Finite Fields and Their Applications 67 (2020) 101714

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Construction of reversible self-dual codes

Hyun Jin Kim [a,1], Whan-Hyuk Choi [b,c,*,2], Yoonjin Lee [d,3]

[a] *University College, Yonsei University, 85 Songdogwahak-ro, Yeonsu-gu, Incheon, 21983, Republic of Korea*
[b] *Department of Mathematics, Kangwon National University, 1 Gangwondaehakgil, Chuncheon, 24341, Republic of Korea*
[c] *Department of Mathematics, Sogang University, 35 Baekbeom-ro, Seoul 04107, Republic of Korea*
[d] *Department of Mathematics, Ewha Womans University, 11-1 Daehyun-Dong, Seodaemun-Gu, Seoul, 03760, Republic of Korea*

ARTICLE INFO

Article history:
Received 16 June 2019
Received in revised form 27 April 2020
Accepted 25 June 2020
Available online 14 July 2020
Communicated by Chaoping Xing

MSC:
primary 94B05
secondary 11T71

ABSTRACT

We study a construction method of binary reversible self-dual codes in this paper. Reversible codes have good properties in applications, and it is interesting to note that a class of reversible codes is closely connected to BCH codes and LCD codes. We first characterize binary reversible self-dual codes. Using these characteristics of reversible self-dual codes, we find an explicit method for constructing *all* the binary reversible self-dual codes up to equivalence. Furthermore, using this construction, we obtain nine *optimal* reversible self-dual codes of length 70 which are all inequivalent, and these codes are all *new* with respect to binary self-dual

* Corresponding author at: Department of Mathematics, Kangwon National University, 1 Gangwondaehakgil, Chuncheon, 24341, Republic of Korea.

E-mail addresses: guswls41@yonsei.ac.kr (H.J. Kim), whchoi@kangwon.ac.kr (W.-H. Choi), yoonjinl@ewha.ac.kr (Y. Lee).

[1] The author is supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2017R1D1A1B03028251).

[2] The author is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2018R1A6A3A01013052) and also by Basic Science Research Program through the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2019R1I1A1A01057755).

[3] The author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant No. 2019R1A6A1A11051177) and also by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (NRF-2017R1A2B2004574).

https://doi.org/10.1016/j.ffa.2020.101714
1071-5797/

Keywords:
Reversible code
Self-dual code
Automorphism
Equivalence
Optimal code

codes; they all have the same parameter $[70, 35, 12]$ and their automorphism groups have the same order two.

1. Introduction

Reversible codes were introduced by Massey [13], and it is known that they have some good properties in certain data storage and retrieval systems. Furthermore, some reversible codes have a good capability of correcting solid burst errors, and they have high transmission efficiency [15,18]. Recently, it is noted that reversible codes are very useful in applied mathematics such as cryptography [4,16] and bio-mathematics, especially DNA coding theory [8,12]; this is due to the fact that a DNA code was constructed by using reversible codewords of a linear code [6].

It is interesting to note that a class of reversible codes is closely connected to BCH codes and LCD codes. In fact, a class of reversible codes is an important subclass of BCH codes. In 1992, Massey introduced another class of codes, linear complementary dual codes (*LCD* codes for short) [14]; an LCD code is defined to be a linear code C whose dual code $C^\perp$ satisfies $C \cap C^\perp = \{0\}$. Massey and Yang proved that a cyclic code is an LCD code if and only if it is a reversible code [19]. Noting that a self-dual code C is defined to satisfy $C = C^\perp$, LCD codes and self-dual codes have an extreme contrast in terms of the intersection of C and its dual $C^\perp$. Moreover, a self-dual code is one of the major subjects in coding theory due to its variety of nice properties as codes. However, there has been no investigation on the self-duality of reversible codes yet as far as we know.

We study a construction method of binary reversible self-dual codes in this paper. We first characterize binary reversible self-dual codes. Using these characteristics of reversible self-dual codes, we find an explicit method for constructing *all* the binary reversible self-dual codes up to equivalence. We also introduce a notion of *R-equivalence* for reversible codes; this notion is distinguished from a usual notion of equivalence of codes. We show that a reversible self-dual code has a generator matrix in the standard form under the R-equivalence. We find an explicit method for constructing *all* the binary reversible self-dual codes up to R-equivalence. Furthermore, using this construction, we obtain nine *optimal* reversible self-dual codes of length 70 which are all inequivalent, and these codes are all *new* with respect to binary self-dual codes; they all have the same parameter $[70, 35, 12]$ and their automorphism groups have the same order two.

We discuss the comparison of our result with the result of Buyuklieva et al. [1,2]. In fact, reversible self-dual codes can be regarded as self-dual codes with an automorphism of order two without fixed points. Buyuklieva et al. obtained some interesting results on this class of codes [1,2]. However, we point out that there is some significant difference between their result and ours. First of all, we construct reversible self-dual codes of length $2n+2$ from reversible self-dual codes of length $2n$ taking it into consideration the equivalence relation between them. This is a *successive* construction in the sense that for finding all reversible self-dual codes of all even lengths, we can keep using this method by successively increasing lengths by two. On the other hand, Buyuklieva et al. focus on finding extremal self-dual codes of length $2n$ from self-orthogonal codes of length n in [1,2]; their construction is a *non-successive* one in the following sense. In their method, for construction of all extremal self-dual codes of length $2n$ one should search for all self-orthogonal codes of length n, and in order to find all extremal self-dual codes of length $2n+2$ one need all self-orthogonal codes of length $n+1$, and so forth; that is, each step has to be restarted. Furthermore, their construction is also involved with a heuristic algorithm, while our method is an explicit and deterministic one. Lastly, in our construction, it was a crucial issue to preserve the reversible form of self-dual codes due to their applications to DNA codes, while in their work, it was not necessary.

