Operator Theory:
Advances and Applications, Vol. 1, 1–13

Ranks of Hadamard Matrices and Equivalence of Sylvester Hadamard and Pseudo-Noise Matrices

Tom Bella, Vadim Olshevsky and Lev Sakhnovich

Abstract. In this paper we obtain several results on the rank properties of Hadamard matrices (including Sylvester Hadamard matrices) as well as (generalized) Hadamard matrices. These results are used to show that the classes of (generalized) Sylvester Hadamard matrices and of generalized pseudo-noise matrices are equivalent, i.e., they can be obtained from each other by means of row/column permutations.

Mathematics Subject Classification (2000). Primary 15A57, 15A23; Secondary 05B15, 05B20 .

Keywords. Hadamard matrices, generalized Hadamard matrices, pseudo-random sequences, pseudo-noise sequences, pseudo-random matrices, pseudo-noise matrices, rank, equivalence.

Contents

1. Ranks of certain matrices related to classical Hadamard matrices

1.1. Hadamard and exponent Hadamard matrices

The classical $n \times n$ *Hadamard matrices* $H(2,n)$ are defined as those composed of ± 1's and satisfying

$$H(2,n)H(2,n)^T = nI_n, \tag{1.1}$$

that is, their distinct rows are orthogonal. Hadamard matrices are widely used in communication systems, data compression, error control coding, cryptography, linear filtering and spectral analysis, see, e.g., [H06], [SM77], and the references therein. This popularity of Hadamard matrices is explained, among other reasons, by their simplicity and efficiency in a variety of concrete practical applications. For example, one simple way to construct a Hadamard matrix of the order $n = 2^m$ is due to Sylvester. The method starts with defining 1×1 matrix via $H(2,1) = 1$, and proceeds recursively:

$$H(2,2n) = \begin{bmatrix} H(2,n) & H(2,n) \\ H(2,n) & -H(2,n) \end{bmatrix}. \tag{1.2}$$

It is immediate to see that $H(2,2n)$ of (1.2) satisfies (1.1). Matrices generated in this fashion are referred to as *Sylvester Hadamard* matrices. In addition to the Sylvester construction (1.2), there are alternate ways to construct Hadamard matrices, one of them is due to Paley, see, e.g., [H06] and the references therein.

In many applications it is useful to consider matrices over $GF(2)$, so one typically changes -1's to 0's, e.g.,

$$H(2,2) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \longrightarrow \widetilde{H}(2,2) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \tag{1.3}$$

or, alternatively, one replaces -1's by 1's and 1's by 0's, e.g.,

$$H(2,2) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \longrightarrow \widehat{H}(2,2) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \tag{1.4}$$

We suggest to refer to matrices $\widehat{H}(2,2n)$ and $\widetilde{H}(2,2n)$ obtained in this fashion as *exponent* Hadamard matrices and *complimentary exponent* Hadamard matrices, respectively. (The justification for the above nomenclatures is in that using the entries of $\widehat{H}(2,2n)$ as exponents for -1 one obtains the entries of $H(2,n)$.)

In what follows we will adopt similar notations for any matrix A composed of ± 1's, and denote by $\widetilde{A}$ the matrix obtained from A by changing -1's to 0's, and denote by $\widehat{A}$ the matrix obtained from A by replacing -1's by 1's, and 1's by 0's.

1.2. General Hadamard Matrices and Ranks

In order to study the ranks of arbitrary Hadamard matrices we need to establish the following auxiliary result that applies to row/column scaled $H(2,n)$.

