# BACHELOR’S THESIS

# OPTIMAL DETERMINATION OF STATES OF D-LEVEL QUANTUM SYSTEMS

Petr Šulc

June 1, 2006

*Název práce:*
**Optimální určování stavů d-hladinových kvantových soustav**

*Autor:* Petr Šulc

*Obor:* Matematické inženýrství

*Zaměření:* Matematická fyzika

*Druh práce:* Bakalářská práce

*Vedoucí práce:* Prof. Ing. Jiří Tolar, DrSc., Katedra fyziky, Fakulta jaderná a fyzikálně inženýrská, České vysoké učení technické v Praze

*Konzultant:* Prof. Ing. Igor Jex, DrSc., Katedra fyziky, Fakulta jaderná a fyzikálně inženýrská, České vysoké učení technické v Praze

*Abstrakt:* Nejprve jsou uvedeny základní pojmy z kvantové teorie (čisté stavy, matice hustoty, pozorovatelné) a blíže prozkoumány matice hustoty na konečně rozměrných Hilbertových prostorech. Poté je rozebrán problém optimálního určování stávů kvantového systému, což vede k definici mutually unbiased bází. Je uveden jejich tvar pro prvočíselné dimenze. Nakonec je prezentován alternativní důkaz existence $N + 1$ mutually unbiased bází v Hilbertových prostorech o prvočíselné dimenzi $N$ za využití Pauliho grupy a vektorového prostoru $\mathbb{Z}_N \times \mathbb{Z}_N$.

*Klíčová slova:* kvantová mechanika, určování stavů, mutually unbiased báze, matice hustoty, Pauliho grupa

*Title:*
**Optimal determination of states of d-level quantum systems**

*Author:* Petr Šulc

*Abstract:* A basic overview of quantum theory fundamentals (pure states, density matrix, observables) is presented, then density matrices in finite dimensional Hilbert spaces are examined in more detail. Then the problem of optimal quantum state determination is dealt with. This leads to definition of mutually unbiased bases. An explicit form of such bases for prime dimensions is given. An alternative proof of existence of $N + 1$ mutually unbiased bases in Hilbert spaces of prime dimension $N$ is given by exploiting the Pauli group and vector space $\mathbb{Z}_N \times \mathbb{Z}_N$.

*Key words:* quantum mechanics, state determination, mutually unbiased bases, density matrix, Pauli group

# Acknowledgements

I would like to thank to prof. Jiří Tolar for support, consultations and ideas concerning mutually unbiased measurements. I also thank to prof. Edita Pelantová and RNDr. Vojtěch Petráček for consultations.

# Contents

# Introduction

The problem of optimal quantum state determination is closely related to mutually unbiased measurements. The aim of this work is to present a basic overview of quantum mechanics in finite dimensions and then proceed to the problem of state determination and mutually unbiased measurements. Relations between the Pauli group $\Pi_N$, vector space $\mathbb{Z}_N \times \mathbb{Z}_N$ and the existence of mutually unbiased bases in prime dimensions $N$ shall be examined too.

# Chapter 1

# Fundamental notions of quantum theory

Quantum mechanics provides us with a mathematical framework for the development of physical theories. The fundamental role in quantum mechanics is played by vectors in a Hilbert space:

**Definition 1** (Hilbert space)**.** Hilbert space is a vector space with inner product and complete with respect to the metric induced by the inner product.

Hilbert space $\mathcal{H}$ represents the state space of a given physical system, meaning that every state of the system corresponds to a vector from $\mathcal{H}$. According to classical mechanics it is possible to determine a result of any measurement performed at time *t* on a system consisting of *N* mass points once we know its 3*N* coordinates and 3*N* momenta that describe the system at the same time *t*. While in quantum theory, one can give only probabilities of outcomes of a given measurement.

## 1.1 Pure states

Hilbert space that is often encountered in quantum mechanics is $\mathbf{L}^2(\mathbb{R}^3)$, an infinite-dimensional vector space composed of functions $f(x, y, z)|x, y, z \in \mathbb{R}$ such that

$$\|f\|^2 = \int_{\mathbb{R}^3} |f|^2 < +\infty$$

and with inner product defined as $\langle f|g\rangle = \int_{\mathrm{R}^3} \overline{f} g$.

However, for quantum systems with a finite dimensional Hilbert space, for example describing the spin of a particle, we can use the vector space $\mathbb{C}^n$ which is the Hilbert space with inner product $\langle \psi_1|\psi_2\rangle = \sum_i^n \overline{\alpha_i}\beta_i$ and $\|\psi\|^2 = \sum_i^n |\alpha_i|^2$. The notation used to describe vectors from Hilbert space was introduced by P.A.M. Dirac [1]: $|\psi\rangle$ is called a *ket vector* or simply a *ket*. In a finite *n*-dimensional Hilbert space, $|\psi\rangle$ may be expressed as:

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

An inner product of two vectors, denoted as $\langle\psi_1|\psi_2\rangle$ can be regarded as a product of two vectors $\langle\psi_1|$ and $|\psi_2\rangle$, where $\langle\psi_1|$ is called a *bra* vector. In a finite dimensional Hilbert space, it can be expressed as:

$$\langle\psi_1| = \begin{pmatrix} \overline{\alpha_1} & \overline{\alpha_2} & \cdots & \overline{\alpha_n} \end{pmatrix}.$$

There exists an unambiguous antilinear one-to-one correspondence of bra vectors and kets:

$$\begin{aligned} \langle\psi_1| &\leftrightarrows |\psi_1\rangle, \\ \overline{\alpha_1}\langle\psi_1| + \overline{\alpha_2}\langle\psi_2| &\leftrightarrows \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle. \end{aligned}$$

The probability of finding a system which is in state $|\psi\rangle$ in a state $|a\rangle$, or in other words, the transition probability is given by:

$$p_{\psi\rightarrow a} = \frac{|\langle\psi|a\rangle|^2}{\|\psi\|^2\|a\|^2}. \tag{1.1}$$

The measurement can be realized by an ideal 'filter' $F_a$ applied on our quantum system, which allows only system in state $|a\rangle$ to go through. The results we can obtain from quantum mechanics are always in terms of probabilities, and since all multiples $\alpha|\psi\rangle$ ($\alpha \in \mathbb{C}$) correspond to the same state (i.e. one dimensional span of vector $|\psi\rangle$) we usually restrict only to vectors normalized to 1. If we want to describe $F_a$ as an operator in Hilbert space, it is an orthogonal projector to one-dimensional subspace span($|a\rangle$). Using notation introduced by Dirac, it can be expressed as

$$P_a = |a\rangle\langle a|.$$

Assuming that we work only with vectors normalized to 1, the normalized state of the system after applying the filter $F_a$ (realized by applying operator $P_a$ in Hilbert space) will be

$$\frac{P_a|\psi\rangle}{\|P_a|\psi\rangle\|} = e^{i\varphi}|a\rangle. \tag{1.2}$$

Multiplying a vector by complex unity does not change the state represented by the vector nor its norm. It should be pointed out that since we assume $\|a\| = \|\psi\| = 1$, we can see by comparing (1.1) and (1.2) that the probability of finding $|\psi\rangle$ in a state $|a\rangle$ is

$$p_{\psi\to a} = \|P_a|\psi\rangle\|^2 = |\langle\psi|a\rangle|^2 = \langle\psi|P_a|\psi\rangle. \tag{1.3}$$

In the last equation we used the fact that $P_a$ is an orthogonal projector, meaning that $P_a^\dagger = P_a = P_a^2$.

## 1.2 Observables

When we make an observation we measure some dynamical variable. The result of such a measurement must be a real number. When we measure some physical quantity A of a system in state $|\psi\rangle$ and we always obtain result $\lambda$, we say that state $|\psi\rangle$ is an eigenstate of observable A belonging to eigenvalue $\lambda$. The term *observable* is usually used in a sense of a physical quantity that can be measured, but it is also often used as a reference to a particular selfadjoint operator in Hilbert space. By performing a measurement of observable $A$ on a system in state $|\psi\rangle$ we mean an application of a linear operator $A$ that is assigned to a particular physical quantity on a vector corresponding to the given state: $A|\psi\rangle$. In general case we can't speak of an observable having a value for a particular state $|\psi\rangle$, but we can speak of its mean value for the state $|\psi\rangle$. According to quantum mechanics, the average value of observable $A$ in a system in state $|\psi\rangle$ is given by:

$$\langle A\rangle_\psi = \langle\psi|A|\psi\rangle. \tag{1.4}$$

$\langle\psi|A|\psi\rangle$ is a standard notion used for the inner product of $\langle\psi|A\psi\rangle$ because $A$ is assumed selfadjoint and therefore it doesn't matter at which side of the inner product it is standing.

In a finite dimensional Hilbert space $\mathcal{H} = \mathbb{C}^n$ every observable $A$, being a selfadjoint (or Hermitian) operator, can be expressed (by the spectral theorem) as a linear combination of orthogonal projectors:

$$A = \sum_{j=0}^{n} \lambda_j P_{a_j} = \sum_{j=0}^{n} \lambda_j |a_j\rangle\langle a_j|, \tag{1.5}$$

where $\lambda_j$ are eigenvalues (not necessarily distinct) corresponding to eigenvectors $|a_j\rangle$, which form an orthonormal basis of $\mathcal{H} = \mathbb{C}^n$. The possible outcomes of a measurement of an observable are its eigenvalues. For example, if a system is in state $|\psi\rangle = \alpha|a_j\rangle + \beta|a_i\rangle$ that corresponds to a superposition of two eigenvectors belonging to two different eigenvalues $\lambda_j$ and $\lambda_i$, the probability of obtaining $\lambda_j$ is $|\alpha|^2$ and the probability of obtaining $\lambda_i$ is $|\beta|^2$. We assume that $\||\psi\rangle\| = 1$, hence $|\alpha|^2 + |\beta|^2 = 1$.

As was mentioned before, every observation we make on a quantum system affects the system. So if we obtain $\lambda_j$ as a result of the measurement, the system is then in a state described by eigenvector that corresponds to obtained eigenvalue. In order to determine the state of the system uniquely, it might be necessary to perform several different measurements. It is also required that operators corresponding to these measurements commute with each other (i.e. it doesn't matter in which order the measurements are performed). A set of measurements that commute with each other and can determine the state uniquely is called complete.

## 1.3 Density matrix

So far, we used the description of states of a system by so called 'pure states', meaning that the state of a system was described by a vector from the state space. However, while working with quantum systems, we also have to face a situation when we need to describe a system that is not capable of producing the same pure states for multiple measurements, for example when we have a source of partially polarized light. We may say that the information on such a system is less than a maximum.

