View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Bradford Scholars

UNIVERSITY of BRADFORD

Library

University of Bradford eThesis

This thesis is hosted in Bradford Scholars – The University of Bradford Open Access repository. Visit the repository for full metadata or to contact the repository team

© University of Bradford. This work is licenced for reuse under a Creative Commons Licence.

Weak mutually unbiased bases with applications to quantum cryptography and tomography

Weak mutually unbiased bases

Mohamed Mahmoud Youssef Shalaby

Submitted for the Degree
of Doctor of Philosophy

Department of Computing
University of Bradford

2012

Abstract

Mutually unbiased bases is an important topic in the recent quantum system researches. Although there is much work in this area, many problems related to mutually unbiased bases are still open. For example, constructing a complete set of mutually unbiased bases in the Hilbert spaces with composite dimensions has not been achieved yet. This thesis defines a weaker concept than mutually unbiased bases in the Hilbert spaces with composite dimensions. We call this concept, weak mutually unbiased bases. There is a duality between such bases and the geometry of the phase space $\mathcal{Z}_d \times \mathcal{Z}_d$, where d is the phase space dimension. To show this duality we study the properties of lines through the origin in $\mathcal{Z}_d \times \mathcal{Z}_d$, then we explain the correspondence between the properties of these lines and the properties of the weak mutually unbiased bases. We give an explicit construction of a complete set of weak mutually unbiased bases in the Hilbert space $\mathcal{H}_d$, where d is odd and $d = p_1 p_2$; p_1, p_2 are prime numbers. We apply the concept of weak mutually unbiased bases in the context of quantum tomography and quantum cryptography.

Keywords : Finite quantum systems, quantum tomography, quantum cryptography

Acknowledgements

I would like to thank Professor Apostolos Vourdas, my supervisor for his unlimited support and guidance. I owe a deep gratitude to him for his advice and assistance. It was my pleasure to work under his supervision during this research. He has always found time to meet me and comment on my work.

I wish to express my warm and sincere thanks to my last and present colleagues in the Quantum Information research group for the exciting research atmosphere, as well as the friendship.

I would also like to thank the School of Computing, Informatics and Media at the University of Bradford for the technical support and hospitality throughout my research journey.

I should also mention that my research study in UK was fully sponsored by the Egyptian government.

Finally, I am very grateful to my family members for their continuous encouragement and support.

Declaration

Some parts of the work presented in this thesis have been published in the following articles:

M. Shalaby, and A. Vourdas, "Tomographically complete sets of orthonormal bases in finite systems", J. Phys. A: Math. Theor., 44:345303 (2011)

M. Shalaby, and A. Vourdas, "Weak mutually unbiased bases", J. Phys. A: Math. Theor., 45:052001 (2012)

M. Shalaby, "Two-way and one-way quantum cryptography protocols", Optik - Int. J. Light Electron Opt., 123:1852 (2012)

M. Shalaby, and A. Vourdas, "Mutually unbiased projectors and duality between lines and bases in finite quantum systems", submitted to Letters in Mathematical Physics.

Table of Contents

List of figures

List of tables

Chapter 1

Introduction

Finite quantum systems are the systems whose quantum states are labeled by elements in $\mathcal{Z}_d$, where $\mathcal{Z}_d$ is the set of integers modulo d. There are three topics which are related to finite quantum systems.

The first topic, is quantum computation and information which is the analogous term of classical computation and information, where computational tasks are implemented using quantum mechanical systems [1]. The concept of mutually unbiased bases plays an important role in many applications of quantum computation and information such as quantum cryptography and quantum tomography. Two bases are called mutually unbiased if the quantum measurement corresponding to one basis gives no information about the quantum measurement corresponding to the other bases. The maximum number of mutually unbiased bases in d-dimensional system is $d + 1$. In the case that d is power of prime, a complete set of such bases can be constructed. However, the existence of a complete set of mutually unbiased bases in d-dimensional systems where d is composite, has not been

proved yet.

The security of quantum cryptography protocols relies on the physical properties of quantum systems as the quantum systems are prepared using two (or more than two) mutually unbiased bases. In 1984, Bennett and Brassard [2] designed the first quantum cryptography protocol. Later, much work has been done in this area. Reviews of this work have been presented in [3].

Quantum tomography is the process of state determination of quantum systems using experimental measurements according to different bases. It has been proved that a complete set of mutually unbiased bases is optimal for quantum tomography [4].

The second topic which is related to finite quantum systems is the finite geometry of the phase space $\mathcal{Z}_d \times \mathcal{Z}_d$. In the case that d is prime, $\mathcal{Z}_d \times \mathcal{Z}_d$ is near-linear geometry, and two lines have at most one point in common. However, if d is composite, $\mathcal{Z}_d \times \mathcal{Z}_d$ is not near-linear geometry, and two lines may have more than one point in common.

The third topic which is related to finite quantum systems is the factorization of such systems into smaller subsystems. Consider a d-dimensional quantum system with Hilbert space $\mathcal{H}_d$, where $d = \prod p_i$ and $p_i,\ p_j$ are different prime numbers. Such a quantum system can be factorized in terms of smaller subsystems with Hilbert spaces $\mathcal{H}_{p_i}$ [5] based on the mapping introduced by Good [6].

1.1 Motivation

Our study of mutually unbiased bases in the Hilbert space $\mathcal{H}_d$ and the finite geometry of the $\mathcal{Z}_d \times \mathcal{Z}_d$ phase space, showed that there is a correspondence between the mutually unbiased bases in $\mathcal{H}_d$ and the lines through the origin in $\mathcal{Z}_d \times \mathcal{Z}_d$ when d is prime. However, such correspondence does not exist when d is composite number. Motivated by this fact, we introduce the concept of weak mutually unbiased bases that weakens the concept of mutually unbiased bases in odd dimensional systems (also, this concept can be applied for systems with even dimensions), and designed for the geometry $\mathcal{Z}_d \times \mathcal{Z}_d$ in the sense that there is a duality between weak mutually unbiased bases in $\mathcal{H}_d$ and the lines through the origin in $\mathcal{Z}_d \times \mathcal{Z}_d$. For simplicity we consider $d = p_1 p_2$, where d is odd and p_1, p_2 are prime numbers, however these bases are valid with any Hilbert space $\mathcal{H}_d$, where d is odd and $d = \prod p_i$. A complete set of these bases can be constructed by combining (as it will be shown later) the mutually unbiased in $\mathcal{H}_{p_1}$ and the mutually unbiased in $\mathcal{H}_{p_2}$. To make the duality between bases and lines clear, we discuss the factorization of a line in $\mathcal{Z}_d \times \mathcal{Z}_d$ in terms of two lines in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$ and $\mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$, respectively.

We show with examples that a complete set of weak mutually unbiased bases is tomographically complete in the sense that the probabilities from tomography experiments corresponding to these bases, can be used to construct an arbitrary density matrix. Another application of weak mutually unbiased bases is using these bases to generalize the BB84 quantum cryptography protocol to work with qudits of dimension $d = p_1 p_2$ where p_1, p_2 are prime numbers.

1.2 Structure of the thesis

This thesis consists of six chapters. This first chapter gives a brief introduction and the outline of the thesis. While chapter 2 gives a background review, chapters 3, 4, and 5 present our novel work.

In chapter 2, we present the fundamentals of finite quantum system. We discuss some operators that play an important role in finite quantum systems. We study symplectic transformations with an explicit numerical example. We introduce Wigner functions and Weyl functions as well as their properties. We consider the inverse Radon transform and its use in quantum tomography, and finally we present a review of mutually unbiased bases.

Chapter 3 discusses the lines in $\mathcal{Z}_d \times \mathcal{Z}_d$. We introduce the concept of line factorization and we present some properties of lines in $\mathcal{Z}_d \times \mathcal{Z}_d$.

In chapter 4, we present the new concept of weak mutually unbiased bases. We construct a complete set of weak mutually unbiased bases explicitly, and we show (with examples) that such set is tomographically complete. We discuss the duality between weak mutually unbiased bases and lines in $\mathcal{Z}_d \times \mathcal{Z}_d$. We end this chapter with presenting weak mutually unbiased bases in the context of complex projective t-design.

Chapter 5 gives a brief overview of the one-way and two-way quantum cryptography protocols. We propose a generalization of the BB84 protocol to work with qudits of dimension $d = p_1 p_2$ where p_1, p_2 are prime numbers, using weak mutually unbiased bases. Also we generalize the two way protocol to work with qudits rather than qubits. The proposed protocols are analyzed against the intercept and resend attack.

Finally, Chapter 6 concludes and discusses our results.

Chapter 2

Finite quantum systems

Quantum mechanics are often formulated in the framework of harmonic oscillator using position and momentum states, where the values of position and momentum are described by the set of real numbers $\mathcal{R}$. Therefore, the position and momentum phase space is $\mathcal{R} \times \mathcal{R}$. This chapter reviews their analogous formalism in quantum systems with finite Hilbert space $\mathcal{H}_d$. The coordinate axes of Hilbert space are mutually orthogonal. Finite systems were initially studied by Weyl [7] and Schwinger [8, 9], later some authors [4, 5, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21] have studied either finite systems or their applications. In a d-dimensional Hilbert space both position and momentum states are labeled by elements in $\mathcal{Z}_d$, where $\mathcal{Z}_d$ is the set of integers modulo d, and hence the position and momentum phase space is the toroidal lattice $\mathcal{Z}_d \times \mathcal{Z}_d$.

2.1 Introduction

We consider a quantum system with finite Hilbert space $\mathcal{H}_d$ where d is the dimension of this quantum system. we denote the position and momentum states as $|X;n\rangle$, $|P;n\rangle$ respectively, where $n \in \mathcal{Z}_d$. $|X;n\rangle$ and $|P;n\rangle$ are orthonormal bases, therefore

$$\langle X,m|X,n\rangle = \delta(m,n), \tag{2.1}$$

where $m,n \in \mathcal{Z}_d$ and $\delta(m,n)$ is the Kronecker delta. Also they obey the completeness relation

$$\sum_n |X;n\rangle\langle X;n| = \sum_n |P;n\rangle\langle P;n| = \mathcal{I}, \tag{2.2}$$

where $\mathcal{I}$ is the unity matrix.

An important application of the above relation is that any arbitrary vector $|u\rangle$ in $\mathcal{H}_d$ can be represented as a linear combination of the orthonormal states $|X;n\rangle$ or $|P;n\rangle$

$$\begin{aligned} |u\rangle &= \sum_n u_{X,n}|X;n\rangle \\ |u\rangle &= \sum_n u_{P,n}|P;n\rangle, \end{aligned} \tag{2.3}$$

where

$$u_{X,n} = \langle X; n|u\rangle$$
$$u_{P,n} = \langle P; n|u\rangle. \tag{2.4}$$

2.2 Linear operators

Linear operator $A : \mathcal{H}_{d_1} \to \mathcal{H}_{d_2}$ from vector space $\mathcal{H}_{d_1}$ to vector space $\mathcal{H}_{d_2}$ can be represented as a matrix of dimension $d_1 \times d_2$ [1, 22]. In the case that A is linear operator from $\mathcal{H}_d$ to $\mathcal{H}_d$, we call A a linear operator defined on $\mathcal{H}_d$. The operator A is called normal if it obeys the following equation

$$AA^\dagger = A^\dagger A, \tag{2.5}$$

where $A^\dagger$ is the conjugate transpose of A. The operator A is called unitary operator if it satisfies the following condition

$$A^{-1} = A^\dagger. \tag{2.6}$$

If A is unitary operator, then

$$AA^\dagger = A^\dagger A = \mathcal{I}, \tag{2.7}$$

therefore the unitary operators are also normal operators.
For any unitary operators $A : \mathcal{H}_d \to \mathcal{H}_d$ and $B : \mathcal{H}_d \to \mathcal{H}_d$, and any vectors $|u\rangle, |v\rangle \in \mathcal{H}_d$ The following properties hold.

(1) $A^\dagger$ is also unitary operator (because $(A^\dagger)^\dagger A^\dagger = AA^\dagger = \mathcal{I}$)

(2) The inner product between $|u\rangle, |v\rangle$ is preserved if the two vectors are transformed by A as
$\langle u|A^\dagger A|v\rangle = \langle u|v\rangle$.

(3) The unitary transformation can be reversed since $A^\dagger(A|u\rangle) = |u\rangle$

(4) The columns of A form an orthonormal basis.

(5) The rows of A form an orthonormal basis.

(6) The unitary transformation preserves the vector length as
$\sqrt{\langle u|A^\dagger A|u\rangle} = \sqrt{\langle u|u\rangle}$.

(7) For any orthonormal basis $|u;n\rangle$, $|v;n\rangle = A|u;n\rangle$ is also orthonormal basis.

(8) Unitary operators form a group because
$\langle u|v\rangle = \langle u|A^\dagger A|v\rangle = \langle u|B^\dagger B|v\rangle = \langle u|(AB)^\dagger(AB)|v\rangle$.

Another special class of normal operators is Hermitian operators (also called self-adjoint operators). Operator A is called Hermitian if it satisfies the following property

$$A = A^\dagger \tag{2.8}$$

Eq. (2.8) shows that Hermitian operators are normal operators. One important property of the Hermitian operator is that its eigenvalues are real. Positive operators is a subclass of Hermitian operators where for any vector

$|u\rangle, \langle u|A|u\rangle$ is non-negative real number; i.e. $\langle u|A|u\rangle \geq 0$. In the case that $\langle u|A|u\rangle > 0$ for all $|u\rangle \neq 0, A$ is called positive definite.

2.2.1 Pauli operators

Pauli operators $\sigma_x, \sigma_y, \sigma_z$ are operators in $\mathcal{H}_2$ that have important applications in quantum computation and quantum information where

$$\begin{aligned} \sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{2.9}$$

Pauli operators satisfy Eqs.(2.7, 2.8), therefore they are unitary and Hermitian operators

2.2.2 Fourier operator

We consider a quantum system with dimension d. The position and momentum states $|X; n\rangle, |P; n\rangle$ are two orthonormal bases in $\mathcal{H}_d$, where $n \in \mathcal{Z}_d$ and they are related to each other through Fourier transform. We define the

Fourier operator $\mathscr{F}$ as

$$\mathscr{F} = d^{-1/2} \sum_{m,n} \Omega^{mn} |X; m\rangle\langle X; n|, \tag{2.10}$$

where

$$\Omega^n = \Omega(n) = \exp\left(i\frac{2\pi n}{d}\right), \quad \frac{1}{d}\sum_n \Omega^{n(m_1-m_2)} = \delta(m_1, m_2). \tag{2.11}$$

Fourier transform is unitary operator so

$$\mathscr{F}\mathscr{F}^\dagger = \mathscr{F}^\dagger\mathscr{F} = \mathcal{I}. \tag{2.12}$$

Operating the Fourier operator twice gives the original data in reverse order, so operating it four times gives the original data back, then

$$\mathscr{F}^4 = \mathcal{I}. \tag{2.13}$$

Eq. (2.13) implies that Fourier operator has only four distinct eigenvalues namely $1, -1, i, -i$ with certain multiplicity [23]. Table (2.1) shows the multiplicity of these eigenvalues at all possible system dimensions and the trace of Fourier operator $Tr(\mathscr{F})$ according to these dimensions.

Since the momentum states are related to the position states through Fourier transform

$$|P; m\rangle = \mathscr{F}|X; m\rangle = d^{-1/2} \sum_n \Omega^{mn} |X; n\rangle, \tag{2.14}$$

Table 2.1: The multiplicity of the eigenvalues of Fourier operator at all possible system dimensions and the trace of Fourier operator according to these dimensions

	1	-1	i	$-i$	$Tr(\mathscr{F})$
$d = 4m$	$m+1$	m	m	$m-1$	$1+i$
$d = 4m+1$	$m+1$	m	m	m	1
$d = 4m+2$	$m+1$	$m+1$	m	m	0
$d = 4m+3$	$m+1$	$m+1$	$m+1$	m	i

therefore arbitrary state $|\psi\rangle$ can be represented using position and momentum states as

$$|\psi\rangle = \sum_n \alpha_n |X;n\rangle = \sum_m \beta_m |P;m\rangle, \quad \alpha_n = d^{-1/2} \sum_m \beta_m \Omega^{mn}. \tag{2.15}$$

2.2.3 Position and momentum operators

The position operator x and the momentum operator p are defined as

$$\begin{aligned} x &= \sum_n n|X;n\rangle\langle X;n|, \\ p &= \sum_n n|P;n\rangle\langle P;n|. \end{aligned} \tag{2.16}$$

The position operator and momentum operator are related to each other through Fourier transform

$$\begin{aligned} p &= \mathscr{F} x \mathscr{F}^\dagger, \\ x &= -\mathscr{F} p \mathscr{F}^\dagger. \end{aligned} \tag{2.17}$$

2.2.4 Density operator

Quantum states are described using state vectors. Another description of quantum states is using density operators (matrices) that give the measurement probabilities in more compact form. The density matrix $\mathcal{D}$ for a quantum system in a pure state $|\psi\rangle$ is

$$\mathcal{D} = |\psi\rangle\langle\psi| \tag{2.18}$$

If $|\psi\rangle$ is a superposition of N states

$$|\psi\rangle = \sum_{n=0}^{N-1} \alpha_n |\psi_n\rangle, \tag{2.19}$$

then

$$\mathcal{D} = \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} \alpha_m \alpha_n^* |\psi_m\rangle\langle\psi_n| \tag{2.20}$$

Density matrix is useful to represent a quantum system in mixed state as a mixed state cannot be described using a single state vector. The density matrix for a quantum system in a mixed state of N pure states $|\psi_n\rangle$ is

$$\mathcal{D} = \sum_{n=0}^{N-1} p_n |\psi_n\rangle\langle\psi_n|, \tag{2.21}$$

where p_n is the corresponding probability of the pure state $|\psi_n\rangle$. If the states $|\psi_n\rangle$ are transformed under the action of the unitary operator U, then the density matrix after this transformation $\mathcal{D}'$ is calculated as

$$\mathcal{D}' = \sum_n p_n U|\psi_n\rangle\langle\psi_n|U^\dagger = UDU^\dagger. \tag{2.22}$$

The probability p_n of the outcome $|n\rangle$ using the density matrix is

$$p_n = Tr(\mathcal{D}|n\rangle\langle n|). \tag{2.23}$$

The density matrix $\mathcal{D}$ has the following properties

(1) $\mathcal{D}$ is Hermitian.

(2) $\mathcal{D}$ is positive-semidefinite (i.e. for any arbitrary vector $|\chi\rangle$, $\langle\chi|\mathcal{D}|\chi\rangle \geq 0$) [1].

(3) $Tr(\mathcal{D}) = 1$ (when $\mathcal{D}$ is normalized).

(4) For systems in pure states $\mathcal{D}^2 = \mathcal{D}$.

(5) For systems in pure states $Tr(\mathcal{D}^2) = 1$ and for systems in mixed states $Tr(\mathcal{D}^2) < 1$ [22].

Since the density operator is Hermitian and its trace is equal to 1 then it contains $d^2 - 1$ real independent parameters.

2.2.5 Displacement operator

In finite quantum systems the position states and momentum states are labeled by elements in $\mathcal{Z}_d$ where d is the system dimension. Therefore, the position-momentum phase-space is the toroidal lattice $\mathcal{Z}_d \times \mathcal{Z}_d$. We define the displacement operators that perform displacements along the momentum and position axes in the position-momentum phase-space as

$$\mathscr{Z} = \exp\left(i\frac{2\pi}{d}x\right), \quad \mathscr{X} = \exp\left(-i\frac{2\pi}{d}p\right). \tag{2.24}$$

$\mathscr{Z}$ and $\mathscr{X}$ are unitary operators that satisfy the relations

$$\mathscr{Z}^{\alpha} = \sum_{n \in \mathcal{Z}_d} \Omega^{n\alpha} |X; n\rangle\langle X; n|, \tag{2.25}$$

$$\mathscr{X}^{\beta} = \sum_{n \in \mathcal{Z}_d} \Omega^{-n\beta} |P; n\rangle\langle P; n|, \tag{2.26}$$

and act on both position and momentum states as follows

$$\begin{aligned} \mathscr{Z}^{\alpha}|X; m\rangle = \Omega^{\alpha m}|X; m\rangle, \quad \mathscr{Z}^{\alpha}|P; m\rangle = |P; m+\alpha\rangle, \\ \mathscr{X}^{\beta}|X; m\rangle = |X; m+\beta\rangle, \quad \mathscr{X}^{\beta}|P; m\rangle = \Omega^{-\beta m}|P; m\rangle, \end{aligned} \tag{2.27}$$

where $\alpha, \beta \in \mathcal{Z}_d$.

Eq. (2.24) shows that

$$\mathscr{X}^{d} = \mathscr{Z}^{d} = \mathcal{I}. \tag{2.28}$$

Based on Eqs. (2.27), $\mathscr{Z}, \mathscr{X}$ obey the following relation

$$\mathscr{X}^{\beta}\mathscr{Z}^{\alpha} = \mathscr{Z}^{\alpha}\mathscr{X}^{\beta}\Omega^{-\alpha\beta}. \tag{2.29}$$

Acting with Fourier operator on $\mathscr{Z}, \mathscr{X}$ we find

$$\mathscr{F}\mathscr{Z}\mathscr{F}^{\dagger} = \mathscr{X}^{-1}, \quad \mathscr{F}\mathscr{X}\mathscr{F}^{\dagger} = \mathscr{Z}. \tag{2.30}$$

When $d = 2$, the two matrices $\langle X; m|\mathscr{X}|X; n\rangle$ and $\langle X; m|\mathscr{Z}|X; n\rangle$ are indeed the Pauli matrices σ_x, σ_z, respectively.

In the case that d is odd, we define the general displacement operator as

$$\mathscr{D}(\alpha,\beta)=\mathscr{Z}^{\alpha}\mathscr{X}^{\beta}\Omega^{-2^{-1}\alpha\beta},\quad [\mathscr{D}(\alpha,\beta)]^{\dagger}=\mathscr{D}(-\alpha,-\beta). \tag{2.31}$$

The existence of 2^{-1} is guaranteed by the fact that $2, d$ are coprime (if $d = 2n+1, n$ is integer, then $2^{-1} = n+1$). Eq. (2.31) shows that the general displacement operator acts on both position and momentum states as follows

$$\mathscr{D}(\alpha,\beta)|X;m\rangle=\Omega^{(2^{-1}\alpha\beta+\alpha m)}|X;m+\beta\rangle, \tag{2.32}$$

$$\mathscr{D}(\alpha,\beta)|P;m\rangle=\Omega^{(-2^{-1}\alpha\beta-\beta m)}|P;m+\alpha\rangle. \tag{2.33}$$

The general displacement operators are unitary operators that form Heisenberg-Weyl group [5, 24]. Starting with Eq. (2.31) and using Eq. (2.29) we get

$$\mathscr{D}(\alpha_1,\beta_1)\mathscr{D}(\alpha_2,\beta_2)=\mathscr{D}(\alpha_1+\alpha_2,\beta_1+\beta_2)\Omega^{[2^{-1}(\alpha_1\beta_2-\alpha_2\beta_1)]}. \tag{2.34}$$

Eq. (2.30) leads us to find the action of Fourier transform on the displacement operator

$$\mathscr{F}\mathscr{D}(\alpha,\beta)\mathscr{F}^{\dagger}=\mathscr{D}(\beta,-\alpha). \tag{2.35}$$

Displacement operators have the following marginal properties [5]

$$\begin{aligned}\frac{1}{d}\sum_{\beta}\mathscr{D}(\alpha,\beta)&=|P;2^{-1}\alpha\rangle\langle P;-2^{-1}\alpha|,\\ \frac{1}{d}\sum_{\alpha}\mathscr{D}(\alpha,\beta)&=|X;2^{-1}\beta\rangle\langle X;-2^{-1}\beta|.\end{aligned} \tag{2.36}$$

2.2.6 Parity operator

The parity operator around arbitrary point in the position-momentum phase space is presented in [5]. Around the origin it is defined as

$$\mathscr{P}(0,0) = \mathscr{F}^2, \qquad [\mathscr{P}(0,0)]^2 = \mathcal{I}. \tag{2.37}$$

The parity operator has the following properties

$$\begin{aligned} \mathscr{P}(0,0)|X;m\rangle = |X;-m\rangle, \qquad \mathscr{P}(0,0)|P;m\rangle = |P;-m\rangle, \\ \mathscr{P}(0,0)x[\mathscr{P}(0,0)]^\dagger = -x, \qquad \mathscr{P}(0,0)p[\mathscr{P}(0,0)]^\dagger = -p, \\ \mathscr{P}(0,0)\mathscr{Z}[\mathscr{P}(0,0)]^\dagger = \mathscr{Z}^\dagger, \qquad \mathscr{P}(0,0)\mathscr{X}[\mathscr{P}(0,0)]^\dagger = \mathscr{X}^\dagger. \end{aligned} \tag{2.38}$$

The parity operator around the origin has two eigenvalues, 1, and -1 (as $[\mathscr{P}(0,0)]^2 = \mathcal{I}$). The multiplicity of these eigenvalues is presented in [5]. Table (2.2) shows the multiplicity of the eigenvalues of the parity operator around the origin and its trace $Tr[\mathscr{P}(0,0)]$ for both even and odd dimensional systems. The displaced parity operator around the point (α, β) is defined as

Table 2.2: The multiplicity of the eigenvalues of the parity operator around the origin for both even and odd dimensional systems and its trace according to these dimensions

	1	-1	$Tr[\mathscr{P}(0,0)]$
$d = 2m$	$m+1$	$m-1$	2
$d = 2m+1$	$m+1$	m	1

$$\mathscr{P}(\alpha,\beta) = \mathscr{D}(\alpha,\beta)\mathscr{P}(0,0)[\mathscr{D}(\alpha,\beta)]^\dagger. \tag{2.39}$$

using Eqs.(2.31, 2.35, 2.37) we find

$$\mathscr{P}(\alpha,\beta)=\mathscr{D}(2\alpha,2\beta)\mathscr{P}(0,0)=\mathscr{P}(0,0)[\mathscr{D}(2\alpha,2\beta)]^{\dagger}. \tag{2.40}$$

Like the parity operator around the origin $\mathscr{P}(0,0)$, the displaced parity operator $\mathscr{P}(\alpha,\beta)$ has the property

$$[\mathscr{P}(\alpha,\beta)]^2=\mathcal{I}. \tag{2.41}$$

Also the trace and the eigenvalues of $\mathscr{P}(\alpha,\beta)$ and their multiplicity are the same as $\mathscr{P}(0,0)$. It is worth noting that the displaced parity operator is the Fourier transform of the displacement operator

$$\mathscr{P}(\alpha,\beta)=\frac{1}{d}\sum_{\gamma,\delta}\mathscr{D}(\gamma,\delta)\Omega(\delta\alpha-\gamma\beta), \tag{2.42}$$

$$\mathscr{D}(\gamma,\delta)=\frac{1}{d}\sum_{\alpha,\beta}\mathscr{P}(\alpha,\beta)\Omega(-\delta\alpha+\gamma\beta). \tag{2.43}$$

The marginal properties of parity operators are

$$\begin{aligned}\frac{1}{d}\sum_{\beta}\mathscr{P}(\alpha,\beta)&=|P;\alpha\rangle\langle P;\alpha|,\\ \frac{1}{d}\sum_{\alpha}\mathscr{P}(\alpha,\beta)&=|X;\beta\rangle\langle X;\beta|.\end{aligned} \tag{2.44}$$

2.3 Symplectic transformations

The symplectic transformation $\mathcal{S}(\kappa, \lambda|\mu, \nu)$ is a unitary transformation with the parameters $\kappa, \lambda, \mu, \nu \in \mathcal{Z}_d$ such that

$$\kappa\nu - \lambda\mu = 1 \ \ (mod \quad d). \tag{2.45}$$

The four parameters of the symplectic transformation contain three independent parameters and one dependent parameter. For this reason this transformation has to do with the multiplicative inverses in $\mathcal{Z}_d$. For example, if we choose λ to be the dependent parameter, the multiplicative inverse of μ must be exist as $\lambda = \mu^{-1}(\kappa\nu - 1)$. The matrices

$$\mathrm{g}(\kappa, \lambda|\mu, \nu) = \begin{pmatrix} \kappa & \lambda \\ \\ \mu & \nu \end{pmatrix} \tag{2.46}$$

with the constraint of Eq.(2.45) form the group of symplectic matrices $\mathcal{S}p(2, \mathcal{Z}_d)$. The cardinality of this group is $\mathbb{J}_2(d)$ [25], where $\mathbb{J}_2(d)$ is the Jordan totient function.

