



New binary self-dual codes of lengths 80, 84 and 96 from composite matrices

Joe Gildea¹ · Adrian Korban¹ · Adam Michael Roberts¹

Received: 19 April 2021 / Revised: 19 August 2021 / Accepted: 8 November 2021 /
Published online: 19 December 2021
© The Author(s) 2021

Abstract

In this work, we apply the idea of composite matrices arising from group rings to derive a number of different techniques for constructing self-dual codes over finite commutative Frobenius rings. By applying these techniques over different alphabets, we construct best known singly-even binary self-dual codes of lengths 80, 84 and 96 as well as doubly-even binary self-dual codes of length 96 that were not known in the literature before.

Keywords Self-dual codes · Group rings · Codes over rings · Best known codes

Mathematics Subject Classification 94B0 · 16S34 · 15B10 · 15B33

1 Introduction

Self-dual codes form a family of widely studied linear codes which have many interesting properties and are intimately connected with many mathematical structures such as designs, lattices, modular forms and sphere packings. In recent history, much work has particularly been invested in developing techniques to construct extremal and optimal binary self-dual codes. The most famous of these techniques is quite possibly the pure double circulant construction, which utilises a generator matrix of the form $G = (I_n | A)$ where I_n is the $n \times n$ identity matrix and A is an $n \times n$ circulant matrix. It follows that G is a generator matrix of a self-dual $[2n, n]$ code if and only if $AA^T = -I_n$. This technique has since been generalised by assuming a generator matrix of the form $G = (I_n | \sigma(v))$ where σ is an isomorphism

Communicated by V. A. Zinoviev.

✉ Adam Michael Roberts
adamichaelroberts@outlook.com

Joe Gildea
j.gildea@chester.ac.uk

Adrian Korban
adrian3@windowslive.com

¹ Department of Physical, Mathematical and Engineering Sciences, University of Chester, Exton Park, Chester CH1 4AR, UK

from a group ring to the ring of matrices which was introduced in [23]. The isomorphism σ is such that G is a generator matrix of a self-dual $[2n, n]$ code if and only if v is unitary (see Sect. 2.4 for more details). Recent applications of this isomorphism in constructing self-dual codes can be seen in [1,8,15,16].

In this work, we assume a generator matrix of the form $G = (I_n | \Omega(v))$ where $\Omega(v)$ is a matrix that arises from group rings which we call a composite matrix. It clearly follows that $(I_n | \Omega(v))$ is a generator matrix of a self-dual code if and only if $\Omega(v)\Omega(v)^T = -I_n$. The idea of composite matrices was first introduced in [11] as a way of generalising the structure of $\sigma(v)$. The primary motivation for employing this technique is obtaining codes whose structures are atypical compared with those of codes constructed by more classical techniques. The main problem we face when attempting to construct codes with such a generator matrix is choosing parameters in such a way that allows for structural complexity of $\Omega(v)$ while also allowing for a reasonable set of necessary and sufficient conditions for the satisfaction of $\Omega(v)\Omega(v)^T = -I_n$.

Using generator matrices of the form $(I_n | \Omega(v))$ for a number of different composite matrices $\Omega(v)$, we find many self-dual codes with weight enumerator parameters of previously unknown values (relative to referenced sources). In total, 361 new codes are found, including 28 singly-even binary self-dual [80, 40, 14] codes, 107 binary self-dual [84, 42, 14] codes, 105 singly-even binary self-dual [96, 48, 16] codes and 121 doubly-even binary self-dual [96, 48, 16] codes.

The rest of the work is organised as follows. In Sect. 2, we give preliminary definitions on self-dual codes, Gray maps, circulant matrices and the alphabets we use. We also prove a few results concerning a simple matrix transformation, which we use in two of the composite matrix definitions. In Sect. 3, we define the composite matrices which we utilise in our constructions and we also prove the necessary and sufficient conditions needed by each construction to produce a self-dual code. In Sect. 4, we apply the constructions to obtain the new self-dual codes of length 80, 84 and 96 whose weight enumerator parameter values and automorphism group orders we detail. We also tabulate the results in this section. We finish with concluding remarks and discussion of possible expansion on this work.

2 Preliminaries

2.1 Self-dual codes

Let R be a commutative Frobenius ring. We consider codes over Frobenius due to their good duality properties, which are reflected by the equivalent statements in the following theorem given in [31].

Theorem 2.1 ([31]) *If R is a finite ring, then the following are equivalent*

- (i) R is a Frobenius ring,
- (ii) As a left module, $\widehat{R} \cong {}_R R$,
- (iii) As a right module, $\widehat{R} \cong R_R$.

See [5] for a full description of Frobenius rings and codes over Frobenius rings. Throughout this work, we always assume R has unity. A code C of length n over R is a subset of R^n whose elements are called codewords. If C is a submodule of R^n , then we say that C is linear. Let $\mathbf{x}, \mathbf{y} \in R^n$ where $\mathbf{x} = (x_1, x_2, \dots, x_n)$ and $\mathbf{y} = (y_1, y_2, \dots, y_n)$. The (Euclidean) dual

C^\perp of C is given by

$$C^\perp = \{ \mathbf{x} \in R^n : \langle \mathbf{x}, \mathbf{y} \rangle = 0, \forall \mathbf{y} \in C \},$$

where $\langle \cdot, \cdot \rangle$ denotes the Euclidean inner product defined by

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i y_i.$$

We say that C is self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$.

A binary self-dual code C is said to be *doubly-even* (Type II), if all codewords $\mathbf{c} \in C$ have weight $w(\mathbf{c}) \equiv 0 \pmod{4}$, otherwise C is said to be *singly-even* (Type I).

An upper bound on the minimum (Hamming) distance of a doubly-even binary self-dual code was given in [27] and likewise for a singly-even binary self-dual code in [28]. Let $d_I(n)$ and $d_{II}(n)$ be the minimum distance of a singly-even and doubly-even binary self-dual code of length n , respectively. Then

$$d_{II}(n) \leq 4\lfloor n/24 \rfloor + 4$$

and

$$d_I(n) \leq \begin{cases} 4\lfloor n/24 \rfloor + 2, & n \equiv 0 \pmod{24}, \\ 4\lfloor n/24 \rfloor + 4, & n \not\equiv 22 \pmod{24}, \\ 4\lfloor n/24 \rfloor + 6, & n \equiv 22 \pmod{24}. \end{cases}$$

A self-dual code whose minimum distance meets its corresponding bound is called *extremal*. A self-dual code with the highest possible minimum distance for its length is said to be *optimal*. Extremal codes are necessarily optimal but optimal codes are not necessarily extremal. A *best known* self-dual code is a self-dual code with the highest known minimum distance for its length.

2.2 Alphabets

In this paper, we consider the alphabets $\mathbb{F}_2, \mathbb{F}_2 + u\mathbb{F}_2$ and \mathbb{F}_4 .

Define

$$\mathbb{F}_2 + u\mathbb{F}_2 = \{ a + bu : a, b \in \mathbb{F}_2, u^2 = 0 \}.$$

Then $\mathbb{F}_2 + u\mathbb{F}_2$ is a commutative ring of order 4 and characteristic 2 such that $\mathbb{F}_2 + u\mathbb{F}_2 \cong \mathbb{F}_2[u]/\langle u^2 \rangle$.

We define $\mathbb{F}_4 \cong \mathbb{F}_2[\omega]/\langle \omega^2 + \omega + 1 \rangle$ so that

$$\mathbb{F}_4 = \{ a\omega + b(1 + \omega) : a, b \in \mathbb{F}_2, \omega^2 + \omega + 1 = 0 \}.$$

We recall the following Gray maps from [7,13]:

$$\begin{aligned} \varphi_{\mathbb{F}_2 + u\mathbb{F}_2} : (\mathbb{F}_2 + u\mathbb{F}_2)^n &\rightarrow \mathbb{F}_2^{2n} \\ a + bu &\mapsto (b, a + b), \quad a, b \in \mathbb{F}_2^n, \end{aligned}$$

$$\begin{aligned} \psi_{\mathbb{F}_4} : \mathbb{F}_4^n &\rightarrow \mathbb{F}_2^{2n} \\ a\omega + b(1 + \omega) &\mapsto (a, b), \quad a, b \in \mathbb{F}_2^n. \end{aligned}$$

Note that these Gray maps preserve orthogonality in their respective alphabets. The Lee weight of a codeword is defined to be the Hamming weight of its binary image under any of the aforementioned Gray maps. A self-dual code in R^n where R is equipped with a Gray map to the binary Hamming space is said to be of Type II if the Lee weights of all codewords are multiples of 4, otherwise it is said to be of Type I.

Proposition 2.2 ([7]) *Let C be a code over $\mathbb{F}_2 + u\mathbb{F}_2$. If C is self-orthogonal, then $\varphi_{\mathbb{F}_2 + u\mathbb{F}_2}(C)$ is self-orthogonal. The code C is a Type I (resp. Type II) code over $\mathbb{F}_2 + u\mathbb{F}_2$ if and only if $\varphi_{\mathbb{F}_2 + u\mathbb{F}_2}(C)$ is a Type I (resp. Type II) code over \mathbb{F}_2 . The minimum Lee weight of C is equal to the minimum Hamming weight of $\varphi_{\mathbb{F}_2 + u\mathbb{F}_2}(C)$.*

Proposition 2.3 ([13]) *Let C be a code over \mathbb{F}_4 . If C is self-orthogonal, then $\psi_{\mathbb{F}_4}(C)$ is self-orthogonal. The code C is a Type I (resp. Type II) code over \mathbb{F}_4 if and only if $\psi_{\mathbb{F}_4}(C)$ is a Type I (resp. Type II) code over \mathbb{F}_2 . The minimum Lee weight of C is equal to the minimum Hamming weight of $\psi_{\mathbb{F}_4}(C)$.*

The next two corollaries follow directly from Propositions 2.2 and 2.3, respectively.

Corollary 2.4 *Let C be a self-dual code over $\mathbb{F}_2 + u\mathbb{F}_2$ of length n and minimum Lee distance d . Then $\varphi_{\mathbb{F}_2 + u\mathbb{F}_2}(C)$ is a binary self-dual $[2n, n, d]$ code. Moreover, the Lee weight enumerator of C is equal to the Hamming weight enumerator of $\varphi_{\mathbb{F}_2 + u\mathbb{F}_2}(C)$. If C is a Type I (resp. Type II) code, then $\varphi_{\mathbb{F}_2 + u\mathbb{F}_2}(C)$ is a Type I (resp. Type II) code.*

Corollary 2.5 *Let C be a self-dual code over \mathbb{F}_4 of length n and minimum Lee distance d . Then $\psi_{\mathbb{F}_4}(C)$ is a binary self-dual $[2n, n, d]$ code. Moreover, the Lee weight enumerator of C is equal to the Hamming weight enumerator of $\psi_{\mathbb{F}_4}(C)$. If C is a Type I (resp. Type II) code, then $\psi_{\mathbb{F}_4}(C)$ is a Type I (resp. Type II) code.*

2.3 Special matrices

We now recall the definitions and properties of some special matrices which we use in our work. We begin by defining a matrix transformation whose properties we utilise in some of the composite constructions we consider.

The following proposition is trivial and therefore the proof is omitted.

Proposition 2.6 *Let A be $n \times n$ matrix over a commutative ring R . Let $\star : R^{n \times n} \rightarrow R^{n \times n}$ be the transformation such that A^\star is defined to be the matrix obtained after circularly shifting the columns of A to the right by one position. If*

$$P = \begin{pmatrix} \mathbf{0} & I_{n-1} \\ 1 & \mathbf{0} \end{pmatrix},$$

then $A^\star = AP$.

The matrix P as defined in Proposition 2.6 is a permutation matrix and is therefore orthogonal, i.e. $PP^T = I_n$. To see this, we have

$$P^T = \begin{pmatrix} \mathbf{0} & 1 \\ I_{n-1} & \mathbf{0} \end{pmatrix},$$

which corresponds to P after circularly shifting its columns to the right by $n - 2$ places and so by Proposition 2.6 we have $P^T = P P^{n-2} = P^{n-1}$. Clearly, if we circularly shift the columns of $P^T = P^{n-1}$ to the right by one place we obtain I_n so that $P^T P = P^{n-1} P = P^n = I_n$.

