Group theoretical construction of mutually unbiased bases in Hilbert spaces of prime dimensions

P Šulc and J Tolar

Department of Physics
Faculty of Nuclear Sciences and Physical Engineering
Czech Technical University
Břehová 7, CZ - 115 19 Prague, Czech Republic

E-mail: `sulcp1@km1.fjfi.cvut.cz`, `jiri.tolar@fjfi.cvut.cz`

Abstract. Mutually unbiased bases in Hilbert spaces of finite dimensions are closely related to the quantal notion of complementarity. An alternative proof of existence of a maximal collection of $N + 1$ mutually unbiased bases in Hilbert spaces of prime dimension N is given by exploiting the finite Heisenberg group (also called the Pauli group) and the action of $SL(2, \mathbb{Z}_N)$ on finite phase space $\mathbb{Z}_N \times \mathbb{Z}_N$ implemented by unitary operators in the Hilbert space. Crucial for the proof is that, for prime N, $\mathbb{Z}_N$ is also a finite field.

1. Introduction

Position coordinates and corresponding components of linear momentum of a free quantum particle are — according to usual quantum mechanics — *complementary observables*, a term coined by Niels Bohr. The main expression of this property (for quantum mechanics on the real line) are Heisenberg's uncertainty relations $\Delta q \Delta p \geq \hbar/2$, implying that there are no quantum states with arbitrarily narrow distributions of both q and p. If there were normalized states with $\Delta q = 0$, i.e. eigenstates of q, then Δp would diverge, hence measured values of p couldn't be predicted. However, due to continuity of spectra of q and p, the strict limits $\Delta q = 0$ or $\Delta p = 0$ cannot be physically attained. Complementarity thus means that quantum systems possess properties that are mutually exclusive: the observation of one of them precludes the observation of the other. A mathematical expression of complementarity of coordinate and momentum is

$$|\langle p|q \rangle|^2 = const., \tag{1}$$

i.e. if we know everything about position, we know nothing of momentum, and vice versa.

It is interesting and may have deep physical significance that pairs of complementary observables also exist for systems with finite-dimensional Hilbert spaces, as noted by J. Schwinger [1] (see also [2, 3]). For such pairs precise knowledge of one of them

implies that all possible outcomes of measuring the other one are equally probable, as exemplified in (1).

If complementary observables have non-degenerate spectra, complementarity can be expressed in terms of the corresponding normalized eigenstates forming complementary bases. Then a measurement over one basis provides maximum uncertainty as to the outcome of a measurement in the other because all N possible outcomes will have equal probabilities $1/N$. The first attempt to use complementary bases in quantum state determination is due to Ivanović [4] who provided explicit formulae for $N + 1$ such bases if N is an odd prime. The idea of using these bases for optimal quantum state determination was further developed by Wootters [5] and by Wootters and Fields [6] who called them *mutually unbiased*. In the latter paper they presented a construction of $N + 1$ mutually unbiased bases in an arbitrary prime power-dimensional Hilbert space and also demonstrated that they may serve as a maximal collection of measurements for optimal state determination.

Our main concern are N-level systems which provide basic models proposed for quantum information processing, since mutually unbiased bases find important applications there [7]. Their property that the outcome of a measurement in one selected basis gives no information about the possible results of measurements in all other mutually unbiased bases is of advantage for instance in key distribution protocols in quantum cryptography [8]. Observables with such a property for two-level systems (whose vectors are called *qubits* in quantum computation) are three Pauli matrices. Recently, d-level quantum systems (with vectors called *qudits*) have come to a closer attention. It has been shown that such systems can be realized experimentally and quantum key distribution protocols using qudits have been introduced (see e.g. [9]). Since such protocols use mutually unbiased bases in dimensions higher than two, it is desirable to study constructions of mutually unbiased bases for higher dimensions, too. It is also known that complementary observables are useful in quantum state tomography [10].

2. Quantum structures in finite-dimensional Hilbert spaces

Our starting point for quantum mechanics in the Hilbert space of finite dimension N is a model of quantum kinematics due to H. Weyl [11]. Its geometric interpretation as the simplest quantum kinematic on a finite discrete configuration space formed by a periodic chain of N points was elaborated by J. Schwinger [2]. In [12, 13] we proposed its group theoretical formulation based on Mackey's system of imprimitivity [14] which provides a group theoretical generalization of Heisenberg's commutation relations. For a recent review of the topic see [15, 16].

In an N-dimensional Hilbert space with orthonormal basis $\mathcal{B} = \{|0\rangle, |1\rangle, \ldots |N-1\rangle\}$ we can establish a group generated by unitary operators Q_N, P_N defined by the relations

$$Q_N|j\rangle = \omega_N^j|j\rangle, \quad j = 0, 1, \ldots, N-1, \tag{2}$$
$$P_N|j\rangle = |j - 1 \pmod{N}\rangle; \tag{3}$$

here ω_N is a primitive N-th root of unity, e.g. $\omega_N = \exp(2\pi i/N)$. If $\mathcal{B}$ is the standard (or canonical) basis of $\mathbb{C}^N$, the operators P_N and Q_N are represented by matrices

$$Q_N = \mathrm{diag}\left(1, \omega_N, \omega_N^2, \cdots, \omega_N^{N-1}\right) \tag{4}$$

and

$$P_N = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \tag{5}$$

In finite-dimensional quantum mechanics the unitary matrices Q_N and P_N are analogues of exponentials of position and momentum in the continuous coordinate representation [11]. Namely, they fulfil an algebraic relation

$$P_N Q_N = \omega_N Q_N P_N \tag{6}$$

which is analogous to the relation for Weyl's exponential form of Heisenberg's commutation relations. Further,

$$\omega_N P_N = P_N \omega_N, \quad \omega_N Q_N = Q_N \omega_N, \quad P_N^N = Q_N^N = I_N, \quad \omega_N^N = 1, \tag{7}$$

where I_N is the $N \times N$ unit matrix.

