Discrete canonical transforms that are Hadamard matrices

2011 J. Phys. A: Math. Theor. 44 265302

(http://iopscience.iop.org/1751-8121/44/26/265302)

IOP Publishing Journal of Physics A: Mathematical and Theoretical

J. Phys. A: Math. Theor. **44** (2011) 265302 (10pp) doi:10.1088/1751-8113/44/26/265302

Discrete canonical transforms that are Hadamard matrices

John J Healy and Kurt Bernardo Wolf

Instituto de Ciencias Físicas, Universidad Nacional Autónoma de México, Av. Universidad s/n,
Cuernavaca, Morelos 62210, Mexico

E-mail: johnjhealy@gmail.com and bwolf@fis.unam.mx

Received 12 November 2010, in final form 4 May 2011
Published 1 June 2011
Online at stacks.iop.org/JPhysA/44/265302

Abstract

The group $\mathsf{Sp}(2, \Re)$ of symplectic linear canonical transformations has an integral kernel which has quadratic and linear phases, and which is realized by the geometric paraxial optical model. The discrete counterpart of this model is a finite Hamiltonian system that acts on N-point signals through $N \times N$ matrices whose elements also have a constant absolute value, although they do not form a representation of that group. Those matrices that are also unitary are Hadamard matrices. We investigate the manifolds of these $N \times N$ matrices under the $\mathsf{Sp}(2, \Re)$ equivalence imposed by the model, and find them to be on two-sided cosets. By means of an algorithm we determine representatives that lead to collections of mutually unbiased bases.

PACS numbers: 02.10.Ud, 02.10.Yn, 03.65.Wj

1. Introduction

One of the reasons to be interested in Hadamard matrices is because they define Weyl pairs of observables, where complete knowledge of one is paired with complete indeterminacy of the other. The classical example is provided by $\mathcal{F}$, the Fourier integral transform: under this, a function whose position is exactly determined —a Dirac $\delta(x - x_o)$— is transformed into a function of momentum $\sim \mathrm{e}^{-\mathrm{i}x_o p}$, whose probability is equally spread over the full real line $\Re$. This transform has a natural finite-dimensional counterpart $\mathbf{F}$, the discrete Fourier transform (DFT), represented by the $N \times N$ Fourier matrix $\mathbf{F} = \|F_{m,n}\|$, with elements

$$F_{m,n} = \frac{1}{\sqrt{N}} \exp\left(-\mathrm{i}\frac{2\pi mn}{N}\right), \tag{1}$$

where m, n range over the integers modulo N, namely $\{0, 1, \ldots, N-1\}$. Here also, every Kronecker δ_{m,m_o} is paired through the DFT matrix with a phase $\sim \mathrm{e}^{-2\pi\mathrm{i}\,m_o n/N}$; the former are orthogonal under the common sesquilinear inner product of N-vectors, and so are the latter because the matrix is unitary. All elements of the DFT matrix (1) have an absolute value

$1/\sqrt{N}$; such matrices are called complex Hadamard matrices. Originally, only real matrices were considered [1], and with this definition many interesting mathematical properties were found. Studies in quantum computation are using these matrices to characterize measurements that will yield complete knowledge of a quantum state [2, 3].

In this paper, we provide a source of Hadamard matrices based on a discretized model of plane paraxial geometric optics, where the group $\mathsf{Sp}(2, \Re)$ of 2×2 real symplectic matrices of linear canonical transforms (LCTs) is associated with a manifold of $N \times N$ matrices: the *discrete* LCTs (DLCTs). Although these matrices do not represent $\mathsf{Sp}(2, \Re)$ faithfully —all optical magnifiers are represented by the unit matrix—their elements are complex, have an absolute value $1/\sqrt{N}$ (exc. magnifiers) and are natural candidates to be Hadamard matrices. In section 2, we remind the reader of the role of LCTs in linear optical and quantum systems, and in section 3 of their discrete $N \times N$ matrix counterparts, where certain submanifolds are unitary and hence Hadamard matrices. Each of these matrices H represents an optical system which acts on N-point signals, transforming an input orthonormal basis $\{e_i\}_{i=1}^{N}$ into an output $\{f_i\}_{i=1}^{N}$, which is also an orthonormal basis, and said to be *mutually unbiased* with respect to the first, because their $\mathcal{C}^N$ inner product $H_{i,j} := (e_i, f_j)$ is such that $|H_{i,j}| = 1/\sqrt{N}$. One of the issues in quantum tomography is to find maximal sets of such mutually unbiased bases (MUBs), modulo equivalences of phase and row permutation.