Lemma 1.1. *Let*

$$H(2,n)=\left[\begin{array}{cc} 1 & e \\ e^T & H_{n-1} \end{array}\right] \tag{1.5}$$

be a Hadamard matrix whose first column and top row contain only 1*'s, i.e.,*

$$e=\underbrace{\left[\begin{array}{ccc} 1 & \cdots & 1 \end{array}\right]}_{n-1}.$$

Let $\widetilde{H}_{n-1}$ *denote the complimentary exponent matrix of* H_{n-1} *defined in subsection* 1.1*. Then*

$$\widetilde{H}_{n-1}\widetilde{H}_{n-1}^T=tI_{n-1}+(t-1)J_{n-1}, \quad \text{where} \quad t=\frac{n}{4}, \quad \text{and} \quad J_{n-1}=ee^T. \tag{1.6}$$

Proof. It follows from (1.5) and the definition (1.1) that

$$e+eH_{n-1}^T=0, \qquad J_{n-1}+H_{n-1}H_{n-1}^T=nI_{n-1}. \tag{1.7}$$

Consider an auxiliary matrix

$$B_{n-1}=H_{n-1}+J_{n-1}, \tag{1.8}$$

and observe, before proceeding further, that

$$\widetilde{H}_{n-1}=\frac{1}{2}B_{n-1}. \tag{1.9}$$

In view of (1.7) and (1.8) we have

$$B_{n-1}B_{n-1}^T=H_{n-1}H_{n-1}^T+J_{n-1}H_{n-1}^T+H_{n-1}J_{n-1}+J_{n-1}J_{n-1}=$$

$$(nI_{n-1}-J_{n-1})-J_{n-1}-J_{n-1}+(n-1)J_{n-1}=nI_{n-1}+(n-4)J_{n-1}. \tag{1.10}$$

Finally, (1.6) follows from (1.9) and (1.10). □

We are now ready to prove the following result.

Theorem 1.2. *Let us partition* $H(2,n)$ *by singling its top row and first column out:*

$$H(2,n)=\left[\begin{array}{cc} h_{11} & r_1 \\ c_1 & H_{n-1} \end{array}\right].$$

Here h_{11} *is a scalar, and* H_{n-1} *is an* $(n-1)\times(n-1)$ *submatrix of* $H(2,n)$*. Let* $\widetilde{H}_{n-1}$ *denote the complimentary exponent matrix of* H_{n-1} *defined in Section* 1.1*.*

If 8 *divides* n *then*

$$\mathrm{rank}\widetilde{H}_{n-1}(\mathrm{mod}\ 2)\le\frac{n}{2}. \tag{1.11}$$

If 8 *does not divide* n *then*

$$\mathrm{rank}\widetilde{H}_{n-1}(\mathrm{mod}\ 2)=n-1. \tag{1.12}$$

Proof. Without loss of generality we may assume that $H(2,n)$ has the form shown in (1.5) and that the result in (1.6) holds. Let us consider two cases.

- If 8 divides n then $t = \frac{n}{4}$ is even, and (1.6) implies

$$\widetilde{H}_{n-1}\widetilde{H}_{n-1}^T = J_{n-1}(\text{mod } 2). \tag{1.13}$$

  If we denote by $k = \text{rank } \widetilde{H}_{n-1}(\text{mod } 2)$, then (1.13) implies

$$(n-1) - k \geq k - 1$$

  and (1.11) follows.
- If 8 does not divide n then $t = \frac{n}{4}$ is odd, and (1.6) implies

$$\widetilde{H}_{n-1}\widetilde{H}_{n-1}^T = tI_{n-1}(\text{mod } 2), \tag{1.14}$$

  so that (1.12) follows.

□

1.3. Sylvester Hadamard Matrices, Ranks and Factorizations

In the previous subsection the result applied to arbitrary Hadamard matrices. Here we consider special Sylvester Hadamard matrices. Here is the main result of this subsection.

Theorem 1.3. *Let $H(2, 2^m)$ be a Sylvester Hadamard matrix, i.e., one constructed via the recipe (*1.2*). Then*

$$\text{rank } \widehat{H}(2, 2^m) = m(\text{mod } 2), \tag{1.15}$$

where $\widehat{H}(2, 2^m)$ denotes the exponent matrix of $H(2, 2^m)$ defined in Section 1.1*.*

The result (1.15) follows from the following lemma.