Our paper is organized as follows. We introduce some basic notions and definitions in Section 2. We then study various properties of reversible self-dual codes and define a notion of *R-equivalence* of reversible codes in Section 3; we prove some lemmas which are necessary for the proof of our main results in Section 4. Section 4 presents our main results, where we find a construction method of binary reversible self-dual codes, and we also show that every binary reversible self-dual code can be obtained by this method. In Section 5, we obtain nine new optimal reversible binary self-dual codes with parameter $[70, 35, 12]$ are presented. All computations are done using MAGMA [3].

2. Preliminaries

A binary linear code of length n is a subspace of $\mathbb{F}_2^n$. An element of code is called a *codeword*. The space $\mathbb{F}_2^n$ is equipped with the standard inner product, $\mathbf{x}\cdot\mathbf{y} = \sum_{i=1}^n x_i y_i$, where $\mathbf{x} = (x_i), \mathbf{y} = (y_i)$ are vectors in $\mathbb{F}_2^n$. Let $\mathcal{C}$ be a code of length n over $\mathbb{F}_2$. Then the *dual code* $\mathcal{C}^\perp$ is defined by

$$\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{F}_2^n \mid \mathbf{v}\cdot\mathbf{w} = 0 \text{ for all } \mathbf{w} \in C\}.$$

$\mathcal{C}$ is called *self-orthogonal* if $\mathcal{C} \subset \mathcal{C}^\perp$ and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$.

Two codes $\mathcal{C}$ and $\mathcal{C}'$ are called *permutation equivalent* and denoted by $\mathcal{C} \simeq \mathcal{C}'$ if one can be obtained from the other by a permutation of coordinates. A permutation $\sigma \in S_n$ is called an *automorphism* of $\mathcal{C}$ if $\mathcal{C} = \mathcal{C}\sigma$, where $\mathcal{C}\sigma = \{c\sigma \mid c \in \mathcal{C}\}$. The set of all automorphisms of $\mathcal{C}$ forms the automorphism group $\mathrm{Aut}(\mathcal{C})$ of $\mathcal{C}$. A code is called *reversible* if it is invariant as a set under a reversal of each codeword. In particular, a code $\mathcal{C}$ of length $2n$ for an integer n, $\mathcal{C}$ is reversible if $\mathcal{C} = \mathcal{C}\tau$ for $\tau = (1, 2n)(2, 2n-1)\cdots(k, 2n-k+1)\cdots(n, n+1) \in S_{2n}$. A self-dual code which is reversible is called a *reversible self-dual code*. Since any self-dual code has an even length $2n$ for an integer n, it is obvious that a self-dual code $\mathcal{C}$ is reversible self-dual if and only if $\tau \in \mathrm{Aut}(\mathcal{C})$.

Let A be a matrix of size $m \times n$ denoted by $(a_{ij})_{m\times n}$. Then A^T is the transpose of A, i.e., $A^T = (a_{ji})_{n\times m}$, A^F is the flip-transpose of A, which flips A across its anti-diagonal, i.e., $A^F = (a_{n-j+1,m-i+1})_{n\times m}$ and A^r is the column reversed matrix of A, i.e., $A^r = (a_{i,n-j+1})_{m\times n}$. These notations are also used on vectors regarding a vector $\mathbf{v} \in \mathbb{F}_2^n$ as a $1 \times n$ matrix over $\mathbb{F}_2$. Let I_n be the identity matrix and A be a square matrix of order n. Then a matrix A is called *orthogonal* if $AA^T = I_n$, A is called *symmetric* if $A = A^T$, and A is called *persymmetric* if $A = A^F$.

Let A and B be $n \times n$ matrices and R_n be the $n \times n$ anti-diagonal matrix whose anti-diagonal elements are all 1, i.e., $R_n = I_n^r$. Then the following properties are straightforward:

$$R_n^T = R_n^F = R_n, R_n^2 = I_n, A^F = R_n A^T R_n, A^r = AR_n,$$
$$(A^F)^F = A, (A^T)^F = (A^F)^T, (A+B)^F = A^F + B^F, (AB)^F = B^F A^F.$$

We use the following notations throughout this paper.

Notations

$\mathcal{C}$	a binary linear code
$\mathrm{Aut}(\mathcal{C})$	the automorphism group of $\mathcal{C}$
S_n	the symmetric group of degree n
τ	the permutation $(1, 2n)(2, 2n-1)\cdots(n, n+1) \in S_{2n}$
σ_i	a permutation $(i, 2n-i+1) \in S_{2n}$
$\sigma_{i,j}$	a permutation $(i, j)(2n-i+1, 2n-j+1) \in S_{2n}$
I_n	the identity matrix of degree n
R_n	the column reversed matrix of I_n
A^T	the transpose of a matrix A
A^F	the flip-transpose of a matrix A
A^r	the column reversed matrix of a matrix A

3. Some properties of reversible self-dual codes and their R-equivalence

In this section, we discuss some properties of reversible self-dual codes and introduce a notion of R-equivalence for reversible self-dual codes. We prove some lemmas which are necessary for the proof of our main results in Section 4.

A *generator matrix* of $\mathcal{C}$ is a matrix whose rows form a basis of $\mathcal{C}$. It is well-known that a self-dual code of length $2n$ over a field has a standard generator matrix, up to equivalence, in the following form:

$$\left(I_n \mid A \right), \tag{1}$$

where A is an $n \times n$ orthogonal matrix.