The model of paraxial optics limits the equivalence between Hadamard matrices [4] to those that can be achieved with (discrete counterparts of) lenses and free flights that carry quadratic phase transformations. Thus, permutations of the rows and columns of the $N \times N$ matrices cannot be realized. Considering equivalence within $\mathsf{Sp}(2, \Re)$, we characterize the submanifolds of Hadamard matrices as two-sided cosets in section 4. We have privileged the group-theoretical context of linear systems that could harbor possible optical or quantum-mechanical realizations, as well as an associated fast computer algorithm [5, 6]. In section 5, we determine the parametric form of collections of Hadamard matrices $\{H_i\}_{i=1}^{k}$, such that $H_i^{\dagger} H_j$ is equivalent to a matrix in the same linear space; also, we provide an algorithm to find sets of such partners, which yields collections of MUBs for any dimension N, although we claim completeness (i.e. a collection of size N) only for the case of N odd prime. We are aware of the copious literature searching for complete sets of Hadamard matrices for composite N (in particular $N = 6$), but we regard this problem to be outside our present concerns. In section 6, we relate the DLCT Hadamard matrices with the quadratic DFTs introduced by Kibler [7, 8], and with a form of discrete fractional Fourier matrices. We add some comments in section 7.

2. Linear canonical integral transforms

LCTs in a two-dimensional phase space $(x, p) \in \Re^2$ are determined by the 2×2 real matrices $\mathbf{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ that are symplectic; in the 2×2 case this condition reduces to $\det \mathbf{M} = ad - bc = 1$. These were first investigated by Moshinsky and Quesne [9] in the context of quantum mechanics and by Collins [10] in paraxial optics; they provide a two-fold cover of the symplectic group $\mathsf{Sp}(2, \Re)$ realized by unitary integral transforms on the Hilbert space $\mathcal{L}^2(\Re)$ of the Lebesgue square-integrable functions space. Their integral kernel, with a stringent specification of phase, is

$$(\mathcal{C}_M f)(x) = \int_{\Re} \mathrm{d}x' C_M(x, x') f(x'), \tag{2}$$

$$C_M(x, x') = K_M \exp\left(\mathrm{i}\frac{\mathrm{d}x^2 - 2xx' + ax'^2}{2b}\right) = C_{M^{-1}}(x', x)^*, \tag{3}$$

$$K_M := \frac{1}{\sqrt{2\pi \mathrm{i} b}} := \frac{\mathrm{e}^{-\mathrm{i}\pi/4} \exp\big(-\mathrm{i}\frac{1}{2}\arg b\big)}{\sqrt{2\pi |b|}}. \tag{4}$$

In the submanifold $b = 0$ they limit to a Dirac distribution:

$$C_M(x, x') = \delta(x - x'/a)\frac{1}{\sqrt{a}} \exp\left(\mathrm{i}\frac{cx^2}{2a}\right), \tag{5}$$

and thus $\mathcal{C}_1 = \mathit{1}$ is the $\mathsf{Sp}(2, \Re)$ group unit.

The product of two canonical transforms follows that of the $\mathsf{Sp}(2, \Re)$ matrices (up to a sign as we explain below):

$$\mathcal{C}_{M_1}\mathcal{C}_{M_2} = \pm\mathcal{C}_{M_1 M_2}. \tag{6}$$

The LCT contains the Fourier transform $\mathcal{F} = \mathrm{e}^{\mathrm{i}\pi/4}\mathcal{C}_\Phi$, corresponding to the matrix $\mathbf{\Phi} := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Indeed, it provides its fractional powers as a one-parameter subgroup:

$$\mathcal{F}^\nu = \mathrm{e}^{\mathrm{i}\pi\nu/4}\mathcal{C}_{\mathbf{\Phi}^\nu}, \qquad \mathbf{\Phi}^\nu := \begin{pmatrix} \cos\frac{1}{2}\pi\nu & \sin\frac{1}{2}\pi\nu \\ -\sin\frac{1}{2}\pi\nu & \cos\frac{1}{2}\pi\nu \end{pmatrix}, \tag{7}$$

with ν mod 4. The two-fold cover of LCTs over the $\mathsf{Sp}(2, \Re)$ matrices can be seen here: since $\mathcal{F}^4 = \mathit{1}$, the phase $\mathrm{i}\frac{1}{4}\pi\nu$ shows that the fourth power of the LCT operator is $\mathcal{C}_\Phi^4 = -\mathit{1}$. Due to the square root, the LCT realization covers the fractional Fourier subgroup twice, bearing the onus of the sign in (6). See [11, chapter 9] and [12, sections 9.4 and C.2].

LCT transforms act on the classical and quantum-mechanical Schrödinger operators of position $\mathcal{X}$ [$\mathcal{X} f(x) = x\, f(x)$] and momentum $\mathcal{P}$ [$\mathcal{P} f(x) = -\mathrm{i}\, \mathrm{d} f(x)/\mathrm{d}x$]:

$$\mathcal{C}_M \begin{pmatrix} \mathcal{X} \\ \mathcal{P} \end{pmatrix} \mathcal{C}_M^{-1} = \mathbf{M}^{-1} \begin{pmatrix} \mathcal{X} \\ \mathcal{P} \end{pmatrix}. \tag{8}$$

