Equivalence of Hadamard matrices and Pseudo-Noise matrices

T.Bella[*], V.Olshevsky[*], L.Sakhnovich[*]

ABSTRACT

Several classes of structured matrices (e.g., the Hadamard-Sylvester matrices and the pseudo-noise matrices) are used in the design of error-correcting codes. In particular, the columns of matrices belonging to the above two matrix classes are often used as codewords.

In this paper we show that the two above classes essentially coincide: the pseudo-noise matrices can be obtained from the Hadamard-Sylvester matrices by means of the row/column permutations.

1. INTRODUCTION

This paper will consist of several sections. Section 1 is the introduction, and herein we will present some basic ideas and definitions from the theory of error correcting codes. In Section 2, we introduce PN sequences and PN matrices, and discuss their roles in coding theory. In Section 3, we define the generalized Hadamard matrices, and illustrate their uses in code design. Section 4 contains the main result on the equivalence of the two matrices by factorizations.

The problem that the theory of error-correcting codes addresses is this: We are attempting to transmit a message over a noisy channel, and because of this the message that is received is not necessarily exactly the same message that was sent. In order to be able to communicate reliably over such a channel, we must build into what is sent some kind of redundancy that will allow the receiver to reconstruct the original message with greater reliability. The theory of error-correcting codes is the theory of developing such systems.

The overall process is as follows: First, a message u to be transmitted is given. It is then *encoded* into a codeword x, and then transmitted over the channel. The received codeword y is then *decoded*, and the result is the message (hopefully!). For details of the overall procedure, see for instance [SM77], [L82].

The code that is used consists of the set of codewords that messages are translated into before transmission. In order to establish a system by which codes can be given ratings, we provide some elementary definitions from the theory of error correcting codes.

Definition 1.1. *A length n, q-ary code $\mathcal{C}$ is a subset of the finite field $\mathbb{F}_q^n$. The elements of a code are called codewords.*

Definition 1.2. *The Hamming Distance between two codewords x and y, denoted by $d(x,y)$ is the number of places in which x and y differ:*

$$d(x,y) = |\{i : 1 \leq i \leq n,\ x_i \neq y_i\}| \tag{1.1}$$

Also, the Hamming Weight of a codeword x is $wt(x) = d(x, \mathbf{0})$, where $\mathbf{0} = 000\ldots0$, or the number of non-zero x_i.

The concept of Hamming distance is very important for determining how many errors a code can correct. It provides the concept of a "closest" codeword, in fact, it can be shown that the Hamming distance defines a metric on $\mathbb{F}_q^n$, [SM77], [PW72], [B84].

Definition 1.3. *The minimum distance d of a code $\mathcal{C}$ is given by*

$$d = \min_{x,y \in \mathcal{C}} d(x,y) \tag{1.2}$$

[*] Department of Mathematics, University of Connecticut, Storrs CT 06269-3009, USA

The minimum distance of a code is one of its most important parameters and gives a sense of how "spread out" the codewords of $\mathcal{C}$ are within $\mathbb{F}_q^n$. Intuitively, having the codewords spread out in this fashion should make correcting errors easier, as each error can increase the distance between the sent codeword and the received codeword by at most one.

More precisely, it is well known in coding theory that a code with minimum distance d can correct $\left\lfloor \frac{1}{2}(d-1) \right\rfloor$ errors. See, for instance, [CS91], [SM77], [PW72].

It can be seen from this brief introduction that in order to create codes that are more effective, i.e. can correct more errors, we need to create codes with larger minimum distances. We next introduce PN sequences, and show that they can be used to find codes with this property.

2. PSEUDO-NOISE SEQUENCES

Definition 2.1. *Let k be a positive integer, and $h_0, h_1, \ldots, h_{k-1}$ be given elements of a finite field $\mathbb{F}_q$. A sequence $a_0, a_1, \ldots$ of elements of $\mathbb{F}_q$ satisfying*

$$a_i = a_{i-1}h_{m-1} + a_{i-2}h_{m-2} + \cdots + a_{i-m+1}h_1 + a_{i-m}h_0 \quad \textit{for } i \geq m \tag{2.1}$$

is called a (k^{th} order) linear recurring sequence in $\mathbb{F}_q$.

