



<http://ijgt.ui.ac.ir>

---

**International Journal of Group Theory**

ASSN (print): 2251-7650, ISSN (on-line): 2251-7669

Vol. 13 No. 3 (2024), pp. 271-291.

© 2024 University of Isfahan

---



[www.ui.ac.ir](http://www.ui.ac.ir)

## NON-SEPARABLE MATRIX BUILDERS FOR SIGNAL PROCESSING, QUANTUM INFORMATION AND MIMO APPLICATIONS

TED HURLEY\* AND BARRY HURLEY

**ABSTRACT.** Matrices are built and designed by applying procedures from lower order matrices. Matrix tensor products, direct sums or multiplication of matrices are such procedures and a matrix built from these is said to be a *separable* matrix. A *non-separable* matrix is a matrix which is not separable and is often referred to as *an entangled matrix*. The matrices built may retain properties of the lower order matrices or may also acquire new desired properties not inherent in the constituents. Here design methods for non-separable matrices of required types are derived. These can retain properties of lower order matrices or have new desirable properties. Infinite series of required type non-separable matrices are constructible by the general methods.

Non-separable matrices of required types are required for applications and other uses; they can capture the structure in a unique way and thus perform much better than separable matrices. General new methods are developed with which to construct *multidimensional entangled paraunitary matrices*; these have applications for wavelet and filter bank design. The constructions are used to design new systems of non-separable unitary matrices; these have applications in quantum information theory. Some consequences include the design of full diversity constellations of unitary matrices, which are used in MIMO systems, and methods to design infinite series of special types of Hadamard matrices.

---

Keywords: Non-separable, signal processing, quantum, mimo.

MSC(2010): Primary: 15A30, 16S50. Secondary: 94A155.

Communicated by Patrizia Longobardi.

Article Type: 2022 CCGTA IN SOUTH FLA.

\*Corresponding Author.

Received: 13 January 2023, Accepted: 23 August 2023.

Cite this article: T. Hurley and B. Hurley, Non-separable matrix builders for signal processing, quantum information and mimo applications, Int. J. Group Theory, **13** no. 3 (2024) 271–291. <http://dx.doi.org/10.22108/ijgt.2023.136437.1824> .

## 1. Introduction

Matrices are built and designed from lower order matrices. A *separable matrix* is a matrix built using a direct sum, tensor product or multiplication. These procedures preserve many properties of the constituents; for example the tensor product or direct sum of invertible matrices is invertible and the tensor product of unitary matrices is a unitary matrices. A design procedure may or may not retain properties of the constituents or may acquire new properties not inherent in the constituents. A non-separable matrix is often referred to as an *entangled matrix*. Non-separable matrices with specific properties are required for structures and applications. These are required for specific application purposes in for example *quantum information theory* or *signal processing*.

Building blocks for non-separable matrices to specific requirements and types are presented. These may retain specific properties of the constituents or, more importantly, may acquire new desired properties not inherent in the constituents. The constructions enable infinite series of entangled matrices of a required type to be built.

Building blocks for *paraunitary matrices* are fundamental in *signal processing*. The concept of a paraunitary matrix is fundamental in this area and non-separable paraunitary matrices are required for *better performance*. Filter banks play an important role in signal processing but multidimensional entangled filter banks have been hard to design. In the huge research area of multirate filterbanks and wavelets, paraunitary matrices play a fundamental role, see for example [2, 11]. See section 2.6 below for further background.

Non-separable unitary matrices have applications in diverse areas such as for example in *quantum information theory*, [14].

Results and constructions on special unitary matrices are carried over to give new perspectives on the design of Hadamard special matrices, such as skew Hadamard and symmetric Hadamard matrices, section 2.7.

Full diversity sets of constellations of unitary matrices of many forms and of good quality are designed from the constructions, see section 3. These are required for MIMO (multiple input, multiple output) systems. The ones designed here have excellent *quality* (a defined concept) and infinite series of such constellations may be designed.

Non-separable multidimensional systems are designed and these can capture geometric structure rather than those constructed from one dimensional schemes using separable constructs.

Infinite series of such required matrices can be built from the constructions and processes may be selected. Applications to cryptography are inherent but are not dealt with here.

The two basic constructions are described separately in sections 2.1 and 2.2; these are combined to give additional design techniques in section 2.8. Applications are expanded on substantially in later sections. The non-separability/entanglement concept is important at all stages.

A formula for the determinant of a designed square matrix is obtained in subsection 2.3 and is of independent interest; it may be considered as a major generalisation of the determinant formula for a tensor product. This determinantal formula has a number of applications including the computation of the quality of full diversity sets of constellations as constructed in Section 3; these are used in MIMO (multiple input, multiple output) schemes.

**1.1. Notation.** Basic algebra notation and background may be found in many books on matrix theory or linear algebra but also found extensively online nowadays. Matrices are formed over rings in general including over polynomial rings in particular here.

$A^T$  denotes the transpose of the matrix  $A$ . For a matrix  $A$  over  $\mathcal{C}$ ,  $A^*$  denotes the complex conjugate transposed of  $A$ ; over other rings by convention  $A^* = A^T$ . Now  $I_n$  denotes the identity  $n \times n$  matrix which is also denoted by  $I$  when the size is understood. The notation  $1_R$  is used for the identity of the ring  $R$  which is abbreviated to  $1$  when the ring is understood. Say  $A$  is a *unitary*  $n \times n$  matrix provided  $AA^* = I_n$ , and say  $H$  is a *symmetric* (often called Hermitian) matrix provided  $H^* = H$ .

A one-dimensional (1D) paraunitary matrix over  $\mathcal{C}$  is a square matrix  $U(z)$  satisfying  $U(z)U^*(z^{-1}) = 1$ . In general a  $k$ -dimensional (kD) paraunitary matrix over  $\mathcal{C}$  is a matrix  $U(\mathbf{z})$ , where  $\mathbf{z} = (z_1, z_2, \dots, z_k)$  is a vector of (commuting) variables  $\{z_1, z_2, \dots, z_k\}$ , such that  $U(\mathbf{z})U^*(\mathbf{z}^{-1}) = 1$  with the definition  $\mathbf{z}^{-1} = (z_1^{-1}, z_2^{-1}, \dots, z_k^{-1})$ . Over fields other than  $\mathcal{C}$  a paraunitary matrix is a matrix  $U(\mathbf{z})$  satisfying  $U(\mathbf{z})U^T(\mathbf{z}^{-1}) = 1$ .

An idempotent matrix  $E$  is a matrix satisfying  $E^2 = E$ . The idempotent is *symmetric* provided  $E^* = E$ ; idempotents considered here are symmetric. A complete orthogonal symmetric idempotent (COSI) set is a set of  $n \times n$  matrices  $\{E_1, E_2, \dots, E_k\}$  where each  $E_i$  is a symmetric idempotent,  $E_i E_j = 0 = E_j E_i$  for  $i \neq j$  and  $E_1 + E_2 + \dots + E_k = I_n$ . Further definitions are given as required within sections. Definitions related to constellations of unitary matrices are given in Section 3; definitions related to special Hadamard matrices, (real or complex) are given in section 2.7.

## 2. The constructions

The basic designs use (i) COSI sets, section 2.1, and (ii) methods related to Diță type construction, section 2.2. These are then combined.

**2.1. Design with COSI.** Methods are now developed with which to design and construct required types of non-separable matrices using complete orthogonal symmetric idempotent (COSI) sets. Using COSI sets for constructing series of unitary and paraunitary matrices was initiated in [7].

**Proposition 2.1.** Let  $\{E_1, E_2, \dots, E_k\}$  be a COSI set in  $\mathcal{C}_n$ . Define  $G = \begin{pmatrix} E_{11} & E_{12} & \dots & E_{1k} \\ E_{21} & E_{22} & \dots & E_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ E_{k1} & E_{k2} & \dots & E_{kk} \end{pmatrix}$  where each  $E_j$  appears once in each (block) row and once in each (block) column. Then  $G$  is a unitary  $nk \times nk$  matrix.

*Proof.* Take the block inner product of two different rows of blocks. The  $E_i$  are orthogonal to one another so the result is 0. Take the block inner product of the row,  $j$ , of blocks with itself. This gives  $E_{j1}^2 + E_{j2}^2 + \dots + E_{jk}^2 = E_{j1} + E_{j2} + \dots + E_{jk} = 1 (= I_n)$ . Hence  $GG^* = 1 (= I_{nk})$ .  $\square$

A block circulant matrix is one of the form  $\begin{pmatrix} A_1 & A_2 & \dots & A_n \\ A_n & A_1 & \dots & A_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ A_2 & A_3 & \dots & A_1 \end{pmatrix}$  where the  $A_i$  are blocks of the same size. A reverse circulant block matrix is one of the form  $\begin{pmatrix} A_1 & A_2 & \dots & A_{n-1} & A_n \\ A_2 & A_1 & \dots & A_n & A_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ A_n & A_1 & \dots & A_{n-2} & A_{n-1} \end{pmatrix}$  where the  $A_i$  are blocks of the same size. A circulant block matrix may be transformed into a reverse circulant block matrix by block row operations. For example  $\begin{pmatrix} E_1 & E_2 & E_3 & E_4 \\ E_4 & E_1 & E_2 & E_3 \\ E_3 & E_4 & E_1 & E_2 \\ E_2 & E_3 & E_4 & E_1 \end{pmatrix} \longleftrightarrow \begin{pmatrix} E_1 & E_2 & E_3 & E_4 \\ E_2 & E_3 & E_4 & E_1 \\ E_3 & E_4 & E_1 & E_2 \\ E_4 & E_1 & E_2 & E_3 \end{pmatrix}$ , where  $\longleftrightarrow$  here indicates that one can be obtained from the other by block row operations. The one on the left is block circulant and the one on the right is reverse block circulant.