It also follows that $(P^k)^T = P^{-k \pmod n}$ for $k \in \mathbb{N}$. We can easily prove this by induction on $k \in \mathbb{N}$. The cases $k = 0$ and $k = 1$ are trivial. Assume $(P^k)^T = P^{-k \pmod n}$. Then we have $(P^{k+1})^T = (P^k P)^T = P^T (P^k)^T = P^{n-1} P^{-k \pmod n} = P^{n-k-1 \pmod n} = P^{-(k+1) \pmod n}$ which concludes our induction step.

We also have the following properties which are easy to prove.

Lemma 2.7 *Let A and B be $n \times n$ matrices over a commutative ring R where $n \geq 2$ and let \star be the transformation defined in Proposition 2.6.*

- (i) $(A + B)^\star = A^\star + B^\star$.
- (ii) $AB^T = A^\star B^{\star T}$.

Proof (i) By Proposition 2.6, we have $(A + B)^\star = (A + B)P = AP + BP = A^\star + B^\star$.

(ii) By Proposition 2.6 and the fact that P is orthogonal, we have $A^\star B^{\star T} = AP(BP)^T = AP P^T B^T = A(I_n)B^T = AB^T$. □

Let $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in R^n$ where R is a commutative ring and let

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}.$$

Then A is an $n \times n$ matrix called the *circulant* matrix generated \mathbf{a} , denoted by $A = \text{circ}(\mathbf{a})$.

If $A = \text{circ}(a_0, a_1, \dots, a_{n-1})$, then we see that $A = a_0 I_n + a_1 I_n^\star + a_2 (I_n^\star)^\star + \dots$ and so on. Using Proposition 2.6 and the properties of the matrix P , it follows that $A = \sum_{i=0}^{n-1} a_i P^i$. Clearly, the sum of any two circulant matrices is also a circulant matrix. If $B = \text{circ}(\mathbf{b})$ where $\mathbf{b} = (b_0, b_1, \dots, b_{n-1}) \in R^n$, then $AB = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j P^{i+j}$. Since $P^n = I_n$ there exist $c_k \in R$ such that $AB = \sum_{k=0}^{n-1} c_k P^k$ so that AB is also circulant. In fact, it is true that

$$c_k = \sum_{[i+j]_n=k} a_i b_j = \mathbf{x}_1 \mathbf{y}_{k+1}$$

for $k \in \{0, \dots, n - 1\}$, where \mathbf{x}_i and \mathbf{y}_i respectively denote the i^{th} row and column of A and B and $[i + j]_n$ denotes the smallest non-negative integer such that $[i + j]_n \equiv i + j \pmod n$. From this, we can see that circulant matrices commute multiplicatively. We also see that A^T is circulant such that $A^T = \sum_{i=0}^{n-1} a_i (P^i)^T = \sum_{i=0}^{n-1} a_i P^{n-i}$.

Lemma 2.8 *Let A be an $n \times n$ matrix over a commutative ring R where $n \geq 2$ and let \star be the transformation defined in Proposition 2.6. Let B be an $n \times n$ circulant matrix over R .*

- (i) $BP = PB$.
- (ii) $(AB^T)^\star = A^\star B^T$.
- (iii) $(AB^{\star T})^\star = AB^T$.

Proof (i) Let $B = \text{circ}(b_0, b_1, \dots, b_{n-1})$. Then B can be expressed as $B = \sum_{i=0}^{n-1} b_i P^i$ and so it is obvious that $BP = PB$.

(ii) Since B is circulant, then B^T is circulant and so by (i), we have $(AB^T)^\star = (AB^T)P = A(B^T P) = (AP)B^T = A^\star B^T$.

(iii) Since B is circulant, then B^T is circulant and so by (i) and the fact that P is orthogonal, we have $(AB^{\star T})^\star = (A(BP)^T)P = AP^T B^T P = AP^T P B^T = A(I_n)B^T = AB^T$. □

Let J_n be an $n \times n$ matrix over R whose (i, j) th entry is 1 if $i + j = n + 1$ and 0 if otherwise. Then J_n is called the $n \times n$ exchange matrix and corresponds to the row-reversed (or column-reversed) version of I_n . Note that $[i + j]_n$ corresponds to the $(i + 1, j + 1)$ th entry of the matrix $J_n V$ where $V = \text{circ}(n - 1, 0, 1, \dots, n - 2)$ for $i, j \in \{0, \dots, n - 1\}$.

Let A_0, A_1, \dots, A_{k-1} be $m \times n$ matrices over R and let

$$X = \begin{pmatrix} A_0 & A_1 & A_2 & \cdots & A_{k-1} \\ A_{k-1} & A_0 & A_1 & \cdots & A_{k-2} \\ A_{k-2} & A_{k-1} & A_0 & \cdots & A_{k-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_1 & A_2 & A_3 & \cdots & A_0 \end{pmatrix}.$$

Then X is an $km \times kn$ matrix called the *block circulant* matrix generated A_0, A_1, \dots, A_{k-1} , denoted by $X = \text{CIRC}(A_0, A_1, \dots, A_{k-1})$.

2.4 Group rings and composite matrices

In this section, we recall the basic definition of a finite group ring and proceed to define the concept of a composite matrix.

Let G be a finite group order n and let R be a finite commutative Frobenius ring. Let $RG = \{\sum_{i=1}^n \alpha_{g_i} g_i : \alpha_{g_i} \in R, g_i \in G\}$ and define addition in RG by

$$\sum_{i=1}^n \alpha_{g_i} g_i + \sum_{i=1}^n \beta_{g_i} g_i = \sum_{i=1}^n (\alpha_{g_i} + \beta_{g_i}) g_i$$

and define multiplication in RG by

$$\sum_{i=1}^n \alpha_{g_i} g_i \cdot \sum_{j=1}^n \beta_{g_j} g_j = \sum_{k=1}^n \left(\sum_{i,j:g_i g_j = g_k} \alpha_{g_i} \beta_{g_j} \right) g_k.$$

Then RG is called the group ring of G over R and is a ring with respect to the aforementioned definitions of addition and multiplication.

Let (g_1, g_2, \dots, g_n) be a fixed listing of the elements of G with $g_1 = 1$ and let $v = \sum_{i=1}^n \alpha_{g_i} g_i \in RG$. Define $\sigma(v)$ to be the $n \times n$ matrix whose (i, j) th entry is α_{g_k} where $g_k = g_i^{-1} g_j$ for $i, j \in \{1, \dots, n\}$, i.e.

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1} g_1} & \alpha_{g_1^{-1} g_2} & \cdots & \alpha_{g_1^{-1} g_n} \\ \alpha_{g_2^{-1} g_1} & \alpha_{g_2^{-1} g_2} & \cdots & \alpha_{g_2^{-1} g_n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1} g_1} & \alpha_{g_n^{-1} g_2} & \cdots & \alpha_{g_n^{-1} g_n} \end{pmatrix}.$$

The matrix $\sigma(v)$ was first given in [23] wherein it was proved that σ is an isomorphism from the ring RG to $R^{n \times n}$. It follows that $\sigma(v)\sigma(v)^T = -I_n$ if and only if $vv^* = -1$ where $v^* = \sum_{i=1}^n \alpha_{g_i} g_i^{-1}$. When R is of characteristic 2, we see that $\sigma(v)\sigma(v)^T = I_n$ if and only if $vv^* = 1$, i.e. v is unitary with respect to the involution $*$.

Suppose now that $n > 1$ is composite and let r be a fixed integer such that $r \mid n : 1 < r < n$ and let $m = n/r$. Let $\{H_1, H_2, \dots, H_\eta\}$ be a collection of η groups of order r . Let H_t be a representative of one of these groups for $t \in \{1, \dots, \eta\}$ and let $(h_{t:1}, h_{t:2}, \dots, h_{t:r})$ be a fixed listing of the elements of H_t with $h_{t:1} = 1$. Let H' be an $m \times m$ matrix whose (y, z) th entry

is $h'_{y,z} \in \{1, \dots, \eta\}$ for $y, z \in \{1, \dots, m\}$ and let P' be an $m \times m$ matrix whose $(y, z)^{\text{th}}$ entry is $p'_{y,z} \in \mathbb{F}_2$ for $y, z \in \{1, \dots, m\}$. Define the mapping $\varrho(y, z, i, j) = g_{r(y-1)+i}^{-1} g_{r(z-1)+j}$ for $y, z \in \{1, \dots, m\}$ and $i, j \in \{1, \dots, r\}$.

Define $Z_{y,z}$ to be the $r \times r$ matrix whose $(i, j)^{\text{th}}$ entry is given by

$$z_{y,z|i,j} = \alpha_{\varrho(y,z,i,j)}$$

and define $Z'_{t;y,z}$ to be the $r \times r$ matrix whose $(i, j)^{\text{th}}$ entry is given by

$$z'_{t;y,z|i,j} = \alpha_{\varrho(y,z,1,\mathcal{M}_{H_t}(i,j))},$$

where $\mathcal{M}_{H_t}(i, j)$ is the $(i, j)^{\text{th}}$ entry of the matrix of integers $\ell \in \{1, \dots, r\}$ such that $h_{t:\ell} = h_{t:i}^{-1} h_{t:j}$.

Define $\Omega(v)$ to be the block matrix whose $(y, z)^{\text{th}}$ block entry is given by

$$\omega_{y,z} = \begin{cases} Z_{y,z}, & p'_{y,z} = 0, \\ Z'_{h'_{y,z}:y,z}, & p'_{y,z} = 1. \end{cases}$$

Then $\Omega(v)$ is an $n \times n$ matrix composed of m^2 blocks of size $r \times r$ which we call the composite $(G, H_1, H_2, \dots, H_\eta)$ -matrix of $v \in RG$ with respect to H' and P' . If $P' = \mathbf{0}$ (i.e. the $m \times m$ zero matrix), the matrix $\Omega(v)$ reduces to $\sigma(v)$.

The concept of composite matrices defined in this way was first introduced in [11] as a way of generalising the structure of $\sigma(v)$. See [9,10,26] for recent applications of composite matrices in constructing binary self-dual codes.

Example 2.9 Let $G \cong D_4 \cong \langle a, b \mid a^4 = b^2 = 1, bab = a^{-1} \rangle$ with the fixed listing $G = (g_{4j+i+1}) = a^i b^j$ for $i \in \{0, \dots, 3\}$ and $j \in \{0, 1\}$. Then $G = (g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8) = (1, a, a^2, a^3, b, ab, a^2b, a^3b)$. We have $n = 8$ and suppose we let $r = 4 \mid n$ so that $m = n/r = 2$. Let $\{H_1, H_2\}$ be a collection of groups of order $r = 4$. Let $H_1 \cong C_2 \times C_2 \cong \langle c, d \mid c^2 = d^2 = 1, cd = dc \rangle$ with the fixed listing $H_1 = (h_{1:2j+i+1}) = c^i d^j$ for $i \in \{0, 1\}$ and $j \in \{0, 1\}$. Then $H_1 = (h_{1:1}, h_{1:2}, h_{1:3}, h_{1:4}) = (1, c, d, cd)$. Let $H_2 \cong C_{2,2} \cong \langle e \mid e^{2,2} = 1 \rangle$ with the fixed listing $H_2 = (h_{2:2j+i+1}) = e^{2i+j}$ for $i \in \{0, 1\}$ and $j \in \{0, 1\}$. Then $H_2 = (h_{2:1}, h_{2:2}, h_{2:3}, h_{2:4}) = (1, e^2, e, e^3)$. Let

$$H' = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

and let $P' = \mathbf{1}$ (i.e. the 2×2 matrix of ones). Let $v = \sum_{i=1}^8 \alpha_{g_i} g_i \in RG$ and let $\Omega(v)$ be the composite (G, H_1, H_2) -matrix of $v \in RG$ with respect to H' and P' . We have

$$\Omega(v) = \begin{pmatrix} \omega_{1,1} & \omega_{1,2} \\ \omega_{2,1} & \omega_{2,2} \end{pmatrix} = \begin{pmatrix} Z'_{h'_{1,1}:1,1} & Z'_{h'_{1,2}:1,2} \\ Z'_{h'_{2,1}:2,1} & Z'_{h'_{2,2}:2,2} \end{pmatrix} = \begin{pmatrix} Z'_{1:1,1} & Z'_{2:1,2} \\ Z'_{2:2,1} & Z'_{1:2,2} \end{pmatrix}$$

and we also find that

$$\mathcal{M}_{H_1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad \text{and} \quad \mathcal{M}_{H_2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 1 & 2 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

