Advances in Mathematics of Communications
Volume X, No. 0X, 200X, X–XX

THERE IS NO $[24, 12, 9]$ DOUBLY-EVEN SELF-DUAL CODE OVER $\mathbb{F}_4$

Sihuang Hu

Department of EE–Systems
Tel Aviv University
Tel Aviv, Israel

Gabriele Nebe

Lehrstuhl D für Mathematik
RWTH Aachen University
52056 Aachen, Germany

(Communicated by Aim Sciences)

Abstract. We show that there is no $[24, 12, 9]$ doubly-even self-dual code over $\mathbb{F}_4$ by attempting to construct the generator matrix of this code directly.

1. Introduction

Some of the nicest and best known error-correcting codes are found among self-dual codes. The theory of self-dual codes has strong connections with other areas of combinatorics, group theory and lattices. Of particular interest are extremal doubly-even self-dual binary codes with length divisible by 24 because for any nonzero weight w, the codewords of weight w form a 5-design [1]. In 1991, Quebbemann [10] introduced a generalization of doubly-even codes to arbitrary finite fields of characteristic 2. Over the field $\mathbb{F}_4$ these doubly-even self-dual codes are called "Type II" codes in [3, 6, 2]. In [6], Gaborit, Pless, Solé and Atkin proved the mass formula for doubly-even self-dual codes over $\mathbb{F}_4$ and classified them up to length 8. The classification results of length 12 and 16 are given by Betsumiya, Gulliver, Harada, and Munemasa [3] and Betsumiya [2] respectively. Nebe, Quebbemann, Rains and Sloane [9] studied the complete weight enumerators of these codes. Note that the proof of [9, Theorem 21] for the case $n = 24$ errornessly investigated only an affine sublattice of the relevant set of integral polynomials and concluded that for a $[24, 12, 9]$ doubly-even self-dual code $\mathcal{C}$ over $\mathbb{F}_4$ the number of codewords in the subcode $\mathcal{C} \cap \mathbb{F}_2^{24}$ is divisible by 3 and hence not a power of 2. The diploma thesis [7, Section 9.6.1] corrected this error by showing that there are exactly two possible candidates for complete weight enumerators of $[24, 12, 9]$ doubly-even self-dual codes over $\mathbb{F}_4$. The aim of the present paper is to show that none of these candidates is a weight enumerator of such a code, so the statement of [9, Theorem 21] is correct. Using extensive computations in Magma and Sage we attempt to construct the generator matrix of a $[24, 12, 9]$ doubly-even code over $\mathbb{F}_4$ directly. It turns out that there is no such code, which shows that the largest possible minimum

2010 *Mathematics Subject Classification:* Primary: 94B05;
Key words and phrases: Doubly-even, self-dual.
The first author is supported by a Sino-German (CSC-DAAD) Postdoc Scholarship Program.

Hamming distance d of a doubly-even self-dual code over $\mathbb{F}_4$ of length n is given as in [9, Theorem 21]:

n	4	8	12	16	20	24
d	3	4	6	6	8	8

2. Preliminaries

Let $\mathbb{F}$ denote a field. As usual an $[n,k,d]$ code $\mathcal{C}$ over $\mathbb{F}$ is a k-dimensional subspace of $\mathbb{F}^n$ so that the minimum Hamming distance of $\mathcal{C}$ is d. The dual code of $\mathcal{C}$ is

$$\mathcal{C}^\perp := \{x \in \mathbb{F}^n \mid \sum_{i=1}^{n} x_i c_i = 0 \text{ for all } c \in \mathcal{C}\}.$$

Lemma 1. *Let $\mathcal{C}$ be an $[n,k,d]$ linear code over $\mathbb{F}$. Let $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ be any weight d word of $\mathcal{C}$ with $v_i = 1$ for some i. Then there exists a code $\mathcal{C}'$, permutation equivalent to $\mathcal{C}$, generated by $G' = [I_k \mid A']$, such that $\mathbf{v}'$, the codeword of $\mathcal{C}'$ corresponding to $\mathbf{v}$, is the first row of G'.*

