A code C is said be reversible code if for all $\mathbf{c} = (c_1, c_2, \dots, c_{n-1}, c_n) \in C$ there is $\mathbf{c}^{\mathrm{r}} = (c_n, c_{n-1}, \dots, c_2, c_1) \in C$.

Definition 2 [21] A self-dual code C is said be a reversible self-dual code if C is reversible code.

In the study by Kim et al. [21], a reversible self-dual code over F_2 was constructed using the concepts of flip transpose matrix, reverse column matrix, and persymmetric matrix. Let $B = \left(b_{i,j}\right)_{p \times q}$, then flip transpose of matrix B is $B^F = \left(b_{q-j+1,p-i+1}\right)_{q \times p}$ and $B^r = \left(b_{p,q-j+1}\right)_{p \times q}$ is the column reversed matrix of B. If $B = B^F$, then B is a persymmetric matrix. Let C and D be square matrix of size $n \times n$, I_n be the identity matrix of size $n \times n$, and I_n^r be coloumn reversed matrix of I_n. The subsequent properties are straightforward.

$$(C^F)^F = C, \quad (C+D)^F = C^F + D^F, \quad (C^T)^F = (C^F)^T, \quad (CD)^F = D^F C^F,$$
$$(I_n^r)^T = (I_n^r)^F = I_n^r, \; (I_n^r)^2 = I_n, \; C^r = CI_n^r \text{ and } C^F = I_n^r C^T I_n^r.$$

Kim et al. [21] and [22] proved that a self-dual code over F_2 and F_4 with generator matrix $G = (I|A)$ is said to be reversible if the matrix A is a persymmetric matrix. By analogical related concepts from [21] and [22], the research methodology is given as follows:

i. Investigating some properties of a generator matrix of a self-dual code over F_q that are reversible.
ii. Analysing the construction of a new reversible self-dual code over F_q using known self-dual codes reversible self-dual codes in the form of a standard (non-standard) generator matrix.
iii. Determining the minimum distance of the generated code.
iv. Generating a new generator matrix of reversible self-dual code over F_q and finding the minimum distance of the code.
v. Form some theorems and give relevant examples with the proofs.

RESULTS AND DISCUSSION

In this section, the properties of reversible self-dual codes over F_q are provided. Next, the code will be constructed based on these properties. Consider a self-dual code C with length n over the field F_q. Let the generator matrix of the code C be given as $G = (I_n|A)$. Therefore, the following properties will result.

Theorem 2 Let C be a self-dual code over F_q length n with standard generator matrix $(I_n \mid A)$. The code C is reversible if and only if $A = -A^F$.

Proof.

Let C be a self-dual code over F_q. Suppose that C is a reversible code, then the column reversed matrix of G,

$$G^r = (A^r \mid I_n^r)$$

also generates the code C. Since C is self-dual, $AA^T = -I_n$. Thus, A and A^r are non-singular. Consider the matrix below,

$$-(A^r)^{-1}G^r = ((A^r)^{-1}A^r \mid (A^r)^{-1} I_n^r) = (I_n|(A^r)^{-1} I_n^r).$$

The matrix $-(A^r)^{-1}G^r$ and G become the same standard generator matrix for C if $A = (A^r)^{-1} I_n^r$.

Thus $A = (A^r)^{-1} I_n^r \Leftrightarrow A = -I_n^r A^T I_n^r \Leftrightarrow A = -A^F$. The reverse case can be shown in the same way. ■

Then, we study the existence of reversible self-dual code over F_q by Theorem 2.

Lemma 1 For any self-dual code C with length 2 over a field F_q whose its characteristic not equal to 2, the code C is not a reversible self-dual code.

Proof.

Assume that the code C is a reversible self-dual code. Let $G = (a\ b)$ with $a, b \in F_q$ be a generator matrix of code C. Because C is reversible self-dual, we have $GG^T = O$ and $G^r G^T = O$. Since the rows of matrix G are linearly independent, the values of a and b cannot both be zero. Consider $GG^T = O$ and $G^r G^T = O$, which yield $ba.ba$ equal to zero if one of them is zero. Assume a is zero. However, if $a = 0$, then the $GG^T = b^2$, and $b^2 \neq 0$, because $b^2 \neq 0, b \neq 0$. Therefore, code C is not a reversible self-dual code. ■

Based on Lemma 1, there is no reversible self-dual code of length 2 over the field F_q. Next, the general form of a generator matrix for a reversible self-dual code of length 4 we present.