Lemma 1.4. *The Sylvester Hadamard matrix $H(2, 2^m)$ admits the following decomposition*

$$\widehat{H}(2, 2^m) = L_m L_m^T(\text{mod } 2), \tag{1.16}$$

where the rows of the $2^m \times m$ matrix

$$L_m = \begin{bmatrix} 0 & \cdots & 0 & 0 & 0 \\ 0 & \cdots & 0 & 0 & 1 \\ 0 & \cdots & 0 & 1 & 0 \\ 0 & \cdots & 0 & 1 & 1 \\ 0 & \cdots & 1 & 0 & 0 \\ \vdots & \cdots & \vdots & \vdots & \vdots \\ 1 & \cdots & 1 & 1 & 1 \end{bmatrix}$$

contain all possible binary m-tuples ordered naturally.

Proof. It is easy to see that for $m = 1$ we have

$$\widehat{H}(2, 2) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix}.$$

By applying the inductive argument we obtain

$$\widehat{H}(2,2^{m+1}) = \begin{bmatrix} \widehat{H}(2,2^m) & \widehat{H}(2,2^m) \\ \widehat{H}(2,2^m) & \widetilde{H}(2,2^m) \end{bmatrix} = \begin{bmatrix} \overrightarrow{0} & L_m \\ \overrightarrow{1} & L_m \end{bmatrix} \begin{bmatrix} \overrightarrow{0}^T & \overrightarrow{1}^T \\ L_m^T & L_m^T \end{bmatrix} \quad (1.17)$$

with

$$\overrightarrow{0} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \qquad \overrightarrow{1} = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}.$$

The relations (1.17) and (1.16) coincide which completes the proof of the lemma. □

2. Pseudo-Noise Matrices

2.1. Linear recurrence relations and shift registers

Let m be a fixed positive integer, and $h_0, h_1, \ldots, h_{m-1} \in GF(2)$. Consider a linear m-term recurrence relation

$$a_i = a_{i-1}h_{m-1} + a_{i-2}h_{m-2} + \cdots + a_{i-m+1}h_1 + a_{i-m}h_0 \quad \text{for } i \geq m \qquad (2.1)$$

over $GF(2)$. Observe that the above recurrence relation can be written in a matrix form:

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

The m-tuple

$$\{a_{i-m}, \ldots, a_{i-2}, a_{i-1},\}$$

is called the *state vector* corresponding to the time moment $i-m$. The semi-infinite sequence

$$a_0, a_1, a_2, a_3, a_4, a_5, \ldots\ldots, \qquad (2.3)$$

is called an *(m^{th} order) linear recurring sequence* corresponding to (2.1). Clearly, the latter is fully determined by the *initial state vector* $\{a_0, a_1, \ldots, a_{m-2}, a_{m-1}\}$ and the coefficients $h_0, h_1, \ldots, h_{m-1}$ of (2.1).

In order to define the concept of a pseudo-noise sequence it is useful to associate (2.1) with a *shift register*. As an example, consider a special case of (2.1), a 4-term linear recurrence relation with $h_0 = 1, h_1 = 0, h_2 = 0, h_3 = 1$, and visualize

$$a_i = a_{i-1} + a_{i-4} \qquad (2.4)$$

with the help of the following figure:

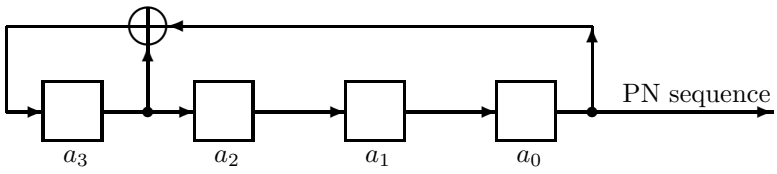

FIGURE 1. Shift register for (2.4). Time moment "zero."