The recurrence relation satisfied by linear recurring sequences can be written in terms of matrices:

$$\begin{bmatrix} a_{i-(m+1)} \\ a_{i-(m+2)} \\ a_{i-(m+3)} \\ \vdots \\ a_{i-1} \\ a_i \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ h_0 & h_1 & h_2 & \ldots & h_{m-2} & h_{m-1} \end{bmatrix} \begin{bmatrix} a_{i-(m)} \\ a_{i-(m+1)} \\ a_{i-(m+2)} \\ \vdots \\ a_{i-2} \\ a_{i-1} \end{bmatrix} \tag{2.2}$$

Definition 2.2. *The degree m polynomial*

$$h(x) = x^m + h_{m-1}x^{m-1} + \cdots + h_1 x + h_0 \tag{2.3}$$

is called the characteristic polynomial of the linear recurring sequence $\{a_i\}$.

Proposition 2.3. *Let $\mathbb{F}_q$ be any finite field and k be any positive integer. Then every k^{th} order linear recurring sequence is periodic with period at least $r \leq q^k - 1$. Furthermore, equality holds if and only if the corresponding characteristic polynomial $h(x)$ is primitive.*

This proposition can be found, for instance, in [SM77].

Definition 2.4. *For the finite field $\mathbb{F}_q$ and any positive integer k, a Pseudo-Noise (PN) Sequence is a k^{th} order linear recurring sequence with period $q^k - 1$.*

Equivalently, by Proposition 2.3 a PN sequence is a linear recurring sequence whose characteristic polynomial is primitive.

A very important property of PN sequences that directly relates to their uses in generating codes with large minimum distance is their autocorrelation function. The autocorrelation function of a linear recurring sequence gives a sense of how that similar that sequence is to a shifted version of itself.

Definition 2.5. *The autocorrelation function $\rho(\tau)$ for a real or complex sequence $a_0 a_1 a_2 \ldots$ with period r is given by*

$$\rho(\tau) = \frac{1}{r} \sum_{j=0}^{n-1} a_j \bar{a}_{\tau+j} \tag{2.4}$$

We will see next that not only is this function of PN sequences low, but it is level; that is, all cyclic shifts of a PN sequence (except those shifts of multiples of the period) correlate to the unshifted sequence in the same number of places.

PROPOSITION 2.6. *The autocorrelation function $\rho(\tau)$ of a PN sequence $\{a_i\}$ of period r is given by*

$$\rho(\tau) = \begin{cases} 1 & \tau = 0 \\ -\dfrac{1}{r} & 1 \leq \tau \leq r-1 \end{cases} \tag{2.5}$$

Again, this proposition and many other properties of pseudo-noise sequences can be found in [SM77].

We next define the closely related Pseudo-Noise matrices, and we will see how the autocorrelation of PN sequences allows us to use Pseudo-Noise matrices to construct codes of large minimum distance.

DEFINITION 2.7. *A Pseudo-Noise (PN) matrix $T(q,n)$ is an $n \times n$ matrix of the form*

$$T(q,n) = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \tilde{T} & \\ 0 & & & \end{bmatrix} \tag{2.6}$$

where $\tilde{T}$ is a circulant Hankel matrix with each row being a PN sequence with elements from a finite field $\mathbb{F}_q$.

In other words, each row of $\tilde{T}$ is a shifted version of the PN sequence that is the first row of $\tilde{T}$.

To see why the rows of PN matrices are useful in designing codes with large minimum distances, we need only apply Proposition 2.6 above. Notice that a small, constant autocorrelation between a PN sequence and shifted versions of itself imply that distinct rows of PN matrices will differ in a larger number of positions, and thus if used as codewords, they will be far apart. Further, the fact that the autocorrelation function is level for $1 \leq \tau \leq r-1$ shows that the codewords are equidistant.