The inverse of the matrix on the right ensures that the LCT product (6) is in the correct order. Paraxial optics provides an attractive interpretation of various basic one-parameter subgroups of LCTs [13], that we quote as follows:

$$\left.\begin{array}{r}\text{Free propagation by} \\ \text{distance or time}\end{array}\right\} z \geqslant 0, \qquad \mathcal{C}^{\text{Fr}}(z) = \mathcal{C}\begin{pmatrix} 1 & -z \\ 0 & 1 \end{pmatrix}, \tag{9}$$

$$\left.\begin{array}{r}\text{Lens of Gaussian power} \\ x^2\text{-potential jolt of strength}\end{array}\right\} g, \qquad \mathcal{C}^{\text{L}}(g) = \mathcal{C}\begin{pmatrix} 1 & 0 \\ g & 1 \end{pmatrix}, \tag{10}$$

$$\text{Magnifier by the factor } \mu, \qquad \mathcal{C}^{\text{M}}(\mu) = \mathcal{C}\begin{pmatrix} \mu & 0 \\ 0 & 1/\mu \end{pmatrix}, \tag{11}$$

$$\left.\begin{array}{r}\text{Waveguide evolution} \\ \text{harmonic oscillator}\end{array}\right\} \text{by } z \geqslant 0, \qquad \mathcal{C}^{\text{wav}}(z) = \mathrm{e}^{-\mathrm{i}\pi z/4}\mathcal{F}^{-z}. \tag{12}$$

Out of the products of elements in the first two subgroups, one can recover the full $\mathsf{Sp}(2, \Re)$, while the last three provide its modified Iwasawa decomposition [12, section 9.5].

3. Discrete LCTs

In models where measurements are made through a linear array of N sensors, the LCT integral kernel is replaced by an $N \times N$ matrix that must be invertible if no loss of information is desired, and unitary if we demand that orthogonal signal bases remain orthogonal. Generally, they are called DLCTs.

Consider a field $f(x)$ sensed at an input screen (or initial time) $z = 0$; after having passed through a system characterized by the 2×2 symplectic matrix $\mathbf{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathsf{Sp}(2, \Re)$, $ad - bc = 1$, the output field is $(\mathcal{C}_M f)(x)$. When the field is sensed at N points placed at $x_m \equiv m$ integers, the input signal is represented by the N-vector $\mathbf{f}^{\text{in}} = \left\{f_m^{\text{in}}\right\}_{m=1}^{N}$ and the output by $\mathbf{f}^{\text{out}} = \left\{f_m^{\text{out}}\right\}_{m=1}^{N}$ multiplied with the $N \times N$ matrix $\mathbf{W}(\mathbf{M})$ given by

$$\mathbf{f}^{\text{out}} = \mathbf{W}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\mathbf{f}^{\text{in}}, \tag{13}$$

which depends on three independent parameters of the group $\mathsf{Sp}(2, \Re)$. The discretization of the LCT integral kernel (2)–(5) that we adopt follows [6]. These DLCT matrices $\mathbf{W}(\mathbf{M}; N) \equiv \mathbf{W}(\mathbf{M}) \equiv \mathbf{W}_{\mathrm{M}}$ have elements

$$W\begin{pmatrix} a & b \\ c & d \end{pmatrix}_{m,n} := \frac{1}{\sqrt{N}} \exp\left(\frac{\mathrm{i}\pi}{bN}(am^2 - 2mn + dn^2)\right), \tag{14}$$

all of whose absolute values are $1/\sqrt{N}$ —except for $b = 0$, where we adopt

$$W\begin{pmatrix} a & 0 \\ c & 1/a \end{pmatrix}_{m,n} := \delta_{m,n} \exp(\mathrm{i}\pi c n^2/aN). \tag{15}$$

Because the elements are generally not periodic modulo N, we count rows and columns by the integers $m, n \in \{1, 2, \ldots, N\}$.

To compute the matrices $\mathbf{W}(\mathbf{M})$ efficiently, most often the 2×2 matrix $\mathbf{M}$ is decomposed into a product of lower-triangular matrices, whose $\mathbf{W}$'s are diagonal, and the Fourier factor $\mathbf{\Phi} := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, whose DLCT is $\mathbf{W}(\mathbf{\Phi}) = \mathbf{F}$. For the latter, the fast Fourier transform (FFT) algorithm is available to radically reduce the complexity of the computation. This process has been studied extensively in [14–17]. Alternatively, one may decompose $\mathbf{W}(\mathbf{M})$ in a fashion comparable to the FFT [5, 6].