This model has a simple geometric interpretation. The cyclic group $\mathbb{Z}_N = \{0, 1, \ldots N - 1\}$ serves as a configuration space for N-dimensional quantum mechanics. Elements of $\mathbb{Z}_N$ label the vectors of the basis $\mathcal{B} = \{|0\rangle, |1\rangle, \ldots |N - 1\rangle\}$ with the physical interpretation that $|j\rangle$ is the normalized eigenvector of position at $j \in \mathbb{Z}_N$. The natural transitive action of $\mathbb{Z}_N$ on $\mathbb{Z}_N$ via addition modulo N is represented by unitary operators $U(k) = P_N^k$. Their action on vectors $|j\rangle$ from basis $\mathcal{B}$ is given by

$$U(k)|j\rangle = P_N^k|j\rangle = |j - k \pmod{N}\rangle \tag{8}$$

The $\mathbb{Z}_N$ analogue of the Fourier transformation is the discrete Fourier transformation given by the unitary Sylvester matrix S_N with elements

$$(S_N)_{jk} = \langle j|S_N|k\rangle = \frac{\omega_N^{jk}}{\sqrt{N}}. \tag{9}$$

The relations

$$S_N^{-1} P_N S_N = Q_N, \quad S_N^{-1} Q_N S_N = P_N^{-1} \tag{10}$$

show that the discrete Fourier transform diagonalizes the momentum operator, i.e. performs the transition from the coordinate representation to the momentum representation.

The finite group generated by ω_N, Q_N and P_N

$$\Pi_N = \left\{ \omega_N^l Q_N^i P_N^j | l, i, j = 0, 1, 2, \ldots, N - 1 \right\} \tag{11}$$

consists of N^3 unitary matrices and is called the *finite Heisenberg group* [17] or the *Pauli group* [18]. It has been found useful in connection with mutually unbiased bases [19]. Note also that the set of N^2 unitary matrices $\left\{ Q_N^a P_N^b | a, b \in \{0, 1, \ldots, N - 1\} \right\}$ constitutes, as Schwinger [1] has shown, a complete operator basis of the Hilbert space of all complex matrices orthogonal in the sense of the inner product

$$\mathrm{Tr}\left(\left(Q_N^a P_N^b \right)^\dagger Q_N^c P_N^d \right) = N \delta_{ac} \delta_{bd} \quad \text{for all} \quad a, b, c, d \in \mathbb{Z}_N. \tag{12}$$

3

3. Complementary observables and mutually unbiased bases

Mutually unbiased bases in Hilbert spaces of finite dimensions are closely related to the quantal notion of complementarity. Let us start with two almost identical definitions.

Definition 1 [3]. *Two observables $\mathbf{A}$ and $\mathbf{B}$ of a quantum system with Hilbert space of finite dimension N are called complementary, if their eigenvalues are non-degenerate and any two normalized eigenvectors $|u_i\rangle$ of $\mathbf{A}$ and $|v_j\rangle$ of $\mathbf{B}$ satisfy*

$$|\langle u_i|v_j\rangle| = \frac{1}{\sqrt{N}}. \tag{13}$$

Then in an eigenstate $|u_i\rangle$ of $\mathbf{A}$ all eigenvalues $b_1, \ldots, b_N$ of $\mathbf{B}$ are measured with equal probabilities, and vice versa. This means that exact knowledge of the measured value of $\mathbf{A}$ implies maximal uncertainty to any measured value of $\mathbf{B}$. For the next definition note that the (non-degenerate) eigenvalues a_i of $\mathbf{A}$ and b_j of $\mathbf{B}$ are in fact irrelevant, since only the corresponding orthonormal bases $|u_i\rangle$ and $|v_j\rangle$ are involved.

Definition 2 [5, 6]. *Two orthonormal bases in an N-dimensional complex Hilbert space*

$$\{|u_i\rangle|i = 1, 2, \ldots, N\} \quad and \quad \{|v_j\rangle|j = 1, 2, \ldots, N\}$$

are called mutually unbiased if inner products between all possible pairs of vectors taken from distinct bases have the same magnitude $1/\sqrt{N}$,

$$|\langle u_i|v_j\rangle| = \frac{1}{\sqrt{N}} \quad for\ all \quad i, j \in \{1, 2, \ldots, N\}. \tag{14}$$

In the above sense one may call two measurements to be mutually unbiased, if the bases composed of the eigenstates of their observables (with non-degenerate spectra) are mutually unbiased. Further, a set of bases is called mutually unbiased if every two different bases from the set are mutually unbiased.

An important fact was proved in [6] (for further references see also [20]) that the upper limit to the maximal possible number of bases that can form a set of mutually unbiased bases in an N-dimensional Hilbert space is $N + 1$:

Theorem 1. *In an N-dimensional Hilbert space, there cannot be more than $N + 1$ mutually unbiased bases.*

Finally we remark that a criterion of equivalence of two pairs of mutually unbiased bases was formulated in [3].

