Some results on the parametrization of complex Hadamard matrices

2004 J. Phys. A: Math. Gen. 37 5355

(http://iopscience.iop.org/0305-4470/37/20/008)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **37** (2004) 5355–5374 PII: S0305-4470(04)73169-8

Some results on the parametrization of complex Hadamard matrices

P Diţă

Institute of Physics and Nuclear Engineering, PO Box MG6, Bucharest, Romania

E-mail: dita@zeus.theory.nipne.ro

Received 9 December 2003, in final form 10 March 2004
Published 5 May 2004
Online at stacks.iop.org/JPhysA/37/5355
DOI: 10.1088/0305-4470/37/20/008

Abstract

In this paper we provide an analytical procedure which leads to a system of $(n-2)^2$ polynomial equations whose solutions give the parametrization of the complex $n \times n$ Hadamard matrices. It is shown that in general the Hadamard matrices depend on a number of arbitrary phases and a lower bound for this number is given. The moduli equations define interesting geometrical objects whose study will shed light on the parametrization of the Hadamard matrices, as well as on some interesting geometrical varieties defined by them.

PACS number: 02.10.Sp

1. Introduction

Quantum information theory whose main source comes from a few astonishing features in the foundations of quantum mechanics is the theory of information which is carried by quantum systems from the preparation device to the measuring apparatus in a quantum mechanical experiment, see, e.g., [29]. Defining new concepts such as entangled states, teleportation or dense coding one hopes to be able to design and construct new devices, such as quantum computers, which will be useful in solving many problems 'unresolvable' by classical methods. Recently the mathematical structure which is behind such miracle machines was better understood by establishing a one-to-one correspondence between quantum teleportation schemes, dense coding schemes, orthogonal bases of maximally entangled vectors, bases of unitary operators and unitary depolarizers. The construction procedure will be efficient to the extent that the unitary bases can be generated, and the construction of these bases makes explicit use of the complex Hadamard matrices and Latin squares. The Hadamard matrices enter explicitly in the construction of the so-called shift-and-multiply bases of unitaries consisting of n^2 unitary operators U_{ij} acting on the standard canonical basis $\{e_k\} \in C^n$ as

$$U_{ij}e_k = H_{ik}^j e_{\tau(k,j)}$$

where H^j_{ik} are phases, and H^j is a complex Hadamard matrix for every j, and τ is a permutation on the set $(1, 2, \ldots, n)$. See Vollbrecht and Werner [27] and Werner [28] for details. They also appear in coding theory as 'nice error bases' in the form of the Fourier transform, or more generally, unitary bases of group type, see [18]. It seems that in physics the complex Hadamard matrices first appeared in quantum optics under the name of symmetric multiports [17, 24, 26], and they are the simplest examples of the complex Hadamard matrices which can be realized in the laboratory.

The aim of this paper is to provide a procedure for the parametrization of the complex Hadamard matrices for an arbitrary integer n. More precisely we will obtain a set of $(n-2)^2$ equations whose solutions will give all the complex Hadamard matrices of size n. The complex n-dimensional Hadamard matrices are unitary $n \times n$ matrices whose entries have modulus $1/\sqrt{n}$.

The term *Hadamard matrix* has its root in Hadamard's paper [15], where he gave the solution to the question of the maximum possible absolute value of the determinant of a complex $n \times n$ matrix whose entries are bounded by some constant, which, without loss of generality, can be taken equal to unity. Hadamard has shown that the maximum is attained by complex unitary matrices whose entries have the same modulus and he asked the question if the maximum can also be attained by orthogonal matrices. These last matrices have come to be known as *Hadamard matrices* in his honour, and have many applications in combinatorics, coding theory, orthogonal designs, quantum information theory, etc, and the standard reference for the obtained results is Agaian [1].

However, the first complex Hadamard matrices were found by Sylvester [25]. He observed that if $a_i, i = 0, 1, \ldots, n-1$, denote the solutions of the equation $x^n - 1 = 0$ for a prime n then the Vandermonde matrix built from a_i is unitary and Hadamard. In the same paper Sylvester found a method for obtaining a Hadamard matrix of size mn if one knows two Hadamard matrices of order m and n, respectively, by taking their Kronecker product. Soon after the publication of the paper by Hadamard interest was mainly in *real* Hadamard matrices such that the Sylvester contribution fell into oblivion and the *complex Hadamard matrices* were much later reinvented in a particular case: only those matrices whose entries are $\pm 1, \pm \mathrm{i}$ where $\mathrm{i} = \sqrt{-1}$.

Nevertheless a few other problems apparently unrelated to the complex Hadamard matrices were those connected with bounds on polynomial coefficients when the indeterminate runs on the unit circle. They are better expressed in terms of the discrete Fourier transform. For any finite sequence $x = (x_0, x_1, \ldots, x_{n-1})$ of n complex numbers, its (discrete) Fourier transform is defined by

$$y_j = n^{-1/2} \sum_{k=0}^{n-1} x_k \, \mathrm{e}^{2\mathrm{i}\pi kj/n} \qquad j = 0, 1, \ldots, n-1.$$

If the components x_k, y_k are such that $|x_k| = |y_k| = 1$ for $k = 0, 1, \ldots, n-1$ the sequence x is called bi-unimodular. The existence of a bi-unimodular sequence of side n is equivalent to the existence of a complex circulant Hadamard matrix of side n; a circulant matrix is obtained by circulating its first row, in our case the components of the vector $x/\sqrt{n}$. Now the Gauss sequence

$$x_k = \begin{cases} \mathrm{e}^{2\mathrm{i}\pi(ak^2+bk)/n} & a, b \in \mathbb{Z}, a \text{ coprime to } n, k = 0, 1, \ldots, n-1 \quad \text{for } n \text{ odd} \\ \mathrm{e}^{k^2\mathrm{i}\pi/n} & k = 0, 1, \ldots, n-1 \quad \text{for } n \text{ even} \end{cases}$$

is a bi-unimodular sequence [7]. The problem of the complete determination of all bi-unimodular sequences is still open, despite the problem being simpler than the

parametrization of arbitrary complex Hadamard matrices. However, this approach gave the first non-trivial examples of the complex Hadamard matrices for $n \geqslant 6$.

A step towards its solution was the reduction of the bi-unimodular problem to the problem of finding all cyclic n-roots [4], and all cyclic n-roots have been found for $2 \leqslant n \leqslant 8$, see Björck and Fröberg [5, 6]. The formalism we will develop in this paper is more general, showing that the parametrization of the complex Hadamard matrices is more complicated than the finding of all cyclic n-roots. Using our approach we find, e.g., when $n = 6$, the following matrix which is not contained in the above solutions

$$\frac{1}{\sqrt{6}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} \\ 1 & \mathrm{i} & -1 & \mathrm{e}^{\mathrm{i}t} & -\mathrm{e}^{\mathrm{i}t} & -\mathrm{i} \\ 1 & -\mathrm{i} & -\mathrm{e}^{-\mathrm{i}t} & -1 & \mathrm{i} & \mathrm{e}^{-\mathrm{i}t} \\ 1 & -\mathrm{i} & \mathrm{e}^{-\mathrm{i}t} & \mathrm{i} & -1 & -\mathrm{e}^{-\mathrm{i}t} \\ 1 & \mathrm{i} & -\mathrm{i} & -\mathrm{e}^{\mathrm{i}t} & \mathrm{e}^{\mathrm{i}t} & -1 \end{pmatrix}$$

a matrix that depends on an arbitrary phase.

The parametrization of the complex Hadamard matrices is a special case of a more general problem: the problem of reconstructing the phases of a unitary matrix from the knowledge of the moduli of its entries, a problem which was a fashionable one at the end of eighties in the last century in the high energy physics community, see Auberson [2], Björken and Dunietz [8], Branco and Lavoura [9], Auberson *et al* [3]. An existence theorem as well as an estimation for the number of solutions was obtained in [11]. Particle physicists abandoned the problem when they realized that for $n \geqslant 4$ there exists a continuum of solutions, i.e. solutions depending on arbitrary phases—a result that was considered uninteresting from the physical point of view. In our opinion, the reason was the difficulty of the problem; since the experiments provide only the squares of the moduli, the first problem is to decide if from the experimental results, which in the best case generate a doubly stochastic matrix, one can reconstruct a unitary matrix, or a unistochastic matrix. Only for $n = 3$ does there exist an unambiguous procedure. For $n \geqslant 4$ there are no known necessary and sufficient conditions to separate the unistochastic matrices from the doubly stochastic ones [31].

Almost at the same time the complex Hadamard matrices emerged in the construction of some $*$-subalgebras in finite von Neumann algebras, see Popa [23], de la Harpe and Jones [16] and Munemasa and Watatani [20]. In the last two papers one constructs the complex Hadamard matrices not of Sylvester type when n is a prime number such that $n \equiv \pm 1 \pmod 4$. A little later Haagerup [14] obtained the first example of a six-dimensional matrix which is not covered by the solutions to cyclic n-roots equations [4].

In this paper we use a few analytic techniques from the operator contraction theory and the factorization of unitary matrices to obtain a convenient representation of unitary matrices of arbitrary order n that leads easily to a system of $(n-2)^2$ trigonometric (or equivalently polynomial) equations whose solutions give all the complex Hadamard matrices of order n. Our approach is also useful for finding the *real* Hadamard matrices, being complementary to the combinatorial approach almost exclusively used until now.