Although for $b \neq 0$ the absolute value of all elements (14) is $1/\sqrt{N}$, not all DLCT matrices are unitary. Unitarity is important for us, so we determine that for which $\mathbf{M}$'s $\mathbf{W}_M^\dagger \mathbf{W}_M = \mathbf{1}$ holds. The matrix elements of this product are

$$\begin{aligned}\left(\mathbf{W}_M^\dagger \mathbf{W}_M\right)_{k,n} &= \frac{1}{N} \sum_{m=1}^{N} \exp\left(\frac{\mathrm{i}\pi}{bN}(2km - dk^2 - 2mn + dn^2)\right) \\ &= \frac{1}{N} \exp\left(\frac{\mathrm{i}\pi d}{bN}(n^2 - k^2)\right) \sum_{m=1}^{N} \exp\left(\frac{-2\mathrm{i}\pi}{bN} m(k-n)\right).\end{aligned} \tag{16}$$

The $\mathbf{W}_M$'s will thus be unitary when the sum over m in (16) yields $N\delta_{k,n}$. This occurs when the summands form a 'balanced' set of points in the complex plane (we say a set of point masses on a circle is balanced when their center of mass is at the center of the circle). This happens when $1/bN$ is a fraction $1/N,\ 2/N,\ \ldots,\ (N-1)/N$, excepting those where $1/bN = 1/N'$ for the integer N' that is a divisor of N—because then the summands would be periodic in $k-n$ mod $N' = N/N_o$ for some other integer N_o, the matrix would then contain two equal columns, and thence $\det \mathbf{W}_{\mathrm{M}} = 0$. We thus conclude that the DLCT matrices $\mathbf{W}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ are unitary when

$$b = 1/B, \quad B \text{ integer mod } N, \quad \gcd(B, N) = 1, \tag{17}$$

i.e., it is sufficient that the b-parameter be the inverse of an integer B relatively prime to N. For low dimensions we thus have

$$\begin{array}{rll} N=3, & B\in\ \{1,2\}, & \text{total:}\ \ 2\\ 4, & \{1,3\}, & 2\\ 5, & \{1,2,3,4\}, & 4\\ 6, & \{1,5\}, & 2\\ 7, & \{1,2,3,4,5,6\}, & 6\\ 8, & \{1,3,5,7\}, & 4\\ 9, & \{1,2,4,5,7,8\}, & 6\\ 10, & \{1,3,7,9\}, & 4. \end{array} \tag{18}$$

For N prime there will be $N-1$ acceptable values of B.

Which of the group properties of LCTs, action (8) and multiplication (6), are inherited by the $N\times N$ DLCTs? Evidently the unit is $\mathbf{W}(\mathbf{1})=\mathbf{1}$ from (15) and, provided (17) holds, the explicit form (14)–(15) of the unitary $N\times N$ $\mathbf{W}$-matrices also respects Hermitian inversion:

$$\mathbf{W}\left(\begin{pmatrix} a & b\\ c & d\end{pmatrix}^{-1}\right)=\left(\mathbf{W}\begin{pmatrix} a & b\\ c & d\end{pmatrix}\right)^{\dagger}=\mathbf{W}\begin{pmatrix} d & -b\\ -c & a\end{pmatrix}. \tag{19}$$

On the other hand, *unlike* (6), the unitary $\mathbf{W}(\mathbf{M})$ matrices do not form a group. A well-known theorem states that a noncompact Lie group, such as $\mathsf{Sp}(2,\Re)$, *cannot* be represented faithfully by finite unitary matrices [18]. So we note that due to (15), all diagonal $\mathsf{Sp}(2,\Re)$ matrices are represented by the $N\times N$ unit matrix, $\mathbf{W}\left(\begin{smallmatrix} a & 0\\ 0 & 1/a\end{smallmatrix}\right)=\mathbf{1}$; there are no DLCT magnifiers. We also note that lower-triangular $\mathsf{Sp}(2,\Re)$ matrices correspond to diagonal $N\times N$ matrices $\mathbf{W}\left(\begin{smallmatrix} a & 0\\ c & 1/a\end{smallmatrix}\right)=\mathbf{W}\left(\begin{smallmatrix} 1 & 0\\ c/a & 1\end{smallmatrix}\right)$ with quadratic phases $\sim\exp(\mathrm{i}cm^2/a)$. These represent thin lenses of Gaussian power c/a. And generally $\mathbf{W}(\mathbf{M_1})\,\mathbf{W}(\mathbf{M_2})\neq\mathbf{W}(\mathbf{M}_2\mathbf{M}_1)$. (The inversion of the order of the factors is due to (8) and (13).)

4. DLCT matrices that are Hadamard

In the current literature, an $N\times N$ matrix $\mathbf{H}=\|H_{m,n}\|$ is called complex Hadamard when it is unitary and all its elements have the same absolute value $|H_{m,n}|=1/\sqrt{N}$. Thus, all unitary DLCT matrices that satisfy (17) are Hadamard matrices. Commonly, two Hadamard matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ are said to be equivalent if there exist two diagonal phase matrices $\mathbf{D}_A$, $\mathbf{D}_B$ and two permutation matrices $\mathbf{P}_A$, $\mathbf{P}_B$ such that [4]

$$\mathbf{H}_2=\mathbf{P}_A\mathbf{D}_A\mathbf{H}_1\mathbf{D}_B\mathbf{P}_B. \tag{20}$$

Since we are interested in the realization of Hadamard transformations by $\mathsf{Sp}(2,\Re)$ homogeneous linear systems, we cautioned above that diagonal DLCT matrices can only bear quadratic phases $\mathrm{e}^{\mathrm{i}m^2\gamma}\delta_{m,n}$ (corresponding to thin lenses or $\sim x^2$ potential jolts) at the input and output z-planes, we exclude *linear* phase matrices $\mathrm{e}^{\mathrm{i}m\alpha}\delta_{m,n}$ (corresponding to misalignments or prisms, or free-fall $\sim x$ potential jolts). Permutation matrices must also be excluded because they do not correspond to any paraxial optical or quantum setup (except in Talbot optics, where an N-cycle permutation can be corresponded with translations of the cyclic position coordinate [19]). We note that the DLCT matrices are all equivalent to the Fourier matrix using the normal definition of equivalence.