3. HADAMARD MATRICES

We next present the well-known Hadamard matrices, and a method to construct them of any order $n = 2^m$. Following this, we generalize the idea of a Hadamard matrix, and then show this construction method can be altered to work for the new generalized Hadamard matrices.

3.1. Classical Hadamard matrices and the Sylvester construction

Originally formulated as $n \times n$ matrices $A = [a_{ij}]$, with $|a_{ij}| \leq 1$ for which the maximal determinant inequality

$$|\det(A)| \leq n^{n/2} \tag{3.1}$$

achieves equality, $n \times n$ Hadamard matrices $H(2,n)$ are composed of ± 1's and satisfy

$$H(2,n)H(2,n)^T = nI_n \tag{3.2}$$

that is, distinct rows are orthogonal. The notation $H(2,n)$ is being used to conform with notation to be introduced in Section 3.2.

Classic Hadamard matrices of any order $n = 2^m$ can be constructed by the method of Sylvester, which is based on the following.

Proposition 3.1. *Let $H(2,n)$ be a classic Hadamard matrix. Then the matrix*

$$H(2,2n) = \begin{bmatrix} H(2,n) & H(2,n) \\ H(2,n) & -H(2,n) \end{bmatrix} \tag{3.3}$$

is also a Hadamard matrix.

With this proposition and the observation that

$$H(2,2) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{3.4}$$

is a Hadamard matrix assures that we can generate Hadamard matrices $H(2,2^m)$ for all m. Matrices generated in this fashion we refer to as Hadamard-Sylvester matrices.

The uses of Hadamard matrices for coding can be seen from (3.2). It is easy to see that if two column n-vectors x and y containing only ± 1 as entries satisfy $x^T y = 0$, then x and y must differ in $n/2$ places; that is, their Hamming distance is $n/2$. Since Hadamard matrices consist of ± 1 entries, and (3.2) implies distinct columns are orthogonal, the Hamming distance between any two columns of an $n \times n$ Hadamard matrix is $n/2$. This property parallels that of PN sequences caused by their small, constant autocorrelation function.

3.2. Generalized Hadamard matrices

Definition 3.2. *An $n \times n$ matrix $H(q,n)$ is called a generalized Hadamard matrix if its elements coincide with one of the numbers*

$$\epsilon^k = exp\left(\frac{2\pi i}{q}k\right), \quad 0 \le k \le q-1 \tag{3.5}$$

and such that

$$H(q,n)H(q,n)^* = nI_n \tag{3.6}$$

where $*$ denotes the complex conjugate transposed.

Note that in the case $q = 2$, the generalized Hadamard matrices $H(2,n)$ reduce to the classic Hadamard matrices H_n.

Often times we will be concerned with a matrix that contains not the entries of $H(q,n)$, but the values k from (3.5) corresponding to each entry.

Definition 3.3. *Let $H(q,n) = [h_{ij}]$ be a generalized Hadamard matrix. Then the quasi-random Hadamard matrix corresponding to $H(q,n)$, denoted $H'(q,n) = [h'_{ij}]$ is the matrix such that $h_{ij} = \epsilon^{h'_{ij}}$.*

We will call a matrix $H(q,n)$ normalized if all the elements of the first row and first column are $\epsilon^0 = 1$. Without loss of generality, we will assume that all matrices henceforth are normalized.

The Sylvester method can be generalized to the generalized Hadamard matrices with a Vandermonde-like construction:

Proposition 3.4. *Let $H(q,n)$ be a generalized Hadamard matrix. Then the matrix given by*

$$H(q,qn) = \begin{bmatrix} H(q,n) & H(q,n) & H(q,n) & \dots & H(q,n) \\ H(q,n) & \epsilon H(q,n) & \epsilon^2 H(q,n) & \dots & \epsilon^{q-1} H(q,n) \\ H(q,n) & \epsilon^2 H(q,n) & \epsilon^4 H(q,n) & \dots & \epsilon^{2(q-1)} H(q,n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ H(q,n) & \epsilon^{q-1} H(q,n) & \epsilon^{2(q-1)} H(q,n) & \dots & \epsilon^{(q-1)^2} H(q,n) \end{bmatrix} \tag{3.7}$$

is also a generalized Hadamard matrix.