The paper is organized as follows. In section 2 a theorem showing the existence of the complex Hadamard matrices for every integer n is stated and an upper bound on the number of continuum solutions is obtained. Section 3 contains a one-to-one parametrization of unitary matrices written as block matrices, and in the next section an application of the obtained formulae is given. In section 5 another parametrization of unitary matrices is given in the form of a product of n diagonal phase matrices interlaced with $n-1$ orthogonal matrices each one generated by a real vector from $\mathbb{R}^n$. This form is convenient because it leads to a

simpler form for the moduli equations and at the same time we consider it more appropriate for designing software packages for solving these equations. In section 6 we show how to derive the moduli equations as trigonometric equations and give a few particular solutions for $n = 6$. In section 7 the problem is reformulated as an algebraic geometry problem and we show that the parametrization of the Hadamard matrices can produce interesting examples for many problems currently under study in this field. The paper ends with the conclusions.

2. Existence of complex Hadamard matrices

The complex n-dimensional Hadamard matrices H_n being unitary matrices whose entries have modulus $1/\sqrt{n}$, the natural class for looking for the complex Hadamard matrices is the unitary group $U(n)$. From the definition, it follows that, since the multiplication of a row and/or a column by an arbitrary phase factor does not change the properties of H_n, we can remove the phases of a row and column taken arbitrarily, such that in the following H_n will be a matrix with all the entries of the first row and of the first column positive numbers. Similarly, we can permute any rows and/or columns and get an equivalent matrix. Besides, for the Hadamard matrices we will not distinguish between H_n and its complex conjugate matrix $\bar{H}_n$, the complex conjugation being equivalent to the sign change of all the phases $\varphi_i \to -\varphi_i$ entering the parametrization. More generally we shall consider two equivalent matrices whose phases can be obtained by an arbitrary non-singular linear transformation with constant rational coefficients. In the following we will consider two equivalent matrices that can be made equal by applying a finite number of the above transformations on them.

Since a unitary matrix is parametrized by $n(n-1)/2$ angles and $n(n+1)/2$ phases [10] we deduce that the number of remaining phases is $n(n+1)/2 - (2n-1) = (n-1)(n-2)/2$, and so the number of free real parameters entering a unitary matrix is reduced from n^2 to $n^2 - (2n-1) = (n-1)^2$.

The parametrization of a unitary matrix by the moduli of its entries is very appealing, and in the case of the Hadamard matrices compulsory, although it is not a natural one in the general case. A natural parametrization would be one whose parameters are free, i.e. there are no supplementary restrictions upon them to enforce unitarity. In this sense natural parametrizations are the Euler-type parametrization by Murnagham [21], or that found in [10].

The problem we raised in [11] was to what extent the knowledge of the moduli $|a_{ij}|$ of an $n \times n$ unitary matrix $A_n = (a_{ij})$ determines A_n. Implicitly we supposed that A_n is parametrized by n^2 independent parameters. But from what we said before we know that we may ignore $2n-1$ phases entering the first row and the first column, and consequently the number of independent parameters reduces to $(n-1)^2$, which coincides with the number of independent moduli implied by unitarity. If we identify the parameters with the moduli they will be lying within the simple domain

$$D = (0,1) \times \cdots \times (0,1) \equiv (0,1)^{(n-1)^2}$$

where the above notation means that the number of factors entering the topological product is $(n-1)^2$. We excluded only the extremities of each interval, i.e. the points 0 and 1, that is a zero measure set within $U(n)$ and has no relevance to the parametrization of the complex Hadamard matrices.

Thus, in principle, we can parametrize an $n \times n$ unitary rephasing invariant matrix by the upper-left corner moduli; we exclude the moduli of the last row and of the last column since they follow from unitarity. Nothing remains but to check if the new parametrization is one-to-one. A solution to the last problem is the following: start with a one-to-one parametrization of $U(n)$ and then change the coordinates taking as new coordinates the moduli of the $(n-1)^2$ upper-left

corner entries (and $2n-1$ ignorable phases). Afterwards use the implicit function theorem to find the points where the new parametrization fails to be one-to-one. The corresponding variety upon which the application is not a bijective one is given by setting to zero the Jacobian of the transformation. One gets that generically for $n \geqslant 4$ the unitary group $U(n)$ cannot be fully parametrized by the moduli of its entries, i.e. for a given set of moduli there could exist a continuum of solutions, but this negative result is good for the parametrization of the Hadamard matrices by decreasing the number of independent solutions.

If the moduli are outside the above variety an upper bound for the multiplicity is $2^{\frac{n(n-3)}{2}}$. However, in the case of the Hadamard matrices the equivalence constraints reduce this number to lower values than the above upper bound. The bound is saturated for $n = 3$ when there is essentially only one complex matrix, i.e. for given moduli values for the first row and column entries compatible with unitarity, the sole freedom is an arbitrary phase. If we denote the relevant squared moduli by m_1, m_2, m_3, m_4 and the phase by φ then the compatibility condition has the form

$$-1 \leqslant \cos\varphi = \big(-1 + 2m_1 - m_1^2 + m_2 + m_3 + m_4 - m_1m_2 - m_1m_3 - m_2m_3 - 2m_1m_4 - m_1m_2m_3m_1^2m_4\big)\big/2\sqrt{m_1m_2m_3(1-m_1-m_2)(1-m_1-m_3)} \leqslant 1.$$

This is also the necessary and sufficient condition which the squared moduli m_i, $i = 1, \ldots, 4$, have to satisfy in order to obtain a unistochastic matrix from a general doubly stochastic matrix. Because unitary matrices of arbitrary dimension do exist and on the other hand the number of independent essential parameters of a $U(n)$ matrix is $(n-1)^2$ the following is true:

Theorem 1. *Suppose $(x_1, \ldots, x_{n^2})$ is a coordinate system on the unitary group $U(n)$ consisting of $n(n-1)/2$ angles each taking values in $[0, \pi/2]$ and $n(n+1)/2$ phases taking values in $[0, 2\pi)$. By discarding $2n-1$ non-essential phases the number of coordinates reduces to $(n-1)^2$, $(x_1, \ldots, x_{(n-1)^2})$, which coincides with the number of independent moduli $(m_1, \ldots, m_{(n-1)^2})$ implied by unitarity. Taking as new coordinates the moduli m_i, $i = 1, \ldots, (n-1)^2$, the new parametrization is generically not one-to-one for $n \geqslant 4$, the non-uniqueness variety being obtained by setting to zero the Jacobian of the transformation*

$$\frac{\partial(m_1, \ldots, m_{(n-1)^2})}{\partial(x_1, \ldots, x_{(n-1)^2})} = 0. \tag{1}$$

Outside this variety the number of discrete solutions N_s satisfies $1 \leqslant N_s \leqslant 2^{\frac{n(n-3)}{2}}$ and on the variety described by (1) there is a continuum of solutions, i.e. solutions that depend on arbitrary phases. In the special case of the complex Hadamard matrices all the solutions are given by the system of trigonometric equations

$$m_i^2(x_1, \ldots, x_{(n-1)^2}) = \frac{1}{n} \qquad i = 1, \ldots, (n-1)^2. \tag{2}$$

Suppose we know the irreducible components of the variety (1) and let $r(n)$ be the rank of the system (2) in every irreducible component, then every solution of (2) in such an irreducible component will depend upon $(n-1)^2 - r(n)$ arbitrary parameters and the number of (continuum) solutions satisfies $1 \leqslant N_s \leqslant 2^{r(n)-1-n(n-1)/2}$.

Proof. In the general case equations (2) have the form

$$m_i^2\big(x_1, \ldots, x_{(n-1)}^2\big) = a_i \qquad \text{where} \quad a_i \in (0,1) \quad i = 1, \ldots, (n-1)^2. \tag{3}$$

The parameters a_i generate a doubly stochastic matrix. Equations (3), as we will see later, are trigonometric equations in our parametrization, and consequently the multiplicity of the solutions may arise from the two possible phase solutions for all values of sine or cosine

functions that satisfy (3). The number of independent phases is $(n-1)(n-2)/2$ and, since we do not make any distinction between H_n and $\bar{H}_n$, where a bar denotes complex conjugation, a condition which halves the number of solutions, the above bound for N_s follows. A similar argument establishes the upper bound for the number of continuum solutions. □

For $n = 3$ the Jacobian is positive and $1 \leqslant N_s \leqslant 1$, which implies the existence of one complex matrix irrespective of the values a_i, compatible with unitarity.

It is easily seen that the equations which correspond to the first row and the first column entries have a unique solution and the number of equations reduces to $(n-2)^2$. Indeed, because these entries are positive we can take the following parametrization in terms of $2n-3$ angles, e.g., for the first row

$$(a_{11}, \ldots, a_{1n}) = (\cos\chi_1, \sin\chi_1 \cos\chi_2, \ldots, \sin\chi_1 \cdots \sin\chi_{n-1})$$

and similarly for the first column. Equations (3) give the unique solution

$$\cos^2\chi_k = \frac{a_k}{\prod_{i=1}^{k-1}(1-a_i)} \qquad k = 1, 2, \ldots, n-1$$

where $a_k = |a_{1k}|^2$, $k = 1, 2, \ldots, n-1$. In the case of the Hadamard matrices one gets

$$\cos\chi_k = \frac{1}{\sqrt{n+1-k}} \qquad k = 1, 2, \ldots, n-1$$

and the same solution for the angles parametrizing the first column. In this way the number of equations reduces to $(n-1)^2 - (2n-3) = (n-2)^2$ and the upper bound for the continuous solutions may be written as $1 \leqslant N_s \leqslant 2^{r(n)-1-(n-2)(n-3)/2}$, where $r(n)$ is the rank of the reduced system. Even so the number of equations grows quadratically with n, which shows that even for moderate values of n the problem is not easy to solve.