The Hadamard equivalence (20) will thus be reduced and characterized as an equivalence between $\mathsf{Sp}(2,\Re)$ 2×2 matrices. Consider elements of the subgroup (10) placed at the input and output planes:

$$\mathbf{L}(\gamma)=\begin{pmatrix} 1 & 0\\ \gamma & 1\end{pmatrix}\in\mathsf{L},\qquad \gamma\in\Re, \tag{21}$$

and the equivalence relation that determines its *two-sided cosets* [18] within $\mathsf{Sp}(2, \mathfrak{R})$:

$$\mathbf{M}' \equiv \mathbf{L}(\gamma)\mathbf{M}\mathbf{L}(\gamma'), \qquad \gamma, \gamma' \in \mathfrak{R}. \tag{22}$$

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \gamma' & 1 \end{pmatrix} \tag{23}$$

$$= \begin{pmatrix} a + b\gamma' & b \\ c+\gamma a+d\gamma'+\gamma b\gamma' & \gamma b + d \end{pmatrix}. \tag{24}$$

From (24) we see that each value of $b \in \mathfrak{R}$ determines one two-sided coset in $\mathsf{L}\backslash\mathsf{Sp}(2, \mathfrak{R})/\mathsf{L}$, whose union is $\mathsf{Sp}(2, \mathfrak{R})$, and whose intersection is null—since they are disjoint equivalence classes. The manifold of each two-sided coset is two dimensional and can be parametrized by $(\gamma, \gamma') \in \mathfrak{R}^2$. When $b = 1/B$ satisfies the unitarity condition (17), with B integer and relatively prime to N, all $\mathbf{W}(\mathbf{M}(b))$'s in that (γ, γ') plane are equivalent Hadamard matrices. When in (22)–(24) we fix $\gamma' = 0$, the matrices $\left(\begin{smallmatrix} a & b \\ c+\gamma a & \gamma b+d \end{smallmatrix}\right)$, $\gamma \in \mathfrak{R}$, will form *left* cosets $\mathsf{L}\backslash\mathsf{Sp}(2, \mathfrak{R})$, which are lines parametrized by γ, and each left coset is characterized by two parameters, $(a, b) \in \mathfrak{R}^2 - \{0, 0\}$. On the line of each left coset we can choose a matrix to be *representative* of that coset. In particular, we set $\gamma = -d/b$ $(b \neq 0)$ and regard the unitary matrices

$$\mathbf{M}(a, b) := \begin{pmatrix} a & b \\ -1/b & 0 \end{pmatrix}, \quad \begin{matrix} a \in \mathfrak{R}, \\ b \in (17). \end{matrix} \tag{25}$$

$$W(\mathbf{M}(a, b))_{m,n} = \frac{1}{\sqrt{N}} \exp\left(\mathrm{i}\pi \frac{am^2 - 2mn}{bN}\right). \tag{26}$$

Their manifold is the set of lines $a \in \mathfrak{R}$, $b = 1/B$, $\gcd(B, N) = 1$. (A similar construction can be made for *right* cosets $\mathsf{Sp}(2, \mathfrak{R})/\mathsf{L}$ by setting $\gamma = 0$, and using (b, d) to characterize each right coset.)

5. Mutually unbiased bases of DLCTs

The definition of a collection of MUBs of Hadamard matrices is the following [20]. If $\mathcal{H}$ is the set of $N \times N$ Hadamard matrices, a collection of k MUBs $\{\mathbf{H}_i\}_{i=1}^k \in \mathcal{H}$ is such that their 'Hadamard' product remains within $\mathcal{H}$, i.e.

$$\frac{1}{\sqrt{N}} \mathbf{H}_i^\dagger \mathbf{H}_{i'} \in \mathcal{H}. \tag{27}$$