The symplectic transformations of the operators $\mathscr{X}$, and $\mathscr{Z}$ obey the relation

$$\begin{aligned} \mathscr{X}' &= \mathcal{S}(\kappa, \lambda|\mu, \nu)\mathscr{X}[\mathcal{S}(\kappa, \lambda|\mu, \nu)]^\dagger = \mathscr{X}^\kappa \mathscr{Z}^\lambda \Omega(2^{-1}\kappa\lambda) = \mathscr{D}(\lambda, \kappa), \\ \mathscr{Z}' &= \mathcal{S}(\kappa, \lambda|\mu, \nu)\mathscr{Z}[\mathcal{S}(\kappa, \lambda|\mu, \nu)]^\dagger = \mathscr{X}^\mu \mathscr{Z}^\nu \Omega(2^{-1}\mu\nu) = \mathscr{D}(\nu, \mu). \end{aligned} \tag{2.47}$$

The constraint of Eq. (2.45) guarantees that the operators $\mathscr{X}', \mathscr{Z}'$ obey

Eqs. (2.28 and 2.29), and therefore they are displacement operators.
Also the general displacement operator is affected by the symplectic transformation

$$\mathcal{S}(\kappa,\lambda|\mu,\nu)\mathscr{D}(\alpha,\beta)[\mathcal{S}(\kappa,\lambda|\mu,\nu)]^{\dagger}=\mathscr{D}(\nu\alpha+\lambda\beta,\mu\alpha+\kappa\beta). \tag{2.48}$$

Acting on $\mathscr{X}$ with the symplectic transformation $\mathcal{S}(\kappa_1,\lambda_1|\mu_1,\nu_1)$ we get

$$\mathcal{S}(\kappa_1,\lambda_1|\mu_1,\nu_1)\mathscr{X}[\mathcal{S}(\kappa_1,\lambda_1|\mu_1,\nu_1)]^{\dagger}=\mathscr{D}(\lambda_1,\kappa_1). \tag{2.49}$$

Acting on $\mathscr{D}(\lambda_1,\kappa_1)$ with the symplectic transformation $\mathcal{S}(\kappa_2,\lambda_2|\mu_2,\nu_2)$ we get

$$\mathcal{S}(\kappa_2,\lambda_2|\mu_2,\nu_2)\mathscr{D}(\lambda_1,\kappa_1)[\mathcal{S}(\kappa_2,\lambda_2|\mu_2,\nu_2)]^{\dagger}=\mathscr{D}(\nu_2\lambda_1+\lambda_2\kappa_1,\mu_2\lambda_1+\kappa_2\kappa_1). \tag{2.50}$$

Similarly, acting on $\mathscr{Z}$ with the symplectic transformation $\mathcal{S}(\kappa_1,\lambda_1|\mu_1,\nu_1)$, we get $\mathscr{D}(\nu_1,\mu_1)$, then acting with the symplectic transformation $\mathcal{S}(\kappa_2,\lambda_2|\mu_2,\nu_2)$ on $\mathscr{D}(\nu_1,\mu_1)$ we get

$$\mathcal{S}(\kappa_2,\lambda_2|\mu_2,\nu_2)\mathscr{D}(\nu_1,\mu_1)[\mathcal{S}(\kappa_2,\lambda_2|\mu_2,\nu_2)]^{\dagger}=\mathscr{D}(\nu_2\nu_1+\lambda_2\mu_1,\mu_2\nu_1+\kappa_2\mu_1). \tag{2.51}$$

Eqs. (2.50, 2.51) show that

$$\mathcal{S}(\kappa_2,\lambda_2|\mu_2,\nu_2)\mathcal{S}(\kappa_1,\lambda_1|\mu_1,\nu_1)=\mathcal{S}(\kappa,\lambda|\mu,\nu), \tag{2.52}$$

where

$$\begin{pmatrix} \kappa_1 & \lambda_1 \\ \mu_1 & \nu_1 \end{pmatrix} \begin{pmatrix} \kappa_2 & \lambda_2 \\ \mu_2 & \nu_2 \end{pmatrix} = \begin{pmatrix} \kappa & \lambda \\ \mu & \nu \end{pmatrix}. \tag{2.53}$$

The identity element of the symplectic transformation is $\mathcal{S}(1,0|0,1)$ and the inverses of the symplectic transformations exist, then symplectic transformations form a group $\mathcal{S}p(2,\mathcal{Z}_d)$.

The symplectic transformation in finite dimensional systems can be calculated numerically [5] as follows

(1) Consider the matrix

$$\langle X;m|\mathscr{Z}'|X;n\rangle = \Omega(2^{-1}\nu\mu + n\nu)\delta(m,n+\mu). \tag{2.54}$$

(2) Consider the matrix

$$\langle X;m|\mathscr{X}'|X;n\rangle = \Omega(2^{-1}\kappa\lambda + n\lambda)\delta(m,n+\kappa). \tag{2.55}$$

(3) Calculate the normalized eigenvectors of the matrix $\langle X;m|\mathscr{Z}'|X;n\rangle$ and their corresponding eigenvalues. We note that the eigenvectors of this matrix are the states $|X';m\rangle$ up to a phase factor.

(4) Starting with the eigenvector $|X';0\rangle$ corresponding to the eigenvalue 1 we get the other eigenvectors $|X';m\rangle, m \neq 0$ according to the relation

$$|X';m\rangle = (\mathscr{X}')^m|X';0\rangle. \tag{2.56}$$

(5) Calculate the symplectic transformation $\mathcal{S}$ as

$$\mathcal{S}(m,n) = \langle X; m | X'; n \rangle, \tag{2.57}$$

where $\mathcal{S}(m,n)$ is the matrix form of the operator $\mathcal{S}$.

As an example we apply the previously mentioned steps to get the symplectic transformation $\mathcal{S}(2,3|1,2)$ in a five-dimensional Hilbert space.
According to Eqs. (2.47)

$$\mathscr{X}' = \mathscr{X}^2 \mathscr{Z}^3 \Omega(3), \tag{2.58}$$

$$\mathscr{Z}' = \mathscr{X} \mathscr{Z}^2 \Omega(1). \tag{2.59}$$

Starting with the computational basis and using Eqs. (2.54, 2.55)

$$\langle X; m | \mathscr{Z}' | X; n \rangle = \begin{pmatrix} 0 & 0 & 0 & 0 & 0.309 - 0.951i \\ 0.309 + 0.951i & 0 & 0 & 0 & 0 \\ 0 & -0.809 - 0.588i & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -0.809 - 0.588i & 0 \end{pmatrix} \tag{2.60}$$

$$\langle X;m|\mathscr{X}'|X;n\rangle = \begin{pmatrix} 0 & 0 & 0 & -0.809+0.588i & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -0.809-0.588i & 0 & 0 & 0 & 0 \\ 0 & 0.309+0.951i & 0 & 0 & 0 \\ 0 & 0 & 0.309-0.951i & 0 & 0 \end{pmatrix} \tag{2.61}$$

The eigenvector corresponding to eigenvalue 1 is

$$|X';0\rangle = \begin{pmatrix} 0.138-0.425i \\ 0.447 \\ -0.362-0.263i \\ -0.362-0.263i \\ 0.447 \end{pmatrix} \tag{2.62}$$

Using Eqn. (2.56) we get $|X';m\rangle$, $m = 1,2,3,4$.

We use Eqn (2.57) to calculate the Operator $\mathcal{S}(2,3|1,2)$

$$\mathcal{S}(2,3|1,2) = \begin{pmatrix} 0.138-0.425i & 0.447 & -0.362-0.263i & -0.362-0.263i & 0.447 \\ 0.447 & 0.447 & -0.362+0.263i & 0.138+0.425i & -0.362+0.263i \\ -0.362-0.263i & -0.362+0.263i & -0.362-0.263i & 0.138+0.425i & 0.138+0.425i \\ -0.362-0.263i & 0.138+0.425i & 0.138+0.425i & -0.362-0.263i & -0.362+0.263i \\ 0.447 & -0.362+0.263i & 0.138+0.425i & -0.362+0.263i & 0.447 \end{pmatrix}$$

Let $|X(\kappa,\lambda|\mu,\nu);m\rangle = \mathcal{S}(\kappa,\lambda|\mu,\nu)|X;m\rangle$ and $|P(\kappa,\lambda|\mu,\nu);m\rangle = \mathcal{S}(\kappa,\lambda|\mu,\nu)|P;m\rangle$.

Acting with the symplectic transformation $\mathcal{S}(\kappa,\lambda|\mu,\nu)$ on both sides of Eqs. (2.36) and taking into account Eq.(2.48) we get

$$\frac{1}{d}\sum_{\beta}\mathscr{D}(\alpha\nu+\beta\lambda,\alpha\mu+\beta\kappa)= \\ |P(\kappa,\lambda|\mu,\nu);2^{-1}\alpha\rangle\langle P(\kappa,\lambda|\mu,\nu);-2^{-1}\alpha|, \\ \frac{1}{d}\sum_{\alpha}\mathscr{D}(\alpha\nu+\beta\lambda,\alpha\mu+\beta\kappa)= \\ |X(\kappa,\lambda|\mu,\nu);2^{-1}\beta\rangle\langle X(\kappa,\lambda|\mu,\nu);-2^{-1}\beta|. \tag{2.63}$$

In similar way we act with the symplectic transformation $\mathcal{S}(\kappa,\lambda|\mu,\nu)$ on both sides of Eqs. (2.44), then we get

$$\frac{1}{d}\sum_{\beta}\mathcal{S}(\kappa,\lambda|\mu,\nu)\mathscr{P}(\alpha,\beta)[\mathcal{S}(\kappa,\lambda|\mu,\nu)]^{\dagger}= \\ |P(\kappa,\lambda|\mu,\nu);\alpha\rangle\langle P(\kappa,\lambda|\mu,\nu);\alpha|, \\ \frac{1}{d}\sum_{\alpha}\mathcal{S}(\kappa,\lambda|\mu,\nu)\mathscr{P}(\alpha,\beta)[\mathcal{S}(\kappa,\lambda|\mu,\nu)]^{\dagger}= \\ |X(\kappa,\lambda|\mu,\nu);\beta\rangle\langle X(\kappa,\lambda|\mu,\nu);\beta|. \tag{2.64}$$

2.4 Wigner functions and Weyl functions

In 1932 Eugene Wigner [26] defined Wigner function as

$$\mathcal{W}(x,p)=\frac{1}{2\pi}\int_{-\infty}^{\infty}\langle x+\frac{1}{2}\xi|\ \mathcal{D}|x-\frac{1}{2}\xi\rangle\ \exp(-ip\xi)\ d\xi, \tag{2.65}$$

Where ξ is the quantum jump between two position states, and $\hbar = 1$ (here and throughout the thesis). Also Wigner function can be defined using the momentum representation as

$$\mathcal{W}(x,p) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \langle p + \frac{1}{2}\varepsilon|\ \mathcal{D}|p - \frac{1}{2}\varepsilon\rangle\ \exp(ix\varepsilon)\ d\varepsilon, \tag{2.66}$$

Where ε is the quantum jump between two momentum states.

Wigner function aims to link quantum states to a probability distribution, however it might have negative values when it describes a quantum system in a superposition state (superposition of two or more states). In this case the negative values can be related to the interference between these states. Due to the fact that Wigner function might have negative values, the Wigner distribution is called a quasi-probability distribution.

The two dimensional Fourier transform of Wigner function is Weyl function, and it is defined as

$$\widetilde{\mathcal{W}}(\xi,\varepsilon) = \int_{-\infty}^{\infty} \langle x + \frac{1}{2}\xi|\ \mathcal{D}|x - \frac{1}{2}\xi\rangle\ \exp(-ix\varepsilon)\ dx, \tag{2.67}$$

or

$$\widetilde{\mathcal{W}}(\xi,\varepsilon) = \int_{-\infty}^{\infty} \langle p + \frac{1}{2}\varepsilon|\ \mathcal{D}|p - \frac{1}{2}\varepsilon\rangle\ \exp(ip\xi)\ dp, \tag{2.68}$$

Wigner function and Weyl function have been discussed in [27, 28, 29, 30, 31]. They are commonly used in the phase space formulation of quantum mechanics and have many applications in quantum tomography [33, 34, 35, 36, 37, 38, 39, 40, 41], quantum teleportation [42, 43], and quantum cryptography

[44, 45].

The analogous definitions for Wigner function and Weyl function in finite dimensional systems have been studied in [5, 46, 47], in the next two subsections we shed the light on these studies.

2.4.1 Wigner functions

In finite dimensional systems we consider the operator θ, and define the two matrices θ_X, θ_P such that

$$\begin{aligned} \theta_X &= \langle X; m|\theta|X; n\rangle, \\ \theta_P &= \langle P; m|\theta|P; n\rangle. \end{aligned} \tag{2.69}$$

The Wigner function corresponding to the operator θ is defined in terms of the parity operator as

$$\mathcal{W}_\theta(\alpha, \beta) = Tr[\theta \mathscr{P}(\alpha, \beta)] \tag{2.70}$$

It can also be defined as

$$\begin{aligned} \mathcal{W}_\theta(\alpha, \beta) &= \Omega(2\alpha\beta) \sum_n \Omega(-2\alpha n)\theta_X(n, 2\beta - n), \\ &= \Omega(-2\alpha\beta) \sum_n \Omega(2\beta n)\theta_P(n, 2\alpha - n) \end{aligned} \tag{2.71}$$

For odd $d-$ dimensional systems, [5] has shown the marginal properties of Wigner function

$$\begin{aligned}\frac{1}{d}\sum_{\alpha}\mathcal{W}_{\theta}(\alpha,\beta)&=\theta_X(\beta,\beta),\\ \frac{1}{d}\sum_{\beta}\mathcal{W}_{\theta}(\alpha,\beta)&=\theta_P(\alpha,\alpha),\\ \frac{1}{d}\sum_{\alpha,\beta}\mathcal{W}_{\theta}(\alpha,\beta)&=Tr(\theta).\end{aligned}\tag{2.72}$$

Wigner functions corresponding to density operators $\mathcal{D}$ are real because density operators are Hermitian. Eqs. (2.72) show that Wigner function can be read as the probability distribution of the particle in the position-momentum phase space because the probability distribution of position states $p_X(\alpha) = \langle X;\alpha|\mathcal{D}|X;\alpha\rangle$, is the summation of Wigner function along the $P-$ axis and the probability distribution of momentum states $p_P(\beta) = \langle P;\beta|\mathcal{D}|P;\beta\rangle$, is the summation of Wigner function along the $X-$ axis.

As an example we consider a five dimensional quantum system with a pure state $|\psi\rangle$ where

$$\begin{aligned}|\psi\rangle = \frac{1}{\sqrt{37}}[&i|X;0\rangle + (3-i)|X;1\rangle + 4|X;2\rangle + (i+2)|X;3\rangle\\ &+ (2i-1)|X;4\rangle]\end{aligned}\tag{2.73}$$

Fig.(2.1) shows the Wigner function corresponding to the density matrix of this system, and Figs. (2.2, 2.3) illustrate the probability distribution of the position states and momentum states, respectively.

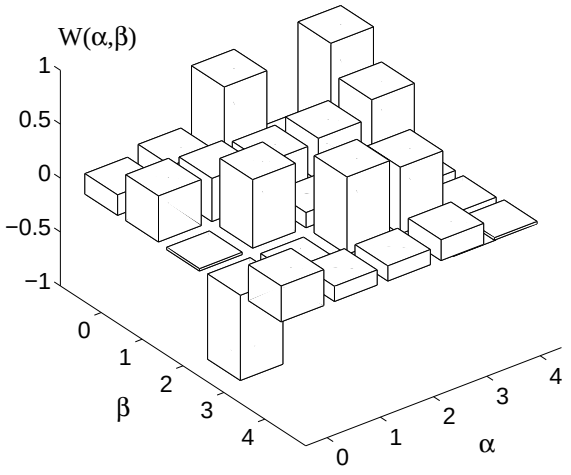

Figure 2.1: Wigner function for the pure state of Eq.(2.73).

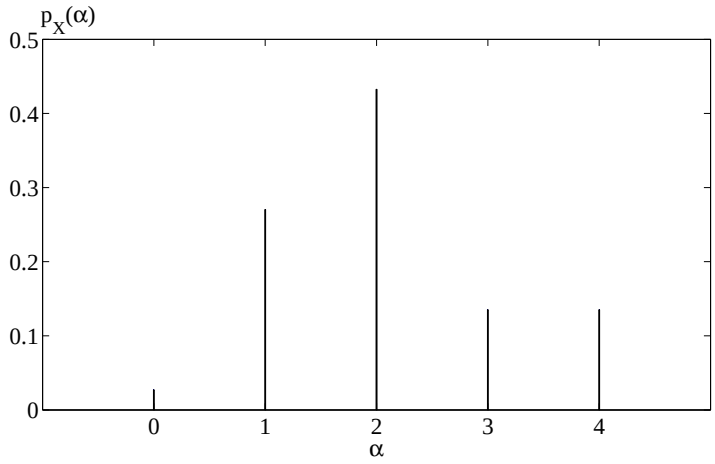

Figure 2.2: The probability distribution of the position states for the quantum system in pure state of Eq.(2.73).

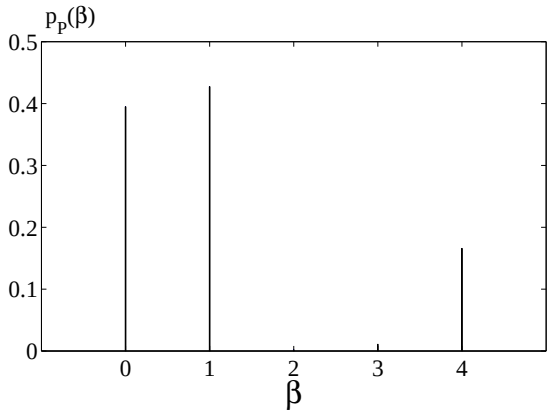

Figure 2.3: The probability distribution of the momentum states for the quantum system in the pure state of Eq.(2.73).

2.4.2 Weyl functions

Weyl function corresponding to the operator θ is related to the displacement operator as

$$\widetilde{\mathcal{W}}_\theta(\gamma,\delta) = Tr[\theta\mathscr{D}(\gamma,\delta)]. \tag{2.74}$$

Also we define it as

$$\begin{aligned}\widetilde{\mathcal{W}}_\theta(\gamma,\delta) &= \Omega(2^{-1}\gamma\delta)\sum_n \Omega(\gamma n)\theta_X(n,\delta+n),\\ &= \Omega(-2^{-1}\gamma\delta)\sum_n \Omega(-\delta n)\theta_P(n,\gamma+n).\end{aligned} \tag{2.75}$$

For odd $d-$ dimensional systems the marginal properties of Weyl function are

$$\frac{1}{d}\sum_{\gamma}\widetilde{\mathcal{W}}_{\theta}(\gamma,\delta)=\theta_X(-2^{-1}\delta,2^{-1}\delta),$$
$$\frac{1}{d}\sum_{\delta}\widetilde{\mathcal{W}}_{\theta}(\gamma,\delta)=\theta_P(-2^{-1}\gamma,2^{-1}\gamma),$$
$$\frac{1}{d}\sum_{\gamma,\delta}\widetilde{\mathcal{W}}_{\theta}(\gamma,\delta)=\mathcal{W}_{\theta}(0,0). \tag{2.76}$$

Weyl function and Wigner function are related to each other through Fourier transform [5]

$$\widetilde{\mathcal{W}}_{\theta}(\gamma,\delta)=\frac{1}{d}\sum_{\alpha,\beta}\mathcal{W}_{\theta}(\alpha,\beta)\Omega(\gamma\beta-\delta\alpha). \tag{2.77}$$

Fig.(2.4) shows the Weyl function of the pure state of Eq.(2.73)

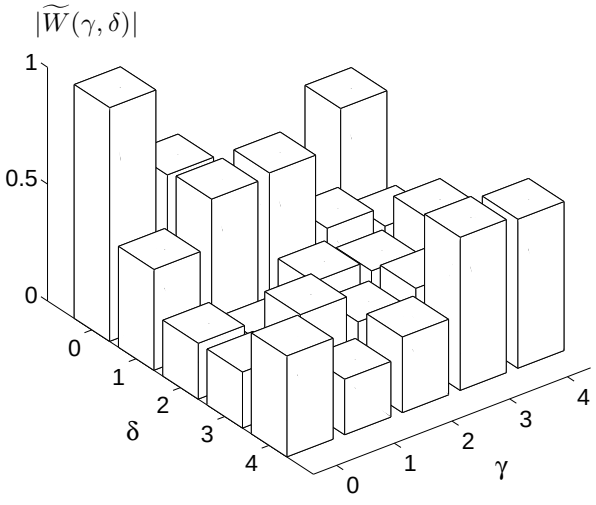

Figure 2.4: Weyl function for the pure state of Eq.(2.73).

2.5 Radon transforms and quantum tomography

Radon transforms for quantum systems with variables in $\mathcal{Z}_d$ have been introduced in [5]. We can write the first Eq. of Eqs.(2.63) as

$$\frac{1}{d}\sum_{\beta,\alpha'}\mathscr{D}(\alpha'\nu+\beta\lambda,\alpha'\mu+\beta\kappa)\delta(\alpha,\alpha') = |P(\kappa,\lambda|\mu,\nu);2^{-1}\alpha\rangle\langle P(\kappa,\lambda|\mu,\nu);-2^{-1}\alpha|. \tag{2.78}$$

We define the two varibles ρ,σ in $\mathcal{Z}_d$ such that

$$\rho=\alpha'\nu+\beta\lambda,\quad \sigma=\alpha'\mu+\beta\kappa. \tag{2.79}$$

Using Eqs.(2.45, 2.79) we prove that

$$\alpha'=\kappa\rho-\lambda\sigma,\quad \beta=-\mu\rho+\nu\sigma. \tag{2.80}$$

As long as α' and β take all values in $\mathcal{Z}_d$, ρ and σ take all values in $\mathcal{Z}_d$. Therefore, Eq.(2.78) is equivalent to

$$\frac{1}{d}\sum_{\rho,\sigma}\mathscr{D}(\rho,\sigma)\delta(\alpha,\kappa\rho-\lambda\sigma) = |P(\kappa,\lambda|\mu,\nu);2^{-1}\alpha\rangle\langle P(\kappa,\lambda|\mu,\nu);-2^{-1}\alpha|. \tag{2.81}$$

Similarly we can prove that

$$\frac{1}{d}\sum_{\rho,\sigma}\mathscr{D}(\rho,\sigma)\delta(\beta,-\mu\rho+\nu\sigma)= \\ |X(\kappa,\lambda|\mu,\nu);2^{-1}\beta\rangle\langle X(\kappa,\lambda|\mu,\nu);-2^{-1}\beta|. \tag{2.82}$$

Also, it has been proved that Radon transform can be formulated using parity operators as [5]

$$\frac{1}{d}\sum_{\rho,\sigma}\mathscr{P}(\rho,\sigma)\delta(\alpha,\kappa\rho-\lambda\sigma)=|P(\kappa,\lambda|\mu,\nu);\alpha\rangle\langle P(\kappa,\lambda|\mu,\nu);\alpha|, \\ \frac{1}{d}\sum_{\rho,\sigma}\mathscr{P}(\rho,\sigma)\delta(\beta,-\mu\rho+\nu\sigma)=|X(\kappa,\lambda|\mu,\nu);\beta\rangle\langle X(\kappa,\lambda|\mu,\nu);\beta|. \tag{2.83}$$

Eq.(2.83) shows that starting with the parity operator we can get the projectors $|P(\kappa,\lambda|\mu,\nu);\alpha\rangle\langle P(\kappa,\lambda|\mu,\nu);\alpha|$ and $|X(\kappa,\lambda|\mu,\nu);\beta\rangle\langle X(\kappa,\lambda|\mu,\nu);\beta|$. Also the reverse is applicable, starting with the projectors $|P(\kappa,\lambda|\mu,\nu);\beta\rangle\langle P(\kappa,\lambda|\mu,\nu);\beta|$ or $|X(\kappa,\lambda|\mu,\nu);\beta\rangle\langle X(\kappa,\lambda|\mu,\nu);\beta|$, we can find the displacement operator using the following equation [5]

$$\mathscr{D}(\alpha\lambda,\alpha\kappa)=\sum_{\beta}|P(\kappa,\lambda|\mu,\nu);\beta\rangle\langle P(\kappa,\lambda|\mu,\nu);\beta|\Omega(-\alpha\beta), \\ \mathscr{D}(\alpha\nu,\alpha\mu)=\sum_{\beta}|X(\kappa,\lambda|\mu,\nu);\beta\rangle\langle X(\kappa,\lambda|\mu,\nu);\beta|\Omega(\alpha\beta), \tag{2.84}$$

then using Eq. (2.42) we can get the parity operator. This is called inverse Radon transform. Similarly inverse Radon transform of Eqs. (2.81,2.82) can be done.

One important application of inverse Radon transform is quantum tomography. Quantum tomography is the process of reconstructing the density matrix of the quantum system using the probabilities corresponding to experimental measurements according to different projectors. In the following we discuss how we can apply inverse Radon transform using these probabilities to construct the density matrix.