In particular given a COSI set  $\{E_1, E_2, \dots, E_k\}$ , block circulant unitary matrices and block reverse circulant unitary matrices may be formed. Note that the block reverse circulant matrix is *symmetric* as the  $E_i$  are symmetric.

When variables are attached to the  $E_i$  a paraunitary matrix is obtained; when elements of modulus 1 are attached to the  $E_i$  a unitary matrix is obtained.

For a variable  $\alpha$  define  $\alpha^* = \alpha^{-1}$ .

**Proposition 2.2.** Let  $\{E_1, E_2, \dots, E_k\}$  be a COSI set in  $\mathcal{C}_n$ .

Define  $G = \begin{pmatrix} E_{11}\alpha_{11} & E_{12}\alpha_{12} & \dots & E_{1k}\alpha_{1k} \\ E_{21}\alpha_{21} & E_{22}\alpha_{22} & \dots & E_{2k}\alpha_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ E_{k1}\alpha_{k1} & E_{k2}\alpha_{k2} & \dots & E_{kk}\alpha_{kk} \end{pmatrix}$  where each  $E_k$  appears once in each (block) row and once in each (block) column.

- (i) Let the  $\alpha_{ij}$  be variables. Then  $GG^* = I$  so that  $G$  is a paraunitary matrix.
- (ii) If  $|\alpha_{ij}| = 1$  for each  $\alpha_{ij}$ , then  $G$  is a unitary matrix.

The proof is similar to the proof of Proposition 2.1.

Block circulant and block reverse circulant matrices may be formed. The reverse circulant block matrix is symmetric provided  $\alpha_{ij} = \alpha_{ji}^*$ .

There is no limit on size and large constructions may also be formulated iteratively. The designs are direct and efficient.

**Example 2.3.** Let  $E_0 = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, E_1 = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ . Then  $\{E_1, E_2\}$  is a COSI set. Define  $W = \begin{pmatrix} xE_0 & yE_1 \\ zE_1 & tE_0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} x & x & y & -y \\ x & x & -y & y \\ z & -z & t & t \\ -z & z & t & t \end{pmatrix}$ . Then  $WW^* = I_4$ .

Let  $x = 1 = t = y = z$  in  $W$  and the following matrix is obtained:  $H = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}$ ; this is a common matrix used, or given as an example, in quantum theory as a non-separable/entangled matrix.

**Example 2.4.** Let  $Q_0 = \frac{1}{2} \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}, Q_1 = \frac{1}{2} \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$ . Then  $\{Q_0, Q_1\}$  is a COSI set. Define  $Q = \begin{pmatrix} xQ_0 & yQ_1 \\ zQ_1 & tQ_0 \end{pmatrix}$ .

Then  $Q$  is a paraunitary matrix. Now letting the variables have complex values of modulus 1 gives rise to complex Hadamard matrices as for example  $\begin{pmatrix} 1 & i & 1 & -i \\ -i & 1 & i & 1 \\ 1 & -i & 1 & i \\ i & 1 & -i & 1 \end{pmatrix}$ .

**Example 2.5.** Consider the matrices in Example 2.3 where  $E_1 = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, E_2 = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ . Then  $G = \begin{pmatrix} E_1 & E_2 \\ E_2 & E_1 \end{pmatrix}$  and  $H = \begin{pmatrix} E_2 & E_1 \\ E_1 & E_2 \end{pmatrix}$  are unitary matrices. Then  $2G, 2H$  are Hadamard real  $4 \times 4$  matrices. Form  $F_i = u_i u_i^*$  where  $\{u_1, u_2, u_3, u_4\}$  are the columns of  $G$  and then  $\{F_1, F_2, F_3, F_4\}$  is a COSI set. These may then be used to form  $16 \times 16$  unitary matrices; the entries are  $\pm \frac{1}{4}$  and thus 4 times these matrices are Hadamard  $16 \times 16$  matrices. In particular  $G = \begin{pmatrix} F_1 & F_2 & F_3 & F_4 \\ F_2 & F_3 & F_4 & F_1 \\ F_3 & F_4 & F_1 & F_2 \\ F_4 & F_1 & F_2 & F_3 \end{pmatrix}$  is a symmetric unitary matrix and thus  $4G$  is a symmetric Hadamard real matrix.

Here is a list of some properties of idempotents which are well-known or easily deduced.

- Let  $\{u_1, u_2, \dots, u_k\}$  be an orthonormal set of column vectors. Define  $E_i = u_i u_i^*$  and then  $\{E_1, E_2, \dots, E_k\}$  is an orthogonal symmetric set of idempotents. If  $S = \{E_1, E_2, \dots, E_k\}$  is not complete, set  $E = (I - E_1 - E_2 - \dots - E_k)$  and then  $\{E_1, E_2, \dots, E_k, E\}$  is a COSI set.
- If  $\{E_1, E_2, \dots, E_k\}$  is an orthogonal symmetric idempotent set, then  $\text{rank}(\sum_{i=1}^k E_i) = \sum_{i=1}^k (\text{rank } E_i)$ .
- If  $E$  is an idempotent of rank  $k$  then  $E$  is the sum of  $k$  orthogonal idempotents of rank 1. A method for writing such an idempotent as the sum of rank 1 idempotents is given in [13].<sup>1</sup>
- When  $U$  is unitary, its columns  $\{u_1, u_2, \dots, u_n\}$  form an orthonormal basis and thus  $\{E_1, E_2, \dots, E_n\}$  with  $E_i = u_i u_i^*$  is a COSI set which may then be used to form unitary or paraunitary matrices.
- If  $\{E, F\}$  are orthogonal idempotents then  $E + F$  is an idempotent orthogonal to any idempotent which is orthogonal to both  $E, F$ . Thus if  $\{E, F, K_1, K_2, \dots, K_t\}$  is an orthogonal idempotent set so is  $\{E + F, K_1, K_2, \dots, K_t\}$  and if  $\{E, F, K_1, K_2, \dots, K_t\}$  is a COSI set so is  $\{E + F, K_1, \dots, K_t\}$

<sup>1</sup>The summation is not unique but a unique expression can be obtained by expressing the idempotent as the sum of rank 1 idempotents with increasing initial zeros.

Orthogonal idempotents may be combined to form new idempotents and thus elements in a COSI set may be combined to form a new COSI set with a smaller number of elements but of the same size. This new COSI set may then be used to design unitary, paraunitary matrices and others. The following examples illustrate the general method.

Denote the circulant matrix  $\begin{pmatrix} a_1 & a_2 & \dots & a_k \\ a_k & a_1 & \dots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \dots & a_1 \end{pmatrix}$  by  $\text{circ}(a_1, a_2, \dots, a_k)$ .

Note that if  $\omega = e^{i\theta}$  then  $\omega + \omega^* = 2 \cos \theta$ .

**Example 2.6.** Denote the columns of the  $5 \times 5$  normalised Fourier matrix by  $\{u_0, u_1, u_2, u_3, u_4\}$ . Define  $E_i = u_i u_i^*$ . Then  $E_i = \frac{1}{5} \text{circ}(1, \omega^{4i}, \omega^{3i}, \omega^{2i}, \omega^i)$  where  $\omega = e^{i\frac{2\pi}{5}}$  is a primitive 5<sup>th</sup> root of 1 and  $\{E_0, E_1, E_2, E_3, E_4\}$  is a COSI set. Now combine  $\{E_1, E_4\}$  and  $\{E_2, E_3\}$  to get the COSI set  $S = \{E_0, E'_1, E'_2\}$  where  $E'_1 = E_1 + E_4, E'_2 = E_2 + E_3$ . The elements in this COSI set are circulant matrices also but in addition have real entries:  $E'_1 = \frac{2}{5} \text{circ}(1, \cos \theta, \cos 2\theta, \cos 3\theta, \cos 4\theta), E'_2 = \frac{2}{5} \text{circ}(1, \cos 2\theta, \cos 4\theta, \cos \theta, \cos 3\theta)$  where  $\theta = \frac{2\pi}{5}$ . It is noted that  $\cos 4\theta = \cos \theta, \cos 3\theta = \cos 2\theta$  – which could be deduced from the fact that  $\{E'_1, E'_2\}$  are symmetric!

This  $S$  can then be used to design unitary and paraunitary matrices with real coefficients as for example  $\begin{pmatrix} E_0 & E'_1 & E'_2 \\ E'_1 & E_2 & E_0 \\ E'_2 & E_0 & E'_1 \end{pmatrix}$ .

**Example 2.7.** Let  $\{u_0, u_1, \dots, u_5\}$  be the columns of the normalised Fourier  $6 \times 6$  matrix and form  $E_i = u_i u_i^*$ . Combine  $\{E_1, E_5\}$  and  $\{E_2, E_4\}$  to obtain the real COSI set  $S = \{E_0, E'_1, E_3, E'_2\}$  where  $E'_1 = E_1 + E_5, E'_2 = E_2 + E_4$ . Now a primitive 6<sup>th</sup> root of 1 is  $\omega = e^{i\frac{2\pi}{6}} = \cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6}$  and  $\cos \frac{2\pi}{6} = \frac{1}{2}, \cos \frac{4\pi}{6} = -\frac{1}{2}$ . Hence  $E_0 = \frac{1}{6} \text{circ}(1, 1, 1, 1, 1, 1), E_3 = \frac{1}{6} \text{circ}(1, -1, 1, -1, 1, -1), E'_1 = \frac{1}{6} \text{circ}(2, 1, -1, -2, -1, 1), E'_2 = \frac{1}{6} \text{circ}(2, -1, -1, 2, -1, -1)$ .

