Mutually Unbiased Bases for Continuous Variables

Stefan Weigert
Department of Mathematics, University of York
Heslington, UK-York YO10 5DD
slow500@york.ac.uk
and
Michael Wilkinson
Department of Applied Mathematics
Open University, UK-Milton Keynes MK6 7AA
M.Wilkinson@open.ac.uk

February 2008

Abstract

The concept of mutually unbiased bases is studied for N pairs of continuous variables. To find mutually unbiased bases reduces, for specific states related to the Heisenberg-Weyl group, to a problem of symplectic geometry. Given a *single* pair of continuous variables, *three* mutually unbiased bases are identified while *five* such bases are exhibited for *two* pairs of continuous variables. For $N = 2$, the golden ratio occurs in the definition of these mutually unbiased bases suggesting the relevance of number theory not only in the finite-dimensional setting.

PACS: 03.65.-w,03.67.-a,03.65.Ta

Mutually unbiased (MU) bases of Hilbert spaces with finite dimension d (as defined by Eq. (1) below) are a useful tool. If you want to experimentally determine the state of a quantum system, given only a limited supply of identical copies, the optimal strategy is to perform measurements with respect to MU bases [1]. To pass a secret message to a second party, you could use quantum cryptography to establish a shared key, a procedure which relies on MU bases in the space $\mathbb{C}^2$ [2, 3] or $\mathbb{C}^d$ [4]. Sending a physical system carrying a spin through a noisy environment, the effect of the interactions on the state of the spin might be modelled by a specific quantum channel, conveniently described in terms of MU bases [5]. Finally, if you happen to be captured by a mean king, you might be able to meet his challenge by knowing about entangled states and MU bases [6].

Many of the ideas which underlie physical concepts defined for *discrete* variables, that is, in a Hilbert space of finite dimension, survive the transition from spin operators to position and momentum operators. Quantum key distribution [7] and quantum teleportation [8], for example, possess counterparts for *continuous* variables [9]

which act on an infinite-dimensional Hilbert space. It is thus natural to inquire into MU bases for continuous variables. This approach might also provide a new perspective on the existence of *complete* sets of MU bases in spaces of finite dimension given by a *product* of prime numbers as discussed below.

Let us recall the definition of MU bases in $\mathbb{C}^d$ and some of their properties. Two orthonormal bases $\mathcal{B}_b = \{|\psi_j^b\rangle\}_{j=1\ldots d}$ and $\mathcal{B}_{b'} = \{|\psi_j^{b'}\rangle\}_{j=1\ldots d}$ are called MU if

$$|\langle\psi_j^b|\psi_{j'}^{b'}\rangle| = \begin{cases} \delta_{jj'} & \text{if} \quad b = b' \,, \\ \kappa > 0 & \text{if} \quad b \neq b' \,, \end{cases} \tag{1}$$

since each state of one basis gives rise to the same probability distribution when measured with respect to the other basis. The value of the overlap κ is *not* arbitrary but one *derives* from (1) that $\kappa \equiv 1/\sqrt{d}$ by using the completeness of the basis $\mathcal{B}_b$, say.

Schwinger [10] describes how to construct two MU bases from any orthonormal basis of $\mathbb{C}^d$. They are found to be the eigenbases of two operators $\hat{U}$ and $\hat{V}$ each shifting cyclically the elements of the other basis. These operators satisfy commutation relations of Heisenberg-Weyl type, $\hat{U}\hat{V} = e^{2\pi i/d}\hat{V}\hat{U}$, describing finite translations in a discrete phase space [11]. This approach has been generalized in [12], where it is shown that if one finds n unitaries each cyclically shifting the eigenbases of all other unitaries then these n bases are MU.

The number of MU bases in $\mathbb{C}^d$ is limited to $d+1$. Such *complete* sets of MU bases were constructed first in the case of d being a prime number [13] and subsequently for d being a power of a prime [1]. For composite dimensions $d = d_1 d_2 \ldots d_k$, the factors being (powers of) different primes, it is currently unknown whether complete sets of MU bases exist [14]. While it is possible to construct three MU bases for any $d \geq 2$, numerical evidence suggests that already for $d = 6$ (the smallest composite integer), no four MU bases exist [15]. Interestingly, composite dimensions are rare for small values of d but predominate for large d.