Lemma 3.1. *A dual code of a reversible code is also reversible.*

Proof. Let $\mathcal{C}$ be a reversible code. For any $\mathbf{u} \in \mathcal{C}^\perp$, we have that $\mathbf{u} \cdot \mathbf{x} = 0$ for all $\mathbf{x} \in \mathcal{C}$. This implies $\mathbf{u}^r \cdot \mathbf{x}^r = 0$ for all $\mathbf{x} \in \mathcal{C}$. Since $\mathcal{C}$ is reversible, $\mathbf{u}^r \cdot \mathbf{x} = 0$ for all $\mathbf{x} \in \mathcal{C}$. Therefore, $\mathbf{u}^r \in \mathcal{C}^\perp$. $\square$

Lemma 3.2. *Let A be an $n \times n$ binary matrix. Then any two of the following statements imply the third.*

(i) *A is orthogonal.*
(ii) $(A^r)^2 = I_n$.
(iii) *A is persymmetric.*

Proof. Assume that A is orthogonal. We then have that $A^{-1} = A^T$ and $R_n^{-1} = R_n$. Then

$$\begin{aligned}(A^r)^2 = I_n &\Leftrightarrow (AR_n)^{-1} = AR_n \\ &\Leftrightarrow R_n A^{-1} = AR_n \\ &\Leftrightarrow R_n(A^T) = AR_n \\ &\Leftrightarrow R_n A^T R_n = A \\ &\Leftrightarrow A^F = A.\end{aligned}$$

Now we show that (ii) and (iii) imply (i).
Assume that (ii) and (iii) hold. Then $A = A^F = R_n A^T R_n$ and

$$\begin{aligned}(A^r)^2 = I_n &\Rightarrow (AR_n)^{-1} = AR_n \\ &\Rightarrow R_n A^{-1} = (R_n A^T R_n)R_n \\ &\Rightarrow R_n A^{-1} = R_n A^T \\ &\Rightarrow A^{-1} = A^T \\ &\Rightarrow AA^T = I_n;\end{aligned}$$

thus A is orthogonal and this completes the proof. $\square$

Lemma 3.3. *Let $\mathcal{C}$ be a self-dual code of length $2n$ with generator matrix in the standard form $(I_n \mid A)$. Then $\mathcal{C}$ is reversible if and only if the matrix A satisfies one of the followings:*

(i) $(A^r)^2 = I_n$
(ii) *A is persymmetric.*

Proof. Suppose that a self-dual code $\mathcal{C}$ is reversible. Then the reversed generator matrix G of $\mathcal{C}$ with

$$G = \left(A^r \mid R_n \right)$$

generates $\mathcal{C}$ as well. Recall that A is orthogonal since $\mathcal{C}$ is self-dual; therefore, A is non-singular and so is A^r. Thus, $(A^r)^{-1}G$ is a generator matrix of $\mathcal{C}$ in the standard form since

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

We note that the row vectors of $(A^r)^{-1}G$ and those of $(I_n \mid A)$ generate the same code $\mathcal{C}$; this implies

$$(A^r)^{-1}R_n = A.$$

Thus, we have

$$(A^r)^{-1}R_n = A \;\Leftrightarrow\; (AR_n)^{-1} = AR_n \Leftrightarrow\; (A^r)^2 = I_n,$$

and hence (i) holds. By the previous lemma, (ii) also follows. The other direction follows immediately in a similar way. □

A code with generator matrix $(I_n \mid R_n)$ is also a reversible self-dual code of length $2n$; we call this code *the trivial reversible self-dual code*. Using these trivial codes, we obtain the following corollary.

Corollary 3.4. *There exist binary reversible self-dual codes for all even lengths.*

Corollary 3.5. *Let $J_n = (1)_{n\times n}$ be an $n \times n$ matrix over $\mathbb{F}_2$ consisting of all 1 entries. Then a code with generator matrix $(I_n \mid I_n + J_n)$ is a reversible self-dual code if and only if n is even.*

Proof. We note that $(J_n + I_n)(J_n + I_n)^T = J_nJ_n^T + I_n$ and $J_nJ_n^T + I_n$ is equal to I_n if and only if n is even. Thus, $\mathcal{C}$ is self-dual if and only if n is even. Clearly, $J_n + I_n$ is a persymmetric matrix for all n. By Lemma 3.3, $\mathcal{C}$ is a reversible self-dual code if and only if n is even. □

The following example shows that the class of reversible self-dual codes may contain some optimal codes. The extended Hamming [8,4,4] code and extremal self-dual codes of lengths 24 and 48 are also reversible self-dual codes up to equivalence, which can be shown by using Lemma 3.3.

Example 3.6. The extended Hamming [8,4,4] code is a binary reversible self-dual code of length 8. The generator matrix of extended Hamming [8,4] code is

$$\begin{pmatrix} I_4 \mid A \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

and we can check that the matrix A is orthogonal and persymmetric.

The extremal [24,12,8] extended Golay code is a reversible self-dual code with generator matrix $(I_n \mid A)$, where A is given as follows:

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

The extremal [48,24,12] extended quadratic residue code is also a reversible self-dual code with generator matrix $(I_n \mid A)$, where A is given as follows:

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

From now on, we discuss the equivalence of reversible codes. Equivalence of reversible codes is to be distinguished from a usual notion of equivalence of codes. The main reason why they should be distinguished is that a code which is equivalent to a reversible code may not be reversible any more. For example, we consider two codes $\mathcal{C}$ and $\mathcal{C}'$ generated by the matrices G and G', respectively:

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \text{ and } G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Clearly, the codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent to each other. However, the code $\mathcal{C}$ is a trivial reversible self-dual code, but the code $\mathcal{C}'$ is not reversible. We thus need to define a notion of equivalence which preserves reversibility of codes. Now we define a notion of *R-equivalence* of reversible codes as follows.

Definition 3.7. Let $\sigma_i = (i, 2n-i+1)$ and $\sigma_{i,j} = (i,j)(2n-i+1, 2n-j+1)$ be elements of the symmetric group S_{2n} for $1 \leq i,j \leq n$. Let $\mathcal{C}$ be a reversible code of length $2n$. Then any composition of these permutations acting on $\mathcal{C}$ preserves the reversibility. If two reversible codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent under permutations σ_i's and $\sigma_{i,j}$'s, then they are called *R-equivalent* and denoted by $\mathcal{C} \simeq_R \mathcal{C}'$.