In conclusion we have a system of trigonometric equations whose solutions will give all the complex Hadamard matrices, but to be effective we have to start with a one-to-one parametrization of unitary matrices in order to find the explicit form of the $(n-2)^2$ equations and try to solve them. In the following section we will provide one of the two parametrizations of unitary matrices that we will use in this paper.

3. Parametrization of unitary matrices

The aim of this section is to provide a one-to-one parametrization of unitary matrices that will be useful in describing the complex Hadamard matrices. We shall present two such parametrizations and for the first one we follow closely our paper [10] showing here only the points which are important in the following. The algorithm we provide is a recursive one, allowing the parametrization of $n \times n$ unitary matrices through the parametrization of lower-dimensional ones. The parametrization will be one-to-one and given in terms of $a(n)$ angles taking values in $[0, \pi/2]$ and $\varphi(n)$ phases taking values in $[0, 2\pi)$ such that the application

$$A_n (A_n \in U(n),\, A_n A_n^* = I_n) \to E = (0, \pi/2)^{a(n)} [0, 2\pi)^{\varphi(n)} \subset \mathbb{R}^{n^2}$$

is bijective. In the following the ends of the interval $[0, \pi/2]$ will be obtained by continuation in the relevant parameters, if necessary.

The starting point is the partitioning of the matrix $A_n \in U(n)$ into blocks

$$A_n = \begin{pmatrix} A & B \\ C & D \end{pmatrix}. \tag{4}$$

For definiteness we suppose the order of A is equal to m with $m \leqslant n/2$. The blocks entering (4) are contractions as follows from unitarity

$$AA^* + BB^* = I_m \qquad A^*A + C^*C = I_m \qquad CC^* + DD^* = I_{n-m} \tag{5}$$

where in the following I_k denotes the $k \times k$ unit matrix. Suppose we know the contraction A, then the problem reduces to finding the B, C and D blocks such that A_n should be unitary. In other words the problem is knowing a contraction A of side m how we can border it for getting a unitary $n \times n$ matrix A_n. The complete solution is found in [10]. For any contraction T, with $\|T\| \leqslant 1$, we have $T^*T \leqslant I_{\mathcal{H}'}$ and $TT^* \leqslant I_{\mathcal{H}}$ such that the defect operators

$$D_T = (I_{\mathcal{H}} - T^*T)^{1/2} \qquad D_{T^*} = (I_{\mathcal{H}'} - TT^*)^{1/2}$$

are Hermitian operators that have the property

$$TD_T = D_{T^*}T \qquad T^*D_{T^*} = D_T T^*. \tag{6}$$

The most difficult part is to find the D block; it is given by

$$D = -VA^*U + XMY \tag{7}$$

such that the following holds.

Lemma 1. *The unitary matrix A_n in equation (4) is given by*

$$A_n = \begin{pmatrix} A & D_{A^*}U \\ VD_A & -VA^*U + XMY \end{pmatrix}$$

where U and V are two isometries such that $B = UD_{A^*}$, $C = D_A V$, X and Y are those unitary matrices that diagonalize the Hermitian defect operators D_{V^*} and D_U respectively, i.e.

$$X^*D_{V^*}X = P \qquad Y^*D_U Y = P$$

P is the projection

$$P = \begin{pmatrix} 0 & 0 \\ 0 & I_{n-2m} \end{pmatrix}$$

and the matrix M has the form

$$M = \begin{pmatrix} 0 & 0 \\ 0 & A_{n-2m} \end{pmatrix}$$

where A_{n-2m} denotes an arbitrary $(n-2m) \times (n-2m)$ unitary matrix.

In the above formulae we supposed that the eigenvectors of the D_U and D_{V^*} operators entering the matrices X and Y are ordered in increasing order of the eigenvalues.

Therefore the parametrization of an $n \times n$ unitary matrix requires the parametrization of an $m \times m$ contraction, of two isometries U and V and of an $(n-2m) \times (n-2m)$ unitary matrix. Taking into account the recursive nature of the form for A_n we may consider the case $m = 1$ and provide an explicit algorithm for getting the unitary matrices X and Y. Since for $m = 1$, A is the simplest contraction, a complex number whose modulus is less than 1, one finds that V is an $(n-1)$-dimensional vector, and the isometry property allows us to parametrize it as $V = (\cos\chi_1, \sin\chi_1 \cos\chi_2, \ldots, \sin\chi_1, \ldots, \sin\chi_{n-2})^t$ where t denotes the transpose. V is the eigenvector of D_{V^*} corresponding to the zero eigenvalue. Indeed from relations (6) we have

$$D_{V^*}V = VD_V = 0$$

showing that V is the eigenvector of D_{V^*} corresponding to the zero eigenvalue. Thus the problem is how to complete an orthogonal matrix X knowing its first column (row) such that no supplementary parameters enter. The other columns of this matrix we are looking for will

be given by the other eigenvectors of D_{V^*}. One easily verifies that D_{V^*} is a projection operator such that the other eigenvalues equal unity. Indeed the following holds:

Lemma 2. *The orthonormalized eigenvectors of the eigenvalue problem*

$$D_{V^*}v_k = \lambda_k v_k \qquad k = 1, \ldots, n-1$$

are the columns of the orthogonal matrix $X \in SO(n-1)$ and are generated by the vector V as

$$v_1 = \begin{pmatrix} \cos\chi_1 \\ \sin\chi_1 \cos\chi_2 \\ . \\ . \\ . \\ \sin\chi_1 \ldots \sin\chi_{n-2} \end{pmatrix}$$

and

$$v_{k+1} = \frac{\mathrm{d}}{\mathrm{d}\chi_k} v_1 \left(\chi_1 = \cdots = \chi_{k-1} = \frac{\pi}{2}\right) \qquad k = 1, \ldots, n-2$$

where in the above formula one calculates first the derivative and afterwards the restriction to $\pi/2$.

In a similar way one finds Y, see [12] for a proof.

In the case of the $n \times n$ Hadamard matrices whose elements of the first row and of the first column are positive numbers $a_{1j} = a_{j1} = \frac{1}{\sqrt{n}}$, $j = 1, \ldots, n$, X has the form

$$\begin{pmatrix} \frac{1}{\sqrt{n-1}} & -\sqrt{\frac{n-2}{n-1}} & 0 & 0 & \cdots & \cdots & 0 & 0 \\ \frac{1}{\sqrt{n-1}} & \frac{1}{\sqrt{(n-1)(n-2)}} & -\sqrt{\frac{n-3}{n-2}} & 0 & \cdots & \cdots & 0 & 0 \\ \frac{1}{\sqrt{n-1}} & \frac{1}{\sqrt{(n-1)(n-2)}} & \frac{1}{\sqrt{(n-2)(n-3)}} & -\sqrt{\frac{n-4}{n-3}} & \cdots & \cdots & 0 & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ \frac{1}{\sqrt{n-1}} & \frac{1}{\sqrt{(n-1)(n-2)}} & \frac{1}{\sqrt{(n-2)(n-3)}} & \frac{1}{\sqrt{(n-3)(n-4)}} & \cdots & \cdots & \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{n-1}} & \frac{1}{\sqrt{(n-1)(n-2)}} & \frac{1}{\sqrt{(n-2)(n-3)}} & \frac{1}{\sqrt{(n-3)(n-4)}} & \cdots & \cdots & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

and $Y = X^t$, where t denotes the transpose.

In this way all the quantities entering formula (7) are known and the parametrization of A_n can be obtained recursively starting with the known parametrization of 2×2 unitary matrices.

When the block A is one dimensional, i.e. a simple number equal to $1/\sqrt{n}$, the term VA^*U entering equation (7) has the form $\frac{1}{(n-1)\sqrt{n}} J$, where J is the $(n-1) \times (n-1)$ matrix each of whose entries is +1, which appears in many constructions of the *real* Hadamard matrices, see Agaian [1].

