TWMS J. App. and Eng. Math. V.13, N.1, 2023, pp. 300-308

FORMALLY SELF-DUAL CODES OVER $\mathbb{F}_2[u]/\langle u^4\rangle$

Z. Ö. ÖZGER[1*], B. YILDIZ[2], §

Abstract. In this work, Gray images of formally self-dual codes over the ring $\mathcal{S}_4 = \mathbb{F}_2[u]/\langle u^4\rangle$ and some of their construction methods are considered. As a result, a considerable number of good formally self-dual binary codes with large automorphism groups have been obtained from the Gray images of formally self-dual codes over $\mathcal{S}_4$. Some have better minimum distances than the best known binary self-dual codes of the same lengths.

Keywords: Lee weight, finite chain rings, formally self-dual codes, double-circulant construction.

AMS Subject Classification: 94B05, 94B15.

1. Introduction

Formally self-dual codes and their construction methods have generated a considerable amount of interest among researchers in recent years since these codes can have better parameters than extremal self-dual codes of the same lengths. Another motivation is that the Assmus-Mattson Theorem, which works well with self-dual codes of high minimum distance works equally well with formally self-dual codes. The first construction methods for binary formally self-dual codes came from [7], which then were generalized to other rings and alphabets in [5, 6, 8, 9]. Some of the constructions for binary codes from [7] are proven to be valid for every ring of characteristic 2 as shown in [8].

In [11], cyclic and constacyclic codes over the ring

$$\mathcal{S}_4 = \mathbb{F}_2[u]/\langle u^4\rangle = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$$

were studied based on a newly defined Gray map and Lee weight. Unlike the Gray map defined in [8], the Gray map introduced here is not orthogonality-preserving. This means that the Gray image of a self-dual code over $\mathcal{S}_4$ is not necessarily a self-dual code over the binary field. However, in [11] again, the MacWilliams identities were proven for the Lee

[1] Department of Engineering Sciences, İzmir Katip Çelebi University, İzmir, Turkey.
e-mail: zynp.odemis@gmail.com; ORCID: https://orcid.org/0000-0002-3941-1726.

[*] Corresponding author.

[2] Department of Mathematics and Statistics, Northern Arizona University, AZ, USA.
e-mail: Bahattin.Yildiz@nau.edu; ORCID: https://orcid.org/0000-0001-8106-3123.

§ Manuscript received: November 02, 2020; accepted: March 15, 2021.
TWMS Journal of Applied and Engineering Mathematics, Vol.13, No.1 © Işık University, Department of Mathematics, 2023; all rights reserved.
This work is a part of the research project 2014-1-MÜH-17 supported by İzmir Katip Çelebi University Scientific Research Project Coordination Unit.

weight enumerators, which implies that the binary images of formally self-dual codes over $\mathcal{S}_4$ are also formally self-dual.

In this work, we consider formally self-dual codes over $\mathcal{S}_4$ using several constructions similar to the ones found in [8] and [7]. Applying the Gray map to the formally self-dual codes over $\mathcal{S}_4$, we are able to construct many good binary formally self-dual codes of length $40, 48, 56, 64$, and 72. The codes we have obtained have large automorphism groups and in some cases have better minimum distances than the extremal self-dual codes of the same lengths.

The rest of the paper is organized as follows: In section 2, we give the preliminaries about codes over the ring $\mathcal{S}_4$ as well as some of the definitions associated with formally self-dual codes. Also in the same section, we give the necessary results about MacWilliams identities with the Lee weight enumerator over $\mathcal{S}_4$. In section 3, we give the theoretical basis of the construction methods. In section 4, we obtain formally self-dual binary codes with large automorphism groups from the Gray images of formally self-dual codes over $\mathcal{S}_4$. In our constructions, we use computer algorithms such as the Magma Algebra System [1], which is a large, well-supported software package designed for computations in algebra, coding theory, number theory, algebraic geometry, and algebraic combinatorics. We have constructed a search algorithm for large matrix groups in Magma that allows us to find formally self-dual codes, their Gray images and some other relevant information.

2. Preliminaries

2.1. **The Ring $\mathcal{S}_4$ and Its Properties.** In this section, we will be focusing on the algebraic properties of $\mathcal{S}_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ with $u^4 = 0$, and codes over $\mathcal{S}_4$. For more details, we refer the reader to [11].