Proof. Up to permutation equivalence we can assume that $v_1 = 1$ and $v_i = 0$ for $2 \le i \le n-d+1$. Define a projection $\pi : \mathcal{C} \to \mathbb{F}^{n-d+1}$ by $\pi(\mathbf{c}) = (c_1, \ldots, c_{n-d+1})$ for $\mathbf{c} = (c_1, \ldots, c_n) \in \mathcal{C}$. If $\pi(\mathbf{c}) = 0$, then $\mathrm{wt}(\mathbf{c}) \le d-1$, implying that $\mathbf{c}$ is the all-zero word. So π is injective and its image has dimension $k = \dim(\mathcal{C})$. Let G be a generator matrix for the code $\mathcal{C}$ with its first row equal to the word $\mathbf{v}$. Since $\dim(\pi(\mathcal{C})) = k$, there exist k linearly independent columns $\mathcal{I}$ of the first $n-d+1$ columns of G. We have $1 \in \mathcal{I}$, otherwise the rank of columns $\mathcal{I}$ will be less than k. Applying a permutation to the first $n-d+1$ coordinates of $\mathcal{C}$ (fixing column 1), we can get a code $\mathcal{C}'$ such that the first k coordinates form an information set for $\mathcal{C}'$. Now the code $\mathcal{C}'$ has a unique generator matrix of the form $G' = [I_k \mid A']$ with its first row equal to $\mathbf{v}$. □

Let $\mathcal{C}$ be an $[n, n/2]$ self-dual code. Fix n_1 and n_2 so that $n_1 + n_2 = n$. Let $\mathcal{B}$ and $\mathcal{D}$ be the largest subcode of $\mathcal{C}$ whose support is contained entirely in the left n_1 and right n_2 coordinates, respectively. Suppose $\mathcal{B}$ and $\mathcal{D}$ have dimensions k_1 and k_2, respectively. Let $k_3 = n/2 - k_1 - k_2$. Then there exists a generator matrix for $\mathcal{C}$ in the form

$$\mathrm{gen}(\mathcal{C}) = \begin{pmatrix} B & O \\ O & D \\ E & F \end{pmatrix}$$

where B is a $k_1 \times n_1$ matrix with $(B\ O)$ being a generator matrix for $\mathcal{B}$, D is a $k_2 \times n_2$ matrix with $(O\ D)$ being a generator matrix for $\mathcal{D}$, O is a zero matrix of appropriate size, and $(E\ F)$ is a $k_3 \times n_3$ matrix. Let $\mathcal{B}^*$ be the code of length n_1 generated by B, $\mathcal{B}_E$ be the code of length n_1 generated by the rows of B and E, $\mathcal{D}^*$ be the code of length n_2 generated by D, $\mathcal{D}_F$ be the code of length n_2 generated by the rows of D and F. The following result is known as the *Balance Principle* [8, Theorem 9.4.1].

Lemma 2. *(i)* $\mathrm{rank}(E) = \mathrm{rank}(F) = k_3$;
(ii) $n_1 - 2k_1 = n_2 - 2k_2$;
(iii) $\mathcal{B}_E^\perp = \mathcal{B}^*, \mathcal{D}_F^\perp = \mathcal{D}^*$.

3. The main result

This section describes the computations that lead to the main result of this note, the non-existence of a doubly-even self-dual code over $\mathbb{F}_4$ of length 24 with minimum distance ≥ 9. Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ be the finite field of order 4.

Definition 3. (Quebbemann [10]) A vector $c \in \mathbb{F}_4^n$ is called *doubly-even* if $\sum_{i=1}^n c_i = \sum_{i<j} c_i c_j = 0$. We say that a linear code $\mathcal{C} \leq \mathbb{F}_4^n$ is *doubly-even* if each codeword in $\mathcal{C}$ is doubly-even.

Doubly-even codes are self-orthogonal. This follows from the identity

$$\sum_{i<j}(c_i + c_i')(c_j + c_j') = \sum_{i<j} c_i c_j + \sum_{i<j} c_i' c_j' + \sum_{i=1}^n c_i \sum_{i=1}^n c_i' - \sum_{i=1}^n c_i c_i'.$$

We will show the following theorem.