Multiplying Eq. (2.83) by the density matrix then taking the trace we find

$$\frac{1}{d}\sum_{\rho,\sigma}\mathcal{W}(\rho,\sigma)\delta(\alpha,\kappa\rho-\lambda\sigma)= Tr(\mathcal{D}|P(\kappa,\lambda|\mu,\nu);\alpha\rangle\langle P(\kappa,\lambda|\mu,\nu);\alpha|),$$
$$\frac{1}{d}\sum_{\rho,\sigma}\mathcal{W}(\rho,\sigma)\delta(\beta,-\mu\rho+\nu\sigma)= Tr(\mathcal{D}|X(\kappa,\lambda|\mu,\nu);\beta\rangle\langle X(\kappa,\lambda|\mu,\nu);\beta|). \quad (2.85)$$

Now we apply inverse Radon transform to Eqs. (2.85) similar to the inverse Radon transform of Eq. (2.83), and we get

$$\widetilde{\mathcal{W}}(\beta\lambda,\beta\kappa)=\sum_{\alpha}p_P(\alpha|\lambda,\kappa)\Omega(-\alpha\beta),$$
$$\widetilde{\mathcal{W}}(\alpha\nu,\alpha\mu)=\sum_{\beta}p_X(\beta|\nu,\mu)\Omega(\alpha\beta), \quad (2.86)$$

where $p_P(\alpha|\lambda,\kappa)=Tr(\mathcal{D}|P(\kappa,\lambda|\mu,\nu);\alpha\rangle\langle P(\kappa,\lambda|\mu,\nu);\alpha|)$ and $p_X(\beta|\nu,\mu)=Tr(\mathcal{D}|X(\kappa,\lambda|\mu,\nu);\beta\rangle\langle X(\kappa,\lambda|\mu,\nu);\beta|)$. $p_P(\beta|\lambda,\kappa)$ and $p_X(\beta|\nu,\mu)$ denote the probabilities from the experimental measurements according to the projector $|P(\kappa,\lambda|\mu,\nu);\beta\rangle\langle P(\kappa,\lambda|\mu,\nu);\beta|$ and $|X(\kappa,\lambda|\mu,\nu);\beta\rangle\langle X(\kappa,\lambda|\mu,\nu);\beta|$, respectively. In [5] it has been shown that density matrix is related to Weyl function

and displacement operator as

$$\mathcal{D} = \frac{1}{d}\sum_{\alpha,\beta}\widetilde{\mathcal{W}}(-\alpha,-\beta)\mathscr{D}(\alpha,\beta). \tag{2.87}$$

Eqs. (2.86, 2.87) show that, starting with the probabilities and using inverse Radon transform we can construct the density matrix.

We give an example of quantum system where $d = 11$ and the system in the pure state $|\psi\rangle$ where

$$|\psi\rangle = \frac{1}{\sqrt{61}}[(1+i)|X;0\rangle + (-2+i)|X;1\rangle + (3+2i)|X;4\rangle + 2|X;5\rangle + (3i)|X;7\rangle + (-1+i)|X;8\rangle + (3+i)|X;9\rangle + 4|X;10\rangle]. \tag{2.88}$$

We start with the probabilities $p_X(\beta|\nu,\mu)$ corresponding to all possible lines $\mathscr{L}(\nu,\mu)$ such that the symplectic transformation $\mathcal{S}(\kappa,\lambda|\mu,\nu)$ exists. Using these probabilities we use the second Eq. of Eqs. (2.86) and find $\widetilde{\mathcal{W}}(\gamma = \alpha\nu, \delta = \alpha\mu)$ then using Eq. (2.87) we get the density matrix. Figs. (2.5, 2.6) show the Weyl function and Wigner function of this system.

2.6 Factorization of quantum systems

The calculations discussed above are convenient when the dimensions of the quantum systems are small. For quantum systems with large dimensions these calculations become harder as the computational time increases rapidly. An example of this problem is the calculation of Fourier transform where the computational time required to implement this transformation increases

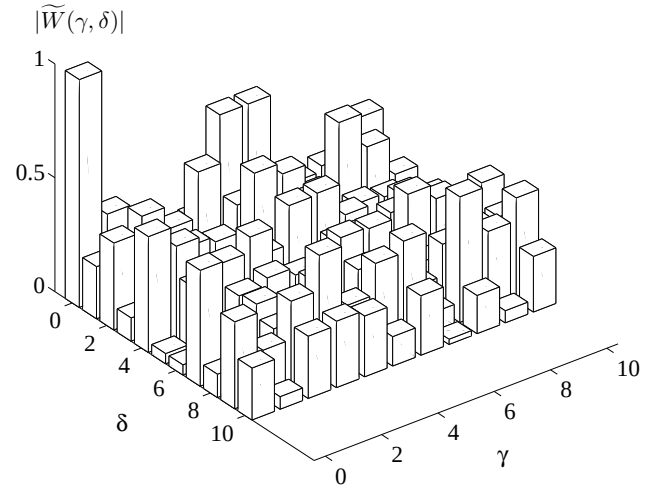

Figure 2.5: Weyl function for the quantum system in the pure state of Eq.(2.88).

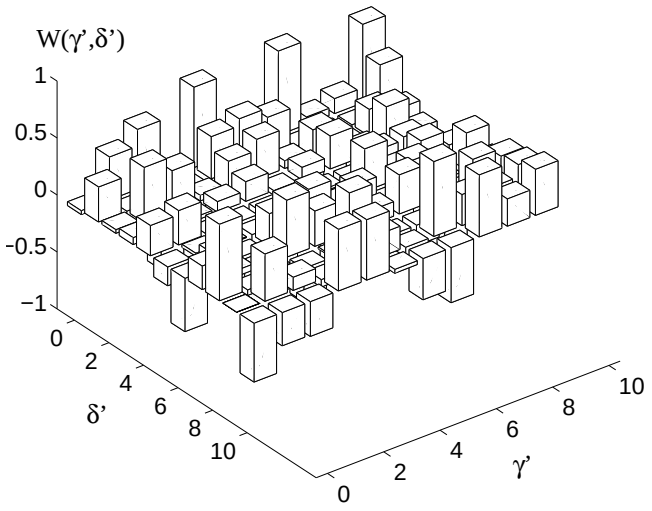

Figure 2.6: Wigner function for the quantum system in the pure state of Eq.(2.88).

rapidly as the system dimension becomes larger. Fast Fourier transform [48] overcame this problem by factorizing the large space into smaller subspaces, performing Fourier transform in each subspace, and finally combining the results to obtain Fourier transform in the large system. This concept of factorization is extensively studied in the context of finite systems [20, 5] using the mapping scheme introduced by Good [6]. In this section we discuss the one-to-one mapping scheme introduced by Good. Then we give a brief review for the factorization in the context of finite quantum systems.

2.6.1 One-to-one mappings

Consider the composite integer number $d = d_1 \times ... \times d_N$ where $d_1, ..., d_N$ are pairwise coprime. We define the integers r_n, t_n, and s_n such that

$$\begin{aligned} r_n &= \frac{d}{d_n}, \\ t_n r_n &= 1 \pmod{d_n}, \\ s_n &= t_n r_n \pmod{d} \end{aligned} \tag{2.89}$$

We note that the inverse of r_n exists because r_n is coprime with d_n.
Then we can define two one-to-one mappings between $\mathcal{Z}_d$ and $\mathcal{Z}_{d_1} \times ... \times \mathcal{Z}_{d_N}$, the first one is

$$\begin{aligned} k &\leftrightarrow (k_1, ..., k_N), \\ k_n &= k \ (mod \ d_n), \\ k &= \sum_n k_n s_n \ (mod \ d) \end{aligned} \tag{2.90}$$

The second map (dual map) is

$$\begin{aligned} k &\leftrightarrow (\tilde{k}_1, ..., \tilde{k}_N), \\ \tilde{k}_n = kt_n &= k_n t_n \ (mod\ d_n), \\ k &= \sum_n \tilde{k}_n r_n \ (mod\ d) \end{aligned} \tag{2.91}$$

For example let $d = 21$ then $r_1 = 7, r_2 = 3, t_1 = 1, t_2 = 5, s_1 = 7, s_2 = 15$. The number $k = 19$ where $k \in \mathcal{Z}_{21}$ is factorized to $k_1 = 1$, and $k_2 = 5$ where $k_1 \in \mathcal{Z}_3$ and $k_2 \in \mathcal{Z}_7$. Also it can be factorized according to the dual map into $\tilde{k}_1 = 1$ and $\tilde{k}_2 = 4$, where $\tilde{k}_1 \in \mathcal{Z}_3$ and $\tilde{k}_2 \in \mathcal{Z}_7$.

2.6.2 Factorization of finite quantum systems

If $d = d_1 \times ... \times d_N$ where d_m is coprime with $d_n,\ n \neq m$, then there is an isomorphism between the Hilbert space $\mathcal{H}_d$ and the product of the Hilbert spaces $\mathcal{H}_{d_1} \otimes ... \otimes \mathcal{H}_{d_N}$. The position and momentum states in $\mathcal{H}_d$ are mapped to their corresponding states in $\mathcal{H}_{d_n}$ as follows

$$\begin{aligned} |X; k\rangle &\leftrightarrow |X^{(1)}; \tilde{k}_1\rangle \otimes ... \otimes |X^{(N)}; \tilde{k}_N\rangle, \\ |P; k\rangle &\leftrightarrow |P^{(1)}; k_1\rangle \otimes ... \otimes |P^{(N)}; k_N\rangle \end{aligned} \tag{2.92}$$

In [5], it has been shown that the Fourier transform $\mathscr{F}$ in $\mathcal{H}_d$ is equivalent to the combination of Fourier transforms in $\mathcal{H}_{d_1}, ..., \mathcal{H}_{d_N}$.

$$\mathscr{F} = \mathscr{F}^{(1)} \otimes ... \otimes \mathscr{F}^{(N)}. \tag{2.93}$$

Also, based on Eqs. (2.92) the displacement operator in $\mathcal{H}_d$ can be calculated in terms of the displacement operators in $\mathcal{H}_{d_n}$ according to the following relation

$$\mathscr{D}(\alpha,\beta)=\bigotimes_n \mathscr{D}^{(n)}(\alpha_n,\tilde{\beta}_n). \tag{2.94}$$

Moreover if the operator θ in $\mathcal{H}_d$ can be factorized to the operators θ_n in $\mathcal{H}_{d_n}$ such that

$$\theta=\bigotimes_n \theta_n, \tag{2.95}$$

then Wigner function and Weyl function of the operator θ are factorized as follows

$$\begin{aligned}\mathcal{W}_\theta(\alpha,\beta)&=\bigotimes_n \mathcal{W}^{(n)}_{\theta_n}(\alpha_n,\tilde{\beta}_n),\\ \widetilde{\mathcal{W}}_\theta(\alpha,\beta)&=\bigotimes_n \widetilde{\mathcal{W}}^{(n)}_{\theta_n}(\alpha_n,\tilde{\beta}_n).\end{aligned} \tag{2.96}$$

2.7 Mutually unbiased bases

In 1960 Schwinger [8] used the notion of mutually unbiased bases in the literature of quantum mechanics. Two orthonormal bases $|\mathcal{B}_m;j\rangle$ and $|\mathcal{B}_n;k\rangle$ in $\mathcal{H}_d$ are mutually unbiased if

$$|\langle\mathcal{B}_m;j|\mathcal{B}_n;k\rangle|^2=\frac{1}{d}. \tag{2.97}$$

One important example of these bases is the position and momentum bases of a particle moving in one dimensional system. It has been proved that the maximum number of mutually unbiased bases cannot exceed $d+1$ where d

is the system dimension. For Hilbert spaces with $d = p^e$, where p is prime, the complete set of mutually unbiased bases exists. For Hilbert spaces with $d = p_1^{e_1}...p_n^{e_n}$; $p_1 < ... < p_n$ one can construct $\mathbb{M}(d)$ mutually unbiased bases such that $p_1^{e_1} + 1 \leq \mathbb{M}(d) \leq d + 1$ [49].

The importance of Eq. (2.97) is that the probability on the left hand side does not depend on the variables j, k. Therefore, if we have two mutually unbiased bases, then using one of them to prepare the quantum states and using the other to measure these states, makes the probabilities of all outcomes equal (i.e. the result is totally random), and hence the use of mutually unbiased bases in quantum cryptography [2]. Also the complete set of mutually unbiased bases is optimal in the context of quantum tomography [50]. Since each basis is associated with $d - 1$ independent probabilities then the total number of independent probabilities that we can get using such set is $d^2 - 1$, therefore using inverse Radon transform we can construct the density matrix. Apart from quantum cryptography and quantum tomography, mutually unbiased bases have many other applications like quantum teleportation [51], quantum dense coding [52], and Mean king's problem [53].

The construction of mutually unbiased bases has been active area of research in the recent years. These constructions are based on different methods like generalized Pauli operators [54], Hadmard matrices [55], orthogonal Latin squares [56] , and equiangular lines [57]. Below we show an explicit construction of the set of mutually unbiased bases that is based on the generalized Pauli operators.

In [54] it has been proved that in the power of prime dimensional systems

the eigenvectors of the generalized Pauli operators

$$\mathscr{Z}, \mathscr{X}, \mathscr{X}\mathscr{Z}, ..., \mathscr{X}\mathscr{Z}^{d-1} \tag{2.98}$$

form a set of mutually unbiased bases. Although mutually unbiased bases have been studied extensively, there exist some open problems that are related to them. An example of these problems is to find the complete set of mutually unbiased bases in Hilbert spaces with composite dimensions (which is not a power of prime dimensions) of which $d = 6$ is the smallest one [58]. There is a strong conjecture that one cannot find more than three mutually unbiased bases in systems with $d = 6$, however this conjecture has not been proved yet. Another question that has not been answered yet is the relation between mutually unbiased bases and the geometrical structure of affine planes. Mutually unbiased bases have been surveyed in details in [59].

2.8 Summary

In this chapter we have introduced the basic concepts of quantum systems with variables in $\mathcal{Z}_d$. We have presented the position and momentum states. We discussed the linear operators that transform vectors from $\mathcal{H}_d$ to $\mathcal{H}_d$. We studied the symplectic transformation then we presented the steps to calculate it numerically with example in a five-dimensional Hilbert space. We have considered Wigner function and Weyl function, we have discussed their properties and we have complemented this discussion with examples. We have presented Radon transform then we have shown (with an example)

the use of inverse Radon transform in quantum tomography. We considered the factorization of finite quantum systems then this chapter has ended with brief survey of mutually unbiased bases.

Chapter 3

Beyond near-linear finite geometry

We consider the lines $\mathscr{L}(\rho, \sigma)$ in the phase space $\mathscr{Z}_d \times \mathscr{Z}_d$. In general $\mathscr{Z}_d$ is a ring. When d is prime, $\mathscr{Z}_d$ is a field. Also in the case that $d = p^n$ where p is prime, the Galois field $G(p^n)$ can be used. In this chapter we prove several properties of the lines through the origin (particularly when $\mathscr{Z}_d$ is a ring) and we show that symplectic transformation can be used to get lines from other lines. Also we introduce the concept of factorizing lines in $\mathscr{Z}_d \times \mathscr{Z}_d$ in terms of 'component lines' in $\mathscr{Z}_{d_j} \times \mathscr{Z}_{d_j}$ such that $d = \prod d_j$ and (d_j, d_k) are coprime. The propositions in this chapter and the following chapters are the novel contribution of this research.

3.1 Introduction

The element $\rho \in \mathcal{Z}_d$ is called invertible (unit) if the multiplicative inverse of ρ exists in $\mathcal{Z}_d$. If σ is the multiplicative inverse of ρ, then

$$\rho\sigma = 1 \pmod{d} \tag{3.1}$$

ρ is invertible in $\mathcal{Z}_d$ if ρ is coprime with d, i.e.

$$\mathbb{G}(\rho, d) = 1, \tag{3.2}$$

where $\mathbb{G}(\rho, d)$ is the greatest common divisor of the two integers ρ, d.
In the case that d is prime, $\mathcal{Z}_d$ is a field and all elements (apart from 0) in $\mathcal{Z}_d$ are invertible. This is why fields have much stronger properties than rings. The invertible elements in $\mathcal{Z}_d$ form a group for the multiplication operation (as the product of two invertible elements is again an invertible element). Such a group is called the group of reduced residue classes modulo d. The number of invertible elements in $\mathcal{Z}_d$ is $\varphi(d)$ where $\varphi(d)$ is the Euler totient function. If $d = \prod_{n=1}^{N} p_n^{e_n}$; e_n is positive integer, then $\varphi(d)$ obeys the relation

$$\varphi(d) = d \prod_{n=1}^{N} \left(1 - \frac{1}{p_n}\right), \tag{3.3}$$

as a result if $d = p$, then $\varphi(p) = p - 1$, and if $d = p^k$, then $\varphi(p^k) = p^k - p^{k-1}$. Another important function in number theory is Jordan totient function $J_m(d)$. Jordan totient function shows the number of $m-$tuples of elements in $\mathcal{Z}_d$ such that each tuple together with d forms a coprime $(m+1)$-

tuple. Jordan totient function is calculated as

$$J_m(d) = d^m \prod_{n=1}^{N} \left(1 - \frac{1}{p_n^m}\right), \tag{3.4}$$

consequently, when $d = p$ then $J_m(p) = p^m - 1$, and when $d = p^k$ then $J_m(p^k) = p^{m(k-1)}(p^m - 1)$. Euler totient function is a special case of Jordan totient function (where $m = 1$). In the case that $m = 2$, Jordan totient function is the product of Euler totient function $\varphi(d)$ and Dedekind $\psi-$function

$$J_2(d) = d^2 \prod_{n=1}^{N} \left(1 - \frac{1}{p_n^2}\right) = \varphi(d)\psi(d), \tag{3.5}$$

where

$$\psi(d) = d \prod_{n=1}^{N} \left(1 + \frac{1}{p_n}\right). \tag{3.6}$$

The functions $\varphi(d), J_2(d), \psi(d)$ are multiplicative in the sense that $g(d_1 d_2) = g(d_1)g(d_2)$; d_1, d_2 are coprime.

The phase space $\mathcal{Z}_d \times \mathcal{Z}_d$ is a finite geometry. Although there is much work in finite geometry [60], most of this work is based on near-linear geometry where two points must not belong to more than one line. In this chapter we show that $\mathcal{Z}_d \times \mathcal{Z}_d$ violates this axiom. $\mathcal{Z}_d \times \mathcal{Z}_d$ is near-linear geometry if and only if d is prime (or power of primes in the case of Galois field).

3.2 Properties of lines in $\mathcal{Z}_d \times \mathcal{Z}_d$

We define the lines $\mathscr{L}(\rho, \sigma)$ through the origin in the phase space $\mathcal{Z}_d \times \mathcal{Z}_d$ (also called cyclic submodule) as

$$\mathscr{L}(\rho, \sigma) = \{(u\rho, u\sigma) \mid u \in \mathcal{Z}_d\} , \tag{3.7}$$

where the points $(u\rho, u\sigma)$ are calculated modulo d. As an example in $\mathcal{Z}_6 \times \mathcal{Z}_6$

$$\mathscr{L}(1, 2) = \{(0, 0), (1, 2), (2, 4), (3, 0), (4, 2), (5, 4)\} . \tag{3.8}$$

From now on we use the term 'line' to denote the lines through the origin. Unlike near-linear geometry, two lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ (where d is not prime) might intersect at more than one point. For example, the two lines $\mathscr{L}(1, 2), \mathscr{L}(1, 4)$ in $\mathcal{Z}_6 \times \mathcal{Z}_6$ have the two points $(0, 0), (3, 0)$ in common. We define the line $\mathscr{L}(\rho_1, \sigma_1)$ as a 'subline' of the line $\mathscr{L}(\rho_2, \sigma_2)$ if the set of points on the line $\mathscr{L}(\rho_1, \sigma_1)$ is subset of the set of points on the line $\mathscr{L}(\rho_2, \sigma_2)$. We call the line $\mathscr{L}(\rho, \sigma)$ 'maximal line' in $\mathcal{Z}_d \times \mathcal{Z}_d$ if $\mathscr{L}(\rho, \sigma)$ has exactly d points. We note that the authors in [61] use the term 'isotropic lines' to denote the lines with d points.

In chapter (2) we introduced the symplectic matrices

$$\mathrm{g}(\kappa, \lambda|\mu, \nu) = \begin{pmatrix} \kappa & \lambda \\ \mu & \nu \end{pmatrix} , \tag{3.9}$$

where $\kappa, \lambda, \mu, \nu \in \mathcal{Z}_d$ and $\kappa\nu - \lambda\mu = 1 \pmod{d}$. These matrices form the group $\mathcal{S}p(2, \mathcal{Z}_d)$. The symplectic transformation of the point (ρ, σ) is the

point $\mathrm{g}(\kappa, \lambda|\mu, \nu)(\rho, \sigma)$ where

$$\mathrm{g}(\kappa, \lambda|\mu, \nu)(\rho, \sigma) = (\kappa\rho + \lambda\sigma, \mu\rho + \nu\sigma). \tag{3.10}$$

Therefore the symplectic transformation of the line $\mathscr{L}(\rho, \sigma)$ is the line $\mathrm{g}(\kappa, \lambda|\mu, \nu)\mathscr{L}(\rho, \sigma)$. In what follows we prove some propositions that shed the light on the properties of lines in $\mathcal{Z}_d \times \mathcal{Z}_d$.

Proposition 3.2.1. *In the phase space $\mathcal{Z}_d \times \mathcal{Z}_d$ the following hold*

(1) The line $\mathscr{L}(\lambda\rho, \lambda\sigma) = \mathscr{L}(\rho, \sigma)$ if λ is invertible. If λ is non-invertible, then $\mathscr{L}(\lambda\rho, \lambda\sigma) \subset \mathscr{L}(\rho, \sigma)$

(2) The line $\mathscr{L}(\rho, \sigma)$ has $d/\mathbb{G}(\rho, \sigma, d)$ points. If d is prime, all lines (apart from the line $\mathscr{L}(0, 0)$) are maximal.

(3) The number of maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ is $\psi(d)$.

(4) If d_i is a divisor of d, then the lines $\mathscr{L}(\rho, \sigma)$ with exactly d_i points, consist of points (γ, δ) such that $\gamma, \delta \in (d/d_i)\mathcal{Z}_{d_i}$ ($(d/d_i)\mathcal{Z}_{d_i}$ is a subgroup of $\mathcal{Z}_d$).

(5) If d_i is a divisor of d, then the number of lines with d_i points is $\psi(d_i)$.

(6) The intersection of any two lines is a subline with d_j points, where d_j is a divisor of d. When d is prime, any two lines intersect only in the origin.

(7) The lines $\mathscr{L}(\rho, \sigma)$ and $\mathrm{g}(\kappa, \lambda|\mu, \nu)\mathscr{L}(\rho, \sigma)$ have the same number of points.

(8) If d is prime, then the set of all maximal lines are described by

$$\mathscr{L}(0,1); \;\; \mathrm{g}(0,1|-1,-\lambda)\mathscr{L}(0,1); \;\; \lambda \in \mathcal{Z}_d \tag{3.11}$$

Proof. (1) Consider the point $(u\lambda\rho, u\lambda\sigma)$ that belongs to the line $\mathscr{L}(\lambda\rho, \lambda\sigma)$. Let $u' = u\lambda$, then the point $(u\lambda\rho, u\lambda\sigma) = (u'\rho, u'\sigma)$ is also a point on the line $\mathscr{L}(\rho, \sigma)$. Therefore, $\mathscr{L}(\lambda\rho, \lambda\sigma) \subset \mathscr{L}(\rho, \sigma)$. Conversely, if λ is an invertible element, then there exists u' such that $u' = \lambda^{-1}u$. Therefore, the point $(u\rho, u\sigma)$ on the line $\mathscr{L}(\rho, \sigma)$ can be written as $(u'\lambda\rho, u'\lambda\sigma)$ and hence it belongs to the line $\mathscr{L}(\lambda\rho, \lambda\sigma)$. This proves that if λ is invertible, then $\mathscr{L}(\lambda\rho, \lambda\sigma) = \mathscr{L}(\rho, \sigma)$.

(2) Theorems (5.13, 5.14) in [62] show that if ρ is fixed in $\mathcal{Z}_d$ and u takes all values in $\mathcal{Z}_d$, then the number of values $u\rho$ in $\mathcal{Z}_d$ is $d/\mathbb{G}(\rho, d)$. Moreover, if $u = u'$ leads to $u'\rho$, then we conclude that

$$u', u' + \frac{d}{\mathbb{G}(\rho, d)}, ..., u' + [\mathbb{G}(\rho, d) - 1]\frac{d}{\mathbb{G}(\rho, d)} \tag{3.12}$$

lead to the same value $u'\rho$. If $N = \mathbb{G}(\rho, d)$, then Eq. (3.12) shows that we can describe these values of u as a variable in $\mathcal{Z}_N$. The N values of u lead to N values of $u\sigma$ but only $N/\mathbb{G}(\sigma, N)$ are different (the proof of the number of values of $u\sigma$ is similar to the proof of the number of values of $u\rho$, the only difference is that we get the number of values of $u\sigma$ in $\mathcal{Z}_N$). Let M denote the total number of points $(u\rho, u\sigma)$ on the

line $\mathscr{L}(\rho, \sigma)$, therefore

$$M = \frac{d}{N} \times \frac{N}{\mathbb{G}(\sigma, N)} \ , \tag{3.13}$$

but

$$\mathbb{G}(\sigma, N) = \mathbb{G}(\sigma, \mathbb{G}(\rho, d)) = \mathbb{G}(\rho, \sigma, d) \ , \tag{3.14}$$

then the total number of points $(u\rho, u\sigma)$ on the line $\mathscr{L}(\rho, \sigma)$ is

$$M = \frac{d}{\mathbb{G}(\rho, \sigma, d)} \ . \tag{3.15}$$

When d is prime, $\mathbb{G}(\rho, \sigma, d) = 1$ (where $(\rho, \sigma) \neq (0, 0)$). Therefore, the lines (apart from the line $\mathscr{L}(0, 0)$) in $\mathcal{Z}_d \times \mathcal{Z}_d$ where d is prime, are maximal.

(3) If the line $\mathscr{L}(\rho, \sigma)$ is maximal, then $\mathbb{G}(\rho, \sigma, d) = 1$. The number of pairs (ρ, σ) where $\mathbb{G}(\rho, \sigma, d) = 1$, is $J_2(d)$. In the case that u is invertible, $\mathscr{L}(\rho, \sigma) = \mathscr{L}(u\rho, u\sigma)$. Since the number of invertible elements is $\varphi(d)$, then the number of maximal lines is $J_2(d)/\varphi(d) = \psi(d)$.

(4) Since the lines $\mathscr{L}(\rho, \sigma)$ have exactly d_i points, then $\mathbb{G}(\rho, \sigma, d) = d/d_i$. Therefore, the line $\mathscr{L}(\rho, \sigma)$ can be written as $\mathscr{L}(\rho' \frac{d}{d_i}, \sigma' \frac{d}{d_i})$ where $\rho', \sigma' \in \mathcal{Z}_{d_i}$. If (γ, δ) are the points on the line $\mathscr{L}(\rho, \sigma)$, then the coordinates $\gamma, \delta \in (d/d_i)\mathcal{Z}_{d_i}$.

(5) In (4) we have proved that the lines $\mathscr{L}(\rho, \sigma)$ with d_i points in $\mathcal{Z}_d$ have the points (γ, δ) such that $\gamma, \delta \in (d/d_i)\mathcal{Z}_{d_i}$, but the number of lines with d_i points in $\mathcal{Z}_{d_i}$ is $\psi(d_i)$. Therefore, the number of lines with d_i

points in $\mathcal{Z}_d \times \mathcal{Z}_d$ is $\psi(d_i)$.