Let us now turn to continuous variables $\hat{p}$ and $\hat{q}$, with $[\hat{q}, \hat{p}] = i\hbar$, acting on the Hilbert space $\mathcal{L}_2(\mathbb{R})$ of square-integrable functions on the real line. The (generalized) eigenstates of position and momentum by $|q\rangle, q \in \mathbb{R}$, and $|p\rangle, p \in \mathbb{R}$, respectively, are known to satisfy

$$\langle q|p\rangle = \frac{1}{\sqrt{2\pi\hbar}} e^{iqp/\hbar} \,. \tag{2}$$

Thus, a natural generalization of (1) for bases $\{|\psi_s^b\rangle\}_{s\in\mathbb{R}}$ of an infinite-dimensional Hilbert space takes the form

$$|\langle\psi_s^b|\psi_{s'}^{b'}\rangle| = \begin{cases} \delta(s-s') & \text{if} \quad b = b' \,, \\ k > 0 & \text{if} \quad b \neq b' \,, \end{cases} \tag{3}$$

where the δ-normalization of the states reflects the fact that the labels s, s' are *continous*. Consequently, the eigenstates of the position and momentum operators provide an example of MU bases with $k = 1/\sqrt{2\pi\hbar}$. The appearance of generalized eigenstates is inevitable, because no normalizable state exists which has a non-zero overlap with all elements of a countable orthonormal basis.

Is it possible to find three or more MU bases for one pair of continuous variables? The momentum basis $\mathcal{B}_p$ results from a rotation of the position basis $\mathcal{B}_q$ by an angle $\pi/2$. Thus, a third MU basis might be given by $\mathcal{B}_\vartheta = \{|q_\vartheta\rangle\}_{q_\vartheta \in \mathbb{R}}$, the eigenbasis of the operator $\hat{q}_\vartheta = \hat{q}\cos\vartheta + \hat{p}\sin\vartheta$ with eigenvalue q_ϑ (with $\vartheta \in (0, \pi/2)$). Using Wigner functions, one finds that the modulus of the overlap between states of $\mathcal{B}_q$ and $\mathcal{B}_\vartheta$ is

$$|\langle q_\vartheta | q \rangle|^2 = \frac{1}{2\pi\hbar\,|\sin\vartheta|} \neq \frac{1}{2\pi\hbar}\,. \tag{4}$$

Thus, no basis $\mathcal{B}_\vartheta$ with $\vartheta \in (0, \pi/2)$ combines with $\mathcal{B}_q$ and $\mathcal{B}_p$ to give a triple of MU bases.

There is, however, a *symmetric* choice of operators which does provide *three* MU bases. Consider the bases $\mathcal{B}_\pm = \{|q_\pm\rangle\}_{q_\pm \in \mathbb{R}}$ where $\hat{q}_\pm = \hat{q}\cos(2\pi/3) \pm \hat{p}\sin(2\pi/3)$, obtained from rotating the position basis by the angles $\pm 2\pi/3$, respectively. One finds

$$|\langle q | q_+ \rangle|^2 = |\langle q_+ | q_- \rangle|^2 = |\langle q_- | q \rangle|^2 = \frac{1}{2\pi\hbar|\,|\sin(2\pi/3)|}\,, \tag{5}$$

so that the triple $\mathcal{B}_+$, $\mathcal{B}_-$, and $\mathcal{B}_q$ *is* MU with overlap $k = 1/\sqrt{\pi\hbar\sqrt{3}}$ in (3). Comparing this result with (2), we realize that, for continuous variables, the constant k in (3) may take different values for different MU bases.

In spite of (4), it is possible to complement $\mathcal{B}_q$ and $\mathcal{B}_p$ with a third basis resulting in an *asymmetric* triple of MU bases. Consider $\mathcal{B}_{q-p}$ consisting of the eigenstates of the operator $\hat{q} - \hat{p} \equiv \sqrt{2}\hat{q}_{\pi/4}$ which *cannot* be obtained from $\hat{q}$ by a rotation due to the factor $\sqrt{2}$. Nevertheless, one finds (as stated in [16]) that

$$|\langle q | q - p \rangle|^2 = |\langle q - p | p \rangle|^2 = |\langle p | q \rangle|^2 = \frac{1}{2\pi\hbar}\,, \tag{6}$$

providing us with an *asymmetric* triple of MU bases.