4. Application

In the following we will use the results of lemma 1 to generalize to the case of the complex Hadamard matrices the tricks used by Sylvester [25] and Hadamard [15] for constructing the complex Hadamard matrices. We take n an even number, $n = 2m$, and we suppose that we

know a parametrization of the A block which is unitary and whose order is m. In that case the B and C blocks are also unitary matrices of order m and we consider them normalized as $AA^* = BB^* = CC^* = I_m$. From (7) we have $D = -CA^*B$ and the matrix

$$\frac{1}{\sqrt{2}}\begin{pmatrix} A & B \\ C & -CA^*B \end{pmatrix}$$

will be unitary by construction. In general, the above matrix will not be Hadamard even when A, B and C are, as the simplest example shows; this happens only when either $C = A$ or $B = A$. Since the second case is obtained by transposing the matrix of the first one, as long as B and C are arbitrary, we will consider only the matrix

$$\frac{1}{\sqrt{2}}\begin{pmatrix} A & B \\ A & -B \end{pmatrix} \tag{8}$$

which is the elementary two-dimensional array that will be used in the construction of more complicated arrays of the Hadamard matrices. In the following we suppose that A and B are the complex Hadamard matrices of size m each depending on $p \geqslant 0$ and $q \geqslant 0$ free phases, respectively, i.e. (8) is a complex Hadamard matrix of size $2m$. Now we make use of Hadamard's trick to get a Hadamard matrix depending on $p + q + m - 1$ arbitrary phases. Indeed we can multiply B at left by the diagonal matrix $d = (1, \mathrm{e}^{\mathrm{i}\varphi_1}, \ldots, \mathrm{e}^{\mathrm{i}\varphi_{m-1}})$ without modifying the Hadamard property. In this way Hadamard obtained a continuum of solutions for the case $n = 4$. We denote $B_1 = d \cdot B$ and then the matrix

$$\frac{1}{\sqrt{2}}\begin{pmatrix} A & B_1 \\ A & -B_1 \end{pmatrix} \tag{9}$$

will be unitary and Hadamard depending on $p + q + m - 1$ parameters. From (9) we obtain in general two non-equivalent $2m \times 2m$ Hadamard matrices when $B \neq B^*$. In this case equation (9) is a realization and the second one is given by $B_1 \to B_2 = d \cdot B^*$. The above procedure can be iterated by taking the matrix (8) as a new A block obtaining a Hadamard matrix of the form

$$\frac{1}{2}\begin{pmatrix} A & B & C & D \\ A & -B & C & -D \\ A & B & -C & -D \\ A & -B & -C & D \end{pmatrix} \tag{10}$$

which is a $4m$-dimensional array similar to the Williamson array [30], and so on. In contradistinction to the Williamson array the A, B, C, D blocks satisfy no supplementary conditions, except their unitarity. Thus the following holds:

Proposition 1. *If the $m \times m$ complex Hadamard matrices A, B, C, D depend on p, q, r, s arbitrary phases then there exists a complex Hadamard matrix of the form (10) which depends on $p + q + r + s + 3(m - 1)$ arbitrary phases.*

We note that the elementary array (8) is different from the Goethals–Seidel one [13] which appears in the construction of the *real* Hadamard matrices and which has the form

$$\frac{1}{\sqrt{2}}\begin{pmatrix} A & B \\ B & -A \end{pmatrix}.$$

The above array is not unitary even when A and B are, the supplementary condition for unitarity being the relation $AB^* = BA^*$. We consider that the form (8) could also be useful for the study of orthogonal designs and *real* Hadamard matrices, it being in some sense complementary to the above form.

As an application of formula (10) we consider the following case: $a_{11} = a_{12} = a_{21} = -a_{22} = b_{11} = b_{12} = c_{11} = c_{12} = d_{11} = d_{12} = 1/\sqrt{2}$ and $b_{21} = -b_{22} = \mathrm{e}^{\mathrm{i}s}/\sqrt{2}$, $c_{21} = -c_{22} = \mathrm{e}^{\mathrm{i}t}/\sqrt{2}$, $d_{21} = -d_{22} = \mathrm{e}^{\mathrm{i}u}/\sqrt{2}$ where the notation is self-explanatory, and we obtain an eight-dimensional Hadamard matrix depending on three arbitrary phases s, t, u.

When $A = B$, equation (8) can be written as

$$\frac{1}{\sqrt{2}}\begin{pmatrix} A & A \\ A & -A \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & \epsilon \end{pmatrix} \otimes A \tag{11}$$

where $\epsilon = -1$, i.e. the first factor is the Sylvester–Vandermonde matrix of the second roots of unity, and $\otimes$ is the ordinary Kronecker product, $A \otimes B = [a_{ij}B]$; of course the first factor can be any complex Hadamard matrix of order m. Now we want to define a new product, the aim being a more general construction of the Hadamard matrices. Let M and N be two matrices of the same order m whose elements are matrices M_{ij} of order n and N_{kl} of order p, respectively. The new product denoted by $\tilde{\otimes}$ is given as

$$Q = M \tilde{\otimes} N$$

which is a matrix of order mnp, where

$$Q_{ij} = \sum_{k=1}^{k=m} M_{ik} \otimes N_{kj}.$$

We will use the above formula only in the case $M = m_{ij}$, where m_{ij} are complex scalars, not matrices, and N is an arbitrary diagonal matrix $N = (N_{11}, \ldots, N_{mm})$, where N_{ii} are matrices of order p obtaining

$$Q = \begin{pmatrix} m_{11}N_{11} & \cdot & \cdot & m_{1m}N_{mm} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ m_{1m}N_{11} & \cdot & \cdot & m_{mm}N_{mm} \end{pmatrix} \tag{12}$$

Thus the following is true.

Proposition 2. *If the matrices M and N_{ii}, $i = 1, \ldots, m$, are Hadamard so will be the matrix Q given by equation (12).*

The order of Q is mp and formula (12) is new even for real Hadamard matrices. This form is the most general array we have obtained and in some sense (12) is the natural generalization of Williamson arrays to the case of complex Hadamard matrices.

If in the above relation we take $m_{11} = m_{12} = m_{21} = -m_{22} = 1/\sqrt{2}$ and $N_{11} = A$ and $N_{22} = B$, then equation (12) reduces to equation (8).

Example 1. If now m_{ij} are the same as above and

$$N_{11} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -\mathrm{e}^{\mathrm{i}s} & \mathrm{e}^{\mathrm{i}s} \\ 1 & -1 & \mathrm{e}^{\mathrm{i}s} & -\mathrm{e}^{\mathrm{i}s} \end{pmatrix}$$

is the complex four-dimensional Hadamard matrix and

$$N_{22} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}t} & 0 & 0 \\ 0 & 0 & \mathrm{e}^{\mathrm{i}u} & 0 \\ 0 & 0 & 0 & \mathrm{e}^{\mathrm{i}v} \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -\mathrm{e}^{\mathrm{i}y} & \mathrm{e}^{\mathrm{i}y} \\ 1 & -1 & \mathrm{e}^{\mathrm{i}y} & -\mathrm{e}^{\mathrm{i}y} \end{pmatrix}$$

we obtain an eight-dimensional matrix depending now on five arbitrary phases s, t, u, v, y instead of three as in the preceding example obtained by using the Williamson-type array (12).

Thus the following holds.

Proposition 3. *If M, N_i, $i = 1, \ldots, m$, are $m \times m$ and $n \times n$-dimensional complex Hadamard matrices, respectively, depending on m and n_i arbitrary phases, respectively, then there is an array of the form (12) that depends on*

$$m + n_1 + (m-1)\sum_{i=2}^{m} n_i$$

free phases.

The above example shows the necessity for getting upper and lower bounds on the number of arbitrary phases entering a Hadamard matrix of size N. Taking into account the standard decomposition of any integer in the form $N = p_1^{q_1} \cdots p_m^{q_m}$, where $p_1 < \cdots < p_m$ are primes and $q_1 \cdots q_m$ their respective powers, we may use proposition 3 for obtaining lower bounds on the number of free phases, which we shall denote by $\varphi(N)$. Since until now there does not exist an example of a Hadamard matrix of size N with N prime which depends on free phases, in the following we will consider the normalization $\varphi(N) = 0$, for N prime. Thus the following holds.

Theorem 2. *Let $N = p_1^{q_1}$ be the power of a prime p_1, with $q \geqslant 2$. Then a lower bound for $\varphi\big(p_1^{q_1}\big)$, the number of free phases entering the parametrization of the $N \times N$ complex Hadamard matrix, is given by*

$$\varphi\big(p_1^{q_1}\big) = 1 + [(p_1 - 1)(q_1 - 1) - 1]p_1^{q_1 - 1}.$$

If $N = p_1^{q_1} \cdots p_m^{q_m} = p_1^{q_1} N_1$ then $\varphi\big(p_1^{q_1} N_1\big)$ is given by

$$\varphi\big(p_1^{q_1} N_1\big) = 1 + [(p_1 - 1)q_1 N_1 - p_1]p_1^{q_1 - 1} + \varphi(N_1)p_1^{q_1}.$$

Proof. Using proposition 3 we find the recurrence relation

$$\varphi\big(p_1^{q_1}\big) = p_1 \varphi\big(p_1^{q_1 - 1}\big) + (p_1 - 1)\big(p_1^{q_1 - 1} - 1\big)$$

with the initial condition $\varphi(p_1) = 0$ and the solution follows.

In the second case the recurrence relation reads

$$\varphi\big(p_1^{q_1} N_1\big) = p_1 \varphi\big(p_1^{q_1 - 1} N_1\big) + (p_1 - 1)\big(p_1^{q_1 - 1} N_1 - 1\big)$$

and the initial condition can be taken as

$$\varphi(p_1 N_1) = p_1 \varphi(N_1) + (p_1 - 1)(N_1 - 1)$$

and the solution follows. The above recurrence relation allows us to obtain lower bounds for any integer N in the form

$$\begin{aligned}
\varphi\big(p_1^{q_1} \cdots p_m^{q_m}\big) = {} & 1 + \big[(p_1 - 1)q_1 p_2^{q_2} \cdots p_m^{q_m} - p_1\big]p_1^{q_1 - 1} \\
& + p_1^{q_1}\big\{1 + \big[(p_2 - 1)q_2 p_3^{q_3} \cdots p_m^{q_m} - p_2\big]p_2^{q_2 - 1}\big\} \\
& + p_2^{q_2}\big\{1 + \big[(p_3 - 1)q_3 p_4^{q_4} \cdots p_m^{q_m} - p_3\big]p_3^{q_3 - 1}\big\} \\
& + p_3^{q_3}\big\{1 + \cdots + p_{m-1}^{q_{m-1}}\big\{1 + [(p_m - 1)q_m - p_m]p_m^{q_m - 1}\big\} \\
& + p_{m-1}^{q_{m-1}}\big\{1 + [(p_m - 1)(q_m - 1) - 1]p_m^{q_m - 1}\big\} \cdots \big\}.
\end{aligned}$$

□

We give now a few examples.