4. Mutually unbiased bases for prime N

The question whether it is possible to attain the maximal number of $N + 1$ mutually unbiased bases was answered in positive in [6], but under a number theoretic proviso: a maximal collection of $N + 1$ mutually unbiased bases exists in Hilbert spaces of dimensions equal to arbitrary powers of prime numbers. In this paper we will devote our attention to prime dimensions.

In the particular case $N = 2$ it can be easily verified that the set of eigenvectors of the Pauli matrices forms a complete collection of three mutually unbiased bases:

$$\{|0\rangle, |1\rangle\}, \quad \left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}, \quad \left\{\frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right\}. \tag{15}$$

The construction of such a set of bases in higher dimensions can be understood as a generalization of this property. The formulae for $N + 1$ mutually unbiased bases forming

a maximal set *for any odd prime dimension N* were first given (not derived) in [4]; we quote them according to [6]:

$$
\begin{aligned}
|v_k^{(0)}\rangle_j &= \delta_{jk}, \\
|v_k^{(1)}\rangle_j &= \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N}(j^2+jk)}, \\
&\vdots \\
|v_k^{(r)}\rangle_j &= \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N}(rj^2+jk)}, \\
&\vdots \\
|v_k^{(N-1)}\rangle_j &= \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N}((N-1)j^2+jk)}, \\
|v_k^{(N)}\rangle_j &= \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N}jk}.
\end{aligned}
$$

Here $|v_k^{(r)}\rangle_j$ denotes the j-th component of the k-th vector in r-th basis, $r = 0, 1, \ldots, N$. The first ($r = 0$) basis is the canonical basis, the last one ($r = N$) is its discrete Fourier transform. Mutual unbiasedness of the bases follows from the Gauss sums of number theory valid for p odd prime [21]

$$
\left| \sum_{k=0}^{p-1} e^{\frac{2\pi i}{p}(ak^2+bk)} \right| = \frac{1}{\sqrt{p}}; \tag{16}
$$

here $a, b \in \mathbb{N}$, $a \neq 0$ and a is not an integral multiple of p.

A derivation of these $N + 1$ mutually unbiased bases has been given for any prime dimension N in [19] in terms of unitary operators Q_N, P_N defined in Section 2:

Theorem 2. *Let N be a prime. Then the bases composed of eigenvectors of $N + 1$ operators*

$$
Q_N, P_N, P_N Q_N, P_N Q_N^2, \ldots, P_N Q_N^{N-1} \tag{17}
$$

are pairwise mutually unbiased and form therefore a maximal set of $N + 1$ mutually unbiased bases.

In this paper we are going to give an alternative construction of a complete collection of $N + 1$ mutually unbiased bases in a prime-dimensional Hilbert space by using the finite phase space related to the finite Heisenberg group. We hope that our approach could provide better insight also in the open problem of composite dimensions.

5. Finite phase space and its group of automorphisms

In order to arrive at an independent proof of Theorem 2 we have to introduce the necessary group theoretical notions.

First we need to establish a connection between the finite Heisenberg group and the *finite phase space* $\Gamma_N = \mathbb{Z}_N \times \mathbb{Z}_N$, $N = 2, 3, \ldots$ [17, 10]. The elements (l, i, j) of the finite Heisenberg group were given in (11) with $l, i, j = 0, 1, \ldots, N - 1$. Its center $Z(\Pi_N)$ is the set of those elements of Π_N which commute with all elements in Π_N,

$$
Z(\Pi_N) = \{(l, 0, 0)|l = 0, 1, \ldots, N - 1\}. \tag{18}
$$

Since the center is a normal subgroup, we can go over to the quotient group $\Pi_N/Z(\Pi_N)$. Its elements are the cosets labeled by pairs (i, j), $i, j = 0, 1, \ldots, N - 1$. The quotient

group is identified with the finite phase space Γ_N. To simplify notation, we shall denote the cosets corresponding to elements (i,j) of the phase space Γ_N by $Q^i P^j$ without subscripts N,

$$Q^i P^j = \left\{ \omega_N^l Q_N^i P_N^j \mid \quad l = 0, 1, \ldots, N-1 \right\}. \tag{19}$$

Note that all operators belonging to the same coset have the same eigenvectors because they differ only by multipliers ω_N^l.

Now it is easily seen that the correspondence

$$\phi : \Pi_N / Z(\Pi_N) \to \Gamma_N = \mathbb{Z}_N \times \mathbb{Z}_N \quad : \quad Q^i P^j \mapsto (i,j),$$

is an isomorphism of Abelian groups, since

$$\phi \left(\left(Q^i P^j \right) \left(Q^{i'} P^{j'} \right) \right) = \phi \left(\left(Q^i P^j \right) \right) \phi \left(\left(Q^{i'} P^{j'} \right) \right) =$$

$$= (i,j) + (i', j') = (i + i', j + j').$$

We shall now focus on the group of automorphisms of the phase space Γ_N. It was studied in [17]. However, we follow the approach of [22], where instead of cosets the one-dimensional grading subspaces of the Pauli graded Lie algebra $gl(N, \mathbb{C})$ were considered and their transformations under the automorphisms of $gl(N, \mathbb{C})$ were investigated. The subgroup of inner automorphisms was induced by the action

$$\psi_X(A) = X^{-1} A X \tag{20}$$

of matrices X from $GL(N, \mathbb{C})$.