The ring $\mathcal{S}_4$ is a commutative finite chain ring of 16 elements. The group of units of $\mathcal{S}_4$ is given by

$$\begin{aligned}\mathcal{U}(\mathcal{S}_4) &= \{1, 1+u, 1+u^2, 1+u^3, 1+u+u^2, 1+u+u^3, 1+u^2+u^3, 1+u+u^2+u^3\}\\ &= \langle 1+u, 1+u^2+u^3\rangle.\end{aligned}$$

The non-units are

$$\{0, u, u^2, u^3, u+u^2, u+u^3, u^2+u^3, u+u^2+u^3\} = \langle u\rangle.$$

The ideals of $\mathcal{S}_4$ are $\langle 0\rangle$, $\langle 1\rangle$, $\langle u\rangle$, $\langle u^2\rangle$ and $\langle u^3\rangle$. We have

$$\mathcal{S}_4 \supset u\mathcal{S}_4 \supset u^2\mathcal{S}_4 \supset u^3\mathcal{S}_4 \supset u^4\mathcal{S}_4 = \{0\}.$$

The ring $\mathcal{S}_4$ is also a local ring with the unique maximal ideal $u\mathcal{S}_4$, with $\mathcal{S}_4/u\mathcal{S}_4 \cong \mathbb{F}_2$ as its residue field.

To define the Lee weights and Gray maps for codes over $\mathcal{S}_4$, we will extend the corresponding definitions from the ring $\mathbb{F}_2 + u\mathbb{F}_2$, in [2].

As w_H denoting the Hamming weight for binary codes, we define w_L, the Lee weight for $\mathcal{S}_4$, with the following identity:

$$w_L(a+ub+u^2c+u^3d) = w_H(a+b+c+d, c+d, b+d, d), \quad \forall a,b,c,d \in \mathbb{F}_2.$$

The definition of the weight immediately leads to a Gray map ϕ_L from $\mathcal{S}_4$ to $\mathbb{F}_2^4$ which can naturally be extended to $(\mathcal{S}_4)^n$ as follows:

$$\begin{aligned}\phi_L : (\mathcal{S}_4^n,\ \text{Lee weight}) &\to (\mathbb{F}_2^{4n},\ \text{Hamming weight})\\ (\overline{a}+u\overline{b}+u^2\overline{c}+u^3\overline{d}) &\mapsto (\overline{a}+\overline{b}+\overline{c}+\overline{d}, \overline{c}+\overline{d}, \overline{b}+\overline{d}, \overline{d}),\end{aligned}$$

where $\overline{a}, \overline{b}, \overline{c}, \overline{d} \in \mathbb{F}_2^n$. It is clear that ϕ_L is a linear distance preserving isometry, leading to the following theorem:

Theorem 2.1. *If C is a linear code over $\mathcal{S}_4$ of length n, size 2^k, and minimum Lee weight d, then $\phi_L(C)$ is a binary linear code with parameters $[4n, k, d]$.*

The subgroup $U_b = \langle 1+u \rangle$ of the unit group is called the subgroup of basic units. Basic units can also be characterized as the elements in $\mathcal{S}_4$ of Lee weight 1. Other units are of weight 3 and non-units have weight 2 except u^3 and 0. Basic units have the additional properties, which are characterized in the following lemma:

Lemma 2.1. *Let γ, β be elements of the ring $\mathcal{S}_4$ such that $\gamma = \alpha.\beta$ for some $\alpha \in U_b$. Then $w_L(\gamma) = w_L(\beta)$. Thus, for any $\overline{x}, \overline{y} \in \mathcal{S}_4^n$ with $\overline{x} = \alpha \cdot \overline{y}$, where $\alpha \in U_b$, we have $w_L(\overline{x}) = w_L(\overline{y})$.*

Proof. We prove the lemma by a case-by-case analysis:

Case 1. Let $\beta \in \mathcal{U}(\mathcal{S}_4)$. Then we have two subcases. First we assume that $\beta \in U_b$. In this case $\gamma = \alpha.\beta \in U_b$ and $w_L(\gamma) = w_L(\beta) = 1$.

The other subcase is when $\beta \in \mathcal{U}(\mathcal{S}_4) - U_b$. Then $w_L(\beta) = 3$ and $\alpha.\beta = \gamma \notin U_b$ is also a unit. Therefore $w_L(\gamma) = w_L(\beta) = 3$.

Case 2. Let $\beta \in \mathcal{S}_4 - \mathcal{U}(\mathcal{S}_4)$. There are three subcases. First letting $\beta = 0$ gives us $\gamma = 0$, which leads to $w_L(\gamma) = w_L(\beta) = 0$.

In the second subcase assume that $\beta = u^3$. Since α is a unit, it is in the form of $\alpha = 1 + au + bu^2 + cu^3$. So for any such α, we have $\gamma = (1 + au + bu^2 + cu^3)u^3 = u^3$, which means $w_L(\gamma) = w_L(\beta) = 4$.