### 1.3.1 Definition and formulas for mean values

In order to describe a quantum system whose state is not completely known, a mixed state tool known as the *density operator*, *density matrix* or *statistical operator* was developed by von Neumann [2]. For example, imagine a quantum system is in one of a number of states $|\psi_i\rangle$ with respective probabilities $p_i \in [0,1]$. The states $|\psi_i\rangle$ are not necessarily mutually orthogonal. The set $\{p_i, |\psi_i\rangle\}$ is then called an *ensemble of pure states* and the density operator $\rho$ is defined ([3], [4], [5]) as:

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad \sum_i p_i = 1. \tag{1.6}$$

The statistical operator is also well defined for separable Hilbert spaces with infinite dimension [6].

In the previous section, we defined mean value of operator $A$ for a system in a pure state $|\psi_i\rangle$. For a system described by a density matrix $\rho$, the mean value for operator $A$ represented by matrix $A$ can be obtained as follows:

$$\begin{aligned}\langle A\rangle_\rho = \sum_i p_i \langle A\rangle_{\psi_i} &= \sum_i p_i \langle\psi_i|A\psi_i\rangle = \sum_i p_i \sum_{m,n} A_{m,n}\overline{\psi_i^{(m)}}\psi_i^{(n)} = \\ &= \sum_{m,n} A_{m,n}\rho_{n,m} = \sum_m (A\rho)_{m,m} = \mathrm{Tr}(A\rho),\end{aligned}$$

where $\psi_i^{(n)}$ denotes $n$-th component of vector $|\psi_i\rangle$. We also used the fact that $\rho_{nm} = \sum_i p_i \overline{\psi_i^{(m)}}\psi_i^{(n)}$ which follows from the definition (1.6). Thus we have shown that

$$\langle A\rangle_\rho = \mathrm{Tr}(A\rho). \tag{1.7}$$

We can regard the density matrix as a minimum set of input data which serves to calculate the mean value of any operator for a quantum system. The knowledge of the mean values $\langle A_j \rangle$ of as many independent operators $A_j$ as there are independent parameters in the matrix $\rho$ enables us to obtain such data, meaning that by solving an equation (1.7) for the set of operators $A_j$ we can determine the density matrix $\rho$.

### 1.3.2 General properties of the density matrix

We will now have a closer look at the limitations on the elements $\rho_{nm}$ of the density matrix. All these requirements are fulfilled by the definition as presented in (1.6)

1. Because $\langle A \rangle$ must be real for every Hermitian operator, $\rho$ has to be Hermitian, too.
2. In order for the operator $\rho$ to be normalized, its trace has to be equal to one, because

   $$\mathrm{Tr}(\rho) = \sum_i p_i \mathrm{Tr}\left(|\psi_i\rangle\langle\psi_i|\right) = \sum_i p_i = 1$$

   and we naturally assume that the sum of all probabilities is equal to 1.
3. The condition that the eigenvalues of operator $\rho$ play the role of probabilities requires them to be all $\geq 0$, meaning that $\rho$ has to be positive.

Density matrices form a convex subset of a vector space of Hermitian matrices. Any convex combination of density matrices will be again a density matrix and all of the listed conditions will be fulfilled. Density matrix offers a more general description of a quantum system than pure states. Actually, the basic postulates of quantum mechanics can be reformulated using the density matrix formalism. The probability of finding a system described by density matrix $\rho$ in the state $|a\rangle$ is:

$$p_a = \langle a|\rho|a\rangle. \tag{1.8}$$

The previous formula was derived using formula (1.6) and (1.1) as follows:

$$p_a = \sum_i p_i p_{\psi_i \to a} = \sum_i p_i \langle a|\psi_i\rangle\langle\psi_i|a\rangle. \tag{1.9}$$

Formula (1.8) can be rewritten using an orthogonal projector $P_a = |a\rangle\langle a|$. The mean value of this operator will be equal to the probability of measuring state $|a\rangle$:

$$p_a = \langle a|\rho|a\rangle = \mathrm{Tr}(\langle a|\rho|a\rangle) = \mathrm{Tr}(P_a \rho). \tag{1.10}$$

When we perform a measurement of a system in the state described by density matrix $\rho$, we need to know how to transform the density matrix to describe the state of the system after the measurement. We use the fact that if the initial state was described by vector $|\psi_i\rangle$ then the state after obtaining the result $a$ is

$$|\psi_i^a\rangle = \frac{P_a|\psi_i\rangle}{\|P_a|\psi_i\rangle\|} = \frac{P_a|\psi_i\rangle}{\sqrt{p_{\psi_i \to a}}}. \tag{1.11}$$

The probability of passing through the filter $F_a$, meaning the probability that we find the system described by $\rho$ in a state $|a\rangle$ was given in equation (1.9). Now, the probability of the system being in a normalized state (1.11) after performing the measurement is

$$\frac{p_i p_{\psi_i \to a}}{p_a} \tag{1.12}$$

Therefore, the density matrix $\rho$ is transformed to

$$\rho' = \sum_i \frac{p_i p_{\psi_i \to a}}{p_a} \frac{P_a|\psi_i\rangle\langle\psi_i|P_a}{p_{\psi_i \to a}} = \frac{P_a \rho P_a}{\text{Tr}(P_a \rho)}. \tag{1.13}$$

Density matrices provide a more general way of describing a quantum system than pure states. Moreover, pure states represent special cases of density matrices- in fact, they lie on the boundary of the convex set of all density matrices. The following lemma shows how to distinguish whether a given density matrix represents a pure or a mixed state:

**Lemma 1.** State represented by density matrix $\rho$ is pure if and only if $\text{Tr}(\rho^2) = 1$. Otherwise $\text{Tr}(\rho^2) < 1$.

*Proof.* If the state is pure, then the density matrix is a projector onto a one-dimensional subspace with eigenvalue 1, so $\rho^2 = \rho$, so $\text{Tr}(\rho) = 1$. As was mentioned before, $\rho$ can have only non-negative eigenvalues less or equal to one and the sum of them has to be equal to one. If $\lambda$ is an eigenvalue of $\rho$, then $\lambda^2$ is an eigenvalue of $\rho^2$ and would be $< \lambda$ unless it is one. Since $\text{Tr}(\rho^2)$ is equal to the sum of all its eigenvalues and is $< 1$, then $\rho$ cannot have eigenvalue 1 and therefore cannot be a projector onto a one-dimensional state, so the state that it represents has to be mixed. □

Since $\rho$ is a normal operator, it can be diagonalized in an orthonormal basis. However, the representation of a given density matrix by an ensemble is not unique in general. That is, an infinity of different representations as convex combinations of pure states can be constructed for a given state in cases when mixed pure states are not mutually orthogonal or the eigenvalues of $\rho$ are degenerate [7].

### 1.3.3 Expansion in orthogonal operators

So far, we worked with Hilbert spaces $\mathcal{H}$ where pure states corresponded to vectors in $\mathcal{H}$. After introducing the density matrix formalism, it is also useful to define a Hilbert space where the actual vectors will be operators, so that for an $n$-dimensional Hilbert space $\mathcal{H}^n$, we will construct complex $n^2$-dimensional Hilbert space $\mathcal{H}^{n^2}$ whose vectors will be operators in $\mathcal{H}^n$. The inner product in this space is defined as:

$$\langle U_i | U_j \rangle = \mathrm{Tr}(U_i^\dagger U_j) \tag{1.14}$$

We can find an orthonormal set of $n^2$ operators $U_i$ and expand the density matrix $\rho$ in this operator basis:

$$\rho = \sum_i \langle \rho | U_i \rangle U_i = \sum_i \mathrm{Tr}(\rho U_i) U_i = \sum_i \langle U_i \rangle U_i \tag{1.15}$$

**Example 1** (Density matrix in a two dimensional Hilbert space)**.** In a two dimensional Hilbert space $\mathbb{C}^2$ density matrix will be a $2 \times 2$ Hermitian matrix. As an operator basis, we will take the following matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.16}$$

where $I$ is a unity matrix and $\sigma_x, \sigma_y, \sigma_z$ are the Pauli matrices. This basis is orthogonal with respect to the inner product defined in (1.15). In order to fulfil the normalization condition $\mathrm{Tr}(\rho) = 1$, the density matrix $\rho$ must be in a form

$$\rho = \frac{1}{2}(I + P_x\sigma_x + P_y\sigma_y + P_z\sigma_z) = \frac{1}{2}\begin{pmatrix} 1 + P_z & P_x - iP_y \\ P_x + iP_y & 1 - P_z \end{pmatrix}. \tag{1.17}$$

From the fact that $\rho$ has to be positive (i.e. its eigenvalues have to be $\geq 0$) we obtain, by Sylvester's criterion, the condition that $P_x^2 + P_y^2 + P_z^2 \leq 1$. According to lemma 1, the state represented by this density matrix will be pure if and only if $P_x^2 + P_y^2 + P_z^2 = 1$. Also, $P_x, P_y, P_z$ have to be real, because $\langle \sigma_j \rangle = \mathrm{Tr}(\rho\sigma_j) = P_j, j \in \{x, y, z\}$. Density matrix (1.17) describes, e.g., partially polarized light, or a beam of partially polarized spin $\frac{1}{2}$ particles.