In order to preserve the reversibility of code, we define *elementary row operations* (R1), (R2), and *reversible column permutations* (RC1), (RC2) on its generator matrix as follows.

(R1) Permutation of the rows.

(R2) Addition of a row to another.

(RC1) Permutation of the ith and the $(2n-i+1)$th columns for $1 \leq i \leq n$.

(RC2) Permutation of the ith and the jth columns and the $(2n-i+1)$th and the $(2n-j+1)$th columns simultaneously for $1 \leq i,j \leq n$.

We note that two codes are R-equivalent if and only if their generator matrices can be transformed from one to the other by elementary row operations and reversible column permutations (RC1) and (RC2).

Remark 3.8. In general, any linear code has a generator matrix in the standard form in (1) up to equivalence. However, it is not guaranteed that a reversible code has a generator matrix in the standard form in (1) up to R-equivalence. For example, the matrix

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

generates a reversible code; but there is no way to transform G to the standard form up to R-equivalence. We note that this code is not self-dual. The following Lemma 3.9 shows that if a reversible code is self-dual, then it always has a generator matrix in the standard form up to R-equivalence. We will use this lemma for the proof of our main Theorem 4.7.

Lemma 3.9. *Every reversible self-dual code of length $2n$ is R-equivalent to a reversible self-dual code which has a generator matrix in the standard form*

$$\begin{pmatrix} I_n & \mid & A \end{pmatrix},$$

where A is an orthogonal and persymmetric matrix.

Proof. Let $G = (M \mid N)$ be a generator matrix of a reversible self-dual code $\mathcal{C}$ of length $2n$, where M and N are $n \times n$ matrices. It is enough to show that by applying elementary row operations and reversible column permutations (RC1) and (RC2), G can be transformed to a matrix

$$G' = \begin{pmatrix} M' & \mid & N' \end{pmatrix}$$

with $rank(M') = n$.

Let

$$\mathscr{S} = \{\widetilde{G} \mid \widetilde{G} = (\widetilde{M} \mid \widetilde{N}) \simeq_R G\}$$

be a set of $n \times 2n$ matrices which are R-equivalent to G, where $\widetilde{M}$ and $\widetilde{N}$ are $n \times n$ matrices. We take $G' = (M' \mid N') \in \mathscr{S}$ such that $rank(M') \geq rank(\widetilde{M})$ for all $\widetilde{G} \in \mathscr{S}$. If $rank(M') = n$, then we are done. If $rank(M') = k < n$, then we will find a contradiction.

Now, assume that $rank(M') = k < n$. Applying the operations (R1), (R2) and (RC2), G' is transformed to a reduced echelon form:

$$G'' = \left(\begin{array}{c|c|c|c} I_k & A_{k\times(n-k)} & B_{k\times(n-k)} & C_{k\times k} \\ \hline O & O & D_{(n-k)\times(n-k)} & E_{(n-k)\times k} \end{array}\right).$$

The submatrix D must be a zero matrix; if D has a column which has a nonzero element, then applying the operation (RC1) to the column leads to a contradiction to the maximality of $rank(M')$. Thus we have

$$G'' = \left(\begin{array}{c|c|c|c} I_k & A_{k\times(n-k)} & B_{k\times(n-k)} & C_{k\times k} \\ \hline O & O & O & E_{(n-k)\times k} \end{array}\right).$$

Let $\mathbf{v}_i$ be the ith row vector of G''. Since G'' generates a reversible code with $rank(G'') = n$, $\mathbf{v}_{k+1}$ cannot be a zero vector. Hence, at least one of the last k elements of $\mathbf{v}_{k+1}$ is not zero. In other words, at least one of the first k elements of $\mathbf{v}_{k+1}^r$ is not zero; say that the jth element of $\mathbf{v}_{k+1}^r$ with $j \leq k$ is not zero. Then, $\mathbf{v}_j \cdot \mathbf{v}_{k+1}^r \neq 0$ whereas two vectors $\mathbf{v}_j$ and $\mathbf{v}_{k+1}^r$ are also codewords in $\mathcal{C}$; this contradicts the self-duality of $\mathcal{C}$. The result thus follows as desired. □

4. Construction methods

In this section, we present some construction methods of reversible self-dual codes. We start with some basic construction methods.

Proposition 4.1.

(i) *Let G be a generator matrix of a self-dual code of length n. Then*

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

generates a reversible self-dual code of length $2n$.

(ii) *(Direct sum of reversible codes) Let $(A \mid B)$ and $(C \mid D)$ be generator matrices of a reversible self-dual code of length $2n$ and $2m$, respectively, where A and B are $n \times n$ matrices, and C and D are $m \times m$ matrices. Then the direct sum of these two codes*

$$\left(\begin{array}{c|c} A & B \end{array}\right) \oplus_R \left(\begin{array}{c|c} C & D \end{array}\right) := \left(\begin{array}{c|c|c|c} A & O & O & B \\ \hline O & C & D & O \end{array}\right)$$

generates a reversible self-dual code of length $2n + 2m$.

The following proposition shows that every trivial reversible self-dual code of length $2n + 2$ is constructed from the trivial reversible self-dual code of length $2n$.

Proposition 4.2. *The trivial reversible self-dual code of length $2n + 2$ has the generator matrix:*

$$(I_{n+1} \mid R_{n+1}) = (1, 1) \oplus_R (I_n \mid R_n)$$

The following theorem is the main result, which shows a construction method for binary reversible self-dual codes.