(6) Let $(\gamma, \delta) \in \mathscr{L}(\rho_1, \sigma_1)$ and also $(\gamma, \delta) \in \mathscr{L}(\rho_2, \sigma_2)$, therefore $(\gamma, \delta) = (u\rho_1, u\sigma_1) = (u'\rho_2, u'\sigma_2)$, where $u, u' \in \mathcal{Z}_d$. Since $\mathscr{L}(\gamma, \delta) = \mathscr{L}(u\rho_1, u\sigma_1)$, then $\mathscr{L}(\gamma, \delta) \subseteq \mathscr{L}(\rho_1, \sigma_1)$. Similarly $\mathscr{L}(\gamma, \delta) \subseteq \mathscr{L}(\rho_2, \sigma_2)$. Therefore, the intersection of the two lines $\mathscr{L}(\rho_1, \sigma_1)$ and $\mathscr{L}(\rho_2, \sigma_2)$ is the subline $\mathscr{L}(\gamma, \delta)$. Since the number of points on the line $\mathscr{L}(\gamma, \delta)$ is $\frac{d}{\mathbb{G}(\gamma,\delta,d)}$, then the number of points on the subline is a divisor of d. When d is prime the only possible divisor is 1, therefore two lines $\mathcal{Z}_d \times \mathcal{Z}_d$ where d is prime intersect only at the origin. This completes the proof.

(7) We point out that if the two points $(\gamma_1, \delta_1), (\gamma_2, \delta_2) \in \mathscr{L}(\rho, \sigma)$, then the two points $(\kappa\gamma_1+\lambda\delta_1, \mu\gamma_1+\nu\delta_1), (\kappa\gamma_2+\lambda\delta_2, \mu\gamma_2+\nu\delta_2) \in \mathrm{g}(\kappa, \lambda|\mu, \nu)\mathscr{L}(\rho, \sigma)$ because

$$\mathrm{g}(\kappa, \lambda|\mu, \nu)(\gamma_1, \delta_1) = \begin{pmatrix} \kappa & \lambda \\ \mu & \nu \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \delta_1 \end{pmatrix} = \begin{pmatrix} \kappa\gamma_1 + \lambda\delta_1 \\ \mu\gamma_1 + \nu\delta_1 \end{pmatrix}, \quad (3.16)$$

and

$$\mathrm{g}(\kappa, \lambda|\mu, \nu)(\gamma_2, \delta_2) = \begin{pmatrix} \kappa & \lambda \\ \mu & \nu \end{pmatrix} \begin{pmatrix} \gamma_2 \\ \delta_2 \end{pmatrix} = \begin{pmatrix} \kappa\gamma_2 + \lambda\delta_2 \\ \mu\gamma_2 + \nu\delta_2 \end{pmatrix}. \quad (3.17)$$

We assume that $(\gamma_1, \delta_1) \neq (\gamma_2, \delta_2)$. If $(\kappa\gamma_1 + \lambda\delta_1, \mu\gamma_1 + \nu\delta_1) = (\kappa\gamma_2 + \lambda\delta_2, \mu\gamma_2 + \nu\delta_2)$, then by subtracting Eq. (3.17) from Eq. (3.16) we get

the linear equation

$$\begin{pmatrix} \kappa & \lambda \\ \mu & \nu \end{pmatrix} \begin{pmatrix} \gamma_1 - \gamma_2 \\ \delta_1 - \delta_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{3.18}$$

Since $det(g) \neq 0$ then Eq. (3.18) has only one solution (the trivial solution). Therefore, $\gamma_1 = \gamma_2$, and $\delta_1 = \delta_2$ which contradict the assumption that $(\gamma_1, \delta_1) \neq (\gamma_2, \delta_2)$. Consequently, if $(\gamma_1, \delta_1) \neq (\gamma_2, \delta_2)$, then $(\kappa\gamma_1 + \lambda\delta_1, \mu\gamma_1 + \nu\delta_1) \neq (\kappa\gamma_2 + \lambda\delta_2, \mu\gamma_2 + \nu\delta_2)$ and hence the two lines $\mathscr{L}(\rho, \sigma), \mathrm{g}(\kappa, \lambda|\mu, \nu)\mathscr{L}(\rho, \sigma)$ have the same number of points.

(8) We note that the line $\mathscr{L}(0, \beta)$ is the same as the line $\mathscr{L}(0, 1)$. Then we prove that we can get any other line $\mathscr{L}(\rho, \sigma)$ (where $\rho \neq 0$) using the symplectic transformation $\mathrm{g}(0, 1| - 1, -\lambda)$ of the line $\mathscr{L}(0, 1)$. Therefore, we need to prove that for any point $(u\rho, u\sigma)$ (apart from $(0, 0)$ as $\mathrm{g}(0, 1| - 1, -\lambda)(0, 0) = (0, 0)$) on the line $\mathscr{L}(\rho, \sigma)$, there exists a symplectic transformation $\mathrm{g}(0, 1|-1, -\lambda)$ and a point $(0, \alpha)$ on the line $\mathscr{L}(0, 1)$ such that $(u\rho, u\sigma) = \mathrm{g}(0, 1| - 1, -\lambda)(0, \alpha)$. This statement is true because

$$\begin{pmatrix} 0 & 1 \\ -1 & -\lambda \end{pmatrix} \begin{pmatrix} 0 \\ \alpha \end{pmatrix} = \begin{pmatrix} u\rho \\ u\sigma \end{pmatrix}. \tag{3.19}$$

As a result of Eq. (3.19) and taking into account that $u \neq 0$ (as we consider the points $(u\rho, u\sigma)$ where $(u\rho, u\sigma) \neq (0, 0)$), $\alpha = u\rho$, and $-\lambda\alpha = -\lambda u\rho = u\sigma$, therefore we conclude that $\lambda = -\rho^{-1}\sigma$.

□

Example 3.2.2. *In what follows we give examples for the proposition (3.2.1),*

we first consider the phase space $\mathcal{Z}_{15} \times \mathcal{Z}_{15}$.

(1) $\mathscr{L}(2,2) = \mathscr{L}(1,1)$, *and* $\mathscr{L}(5,5) \subset \mathscr{L}(1,1)$.

(2) The number of points on the line $\mathscr{L}(5,5) = \frac{15}{\mathbb{G}(5,5,15)} = 3$.

(3) The number of maximal lines is $\psi(15) = 24$.

(4) The line $\mathscr{L}(3,3) = \{(0,0),(3,3),(6,6),(9,9),(12,12)\}$. *It is clear that the points* $(\gamma,\delta) \in \mathscr{L}(3,3)$ *are such that* $\gamma,\delta \in (15/5)\mathcal{Z}_5$. *Similarly, the line* $\mathscr{L}(5,5)$ *consists of the points* (γ,δ) *such that* $\gamma,\delta \in (15/3)\mathcal{Z}_3$.

(5) The number of sublines with 3 *points is* $\psi(3) = 4$, *and The number of sublines with* 5 *points is* $\psi(5) = 6$.

(6) The two lines $\mathscr{L}(6,5)$ *and* $\mathscr{L}(3,1)$ *have the subline* $\mathscr{L}(0,5)$ *in common, where* $\mathscr{L}(0,5) = \{(0,0),(0,5),(0,10)\}$

(7) The two lines $\mathscr{L}(0,1)$ *and* $\mathrm{g}(10,12|12,10)\mathscr{L}(0,1) = \mathscr{L}(12,10)$ *have* 15 *points each.*

Next, we consider the phase space $\mathcal{Z}_3 \times \mathcal{Z}_3$. *The lines* $\mathscr{L}(0,1), \mathscr{L}(1,0) = \mathrm{g}(0,1|-1,0)\mathscr{L}(0,1), \mathscr{L}(1,2) = \mathrm{g}(0,1|-1,-1)\mathscr{L}(0,1), \mathscr{L}(1,1) = \mathrm{g}(0,1|-1,-2)\mathscr{L}(0,1)$ *form the set of all maximal lines.*

The number of maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ is $\psi(d)$. When d is prime all maximal lines intersect only at the origin and these lines have $\psi(d)(d-1) = d^2-1$ points apart from the origin (exactly the same as the number of points apart from the origin in $\mathcal{Z}_d \times \mathcal{Z}_d$). In the case that d is not prime, the maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ have a total number of $\psi(d)(d-1)$ $(> d^2-1)$

points apart from the origin as two lines may have more than one point in common. To measure the deviation between the geometry $\mathcal{Z}_d \times \mathcal{Z}_d$ and the near-linear geometry, we present the redundancy parameter $\mathscr{R}$ such that

$$\mathscr{R} = \frac{\psi(d)(d-1)}{d^2-1} - 1 = \frac{\psi(d)}{d+1} - 1. \tag{3.20}$$

It is clear that when d is prime, $\mathcal{Z}_d \times \mathcal{Z}_d$ is a field and $\mathscr{R} = 0$.

3.3 Factorization of lines in $\mathcal{Z}_d \times \mathcal{Z}_d$

In this section we present the bijective map between the phase space $\mathcal{Z}_d \times \mathcal{Z}_d$ and the phase space $[\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_2}] \times [\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_2}]$, where $d = p_1 p_2$ and p_1, p_2 are prime numbers,

$$\mathcal{Z}_d \times \mathcal{Z}_d \leftrightarrow [\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_2}] \times [\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_2}]. \tag{3.21}$$

In chapter (2) we introduced two one-to-one mappings based on the Chinese remainder theorem

$$\begin{aligned} k &\leftrightarrow (k_1, k_2), \\ k_n &= k \ (mod \ p_n), \\ k &= \sum_{n=0}^{n=1} k_n s_n \ (mod \ d) \end{aligned} \tag{3.22}$$

and its dual

$$\begin{aligned} k &\leftrightarrow (\tilde{k}_1, \tilde{k}_2), \\ \tilde{k}_n = kt_n &= k_n t_n \ (mod\ p_n), \\ k &= \sum_{n=0}^{n=1} \tilde{k}_n r_n \ (mod\ d) \end{aligned} \tag{3.23}$$

where

$$r_n = \frac{d}{p_n}; \quad t_n r_n = 1 \ \ (mod\ p_n); \quad s_n = t_n r_n \ \ (mod\ d)\ . \tag{3.24}$$

We map the point (α, β) in $\mathcal{Z}_d \times \mathcal{Z}_d$ to the two points $(\alpha_1, \tilde{\beta}_1)$ and $(\alpha_2, \tilde{\beta}_2)$ in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$ and $\mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$, respectively,

$$(\alpha, \beta) \leftrightarrow ((\alpha_1, \alpha_2), (\tilde{\beta}_1, \tilde{\beta}_2)). \tag{3.25}$$

We use the map of Eq. (3.22) for $\alpha \leftrightarrow (\alpha_1, \alpha_2)$ and its dual of Eq. (3.23) for $\beta \leftrightarrow (\tilde{\beta}_1, \tilde{\beta}_2)$.

Consider the point $(u\rho, u\sigma)$ on the line $\mathscr{L}(\rho, \sigma)$. Using the map of Eq. (3.22) we find

$$u\rho \leftrightarrow ((u\rho)_1, (u\rho)_2), \tag{3.26}$$

but

$$(u\rho)_j = (u\rho) \ \ (mod\ p_j) = [u \ \ (mod\ p_j)][\rho \ \ (mod\ p_j)] = u_j \rho_j. \tag{3.27}$$

Using the map of Eq. (3.23) we get

$$u\sigma \leftrightarrow ((\tilde{u\sigma})_1, (\tilde{u\sigma})_2), \tag{3.28}$$

and since

$$(\tilde{u\sigma})_j = (u\sigma)t_j \pmod{p_j} = [u \pmod{p_j}][\sigma t_j \pmod{p_j}] = u_j\tilde{\sigma}_j, \tag{3.29}$$

then using Eqs. (3.27,3.29) we prove that there is a mapping between the line $\mathscr{L}(\rho, \sigma)$ in $\mathcal{Z}_d \times \mathcal{Z}_d$ and the lines $\mathscr{L}(\rho_1, \tilde{\sigma}_1), \mathscr{L}(\rho_2, \tilde{\sigma}_2)$ in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$ and $\mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$, respectively.

$$\mathscr{L}(\rho, \sigma) = \mathscr{L}^{(1)}(\rho_1, \tilde{\sigma}_1) \times \mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2), \tag{3.30}$$

where $\mathscr{L}^{(j)}(\rho_j, \tilde{\sigma}_j)$ is the component line in $\mathcal{Z}_{p_j} \times \mathcal{Z}_{p_j}$.
When $\mathscr{L}^{(1)}(\rho_1, \tilde{\sigma}_1) \neq (0,0)$ and $\mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2) \neq (0,0)$, the two lines $\mathscr{L}^{(1)}(\rho_1, \tilde{\sigma}_1)$ and $\mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2)$ have p_1 and p_2 points, respectively, therefore the line $\mathscr{L}(\rho, \sigma)$ has $p_1 p_2$ points. As an example, the line $\mathscr{L}(1,5)$ in $\mathcal{Z}_6 \times \mathcal{Z}_6$ can be written as

$$\mathscr{L}(1,5) = \mathscr{L}^{(1)}(1,1) \times \mathscr{L}^{(2)}(1,1), \tag{3.31}$$

where the line $\mathscr{L}^{(1)}(1,1)$ in $\mathcal{Z}_2 \times \mathcal{Z}_2$ has 2 points and the line $\mathscr{L}^{(2)}(1,1)$ in $\mathcal{Z}_3 \times \mathcal{Z}_3$ has 3 points, correspondingly the line $\mathscr{L}(1,5)$ in $\mathcal{Z}_6 \times \mathcal{Z}_6$ has 6 points. The following proposition shows a construction of all maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ and the role of symplectic transformation in this construction.

Proposition 3.3.1.

(1) The set of all maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ is given by

$$\begin{aligned}
&\mathscr{L}_1 = \mathscr{L}^{(1)}(0,1) \times \mathscr{L}^{(2)}(0,1) \\
&\mathscr{L}_{2+\lambda_2} = \mathscr{L}^{(1)}(0,1) \times [\mathrm{g}^{(2)}(0,1|-1,-\lambda_2)\mathscr{L}^{(2)}(0,1)] \\
&\mathscr{L}_{2+p_2+\lambda_1} = [\mathrm{g}^{(1)}(0,1|-1,-\lambda_1)\mathscr{L}^{(1)}(0,1)] \times \mathscr{L}^{(2)}(0,1) \\
&\mathscr{L}_{2+p_1+p_2+\lambda_2+\lambda_1 p_2} = [\mathrm{g}^{(1)}(0,1|-1,-\lambda_1)\mathscr{L}^{(1)}(0,1)] \times [\mathrm{g}^{(2)}(0,1|-1,-\lambda_2)\mathscr{L}^{(2)}(0,1)],
\end{aligned} \tag{3.32}$$

where $d = p_1 p_2$, p_1, p_2 are prime numbers, $\lambda_1 \in \mathcal{Z}_{p_1}, \lambda_2 \in \mathcal{Z}_{p_2}$.

(2) These set of maximal lines, can also be derived using the symplectic transformations in $\mathcal{Z}_d \times \mathcal{Z}_d$ acting on the line $\mathscr{L}(0,1)$, as shown below

$$\begin{aligned}
&\mathscr{L}_{2+\lambda_2} = \mathrm{g}(s_1, t_2 s_2|-p_1, s_1 - \lambda_2 s_2)\mathscr{L}_1 \\
&\mathscr{L}_{2+p_2+\lambda_1} = \mathrm{g}(s_2, t_1 s_1|-p_2, s_2 - \lambda_1 s_1)\mathscr{L}_1 \\
&\mathscr{L}_{2+p_1+p_2+\lambda_2+\lambda_1 p_2} = \mathrm{g}(0, \Gamma|-p_1-p_2, -\lambda_1 s_1 - \lambda_2 s_2)\mathscr{L}_1,
\end{aligned} \tag{3.33}$$

where $\Gamma = t_1^2 p_2 + t_2^2 p_1$.

(3) Acting on any maximal line $\mathscr{L}(\rho,\sigma)$ with the matrices $\mathrm{g}(\kappa,\lambda|\mu,\nu)$, we obtain the remaining maximal lines.

Proof. (1) Eq. (3.11) in proposition (3.2.1) shows that $\mathscr{L}^{(1)}(0,1)$, $\mathrm{g}^{(1)}(0,1|-1,-\lambda_1)\mathscr{L}^{(1)}(0,1)$ is the set of all maximal lines in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$ and $\mathscr{L}^{(2)}(0,1)$, $\mathrm{g}^{(2)}(0,1|-1,-\lambda_2)\mathscr{L}^{(2)}(0,1)$ is the set of all maximal lines in $\mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$. Therefore, each line of Eqs. (3.32) has exactly $d = p_1 p_2$ points. The mapping in Eqs. (3.32) is one-to-one, therefore the lines of these Eqs.

are different from each other. The cardinality of this set of lines is $\psi(p_1)\psi(p2) = \psi(d)$. Since the number of maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ is $\psi(d)$ (proposition (3.2.1)) then Eqs. (3.32) give all maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$.

(2) We first prove that

$$\mathrm{g}(\kappa, \lambda|\mu, \nu) \leftrightarrow \mathrm{g}^{(1)}(\kappa_1, \lambda_1 r_1|\tilde{\mu}_1, \nu_1)\ ,\ \mathrm{g}^{(2)}(\kappa_2, \lambda_2 r_2|\tilde{\mu}_2, \nu_2), \tag{3.34}$$

where $\kappa_j \nu_j - \lambda_j r_j \tilde{\mu_j} = 1 \pmod{p_j}$.

Acting on the line $\mathscr{L}(\rho, \sigma)$ in $\mathcal{Z}_d \times \mathcal{Z}_d$ with the symplectic transformation $\mathrm{g}(\kappa, \lambda|\mu, \nu)$ we get

$$\mathrm{g}(\kappa, \lambda|\mu, \nu)\mathscr{L}(\rho, \sigma) = \mathscr{L}(\kappa\rho + \lambda\sigma, \mu\rho + \nu\sigma). \tag{3.35}$$

According to the map of Eq. (3.22) $(\kappa\rho + \lambda\sigma)$ is mapped to $(\kappa_1\rho_1 + \lambda_1\sigma_1), (\kappa_2\rho_2 + \lambda_2\sigma_2)$ in $\mathcal{Z}_{p_1}, \mathcal{Z}_{p_2}$ respectively, and according to the map of Eq. (3.23) $(\mu\rho + \nu\sigma)$ is mapped to $(\mu_1\rho_1 + \nu_1\sigma_1)t_1, (\mu_2\rho_2 + \nu_2\sigma_2)t_2$ in $\mathcal{Z}_{p_1}, \mathcal{Z}_{p_2}$ respectively. Since $t_j r_j = 1 \ \ (mod\ p_j)$ and $\tilde{\sigma}_j = \sigma_j t_j$ then the line $\mathscr{L}(\kappa\rho + \lambda\sigma, \mu\rho + \nu\sigma)$ can be written as

$$\mathscr{L}(\kappa\rho+\lambda\sigma, \mu\rho+\nu\sigma) = \mathscr{L}(\kappa_1\rho_1+\lambda_1 r_1\tilde{\sigma}_1, \tilde{\mu}_1\rho_1+\nu_1\tilde{\sigma_1})\times\mathscr{L}(\kappa_2\rho_2+\lambda_2 r_2\tilde{\sigma}_2, \tilde{\mu}_2\rho_2+\nu_2\tilde{\sigma_2}). \tag{3.36}$$

Acting on the line $\mathscr{L}^{(1)}(\rho_1, \tilde{\sigma}_1)$ in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$ with the symplectic trans-

formation $\mathrm{g}^{(1)}(\kappa_1, \lambda_1 r_1 | \tilde{\mu}_1, \nu_1)$ we get

$$\mathrm{g}^{(1)}(\kappa_1, \lambda_1 r_1 | \tilde{\mu}_1, \nu_1) \mathscr{L}^{(1)}(\rho_1, \tilde{\sigma}_1) = \mathscr{L}^{(1)}(\kappa_1 \rho_1 + \lambda_1 r_1 \tilde{\sigma}_1, \tilde{\mu}_1 \rho_1 + \nu_1 \tilde{\sigma_1}), \tag{3.37}$$

similarly,

$$\mathrm{g}^{(2)}(\kappa_2, \lambda_2 r_2 | \tilde{\mu}_2, \nu_2) \mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2) = \mathscr{L}^{(2)}(\kappa_2 \rho_2 + \lambda_2 r_2 \tilde{\sigma}_2, \tilde{\mu}_2 \rho_2 + \nu_2 \tilde{\sigma_2}). \tag{3.38}$$

Eqs. (3.36, 3.37, 3.38) prove Eq. (3.34).

Since $\kappa, \nu, \lambda, \mu$ obey the constraint

$$\kappa\nu - \lambda\mu = 1 \pmod{d}, \tag{3.39}$$

and

$$\begin{aligned}(\kappa\nu - \lambda\mu) \pmod{p_j} &= (\kappa\nu - \lambda\mu)_j \\ &= [\kappa \pmod{p_j}][\nu \pmod{p_j}] - [\lambda \pmod{p_j}][\mu \pmod{p_j}] \\ &= \kappa_j \nu_j - \lambda_j \mu_j, \end{aligned} \tag{3.40}$$

therefore

$$\kappa_j \nu_j - \lambda_j \mu_j = 1 \pmod{p_j}. \tag{3.41}$$

Using the fact that $t_j r_j = 1 \pmod{p_j}$, we get

$$\kappa_j \nu_j - \lambda_j r_j \tilde{\mu}_j = 1 \pmod{p_j}. \tag{3.42}$$

Eqs. (3.22, 3.23, 3.34) show that

$$\begin{aligned}
&\mathrm{g}(s_1, t_2 s_2| - p_1, s_1 - \lambda_2 s_2) \leftrightarrow \mathrm{g}^{(1)}(1, 0|0, 1), \mathrm{g}^{(2)}(0, 1| - 1, -\lambda_2), \\
&\mathrm{g}(s_2, t_1 s_1| - p_2, s_2 - \lambda_1 s_1) \leftrightarrow \mathrm{g}^{(1)}(0, 1| - 1, -\lambda_1), \mathrm{g}^{(2)}(1, 0|0, 1), \\
&\mathrm{g}(0, t_1^2 p_2 + t_2^2 p_1| - p_1 - p_2, \lambda_1 s_1 - \lambda_2 s_2) \leftrightarrow \mathrm{g}^{(1)}(0, 1| - 1, -\lambda_1), \mathrm{g}^{(2)}(0, 1| - 1, -\lambda_2).
\end{aligned} \tag{3.43}$$

Eqs. (3.32,3.43) show that the lines of Eqs. (3.32) are the same as the lines of Eqs. (3.33).

(3) The line $\mathscr{L}(\rho, \tilde{\sigma})$ can be obtained from the line $\mathscr{L}_1 = \mathscr{L}(0, 1)$ using one of the symplectic matrices of Eqs. (3.33), i.e.

$$\mathscr{L}(\rho, \tilde{\sigma}) = \mathrm{g}_1 \mathscr{L}_1. \tag{3.44}$$

Similarly, any other arbitrary line $\mathscr{L}(\gamma, \tilde{\delta})$ can be obtained from the line $\mathscr{L}_1$

$$\mathscr{L}(\gamma, \tilde{\delta}) = \mathrm{g}_2 \mathscr{L}_1. \tag{3.45}$$

Since g_1 is invertible, then

$$\mathscr{L}(\gamma, \tilde{\delta}) = \mathrm{g}_2 \mathrm{g}_1^{-1} \mathscr{L}(\rho, \tilde{\sigma}) = \mathrm{g}_3 \mathscr{L}(\rho, \tilde{\sigma}), \tag{3.46}$$

where $\mathrm{g}_3 \in \mathcal{S}p(2, \mathcal{Z}_d)$. Eq. (3.46) shows that, acting on an arbitrary line with the symplectic transformations, we get the remaining lines.

□

Table (3.1) shows the set of all maximal lines in $\mathcal{Z}_{15} \times \mathcal{Z}_{15}$ and their

component lines in $\mathcal{Z}_3 \times \mathcal{Z}_3$ and $\mathcal{Z}_5 \times \mathcal{Z}_5$, correspondingly. Also, Table (3.2) shows the set of all maximal lines in $\mathcal{Z}_{21} \times \mathcal{Z}_{21}$ and their component lines in $\mathcal{Z}_3 \times \mathcal{Z}_3$ and $\mathcal{Z}_7 \times \mathcal{Z}_7$, correspondingly.

Table 3.1: The maximal lines $\mathscr{L}(\rho, \sigma)$ in $\mathcal{Z}_{15} \times \mathcal{Z}_{15}$ and their component lines $\mathscr{L}^{(1)}(\rho_1, \tilde{\sigma}_1)$ and $\mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2)$ in $\mathcal{Z}_3 \times \mathcal{Z}_3$ and $\mathcal{Z}_5 \times \mathcal{Z}_5$, respectively, according to Eqs.(3.32,3.33). We stress that $\mathscr{L}^{(1)}(\rho_1, \tilde{\sigma}_1) = \mathscr{L}^{(1)}(\lambda_1\rho_1, \lambda_1\tilde{\sigma}_1)$ where λ_1 is invertible element in $\mathcal{Z}_3$, and similarly $\mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2) = \mathscr{L}^{(2)}(\lambda_2\rho_2, \lambda_2\tilde{\sigma}_2)$ where λ_2 is invertible element in $\mathcal{Z}_5$.