We now develop a systematic approach to MU bases for N pairs of continuous variables residing in product states. For $N = 1$, we will be able to explain the observations above. For $N \geq 2$, we will derive geometric conditions which express whether product-state bases are MU or not. A set of *five* MU bases will be found explicitly for *two* continuous variables. Subsequently, we will formulate conditions to be MU for bases which do not have to consist of product states only.

The Heisenberg-Weyl operator

$$\hat{T}(\mathbf{a}) = \exp[i(P\hat{q} - Q\hat{p})/\hbar] \tag{7}$$

which translates the position of a wavefunction by Q and boosts its momentum by P, will play a central role. We consider the generator $\hat{x}_\mathbf{a}$ of an infinitesimal translation in the direction $\mathbf{a}^t = (Q, P)$, using the notation:

$$\hat{x}_\mathbf{a} \equiv P\hat{q} - Q\hat{p} \equiv \mathbf{a}^t \cdot \mathbf{j} \cdot \hat{\mathbf{x}} \quad \text{with } \mathbf{j} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{8}$$

where $\hat{\mathbf{x}} = (\hat{q}, \hat{p})^t$. Denote the eigenstates of $\hat{x}_{\mathbf{a}}$ by $|\mathbf{a}, \alpha\rangle$ where $\mathbf{a}$ identifies a particular family of states and α labels an element of this family. They satisfy

$$\hat{x}_{\mathbf{a}}|\mathbf{a}, \alpha\rangle = \alpha|\mathbf{a}, \alpha\rangle \, , \; \alpha \in \mathbb{R} \, , \tag{9}$$

forming complete and δ-orthonormal families of states $\mathcal{B}_{\mathbf{a}}$. Their position representations are given by

$$\langle q|\mathbf{a}, \alpha\rangle = \frac{1}{\sqrt{2\pi\hbar|Q|}} e^{iP(q-\alpha/P)^2/2\hbar Q} \, , \tag{10}$$

if both P and Q are non-zero [17]. The scalar product between states from bases with labels $\mathbf{a}$ and $\mathbf{b}$ ($\neq \mathbf{a}$) is found to be

$$|\langle \mathbf{b}, \beta|\mathbf{a}, \alpha\rangle|^2 = \frac{1}{2\pi\hbar|\mathbf{b}^t \cdot \mathbf{j} \cdot \mathbf{a}|} \, . \tag{11}$$

It is crucial for the following that the right-hand-side of (11) depends only on the modulus of the *symplectic* product of the vectors $\mathbf{a}$ and $\mathbf{b}$, which is equal to the (unsigned) area of the parallelogram defined by these vectors. The particular class of states considered here thus picks up the symplectic structure related to the commutation relations $[\hat{x}_{\mathbf{a}}, \hat{x}_{\mathbf{b}}] = -i\hbar \mathbf{a}^t \cdot \mathbf{j} \cdot \mathbf{b}$. Note that Eq. (10) is consistent with (11) since one has $|q\rangle \equiv |\mathbf{e}_P, \alpha\rangle$, with $\mathbf{e}_P^t \equiv (0, 1)$.

We are now in a position to derive sufficient conditions to have MU bases for N pairs of continuous variables $\hat{\mathbf{x}}_n = (\hat{q}_n, \hat{p}_n)$, $n = 1 \ldots N$, with $[\hat{q}_n, \hat{p}_{n'}] = i\hbar\delta_{nn'}$, each pair $\hat{\mathbf{x}}_n$ acting on a copy of $\mathcal{L}_2(\mathbb{R})$.