Theorem 4.3. *Let $(I_n \mid A)$ be a generator matrix of a binary reversible self-dual code of length $2n$ and a column vector $\mathbf{x} = (x_i)$ be an eigenvector of A^r with odd weight, and let $E = \mathbf{x}\mathbf{x}^F$. Then*

$$G' = \left(\begin{array}{c|c|c|c} I_n & O & \mathbf{x} & A + E \\ \hline O & 1 & 0 & \mathbf{x}^F \end{array}\right)$$

generates a reversible self-dual code of length $2n + 2$.

Proof. Let

$$A' = \left(\begin{array}{c|c} \mathbf{x} & A + E \\ \hline 0 & \mathbf{x}^F \end{array}\right).$$

Then clearly A' is a persymmetric matrix. By Lemma 3.3, it is sufficient to show that G' generates a self-dual code. Since G' is in the standard form (1), we will show that A' is orthogonal.

We note that $AA^T = I_n$ and $\mathbf{x} = (x_i)$ is an eigenvector of A^r with odd weight; this implies that

$$\mathbf{x}^F(\mathbf{x}^F)^T \equiv 1 \pmod 2$$

and

$$E(\mathbf{x}^F)^T = (\mathbf{x}\mathbf{x}^F)(\mathbf{x}^F)^T = \mathbf{x}(\mathbf{x}^F(\mathbf{x}^F)^T) = \mathbf{x},\ A(\mathbf{x}^F)^T = A(R\mathbf{x}) = (AR)\mathbf{x} = A^r\mathbf{x} = \mathbf{x}.$$

Thus,

$$\begin{aligned}
A'(A')^T &= \left(\begin{array}{c|c} \mathbf{x} & A+E \\ \hline 0 & \mathbf{x}^F \end{array}\right) \left(\begin{array}{c|c} \mathbf{x} & A+E \\ \hline 0 & \mathbf{x}^F \end{array}\right)^T \\
&= \left(\begin{array}{c|c} \mathbf{x} & A+E \\ \hline 0 & \mathbf{x}^F \end{array}\right) \left(\begin{array}{c|c} \mathbf{x}^T & 0 \\ \hline A^T+E^T & (\mathbf{x}^F)^T \end{array}\right) \\
&= \left(\begin{array}{c|c} \mathbf{x}\mathbf{x}^T + AA^T + AE^T + EA^T + EE^T & A(x^F)^T + E(\mathbf{x}^F)^T \\ \hline \mathbf{x}^F A^T + \mathbf{x}^F E^T & \mathbf{x}^F(\mathbf{x}^F)^T \end{array}\right) \\
&= \left(\begin{array}{c|c} I_n + (AE^T + EA^T) + (\mathbf{x}\mathbf{x}^T + EE^T) & \mathbf{x}+\mathbf{x} \\ \hline \mathbf{x}^T + \mathbf{x}^T & 1 \end{array}\right).
\end{aligned}$$

Clearly, $\mathbf{x}\mathbf{x}^T$ is symmetric, and AE^T is also symmetric since

$$AE^T = A(\mathbf{x}\mathbf{x}^F)^T = A(\mathbf{x}^F)^T\mathbf{x}^T = \mathbf{x}\mathbf{x}^T.$$

Thus

$$AE^T + EA^T = AE^T + (AE^T)^T = 2AE^T = O,$$

and

$$EE^T = (\mathbf{x}\mathbf{x}^F)(\mathbf{x}\mathbf{x}^F)^T = \mathbf{x}((\mathbf{x}^F)(\mathbf{x}^F)^T)\mathbf{x}^T = \mathbf{x}\mathbf{x}^T.$$

Therefore,

$$\mathbf{x}\mathbf{x}^T + EE^T = 2\mathbf{x}\mathbf{x}^T = O.$$

Finally, we have

$$
\begin{aligned}
A'(A')^T &= \left(\begin{array}{c|c} I_n + O + O & 2\mathbf{x} \\ \hline 2\mathbf{x}^T & 1 \end{array}\right) \\
&= \left(\begin{array}{c|c} I_n & \mathbf{0} \\ \hline \mathbf{0} & 1 \end{array}\right) \\
&= I_{n+1};
\end{aligned}
$$

hence G' generates a self-dual code, and the result follows. $\square$

Remark 4.4. The construction method in Theorem 4.3 seems restrictive since the input vectors $\mathbf{x}$ should be chosen to be eigenvectors. However, Theorem 4.7 shows that all non-trivial binary reversible self-dual codes can be constructed by using this method. We note that every eigenvector has the eigenvalue 1 in Theorem 4.3, Lemma 4.5, and Theorem 4.7.

For the proof of Theorem 4.7, we need Lemma 4.5 and Lemma 4.6 as the following.

Lemma 4.5. *Let $\mathcal{C}$ be a reversible self-dual code with generator matrix in the standard form:*

$$
\left(\begin{array}{c|c|c|c} I_n & O & \mathbf{x} & A \\ \hline O & 1 & 0 & \mathbf{x}^F \end{array}\right).
$$

Then $\mathbf{x}$ is an eigenvector of $(A+E)^r$ with odd weight, where $E = \mathbf{x}\mathbf{x}^F$.

Proof. Since $\mathcal{C}$ is self-dual, we have that

$$
\left(\begin{array}{c|c} \mathbf{x} & A \\ \hline 0 & \mathbf{x}^F \end{array}\right)\left(\begin{array}{c|c} \mathbf{x} & A \\ \hline 0 & \mathbf{x}^F \end{array}\right)^T = \left(\begin{array}{c|c} \mathbf{x} & A \\ \hline 0 & \mathbf{x}^F \end{array}\right)\left(\begin{array}{c|c} \mathbf{x}^T & 0 \\ \hline A^T & (\mathbf{x}^F)^T \end{array}\right) = I_{n+1}.
$$

This implies that $\mathbf{x}\mathbf{x}^T + AA^T = I_n$, $A(\mathbf{x}^F)^T = \mathbf{0}$ and $\mathbf{x}^F(\mathbf{x}^F)^T = 1$.

