Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 99–104*

A novel sparse orthogonal matrix construction over the fields of characteristic two [1]

Yuri L. Borissov youri@math.bas.bg
Department of Mathematical Foundation of Informatics, Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria
Moon Ho Lee moonho@jbnu.ac.kr
Institute of Information and Communication, Chonbuk National University, 561-756 Jeonju, R. of Korea

Abstract. In this paper, we present a construction of orthogonal matrices over the fields of characteristic two which to the best of our knowledge has attracted minor attention in the existing literature. An interesting feature of the proposed construction is that when applied iteratively very soon the matrices obtained become sparse.

1 Introduction

It is well-known that orthogonal matrices (transforms) play an important role in many branches of mathematics and physics (see, e.g. [1] and [2], respectively) as well as they have numerous applications in contemporary information technologies (see, e.g. [3] – [5]). In mathematics, apart from the classical orthogonal matrices over the field $\mathcal{R}$ of real numbers having great importance in the theory of isometries, the orthogonal matrices over finite characteristic fields (in particular, over finite fields) were well studied too, for instance in connection with some classes of linear codes (see, [6] and [7]).

An widely applicable approach to constructing new mathematical objects (e.g., matrices, codes, etc.) is by making use of similar objects of smaller sizes, orders or dimensions (see, e.g. [8], [9], etc.). In this paper, we apply such an approach to yield orthogonal matrices over field of characteristic two, starting with matrices of four times smaller size. The origins of the proposed construction could be found in [10].

The paper is organized as follows. In the next section we give some necessary definitions and preliminaries. In Section II and Section III, we present our results and examples, respectively, and the paper ends with some conclusions.

[1] This research is partially supported by WCU R32-2012-000-20014-0, NRF, Korea.

2 Preliminaries

First, we recall some definitions.

Definition 1. *A square matrix* $\mathbf{A}$ *of size* n *over the filed* $\mathcal{F}$ *is said to be orthogonal if*

$$\mathbf{A}\mathbf{A}^T = \mathbf{I},$$

where $\mathbf{I}$ *denotes the identity matrix of the same size, and (as usually) the notation* $\mathbf{M}^T$ *is used for the transpose matrix of a given matrix* $\mathbf{M}$*.*

Note also, that Definition 1 implies that $\mathbf{A}$ is an orthogonal just when $\mathbf{A}^T = \mathbf{A}^{-1}$, and hence $\mathbf{A}^T(\mathbf{A}^T)^T = \mathbf{A}^T\mathbf{A} = \mathbf{I}$, i.e. $\mathbf{A}^T$ is an orthogonal matrix as well.

Definition 2. *The ratio* $\Delta(\mathbf{A}) = N/n^2$*, where* N *is the number of nonzero entries of a square matrix* $\mathbf{A}$ *of size* n*, we call density of that matrix.*

An non-singular matrix must contain in each row/column at least one nonzero entry. Therefore, for the density of a such matrix $\mathbf{A}$ of size n, we have the following lower bound:

$$1/n \leq \Delta(\mathbf{A}).$$

In particular, this bound is valid for the orthogonal matrices.

Definition 3. *A square matrix* $\mathbf{P}$ *that has exactly one nonzero entry in each row and each column is said to be permutation matrix.*

The matrices which are simultaneously permutation and orthogonal over some field could be easily characterized. Namely, every non-zero element of such a matrix equals either to 1 or to -1. Therefore over field of characteristic two, every permutation orthogonal matrix is a binary matrix.

Note also, that the lower bound for the density of non-singular matrices is achieved in the set of permutation matrices, i.e. for arbitrary permutation matrix $\mathbf{P}$ of size n, we have: $\Delta(\mathbf{P}) = 1/n$.

3 The construction

At the beginning of this section, we again underline that all matrices considered in this paper are square matrices.

Let $\mathbf{M}$ be a matrix of size n, and $\mathbf{O}$ and $\mathbf{I}$ denote the all-zero and the identity matrix of the same size, respectively. We introduce two matrix operators A_* and B_* involving $\mathbf{M}$.

- A_* maps the matrix $\mathbf{M}$ into a matrix of size $2n$ defined as:

$$\alpha(\mathbf{M}) = \begin{pmatrix} \mathbf{I} & \mathbf{O} \\ \mathbf{M} & \mathbf{I} \end{pmatrix}$$

- B_* maps the matrix $\mathbf{M}$ into a matrix of size $2n$ defined as:

$$\beta(\mathbf{M}) = \begin{pmatrix} \mathbf{M} & \mathbf{M}^T \\ \mathbf{M}^T & \mathbf{M} \end{pmatrix}$$

Below, for the sake of simplicity with some abuse of notations we shall write A_* instead of $\alpha(\mathbf{M})$, and B_* instead of $\beta(\mathbf{M})$ when the matrix-operand is known by default.

