A Novel Sparse Orthogonal Matrix Construction over the Fields of Characteristic 2

Yuri L. Borissov[1] Moon Ho Lee[2]

[1]Department of Mathematical Foundations of Informatics
Institute of Mathematics and Informatics, BAS, Bulgaria

[2]Institute of Information and Communication
Chonbuk National University, R. of Korea

ACCT-13, 2012

Outline of Topics

- Some Preliminaries
- Description of the Construction
- Sparseness of the Constructed Matrices
- Examples

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 $\mathbf{M}^T$ stands for the transpose matrix of a given matrix $\mathbf{M}$.

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.
- The lower bound is achieved in the set of permutation matrices, i.e.

  $$\Delta(\mathbf{P}) = 1/n,$$

  for arbitrary permutation matrix $\mathbf{P}$ of size n.

Let **M** be a matrix of size *n*, and **O** and **I** denote the all-zero and the identity matrix of the same size, respectively.
We introduce two matrix mappings α and β involving **M**.

- α maps the matrix **M** into a matrix of size 2*n* defined as:

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

- β maps the matrix **M** into a matrix of size 2*n* defined as:

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

Let γ be the superposition of α and β, i.e. γ maps the matrix **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:

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

Theorem 3.

For arbitrary orthogonal matrix $\mathbf{M}$ *over a field* $\mathcal{F}$ *of characteristic two, the matrix* $\gamma(\mathbf{M})$ *is orthogonal over* $\mathcal{F}$ *too.*

Starting from some initial orthogonal matrix $\mathbf{A}_0$ over the field $\mathcal{F}$, let us define $\mathbf{A}_m = \gamma(\mathbf{A}_{m-1})$, $m = 1, 2, \ldots$.
By **Theorem 3**, the matrix $\mathbf{A}_m$ will be an orthogonal matrix over $\mathcal{F}$ of size $4^m \times$ size of $\mathbf{A}_0$.

Proposition 4.

For arbitrary matrix $\mathbf{M}$ *of size n, it holds:*

$$\Delta(\gamma(\mathbf{M})) = \frac{1}{2} * 1/n + \frac{1}{4}\Delta(\mathbf{M}).$$

Proposition 5.

Let $\mathbf{A}_0$ *be a matrix of size n. Then for the density of matrix* $\mathbf{A}_m$ *(from the iterative procedure), it holds:*

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

The Sparseness of the Constructed Matrices 2

Corollary 6.

If a permutation matrix $\mathbf{P}_0$ *is picked up as initial seed in the iterative procedure then the density of the matrix* $\mathbf{P}_m$ *obtained after the* $m-$*th stage,* $m \geq 1$, *is:*

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

Proposition 5 and the above corollary show **sub-exponential decreasing** in the density of the constructed matrices with *m*.

Example 7.

The first example is the simplest possible where the seed is: $\mathbf{P}_0 = (1)$.

$$\mathbf{P}_1 = \gamma(\mathbf{P}_0) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Let $\mathbf{A_{16}}$ be the tensor square of the matrix $\mathbf{P}_1$. The 16×32 matrix $[\mathbf{I}_{16}|\mathbf{A_{16}}]$ is a generator matrix of an self-dual code of length 32 whose minimum weight equals 6. But the optimal self-dual codes of length 32 have minimum weight 8, e.g. $RM(2,5)$ is such a code.

Example 8.

Let $char(\mathcal{F}) = 2$, and $\bar{\theta} = \theta + 1$ for an arbitrary $\theta \in \mathcal{F}$. Form the orthogonal 2×2 matrix:

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

$$\mathbf{A}_1 = \gamma(\mathbf{A}_0) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & \theta & \bar{\theta} \\ 0 & 1 & 0 & 0 & 0 & 1 & \bar{\theta} & \theta \\ \theta & \bar{\theta} & 1 & 0 & 0 & 0 & 1 & 0 \\ \bar{\theta} & \theta & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & \theta & \bar{\theta} & 1 & 0 & 0 & 0 \\ 0 & 1 & \bar{\theta} & \theta & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & \theta & \bar{\theta} & 1 & 0 \\ 0 & 0 & 0 & 1 & \bar{\theta} & \theta & 0 & 1 \end{pmatrix}$$

The End

THANK YOU FOR ATTENTION!