The above figure corresponds to the time moment "zero," i.e., it is characterized by the initial state vector

$$\{a_0, a_1, a_2, a_3\}. \tag{2.5}$$

The next figure corresponds to the time moment "one,"

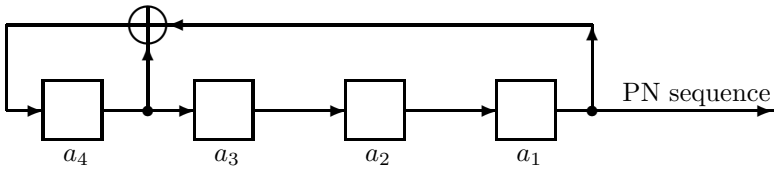

FIGURE 2. Shift register for (2.4). Time moment "one."

and its state vector is

$$\{a_1, a_2, a_3, a_4\} \tag{2.6}$$

is obtained from the one in (2.5) by shifting entries to the left (a_0 disappears), and computing a_4 via (2.4). Figures 1 and 2 graphically express both the shift and computing a_4. That is, a_4 of Figure 2 is computed as $a_3 + a_0$ of Figure 1.

2.2. Pseudo-Noise Sequences and Matrices

Recall that the semi-infinite sequence in (2.3) is fully determined by the *initial state vector* $\{a_0, a_1, \ldots, a_{m-2}, a_{m-1}\}$ and the coefficients $h_0, h_1, \ldots, h_{m-1}$ of (2.1).

Indeed, the rule (2.1) maps the state vectors to the next ones, i.e.,

$$\begin{bmatrix} a_{m-1} \\ a_{m-2} \\ \vdots \\ a_2 \\ a_1 \\ a_0 \end{bmatrix} \longrightarrow \begin{bmatrix} a_m \\ a_{m-1} \\ \vdots \\ a_3 \\ a_2 \\ a_1 \end{bmatrix} \longrightarrow \begin{bmatrix} a_{m+1} \\ a_m \\ \vdots \\ a_4 \\ a_3 \\ a_2 \end{bmatrix} \longrightarrow$$

Since all the elements $\{a_i\}$ belong to $GF(2)$, none of the recurrence relations of the form (2.1) can generate more than $2^m - 1$ different state vectors (we exclude the trivial zero initial state vector). It follows that the sequence in (2.3) has to be periodic with the period not exceeding $2^m - 1$ (of course, there are coefficients $h_0, h_1, \ldots, h_{m-1}$ of (2.1) for which any sequence will have a period smaller that $2^m - 1$).

If the sequence (2.3) has the maximal possible period $2^m - 1$, then it is called a *Pseudo-Noise* sequence, see, e.g., [SM77]. Pseudo-noise sequences are useful in a number of applications, see, e.g., [HT99], [CS91].

A *Pseudo-Noise* matrix $T(2, n)$ with $n = 2^m$ is defined (see, e.g., [SM77]) as an $n \times n$ matrix of the form

$$T(2,n) = \begin{bmatrix} 0 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & \check{T} & \\ 0 & & & \end{bmatrix} \tag{2.7}$$

where $\check{T}$ is a circulant Hankel matrix whose top row is a $1 \times (2^m - 1)$ array that is a period of the pseudo-noise sequence, and whose first m entries coincide with the initial state.

Example. Let us again consider 4-term recurrent relations (2.4) with with $h_0 = 1, h_1 = 0, h_2 = 0, h_3 = 1$ and the initial state

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}.$$

This choice gives rise to the pseudo-noise sequence

$$\underbrace{\mathbf{1000}11110101100}_{\text{period } 15 = 2^3 - 1}\underbrace{\mathbf{1000}11110101100}_{\text{period } 15}\underbrace{\mathbf{1000}11110101100}_{\text{period } 15}\ldots\ldots$$

and the 15×15 matrix $\check{T}$ of (2.7) is given by

$$\check{T} = \begin{bmatrix} 100011110101100 \\ 000111101011001 \\ 001111010110010 \\ 011110101100100 \\ 111101011001000 \\ 111010110010001 \\ 110101100100011 \\ 101011001000111 \\ 010110010001111 \\ 101100100011110 \\ 011001000111101 \\ 110010001111010 \\ 100100011110101 \\ 001000111101011 \\ 010001111010110 \end{bmatrix}.$$

□

2.3. Equivalence of Pseudo-Noise and Sylvester Hadamard Exponent Matrices

In order to establish the equivalence of the two classes of matrices we will need the following counterpart of Theorem 1.3.