$\mathscr{L}(\rho,\sigma)$	$\mathrm{g}(\kappa,\lambda\|\mu,\nu)\mathscr{L}_1$	$\mathscr{L}^{(1)}(\rho_1,\tilde{\sigma}_1)$	$\mathscr{L}^{(2)}(\rho_2,\tilde{\sigma}_2)$
$\mathscr{L}_1 = \mathscr{L}(0,1)$	$\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_2 = \mathscr{L}(6,5)$	$\mathrm{g}(10,12\|12,10)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,0) = \mathrm{g}(0,1\|-1,0)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_3 = \mathscr{L}(3,1)$	$\mathrm{g}(10,12\|12,4)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,4) = \mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_4 = \mathscr{L}(3,7)$	$\mathrm{g}(10,12\|12,13)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,3) = \mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_5 = \mathscr{L}(6,11)$	$\mathrm{g}(10,12\|12,7)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,2) = \mathrm{g}(0,1\|-1,-3)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_6 = \mathscr{L}(3,4)$	$\mathrm{g}(10,12\|12,1)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,1) = \mathrm{g}(0,1\|-1,-4)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_7 = \mathscr{L}(10,3)$	$\mathrm{g}(6,5\|10,6)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0) = \mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_8 = \mathscr{L}(10,13)$	$\mathrm{g}(6,5\|10,11)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2) = \mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_9 = \mathscr{L}(5,4)$	$\mathrm{g}(6,5\|10,1)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1) = \mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{10} = \mathscr{L}(1,0)$	$\mathrm{g}(0,2\|7,0)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0) = \mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,0) = \mathrm{g}(0,1\|-1,0)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{11} = \mathscr{L}(1,12)$	$\mathrm{g}(0,2\|7,9)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0) = \mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,4) = \mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{12} = \mathscr{L}(1,9)$	$\mathrm{g}(0,2\|7,3)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0) = \mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,3) = \mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{13} = \mathscr{L}(1,6)$	$\mathrm{g}(0,2\|7,12)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0) = \mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,2) = \mathrm{g}(0,1\|-1,-3)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{14} = \mathscr{L}(1,3)$	$\mathrm{g}(0,2\|7,6)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0) = \mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,1) = \mathrm{g}(0,1\|-1,-4)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{15} = \mathscr{L}(1,10)$	$\mathrm{g}(0,2\|7,5)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2) = \mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,0) = \mathrm{g}(0,1\|-1,0)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{16} = \mathscr{L}(1,7)$	$\mathrm{g}(0,2\|7,14)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2) = \mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,4) = \mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{17} = \mathscr{L}(1,4)$	$\mathrm{g}(0,2\|7,8)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2) = \mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,3) = \mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{18} = \mathscr{L}(1,1)$	$\mathrm{g}(0,2\|7,2)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2) = \mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,2) = \mathrm{g}(0,1\|-1,-3)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{19} = \mathscr{L}(1,13)$	$\mathrm{g}(0,2\|7,11)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2) = \mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,1) = \mathrm{g}(0,1\|-1,-4)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{20} = \mathscr{L}(1,5)$	$\mathrm{g}(0,2\|7,10)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1) = \mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,0) = \mathrm{g}(0,1\|-1,0)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{21} = \mathscr{L}(1,2)$	$\mathrm{g}(0,2\|7,4)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1) = \mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,4) = \mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{22} = \mathscr{L}(1,14)$	$\mathrm{g}(0,2\|7,13)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1) = \mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,3) = \mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{23} = \mathscr{L}(1,11)$	$\mathrm{g}(0,2\|7,7)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1) = \mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,2) = \mathrm{g}(0,1\|-1,-3)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{24} = \mathscr{L}(1,8)$	$\mathrm{g}(0,2\|7,1)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1) = \mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,1) = \mathrm{g}(0,1\|-1,-4)\mathscr{L}^{(2)}(0,1)$

We mentioned earlier that when the geometry is not near-linear two lines might have more than one point in common. The following proposition explains the relation between the number of common points between two lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ and their first and second component lines in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$ and

Table 3.2: The maximal lines $\mathscr{L}(\rho,\sigma)$ in $\mathcal{Z}_{21}\times\mathcal{Z}_{21}$ and their component lines $\mathscr{L}^{(1)}(\rho_1,\tilde{\sigma}_1)$ and $\mathscr{L}^{(2)}(\rho_2,\tilde{\sigma}_2)$ in $\mathcal{Z}_3\times\mathcal{Z}_3$ and $\mathcal{Z}_7\times\mathcal{Z}_7$, respectively, according to Eqs.(3.32,3.33). We stress that $\mathscr{L}^{(1)}(\rho_1,\tilde{\sigma}_1)=\mathscr{L}^{(1)}(\lambda_1\rho_1,\lambda_1\tilde{\sigma}_1)$ where λ_1 is invertible element in $\mathcal{Z}_3$, and similarly $\mathscr{L}^{(2)}(\rho_2,\tilde{\sigma}_2)=\mathscr{L}^{(2)}(\lambda_2\rho_2,\lambda_2\tilde{\sigma}_2)$ where λ_2 is invertible element in $\mathcal{Z}_7$.

$\mathscr{L}(\rho,\sigma)$	$\mathrm{g}(\kappa,\lambda\|\mu,\nu)\mathscr{L}_1$	$\mathscr{L}^{(1)}(\rho_1,\tilde{\sigma}_1)$	$\mathscr{L}^{(2)}(\rho_2,\tilde{\sigma}_2)$
$\mathscr{L}_1=\mathscr{L}(0,1)$	$\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_2=\mathscr{L}(15,7)$	$\mathrm{g}(7,12\|18,7)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_3=\mathscr{L}(15,4)$	$\mathrm{g}(7,12\|18,13)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,6)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_4=\mathscr{L}(15,1)$	$\mathrm{g}(7,12\|18,19)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,5)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_5=\mathscr{L}(15,19)$	$\mathrm{g}(7,12\|18,4)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,4)=\mathrm{g}(0,1\|-1,-3)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_6=\mathscr{L}(15,16)$	$\mathrm{g}(7,12\|18,10)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,3)=\mathrm{g}(0,1\|-1,-4)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_7=\mathscr{L}(15,13)$	$\mathrm{g}(7,12\|18,16)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,2)=\mathrm{g}(0,1\|-1,-5)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_8=\mathscr{L}(15,10)$	$\mathrm{g}(7,12\|18,1)\mathscr{L}_1$	$\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,1)=\mathrm{g}(0,1\|-1,-6)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_9=\mathscr{L}(7,3)$	$\mathrm{g}(15,7\|14,15)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{10}=\mathscr{L}(7,17)$	$\mathrm{g}(15,7\|14,8)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{11}=\mathscr{L}(7,10)$	$\mathrm{g}(15,7\|14,1)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{12}=\mathscr{L}(1,0)$	$\mathrm{g}(0,19\|11,0)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{13}=\mathscr{L}(1,18)$	$\mathrm{g}(0,19\|11,6)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,6)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{14}=\mathscr{L}(1,15)$	$\mathrm{g}(0,19\|11,12)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,5)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{15}=\mathscr{L}(1,12)$	$\mathrm{g}(0,19\|11,18)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,4)=\mathrm{g}(0,1\|-1,-3)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{16}=\mathscr{L}(1,9)$	$\mathrm{g}(0,19\|11,3)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,3)=\mathrm{g}(0,1\|-1,-4)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{17}=\mathscr{L}(1,6)$	$\mathrm{g}(0,19\|11,9)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,2)=\mathrm{g}(0,1\|-1,-5)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{18}=\mathscr{L}(1,3)$	$\mathrm{g}(0,19\|11,15)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,1)=\mathrm{g}(0,1\|-1,-6)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{19}=\mathscr{L}(1,14)$	$\mathrm{g}(0,19\|11,14)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{20}=\mathscr{L}(1,11)$	$\mathrm{g}(0,19\|11,20)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,6)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{21}=\mathscr{L}(1,8)$	$\mathrm{g}(0,19\|11,5)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,5)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{22}=\mathscr{L}(1,5)$	$\mathrm{g}(0,19\|11,11)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,4)=\mathrm{g}(0,1\|-1,-3)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{23}=\mathscr{L}(1,2)$	$\mathrm{g}(0,19\|11,17)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,3)=\mathrm{g}(0,1\|-1,-4)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{24}=\mathscr{L}(1,20)$	$\mathrm{g}(0,19\|11,2)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,2)=\mathrm{g}(0,1\|-1,-5)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{25}=\mathscr{L}(1,17)$	$\mathrm{g}(0,19\|11,8)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,2)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,1)=\mathrm{g}(0,1\|-1,-6)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{26}=\mathscr{L}(1,7)$	$\mathrm{g}(0,19\|11,7)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,0)=\mathrm{g}(0,1\|-1,0)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{27}=\mathscr{L}(1,4)$	$\mathrm{g}(0,19\|11,13)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,6)=\mathrm{g}(0,1\|-1,-1)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{28}=\mathscr{L}(1,1)$	$\mathrm{g}(0,19\|11,19)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,5)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{29}=\mathscr{L}(1,19)$	$\mathrm{g}(0,19\|11,4)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,4)=\mathrm{g}(0,1\|-1,-3)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{30}=\mathscr{L}(1,16)$	$\mathrm{g}(0,19\|11,10)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,3)=\mathrm{g}(0,1\|-1,-4)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{31}=\mathscr{L}(1,13)$	$\mathrm{g}(0,19\|11,16)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,2)=\mathrm{g}(0,1\|-1,-5)\mathscr{L}^{(2)}(0,1)$
$\mathscr{L}_{32}=\mathscr{L}(1,10)$	$\mathrm{g}(0,19\|11,1)\mathscr{L}_1$	$\mathscr{L}^{(1)}(1,1)=\mathrm{g}(0,1\|-1,-2)\mathscr{L}^{(1)}(0,1)$	$\mathscr{L}^{(2)}(1,1)=\mathrm{g}(0,1\|-1,-6)\mathscr{L}^{(2)}(0,1)$

$\mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$, correspondingly.

Proposition 3.3.2. *If* $\mathscr{L}(\rho,\sigma) = \mathscr{L}^{(1)}(\rho_1,\tilde{\sigma}_1)\times\mathscr{L}^{(2)}(\rho_2,\tilde{\sigma}_2)$ *and* $\mathscr{L}(\rho',\sigma') = \mathscr{L}^{(1)}(\rho'_1,\tilde{\sigma'}_1)\times\mathscr{L}^{(2)}(\rho'_2,\tilde{\sigma'}_2)$ *is a pair of two different maximal lines in* $\mathcal{Z}_d \times \mathcal{Z}_d$ *where* $d = p_1p_2$*, then the number of these such (not ordered) pairs is* $\psi(d)[\psi(d)-1]/2$*. Moreover the following statements hold:*

(1) Two lines have p_2 points in common if and only if they have the same second component line (i.e. $\rho_2 = \lambda\rho'_2$ and $\tilde{\sigma}_2 = \lambda\tilde{\sigma'}_2$ where $\lambda \in \mathcal{Z}_{p_2}$ and $\lambda \neq 0$). The number of such pairs of lines is $p_1\psi(d)/2$.

(2) Two lines have p_1 points in common if and only if they have the same first component line (i.e. $\rho_1 = \lambda\rho'_1$ and $\tilde{\sigma}_1 = \lambda\tilde{\sigma'}_1$ where $\lambda \in \mathcal{Z}_{p_1}$ and $\lambda \neq 0$). The number of such pairs of lines is $p_2\psi(d)/2$.

(3) Two lines have only the origin in common if and only if both component lines in one line differ from their counterparts in the other line. The number of such pairs of lines is $d\psi(d)/2$.

Proof. Since we have $\psi(d)$ maximal lines in $\mathcal{Z}_d\times\mathcal{Z}_d$, then we have $\psi(d)[\psi(d)-1]$ ordered pairs of maximal lines such that the two lines in each pair are different from each other. Therefore, we have $\psi(d)[\psi(d)-1]/2$ (not ordered) pairs of maximal lines.

(1) Consider the pairs of maximal lines where the two lines in each pair have the same second component line $\mathscr{L}^{(2)}(\rho_2,\tilde{\sigma}_2)$. The two lines in each pair have two different first component lines $\mathscr{L}^{(1)}(\rho_1,\tilde{\sigma}_1), \mathscr{L}^{(1)}(\rho'_1,\tilde{\sigma'}_1)$. The maximal lines $\mathscr{L}^{(1)}(\rho_1,\tilde{\sigma}_1), \mathscr{L}^{(1)}(\rho'_1,\tilde{\sigma'}_1)$ in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$ have only the origin in common. Therefore, by combining the origin in $\mathcal{Z}_{p_1} \times$

$\mathcal{Z}_{p_1}$ with the p_2 points of the line $\mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2)$ in $\mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$ we get p_2 points in common between the two lines $\mathscr{L}^{(1)}(\rho_1, \tilde{\sigma}_1) \times \mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2)$ and $\mathscr{L}^{(1)}(\rho'_1, \tilde{\sigma'}_1) \times \mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2)$. The number of such pairs is $[p_1(p_1 + 1)][(p_2 + 1)]/2 = p_1\psi(d)/2$.

(2) Regarding the pairs of maximal lines where the two lines in each pair have the same first component line, the proof is analogous to case (1). The number of such pairs is $[p_2(p_2 + 1)][(p_1 + 1)]/2 = p_2\psi(d)/2$.

(3) When both component lines are different, the two maximal lines $\mathscr{L}^{(1)}(\rho_1, \tilde{\sigma}_1)$, $\mathscr{L}^{(1)}(\rho'_1, \tilde{\sigma'}_1)$ in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$ have only the origin in common, also the two maximal lines $\mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2), \mathscr{L}^{(2)}(\rho'_2, \tilde{\sigma'}_2)$ in $\mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$ have only the origin in common. Therefore the two lines in these pairs have only the origin in common. We have $p_1p_2\psi(d)/2 = d\psi(d)/2$ of such pairs.

The three statements mentioned above have described all cases of lines in $\mathcal{Z}_d \times \mathcal{Z}_d$, therefore the inverse of these statements hold. □

Example 3.3.3. *In the phase space $\mathcal{Z}_{15} \times \mathcal{Z}_{15}$, the two lines $\mathscr{L}(0,1) = \mathscr{L}^{(1)}(0,1) \times \mathscr{L}^{(2)}(0,1)$ and $\mathscr{L}(10,13) = \mathscr{L}^{(1)}(1,2) \times \mathscr{L}^{(2)}(0,1)$ have 5 points in common, the two lines $\mathscr{L}(0,1) = \mathscr{L}^{(1)}(0,1) \times \mathscr{L}^{(2)}(0,1)$ and $\mathscr{L}(6,5) = \mathscr{L}^{(1)}(0,1) \times \mathscr{L}^{(2)}(1,0)$ have 3 points in common, and the two lines $\mathscr{L}(6,5) = \mathscr{L}^{(1)}(0,1) \times \mathscr{L}^{(2)}(1,0)$ and $\mathscr{L}(10,13) = \mathscr{L}^{(1)}(1,2) \times \mathscr{L}^{(2)}(0,1)$ have only the origin in common.*

For the purpose of showing the duality between the lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ (where $d = p_1p_2$; p_1, p_2 are prime numbers such that $p_1 < p_2$) and the weak mutually unbiased bases in $\mathcal{H}_d$, we introduce the following notation for the

set of maximal lines in $\mathcal{Z}_{p_j} \times \mathcal{Z}_{p_j}$; $j = 1, 2$.

$$\begin{aligned} \mathscr{L}_{-1}^{(j)} &= \mathscr{L}(0,1) \\ \mathscr{L}_{\lambda}^{(j)} &= \mathrm{g}(0,1|-1,-\lambda)\mathscr{L}(0,1), \end{aligned} \tag{3.47}$$

where $\lambda = 0, ..., p_j - 1$. The lines $\mathscr{L}_k^{(j)}$ in this set are defined such that $k = -1, ..., p_j - 1$ (i.e. $k \in \mathcal{Z}_{p_j+1}$). Let $\mathbb{S}$ be the set of maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ and $\mathbb{S}_n$ be the subsets of this set such that

$$\mathbb{S}_n = \{\mathscr{L}_m^{(1)} \times \mathscr{L}_{m+n}^{(2)} | m \in \mathcal{Z}_{p_1+1}\}; \quad n \in \mathcal{Z}_{p_2+1} \tag{3.48}$$

We note that $\mathbb{S} = \{\mathbb{S}_0 \cup ... \cup \mathbb{S}_{p_2}\}$, and the cardinality of $\mathbb{S}_n$ is $p_1 + 1$. The lines in the same subset $\mathbb{S}_n$ have only the origin in common, however lines in two different subsets $\mathbb{S}_n, \mathbb{S}_m$ might have more than one point in common. Table (3.3) shows an example of the subsets S_j in $\mathcal{Z}_{15} \times \mathcal{Z}_{15}$ and table (3.4) shows an example of the subsets S_j in $\mathcal{Z}_{21} \times \mathcal{Z}_{21}$.

Table 3.3: The subsets S_j of the maximal lines in $\mathcal{Z}_{15} \times \mathcal{Z}_{15}$. The lines in the same column (i.e., in the same subset S_j) have only the origin in common.

S_0	S_1	S_2	S_3	S_4	S_5
$\mathscr{L}_1$	$\mathscr{L}_2$	$\mathscr{L}_3$	$\mathscr{L}_4$	$\mathscr{L}_5$	$\mathscr{L}_6$
$\mathscr{L}_{10}$	$\mathscr{L}_{11}$	$\mathscr{L}_{12}$	$\mathscr{L}_9$	$\mathscr{L}_8$	$\mathscr{L}_7$
$\mathscr{L}_{16}$	$\mathscr{L}_{17}$	$\mathscr{L}_{18}$	$\mathscr{L}_{13}$	$\mathscr{L}_{14}$	$\mathscr{L}_{15}$
$\mathscr{L}_{22}$	$\mathscr{L}_{23}$	$\mathscr{L}_{24}$	$\mathscr{L}_{19}$	$\mathscr{L}_{20}$	$\mathscr{L}_{21}$

Table 3.4: The subsets S_j of the maximal lines in $\mathcal{Z}_{21} \times \mathcal{Z}_{21}$. The lines in the same column (i.e., in the same subset S_j) have only the origin in common.

S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
$\mathscr{L}_1$	$\mathscr{L}_2$	$\mathscr{L}_3$	$\mathscr{L}_4$	$\mathscr{L}_5$	$\mathscr{L}_6$	$\mathscr{L}_7$	$\mathscr{L}_8$
$\mathscr{L}_{12}$	$\mathscr{L}_{13}$	$\mathscr{L}_{14}$	$\mathscr{L}_{15}$	$\mathscr{L}_{16}$	$\mathscr{L}_{11}$	$\mathscr{L}_{10}$	$\mathscr{L}_9$
$\mathscr{L}_{20}$	$\mathscr{L}_{21}$	$\mathscr{L}_{22}$	$\mathscr{L}_{23}$	$\mathscr{L}_{24}$	$\mathscr{L}_{17}$	$\mathscr{L}_{18}$	$\mathscr{L}_{19}$
$\mathscr{L}_{28}$	$\mathscr{L}_{29}$	$\mathscr{L}_{30}$	$\mathscr{L}_{31}$	$\mathscr{L}_{32}$	$\mathscr{L}_{25}$	$\mathscr{L}_{26}$	$\mathscr{L}_{27}$

3.4 Summary

We have considered the lines in $\mathcal{Z}_d \times \mathcal{Z}_d$. We discussed the properties of these lines in details. We presented the concept of factorizing a line in $\mathcal{Z}_d \times \mathcal{Z}_d$ where $d = p_1 p_2$; p_1, p_2 are prime numbers, into two lines in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$ and $\mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$. It is straightforward to generalize this concept for $d = p_1 p_2 ... p_n$. For example if $d = p_1 p_2 p_3$, a line in $\mathcal{Z}_d \times \mathcal{Z}_d$ can be factorized into three lines in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$, $\mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$, and $\mathcal{Z}_{p_3} \times \mathcal{Z}_{p_3}$. In this case two lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ might have 1 or p_1 or p_2 or p_3 or $p_1 p_2$ or $p_1 p_3$ or $p_2 p_3$ points in common. In chapter (4) we use the properties of lines discussed in this chapter to show that there is a duality between the lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ and the weak mutually unbiased bases in $\mathcal{H}_d$.

Chapter 4

Weak mutually unbiased bases

In chapter (3), we have studied the finite geometry of the $\mathcal{Z}_d \times \mathcal{Z}_d$ phase space. Motivated by the properties of this geometry, we introduce a weaker concept than mutually unbiased bases in the d-dimensional quantum systems associated with this geometry, and we call it weak mutually unbiased bases. Weak mutually unbiased bases is a generalization of mutually unbiased bases in the sense that when d is a prime number, weak mutually unbiased bases are nothing but mutually unbiased bases. We present an explicit construction for a complete set of weak mutually unbiased bases where d is odd and $d = p_1 p_2;\ p_1, p_2$ are prime numbers. The generalization of this construction for quantum systems with $d = p_1 p_2 ... p_n$ is possible but lengthy. A complete set of $(d+1)$ mutually unbiased bases is sufficient for quantum tomography, however the existence of such sets have been proved only for power of prime dimensional systems ($d = p^n$). Like mutually unbiased bases, we prove that the proposed construction of weak mutually unbiased bases for systems with composite dimensions is tomographically complete. We show explicitly that

there is a duality between weak mutually unbiased bases in $\mathcal{H}_d$ and the maximal lines in the associated geometry $\mathcal{Z}_d \times \mathcal{Z}_d$ phase space. This chapter ends with presenting weak mutually unbiased bases as a complex projective 1-design with the angle set $\{0, 1/p_1, 1/p_2, 1/d\}$.

4.1 Introduction

Mutually unbiased bases play an important role in the context of finite quantum systems [63, 64, 65, 66, 67, 68]. In chapter (2) we have shown that the absolute value of the overlap of any two vectors belonging to two different mutually unbiased bases is $\frac{1}{\sqrt{d}}$, and the maximum number of mutually unbiased bases is $d + 1$, where d is the system dimension. One can construct a complete set of mutually unbiased bases (a set that contains the maximum number of such bases) if d is power of prime number. Currently, there is a lot of work on the construction of the complete set of mutually unbiased bases in systems with composite dimensions (other than power of prime dimensions) [58]. In this chapter, we introduce the concept of weak mutually unbiased bases where the absolute value of the overlap of any two vectors that belong to two different weak mutually unbiased bases is $\frac{1}{\sqrt{d}}$, or alternatively one of the values 0, $\frac{1}{\sqrt{p_i}}$ where p_i is a divisor of d (apart from $1, d$). We present a construction of complete set of $\psi(d)$ weak mutually unbiased bases for systems with dimensions d where d is odd and $d = p_1 p_2$; p_1, p_2 are prime numbers. This construction is based on factorizing the system with dimension d into two component systems with dimensions p_1 and p_2, respectively [20], then we combine the $(p_1 + 1)$ mutually unbiased bases in the first component system

with the $(p_2 + 1)$ mutually unbiased bases in the second component system to get $(p_1 + 1)(p_2 + 1) = \psi(d)$ weak mutually unbiased bases. We show that this construction is tomographically complete in the sense that the probabilities (from quantum tomography experiments) related to Von Neumann measurements using the bases of this construction can be used to calculate an arbitrary density matrix through inverse Radon transform.

'Symmetric informationally complete positive operator valued measures (SIC-POVM)' [69, 70, 71, 72] is relevant to our context of tomographical completeness, however SIC-POVM uses none-orthogonal bases. We note that another methodologies which are based on designs [73, 74] are used for quantum tomography [75, 76] as well as other quantum mechanical problems [74, 77, 78].

The concept of weak mutually unbiased bases modifies appropriately the concept of mutually unbiased bases and makes it suitable for the geometry of the phase space $\mathcal{Z}_d \times \mathcal{Z}_d$. We emphasize the intimate relation between weak mutually unbiased bases and lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ by illustrating the duality between them.

In the view of designs we show the contrast between mutually unbiased bases and weak mutually unbiased bases as mutually unbiased bases are complex projective 2-design while weak mutually unbiased bases are complex projective 1-design.

4.2 Factorization

Here we consider the systems with dimensions $d = p_1...p_N$ where p_i, p_j are coprime. Again we use the two one-to-one mapping introduced by Good [6]

$$k \leftrightarrow (k_1, ..., k_N); \;\; k_n = k \; (mod \; p_n); \;\; k = \sum_n k_n s_n \; (mod \; d) \tag{4.1}$$

and

$$k \leftrightarrow (\tilde{k}_1, ..., \tilde{k}_N); \;\; \tilde{k}_n = kt_n = k_n t_n \; (mod \; p_n); \;\; k = \sum_n \tilde{k}_n r_n \; (mod \; d), \tag{4.2}$$

where

$$r_n = \frac{d}{p_n}; \;\; t_n r_n = 1 \; (\text{mod } p_n); \;\; s_n = t_n r_n \; (\text{mod } d). \tag{4.3}$$

In chapter (2) we have shown that there is a one-to-one map between the position states and the momentum states in $\mathcal{H}_d$, and the position states and the momentum states in $\mathcal{H}_{p_1}, ..., \mathcal{H}_{p_N}$, as follows

$$\begin{aligned} |X; k\rangle &\leftrightarrow |X^{(1)}; \tilde{k}_1\rangle \otimes ... \otimes |X^{(N)}; \tilde{k}_N\rangle, \\ |P; k\rangle &\leftrightarrow |P^{(1)}; k_1\rangle \otimes ... \otimes |P^{(N)}; k_N\rangle. \end{aligned} \tag{4.4}$$

We also have shown the relation between the displacement operator in $\mathcal{H}_d$ and the displacement operators in $\mathcal{H}_{p_1}, ..., \mathcal{H}_{p_N}$,

$$\mathscr{D}(\alpha, \beta) = \bigotimes_j \mathscr{D}^{(j)}(\alpha_j, \tilde{\beta}_j). \tag{4.5}$$

In proposition (4.2.1) we explain that the symplectic transformation $\mathcal{S}(\kappa,\lambda|\mu,\nu)$ in $\mathcal{H}_d$ where $\kappa,\lambda,\mu,\nu \in \mathcal{Z}_d$ is the tensor product of the symplectic transformations $\mathcal{S}(\kappa_j,\lambda_j r_j|\tilde{\mu}_j,\nu_j)$ in $\mathcal{H}_{p_j}$ where $\kappa_j,\lambda_j,\tilde{\mu}_j,\nu_j \in \mathcal{Z}_{p_j}$ and $r_j = \frac{d}{p_j}$. The parameters $\kappa,\lambda,\nu \in \mathcal{Z}_d$ are related to their corresponding parameters $\kappa_j,\lambda_j,\nu_j \in \mathcal{Z}_{p_j}$ through the map of Eq. (4.1), and the parameter $\mu \in \mathcal{Z}_d$ is related to its corresponding parameter $\tilde{\mu}_j \in \mathcal{Z}_{p_j}$ through the map of Eq. (4.2).

Proposition 4.2.1.

$$\mathcal{S}(\kappa,\lambda|\mu,\nu) = \bigotimes_j \mathcal{S}^{(j)}(\kappa_j,\lambda_j r_j|\tilde{\mu}_j,\nu_j). \tag{4.6}$$

Where $r_j = \frac{d}{p_j}$; $\kappa_j,\lambda_j,\nu_j \in \mathcal{Z}_{p_j}$ are the components of $\kappa,\lambda,\nu \in \mathcal{Z}_d$, respectively as stated by the map of Eq. (4.1), and $\tilde{\mu}_j \in \mathcal{Z}_{p_j}$ is the component of $\mu \in \mathcal{Z}_d$ as stated by the map of Eq. (4.2). Furthermore, $\kappa_j,\lambda_j r_j,\tilde{\mu}_j,\nu_j$ satisfy the relation

$$\kappa_j\nu_j - \lambda_j r_j \tilde{\mu}_j = 1 \pmod{p_j}. \tag{4.7}$$

Proof. In chapter (2) we have shown that

$$\mathcal{S}(\kappa,\lambda|\mu,\nu)\mathscr{D}(\alpha,\beta)[\mathcal{S}(\kappa,\lambda|\mu,\nu)]^\dagger = \mathscr{D}(\alpha\nu+\beta\lambda,\alpha\mu+\beta\kappa). \tag{4.8}$$

Using the two equations (4.5,4.8) we get

$$\begin{aligned}\mathcal{S}(\kappa,\lambda|\mu,\nu)\mathscr{D}(\alpha,\beta)[\mathcal{S}(\kappa,\lambda|\mu,\nu)]^\dagger &= \mathscr{D}(\alpha\nu+\beta\lambda,\alpha\mu+\beta\kappa)\\ &= \bigotimes_j \mathscr{D}^{(j)}((\alpha\nu+\beta\lambda)_j,(\alpha\mu \tilde{+} \beta\kappa)_j)\end{aligned} \tag{4.9}$$

In chapter (3)- Proposition (3.3.1) we have proved that

$$\begin{aligned}(\alpha\nu+\beta\lambda)_j &= \alpha_j\nu_j+\tilde{\beta}_j\lambda_j r_j\\ (\alpha\mu\tilde{+}\beta\kappa)_j &= \alpha_j\tilde{\mu}_j+\tilde{\beta}_j\kappa_j.\end{aligned}\tag{4.10}$$

Using Eq. (4.9) in conjunction with (4.10) we find

$$\mathcal{S}(\kappa,\lambda|\mu,\nu)\mathscr{D}(\alpha,\beta)[\mathcal{S}(\kappa,\lambda|\mu,\nu)]^\dagger=\bigotimes_j\mathscr{D}^{(j)}(\alpha_j\nu_j+\tilde{\beta}_j\lambda_j r_j,\alpha_j\tilde{\mu}_j+\tilde{\beta}_j\kappa_j).\tag{4.11}$$

But

$$\begin{aligned}&\left[\bigotimes_j\mathcal{S}^{(j)}(\kappa_j,\lambda_j r_j|\tilde{\mu}_j,\nu_j)\right]\left[\bigotimes_j\mathscr{D}^{(j)}(\alpha_j,\tilde{\beta}_j)\right]\left[\bigotimes_j\mathcal{S}^{(j)}(\kappa_j,\lambda_j r_j|\tilde{\mu}_j,\nu_j)\right]^\dagger\\ &=\bigotimes_j\mathscr{D}^{(j)}(\alpha_j\nu_j+\tilde{\beta}_j\lambda_j r_j,\alpha_j\tilde{\mu}_j+\tilde{\beta}_j\kappa_j).\end{aligned}\tag{4.12}$$

By comparing Eqs. (4.11,4.12), we prove Eq. (4.6).