In a first step, we restrict the candidates for MU bases to N-fold tensor products of the states in (9),

$$|\vec{\mathbf{a}}, \vec{\alpha}\rangle \equiv |\mathbf{a}_1, \alpha_1\rangle \otimes \ldots \otimes |\mathbf{a}_N, \alpha_N\rangle \equiv \bigotimes_{n=1}^{N} |\mathbf{a}_n, \alpha_n\rangle \, , \tag{12}$$

which define a complete and δ-orthonormal basis $\mathcal{B}_{\vec{\mathbf{a}}}$. Using (11), the modulus of the scalar product of $|\vec{\mathbf{a}}, \vec{\alpha}\rangle$ and $|\vec{\mathbf{b}}, \vec{\beta}\rangle$ is given by

$$|\langle \vec{\mathbf{a}}, \vec{\alpha}|\vec{\mathbf{b}}, \vec{\beta}\rangle|^2 = \prod_{n=1}^{N} |\langle \mathbf{a}_n, \alpha_n|\mathbf{b}_n, \beta_n\rangle|^2 = \frac{1}{(2\pi\hbar)^N} \prod_{n=1}^{N} \frac{1}{|\mathbf{a}_n^t \cdot \mathbf{j} \cdot \mathbf{b}_n|} \, , \tag{13}$$

which can be written as

$$|\langle \vec{\mathbf{a}}, \vec{\alpha}|\vec{\mathbf{b}}, \vec{\beta}\rangle|^2 = (2\pi\hbar)^{-N} |\vec{\mathbf{a}}^t \cdot \mathbf{j}_N \cdot \vec{\mathbf{b}}|^{-1} \tag{14}$$

where

$$\vec{\mathbf{a}} = \mathbf{a}_1 \otimes \ldots \otimes \mathbf{a}_N \; , \quad \mathbf{j}_N = \mathbf{j}^{\otimes N} \, , \tag{15}$$

etc. Thus, in order that some bases $\mathcal{B}_{\vec{a}}$, $\mathcal{B}_{\vec{b}}$, ..., be MU, the unsigned symplectic products between any pairs of the vectors $\vec{\mathbf{a}}, \vec{\mathbf{b}}, \ldots$ must take one and the same value,

$$|\vec{\mathbf{a}}^t \cdot \mathbf{j}_N \cdot \vec{\mathbf{b}}| = |\vec{\mathbf{b}}^t \cdot \mathbf{j}_N \cdot \vec{\mathbf{c}}| = \ldots = K > 0 \, , \tag{16}$$

reducing the search for MU bases of product form (11) to the search of product vectors $\vec{\mathbf{a}}, \vec{\mathbf{b}}, \ldots$ in $\mathbb{R}^{2^N}$ satisfying (16). Having found a solution $\{\vec{\mathbf{a}}, \vec{\mathbf{b}}, \ldots\}$ for some value of the constant K, one finds a solution for any other positive K' by rescaling each vector with the factor $\sqrt{K/K'}$.

What is the maximal number of vectors satisfying (16) for N pairs of continuous variables? Lacking a general solution, we consider this problem of symplectic geometry in some detail for $N = 1$ and $N = 2$.

$N = 1$: The constraints (16) now read $|\mathbf{a}^t \cdot \mathbf{j} \cdot \mathbf{b}| = |\mathbf{b}^t \cdot \mathbf{j} \cdot \mathbf{c}| = |\mathbf{c}^t \cdot \mathbf{j} \cdot \mathbf{a}| = k > 0$. In fact, only three vectors need to be written here since one can show that it is *impossible* to have a fourth vector $\mathbf{d}$ of symplectic product k with $\mathbf{a}, \mathbf{b}$ and $\mathbf{c}$ satisfying these conditions. This does not exclude, however, the existence of four or more MU bases built from an entirely different set of states.

Working out the unsigned symplectic product of the vectors $(0, -1)$, $(1, 0)$, and $(1, 1)$ leads to $k = 1$, correctly reproducing the asymmetric solution presented in (6). Similarly, the set of unit vectors $(0, -1)$ and $(\pm\sqrt{3}/2, 1)$, which is invariant under three-fold rotations, describes the *symmetric* configuration (5), with $k = \sqrt{3}/2$. These apparently different solutions are, in fact, closely related. Consider all real 2×2 matrices $\mathbf{m}$ with unit determinant which, under conjugation, leave the matrix $\mathbf{j}$ invariant up to a sign,