The weight of $\mathbf{x}$ is odd since

$$
wt(\mathbf{x}) = wt(\mathbf{x}^F) \equiv \mathbf{x}^F \cdot \mathbf{x}^F = \mathbf{x}^F(\mathbf{x}^F)^T = 1 \pmod 2.
$$

Furthermore, $\mathbf{x}$ is an eigenvector of $(A + \mathbf{x}\mathbf{x}^F)^r$ since

$$
\begin{aligned}
(A + \mathbf{x}\mathbf{x}^F)^r\mathbf{x} &= (A + \mathbf{x}\mathbf{x}^F)R\mathbf{x} \\
&= (A + \mathbf{x}\mathbf{x}^F)(\mathbf{x}^F)^T \\
&= A(\mathbf{x}^F)^T + (\mathbf{x}\mathbf{x}^F)(\mathbf{x}^F)^T
\end{aligned}
$$

$$= 0 + \mathbf{x}(\mathbf{x}^F(\mathbf{x}^F)^T)$$
$$= \mathbf{x}. \quad \square$$

Lemma 4.6. *Let $\mathcal{C}$ be a non-trivial reversible self-dual code. Then $\mathcal{C}$ is R-equivalent to a reversible self-dual code with generator matrix*

$$\left(I_n \mid A \right),$$

where $a_{n,1} = 0$ for $A = (a_{i,j})$.

Proof. Let $(I_n \mid B)$ be a generator matrix of $\mathcal{C}$, where $B = (b_{i,j})$. Then we consider the following two cases: there is a zero in the anti-diagonal entries of the matrix B or not.

Case 1. $b_{k,n-k+1} = 0$ for some k.

By interchanging the kth row and the nth row of the generator matrix of $\mathcal{C}\sigma_{k,n}$, we get the generator matrix of the form

$$\left(I_n \mid A \right),$$

where $a_{n,1} = 0$, and then we are done.

Case 2. $b_{k,n-k+1} = 1$ for all k.

Since $\mathcal{C}$ is a non-trivial reversible self-dual code, B has a nonzero element except anti-diagonal entries. Without loss of generality, we assume that the last row vector of B is $(1, \mathbf{x}^F)$, where the jth element of $\mathbf{x}$ is nonzero, i.e.,

$$G = \left(I_n \mid B \right) = \left(\begin{array}{c|c|c|c} I_{n-1} & O & \mathbf{x} & B_{n-1} \\ \hline O & 1 & 1 & \mathbf{x}^F \end{array} \right),$$

where $b_{n,n-j+1} = 1$. By adding the last row to every other ith row wherever $x_i = 1$, we get the matrix

$$G' = \left(\begin{array}{c|c|c|c} I_{n-1} & \mathbf{x} & O & B_{n-1} + E \\ \hline O & 1 & 1 & \mathbf{x}^F \end{array} \right),$$

where $E = \mathbf{x}\mathbf{x}^F$. We note that the ith anti-diagonal element of E is x_i^2; thus the jth anti-diagonal element of $B_{n-1} + E$ is $1 + x_j^2 = 0$. Applying $\sigma_n = (n, n+1) \in S_{2n}$ to G', the R-equivalent matrix of G' is as follows:

$$G'\sigma_n = \left(\begin{array}{c|c|c|c} I_{n-1} & O & \mathbf{x} & B_{n-1} + E \\ \hline O & 1 & 1 & \mathbf{x}^F \end{array} \right)$$

and letting

$$B' = (b'_{i,j}) = \left(\begin{array}{c|c} \mathbf{x} & B_{n-1}+E \\ \hline 1 & \mathbf{x}^F \end{array}\right),$$

we get the generator matrix in the standard form

$$\left(\begin{array}{c|c} I_n & B' \end{array}\right),$$

where the jth anti-diagonal element $b_{j,n-j+1} = 0$. Consequently, the result follows by the similar argument as the case 1. □

Theorem 4.7. *Any non-trivial binary reversible self-dual code of length* $2n$ *can be constructed from some binary reversible self-dual code of length* $2n-2$ *by the construction method in Theorem 4.3.*

Proof. Let $\mathcal{C}$ be a non-trivial reversible self-dual code of length $2n$ with generator matrix

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

where $A = (a_{i,j})$ and persymmetric. By Lemma 4.6, we may assume that $a_{n,1} = 0$, i.e.,

$$G = \left(\begin{array}{c|c|c|c} I_{n-1} & O & \mathbf{x} & A' \\ \hline O & 1 & 0 & \mathbf{x}^F \end{array}\right),$$

where A' is a persymmetric matrix of degree $n-1$. By Lemma 4.5 the vector $\mathbf{x}^F$ is an eigenvector of $(A'+E)^r$ with odd weight, where $E = \mathbf{x}\mathbf{x}^F$. Then

$$G = \left(\begin{array}{c|c|c|c} I_{n-1} & \mathbf{x} & \mathbf{x} & A'+E \\ \hline O & 1 & 0 & \mathbf{x}^F \end{array}\right),$$

and clearly, $A'+E$ is persymmetric, and the submatrix

$$\left(\begin{array}{c|c|c|c} I_{n-1} & \mathbf{x} & \mathbf{x} & A'+E \end{array}\right)$$

generates a self-orthogonal code. By puncturing the two identical nth and $(n+1)$th columns we obtain a standard generator matrix

$$\left(\begin{array}{c|c} I_{n-1} & A'+E \end{array}\right)$$

of a reversible self-dual code of length $2n-2$, and this proves the result. □

5. New optimal binary self-dual codes

In this section, we present nine *new optimal* reversible self-dual codes of length 70; they are all *new* binary self-dual codes according to the data in [5,7,9,10,20].