By definition, the $(i, j)^{\text{th}}$ entry of $Z'_{1:1,1}$ is given by $\alpha_{\varrho(1,1,1,\mathcal{M}_{H_1}(i,j))}$ where $\varrho(1, 1, 1, \mathcal{M}_{H_1}(i, j)) = g_1^{-1}g\mathcal{M}_{H_1}(i, j) = g\mathcal{M}_{H_1}(i, j)$ so that

$$Z'_{1:1,1} = \begin{pmatrix} \alpha_{g_1} & \alpha_{g_2} & \alpha_{g_3} & \alpha_{g_4} \\ \alpha_{g_2} & \alpha_{g_1} & \alpha_{g_4} & \alpha_{g_3} \\ \alpha_{g_3} & \alpha_{g_4} & \alpha_{g_1} & \alpha_{g_2} \\ \alpha_{g_4} & \alpha_{g_3} & \alpha_{g_2} & \alpha_{g_1} \end{pmatrix}$$

and similarly we find that

$$Z'_{2:1,2} = \begin{pmatrix} \alpha_{g_5} & \alpha_{g_6} & \alpha_{g_7} & \alpha_{g_8} \\ \alpha_{g_6} & \alpha_{g_5} & \alpha_{g_8} & \alpha_{g_7} \\ \alpha_{g_8} & \alpha_{g_7} & \alpha_{g_5} & \alpha_{g_6} \\ \alpha_{g_7} & \alpha_{g_8} & \alpha_{g_6} & \alpha_{g_5} \end{pmatrix},$$

$$Z'_{2:2,1} = \begin{pmatrix} \alpha_{g_5} & \alpha_{g_8} & \alpha_{g_7} & \alpha_{g_6} \\ \alpha_{g_8} & \alpha_{g_5} & \alpha_{g_6} & \alpha_{g_7} \\ \alpha_{g_6} & \alpha_{g_7} & \alpha_{g_5} & \alpha_{g_8} \\ \alpha_{g_7} & \alpha_{g_6} & \alpha_{g_8} & \alpha_{g_5} \end{pmatrix},$$

$$Z'_{1:2,2} = \begin{pmatrix} \alpha_{g_1} & \alpha_{g_4} & \alpha_{g_3} & \alpha_{g_2} \\ \alpha_{g_4} & \alpha_{g_1} & \alpha_{g_2} & \alpha_{g_3} \\ \alpha_{g_3} & \alpha_{g_2} & \alpha_{g_1} & \alpha_{g_4} \\ \alpha_{g_2} & \alpha_{g_3} & \alpha_{g_4} & \alpha_{g_1} \end{pmatrix}.$$

Therefore, we obtain

$$\Omega(v) = \begin{pmatrix} Z'_{1:1,1} & Z'_{2:1,2} \\ Z'_{2:2,1} & Z'_{1:2,2} \end{pmatrix} = \begin{pmatrix} A_1 & A_2 & B_1 & B_2 \\ A_2 & A_1 & B_2J_2 & B_1 \\ C_1 & C_2 & D_1 & D_2 \\ C_2J_2 & C_1 & D_2 & D_1 \end{pmatrix}$$

where $A_1 = \text{circ}(\alpha_{g_1}, \alpha_{g_2})$, $A_2 = \text{circ}(\alpha_{g_3}, \alpha_{g_4})$, $B_1 = \text{circ}(\alpha_{g_5}, \alpha_{g_6})$, $B_2 = \text{circ}(\alpha_{g_7}, \alpha_{g_8})$, $C_1 = \text{circ}(\alpha_{g_5}, \alpha_{g_8})$, $C_2 = \text{circ}(\alpha_{g_7}, \alpha_{g_6})$ and $D_1 = \text{circ}(\alpha_{g_1}, \alpha_{g_4})$, $D_2 = \text{circ}(\alpha_{g_3}, \alpha_{g_2})$.

3 Composite matrix constructions

In this section, we present our constructions which assume a generator matrix of the form $(I_n | \Omega(v))$ where $\Omega(v)$ is a composite matrix. For each construction, we first define the structure of the corresponding composite matrix $\Omega(v)$ and subsequently prove the conditions that hold if and only if $(I_n | \Omega(v))$ is a generator matrix of a self-dual $[2n, n]$ code over R . We will hereafter assume that R is a finite commutative Frobenius ring of characteristic 2. For each $v = \sum_{i=1}^n \alpha_{g_i} g_i \in RG$ that we define, we denote $\mathbf{v} = (v_1, v_2, \dots, v_n) = (\alpha_{g_1}, \alpha_{g_2}, \dots, \alpha_{g_n})$ where \mathbf{v}_i denotes $v_i = \alpha_{g_i}$ for $i \in \{1, \dots, n\}$. We also use the following notation

$$\mathbf{v}_{i:j} = \begin{cases} (v_i, v_{i+1}, v_{i+2}, \dots, v_{j-1}, v_j), & i < j, \\ (v_i, v_{i-1}, v_{i-2}, \dots, v_{j+1}, v_j), & i > j, \end{cases}$$

for $i, j \in \{1, \dots, n\}$. We also let $\text{circ}(\mathbf{u}, \mathbf{v})$ denote $\text{circ}(u_1, u_2, \dots, u_n, v_1, v_2, \dots, v_n)$ for any $\mathbf{u}, \mathbf{v} \in R^n$ such that $\mathbf{u} = (u_1, u_2, \dots, u_n)$ and $\mathbf{v} = (v_1, v_2, \dots, v_n)$.

Definition 3.1 Let $G \cong D_{10} \cong \langle a, b \mid a^{10} = b^2 = 1, bab = a^{-1} \rangle$ with the fixed listing $G = (g_{10j+i+1}) = a^i b^j$ for $i \in \{0, \dots, 9\}$ and $j \in \{0, 1\}$. Let $H \cong D_5 \cong \langle c, d \mid c^5 =$

$d^2 = 1, dcd = c^{-1}$) with the fixed listing $H = (h_{5j+i+1}) = a^i b^j$ for $i \in \{0, \dots, 4\}$ and $j \in \{0, 1\}$. Let $H' = \mathbf{1}$ and $P' = \mathbf{1}$. Let $v = \sum_{i=1}^{20} \alpha_{g_i} g_i \in RG$. If $\Omega_1^{20}(v)$ is the composite (G, H) -matrix of $v \in RG$ with respect to H' and P' , then

$$\Omega_1^{20}(v) = \begin{pmatrix} A_1 & B_1 & C_1 & D_1 \\ B_1^T & A_1^T & D_1^T & C_1^T \\ C_2 & D_2 & A_2 & B_2 \\ D_2^T & C_2^T & B_2^T & A_2^T \end{pmatrix},$$

where $A_1 = \text{circ}(\mathbf{v}_{1:5}), B_1 = \text{circ}(\mathbf{v}_{6:10}), C_1 = \text{circ}(\mathbf{v}_{11:15}), D_1 = \text{circ}(\mathbf{v}_{16:20}), A_2 = \text{circ}(\mathbf{v}_1, \mathbf{v}_{10:7}), B_2 = \text{circ}(\mathbf{v}_{6:2}), C_2 = \text{circ}(\mathbf{v}_{11}, \mathbf{v}_{20:17})$ and $D_2 = \text{circ}(\mathbf{v}_{16:12})$.

Theorem 3.2 *Let $G = (I \mid \Omega_1^{20}(v))$ where $\Omega_1^{20}(v)$ is as defined in Definition 3.1. Then G is a generator matrix of a self-dual code of length 40 over R if and only if*

$$\begin{cases} A_1 A_1^T + B_1 B_1^T + C_1 C_1^T + D_1 D_1^T = I_5, \\ A_2 A_2^T + B_2 B_2^T + C_2 C_2^T + D_2 D_2^T = I_5, \\ A_1 C_2^T + B_1 D_2^T + C_1 A_2^T + D_1 B_2^T = \mathbf{0}, \\ A_1 D_2 + B_1 C_2 + C_1 B_2 + D_1 A_2 = \mathbf{0}. \end{cases}$$

Proof We know that G is a generator matrix of a self-dual code of length 40 over R if and only if $\Omega_1^{20}(v)\Omega_1^{20}(v)^T = I_{20}$. We find that

$$\Omega_1^{20}(v)\Omega_1^{20}(v)^T = \begin{pmatrix} X_1 & \mathbf{0} & Y_1 & Y_2 \\ \mathbf{0} & X_1 & Y_2^T & Y_1^T \\ Y_1^T & Y_2 & X_2 & \mathbf{0} \\ Y_2^T & Y_1 & \mathbf{0} & X_2 \end{pmatrix},$$

where

$$\begin{aligned} X_1 &= A_1 A_1^T + B_1 B_1^T + C_1 C_1^T + D_1 D_1^T, \\ X_2 &= A_2 A_2^T + B_2 B_2^T + C_2 C_2^T + D_2 D_2^T \end{aligned}$$

and

$$\begin{aligned} Y_1 &= A_1 C_2^T + B_1 D_2^T + C_1 A_2^T + D_1 B_2^T, \\ Y_2 &= A_1 D_2 + B_1 C_2 + C_1 B_2 + D_1 A_2. \end{aligned}$$

Clearly, $Y_i = \mathbf{0}$ if and only if $Y_i^T = \mathbf{0}$ for $i \in \{1, 2\}$. Thus, $\Omega_1^{20}(v)\Omega_1^{20}(v)^T = I_{20}$ if and only if

$$\begin{cases} X_1 = X_2 = I_5, \\ Y_1 = Y_2 = \mathbf{0}. \end{cases}$$

□

Definition 3.3 Let $G \cong C_5 \times C_4 \cong \langle a, b \mid a^5 = b^4 = 1, ab = ba \rangle$ with the fixed listing $G = (g_{5j+i+1}) = a^i b^j$ for $i \in \{0, \dots, 4\}$ and $j \in \{0, \dots, 3\}$. Let $H \cong D_5 \cong \langle c, d \mid c^5 = d^2 = 1, dcd = c^{-1} \rangle$ with the fixed listing $H = (h_{5j+i+1}) = a^i b^j$ for $i \in \{0, \dots, 4\}$ and $j \in \{0, 1\}$. Let $H' = \mathbf{1}$ and $P' = \mathbf{1}$. Let $v = \sum_{i=1}^{20} \alpha_{g_i} g_i \in RG$. If $\Omega_2^{20}(v)$ is the composite

(G, H) -matrix of $v \in RG$ with respect to H' and P' , then

$$\Omega_2^{20}(v) = \begin{pmatrix} A & B & C & D \\ B^T & A^T & D^T & C^T \\ C & D & A & B \\ D^T & C^T & B^T & A^T \end{pmatrix},$$

where $A = \text{circ}(\mathbf{v}_{1:5})$, $B = \text{circ}(\mathbf{v}_{6:10})$, $C = \text{circ}(\mathbf{v}_{11:15})$ and $D = \text{circ}(\mathbf{v}_{16:20})$.