In the same vein we will concentrate on the automorphisms of the form (20), acting on elements of Π_N, which induce permutations of cosets in $\Pi_N / Z(\Pi_N)$. Since the operators $\omega_N^l Q_N^a P_N^b$ have the same spectra, the matrices X which induce the automorphisms (20) are unitary. They can be understood as transformation matrices that transform a unitary operator (of the form $\omega_N^l Q_N^a P_N^b$) to a different basis, in which the operator is of the form $\omega^m Q^c P^d$. Thus X is a transformation matrix between two orthonormal bases. For explicit forms of matrices X see [17] (for N odd prime), but the results of [22] will suit better to our purpose.

Automorphisms ψ of the form (20) are equivalent if they define the same transformation of cosets in $\Pi_N / Z(\Pi_N)$:

$$\psi_Y \sim \psi_X \Leftrightarrow Y^{-1} Q^i P^j Y = X^{-1} Q^i P^j X \quad \text{for all} \quad (i,j) \in \mathbb{Z}_N \times \mathbb{Z}_N. \tag{21}$$

Since the group $\Pi_N / Z(\Pi_N)$ has only two generators — the cosets P and Q — condition (21) is equivalent to

$$\psi_Y \sim \psi_X \Leftrightarrow Y^{-1} P Y = X^{-1} P X \text{ and } Y^{-1} Q Y = X^{-1} Q X. \tag{22}$$

If ψ_Y induces a transformation of $\Pi_N / Z(\Pi_N)$, then there must exist elements $a, b, c, d \in \mathbb{Z}_N$ such that

$$Y^{-1} Q Y = Q^a P^b \quad \text{and} \quad Y^{-1} P Y = Q^c P^d. \tag{23}$$

It follows that to each equivalence class of automorphisms ψ_Y a quadruple (a, b, c, d) of elements in $\mathbb{Z}_N$ is assigned. We shall prove more, namely:

Theorem 3. *For N prime there is an isomorphism Φ between the set of equivalence classes of automorphisms ψ_Y and the group $SL(2, \mathbb{Z}_N)$ of 2×2 matrices with determinant equal to 1 modulo N,*

$$\Phi(\psi_Y) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad a, b, c, d \in \mathbb{Z}_N;$$

the action of these automorphisms on $\Pi_N/Z(\Pi_N)$ is given by the right action of $SL(2, \mathbb{Z}_N)$ on the phase space $\Gamma_N = \mathbb{Z}_N \times \mathbb{Z}_N$,

$$(i', j') = (i, j) \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{24}$$

Proof: To the composition of two automorphisms ψ_X, ψ_Y corresponding to (a_X, b_X, c_X, d_X) and (a_Y, b_Y, c_Y, d_Y), respectively, the product of matrices corresponding to ψ_X and ψ_Y is assigned, as can be seen from

$$(XY)^{-1}Q(XY) = (Y^{-1}QY)^{a_X}(Y^{-1}PY)^{b_X} =$$

$$= Q^{a_Y a_X}P^{b_Y a_X}Q^{c_Y b_X}P^{d_Y b_X} = Q^{a_X a_Y + b_X c_Y}P^{a_X b_Y + b_X d_Y},$$

and similarly for P

$$(XY)^{-1}P(XY) = Q^{c_X a_Y + d_X c_Y}P^{c_X b_Y + d_X d_Y}.$$

Hence

$$\Phi(\psi_X \psi_Y) = \Phi(\psi_X)\Phi(\psi_Y) \tag{25}$$

and Φ is an injective homomorphism.

Now matrix elements a, b, c, d cannot be chosen arbitrarily. Consider the action of ψ_Y:

$$Y^{-1}QY = Q^a P^b \quad \Longrightarrow \quad Y^{-1}Q_N Y = \mu Q_N^a P_N^b, \quad |\mu| = 1, \tag{26}$$

$$Y^{-1}PY = Q^c P^d \quad \Longrightarrow \quad Y^{-1}P_N Y = \lambda Q_N^c P_N^d, \quad |\lambda| = 1. \tag{27}$$

By multiplying equation (26) by equation (27) once from the left and once from the right, we obtain

$$P_N Q_N Y = \mu\lambda Y Q_N^c P_N^d Q_N^a P_N^b, \quad Q_N P_N Y = \mu\lambda Y Q_N^a P_N^b Q_N^c P_N^d. \tag{28}$$

Using the commutation relation (6) we obtain

$$\omega_N^{-ad}\mu\lambda Y Q_N^{a+c} P_N^{b+d} = P_N Q_N Y = \omega_N^{-1}Q_N P_N Y = \omega_N^{-1}\omega_N^{-bc}\mu\lambda Y Q_N^{a+c} P_N^{b+d} \tag{29}$$

leading to the condition

$$\omega_N^{-ad} = \omega_N^{-bc-1}. \tag{30}$$

It will be fulfilled if and only if $ad - bc = 1 \pmod{N}$, i.e.