Example 2. If $N = p_1^{q_1} p_2^{q_2}$ then the lower bound for $\varphi\big(p_1^{q_1} p_2^{q_2}\big)$, the number of free phases entering the parametrization of the $N \times N$ complex Hadamard matrix, is given by

$$\varphi\big(p_1^{q_1} p_2^{q_2}\big) = 1 + (p_1 - 1)q_1 p_1^{q_1 - 1} p_2^{q_2} + [(p_2 - 1)(q_2 - 1) - 1] p_1^{q_1} p_2^{q_2 - 1}. \tag{13}$$

Numerical examples: $\varphi(2^3) = 5, \varphi(2^4) = 17, \varphi(2^5) = 49, \varphi(6) = 2, \varphi(3^2) = 4, \varphi(3^3) = 28, \varphi(2^2 3) = 9, \varphi(2^2 3^2) = 49, \varphi(2^2 5) = 17, \varphi(5^2) = 16, \varphi(2^3 5) = 53, \varphi(42) = 44$, etc.

5. Another parametrization of unitary matrices

In the following we will present another parametrization of unitary matrices [12] in the form of a product of n diagonal matrices containing phases interlaced with $n - 1$ orthogonal matrices each generated by a real vector $v \in \mathbb{R}^n$. This new form will be more appropriate for design and implementation of the software packages necessary for solving equations (2) for arbitrary n.

It is easily seen that we can write any unitary matrix as a product of two diagonal matrices of the form $d_n = (\mathrm{e}^{\mathrm{i}\varphi_1}, \ldots, \mathrm{e}^{\mathrm{i}\varphi_n})$ with $\varphi_j \in [0, 2\pi)$, $j = 1, \ldots, n$, arbitrary phases and a unitary matrix with positive elements in the first row and the first column. We also make the notation $d_k^{n-k} = (1_{n-k}, \mathrm{e}^{\mathrm{i}\psi_1}, \ldots, \mathrm{e}^{\mathrm{i}\psi_k})$, $k < n$, where 1_{n-k} means that the first $(n-k)$ diagonal entries equal unity, i.e. it can be obtained from d_n by making the first $n - k$ phases equal zero. These diagonal phase matrices are the first building blocks in our construction. Other building blocks that will appear in the factorization of unitary matrices A_n are the two-dimensional rotations which operate in the $i, i + 1$-plane of the form

$$J_{i,i+1} = \begin{pmatrix} I_{i-1} & 0 & 0 \\ 0 & \cos\theta_i \quad -\sin\theta_i & 0 \\ 0 & \sin\theta_i \quad \cos\theta_i & \\ 0 & 0 & I_{n-i-1} \end{pmatrix} \qquad i = 1, \ldots, n-1. \tag{14}$$

The factorization idea comes from the well-known fact that $U(n)$ acts transitively on the n-dimensional complex sphere $\mathbf{S}_{2n-1} \in \mathbb{C}^n$, and explicitly from the coset relation

$$\mathbf{S}_{2n-1} = \text{coset space } U(n)/U(n-1).$$

A direct consequence of the last relation is that we expect that any element of $U(n)$ should be uniquely specified by a pair of a vector $v \in \mathbf{S}_{2n-1}$ and an arbitrary element of $U(n-1)$. Thus we are looking for a factorization of an arbitrary element $A_n \in U(n)$ in the form

$$A_n = B_n \cdot \begin{pmatrix} 1 & 0 \\ 0 & A_{n-1} \end{pmatrix}$$

where $B_n \in U(n)$ is a unitary matrix whose first column is uniquely defined by a vector $v \in \mathbf{S}_{2n-1}$, but otherwise arbitrary, and A_{n-1} is an arbitrary element of $U(n-1)$. Iterating the previous equation we arrive at the conclusion that an element of $U(n)$ can be written as a product of n unitary matrices

$$A_n = B_n \cdot B_{n-1}^1 \cdots B_1^{n-1}$$

where

$$B_{n-k}^k = \begin{pmatrix} I_k & 0 \\ 0 & B_{n-k} \end{pmatrix}$$

$B_k, k = 1, \ldots, n-1$, are $k \times k$ unitary matrices whose first columns are generated by vectors $b_k \in \mathbf{S}_{2k-1}$; for example B_1^{n-1} is the diagonal matrix $(1, \ldots, 1, \mathrm{e}^{\mathrm{i}\varphi_{n(n+1)}})$.

The still arbitrary columns of B_k will be chosen in such a way that we should obtain a simple form for the matrices B_k^{n-k}, and we require that B_k should be completely specified by the parameters entering the vector b_k and nothing else.

Thus it follows that $B_n(B_{n-k})$ can be written as

$$B_n = d_n \tilde{B}_n$$

where the first column of $\tilde{B}_n$ has non-negative entries.

Denoting this column by v_1 we will use the parametrization

$$v_1 = (\cos\theta_1, \cos\theta_2 \sin\theta_1, \ldots, \sin\theta_1 \cdots \sin\theta_{n-1})^t$$

where $\theta_i \in [0, \pi/2]$, $i = 1, \ldots, n-1$. Thus B_n will be parametrized by n phases and $n-1$ angles. According to the above factorization $\tilde{B}_n$ is nothing other than the orthogonal matrix generated by the vector v_1 and its form is given by lemma 2 with $n \to n+1$. Thus without loss of generality $B_n = d_n \mathcal{O}_n$ with $\mathcal{O}_n \in SO(n)$. In this way the factorization of A_n will be

$$A_n = d_n \mathcal{O}_n d_{n-1}^1 \mathcal{O}_{n-1}^1 \cdots d_2^{n-2} \mathcal{O}_2^{n-1} d_1^{n-1} I_n \tag{15}$$

where $\mathcal{O}_{n-k}^k$ has the same structure as B_{n-k}^k, i.e

$$\mathcal{O}_{n-k}^k = \begin{pmatrix} I_k & 0 \\ 0 & \mathcal{O}_{n-k} \end{pmatrix}$$

and $d_{n-k}^k = (1, \ldots, 1, \mathrm{e}^{\mathrm{i}\phi_1}, \ldots, \mathrm{e}^{\mathrm{i}\phi_{n-k}})$.

The orthogonal matrices $\mathcal{O}_n$ can be factored in terms of $J_{i,i+1}$ as follows:

Lemma 3. *The orthogonal matrices $\mathcal{O}_n$ $\left(\mathcal{O}_{n-k}^k\right)$ in their turn can be factored into a product of $n-1$ $(n-k-1)$ matrices of the form $J_{i,i+1}$; e.g. we have*

$$\mathcal{O}_n = J_{n-1,n} J_{n-2,n-1} \cdots J_{1,2}$$

where $J_{i,i+1}$ are $n \times n$ rotations introduced by equation (14).

In this way the parametrization of unitary matrices reduces to a product of simpler matrices: diagonal phase matrices and two-dimensional rotation matrices. For more details see [12]. Now we propose a disentanglement of the angles and phases entering each 'generation' and denote the angles by Latin letters, e.g., those that parametrize $\mathcal{O}_n$ will be denoted by $a_1, \ldots, a_{n-1}$, the angles that parametrize $\mathcal{O}_{n-1}^1$, by $b_1, \ldots, b_{n-2}$, etc, the last angle entering $\mathcal{O}_2^{n-1}$ by z_1. The phases will be denoted by Greek letters; e.g., the phases entering d_1 will be denoted by $\alpha_1, \ldots, \alpha_n$, those entering d_{n-1}^1 by $\beta_1, \ldots, \beta_{n-1}$, etc. The above factorization will be used in the next section for obtaining the equations for the moduli of the matrix elements.

6. Explicit equations of the moduli

Our choice for the orthogonal vectors in lemma 2 was such that the resulting matrix should have as many zero entries as possible. Thus $\mathcal{O}_n$ has $(n-1)(n-2)/2$ zeros in the right-upper corner and the entries of the Hadamard matrix will become more and more complicated when going from left to right and from top to bottom. We will start using the form (15) of the unitary

matrix and then $d_n \equiv I_n$. Since the first column has the form $a_{i1} = 1/\sqrt{n}$, $i = 1, \ldots, n$, and $d^1_{n-1} = (1, \mathrm{e}^{\mathrm{i}\alpha}, \mathrm{e}^{\mathrm{i}\alpha_1}, \ldots, \mathrm{e}^{\mathrm{i}\alpha_{n-2}})$ the product $\mathcal{O}_n d^1_{n-1}$ is