We next prove that $\kappa_j\nu_j-\lambda_j r_j\tilde{\mu}_j=1 \pmod{p_j}$. Since

$$\kappa\nu-\lambda\mu=1 \pmod{d}.\tag{4.13}$$

Then

$$(\kappa\nu-\lambda\mu)_j=1 \pmod{p_j},\tag{4.14}$$

where $(\kappa\nu-\lambda\mu)_j=(\kappa\nu-\lambda\mu) \pmod{p_j}$ are the components of $(\kappa\nu-\lambda\mu)$ as stated by the map of Eq. (4.1). Therefore,

$$\kappa_j\nu_j-\lambda_j\mu_j=1 \pmod{p_j}.\tag{4.15}$$

Since $t_j r_j = 1 \pmod{p_j}$, then

$$\kappa_j \nu_j - \lambda_j r_j \tilde{\mu_j} = 1 \pmod{p_j}. \tag{4.16}$$

□

4.3 Weak mutually unbiased bases

We consider the systems with dimensions $d = p_1 p_2$, where p_1, p_2 are odd prime numbers and $p_1 < p_2$.

Definition 4.3.1. Consider a set of ℓ orthonormal bases $|\mathcal{B}_j; n\rangle$ in H_d, where $n \in \mathcal{Z}_d$ and $j = 0, ..., \ell - 1$. Let

$$v_{jk}(n,m) = |\langle \mathcal{B}_j; n | \mathcal{B}_k; m \rangle|; \qquad v_{jk}(n,m) = v_{kj}(m,n). \tag{4.17}$$

Such bases are called weak mutually unbiased bases if for any pair of them $(|\mathcal{B}_j; n\rangle, |\mathcal{B}_k; m\rangle;\ j \neq k)$, one of the following three cases occurs :

(1)

$$\begin{aligned} v_{jk}(n,m) &= p_1^{-1/2}; \text{ for the } p_1 d \text{ pairs } (n,m) \in \mathcal{Z}_d \times \mathcal{Z}_d \text{ such that } n = m \pmod{p_2} \\ v_{jk}(n,m) &= 0; \quad \text{for the remaining } (n,m) \text{ pairs} \end{aligned} \tag{4.18}$$

(2)

$$\begin{aligned} v_{jk}(n,m) &= p_2^{-1/2}; \text{ for the } p_2 d \text{ pairs } (n,m) \in \mathcal{Z}_d \times \mathcal{Z}_d \text{ such that } n = m \pmod{p_1} \\ v_{jk}(n,m) &= 0; \quad \text{for the remaining } (n,m) \text{ pairs} \end{aligned} \tag{4.19}$$

(3)

$$v_{jk}(n,m) = d^{-1/2}; \quad \text{for all } (n,m) \in \mathcal{Z}_d \times \mathcal{Z}_d \tag{4.20}$$

In the following theorem, we explain that the complete set of weak mutually unbiased bases is a combination of the mutually unbiased bases in the first component system and the mutually unbiased bases in the second component system.

Theorem 4.3.2. *Consider the Hilbert space $\mathcal{H}_d$. Let $|B_j^{(1)}; \tilde{n}_1\rangle$ be a set of mutually unbiased bases in $\mathcal{H}_{p_1}$ and $|B_j^{(2)}; \tilde{n}_2\rangle$ be a set of mutually unbiased bases in $\mathcal{H}_{p_2}$.*

(1) Any set of weak mutually unbiased bases can be described as $|\mathcal{B}_j^{(1)}; \tilde{n}_1\rangle \otimes |\mathcal{B}_j^{(2)}; \tilde{n}_2\rangle$. Some of the bases $|\mathcal{B}_j^{(1)}; \tilde{n}_1\rangle$ with different j may be the same, in the same way some of the bases $|\mathcal{B}_j^{(2)}; \tilde{n}_2\rangle$ with different j may be the same.

(2) The maximum number of the weak mutually unbiased bases is $\psi(d)$. For a complete set of weak mutually unbiased bases, there are $\psi(d)[\psi(d) - 1]/2$ sets of values $v_{jk}(n,m)$ of which $p_1\psi(d)/2$ belong to the category of Eq. (4.18), $p_2\psi(d)/2$ belong to the category of Eq. (4.19), and $d\psi(d)/2$

belong to the category of Eq. (4.20).

Proof. (1) Consider a set of weak mutually unbiased bases $|\mathcal{B}_j; n\rangle$ (in $\mathcal{H}_d$) according to definition (4.3.1), where $j = 0, ..., \ell - 1$. Using the map of Eq. (4.2), any two orthonormal basis $|\mathcal{B}_j; n\rangle, |\mathcal{B}_k; m\rangle$ can be described as

$$\begin{aligned} |\mathcal{B}_j; n\rangle &= |\mathcal{B}_j^{(1)}; \tilde{n}_1\rangle \otimes |\mathcal{B}_j^{(2)}; \tilde{n}_2\rangle \\ |\mathcal{B}_k; m\rangle &= |\mathcal{B}_k^{(1)}; \tilde{m}_1\rangle \otimes |\mathcal{B}_k^{(2)}; \tilde{m}_2\rangle, \end{aligned} \tag{4.21}$$

where $|\mathcal{B}_j^{(1)}; \tilde{n}_1\rangle, |\mathcal{B}_k^{(1)}; \tilde{m}_1\rangle$ are two orthonormal bases in $\mathcal{H}_{p_1}$, and $|\mathcal{B}_j^{(2)}; \tilde{n}_2\rangle$, $|\mathcal{B}_k^{(2)}; \tilde{m}_2\rangle$ are two orthonormal bases in $\mathcal{H}_{p_2}$. We take into account the three cases considered in definition (4.3.1). For each case we prove that the two bases $|\mathcal{B}_j^{(1)}; \tilde{n}_1\rangle, |\mathcal{B}_k^{(1)}; \tilde{m}_1\rangle$ are either the same or mutually unbiased in $\mathcal{H}_{p_1}$. The same holds for the two bases $|\mathcal{B}_j^{(2)}; \tilde{n}_2\rangle, |\mathcal{B}_k^{(2)}; \tilde{m}_2\rangle$ in $\mathcal{H}_{p_2}$.

(a) Taking into consideration the case of Eq. (4.18).

$$|\langle \mathcal{B}_j; n | \mathcal{B}_k; m\rangle| = p_1^{-1/2} \text{ for all } n, m \in \mathcal{Z}_d \text{ such that } n = m \pmod{p_2}. \tag{4.22}$$

In the case that $n = m \pmod{p_2}$,

$$\tilde{n}_2 = nt_2 \pmod{p_2} = mt_2 \pmod{p_2} = \tilde{m}_2. \tag{4.23}$$

Moreover, as n, m take all values in $\mathcal{Z}_d$ such that $n = m \pmod{p_2}$,

$\tilde{n}_1, \tilde{m}_1$ take all values in $\mathcal{Z}_{p_1}$. Using Eq. (4.22) we find

$$|\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle| |\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle| = p_1^{-1/2}, \tag{4.24}$$

but

$$|\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle| \leq 1, \tag{4.25}$$

then, multiplying Eq. (4.25) by $|\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle|$ we find

$$|\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle| |\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle| \leq |\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle|. \tag{4.26}$$

Therefore,

$$|\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle| \geq p_1^{-1/2}. \tag{4.27}$$

Since $|\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle| \leq 1$, then

$$p_1^{-1/2} \leq |\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle| \leq 1. \tag{4.28}$$

Since

$$\sum_{\tilde{m}_1 \in \mathcal{Z}_{p_1}} |\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle|^2 = 1. \tag{4.29}$$

From Eq. (4.28,4.29) follows that

$$|\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle| = p_1^{-1/2} \text{ for all } (\tilde{n}_1, \tilde{m}_1) \in \mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}. \tag{4.30}$$

Therefore, the bases $|\mathcal{B}_j^{(1)}; \tilde{m}_1\rangle$ form a set of mutually unbiased bases in $\mathcal{H}_{p_1}$. This case explains that the two bases $|\mathcal{B}_j^{(2)}, \tilde{n}_2\rangle, |\mathcal{B}_k^{(2)}, \tilde{m}_2\rangle$

are the same basis as $|\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle| = 1;\ \tilde{n}_2 = \tilde{m}_2$.

(b) Similar to (a), regarding the case of Eq. (4.19) we find

$$p_2^{-1/2} \leq |\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle| \leq 1, \tag{4.31}$$

and

$$\sum_{\tilde{m}_2 \in \mathcal{Z}_{p_2}} |\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle|^2 = 1. \tag{4.32}$$

Therefore,

$$|\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle| = p_2^{-1/2} \text{ for all } (\tilde{n}_2, \tilde{m}_2) \in \mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}, \tag{4.33}$$

i.e. the bases $|\mathcal{B}_j^{(2)}; \tilde{n}_2\rangle$ are mutually unbiased bases in $\mathcal{H}_{p_2}$. Since $|\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle| = 1;\ \tilde{n}_1 = \tilde{m}_1$, therefore $|\mathcal{B}_j^{(1)}, \tilde{n}_1\rangle, |\mathcal{B}_k^{(1)}, \tilde{m}_1\rangle$ are the same basis.

(c) Taking into consideration the case of Eq. (4.20) we find

$$|\langle \mathcal{B}_j; n | \mathcal{B}_k; m \rangle| = d^{-1/2} \ \text{ for all } \ (n, m) \in \mathcal{Z}_d \times \mathcal{Z}_d. \tag{4.34}$$

Using the map of Eq. (4.2), Eq. (4.34) can be written as

$$|\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle| |\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle| = d^{-1/2}, \tag{4.35}$$

First we prove that $|\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle| = p_2^{-1/2}$ for all $\tilde{n}_2, \tilde{m}_2 \in \mathcal{Z}_{p_2}$. We choose the vectors $|\mathcal{B}_k; m'\rangle$ in the k-basis such that $m = m' \pmod{\mathrm{p}_1}$. Then $\tilde{m}_2'$ takes all values in $\mathcal{Z}_{p_2}$, and $\tilde{m}_1 = \tilde{m}_1'$.

Therefore,

$$|\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle| |\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2' \rangle| = d^{-1/2}. \tag{4.36}$$

Comparing Eq. (4.35,4.36) we conclude that $|\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle| = |\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2' \rangle|$, i.e. $|\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle|$ is constant for all $\tilde{m}_2 \in \mathcal{Z}_{p_2}$. But

$$\sum_{\tilde{m}_2 \in \mathcal{Z}_{p_2}} |\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle|^2 = 1. \tag{4.37}$$

Therefore, $|\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle| = p_2^{-1/2}$ for all $\tilde{m}_2 \in \mathcal{Z}_{p_2}$. This is also valid for any $\tilde{n}_2 \in \mathcal{Z}_{p_2}$, and hence $|\langle \mathcal{B}_j^{(2)}; \tilde{n}_2 | \mathcal{B}_k^{(2)}; \tilde{m}_2 \rangle| = p_2^{-1/2}$ for all $\tilde{n}_2, \tilde{m}_2 \in \mathcal{Z}_{p_2}$. Similarly $|\langle \mathcal{B}_j^{(1)}; \tilde{n}_1 | \mathcal{B}_k^{(1)}; \tilde{m}_1 \rangle| = p_1^{-1/2}$ for all $\tilde{n}_1, \tilde{m}_1 \in \mathcal{Z}_{p_1}$, therefore the bases $|\mathcal{B}_j^{(1)}; \tilde{n}_1\rangle$ are mutually unbiased in $\mathcal{H}_{p_1}$, and the bases $|\mathcal{B}_j^{(2)}; \tilde{n}_2\rangle$ are mutually unbiased in $\mathcal{H}_{p_2}$.

(2) Since the maximum number of mutually unbiased bases in $\mathcal{H}_{p_1}$ and $\mathcal{H}_{p_2}$ are $p_1 + 1$ and $p_2 + 1$, correspondingly, then the maximum number of weak mutually unbiased bases in $\mathcal{H}_d$ is $(p_1 + 1)(p_2 + 1) = \psi(d)$. Therefore, the number of the sets of values $v_{jk}(n, m)$ defined in Eq. (4.17) ; $j \neq k$ and $1 \leq j, k \leq \psi(d)$ is $\psi(d)[\psi(d) - 1]/2$. Any two bases corresponding to the first category of the weak mutually unbiased bases (Eq. (4.18)) can be written as

$$\begin{aligned} |\mathcal{B}_j; n\rangle &= |\mathcal{B}_j^{(1)}; \tilde{n}_1\rangle \otimes |\mathcal{B}_j^{(2)}; \tilde{n}_2\rangle \\ |\mathcal{B}_k; m\rangle &= |\mathcal{B}_k^{(1)}; \tilde{m}_1\rangle \otimes |\mathcal{B}_k^{(2)}; \tilde{m}_2\rangle, \end{aligned} \tag{4.38}$$

where $|\mathcal{B}_j^{(2)};\tilde{n}_2\rangle, |\mathcal{B}_k^{(2)};\tilde{m}_2\rangle$ are the same basis in $\mathcal{H}_{p_2}$, and $|\mathcal{B}_j^{(1)};\tilde{n}_1\rangle, |\mathcal{B}_k^{(1)};\tilde{m}_1\rangle$ are two mutually unbiased bases in $\mathcal{H}_{p_1}$. In the complete set of weak mutually unbiased bases, there are $(p_1+1)^2-(p_1+1)$ pairs of $|\mathcal{B}_j^{(1)};\tilde{n}_1\rangle, |\mathcal{B}_k^{(1)};\tilde{m}_1\rangle;\ j \neq k$. Multiplying this number with (p_2+1) (the maximum number of mutually unbiased bases in $\mathcal{H}_{p_2}$), and taking into account that $v_{jk}(n,m) = v_{kj}(m,n)$ we get $p_1(p_1+1)(p_2+1)/2 = p_1\psi(d)/2$ of the values $v_{jk}(n,m)$ that belong to the first category of Eq. (4.18). Similarly we prove that there are $p_2\psi(d)/2$ of the values $v_{jk}(n,m)$ that belong to the second category of Eq. (4.19). Since the total number of the values $v_{jk}(n,m)$ is $\psi(d)[\psi(d)-1]/2$, therefore the number of the values $v_{jk}(n,m)$ that belong to the third category of Eq. (4.20) is $d\psi(d)/2$.

□

We note that the two bases corresponding to any pair that belongs to the third category of Eq. (4.20) are mutually unbiased, however, in general, the two bases corresponding to any pair are not necessarily mutually unbiased.

4.4 Constructing Weak mutually unbiased bases

In this section we present an explicit construction of weak mutually unbiased bases in $\mathcal{H}_d$; $d = p_1p_2$ and p_1, p_2 are prime numbers. We begin with constructing the mutually unbiased bases in $\mathcal{H}_{p_1}$ and $\mathcal{H}_{p_2}$. To establish these constructions we adopt the one introduced in [54]. Then we combine the mutually unbiased bases in $\mathcal{H}_{p_1}$ and the mutually unbiased bases in $\mathcal{H}_{p_2}$ to construct weak mutually unbiased bases in $\mathcal{H}_d$. We prove that such construction satisfy Eqs. (4.18,4.19,4.20).

4.4.1 Constructing mutually unbiased bases in prime-dimensional systems

The eigenvectors of the generalized Pauli operators (displacement operators)

$$\mathscr{Z}, \mathscr{X}, \mathscr{X}\mathscr{Z}, ..., \mathscr{X}\mathscr{Z}^{p-1} \tag{4.39}$$

form a set of mutually unbiased bases in $\mathcal{H}_p$ where p is prime number [54]. Below we show that these bases are related to $|X; n\rangle$ through symplectic transformations. In chapter (2) we have presented symplectic transformations in $\mathcal{H}_p$ as the group of the symplectic matrices $\mathcal{S}p(2, \mathcal{Z}_p)$ with the parameters $\kappa, \lambda, \mu, \nu \in \mathcal{Z}_p$ such that

$$\kappa\nu - \lambda\mu = 1 \ \ (mod \quad p). \tag{4.40}$$

Acting with the symplectic transformation $\mathcal{S}(\kappa, \lambda|\mu, \nu)$ on $\mathscr{X}$, and $\mathscr{Z}$ we get

$$\begin{aligned}\mathscr{X}^{'} &= \mathcal{S}(\kappa, \lambda|\mu, \nu)\mathscr{X}[\mathcal{S}(\kappa, \lambda|\mu, \nu)]^{\dagger} = \mathscr{X}^{\kappa}\mathscr{Z}^{\lambda}\Omega(2^{-1}\kappa\lambda) = \mathscr{D}(\lambda, \kappa),\\ \mathscr{Z}^{'} &= \mathcal{S}(\kappa, \lambda|\mu, \nu)\mathscr{Z}[\mathcal{S}(\kappa, \lambda|\mu, \nu)]^{\dagger} = \mathscr{X}^{\mu}\mathscr{Z}^{\nu}\Omega(2^{-1}\mu\nu) = \mathscr{D}(\nu, \mu).\end{aligned} \tag{4.41}$$

We have proved that

$$\mathcal{S}(\kappa_2, \lambda_2|\mu_2, \nu_2)\mathcal{S}(\kappa_1, \lambda_1|\mu_1, \nu_1) = \mathcal{S}(\kappa, \lambda|\mu, \nu), \tag{4.42}$$

where

$$\begin{pmatrix} \kappa_1 & \lambda_1 \\ \mu_1 & \nu_1 \end{pmatrix} \begin{pmatrix} \kappa_2 & \lambda_2 \\ \mu_2 & \nu_2 \end{pmatrix} = \begin{pmatrix} \kappa & \lambda \\ \mu & \nu \end{pmatrix}. \tag{4.43}$$

Since

$$\mathscr{Z} = \mathscr{F}\mathscr{X}\mathscr{F}'; \quad \mathscr{X}^{-1} = \mathscr{F}\mathscr{Z}\mathscr{F}' \tag{4.44}$$

Then comparing Eqs. (4.41,4.44) we conclude that

$$\mathscr{F} = \mathcal{S}(0,1|-1,0). \tag{4.45}$$

Eq. (4.41) also shows that the operators $\mathscr{X}\mathscr{Z}^{\lambda}$ are related to the operator $\mathscr{X}$ through the relation

$$\mathcal{S}(1,\lambda|0,1)\mathscr{X}[\mathcal{S}(1,\lambda|0,1)]^{\dagger} = \mathscr{X}\mathscr{Z}^{\lambda}\Omega(2^{-1}\lambda); \quad \lambda = 1,...,p-1. \tag{4.46}$$

Using Eq. (4.42) we get

$$\mathcal{S}(1,\lambda|0,1)\mathcal{S}(1,\lambda'|0,1) = \mathcal{S}(1,\lambda+\lambda'|0,1); \tag{4.47}$$

where $\lambda, \lambda' \in \mathcal{Z}_p$. Eq. (4.47) shows that the symplectic transformations $\mathcal{S}(1,\lambda|0,1)$ form a subgroup of the $\mathcal{S}p(2,\mathcal{Z}_p)$ group.

Let $|\mathscr{X}(1,\lambda|0,1);n\rangle = \mathcal{S}(1,\lambda|0,1)|X;n\rangle$, and $|\mathscr{P}(1,\lambda|0,1);n\rangle = \mathcal{S}(1,\lambda|0,1)|P;n\rangle$. Therefore, From Eq. (4.39,4.46) follows that the bases

$$|X;n\rangle; \;\; |P;n\rangle; \;\; |P(1,1|0,1);n\rangle; \;\; ... \; ; \;\; |P(1,p-1|0,1);n\rangle. \tag{4.48}$$

form a set of mutually unbiased bases. Since

$$|P(1,\lambda|0,1);n\rangle = \mathcal{S}(1,\lambda|0,1)|P;n\rangle = \mathcal{S}(1,\lambda|0,1)\mathscr{F}|X;n\rangle, \tag{4.49}$$

therefore using Eq. (4.42,4.45) we get

$$|P(1,\lambda|0,1);n\rangle = \mathcal{S}(0,1|-1,-\lambda)|X;n\rangle = |X(0,1|-1,-\lambda);n\rangle. \tag{4.50}$$

Therefore, starting with the position states we use the symplectic transformations $\mathcal{S}(0,1|-1,-\lambda);\ \lambda \in \mathcal{Z}_p$ to construct the set of mutually unbiased bases in $\mathcal{H}_p$.

$$|X;n\rangle;\ \ |X(0,1|-1,-\lambda);n\rangle \quad \lambda \in \mathcal{Z}_p. \tag{4.51}$$

We note that, the above construction can also be used for power of prime dimensional systems ($d = p^m$), and in this case states have to be labeled with variables in the Galois field $G(p^m)$.

4.4.2 An explicit construction of weak mutually unbiased bases

We consider the systems with dimensions $d = p_1p_2;\ \ p_1, p_2$ are prime numbers. Using Eq. (4.51), starting from the position states we construct the set of mutually unbiased bases in $\mathcal{H}_{p_1}$, $|X^{(1)};\tilde{n}_1\rangle;\ \ |X^{(1)}(0,1|-1,-\lambda_1);\tilde{n}_1\rangle$. Similarly we construct the mutually unbiased bases in $\mathcal{H}_{p_2}$, $|X^{(2)};\tilde{n}_2\rangle;\ \ |X^{(2)}(0,1|-1,-\lambda_2);\tilde{n}_2\rangle$. We combine the set of mutually unbiased bases in $\mathcal{H}_{p_1}$ with the set of mutually unbiased bases in $\mathcal{H}_{p_2}$ to get the following set of bases T in

$\mathcal{H}_d$.

$$
\begin{aligned}
&|\mathcal{B}_1; n\rangle = |X^{(1)}; \tilde{n}_1\rangle \otimes |X^{(2)}; \tilde{n}_2\rangle \\
&|\mathcal{B}_{2+\lambda_2}; n\rangle = |X^{(1)}; \tilde{n}_1\rangle \otimes |X^{(2)}(0,1|-1,-\lambda_2); \tilde{n}_2\rangle \\
&|\mathcal{B}_{2+p_2+\lambda_1}; n\rangle = |X^{(1)}(0,1|-1,-\lambda_1); \tilde{n}_1\rangle \otimes |X^{(2)}; \tilde{n}_2\rangle \\
&|\mathcal{B}_{2+p_1+p_2+\lambda_2+\lambda_1 p_2}; n\rangle = |X^{(1)}(0,1|-1,-\lambda_1); \tilde{n}_1\rangle \otimes |X^{(2)}(0,1|-1,-\lambda_2); \tilde{n}_2\rangle,
\end{aligned}
\tag{4.52}
$$

where $n \in \mathcal{Z}_d$; $\tilde{n}_1, \lambda_1 \in \mathcal{Z}_{p_1}$; $\tilde{n}_2, \lambda_2 \in \mathcal{Z}_{p_2}$.

To unify the notation of the mutually unbiased bases in $\mathcal{H}_{p_j};\ j = 1, 2$, let

$$
\begin{aligned}
&|\mathcal{B}^{(j)}_{-1}; \tilde{n}_j\rangle = |X^{(j)}; \tilde{n}_j\rangle \\
&|\mathcal{B}^{(j)}_{\lambda_j}; \tilde{n}_j\rangle = |X^{(j)}(0,1|-1,-\lambda_j); \tilde{n}_j\rangle; \quad n_j, \lambda_j \in \mathcal{Z}_{p_j}
\end{aligned}
\tag{4.53}
$$

The following proposition proves that the above set is a set of weak mutually unbiased bases.

Proposition 4.4.1. *The absolute value of the overlap of any two vectors in two different bases $|\mathcal{B}_j; n\rangle, |\mathcal{B}_k; m\rangle$ (defined in Eq. (4.52)) where $1 \leq j, k \leq \psi(d)$ is equal to one of the following*

(1)

$$
\begin{aligned}
|\langle \mathcal{B}_j; n|\mathcal{B}_k; m\rangle| &= p_1^{-1/2};\ \text{for the } p_1 d \text{ pairs } (n,m) \in \mathcal{Z}_d \times \mathcal{Z}_d \text{ such that } n = m \pmod{p_2} \\
|\langle \mathcal{B}_j; n|\mathcal{B}_k; m\rangle| &= 0; \quad \text{for the rest } (n,m) \text{ pairs}
\end{aligned}
\tag{4.54}
$$

(2)

$$\begin{aligned} |\langle \mathcal{B}_j; n|\mathcal{B}_k; m\rangle| &= p_2^{-1/2}; \text{ for the } p_2 d \text{ pairs } (n,m) \in \mathcal{Z}_d \times \mathcal{Z}_d \text{ such that } n = m \pmod{p_1} \\ |\langle \mathcal{B}_j; n|\mathcal{B}_k; m\rangle| &= 0; \quad \text{for the rest } (n,m) \text{ pairs} \end{aligned} \tag{4.55}$$

(3)

$$|\langle \mathcal{B}_j; n|\mathcal{B}_k; m\rangle| = d^{-1/2}; \quad \text{for all } (n,m) \in \mathcal{Z}_d \times \mathcal{Z}_d \tag{4.56}$$

Proof.

$$|\mathcal{B}_j; n\rangle = |\mathcal{B}^{(1)}_{\alpha_1}; \tilde{n}_1\rangle \otimes |\mathcal{B}^{(2)}_{\alpha_2}; \tilde{n}_2\rangle, \tag{4.57}$$

where j is related to (α_1, α_2) through the two Eqs. (4.52,4.53), and n is related to $(\tilde{n}_1, \tilde{n}_2)$ according to the map of Eq. (4.2). Therefore,

$$|\langle \mathcal{B}_j; n|\mathcal{B}_k; m\rangle| = |\langle \mathcal{B}^{(1)}_{\alpha_1}; \tilde{n}_1|\mathcal{B}^{(1)}_{\beta_1}; \tilde{m}_1\rangle||\langle \mathcal{B}^{(2)}_{\alpha_2}; \tilde{n}_2|\mathcal{B}^{(2)}_{\beta_2}; \tilde{m}_2\rangle| \tag{4.58}$$

where $-1 \leq \alpha_1, \beta_1 \leq p_1 - 1$, and $-1 \leq \alpha_2, \beta_2 \leq p_2 - 1$. Since

$$\begin{aligned} |\langle \mathcal{B}^{(1)}_{\alpha_1}; \tilde{n}_1|\mathcal{B}^{(1)}_{\alpha_1}; \tilde{m}_1\rangle| &= \delta(\tilde{n}_1, \tilde{m}_1) \\ |\langle \mathcal{B}^{(1)}_{\alpha_1}; \tilde{n}_1|\mathcal{B}^{(1)}_{\beta_1}; \tilde{m}_1\rangle| &= p_1^{-1/2}; \quad \alpha_1 \neq \beta_1, \end{aligned} \tag{4.59}$$

and $|\langle \mathcal{B}^{(2)}_{\alpha_2}; \tilde{n}_2|\mathcal{B}^{(2)}_{\beta_2}; \tilde{m}_2\rangle|$ obeys similar relations, therefore we have only three cases for the absolute value of the overlap of any two vectors in two different bases $|\mathcal{B}_j; n\rangle, |\mathcal{B}_k; m\rangle$. The first case where the two bases in the first component system are different and the two bases in the second component system

are the same. This case agrees with the results in Eq. (4.54). The second case where the two bases in the first component system are the same and the two bases in the second component system are different. This case agrees with the results in Eq. (4.55). The third case where the two bases in both component systems are different. This case agrees with the results in Eq. (4.56). □

It is worth noting that the weak mutually unbiased bases construction of Eq. (4.52) can be Partitioned into $p_2 + 1$ subsets T_u such that

$$T_u = \{|\mathcal{B}^{(1)}_{j_1}; \tilde{n}_1\rangle \otimes |\mathcal{B}^{(2)}_{j_1+u}; \tilde{n}_2\rangle \mid j_1 \in \mathcal{Z}_{p_1+1}\}, \tag{4.60}$$

where $u \in \mathcal{Z}_{p_2+1}$, and hence the set of weak mutually unbiased bases can be written as

$$T = T_0 \cup ... \cup T_{p_2}; \tag{4.61}$$

such that $T_j \cap T_k = \emptyset$. The p_1+1 bases in each subset are mutually unbiased, however the bases in different subsets are not necessarily mutually unbiased.