Lemma 2.1. *For $n = 2^m$, the rank of any $n \times n$ Pseudo-noise matrix T is m.*

Proof. This follows from the immediate observation that the rows of the matrix

$$\check{T} = \begin{bmatrix} \mathbf{a}_0 \\ \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{2^m-2} \end{bmatrix}$$

satisfy the m-term recurrence relations

$$\mathbf{a}_i = \mathbf{a}_{i-1}h_{m-1} + \mathbf{a}_{i-2}h_{m-2} + \cdots + \mathbf{a}_{i-m+1}h_1 + \mathbf{a}_{i-m}h_0 \tag{2.8}$$

(of the form (2.1)), and hence they are linearly dependent. □

The following theorem implies that the Sylvester Hadamard matrices and Pseudo-noise matrices are equivalent, i.e., they can be obtained from each other via row/column permutations.

Theorem 2.2. *Let $H(2, 2^m)$ be the Sylvester Hadamard matrix, and let $T(2, 2^m)$ be a $2^m \times 2^m$ Pseudo-Noise matrix. Then $H(2, 2^m)$ is equivalent to $T(2, 2^m)$; i.e., there exist permutation matrices P_1 and P_2 such that $H(2, 2^m) = P_1 T(2, 2^m) P_2$.*

Proof. Recall that the matrix $H(2, 2^m)$ admits a factorization (1.16) into the product of a $2^m \times m$ matrix L_m and a $m \times 2^m$ matrix L_m^T, each of which contains all possible binary m-tuples as rows/columns.

Secondly, by Lemma 2.1, $T(2, 2^m)$ also has a similar factorization $T = MR$ where M is a $2^m \times m$ matrix, and R is an $m \times 2^m$ matrix. Further, the rows of M are all distinct and hence they must contain all possible binary m-tuples, and the same is true of the columns of R.

Hence these factorizations of $H(2, 2^m)$ and of $T(2, 2^m)$ differ only by the order in which the rows/columns appear, and this completes the proof. □

Theorem 2.2 was numerically checked to be valid for $n = 8$ and $n = 16$ in [MST99].

3. Generalized Hadamard Matrices, Ranks and Factorizations

An $n \times n$ matrix $H(q, n)$ is called a generalized Hadamard matrix [B62] if its elements coincide with one of the numbers

$$\epsilon^k = \exp\left(\frac{2\pi i}{q}k\right), \quad 0 \le k \le q-1, \tag{3.1}$$

and it satisfies

$$H(q, n)H(q, n)^* = nI_n, \tag{3.2}$$

where $*$ denotes the complex conjugate transposed. Clearly, in the case $q = 2$, the generalized Hadamard matrices $H(2, n)$ reduce to the classic Hadamard matrices $H(2, n)$.

Often times we will be concerned with a matrix that contains not the entries ϵ^k of $H(q, n)$, but the values k from (3.1) corresponding to each entry. Specifically (as in Section 1.1), for a generalized Hadamard matrix $H(q, n) = [h_{ij}]$ we define its *exponent generalized Hadamard* matrix $\widehat{H}(q, n) = [\widehat{h}_{ij}]$ such that $h_{ij} = \epsilon^{\widehat{h}_{ij}}$.