Main Theorem. *Let $\mathcal{C} \leq \mathbb{F}_4^{24}$ be a doubly-even self-dual code. Then $d(\mathcal{C}) \leq 8$.*

For the proof let $\mathcal{C}$ be a doubly-even self-dual code in $\mathbb{F}_4^{24}$ so that its minimum Hamming weight is $d(\mathcal{C}) \geq 9$. Then by [7, Section 9.6.1] there are two possibilities for the complete weight enumerator of $\mathcal{C}$:

$$p_1 = x_0^{24} + 2280 x_0^{15} x_1^3 x_\omega^3 x_{\omega^2}^3 + 2652(x_0^{14} x_1^6 x_\omega^2 x_{\omega^2}^2 + x_0^{14} x_1^2 x_\omega^6 x_{\omega^2}^2 + x_0^{14} x_1^2 x_\omega^2 x_{\omega^2}^6) + \dots$$
$$p_2 = x_0^{24} + 2376 x_0^{15} x_1^3 x_\omega^3 x_{\omega^2}^3 + 2508(x_0^{14} x_1^6 x_\omega^2 x_{\omega^2}^2 + x_0^{14} x_1^2 x_\omega^6 x_{\omega^2}^2 + x_0^{14} x_1^2 x_\omega^2 x_{\omega^2}^6) + \dots$$

In particular $d(\mathcal{C}) = 9$. Replacing $\mathcal{C}$ by a permutation equivalent code, we assume that

$$\alpha := (1\ 1\ 1\ \omega\ \omega\ \omega\ \omega^2\ \omega^2\ \omega^2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0) \in \mathcal{C}.$$

We apply the Balance Principle with $n_1 = 9$ and $n_2 = 15$:

Corollary 4. *Let $\mathcal{C}$ be a doubly-even self-dual code in $\mathbb{F}_4^{24}$ containing the vector α from above and so that its minimum Hamming weight is $d(\mathcal{C}) \geq 9$. Then $\mathcal{C}$ has a generator matrix of the form*

$$\mathrm{gen}(\mathcal{C}) = \begin{pmatrix} 1\ 1\ 1\ \omega\ \omega\ \omega\ \omega^2\ \omega^2\ \omega^2 & 0 \\ & O \quad D \\ & E \quad F \end{pmatrix}$$

with $D \in \mathbb{F}_4^{4\times 15}$. In the notation of Lemma 2 the code $\mathcal{B}$ is the one-dimensional code generated by the vector α, $k_1 = 1$, and $k_2 = 4$. Also $\mathcal{D}^*$ is a $[15, 4, d]$ doubly-even code with minimum distance $d \geq 9$.

Lemma 5. *In the notation of Corollary 4 let $\mathcal{D}_F = (\mathcal{D}^*)^\perp$ be the code with generator matrix $\begin{pmatrix} D \\ F \end{pmatrix} \in \mathbb{F}_4^{11\times 15}$. Then the minimum weight of $\mathcal{D}_F$ is greater than 2.*

Proof. Suppose that there exists a codeword $y \in \mathcal{D}_F$ with weight 2. Then we can find a codeword $\beta = (x\ y) \in \mathcal{C}$, where $x \in \mathbb{F}_4^9$ with $\mathrm{wt}(x) \geq 7$. Consider the multiset $\{\beta_i \alpha_i^{-1} \mid i \in \mathrm{supp}(x)\}$ consisting of non-zero values, where $\alpha \in \mathcal{C}$ is the vector defined above. As this multiset contains at least 7 elements one of the 3 non-zero elements in $\mathbb{F}_4$ has to occur at least 3 times. Denote this common value by a. Then the weight of the codeword $\beta - a\alpha$ is less than 9, which is impossible. Similar arguments show that there is no codeword of weight 1 in $\mathcal{D}_F$. The lemma follows. □

A linear code is called *projective* if its dual distance is greater than 2. ¿From the above discussion, we know that the code $\mathcal{D}^*$ is a $[15, 4, d]$ doubly-even projective code with minimum distance $d \geq 9$.

3.1. THE $[15, 4, \geq 9]$ DOUBLY-EVEN PROJECTIVE CODES $\mathcal{D}^*$. Using direct computations we show the following proposition.