We proceed to show that the sets of left coset representative matrices (26) contain collections of MUBs. We look for conditions on the parameter a that allow for (27) to hold; denoting by $\mathbf{M}_1$ and $\mathbf{M}_2$ two matrices of the form (25), we compute the Hadamard product of their corresponding DLCT matrices (with $B_i = 1/b_i$):

$$\mathbf{H}^{(1,2)} := \mathbf{W}(\mathbf{M}_1)^\dagger \mathbf{W}(\mathbf{M}_2), \tag{28}$$

$$H_{k,n}^{(1,2)} = \frac{1}{N} \sum_{m=0}^{N-1} \exp \frac{\mathrm{i}\pi}{N} \left[\left(\frac{a_2}{b_2} - \frac{a_1}{b_1} \right) m^2 + 2 \left(\frac{k}{b_1} - \frac{n}{b_2} \right) m \right] \tag{29}$$

$$= G\!\left(\frac{1}{2} \left(\frac{a_2}{b_2} - \frac{a_1}{b_1} \right), \left(\frac{k}{b_1} - \frac{n}{b_2} \right), N \right) \tag{30}$$

$$= \frac{1}{\sqrt{N}} \varepsilon_N \, \mathrm{e}^{\mathrm{i}\varphi} J\left(\frac{1}{2}(a_2 B_2 - a_1 B_1)\middle| N\right). \tag{31}$$

In (30), $G(\alpha, \beta, N)$ is the generalized quadratic Gauss sum [21]; $J(\alpha \mid N)$ in (31) is the Jacobi symbol [22], which is defined for integer arguments α only, and when N is odd and relatively prime to $\alpha \neq 0$, it is a sign. And finally, ε_N is a sign and $\exp \mathrm{i}\varphi(a, b)$ is also a phase; these we also disregard because we are interested in the absolute value $\left|H^{(1,2)}_{k,n}\right|$. We thus conclude that

$$\mathbf{W}(\mathbf{M}(a_1, 1/B_1))^{\dagger}\mathbf{W}(\mathbf{M}(a_2, 1/B_2)) \in \mathcal{H} \tag{32}$$

when $\frac{1}{2}(a_2 B_2 - a_1 B_1)$ is an integer not congruent to 0 mod N.

We proceed to show how many collections of N MUBs exist for $N \times N$ DLCT matrices of the form (25) and (26). For prime N, the following algorithm will generate a random collection of N MUBs from the space of all possible collections of this type.

(1) Select a real number $0 \leqslant a_o < 2$.

(2) Enumerate the sets of points (a, B), with a mod $2N$ so $0 \leqslant a < 2N$, and $B \in \{1, 2, \ldots, N-1\}$ with $\gcd(B, N) = 1$, such that $aB = a_o + 2n$ mod $2N$, for $n \in \{0, 1, 2, \ldots, N-1\}$. When N is prime, these points will be

$$\begin{array}{llll} (a_o+2n, 1), & & & \\ \left(\frac{a_o+2n}{2}, 2\right), & \left(\frac{a_o+2n+2N}{2}, 2\right), & & \\ \left(\frac{a_o+2n}{3}, 3\right), & \left(\frac{a_o+2n+2N}{3}, 3\right), & \left(\frac{a_o+2n+4N}{3}, 3\right), & \\ \vdots & \vdots & \ddots & \\ \left(\frac{a_o+2n}{N-1}, N-1\right), & \left(\frac{a_o+2n+2N}{N-1}, N-1\right), \ldots, & \left(\frac{a_o+2n+2(N-2)N}{N-1}, N-1\right). & \end{array} \tag{33}$$

(3) Randomly choose N points—one from each column—such that the N values aB are distinct, i.e. one point for each choice of n. These N points (a, B) yield a collection of MUBs of $N \times N$ matrices $\mathbf{W}(\mathbf{M}(a, 1/B)) \in \mathcal{H}$.

We now prove that the algorithm given above always generates a collection of MUBs. From equation (32), we know that two DLCT Hadamard matrices, $\mathbf{M}_1(a, b)$ and $\mathbf{M}_2(a, b)$, multiply to produce a third Hadamard matrix, $\mathbf{M}_3(a, b)$, if and only if $a_2 B_2 - a_1 B_1 = 2n$, where n is an integer and $2n$ is not congruent to zero modulo $2N$. Any two points in (33) have $a_1 B_1 = a_o + 2p_1$ mod $2N$ and $a_2 B_2 = a_o + 2p_2$ mod $2N$, for the integers p_1 and p_2, $p_2 \neq p_1$. Thus, $a_2 B_2 - a_1 B_1 = 2(p_2 - p_1)$ mod $2N$. As $p_2 \neq p_1$, $0 \leqslant p_2, p_1 < N$, and $-2N < p_2 - p_1 < 2N$, so $2(p_2 - p_1)$ is not congruent with zero modulo $2N$.

The choice of a_o selects from a continuum, and each choice is unique. Changing a_o simply shifts the points in the a-direction modulo $2N$ (accounting for some wrapping effects). Hence there are infinitely many collections of MUBs. For a given a_o we can calculate how many such collections exist: for N prime, step 2 generates N sets of $1 + 2 + 3 + \cdots + N-1 = \frac{1}{2}(N-1)N$ Hadamard matrices. Every combination of one of these elements from each set is a collection of MUBs, giving a total of $(\frac{1}{2}(N-1)N)^N$ for each choice of a_o. In figure 1 we show the points generated by choosing $a_o = 1$ and $N = 5$.