Theorem 3.4 *Let $G = (I \mid \Omega_2^{20}(v))$ where $\Omega_2^{20}(v)$ is as defined in Definition 3.3. Then G is a generator matrix of a self-dual code of length 40 over R if and only if*

$$\begin{cases} AA^T + BB^T + CC^T + DD^T = I_5, \\ AC^T + BD^T + CA^T + DB^T = \mathbf{0}. \end{cases}$$

Proof We know that G is a generator matrix of a self-dual code of length 40 over R if and only if $\Omega_2^{20}(v)\Omega_2^{20}(v)^T = I_{20}$. We find that

$$\Omega_2^{20}(v)\Omega_2^{20}(v)^T = \text{circ}(X, \mathbf{0}, Y, \mathbf{0}),$$

where

$$X = AA^T + BB^T + CC^T + DD^T$$

and

$$Y = AC^T + BD^T + CA^T + DB^T.$$

Thus, $\Omega_2^{20}(v)\Omega_2^{20}(v)^T = I_{20}$ if and only if

$$\begin{cases} X = I_5, \\ Y = \mathbf{0}. \end{cases}$$

□

Definition 3.5 Let $G \cong D_{21} \cong \langle a, b \mid a^{21} = b^2 = 1, bab = a^{-1} \rangle$ with the fixed listing $G = (g_{21j+i+1}) = a^i b^j$ for $i \in \{0, \dots, 20\}$ and $j \in \{0, 1\}$. Let $H \cong C_7 \times C_3 \cong \langle c, d \mid c^7 = d^3 = 1, cd = dc \rangle$ with the fixed listing $H = (h_{7j+i+1}) = a^i b^j$ for $i \in \{0, \dots, 6\}$ and $j \in \{0, 1, 2\}$. Let $H' = \mathbf{1}$ and $P' = \mathbf{1}$. Let $v = \sum_{i=1}^{42} \alpha_{g_i} g_i \in RG$. If $\Omega_1^{42}(v)$ is the composite (G, H) -matrix of $v \in RG$ with respect to H' and P' , then

$$\Omega_1^{42}(v) = \begin{pmatrix} \text{CIRC}(A_1, A_2, A_3) & \text{CIRC}(B_1, B_2, B_3) \\ \text{CIRC}(C_1, C_2, C_3) & \text{CIRC}(D_1, D_2, D_3) \end{pmatrix},$$

where $A_1 = \text{circ}(\mathbf{v}_{1:7})$, $A_2 = \text{circ}(\mathbf{v}_{8:14})$, $A_3 = \text{circ}(\mathbf{v}_{15:21})$, $B_1 = \text{circ}(\mathbf{v}_{22:28})$, $B_2 = \text{circ}(\mathbf{v}_{29:35})$, $B_3 = \text{circ}(\mathbf{v}_{36:42})$, $C_1 = \text{circ}(\mathbf{v}_{22}, \mathbf{v}_{42:37})$, $C_2 = \text{circ}(\mathbf{v}_{36:30})$, $C_3 = \text{circ}(\mathbf{v}_{29:23})$, $D_1 = \text{circ}(\mathbf{v}_1, \mathbf{v}_{21:16})$, $D_2 = \text{circ}(\mathbf{v}_{15:9})$ and $D_3 = \text{circ}(\mathbf{v}_{8:2})$.

Theorem 3.6 Let $G = (I \mid \Omega_1^{42}(v))$ where $\Omega_1^{42}(v)$ is as defined in Definition 3.5. Then G is a generator matrix of a self-dual code of length 84 over R if and only if

$$\begin{cases} A_1A_1^T + A_2A_2^T + A_3A_3^T + B_1B_1^T + B_2B_2^T + B_3B_3^T = I_7, \\ C_1C_1^T + C_2C_2^T + C_3C_3^T + D_1D_1^T + D_2D_2^T + D_3D_3^T = I_7, \\ A_1A_3^T + A_2A_1^T + A_3A_2^T + B_1B_3^T + B_2B_1^T + B_3B_2^T = \mathbf{0}, \\ A_1C_1^T + A_2C_2^T + A_3C_3^T + B_1D_1^T + B_2D_2^T + B_3D_3^T = \mathbf{0}, \\ A_1C_3^T + A_2C_1^T + A_3C_2^T + B_1D_3^T + B_2D_1^T + B_3D_2^T = \mathbf{0}, \\ A_1C_2^T + A_2C_3^T + A_3C_1^T + B_1D_2^T + B_2D_3^T + B_3D_1^T = \mathbf{0}, \\ C_1C_3^T + C_2C_1^T + C_3C_2^T + D_1D_3^T + D_2D_1^T + D_3D_2^T = \mathbf{0}. \end{cases}$$

Proof We know that G is a generator matrix of a self-dual code of length 84 over R if and only if $\Omega_1^{42}(v)\Omega_1^{42}(v)^T = I_{42}$. We find that

$$\Omega_1^{42}(v)\Omega_1^{42}(v)^T = \begin{pmatrix} \text{CIRC}(X_1, Y_1, Y_1^T) & \text{CIRC}(Y_2, Y_3, Y_4) \\ \text{CIRC}(Y_2^T, Y_4^T, Y_3^T) & \text{CIRC}(X_2, Y_5, Y_5^T) \end{pmatrix},$$

where

$$\begin{aligned} X_1 &= A_1A_1^T + A_2A_2^T + A_3A_3^T + B_1B_1^T + B_2B_2^T + B_3B_3^T, \\ X_2 &= C_1C_1^T + C_2C_2^T + C_3C_3^T + D_1D_1^T + D_2D_2^T + D_3D_3^T \end{aligned}$$

and

$$\begin{aligned} Y_1 &= A_1A_3^T + A_2A_1^T + A_3A_2^T + B_1B_3^T + B_2B_1^T + B_3B_2^T, \\ Y_2 &= A_1C_1^T + A_2C_2^T + A_3C_3^T + B_1D_1^T + B_2D_2^T + B_3D_3^T, \\ Y_3 &= A_1C_3^T + A_2C_1^T + A_3C_2^T + B_1D_3^T + B_2D_1^T + B_3D_2^T, \\ Y_4 &= A_1C_2^T + A_2C_3^T + A_3C_1^T + B_1D_2^T + B_2D_3^T + B_3D_1^T, \\ Y_5 &= C_1C_3^T + C_2C_1^T + C_3C_2^T + D_1D_3^T + D_2D_1^T + D_3D_2^T. \end{aligned}$$

Clearly, $Y_i = \mathbf{0}$ if and only if $Y_i^T = \mathbf{0}$ for $i \in \{1, \dots, 5\}$. Thus, $\Omega_1^{42}(v)\Omega_1^{42}(v)^T = I_{42}$ if and only if

$$\begin{cases} X_1 = X_2 = I_7, \\ Y_1 = Y_2 = Y_3 = Y_4 = Y_5 = \mathbf{0}. \end{cases}$$

□

Definition 3.7 Let $G \cong D_{21} \cong \langle a, b \mid a^{21} = b^2 = 1, bab = a^{-1} \rangle$ with the fixed listing $G = (g_{21j+i+1}) = a^i b^j$ for $i \in \{0, \dots, 20\}$ and $j \in \{0, 1\}$. Let $H \cong C_3 \times C_7 \cong \langle c, d \mid c^3 = b^7 = 1, cd = dc \rangle$ with the fixed listing $H = (h_{3j+i+1}) = c^i d^j$ for $i \in \{0, 1, 2\}$ and $j \in \{0, \dots, 6\}$. Let $H' = \mathbf{1}$ and $P' = \mathbf{1}$. Let $v = \sum_{i=1}^{42} \alpha_{g_i} g_i \in RG$. If $\Omega_2^{42}(v)$ is the composite (G, H) -matrix of $v \in RG$ with respect to H' and P' , then

$$\Omega_2^{42}(v) = \begin{pmatrix} A_1 & A_2 & A_3 & B_1 & B_2 & B_3 \\ A_3^* & A_1 & A_2 & B_3^* & B_1 & B_2 \\ A_2^* & A_3^* & A_1 & B_2^* & B_3^* & B_1 \\ C_1 & C_2 & C_3 & D_1 & D_2 & D_3 \\ C_3^* & C_1 & C_2 & D_3^* & D_1 & D_2 \\ C_2^* & C_3^* & C_1 & D_2^* & D_3^* & D_1 \end{pmatrix},$$

where $A_1 = \text{circ}(\mathbf{v}_{1:7})$, $A_2 = \text{circ}(\mathbf{v}_{8:14})$, $A_3 = \text{circ}(\mathbf{v}_{15:21})$, $B_1 = \text{circ}(\mathbf{v}_{22:28})$, $B_2 = \text{circ}(\mathbf{v}_{29:35})$, $B_3 = \text{circ}(\mathbf{v}_{36:42})$, $C_1 = \text{circ}(\mathbf{v}_{22}, \mathbf{v}_{42:37})$, $C_2 = \text{circ}(\mathbf{v}_{36:30})$, $C_3 = \text{circ}(\mathbf{v}_{29:23})$, $D_1 = \text{circ}(\mathbf{v}_1, \mathbf{v}_{21:16})$, $D_2 = \text{circ}(\mathbf{v}_{15:9})$, $D_3 = \text{circ}(\mathbf{v}_{8:2})$ and \star is the transformation defined in Proposition 2.6.

Theorem 3.8 *Let $G = (I \mid \Omega_2^{42}(v))$ where $\Omega_2^{42}(v)$ is as defined in Definition 3.7. Then G is a generator matrix of a self-dual code of length 84 over R if and only if*

$$\left\{ \begin{array}{l} A_1A_1^T + A_2A_2^T + A_3A_3^T + B_1B_1^T + B_2B_2^T + B_3B_3^T = I_7, \\ C_1C_1^T + C_2C_2^T + C_3C_3^T + D_1D_1^T + D_2D_2^T + D_3D_3^T = I_7, \\ A_2A_1^T + A_3A_2^T + A_1A_3^{\star T} + B_2B_1^T + B_3B_2^T + B_1B_3^{\star T} = \mathbf{0}, \\ A_1C_1^T + A_2C_2^T + A_3C_3^T + B_1D_1^T + B_2D_2^T + B_3D_3^T = \mathbf{0}, \\ A_2C_1^T + A_3C_2^T + A_1C_3^{\star T} + B_2D_1^T + B_3D_2^T + B_1D_3^{\star T} = \mathbf{0}, \\ A_3C_1^T + A_1C_2^{\star T} + A_2C_3^{\star T} + B_3D_1^T + B_1D_2^{\star T} + B_2D_3^{\star T} = \mathbf{0}, \\ C_2C_1^T + C_3C_2^T + C_1C_3^{\star T} + D_2D_1^T + D_3D_2^T + D_1D_3^{\star T} = \mathbf{0}. \end{array} \right.$$

Proof We know that G is a generator matrix of a self-dual code of length 84 over R if and only if $\Omega_2^{42}(v)\Omega_2^{42}(v)^T = I_{42}$. Using Lemmas 2.7 and 2.8, we find that

$$\Omega_2^{42}(v)\Omega_2^{42}(v)^T = \begin{pmatrix} X_1 & Y_1 & Y_1^{\star T} & Y_2 & Y_3 & Y_4 \\ Y_1^T & X_1 & Y_1 & Y_4^{\star} & Y_2 & Y_3 \\ Y_1^{\star} & Y_1^T & X_1 & Y_3^{\star} & Y_4^{\star} & Y_2 \\ Y_2^T & Y_4^{\star T} & Y_3^{\star T} & X_2 & Y_5 & Y_5^{\star T} \\ Y_3^T & Y_2^T & Y_4^{\star T} & Y_5^T & X_2 & Y_5 \\ Y_4^T & Y_3^T & Y_2^T & Y_5^{\star} & Y_5^T & X_2 \end{pmatrix},$$

where

$$\begin{aligned} X_1 &= A_1A_1^T + A_2A_2^T + A_3A_3^T + B_1B_1^T + B_2B_2^T + B_3B_3^T, \\ X_2 &= C_1C_1^T + C_2C_2^T + C_3C_3^T + D_1D_1^T + D_2D_2^T + D_3D_3^T \end{aligned}$$

and

$$\begin{aligned} Y_1 &= A_2A_1^T + A_3A_2^T + A_1A_3^{\star T} + B_2B_1^T + B_3B_2^T + B_1B_3^{\star T}, \\ Y_2 &= A_1C_1^T + A_2C_2^T + A_3C_3^T + B_1D_1^T + B_2D_2^T + B_3D_3^T, \\ Y_3 &= A_2C_1^T + A_3C_2^T + A_1C_3^{\star T} + B_2D_1^T + B_3D_2^T + B_1D_3^{\star T}, \\ Y_4 &= A_3C_1^T + A_1C_2^{\star T} + A_2C_3^{\star T} + B_3D_1^T + B_1D_2^{\star T} + B_2D_3^{\star T}, \\ Y_5 &= C_2C_1^T + C_3C_2^T + C_1C_3^{\star T} + D_2D_1^T + D_3D_2^T + D_1D_3^{\star T}. \end{aligned}$$

Clearly, $Y_i = \mathbf{0}$ if and only if $Y_i^T = \mathbf{0}$, $Y_i^{\star} = \mathbf{0}$ and $Y_i^{\star T} = \mathbf{0}$ for $i \in \{1, \dots, 5\}$. Thus, $\Omega_2^{42}(v)\Omega_2^{42}(v)^T = I_{42}$ if and only if

$$\begin{cases} X_1 = X_2 = I_5, \\ Y_1 = Y_2 = Y_3 = Y_4 = Y_5 = \mathbf{0}. \end{cases}$$