$$\mathbf{m}^t \cdot \mathbf{j} \cdot \mathbf{m} = \pm \mathbf{j}\,; \tag{17}$$

we will call these matrices *unsigned symplectic*. They clearly form a group which consists of the union of all real symplectic 2×2 matrices, denoted by $\mathrm{Sp}(1, \mathbb{R})$, and all these matrices multiplied by the matrix $\mathbf{j}$ in (8) which (is not symplectic but) satisfies (17) with the minus sign. Due to (17), symplectic products $\mathbf{a}^t \cdot \mathbf{j} \cdot \mathbf{b}$ remain invariant up to a sign under transformations of the form $\mathbf{a} \to \mathbf{m} \cdot \mathbf{a}$. Using unsigned symplectic transformations, it becomes possible to map the triple of vectors $(0, -1)$, $(1, 0)$, and $(1, 1)$ into a configuration with three-fold rotational symmetry which is equivalent to the three MU bases in (5), up to a non-unitary scaling transformation as described after Eq. (16).

$N = 2$: MU bases correspond to sets of product vectors $\vec{\mathbf{a}} = \mathbf{a}_1 \otimes \mathbf{a}_2$, $\vec{\mathbf{b}} = \mathbf{b}_1 \otimes \mathbf{b}_2, \ldots$, with equal unsigned symplectic products. We now exhibit *five* vectors which satisfy (16) with $K = 1$, namely

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 \\ 1-R \end{pmatrix} \otimes \begin{pmatrix} 1 \\ R \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 2-R \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1+R \end{pmatrix}. \tag{18}$$

Here the number R is the *golden ratio*, i.e. the positive solution of $R^2 = R + 1$. Each coefficient of the five vectors is a sum of integer multiples of the numbers 1 and R. Hence, we find that the coefficients are elements of a number field given by a quadratic extension of the integers (just as the field of complex numbers is an extension of the real numbers where i, the solution of $r^2 + 1 = 0$, plays the same role as R). Thus the link between MU bases and number theory which pervades the finite-

dimensional case (surveyed in, e.g. [18]) also exists for continous-variables. Interestingly, MU bases for multiple qubits [19] or qutrits [20, 21] must contain entangled states, contrary to what we find here.

In a second step, we construct MU bases for N continuous variables from states not limited to the tensor products (12). To do so we introduce *metaplectic* operators which represent linear canonical phase space transformations in Hilbert space. Explicitly, consider the transformation $\mathbf{A}' = \mathbf{M}\cdot\mathbf{A}$, with $\mathbf{A} = (q_1, \cdots, p_N) \equiv (\mathbf{q}, \mathbf{p}) \in \mathbb{R}^{2N}$ and $\mathbf{M}$ being a symplectic matrix of size $2N \times 2N$. Then there is a unitary operator $\hat{U}_\mathbf{M}$ such that the translation operators $\hat{T}(\mathbf{A})$–each a product of N operators of the form (7)–transform according to

$$\hat{U}_\mathbf{M}\hat{T}(\mathbf{A}) = \hat{T}(\mathbf{M}\cdot\mathbf{A})\hat{U}_\mathbf{M}\,, \tag{19}$$

defining the metaplectic $\hat{U}_\mathbf{M}$. If symplectic transformations are composed, $\mathbf{M} = \mathbf{M}'\cdot\mathbf{M}''$, then the corresponding metaplectic operators are composed in the same manner: $\hat{U}_\mathbf{M} = \hat{U}_{\mathbf{M}'}\hat{U}_{\mathbf{M}''}$.

The use of metaplectic operators has been implicit in our earlier discussion where we obtained a set of states $|\mathbf{a}, \alpha\rangle$, satisfying (9), which are MU with respect to the position eigenstates $|q\rangle$. We now show that these states can be obtained directly by application of a metaplectic operator. Expand (19) in $\mathbf{A}$ and consider the linear term to obtain $\hat{U}_\mathbf{M}\hat{x}_\mathbf{A} = \hat{x}_{\mathbf{M}\cdot\mathbf{A}}\hat{U}_\mathbf{M}$. First, let $N = 1$ and choose the symplectic matrix $\mathbf{m}$ such that $\mathbf{m}\cdot\mathbf{a} = (0, 1)^t$, so $\hat{x}_{\mathbf{m}\cdot\mathbf{a}} = \hat{q}$. The eigenfunctions of $\hat{x}_\mathbf{a}$ in (9) are then generated by $|\mathbf{a}, \alpha\rangle = \hat{U}_\mathbf{m}|q\rangle$. The symplectic matrix satisfying $\mathbf{m}\cdot(Q, P)^t = (0, 1)^t$ is

$$\mathbf{m} = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}\begin{pmatrix} P & -Q \\ 1/Q & 0 \end{pmatrix} \tag{20}$$

where $\mu \in \mathbb{R}$ parametrises a shear along the line defining the states $|\mathbf{a}, \alpha\rangle$. It affects the phase of $\langle q|\mathbf{a}, \alpha\rangle$, but not its magnitude.