Lemma 2 Given the matrix $(I_2 \mid M)$ where the matrix M of size 2×2 over the field F_q as follows:

$$M = \begin{pmatrix} b & 0 \\ 0 & -b \end{pmatrix}$$

The matrix $(I_2|M)$ is the standard generator matrix of a reversible self-dual code of length 2, if $b^2 = -1 \in F_q$.

Proof.

Suppose $b^2 = -1 \in F_q$. Consider that,

$$MM^T = \begin{pmatrix} b^2 & 0 \\ 0 & b^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_{2,}$$

$$M^F = \begin{pmatrix} -b & 0 \\ 0 & b \end{pmatrix} = -M.$$

Since $MM^T = -I_2$ and $M^F = -M$, by Theorem 2, the matrix $(I_2 \mid M)$ is the standard generator matrix of a reversible self-dual code. ■

Following the construction results in Lemma 2, the message generating the reversed codeword can be determined. Additionally, the code parameters of the

generated code can be found. For more details, see Corollary 1 below.
Corollary 1. Let C be a reversible self-dual code of length 4 over field F_q. If the generator matrix of C as described in Lemma 2, then the minimum distance of C is 2. Furthermore, the code C is a code with parameters $[4,2,2]_q$.
Example 1. Given linear code C of length 4 over F_5. Code C has the following generator matrix,

$$G = \begin{pmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix} = (I_2 \,|A\,).$$

Consider that, $AA^T = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_{2,}$ and $A^F = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = -A^F$.
Then, code C is reversible self-dual code over F_5 by Theorem 2. If the minimum distance of C is determined, then $d(C) = 2$. This is in accordance with Corollary 1.

The structure of the generator matrix for the shortest reversible self-dual code over F_q is established based on Lemma 2. Next, a larger reversible self-dual code over F_q will be constructed. We build a reversible self-dual code over F_q from one known self-dual (reversible self-dual) code.
Theorem 3. Let C_1 be a self-dual code of length $2n$ over F_q. If G_1 is the generator matrix of code C_1 and $\alpha \neq 0 \in F_q$, then there exists a reversible self-dual code C_2 of length $4n$ over F_q. The generator matrix of code C_2 is

$$G_2 = \left(\begin{array}{c|c} \alpha G & O \\ \hline O & \alpha G^r \end{array}\right)$$

with O is zero matrix of size $n \times 2n$. Furthermore, $d(C_2) = d(C_1)$.
Proof.
Consider that, $G_2 G_2^T = O$ and $G_2(G_2^r)^T = O$. Thus, code C_2 is a reversible self-dual code. Consequently, the minimum distance of code C_2 is obtained when encoding the codewords from the vector,

$$\mathbf{x} = (\,x_1\, x_2\, \cdots\, x_n \mid \mathbf{0}\,) = (\,\mathbf{y} \mid \mathbf{0}\,) \text{ or } \mathbf{x} = (\mathbf{0}|x_{n+1}\, x_{n+2}\, \cdots\, x_{2n}) = (\mathbf{0}\,|\mathbf{w}) \in F_q^{2n}\,.$$

Since $\mathbf{y}$ and $\mathbf{w} \in F_q^n$, the resulting codewords are either $(\mathbf{c} \mid \mathbf{0})$or $(\mathbf{0} \mid \mathbf{c})$ with $\mathbf{c} \in C_1$. Therefore, the Hamming weight of each codeword in C_2 will be the same as in C_1, because the remaining n digits are zero. Thus, the minimum distance of C_2 will be the same as the minimum distance of C_1 in other words, $d(C_2) = d(C_1)$. ∎

According to Theorem 3, a reversible self-dual code with a length of $4n$ digits can be constructed from a self-dual code with a length of $2n$ digits. The minimum distance will be the same as that of the self-dual code used for the construction. An example of this construction is provided below.
Example 2. Let C_1 be a self-dual code$-[4,2,3]_3$ with a generator matrix,

$$G_1 = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 2 \end{pmatrix}.$$

From the code C_1, a new reversible self-dual code$-[8,4,3]_3$ can be constructed as in Theorem 3. If $a = 2 \in F_3$ is chosen, the generator matrix of the code$-[8,4,3]_3$ is as follows

$$G_2 = \left(\begin{array}{c|c} 2G_1 & O \\ \hline O & 2G_1^r \end{array}\right) = \left(\begin{array}{cccc|cccc} 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 \\ \hline 0 & 0 & 0 & 0 & 1 & 2 & 2 & 0 \end{array}\right).$$