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 FFT-like construction:

Proposition 3.1. *Let $H(q, n)$ be a generalized Hadamard matrix. Then the matrix given by*

$$H(q, qn) = \begin{bmatrix} H(q,n) & H(q,n) & H(q,n) & \dots & H(q,n) \\ H(q,n) & \epsilon H(q,n) & \epsilon^2 H(q,n) & \dots & \epsilon^{q-1} H(q,n) \\ H(q,n) & \epsilon^2 H(q,n) & \epsilon^4 H(q,n) & \dots & \epsilon^{2(q-1)} H(q,n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ H(q,n) & \epsilon^{q-1} H(q,n) & \epsilon^{2(q-1)} H(q,n) & \dots & \epsilon^{(q-1)^2} H(q,n) \end{bmatrix} \tag{3.3}$$

is also a generalized Hadamard matrix.

As with the Sylvester method for classical Hadamard matrices, the previous proposition as well as the initial generalized Hadamard matrix (which is just the DFT matrix)

$$H(q,q) = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \epsilon & \epsilon^2 & \epsilon^3 & \dots & \epsilon^{q-1} \\ 1 & \epsilon^2 & \epsilon^4 & \epsilon^6 & \dots & \epsilon^{2(q-1)} \\ 1 & \epsilon^3 & \epsilon^6 & \epsilon^9 & \dots & \epsilon^{3(q-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \epsilon^{q-1} & \epsilon^{2(q-1)} & \epsilon^{2(q-1)} & \dots & \epsilon^{(q-1)^2} \end{bmatrix} \tag{3.4}$$

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

The following result is a generalization of Theorem 1.3.

Theorem 3.2. *Let $H(q,q^m)$ be a generalized Sylvester Hadamard matrix. The rank of its exponent matrix $\widehat{H}(q,q^m)$ is m*(mod q)*.*

This theorem follows from the following factorization result.

Theorem 3.3. *Let $\widehat{H}(q,q^m)$ be the exponent matrix corresponding to the generalized Sylvester Hadamard matrix $H(q,q^m)$. Then $\widehat{H}(q,q^m)$ admits the decomposition*

$$\widehat{H}(q,q^m) = L_m L_m^T \pmod q \tag{3.5}$$

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

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

$$\widehat{H}(q,q) = L_1 L_1^T \pmod q \tag{3.6}$$

with

$$L_1^T = \begin{bmatrix} 0 & 1 & 2 & \dots & q-1 \end{bmatrix} \tag{3.7}$$

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

Proceeding inductively we see that

$$\widehat{H}(q,q^m) = L_m L_m^T (\text{mod } q)$$

implies

$$\widehat{H}(q,q^{m+1}) = \begin{bmatrix} 0_m & L_m \\ 1_m & L_m \\ \vdots & \vdots \\ (q-1)_m & L_m \end{bmatrix} \begin{bmatrix} 0_m^T & 1_m^T & \dots & (q-1)_m^T \\ L_m^T & L_m^T & \dots & L_m^T \end{bmatrix} \tag{3.8}$$

modulo q, where we note that

$$r_m^T = \begin{bmatrix} r & r & \dots & r \end{bmatrix} \tag{3.9}$$

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 $0_m, 1_m, \ldots, (q-1)_m$. This completes the proof. □

4. Generalized Pseudo-Noise Matrices

In this section we generalize the results of section 2 from $GF(2)$ to $GF(q)$.

Again, for a positive integer m, and $h_0, h_1, \ldots, h_{m-1} \in GF(q)$ we define an (m^{th} order) linear recurring sequence

$$a_0, a_1, a_2, \ldots$$

via

$$a_i = a_{i-1}h_{m-1} + a_{i-2}h_{m-2} + \cdots + a_{i-m+1}h_1 + a_{i-m}h_0 \quad \text{for } i \geq m \tag{4.1}$$

As in Section 2, it is easy to see that every m^{th} order linear recurring sequence is periodic with period at least $r \leq q^m - 1$. A *Pseudo-Noise Sequence* is an m^{th} order linear recurring sequence with the maximal possible period $q^m - 1$. Furthermore, a *Pseudo-Noise* matrix $T(q, q^m)$ is an $q^m \times q^m$ matrix of the form

$$T(q, q^m) = \begin{bmatrix} 0 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & \check{T} & \\ 0 & & & \end{bmatrix} \tag{4.2}$$

where $\check{T}$ is a circulant Hankel matrix with top row a Pseudo-Noise Sequence

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{2^m-2} \end{bmatrix}.$$

The following result is a generalization of Lemma 2.1.