□

Definition 3.9 Let $G \cong C_{12} \times C_2 \cong \langle a, b \mid a^{12} = b^2 = 1, ab = ba \rangle$ with the fixed listing $G = (g_{12j+i+1}) = a^i b^j$ for $i \in \{0, \dots, 11\}$ and $j \in \{0, 1\}$. Let $H \cong D_3 \cong \langle c, d \mid c^3 = d^2 = 1, dcd = c^{-1} \rangle$ with the fixed listing $H = (h_{3j+i+1}) = c^i d^j$ for $i \in \{0, 1, 2\}$ and $j \in \{0, 1\}$. Let $H' = \mathbf{1}$ and $P' = \mathbf{1}$. Let $v = \sum_{i=1}^{24} \alpha_{g_i} g_i \in RG$. If $\Omega_1^{24}(v)$ is the composite (G, H) -matrix of $v \in RG$ with respect to H' and P' , then

$$\Omega_1^{24}(v) = I_2 \otimes \text{CIRC}(\tilde{A}, \tilde{B}) + J_2 \otimes \text{CIRC}(\tilde{C}, \tilde{D}),$$

where \otimes, I_2 and J_2 denote the Kronecker product, 2×2 identity matrix and 2×2 exchange matrix, respectively and

$$\begin{aligned} \tilde{A} &= \begin{pmatrix} A_1 & A_2 \\ A_2^T & A_1^T \end{pmatrix}, & \tilde{B} &= \begin{pmatrix} B_1 & B_2 \\ B_2^T & B_1^T \end{pmatrix}, \\ \tilde{C} &= \begin{pmatrix} C_1 & C_2 \\ C_2^T & C_1^T \end{pmatrix}, & \tilde{D} &= \begin{pmatrix} D_1 & D_2 \\ D_2^T & D_1^T \end{pmatrix}, \end{aligned}$$

where $A_1 = \text{circ}(\mathbf{v}_{1:3}), A_2 = \text{circ}(\mathbf{v}_{4:6}), B_1 = \text{circ}(\mathbf{v}_{7:9}), B_2 = \text{circ}(\mathbf{v}_{10:12}), C_1 = \text{circ}(\mathbf{v}_{13:15}), C_2 = \text{circ}(\mathbf{v}_{16:18}), D_1 = \text{circ}(\mathbf{v}_{19:21})$ and $D_2 = \text{circ}(\mathbf{v}_{22:24})$.

Theorem 3.10 Let $G = (I \mid \Omega_1^{24}(v))$ where $\Omega_1^{24}(v)$ is as defined in Definition 3.9. Then G is a generator matrix of a self-dual code of length 48 over R if and only if

$$\begin{cases} A_1 A_1^T + A_2 A_2^T + B_1 B_1^T + B_2 B_2^T + C_1 C_1^T + C_2 C_2^T + D_1 D_1^T + D_2 D_2^T = I_3, \\ A_1 B_1^T + A_2 B_2^T + B_1 A_1^T + B_2 A_2^T + C_1 D_1^T + C_2 D_2^T + D_1 C_1^T + D_2 C_2^T = \mathbf{0}, \\ A_1 C_1^T + A_2 C_2^T + B_1 D_1^T + B_2 D_2^T + C_1 A_1^T + C_2 A_2^T + D_1 B_1^T + D_2 B_2^T = \mathbf{0}, \\ A_1 D_1^T + A_2 D_2^T + B_1 C_1^T + B_2 C_2^T + C_1 B_1^T + C_2 B_2^T + D_1 A_1^T + D_2 A_2^T = \mathbf{0}. \end{cases}$$

Proof We know that G is a generator matrix of a self-dual code of length 48 over R if and only if $\Omega_1^{24}(v)\Omega_1^{24}(v)^T = I_{24}$. We find that

$$\Omega_1^{24}(v)\Omega_1^{24}(v)^T = I_2 \otimes \text{CIRC}(\tilde{X}, \tilde{Y}_1) + J_2 \otimes \text{CIRC}(\tilde{Y}_2, \tilde{Y}_3),$$

where

$$\begin{aligned} \tilde{X} &= \begin{pmatrix} X & \mathbf{0} \\ \mathbf{0} & X \end{pmatrix}, & \tilde{Y}_1 &= \begin{pmatrix} Y_1 & \mathbf{0} \\ \mathbf{0} & Y_1 \end{pmatrix}, \\ \tilde{Y}_2 &= \begin{pmatrix} Y_2 & \mathbf{0} \\ \mathbf{0} & Y_2 \end{pmatrix}, & \tilde{Y}_3 &= \begin{pmatrix} Y_3 & \mathbf{0} \\ \mathbf{0} & Y_3 \end{pmatrix} \end{aligned}$$

with

$$X = A_1 A_1^T + A_2 A_2^T + B_1 B_1^T + B_2 B_2^T + C_1 C_1^T + C_2 C_2^T + D_1 D_1^T + D_2 D_2^T$$

and

$$\begin{aligned} Y_1 &= A_1 B_1^T + A_2 B_2^T + B_1 A_1^T + B_2 A_2^T + C_1 D_1^T + C_2 D_2^T + D_1 C_1^T + D_2 C_2^T, \\ Y_2 &= A_1 C_1^T + A_2 C_2^T + B_1 D_1^T + B_2 D_2^T + C_1 A_1^T + C_2 A_2^T + D_1 B_1^T + D_2 B_2^T, \\ Y_3 &= A_1 D_1^T + A_2 D_2^T + B_1 C_1^T + B_2 C_2^T + C_1 B_1^T + C_2 B_2^T + D_1 A_1^T + D_2 A_2^T. \end{aligned}$$

Thus, $\Omega_1^{24}(v)\Omega_1^{24}(v)^T = I_{24}$ if and only if

$$\begin{cases} X_1 = X_2 = I_3, \\ Y_1 = Y_2 = Y_3 = \mathbf{0}. \end{cases}$$

□

Definition 3.11 Let $G \cong D_{12} \cong \langle a, b \mid a^{12} = b^2 = 1, bab = a^{-1} \rangle$ with the fixed listing $G = (g_{12j+i+1}) = a^i b^j$ for $i \in \{0, \dots, 11\}$ and $j \in \{0, 1\}$. Let $H \cong C_{2.6} \cong \langle c \mid c^{2.6} = 1 \rangle$ with the fixed listing $H = (h_{6j+i+1}) = c^{2i+j}$ for $i \in \{0, \dots, 5\}$ and $j \in \{0, 1\}$. Let $H' = \mathbf{1}$ and $P' = \mathbf{1}$. Let $v = \sum_{i=1}^{24} \alpha_{g_i} g_i \in RG$. If $\Omega_2^{24}(v)$ is the composite (G, H) -matrix of $v \in RG$ with respect to H' and P' , then

$$\Omega_2^{24}(v) = \begin{pmatrix} A_1 & A_2 & B_1 & B_2 \\ A_2^* & A_1 & B_2^* & B_1 \\ C_1 & C_2 & D_1 & D_2 \\ C_2^* & C_1 & D_2^* & D_1 \end{pmatrix},$$

where $A_1 = \text{circ}(\mathbf{v}_{1:6})$, $A_2 = \text{circ}(\mathbf{v}_{7:12})$, $B_1 = \text{circ}(\mathbf{v}_{13:18})$, $B_2 = \text{circ}(\mathbf{v}_{19:24})$, $C_1 = \text{circ}(\mathbf{v}_{13}, \mathbf{v}_{24:20})$, $C_2 = \text{circ}(\mathbf{v}_{19:14})$, $D_1 = \text{circ}(\mathbf{v}_1, \mathbf{v}_{12:8})$, $D_2 = \text{circ}(\mathbf{v}_{7:2})$ and \star is the transformation defined in Proposition 2.6.

Theorem 3.12 Let $G = (I \mid \Omega_2^{24}(v))$ where $\Omega_2^{24}(v)$ is as defined in Definition 3.11. Then G is a generator matrix of a self-dual code of length 48 over R if and only if

$$\begin{cases} A_1 A_1^T + A_2 A_2^T + B_1 B_1^T + B_2 B_2^T = I_6, \\ C_1 C_1^T + C_2 C_2^T + D_1 D_1^T + D_2 D_2^T = I_6, \\ A_1 A_2^{*T} + A_2 A_1^T + B_1 B_2^{*T} + B_2 B_1^T = \mathbf{0}, \\ A_1 C_1^T + A_2 C_2^T + B_1 D_1^T + B_2 D_2^T = \mathbf{0}, \\ A_1 C_2^{*T} + A_2 C_1^T + B_1 D_2^{*T} + B_2 D_1^T = \mathbf{0}, \\ C_1 C_2^{*T} + C_2 C_1^T + D_1 D_2^{*T} + D_2 D_1^T = \mathbf{0}. \end{cases}$$

Proof We know that G is a generator matrix of a self-dual code of length 48 over R if and only if $\Omega_2^{24}(v)\Omega_2^{24}(v)^T = I_{24}$. Using Lemmas 2.7 and 2.8, we find that

$$\Omega_2^{24}(v)\Omega_2^{24}(v)^T = \begin{pmatrix} X_1 & Y_1 & Y_2 & Y_3 \\ Y_1^T & X_1 & Y_3^* & Y_2 \\ Y_2^T & Y_3^{*T} & X_2 & Y_4 \\ Y_3^T & Y_2^T & Y_4^T & X_2 \end{pmatrix},$$

where

$$\begin{aligned} X_1 &= A_1 A_1^T + A_2 A_2^T + B_1 B_1^T + B_2 B_2^T, \\ X_2 &= C_1 C_1^T + C_2 C_2^T + D_1 D_1^T + D_2 D_2^T \end{aligned}$$

and

$$\begin{aligned} Y_1 &= A_1 A_2^{*T} + A_2 A_1^T + B_1 B_2^{*T} + B_2 B_1^T, \\ Y_2 &= A_1 C_1^T + A_2 C_2^T + B_1 D_1^T + B_2 D_2^T, \\ Y_3 &= A_1 C_2^{*T} + A_2 C_1^T + B_1 D_2^{*T} + B_2 D_1^T, \\ Y_4 &= C_1 C_2^{*T} + C_2 C_1^T + D_1 D_2^{*T} + D_2 D_1^T. \end{aligned}$$

Clearly, $Y_i = \mathbf{0}$ if and only if $Y_i^T = \mathbf{0}$, $Y_i^* = \mathbf{0}$ and $Y_i^{*T} = \mathbf{0}$ for $i \in \{1, \dots, 4\}$. Thus, $\Omega_2^{24}(v)\Omega_2^{24}(v)^T = I_{24}$ if and only if

$$\begin{cases} X_1 = X_2 = I_6, \\ Y_1 = Y_2 = Y_3 = Y_4 = \mathbf{0}. \end{cases}$$

□

Definition 3.13 Let $G \cong D_{12} \cong \langle a, b \mid a^{12} = b^2 = 1, bab = a^{-1} \rangle$ with the fixed listing $G = (g_{12j+i+1}) = a^i b^j$ for $i \in \{0, \dots, 11\}$ and $j \in \{0, 1\}$. Let $H \cong D_6 \cong \langle c, d \mid c^6 = d^2 = 1, dcd = c^{-1} \rangle$ with the fixed listing $H = (h_{6j+i+1}) = c^i d^j$ for $i \in \{0, \dots, 5\}$ and $j \in \{0, 1\}$. Let $H' = \mathbf{1}$ and $P' = \mathbf{1}$. Let $v = \sum_{i=1}^{24} \alpha_{g_i} g_i \in RG$. If $\Omega_3^{24}(v)$ is the composite (G, H) -matrix of $v \in RG$ with respect to H' and P' , then

$$\Omega_3^{24}(v) = \begin{pmatrix} A_1 & A_2 & B_1 & B_2 \\ A_1^T & A_2^T & B_1^T & B_2^T \\ C_1 & C_2 & D_1 & D_2 \\ C_1^T & C_2^T & D_1^T & D_2^T \end{pmatrix},$$

where $A_1 = \text{circ}(\mathbf{v}_{1:6})$, $A_2 = \text{circ}(\mathbf{v}_{7:12})$, $B_1 = \text{circ}(\mathbf{v}_{13:18})$, $B_2 = \text{circ}(\mathbf{v}_{19:24})$, $C_1 = \text{circ}(\mathbf{v}_{13, \mathbf{v}_{24:20}})$, $C_2 = \text{circ}(\mathbf{v}_{19:14})$, $D_1 = \text{circ}(\mathbf{v}_1, \mathbf{v}_{12:8})$ and $D_2 = \text{circ}(\mathbf{v}_{7:2})$.