In Theorem 3, a reversible self-dual code of length $4n$ has been generated in the form of an arbitrary generator matrix. Next, we study the construction of a reversible self-dual code in standard form.
Theorem 4. Let C_1 be a self-dual code of length $2n$ over F_q . If $G_1 = (I_n|A)$ is a generator

matrix of C_1 then,

$$G_2 = \left(\begin{array}{c|c|c|c} I_n & O & A & O \\ \hline O & I_n & O & -A^F \end{array}\right),$$

Is a generator matrix of reversible self-dual code C_2 of length $4n$ and $d(C_1) = d(C_2)$.

Proof. It is known that $G_1 = (I_n \ |A)$ serves as a generator matrix for a self-dual code C_1. Let $B = \begin{pmatrix} A & O \\ O & -A^F \end{pmatrix}$. We prove that $G_2 = (I_{2n}|B)$ is a generator matrix of a reversible self-dual code C_2 of length $4n$. Consider that,

$$BB^T = \left(\begin{array}{c|c} A & O \\ \hline O & -A^F \end{array}\right)\left(\begin{array}{c|c} A^T & O \\ \hline O & -(A^F)^T \end{array}\right) = \left(\begin{array}{c|c} AA^T & O \\ \hline O & A^F(A^F)^T \end{array}\right) = \left(\begin{array}{c|c} -I_n & O \\ \hline O & -I_n \end{array}\right) = -I_{2n}.$$

and

$$B^F = \left(\begin{array}{c|c} -A & O \\ \hline O & A^F \end{array}\right) = -B.$$

Then, by Theorem 1 and 2 the constructed code is a reversible self-dual code C_2 of length $4n$ over the field F_q. To show the minimum distance of the code C_2 is equal to C_1, the steps are the same as in Theorem 3. ■

Example 3. Let G_1 be a generator matrix of self-dual code C_1 of length 4 over F_3 where $d(C_1) = 3$.

$$G_1 = (I_2 \ |A) = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{array}\right).$$

Then,

$$G_2 = \left(\begin{array}{c|c|c|c} I_2 & O & A & O \\ \hline O & I_2 & O & -A^F \end{array}\right) = \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 2 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 \end{array}\right)$$

generates a reversible self-dual code C_2 of length 8 over F_3. If the minimum distance of C_2 is computed, $d(C_2) = 3$. Therefore, $d(C_2) = d(C_1)$.

A reversible self-dual code of length 4n has been constructed using a self-dual code as described in Theorem 3 and 4. In the next theorem, we construct a code from a reversible self-dual code.

Theorem 5. If $(I_n \ |A)$ is a generator matrix of a reversible self-dual code C_1 of length 2n over field F_q , then

$$G = \left(\begin{array}{c|c|c|c} I_n & O & A & O \\ \hline O & I_n & O & A \end{array}\right)$$

generates a reversible self-dual code C_2 of length $4n$. The minimum distance of the code is equal to $d(C_1)$.

Proof.

Let

$$M = \left(\begin{array}{c|c} A & O \\ \hline O & A \end{array}\right).$$

Since $(I_n \ |A)$ is the generator matrix of a reversible self-dual code of length 2n over field F_q. by Theorem 2 we get $A = -A^F$, hence $M = -M^F$. Thus, we compute that $MM^T = -I_{2n}$. Based on Theorem 2, G generates a reversible self-dual code of length $4n$. The method for finding the minimum distance is similar to their proof in Theorem 3. ■

If we construct a reversible self-dual code with a greater length, Theorem 5 can be extended into Corollary 2.

Corollary 2. If $(I_n|A)$ is a generator matrix of a reversible self-dual code over the field F_q

with length $2n$, then

$$G = (I_{kn}\ |M)$$

represents a generator matrix of size $kn \times 2kn$, where M is a block diagonal matrix with diagonal entries consisting of the matrix A repeated k times. The matrix M can be expressed as

$$M = \underbrace{A \oplus A \oplus A \dots\dots \oplus A}_{k\ times}$$

Furthermore, when multiplying an element in F_q (satisfies certain conditions) by the matrix A in the Theorem 5, we obtain a new construction of reversible self-dual code.