In order to discuss a more general construction of MU bases (with $N \geq 1$) we use a general expression [22] for a metaplectic operators which correspond to a symplectic matrix $\mathbf{M}$ of dimension $2N$,

$$\hat{U}_\mathbf{M} = \frac{\exp(i\Theta)}{\sqrt{|\det(\mathbf{M}-\mathbf{I})|}}\int\frac{d\mathbf{A}}{(2\pi\hbar)^N}\exp\left[\frac{i}{2\hbar}\mathbf{A}^t\cdot\mathbf{N}\cdot\mathbf{A}\right]\hat{T}(\mathbf{A}); \tag{21}$$

here Θ is a phase which need not concern us further, $\mathbf{N} = \frac{1}{2}\mathbf{J}(\mathbf{M}+\mathbf{I})(\mathbf{M}-\mathbf{I})^{-1}$ is a symmetric matrix, $\mathbf{J} = \mathbf{j}\oplus\ldots\oplus\mathbf{j}$ a block diagonal generalization of $\mathbf{j}$ in (8), and the integration is over the $2N$ dimensions of phase space, $d\mathbf{A} = dQ_1\, dQ_2 \ldots dP_N$. The matrices $\mathbf{M}$ and $\mathbf{N}$ may be written using blocks of dimension $N \times N$,

$$\begin{pmatrix} \mathbf{q}' \\ \mathbf{p}' \end{pmatrix} = \begin{pmatrix} \mathbf{M}_{qq} & \mathbf{M}_{qp} \\ \mathbf{M}_{pq} & \mathbf{M}_{pp} \end{pmatrix}\begin{pmatrix} \mathbf{q} \\ \mathbf{p} \end{pmatrix}\,, \quad \mathbf{N} = \begin{pmatrix} \mathbf{N}_{qq} & \mathbf{N}_{qp} \\ \mathbf{N}_{pq} & \mathbf{N}_{pp} \end{pmatrix}\,. \tag{22}$$

Consider the action of $\hat{U}_\mathbf{M}$ on N-fold products of position eigenstates, $|\mathbf{q}\rangle \equiv |q_1\rangle\otimes\ldots\otimes|q_N\rangle$. Using (21) and (22), we find that states $\hat{U}_\mathbf{M}|\mathbf{q}\rangle \equiv |\mathbf{M}, \mathbf{q}\rangle$ are unbiased relative to

the position eigenstates, i.e.,

$$|\langle \mathbf{q}'|\mathbf{M},\mathbf{q}\rangle|^2 = \frac{1}{(2\pi\hbar)^N}\frac{1}{|\det(\mathbf{M}-\mathbf{I})\det(\mathbf{N}_{pp})|}\ . \tag{23}$$

It follows from the composition property of metaplectic matrices that different states of the type $|\mathbf{M},\mathbf{q}\rangle$ are also unbiased with respect to each other, and that the magnitude of their overlap can be calculated by composing the underlying symplectic matrices:

$$|\langle \mathbf{M},\mathbf{q}|\mathbf{M}',\mathbf{q}'\rangle|^2 = |\langle \mathbf{q}|\hat{U}_{\mathbf{M}}^{-1}\hat{U}_{\mathbf{M}'}|\mathbf{q}'\rangle|^2 = |\langle \mathbf{q}|(\mathbf{M}^{-1}\mathbf{M}'),\mathbf{q}'\rangle|^2\,, \tag{24}$$

where the final expression is evaluated using (23). Thus, the problem of finding MU bases associated with metaplectic operators can be solved by finding symplectic transformations such that the resulting expressions on the right-hand-side of (23) take the same values. This may allow for a much larger set of MU bases than (16).