Theorem 3.14 Let $G = (I \mid \Omega_3^{24}(v))$ where $\Omega_3^{24}(v)$ is as defined in Definition 3.13. Then G is a generator matrix of a self-dual code of length 48 over R if and only if

$$\begin{cases} A_1 A_1^T + A_2 A_2^T + B_1 B_1^T + B_2 B_2^T = I_6, \\ C_1 C_1^T + C_2 C_2^T + D_1 D_1^T + D_2 D_2^T = I_6, \\ A_1 C_1^T + A_2 C_2^T + B_1 D_1^T + B_2 D_2^T = \mathbf{0}, \\ A_1 C_2 + A_2 C_1 + B_1 D_2 + B_2 D_1 = \mathbf{0}. \end{cases}$$

Proof We know that G is a generator matrix of a self-dual code of length 48 over R if and only if $\Omega_3^{24}(v)\Omega_3^{24}(v)^T = I_{24}$. We find that

$$\Omega_3^{24}(v)\Omega_3^{24}(v)^T = \begin{pmatrix} X_1 & \mathbf{0} & Y_1 & Y_2 \\ \mathbf{0} & X_1 & Y_2^T & Y_1^T \\ Y_1^T & Y_2 & X_2 & \mathbf{0} \\ Y_2^T & Y_1 & \mathbf{0} & X_2 \end{pmatrix},$$

where

$$\begin{aligned} X_1 &= A_1 A_1^T + A_2 A_2^T + B_1 B_1^T + B_2 B_2^T, \\ X_2 &= C_1 C_1^T + C_2 C_2^T + D_1 D_1^T + D_2 D_2^T \end{aligned}$$

and

$$\begin{aligned} Y_1 &= A_1 C_1^T + A_2 C_2^T + B_1 D_1^T + B_2 D_2^T, \\ Y_2 &= A_1 C_2 + A_2 C_1 + B_1 D_2 + B_2 D_1. \end{aligned}$$

Clearly, $Y_i = \mathbf{0}$ if and only if $Y_i^T = \mathbf{0}$ for $i \in \{1, 2\}$. Thus, $\Omega_3^{24}(v)\Omega_3^{24}(v)^T = I_{24}$ if and only if

$$\begin{cases} X_1 = X_2 = I_6, \\ Y_1 = Y_2 = \mathbf{0}. \end{cases}$$

□

Table 1 Quaternary notation system for elements of $\mathbb{F}_2 + u\mathbb{F}_2$ and \mathbb{F}_4

$\mathbb{F}_2 + u\mathbb{F}_2$	\mathbb{F}_4	Symbol
0	0	0
1	1	1
u	w	2
$1 + u$	$1 + w$	3

4 Results

In this section, we apply the theorems given in the previous section to obtain many new best known binary self-dual codes. In particular, we obtain 28 singly-even [80, 40, 14] codes, 107 [84, 42, 14] codes, 105 singly-even [96, 48, 16] codes and 121 doubly-even [96, 48, 16] codes.

We search for these codes using MATLAB and determine their properties using Q-extension [3] and Magma [2]. In MATLAB, we employ an algorithm which randomly searches for the construction parameters that satisfy the necessary and sufficient conditions stated in the corresponding theorem. For such parameters, we then build the corresponding binary generator matrices and print them to text files. We then use Q-extension to read these text files and determine the minimum distance and partial weight enumerator of each corresponding code. Furthermore, we determine the automorphism group order of each code using Magma. A database of generator matrices of the new codes is given online at [19]. The database is partitioned into text files (interpretable by Q-extension) corresponding to each code type. In these files, specific properties of the codes including the construction parameters, weight enumerator parameter values and automorphism group order are formatted as comments above the generator matrices. Partial weight enumerators of the codes are also formatted as comments below the generator matrices. Table 1 gives the quaternary notation system we use to represent elements of $\mathbb{F}_2 + u\mathbb{F}_2$ and \mathbb{F}_4 .

4.1 New self-dual codes of length 80

The weight enumerator of a singly-even binary self-dual [80, 40, 14] code is given in [33] as

$$W_{80} = 1 + (3200 + 4\alpha)x^{14} + (47645 - 8\alpha + 256\beta)x^{16} + \dots,$$

where $\alpha, \beta \in \mathbb{Z}$. Previously known (α, β) values for weight enumerator W_{80} can be found online at [30] (see [14, 16–18, 20, 29, 33]).

We obtain 28 new best known singly-even binary self-dual codes of length 80 which have weight enumerator W_{80} for

$$\begin{aligned} &\beta = 0 \text{ and } \alpha \in \{-z : z = 65, 80, 120, 125, 130, 135, 140, 145, 150, 155, 165, 175, \\ &\quad 190, 195, 205, 210, 215, 230, 235, 250, 270, 275, 280, 360\}; \\ &\beta = 10 \text{ and } \alpha \in \{-2z : z = 130, 150, 160, 185\}. \end{aligned}$$

Of the 28 new codes, 19 are constructed by applying Theorem 3.2 over \mathbb{F}_4 (Table 2); 4 are constructed by applying Theorem 3.4 over $\mathbb{F}_2 + u\mathbb{F}_2$ (Table 3) and 5 are constructed by applying Theorem 3.4 over \mathbb{F}_4 (Table 4).

Table 2 New singly-even binary self-dual [80, 40, 14] codes from Theorem 3.2 over \mathbb{F}_4

$C_{80,i}$	\mathbf{v}	α	β	$ \text{Aut}(C_{80,i}) $
1	(31223333300320201200)	-275	0	$2^2 \cdot 5$
2	(13111130203000233223)	-270	0	$2^2 \cdot 5$
3	(00302012331122313103)	-250	0	$2^2 \cdot 5$
4	(013320302221111113310)	-235	0	$2^2 \cdot 5$
5	(23320213130330103221)	-230	0	$2^3 \cdot 5$
6	(22011233231033013100)	-210	0	$2^2 \cdot 5$
7	(11333122033223331212)	-205	0	$2^2 \cdot 5$
8	(02222010112332220213)	-195	0	$2^2 \cdot 5$
9	(30333313000233100021)	-190	0	$2^2 \cdot 5$
10	(00111023231213313321)	-175	0	$2^2 \cdot 5$
11	(22310231030332003032)	-165	0	$2^2 \cdot 5$
12	(02002030232203221313)	-155	0	$2^2 \cdot 5$
13	(03121003232002123332)	-150	0	$2^2 \cdot 5$
14	(23200233120101002302)	-145	0	$2^2 \cdot 5$
15	(22133232333121133232)	-140	0	$2^3 \cdot 5$
16	(31031330230000203122)	-135	0	$2^2 \cdot 5$
17	(01103022122003122122)	-130	0	$2^2 \cdot 5$
18	(22010203131000112213)	-65	0	$2^2 \cdot 5$
19	(02330020210322001303)	-260	10	$2^3 \cdot 5$

Table 3 New singly-even binary self-dual [80, 40, 14] codes from Theorem 3.4 over $\mathbb{F}_2 + u\mathbb{F}_2$

$C_{80,i}$	\mathbf{v}	α	β	$ \text{Aut}(C_{80,i}) $
20	(12222331200322021203)	-280	0	$2^3 \cdot 5$
21	(23330310032021331010)	-120	0	$2^3 \cdot 5$
22	(30320122023203322322)	-80	0	$2^3 \cdot 5$
23	(21222311321120112303)	-320	10	$2^4 \cdot 5$

4.2 New self-dual codes of length 84

The possible weight enumerators of a binary self-dual [84, 42, 14] code are given in [6,33] as

$$\begin{aligned}
 W_{84,1} &= 1 + (4080 - \alpha)x^{14} + 39524x^{16} \\
 &\quad + (247264 + 14\alpha)x^{18} + \dots, \\
 W_{84,2} &= 1 + (4080 - \alpha)x^{14} + (28644 + 64\beta)x^{16} \\
 &\quad + (390368 + 14\alpha - 384\beta)x^{18} + \dots, \\
 W_{84,3} &= 1 + (4080 - \alpha)x^{14} + (28644 + 64\beta)x^{16} \\
 &\quad + (394464 + 14\alpha - 384\beta)x^{18} + \dots,
 \end{aligned}$$

Table 4 New singly-even binary self-dual [80, 40, 14] codes from Theorem 3.4 over \mathbb{F}_4

$C_{80,i}$	\mathbf{v}	α	β	$ \text{Aut}(C_{80,i}) $
24	(31211223330300232332)	-360	0	$2^2 \cdot 5$
25	(10201301032322330300)	-215	0	$2^2 \cdot 5$
26	(01021003132222203113)	-125	0	$2^2 \cdot 5$
27	(31003000101110232322)	-370	10	$2^2 \cdot 5$
28	(11210213102203230313)	-300	10	$2^2 \cdot 5$

where $\alpha, \beta \in \mathbb{Z}$. It is unknown whether or not a code with weight enumerator $W_{84,3}$ has been previously reported.

We obtain 107 new best known binary self-dual codes of length 84 which have weight enumerator $W_{84,3}$ for

- $\beta = 0$ and $\alpha \in \{6z : z = 336, 350, 358, 365, 372, 386, 392, 393, 399, 400, 406, 407, 413, 414, 420, 421, 427, 428, 434, 435, 441, 442, 448, 449, 455, 456, 462, 463, 469, 470, 476, 477, 483, 484, 490, 491, 497, 498, 504, 505, 511, 512, 518, 519, 525, 526, 532, 533, 539, 540, 546, 553, 554, 560, 567\}$;
- $\beta = 21$ and $\alpha \in \{6z : z = 413, 434, 435, 441, 442, 449, 455, 456, 462, 463, 469, 470, 476, 477, 483, 484, 490, 491, 497, 498, 504, 505, 511, 512, 518, 519, 525, 526, 532, 533, 539, 540, 546, 547, 553, 560, 568, 575, 595\}$;
- $\beta = 42$ and $\alpha \in \{6z : z = 490, 512, 518, 525, 526, 539, 540, 547, 553, 560, 568\}$;
- $\beta = 63$ and $\alpha \in \{6z : z = 574, 575\}$.

Of the 107 new codes, 55 are constructed by applying Theorem 3.6 over \mathbb{F}_2 (Table 5) and 52 are constructed by applying Theorem 3.8 over \mathbb{F}_2 (Table 6). In Tables 5 and 6, we only list 10 codes to save space. We refer to Database 2 of [19] for the remaining unlisted codes.

4.3 New self-dual codes of length 96

The possible weight enumerators of a singly-even binary self-dual [96, 48, 16] code are given in [21] as

$$\begin{aligned}
 W_{96,1}^I &= 1 + (\alpha - 5814)x^{16} + (97280 + 64\beta)x^{18} \\
 &\quad + (1784320 - 16\alpha - 384\beta)x^{20} \\
 &\quad + (17626112 + 192\beta)x^{22} + \dots, \\
 W_{96,2}^I &= 1 + (\alpha - 5814)x^{16} + (97280 + 64\beta)x^{18} \\
 &\quad + (1694208 - 16\alpha - 384\beta + 4096\gamma)x^{20} \\
 &\quad + (18969600 + 192\beta - 49152\gamma)x^{22} + \dots,
 \end{aligned}$$

where $\alpha, \beta, \gamma \in \mathbb{Z}$. Previously known (α, β, γ) values for weight enumerator $W_{96,2}^I$ can be found online at [30] (see [21]).

