ON THE NON $\mathbb{Z}_4$-LINEARITY OF CERTAIN GOOD BINARY CODES

JOE FIELDS AND PHILIPPE GABORIT

Abstract. In this paper we prove that any extremal doubly-even self-dual linear binary code of length 48 is not $\mathbb{Z}_4$-linear. We also show that the putative extremal doubly-even self-dual linear binary codes of lengths 72 and 96 with minimum weight respectively 16 and 20 cannot be constructed as the Gray images of linear codes over $\mathbb{Z}_4$.

Keywords: $\mathbb{Z}_4$-linearity, binary Type II, doubly-even self-dual extremal linear binary codes

1. Introduction

A binary code is said to be $\mathbb{Z}_4$-linear if it is the image under the well-known Gray map of a linear $\mathbb{Z}_4$ code.

Many papers have dealt with $\mathbb{Z}_4$ codes. Especially since the paper of Hammons et al. [4] where the $\mathbb{Z}_4$-linearity of the Kerdock, Preparata, and other good families of non-linear binary codes was demonstrated. They showed that the Nordstrom-Robinson code is the Gray image of the self-dual $\mathbb{Z}_4$ octacode – and that the Golay code is not $\mathbb{Z}_4$-linear. The $\mathbb{Z}_4$-linearity of optimal binary codes with minimum weight 6 or less was also considered by Encheva and Jensen in [3].

If we know that a binary code is $\mathbb{Z}_4$-linear, we get information about its structure. It is possible to exploit $\mathbb{Z}_4$-linearity in the decoding problem. We are also interested in the question – can good new linear binary codes be constructed as the Gray images of $\mathbb{Z}_4$-linear codes? In particular one could ask whether a new extremal binary Type II code of length 48 or the putative extremal binary Type II codes of length 72 or 96 (with minimum weights respectively 16 and 20) could be the Gray images of $\mathbb{Z}_4$-linear codes.

In this paper we prove that any extremal binary doubly-even codes of length 48 with minimum weight 12, and the putative extremal doubly-even self-dual codes of length 72 and 96 are not $\mathbb{Z}_4$-linear. Section §2 recalls some basic facts about $\mathbb{Z}_4$ codes. Section §3 introduces the notion of a Hadamard pair, which is used in the sections §4, 5, 6 to prove the non $\mathbb{Z}_4$-linearity of the binary extremal type II codes considered. The same method applied to the length 24 gives another simple proof of the non $\mathbb{Z}_4$-linearity of the Golay code different from that of [4].

2. Notations and Definitions

A linear code $\mathcal{C}$ of length n over $\mathbb{Z}_4$ is an additive sub-module of $\mathbb{Z}_4^n$. An element of $\mathcal{C}$ is called a codeword. A generator matrix of $\mathcal{C}$ is a matrix whose rows generate $\mathcal{C}$ as a $\mathbb{Z}_4$-module. There are three different weights for codes over $\mathbb{Z}_4$, namely the Hamming weight, the Lee weight and the Euclidean weight. In this paper we only consider the Lee weight. The Lee weights of the elements $0, 1, 2$ and 3 of $\mathbb{Z}_4$ are $0, 1, 2$ and 1 respectively and the Lee weight of a codeword is the rational sum of the Lee weights of its components. The Lee distance between two elements a and b of $\mathbb{Z}_4^n$ is defined by the rational sum of the Lee weights of the components of $a-b$. The usual Hamming weight of binary vector c, i.e the number of its non-zero components, is denoted by $w(c)$. In the case where all the codewords of a binary code have weight a multiple of 4 the code is said to be doubly-even. A binary Type II code is a binary self-dual doubly-even code.

We recall that the Gray map Φ is a distance preserving map from ($\mathbb{Z}_4^n$, Lee distance) to ($\mathbb{F}_2^{2n}$, Hamming distance). Therefore the minimum (Hamming) weight of the binary Gray image $\Phi(\mathcal{C})$ of a $\mathbb{Z}_4$-linear code $\mathcal{C}$ is the minimum Lee weight of the $\mathbb{Z}_4$ code $\mathcal{C}$.