Now, we state the following three simple lemmas.

Lemma 1. *For arbitrary matrix* $\mathbf{M}$ *over a field of characteristic* 2*, it holds:*

$$\mathrm{A}_*{}^2 + (\mathrm{A}_*{}^T)^2 = \mathbf{O}_2, \tag{1}$$

where $\mathbf{O}_2$ *is the all-zero matrix of size twice the size of* $\mathbf{M}$*.*

Lemma 2. *For an orthogonal matrix* $\mathbf{M}$ *over a field of characteristic* 2*, it holds:*

$$\mathrm{A}_*\mathrm{A}_*{}^T + \mathrm{A}_*{}^T\mathrm{A}_* = \mathbf{I}_2, \tag{2}$$

where $\mathbf{I}_2$ *is the identity matrix of size twice the size of* $\mathbf{M}$*.*

Lemma 3. *For arbitrary matrix* $\mathbf{M}$*, it holds:*

$$\mathrm{B}_*\mathrm{B}_*{}^T = \begin{pmatrix} \mathbf{M}\mathbf{M}^T + \mathbf{M}^T\mathbf{M} & \mathbf{M}^2 + (\mathbf{M}^T)^2 \\ \mathbf{M}^2 + (\mathbf{M}^T)^2 & \mathbf{M}\mathbf{M}^T + \mathbf{M}^T\mathbf{M} \end{pmatrix}. \tag{$*$}$$

For a given matrix $\mathbf{M}$ of size n, let $\mathbf{\Gamma}_*$ be the matrix operator that maps $\mathbf{M}$ into a matrix defined as: $\gamma(\mathbf{M}) = \beta(\alpha(\mathbf{M}))$. As a 4×4 block structured matrix $\gamma(\mathbf{M})$ looks as:

$$\gamma(\mathbf{M}) = \begin{pmatrix} \mathbf{I} & \mathbf{O} & \mathbf{I} & \mathbf{M}^T \\ \mathbf{M} & \mathbf{I} & \mathbf{O} & \mathbf{I} \\ \mathbf{I} & \mathbf{M}^T & \mathbf{I} & \mathbf{O} \\ \mathbf{O} & \mathbf{I} & \mathbf{M} & \mathbf{I} \end{pmatrix}$$

The main theorem of this paper is stated as follows.

Theorem 1. *For arbitrary orthogonal matrix* $\mathbf{A}$ *over a field of characteristic two, the operator* $\mathbf{\Gamma}_*$ *defined above maps* $\mathbf{A}$ *into an orthogonal matrix.*

Proof. The proof follows by equation (*) substituting $\mathbf{M}$ with $\mathrm{A}_* = \alpha(\mathbf{A})$, and then taking into account the equations (2) and (1). □

The next proposition is about the density of the matrices obtained by $\mathbf{\Gamma}_*$.

Proposition 1. *For arbitrary matrix* $\mathbf{M}$ *of size* n*, it holds:* $\Delta(\gamma(\mathbf{M})) = \frac{1}{2} * 1/n + \frac{1}{4}\Delta(\mathbf{M})$.

In many cases of interest it might be useful to repeat iteratively the described construction. More formally, starting from some initial orthogonal matrix $\mathbf{A}_0$ over a field $\mathcal{F}$ with $char(\mathcal{F}) = 2$, let us define $\mathbf{A}_m = \gamma(\mathbf{A}_{m-1})$, for $m = 1, 2, \ldots$. By Theorem 1, the matrix $\mathbf{A}_m$ will be an orthogonal matrix over $\mathcal{F}$ of size $4^m \times$ size of $\mathbf{A}_0$.

By induction on m it can be proven a proposition about the density of $\mathbf{A}_m$ in terms of the size and density of the initial matrix $\mathbf{A}_0$.

Proposition 2. *Let* $\mathbf{A}_0$ *be a matrix of size* n*. Then for the density of the matrix* $\mathbf{A}_m$ *defined above, it holds:*

$$\Delta(\mathbf{A}_m) = \frac{m}{2^{2m-1}}.\frac{1}{n} + \frac{1}{4^m}\Delta(\mathbf{A}_0).$$

Corollary 1. *If a permutation matrix* $\mathbf{P}$ *is picked up as initial seed in the above described iterative procedure then the density of the matrix* $\mathbf{A}_m$ *obtained after the* $m-th$ *stage,* $m \geq 1$*, is:*

$$\Delta(\mathbf{A}_m) = \frac{2m+1}{4^m}\Delta(\mathbf{P}).$$

The above proposition and subsequent corollary show sub-exponential decreasing in the density of the constructed matrices when m increases.

4 Examples

To illustrate the construction, we shall present two examples.