We obtain 105 new best known singly-even binary self-dual codes of length 96 which have weight enumerator $W_{96,2}^I$ for

- $\gamma = 0$ and $(\alpha, \beta) \in \{(12z_1, -4z_2) : (z_1, z_2) = (850, 0), (896, 0), (904, 0), (805, 1), (854, 3), (808, 4), (837, 6), (926, 6), (822, 7), (865, 9), (860, 10), (860, 12), (897, 12),$

Table 5 New binary self-dual [84, 42, 14] codes from Theorem 3.6 over \mathbb{F}_2 (see Database 2 of [19] for codes $\mathcal{C}_{84,11}$ to $\mathcal{C}_{84,55}$)

$\mathcal{C}_{84,i}$	\mathbf{v}	$W_{84,j}$	α	β	$ \text{Aut}(\mathcal{C}_{84,i}) $
1	(11000111010010111110100000111000100000111111)	3	2988	0	2 · 3 · 7
2	(11111101111011000011010010000101000001001)	3	3024	0	2 · 3 · 7
3	(001001101100110111101011010000011100011010)	3	3030	0	2 · 3 · 7
4	(10111111010011001101100101011000001001000)	3	3066	0	2 · 3 · 7
5	(1010010110101111011010011111001011010100)	3	3072	0	2 · 3 · 7
6	(111100010111001011001010011100110100001001)	3	3108	0	2 · 3 · 7
7	(110101110100001100100000110101010010101111)	3	3114	0	2 · 3 · 7
8	(00000000110000110110010101101100110111000)	3	3150	0	2 · 3 · 7
9	(10101011100111011101001100100110100100000)	3	3156	0	2 · 3 · 7
10	(101100110111001110010100000010110101111000)	3	3192	0	2 · 3 · 7

Table 6 New binary self-dual [84, 42, 14] codes from Theorem 3.8 over \mathbb{F}_2 (see Database 2 of [19] for codes $C_{84,66}$ to $C_{84,107}$)

$C_{84,i}$	v	$W_{84,j}$	α	β	$ \text{Aut}(C_{84,i}) $
56	(011001100101000001010100000000011110111100)	3	2016	0	$2^2 \cdot 3 \cdot 7$
57	(10010101000111110100110011011000001011001)	3	2100	0	$2 \cdot 3 \cdot 7$
58	(0101100010010100011100001111000111011011)	3	2148	0	$2 \cdot 3 \cdot 7$
59	(0101011001110000100110010000010000000001)	3	2190	0	$2 \cdot 3 \cdot 7$
60	(1011101100000010100010111110010000000101)	3	2232	0	$2 \cdot 3 \cdot 7$
61	(00100010001011001100110111101100100111100)	3	2316	0	$2 \cdot 3 \cdot 7$
62	(010010101101010100100111001011011001110001)	3	2352	0	$2 \cdot 3 \cdot 7$
63	(001101000100110000001101011011011110011)	3	2358	0	$2 \cdot 3 \cdot 7$
64	(000011000001100101110100000101011101110111)	3	2394	0	$2 \cdot 3 \cdot 7$
65	(0111011001001100110000111001110111101000000)	3	2400	0	$2 \cdot 3 \cdot 7$

Table 7 New singly-even binary self-dual [96, 48, 16] codes from Theorem 3.10 over $\mathbb{F}_2 + u\mathbb{F}_2$

$C_{96,i}^1$	\mathbf{v}	$W_{96,j}^1$	α	β	γ	$ \text{Aut}(C_{96,i}^1) $
1	(021111013112231302031321)	2	15336	-240	0	$2^4 \cdot 3$
2	(332030221021223333303031)	2	14664	-144	0	$2^4 \cdot 3$
3	(310201300213103023131203)	2	12456	-120	0	$2^4 \cdot 3$
4	(110330330331133112022003)	2	16608	-432	12	$2^6 \cdot 3$
5	(301201202300231031203031)	2	14712	-336	12	$2^5 \cdot 3$

Table 8 New singly-even binary self-dual [96, 48, 16] codes from Theorem 3.10 over \mathbb{F}_4 (see Database 3 of [19] for codes $C_{96,16}^1$ to $C_{96,61}^1$)

$C_{96,i}^1$	\mathbf{v}	$W_{96,j}^1$	α	β	γ	$ \text{Aut}(C_{96,i}^1) $
6	(30122010233322223210331)	2	14448	-208	0	$2^4 \cdot 3$
7	(111322103200321233201211)	2	13776	-184	0	$2^4 \cdot 3$
8	(333110012302102113330110)	2	11652	-136	0	$2^4 \cdot 3$
9	(321212110001220122211301)	2	12624	-124	0	$2^3 \cdot 3$
10	(000232332103103311032121)	2	11364	-112	0	$2^3 \cdot 3$
11	(231232002131031220200120)	2	12036	-108	0	$2^3 \cdot 3$
12	(021301113010112220211130)	2	11580	-100	0	$2^3 \cdot 3$
13	(000332130323021220110022)	2	11880	-96	0	$2^3 \cdot 3$
14	(001022122300133130333310)	2	11424	-88	0	$2^3 \cdot 3$
15	(213121322231133130230323)	2	11256	-84	0	$2^3 \cdot 3$

(900, 12), (929, 12), (1014, 12), (877, 13), (910, 15), (877, 16), (933, 18), (908, 19), (938, 21), (952, 22), (957, 24), (990, 24), (965, 25), (1003, 27), (947, 28), (1038, 30), (1052, 31), (971, 34), (1045, 36), (1222, 36), (1148, 46), (1244, 48), (1260, 48), (1204, 52), (1278, 60));

$\gamma = 6$ and $(\alpha, \beta) \in \{(12z_1, -4z_2) : (z_1, z_2) = (909, 30), (913, 31), (922, 33), (901, 34), (902, 36), (918, 37), (944, 39), (948, 40), (932, 42), (995, 43), (949, 45), (980, 46), (1034, 48), (1018, 49), (969, 51), (978, 52), (1120, 64)\}$;

$\gamma = 12$ and $(\alpha, \beta) \in \{(12z_1, -4z_2) : (z_1, z_2) = (928, 60), (988, 60), (992, 60), (1048, 60), (1056, 60), (1076, 60), (1096, 60), (1104, 60), (1120, 60), (1148, 60), (1160, 60), (1168, 60), (1176, 60), (1208, 60), (1216, 60), (1232, 60), (1240, 60), (1264, 60), (1280, 60), (1288, 60), (1320, 60), (1336, 60), (1520, 60), (982, 61), (975, 63), (984, 64), (997, 66), (1133, 66), (1148, 66), (1236, 66), (977, 67), (1075, 69), (1042, 70), (1080, 72), (1112, 72), (1120, 72), (1137, 72), (1272, 72), (1544, 72), (1036, 73), (1046, 76), (1098, 78), (1121, 78), (1072, 79), (1226, 84), (1352, 84), (1528, 84), (1224, 85), (1332, 100), (1384, 108)\}$.

Of the 105 new codes, 5 are constructed by applying Theorem 3.10 over $\mathbb{F}_2 + u\mathbb{F}_2$ (Table 7); 56 are constructed by applying Theorem 3.10 over \mathbb{F}_4 (Table 8); 29 are constructed by applying Theorem 3.12 over $\mathbb{F}_2 + u\mathbb{F}_2$ (Table 9) and 15 are constructed by applying Theorem 3.14 over $\mathbb{F}_2 + u\mathbb{F}_2$ (Table 10). In Tables 8 and 9, we only list 10 codes to save space. We refer to Database 3 of [19] for the remaining unlisted codes.

Table 9 New singly-even binary self-dual [96, 48, 16] codes from Theorem 3.12 over $\mathbb{F}_2 + u\mathbb{F}_2$ (see Database 3 of [19] for codes $C_{96,72}^I$ to $C_{96,90}^I$)

$C_{96,i}^I$	\mathbf{v}	$W_{96,j}^I$	α	β	γ	$ \text{Aut}(C_{96,i}^I) $
62	(22222222220220133213123)	2	14928	-192	0	$2^6 \cdot 3$
63	(22222222220220133211121)	2	15120	-192	0	$2^6 \cdot 3$
64	(222220222011020210021113)	2	12540	-144	0	$2^4 \cdot 3$
65	(222222222011021013011303)	2	11484	-96	0	$2^4 \cdot 3$
66	(222222222011202110211131)	2	10764	-48	0	$2^4 \cdot 3$
67	(222222222101200131212230)	2	10800	-48	0	$2^5 \cdot 3$
68	(222222222011202110213111)	2	11148	-48	0	$2^4 \cdot 3$
69	(222222220103021223012121)	2	12168	-48	0	$2^4 \cdot 3$
70	(222222222101200131221023)	2	10752	0	0	$2^5 \cdot 3$
71	(222222202121200111221203)	2	10848	0	0	$2^5 \cdot 3$

Table 10 New singly-even binary self-dual [96, 48, 16] codes from Theorem 3.14 over $\mathbb{F}_2 + u\mathbb{F}_2$

$C_{96,i}^I$	\mathbf{v}	$W_{96,j}^I$	α	β	γ	$ \text{Aut}(C_{96,i}^I) $
91	(222220222111201001210311)	2	11112	-24	0	$2^4 \cdot 3$
92	(222222202111001223010313)	2	16224	-336	12	$2^6 \cdot 3$
93	(222222222011101333122333)	2	18336	-336	12	$2^5 \cdot 3$
94	(222222222101220113212010)	2	15264	-288	12	$2^5 \cdot 3$
95	(222220222111221003212111)	2	18528	-288	12	$2^6 \cdot 3$
96	(222220220101211331210113)	2	14832	-264	12	$2^4 \cdot 3$
97	(222220200103211331212113)	2	13776	-240	12	$2^4 \cdot 3$
98	(222220222111221003212313)	2	13920	-240	12	$2^5 \cdot 3$
99	(22222220021202121211101)	2	14496	-240	12	$2^6 \cdot 3$
100	(222222222113212131201003)	2	14592	-240	12	$2^5 \cdot 3$
101	(222222222011212313201101)	2	14784	-240	12	$2^5 \cdot 3$
102	(222222220021020101011121)	2	14880	-240	12	$2^5 \cdot 3$
103	(222222222113212333201003)	2	15360	-240	12	$2^5 \cdot 3$
104	(222222222011011111002013)	2	15456	-240	12	$2^5 \cdot 3$
105	(22222222211020101021321)	2	16032	-240	12	$2^5 \cdot 3$

The weight enumerator of a doubly-even binary self-dual [96, 48, 16] code is given in [21] as

$$W_{96}^{\text{II}} = 1 + \alpha x^{16} + (3217056 - 16\alpha)x^{20} + \dots,$$

where $\alpha \in \mathbb{Z}$. Previously known α values for weight enumerator W_{96}^{II} can be found online at [30] (see [4,6,12,21,22,24,25,32]).

We obtain 121 new best known doubly-even binary self-dual codes of length 96 which have weight enumerator W_{96}^{II} for

Table 11 New doubly-even binary self-dual [96, 48, 16] codes from Theorem 3.10 over $\mathbb{F}_2 + u\mathbb{F}_2$ (see Database 4 of [19] for codes $C_{96,11}^{II}$ to $C_{96,88}^{II}$)

$C_{96,i}^{II}$	\mathbf{v}	α	$ \text{Aut}(C_{96,i}^{II}) $
1	(320210300223213323022021)	8514	$2^4 \cdot 3$
2	(1223131111112022110302021)	8754	$2^4 \cdot 3$
3	(122123010133300221011031)	8994	$2^4 \cdot 3$
4	(001212011312020203212003)	9042	$2^4 \cdot 3$
5	(122000032021320000301313)	9138	$2^4 \cdot 3$
6	(010220032021103212312322)	9234	$2^4 \cdot 3$
7	(210231130330223123221020)	9282	$2^4 \cdot 3$
8	(032311303332300120032321)	9378	$2^4 \cdot 3$
9	(213201111011203112303130)	9474	$2^4 \cdot 3$
10	(110230310113303323101232)	9618	$2^4 \cdot 3$

Table 12 New doubly-even binary self-dual [96, 48, 16] codes from Theorem 3.10 over \mathbb{F}_4

$C_{96,i}^{II}$	\mathbf{v}	α	$ \text{Aut}(C_{96,i}^{II}) $
89	(332010230212013330233103)	8274	$2^3 \cdot 3$
90	(121001211131002223313030)	8418	$2^3 \cdot 3$
91	(330222312102031223221213)	8658	$2^3 \cdot 3$
92	(331001322120111003113202)	8838	$2^3 \cdot 3$
93	(322112032202123203331221)	11478	$2^3 \cdot 3$
94	(333003302201123232100313)	11526	$2^3 \cdot 3$
95	(201120113100000113122122)	11742	$2^3 \cdot 3$
96	(000232210010130121123202)	13194	$2^5 \cdot 3$

$\alpha \in \{6z : z = 1379, 1403, 1419, 1443, 1459, 1473, 1499, 1507, 1523, 1539, 1547, 1563, 1579, 1603, 1619, 1627, 1643, 1659, 1667, 1683, 1699, 1707, 1723, 1747, 1759, 1763, 1779, 1787, 1795, 1803, 1811, 1819, 1827, 1835, 1843, 1851, 1859, 1867, 1875, 1879, 1883, 1891, 1899, 1903, 1907, 1913, 1915, 1921, 1923, 1931, 1939, 1947, 1957, 1963, 1971, 1975, 1979, 1987, 1995, 2003, 2007, 2011, 2015, 2019, 2023, 2027, 2031, 2039, 2043, 2055, 2059, 2067, 2071, 2079, 2083, 2087, 2091, 2095, 2103, 2107, 2119, 2127, 2135, 2143, 2147, 2151, 2163, 2167, 2175, 2195, 2199, 2203, 2207, 2211, 2215, 2223, 2231, 2247, 2255, 2259, 2263, 2279, 2283, 2295, 2311, 2359, 2379, 2407, 2423, 2471, 2483, 2503, 2519, 2567, 2599, 2663, 2695, 2711, 2759, 2887, 4751\}$.