$S$  may then be used to form unitary and paraunitary matrices with real coefficients.

The same process may be applied in general to the normalised Fourier  $n \times n$  matrix to obtain COSI sets with real coefficients.

By Propositions 2.1 and 2.2, paraunitary and unitary matrices of size  $kn \times kn$  are designed from a COSI set  $\{E_1, E_2, \dots, E_k\}$  of  $k$  elements of size  $n \times n$ . The following constructs paraunitary and unitary matrices of size  $n \times n$  from a COSI set of size  $n \times n$ .

**Proposition 2.8.** [7]. Let  $\{E_1, E_2, \dots, E_k\}$  be a COSI set.

(i) Define  $U(z) = \sum_{j=1}^k \pm E_j z^{t_j}$ . Then  $U(z)U^*(z^{-1}) = I$ .

(ii) Let  $\mathbf{z} = (z_1, z_2, \dots, z_k)$  and  $U(\mathbf{z}) = \sum_{j=1}^k E_j z_j$ . Then  $U(\mathbf{z})U^*(\mathbf{z}^{-1}) = I$ .

(iii) Define  $U(z) = \sum_{j=1}^k e^{i\theta_j} E_j z^{t_j}$ . Then  $U(z)U^*(z^{-1}) = I$ .

When the  $z$  is replaced by an element of modulus 1 in part (i) of Proposition 2.8, a unitary matrix is obtained. Other versions of Proposition 2.8 may be formulated, for example by letting some of the  $z_j$  in part (ii) of Proposition 2.8 be equal.

Using COSI sets to design paraunitary matrices is developed further in section 2.6. Using COSI sets to construct types of Hadamard matrices is developed in section 2.7. In these sections, the COSI methods are combined with the designs methods of section 2.2.

**2.1.1. Symmetric unitary matrix and further paraunitary matrices using COSI.**  $U$  is a symmetric unitary matrix if and only if  $U = (I - 2E)$  where  $E$  is a (symmetric) idempotent, see [13, Proposition 8]. This gives the method for constructing a unitary symmetric matrix from any idempotent.

Let  $E$  be a symmetric idempotent. Then  $\{E, I - E\}$  is a COSI set. Define  $U = (I - 2E)$  which is then a unitary symmetric matrix and every symmetric unitary matrix is of this form. Note  $(I - 2E)E = -E$ ,  $(I - 2E)(I - E) = I - E$  and thus  $(I - 2E)$  has eigenvalue  $-1$  occurring to multiplicity equal to  $\text{rank } E$  and has eigenvalue  $1$  occurring to multiplicity equal to  $\text{rank}(I - E)$ .

The renowned building blocks for 1D (one dimensional) paraunitary matrices over  $\mathcal{C}$  due to Belevitch and Vaidyanathan as described in [16] are constructed from a complete orthogonal idempotent set of two elements in this manner.

The requirement that  $U$  be of a particular type of symmetric matrix can be more difficult. Now  $H$  is a symmetric Hadamard matrix if and only if  $U = \frac{1}{\sqrt{n}}H$  is a symmetric unitary matrix if and only if this  $U$  has a form  $(I - 2E)$  for a symmetric idempotent  $E$ . Thus a search for symmetric Hadamard matrices could begin with a search for such idempotents.

Suppose  $U$  is any unitary matrix. Then its columns  $\{u_1, u_2, \dots, u_n\}$  give rise to the COSI set  $\{E_1, E_2, \dots, E_n\}$  with  $E_i = u_i u_i^*$ . Some of the  $E_i$  may be combined to form different COSI sets:  $\sum_{i=1}^k E_{j_i}$  is also a symmetric idempotent, with  $J = \{j_1, j_2, \dots, j_k\} \subset \{1, 2, \dots, n\}$ , and this idempotent is orthogonal to each  $\{E_j | j \notin J\}$  or any idempotent formed in this way from  $\{E_j | j \notin J\}$ .

**Example 2.9.** Let  $E = \frac{1}{3} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ ,  $F = \frac{1}{3} \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \\ \omega & \omega^2 & 1 \end{pmatrix}$  where  $\omega$  is a primitive  $3^{rd}$  root of unity. Then  $\{E, F\}$  are idempotents and  $U = (I - 2E), V = (I - 2F)$  are unitary matrices. Note  $K = \sqrt{3}U$  satisfies  $KK^* = K^2 = 3I_3$  but is not a Hadamard matrix. Also  $UV = VU$  as  $E, F$  are orthogonal.

Infinite series of symmetric unitary matrices may be obtained as illustrated in the following example.

**Example 2.10.** Let  $\{E_1, E_2\}$  be a COSI set. Then  $U = \begin{pmatrix} E_1 & E_2 \\ E_2 & E_1 \end{pmatrix}$  is a symmetric unitary matrix. Thus  $F_1 = \frac{1}{2}(I - U), F_2 = \frac{1}{2}(I + U)$  is an orthogonal set of idempotents and so  $U_1 = \begin{pmatrix} F_1 & F_2 \\ F_2 & F_1 \end{pmatrix}$  is a symmetric unitary matrix. Then  $\{\frac{1}{2}(I - U_1), \frac{1}{2}(I + U_1)\}$  is a COSI set with which to form symmetric unitary matrices. This process may be continued to produce an infinite series of symmetric unitary matrices.

Initial choices for  $\{E_1, E_2\}$  include  $\{E_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, E_2 = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\}$  and  $\{E_1 = \frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}, E_2 = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}\}$ . The  $\{E_1, E_2\}$  can be of any size and not just  $2 \times 2$  matrices and any COSI set may be used initially.

**Example 2.11.** Let  $U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} u_1 & u_2 \end{pmatrix}$ . Define  $E_1 = u_1 u_1^* = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, E_2 = u_2 u_2^* = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ . Then  $U(z) = E_1 z^i + E_2 z^j$  is a paraunitary matrix.  $U(z)$  has real entries and is symmetric in that  $U(z)^* = U^*(z^{-1}) = U(z^{-1})$ . Multiplying any two of the form  $U(z)$  using the same COSI set gives another of this form. However different COSI sets may be used to form paraunitary of the form  $U(z)$  and these may be combined to give different types of paraunitary matrices.

**Example 2.12.** This gives an example of the design of a filter bank from COSI sets. A unitary real  $2 \times 2$  matrix is of the form  $\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$ . The above matrix  $U$  of Example 2.11 is of this form where  $\theta = -\frac{\pi}{4}$ . Define  $E_1 = \begin{pmatrix} \cos^2 \theta & -\cos \theta \sin \theta \\ -\sin \theta \cos \theta & \sin^2 \theta \end{pmatrix}, E_2 = \begin{pmatrix} \sin^2 \theta & \cos \theta \sin \theta \\ \sin \theta \cos \theta & \cos^2 \theta \end{pmatrix}$ . Then  $\{E_1, E_2\}$  is a COSI set and  $U(z) = E_1 z^i + E_2 z^j$  is a paraunitary matrix. Different  $U(z)$  are obtained by taking different values of  $\theta$  and these can then be used to design other paraunitary matrices of different forms. Paraunitary matrices of the type  $A_0 + A_1 z + \dots + A_{2n-1} z^{2n-1}$  are obtained with real coefficients. From this a 2-channel filter bank with  $n$  taps may be constructed.

**2.1.2. Group ring.** The primitive central idempotents, see [1], of the group ring  $\mathcal{C}G$  form a complete orthogonal set of idempotents and these can be realised as a COSI set in  $\mathcal{C}_{n \times n}$  where  $n$  is the order of the group  $G$ . Interesting unitary and paraunitary matrices may be formed from the group ring  $\mathcal{C}G$  of a finite group.

The unitary and paraunitary matrices formed have rational coefficients when  $G = S_n$ , the symmetric group on  $n$  letters, and have real coefficients when  $G = D_n$  the dihedral group of order  $2n$ . Central primitive idempotents may also be combined to give a COSI with real entries. Some examples may be found in [7]. The group ring aspects need to be investigated further; some ideas for this paper occurred while looking at COSI sets in group rings.

**2.2. Diță type.** The following constructions were initiated by Diță, [10], and were essentially designed in order to build Hadamard matrices from lower order Hadamard matrices. They have been rediscovered in various forms a number of times including by us. The original definition involved square matrices only and here it is generalised to work for non-square matrices and with two ‘sides’, left and right.

**Definition 2.13.** [10] Let  $\{A_1, A_2, \dots, A_k\}$  be  $m \times n$  matrices and let  $U = (u_{ij})$  be a  $k \times k$  matrix. Define the left matrix tangle product of  $\{A_1, A_2, \dots, A_k\}$  relative to  $U$  to be the  $mk \times nk$  matrix



$$\begin{pmatrix} A_1u_{11} & A_2u_{12} & \cdots & A_ku_{1k} \\ A_1u_{21} & A_2u_{22} & \cdots & A_ku_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ A_1u_{k1} & A_2u_{k2} & \cdots & A_ku_{kk} \end{pmatrix}$$

and the right matrix tangle product of  $\{A_1, A_2, \dots, A_k\}$  relative to  $U$  to be the  $mk \times nk$  matrix

$$\begin{pmatrix} A_1u_{11} & A_1u_{12} & \cdots & A_1u_{1k} \\ A_2u_{21} & A_2u_{22} & \cdots & A_2u_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ A_ku_{k1} & A_ku_{k2} & \cdots & A_ku_{kk} \end{pmatrix}$$

The notation  $(U; A_1, A_2, \dots, A_k)$  is used for the left matrix tangle product and  $(A_1, A_2, \dots, A_k; U)$  is used for the right matrix tangle product. From the context it will often be clear which (left or right) matrix tangle product is being used and in this case the term matrix tangle product is utilised.