## 1.4 Tensor products

Suppose we have Hilbert spaces $\mathcal{V}$ and $\mathcal{W}$. Then we can define a Hilbert space $\mathcal{H}$ as their tensor product, which is denoted as

$$\mathcal{H} = \mathcal{V} \otimes \mathcal{W}.$$

It is a linear span of $|v\rangle \otimes |w\rangle$, where $|v\rangle \in \mathcal{V}$ and $|w\rangle \in \mathcal{W}$. If the set of vectors $|e_j^{\mathcal{V}}\rangle$ and $|e_i^{\mathcal{W}}\rangle$ form orthonormal bases of $\mathcal{V}$ and $\mathcal{W}$, respectively, then the set $|e_i^{\mathcal{W}}\rangle \otimes |e_j^{\mathcal{V}}\rangle$ forms an orthonormal basis of $\mathcal{V} \otimes \mathcal{W}$. In finite dimensional spaces, if $\dim\mathcal{V} = n$ and $\dim\mathcal{W} = m$, then $\dim\mathcal{V} \otimes \mathcal{W} = mn$. The following relations are satisfied in $\mathcal{V} \otimes \mathcal{W}$ by definition:

1. For $\lambda \in \mathbb{C}, |v\rangle \in \mathcal{V}, |w\rangle \in \mathcal{W}$

$$\lambda(|v\rangle \otimes |w\rangle) = (\lambda|v\rangle) \otimes |w\rangle = |v\rangle \otimes (\lambda|w\rangle). \tag{1.18}$$

2. For arbitrary vectors $|v_1\rangle, |v_2\rangle \in \mathcal{V}, |w\rangle \in \mathcal{W}$

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle. \tag{1.19}$$

3. If $A$ and $B$ are operators acting in $\mathcal{V}$ and $\mathcal{W}$ respectively, then one can define an operator $A \otimes B$ acting in $\mathcal{V} \otimes \mathcal{W}$ as

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A|v\rangle \otimes B|w\rangle. \tag{1.20}$$

4. The inner product in $\mathcal{V} \otimes \mathcal{W}$ is defined by using the inner products in $\mathcal{V}$ and $\mathcal{W}$ as

$$\left\langle \sum_i \alpha_i |v_i\rangle \otimes |w_i\rangle \middle| \sum_j \beta_j |\tilde{v_j}\rangle \otimes |\tilde{w_j}\rangle \right\rangle \equiv \sum_{i,j} \overline{\alpha_i} \beta_j \langle v_i|\tilde{v_j}\rangle \langle w_i|\tilde{w_j}\rangle. \tag{1.21}$$

The above definitions can be extended to a product of $n$ Hilbert spaces: $\mathcal{V}_1 \otimes \mathcal{V}_2 \otimes \ldots \otimes \mathcal{V}_n$. Tensor product of Hilbert spaces is usually used to describe a composite quantum system.

# Chapter 2

# Quantum systems in finite dimensional Hilbert spaces

In the previous chapter, basic apparatus was introduced to describe a quantum system. We assumed that we are working in a finite dimensional Hilbert space. However, the relations presented in the previous chapter have their equivalents in the infinite dimensional Hilbert spaces as well, but are generally more complicated. In the infinite dimensional Hilbert space $\mathbf{L}^2(\mathbb{R}^3)$, coordinate operators $Q_i$ and momentum operators $P_j$ fulfil the following relations:

$$
\begin{aligned}
[P_i, P_j] &= P_iP_j - P_jP_i = 0, && (2.1)\\
[Q_i, Q_j] &= Q_iQ_j - Q_jQ_i = 0, && (2.2)\\
[Q_i, P_j] &= Q_iP_j - P_jQ_i = i\hbar\delta_{ij}I, && (2.3)
\end{aligned}
$$

where $i, j \in \{1, 2, 3\}$. The relations are known as the Heisenberg commutation relations and can be understood as the quantal analogue of Poisson brackets from classical mechanics:

$$
\begin{aligned}
\{q_r, q_s\} &= 0, && (2.4)\\
\{p_r, p_s\} &= 0, && (2.5)\\
\{q_r, p_s\} &= \delta_{rs}. && (2.6)
\end{aligned}
$$

In finite dimensional Hilbert spaces, we use Hermitian matrices to represent linear operators. From equation (2.3) it can be seen that we can never represent operators $P_i, Q_i$ in a finite dimension that would fulfil such a relation, because taking matrix traces of both sides of (2.3) would lead to a contradiction:

$$
\mathrm{Tr}(Q_iP_i - P_iQ_i) = 0 \neq i\hbar\mathrm{Tr}(I). \qquad (2.7)
$$

However, in a finite $N$-dimensional Hilbert space, with an orthonormal basis $B = \{|\mathit{0}\rangle, |\mathit{1}\rangle, \ldots |N-\mathit{1}\rangle\}$, we can establish a group generated by matrices $Q_N, P_N$ which are defined by the relations

$$Q_N|j\rangle = \omega_N^j|j\rangle, \tag{2.8}$$

$$P_N|j\rangle = |j+\mathit{1} \mod N\rangle. \tag{2.9}$$

Here $\omega_N$ is the primitive $N$-th root of unity, we shall take $e^{\frac{2\pi i}{N}}$. The unitary operators $P_N$ and $Q_N$ are represented by unitary matrices:

$$Q_N = \text{diag}\left(1, \omega_N, \omega_N^2, \cdots, \omega_N^{N-1}\right) \tag{2.10}$$

and

$$P_N = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \tag{2.11}$$

In finite dimensional quantum mechanics, the unitary matrices $P_N$ and $Q_N$ play the roles of exponential operators of position and momentum in the coordinate representation [8]. They fulfil the following algebraic relations, analogous to relations for Weyl's exponential form of Heisenberg's commutation relations:[1]

$$\omega_N P_N Q_N = Q_N P_N \tag{2.12}$$

$$\omega_N P_N = P_N \omega_N \tag{2.13}$$

$$\omega_N Q_N = Q_N \omega_N \tag{2.14}$$

$$P_N^N = Q_N^N = \omega_N^N = I. \tag{2.15}$$

$P_N$ and $Q_N$ were first studied by Hermann Weyl [9]. The cyclic group

$$\mathbb{Z}_N = \{0, 1, \ldots N-1\}$$

acts as a configuration space for our finite dimensional quantum system. The elements of

[1] Note that in the infinite Hilbert space $\mathcal{H} = \mathbf{L}^2(\mathbb{R})$, the action of of $e^{itP}$ and $e^{isQ}$ for $t, s \in \mathbb{R}$ is:

$$\begin{aligned} \left(e^{itP}|\psi\rangle\right)(x) &= |\psi\rangle(x+t) \quad |\psi\rangle \in \mathbf{L}^2(\mathbb{R}) \\ \left(e^{isQ}|\psi\rangle\right)(x) &= e^{isx}|\psi\rangle(x) \quad |\psi\rangle \in \mathbf{L}^2(\mathbb{R}) \end{aligned}$$

this group can be assigned to vectors from the basis $B = \{|\mathit{0}\rangle, |\mathit{1}\rangle, \ldots |N - \mathit{1}\rangle\}$. Note that there exists a natural transitive action of $\mathbb{Z}_N$ on $\mathbb{Z}_N$, an addition modulo $N$. The action of operators $U(k) = P_N^k$ on a vector $|j\rangle$ from basis $B$ is then

$$U(k)|j\rangle = P_N^k|j\rangle = |j + k \mod N\rangle \tag{2.16}$$

The $\mathbb{Z}_N$ analogue of the Fourier transformation, which allows us the transition from the coordinate representation (corresponding to the above matrix forms) to the momentum representation, is given by the unitary Sylvester matrix $S$:

$$S_{jk} = \frac{\omega_N^{jk}}{\sqrt{N}}. \tag{2.17}$$

The following relations are then fulfilled [10]:

$$S^{-1}P_N S = Q_N^{-1} = Q_N^{N-1} = Q_N^\dagger, \quad S^{-1}Q_N S = P_N \tag{2.18}$$

i.e. finite Fourier transform diagonalizes the momentum operator.

**Theorem 1.** The set of $N^2$ unitary matrices $B = \left\{Q_N^a P_N^b | a, b = \{0, 1, \ldots, N-1\}\right\}$ constitutes an orthogonal basis of Hilbert space of all complex matrices $\mathcal{H}^{N^2}$.

*Proof.* This theorem can be easily proved by showing that the matrices $Q_N^a P_N^b$ and $Q_N^c P_N^d$ are orthogonal for all different pairs of coefficients $((a, b) \neq (c, d))$. The inner product (defined by (1.15)) of such unitary matrices is then:

$$\text{Tr}\left(\left(Q_N^a P_N^b\right)^\dagger Q_N^c P_N^d\right) = \text{Tr}\left(\left(P_N^b\right)^\dagger \left(Q_N^a\right)^\dagger Q_N^c P_N^d\right) = \text{Tr}\left(P_N^d \left(P_N^b\right)^\dagger \left(Q_N^a\right)^\dagger Q_N^c\right) \tag{2.19}$$

where we used the invariance of trace under cyclic permutation of matrices. We will now suppose without loss of generality that $a \geq c$, $b \geq d$. Then:

$$P_N^d \left(P_N^b\right)^\dagger \left(Q_N^a\right)^\dagger Q_N^c = \left(P_N^{b-d}\right)^\dagger \left(Q_N^{a-c}\right)^\dagger \tag{2.20}$$

and if $b \neq d$, we will have a matrix $\left(P_N^{b-d}\right)^\dagger$ (with diagonal elements equal to zero) multiplied by a a diagonal matrix $\left(Q_N^{a-c}\right)^\dagger$ which gives a traceless matrix. In case $b = d$, we will take the trace of a matrix with powers of $e^{\frac{2\pi i}{N}}$ on its diagonal, which would give us again $0$, because:

$$\sum_{k=0}^{N-1} \left(e^{\frac{2\pi i m}{N}}\right)^k = \frac{\left(e^{\frac{2\pi i m}{N}}\right)^N - 1}{e^{\frac{2\pi i m}{N}} - 1} = 0, \quad \forall m \in \mathbb{N} \tag{2.21}$$

We can therefore summarize that:

$$\text{Tr}\left(\left(Q_N^a P_N^b\right)^\dagger Q_N^c P_N^d\right) = 0 \quad \forall (a,b) \neq (c,d), \quad (a,b) \in \mathbb{Z}_N \times \mathbb{Z}_N \tag{2.22}$$

□

The finite group

$$\Pi_N = \left\{\omega_N^l Q_N^i P_N^j | l,i,j = 0,1,2,\ldots,N-1\right\}, |\Pi_N| = N^3 \tag{2.23}$$

is called the *Pauli group* or the *finite Heisenberg-Weyl group*. It has applications in finite dimensional quantum mechanics and is also useful in connection with mutually unbiased bases, as we shall see in the next chapters.

# Chapter 3

# Quantum state determination

## 3.1 Number of independent parameters

We will now discuss the number of independent parameters that identify a state of a quantum system with an $N$-dimensional Hilbert space. A pure state is identified by $N$ complex numbers (which are its components $c_i$ in a given basis), but the number of meaningful real parameters is reduced from $2N$ to $2N-1$ by the normalization condition $\||\psi\rangle\|^2 = \sum_i |\alpha_i|^2 = 1$, and further to $2N-2$ because the phase of the state vector $|\psi\rangle$ is physically meaningless. An $N \times N$ density matrix has $N^2$ elements. Because it is Hermitian, the number of real parameters is reduced to $N^2$. This number is further reduced by the normalization condition Tr$(\rho) = 1$ to $N^2-1$ independent parameters.

Now, we should consider the number of measurements that are necessary to determine the density matrix. We suppose that we have an ensemble of identically prepared states large enough to perform all necessary measurements. We are measuring a state of an $N$-dimensional quantum system. One complete measurement will give us $N-1$ independent probabilities of possible outcomes. Since the number of necessary real parameters to determine the density matrix is $N^2-1$, we need $\frac{N^2-1}{N-1} = N+1$ different measurements.