We say that two codes are *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. Codes differing by only a permutation of coordinates are called *permutation-equivalent.* The automorphism group of $\mathcal{C}$ consists of all permutations and sign-changes of the coordinates that fix $\mathcal{C}$ as a set. Any code is permutation-equivalent to a code with a generator matrix of the form

$$\begin{pmatrix} I_{k_1} & A & B_1 + 2B_2 \\ 0 & 2I_{k_2} & 2C \end{pmatrix}, \tag{1}$$

where the component sub-matrices A, B_1, B_2 and C are binary matrices.

We say that a code with generator matrix (1) has *type* $4^{k_1}2^{k_2}$ (cf. [2]). The binary $[n, k_1]$ code C_1 with generator matrix

$$\begin{pmatrix} I_{k_1} & A & B_1 \end{pmatrix}, \tag{2}$$

is called the *residue code* of the $\mathbb{Z}_4$ code. The binary $[n, k_1 + k_2]$ code C_2 with generator matrix

$$\begin{pmatrix} I_{k_1} & A & B_1 \\ 0 & I_{k_2} & C \end{pmatrix}, \tag{3}$$

is called the *torsion code* of the $\mathbb{Z}_4$ code.

3. $\mathbb{Z}_4$-LINEARITY OF DOUBLY-EVEN BINARY CODES

In this section we give necessary conditions on a $\mathbb{Z}_4$ code for its Gray image to be a doubly-even self-dual binary code. We begin with a linearity condition which is equivalent to theorem 5 in [4].

Proposition 1. *If $\mathcal{C}$ is a $\mathbb{Z}_4$ code, its Gray image $\Phi(\mathcal{C})$ is linear if and only if:*

$$\forall\, a, b \in C_1,\; a * b \in C_2,$$

where '' stands for the Hadamard product.*

Proof. This proposition follows from the formula

$$\Phi(u) + \Phi(v) = \Phi(2(\alpha(u) * \alpha(v)) + (u + v))$$

where α denotes the "reduction mod 2" map.

$\Phi(\mathcal{C})$ is linear $\Leftrightarrow$ $2(\alpha(u) * \alpha(v)) \in \mathcal{C}$ $\forall u, v \in \mathcal{C}$ $\Leftrightarrow$ $a * b \in C_2$ $\forall a, b \in C_1$.

(Recall that $a \in C_1$ means that there is a $u \in \mathcal{C}$ such that $\alpha(u) = a$.)

□

As a matter of convenience we introduce the following definition:

Definition 1. *Given a binary $k_1 \times n - k_1$ matrix M with rows m_i, a binary code D of length n with generator matrix G_D and an integer b, we say that the pair (M, D) is a Hadamard pair with parameters (n, k_1, b) if and only if:*

1) for all $i, j \in [1, \ldots, k_1]$, $i \neq j$, $m_i * m_j \in D$.

2) the code $\tilde{C}$ with generator matrix

$$\begin{pmatrix} I_{k_1} & M \\ 0 & G_D \end{pmatrix}$$

is even and its minimum weight $w_{\tilde{C}}$ is at least b.

We consider in the next lemma a particular case of Hadamard pairs.

Lemma 1. *Let (M, D) be a Hadamard pair with parameters (n, k_1, b), with D null and $n \leq 3k_1$, then $b \leq 2$.*

Proof. Let (M, D) be such a Hadamard pair, since D is null the first condition of the definition of a Hadamard pair implies that there is at most one 1 in each column of M. And since $n \leq 3k_1$ the average number of 1's in each row is less or equal to 2, which implies that a certain row m_i of M has weight 2 or less and therefore since $\tilde{C}$ is even it contains at least one word of weight 2 and $b \leq 2$. □

Now we give necessary conditions for the existence of a $\mathbb{Z}_4$-linear Type II binary code.