The Diță construction as in [10, 9, 3] is given as a left matrix tangle product with square matrices. The right tangle product is not equal to the left tangle product but  $(A_1, A_2, \dots, A_k; U) = (U^T; A_1^T, A_2^T, \dots, A_k^T)^T$  for square matrices. It is convenient here for applications to have both left and right constructions and also for constructions when the matrix  $U$  is not square, see Definition 2.14 below.

A generalised version of this construction has also been used but this is not needed here. The present constructions are used with a view to designing non-separable matrices in particular.

Definition 2.2 can be generalised as follows to the case where  $U$  is not square but has size either  $k \times n$  or  $n \times k$  where  $k$  is the number of matrices to be entangled; this requires the left or right matrix tangle product definitions.

**Definition 2.14.** (i) Let  $\{A_1, A_2, \dots, A_k\}$  be  $m \times n$  matrices and let  $U = (u_{ij})$  be a  $t \times k$  matrix. Define the left matrix tangle product of  $\{A_1, A_2, \dots, A_k\}$  relative to  $U$  to be the  $tm \times nk$  matrix

$$\begin{pmatrix} A_1u_{11} & A_2u_{12} & \cdots & A_ku_{1k} \\ A_1u_{21} & A_2u_{22} & \cdots & A_ku_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ A_1u_{t1} & A_2u_{t2} & \cdots & A_ku_{tk} \end{pmatrix}$$

(ii) Let  $\{A_1, A_2, \dots, A_k\}$  be  $m \times n$  matrices and let  $U = (u_{ij})$  be a  $k \times t$  matrix. Define the right matrix tangle product of  $\{A_1, A_2, \dots, A_k\}$  relative to  $U$  to be the  $mk \times nk$  matrix

$$\begin{pmatrix} A_1u_{11} & A_1u_{12} & \cdots & A_1u_{1t} \\ A_2u_{21} & A_2u_{22} & \cdots & A_2u_{2t} \\ \vdots & \vdots & \cdots & \vdots \\ A_ku_{k1} & A_ku_{k2} & \cdots & A_ku_{kt} \end{pmatrix}$$

The notation  $(U; A_1, A_2, \dots, A_k)$  is used for the left matrix tangle product and  $(A_1, A_2, \dots, A_k; U)$  is used for the right matrix tangle product. From the context it may be clear which (left or right) tangle product is being used and in this case the term matrix tangle product is utilised.

The matrix tangle product depends on the order of the  $A_i$  and different tangle products are obtained from different permutations of the  $A_i$  - ‘different permutations’ should take into account that some of the  $A_i$  may be the same. This can be particularly useful in designing series of different entangled matrices with desired properties.

If all the  $A_i = A$  are the same then the matrix tangle product is the matrix tensor<sup>2</sup> product  $U \otimes A$ . The direct sum of matrices is also a very special matrix tangle product as  $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = (I_2; A, B)$ .

Say  $U$  is the *shuffler* matrix and say  $\{A_1, A_2, \dots, A_k\}$  are the *tangle* matrices of the matrix tangle product  $(U; A_1, A_2, \dots, A_k)$  or of  $(A_1, A_2, \dots, A_k; U)$  depending on which, left or right, matrix tangle product is under consideration. Suppose now an  $m \times n$  matrix  $U$  is to be a shuffler matrix of a matrix tangle product. Then either  $m$  or  $n$  matrices are required for the tangles *but* they need not all be different. If they are all the same and equal to  $A$  then the tensor product  $U \otimes A$  is obtained which is an  $mt \times nq$  matrix when  $A$  is  $t \times q$ . If less than  $n$  or  $m$  different matrices are to be used as tangles then these are repeated until  $m$  or  $n$  matrices are obtained as appropriate. The matrix tangle product may be square even though neither the tangles nor the shuffler are square. For example if  $\{A, B\}$  are  $2 \times 3$  matrices and  $U$  is a  $3 \times 2$  matrix then  $(U; A, B)$  is a  $6 \times 6$  matrix. In general if  $\{A_1, A_2, \dots, A_k\}$  are  $k \times t$  matrices and  $U$  is  $t \times k$  then  $(U; A_1, A_2, \dots, A_k)$  is a  $kt \times kt$  matrix; if  $\{A_1, A_2, \dots, A_k\}$  are  $t \times k$  matrices and  $U$  is  $k \times t$  then  $(A_1, A_2, \dots, A_k; U)$  is a  $kt \times kt$  matrix.

The matrix tangle product is not a matrix tensor product unless there is a fixed  $A$  such that  $A_i = \alpha_i A$  for some  $\alpha_i$ . In this situation  $(U; \alpha_1 A, \alpha_2 A, \dots, \alpha_k A) = (U'; A, A, \dots, A) = U' \otimes A$  where  $U'$  is obtained from  $U$  by multiplying rows or columns of  $U$  by appropriate  $\alpha_i$ . product.

The matrix tangle product has some linearity:

- $\alpha(U; A_1, A_2, \dots, A_k) = (U; \alpha A_1, \alpha A_2, \dots, \alpha A_k) = (\alpha U; A_1, A_2, \dots, A_k)$ .
- $(U + V; A_1, A_2, \dots, A_k) = (U; A_1, A_2, \dots, A_k) + (V; A_1, A_2, \dots, A_k)$ .
- $(U; A_1, A_2, \dots, A_k) + (U; B_1, B_2, \dots, B_k) = (U; A_1 + B_1, A_2 + B_2, \dots, A_k + B_k)$ .

<sup>2</sup>Matrix tensor product is often called *Kronecker product*. See however [4] for discussion on this name.

Similar results hold for the right matrix tangle product.

Note however for example that  $(U; A_1 + A'_1, A_2)$  is not in general the same as  $(U; A_1, A_2) + (U; A'_1, A_2)$ .

**2.3. Determinant.** The determinant value of a matrix tangle product of square matrices in terms of the constituents is interesting and valuable. It can be obtained in terms of the determinants of the tangles and shuffler, see Proposition 2.15 below. However the spectrum does not have a relationship with the spectrums of the constituents, as happens for a matrix tensor product, as the process produces an *entangled* matrix in general.

Let  $T = (U; A_1, A_2, \dots, A_k)$ . It is of interest to know the value of  $\det T = |T|$  when the  $A_i$  and  $U$  are square matrices. It is given in terms of the determinants of the constituents as follows.

**Proposition 2.15.** *Let  $T = (U; A_1, A_2, \dots, A_k)$  where  $U$  is a  $k \times k$  matrix and the  $A_i$  are  $n \times n$  matrices. Then  $|T| = |A_1||A_2| \cdots |A_k||U|^n$ .*

*Proof.* This can be shown using results on determinants of block matrices as for example in [5]. Alternatively a direct proof may be given by applying the techniques used when working with proofs of determinants on block matrices. Proceed inductively as follows. Let  $U = (\alpha_{ij})$ . If  $A_1 = 0$  or if all  $\alpha_{1i} = 0$  the result is clear. We can assume we can assume  $\alpha_{1i} \neq 0$  for some  $\alpha_i$  and hence by block operations we can assume  $\alpha_{11} \neq 0$ . Then apply block operations on  $T$  to reduce the first column of

blocks to the form  $\begin{pmatrix} \alpha_{11}A_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ ; these block operations do not alter the value of the determinant. Then  $|T| = \det(\alpha_{11}A_1) \times |B|$  where  $B$  is a similar matrix to  $T$  but of one block size smaller; induction may then be applied. □

A similar result holds for the right matrix tangle product.

This property is particularly useful in applications, see for example Section 3. Proposition 2.15 generalises the determinant value of a matrix tensor product – if all the  $A_i$  are the same,  $A_i = A$ , then  $|T| = |A|^k|U|^n$  and  $T = U \otimes A$ . For example let  $\{A, B\}$  be  $n \times n$  matrices and let  $U$  be of size  $2 \times 2$ . Then  $T = (U; A, B)$  has  $|T| = |A||B||U|^n$ . The determinantal property of tensor products which is a special case of Proposition 2.15 is in itself very useful in many areas.

Finding the eigenvalues of a matrix tangle product is difficult and no formula in terms of the eigenvalues of the constituents exists. The eigenvalues of a matrix tangle product are ‘entangled’.

**2.4. Preserved properties.** Which properties of the shuffler and tangles of a matrix tangle product are preserved? Let  $\mathcal{P}$  be a property of a matrix, such as for example being unitary or invertible. Say

$M \in \mathcal{P}$  if and only if  $M$  has this property  $\mathcal{P}$ . If for any  $G = (U; A_1, A_2, \dots, A_k)$  with  $A_i \in \mathcal{P}$  for  $i = 1, 2, \dots, k$  and  $U \in \mathcal{P}$ , implies that  $G \in \mathcal{P}$  then say the matrix tangle product *preserves*  $\mathcal{P}$ .

- The property of being a unitary matrix is preserved.
- The property of being an invertible matrix is preserved.
- The property of being a paraunitary matrix is preserved.
- The property of being a normal matrix is not preserved.
- The property of being a symmetric matrix is not preserved.
- The property of being a Hadamard matrix is preserved.

The preserved properties are stated as Propositions in the following subsections 2.5, 2.6 and 2.7. These subsections derive applications, constructions and designs.