Corollary 3. Let $(I_n|A)$ be a generator matrix of a reversible self-dual code over a field F_q of length $2n$ and $b^2 = 1 \in F_q$. Then

$$G = \left(\begin{array}{c|c|c|c} I_n & O & bA & O \\ O & I_n & O & bA \end{array}\right)$$

is a generator of a reversible self-dual code of length $4n$.

We give an example of how to construct a reversible self-dual code of length 8 from reversible self-dual code of length 4 according in corollary 3 as follow.

Example 4. Assume C is a reversible self-dual code over the field F_5. The generator matrix of the code C is as follows.

$$G = (I_2\ |A) = \left(\begin{array}{cc|cc} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 3 \end{array}\right).$$

We can construct a reversible self-dual code C_1 of length 8 as in Corollary 3 by taking $b = 4 \in F_5$ which satisfies $b^2 = 1 \in F_5$. The generator matrix of the code is as follows.

$$G_1 = \left(\begin{array}{c|c|c|c} I_2 & O & 4A & O \\ O & I_2 & O & 4A \end{array}\right) = \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \end{array}\right).$$

Moreover, we develop a new reversible self-dual code over the field F_q using known two self-dual codes and reversible self-dual codes.

Theorem 6. Let G_1 and G_2 be the generator matrix of self-dual codes of lengths $2m$ and $2n$, respectively $C_1$and C_2, over a field F_q. The matrix G below represents the generator matrix of a reversible self-dual code C_3 of length $4m + 4n$.

$$G_3 = \left(\begin{array}{c|c|c|c} G_1 & O & O & O \\ \hline O & O & O & G_1^r \\ \hline O & G_2 & O & O \\ \hline O & O & G_2^r & O \end{array}\right)$$

The minimum distance of the code constructed by the matrix G is $\min\{d(C_1), d(C_2)\}$.

Proof.

Consider that,

$$G_3{G_3}^T = \left(\begin{array}{c|c|c|c} G_1 & O & O & O \\ \hline O & O & O & G_1^r \\ \hline O & G_2 & O & O \\ \hline O & O & G_2^r & O \end{array}\right)\left(\begin{array}{c|c|c|c} G_1^T & O & O & O \\ \hline O & O & G_2^T & O \\ \hline O & O & O & (G_2^r)^T \\ \hline O & (G_1^r)^T & O & O \end{array}\right) = O$$

and

$$G_3({G_3}^r)^T = \left(\begin{array}{c|c|c|c} G_1 & O & O & O \\ \hline O & O & O & G_1^r \\ \hline O & G_2 & O & O \\ \hline O & O & G_2^r & O \end{array}\right)\left(\begin{array}{c|c|c|c} G_1^T & O & O & O \\ \hline O & O & G_2^T & O \\ \hline O & O & O & (G_2^r)^T \\ \hline O & (G_1^r)^T & O & O \end{array}\right) = O.$$

Then, the code generated by the matrix G_3 is a reversible self-dual code. The code C_3 can be generated from the encoding function as follows.

$$E : F_q^{2m+2n} \to F_q^{4m+4n}.$$
$$E(\mathbf{x}) = \mathbf{x}G_3$$

According to G_3, the minimum distance of the code C_3 is obtained from the following 4 cases of vector $\mathbf{x} \in F_q^{2m+2n}$.

Case 1: if $\mathbf{x} = (\mathrm{x}_1\mathrm{x}_2 \cdots \mathrm{x}_\mathrm{m} \mid \mathbf{0})$, we get codeword $\mathbf{c} = \left((\mathrm{x}_1\mathrm{x}_2 \cdots \mathrm{x}_\mathrm{m})G_1\middle|\mathbf{0}\right) = (\mathbf{y}|\mathbf{0}) \in C_3$. Note that for $(\mathrm{x}_1\mathrm{x}_2 \cdots \mathrm{x}_\mathrm{m})$ can be represented as element in F_q^m, then $\mathbf{y} \in C_1$. Since the remaining $2m + 4n$ digits of $\mathbf{c}$ are zero, then the Hamming weight of $\mathbf{c} \in C_3$ is equal as $\mathbf{y} \in C_1$. Therefore, the minimum distance of C_3 is equal to C_1.