The number of $N+1$ necessary measurements can also be obtained by a slightly different argument. Suppose we have a set of $m$ observables $A_i$. We want to find out the minimal number of these observables that have to be measured on the system in order to identify its state. As was mentioned before, we suppose we have a large ensemble which we observe. Now, every observable $A_i$ can be expressed in terms of orthogonal projectors $P_k^i$ which project onto vectors $|\psi_k\rangle$, respectively, and which form an orthonormal basis. Note that these vectors are in general different for each $A_i$

$$A_i = \sum_{k=1}^{N} \alpha_k^i P_k^i.$$

Measuring the mean value of observable $A_i$ can be understood as measuring the mean values of projectors $P_k^i$ (i.e. probabilities of measuring $|\psi_k\rangle$). So for every observable $A_i$ we obtain $N$ equations. Since the sum of all probabilities has to be equal to one, only $N-1$ out of $N$ equations can be independent. Every observable will thus provide $N-1$ linearly independent equations (at most). Now, we need to solve a system of linear equations for $N^2-1$ independent real parameters, so we need the same number of linearly independent equations. Assuming that every observable's mean value will provide a set of equations that are not a linear combination of equations provided by other observables, we get

$$m(N-1) = N^2 - 1$$

where $m$ is the minimal number of necessary observables to be measured, which is then $N+1$.

From measuring the probabilities of possible outcomes we are able to reconstruct the density matrix that describes the system. For example, we can imagine the measurements on a beam of partially polarized photons. We perform measurements of selected observables, determine the probabilities of possible outcomes and then compute the polarization density matrix that corresponds to obtained probabilities. However, we will never have an infinite number of samples, and therefore the results of our measurement will always include some statistical error because the probabilities that we shall obtain from measurements will not be necessarily equal to probabilities that are given for a system in a particular state described by density matrix $\rho$. The problem of choosing optimal observables in order to minimize this error will be discussed in the next section.

## 3.2 Optimal set of measurements

In the previous section, it was shown how we can reconstruct the density matrix by measuring probabilities of possible outcomes for a given observable. Those possible outcomes were represented by eigenvectors $|\psi_i\rangle$ of the corresponding operators, and the probabilities were equal to mean values of their orthogonal projectors $P_i$. Therefore, the problem of choosing the optimal observables is a problem of choosing an operator basis in $\mathcal{H}^{N^2}$.

In this section we shall reformulate the reasoning of Wootters and Fields [11]. They introduced a vector space of traceless Hermitian matrices. Instead of representing a state by its density matrix $\rho$, they use a matrix

$$Y_\rho = \rho - \frac{1}{N} I \tag{3.1}$$

where $I$ denotes a unit matrix. The inner product is the same as was defined in (1.15). The Hilbert space of all traceless Hermitian matrices will be denoted by $\mathcal{H}_s$. It has dimension $N^2-1$. The subspace of all matrices $Y_\rho$ such that $\rho = Y_\rho + \frac{1}{N} I$ is a density matrix will be denoted by $\mathcal{S}$ .

We also need to introduce a way in which we are going to quantify the amount of information that will be obtained after performing the measurements in order to find such a set of measurements that will actually maximize this information. To find such a suitable function, we will suppose that, as a result of our measurements, a certain set of 'probable states' will be obtained. The actual construction of such set will be given later. Volume of this set will be denoted as $V$, volume of space $\mathcal{S}$ will be given by $V_0$. We will impose several requirements on the information function. We expect it to be simple and monotonous and since it is called information function, the smaller the volume of probable states $V$, the higher value of the function and vice versa: we expect it to be in its minimum in case the set of probable states will be equal to the whole space of possible states $\mathcal{S}$. Such requirements are fulfilled e.g. by function:

$$f(V) = -\ln\left(\frac{V}{V_0}\right). \tag{3.2}$$

Before the measurement, the state can be anywhere in the set $\mathcal{S}$. Our goal is to find an operator $Y_\rho$ that describes the state, or, more precisely, to find a set of suitable operators $\tilde{Y}_\rho$ that include the desired $Y_\rho$ with a given probability, since we will never be able to determine the state with absolute precision because of statistical error. In other words, we shall obtain a probability distribution over the space $\mathcal{S}$. We found that a set of $N+1$ measurements is to be performed, where the $k$-th measurement is given by $N$ orthogonal projectors $P_i^k = |a_i^k\rangle\langle a_i^k|$, with the probabilities of outcomes given (as was shown in (1.10)) by

$$p_i = \text{Tr}(P_i^k \rho). \tag{3.3}$$

Because we are working with traceless matrices $Y_\rho = \rho - \frac{1}{N}I$ instead of density matrices, we will also use numbers $q_i = p_i - \frac{1}{N}$ instead of $p_i$. They can be obtained as

$$q_i = \text{Tr}(Y_\rho P_i^k) = \text{Tr}\left(\left(\rho - \frac{1}{N}I\right)P_i^k\right) = p_i - \frac{1}{N}. \tag{3.4}$$

Instead of $P_i^k$, we can use traceless operators $P_i^k - \frac{1}{N}I$, because they give the same

$$q_i = \text{Tr}(Y_\rho P_i^k) = \text{Tr}\left(Y_\rho\left(P_i^k - \frac{1}{N}I\right)\right). \tag{3.5}$$

Since the family of N operators $\left\{P_i^k - \frac{1}{N}I | i = 1,\ldots,N\right\}$ satisfies linear relation

$$\sum_i^N \left(P_i^k - \frac{1}{N}I\right) = I - I = 0, \tag{3.6}$$

it spans an $N-1$ dimensional subspace in $\mathcal{H}_s$ which will be denoted as $T_k$. The set of

$q_i$'s determines the projection of $Y_\rho$ on this subspace. Therefore, if we could determine the $q_i$'s with absolute precision, we would know the projection of state $Y_\rho$ to subspace $T_k$. However, because of impossibility of determining these values exactly, we will not have a projection to single point in subspace $T_k$, but rather we will have a distribution function over the subspace $T_k$. Geometrically spoken, the intersection of the measured state $Y_\rho$ with the subspace $T_k$ will spread according to a probability distribution function. The distribution function for a series of $M$ trials (corresponding to performing a measurement on $M$ members of the ensemble in our case) with probabilities of possible outcomes $p_1, p_2, \ldots, p_N$, respectively, is given by a multinomial distribution. Out of $M$ trials, the probability of obtaining the results $A_i$ with corresponding probabilities $p_i$'s exactly $k_i$ times $(k_1 + k_2 + \ldots + k_N = M)$ is

$$P_M(k_1, k_2, \ldots, k_N) = \frac{M!}{k_1!k_2!\ldots k_N!} p_1^{k_1} p_2^{k_2} \ldots p_N^{k_N} \tag{3.7}$$

However, in order to compute the volume $V$ approximately, for our purposes we will suppose that we have a large ensemble available and therefore we can use the fact that for sufficiently large $M$, the above distribution can be well approximated by a Gaussian distribution [12]:

$$P_M(k_1, k_2, \ldots, k_N) \approx \frac{e^{-\frac{1}{2}\sum_{i=1}^{N} q_i x_i^2}}{(2\pi M)^{\frac{N-1}{2}} \sqrt{p_1 p_2 \ldots p_N}}, \quad q_i = 1 - p_i, \quad x_i = \frac{k_i - M p_i}{\sqrt{M p_i q_i}}. \tag{3.8}$$

For the volume of 'probable' states $V$ on which our information function (3.2) depends, we take the volume of the smallest rectangular parallelepiped that encloses the region of all states for which the probability density exceeds its maximum value divided by $e$. We can assume that the probability of the outcome based on the outcomes of our measurements will be

$$\tilde{p_i} = \frac{k_i}{M},$$

where $k_i$ stands for the number of positive outcomes and $M$ is the number of measurements. The value of $\tilde{p_i}$ will lie in the interval

$$\tilde{p_i} \in [p_i - \Delta, p_i + \Delta],$$

where $2\Delta$ is equal to the length of interval where the probability density exceeds $\frac{1}{e}$ times its maximal value. Further, from (3.8) we can see that $k_i$'s that have probability higher than $\frac{1}{e}$ times the maximum of the Gaussian lie in the interval

$$k_i \in \left[ p_i M - \sqrt{2Mp_i}, p_i M + \sqrt{2Mp_i} \right].$$

Considering that the probability that we measure is $\tilde{p_i} = \frac{k_i}{M}$, it will lie in the interval

$$\tilde{p_i} \in \left[ p_i - \sqrt{\frac{2p_i}{M}}, p_i + \sqrt{\frac{2p_i}{M}} \right].$$

And since we take the smallest rectangular parallelepiped that encloses the volume of 'probable states' (i.e. those states whose probability exceeds $\frac{1}{e}$ times the maximum of Gaussian), then the uncertainty volume in subspace $T_k$ is given by

$$V_k = 2^{N-1} \left( \sqrt{\frac{2}{M}} \right)^{N-1} \sqrt{p_1 p_2 \ldots p_{N-1}}, \tag{3.9}$$

where we take into account only $N-1$ measured probabilities, the last one will be given by the condition $\sum_{i=1}^{N} \tilde{p_i} = 1$. Note that it does not matter whether we measure the uncertainty of $\tilde{p_i}$ or $\tilde{q_i} = \tilde{p_i} - \frac{1}{N}$, because they differ just by a constant. $k-$th measurement restricts the projection of unknown state to an $N-1$ dimensional subspace $V_k$ to a set of possible values, but leaves it unrestricted in the remaining $N^2 - N$ dimensions. The resulting uncertainty volume in space $\mathcal{S}$ is then given by the intersection of all these 'probable' volumes in $N+1$ subspaces. The uncertainty volume is given by the following equation:

$$V = \frac{V_1 V_2 \ldots V_{N+1}}{\text{vol}(T_1 T_2 \ldots T_{N+1})} \tag{3.10}$$

where $V_k$ stands for the uncertainty volume in subspace $T_k$ as defined by equation (3.9). The quantity vol$(T_1 T_2 \ldots T_{N+1})$ stands for the volume of an $(N^2 - 1)$ dimensional parallelepiped in $\mathcal{S}$, whose edges are unit vectors from orthonormal bases of subspaces $T_1, T_2, \ldots, T_{N+1}$. The actual volume depends on geometrical relations between vectors from different bases. It will reach its maximal value if these vectors are orthogonal. The total uncertainty volume is an intersection of all uncertainty volumes $V_i$. The total volume of the intersection is then given by the formula (3.10). We will now evaluate the infomation function (as defined in (3.2)) for the computed uncertainty volume $V$ in the whole space $\mathcal{S}$:

$$f(V) = -\sum_{k=1}^{N+1} \ln(V_k) + \ln(\text{vol}(T_1 T_2 \ldots T_{N+1})) + \ln(V_0) \tag{3.11}$$

Averaging over the set of all possible density matrices we obtain

$$\langle f(V) \rangle = -\sum_{k=1}^{N+1} \langle \ln(V_k) \rangle + \ln(\text{vol}(T_1 T_2 \ldots T_{N+1})) + \ln(V_0) \tag{3.12}$$

The first term on the right hand side of the equation does not depend on the actual selection of the set of measurements, because $\langle \ln(V_k) \rangle$ cannot depend on the actual eigenvectors of the $k$-th measurement, because the set of all possible states over which we are averaging is invariant under unitary transformations and bases corresponding to different measurements are always related by a unitary transformation, so the quantity $\langle \ln(V_k) \rangle$ has to be the same for all measurements.