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1 \pmod{N}. \tag{31}$$

This means that to every ψ_Y acting on $\Pi_N/Z(\Pi_N)$ a matrix from $SL(2, \mathbb{Z}_N)$

$$\Phi(\psi_Y) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is assigned. Now to every coset from $\Pi_N/Z(\Pi_N)$ an element (i, j) of the phase space $\mathbb{Z}_N \times \mathbb{Z}_N$ was associated. So finally we check that the action of ψ_Y on $Q^i P^j$ is given by

$$(i', j') = Q^{i'}P^{j'} = \psi_Y\left(Q^i P^j\right) = Y^{-1}Q^i P^j Y =$$

$$= Y^{-1}Q^i Y Y^{-1}P^j Y = Q^{ia+jc}P^{ib+jd} = (ia + jc, ib + jd),$$

and this means that the transformation of (i, j) can be written as the right action of $SL(2, \mathbb{Z}_N)$ on $\mathbb{Z}_N \times \mathbb{Z}_N$

$$(i', j') = (i, j) \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{32}$$

Finally observe that mapping Φ is an isomorphism, since

$$\Phi : \psi_X \mapsto I_2 \quad \Longrightarrow \quad \psi_X \in [\psi_{I_N}]$$

follows from

$$(i', j') = (i, j) \quad \text{if and only if} \quad X^{-1} Q^i P^j X = I_N^{-1} Q^i P^j I_N. \quad \square$$

We conclude this section with

Lemma 1 [23]. *The right action of $SL(2, \mathbb{Z}_N)$ on the phase space $\mathbb{Z}_N \times \mathbb{Z}_N$ does not change the determinant of a matrix composed of components of two vectors from $\mathbb{Z}_N \times \mathbb{Z}_N$.*

Proof: Consider two vectors (i, j) and (k, l) from $\mathbb{Z}_N \times \mathbb{Z}_N$ and the matrix $\begin{pmatrix} i & j \\ k & l \end{pmatrix}$. Since the action of A is given by $(i', j') = (i, j)A$ and $(k', l') = (k, l)A$, and because $\det A = 1$, one immediately gets the result

$$\det \begin{pmatrix} i' & j' \\ k' & l' \end{pmatrix} = \det \left(\begin{pmatrix} i & j \\ k & l \end{pmatrix} A \right) =$$

$$= \det \begin{pmatrix} i & j \\ k & l \end{pmatrix} \det A = \det \begin{pmatrix} i & j \\ k & l \end{pmatrix}. \quad \square \qquad (33)$$

Remarks. For N prime the right action of $SL(2, \mathbb{Z}_N)$ on the phase space $\mathbb{Z}_N \times \mathbb{Z}_N$ has exactly two orbits — the single point $\{(0,0)\}$ and $\mathcal{O}_N = \mathbb{Z}_N \times \mathbb{Z}_N \setminus \{(0,0)\}$ consisting of $N^2 - 1$ points. The stationary subgroup of the point $(1, 0)$ from $\mathcal{O}_N$ is the Abelian subgroup $\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} | b = 0, 1, \ldots, N - 1 \}$ of order N. Hence the order of $SL(2, \mathbb{Z}_N)$ is $N(N^2 - 1)$. Further, according to Lemma 1, the determinant (33) is an invariant of the right action of $SL(2, \mathbb{Z}_N)$ on $\Gamma_N \times \Gamma_N$. Let us note that $SL(2, \mathbb{Z}_N)$ transformations of the finite phase space were also studied in [24].

6. New construction of the maximal set of mutually unbiased bases for N prime

In this section the finite phase space and its transformations of the form (20) will be used to introduce an interesting algebraic structure that proves the existence of $N + 1$ mutually unbiased bases for prime N, thus providing an alternative approach to their construction. We shall exploit the fact that, for prime N, $\mathbb{Z}_N$ is a finite field, i.e., there is also a multiplicative group structure modulo N in $\mathbb{Z}_N^* = \mathbb{Z}_N \setminus \{0\}$.

Our construction starts with the partition of the finite phase space $\Gamma_N = \mathbb{Z}_N \times \mathbb{Z}_N$ into equivalence classes $[(i, j)]$ defined by the equivalence relation $(i, j) \sim (i', j')$, if there exists $r \in \mathbb{Z}_N^*$ such that $(i', j') = (ri, rj)$, where the multiplication is understood modulo N.

We exclude the trivial class $[(0, 0)]$ containing only $(0, 0)$. Then the orbit $\mathcal{O}_N = \mathbb{Z}_N \times \mathbb{Z}_N \setminus \{(0, 0)\}$ is decomposed into $N + 1$ classes $[(1, 0)]$ and $[(i, 1)]$ where $i = 0, 1, \ldots, N - 1$. The fact that $\mathbb{Z}_N$ is a field for prime N is crucial in the proof that every element of the orbit $\mathcal{O}_N$ belongs to some class. Since each class has $N - 1$ elements, this decomposition contains $N^2 - 1$ elements in total, with the only element $(0, 0)$ not included.