In the last subcase assume $\beta \neq 0$ and $\beta \neq u^3$. Then we have $w_L(\beta) = 2$ for all such βs. Any α is of the form $\alpha = 1 + au + bu^2 + cu^3$ and every β which is neither 0 nor u^3 should start with a u and/or a u^2 component in lexicographic order. Hence $\alpha.\beta$ should start with a u and/or a u^2 component in lexicographic order, since α starts with 1. Therefore $\alpha.\beta$ is a non-unit which is neither 0 nor u^3 and hence $w_L(\gamma) = w_L(\beta) = 2$. □

2.2. **MacWilliams Identities For Codes Over $\mathcal{S}_4$.** We first start by defining the dual of a code C over $\mathcal{S}_4$. Let $\langle \cdot, \cdot \rangle$ denote the usual Euclidean inner product defined on $\mathcal{S}_4$. Then the dual $C^{\perp}$ of a linear code C of length n over $\mathcal{S}_4$ is defined as

$$C^{\perp} = \{\overline{x} \in (\mathcal{S}_4)^n | \langle \overline{c}, \overline{x} \rangle = 0, \forall \overline{c} \in C\}.$$

The dual $C^{\perp}$ is also a linear code of length n and since $\mathcal{S}_4$, being a finite chain ring, is Frobenius we have by [13]:

$$|C|.|C^{\perp}| = 16^n.$$

Definition 2.1. *A code C is called **self-dual** if $C = C^{\perp}$, it is called **isodual** if C and $C^{\perp}$ are equivalent and it is called **formally self-dual (f.s.d.)** if C and $C^{\perp}$ have the same weight enumerator. A self-dual code is called **Type II** if the weight of every codeword in C is a multiple of 4, and is called **Type I** otherwise.*

Clearly any self-dual code is both isodual and formally self-dual and isodual codes are formally self-dual but the reverse implications are not true in general.

A formally self-dual code is said to be *even* (E) if all its codewords have even weight, otherwise it is said to be *odd* (O).

Definition 2.2. *Let C be a linear code over $\mathcal{S}_4$ of length n. The Lee weight enumerator of C is given by*

$$Lee_C(W, X) = \sum_{\overline{c} \in C} W^{4n - w_L(\overline{c})} X^{w_L(\overline{c})}. \tag{1}$$

Theorem 2.2. *Let C be a linear code over $\mathcal{S}_4$ of length n and $C^\perp$ be its dual. With $Lee_C(W,X)$ denoting its Lee weight enumerator as was given in (1), we have*

$$Lee_{C^\perp}(W,X) = \frac{1}{|C|} Lee_C(W+X, W-X).$$

During our computations we simply let $W = 1$. For proof of Theorem 2.2, we refer to [11]. Note that the identity in Theorem 2.2 is precisely the identity that the Hamming weight enumerators of binary codes satisfy. Hence, as a consequence, we have the following corollary:

Corollary 2.1. *If C is a linear formally self-dual code over $\mathcal{S}_4$ of length n, then $\phi_L(C)$ is a binary formally self-dual code of length $4n$.*

3. Constructing formally self-dual codes over $\mathcal{S}_4$

In [7, p. 378], an exercise asking to prove the following for binary codes is given:

Theorem 3.1. *Let A be a square binary matrix and let I_k be the $k \times k$ identity matrix, then the following hold:*

(i) *A code of length $2k$ with generator matrix $[I_k|A]$ where $A = A^\perp$ is isodual.*

(ii) *A code with a double-circulant construction, i.e., a code with the generating matrix $[I_k|A]$, where A is a circulant matrix, is isodual.*

(iii) *A code with a bordered double-circulant construction, i.e., a code with generating matrix*

$$G = \left[\begin{array}{c|c|ccccc} & \alpha & \beta & \beta & \cdot & \cdot & \beta \\ & \gamma & & & & & \\ & \gamma & & & & & \\ I_k & \cdot & & & A & & \\ & \cdot & & & & & \\ & \cdot & & & & & \\ & \gamma & & & & & \end{array}\right]$$

where A is a $(k-1) \times (k-1)$ circulant matrix, is isodual provided $\beta = \gamma = 0$ or both β and γ are non-zero.