Proposition 6. *Let $\mathcal{D}^*$ be a $[15, 4, d]$ doubly-even projective code with minimum distance $d \geq 9$. Then $d = 9$ and there are* 18231 *such $[15, 4, 9]$ codes $\mathcal{D}^*$ up to permutation equivalence.*

TABLE 1. Number of nonisomorphic doubly-even $[11 + r, r, d]$

r	d=9	d=10
1	1	1
2	39	4
3	1180	1
4	18231*	0*

Here * indicates that we only count projective codes.

Proof. By the Griessmer bound the minimum weight of $\mathcal{D}^*$ is either 9 or 10. We can easily check that there is only one weight 9 doubly-even vector

$$(1\ 0\ 0\ 0\ 0\ 0\ 0\ \omega\ \omega\ \omega\ \omega^2\ \omega^2\ \omega^2\ 1\ 1)$$

and one weight 10 doubly-even vector

$$(1\ 0\ 0\ 0\ 0\ 0\ w\ w\ w^2\ w^2\ 1\ 1\ 1\ 1\ 1)$$

in $\mathbb{F}_4^{15}$ up to permutation equivalence and multiplication by elements in $\mathbb{F}_4^*$.

By Lemma 1, every $[15, 4, 9]$ doubly-even projective code over $\mathbb{F}_4$ is permutation equivalent to a code which has a generator matrix of the following form

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & w & w & w & w^2 & w^2 & w^2 & 1 & 1 \\ 0 & 1 & 0 & 0 & & & & & & & & & & & \\ 0 & 0 & 1 & 0 & & & & & & \mathrm{A} & & & & & \\ 0 & 0 & 0 & 1 & & & & & & & & & & & \end{pmatrix}$$

where A is a 3×11 matrix over $\mathbb{F}_4$. We attempt to complete this generator matrix row by row. For each row in turn, our first step is to create a list of candidates. A row vector is a candidate if the subcode generated by the completed rows is doubly-even and has minimum distance 9. For Row 4, we should also check that the generated subcode is projective. We then check for permutation equivalence among the subcodes generated by the completed rows. Our method for testing isomorphism of codes is based on that of Feulner [5]. The results are shown in Table 1 (column d=9), showing that there are in total 18231 nonisomorphic $[15, 4, 9]$ doubly-even projective codes.

Similarly, every $[15, 4, 10]$ doubly-even projective code is permutation equivalent to a code which has a generator matrix of the following form

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & w & w & w^2 & w^2 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & & & & & & & & & & & \\ 0 & 0 & 1 & 0 & & & & & & \mathrm{A} & & & & & \\ 0 & 0 & 0 & 1 & & & & & & & & & & & \end{pmatrix}$$

where A is a 3×11 matrix over $\mathbb{F}_4$. The results are shown in Table 1 (column d=10). Hence there is no $[15, 4, 10]$ doubly-even projective code. □

3.2. Completing the remaining rows. This final section completes the proof of the Main Theorem.

For each of the $[15, 4, 9]$ doubly-even projective codes $\mathcal{D}^*$ from Proposition 6 we choose a generator matrix $D \in \mathbb{F}_4^{4\times 15}$ of $\mathcal{D}^*$ and use Magma to compute a matrix $F \in \mathbb{F}_4^{7\times 15}$ such that the dual code $(\mathcal{D}^*)^\perp = \mathcal{D}_F$ is generated by the rows of D and F. To simplify computations we try to find matrices F whose rows have small weight: for 18217 out of 18231 nonisomorphic codes $\mathcal{D}^*$ from Proposition 6 the row vectors of F can be chosen to be all-one vector and six weight 3 vectors. Then we try to complete the generator matrix of $\mathcal{C}$ as in Corollary 4 by filling the matrix $E \in \mathbb{F}_4^{7\times 9}$ row by row. Let us illustrate this by an example.