2.5. Unitary.

**Proposition 2.16.** *Let  $\{A_1, A_2, \dots, A_k\}$  be  $m \times m$  unitary matrices and let  $U = (u_{ij})$  be a unitary  $k \times k$  matrix. Then*

$$\begin{pmatrix} A_1 u_{11} & A_2 u_{12} & \cdots & A_k u_{1k} \\ A_1 u_{21} & A_2 u_{22} & \cdots & A_k u_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ A_1 u_{k1} & A_2 u_{k2} & \cdots & A_k u_{kk} \end{pmatrix} \text{ and } \begin{pmatrix} A_1 u_{11} & A_1 u_{12} & \cdots & A_1 u_{1k} \\ A_2 u_{21} & A_2 u_{22} & \cdots & A_2 u_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ A_k u_{k1} & A_k u_{k2} & \cdots & A_k u_{kk} \end{pmatrix} \text{ are unitary } mk \times mk \text{ matrices.}$$

Thus the matrix tangle products of unitary matrices are unitary matrices. Section 2.1 also constructs unitary matrices from COSI (complete orthogonal symmetric idempotent) sets. This greatly expands the pools of unitary matrices available for various purposes. Entangled matrices are often required and this condition can be realised by these constructions.

A matrix is unitary if and only if its rows or columns form an orthonormal basis and thus new orthonormal bases are constructed when a new unitary matrix is constructed.

**Example 2.17.** *Pauli unitary matrices as builders for higher order matrices*

*Applying the process to the Pauli matrices  $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  gives interesting entangled unitary matrices. The following six  $4 \times 4$  matrices are obtained when each of the matrices is used (once) as a tangle or as a shuffler:*

$$(\sigma_z; \sigma_x, \sigma_y), (\sigma_z; \sigma_y, \sigma_x), (\sigma_y; \sigma_x, \sigma_z), (\sigma_y; \sigma_z, \sigma_x), (\sigma_x; \sigma_z, \sigma_y), (\sigma_x; \sigma_y, \sigma_z)$$

*Other  $4 \times 4$  unitary matrices may be formed from  $\{\sigma_x, \sigma_y, \sigma_z\}$ ; some are tensor products such as  $(\sigma_x, \sigma_x; \sigma_z)$  and ones are like  $(\sigma_x, \sigma_y; \sigma_x)$  where a matrix appears as both a tangle and the shuffler. Taking two of these  $4 \times 4$  unitary matrices as tangles and using one of  $\{\sigma_x, \sigma_y, \sigma_z\}$  as a shuffler produces an  $8 \times 8$  unitary matrix in which the Pauli matrices are constituents and entangled.*

*This process may be continued to produce  $2^n \times 2^n$  unitary entangled matrices from the Pauli matrices. The significance of these needs to be explored.*

**Example 2.18.** *Real unitary*

Start with the following real  $2 \times 2$  matrices  $\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  from which to build new matrices. Make these unitary by dividing by  $\sqrt{2}$  and then unitary matrices are built by the construction methods.

The following real unitary (orthogonal) matrices  $\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$  are often used in practice. Different  $\theta$  may be used from which real  $2^n \times 2^n$  real orthogonal matrices are built.

Now  $A_i = e^{i\theta_i}$  are  $1 \times 1$  unitary matrices. Let  $U$  be a  $k \times k$  unitary matrix. Then  $(U; A_1, A_2, \dots, A_k), (A_1, A_2, \dots, A_k; U)$  are also unitary  $k \times k$  matrices.

**Example 2.19.** *Unbiased bases example*

- Let  $U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  and let  $A = (1), B = (i)$ . Then  $\{U, A, B\}$  are unitary matrices. Now  $(A, B; U)$  is a unitary matrix  $G = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$ . Then  $\{U, G, I_2\}$  constitute three matrices consisting of mutual unbiased bases for  $\mathcal{C}^2$ .
- Let  $U = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$ . Let  $A = (1), B = (\omega), C = (\omega)$  and form  $U_1 = (A, B, C; U)$ . Let  $A = (1), B = (\omega^2), C = (\omega^2)$  and form  $U_2 = (A, B, C; U)$ . Then  $\{U, U_1, U_2, I_3\}$  are 4 matrices consisting of mutually unbiased bases for  $\mathcal{C}^3$ .

**2.6. Additional Paraunitary concepts.** Paraunitary matrices are fundamental in signal processing and the concept of a paraunitary matrix plays an important role in the research area of multirate filterbanks and wavelets. In the polyphase domain, the synthesis matrix of an orthogonal filter bank is a paraunitary matrix; a Filter Bank is orthogonal if its polyphase matrix is paraunitary, see [2]. Thus designing an orthogonal filter bank is *equivalent* to designing a paraunitary matrix. The book [2, Chapters 4-6], makes the design of paraunitary matrices a primary aim. Designing *entangled* paraunitary matrices is often a requirement and has been a difficult task.

The literature is huge and expanding rapidly; of particular note is [11], where further background and many references may be found. From the literature: “Designing nonseparable multidimensional orthogonal filter banks is a challenging task.”; “Multirate filter banks give the structure required to generate important cases of wavelets and the wavelet transform.”; “In filter bank literature the terms orthogonality, paraunitary and lossless are often used interchangeably.” “Paraunitarity is a necessary and sufficient condition for wavelet orthogonality.” “Designing an orthogonal filter bank is equivalent to designing a paraunitary matrix.”

Paraunitary matrices are constructed using COSI sets by methods of Propositions 2.2 and 2.8, see Section 2.1; paraunitary matrices which are symmetric may be built with this method.

‘Being a paraunitary matrix’ is a property preserved by matrix tangle products.

**Proposition 2.20.** *Let  $\{A_1, A_2, \dots, A_k\}$  be  $m \times m$  paraunitary matrices and let  $U = (u_{ij})$  be a paraunitary  $k \times k$  matrix. Then*

$$\begin{pmatrix} A_1u_{11} & A_2u_{12} & \cdots & A_ku_{1k} \\ A_1u_{21} & A_2u_{22} & \cdots & A_ku_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ A_1u_{k1} & A_2u_{k2} & \cdots & A_ku_{kk} \end{pmatrix} \text{ and } \begin{pmatrix} A_1u_{11} & A_1u_{12} & \cdots & A_1u_{1k} \\ A_2u_{21} & A_2u_{22} & \cdots & A_2u_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ A_ku_{k1} & A_ku_{k2} & \cdots & A_ku_{kk} \end{pmatrix}$$
 are paraunitary  $mk \times mk$  matrix in the union of the variables in  $\{A_1, A_2, \dots, A_k, U\}$ .

The constructions in Propositions 2.2, 2.8 and 2.20 may be combined. Building blocks for paraunitary matrices are available; these are not tensor products and are entangled in general. The shuffler itself may be a unitary matrix as may any of the tangles. Examples are given in [7] where a more restricted tangle definition is given. Although the systems here give building blocks for multidimensional paraunitary matrices, it is not claimed that every multidimensional paraunitary matrix is built in this way although many such are built in this manner. The renowned building blocks for 1D paraunitary matrices over  $\mathcal{C}$  due to Belevitch and Vaidyanathan as described in [16] are constructed from a complete orthogonal idempotent set of two elements.

Now  $A_i = z_i$  are  $1 \times 1$  paraunitary matrices. Let  $P$  be a  $k \times k$  paraunitary matrix. Then  $G = (P; A_1, A_2, \dots, A_k)$  is a paraunitary  $k \times k$  matrix in the union of the variables in  $P$  and  $\{z_1, z_2, \dots, z_k\}$ .

By replacing the variables by elements of modulus 1 in a paraunitary matrix, a unitary matrix is obtained. Constructing paraunitary matrices leads to the construction of unitary matrices.

**2.7. Hadamard  $\leftrightarrow$  Unitary.**  $H$  is a real Hadamard  $n \times n$  matrix if its entries are elements of modulus 1 and  $HH^* = nI_n$ . A Hadamard matrix of type  $H(n, p)$  is a matrix in which each element of  $H(n, p)$  is a  $p^{th}$  root of 1 and  $H(n, p)H(n, p)^* = nI_n$ . A  $H(n, 2)$  matrix is a real Hadamard matrix  $n \times n$  matrix. It is known that the Diță construction preserves Hadamard matrices, [10, 9, 3].

**Proposition 2.21.** [10] Let  $\{A_1, A_2, \dots, A_k\}$  be  $m \times m$  Hadamard matrices and let  $U = (u_{ij})$  be a Hadamard  $k \times k$  matrix. Then

- (i)  $\begin{pmatrix} A_1u_{11} & A_2u_{12} & \cdots & A_ku_{1k} \\ A_1u_{21} & A_2u_{22} & \cdots & A_ku_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ A_1u_{k1} & A_2u_{k2} & \cdots & A_ku_{kk} \end{pmatrix}$  is a Hadamard  $km \times km$  matrix. If the  $A_i$  and  $U$  have entries which are  $n^{th}$  roots of 1 then this matrix has entries which are  $n^{th}$  roots of 1.
- (ii)  $\begin{pmatrix} A_1u_{11} & A_1u_{12} & \cdots & A_1u_{1k} \\ A_2u_{21} & A_2u_{22} & \cdots & A_2u_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ A_ku_{k1} & A_ku_{k2} & \cdots & A_ku_{kk} \end{pmatrix}$  is a Hadamard  $km \times km$  matrix. If the  $A_i$  and  $U$  have entries which are  $n^{th}$  roots of 1 then this matrix has entries which are  $n^{th}$  roots of 1.

The Diță product has been used in a number of papers to construct Hadamard matrices from lower order Hadamard matrices, see for example [10] itself, and also [9] and [3]. Hadamard matrices have been also constructed in section 2.1 by the COSI method.