If an element is of the form $(0, i)$ or $(i, 0)$, then it is obvious that it belongs to classes $[(0, 1)]$ or $[(1, 0)]$, respectively. An element of the form (i, j), $i, j = 1, 2, \ldots, N - 1$,

will belong to the class $[(k,1)]$ where $k \in \{1,2,\ldots,N-1\}$ is the solution of $kj = i$ (mod N). The existence and uniqueness of such k is guaranteed by the fact that $\mathbb{Z}_N$ is a field for N prime. The partition into classes can be visualized in the following table of all elements in $\mathbb{Z}_N \times \mathbb{Z}_N \setminus \{(0,0)\}$:

	0	1	2	$\cdots$	N-1
0		(0,1)	(0,2)	$\cdots$	(0,N-1)
1	(1,0)	(1,1)	(1,2)	$\cdots$	(1,N-1)
2	(2,0)	(2,1)	(2,2)	$\cdots$	(2,N-1)
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
N-1	(N-1,0)	(N-1,1)	(N-1,2)	$\cdots$	(N-1,N-1)

Here every element (i,j) corresponds to a coset $Q^i P^j$. All operators in the same coset differ just by a complex multiplier. Every multiple (ri, rj) of a vector (i,j) by $r \in \{1,2,\ldots,N-1\}$ will therefore correspond to the coset $Q^{ri} P^{rj}$. Because of relation (6) it is obvious that operators $(Q^i P^j)^r$ and $(Q^{ri} P^{rj})$ belong to the same coset. An important consequence is that elements (ri, rj), $r = 1,2,\ldots,N-1$, correspond to commuting operators, hence have the same eigenvectors. Thus we have proved

Lemma 2. *If N is a prime, then there are exactly $N+1$ classes of elements from $\mathcal{O}_N = \mathbb{Z}_N \times \mathbb{Z}_N \setminus \{(0,0)\}$, each class containing $N-1$ elements. All elements of the same class correspond to commuting operators with the same eigenvectors.*

We will now demonstrate that the bases composed of the eigenvectors of two different operators corresponding to elements from distinct classes in $\mathcal{O}_N$ are mutually unbiased.

Theorem 4. *Let N be a prime and let (a,b) and (c,d) be two elements from $\mathcal{O}_N = \mathbb{Z}_N \times \mathbb{Z}_N \setminus \{(0,0)\}$ which belong to distinct classes $[(a,b)] \neq [(c,d)]$. Then the bases composed of eigenvectors of the operators from the corresponding cosets $Q^a P^b$ and $Q^c P^d$ are mutually unbiased.*

Proof: The first step is to show that the bases composed of eigenvectors of Q_N and P_N are mutually unbiased. This follows directly from equation (10). Namely,

$$P_N S_N |j\rangle = S_N Q_N |j\rangle = \omega_N^j S_N |j\rangle, \tag{34}$$

where $|j\rangle$ is an eigenvector of Q_N, so $S_N |j\rangle$ is an eigenvector of P_N. Further, because of (9), the inner product of $|j\rangle$ and $S_N |k\rangle$ has absolute value

$$|(|j\rangle, S_N |k\rangle)| = |\langle j | S_N | k \rangle| = \left| \frac{\omega_N^{jk}}{\sqrt{N}} \right| = \frac{1}{\sqrt{N}}. \tag{35}$$

Hence if we have two elements where one belongs to the class $[(1,0)]$ and the other to the class $[(0,1)]$, then we already know that their corresponding bases are mutually unbiased, because they are composed of eigenvectors of Q_N and P_N, respectively.

Because of the partition of $\mathcal{O}_N$ it is sufficient to consider now only the case of two distinct elements $(a,1)$ and $(b,1)$, with $a, b \in \{1,2,\ldots,N-1\}$, $a \neq b$. We are going to show that the bases of eigenvectors of the corresponding operators $Q_N^a P_N$ and $Q_N^b P_N$ are mutually unbiased (hence also the eigenvectors of powers of these operators). According to Theorem 3, to unitary operators X that permute the cosets in the Heisenberg group

$$X^{-1} Q^i P^j X = Q^{i'} P^{j'}$$

9

matrices from $\mathrm{SL}(2, \mathbb{Z}_N)$ are assigned. Conversely, to every matrix from $\mathrm{SL}(2, \mathbb{Z}_N)$ there is an equivalence class of unitary operators which induce the same permutation of the cosets. In this sense a special unitary representation of $\mathrm{SL}(2, \mathbb{Z}_N)$ was described in [17].

We will now show, if $a \neq b$, then there exists a matrix A from $\mathrm{SL}(2, \mathbb{Z}_N)$ such that

$$(a, 1)A = (\tilde{a}, 0) \quad \text{and} \quad (b, 1)A = (0, \tilde{b})$$

If we indeed can find such a matrix, then there exists a corresponding unitary operator X such that

$$X^{-1}Q^a P X = Q^{\tilde{a}}, \qquad X^{-1}Q^b P X = P^{\tilde{b}},$$

hence the eigenvectors of $Q^a P$ and $Q^b P$ can be expressed as $X|j\rangle$ and $XS_N|k\rangle$, respectively. According to (35) modulus of their inner product is

$$|(X|j\rangle, XS_N|k\rangle)| = |(|j\rangle, S_N|k\rangle)| = \frac{1}{\sqrt{N}},$$

proving that these bases are mutually unbiased, too.