Example 1. Let $\mathcal{D}^*$ be a $[15, 4, 9]$ doubly-even projective code with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & w & w & w & w^2 & w^2 & w^2 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & w^2 & w^2 & w^2 & w & w & w & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & w^2 & w^2 & 0 & w & w^2 & 0 & 0 & w & w & 1 \\ 0 & 0 & 0 & 1 & 1 & w & w^2 & w^2 & 0 & w & 0 & w & w^2 & 1 & 0 \end{pmatrix}.$$

Then $\mathcal{C}$ has a generator matrix of the following form

$$\begin{pmatrix} 111\omega\omega\omega\omega^2\omega^2\omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 0 & 0 & 0 & w & w & w & w^2 & w^2 & w^2 & 1 & 1 \\ \mathrm{O} & 0 & 1 & 0 & 0 & 0 & 1 & 1 & w^2 & w^2 & w^2 & w & w & w & 0 & 0 \\ & 0 & 0 & 1 & 0 & 1 & w^2 & w^2 & 0 & w & w^2 & 0 & 0 & w & w & 1 \\ & 0 & 0 & 0 & 1 & 1 & w & w^2 & w^2 & 0 & w & 0 & w & w^2 & 1 & 0 \\ 1111111\ \ 1\ \ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ & 0 & 0 & 0 & 0 & 0 & 0 & 1 & w^2 & 0 & 0 & 0 & 0 & w & 0 & 0 \\ & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w & 0 & 0 & 0 & w^2 & 0 \\ \mathrm{wt} \geq 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & w^2 & w & 0 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & w^2 & 0 & 0 & w & 0 \\ & 0 & 1 & 0 & 0 & w^2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & w^2 & 0 & w & 0 \end{pmatrix}.$$

As the first row of F is the all-one vector, also the first row of E needs to be the all-one vector. To complete the remainder of the matrix E, we use the method described earlier. We find (up to equivalence) 6 possibilities for the second row of E, 442 possibilities for the third row of E, then 8202, 6843, only 2 possibilities for rows 4–6, and none of them can be completed to obtain a generator matrix of a self-dual doubly-even $[24, 12, 9]$ code over $\mathbb{F}_4$. Therefore there is no $[24, 12, 9]$ doubly-even code in this case.

Similar computations exclude all the 18231 possibilities from Proposition 6. Thus we have proved that there is no $[24, 12, 9]$ doubly-even self-dual code over $\mathbb{F}_4$ and hence completed the proof of the Main Theorem.

Acknowledgements

All results are obtained using extensive computations in Magma [4] and Sage [11].

References

[1] E. F. Assmus Jr. and H. F. Mattson Jr., New 5-designs, *J. Combinatorial Theory*, **6** (1969), 122–151.

[2] K. Betsumiya, On the classification of type II codes over $\mathbb{F}_{2^r}$ with binary length 32, *Preprint*.

[3] K. Betsumiya, T. A. Gulliver, M. Harada and A. Munemasa, On type II codes over $\mathbb{F}_4$, *IEEE Trans. Inform. Theory*, **47** (2001), 2242–2248, URL `http://dx.doi.org/10.1109/18.945245`.

[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** (1997), 235–265, URL http://dx.doi.org/10.1006/jsco.1996.0125, Computational algebra and number theory (London, 1993).

[5] T. Feulner, The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes, *Adv. Math. Commun.*, **3** (2009), 363–383, URL http://dx.doi.org/10.3934/amc.2009.3.363.

[6] P. Gaborit, V. Pless, P. Solé and O. Atkin, Type II codes over $\mathbb{F}_4$, *Finite Fields Appl.*, **8** (2002), 171–183, URL http://dx.doi.org/10.1006/ffta.2001.0333.

[7] A. Günther, *Codes und Invariantentheorie*, Master's thesis, RWTH Aachen, 2006, URL http://www.math.rwth-aachen.de/~Gabriele.Nebe/dipl/guenther.pdf.

[8] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003, URL http://dx.doi.org/10.1017/CBO9780511807077.

[9] G. Nebe, H.-G. Quebbemann, E. M. Rains and N. J. A. Sloane, Complete weight enumerators of generalized doubly-even self-dual codes, *Finite Fields Appl.*, **10** (2004), 540–550, URL http://dx.doi.org/10.1016/j.ffa.2003.12.001.

[10] H.-G. Quebbemann, On even codes, *Discrete Math.*, **98** (1991), 29–34, URL http://dx.doi.org/10.1016/0012-365X(91)90410-4.

[11] W. Stein et al., *Sage Mathematics Software (Version 6.4.1)*, The Sage Development Team, 2014, http://www.sagemath.org.