Therefore the problem to maximize the obtained information boils down to maximize the quantity $\ln(\text{vol}(T_1 T_2 \dots T_{N+1}))$. The volume of such a parallelepiped will be maximal if its edges will be mutually orthogonal with respect to the operator inner product. Since the subspaces $T_k$ and $T_s$ for $k \neq s$ are spanned by the families $\left\{P_i^k - \frac{1}{N} I, \quad | i = 1, 2, \dots, N\right\}$ and $\left\{P_j^s - \frac{1}{N} I, \quad | j = 1, 2, \dots, N\right\}$, respectively, we are looking for a condition which would guarantee that $P_i^k - \frac{1}{N} I$ and $P_j^s - \frac{1}{N} I$ are orthogonal for all $i, j$ if $s \neq k$. Using our definition (1.15) of inner product in Hilbert space of operators, we obtain a condition

$$\text{Tr}\left(\left(P_i^k - \frac{1}{N} I\right)\left(P_j^s - \frac{1}{N} I\right)\right) = 0 \quad \text{for } k \neq s \text{ and } \forall i, j. \tag{3.13}$$

Because

$$\text{Tr}\left(\left(P_i^k - \frac{1}{N} I\right)\left(P_j^s - \frac{1}{N} I\right)\right) = \text{Tr}\left(P_i^k P_j^s\right) - \frac{2}{N} + \frac{1}{N}, \tag{3.14}$$

the condition (3.13) holds if and only if

$$\text{Tr}\left(P_i^k P_j^s\right) = \frac{1}{N} I \quad \text{for } k \neq s \text{ and } \forall i, j. \tag{3.15}$$

Therefore, if we could find $N+1$ bases such that (3.15) would be fulfilled, we would have an optimal set of measurements. Bases with property (3.15) are called *mutually unbiased* and will be investigated in the following chapters.

# Chapter 4

# Mutually unbiased measurements

Let us start with the definition of mutually unbiased bases:

**Definition 2** (Mutually unbiased bases)**.** Two bases

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

in an $N$-dimensional complex Hilbert space are *mutually unbiased* if inner products between all possible pairs of vectors with one vector from each basis have the same magnitude $\frac{1}{\sqrt{N}}$:

$$|\langle u_i | v_j \rangle| = \frac{1}{\sqrt{N}} \ \forall i, j \in \{1, 2, \ldots, N\} \tag{4.1}$$

**Definition 3** (Mutually unbiased measurements)**.** Two measurements are defined to be mutually unbiased if the bases composed of the eigenstates of their observables (with nondegenerate spectra) are mutually unbiased.

**Definition 4** (Set of mutually unbiased bases)**.** A set of $d$ bases is called mutually unbiased if every two different bases from the set are mutually unbiased with respect to each other.

One of interesting properties of these bases is that a measurement over one basis provides maximum uncertainty as to the outcome of a measurement in a basis that is unbiased with respect to the first one (because all $N$ possible outcomes will have equal probabilities $\frac{1}{N}$). This property was first noted by Schwinger [13]. The first attempt to use these bases in a state determination was made by Ivanović [14], who also provided an explicit construction of $N+1$ mutually unbiased bases for odd prime number dimensional Hilbert spaces. The idea of using mutually unbiased bases for quantum system state determination was further developed by Wootters [15] and Wootters and Fields ([11]). In [11], they presented a construction of $N + 1$ mutually unbiased bases in an arbitrary prime power $p^a = N$-dimensional Hilbert space and also demonstrated that they form a complete set of measurements for state determination which is optimal in the sense of chapter 3.

Mutually unbiased bases find important applications in quantum information theory. 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 used in key distribution protocols in quantum cryptography. Matrices with such a property for two-level systems (whose vectors are called *qubits* in quantum computation) are the Pauli matrices. However, a $d$-level quantum systems (with vectors called $qudits$) have come to a closer attention recently. It has been shown that such systems can be realized experimentally and quantum key distribution protocols using qudits have been introduced (see e.g. [16]). Such protocols use mutually unbiased bases in higher dimensions than two, and therefore the study of construction of mutually unbiased bases for higher dimensions has attracted more attention, too.

## 4.1 Minimal and maximal number of mutually unbiased bases

We shall first prove two theorems (that are given in [11] and [17]) that limit the maximal and minimal possible number of mutually unbiased bases that can exist in a given $N$-dimensional Hilbert space.

**Theorem 2.** In an $N$-dimensional Hilbert space, there cannot be more than $N+1$ mutually unbiased bases.

*Proof.* In chapter 3, we worked with an $N^2-1$ dimensional vector space of $N \times N$ traceless Hermitian matrices. A set of $N+1$ mutually unbiased bases allows us to construct $N+1$ sets of subspaces $T_k$, which are spanned by operators

$$P_i^k - \frac{1}{N}I = |\psi_i^k\rangle\langle\psi_i^k| - \frac{1}{N}I, \quad i = 1, 2, \ldots, N,$$

where $|\psi_i^k\rangle$ denotes an $i-$th vector from $k-$th basis. Such subspaces are $N-1$ dimensional and since we have $N+1$ of them, it is impossible to find even a single vector that would be mutually unbiased to all the $N+1$ bases. Namely, if we could find such a vector $|\psi\rangle$, than an operator defined as

$$\tilde{P} = |\psi\rangle\langle\psi| - \frac{1}{N}I$$

would not belong to any subspace $T_k$, because according to equation (3.14) it would be orthogonal to all the subspaces $T_1, T_2, \ldots T_{N+1}$ . This contradicts the fact that we have $N+1$ mutually orthogonal $(N-1)$-dimensional subspaces in an $(N+1)(N-1) = N^2-1$ dimensional space. Therefore there cannot be any operator that would not belong to the span of all subspaces $T_k$. And since there does not exist even a single vector that would be mutually unbiased to a set of $N+1$ mutually unbiased bases, then it is also impossible to find such a basis. □

To formulate next theorem, we shall use the fact given in section 4.3 that it is possible to find a set of $N+1$ mutually unbiased bases in a Hilbert space of dimension equal to an arbitrary power of a prime number. We will now assume that we are able to find such a set for arbitrary power of a prime $p$. Then we can easily prove the following theorem:

**Theorem 3.** Let $\mathcal{H}$ be an $N$- dimensional Hilbert space $\mathcal{H}$, where

$$N = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$$

is a factorization of $N$ into distinct primes $p_i$. Then the minimal number of mutually unbiased bases in $\mathcal{H}$ is

$$\min \{p_1^{m_1}+1, p_2^{m_2}+1, \dots, p_r^{m_r}+1\}.$$

*Proof.* Let $\mathcal{H}$ be a composite Hilbert space of dimension $N = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ constructed as

$$\mathcal{H} = \mathcal{Q}_1 \otimes \mathcal{Q}_2 \otimes \dots \otimes \mathcal{Q}_r$$

where $\mathcal{Q}_i$ denotes a $p_i^{m_i}$-dimensional Hilbert space, for which we can construct a set of $p_i^{m_i}+1$ mutually unbiased bases. Therefore, if we take $d = \min\{p_1^{m_1}, p_2^{m_2}, \dots, p_r^{m_r}\}$, then we can find in all spaces $\mathcal{Q}_i$ at least $d+1$ mutually unbiased bases. If we take the family $B_1^j, B_2^j, \dots, B_r^j$ of bases where $j = 1, 2, \dots d+1$, we can construct a set of $d+1$ mutually unbiased bases in $\mathcal{H}$ by forming their tensor products

$$\left\{B^j = B_1^j \otimes B_2^j \otimes \dots \otimes B_r^j, \quad j = 1, 2, \dots d+1\right\}.$$

To verify that the above set of bases in $\mathcal{H}$ is really mutually unbiased, consider the inner product of two vectors $|\psi_j\rangle$ and $|\psi_k\rangle$ belonging to two different bases $B^j$ and $B^k$, $j \neq k$:

$$\begin{aligned}
|\psi_j\rangle &= |a_1^j\rangle \otimes |a_2^j\rangle \otimes \dots |a_r^j\rangle, \quad |a_i^j\rangle \in B_i^j \\
|\psi_k\rangle &= |a_1^k\rangle \otimes |a_2^k\rangle \otimes \dots |a_r^k\rangle, \quad |a_i^k\rangle \in B_i^k \\
|\langle\psi_j|\psi_k\rangle| &= |\langle a_1^j|a_2^k\rangle\langle a_2^j|a_2^k\rangle \dots \langle a_r^j|a_r^k\rangle| = \frac{1}{\sqrt{p_1^{m_1}}}\frac{1}{\sqrt{p_2^{m_2}}}\dots\frac{1}{\sqrt{p_r^{m_r}}} = \frac{1}{\sqrt{N}}
\end{aligned}$$

Therefore, such a set of bases is mutually unbiased. □

## 4.2 Construction of mutually unbiased bases for prime dimensions

It can be easily verified that the set of eigenvectors of Pauli matrices form a set of mutually unbiased bases:

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

Therefore, they form a maximal set of $3$ mutually unbiased bases in a two-dimensional Hilbert space. The construction of such a set of bases in higher dimensions can be understood as a generalization of this property. The set of mutually unbiased bases for any odd prime dimension $p$ was first discovered by Ivanović [14]. For a $p$-dimensional Hilbert space he gave the set of $p+1$ mutually unbiased bases:

$$\begin{aligned}
|\psi\rangle_j^{(0,k)} &= \delta_{jk}, \\
|\psi\rangle_j^{(1,k)} &= \frac{1}{\sqrt{p}} e^{\frac{2\pi i}{p}(j+k-1)^2}, \\
&\vdots \\
|\psi\rangle_j^{(n,k)} &= \frac{1}{\sqrt{p}} e^{\frac{2\pi i}{p}n(j+k-1)^2}, \\
&\vdots \\
|\psi\rangle_j^{(p-1,k)} &= \frac{1}{\sqrt{p}} e^{\frac{2\pi i}{p}(p-1)(j+k-1)^2}, \\
|\psi\rangle_j^{(p,k)} &= \frac{1}{\sqrt{p}} e^{\frac{2\pi i}{p}(jk)},
\end{aligned}$$

where $|\psi\rangle_j^{(n,k)}$ denotes the $j$-th component of the $k$-th vector in $n$-th basis. The first basis is the standard (or canonical) basis. Every basis from the set is orthonormal, which follows from (2.21). The mutual unbiasedness follows from the Gauss sums of number theory [18]:

$$\left|\sum_{i=1}^{p} e^{\frac{2\pi}{p}(ai^2+bi)}\right| = \frac{1}{\sqrt{p}} \qquad a, b \in \mathbb{N}, a \neq 0, a \neq \pm p, \pm 2p, \quad p \text{ odd prime}. \qquad (4.2)$$

Namely, the magnitude of the inner product of two vectors $|\psi\rangle^{(n,k)}$ and $|\psi\rangle^{(m,l)}$ taken from $m$-th and $n$-th basis, respectively, ($m \neq n, \;\; m, n \neq 0$) is of the form (4.2). The case when one of the vectors is taken from the standard basis is trivial.