$$\begin{pmatrix}
\frac{1}{\sqrt{n}} & -\sqrt{\frac{n-1}{n}}\,\mathrm{e}^{\mathrm{i}\alpha} & 0 & 0 & \cdots & 0 & 0 \\
\frac{1}{\sqrt{n}} & \frac{\mathrm{e}^{\mathrm{i}\alpha}}{\sqrt{n(n-1)}} & -\sqrt{\frac{n-2}{n-1}}\,\mathrm{e}^{\mathrm{i}\alpha_1} & 0 & \cdots & 0 & 0 \\
\frac{1}{\sqrt{n}} & \frac{\mathrm{e}^{\mathrm{i}\alpha}}{\sqrt{n(n-1)}} & \frac{\mathrm{e}^{\mathrm{i}\alpha_1}}{\sqrt{(n-1)(n-2)}} & -\sqrt{\frac{n-3}{n-2}}\,\mathrm{e}^{\mathrm{i}\alpha_2} & \cdots & 0 & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\frac{1}{\sqrt{n}} & \frac{\mathrm{e}^{\mathrm{i}\alpha}}{\sqrt{n(n-1)}} & \frac{\mathrm{e}^{\mathrm{i}\alpha_1}}{\sqrt{(n-1)(n-2)}} & \frac{\mathrm{e}^{\mathrm{i}\alpha_2}}{\sqrt{(n-2)(n-3)}} & \cdots & \frac{\mathrm{e}^{\mathrm{i}\alpha_{n-3}}}{\sqrt{6}} & \frac{-\mathrm{e}^{\mathrm{i}\alpha_{n-2}}}{\sqrt{2}} \\
\frac{1}{\sqrt{n}} & \frac{\mathrm{e}^{\mathrm{i}\alpha}}{\sqrt{n(n-1)}} & \frac{\mathrm{e}^{\mathrm{i}\alpha_1}}{\sqrt{(n-1)(n-2)}} & \frac{\mathrm{e}^{\mathrm{i}\alpha_2}}{\sqrt{(n-2)(n-3)}} & \cdots & \frac{\mathrm{e}^{\mathrm{i}\alpha_{n-3}}}{\sqrt{6}} & \frac{\mathrm{e}^{\mathrm{i}\alpha_{n-2}}}{\sqrt{2}}
\end{pmatrix} \tag{16}$$

where α, α_i, $i = 1, \ldots, n-2$, are $n-1$ arbitrary phases.

The next building block $\mathcal{O}^1_{n-1} d^2_{n-2}$ will have the form

$$\begin{pmatrix}
1 & 0 & 0 & \cdot & 0 \\
0 & \cos a & -\sin a\,\mathrm{e}^{\mathrm{i}\beta} & \cdot & 0 \\
0 & \sin a \cos a_1 & \cos a \cos a_1\,\mathrm{e}^{\mathrm{i}\beta} & \cdot & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot \\
0 & \sin a \cdots \sin a_{n-3} & \cos a \sin a_1 \cdots \sin a_{n-3}\,\mathrm{e}^{\mathrm{i}\beta} & \cdot & \cos a_{n-3}\,\mathrm{e}^{\mathrm{i}\beta_{n-3}}
\end{pmatrix} \tag{17}$$

in terms of $n-2$ phases $\beta, \beta_1, \ldots, \beta_{n-3}$ and $n-2$ angles $a, a_1, \ldots, a_{n-3}$, and so on.

It is easy to see that the first two columns of the product of matrices (16) and (17) do not change when multiplied by $\mathcal{O}^2_{n-2} d^3_{n-3}$; however, the first row does. If the angles entering $\mathcal{O}^2_{n-2}$ are denoted by $b, b_1, \ldots, b_{n-4}$ and the phases are $\gamma, \gamma_1, \ldots, \gamma_{n-4}$, etc, then the entries of the first row are

$$a_{12} = -\sqrt{\frac{n-1}{n}}\cos a\,\mathrm{e}^{\mathrm{i}\alpha} \qquad a_{13} = \sqrt{\frac{n-1}{n}}\sin a \cos b\,\mathrm{e}^{\mathrm{i}(\alpha+\beta)} \qquad \cdots$$
$$a_{1n-1} = (-1)^{n-1}\sqrt{\frac{n-1}{n}}\sin a \sin b \cdots \cos z\,\mathrm{e}^{\mathrm{i}(\alpha+\beta+\cdots+\omega)}$$

where z and ω are the last angle and phase respectively. Since we use the standard form of the Hadamard matrices, i.e. the entries of the first row and of the first column are positive and equal $1/\sqrt{n}$, the above equations imply

$$\alpha = \beta = \cdots = \omega = \pi \qquad \cos a = \frac{1}{\sqrt{n-1}} \qquad \cos b = \frac{1}{\sqrt{n-2}} \quad \cdots \quad \cos z = \frac{1}{\sqrt{2}}.$$

We substitute the above values in equation (15) and find a complex $n \times n$ matrix depending on $(n-1)(n-2)/2$ phases $\alpha_1, \ldots, \alpha_{n-2}, \beta_1, \ldots, \psi_1$ and $(n-2)(n-3)/2$ angles $a_1, \ldots, a_{n-3}, b_1, \ldots, y_1$, i.e. $(n-2)^2$ parameters which have to be found by solving the corresponding equations given by the moduli. The first simplest entries of the unitary matrix

have the form

$$a_{22} = -\frac{1}{(n-1)\sqrt{n}} - \frac{n-2}{n-1}\cos a_1\, \mathrm{e}^{\mathrm{i}\alpha_1}, \ldots$$

$$a_{k2} = -\frac{1}{(n-1)\sqrt{n}} + \sqrt{\frac{n-2}{n-1}}\left(\frac{\cos a_1\, \mathrm{e}^{\mathrm{i}\alpha_1}}{\sqrt{(n-1)(n-2)}} + \cdots + \frac{\sin a_1 \cdots \cos a_{k-2}\, \mathrm{e}^{\mathrm{i}\alpha_{k-2}}}{\sqrt{(n-k+2)(n-k+1)}}\right.$$
$$\left. - \sqrt{\frac{n-k}{n-k+1}} \sin a_1 \cdots \sin a_{k-2} \cos a_{k-1}\, \mathrm{e}^{\mathrm{i}\alpha_{k-1}}\right) \qquad k = 3, \ldots, n-1 \tag{18}$$

$$a_{2k} = -\frac{1}{(n-1)\sqrt{n}} + \sqrt{\frac{n-2}{n-1}}\left(\frac{\cos a_1\, \mathrm{e}^{\mathrm{i}\alpha_1}}{\sqrt{(n-1)(n-2)}} - \frac{\sin a_1 \cos b_1\, \mathrm{e}^{\mathrm{i}(\alpha_1+\beta_1)}}{\sqrt{(n-2)(n-3)}} + \cdots\right.$$
$$\left. + (-1)^{k-1}\sqrt{\frac{n-k}{n-k+1}} \sin a_1 \sin b_1 \cdots \cos l(k)_1\, \mathrm{e}^{\mathrm{i}(\alpha_1+\beta_1+\cdots+\lambda(k)_1)}\right) \qquad \text{etc}$$

where $l(k)$ and $\lambda(k)$ denote the angle and phase corresponding to index k respectively and the signs in the last bracket alternate.

The matrix elements become more complicated when going from the upper left corner to the bottom right corner. The entries a_{22}, a_{32} and a_{23} lead, for example, to the following moduli equations:

$$(n-2)\cos^2 a_1 + \frac{2}{\sqrt{n}}\cos a_1 \cos\alpha_1 - 1 = 0$$

$$\sin a_1 \left((n-3)\sin a_1 \cos^2 a_2 \right.$$
$$\left. + 2\sqrt{\frac{n-3}{n-1}}\cos a_2 \left(\frac{\cos\alpha_2}{\sqrt{n}} - \cos a_1 \cos(\alpha_1 - \alpha_2)\right) - \sin a_1\right) = 0 \tag{19}$$

$$\sin a_1 \left((n-3)\sin a_1 \cos^2 b_1 \right.$$
$$\left. + 2\sqrt{\frac{n-3}{n-1}}\cos b_1 \left(-\frac{\cos(\alpha_1+\beta_1)}{\sqrt{n}} + \cos a_1 \cos\beta_1\right) - \sin a_1\right) = 0$$

and so on. The form of the last two equations was obtained after the elimination of the term containing $\cos a_1 \cos\alpha_1$ by using the first equation (19), i.e. we work in the ideal generated by the moduli equations. It is easily seen that the other equations contain as factors $\sin a_2, \ldots, \sin a_{n-2}, \sin b_1, \ldots,$ etc. Thus a particular solution can be obtained when

$$\sin a_1 = 0$$

which implies $a_1 = 0, \pi$, and from the first equation (19) we get

$$\cos\alpha_1 = \pm\frac{(n-3)\sqrt{n}}{2}.$$

It is easily seen that the above equation has solution only for $n = 2, 3, 4$; for $n \geqslant 5$ the factor $\sin a_1$ will be omitted from equations (19) because then $a_1 \neq 0, \pi$. When $n = 2$ we obtain $\alpha_1 = \pi/4$, so $a_{22} = -1/\sqrt{2}$. If $n = 3$, then $\alpha_1 = 3\pi/2$ and from the first equation (18) one gets

$$a_{22} = -\frac{1}{2\sqrt{3}} + \frac{\mathrm{i}}{2} = \frac{1}{\sqrt{3}}\,\mathrm{e}^{\frac{2\pi\mathrm{i}}{3}} \qquad \text{etc.}$$

The case $n = 4$ leads to $\alpha_1 = \pi$ which gives

$$a_{22} = -a_{23} = -a_{32} = \frac{1}{2} \qquad \text{and} \qquad a_{33} = -a_{34} = -\frac{\mathrm{e}^{\mathrm{i}(\alpha_2+\beta_1)}}{2}.$$

