An Extremal Type I Self-Dual Code of Length 16 over $\mathbb{F}_2 + u\mathbb{F}_2$

T. Aaron Gulliver

Department of Electrical and Electronic Engineering
University of Canterbury
Christchurch, New Zealand
gulliver@elec.canterbury.ac.nz

Abstract

Recently, a comprehensive examination of self-dual codes over the alphabet $\mathbb{F}_2 + u\mathbb{F}_2$ was published. This included a classification of all self-dual codes up to length 8, and tables of extremal codes up to length 36 for Type I codes and length 40 for Type II codes. Explicit constructions were given except for the Type I code of length 16. A construction for this code is given here.

1 Introduction

The introduction of codes over $\mathbb{Z}_4$ and their connection with nonlinear binary codes [8] and unimodular lattices [3, 7] has created tremendous interest in codes over rings. Another alphabet of size 4, $\mathbb{F}_2 + u\mathbb{F}_2$, was used in [1] to construct lattices. Codes over $\mathbb{F}_2 + u\mathbb{F}_2$ have also been used in the construction of self-dual binary codes [7] and formally self-dual binary codes [2].

A linear code C over $\mathbb{F}_2+u\mathbb{F}_2$ of length n is an $\mathbb{F}_2+u\mathbb{F}_2$-submodule of $(\mathbb{F}_2+u\mathbb{F}_2)^n$. The *Lee weight* $w_L(x)$ of $x = (x_1, x_2, \ldots, x_n)$ is defined as $n_1(x) + 2n_2(x)$ where $n_0(x)$ is the number of $x_i = 0$, $n_2(x)$ the number of $x_i = u$ and $n_1(x) = n - n_0(x) - n_2(x)$. The *Lee distance* $d_L(x, y)$ between two codewords x and y is the Lee weight $wt_L(x-y)$ of $x - y$. The minimum Lee weight d_L of C is the smallest Lee weight among all non-zero codewords of C.

Define the inner-product $x \cdot y$ of $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ in $(\mathbb{F}_2 + u\mathbb{F}_2)^n$ by $x_1y_1 + x_2y_2 + \cdots + x_ny_n$. The dual code $C^\perp$ of C is defined as $\{x \in (\mathbb{F}_2 + u\mathbb{F}_2)^n \mid x \cdot y = 0 \text{ for all } y \in C\}$. C is said to be self-dual if $C = C^\perp$. A self-dual code over $\mathbb{F}_2+u\mathbb{F}_2$ is said to be **Type II** if the Lee weight of every codeword is a multiple of 4 and **Type I** otherwise.

Corollary 1.1 ([5]) *Let $d_L(II,n)$ and $d_L(I,n)$ be the highest minimum Lee weights of a Type II code and a Type I code, respectively, of length n. Then*

$$d_L(II,n) \leq 4\left[\frac{n}{12}\right]+4,$$

$$d_L(I,n) \leq \begin{cases} 2\left[\frac{2n+6}{10}\right], & \text{if } n \neq 1,6,11,16, \\ 2\left[\frac{2n+6}{10}\right]+2, & \text{otherwise.} \end{cases}$$

Codes which meet these bounds are called *extremal.*

For this ring, the Gray map is defined in [1] as follows:

$$\phi : ((\mathbb{F}_2+u\mathbb{F}_2)^n,\ \text{Lee distance}) \to (\mathbb{F}_2^{2n},\ \text{Hamming distance})$$

where $\phi(x+uy)=(y,x+y)$ for an element $x+uy \in (\mathbb{F}_2+u\mathbb{F}_2)^n, x,y \in \mathbb{F}_2^n$. The Gray map is a distance preserving map.

Proposition 1.2 ([2]) *The image of the Gray map of a self-dual code C over $\mathbb{F}_2+u\mathbb{F}_2$ is a self-dual binary code. The minimum Lee weight of C is the same as the minimum weight of $\phi(C)$.*

2 Double Circulant Codes

A *pure double circulant* code of length $2n$ has a generator matrix of the form $(\ I\ ,\ R\ )$ where I is the identity matrix of order n and R is an n by n circulant matrix. A code with a generator matrix of the form

$$\left(\begin{array}{c|c|ccc} & \alpha & \beta & \cdots & \beta \\ & \gamma & & & \\ I & \vdots & & R' & \\ & \gamma & & & \end{array}\right), \tag{1}$$

where R' is an $n-1$ by $n-1$ circulant matrix, is called a *bordered double circulant* code of length $2n$. These two families of codes are collectively called *double circulant* codes.

Self-dual binary double circulant codes can be used to construct self-dual codes over $\mathbb{F}_2+u\mathbb{F}_2$ via the following corollary.

Corollary 2.1 ([5]) *The inverse Gray map of a binary pure double circulant self-dual code of length $4n$ is a self-dual code over $\mathbb{F}_2+u\mathbb{F}_2$.*

Every binary pure double circulant self-dual code of length 32 is a Type II code [6]. Therefore this technique cannot be used to obtain a Type I code of length 16 over $\mathbb{F}_2+u\mathbb{F}_2$. A direct approach is used here to obtain such a code. The highest possible minimum weight for a self-dual code over $\mathbb{F}_2+u\mathbb{F}_2$ of length 16 is 8, so a search was executed to find a double circulant self-dual code with this minimum weight. The

Table 1: Weight Enumerators for [16,8,8] Double Circulant Self-Dual Codes.

Weight	W_{II}	W_I
0	1	1
8	620	364
10	0	2048
12	13888	6720
14	0	14336
16	36518	18598
18	0	14336
20	13888	6720
22	0	2048
24	620	364
32	1	1

following were among the codes obtained. The pure double circulant code with first row of R equal to

$$12121000$$

corresponds to a Type II code with weight enumerator W_{II} given in Table 1. The pure double circulant code with first row of R equal to

$$12221010$$

corresponds to a Type I code with weight enumerator W_I given in Table 1.

Note that these are the only two possible weight enumerators for binary self-dual codes of length 32 [4], and so are the only possible for length 16 self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. All bordered double circulant codes of length 16 are Type II codes, and so have weight enumerator W_{II}.

Based on the above results, we have the following.

Lemma 2.2 *There exist pure double circulant self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ which are not the inverse Gray map image of binary pure double circulant self-dual codes.*

References

[1] C. Bachoc, Application of coding theory to the construction of modular lattices, *J. Combin. Theory Ser. A* **78** (1997), 92–119.

[2] K. Betsumiya, T.A. Gulliver and M. Harada, On binary extremal formally self-dual even codes, *Kyushu J. Math.* (submitted).

[3] A. Bonnecaze, P. Solé and A.R. Calderbank, Quaternary quadratic residue codes and unimodular lattices, *IEEE Trans. Inform. Theory* **41** (1995), 366–377.

[4] J.H. Conway, N.J.A. Sloane, An upper bound on the minimum distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.

[5] S.T. Dougherty, P. Gaborit, M. Harada and P. Solé, Type II Codes over $\mathbb{F}_2+u\mathbb{F}_2$, *IEEE Trans. Inform. Theory*, (submitted).

[6] M. Harada, T.A. Gulliver and H. Kaneta, Classification of extremal double circulant self-dual codes of length up to 62, *Discrete Math.*, (to appear).

[7] M. Harada, P. Solé and P. Gaborit, Self-dual codes over $\mathbb{Z}_4$ and unimodular lattices: a survey, (submitted).

[8] A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory* **40** (1994), 301–319.

(Received 13/7/98)