We note that the algorithm is constrained to the case of N odd prime. As collections of MUBs for non-primes are of interest in the literature, we will comment briefly on them. Modifications are possible for non-prime N; however, these produce fewer points than the prime cases. For example, if $N = p^m$, with p an odd prime and m integer, the algorithm works

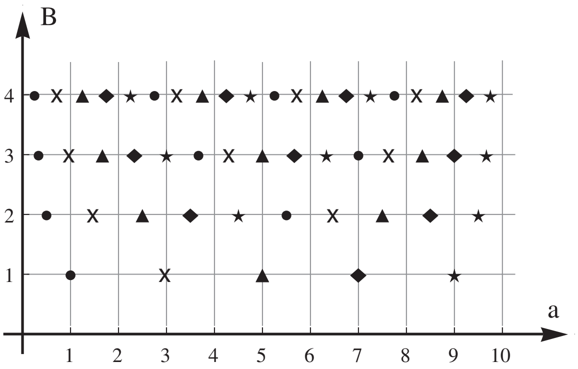

Figure 1. The (a, B) plane of $N \times N$ Hadamard DLCT matrices $\mathbf{W}(\mathbf{M}(a, 1/B))$ for $N = 5$ and $B = 1/b \in \{1, 2, 3, 4\}$. We arbitrarily select $a_o = 1$; then our algorithm produces, for $n \in \{0, 1, 2, 3, 4\}$, the points where $aB \equiv 1 \bmod 10$ (•), $aB \equiv 3 \bmod 10$ (×), $aB \equiv 5 \bmod 10$ (△), $aB \equiv 7 \bmod 10$ (◇), and $aB \equiv 9 \bmod 10$ (⋆). Any combination of one of these five types of points constitutes a collection of MUBs.

as for primes except for the points where n is of the form $(1 + 2qp)$, for the positive integer q. For example, for $N = 9$, $a_0 = 1$, the points (1,1), (3,1), (5,1), (9,1), (11, 1), (15, 1), (17, 1), form a collection of seven MUBs. For such non-prime N's our algorithm produces collections of fewer than N MUBs, though not necessarily much fewer. We note that algorithms are known which produce larger collections of MUBs for this case. Finally, it must be said that the 2×2 matrices $\mathbf{M}(a, 1/B)$ do not show any recognizable group properties yet.

6. Quadratic and fractional Fourier matrices

In [7, 8] Kibler introduced the quadratic Fourier transform matrices

$$(\mathbf{F}^{r,s})_{m,n} = \frac{1}{\sqrt{N}} \exp\left[\frac{\mathrm{i}\pi}{N}\big(m(N-m)s + m[2n-(N-1)r] + \tfrac{1}{2}(N-1)^2 r\big)\right], \tag{34}$$

for $r \in \Re$ and $s \in \{0, 1, \ldots, N-1\}$; the case $r = 0 = s$ corresponds to the DFT matrix (1). We can relate (34) with the DLCT matrices modulo phase factors:

$$(\mathbf{F}^{r,s})_{m,n} = \exp\left[\mathrm{i}\pi\frac{1}{2}\left(N - 2 + \frac{1}{N}\right) r\right] \exp\left[\mathrm{i}\pi m\left(s - \left[1 - \frac{1}{N}\right] r\right)\right] W\begin{pmatrix} s & -1 \\ 1 & 0 \end{pmatrix}_{m,n}. \tag{35}$$

The first and second factors are a constant and a linear phase. According to the stronger equivalence relation (20), the Hadamard matrices (34) are thus equivalent to the DLCT MUBs $\mathbf{W}\left(\begin{smallmatrix} a_n & -1 \\ 1 & 0 \end{smallmatrix}\right)$ given above.

The $N \times N$ DFT matrix (1) is considered to be the prototype of a Hadamard matrix. In the $\mathsf{Sp}(2, \Re)$ group of continuous LCTs, its fractionalization is $\mathcal{F}^\nu = \mathrm{e}^{\mathrm{i}\pi\nu/4}\mathcal{C}(\mathbf{\Phi}^\nu)$, with the matrix (7) and ν mod 4. From what we saw above, the corresponding DLCT matrices $\mathbf{W}(\mathbf{\Phi}^\nu)$ in (14) will be unitary, and hence Hadamard matrices when (17) holds, namely for powers

$$\nu = \frac{2}{\pi} \arcsin \frac{1}{B}, \qquad B \in \{1, 2, \ldots N-1\}, \qquad \gcd(B, N) = 1. \tag{36}$$

Yet, these $N \times N$ matrices do not satisfy condition (32) so they do not lead to a collection of MUBs, nor do they form a discrete subgroup of $\mathsf{Sp}(2, \Re)$.

7. Concluding remarks

Motivated by the possibility of physical realization through optical or quantum mechanical systems, we have shown that certain discrete, N-point linear canonical transformations are represented by Hadamard matrices. The equivalence criterion for these matrices had to be correspondingly strengthened due to the impossibility of producing row and column permutations, or impressing arbitrary phases with such systems. In this context we have provided an algorithm to find Hadamard matrices that form maximal collections of MUBs for N prime. We do not assert to have found maximal collections of MUBs Hadamard matrices for non-odd-prime dimensions, nor to have resolved any of the long-standing problems related to these matrices that are found in the mathematical literature.