Example 1. *The first example is the simplest possible where* $\mathbf{P}_0 = (1)$*. The matrix* $\mathbf{P}_1 = \gamma(\mathbf{P}_0)$ *is the following:*

$$\mathbf{P}_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Let $\mathbf{A_{16}}$ *be the tensor square of the matrix* $\mathbf{P}_1$. $\mathbf{A_{16}}$ *is an orthogonal matrix, too. The* 16×32 *matrix* $[\mathbf{I}_{16}|\mathbf{A_{16}}]$ *is a generator matrix of a linear code of length* 32 *having the following weight distribution:*

$$(0,1),(6,32),(8,300),(10,1952),(12,6976),(14,14400),(16,18214),$$
$$(18,14400),(20,6976),(22,1952),(24,300),(26,32),(32,1),$$

and automorphism group of order 23040. *This self-dual code is not an optimal (the minimum weight of the optimal self-dual codes of length 32 being* 8*) but it is included in the table of the self-dual codes of that length given in [11, p. 19].*

Example 2. *Let* $\mathcal{F}$ *be an arbitrary field with* $char(\mathcal{F}) = 2$, *and* θ *be an arbitrary element of* $\mathcal{F}$. *Denote* $\bar{\theta} = \theta + 1$. *The identities* $\theta^2 + \bar{\theta}^2 = 1$ *and* $\theta\bar{\theta} + \bar{\theta}\theta = 0$ *can be easily checked. They imply that the following*

$$\mathbf{A}_0 = \begin{pmatrix} \theta & \bar{\theta} \\ \bar{\theta} & \theta \end{pmatrix}$$

is an orthogonal matrix over $\mathcal{F}$, *so that* $\mathbf{A}_0$ *can be used as a seed in the described construction. For instance,* $\mathbf{A}_1 = \gamma(\mathbf{A}_0)$ *looks as:*

$$\mathbf{A}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & \theta & \bar{\theta} \\ 0 & 1 & 0 & 0 & 0 & 1 & \bar{\theta} & \theta \\ \theta & \bar{\theta} & 1 & 0 & 0 & 0 & 1 & 0 \\ \bar{\theta} & \theta & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & \theta & \bar{\theta} & 1 & 0 & 0 & 0 \\ 0 & 1 & \bar{\theta} & \theta & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & \theta & \bar{\theta} & 1 & 0 \\ 0 & 0 & 0 & 1 & \bar{\theta} & \theta & 0 & 1 \end{pmatrix}$$

Let us also remark that all 2×2 *orthogonal matrices over* $\mathcal{F}$ *are of the form of* $\mathbf{A}_0$ *for some* θ *as it can be easily proven.*

5 Conclusion

In this paper, we have focussed on a little popular construction of orthogonal matrices over the fields of characteristic two. When this construction is applied iteratively, we prove that the density of the produced matrices decreases sub-exponentially with the number of iterations. This feature may be advantageous in applications where sparse orthogonal matrices are preferable.

Acknowledgments

We would like to thank Dr. Nikolay Yankov for useful discussions and help with the GAP system.

References

[1] G. A. Jones, Symmetry, *Handbook of Applicable Mathematics, Combinatorics and Geometry,* W. Lederman and S. Vajda, Eds., Chichester and New York: Wiley, 1985, vol. 5, pp. 329–422.

[2] T. L. Chow, *Mathematical Methods for Physicists: A Concise Introduction,* Cambridge University Press, 2000.

[3] K. R. Rao and N. U. Ahmed, Orthogonal transforms for digital signal processing, in *Proc. Acoustics, Speech, and Signal Processing,* IEEE, 1976.

[4] T. N. Ruckmongathan and A. R. Shashidhara, Sparse Orthogonal Matrices for Scanning Liquid Crystal Displays, *J. Display Technol.* 1, 2005, pp. 240–247.

[5] S. S. Adams, A Journey of Discovery: Orthogonal Matrices and Wireless Communications, *Contemporary Mathematics,* vol. 479, 2009.

[6] J. L. Massey, Orthogonal, Antiorthogonal and Self-Orthogonal Matrices and their Codes, *unpublished manuscript, available online: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.36.3608*, 1998.

[7] F. J. MacWilliams, Orthogonal Matrices Over Finite Fields, *American Mathematical Monthly,* vol. 76, no. 2, 1969, pp. 152–164.

[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[9] J. Seberry, and X. M. Zhang, Some Orthogonal Matrices Constructed by Strong Kronecker Multiplication, *Australasian Journal of Combinatorics* vol. 1, 1993, pp.213–224.

[10] G. L. Feng, and M. H. Lee, An Explicit Construction of Co-Cyclic Jacket Matrices with Any Size, *5th Shanghai Conference in Combinatorics*, Shanghai, China, May 2005.

[11] R. T. Bilous and G. H. J. van Rees, An Enumeration of Binary Self-Dual Codes of Length 32, *available online at http://www.cs.umanitoba.ca/ vanrees/bil.pdf.*