Theorem 1. *If $\mathcal{C}$ is a $\mathbb{Z}_4$ code of length n with associated residue code C_1 of dimension k_1 and torsion code C_2, such that the Gray image of $\mathcal{C}$ is a doubly-even linear binary code C of minimum Hamming weight $min\, C$, then there exists a Hadamard pair (M, D) with parameters $(n, k_1, \frac{min\, C}{2})$.*

Proof. The torsion code C_2 of $\mathcal{C}$ is permutation equivalent to a code with generator matrix:

$$\begin{pmatrix} I_{k_1} & A & B_1 \\ 0 & I_{k_2} & C \end{pmatrix}$$

from which we deduce the matrix $M = (A\ B_1)$ and the code D – the code generated by the matrix $(I_{k_2}\ C)$. Since a permutation of the columns has no effect on the linearity of the Gray image, proposition 1 applied to the code $(I_{k_1}\ M)$, considered as a binary code, gives the first condition of the definition of a Hadamard pair. As a word $c \in C_2$ of weight w corresponds to a $2c \in \mathcal{C}$ of Lee weight $2w$, and as the Gray image of $\mathcal{C}$ is doubly-even, we get that w must be even and that minimum weight of C_2 is at least $\frac{min\, C}{2}$, which gives the second condition of the definition. □

We next prove a lemma which will be useful in the following sections.

Lemma 2. *Let (M, D) be a Hadamard pair with parameters (n, k_1, b), with m_i the rows of M, then for any $1 \leq i, j \leq k_1$, $i \neq j$:*

$$w(m_i) - w(m_i * m_j) \geq b - 1.$$

Proof. The word $m_i * m_j$ is in D and so also (with k_1 zeros prefixed) in $\tilde{C}$. If we call e_i the row of the generator matrix of $(I_{k_1}\, M)$ which contains the row m_i of M, then $e_i + e_i * e_j$ is in $\tilde{C}$ and has weight $w(e_i) - w(e_i * e_j)$ which gives the lemma, since $w(e_i) = w(m_i) + 1$.

□

4. The length 48

It is not known whether the extended binary quadratic residue code of length 48 is the only extremal Type II code for that length. This section proves that neither the extended quadratic residue code of length 48, nor another putative extremal Type II code can be constructed as the Gray image of a linear $\mathbb{Z}_4$ code.

Suppose there is a $\mathbb{Z}_4$-linear code having for Gray image an extremal self-dual doubly-even code of length 48 (which has minimum weight 12). We first consider conditions for the residue and torsion codes of such a code. The torsion code C_2 has weight at least $\frac{12}{2} = 6$. Using the on-line table of [1], we see that the maximum dimension of a linear binary code of length 24 and minimum weight 6 is 14, which implies that C_2 is at most dimension 14 and therefore that k_1 is at least 10.

We begin with a lemma, using the notations of Theorem 1.

Lemma 3. *There is no Hadamard pair* (M, D) *with parameters* $(24, 10, 6)$*.*

Proof. Suppose such a Hadamard pair (M, D) with parameters $(24, 10, 6)$ exists. From lemma 1 the code D is non null. Let us denote by $w(m_i)$ the weight of the row m_i from the matrix M for $1 \leq i \leq 10$. Since $\tilde{C}$ is even and has minimum weight 6 or more, the different possible weights $w(m_i)$ are odd and $5 \leq w(m_i) \leq 14$. The different possible weights are: 5,7,9,11 and 13.

Let us examine how many rows m_i with a given weight w are possible in M.

- $w = 5$

The Hadamard product of two rows of M has to be in D which is even of minimum weight 6, therefore the Hadamard product of a row of weight 5, say m_i, with any other line m_j is 0 and so the matrix M is null in columns where m_i is 1. Since the length of M is 14, there are at most two such rows, but if there were 2, it would mean that all the others rows of M could have weight at most 3, which is impossible. Therefore, there is at most one row of weight 5.

• $w = 7$

The weight of the Hadamard product of two such rows cannot be 6 from Lemma 2, adding the two rows, there would be a word of weight 4 in $\tilde{C}$. So they must be disjoint, and therefore there are at most two rows of weight 7.

• $w = 9$

By the same kind of argument as in the preceding cases, the Hadamard product of two such rows cannot be 8 nor 0, so is 6. But if there were two such rows this would contradict Lemma 2, there would be a word of weight 4 in $\tilde{C}$. So there is at most one row of weight 9.