As with the Sylvester method for classic Hadamard matrices, the previous proposition as well as the generalized Hadamard matrix

$$H(q,q) = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \epsilon & \epsilon^2 & \epsilon^3 & \dots & \epsilon^{q-1} \\ 1 & \epsilon^2 & \epsilon^4 & \epsilon^6 & \dots & \epsilon^{2(q-1)} \\ 1 & \epsilon^3 & \epsilon^6 & \epsilon^9 & \dots & \epsilon^{3(q-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \epsilon^{q-1} & \epsilon^{2(q-1)} & \epsilon^{2(q-1)} & \dots & \epsilon^{(q-1)^2} \end{bmatrix} \tag{3.8}$$

allows us to construct generalized Hadamard matrices $H(q,q^m)$, which we will call the generalized Hadamard-Sylvester matrices.

4. EQUIVALENCE OF THE CLASSES OF MATRICES

Having already shown at this point that the two classes of matrices have properties that imply the codes built from them will have not only large minimum distances, but equal distances between any distinct codewords, we proceed to show the equivalence of the classes. This is to be shown by demonstrating that both matrices admit the same factorization.

In this section, we will assume we are working in the finite field $\mathbb{F}_q$ for some q.

4.1. A factorization of PN matrices

LEMMA 4.1. *For $n = q^m$, the rank of the $n \times n$ PN matrix T is m.*

Proof. This follows immediately from the recurrence relation defining the rows of T given in Equation 2.2 □

THEOREM 4.2. *Let $n = q^m$, and let T be an $n \times n$ PN matrix. Then T admits the decomposition $T = MR$ where M is a $q^m \times m$ matrix, and R is an $m \times q^m$ matrix. Further, the rows of M are all distinct and contain all possible q-ary m-tuples, and the same is true of the columns of R.*

Proof. The factorization $T = MR$ for M of size $q^m \times m$ and R of size $m \times q^m$ exists by Lemma 4.1. By Definition 2.7, the rows of T are distinct, and therefore so are the rows of M. Since M is over $\mathbb{F}_q$ with size $q^m \times m$, we conclude the M must contain all possible q-ary m-tuples as rows.

Similarly, the columns of R are also distinct, and since R is also over $\mathbb{F}_q$, we have that R contains all possible m-tuples as columns, which completes the proof. □

4.2. A factorization of generalized Hadamard matrices

We next wish to show that generalized Hadamard matrices, or more precisely, quasi-random Hadamard matrices, have the same factorization.

THEOREM 4.3. *Let $H'(q,q^m)$ be the quasi-random Hadamard matrix corresponding to the Hadamard-Sylvester matrix $H(q,q^m)$. Then $H'(q,q^m)$ admits the decomposition*

$$H'(q,q^m) = L_m^T L_m \pmod q \tag{4.1}$$

where L_m is a $m \times q^m$ matrix with elements from $\{0,1,\dots,q-1\}$. Further, the columns of L_m contain all possible q-ary m-tuples.

Proof. The proof is by induction on m. Letting $m = 1$, we have

$$H'(q,q) = L_1^T L_1 \pmod q \tag{4.2}$$

with

$$L_1 = \begin{bmatrix} 0 & 1 & 2 & \dots & q-1 \end{bmatrix} \tag{4.3}$$

which by construction contains all q-ary numbers as columns.