In [8], with the help of this idea the following results were shown for codes over any ring R of characteristic 2:

Theorem 3.2 (Construction A)**.** *Let A be an $n \times n$ matrix over R such that $A = A^\perp$. Then the code generated by the matrix $[I_n|A]$ is an isodual code and hence a formally self-dual code of length $2n$.*

Theorem 3.3 (Construction B)**.** *Let M be a circulant matrix over R of order n. Then the matrix $[I_n|M]$ generates an isodual code and hence a formally self-dual code over R.*

We can apply Theorem 3.2 and Theorem 3.3 to $\mathcal{S}_4$, since $\mathcal{S}_4$ is of characteristic 2.

Corollary 3.1 (Construction I)**.** *Let A be an $n \times n$ matrix over $\mathcal{S}_4$ such that $A = A^\perp$. Then the code generated by the matrix $[I_n|A]$ is an isodual code and hence a formally self-dual code of length $2n$.*

Corollary 3.2 (Double-circulant construction)**.** *Let M be a circulant matrix over $\mathcal{S}_4$ of order n. Then the matrix $[I_n|M]$ generates an isodual code and hence a formally self-dual code over $\mathcal{S}_4$.*

Note that constructions given in Corollary 3.1 and Corollary 3.2 match the ones given in (i) and (ii) of Theorem 3.1, respectively. The bordered double-circulant construction for $\mathcal{S}_4$, which matches (iii) of Theorem 3.1, is given as follows:

Theorem 3.4 (Bordered double-circulant construction)**.** *Let M be a circulant matrix over $\mathcal{S}_4$ of order $n-1$. Then the matrix*

$$G = \left[\begin{array}{c|c|cccccc} & \alpha & \beta & \beta & \cdot & \cdot & \cdot & \beta \\ & \gamma & & & & & & \\ & \gamma & & & & & & \\ I_n & \cdot & & & M & & & \\ & \cdot & & & & & & \\ & \cdot & & & & & & \\ & \gamma & & & & & & \end{array}\right]$$

generates a formally self-dual code over $\mathcal{S}_4$, where $\alpha \in \mathcal{S}_4$, $\gamma = r.\beta$ for some $r \in U_b$.

Proof. The proof is very similar to the proof of the same construction given in [8] for R_k, since the characteristic of $\mathcal{S}_4$ is also 2 and Lemma 2.1 holds. Hence we will omit the proof. □

4. Computational results

We use Magma [1] computer algebra to construct binary formally self-dual codes of length 40, 48, 56, 64, and 72 with double-circulant construction by Corollary 3.2 and bordered double-circulant construction by Theorem 3.4. We use circulant matrices of order 5, 6, 7, 8, and 9, respectively for the double-circulant constructions, and circulant matrices of order 4, 5, 6, 7, and 8, respectively for the bordered double-circulant constructions. We then look at the Gray images of these codes to get good binary formally self-dual codes with large automorphism groups. In what follows, we will be giving these numerical results.

4.1. **Results From The Double-Circulant Construction.**

We give Gray images of some good formally self-dual codes over $\mathcal{S}_4$ constructed by the help of Corollary 3.2 with large automorphism groups in the following tables classified according to the lengths.

$\phi_L(C)$	$\lvert aut(\phi_L(C))\rvert$	First row of M	E/O
$[40, 20, 8]$	3686400	$(u^3+u, u^2+1, u^3+1, u^3+1, u^2+1)$	O
$[40, 20, 8]$	2880	$(u^3, u^2+1, u^2+1, u^2+1, u^2+1)$	O
$[40, 20, 8]$	240	$(u^3, u^3+u^2+1, u^2+1, u^2+1, u^3+u^2+1)$	O
$[40, 20, 8]$	160	$(u^3, u^3+u^2+u+1, u+1, u+1, u^3+u^2+u+1)$	O
$[40, 20, 8]$	120	$(0, 1, u^3+1, u^3+1, u^3+1)$	O
$[40, 20, 8]$	80	$(u^3, 1, 1, u^2+1, u^2+1)$	O
$[40, 20, 8]$	40	$(0, u^2+u+1, u^3+u+1, u+1, u^2+u+1)$	O
$[40, 20, 8]$	5760	$(u^2, u^3+u^2+u+1, u^3+u^2+u+1, u^3+u^2+u+1, u^2)$	E
$[40, 20, 8]$	480	$(u^3, u^3+u^2+u+1, u^3+u^2+u+1, u^3+u^2+u+1, u^3)$	E
$[40, 20, 8]$	240	$(0, u^3+1, 1, u^3+1, 0)$	E
$[40, 20, 8]$	160	$(u^2, u^3+1, u^3+1, u^3+1, u^2)$	E
$[40, 20, 8]$	120	$(u^3, u^3+u^2+1, u^3+u^2+1, u^3+u^2+1, 0)$	E
$[40, 20, 8]$	80	$(u^3+u^2, 1, u^3+1, 1, u^3+u^2)$	E
$[40, 20, 8]$	40	$(u^3, u^3+u^2+1, u^3+1, u^3+1, u^2)$	E
$[40, 20, 9]$	20	$(u^3, u^3+u^2+1, u^3+u^2+u, u^2+1, u^3+u)$	O