We shall now have a look at one possible approach (presented in [19]) to derive the $N+1$ mutually unbiased bases for any prime dimension $N$. This approach uses unitary operators $P_N, Q_N$ which were defined in (2.11) and (2.10). In chapter 5, we shall show an independent proof of these results by exploiting the group properties of an algebraic structure formed by operators $P_N$ and $Q_N$. Throughout the rest of this section, we will assume $N$ to be a prime. We shall first prove a useful lemma [19]:

**Lemma 2.** Let $B = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle\}$ be an orthonormal basis in an $N$-dimensional space, N is a prime. Suppose that there is a unitary operator $V$ such that $V$ applied to any vector from basis $B$ shifts the vector modulo N with the following property: for any pair of vectors $|\psi_i\rangle, |\psi_j\rangle$ from the basis $B$, there is $k \in \mathbb{N}$ such that $V^k|\psi_i\rangle = \beta|\psi_j\rangle, |\beta| = 1$. Then the basis $\tilde{B} = \left\{|\tilde{\psi_1}\rangle, |\tilde{\psi_2}\rangle, \ldots, |\tilde{\psi_N}\rangle\right\}$ consisting of eigenvectors of $V$ is mutually unbiased with respect to $B$.

*Proof.* Let $\lambda_k \;\; (|\lambda_k| = 1)$ be an eigenvalue of $V$ corresponding to eigenvector $|\tilde{\psi_k}\rangle$. Then

$$|\langle\tilde{\psi_k}|\psi_j\rangle| = |\lambda_k\langle\tilde{\psi_k}|V|\psi_j\rangle| = |\beta_j||\langle\tilde{\psi_k}|\psi_{j+c \mod N}\rangle| = |\langle\tilde{\psi_k}|\psi_{j+c \mod N}\rangle|.$$

From the fact that the cyclic shifts generated by $V$ act on the vectors of basis $B$ freely and transitively, it follows that

$$|\langle\tilde{\psi_k}|\psi_1\rangle| = |\langle\tilde{\psi_k}|\psi_2\rangle| = \ldots = |\langle\tilde{\psi_k}|\psi_N\rangle| \qquad \forall k \in \{1, 2, \ldots, N\}\,.$$

Now since $B$ is an orthonormal basis, we can use Parseval's equality:

$$1 = \||\tilde{\psi_k}\rangle\|^2 = \sum_{i=1}^{N} |\langle\tilde{\psi_k}|\psi_i\rangle|^2 = N|\langle\tilde{\psi_k}|\psi_j\rangle|^2 \quad \forall j \in \{1, 2, \ldots, N\}$$

from which it follows that bases $B$ and $\tilde{B}$ are mutually unbiased. □

We will now demonstrate an important theorem.

**Theorem 4.** The bases composed of eigenvectors of operators

$$\left\{Q_N, P_N, P_N Q_N, P_N Q_N^2, \ldots, P_N Q_N^{N-1}\right\} \tag{4.3}$$

are mutually unbiased with respect to each other and form therefore a maximal set of $N+1$ mutually unbiased bases.

*Proof.* This theorem can be proved by using the following lemma:

**Lemma 3.** The eigenvectors of $P_N Q_N^k$ are cyclically shifted under the action of $P_N Q_N^l$ $(l, k = 0, 1 \dots N-1)$

*Proof.* Let $\{|\mathit{0}\rangle, |\mathit{1}\rangle, \dots |\mathit{N-1}\rangle\}$ denote the standard basis. It can be checked that vectors

$$|\psi_t^k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} (\omega^t)^{(N-j)} (\omega^{-k})^{\left(\sum_{i=j}^{N-1} i\right)} |j\rangle \tag{4.4}$$

are eigenvectors of $P_N Q_N^k$ corresponding to eigenvalue $\omega^t$:

$$P_N Q_N^k |\psi_t^k\rangle = \omega^t |\psi_t^k\rangle. \tag{4.5}$$

The action of $P_N Q_N^l$ on a vector $|\psi_t^k\rangle$ produces a shift by $k - l$

$$P_N Q_N^l |\psi_t^k\rangle = \omega^{t+k-l} |\psi_{t+k-l}^k\rangle. \tag{4.6}$$

The condition that by a successive application of $P_N Q_N^l$ to $t$-th eigenvector of $P_N Q_N^k$ we can obtain every other eigenvector is fulfilled because $N$ is a prime. The actual number $r$ of necessary successive applications is given by a solution of the congruence:

$$t' = t + r(k - l) \qquad \mathrm{mod}\ N$$

□

Using lemma 2 and 3 we conclude that the bases consisting of eigenvectors of

$$\left\{Q_N, P_N, P_N Q_N, P_N Q_N^2, \dots, P_N Q_N^{N-1}\right\}$$

indeed constitute a set of $N + 1$ mutually unbiased bases in a Hilbert space of prime dimension $N$. □

## 4.3 Mutually unbiased bases for powers of primes

The first construction of mutually unbiased bases for dimension $N = p^a$, $p$ prime, was presented by Wootters and Fields [11]. We will present here the formulas for completeness. They are different for powers of 2 and powers of odd primes.

### 4.3.1 Odd prime powers

Suppose that $N = p^a, \quad p \neq 2$. Than one of the $N + 1$ mutually unbiased bases is the standard basis

$$|\psi\rangle_j^{(0,k)} = \delta_{jk}$$

and the other $N$ bases will be given by

$$|\psi\rangle_j^{(n,k)} = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{p}\text{Tr}(nj^2+jk)}, \quad n = 1, 2, \ldots, N \tag{4.7}$$

where $j$ denotes the $j$-th component of the $k$-th vector in $n$-th base and Tr$(\alpha)$ is defined as

$$\text{Tr}(\alpha) = \sum_{i=0}^{p^{a-1}} \alpha^i.$$

The fact that such bases are mutually unbiased follows from a formula from number theory [18]

$$\left| \sum_{j \in \mathbb{Z}_{p^n}} e^{\frac{2\pi i}{p}\text{Tr}(mj^2+rj)} \right| = \sqrt{p^n} \qquad m \neq 0, \quad p > 2, \quad p \text{ prime} . \tag{4.8}$$

One can verify that for the inner product of two vectors is:

$$\langle \psi^{(n,k)} | \psi^{(n',k')} \rangle = \frac{1}{N} \left| \sum_{j \in \mathbb{Z}_{p^n}} e^{\frac{2\pi i}{p}\text{Tr}((n'-n)j^2+(k'-k)j)} \right| . \tag{4.9}$$

We see that the $N$ bases composed of such vectors are orthonormal and mutually unbiased with respect to each other. It can be seen that all the vectors (4.7) will be mutually unbiased with respect to the standard basis.

### 4.3.2 Even prime powers

For a systems of dimension $N$ equal to $2^n$, we can define $2^n$ bases whose vectors will be in a form

$$|\psi\rangle_j^{(n,k)} = \frac{1}{\sqrt{2^n}} e^{\frac{2\pi i}{4}\text{Tr}(n+2k)j}. \tag{4.10}$$

It is obvious that they will be mutually unbiased with respect to the standard basis. For the proof that these bases are mutually unbiased with respect to each other, we refer to [17] and [11].

# Chapter 5

# A group theory approach to mutually unbiased measurements

## 5.1 The representation in $\mathbb{Z_N} \times \mathbb{Z_N}$

We shall now apply a group theory approach to construct mutually unbiased bases in an $N$-dimensional Hilbert space, $N$ being a prime. First, we need to establish a connection between the Pauli group and vector space $\mathbb{Z}_N \times \mathbb{Z}_N$. The elements of Pauli group (2.23):

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

are labeled by three numbers $(l, i, j)$. Therefore, it has $N^3$ elements. The center of the Pauli group $Z(\Pi_N)$ (i.e. the set of elements of $\Pi_N$ that commute with all elements in $\Pi_N$) is:

$$Z(\Pi_N) = \left\{\omega^l | l = 0, 1, \ldots, N-1\right\} = \{(l, 0, 0)\}. \tag{5.1}$$

Since $Z(\Pi_N)$ is a normal subgroup of $\Pi_N$, we can define an equivalence relation in $\Pi_N$:

$$a, b \in \Pi_N, \qquad a \sim b \Leftrightarrow ab^{-1} \in Z(\Pi_N) \Leftrightarrow a^{-1}b \in Z(\Pi_N),$$

which allows us to define a quotient group $\Pi_N / Z(\Pi_N)$ whose elements are the classes of equivalence (or cosets). The cosets are labeled numbers $(i, j), i, j = 0, 1, \ldots, N-1$. There is a one-to-one correspondence between vectors $(i, j) \in \mathbb{Z}_N \times \mathbb{Z}_N$ and cosets,

$$(i, j) \longleftrightarrow \left\{\omega_N^l Q_N^i P_N^j | \quad l = 0, 1, \ldots, N-1\right\} = Q^i P^j, \tag{5.2}$$

where $Q^i P^j$ (without subscripts $N$) denotes the corresponding coset. Note that all operators belonging to the same coset will have the same eigenvectors, because they have only different multipliers $\omega_N^l$. It is easily seen that the correspondence $\phi$: $\Pi_N / Z(\Pi_N) \rightarrow$

$\mathbb{Z}_N \times \mathbb{Z}_N$

$$\phi\left(Q_N^i P_N^j\right) = (i,j),$$

is an isomorphism of Abelian groups

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

We shall now focus on the group of automorphisms of $\Pi_N/Z(\Pi_N)$. It was studied in [20], [21] and [10]. We shall exploit the approach of [21], where the cosets corresponded to 1-dimensional grading subspaces of the Pauli graded Lie algebra gl$(N,\mathbb{C})$. The inner automorphisms of gl$(N,\mathbb{C})$ are induced by the action

$$\varphi_X(A) = X^{-1}AX \tag{5.3}$$

of an element $X$ from GL$(N,\mathbb{C})$ (a group of regular complex $N \times N$ matrices). Let us now consider a subgroup of automorphisms of the form (5.3) acting on elements of $\Pi_N$ which will induce permutations of cosets in $\Pi_N/Z(\Pi_N)$. Note that matrices corresponding to such automorphisms will be unitary, because they can be understood as transformation matrices that transform a linear operator (of the form $\omega_N^l Q_N^a P_N^b$) to a different basis, in which the operator is again unitary (of the form $\omega^{l'} Q^c P^d$). Therefore the matrix $U$ has to be a transition matrix between two orthonormal bases, and hence unitary. The actual form of these matrices is given in Appendix A.