For the continuum limit $N \to \infty$, the integer sensor points m count coordinates of distance $q := m\,u\sqrt{(2\pi/N)}$, with u a unit such as the reduced wavelength $\lambda/2\pi$ in wave optics, $\Delta q = u\sqrt{(2\pi/N)} \to 0$ is the distance between adjoining sensors and the size of the array grows as $N\,\Delta q \to \infty$. The DLCT summation kernel (14)–(15) then converges weakly to the LCT integral kernel (2) with a phase factor. However, the free-flight parameter (9) in these units becomes $z = u\,b = u/B$, which in optical setups is too small for a true paraxial model to be valid. Quantum mechanical devices that act in time as Hadamard systems may be much different, but we dare not suggest concrete physical realizations for them. The objective achieved here has been to relate Hadamard systems with elements of the symplectic group of linear canonical transformations.

Acknowledgments

The authors acknowledge the support to the *Óptica Matemática* projects DGAPA-UNAM IN-105008 and SEP-CONACYT 79899 by the Universidad Nacional Autónoma de México and the Consejo Nacional de Ciencia y Tecnología. KBW thanks Professors Andrei B Klimov and Apostol Vourdas for illuminating discussions, and both authors thank Guillermo Krötzsch for technical support with the figure.

References

[1] Hadamard J 1893 Résolution d’une question relative aux déterminants *Bull. Sci. Math.* **17** 240–6

[2] Paley R E A C 1933 On orthogonal matrices *J. Math. Phys.* **12** 311–20

[3] Seberry J, Wysocki B and Wysocki T 2005 Some applications of Hadamard matrices *Metrika* **62** 221–39

[4] Haagerup U 1997 Orthogonal maximal Abelian *-subalgebras of the $n \times n$ matrices and cyclic n-roots *Operator Algebras and Quantum Field Theory* (Cambridge, MA: International Press) pp 296–322

[5] Hennelly B M and Sheridan J T 2005 Fast numerical algorithm for the linear canonical transform *J. Opt. Soc. Am.* A **22** 928–37

[6] Healy J J and Sheridan J T 2010 Fast linear canonical transforms *J. Opt. Soc. Am.* A **27** 21–30

[7] Kibler M R 2006 Angular momentum and mutually unbiased bases *Int. J. Mod. Phys.* B **20** 1792–801

[8] Kibler M R 2009 An angular momentum approach to quadratic Fourier transform, Hadamard matrices, Gauss sums, mutually unbiased bases, unitary group and Pauli group *J. Phys. A: Math. Theor.* **42** 353001

[9] Moshinsky M and Quesne C 1974 Oscillator systems *Proc. 15th Solvay Conf. in Physics (1970)* (New York: Gordon and Breach) pp 233–300

[10] Collins S A Jr 1970 Lens-system diffraction integral written in terms of matrix optics *J. Opt. Soc. Am.* **60** 1168–77

[11] Wolf K B 1979 *Integral Transforms in Science and Engineering* (New York: Plenum)

[12] Wolf K B 2004 *Geometric Optics on Phase Space* (Heidelberg: Springer)

[13] Ozaktas H M, Zalevsky Z and Kutay M A 2001 *The Fractional Fourier Transform with Applications in Optics and Signal Processing* (Chichester: Wiley)

[14] Ozaktas H M, Arıkan O, Kutay M A and Bozdagı G 1996 Digital computation of the fractional Fourier transform *IEEE Trans. Signal Process.* **44** 2141–50

[15] Hennelly B M and Sheridan J T 2005 Generalizing, optimizing, and inventing numerical algorithms for the fractional Fourier, Fresnel, and linear canonical transforms *J. Opt. Soc. Am.* A **22** 917–27

[16] Healy J J, Hennelly B M and Sheridan J T 2008 An additional sampling criterion for the linear canonical transform *Opt. Lett.* **33** 2599–601

[17] Koç A, Ozaktas H M, Çandan Ç and Kutay M A 2008 Digital computation of linear canonical transforms *IEEE Trans. Signal Process.* **56** 2383–94

[18] Hamermesh M 1962 *Group Theory and its Applications to Physical Problems* (Reading, MA: Addison-Wesley)

[19] Ibarra J and Ojeda Castañeda J 1993 Talbot interferometry: a new geometry *Opt. Commun.* **96** 294–301

[20] Tadej W and Życzkowsky K 2006 A concise guide to complex Hadamard matrices *Open Syst. Inf. Dyn.* **13** 133–77 (arXiv:quant-ph/0512154)

[21] Berndt B C, Evans R J and Williams K S 1998 *Gauss and Jacobi Sums* (New York: Wiley Interscience)

[22] Cohen H 1993 *A Course in Computational Algebraic Number Theory* (Berlin: Springer)