Table 1. Good f.s.d. codes of length 40 with large automorphism groups formed by double circulant construction

$\phi_L(C)$	$\lvert aut(\phi_L(C))\rvert$	First row of M	E/O
$[48, 24, 10]$	24	$(u^3+u^2, u+1, u^3+1, u^2+u+1, u^3+u+1, u^2+u+1)$	E

Table 2. Good f.s.d. codes of length 48 with large automorphism groups formed by double circulant construction

$\phi_L(C)$	$\lvert aut(\phi_L(C))\rvert$	First row of M	E/O
$[56, 28, 11]$	56	$(u, u^3+u+1, u^3+1, u^3+u+1, u^3+u+1, u^3+1, u^3+u+1)$	O
$[56, 28, 11]$	28	$(0, u^3+1, u^3+1, u+1, u^3+u^2+1, u+1, u+1)$	O
$[56, 28, 12]$	56	$(u^3, u+1, u+1, u^3, 1, u+1, u^2+1)$	E
$[56, 28, 12]$	28	$(u^3+u, u^3+u+1, u^3+u+1, u^3+u, u^3+u^2+1, u^2+u+1, 1)$	E

Table 3. Good f.s.d. codes of length 56 with large automorphism groups formed by double circulant construction

$\phi_L(C)$	$\lvert aut(\phi_L(C))\rvert$	First row of M	E/O
$[64, 32, 12]$	128	$(u^3, u^3+u+1, u^2+1, u^2+1, u^3+u+1, u^3+u^2+1, u^3+u^2+1, u^3+u^2+u+1)$	E
$[64, 32, 12]$	64	$(u^3, u^3+1, u^2+u+1, u^3+1, u+1, u^2+u+1, u^3+u+1, u^3+u+1)$	E
$[64, 32, 12]$	32	$(u^3+u^2+u, 1, u+1, u^3+u^2+u+1, u^3+u^2+u+1, 1, u^3+u^2+1, u+1)$	E
$[64, 32, 12]$	64	$(u^3+u^2+1, u^2+u+1, u^3+u^2, u^3+u^2+u, u^3+u^2, u+1, u^3+u, u^3+1)$	O
$[64, 32, 12]$	32	$(u+1, u^3+u^2+u+1, 0, u^3+u^2+u, u^2+u, u^3+u^2+u+1, u^3, 1)$	O

Table 4. Good f.s.d. codes of length 64 with large automorphism groups formed by double circulant construction

$\phi_L(C)$	$\lvert aut(\phi_L(C))\rvert$	First row of M	E/O
$[72, 36, 13]$	36	$(0, u^3+u^2+u+1, 1, u+1, u^3+u^2+u+1, u+1, u^3+u^2+1, u^3+u+1, u^3+u+1)$	O
$[72, 36, 14]$	36	$(u^3, u+1, u^3+u^2+1, u^3+1, u^2, u^2+u+1, u^2+u, 1, u^3+u^2+u+1, u+1)$	E

Table 5. Good f.s.d. codes of length 72 with large automorphism groups formed by double circulant construction

4.2. **Results From The Bordered Double-Circulant Construction.** We give Gray images of some good formally self-dual codes over $\mathcal{S}_4$ constructed from bordered double circulant (b.d.c.c.) matrices, by the help of Corollary 3.4 with large automorphism groups in the following tables classified according to the lengths.