• $w = 11$ and $w = 13$

The Hadamard product of two rows of weight 11 cannot be 6 since the length of M is 14 and cannot be 8 or 10 because of Lemma 2, so there is at most one row of weight 11.

If you add the number of possible rows, there are at most 6, but the matrix M has to have 10. □

We now prove the main theorem of this section.

Theorem 2. *There is no $\mathbb{Z}_4$-linear extremal binary Type II code of length* 48.

Proof. Otherwise from Theorem 1 there would exist a Hadamard pair (M, D) with parameters $(24, k_1, 6)$ for k_1 equal to $10, 11$ or 12. Lemma 3 shows that the case $k_1 = 10$ is impossible. The cases $k_1 = 11$ and $k_1 = 12$ are also impossible since then we could construct from them a Hadamard pair (M', D') with paramaters $(24, 10, 6)$ proceeding this way: respectively adding one (or two) columns of zeros and deleting one (or two) rows from M to obtain M'. And adding one or two zeros to the code D to obtain D', depending on the case.

□

5. The length 72

In this section we prove similarly to the preceding section that there is no $\mathbb{Z}_4$-linear extremal doubly-even self-dual [72,36,16] code.

Suppose there exists a $\mathbb{Z}_4$ code whose Gray image is such a binary code. Then the residue code C_2 has minimum weight at least $\frac{16}{2} = 8$. The on-line tables of [1] show that the dimension of $\mathcal{C}_2$ is bounded above by 21, which implies that: $k_1 \geq 15$.

Lemma 4. *There is no Hadamard pair (M, D) with parameters $(36, 15, 8)$.*

The proof is similar to the proof of Lemma 3.

Proof. Suppose such a Hadamard pair (M, D) with parameters $(36, 15, 8)$ exists. We examine the different possibilities for the weights of the rows of M. In this case from Lemma 1, D is non null and the minimum of D is 8 more, so that the different possible weights for the rows of M are: 7,9,11,13,15,17,19,21.

- $w = 7$

There are at most three rows possible – the Hadamard product between each pair of them is nil.

- $w = 9$

The Hadamard product of two such rows is 0 or 8, 8 is not possible by Lemma 2, so there are at most 2.

- $w = 11$

The Hadamard product of two such rows has to be 8 or 10, which is not possible by Lemma 2. So there is at most 1.

- $w = 13, 15, 17, 19, 21$

For each of these weights w the weight w_i of the Hadamard product of two lines with the same weight w has to be at least 8 and must also verify:

$$w_i + 2(w - w_i) \leq 21,$$

since the length of M is 21. It is easy to check then that in this case, lemma 2 is never verified so that there is at most one row with each of these weights.

In the end if we count the number of possible rows, there are at most 11 but M has to have 15 rows. □

Theorem 3. *There is no Z_4-linear, extremal binary Type II code of length* 72 *and minimum weight* 16.

Proof. Otherwise from Theorem 1 there would exist a Hadamard pair (M, D) with parameters $(36, k_1, 8)$ for k_1 equal to $15, 16, 17$ or 18. Lemma 4 shows that the case $k_1 = 15$ is impossible. The three other cases are also not possible, since then one could construct (by the same construction as in the proof of Theorem 2) a Hadamard pair with parameters $(36, 15, 8)$. □

6. The length 96

For this length the maximal possible Hamming weight of a doubly-even self-dual binary code is 20, and it is not known if such code(s) exist. We prove in this section that if such a code exists it is not $\mathbb{Z}_4$-linear.

Suppose there exists a $\mathbb{Z}_4$ code whose Gray image is such a [96,48,20] doubly-even self-dual binary code. Then the residue code C_2 has minimum weight at least $\frac{20}{2} = 10$. The on-line tables of [1] show that the dimension of C_2 is bounded above by 28, which implies that $k_1 \geq 20$.

Lemma 5. *There is no Hadamard pair (M, D) with parameters $(48, 20, 10)$.*

Proof. The proof is also similar to the proof of Lemma 3. Suppose such a Hadamard pair (M, D) with parameters $(48, 20, 10)$ exists. We examine the different possibilities for the weights of the rows of M.