Case 2: if $\mathbf{x} = (\mathbf{0}|\mathrm{x}_{\mathrm{m}+1}\mathrm{x}_{m+2} \cdots \mathrm{x}_{2\mathrm{m}}|\mathbf{0})$, we get codeword

$$\mathbf{c} = (\mathbf{0}|(\mathrm{x}_{\mathrm{m}+1}\mathrm{x}_{\mathrm{m}+2} \cdots \mathrm{x}_{2\mathrm{m}})G_1^r|\mathbf{0}) = (\mathbf{y}|\mathbf{0}) \in C_3.$$

Similar in case 1, $(\mathrm{x}_{\mathrm{m}+1}\mathrm{x}_{\mathrm{m}+2} \cdots \mathrm{x}_{2\mathrm{m}})$ also can be represented as element in F_q^m, then $\mathbf{y} \in C_1$. Therefore, as in the first case, we obtain $d(C_3) = d(C_1)$.

Case 3: if $\mathbf{x} = (\mathbf{0}|\mathrm{x}_{2m+1}\mathrm{x}_{2m+2} \cdots \mathrm{x}_{2m+n}|\mathbf{0})$, we get codeword

$$\mathbf{c} = (\mathbf{0}|(\mathrm{x}_{\mathbf{2m+1}}\mathrm{x}_{2m+2} \cdots \mathrm{x}_{2m+n})G_2|\mathbf{0}) = (\mathbf{0}|\mathbf{w}|\mathbf{0}) \in C_3.$$

Note that for $(\mathrm{x}_{2\mathrm{m}+1}\mathrm{x}_{2\mathrm{m}+2} \cdots \mathrm{x}_{2\mathrm{m}+\mathrm{n}})$ can be represented as element in F_q^n, then $\mathbf{w} \in C_2$. Since the last $2n + 4m$ digits of $\mathbf{c}$ have zero values, the Hamming weight of $\mathbf{c} \in \mathrm{C}_3$ is $\mathbf{w} \in C_2$. Thus, $d(C_3) = d(C_2)$.

Case 4: if $\mathbf{x} = (\mathbf{0}|\mathrm{x}_{2m+n+1}\mathrm{x}_{2m+n+2} \cdots \mathrm{x}_{2m+2n})$, we get codeword

$$\mathbf{c} = (\mathbf{0}|(\mathrm{x}_{2m+n+1}\mathrm{x}_{2m+n+2} \cdots \mathrm{x}_{2m+2n})G_2^r) = (\mathbf{0}|\mathbf{w}) \in C_3.$$

Note that for $(\mathrm{x}_{2\mathrm{m}+1}\mathrm{x}_{2\mathrm{m}+2} \cdots \mathrm{x}_{2m+2n})$, also can be represented as element in F_q^n, then $\mathbf{w} \in C_2$. Similar in case 3, we get $d(C_3) = d(C_2)$.

Based on the four cases, it is obtained that $d(C_3) = \min\{d(C_1), d(C_2)\}$. ■

Theorem 6 establishes that the minimum distance of code C_3, which is generated from C_1 and C_2, is equal to the minimum of $d(C_1)$ and $d(C_2)$. Therefore, C_3 can correct $t = \left\lfloor \frac{\min\{d(C_1), d(C_2)\}-1}{2} \right\rfloor$ errors. For further illustration, see the following example.

Example 5. Let C_1 be a code-$[2,1,2]_5$ and C_2 code-$[4,2,4]_5$, each of which is self-dual These codes each have generator matrix G_1 and G_2 as

$$G_1 = \begin{pmatrix} 4 & 2 \end{pmatrix} \quad G_2 = \begin{pmatrix} 4 & 2 & 1 & 3 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

Thus, a reversible self-dual code C_3 is constructed as in Theorem 5. The generator matrix of C_3 as follows.

$$G_3 = \left(\begin{array}{c|c|c|c} G_1 & O & O & O \\ \hline O & O & O & G_1^r \\ \hline O & G_2 & O & O \\ \hline O & O & G_2^r & O \end{array}\right) = \left(\begin{array}{cc|cccc|cccc|cc} 4 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 4 \\ \hline 0 & 0 & 4 & 2 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 3 & 4 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 4 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 4 & 3 & 1 & 0 & 0 \end{array}\right).$$

Additionally, C_3 is a code$-[12,6,2]_5$.