$\phi_L(C)$	$\lvert aut(\phi_L(C))\rvert$	α, r, β	First row of M	E/O
$[40, 20, 8]$	82575360	$u^2+u+1, 1, u$	$(u^3+u, u^3+u, u^2+u+1, u^3+u)$	E
$[40, 20, 8]$	11796480	$u^2+1, 1, u$	$(1, u^2+u+1, u, u+1)$	E
$[40, 20, 8]$	3686400	$u+1, 1, u^3+u^2+1$	$(u^3+u, u^3+u^2+u, u^2+u, 1)$	O
$[40, 20, 8]$	786432	$u^3+1, 1, u$	$(u^3+u^2+u, u, u^3+u^2+u, u^3+1)$	E
$[40, 20, 8]$	262144	$u+1, 1, u$	$(u, u^3+u^2+u+1, u, u^2+u)$	E
$[40, 20, 8]$	196608	$1, 1, u$	(u^3+u, u, u^3+u, u^3+1)	E
$[40, 20, 8]$	131072	$u^3+u^2+u+1, 1, u$	$(1, u^3+u, u^3+u^2+1, u^3+u^2+u+1)$	E
$[40, 20, 8]$	65536	$u^3+u^2+u+1, 1, u$	$(u^3+u, u^2+u+1, u^3+u, u^3+u^2+u)$	E
$[40, 20, 8]$	49152	$u^3+u+1, 1, u$	(u, u^2+1, u, u)	E
$[40, 20, 8]$	32768	$u^3+1, 1, u$	$(u^3+u^2+u, u^2+u, u^2+u, 1)$	E
$[40, 20, 8]$	24576	$u^2+u+1, 1, u$	$(u, u^2+u, u^3+u, u+1)$	E
$[40, 20, 8]$	16384	$1, 1, u$	$(u^3+u^2+1, u+1, 1, u^2+u)$	E
$[40, 20, 8]$	12288	$u^2+1, 1, u$	$(u^3, u^2, u^2+u+1, 0)$	E
$[40, 20, 8]$	8192	$1, 1, u$	$(u^2+1, u^3+u^2+u, u^3+1, u^3+u^2+1)$	E
$[40, 20, 8]$	8192	$u+1, 1, u^3+1$	$(u^2+1, u^3+u^2+u, u^3+u, u)$	O
$[40, 20, 8]$	4608	$u^3+u^2+1, 1, u$	$(u^3+u^2+1, u^2+1, u^3+u^2+1, u)$	E
$[40, 20, 8]$	4096	$u^3+u^2+1, 1, 1$	$(u^3+u^2+u+1, u, u^3+u, u^2+u)$	O
$[40, 20, 8]$	4096	$u^2+1, 1, u$	$(u^2+u, u^3+u^2, 1, u^3+u^2)$	E
$[40, 20, 8]$	2880	$u^3, 1, 1$	$(u^2+1, u^3+u, u^2, u^2+u)$	O
$[40, 20, 8]$	2048	$u^3+u+1, 1, u$	$(0, u^3+u, u^3+u^2, u^2+u+1)$	E
$[40, 20, 8]$	2048	$u^3, 1, 1$	$(u^3+u^2+u+1, 1, u^3+u^2+u+1, u^3+u^2)$	O
$[40, 20, 8]$	1536	$u^3, 1, 1$	$(u^2+1, 1, u^3+u^2+1, u^3+u^2)$	O
$[40, 20, 8]$	1536	$u^3+1, 1, u$	$(u^3+u^2+1, u^2+1, u^2+1, u^2+u)$	E
$[40, 20, 8]$	1024	$u^3+u+1, 1, u$	$(u, u^3, u^3+u^2+1, 0)$	E
$[40, 20, 8]$	1024	$u^2+u+1, 1, 1$	(u^3+u, u, u^3, u^2+1)	O
$[40, 20, 8]$	768	$u^3+u^2+u+1, 1, u$	$(u^2+1, 1, u^2+1, u^3+u^2)$	E
$[40, 20, 8]$	512	$u^3+u^2+1, 1, u$	$(u+1, u^3+u^2+1, u+1, u^3+u)$	E
$[40, 20, 8]$	512	$u^3, 1, 1$	$(u^3+u^2+u+1, u^3+u+1, u^2+u+1, 0)$	O
$[40, 20, 8]$	256	$u^2+u+1, 1, u$	$(u^3+u^2+1, u^3+u+1, u^2+1, u^3+u^2+u)$	E
$[40, 20, 8]$	256	$u^3, 1, 1$	$(u^3, u^3+u, u^2+1, u^2+u)$	O
$[40, 20, 8]$	192	$u^3, 1, 1$	$(u^2+u+1, u^3+u+1, u^2+u+1, u^3+u^2)$	O
$[40, 20, 8]$	192	$u^3+u^2+u+1, 1, u$	$(u^2, u^3+u^2+1, u^2+1, u^3+1)$	E
$[40, 20, 8]$	128	$u^3+u^2+u+1, 1, u$	$(u^2, u^2+1, 0, u)$	E
$[40, 20, 8]$	128	$u^3+1, 1, 1$	$(u^3+u, u^3+u^2+1, u^3+u+1, u^3+1)$	O
$[40, 20, 8]$	96	$u^3+u^2+1, 1, 1$	(u^3+1, u^3+u+1, u^3, u)	E
$[40, 20, 8]$	96	$u^3, 1, 1$	$(u^3, u^2+u+1, u^3+u^2, u^3+u^2+u)$	O
$[40, 20, 8]$	64	$u^3, 1, 1$	$(u^3+u, u^2, u^2+u, 1)$	O
$[40, 20, 8]$	64	$u^3+u^2+1, 1, 1$	$(u^3+1, u^2, u^3+u^2, u^3+u^2+1)$	E
$[40, 20, 8]$	32	$u^3+u^2+1, 1, 1$	$(u^3+u^2+u+1, u^3+u^2, u^3+u^2, u^2+u)$	O
$[40, 20, 8]$	32	$u^3+u+1, 1, 1$	$(u^2+u+1, 1, u^3, u^3+u)$	E