Proposition 4.4.2. *The set of weak mutually unbiased bases T of Eq. (4.52) can be written as*

$$\begin{aligned}
&|\mathcal{B}_1; n\rangle = |X(1,0|0,1); n\rangle \\
&|\mathcal{B}_{2+\lambda_2}; n\rangle = |X(s_1, t_2 s_2| - p_1, s_1 - \lambda_2 s_2); n\rangle \\
&|\mathcal{B}_{2+p_2+\lambda_1}; n\rangle = |X(s_2, t_1 s_1| - p_2, -\lambda_1 s_1 + s_2); n\rangle \\
&|\mathcal{B}_{2+p_1+p_2+\lambda_2+\lambda_1 p_2}; n\rangle = |X(0, \Gamma| - p_1 - p_2, -\lambda_1 s_1 - \lambda_2 s_2); n\rangle
\end{aligned} \tag{4.62}$$

where t_1, s_1, t_2, s_2 are defined in Eq. (4.3) and $\Gamma = t_1^2 p_2 + t_2^2 p_1$.

Proof. Using Eq. (4.6) we get

$$|\mathcal{B}_1; n\rangle = |X^{(1)}; \tilde{n}_1\rangle \otimes |X^{(2)}; \tilde{n}_2\rangle = |X(1,0|0,1); n\rangle. \tag{4.63}$$

Also

$$\begin{aligned}
|\mathcal{B}_{2+\lambda_2}; n\rangle &= |X^{(1)}; \tilde{n}_1\rangle \otimes |X^{(2)}(0,1|-1,-\lambda_2); \tilde{n}_2\rangle \\
&= [\mathcal{I} \otimes \mathcal{S}^{(2)}(0,1|-1,-\lambda_2)][|X^{(1)}; \tilde{n}_1\rangle \otimes |X^{(2)}; \tilde{n}_2\rangle] \\
&= \mathcal{S}(s_1, t_2 s_2| - p_1, s_1 - \lambda_2 s_2)|X; n\rangle = |X(s_1, t_2 s_2| - p_1, s_1 - \lambda_2 s_2); n\rangle.
\end{aligned} \tag{4.64}$$

In the same way

$$\begin{aligned}
|\mathcal{B}_{2+p_2+\lambda_1}; n\rangle &= |X^{(1)}(0,1|-1,-\lambda_1); \tilde{n}_1\rangle \otimes |X^{(2)}; \tilde{n}_2\rangle \\
&= [\mathcal{S}^{(1)}(0,1|-1,-\lambda_1) \otimes \mathcal{I}][|X^{(1)}; \tilde{n}_1\rangle \otimes |X^{(2)}; \tilde{n}_2\rangle] \\
&= \mathcal{S}(s_2, t_1 s_1| - p_2, -\lambda_1 s_1 + s_2)|X; n\rangle = |X(s_2, t_1 s_1| - p_2, -\lambda_1 s_1 + s_2); n\rangle.
\end{aligned} \tag{4.65}$$

Similarly

$$\begin{aligned}
|\mathcal{B}_{2+p_1+p_2+\lambda_2+\lambda_1 p_2}; n\rangle &= |X^{(1)}(0,1|-1,-\lambda_1); \tilde{n}_1\rangle \otimes |X^{(2)}(0,1|-1,-\lambda_2); \tilde{n}_2\rangle \\
&= [\mathcal{S}^{(1)}(0,1|-1,-\lambda_1) \otimes \mathcal{S}^{(2)}(0,1|-1,-\lambda_2)][|X^{(1)}; \tilde{n}_1\rangle \otimes |X^{(2)}; \tilde{n}_2\rangle] \\
&= \mathcal{S}(0, \Gamma| - p_1 - p_2, -\lambda_1 s_1 - \lambda_2 s_2)|X; n\rangle \\
&= |X(0, \Gamma| - p_1 - p_2, -\lambda_1 s_1 - \lambda_2 s_2); n\rangle.
\end{aligned} \tag{4.66}$$

□

From Eqs. (4.63,4.64,4.65,4.66) follows that, only the parameter ν takes many values. The parameters κ, λ, μ take 4 values each, where $\kappa \in \{0, 1, s_1, s_2\}; \lambda \in \{0, t_1 s_1, t_2 s_2, \Gamma\}; \mu \in \{0, -p_1, -p_2, -p_1 - p_2\}$. Table (4.1) summarizes these values.

Table 4.1: Summary of the values of the parameters κ,λ, μ, ν for the construction of the weak mutually unbiased bases of Eq. (4.62), where $\lambda_j \in \mathbb{Z}_{p_j}$ and t_j, s_j, p_j, Γ are constants defined in the text.

κ	λ	μ	ν
1	0	0	1
s_1	$t_2 s_2$	$-p_1$	$s_1 - \lambda_2 s_2$
s_2	$t_1 s_1$	$-p_2$	$-\lambda_1 s_1 + s_2$
0	Γ	$-p_1 - p_2$	$-\lambda_1 s_1 - \lambda_2 s_2$

We give two examples of the construction of weak mutually unbiased bases in $\mathcal{H}_{15}$ and $\mathcal{H}_{21}$. Table (4.2) shows the set of weak mutually unbiased bases in $\mathcal{H}_{15}$ and their component bases $|\mathcal{B}_j^{(1)}; \tilde{m}_1\rangle$ and $|\mathcal{B}_j^{(2)}; \tilde{m}_2\rangle$ in $\mathcal{H}_3$ and $\mathcal{H}_5$, respectively, also table (4.3) shows the set of weak mutually unbiased bases in $\mathcal{H}_{21}$ and their component bases $|\mathcal{B}_j^{(1)}; \tilde{m}_1\rangle$ and $|\mathcal{B}_j^{(2)}; \tilde{m}_2\rangle$ in $\mathcal{H}_3$ and $\mathcal{H}_7$, respectively.

4.5 Weak mutually unbiased bases as tomographically complete set

Using the weak mutually unbiased bases of Eq. (4.52) in tomography experiments results in the probabilities $p(\beta|\nu, \mu)$ along all the maximal lines $\mathscr{L}(\nu, \mu)$

Table 4.2: The weak mutually unbiased bases in $\mathcal{H}_{15}$ and their component bases $|\mathcal{B}_j^{(1)}; \tilde{m}_1\rangle$ and $|\mathcal{B}_j^{(2)}; \tilde{m}_2\rangle$ in $\mathcal{H}_3$ and $\mathcal{H}_5$, respectively, according to Eq.(4.52).

$\lvert\mathcal{B}_j; m\rangle$	$\lvert X(\kappa,\lambda\vert\mu,\nu); m\rangle$	$\lvert B_j^{(1)}; \tilde{m}_1\rangle$	$\lvert B_j^{(2)}; \tilde{m}_2\rangle$
$\lvert\mathcal{B}_1; m\rangle$	$\lvert X; m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}; \tilde{m}_2\rangle$
$\lvert\mathcal{B}_2; m\rangle$	$\lvert X(10,12\vert12,10); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,0); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_3; m\rangle$	$\lvert X(10,12\vert12,4); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-1); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_4; m\rangle$	$\lvert X(10,12\vert12,13); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-2); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_5; m\rangle$	$\lvert X(10,12\vert12,7); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-3); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_6; m\rangle$	$\lvert X(10,12\vert12,1); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-4); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_7; m\rangle$	$\lvert X(6,5\vert10,6); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}; \tilde{m}_2\rangle$
$\lvert\mathcal{B}_8; m\rangle$	$\lvert X(6,5\vert10,11); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}; \tilde{m}_2\rangle$
$\lvert\mathcal{B}_9; m\rangle$	$\lvert X(6,5\vert10,1); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}; \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{10}; m\rangle$	$\lvert X(0,2\vert7,0); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,0); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{11}; m\rangle$	$\lvert X(0,2\vert7,9); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,0); \tilde{m}_2\rangle$	$\lvert X^{(2)}(0,1\vert-1,-1); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{12}; m\rangle$	$\lvert X(0,2\vert7,3); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-2); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{13}; m\rangle$	$\lvert X(0,2\vert7,12); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-3); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{14}; m\rangle$	$\lvert X(0,2\vert7,6); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-4); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{15}; m\rangle$	$\lvert X(0,2\vert7,5); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,0); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{16}; m\rangle$	$\lvert X(0,2\vert7,14); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-1); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{17}; m\rangle$	$\lvert X(0,2\vert7,8); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-2); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{18}; m\rangle$	$\lvert X(0,2\vert7,2); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-3); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{19}; m\rangle$	$\lvert X(0,2\vert7,11); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-4); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{20}; m\rangle$	$\lvert X(0,2\vert7,10); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,0); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{21}; m\rangle$	$\lvert X(0,2\vert7,4); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-1); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{22}; m\rangle$	$\lvert X(0,2\vert7,13); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-2); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{23}; m\rangle$	$\lvert X(0,2\vert7,7); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-3); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{24}; m\rangle$	$\lvert X(0,2\vert7,1); m\rangle$	$\lvert X^{(1)}(0,1\vert-1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\vert-1,-4); \tilde{m}_2\rangle$

Table 4.3: The weak mutually unbiased bases in $\mathcal{H}_{21}$ and their component bases $|\mathcal{B}_j^{(1)}; \tilde{m}_1\rangle$ and $|\mathcal{B}_j^{(2)}; \tilde{m}_2\rangle$ in $\mathcal{H}_3$ and $\mathcal{H}_7$, respectively, according to Eq.(4.52).

$\lvert\mathcal{B}_j; m\rangle$	$\lvert X(\kappa,\lambda\lvert\mu,\nu); m\rangle$	$\lvert B_j^{(1)}; \tilde{m}_1\rangle$	$\lvert B_j^{(2)}; \tilde{m}_2\rangle$
$\lvert\mathcal{B}_1; m\rangle$	$\lvert X; m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}; \tilde{m}_2\rangle$
$\lvert\mathcal{B}_2; m\rangle$	$\lvert X(7,12\lvert 18,7); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,0); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_3; m\rangle$	$\lvert X(7,12\lvert 18,13); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-1); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_4; m\rangle$	$\lvert X(7,12\lvert 18,19); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-2); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_5; m\rangle$	$\lvert X(7,12\lvert 18,4); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-3); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_6; m\rangle$	$\lvert X(7,12\lvert 18,10); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-4); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_7; m\rangle$	$\lvert X(7,12\lvert 18,16); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-5); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_8; m\rangle$	$\lvert X(7,12\lvert 18,1); m\rangle$	$\lvert X^{(1)}; \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-6); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_9; m\rangle$	$\lvert X(15,7\lvert 14,15); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}; \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{10}; m\rangle$	$\lvert X(15,7\lvert 14,8); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}; \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{11}; m\rangle$	$\lvert X(15,7\lvert 14,1); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}; \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{12}; m\rangle$	$\lvert X(0,19\lvert 11,0); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,0); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{13}; m\rangle$	$\lvert X(0,19\lvert 11,6); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-1); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{14}; m\rangle$	$\lvert X(0,19\lvert 11,12); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-2); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{15}; m\rangle$	$\lvert X(0,19\lvert 11,18); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-3); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{16}; m\rangle$	$\lvert X(0,19\lvert 11,3); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-4); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{17}; m\rangle$	$\lvert X(0,19\lvert 11,9); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-5); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{18}; m\rangle$	$\lvert X(0,19\lvert 11,15); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,0); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-6); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{19}; m\rangle$	$\lvert X(0,19\lvert 11,14); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,0); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{20}; m\rangle$	$\lvert X(0,19\lvert 11,20); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-1); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{21}; m\rangle$	$\lvert X(0,19\lvert 11,5); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-2); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{22}; m\rangle$	$\lvert X(0,19\lvert 11,11); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-3); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{23}; m\rangle$	$\lvert X(0,19\lvert 11,17); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-4); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{24}; m\rangle$	$\lvert X(0,19\lvert 11,2); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-5); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{25}; m\rangle$	$\lvert X(0,19\lvert 11,8); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-1); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-6); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{26}; m\rangle$	$\lvert X(0,19\lvert 11,7); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,0); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{27}; m\rangle$	$\lvert X(0,19\lvert 11,13); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-1); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{28}; m\rangle$	$\lvert X(0,19\lvert 11,19); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-2); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{29}; m\rangle$	$\lvert X(0,19\lvert 11,4); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-3); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{30}; m\rangle$	$\lvert X(0,19\lvert 11,10); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-4); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{31}; m\rangle$	$\lvert X(0,19\lvert 11,16); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-5); \tilde{m}_2\rangle$
$\lvert\mathcal{B}_{32}; m\rangle$	$\lvert X(0,19\lvert 11,1); m\rangle$	$\lvert X^{(1)}(0,1\lvert -1,-2); \tilde{m}_1\rangle$	$\lvert X^{(2)}(0,1\lvert -1,-6); \tilde{m}_2\rangle$

(through the origin) in $\mathcal{Z}_d \times \mathcal{Z}_d$. Let $\Pi[X(\kappa,\lambda|\mu,\nu);n] = |X(\kappa,\lambda|\mu,\nu);n\rangle\langle X(\kappa,\lambda|\mu,\nu);n|$ be the projectors corresponding to the weak mutually unbiased bases, therefore

$$p(\beta|\nu,\mu) = Tr(\mathcal{D}|X(\kappa,\lambda|\mu,\nu);\beta\rangle\langle X(\kappa,\lambda|\mu,\nu);\beta|), \tag{4.67}$$

and

$$\sum_{\beta} p(\beta|\nu,\mu) = 1. \tag{4.68}$$

In this section we prove that the probabilities $p(\beta|\nu,\mu)$ corresponding to the weak mutually unbiased bases of Eq. (4.52) in $\mathcal{H}_d$; $d = p_1 p_2$ can be used to calculate the density matrix of an arbitrary quantum system with dimension d, and hence the set of weak mutually unbiased bases is tomographically complete.

The constraint of Eq. (4.40) leads to the existing condition of the symplectic transformation $\mathcal{S}(\kappa,\lambda|\mu,\nu)$

$$\mathbb{G}(\mu,\nu,d) = \mathbb{G}(\kappa,\mu,d) = \mathbb{G}(\lambda,\nu,d) = \mathbb{G}(\kappa,\lambda,d) = 1 \ (\text{mod } d). \tag{4.69}$$

as if $\mathbb{G}(\mu,\nu,d) = n; n \neq 1$, then $\kappa\nu - \lambda\mu = \kappa(n\nu') - \lambda(n\mu') = n(\kappa\nu' - \lambda\mu') = 1 \ (\text{mod } d)$. This would mean that $\kappa\nu' - \lambda\mu'$ is the multiplicative inverse of n, but this is not possible as the inverse of n does not exist in $\mathcal{Z}_d$ because n is a divisor of d. Therefore, $\mathbb{G}(\mu,\nu,d) = 1 \ (\text{mod } d)$. Similarly we can prove that $\mathbb{G}(\kappa,\mu,d) = \mathbb{G}(\lambda,\nu,d) = \mathbb{G}(\kappa,\lambda,d) = 1 \ (\text{mod } d)$.

Now we prove that the values of μ and ν in table (4.1) satisfy the condition $\mathbb{G}(\mu,\nu,d) = 1 \ (\text{mod } d)$. It is clear that $\mathbb{G}(0,1,d) = 1 \ (\text{mod } d)$. Also, $\mathbb{G}(-p_1-p_2, -\lambda_1 s_1 - \lambda_2 s_2, d) = 1 \ (\text{mod } d)$ because $\mathbb{G}(-p_1-p_2,d) = 1 \ (\text{mod } d)$.

Since $s_1 = t_1 r_1 = t_1 p_2$ and $s_2 = t_2 r_2 = t_2 p_1$, then $s_1 = 1 \pmod{p_1}$ and $s_2 = 0 \pmod{p_1}$. Therefore, $s_1 - \lambda_2 s_2 = 1 + M p_1 - \lambda_2 N p_1 = 1 + p_1(M - \lambda_2 N)$; M, N are integers. As a result $s_1 - \lambda_2 s_2$ and p_1 are coprime, and hence $\mathbb{G}(-p_1, s_1 - \lambda_2 s_2, d) = 1 \pmod{d}$. Similarly, we can prove that $\mathbb{G}(-p_2, s_2 - \lambda_1 s_1, d) = 1 \pmod{d}$. Therefore, we conclude that all the lines $\mathscr{L}(\nu, \mu)$ (where ν, μ are defined in table 4.1) in $\mathscr{Z}_d \times \mathscr{Z}_d$ are maximal.

The number of probabilities that we get from the tomography experiments along one maximal line is $d-1$ (because one of the probabilities is dependent on the other $d-1$ probabilities as the total sum of these probabilities is equal to 1), and hence the total number of probabilities that we get along all the maximal lines associated with the weak mutually unbiased bases is $\psi(d)(d-1)$. So we have $\psi(d)(d-1)$ probabilities for the $d^2 - 1$ degrees of freedom of the density matrix, therefore we present the redundancy parameter $\mathscr{R}$ to measure the overcompleteness of the weak mutually unbiased bases,

$$\mathscr{R} = \frac{\psi(d)(d-1)}{d^2 - 1} - 1 = \frac{\psi(d)}{d+1} - 1. \tag{4.70}$$

4.6 Tomographical completeness

In chapter (2) we have shown that applying inverse Radon transform to the probabilities resulted from the quantum measurements along the lines $\mathscr{L}(\nu, \mu)$ leads to Weyl function at the points $(\rho = \alpha\nu, \sigma = \alpha\mu)$, where $\rho, \sigma \in \mathscr{Z}_d$

$$\widetilde{\mathcal{W}}(\alpha\nu, \alpha\mu) = \sum_{\beta} p(\beta|\nu, \mu)\Omega(\alpha\beta). \tag{4.71}$$

Since $d = p_1 p_2$, then $\mathcal{Z}_d$ is not a field, and two sets of probabilities according to two different lines $\mathscr{L}(\nu, \mu), \mathscr{L}(\nu', \mu')$ may lead to the Weyl function at the same point ($\rho = \alpha\nu = \alpha'\nu', \sigma = \alpha\mu = \alpha'\mu'$) (this is where the redundancy comes from). This fact is considered to be an important consistency constraints for such probabilities, as

$$\widetilde{\mathcal{W}}(\rho, \sigma) = \sum_{\beta} p(\beta|\nu, \mu)\Omega(\alpha\beta) = \sum_{\beta} p(\beta|\nu', \mu')\Omega(\alpha'\beta). \tag{4.72}$$

In section (4.7) We will explain these constraints with concrete examples. Wigner function and the density matrix can be calculated in terms of Weyl function using Eqs. (4.73,4.74), correspondingly.

$$\mathcal{W}(\gamma, \delta) = \frac{1}{d} \sum_{\rho,\sigma} \widetilde{\mathcal{W}}(\rho, \sigma)\Omega(\gamma\sigma - \delta\rho) \tag{4.73}$$

$$\mathcal{D} = \frac{1}{d} \sum_{\alpha,\beta} \widetilde{\mathcal{W}}(-\alpha, -\beta)\mathscr{D}(\alpha, \beta). \tag{4.74}$$

Here we prove that the set T of Eq. (4.62) is tomographically complete. Let $(\rho, \sigma) \in \mathcal{Z}_d \times \mathcal{Z}_d$ be an arbitrary point then we need to prove that there are parameters $(\alpha, \kappa, \lambda, \mu, \nu)$ associated with the bases of the set T such that $\rho = \alpha\nu, \sigma = \alpha\mu$, and hence $\widetilde{\mathcal{W}}(\rho, \sigma)$ can be calculated. We note that the probabilities do not depend on the parameters κ, λ however we give their values as they are needed for the symplectic transformations. We consider five cases. In the first case we consider the points (ρ, σ) with $\sigma = 0$. In the second case we consider the points (ρ, σ) with $\rho = 0$. In the third case we consider the points (ρ, σ) where $\sigma \neq 0$ and σ is multiple of p_1. In the

fourth case we consider the points (ρ, σ) where $\sigma \neq 0$ and σ is multiple of p_2. Finally, in case five we consider the points (ρ, σ) where σ is not a multiple of p_1 or p_2. In this sense there is no loss of generality if we consider ρ, σ to be coprime in the last three cases. Let $\mathbb{G}(\rho, \sigma)$ be the greatest common divisor of ρ and σ. Then $\rho' = \rho/\mathbb{G}(\rho, \sigma), \sigma' = \sigma/\mathbb{G}(\rho, \sigma)$ are coprime. if $\widetilde{\mathcal{W}}(\rho', \sigma')$ can be calculated using the parameters $\alpha, \kappa, \lambda, \mu, \nu$, then $\widetilde{\mathcal{W}}(\rho, \sigma)$ can be calculated using the parameters $(\mathbb{G}(\rho, \sigma)\alpha, \kappa, \lambda, \mu, \nu)$. In what follows we discuss each case.

(1) Let $\sigma = 0$. Then $\widetilde{\mathcal{W}}(\rho, 0)$ can be calculated using Eq. (4.72) with the projectors corresponding to the states in Eq. (4.63), i.e. using probabilities along the line $\mathscr{L}(1, 0)$ with the parameters

$$\alpha = \rho; \quad \kappa = 1; \quad \lambda = 0; \quad \mu = 0; \quad \nu = 1. \tag{4.75}$$

(2) Let $\rho = 0$. Then $\widetilde{\mathcal{W}}(0, \sigma)$ can be calculated using Eq. (4.72) with the projectors corresponding to the states in Eq. (4.66), i.e. using probabilities along the line $\mathscr{L}(0, -p_1 - p_2)$ with the parameters

$$\alpha = \sigma[-p_1 - p_2]^{-1}; \quad \kappa = 0; \quad \lambda = \Gamma; \quad \mu = -p_1 - p_2; \quad \nu = 0. \tag{4.76}$$

We note that the used states in this case is the Fourier transform of

the states used in case 1 as

$$\begin{aligned}\mathscr{F}|X^{(1)};\tilde{n}_1\rangle \otimes \mathscr{F}|X^{(2)};\tilde{n}_1\rangle &= [\mathcal{S}^{(1)}(0,1|-1,0)\otimes \mathcal{S}^{(2)}(0,1|-1,0)] \\ &\times [|X^{(1)};\tilde{n}_1\rangle \otimes |X^{(2)};\tilde{n}_2\rangle] \\ &= \mathcal{S}(0,\Gamma|-p_1-p_2,0)|X;n\rangle \end{aligned} \tag{4.77}$$

(3) Let $\sigma = Np_1$ where N is integer and N is not multiple of p_2 (as $\sigma \neq 0$). We choose $\alpha \in \mathcal{Z}_d$ such that

$$\alpha = -N + Mp_2; \qquad M = (\rho + N)p_2^{-1} \text{ (mod } p_1). \tag{4.78}$$

Eq. (4.78) guarantees that α is invertible in $\mathcal{Z}_d$ because it shows that $\alpha = \rho$ (mod p_1). Since ρ is not multiple of p_1 (as ρ, σ are coprime), then α is not multiple of p_1. Also α is not multiple of p_2 because N is not multiple of p_2, and hence α is invertible element in $\mathcal{Z}_d$. These values of α satisfy the equation $\sigma = \alpha\mu;\ \mu = -p_1$. Therefore, $\widetilde{\mathcal{W}}(\rho, Np_1); \rho \neq 0$ can be calculated using Eq. (4.72) with the projectors corresponding to the states in Eq. (4.64), i.e. using probabilities along the line $\mathscr{L}(\rho\alpha^{-1}, -p_1)$ such that

$$\alpha = -N + Mp_2; \quad \kappa = s_1; \quad \lambda = t_2 s_2; \quad \mu = -p_1; \quad \nu = \rho\alpha^{-1}. \tag{4.79}$$

We also prove that Eq. (4.79) is consistent with Eq. (4.64) because there exists $\lambda_2 \in \mathcal{Z}_{p_2}$ that satisfy the equation $\nu = s_1 - \lambda_2 s_2 = \rho\alpha^{-1};\ \nu \in \mathcal{Z}_d$. Since $s_1 = 1$ (mod p_1), $s_1 = 0$ (mod p_2), $s_2 =$

$0 \pmod{p_1}$, and $s_1 = 1 \pmod{p_2}$, then Eqs. (4.64,4.79) show that

$$\rho\alpha^{-1} = 1 \pmod{p_1}; \quad \rho\alpha^{-1} = -\lambda_2 \pmod{p_2}. \tag{4.80}$$

The first equation emphasizes that $\alpha = \rho \pmod{p_1}$ (we have shown this earlier) and the second equation shows the values that λ_2 can take to satisfy Eq. (4.79).

(4) Let $\sigma = Np_2$ where N is integer and N is not multiple of p_1 (as $\sigma \neq 0$). Here the proof is similar to case (3). We choose $\alpha \in \mathcal{Z}_d$ such that

$$\alpha = -N + Mp_1; \qquad M = (\rho + N)p_1^{-1} \pmod{p_2}. \tag{4.81}$$

α is invertible in $\mathcal{Z}_d$ (the proof is similar to case (3)). These values of α satisfy the equation $\sigma = \alpha\mu;\ \mu = -p_2$. Therefore, $\widetilde{\mathcal{W}}(\rho, Np_2); \rho \neq 0$ can be calculated using Eq. (4.72) with the projectors corresponding to the states in Eq. (4.65), i.e. using probabilities along the line $\mathscr{L}(\rho\alpha^{-1}, -p_2)$ such that

$$\alpha = -N + Mp_1; \quad \kappa = s_2; \quad \lambda = t_1 s_1; \quad \mu = -p_2; \quad \nu = \rho\alpha^{-1}. \tag{4.82}$$

In the same way we prove that Eq. (4.82) is consistent with Eq. (4.65) and $\lambda_1 = -\rho\alpha^{-1} \pmod{p_1}$.