Theorem 5.1. *There are at least nine inequivalent optimal reversible self-dual* $[70, 35, 12]$ *codes, which are computed by using our construction given in Theorem 4.3. They are all new with respect to binary self-dual codes. Moreover, their automorphism groups have the same order two.*

It is known [17] that if a self-dual $[24s + 2t, 12s + t, d]$ code exists for $0 \leq t \leq 11$, then

$$d \leq \begin{cases} 4s+4 & \text{if } t < 11, \\ 4s+6 & \text{if } t = 11. \end{cases}$$

In fact, for the code length $n = 70$, extremal codes should have minimum weight 14 from the bound above; however, their existence is not known yet. Consequently, all the $[70, 35, 12]$ binary self-dual codes we obtained have the largest minimum weight so far.

According to [9], all possible weight enumerators of binary self-dual $[70, 35, 12]$ codes have the following forms:

$$\begin{aligned} W_{70,1} &= 1 + 2\beta y^{12} + (11730 - 2\beta - 128\gamma)y^{14} + (150535 - 22\beta + 896\gamma)y^{16} + \cdots, \\ W_{70,2} &= 1 + 2\beta y^{12} + (9682 - 2\beta)y^{14} + (173063 - 22\beta)y^{16} + \cdots, \end{aligned}$$

where β and γ are integer parameters.

All the generator matrices of nine inequivalent self-dual $[70, 35, 12]$ codes we obtained are listed presented in the web [11] due to lack of space. They are all new self-dual codes based on [5,7,9,10,20]. Furthermore, all of them have the same automorphism group of order 2, and they have the weight enumerator form $W_{70,1}$ with the following parameters:

$$\gamma = 0,\ \beta = 282,\ 292,\ 312,\ 318,\ 328;$$

$$\gamma = 2,\ \beta = 328,\ 332,\ 344;$$

$$\gamma = 4,\ \beta = 324.$$

Now, we show four of our computation results by writing the submatrix A of the standard form (1). These codes have the weight enumerator form $W_{70,1}$ with the parameters $\beta = 332, 282, 324, 312$ and $\gamma = 2, 0, 4, 0$, respectively.

$$\begin{pmatrix}
0111110001001000101010100110110000 \\
0101111110111011111101010001100000000 \\
1010111110001100011111010111000010 0 \\
1011001100111010001100111000101100 0 \\
1101100001100011110110100000101110 00 \\
0111101011010011111010111101001000 1 \\
0000001011010100000101110110000100 1 \\
1100000110111010101100100111011011 0 \\
1100000110101000011111111001100011 1 \\
1100000110111011000010001101110010 1 \\
1100000110111010110000001011001010 00 \\
0000000011000110101100001010110110 0 \\
0000001011001010001011100011111101 1 \\
0000001011010011111000100010100010 0 \\
1111100010111101101110100110011011 1 \\
1100000110111010011110010011101110 0 \\
0000001000101001001111110011010111 1 \\
1001101110000111000101001010011011 0 \\
0011010011000111000011011001011001 1 \\
1111010010111001111011000100011001 0 \\
0001011110010010011010111110101110 10 \\
0010111011001010110010010000100011 0 \\
1010001001011101001110101111000110 1 \\
0101111101001001000111001101110101 0 \\
1111110111000011001110001111001101 0 \\
1110000111111100100001110000111001 1 \\
0100101111100101110111111111110010 0 \\
1111001011110010010100001111000111 0 \\
1101010110011110011001100000110111 0 \\
0000011000110111100000000000000011 1 \\
0110000010110100010010000000001101 11 \\
0001001100110011110010000000001110 11 \\
0000100101101101100010000000001011 01 \\
1000101111110001000110001111011001 1 \\
0100001101101001010110001111001110 0
\end{pmatrix},
\begin{pmatrix}
0110000110100001111000100110000111 0 \\
1101101111001101101001011111100000 1 \\
0000111011110011100100100111000100 1 \\
0010101011111100100010100100010111 01 \\
1100000110111010111110101101001100 0 \\
0001100011000101010111000001000000 00 \\
1010011110011011100100001010100101 0 \\
1101100001100011100100101011001011 0 \\
1101100001110001010111110101110011 1 \\
0001111100111011000110000010001011 1 \\
0001111100111010110100011001101101 0 \\
0001110100101111111110001010000001 0 \\
0001111100100011011001100011001010 1 \\
0001111100111010101010100010010101 0 \\
0100000001000101101010101011001100 00 \\
1101100001100011010110011111111110 0 \\
1101100010011001010001110000001001 1 \\
0010001110110001111110111010011000 1 \\
0011000000110011101000101100110101 11 \\
1011001101101010101111011011111011 11 \\
0000101011001101100111111101101010 0 \\
0010101001101010100000001000001000 10 \\
1111110011000111001011011100101101 0 \\
1001110010110000011001001110101110 0 \\
0100010111110101110101111111001110 1 \\
1010011000101111100100000001101011 10 \\
0011000010111010011010000000011111 1 \\
1011010100100001010001111100101001 1 \\
1100110001000111010001101100100111 0 \\
1010001101111000000000111110010001 00 \\
0011101000011110001101111111010111 0 \\
0100100110011001101101111111010001 0 \\
0000110111001101110000000000010010 01 \\
1001001000101000001110000011001001 1 \\
0100011101011001001100000001110100 10
\end{pmatrix},$$