TABLE 6. Good f.s.d. codes of length 40 with large automorphism groups formed by b.d.c.c.

$\phi_L(C)$	$\|aut(\phi_L(C))\|$	α, r, β	First row of M	E/O
$[48, 24, 9]$	20	$u^3, 1, 1$	$(u^3 + u + 1, u + 1, 0, u^3 + u^2 + u + 1, u^3 + u)$	O
$[48, 24, 9]$	40	$u^3 + u^2 + 1, 1, 1$	$(u, u^3 + u^2 + u, u^2 + u + 1, u^3, u^3 + u + 1)$	O
$[48, 24, 10]$	20	$u^3, 1, 1 + u$	$(u^2 + 1, u^3 + u, u^3 + u^2 + u + 1, 0, u^3)$	E
$[48, 24, 10]$	20	$u^3, 1, u + 1$	$(u + 1, u, u^3 + u, u^2, u^2)$	O
$[48, 24, 10]$	40	$u^3, 1, 1$	$(u^3 + u^2 + u + 1, u + 1, u^3 + u^2 + 1, u^3 + u^2 + 1, u^2)$	E
$[48, 24, 10]$	80	$u^2, 1, u^3 + u^2 + 1$	$(u, u^3 + u^2, u, u^3 + u^2 + u + 1, u^3 + u^2 + u + 1)$	E
$[48, 24, 10]$	2640	$u^3 + u^2 + u, 1, u^3 + 1$	$(u^2 + 1, 1, u^3 + u + 1, u, u + 1)$	E

Table 7. Good f.s.d. codes of length 48 with large automorphism groups formed by b.d.c.c.

$\phi_L(C)$	$\|aut(\phi_L(C))\|$	α, r, β	First row of M	E/O
$[56, 28, 10]$	24	$u^3 + u^2 + 1, 1, 1$	$(u^3 + u, u^3 + u, 0, u^2, u, u^2 + u + 1)$	O
$[56, 28, 10]$	24	$u^2 + u + 1, 1, 1$	$(u^3 + u^2 + u, u^3 + u^2 + u, u^2 + u + 1, u, u^3 + u + 1, 0)$	E
$[56, 28, 10]$	48	$u^3 + u^2 + 1, 1, 1$	$(1, u^2 + 1, u^3 + u^2, u^2, u + 1, u^3 + u, u^3 + 1)$	O
$[56, 28, 10]$	48	$u + 1, 1, u^3 + u^2 + 1$	$(1, u^3 + u^2 + u + 1, u, u^3 + u^2, u^2 + 1, u^3 + u^2 + u + 1)$	E
$[56, 28, 11]$	24	$u^3 + u^2 + u, 1, u^3 + u^2 + 1$	$(u^3 + u^2, u^3 + u + 1, u^3 + u + 1, u^3 + u^2 + 1, 1, u^2 + 1)$	O
$[56, 28, 11]$	48	$1, 1, u^3 + u^2 + 1$	$(u^3 + u^2 + u, u^3 + u^2, u^3 + 1, u^2 + u + 1, u, u^3 + u^2 + u + 1)$	O

Table 8. Good f.s.d. codes of length 56 with large automorphism groups formed by b.d.c.c.

$\phi_L(C)$	$\|aut(\phi_L(C))\|$	α, r, β	First row of M	E/O
$[64, 32, 12]$	28	$u^3, 1, 1$	$(u^3 + u^2, u^3, 1, u^2 + u, u^3 + u^2 + u, u^3 + u + 1, u^3 + u + 1)$	O
$[64, 32, 12]$	28	$u^3, 1, 1$	$(1, u, u^2 + 1, u^2 + u + 1, u^3 + u^2 + u, u^3 + 1, u^3 + u^2 + u)$	E
$[64, 32, 12]$	56	$u^3, 1, 1$	$(u^3 + u + 1, u^3 + 1, u^3 + u^2 + 1, u^3 + u^2 + u, u + 1, u^3 + u + 1, 1)$	E

Table 9. Good f.s.d. codes of length 64 with large automorphism groups formed by b.d.c.c.