Now  $A_i = e^{i\theta_i}$  are  $1 \times 1$  Hadamard matrices. Say  $H$  is a  $H(n, p)$  matrix if it has size  $n$  and entries which are  $p^{th}$  roots of 1. Let  $H$  be a  $k \times k$  Hadamard matrix. Then  $G = (H; A_1, A_2, \dots, A_k)$  is a

Hadamard matrix. If  $H = H(k, p)$  and  $\{A_i = A_i(1, p)\}$  then  $G$  is a  $G(k, p)$  matrix. If  $H = H(k, p)$  and  $A_i = A_i(1, n_i)$  then  $G$  is a  $G(k, s)$  matrix where  $s = \text{lcm}(p, n_1, n_2, \dots, n_k)$ .

Symmetric Hadamard matrices are *Type II* matrices; the definition and further information on Type II matrices may be found in [9] and the many references therein. “Type II matrices were introduced explicitly in the study of *spin* models.” The following construction is similar to that formulated in for example [3] but is a useful way with which to look at the formulation of symmetric Hadamard matrices.

**Construction 2.22.** *Construct symmetric Hadamard matrices.* Let  $H$  be a Hadamard matrix of type  $H(n, p)$ . Let  $G$  be the corresponding unitary matrix, that is  $G = \frac{1}{\sqrt{n}}H$ . The columns  $\{u_1, u_2, \dots, u_n\}$  of  $G$  form an orthonormal basis for  $\mathcal{C}_n$ . Let  $E_i = u_i u_i^*$ . Then  $\{E_1, E_2, \dots, E_n\}$  is a COSI set, from which unitary  $n^2 \times n^2$  matrices may be formed as in section 2.1. In particular symmetric  $n^2 \times n^2$  matrices may be formed using the reverse circulant construction. These matrices have entries which are  $\frac{1}{n}$  times a  $p^{\text{th}}$  root of 1 and so multiplying any of these matrices by  $n$  gives a symmetric  $n^2 \times n^2$  Hadamard matrix which is a  $H(n^2, p)$  matrix.

Starting from *any* Hadamard  $H(n, p)$ , Construction 2.22 designs series of Hadamard  $H(n^2, p)$  matrices. These can be designed to be symmetric by using reverse circulant form. The process may then be continued to produce  $H(n^{2^k}, p)$ , for  $k \geq 1$  Hadamard matrices going via unitary matrices. By taking the reverse circulant process at any stage of production the matrices produced are symmetric. Only at the final stage need the reverse circulant process be applied in order to design symmetric Hadamard matrices.

It is also known, see for example [3], that a symmetric  $2n \times 2n$  Hadamard symmetric matrices may be constructed from  $n \times n$  symmetric Hadamard matrices. The construction 2.23 below is similar but different and illustrates the niceness of the tangled product in general for designs.

(Recall: A Hadamard matrix  $H$  is said to be of type  $H(n, p)$  if it is an  $n \times n$  Hadamard matrix and all its entries are  $p^{\text{th}}$  roots of unity.)

**Construction 2.23.** (i) *Let  $H$  be an  $n \times n$  Hadamard symmetric matrix and  $U$  a  $2 \times 2$  symmetric matrix. Then  $(U; A, A^T), (U; A^T, A), (A, A^T; U), (A^T, A : U)$  are symmetric Hadamard  $2n \times 2n$  matrices.*

(ii) *Let  $H$  be an  $n \times n$  Hadamard symmetric matrix of type  $H(n, p)$  and  $U$  a  $2 \times 2$  symmetric matrix. Then  $(U; A, A^T), (U; A^T, A), (A, A^T; U), (A^T, A : U)$  are symmetric Hadamard  $2n \times 2n$  matrices of type  $G(2n, p)$ . More generally if  $H$  is of type  $H(n, p)$  and  $U$  is of type  $U(2, q)$  then  $(U; A, A^T), (U; A^T, A), (A, A^T; U), (A^T, A : U)$  are of type  $G(2n, s)$  where  $s = \text{lcm}(q, p)$ .*

The  $n \times n$  Fourier matrix is a Hadamard  $H(n, n)$  matrix.

**Example 2.24.** Let  $H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$  where  $\omega$  is a primitive third root of 1. Then  $G = \frac{1}{\sqrt{3}}H$  is

a unitary matrix. The columns of  $G$  are  $u_1 = \frac{1}{\sqrt{3}}(1, 1, 1)^T, u_2 = \frac{1}{\sqrt{3}}(1, \omega, \omega^2)^T, u_3 = \frac{1}{\sqrt{3}}(1, \omega^2, \omega)^T$ .

Then  $\{E_1 = u_1u_1^* = \frac{1}{3} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, E_2 = u_2u_2^* = \frac{1}{3} \begin{pmatrix} 1 & \omega^2 & \omega \\ \omega & 1 & \omega^2 \\ \omega^2 & \omega & 1 \end{pmatrix}, E_3 = u_3u_3^* = \frac{1}{3} \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \\ \omega & \omega^2 & 1 \end{pmatrix}\}$

is a COSI set. Thus  $K = \begin{pmatrix} E_1 & E_2 & E_3 \\ E_2 & E_3 & E_1 \\ E_3 & E_1 & E_2 \end{pmatrix}$  is a symmetric unitary matrix and  $L = 3K$  is a symmetric

Hadamard  $L(9, 3)$  matrix.

**Example 2.25.**  $P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, Q = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$ . are Hadamard  $H(2, 4)$  matrices. Then  $A = \frac{1}{\sqrt{2}}P, B = \frac{1}{\sqrt{2}}Q$  are unitary matrices. Infinite series of unitary and Hadamard matrices may be built as follows.

Build  $\{A, B\}$  relative to unitary  $A$  and then build  $\{A, B\}$  relative to unitary  $B$  to obtain Build  $A_1 = (A, B; A) = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & i \\ 1 & -1 & i & 1 \\ 1 & 1 & -1 & -i \\ 1 & -1 & -i & 1 \end{pmatrix}, B_1 = (A, B; B) = \frac{1}{2} \begin{pmatrix} 1 & 1 & i & -1 \\ 1 & -1 & -1 & i \\ i & i & 1 & i \\ i & -i & i & 1 \end{pmatrix}$ . Other options for  $A_1, B_1$  are  $A_1 = (A; A, B), B_1 = (B; A, B)$  but also others such as swapping  $A, B$  around. These are  $4 \times 4$  matrices and  $2A_1, 2B_1$  are Hadamard  $H(4, 4)$  matrices.

Build  $(A_1, B_1; A), (A_1, B_1; B)$  to get unitary  $8 \times 8$  matrices with entries  $\pm 1, \pm i$  and from these get  $H(8, 4)$  matrices. Build  $(A_1, B_1; A_1), (A_1, B_1; B_1)$  to get  $H(16, 4)$  matrices. The process may be continued in many different directions.

**2.7.1. Skew Hadamard.** A Hadamard  $n \times n$  matrix is a skew Hadamard provided  $H = I_n + U$  with  $U^* = -U$ . If interested in real Hadamard matrices then it is required that  $U^* = U^T = -U$ . This implies  $H + H^* = 2I_n$ . The Diță product may be used to produce skew  $2n \times 2n$  Hadamard matrices from a skew  $n \times n$  Hadamard matrix. Skew Hadamard matrices are used in a number of areas including for the construction of orthogonal designs.

**Construction 2.26.** Let  $A$  be an  $n \times n$  skew Hadamard matrix and let  $U$  be a  $2 \times 2$  skew symmetric Hadamard matrix. Then  $(U; A, A^T), (U; A^T, A), (A, A^T; U), (A^T, A; U)$  are skew symmetric  $2n \times 2n$  matrices.

The known method, see for example [3], for producing a  $2n \times 2n$  skew symmetric matrix from a  $n \times n$  skew symmetric matrix is a special case of Construction 2.26 above.

The Construction 2.26 works for general Hadamard skew matrices over  $\mathcal{C}$ .

The  $2 \times 2$  skew Hadamard real matrix used initially could be  $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$  or  $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$  or similar. A skew Hadamard  $2 \times 2$  matrix over  $\mathcal{C}$  in addition are ones of the form  $\begin{pmatrix} 1 & \alpha \\ -\alpha^* & 1 \end{pmatrix}$  where  $|\alpha| = 1$ .



Suppose now  $H = \begin{pmatrix} 1 & e^{i\alpha_1} & -e^{-i\alpha_2} & -e^{-i\alpha_3} \\ -e^{-i\alpha_1} & 1 & -e^{-i\alpha_4} & e^{i\alpha_5} \\ e^{i\alpha_2} & e^{i\alpha_4} & 1 & e^{i\alpha_6} \\ e^{i\alpha_3} & -e^{-i\alpha_5} & -e^{-i\alpha_6} & 1 \end{pmatrix}$  is to be a Hadamard matrix; it already has the skew condition,  $H = I + U$  with  $U^* = -U$ . Then looking at  $HH^* = 4I_n$  the following (just three) conditions are obtained: (i)  $-\alpha_2 + \alpha_4 = -\alpha_5 - \alpha_3$ ; (ii)  $\alpha_1 - \alpha_4 = -\alpha_3 - \alpha_6$ ; (iii)  $\alpha_1 + \alpha_5 = \alpha_6 - \alpha_2$ . Solving this system of equations gives  $\alpha_4 = \alpha_1 + \alpha_2, \alpha_5 = -\alpha_1 - \alpha_3, \alpha_6 = \alpha_2 - \alpha_3$  and  $\alpha_1, \alpha_2, \alpha_3$  can have any value. This gives an infinite number of skew Hadamard (complex) matrices. New infinite sets can be formed using Construction 2.26.