Automorphisms from this subgroup will be equivalent if they define the same transformation of cosets in $\Pi_N/Z(\Pi_N)$:

$$\psi_Y \sim \psi_X \Leftrightarrow Y^{-1}Q^iP^jY = X^{-1}Q^iP^jX \quad \forall (i,j) \in \mathbb{Z}_N \times \mathbb{Z}_N \tag{5.4}$$

Since the group $\Pi_N/Z(\Pi_N)$ has only two generators (the cosets $P$ and $Q$), the previous condition can be rewritten as

$$\psi_Y \sim \psi_X \Leftrightarrow Y^{-1}PY = X^{-1}PX \text{ and } Y^{-1}QY = X^{-1}QX \tag{5.5}$$

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

$$Y^{-1}QY = Q^aP^b \quad \text{and} \quad Y^{-1}PY = Q^cP^d \tag{5.6}$$

Therefore to each equivalence class of automorphisms $\psi_Y$, we can assign a matrix:

$$\Phi(\psi_Y) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad a,b,c,d \in \mathbb{Z}_N \tag{5.7}$$

To the composition of two automorphisms $\psi_X, \psi_Y$ corresponding to $(a_X, b_X, c_X, d_X)$

and $(a_Y, b_Y, c_Y, d_Y)$, respectively, a matrix that corresponds to a product of matrices corresponding to $\psi_X$ and $\psi_Y$ will be assigned, as can be seen from

$$\begin{aligned}(XY)^{-1}Q(XY) = (Y^{-1}QY)^{a_X}(Y^{-1}PY)^{b_X} &= Q^{a_Y a_X}P^{b_Y a_X}Q^{c_Y b_X}P^{d_Y b_X} \\ &= Q^{a_X a_Y + b_X c_Y}P^{a_X b_Y + b_X d_Y}\end{aligned}$$

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

$$\Phi(\psi_X \psi_Y) = \Phi(\psi_X)\Phi(\psi_Y) \tag{5.8}$$

is an injective homorphism.

We shall show now that $(a, b, c, d)$ cannot be chosen arbitrarily. Consider the action of $\psi_Y$:

$$Y^{-1}QY = Q^a P^b \Longrightarrow Y^{-1}Q_N Y = \mu Q_N^a P_N^b, \quad \mu \in \mathbb{C} \tag{5.9}$$

$$Y^{-1}PY = Q^c P^d \Longrightarrow Y^{-1}P_N Y = \lambda Q_N^c P_N^d, \quad \lambda \in \mathbb{C} \tag{5.10}$$

By multiplying the equation (5.9) by the equation (5.10) once from the left and once from the right, we obtain

$$P_N Q_N Y = \mu\lambda Y Q_N^c P_N^d Q_N^a P_N^b, \tag{5.11}$$

$$Q_N P_N Y = \mu\lambda Y Q_N^a P_N^b Q_N^c P_N^d. \tag{5.12}$$

Using the commutation relation (2.12) $\omega_N P_N Q_N = Q_N P_N$ we obtain

$$\omega^{-ad}\mu\lambda Y Q_N^{a+c}P_N^{b+d} = P_N Q_N Y = \omega_N^{-1}Q_N P_N Y = \omega_N^{-1}\omega^{-bc}\mu\lambda Y Q_N^{a+c}P_N^{b+d} \tag{5.13}$$

and therefore we have a condition

$$\omega_N^{-ad} = \omega_N^{-bc-1} \tag{5.14}$$

which will be fulfilled if and only if $ad - bc = 1(\text{mod } N)$, i.e.

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = 1 \mod N. \tag{5.15}$$

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

$2 \times 2$ matrices with determinant equal to $1$ modulo $N$)

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

is assigned. Now to every coset from $\Pi_N/Z(\Pi_N)$ an element $(i, j)$ from $\mathbb{Z}_N \times \mathbb{Z}_N$ was assigned. It can be checked that the action of $\psi_Y$ on $Q^i P^j$ is given by:

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

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

$$(i', j') = (i, j) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{5.16}$$

We will conclude this section with an observation [22], [23]:

**Lemma 4.** The action of a matrix from $\mathrm{SL}(2, \mathbb{Z}_N)$ on $(i, j) \in \mathbb{Z}_N \times \mathbb{Z}_N$ does not change 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 $\mathbb{Z}_N \times \mathbb{Z}_N$. Then

$$\det \begin{pmatrix} i & j \\ k & l \end{pmatrix} = il - kj$$

The action of $A$ is then $(i', j') = (i, j)A$ and $(k', l') = (k, l)A$. Then we have

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

because $\det(A) = 1$.

□

## 5.2 Mutually unbiased bases

Now the representation of automorphisms and operators $Q, P$ will be used to introduce an interesting structure that proves the existence of $N+1$ mutually unbiased bases for prime $N$ and presents an alternative approach to their construction. We shall exploit the fact that cyclic group $\mathbb{Z}_N$ forms a finite field for prime $N$, which means that we can introduce multiplication modulo $N$ in this additive group. The finite 'phase space' $\mathbb{Z}_N \times \mathbb{Z}_N$ can be decomposed into $N$ subclasses $[(i, j)]$ which are represented by elements of the form $(i, 1)$ where $i = 0, 1, \ldots, N-1$, and one subclass represented by an element $[(1, 0)]$. We exclude the trivial class $[(0, 0)]$. The set of all elements that belong to a subclass represented by a given element $(i,j)$ is then defined as a set of elements

$$(i',j') = (ri,rj), \qquad r = 1,2,\ldots,N-1$$

where the multiplication is understood modulo $N$. In the proof that every element from $\mathbb{Z}_N \times \mathbb{Z}_N \backslash \{(0,0)\}$ can be assigned to some subclass, we will exploit the fact that $\mathbb{Z}_N$ is a field for prime $N$. We see that every subclass has $N-1$ elements, so this decomposition has $N^2-1$ elements in total, the only one not included is $(0,0)$. If an element is in form $(0,i)$ or $(i,0)$, then it is obvious that it can be assigned to subclasses $[(0,1)]$ or $[(1,0)]$ respectively. An element in the form $(i,j), i,j = 1,2,\ldots,N-1$ will belong to a subclass

$$(k,1) \quad \text{where} \quad k \in \{1,2,\ldots,N-1\} \quad \text{is the solution of} \quad kj = i \mod N.$$

The existence and uniqueness of such $k$ is guaranteed by the fact that $\mathbb{Z}_N$ is a field. We can illustrate the decomposition in subclasses by a table of all elements in $\mathbb{Z}_N \times \mathbb{Z}_N \backslash \{(0,0)\}$:

| | 0 | 1 | 2 | … | N-1 |
|---|---|---|---|---|---|
| 0 | | $\boxed{(0,1)}$ | (0,2) | … | (0,N-1) |
| 1 | $\boxed{(1,0)}$ | $\boxed{(1,1)}$ | (1,2) | … | (1,N-1) |
| 2 | (2,0) | $\boxed{(2,1)}$ | (2,2) | … | (2,N-1) |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋱ | ⋮ |
| N-1 | (N-1,0) | $\boxed{(N-1,1)}$ | (N-1,2) | … | (N-1,N-1) |

There, every element $(i,j)$ corresponds to a coset $Q^iP^j$ from the Pauli group. All matrices in the same coset differ just by the complex multiplier factor. Every multiple $(ri,rj)$ of a vector $(i,j)$ by $r \in \{1,2,\ldots,N-1\}$ will therefore correspond to a coset $Q^{ri}P^{rj}$[1]. An important consequence is that elements $(i,j)$ and $(ri,rj), \quad r = 1,2,\ldots N-1$, will correspond to matrices that have the same eigenvectors. Thus we have proved the following lemma:

**Lemma 5.** If $N$ is prime, then there are exactly $N+1$ subclasses of elements from $\mathbb{Z}_N \times \mathbb{Z}_N \backslash \{(0,0)\}$, each subclass containing $N-1$ elements. Elements from the same class correspond to operators with the same eigenvectors.

[1] Note that operators $(Q^iP^j)^r$ and $(Q^{ri}P^{rj})$ belong to the same coset, because it follows from the relations (2.12) that they differ just by a complex factor.

We will now demonstrate that bases of two different operators corresponding to elements from different subclasses in $\mathbb{Z}_N \times \mathbb{Z}_N \backslash \{(0,0)\}$ are mutually unbiased. We shall first show that the basis composed of eigenvectors of $Q_N$ is mutually unbiased with respect to the basis of eigenvectors of $P_N$. This is a consequence of lemma 2. However, an easier proof follows immediately from equation (2.18), because then:

$$P_N S|j\rangle = S Q_N^\dagger |j\rangle, \tag{5.17}$$

where $|j\rangle$ (a $j$-th vector from standard basis) is an eigenvector of $Q_N$ (and of $Q_N^\dagger$ as well) and therefore according to (5.17) $S|j\rangle$ will be an eigenvector of $P_N$. Now, using the definition (2.17) of $S$, it can be seen that

$$|(S|j\rangle, |j\rangle)| = \left| \sum_i^N \left( \frac{1}{\sqrt{N}} \omega^{ij} |i\rangle, |j\rangle \right) \right| = \frac{1}{\sqrt{N}}$$

With this fact available, we now proceed to the theorem:

**Theorem 5.** Let $(a,b)$ and $(c,d)$ be two elements from $\mathbb{Z}_N \times \mathbb{Z}_N \backslash \{(0,0)\}$ such that they do not belong to the same subclass. Then the bases composed of eigenvectors of the operators from corresponding cosets $Q^a P^b$ and $Q^c P^d$ are mutually unbiased.