5. Conclusion

Permutation decoding was introduced by Prange [12] and MacWilliams [10], and involves finding a set of automorphisms of a code, which is called a PD-set. In that sense, using codes with large automorphism groups might be convenient for decoding purposes. We have found some formally self-dual binary codes of length 40, 48, 56, 64, and 72 with large automorphism groups as Gray images of formally self-dual codes over $\mathcal{S}_4$. Sizes of automorphism groups of these codes are given in Tables 1-9. Compared to the minimum distances of Type I (`http://www.unilim.fr/pages_perso/philippe.gaborit/SD/GF2/GF2I.htm`) and Type II (`http://www.unilim.fr/pages_perso/philippe.gaborit/SD/GF2/GF2II.htm`) self-dual codes of the same lengths, we also see that codes given in Tables 1-9 can be considered as good codes. For codes of length 40, given in Table 1 and Table 6, we see that the largest minimum distance for Type I and Type II self-dual codes, which is 8, is attained. Also the code with parameters $[40, 20, 9]$ given in Table 1 has higher minimum distance than the extremal self-dual code of the same length. For codes of length 48, 56, 64, and 72, the upper bounds of minimum distances for Type I and Type II self-dual codes are also attained by the codes that we have constructed. In the case of length 72, the best known self-dual codes have not attained the theoretical upper bound, which means the formally self-dual codes we have constructed have outdone the best known self-dual codes.

References

[1] Bosma, W., Cannon, J. and Playoust, C., (1997), The Magma algebra system, I. The user language, Journal of Symbolic Computation, 24, pp. 235-265.

[2] Dougherty, S. T., Gaborit, P., Harada, M. and Solé, P., (1999), Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Transactions on Information Theory, 45, pp. 32-45.

[3] Fields, J. E., Gaborit, P., Huffman, W. C. and Pless, V., (2001), On the classification of extremal even formally self-dual codes of length 20 and 22, Discrete Applied Mathematics, 111(1-2), pp. 75-86.

[4] Fields, J. E., Gaborit, P., Huffman, W. C. and Pless, V., (1998), On the classification of formally self-dual codes, In: Proceedings 36th Allerton Conference on Communication, Control and Computing; University of Illinois Urbana-Champaign, Champaign, IL, USA, pp. 566-575.

[5] Han, S. and Kim, J. L., (2010), Formally self-dual additive codes over $\mathbb{F}_4$, Journal of Symbolic Computation, 45(7), pp. 787-799.

[6] Han, S. and Kim, J. L., (2009), The non-existence of near extremal formally self-dual codes, Design Codes and Cryptography, 51(1), pp. 69-77.

[7] Huffman, W. C. and Pless, V., (2003), Fundamentals of Error Correcting Codes, Cambridge University Press.

[8] Karadeniz, S., Dougherty, S. T. and Yıldız, B., (2014), Constructing formally self-dual codes over R_k, Discrete Applied Mathematics, 167, pp. 188-196.

[9] Kim, J. L. and Pless, V., (2007), A note on formally self-dual codes of length divisible by 8, Finite Fields and Applications, 13(2), pp. 224-229.

[10] MacWilliams, F. J., (1964), Permutation decoding of systematic codes, Bell System Technical Journal, 43, pp. 485-505.

[11] Ödemiş Özger, Z., Kara, Ü. Ü. and Yıldız, B., (2014), Linear, cyclic and constacyclic codes over $\mathcal{S}_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$, Filomat, 28(5), pp. 897-906.

[12] Prange, E., (1962), The use of information sets in decoding cyclic codes, IEEE Transactions on Information Theory, 8(5), pp. 5-9.

[13] Wood, J., (1999), Duality for modules over finite rings and applications to coding theory, American Journal of Mathematics, 121, pp. 555-575.

Zeynep Ödemiş Özger received her BSc from Boğaziçi University in 2008 and her PhD from Fatih University in 2013. Currently she is working as an assistant professor of mathematics at İzmir Katip Çelebi University. Her main research interests are Algebraic Coding Theory, Cryptography, and Approximation Theory.

Bahattin Yıldız received his BSc from Bilkent University in 2001 and his PhD from California Institute of Technology in 2006. Currently he works as an associate professor of mathematics at Northern Arizona University. His main research interests are Algebraic Coding Theory, Combinatorics and Cryptography.