Discrete Mathematics 339 (2016) 460–469

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Various constructions for self-dual codes over rings and new binary self-dual codes

Abidin Kaya [a], Bahattin Yildiz [b,*]

[a] Department of Computer Engineering, Bursa Orhangazi University, 16310, Bursa, Turkey

[b] Department of Mathematics, Fatih University, 34500, Istanbul, Turkey

ARTICLE INFO

Article history:
Received 13 October 2014
Received in revised form 20 September 2015
Accepted 21 September 2015
Available online 18 October 2015

Keywords:
Extremal self-dual codes
Gray maps
Four circulant codes
Extension theorems
Designs

ABSTRACT

In this work, extension theorems are used for self-dual codes over rings and as applications many new binary self-dual extremal codes are found from self-dual codes over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ for $m = 1, 2$. The duality and distance preserving Gray maps from $\mathbb{F}_4+u\mathbb{F}_4$ to $(\mathbb{F}_2+u\mathbb{F}_2)^2$ and $\mathbb{F}_2^4$ are used to obtain self-dual codes whose binary Gray images are [64, 32, 12]-extremal self-dual. An $\mathbb{F}_2+u\mathbb{F}_2$-extension is used and as binary images, 178 extremal binary self-dual codes of length 68 with new weight enumerators are obtained. Especially the first examples of codes with $\gamma = 3$ and many codes with the rare $\gamma = 4, 6$ parameters are obtained. In addition to these, two hundred fifty doubly even self dual [96, 48, 16]-codes with new weight enumerators are obtained from four-circulant codes over $\mathbb{F}_4+u\mathbb{F}_4$. New extremal doubly even binary codes of lengths 80 and 88 are also found by the $\mathbb{F}_2+u\mathbb{F}_2$-lifts of binary four circulant codes and thus a lower bound on the number of non-isomorphic 3-(80, 16, 665) designs is modified.

1. Introduction

The construction of extremal binary self-dual codes has generated a considerable interest among researchers recently. The connection of these codes to designs, lattices and other such mathematical objects has been a source of motivation for this interest. Several construction methods have been employed for this purpose. Among the most common ones, we can mention double and bordered double-circulant constructions, constructions with a specific automorphism group, and recently ring constructions using different rings of characteristic 2. We refer the reader to [3,4,8,10,11,13,14,16,22] and [20] for more on these constructions.

Ling and Sole studied Type II codes over the ring $\mathbb{F}_4+u\mathbb{F}_4$ in [17], which was later generalized to the ring $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ in [1]. These rings behave similar to the oft-studied ring $\mathbb{F}_2+u\mathbb{F}_2$ in the literature. The common theme in the aforementioned works is that a distance and duality preserving Gray map can be defined that takes codes over those rings to binary codes, preserving the linearity, the weight distribution and the duality.

Harada and Kim give two different extension methods in [12] and [16] respectively for binary self-dual codes. Both methods describe how a binary self-dual code of length n can be extended to obtain a binary self-dual code of length $n+2$.

In this work we use the extension methods on binary rings (i.e., rings of characteristic 2). With this method we extend self-dual codes over binary rings to further lengths, which correspond to a more diverse set of lengths. Also with the rich algebraic structure of the ring, we have a better chance to get good self-dual codes. The binary rings that we use are mainly

* Corresponding author.
E-mail addresses: abidin.kaya@bou.edu.tr (A. Kaya), byildiz@fatih.edu.tr (B. Yildiz).

http://dx.doi.org/10.1016/j.disc.2015.09.010
0012-365X/

$\mathbb{F}_4 + u\mathbb{F}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$ as we already have distance and duality-preserving Gray maps for these rings. Using these methods we were able to obtain 178 new extremal binary self-dual codes of length 68 and 14 new extremal codes of length 80. Assmus–Mattson theorem applied to these new self-dual codes of length 80 lead to new 3-designs, updating the lower bound on the number of non-isomorphic 3-(80, 16, 665) designs.

The rest of the paper is organized as follows: Preliminaries about codes over $\mathbb{F}_4 + u\mathbb{F}_4$ and the distance and duality-preserving Gray maps are given in Section 2. In Section 3, we give constructions for binary self-dual codes of length 64 coming from the Gray images of four-circulant self-dual codes over $\mathbb{F}_4 + u\mathbb{F}_4$. In Section 4, we describe the ring extension methods to extend self-dual codes over binary rings. In Section 5, we apply the ring extension to codes obtained in Section 3 to obtain a number of extremal binary self-dual codes of length 68 with new parameters in their weight enumerators. In Section 6, we describe constructions of extremal binary self-dual codes of lengths 80 and 88 as well as new Type II codes of length 96 from codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ for $m = 1, 2$.