Theorem 7. Let $G_1 = (P\,|Q)_{m\times 2m}$ and $G_2 = (R|S)_{n\times 2n}$ are generator matrix of a reversible self-dual codes with lengths $2m$ and $2n$ over F_q, respectively. The following generator matrix constructs a reversible self-dual code C_3 with length $2m + 2n$.

$$G_3 = \left(\begin{array}{c|c|c|c} P & O & O & Q \\ O & R & S & O \end{array}\right).$$

The minimum distance of the code constructed by the matrix is $\min\{d(C_1), d(C_2)\}$.

Proof.

Consider that,

$$G_3G_3^T = \left(\begin{array}{c|c|c|c} P & O & O & Q \\ \hline O & R & S & O \end{array}\right)\left(\begin{array}{c|c} P^T & O \\ \hline O & R^T \\ \hline O & S^T \\ \hline Q^T & O \end{array}\right) = O \text{ and } G_3(G_3^r)^T \left(\begin{array}{c|c|c|c} P & O & O & Q \\ \hline O & R & S & O \end{array}\right)\left(\begin{array}{c|c} (Q^r)^T & O \\ \hline O & (S^r)^T \\ \hline O & (R^r)^T \\ \hline (P^r)^T & O \end{array}\right) = O.$$

Hence, the code C_3 is a reversible self-dual code of length $2m + 2n$. The code C_3 can be expressed as $C_3 = \{\mathbf{x}G_3 | \mathbf{x} \in F_q^{m+n}\}$. According to G_3, the minimum distance of C_3 can be obtained if

$$\mathbf{x} = (x_1\ x_2\ \cdots\ x_m \mid \mathbf{0}) = (x_1\ x_2\ \cdots\ x_m \mid \mathbf{0}) \text{ or } \mathbf{x} = (\mathbf{0} | x_{m+1}\ x_{m+2}\ \cdots\ x_{m+n}).$$

The resulting codewords are

$\mathbf{c} = ((x_1\ x_2\ \cdots\ x_m)P|\mathbf{0}|(x_1\ x_2\ \cdots\ x_m)Q)$ or $\mathbf{c} = (\mathbf{0}|(x_{m+1}\ x_{m+2}\ \cdots\ x_{m+n})R|(x_{m+1}\ x_{m+2}\ \cdots\ x_{m+n})S|\mathbf{0})$. Note that for $(x_1\ x_2\ \cdots\ x_m)$ and $(x_{m+1}\ x_{m+2}\ \cdots\ x_{m+n})$ can each be represented as elements of F_q^m and F_q^m, respectively. Then, $(x_1\ x_2\ \cdots\ x_m)P|(x_1\ x_2\ \cdots\ x_m)Q \in C_1$ and $(x_{m+1}\ x_{m+2}\ \cdots\ x_{m+n})R|(x_{m+1}\ x_{m+2}\ \cdots\ x_{m+n})S \in C_2$. Since the remaining $2m$ digits or $2n$ digits are zero, then the Hamming weight of each codeword in the code is equal to the Hamming weight in C_1 or C_2, the minimum distance of the code is $\min\{d(C_1), d(C_2)\}$. ■

In contrast to Theorem 6, in Theorem 7, the new reversible self-dual code that is constructed has a shorter digit length. Moreover, the code is constructed by combining partitions of each digit from the previous code.

Example 6. Given reversible self-dual codes C_1 and C_2 of length 4 and 8 over the field F_5 with the following generator matrix.

$$G_1 = (P|Q) = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 3 \end{pmatrix} = \left(\begin{array}{ccc|c} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 3 \end{array}\right) \text{ and}$$

$$G_2 = (R\,|S) = \left(\begin{array}{ccccc|ccc} 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \end{array}\right).$$

The minimum distance of each code is equal to 2. Thus, the new reversible self-dual code of length 12 has the following generator matrix,

$$G_3 = \left(\begin{array}{c|c|c|c} P & O & O & Q \\ \hline O & R & S & O \end{array}\right) = \left(\begin{array}{ccc|ccccc|ccc|c} 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 \end{array}\right).$$

The minimum distance of the code is equal to 2.

CONCLUSIONS

Based on the results, it can be concluded that the reversible self-dual codes over the field F_q with characteristic no equal to 2 exists if their length is greater than or equal 4. Additionally, a new reversible self-dual code can be constructed from either self-dual codes or reversible self-dual codes. Finally, the minimum distance of the constructed code is related to the distance of previous generated codes. In this article, the application of the constructed codes and the error correction algorithms has not yet been provided. Therefore, future research can focus on developing their applications and the error correction algorithms.