$$\begin{pmatrix}
0110000110100001111000100110000111 0 \\
0001110010010100100101011100000100 11 \\
1011001110100000110111011111111110 1 \\
0010101011111100100010100100010111 01 \\
1011101110110000100001010110011111 0 \\
1010010110010110000100111010111010 0 \\
1101110110010001111011110001110110 0 \\
0001111100111010101000101000100010 0 \\
0001111100101000011011110110011010 1 \\
0001111100111011000110000010001011 1 \\
1010001001101001100111100001010111 0 \\
1010000001111100101101110010111011 0 \\
1010001001110000000101001101111000 01 \\
1010001001101001111001011010101111 0 \\
1111110111011000000110101110100010 0 \\
0001111100111010011010011100010111 0 \\
0001111111000000001110111001110000 01 \\
1001111011100010101101000010100010 1 \\
0011000000110011101000101100110101 11 \\
1100100101100000100001001100100100 1 \\
1011011110011110110100000101010000 00 \\
0010101001101010100000001000001000 10 \\
0011101110011110000111011111000100 0 \\
1110011010111010000110110101111101 0 \\
0100010111110101110101111111001110 1 \\
1101110000100101111011111000000100 0 \\
0011000010111010011010000000011111 1 \\
1100111100101011001110000111111010 1 \\
0000101100011110011101101111001110 0 \\
1101100101110010011110000111110001 0 \\
1000011101001101011110000111101101 0 \\
1111010011001010111110000111101011 0 \\
1011000010011110100011111000011110 1 \\
0101010101110001000010000000010000 01 \\
0011110101010011010011111000111010 0
\end{pmatrix},
\begin{pmatrix}
1001001111111111111000110100010001 00 \\
1001000100110101010011101101010011 0 \\
1001011100101010001101101001100111 1 \\
1100110011011111010011111001110010 0 \\
0111100110100011101101010001000000 00 \\
0110011110000101001000111101100101 0 \\
0110000000111110100100000100101011 01 \\
1111100111101110001100011001111111 0 \\
0001111110010111111011110110000000 00 \\
0001111110000100100110000010010001 0 \\
0001111110000101010100011001110111 1 \\
1111101111111011011010111011011100 0 \\
1111100111110111111101010010010111 1 \\
0001111110000101001010100010001111 1 \\
0010101101000001100111010110000101 0 \\
1111100111101110111110101101001010 0 \\
0001111101111111111101110011111010 0 \\
0100100001111011001100111010000101 1 \\
0010010010100000101110100110001000 1 \\
1110110111101010011011111010111101 1 \\
1111100001100001011100110011001110 1 \\
0101010111011000001101101111110101 1 \\
1010001010110101011100010001100110 1 \\
0100111111011100011000110010100101 1 \\
1011011110101011111100110001101011 1 \\
1110110011010111011110110001100100 1 \\
0010010001111101100101111111011100 1 \\
0111001000110101001111111111011011 1 \\
1110110100111000000101101111001001 01 \\
1000001011110101101001001110010110 0 \\
0011101001010011011111111111001100 0 \\
0100100100100110001101111111001011 1 \\
1110101111101011100110110001111000 0 \\
1011001101010111010100110001111100 0 \\
0110011001101011000100110001000111 1
\end{pmatrix}.$$

Acknowledgment

We thank an anonymous referee for his/her helpful comments, which improved the clarity of this paper.

References

[1] S. Buyuklieva, On the binary self-dual codes with an automorphism of order 2, Des. Codes Cryptogr. 12 (1) (1997) 39–48.
[2] S. Buyuklieva, I. Boukliev, Extremal self-dual codes with an automorphism of order 2, IEEE Trans. Inf. Theory 44 (1) (1998) 323–328.
[3] J. Cannon, C. Playoust, An Introduction to Magma, University of Sydney, Sydney, Australia, 1994.
[4] C. Carlet, S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, in: Coding Theory and Applications, Springer, Cham, 2015, pp. 97–105.
[5] R. Dontcheva, New binary $[70, 35, 12]$ self-dual and binary $[72, 36, 12]$ self-dual doubly-even codes, Serdica Math. J. 27 (4) (2001) 287–302.
[6] P. Gaborit, O.D. King, Linear constructions for DNA codes, Theor. Comput. Sci. 334 (1) (2005) 99–113.
[7] T.A. Gulliver, M. Harada, Classification of extremal double circulant self-dual codes of lengths 64 to 72, Des. Codes Cryptogr. 13 (3) (1998) 257–269.
[8] F. Gursoy, E.S. Oztas, I. Siap, Reversible DNA codes using skew polynomial rings, Appl. Algebra Eng. Commun. Comput. 28 (2017) 311–320.
[9] M. Harada, The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes, Finite Fields Appl. 3 (1997) 131–139.
[10] H.J. Kim, Y. Lee, Extremal quasi-cyclic self-dual codes over finite fields, Finite Fields Appl. 52 (2018) 301–318.
[11] Y. Lee, http://math.ewha.ac.kr/~yoonjinl/RSDC.pdf, 2018.
[12] J. Liang, L. Wang, On cyclic DNA codes over $\mathbb{F}_2 + u\mathbb{F}_2$, J. Appl. Math. Comput. 51 (2016) 81–91.
[13] J.L. Massey, Reversible codes, Inf. Control 7 (1964) 369–380.
[14] J.L. Massey, Linear codes with complementary duals, Discrete Math. 106 (1992) 337–342.
[15] S.K. Muttoo, S. Lal, A reversible code over $GF(q)$, Kybernetika 22 (1986) 85–91.
[16] X.T. Ngo, S. Bhasin, J.-L. Danger, S. Guilley, 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), IEEE, 2015, pp. 82–87.
[17] E.M. Rains, Shadow bounds for self-dual codes, IEEE Trans. Inf. Theory 44 (1998) 134–139.
[18] Y. Takishima, M. Wada, H. Murakami, Reversible variable length codes, IEEE Trans. Commun. 43 (1995) 158–162.
[19] X. Yang, J.L. Massey, The condition for a cyclic code to have a complementary dual, Discrete Math. 126 (1994) 391–393.
[20] N. Yankov, M.-H. Lee, M. Gürel, M. Ivanova, Self-dual codes with an automorphism of order 11, IEEE Trans. Inf. Theory 61 (3) (2015) 1188–1193.