*Proof.* If we have two pairs where one belongs to the class $[(1,0)]$ and the other one to the class $[(0,1)]$, then we already know that their corresponding bases will be mutually unbiased, because they are composed of eigenvectors of of $Q_N$ and $P_N$ respectively. Let us now consider the case of two distinct pairs

$$(a,1) \quad \text{and} \quad (b,1), \qquad a,b \in \{1,2,\ldots,N-1\} \quad a \neq b$$

and prove that the bases of eigenvectors of the corresponding operators $Q_N^a P_N$ and $Q_N^b P_N$ will be mutually unbiased (and hence the bases of powers of these operators). We have seen that to unitary matrices that permute the cosets in the Pauli group

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

matrices from SL$(2,\mathbb{Z}_N)$ can be assigned and vice versa, to every matrix from SL$(2,\mathbb{Z}_N)$ we can assign a unitary matrix $U$ such that it permutes the elements from the Pauli group. These unitary operators form a so-called metaplectic representation of SL$(2,\mathbb{Z}_N)$ [10], [20]. We will now show, if $a \neq b$, that there exists a matrix $A$ from 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 matrix such that

$$\begin{aligned} U^{-1}Q^{a}PU &= Q^{\tilde{a}}, \\ U^{-1}Q^{b}PU &= P^{\tilde{b}}, \end{aligned}$$

hence their eigenvectors can be expressed as $U|\psi_Q\rangle$ and $U|\psi_P\rangle$, respectively. Their inner product is then

$$|\langle\psi_{Q^aP}|\psi_{Q^bP}\rangle|^2 = |(U|\psi_Q\rangle, U|\psi_P\rangle)|^2 = |\langle\psi_Q|\psi_P\rangle|^2 = \frac{1}{N}$$

proving that these bases are really mutually unbiased.

We will now prove existence of matrix $A$ from SL$(2,\mathbb{Z}_N)$ with desired properties. From lemma 4 we know that the following condition has to be fulfilled:

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

Therefore we select

$$\tilde{a}, \tilde{b} \in \mathbb{Z}_N \qquad \text{such that} \quad \tilde{a}\tilde{b} = a - b \mod N.$$

Now we can equivalently look for a matrix $C \in$ SL$(2,\mathbb{Z}_N)$ producing inverse transformation

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

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

$$\tilde{a}\beta = 1 \mod N \tag{5.18}$$

$$\tilde{a}\alpha = a \mod N \tag{5.19}$$

$$\tilde{b}\gamma = b \mod N \tag{5.20}$$

$$\tilde{b}\delta = 1 \mod N \tag{5.21}$$

The fact that $N$ is a prime guarantees that all these equations have unique solutions in $\mathbb{Z}_N$.

We also need to check that $C$ belongs to SL$(2,\mathbb{Z}_N)$:

$$\det(C) = \det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \alpha\delta - \beta\gamma \mod N$$

By multiplying equations (5.19) and (5.21) and subtracting the product of (5.20) and (5.18) we obtain

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

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

$$\alpha\delta - \beta\gamma = \det(C) = 1 \mod N$$

which means that C indeed belongs to SL$(2,\mathbb{Z}_N)$. The inverse matrix

$$C^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$$

will then transform pairs $(a,1)$ and $(b,1)$ to $(\tilde{a},0)$ and $(\tilde{b},0)$, respectively:

$$\begin{aligned} (a,1)C^{-1} &= (\tilde{a},0), \\ (b,1)C^{-1} &= (0,\tilde{b}). \end{aligned}$$

To complete the proof, we have to show that for any pair $(b,1)$ and $(1,0)$ or $(b,1)$ and $(0,1)$, $b = 1,2,\ldots,N-1$, there exist matrices from SL$(2,\mathbb{Z}_N)$ such that

$$(b,1)A_1 = (0,1) \quad \text{and} \quad (1,0)A_1 = (1,0)$$

or

$$(b,1)A_2 = (b,0) \quad \text{and} \quad (0,1)A_2 = (0,1)$$

In the first case, the matrix

$$A_1 = \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix}$$

fulfils the condition. For the second case, the matrix $A_2$ will be given by

$$A_2 = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}, \qquad \text{where} \quad \beta \in \mathbb{Z}_N, \quad \beta b = N-1 \mod N$$

From these equations, it follows that bases of eigenvectors of $Q^bP$ and $Q$ and $P$ will be mutually unbiased. Therefore, 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 matrices $Q_N, P_N, Q_N^2 P_N, \dots Q_N^{N-1} P_N$, while the matrices chosen in [19] are only modified using the relation (2.12). Note that in our proof, we could have used pairs $(1, a)$, $a = 1, 2, \dots, N-1$, instead of $(a, 1)$. Then, we would obtain as a result that the mutually unbiased bases will be given by bases composed of eigenvectors of matrices

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

which can also be obtained by finite Fourier transformation (2.18).

## 5.3 Unsolved problems

The problem of finding mutually unbiased bases for a composite dimension $N$, where $N$ is not prime nor power of a prime, still remains an open problem. We do not know even the answer for the simplest case $N = 6$. Using theorem 3, we can find $3$ such bases. Some unsuccessful numerical attempts to find more mutually unbiased bases have been made and it remains unclear whether it is indeed possible to find more than $3$ of them for Hilbert spaces 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 in several articles (e.g. [19]), the relation between the decomposition of space $\mathbb{Z}_N \times \mathbb{Z}_N$ whose elements correspond to the elements of Pauli group and the existence of mutually unbiased basis has been left unnoticed so far. However, the relation heavily depends on properties that are consequence of $N$ being a prime and therefore enabling us to multiplication in $\mathbb{Z}_N$. It might be interesting to investigate whether this relation could be generalized to arbitrary dimension and whether it would give us some more information about the existence or non-existence of mutually unbiased bases in composite dimensions.

# Appendix A

# Unitary matrices corresponding to inner automorphisms that permute the elements of the Pauli group

The actual form of unitary matrix $U$ whose action permutes the elements of the Pauli group $\Pi_N$ and that corresponds to a matrix acting in $\mathrm{SL}(2, \mathbb{Z}_N)$ was described in [10]. For an automorphism $g \in \mathrm{SL}(2, \mathbb{Z}_N)$

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

the corresponding unitary matrix $U(g)$ that acts on the elements of the Pauli group is given by:

$$\begin{aligned}
\delta \neq 0 : U &= \frac{\sigma(1)\sigma(\delta)}{N} \sum_{r,s \in \mathbb{Z}_N} \omega^{\frac{br^2+(d-a)rs-cs^2}{2\delta}} \omega^{\frac{rs}{2}} P_N^r Q_N^s \\
\delta = 0, \quad b \neq 0 : U &= \frac{\sigma(-2b)}{\sqrt{N}} \sum_{s \in \mathbb{Z}_N} \omega^{\frac{s^2}{2b}} \omega^{\frac{s^2(a-1)}{2b}} P_N^{\frac{s(a-1)}{b}} Q_N^s \\
\delta = b = 0, \quad c \neq 0 : U &= \frac{\sigma(2c)}{\sqrt{N}} \sum_{r \in \mathbb{Z}_N} \omega^{\frac{r^2}{2c}} P_N^r \\
\delta = b = c = 0 : U &= I
\end{aligned}$$

where $\delta = 2 - a - d$ and $\sigma(a)$ is defined as:

$$\sigma(a) = \frac{1}{\sqrt{N}} \sum_{n \in \mathbb{Z}_N} \omega^{an^2}.$$

# Bibliography

[1] P. A. M. Dirac, *The Principles of Quantum Mechanics*, Oxford University Press, Oxford, 1958

[2] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, 1996

[3] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univeristy Press, 2003

[4] U. Fano, *Description of states in quantum mechanics by density matrix and operator techniques*, Reviews of Modern Physics, Vol. 29, No. 1, 1957, 74-93

[5] J. Formánek, *Úvod do kvantové teorie*, Academia, Praha, 2004

[6] J. Blank, P. Exner, M. Havlíček, *Lineární operátory v kvantové fyzice*, Karolinum, Praha, 1993

[7] J. Tolar, P. Hájíček, *Can differently prepared states be distinguished?*, Physics Letters A 353, 2006, 19-23

[8] P. Šťovíček, J. Tolar, *Quantum Mechanics in a Discrete Space-time*, Rep. Math. Phys. 20, 1984, 157-170

[9] H. Weyl, *The Theory of Groups and Quantum Mechanics*, Dover Publications, New York, 1950

[10] R. Balian, C. Itzykson, *Observation sur la mécanique quantique finie*, C. R. Acad. Sc. Paris, t. 303, Série I., n. 16, 1986, 773-777

[11] W. K. Wootters, B.D. Fields, *Optimal State-Determination by Mutually Unbiased Measurements*, Annals of Physics 191 (1989), 363-381

[12] B. V. Gnedenko, *The Theory of Probability*, MIR Publishers, Moscow, 1969

[13] J. Schwinger, *Unitary operator bases*, Proc. Natl. Acad. Sci. 46, 1960

[14] I. D. Ivanović, *Geometrical description of quantum state determination*, Journal of Physics A, 14 (1981), no.12, pp. 3241 - 3245

[15] W. K. Wootters, *Quantum mechanics without probability amplitudes*, Foundations of Physics, Vol. 16, No. 4, 1986, 391-405

[16] G. M. Nikolopoulos, G. Alber, *Security bound of two-basis quantum-key-distribution protocols using qudits*, Physical Review A 72, 2005

[17] A. Klappenecker, M. Rötteler, *Constructions of Mutually Unbiased Bases*, Lecture Notes in Computer Science, vol. 2984, Springer, 2004, Preprint quant-ph/0401155

[18] T. Nagell, *Introduction to Number Theory*, Wiley, New York, 1951.

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

[20] M. Neuhauser, *An Explicit Construction of the Metaplectic Representation over a Finite Field*, Journal of Lie Theory, vol. 12, 2002, 15-30

[21] M. Havlíček, J. Patera, E. Pelantová, J. Tolar, *Automorphisms of the fine grading of* $sl(n,\mathbb{C})$ *associated with the generalized Pauli matrices*, J. Math Phys., Vol. 43, No. 2, 2002, math-ph/0311015

[22] P. Novotný, *Počet prvků a akce grupy SL*$(m,\mathbb{Z}_n)$, Výzkumný úkol FJFI, 2002

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