Now suppose that the decomposition $H'(q,q^m) = L_m^T L_m \pmod{q}$ is true. Then it follows that

$$H'(q,q^{m+1}) = \begin{bmatrix} 0_m^T & L_m^T \\ 1_m^T & L_m^T \\ \vdots & \vdots \\ (q-1)_m^T & L_m^T \end{bmatrix} \begin{bmatrix} 0_m & 1_m & \dots & (q-1)_m \\ L_m & L_m & \dots & L_m \end{bmatrix} \tag{4.4}$$

modulo q, where we note that

$$r_m = \begin{bmatrix} r & r & \dots & r \end{bmatrix} \tag{4.5}$$

which are of size $1 \times m$.

The fact that L_{m+1} contains all possible q-ary $(m+1)$-tuples as columns is clear from the fact that all possible q-ary m-tuples are present in the columns of L_m by hypothesis, and L_m appears once beneath each of $0_m, 1_m, \dots, (q-1)_m$. This completes the proof. □

Corollary 4.4. *The rank of $H'(q,q^m)$ is m.*

The previous two theorems allow us to conclude the following theorem.

Theorem 4.5. *For integers $q \geq 2$ and $m \geq 0$, let $H(q,q^m)$ be a $q^m \times q^m$ generalized Hadamard matrix, and let $T(q,q^m)$ be an $q^m \times q^m$ PN matrix. Then $H(q,q^m)$ is equivalent to $T(q,q^m)$; that is, there exist permutation matrices P_1 and P_2 such that $H(q,q^m) = P_1 T(q,q^m) P_2$.*

Proof. By Theorem 4.3, $H(q,q^m)$ has a factorization into the product of a $q^m \times m$ matrix and a $m \times q^m$ matrix, each of which contains all possible q-ary m-tuples as rows/columns. By Theorem 4.2, $T(q,q^m)$ also has a factorization into the product of a $q^m \times m$ matrix and a $m \times q^m$ matrix which contain all possible q-ary m-tuples as rows/columns. Thus the factorizations differ only by the order in which the rows/columns appear, and this completes the proof. □

5. CONCLUSION

To conclude, we have demonstrated that the two classes of matrices, those built from PN sequences, and the generalized Hadamard matrices are equivalent up to permutations of the rows and columns. This fact was suggested by the similar properties of the codes generated by the columns of each of these classes.

In the PN matrix case, the autocorrelation function being small and constant gives rise to codes with a large minimum distance, and equally spaced codewords. In the Hadamard case, the orthogonality of distinct columns gives the same results.

The proof was based on a common factorization of the classes, and it was demonstrated that both factors in each factorization must contain, in some order, all possible combinations. This immediately shows that the matrices are unique up to row and column permutation.

REFERENCES

[B84] E.R.Berlekamp *Algebraic Coding Theory*, Aegean Park Press, 1984.

[CS91] J.H.Conway & N.J.A.Sloane *Sphere Packings, Lattices and Groups*, Springer-Verlag, 1991.

[HT99] P.Hoeher, F.Tufvesson *Channel Estimation with Superimposed Pilot Sequence Applied to Multi-Carrier Systems*, Proc. Advanced Signal Processing for Communications Symposium. 1999.

[L82] J.H.van Lint, *Introduction to Coding Theory*, Springer-Verlag, 1982.

[LB98] T.Luo, S.Blostein *Using Sginal Cancellation for Optimum Beamforming in a Cellular CDMA System*, Configurable Computing: Technology and Applications, Proc. (**SPIE 3526**) 1998, 202-211

[MST99a] P.Mukhin, L.Sakhnovich, V.Timofeev *About Equivalence of Hadamard's Matrices*, (in Russian)

[MST99b] P.Mukhin, L.Sakhnovich, V.Timofeev *Characteristics of Silvester Matrices*, (in Russian)

[PW72] W.W.Peterson & E.J.Weldon Jr. *Error-Correcting Codes*, MIT Press, 1972.

[SM77] N.J.A.Sloane & F.J.MacWilliams, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[TSZ96] A.Tewfik, M.Swanson, B.Zhu *Transparent Robust Authentication and Distortion Measurement Technique for Images*, IEEE Digital Signal Processing Workshop (**DSP 96**). Vol. September 1996, 45-48.