To prove the existence of a unique matrix $A \in \mathrm{SL}(2, \mathbb{Z}_N)$ with the desired properties we apply Lemma 1 implying

$$\det \begin{pmatrix} a & 1 \\ b & 1 \end{pmatrix} = a - b \pmod{N} = \det \begin{pmatrix} \tilde{a} & 0 \\ 0 & \tilde{b} \end{pmatrix} = \tilde{a}\tilde{b} \pmod{N}$$

and we select $\tilde{a}, \tilde{b} \in \mathbb{Z}_N$ such that $\tilde{a}\tilde{b} = a - b \pmod{N}$. Equivalently we look for a matrix $C = A^{-1} \in \mathrm{SL}(2, \mathbb{Z}_N)$ producing the inverse transformation

$$(\tilde{a}, 0)C = (\tilde{a}, 0) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (a, 1),$$

$$(0, \tilde{b})C = (0, \tilde{b}) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (b, 1).$$

This gives us the following equations to compute the elements of C:

$$\tilde{a}\beta = 1 \pmod{N}, \tag{36}$$
$$\tilde{a}\alpha = a \pmod{N}, \tag{37}$$
$$\tilde{b}\gamma = b \pmod{N}, \tag{38}$$
$$\tilde{b}\delta = 1 \pmod{N}. \tag{39}$$

The fact that N is a prime guarantees that each of these equations has unique solution in $\mathbb{Z}_N$. Having the values of entries $\alpha, \beta, \gamma, \delta$, we still need to check that $C = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ belongs to $\mathrm{SL}(2, \mathbb{Z}_N)$. By multiplying equations (37) and (39) and subtracting the product of (38) and (36) we obtain

$$\tilde{a}\tilde{b}(\alpha\delta - \beta\gamma) = a - b \pmod{N}.$$

Since $\tilde{a}\tilde{b} = a - b \pmod{N}$ we have

$$\det C = \alpha\delta - \beta\gamma = 1 \pmod{N},$$

verifying that C indeed belongs to $\mathrm{SL}(2, \mathbb{Z}_N)$. The inverse matrix $A = C^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ will then transform pairs $(a, 1)$ and $(b, 1)$ into $(\tilde{a}, 0)$ and $(\tilde{b}, 0)$, respectively:

$$(a, 1)C^{-1} = (\tilde{a}, 0), \quad (b, 1)C^{-1} = (0, \tilde{b}).$$

To complete the proof, it is easy to see that for pairs $(b,1)$, $(1,0)$ and $(b,1)$, $(0,1)$, $b = 1, 2, \ldots, N-1$, there exist unique transformation matrices from $\mathrm{SL}(2, \mathbb{Z}_N)$ such that

$$(b,1)A_1(b) = (0,1), \ (1,0)A_1(b) = (1,0) \implies A_1(b) = \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix}$$

and

$$(b,1)A_2(b) = (b,0), \ (0,1)A_2(b) = (0,1) \implies A_2(b) = \begin{pmatrix} 1 & b^{-1} \\ 0 & 1 \end{pmatrix}.$$

Hence pairs of bases composed of eigenvectors of pairs of operators $Q^b P$, Q and $Q^b P$, P are mutually unbiased. Thus we have shown that there exist $N+1$ mutually unbiased bases in a Hilbert space of prime dimension N. We have therefore reached the same conclusion as [19]. In our case the mutually unbiased bases are composed of eigenvectors of operators

$$Q_N, P_N, Q_N P_N, Q_N^2 P_N, \ldots, Q_N^{N-1} P_N, \tag{40}$$

while the operators in Theorem 2 are only modified using (6).

Note that one could make a different choice of representatives of the classes forming the partition: we could have alternatively used e.g. the pairs $(1,a)$, $a = 1, 2, \ldots, N-1$, instead of $(a,1)$, and the mutually unbiased bases would be given by bases composed of eigenvectors of operators

$$Q_N, P_N, Q_N P_N, Q_N P_N^2, \ldots, Q_N P_N^{N-1}.$$

To provide a constructive proof we should give an explicit way to construct the bases out of the canonical basis $\mathcal{B}$. Let us denote the bases composed of eigenvectors of (40) by

$$\mathcal{B} = \mathcal{B}_{(1,0)}, \ \mathcal{B}_{(0,1)}, \ \mathcal{B}_{(1,1)}, \ \mathcal{B}_{(2,1)}, \ \ldots, \ \mathcal{B}_{(N-1,1)}.$$

We know that the map $\mathcal{B}_{(1,0)} \to \mathcal{B}_{(0,1)}$ is implemented by the unitary operator S_N. The next step $\mathcal{B}_{(0,1)} \to \mathcal{B}_{(1,1)}$, leaving $\mathcal{B}_{(1,0)}$ intact, clearly corresponds to the above transformation matrix $A_1(-1)$ from $\mathrm{SL}(2, \mathbb{Z}_N)$. Its iterations will generate further steps. A unitary transformation D_N which implements $A_1(-1)$,

$$D_N^{-1} Q_N D_N = Q_N, \qquad D_N^{-1} P_N D_N = \varepsilon_N^{-1} Q_N P_N,$$

can be taken from [22]; it is diagonal,

$$D_N = \mathrm{diag}\,(d_0, d_1, \ldots, d_{N-1}), \quad d_j = \varepsilon_N^{-j} \omega_N^{\binom{j}{2}},$$

where $\varepsilon_N = 1$ if N is odd, $\varepsilon_N = \sqrt{\omega_N}$ if N is even. In this way we arrive at a sequence of unitary maps

$$\mathcal{B}_{(1,0)} \overset{S_N}{\to} \mathcal{B}_{(0,1)} \overset{D_N}{\to} \mathcal{B}_{(1,1)} \overset{D_N}{\to} \mathcal{B}_{(2,1)} \overset{D_N}{\to} \ldots \overset{D_N}{\to} \mathcal{B}_{(N-1,1)},$$

and the composite unitary operators $D_N^b S_N$, $b = 0, 1, \ldots, N-1$ will produce all the bases starting from the canonical one. $\square$