2. Preliminaries

Let $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ be the quadratic field extension of $\mathbb{F}_2$, where $\omega^2 + \omega + 1 = 0$. The ring $\mathbb{F}_4 + u\mathbb{F}_4$ defined via $u^2 = 0$ is a commutative binary ring of size 16. We may easily observe that it is isomorphic to $\mathbb{F}_2[\omega, u]/\langle u^2, \omega^2 + \omega + 1\rangle$. The ring has a unique non-trivial ideal $\langle u\rangle = \{0, u, u\omega, u + u\omega\}$. Note that $\mathbb{F}_4 + u\mathbb{F}_4$ can be viewed as an extension of $\mathbb{F}_2 + u\mathbb{F}_2$ and so we can describe any element of $\mathbb{F}_4 + u\mathbb{F}_4$ in the form $\omega a + \bar{\omega} b$ uniquely, where $a, b \in \mathbb{F}_2 + u\mathbb{F}_2$.

A code C of length n over $\mathbb{F}_4 + u\mathbb{F}_4$ is an $(\mathbb{F}_4 + u\mathbb{F}_4)$-submodule of $(\mathbb{F}_4 + u\mathbb{F}_4)^n$. Elements of the code C are called codewords of C. Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be two elements of $(\mathbb{F}_4 + u\mathbb{F}_4)^n$. The duality is understood in terms of the Euclidean inner product; $\langle x, y\rangle_E = \sum x_i y_i$. The dual $C^\perp$ of the code C is defined as

$$C^\perp = \left\{x \in (\mathbb{F}_4 + u\mathbb{F}_4)^n \mid \langle x, y\rangle_E = 0 \text{ for all } y \in C\right\}.$$

We say that C is self-dual if $C = C^\perp$. Let us recall the following Gray Maps from [9] and [5];

$$\begin{array}{l|l} \psi_{\mathbb{F}_4} : (\mathbb{F}_4)^n \to (\mathbb{F}_2)^{2n} & \varphi_{\mathbb{F}_2+u\mathbb{F}_2} : (\mathbb{F}_2 + u\mathbb{F}_2)^n \to \mathbb{F}_2^{2n} \\ a\omega + b\overline{\omega} \mapsto (a, b),\ a, b \in \mathbb{F}_2^n & a + bu \mapsto (b, a + b),\ a, b \in \mathbb{F}_2^n. \end{array}$$

In [17], those were generalized to the following Gray maps;

$$\begin{array}{l|l} \psi_{\mathbb{F}_4+u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n \to (\mathbb{F}_2 + u\mathbb{F}_2)^{2n} & \varphi_{\mathbb{F}_4+u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n \to \mathbb{F}_4^{2n} \\ a\omega + b\overline{\omega} \mapsto (a, b),\ a, b \in (\mathbb{F}_2 + u\mathbb{F}_2)^n & a + bu \mapsto (b, a + b),\ a, b \in \mathbb{F}_4^n. \end{array}$$

Note that these Gray maps preserve orthogonality in the respective alphabets, for the details we refer to [17]. The binary codes $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\psi_{\mathbb{F}_4} \circ \varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ are equivalent to each other. The Lee weight of an element in $\mathbb{F}_4 + u\mathbb{F}_4$ is defined to be the Hamming weight of its binary image under any of the previously mentioned compositions of the maps. A self-dual code 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 2.1 ([17]). *Let C be a code over $\mathbb{F}_4 + u\mathbb{F}_4$. If C is self-orthogonal, so are $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$. C is a Type* I *(resp. Type* II*) code over $\mathbb{F}_4 + u\mathbb{F}_4$ if and only if $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ is a Type* I *(resp. Type* II*) $\mathbb{F}_4$-code, if and only if $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ is a Type* I *(resp. Type* II*) $\mathbb{F}_2 + u\mathbb{F}_2$-code. Furthermore, the minimum Lee weight of C is the same as the minimum Lee weight of $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$.*

Corollary 2.2. *Suppose that C is a self-dual code over $\mathbb{F}_4 + u\mathbb{F}_4$ of length n and minimum Lee distance d. Then $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ is a binary $[4n, 2n, d]$ self-dual code. Moreover, C and $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ have the same weight enumerator. If C is Type* I *(Type* II*), then so is $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$.*

An upper bound on the minimum Hamming distance of a binary self-dual code is as follows:

Theorem 2.3 ([19]). *Let $d_I(n)$ and $d_{II}(n)$ be the minimum distance of a Type* I *and Type* II *binary code of length n, respectively. Then*

$$d_{II}(n) \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4$$

and

$$d_I(n) \leq \begin{cases} 4\left\lfloor \frac{n}{24} \right\rfloor + 4 & \text{if } n \not\equiv 22 \pmod{24} \\ 4\left\lfloor \frac{n}{24} \right\rfloor + 6 & \text{if } n \equiv 22 \pmod{24}. \end{cases}$$

Self-dual codes meeting these bounds are called *extremal*. Throughout the text we obtain extremal Type I binary codes of lengths 64 and 68 and extremal Type II codes of lengths 80 and 88. The existence of extremal Type II codes of length 96 is as yet unknown. But we get Type II codes of parameters [96, 48, 16], which is the best known parameter at the moment.