**Example 2.27.** As an example require now that the  $\{e^{i\alpha_j}\}$  be  $n^{th}$  roots of 1. Say for example  $\alpha_1 = \frac{2\pi}{n}, \alpha_2 = \frac{4\pi}{n}, \alpha_3 = \frac{6\pi}{n}$  and then  $\alpha_4 = \frac{6\pi}{n}, \alpha_5 = -\frac{8\pi}{n}, \alpha_6 = -\frac{2\pi}{n}$ .

This gives the following skew Hadamard matrix  $\begin{pmatrix} 1 & \omega & -\omega^{-2} & -\omega^{-3} \\ -\omega^{-1} & 1 & -\omega^{-3} & \omega^{-4} \\ \omega^2 & \omega^3 & 1 & \omega^{-1} \\ \omega^3 & -\omega^4 & -\omega & 1 \end{pmatrix}$ , where  $\omega = e^{i\frac{2\pi}{n}}$  is a primitive  $n^{th}$  root of 1.

Further taking  $\omega$  to be a primitive third root of unity,  $\omega^3 = 1$ , gives the skew Hadamard matrix  $\begin{pmatrix} 1 & \omega & -\omega & -1 \\ -\omega^2 & 1 & -1 & \omega^2 \\ \omega^2 & 1 & 1 & \omega^2 \\ 1 & -\omega & -\omega & 1 \end{pmatrix}$ . The entries are  $6^{th}$  roots of unity, so this is a  $H(4, 6)$  matrix.

Infinite sequences of skew Hadamard real matrices may be obtained by starting out with a skew Hadamard matrix real matrix  $A$  and with  $U = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$  or  $U = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ .

Then form  $A_1$  which can be one of  $(U; A, A^T), (U; A^T, A), (A, A^T; U), (A^T, A; U)$ .

Replace  $A$  by  $A_1$  to form  $(U; A_1, A_1^T), (U; A_1^T, A_1), (A_1, A_1^T; U), (A_1^T, A_1; U)$  which are skew Hadamard matrices; this process may be continued.

Let  $A$  be a normalised  $n \times n$  Fourier matrix and  $B$  a matrix obtained from  $A$  by interchanging rows (or columns). Then both  $A, B$  are unitary matrices. Let  $C$  be any  $2 \times 2$  unitary matrix. Then  $(A, B; C)$  and  $(B, A; C)$  are unitary  $2n \times 2n$  matrices. Let  $A$  be a Hadamard matrix and  $B$  any permutation of the rows of columns of  $A$ . Let  $C$  be any  $2 \times 2$  Hadamard matrix. Then  $(A, B; C)$  and  $(B, A; C)$  are Hadamard matrices. If  $A$  is of type  $H(n, q)$  and  $C$  is of type  $H(2, q)$  then type of  $(A, B; C), (B, A; C)$  have a determined type.

**Example 2.28.** As an explicit example consider the following:

Let  $A = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, B = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, C = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ , where  $\omega$  is a primitive  $3^{rd}$  root of unity.

Then  $(A, B; C), (B, A; C)$  are  $6 \times 6$  unitary matrices with entries which are  $\alpha = \frac{1}{\sqrt{6}}$  times  $6^{th}$  roots of unity and so  $\alpha(A, B; C), \alpha(B, A; C)$  are Hadamard matrices with entries which are  $6^{th}$  roots of unity.

This can also be played out for the discrete cosine and sine transforms. Let  $A, B$  be discrete transforms and  $C$  any  $2 \times 2$  unitary matrix. Then  $\{(A, B; C), (B, A; C)\}$  are multidimensional transforms which are not matrix tensor products.

Hadamard matrices have been designed from matrix tensor products – if  $A, B$  are Hadamard matrices so is  $A \otimes B$ . Many formulations of Hadamard constructions are equivalent to matrix tensor product constructions.

Thus tangle product generalises the matrix tensor product method for constructing Hadamard matrices; the matrix tensor product method includes Sylvester’s method. Sylvester’s method for producing Walsh matrices starts out with  $U = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  and goes to  $\begin{pmatrix} A & A \\ A & -A \end{pmatrix}$  where  $A$  has already been constructed; this is  $A \otimes U$ . A similar series may be obtained by starting out with for example beginning with the same or different initial  $U$  and then producing  $(A, B; U)$  from previously produced  $A, B$ . Indeed the  $U$  could change at any stage. The Walsh-Hadamard transfer has uses in many areas and is formed using a matrix tensor product starting out with  $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ . Many variations on this may be obtained using matrix tangle products; for instance the related matrices  $\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  could be used and entangled.

Hadamard matrices can also be designed from paraunitary matrices which themselves have been designed by orthogonal symmetric complete sets of idempotents, see section 2.1.

**2.8. Combine COSI and Diță type.** Subsection 2.1 devises COSI constructions and subsection 2.2 initiates Diță type constructions. The two may be combined to derive further builders. The COSI construction can be used to construct unitary, paraunitary or Hadamard matrices and these may then be used to construct matrix types using the Diță construction. On the other hand suppose a unitary matrix is constructed by either method. Then the columns of the matrix may be used to construct COSI sets from which further unitary, paraunitary or other entangled matrix types can be constructed by the COSI method of section 2.1.

**Example 2.29.** Let  $U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$ . Then form  $(U; A, B) = \frac{1}{2} \begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \\ 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \end{pmatrix}$ . Thus  $2.(U; A, B)$  is a Hadamard  $H(4, 4)$  matrix.

Let  $F = u_1 u_1^*, F_2 = u_2 u_2^*, F_3 = u_3 u_3^*, F_4 = u_4 u_4^*$  where  $\{u_1, u_2, u_3, u_4\}$  are the columns of  $(U; A, B)$ .

Then  $\begin{pmatrix} F_1 \alpha_1 & F_2 \alpha_2 & F_3 \alpha_3 & F_4 \alpha_4 \\ F_2 \alpha_5 & F_3 \alpha_6 & F_4 \alpha_7 & F_1 \alpha_8 \\ F_3 \alpha_9 & F_4 \alpha_{10} & F_1 \alpha_{11} & F_2 \alpha_{12} \\ F_4 \alpha_{13} & F_1 \alpha_{14} & F_2 \alpha_{15} & F_3 \alpha_{16} \end{pmatrix}$ , for variables  $\alpha_i$ , is a paraunitary matrix; this is a unitary matrix when the variables are given values of modulus 1. Also  $F_1 \alpha_1 + F_2 \alpha_2 + F_3 \alpha_3 + F_4 \alpha_4$  is a paraunitary matrix when the variables are given values of modulus 1. The process may be continued and infinite sequences obtained.

**2.8.1. Infinite sequences.** Let  $\mathcal{P}$  be a property which is preserved by a matrix tangle product. Infinite series of entangled matrices with property  $\mathcal{P}$  may be obtained from constructions already given. Here we give some more general methods. Example 2.29 above gives the flavour. The methods lead easily to strong encryption techniques including public key systems. Error correcting codes may also be developed and both encryption and error-correcting may be included in the one system.

Construct infinite sequences of entangled matrices with property  $\mathcal{P}$  using initially two matrices with property  $\mathcal{P}$  as follows. Let  $A_1, A_2$  be  $2 \times 2$  matrices with a property  $\mathcal{P}$  which is preserved by matrix tangle product. Form the  $4 \times 4$  (different) entangled matrices  $(A_1; A_1, A_2) = A_{11}, (A_2; A_1, A_2) = A_{12}, (A_1; A_2, A_1) = A_{13}, (A_2; A_2, A_1) = A_{14}$  which then have property  $\mathcal{P}$ . Each of the 12 pairs  $\{A_{1i}, A_{1j} | i \neq j\}$  may be tangles with shuffler  $A_1$  or  $A_2$  giving 24 new entangled matrix tangle products of size  $8 \times 8$  with property  $\mathcal{P}$ . Choose 2 different elements of these 24 and form tangle products with either  $A_1$  or  $A_2$  to get  $16 \times 16$ . This can be continued indefinitely. At each stage, matrices with property  $\mathcal{P}$  are obtained.

**Example 2.30.** *Infinite series with real entries may be obtained. Suppose the initial matrices are real orthogonal as for example  $A_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, A_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$  or more generally of the form  $\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$  for differing  $\theta$ .*

**Construction 2.31.** *Let  $S = \{A_1, A_2, \dots, A_k\}$  be a set of size  $t \times t$  matrices with property  $\mathcal{P}$  and  $U$  an  $n \times n$  matrix with property  $\mathcal{P}$ . Construct  $(U; A_{i_1}, A_{i_2}, \dots, A_{i_n})$  or  $(A_{i_1}, A_{i_2}, \dots, A_{i_n}; U)$  with  $i_j \in \{1, 2, \dots, k\}$ . For example  $\mathcal{P}$  could be the property of being unitary and  $U$  could be the  $n \times n$  unitary Fourier matrix. To be non-separable it is necessary that the  $i_j$  not all be equal. This constructs  $nt \times nt$  matrices with property  $\mathcal{P}$ ; the  $A_i$  and  $U$  can vary. Infinite series are obtained by varying  $n$ . Infinite series may also be obtained by applying the construction again using the matrices constructed which have property  $\mathcal{P}$ . Many such different infinite sequences may be constructed.*

### 3. Unitary space time

In section 2 construction methods were laid out for various types of matrices and applications to the design of unitary, paraunitary and special types of these matrices were given. Here we give applications to the design of *constellations of matrices*. The design problem for unitary space time constellations is set out as follows in [12] and [6]: “Let  $M$  be the number of transmitter antennas and  $R$  the desired transmission rate. Construct a set  $\mathcal{V}$  of  $L = 2^{RM}$  unitary  $M \times M$  matrices such that for any two distinct elements  $A, B$  in  $\mathcal{V}$ , the quantity  $|\det(A - B)|$  is as large as possible. Any set  $\mathcal{V}$  such that  $|\det(A - B)| > 0$  for all distinct  $A, B \in \mathcal{V}$  is said to have *full diversity*.”