Example $N = 2$. The phase space Γ_2 consists of 4 elements $(0,0)$, $(1,0)$, $(0,1)$, $(1,1)$. The group $\mathrm{SL}(2, \mathbb{Z}_2)$ with 6 elements

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

acts transitively on the orbit $\{(1,0),(0,1),(1,1)\}$. Unitary operators transforming the bases (15)

$$\mathcal{B}_{(1,0)} \quad \overset{S_2}{\to} \quad \mathcal{B}_{(0,1)} \quad \overset{D_2}{\to} \quad \mathcal{B}_{(1,1)}$$

are

$$S_2 = \frac{1}{\sqrt{2}} \left(\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array} \right), \quad D_2 = \left(\begin{array}{cc} 1 & 0 \\ 0 & -i \end{array} \right).$$

7. Concluding remarks

The question whether the maximal number $N+1$ can be attained for a composite dimension N, where N is not prime nor a power of a prime, still remains an open problem. The answer is not known even for the simplest case $N=6$ where $N+1=7$. A simple argument [19] leads to 3 such bases. Some numerical attempts to find further mutually unbiased bases were not successful. So it remains unclear whether it is indeed possible to reach the maximal number $N+1$ of them for the Hilbert space of dimension 6 and in other composite dimensions as well.

Although the relation between the eigenvectors of $Q_N^i P_N^j$ and mutually unbiased bases was observed e.g. in [19], the relation between the decomposition of the phase space $\mathbb{Z}_N \times \mathbb{Z}_N$ whose elements correspond to cosets in the finite Heisenberg group and the existence of mutually unbiased bases has been left unnoticed so far. We were thus able to give an independent constructive proof of Theorem 2 using group theory. However, the proof heavily depends on properties that are a consequence of N being a prime. It might be interesting to investigate whether our procedure could be applied in arbitrary dimensions and whether it would give us some hints as to the existence or non-existence of the maximal number of mutually unbiased bases in composite dimensions.

References

[1] Schwinger J 1960 Unitary operator bases *Proc. Nat. Acad. Sci. U.S.A.* **46** 570–579, 1401–1415
[2] Schwinger J 1970 *Quantum Kinematics and Dynamics* (New York: Benjamin) pp 63–72
[3] Kraus K 1987 Complementary observables and uncertainty relations *Phys. Rev. D* **35** 3070–3075
[4] Ivanović I D 1981 Geometrical description of quantum state determination *J. Phys. A: Math. Gen.* **14** 3241–3245
[5] Wootters W K 1986 Quantum mechanics without probability amplitudes *Found. Phys.* **16** 391–405
[6] Wootters W K and Fields B D 1989 Optimal state-determination by mutually unbiased measurements *Ann. Phys. (N.Y.)* **191** 363–381

[7] Nielsen M A and Chuang I L, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge 2003

[8] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145–195

[9] Nikolopoulos G M and Alber G 2005 Security bound of two-basis quantum-key-distribution protocols using qudits *Phys. Rev. A* **72** 032320

[10] Wootters W K 1987 A Wigner-function formulation of finite-state quantum mechanics *Ann. Phys. (N.Y.)* **176** 1–21

[11] Weyl H 1931 *The Theory of Groups and Quantum Mechanics* (New York: Dover) pp 272–280

[12] Tolar J 1977 *Quantization Methods* lecture notes, Institut für Theoretische Physik der Technischen Universität Clausthal

[13] Šťovíček P and Tolar J 1984 Quantum mechanics in a discrete space-time *Rep. Math. Phys.* **20** 157–170

[14] Mackey G W 1968 *Induced Representations and Quantum Mechanics* (New York: Benjamin)

[15] Vourdas A 2004 Quantum systems with finite Hilbert space *Rep. Progr. Phys.* **67** 267–320

[16] Vourdas A 2007 Quantum systems with finite Hilbert space: Galois fields in quantum mechanics *J. Phys. A: Math. Theor.* **40** R285–R331

[17] Balian R and Itzykson C 1986 Observations sur la mécanique quantique finie *C. R. Acad. Sci. Paris* **303** Série I, n. 16, 773–777

[18] Patera J and Zassenhaus H 1988 The Pauli matrices in n dimensions and finest gradings of simple Lie algebras of type A_{n-1} *J. Math. Phys.* **29** 665–673

[19] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 A new proof for the existence of mutually unbiased bases *Algorithmica* **34** 512–528; preprint quant-ph/0103162

[20] Klappenecker A and Rötteler M 2004 *Constructions of Mutually Unbiased Bases* Lecture Notes in Computer Science, Vol. 2984 (Berlin: Springer); preprint quant-ph/0401155

[21] Berndt B C, Evans R J and Williams K S 1998 *Gauss and Jacobi sums*, Canadian Mathematical Society, Series of Monographs and Advanced Texts, Vol. 21 (Wiley–Interscience Publication)

[22] Havlíček M, Patera J, Pelantová E and Tolar J 2002 Automorphisms of the fine grading of $sl(n,\mathbb{C})$ associated with the generalized Pauli matrices *J. Math. Phys.* **43** 1083-1094; preprint math-ph/0311015

[23] Novotný P and Hrivnák J 2005 On orbits of the ring $\mathbb{Z}_n^m$ under action of the group $SL(m,\mathbb{Z}_n)$ *Acta Polytechnica* **45** No. 5, 39–43

[24] Vourdas A 1996 The angle-angular momentum quantum phase space *J. Phys. A: Math. Gen.* **29** 4275–4288