After the substitution $\alpha_2 + \beta_1 = t$ one finds the standard complex form of the 4×4 matrix found by Hadamard. To view the origin of the phase $\alpha_2 + \beta_1$ we have to look at the moduli equations. They have the form

$$\begin{aligned}
&2\cos^2 a_1 + \cos a_1 \cos\alpha_1 - 1 = 0\\
&\sin a_1(\cos\alpha_2 - 2\cos a_1 \cos(\alpha_1 - \alpha_2)) = 0\\
&\sin a_1(2\cos a_1 \cos\beta_1 - \cos(\alpha_1 + \beta_1)) = 0\\
&\cos 2a_1 \cos(\alpha_1 - \alpha_2)\cos\beta_1 + \cos a_1 \cos(\alpha_2 + \beta_1) + \sin(\alpha_1 - \alpha_2)\sin\beta_1 = 0
\end{aligned}$$

and we see that the above system splits into two cases. In the first case, when $\sin a_1 = 0$, the rank of the system is 2, which explains the above dependence of a_{33} on two phases, and in the second case when $\sin a_1 \neq 0$ the rank is 3 and the dependence is only on one arbitrary phase. However, in this case there is no final difference between the two cases. The solution of the above system is obtained directly but for $n \geqslant 5$ the problem is difficult and needs more powerful techniques. Particular solutions can be obtained rather easily, e.g., for $n = 6$ there is a matrix that has the property $a_{ij} = a_{ji}$:

$$\frac{1}{\sqrt{6}}\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1\\
1 & -1 & -1 & 1 & \mathrm{i} & -\mathrm{i}\\
1 & -1 & -\mathrm{i} & -1 & 1 & \mathrm{i}\\
1 & 1 & -1 & -\mathrm{i} & -1 & \mathrm{i}\\
1 & \mathrm{i} & 1 & -1 & -1 & -\mathrm{i}\\
1 & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -1
\end{pmatrix}.$$

There even exists a Hermitian matrix $S = S^*$

$$\frac{1}{\sqrt{6}}\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1\\
1 & -1 & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i}\\
1 & -\mathrm{i} & -1 & 1 & -1 & \mathrm{i}\\
1 & -\mathrm{i} & 1 & -1 & \mathrm{i} & -1\\
1 & \mathrm{i} & -1 & -\mathrm{i} & 1 & -1\\
1 & \mathrm{i} & -\mathrm{i} & -1 & -1 & 1
\end{pmatrix}$$

and so on. As we said before, getting the most general form of a solution is not a simple task; for $n = 6$ we have 16 complicated trigonometric equations to solve. Thus new approaches are necessary and in the next section we suggest such an approach, using methods from algebraic geometry.

7. Connection with algebraic geometry

Equations (19) can be transformed into polynomial equations by the known procedure

$$\sin a \to \frac{2x}{1+x^2} \qquad \cos a \to \frac{1-x^2}{1+x^2}$$

such that we get from (19)

$$p_1 = \left[\left(n-3+\frac{2}{\sqrt{n}}\right)x_1^4 - 2(n-1)x_1^2 + \left(n-3-\frac{2}{\sqrt{n}}\right)\right]y_1^2 + \left(n-3-\frac{2}{\sqrt{n}}\right)x_1^4 - 2(n-1)x_1^2 + \left(n-3+\frac{2}{\sqrt{n}}\right)$$

$$\begin{aligned} p_2 = {} & \left\{\left[-\left(1-\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 + \left(1+\frac{1}{\sqrt{n}}\right)\right]x_2^4 - C_2x_1x_2^2 + \left(1-\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 \right. \\ & \left. - \left(1+\frac{1}{\sqrt{n}}\right)\right\}y_1^2y_2^2 + \left\{\left[\left(1-\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 - \left(1+\frac{1}{\sqrt{n}}\right)\right]x_2^4 - C_2x_1x_2^2 \right. \\ & \left. - \left(1-\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 + \left(1+\frac{1}{\sqrt{n}}\right)\right\}y_1^2 + \left\{\left[\left(1+\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 \right. \right. \\ & \left. \left. - \left(1-\frac{1}{\sqrt{n}}\right)\right]x_2^4 - C_2x_1x_2^2 - \left(1+\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 + \left(1-\frac{1}{\sqrt{n}}\right)\right\}y_2^2 \\ & - 4\left(1-x_1^2\right)\left(1-x_2^4\right)y_1y_2 + \left[-\left(1+\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 + \left(1-\frac{1}{\sqrt{n}}\right)\right]x_2^4 \\ & - C_2x_1x_2^2 + \left(1+\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 - \left(1-\frac{1}{\sqrt{n}}\right) \end{aligned}$$

$$\begin{aligned} p_3 = {} & \left\{\left[-\left(1-\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 + \left(1+\frac{1}{\sqrt{n}}\right)\right]x_3^4 - C_2x_1x_3^2 + \left(1-\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 \right. \\ & \left. - \left(1+\frac{1}{\sqrt{n}}\right)\right\}y_1^2y_3^2 + \left\{\left[\left(1-\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 - \left(1+\frac{1}{\sqrt{n}}\right)\right]x_3^4 - C_2x_1x_3^2 \right. \\ & \left. - \left(1-\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 + \left(1+\frac{1}{\sqrt{n}}\right)\right\}y_1^2 + \left\{\left[-\left(1-\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 \right. \right. \\ & \left. \left. + \left(1-\frac{1}{\sqrt{n}}\right)\right]x_3^4 - C_2x_1x_3^2 + \left(1+\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 - \left(1-\frac{1}{\sqrt{n}}\right)\right\}y_3^2 \\ & - 4\left(1+x_1^2\right)\left(1-x_3^4\right)y_1y_2 + \left[\left(1+\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 - \left(1-\frac{1}{\sqrt{n}}\right)\right]x_3^4 \\ & - C_2x_1x_3^2 - \left(1+\frac{1}{\sqrt{n}}\right)x_1^2 + C_1x_1 + \left(1-\frac{1}{\sqrt{n}}\right) \end{aligned}$$

where

$$C_1 = \frac{(n-1)(n-4)}{\sqrt{(n-1)(n-3)}} \qquad C_2 = \frac{2(n-1)(n-2)}{\sqrt{(n-1)(n-3)}}$$

and the angles by the above transformation go to $x_1, x_2, x_3, \ldots$ and the phases to $y_1, y_2, y_3, \ldots$.

From the matrices such as (16) one sees that the full set of the $(n-2)^2$ equations contains square roots of almost all prime numbers $\leqslant n$ so that not all the coefficients are rational and we have to look for solutions in a field $\mathbf{Q}(\sqrt{d})$ for some $d \in \mathbb{N}$.

The polynomial equation $p_1 = 0$ defines an algebraic curve; however, the most studied are the elliptic and hyperelliptic curves, i.e. those defined by an equation of the form $y^2 = f_p(x)$, where $f_p(x)$ is a polynomial of degree p.

From $p_1 = 0$ we get

$$y_1^2 = -\frac{\left(n-3-\frac{2}{\sqrt{n}}\right)x_1^4 - 2(n-1)x_1^2 + \left(n-3+\frac{2}{\sqrt{n}}\right)}{\left(n-3+\frac{2}{\sqrt{n}}\right)x_1^4 - 2(n-1)x_1^2 + \left(n-3-\frac{2}{\sqrt{n}}\right)} = -\frac{P_1(x_1)}{P_2(x_1)}$$

which defines a meromorphic function. Its zeros and poles are simple,

$$\pm\sqrt{\frac{\sqrt{n}-1}{\sqrt{n}+1}} \qquad \pm\sqrt{\frac{n+\sqrt{n}-2}{n-\sqrt{n}-2}}$$

and

$$\pm\sqrt{\frac{\sqrt{n}+1}{\sqrt{n}-1}} \qquad \pm\sqrt{\frac{n-\sqrt{n}-2}{n+\sqrt{n}-2}}$$

and the poles and the zeros are interlaced. Thus apparently the above equation is not hyperelliptic. However, by the birational transformation

$$y_1 = \frac{Y_1}{P_2(x_1)}$$

we get the equation

$$Y_1^2 = -P_1(x_1)P_2(x_1)$$

which shows that the above curve has genus $g = 3$. For $n \geqslant 5$ the curve has no branch going to infinity since the highest power coefficient is negative and consequently the curve is made of three ovals.

The polynomials $p_1 = p_2 = 0$ define a surface, $p_1 = p_2 = p_3 = 0$ define a three-dimensional variety and so on. We consider that the study of these multi-dimensional varieties will be very interesting from the algebraic geometry point of view, and their parametrizations could reveal unknown properties that may lead to a better understanding of the rational varieties. As we saw in section 4 one can easily construct parametrizations of the Hadamard matrices depending on a number of free phases at least for a non-prime n. This means that the set of moduli equations has to be split into some subsets and for each such subset the solutions are in the k-dimensional torus $T^k = \underbrace{S^1 \otimes \cdots \otimes S^1}_{k \text{ factors}}$, where k is the number of arbitrary phases parametrizing the considered subset. But this could be equivalent to the existence of a rational parametrization for the equations defining this subset. Unfortunately the best-studied case and the best results are for algebraic curves; see [19], theorem 14, for a flavour of recent results. The study of surfaces, three-dimensional varieties, etc is at the beginning and until now the theory was developed only for the simplest varieties, the so-called rationally connected varieties [19]. From what we said before one may conclude that the parametrization of complex Hadamard matrices could be an interesting example of the parametrization of meromorphic varieties, which could be a mixing between a rational parametrization and a parametrization of hyperelliptic curves. Thus the theoretical instrument for the parametrization of complex Hadamard matrices seems to exist, the challenging problem being the transformation of the existing theorems into a symbolic manipulation software program able to find after a reasonable computing time explicit solutions at least for moderate values of n.