Lemma 4.1. *The rank of any $q^m \times q^m$ pseudo-noise matrix $T(q, q^m)$ is m.*

Proof. This follows from the immediate observation that the rows of the matrix

$$\check{T} = \begin{bmatrix} \mathbf{a}_0 \\ \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{2^m-2} \end{bmatrix}$$

satisfy the m-term recurrence relations

$$\mathbf{a}_i = \mathbf{a}_{i-1}h_{m-1} + \mathbf{a}_{i-2}h_{m-2} + \cdots + \mathbf{a}_{i-m+1}h_1 + \mathbf{a}_{i-m}h_0$$

(of the form 4.1), and hence they are linearly dependent. □

The above lemma implies the following result.

Theorem 4.2. *The $q^m \times q^m$ pseudo-noise matrix $T(q, q^m)$ admits the decomposition*

$$T(q, q^m) = MR, \tag{4.3}$$

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 (4.3) exists by Lemma 4.1. By the definition, the rows of $T(q, q^m)$ are distinct, and therefore so are the rows of M. Since M is over $GF(q)$ with size $q^m \times m$, we conclude that 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 $GF(q)$, we have that R contains all possible m-tuples as columns, which completes the proof. □

The following theorem implies that the generalized Sylvester Hadamard matrices and generalized Pseudo-noise matrices are equivalent, i.e., they can be obtained from each other via row/column permutations.

Theorem 4.3. *Let $H(q, q^m)$ be a $q^m \times q^m$ generalized Sylvester Hadamard matrix, and let $T(q, q^m)$ be an $q^m \times q^m$ pseudo-noise matrix where q is prime. Then the exponent matrix $\widehat{H}(q, q^m)$ is equivalent to $T(q, q^m)$; i.e., there exist permutation matrices P_1 and P_2 such that $\widehat{H}(q, q^m) = P_1 T(q, q^m) P_2$.*

Proof. By Theorem 3.3, the exponent matrix $\widehat{H}(q, q^m)$ 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. □

Theorem 4.3 was announced in [BOS05].

5. Conclusion

Several results for the ranks of generalalized Hadamard matrices, Sylvester Hadamard matrices, their exponent matrices and their generalizations were established. These rank properties were used to demonstrate that the two classes of matrices, those built from generalized pseudo-noise sequences, and the generalized Hadamard matrices are equivalent up to permutations of the rows and columns.

References

[B62] A.T.Butson, *Generalized Hadamard matrices*, Proc. Am. Math. Soc. 13, 894-898 (1962).

[BOS05] T. Bella, V. Olshevsky, L. Sakhnovich, *Equivalence of Hadamard matrices and pseudo-noise matrices*, In Advanced Signal Processing Algorithms, Architectures, and Implementations XV. Editor(s): Franklin T. Luk, SPIE Publications, Aug 2005, p. 265-271.

[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.

[H06] K.J.Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, 2006.

[MST99] P.Mukhin, L.Sakhnovich, V.Timofeev *About Equivalence of Hadamard's Matrices*, Praći UNDIRT, 1(17), 1999, 89-94. (in Russian).

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

Tom Bella
Department of Mathematics,
University of Connecticut,
Storrs CT 06269-3009, USA
e-mail: `bella@math.uconn.edu`

Vadim Olshevsky
Department of Mathematics,
University of Connecticut,
Storrs CT 06269-3009, USA
e-mail: `olshevsky@math.uconn.edu`

Lev Sakhnovich
735 Crawford Avenue,
Brooklyn, NY 11223
e-mail: `Lev.Sakhnovich@verizon.net`