The number of transmitter antennas is the size  $M$  of the matrices. The set  $\mathcal{V}$  is known as a *constellation* and the *quality* of the constellation is measured by  $\zeta_{\mathcal{V}} = \frac{1}{2} \min_{V_l, V_m \in \mathcal{V}, V_l \neq V_m} |\det(V_l - V_m)|^{\frac{1}{M}}$

Methods for constructing constellations while determining their quality using orthogonal symmetric idempotent sets was initiated in [8]. These can now be expanded and further constellations obtained using the constructions in Section 2.

The survey article [15] proposes division algebras for this area and, although different, some comparisons can be made with the constructions here.

Let  $\{A_1, A_2, \dots, A_k\}$  be a constellation of  $m \times m$  matrices with quality  $\zeta$  and let  $U$  be a unitary matrix. Then

- (1)  $\{(U; A_{i_1}, A_{i_2}, \dots, A_{i_k}) | (i_1, i_2, \dots, i_k) \text{ is a derangement of } (1, 2, \dots, k)\}$  is a constellation of  $mk \times mk$  matrices of quality  $\zeta$ . A derangement is a permutation such that no element appears in its original position.
- (2) Let  $\{U_i | i = 1, 2, \dots, s\}$  be a constellation of quality  $\zeta$  of  $k \times k$  matrices and  $\{A_1, A_2, \dots, A_k\}$  any  $k$  unitary  $t \times t$  matrices. Then  $\{(U_i; A_1, A_2, \dots, A_k) | i = 1, 2, \dots, s\}$  is a constellation of  $kt \times kt$  matrices with quality also  $\zeta$ .

Unitary matrices and paraunitary matrices are constructed according to Proposition 2.2 using a COSI set  $\{E_1, E_2, \dots, E_k\}$  and forming

$$G = \begin{pmatrix} E_{i_{11}}\alpha_{11} & E_{i_{12}}\alpha_{12} & \dots & E_{i_{1k}}\alpha_{1k} \\ E_{i_{21}}\alpha_{21} & E_{i_{22}}\alpha_{22} & \dots & E_{i_{2k}}\alpha_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ E_{i_{k1}}\alpha_{k1} & E_{i_{k2}}\alpha_{k2} & \dots & E_{i_{kk}}\alpha_{kk} \end{pmatrix} \text{ where } \{E_1, E_2, \dots, E_k\} \text{ appear once in each row and column.}$$

Let  $G = \begin{pmatrix} E_1\alpha_1 & E_2\alpha_2 \\ E_2\alpha_1 & E_1\alpha_2 \end{pmatrix}$  where  $\{E_1, E_2\}$  is a COSI set of  $2 \times 2$  matrices and the  $\alpha_i$  are elements in  $\mathcal{C}$ . Then  $\det G = \alpha_1^2\alpha_2^2$ . Let now  $\alpha_i$  be  $n^{th}$  roots of unity and then  $\left\{ \begin{pmatrix} E_1\alpha_1 & E_2\alpha_2 \\ E_2\alpha_1 & E_1\alpha_2 \end{pmatrix} \right\}$  is a constellation which has full diversity when an  $n^{th}$  root of 1 appears just once in each block column. Let  $A = \begin{pmatrix} E_1\alpha_1 & E_2\alpha_2 \\ E_2\alpha_1 & E_1\alpha_2 \end{pmatrix}, B = \begin{pmatrix} E_1\beta_1 & E_2\beta_2 \\ E_2\beta_1 & E_1\beta_2 \end{pmatrix}$ . Then  $|\det(A - B)| = |(\alpha_1 - \beta_1)^2(\alpha_2 - \beta_2)^2| = |(\alpha_1 - \beta_1)|^2|(\alpha_2 - \beta_2)|^2$ .

The following is well-known and is easily verified.

**Lemma 3.1.** *Let  $z = \cos \theta + i \sin \theta$ . Then  $|1 - z| = 2|\sin \frac{\theta}{2}|$*

**Corollary 3.2.** *Let  $\alpha = \omega^i, \beta = \omega^j$  with  $i \neq j$  and  $\omega = e^{\frac{2i\pi}{n}}$  is a primitive  $n^{th}$  root of unity. Then  $|\alpha - \beta| = 2|\sin \theta|$  where  $\theta = \frac{\pi(j-i)}{n}$ .*

Now from Corollary 3.2,  $|\det(A - B)| \geq 2^4|\sin \theta|^4$  where  $\theta = \frac{\pi}{n}$ . Thus the quality of the constellation is  $\frac{1}{2}(2^4(|\sin \theta|)^4)^{\frac{1}{4}} = |\sin \theta|$ .

The number that can be in each constellation when  $n^{th}$  roots of unity are used is  $n$ . For  $n = 4$ ,  $\theta = \frac{\pi}{4}$  and the quality  $\approx 0.70710\dots$ ; the rate is  $\frac{1}{2}$ . For  $n = 8$ ,  $\theta = \frac{\pi}{8}$  and the quality is  $\approx 0.38268\dots$ ; the rate is  $\frac{3}{4}$ . For  $n = 16$ ,  $\theta = \frac{\pi}{16}$  and the quality is  $\approx 0.19509\dots$ ; the rate is 1.

Higher order constellations may also be designed, and quality determined explicitly, as follows.

Let  $G = \begin{pmatrix} E_1\alpha_1 & E_2\alpha_2 & \dots & E_n\alpha_n \\ E_n\alpha_1 & E_1\alpha_2 & \dots & E_{n-1}\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ E_n\alpha_1 & E_{n-1}\alpha_2 & \dots & E_1\alpha_n \end{pmatrix}$  where  $\{E_1, E_2, \dots, E_n\}$  is a COSI set and the  $\alpha_i$  are elements in  $\mathcal{C}$ . Then it may be shown that  $|\det(G)| = |\alpha_1\alpha_2 \dots \alpha_n|^n$ , where  $n$  is the size of the matrix  $E_j$ . The set of all  $\left\{ \begin{pmatrix} E_1\alpha_1 & E_2\alpha_2 & \dots & E_n\alpha_n \\ E_n\alpha_1 & E_1\alpha_2 & \dots & E_{n-1}\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ E_n\alpha_1 & E_{n-1}\alpha_2 & \dots & E_1\alpha_n \end{pmatrix} \right\}$  with the  $|\alpha_i| = 1$  is then a constellation of unitary matrices.

In particular let the  $\alpha_j$  be  $n^{th}$  of unity such that no  $\alpha_j$  appears in more than one block column. Then

the quality of this constellation is  $|\sin \theta|$  where  $\theta = \frac{\pi}{n}$ . Many such different constellations with good quality may be formed.

## REFERENCES

- [1] C. Polcino Milies and S. K. Sehgal, *An introduction to Group Rings*, Algebra and Applications, **1**, Kluwer Academic Publishers, Dordrecht, 2002.
- [2] G. Strang and T. Nguyen, *Wavelets and Filter Banks*, Wellesley-Cambridge Press, Wellesley, MA, 1996.
- [3] C. J. Colbourn and J. H. Dinitz (Eds.), *Handbook of combinatorial designs*, Discrete Mathematics and its applications, Chapman and Hall, London/New York, 2007.
- [4] H. V. Henderson, F. Pukelsheim and S. R. Searle, On the history of the kronecker product, *Linear and Multilinear Algebra*, **14** (1983) 113–120.
- [5] P. Powell, Calculating determinants of block matrices, 11 pp. <https://doi.org/10.48550/arXiv.1112.4379>.
- [6] B. M. Hochwald and W. Sweldens, Differential unitary space-time modulation, *IEEE Trans. Comm.*, **48** (2000) 2041–2052.
- [7] T. Hurley and B. Hurley, Paraunitary matrices and group rings, *Int. J. Group Theory*, **3** (2014) no. 1 31–56.
- [8] T. Hurley, Full diversity sets of unitary matrices from orthogonal sets of idempotents, <https://doi.org/10.48550/arXiv.1612.02202>.
- [9] R. Hosoya and H. Suzuki, Type II matrices and their Bose-Mesner algebras, *J. Algebraic Combin.*, **17** (2003) 19–37.
- [10] P. Diță, Some results on the parametrization of complex Hadamard matrices, *J. Phys. A*, **37** (2004) 5355–5374.
- [11] J. Zhou, Minh N. Do and J. Kovačević, Special paraunitary matrices, Cayley transform, and multidimensional orthogonal filter banks, *IEEE Trans. Image Process.*, **15** (2006) 511–519.
- [12] A. Shokrollahi, B. Hassibi, B. M. Hochwald and W. Sweldens, Representation theory for high-rate multiple-antenna code design, *IEEE Trans. Inform. Theory*, **47** (2001) 2335–2367.
- [13] T. Hurley, Unique builders for classes of matrices, *Spec. Matrices*, **9** (2021) 52–65.
- [14] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.
- [15] B. A. Sethuraman, Division algebras and wireless communication, *Notices Amer. Math. Soc.*, **57** (2010) 1432–1439.
- [16] P. P. Vaidyanathan, *Multirate systems and filterbanks*, Prentice-Hall, 1993.

### Ted Hurley

University of Galway (Formerly National University of Ireland Galway), Ireland

Email: [Ted.Hurley@universityofgalway.ie](mailto:Ted.Hurley@universityofgalway.ie)

### Barry Hurley

Friar's Hill, Galway, Ireland

Email: Ted. [barryj\\_2000@yahoo.co.uk](mailto:barryj_2000@yahoo.co.uk)