REFERENCES

[1] C. E. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.

[2] S. Ling and C. Xing, *Coding Theory: A First Course*, 1st ed. Cambridge University Press, 2004. doi: 10.1017/CBO9780511755279.

[3] M. J. Golay, "Notes on digital coding," *Proc IEEE*, vol. 37, p. 657, 1949.

[4] E. Nachmani, E. Marciano, L. Lugosch, W. J. Gross, D. Burshtein, and Y. Be'ery, "Deep Learning Methods for Improved Decoding of Linear Codes," *IEEE J. Sel. Top. Signal Process.*, vol. 12, no. 1, pp. 119–131, Feb. 2018, doi: 10.1109/JSTSP.2017.2788405.

[5] S. Bouyuklieva and M. Harada, "[No title found]," *Des. Codes Cryptogr.*, vol. 28, no. 2, pp. 163–169, 2003, doi: 10.1023/A:1022588407585.

[6] M. Grass and T. A. Gulliver, "On self-dual MDS codes," in *2008 IEEE International Symposium on Information Theory*, Toronto, ON, Canada: IEEE, Jul. 2008, pp. 1954–1957. doi: 10.1109/ISIT.2008.4595330.

[7] M. Grassl and T. A. Gulliver, "On circulant self-dual codes over small fields," *Des. Codes Cryptogr.*, vol. 52, no. 1, pp. 57–81, Jul. 2009, doi: 10.1007/s10623-009-9267-1.

[8] Y. H. Park, "The classification of self-dual modular codes," *Finite Fields Their Appl.*, vol. 17, no. 5, pp. 442–460, Sep. 2011, doi: 10.1016/j.ffa.2011.02.010.

[9] M. Shi, L. Sok, P. Solé, and S. Çalkavur, "Self-dual codes and orthogonal matrices over large finite fields," *Finite Fields Their Appl.*, vol. 54, pp. 297–314, Nov. 2018, doi: 10.1016/j.ffa.2018.08.011.

[10] L. Sok, "Explicit Constructions of MDS Self-Dual Codes," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3603–3615, Jun. 2020, doi: 10.1109/TIT.2019.2954877.

[11] J.-L. Kim and W.-H. Choi, "Self-Dual Codes, Symmetric Matrices, and Eigenvectors," *IEEE Access*, vol. 9, pp. 104294–104303, 2021, doi: 10.1109/ACCESS.2021.3099434.

[12] W. H. Choi and J. L. Kim, "An improved upper bound on self-dual codes over finite fields GF(11), GF(19), and GF(23)," *Des. Codes Cryptogr.*, vol. 90, no. 11, pp. 2735–2751, Nov. 2022, doi: 10.1007/s10623-021-00968-3.

[13] J. L. Massey, "Reversible codes," *Inf. Control*, vol. 7, no. 3, pp. 369–380, Sep. 1964, doi: 10.1016/S0019-9958(64)90438-3.

[14] Y. Takishima, M. Wada, and H. Murakami, "Reversible variable length codes," *IEEE Trans. Commun.*, vol. 43, no. 2/3/4, pp. 158–162, Feb. 1995, doi: 10.1109/26.380026.

[15] X. T. Ngo, S. Bhasin, J.-L. Danger, S. Guilley, and Z. Najm, "Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses," in *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Washington, DC: IEEE, May 2015, pp. 82–87. doi: 10.1109/HST.2015.7140242.

[16] P. K. Kadbe and M. G. Waje, "Error Detection in Fault-Tolerant Reversible Circuit Using Fredkin Gates," in *ICCCE 2021*, vol. 828, A. Kumar and S. Mozar, Eds., in Lecture Notes in Electrical Engineering, vol. 828. , Singapore: Springer Nature Singapore, 2022, pp. 579–585. doi: 10.1007/978-981-16-7985-8_58.

[17] H. J. Kim, W.-H. Choi, and Y. Lee, "Construction of reversible self-dual codes," *Finite Fields Their Appl.*, vol. 67, p. 101714, Oct. 2020, doi: 10.1016/j.ffa.2020.101714.

[18] H. J. Kim, W.-H. Choi, and Y. Lee, "Designing DNA codes from reversible self-dual codes over G F (4)," *Discrete Math.*, vol. 344, no. 1, p. 112159, Jan. 2021, doi: 10.1016/j.disc.2020.112159.