Of the 121 new codes, 88 are constructed by applying Theorem 3.10 over $\mathbb{F}_2 + u\mathbb{F}_2$ (Table 11); 8 are constructed by applying Theorem 3.10 over \mathbb{F}_4 (Table 12); 13 are constructed by applying Theorem 3.12 over $\mathbb{F}_2 + u\mathbb{F}_2$ (Table 13) and 12 are constructed by applying Theorem 3.14 over $\mathbb{F}_2 + u\mathbb{F}_2$ (Table 14). In Table 11, we only list 10 codes to save space. We refer to Database 4 of [19] for the remaining unlisted codes.

Table 13 New doubly-even binary self-dual [96, 48, 16] codes from Theorem 3.12 over $\mathbb{F}_2 + u\mathbb{F}_2$

$C_{96,i}^{II}$	\mathbf{v}	α	$ \text{Aut}(C_{96,i}^{II}) $
97	(222222220103200133210030)	10002	$2^4 \cdot 3$
98	(222222220103021003012303)	10098	$2^4 \cdot 3$
99	(222222220103200133212032)	10578	$2^4 \cdot 3$
100	(222222220103021003010123)	10818	$2^4 \cdot 3$
101	(222222220103221203210101)	10866	$2^4 \cdot 3$
102	(222220202013221331211111)	12138	$2^5 \cdot 3$
103	(22222222101122211113131)	12234	$2^6 \cdot 3$
104	(22222222101020131001221)	12522	$2^6 \cdot 3$
105	(222222220103200113212230)	12546	$2^4 \cdot 3$
106	(22222222101201021210101)	12810	$2^6 \cdot 3$
107	(222220222211020212001111)	13290	$2^6 \cdot 3$
108	(222222202013220110213131)	13578	$2^5 \cdot 3$
109	(22222222220222111213123)	28506	$2^8 \cdot 3 \cdot 5$

Table 14 New doubly-even binary self-dual [96, 48, 16] codes from Theorem 3.14 over $\mathbb{F}_2 + u\mathbb{F}_2$

$C_{96,i}^{II}$	\mathbf{v}	α	$ \text{Aut}(C_{96,i}^{II}) $
110	(222220200103011331010113)	12186	$2^4 \cdot 3$
111	(22222222011202121201123)	12426	$2^5 \cdot 3$
112	(22222222011211111220213)	12714	$2^5 \cdot 3$
113	(222220220101011331012113)	12762	$2^4 \cdot 3$
114	(22222222011212313221303)	13002	$2^5 \cdot 3$
115	(222020200101011331012133)	13050	$2^4 \cdot 3$
116	(222220220101011331012133)	13338	$2^4 \cdot 3$
117	(222222220211121333100113)	13866	$2^6 \cdot 3$
118	(222222220211121333100131)	14826	$2^6 \cdot 3$
119	(22222222011211311220213)	15978	$2^6 \cdot 3$
120	(22222222011121333100333)	16170	$2^5 \cdot 3$
121	(22222222011121333100311)	16554	$2^5 \cdot 3$

5 Conclusion

In this work, we applied the idea of composite matrices $\Omega(v)$ to derive a number of techniques assuming a generator matrix of the form $(I_n | \Omega(v))$ to construct new binary self-dual codes. We defined each of the composite matrices that were implemented in the techniques and we proved the necessary conditions required by the techniques to produce self-dual codes. We applied these techniques directly over \mathbb{F}_2 as well as over the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and \mathbb{F}_4 . By so doing, we were able to construct new best known binary self-dual codes with many different weight enumerator parameter values. In particular, we constructed 28 singly-

even $[80, 40, 14]$ codes, 107 $[84, 42, 14]$ codes, 105 singly-even $[96, 48, 16]$ codes and 121 doubly-even $[96, 48, 16]$ codes.

The advantage of using composite matrices is that there are many different combinations of their determining parameters, i.e. the groups G and $\{H_1, H_2, \dots, H_\eta\}$ and the parameter matrices H' and P' . This allows for many different forms of the matrices $\Omega(v)$ which often have very unusual structures. For each of the composite matrices we defined, we assumed that $H' = \mathbf{1}$ and $P' = \mathbf{1}$. A suggestion for future work could be to investigate different choices for both H' and P' . Another suggestion would be to use composite matrices determined by groups G and $\{H_1, H_2, \dots, H_\eta\}$ of different orders. We could also investigate applying composite matrices over rings other than those used in this work.

Funding The authors did not receive support from any organisation for the submitted work.

Data availability Not applicable.

Declarations

Conflict of interest The authors have no conflicts of interest to declare that are relevant to the content of this article.

Code availability Not applicable.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Bortos M., Gildea J., Kaya A., Korban A., Tylyshchak A.: New self-dual codes of length 68 from a 2×2 block matrix construction and group rings. *Adv. Math. Commun.* (2020). <https://doi.org/10.3934/amc.2020111>.
2. Bosma W., Cannon J., Playoust C.: The Magma Algebra System I: the user language. *J. Symb. Comput.* **24**(3–4), 235–265 (1997). <https://doi.org/10.1006/jsc.1996.0125>.
3. Bouyukliev I.G.: What is Q-extension? *Serdica J. Comput.* **1**(2), 115–130 (2007).
4. Dontcheva R.: On the doubly-even self-dual codes of length 96. *IEEE Trans. Inf. Theory* **48**(2), 557–561 (2002). <https://doi.org/10.1109/18.979333>.
5. Dougherty S.T.: *Algebraic Coding Theory over Finite Commutative Rings*, 1st edn. Springer, Cham (2017).
6. Dougherty S.T., Gulliver T.A., Harada M.: Extremal binary self-dual codes. *IEEE Trans. Inf. Theory* **43**(6), 2036–2047 (1997). <https://doi.org/10.1109/18.641574>.
7. Dougherty S.T., Gaborit P., Harada M., Solé P.: Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inf. Theory* **45**(1), 32–45 (1999). <https://doi.org/10.1109/18.746770>.
8. Dougherty S.T., Gildea J., Kaya A.: 2^n bordered constructions of self-dual codes from group rings. *Finite Fields Appl.* (2020). <https://doi.org/10.1016/j.ffa.2020.101692>.
9. Dougherty S.T., Gildea J., Korban A., Kaya A.: Composite matrices from group rings, composite G-codes and constructions of self-dual codes (2020). [arXiv:2002.11614](https://arxiv.org/abs/2002.11614).
10. Dougherty S.T., Gildea J., Korban A., Kaya A.: New extremal self-dual binary codes of length 68 via composite construction, $\mathbb{F}_2 + u\mathbb{F}_2$ lifts, extensions and neighbours. *Int. J. Inf. Coding Theory* **5**(3–4), 211–226 (2020). <https://doi.org/10.1504/IJICOT.2020.110703>.

11. Dougherty S.T., Gildea J., Korban A.: Extending an established isomorphism between group rings and a subring of the $n \times n$ matrices. *Int. J. Algebra Comput.* (2021). <https://doi.org/10.1142/S0218196721500223>.
12. Feit W.: A self-dual even (96, 48, 16) code. *IEEE Trans. Inf. Theory* **20**(1), 136–138 (1974). <https://doi.org/10.1109/TIT.1974.1055153>.
13. Gaborit P., Pless V., Solé P., Atkin O.: Type II codes over \mathbb{F}_4 . *Finite Fields Appl.* **8**(2), 171–183 (2002). <https://doi.org/10.1006/ffa.2001.0333>.
14. Gildea J., Kaya A., Tylyshchak A., Yildiz B.: A group induced four-circulant construction for self-dual codes and new extremal binary self-dual codes (2019). [arXiv:1912.11758](https://arxiv.org/abs/1912.11758).
15. Gildea J., Kaya A., Korban A., Tylyshchak A.: Self-dual codes using bisymmetric matrices and group rings. *Discret. Math.* (2020). <https://doi.org/10.1016/j.disc.2020.112085>.
16. Gildea J., Korban A., Kaya A., Yildiz B.: Constructing self-dual codes from group rings and reverse circulant matrices. *Adv. Math. Commun.* (2020). <https://doi.org/10.3934/amc.2020077>.
17. Gildea J., Taylor R., Kaya A., Tylyshchak A.: Double bordered constructions of self-dual codes from group rings over Frobenius rings. *Cryptogr. Commun.* **12**(4), 769–784 (2020). <https://doi.org/10.1007/s12095-019-00420-3>.
18. Gildea J., Korban A., Roberts A.M.: New binary self-dual codes of lengths 56, 58, 64, 80 and 92 from a modification of the four circulant construction. *Finite Fields Appl.* (2021). <https://doi.org/10.1016/j.ffa.2021.101876>.
19. Gildea J., Korban A., Roberts A.M.: Generator matrix database (2021). <https://amr3-ys3da62trb.netlify.app>.
20. Gulliver T.A., Harada M.: Classification of extremal double circulant self-dual codes of lengths 74–88. *Discret. Math.* **306**(17), 2064–2072 (2006). <https://doi.org/10.1016/j.disc.2006.05.004>.
21. Gulliver T.A., Harada M.: On extremal double circulant self-dual codes of lengths 90–96. *Appl. Algebra Eng. Commun. Comput.* **30**(5), 403–415 (2019). <https://doi.org/10.1007/s00200-019-00381-3>.
22. Harada M., Yorgova R.: Construction of a self-dual [94, 47, 16] code. In: Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, pp. 125–128. Pamporovo, Bulgaria (2008).
23. Hurley T.: Group rings and rings of matrices. *Int. J. Pure Appl. Math.* **31**(3), 319–335 (2006).
24. Kaya A., Yildiz B.: Various constructions for self-dual codes over rings and new binary self-dual codes. *Discret. Math.* **339**(2), 460–469 (2016). <https://doi.org/10.1016/j.disc.2015.09.010>.
25. Kaya A., Yildiz B., Siap I.: New extremal binary self-dual codes of length 68 from quadratic residue codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. *Finite Fields Appl.* **29**, 160–177 (2014). <https://doi.org/10.1016/j.ffa.2014.04.009>.
26. Korban A., Şahinkaya S., Ustun D.: New type I Binary [72, 36, 12] self-dual codes from composite matrices and R_1 Lifts (2021). [arXiv:2102.00474](https://arxiv.org/abs/2102.00474).
27. Mallows C.L., Sloane N.J.A.: An upper bound for self-dual codes. *Inf. Control* **22**(2), 188–200 (1973). [https://doi.org/10.1016/S0019-9958\(73\)90273-8](https://doi.org/10.1016/S0019-9958(73)90273-8).
28. Rains E.M.: Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory* **44**(1), 134–139 (1998). <https://doi.org/10.1109/18.651000>.
29. Roberts, A.M.: Constructions of extremal and optimal self-dual and Hermitian self-dual codes over finite fields using circulant matrices. Master’s thesis, University of Chester, Chester, UK (2020). https://drive.google.com/file/d/1CMjnuBvQtrXOY8foY6_gfXOcFFuHAaFs/view.
30. Roberts, A.M.: Weight enumerator parameter database for binary self-dual codes (2021). <https://amr-wepd-bsdc.netlify.app>.
31. Wood J.A.: Duality for modules over finite rings and applications to coding theory. *Am. J. Math.* **121**(3), 555–575 (1999). <https://doi.org/10.1353/ajm.1999.0024>.
32. Yankov N.: Some new self-dual [96, 48, 16] codes with an automorphism of order 15. *Annu. Konstantin Preslavsky Univ. Shumen. XVI C:99–108* (2014).
33. Yankov N., Anev D., Gürel M.: Self-dual codes with an automorphism of order 13. *Adv. Math. Commun.* **11**(3), 635–645 (2017). <https://doi.org/10.3934/amc.2017047>.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.