8. Conclusion

All the results obtained for complex Hadamard matrices can be used for the construction of *real* Hadamard matrices, the only supplementary constraint being the natural one $n = 4m$.

We believe that the Hadamard conjecture can be solved in our formalism since unlike the classical combinatorial approach we also have at our disposal $(n-1)(n-2)/2$ phases, and the problem is to guess the pattern of 0 and π taken by them.

Conversely many constructions from the theory of the real Hadamard matrices can be extended to the complex case. For example, a complex conference matrix will be a matrix with $a_{ii} = 0, i = 1, \ldots, n$, and $|a_{ij}| = 1/\sqrt{n}$ such that

$$W W^* = \frac{n-1}{n}.$$

It is not difficult to construct complex conference matrices; in fact it is a simpler problem than the construction of the complex Hadamard matrices because the equations $a_{ii} = 0$, $i = 2, \ldots, n-1$, imply the determination of $2(n-2)$ parameters which simplify the other equations.

We give a few examples:

$$W_4 = \frac{1}{2}\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & -\mathrm{e}^{\mathrm{i}t} & \mathrm{e}^{\mathrm{i}t} \\ 1 & \mathrm{e}^{\mathrm{i}t} & 0 & -\mathrm{e}^{\mathrm{i}t} \\ 1 & -\mathrm{e}^{\mathrm{i}t} & \mathrm{e}^{\mathrm{i}t} & 0 \end{pmatrix}$$

and

$$W_6 = \frac{1}{\sqrt{6}}\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & -\mathrm{e}^{\mathrm{i}\alpha} & -\mathrm{e}^{\mathrm{i}\alpha} & \mathrm{e}^{\mathrm{i}\alpha} & \mathrm{e}^{\mathrm{i}\alpha} \\ 1 & -\mathrm{e}^{\mathrm{i}\alpha} & 0 & \mathrm{e}^{\mathrm{i}\alpha} & -\mathrm{e}^{\mathrm{i}(\alpha-\beta)} & \mathrm{e}^{\mathrm{i}(\alpha-\beta)} \\ 1 & -\mathrm{e}^{\mathrm{i}\alpha} & \mathrm{e}^{\mathrm{i}\alpha} & 0 & \mathrm{e}^{\mathrm{i}(\alpha-\beta)} & -\mathrm{e}^{\mathrm{i}(\alpha-\beta)} \\ 1 & \mathrm{e}^{\mathrm{i}\alpha} & -\mathrm{e}^{\mathrm{i}(\alpha+\beta)} & \mathrm{e}^{\mathrm{i}(\alpha+\beta)} & 0 & -\mathrm{e}^{\mathrm{i}\alpha} \\ 1 & \mathrm{e}^{\mathrm{i}\alpha} & \mathrm{e}^{\mathrm{i}(\alpha+\beta)} & -\mathrm{e}^{\mathrm{i}(\alpha+\beta)} & -\mathrm{e}^{\mathrm{i}\alpha} & 0 \end{pmatrix}$$

where the second depends on two arbitrary phases. They are useful because if W_n is a complex conference matrix then

$$M_{2n} = \frac{1}{\sqrt{2}}\begin{pmatrix} W_n + \frac{I_n}{\sqrt{n}} & W_n^* - \frac{I_n}{\sqrt{n}} \\ W_n - \frac{I_n}{\sqrt{n}} & -W_n^* - \frac{I_n}{\sqrt{n}} \end{pmatrix}$$

is a complex Hadamard matrix of order $2n$.

In this paper we have used convenient parametrizations of unitary matrices that allowed us to get a set of $(n-2)^2$ polynomial equations whose solutions will give all the possible parametrizations for the Hadamard matrices. Unfortunately the system is very complicated and only particular solutions have been found; thus from a pragmatic point of view the most important issue would be the design of software packages for solving these equations.

Acknowledgments

I would like to thank the referees for several remarks of an expository nature that lead to an improvement of the manuscript. The work was completed while the author was a visitor at the Institute for Theoretical Physics, University of Bern in the frame of the Swiss National Science Foundation Program 'Scientific Co-operation between Eastern Europe and Switzerland (SCOPES 2000-2003)'. It is a pleasure for me to thank Professor H Leutwyller for many interesting discussions. Also I want to thank Professor J Gasser for the warm hospitality extended to me during my stay in Bern.

References

[1] Agaian A A 1985 *Hadamard Matrices and Their Applications (Lectures Notes in Mathematics* vol 1168*)* (Berlin: Springer)

[2] Auberson G 1989 On the reconstruction of a unitary matrix from its moduli. Existence of continuous ambiguities *Phys. Lett.* B **216** 167–71

[3] Auberson G, Martin A and Mennessier G 1991 On the reconstruction of a unitary matrix from its moduli *Commun. Math. Phys.* **140** 417–31

[4] Björck G 1985 Functions of modulus one on $\mathbf{Z_p}$ whose Fourier transforms have constant modulus *Coll. Math. Soc. János Bolyai* **49** 193–7

[5] Björck G and Fröberg R 1991 A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic *n*-roots *J. Symb. Comput.* **12** 329–36

[6] Björck G and Fröberg R 1994 Methods to 'divide-out' certain solutions from systems of algebraic equations, applied to find all cyclic 8-roots *Analysis, Algebra and Computers in Mathematical Research* (New York: Dekker) pp 57–70

[7] Björck G and Saffari B 1995 New classes of finite unimodular sequences with unimodular Fourier transform. Circulant Hadamard matrices with complex entries *C. R. Acad. Sci., Paris* **320** 319–24

[8] Bjorken J D and Dunietz I 1987 Rephasing invariant parameterisations of generalized Kobayashi–Maskawa matrices *Phys. Rev.* D **36** 2109–18

[9] Branco G C and Lavoura L 1988 Rephasing-invariant parameterisation of the quark matrix *Phys. Lett.* B **208** 123–30

[10] Diţă P 1982 Parametrisation of unitary matrices *J. Phys. A: Math. Gen.* **15** 3465–73

[11] Diţă P 1994 Parameterisation of unitary matrices by moduli of their elements *Commun. Math. Phys.* **159** 581–91

[12] Diţă P 2003 Factorization of unitary matrices *J. Phys. A: Math. Gen.* **36** 2781–9

[13] Goethals J M and Seidel J J 1967 Orthogonal matrices with zero diagonal *Can. J. Math.* **19** 1001–10

[14] Haagerup U 1996 Orthogonal maximal Abelian $*$-subalgebra ot the $n \times n$ matrices and cyclic n-roots *Operator Algebras and Quantum Field Theory (Rome)* (Cambridge, MA: International Press) pp 296–322

[15] Hadamard J 1893 Résolution d'une question rélative aux déterminants *Bull. Sci. Math.* **17** 240–6

[16] de la Harpe P and Jones V R F 1990 Paires de sous-algebres semi-simples et graphes fortement réguliers *C. R. Acad. Sci., Paris* **311** 147–50

[17] Jex I, Stenholm S and Zeilinger A 1995 Hamiltonian theory of a symmetric multiport *Opt. Commun.* **117** 95–1001

[18] Knill E 1996 Group representations, error bases and quantum codes, preliminary reports *Preprint* quant-ph/9608049

[19] Kollár J 2001 Which are the simplest algebraic varieties? *Bull. Am. Math. Soc.* **38** 409–33

[20] Munemasa A and Watatani Y 1992 Orhogonal pairs of $*$-subalgebras and association schemes *C. R. Acad. Sci., Paris* **314** 329–31

[21] Murnagham F D 1962 *The Unitary and Rotation Groups* (Washington, DC: Spartan Books)

[22] Sz-Nagy B and Foias C 1967 *Analyse Harmonique des Opérateurs de l'Espace de Hilbert* (Paris: Masson)

[23] Popa S 1983 Orthogonal pairs of $*$-subalgebras in finite von Neumann algebras *J. Operator Theory* **9** 253–68

[24] Reck M, Zeilinger A, Bernstein H J and Bertani P 1994 Experimental realization of any discrete unitary operator *Phys. Rev. Lett.* **73** 58–61

[25] Sylvester J J 1867 Thoughts on inverse orthogonal matrices, simultaneous sign-succesions, and tessellated pavements in two or more colors, with applications to Newton's rule, ornamental tile-work, and the theory of numbers *Phil. Mag.* **34** 461–75

[26] Törma P and Stenholm S 1995 Hamiltonian theory of symmetric optical network transformd *Phys. Rev.* A **52** 4853–60

[27] Vollbrecht K G H and Werner R F 2000 Why two qubits are special *J. Math. Phys.* **41** 6772–82

[28] Werner R F 2001 All teleportation and dense coding schemes *J. Phys. A: Math. Gen.* **34** 7081–94

[29] Werner R F 2003 Quantum information theory—an invitation *Quantum Information—an Introduction to the Basic Theoretical Concepts and Experiments (Springer Tracts in Modern Physics)* (Berlin: Springer)

[30] Williamson J 1944 Hadamard's determinant theorem and the sum of four squares *Duke Math. J.* **11** 65–81

[31] Życzkowski K, Kus M, Słomczyński W and Sommers H-J 2003 Random unistochastic matrices *J. Phys. A: Math. Gen.* **36** 3425–50