In this case D is non null from Lemma 1 and its minimum weight is 10 or more, so that the different possible weights are: 9,11,13,15,17,19,21,23,25 or 27.

- $w = 9, 11, 13$

By arguments similar to those of the lemma 3 (cases $w = 5$ and $w = 7$) we can show that there are at most 3 rows of weight 9, 2 rows of weight 11, and 2 rows of weight 13.

- $w = 15, 17, 21, 23, 25$ or 27

First we notice that two rows of M with the same weight from the preceding list have a non-null Hadamard product. Let us denote by w the weight of a given row, and denote by w_i, the possible weight of the Hadamard product of two rows with the same weight w. Since the length of M is 28, we necessarily have:

$$w_i + 2(w - w_i) \leq 28,$$

moreover the condition of Lemma 2 can be written

$$w - w_i \geq 9,$$

and the minimum weight condition implies

$$w_i \geq 10.$$

These three conditions delimit three half-planes whose global intersection is empty for the weights w considered. This shows that there cannot be two rows having the same weight among these 6 weights.

- $w = 19$

For this weight there is a possibility for the three preceding conditions: $w_i = 10$. Suppose there are three rows m_0, m_1, m_2 with weight 19 then $w(m_0 * m_1) = w(m_0 * m_2) = w(m_1 * m_2) = 10$. The latter condition implies that $w(m_0 * m_1 * m_2) = 1$, which leads to $w(m_0 + m_0 * m_1 + m_0 * m_2) = 1$. But $m_0 * m_1$ and $m_0 * m_2$ are in $\tilde{C}$ which shows that the word $e_0 + m_0 * m_1 + m_0 * m_2$, has weight 2, which is not possible.

If we count the number of possible rows we obtain 15, but M has to have 20 rows, this proves the lemma. □

Theorem 4. *There is no Z_4-linear binary extremal Type II code of length* 96 *and minimum weight* 20.

Proof. Otherwise from Theorem 1 there would exist a Hadamard pair (M, D) with parameters $(48, k_1, 10)$ for k_1 equal to $20, 21, 22, 23$ or 24. Lemma 5 shows that the case $k_1 = 20$ is impossible. The other cases are also not possible, since then one could construct (by the same construction as in the proof of Theorem 2) a Hadamard pair with parameters $(48, 20, 10)$. □

7. Conclusion

The methods developed in this paper confirm the remark of [3] that it is difficult for the Gray image of a $\mathbb{Z}_4$-linear code to be linear and simultaneously to have a high minimum weight and a high dimension. We have only considered the potentially interesting cases of the lengths 48,72 and 96, when there was a possibility to construct by $\mathbb{Z}_4$-linear codes some new yet unknown extremal self-dual binary codes. It is difficult to find a more general bound for the parameters of Z_4-linear code for its Gray image to be doubly-even with a good minimum weight, because of the use of on-line tables of [1] in each proof, but a case by case consideration can be easily generalized. Our study suggests that it seems unlikely that one could construct linear binary codes with good parameters, even if not extremal, from $\mathbb{Z}_4$-linear codes.

ACKNOWLEDGEMENT

We would like to thank C. Huffman, V. Pless and P. Solé for helpful comments.

References

[1] Brouwer on-line tables: http://www.win.tue.nl/math/dw/voorlincod.html.

[2] J.H. Conway and N.J.A. Sloane, Self-dual codes over the integers modulo 4, *J. Combin. Theory Ser. A* **62**, (1993), pp. 30–45.

[3] S.B. Encheva and H.E. Jensen, Optimal binary linear codes and $\mathbb{Z}_4$-linearity *IEEE Trans. Inf. Theory* **42** (1994) pp. 1216–1222.

[4] 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. Inf. Theory* **40** (1994) pp. 301–319.

[5] E.M. Rains, Optimal codes over $\mathbb{Z}_4$, preprint.

Department of Mathematics, Statistics and Computer Science (m/c 249), University of Illinois at Chicago, 851 South Morgan Street, Chicago IL 60607

E-mail address: `fields@math.uic.edu`

E-mail address: `gaborit@math.uic.edu`