Our principal results are conditions for bases related by a metaplectic transformation to be MU, namely (16) (for which we found a solution (18)) and more generally (24) (as yet unexplored). To conclude we point out open questions. Even in the case of $N = 1$, it is not know whether more than three MU bases exist. To have only three MU bases would be slightly surprising as the limit of $d \to \infty$ passing through prime dimensions suggests the existence of an unlimited number of MU bases. The result (4) confirms this expectation in a restricted sense–any *pair* of bases $\mathcal{B}_\vartheta$ and $\mathcal{B}_{\vartheta'}$ is MU but with possibly *different* values for the overlap. Future studies will reveal whether the pairwise unbiased bases $\mathcal{B}_\vartheta, \vartheta \in (0,\pi/2)$ are as useful as a *complete* set of MU bases.

It is also unknown whether the bases $\mathcal{B}_q$ and $\mathcal{B}_p$ can be supplemented by a third MU basis *qualitatively different* from the one presented in (6). Let the state $|\psi\rangle$ be a member of such a basis. The conditions $|\langle q|\psi\rangle| = |\langle p|\psi\rangle| = 1/\sqrt{2\pi\hbar}$ imply that its expansion coefficients in the position and momentum basis are constant multiples of phase factors $\exp[if(q)]$ and $\exp[ig(p)]$, respectively, related to each other by a Fourier transform,

$$e^{ig(p)} = \frac{1}{\sqrt{2\pi\hbar}}\int_{-\infty}^{\infty} e^{if(x)}e^{-ipq/\hbar}dq\,. \tag{25}$$

Thus, if the only pairs of functions $(f(q), g(p))$ solving this integral equation consist of quadratic polynomials, then there are no MU bases beyond the ones exhibited so far. Unfortunately, the entire set of its solutions is not known to us.

Acknowledgements: We thank Tony Sudbery for his comments and the London Mathematical Society for financial support.

References

[1] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.), **191**, 363, (1989)

[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, p.175, IEEE, New York, (1984)

[3] H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, W. Tittel, Electron. Lett., **33**, 586, (1997)

[4] N. J. Cerf, M. Bourennane, A. Karlsson and N. Gisin, Phys. Rev. Lett., **88**, 127902, (2002)

[5] M. Nathanson and M. B. Ruskai, J. Phys. A: Math. Theor., **40**, 8171, (2007)

[6] Y. Aharonov and B.-G. Englert, Z. Naturforsch. A: Phys. Sci., **56a**, 16, (2001)

[7] F. Grosshans, G. V. van Assche, R. M. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London), **421**, 238, (2003)

[8] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik, Science, **282**, 706, (1998)

[9] S. L. Braunstein and P. van Loock, Rev. Mod. Phys., **77**, 513, (2005)

[10] J. Schwinger, Proc. Nat. Acad. Sci. U.S.A., **46**, 560, (1960)

[11] A. Vourdas, Rep. Prog. Phys., **67**, 267, (2004)

[12] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury and F. Vatan, Algorithmica, **34**, 512, (2002)

[13] I. D. Ivanović, J. Phys. A, **14**, 3241, (1981)

[14] `http://www.imaph.tu-bs.de/qi/problems`

[15] P. Butterley and W. Hall, Phys. Lett., **369**, 1, (2007)

[16] A. C. de la Torre and D. Goyeneche, Am. J. Phys., **71**, 49, (2003)

[17] K. S. Gibbons, M. J. Hoffman and W. K. Wootters, Phys. Rev., **A 70**, 062101, (2004)

[18] M. Planat, H. Rosu, S. Perrine, and M. Saniga, Found. Phys., **36**, 1662, (2006)

[19] J. L. Romero, G. Björk, A. B. Klimov and L. L. Sánchez-Soto, Phys. Rev. A, **72**, 062310, (2005)

[20] J. Lawrence, Č. Brukner, and A. Zeilinger, Phys. Rev. A, **65**, 032320, (2002)

[21] J. Lawrence, Phys. Rev. A, **70**, 012302, (2004)

[22] B. Mehlig and M. Wilkinson, Ann. Phys. (Leipzig), **10**, 541, (2001).