(5) Let σ is not multiple of p_1 or p_2. Therefore, σ is invertible element in $\mathcal{Z}_d$. Also $-p_1 - p_2$ is invertible element in $\mathcal{Z}_d$, then there exists $\alpha = \sigma(-p_1 - p_2)^{-1}$ that satisfies the equation $\sigma = \alpha(-p_1 - p_2)$. Since

$-p_1-p_2$ is invertible element in $\mathcal{Z}_d$, then $\alpha^{-1} = \sigma^{-1}(-p_1-p_2)$, therefore $\nu = \alpha^{-1}\rho = \rho\sigma^{-1}(-p_1 - p_2)$, and hence $\widetilde{\mathcal{W}}(\rho,\sigma)$; σ is not multiple of p_1 or p_2 can be calculated using Eq. (4.72) with the projectors corresponding to the states in Eq. (4.66), i.e. using probabilities along the line $\mathscr{L}(\rho\sigma^{-1}(-p_1 - p_2), -p_1 - p_2)$ such that

$$\alpha = \sigma(-p_1-p_2)^{-1}; \quad \kappa = 0; \quad \lambda = \Gamma; \quad \mu = -p_1-p_2; \quad \nu = \rho\sigma^{-1}(-p_1-p_2). \tag{4.83}$$

Eq. (4.83) is consistent with Eq. (4.66) because there exists $\lambda_1 \in \mathcal{Z}_{p_1}$ and $\lambda_2 \in \mathcal{Z}_{p_2}$ that satisfy the equation $\nu = \rho\sigma^{-1}(-p_1 - p_2) = -\lambda_1 s_1 - \lambda_2 s_2$; $\nu \in \mathcal{Z}_d$. In this case $\lambda_1 = [\rho\sigma^{-1}(p_1 + p_2)](\text{mod } p_1)$ and $\lambda_2 = [\rho\sigma^{-1}(p_1 + p_2)](\text{mod } p_2)$.

4.7 Examples

Starting from the probabilities $p(\beta|\nu,\mu)$ obtained through quantum tomography experiments we reconstruct the density matrix of the quantum system using Eqs. (4.71,4.74). If the probabilities from quantum tomography experiment do not obey the two constraints of Eq. (4.68) and Eq. (4.72), then the experiment should be repeated. In these examples we do the measurements on the lines through the origin with the parameters ν, μ shown in table (4.1), we note that a large number of measurements should be done for each line. To make sure that the probabilities along these lines satisfy the two constraints of Eq. (4.68) and Eq. (4.72), we consider a density matrix then we calculate the probabilities corresponding to the lines $\mathscr{L}(\nu,\mu)$ where ν, μ

are shown in table (4.1). Using inverse Radon transform we calculate Weyl function then using Eq. (4.74) we construct the original density matrix.

Here we consider $d = 15$, therefore $p_1 = 3$ and $p_2 = 5$. In the first example we consider a pure state system with state $|\psi\rangle$ where

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{42}}[2|X;0\rangle + (1+i)|X;1\rangle + i|X;3\rangle + (2+3i)|X;6\rangle + |X;9\rangle \\ &+ (1-i)|X;11\rangle + 3|X;13\rangle + (3-i)|X;14\rangle]. \end{aligned} \tag{4.84}$$

In the second example we consider a mixed state system with density matrix $\mathcal{D}$ where

$$\begin{aligned} \mathcal{D} &= \frac{3}{5}|\psi_1\rangle\langle\psi_1| + \frac{2}{5}|\psi_2\rangle\langle\psi_2| \\ |\psi_1\rangle &= \frac{1}{\sqrt{80}}[(2+i)|X;0\rangle + (1+i)|X;1\rangle + 2|X;4\rangle + (5-i)|X;6\rangle + (3+4i)|X;9\rangle \\ &+ (1+2i)|X;11\rangle + (2-3i)|X;14\rangle] \\ |\psi_2\rangle &= \frac{1}{\sqrt{63}}[i|X;0\rangle + (2-i)|X;1\rangle + (1-2i)|X;3\rangle + 4|X;5\rangle + (2+4i)|X;6\rangle \\ &+ (3+i)|X;12\rangle + (2i)|X;13\rangle + (1-i)|X;14\rangle] \end{aligned} \tag{4.85}$$

For each example we get the probabilities $p(\beta|\nu,\mu)$ corresponding to the lines $\mathscr{L}(\nu,\mu)$ using Eq. (4.67). Then we calculate Weyl function, Wigner function, and the density matrix using Eqs. (4.71,4.73,4.74), respectively. Since $d = 15$ then we calculate the probabilities along $\psi(15) = 24$ lines so we have a total of $24 \times 15 = 360$ probabilities in each example. tables (4.4, 4.5) show a sample of these probabilities for the pure state system and the mixed state system, correspondingly. These probabilities obey the constraint of Eq. (4.68) as the summation of the probabilities along one line

is equal to one. They also obey the constraint of Eq. (4.72) where the probabilities corresponding to lines which have common points lead to the same Weyl function at each of these common points. As an example, the lines $\mathscr{L}(1,12), \mathscr{L}(1,7), \mathscr{L}(6,7), \mathscr{L}(11,7)$ have the points $(0,0), (3,6), (6,12), (9,3), (12,9)$ in common, table (4.6,4.7) show that the probabilities corresponding to these lines lead to the same values of Weyl function at these common points. The results of Weyl function and Wigner function for the pure state system are shown in figures (4.1,4.2), and the results of Weyl function and Wigner function for the mixed state system are shown in figures (4.3,4.4). We calculate the redundancy parameter of Eq. (4.70) in the case that $d = 15$, $\mathscr{R} = \frac{\psi(15)}{16} - 1 = 0.5$.

Table 4.4: A sample of the probabilities $p(\beta|\nu,\mu)$ for the pure state of Eq.(4.84)

ν	μ	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	12	0.023	0.012	0.051	0.073	0.034	0.095	0.037	0.081	0.087	0.055	0.088	0.038	0.264	0.046	0.015
1	7	0.026	0	0.173	0.02	0.071	0.18	0.081	0.219	0.123	0.008	0	0.006	0.005	0.063	0.025
6	7	0.089	0.034	0.068	0.017	0.001	0.092	0.017	0.035	0.007	0.028	0.025	0.035	0.293	0.183	0.075
11	7	0.091	0.042	0.066	0.046	0.066	0.093	0.031	0.107	0.112	0.025	0.023	0.015	0.223	0.049	0.013

Table 4.5: A sample of the probabilities $p(\beta|\nu,\mu)$ for the mixed state of Eq.(4.85)

ν	μ	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	12	0.16	0.022	0.076	0.261	0.027	0.036	0.109	0.023	0.02	0.071	0.015	0.06	0.047	0.015	0.058
1	7	0.065	0.087	0.061	0.055	0.017	0.106	0.055	0.051	0.135	0.07	0.04	0.048	0.035	0.105	0.069
6	7	0.091	0.063	0.006	0.109	0.03	0.055	0.025	0.026	0.082	0.046	0.065	0.103	0.114	0.104	0.08
11	7	0.081	0.052	0.051	0.142	0.05	0.055	0.059	0.027	0.062	0.087	0.075	0.08	0.069	0.091	0.019

Table 4.6: A sample of $\widetilde{W}(\rho,\sigma)$ for the pure state of Eq.(4.84). Results for the common points $(0,0)$, $(3,6)$, $(6,12)$, $(9,3)$, $(12,9)$ between the lines $\mathscr{L}(1,12)$, $\mathscr{L}(1,7)$, $\mathscr{L}(6,7)$, $\mathscr{L}(11,7)$ are presented. It is clear that the constraint of Eq.(4.72) is satisfied.

ν	μ	$\widetilde{W}(0,0)$	$\widetilde{W}(3,6)$	$\widetilde{W}(6,12)$	$\widetilde{W}(9,3)$	$\widetilde{W}(12,9)$
1	12	1	$-0.222+0.095i$	$0.238-0.191i$	$0.238+0.191i$	$-0.222-0.095i$
1	7	1	$-0.222+0.095i$	$0.238-0.191i$	$0.238+0.191i$	$-0.222-0.095i$
6	7	1	$-0.222+0.095i$	$0.238-0.191i$	$0.238+0.191i$	$-0.222-0.095i$
11	7	1	$-0.222+0.095i$	$0.238-0.191i$	$0.238+0.191i$	$-0.222-0.095i$

Table 4.7: A sample of $\widetilde{W}(\rho,\sigma)$ for the mixed state of Eq.(4.85). Results for the common points $(0,0)$, $(3,6)$, $(6,12)$, $(9,3)$, $(12,9)$ between the lines $\mathscr{L}(1,12)$, $\mathscr{L}(1,7)$, $\mathscr{L}(6,7)$, $\mathscr{L}(11,7)$ are presented. It is clear that the constraint of Eq.(4.72) is satisfied.

ν	μ	$\widetilde{W}(0,0)$	$\widetilde{W}(3,6)$	$\widetilde{W}(6,12)$	$\widetilde{W}(9,3)$	$\widetilde{W}(12,9)$
1	12	1	$-0.039-0.054i$	$0.066+0.162i$	$0.066-0.162i$	$-0.039+0.054i$
1	7	1	$-0.039-0.054i$	$0.066+0.162i$	$0.066-0.162i$	$-0.039+0.054i$
6	7	1	$-0.039-0.054i$	$0.066+0.162i$	$0.066-0.162i$	$-0.039+0.054i$
11	7	1	$-0.039-0.054i$	$0.066+0.162i$	$0.066-0.162i$	$-0.039+0.054i$

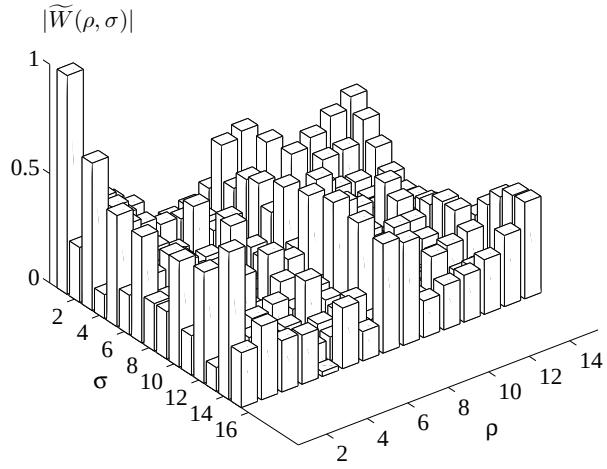

Figure 4.1: Weyl function for the pure state system.

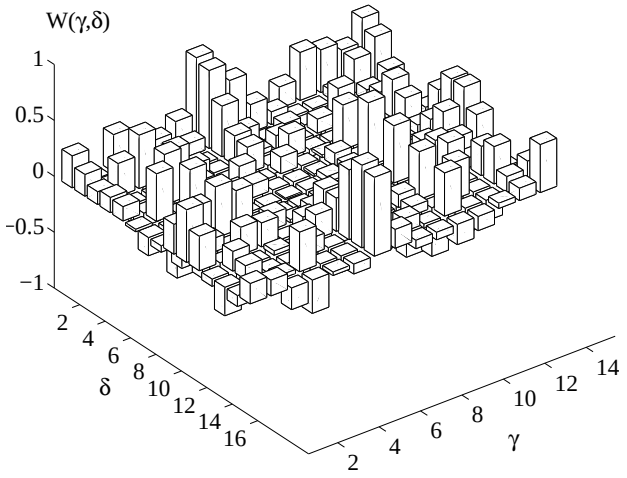

Figure 4.2: Wigner function for the pure state system.

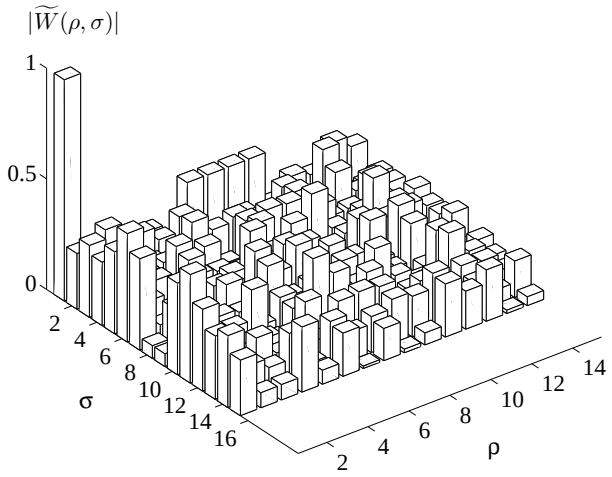

Figure 4.3: Weyl function for the mixed state system.

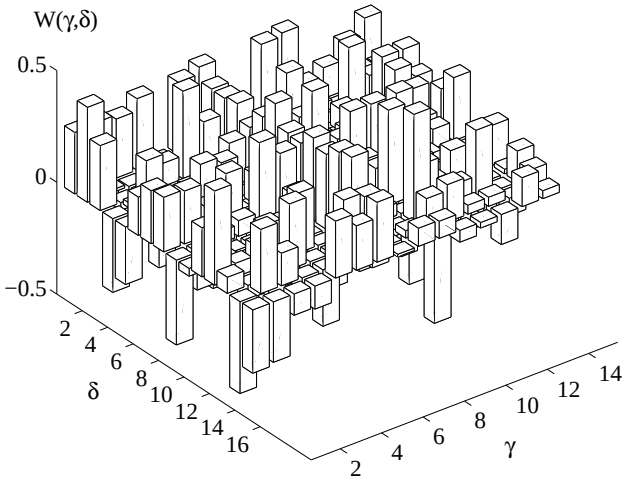

Figure 4.4: Wigner function for the mixed state system.

4.8 Duality between weak mutually unbiased bases in $\mathcal{H}_d$ and the maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$

In chapter (3) we have discussed the properties of lines. We have concluded that we can construct the set of all maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ according to Eqs. (4.86).

$$\begin{aligned}
&\mathscr{L}_1 = \mathscr{L}^{(1)}(0,1) \times \mathscr{L}^{(2)}(0,1) \\
&\mathscr{L}_{2+\lambda_2} = \mathscr{L}^{(1)}(0,1) \times [\mathrm{g}^{(2)}(0,1|-1,-\lambda_2)\mathscr{L}^{(2)}(0,1)] \\
&\mathscr{L}_{2+p_2+\lambda_1} = [\mathrm{g}^{(1)}(0,1|-1,-\lambda_1)\mathscr{L}^{(1)}(0,1)] \times \mathscr{L}^{(2)}(0,1) \\
&\mathscr{L}_{2+p_1+p_2+\lambda_2+\lambda_1 p_2} = [\mathrm{g}^{(1)}(0,1|-1,-\lambda_1)\mathscr{L}^{(1)}(0,1)] \times [\mathrm{g}^{(2)}(0,1|-1,-\lambda_2)\mathscr{L}^{(2)}(0,1)],
\end{aligned} \tag{4.86}$$

where $\lambda_1 \in \mathcal{Z}_{p_1}, \lambda_2 \in \mathcal{Z}_{p_2}$. We have shown that this construction can be derived in terms of symplectic transformations as

$$\begin{aligned}
&\mathscr{L}_{2+\lambda_2} = \mathrm{g}(s_1, t_2 s_2|-p_1, s_1 - \lambda_2 s_2)\mathscr{L}_1 \\
&\mathscr{L}_{2+p_2+\lambda_1} = \mathrm{g}(s_2, t_1 s_1|-p_2, s_2 - \lambda_1 s_1)\mathscr{L}_1 \\
&\mathscr{L}_{2+p_1+p_2+\lambda_2+\lambda_1 p_2} = \mathrm{g}(0,\Gamma|-p_1-p_2, -\lambda_1 s_1 - \lambda_2 s_2)\mathscr{L}_1; \;\; \Gamma = t_1^2 p_2 + t_2^2 p_1.
\end{aligned} \tag{4.87}$$

Here we introduce the duality (correspondence) between the maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ and the weak mutually unbiased bases which are presented in this chapter. In what follows we discuss the 'dictionary' for this correspondence.

(1) The line $\mathscr{L}_j$ of Eq. (4.86) corresponds to the basis $\mathcal{B}_j$ of Eq. (4.52). We stress that the symplectic parameters used in Eq. (4.87) for the line $\mathscr{L}_j$ are the same as the symplectic parameters used in Eq. (4.62) for the basis $\mathcal{B}_j$.

(2) The number of maximal lines corresponds to the maximum number of weak mutually unbiased bases ($\psi(d)$ each).

(3) A pair of maximal lines that intersect only at the origin corresponds to a pair of weak mutually unbiased bases whose overlap absolute value equals to $d^{-1/2}$ (Eq.(4.20)). The two bases in this case are mutually unbiased. There are $d\psi(d)/2$ such pairs of maximal lines and $d\psi(d)/2$ corresponding pairs of weak mutually unbiased bases.

(4) A pair of maximal lines that have p_1 points in common corresponds to a pair of weak mutually unbiased bases whose overlap absolute value equals to ${p_2}^{-1/2}$ (Eq.(4.19)). There are $p_2\psi(d)/2$ such pairs of maximal lines and $p_2\psi(d)/2$ corresponding pairs of weak mutually unbiased bases.

(5) A pair of maximal lines that have p_2 points in common corresponds to a pair of weak mutually unbiased bases whose overlap absolute value equals to ${p_1}^{-1/2}$ (Eq.(4.18)). There are $p_1\psi(d)/2$ such pairs of maximal lines and $p_1\psi(d)/2$ corresponding pairs of weak mutually unbiased bases.

(6) In chapter (3), Eq. (3.20) has presented the redundancy parameter to measure the deviation of the geometry $\mathcal{Z}_d \times \mathcal{Z}_d$ from the near-linear

geometry. This parameter corresponds to the redundancy parameter presented in this chapter (Eq. (4.70)) which measures the 'tomographical overcompleteness' of the weak mutually unbiased bases. The fact that these two parameters are equal shows that the concept of weak mutually unbiased bases is customized with the geometry $\mathcal{Z}_d \times \mathcal{Z}_d$. In the case that d is prime number, the redundancy parameters become 0, the geometry $\mathcal{Z}_d \times \mathcal{Z}_d$ is near-linear, and weak mutually unbiased bases are mutually unbiased bases.

4.8.1 Duality example

In this subsection we clarify the duality between the maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ and the weak mutually unbiased bases with actual examples. We construct the maximal lines in $\mathcal{Z}_{15} \times \mathcal{Z}_{15}$ and $\mathcal{Z}_{21} \times \mathcal{Z}_{21}$ according to Eq. (4.86). Table (3.1) shows all maximal lines $\mathscr{L}(\rho, \sigma)$ in $\mathcal{Z}_{15} \times \mathcal{Z}_{15}$ and their component lines $\mathscr{L}^{(1)}(\rho_1, \tilde{\sigma}_1)$ and $\mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2)$ in $\mathcal{Z}_3 \times \mathcal{Z}_3$ and $\mathcal{Z}_5 \times \mathcal{Z}_5$, respectively, and table (3.2) shows all maximal lines $\mathscr{L}(\rho, \sigma)$ in $\mathcal{Z}_{21} \times \mathcal{Z}_{21}$ and their component lines $\mathscr{L}^{(1)}(\rho_1, \tilde{\sigma}_1)$ and $\mathscr{L}^{(2)}(\rho_2, \tilde{\sigma}_2)$ in $\mathcal{Z}_3 \times \mathcal{Z}_3$ and $\mathcal{Z}_7 \times \mathcal{Z}_7$, respectively. We also construct the weak mutually unbiased bases according to Eq. (4.52). Table (4.2) shows the weak mutually unbiased bases $|\mathcal{B}_j; \tilde{m}\rangle$ in $\mathcal{H}_{15}$ and their corresponding component bases $|\mathcal{B}_j^{(1)}; \tilde{m}_1\rangle$ and $|\mathcal{B}_j^{(2)}; \tilde{m}_2\rangle$ in $\mathcal{H}_3$ and $\mathcal{H}_5$, respectively, and table (4.3) shows the weak mutually unbiased bases $|\mathcal{B}_j; \tilde{m}\rangle$ in $\mathcal{H}_{21}$ and their corresponding component bases $|\mathcal{B}_j^{(1)}; \tilde{m}_1\rangle$ and $|\mathcal{B}_j^{(2)}; \tilde{m}_2\rangle$ in $\mathcal{H}_3$ and $\mathcal{H}_7$, respectively. Comparing any line with its corresponding basis shows that the parameters used in the symplectic transformations for

this line and its corresponding basis are the same. For example, by comparing the line $\mathscr{L}_5 = \mathscr{L}(6,11) = \mathrm{g}(10,12|12,7)\mathscr{L}_1$ in $\mathcal{Z}_{15} \times \mathcal{Z}_{15}$ with the basis $|\mathcal{B}_5; m\rangle = |X(10,12|12,7); m\rangle$ in $\mathcal{H}_{15}$, we easily see that the parameters used in the symplectic transformations for $\mathscr{L}_5$ and $|\mathcal{B}_5; m\rangle$ are the same. Also, the line $\mathscr{L}_3 = \mathscr{L}(15,4) = \mathrm{g}(7,12|18,13)\mathscr{L}_1$ in $\mathcal{Z}_{21} \times \mathcal{Z}_{21}$ and the basis $|\mathcal{B}_3; m\rangle = |X(7,12|18,13); m\rangle$ in $\mathcal{H}_{21}$ have the same symplectic parameters.

We showed earlier that the weak mutually unbiased bases of Eq. (4.52) can be partitioned into $p_2 + 1$ subsets T_j of $p_1 + 1$ mutually unbiased bases according to Eq. (4.60). Tables (4.8,4.9) show the two partitions and the subsets of mutually unbiased bases in each partition, in $\mathcal{H}_{15}$ and $\mathcal{H}_{21}$, respectively. Similarly, tables (3.3,3.4) show the corresponding subsets S_j of maximal lines, in $\mathcal{Z}_{15} \times \mathcal{Z}_{15}$ and $\mathcal{Z}_{21} \times \mathcal{Z}_{21}$, respectively. The lines in one subset S_j have only the origin in common, but lines in different subsets may have more than one point in common.

Table 4.8: The subsets of the set of the weak mutually unbiased bases according to the partition of Eq. (4.60) in the case that $d = 15$. These subsets correspond to the subsets S_j of the maximal lines in table (3.3). The bases in the same column (i.e. in the same subset T_j) are mutually unbiased.

T_0	T_1	T_2	T_3	T_4	T_5
$\|\mathcal{B}_1; m\rangle$	$\|\mathcal{B}_2; m\rangle$	$\|\mathcal{B}_3; m\rangle$	$\|\mathcal{B}_4; m\rangle$	$\|\mathcal{B}_5; m\rangle$	$\|\mathcal{B}_6; m\rangle$
$\|\mathcal{B}_{10}; m\rangle$	$\|\mathcal{B}_{11}; m\rangle$	$\|\mathcal{B}_{12}; m\rangle$	$\|\mathcal{B}_9; m\rangle$	$\|\mathcal{B}_8; m\rangle$	$\|\mathcal{B}_7; m\rangle$
$\|\mathcal{B}_{16}; m\rangle$	$\|\mathcal{B}_{17}; m\rangle$	$\|\mathcal{B}_{18}; m\rangle$	$\|\mathcal{B}_{13}; m\rangle$	$\|\mathcal{B}_{14}; m\rangle$	$\|\mathcal{B}_{15}; m\rangle$
$\|\mathcal{B}_{22}; m\rangle$	$\|\mathcal{B}_{23}; m\rangle$	$\|\mathcal{B}_{24}; m\rangle$	$\|\mathcal{B}_{19}; m\rangle$	$\|\mathcal{B}_{20}; m\rangle$	$\|\mathcal{B}_{21}; m\rangle$

Table 4.9: The subsets of the set of the weak mutually unbiased bases according to the partition of Eq. (4.60) in the case that $d = 21$. These subsets correspond to the subsets S_j of the maximal lines in table (3.4). The bases in the same column (i.e., in the same subset T_j) are mutually unbiased.

T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7
$\|\mathcal{B}_1;m\rangle$	$\|\mathcal{B}_2;m\rangle$	$\|\mathcal{B}_3;m\rangle$	$\|\mathcal{B}_4;m\rangle$	$\|\mathcal{B}_5;m\rangle$	$\|\mathcal{B}_6;m\rangle$	$\|\mathcal{B}_7;m\rangle$	$\|\mathcal{B}_8;m\rangle$
$\|\mathcal{B}_{12};m\rangle$	$\|\mathcal{B}_{13};m\rangle$	$\|\mathcal{B}_{14};m\rangle$	$\|\mathcal{B}_{15};m\rangle$	$\|\mathcal{B}_{16};m\rangle$	$\|\mathcal{B}_{11};m\rangle$	$\|\mathcal{B}_{10};m\rangle$	$\|\mathcal{B}_9;m\rangle$
$\|\mathcal{B}_{20};m\rangle$	$\|\mathcal{B}_{21};m\rangle$	$\|\mathcal{B}_{22};m\rangle$	$\|\mathcal{B}_{23};m\rangle$	$\|\mathcal{B}_{24};m\rangle$	$\|\mathcal{B}_{17};m\rangle$	$\|\mathcal{B}_{18};m\rangle$	$\|\mathcal{B}_{19};m\rangle$
$\|\mathcal{B}_{28};m\rangle$	$\|\mathcal{B}_{29};m\rangle$	$\|\mathcal{B}_{30};m\rangle$	$\|\mathcal{B}_{31};m\rangle$	$\|\mathcal{B}_{32};m\rangle$	$\|\mathcal{B}_{25};m\rangle$	$\|\mathcal{B}_{26};m\rangle$	$\|\mathcal{B}_{27};m\rangle$

4.9 Weak mutually unbiased bases as complex projective 1-design

In [79], it has been shown that the complete set of mutually unbiased bases are complex projective 2-design with the angle set $\{0, 1/d\}$. Below, we give a brief introduction about this study, then we give analogous study for the complete set of weak mutually unbiased bases (in the case that $d = p_1 p_2;\ p_1, p_2$ are prime numbers), and we show that the bases of this set are complex projective 1-design with the angle set $\{0, 1/p_1, 1/p_2, 1/d\}$.

Let $\mathcal{B}_j$ denote the orthonormal basis $\{|\mathcal{B}_j; n\rangle | n \in \mathcal{Z}_d\}$. Any set $S = \mathcal{B}_0 \cup ... \cup \mathcal{B}_{\ell-1}$ obeys Welch bound inequality of Eq. (4.88) [80]

$$\frac{1}{|S|^2} \sum_{\mathcal{B}_j, \mathcal{B}_k \subset S} [v_{jk}(n,m)]^{2Q} \geq \frac{1}{\begin{pmatrix} d+Q-1 \\ Q \end{pmatrix}}, \tag{4.88}$$

where $Q \geq 0, v_{jk}(n,m)$ is defined in Eq. (4.17) and $|S|$ is the cardinality of the set S. If the set S achieves Welch bounds at $Q = 1$, we call it WBE-

sequence set [81]. If S achieves Welch bound for all $Q \leq t$, therefore the set of bases in S are complex projective t-design [79].

The 'angle' set $\mathcal{A}$ of S is defined as

$$\mathcal{A} = \{[v_{jk}(n,m)]^2 | \mathcal{B}_j, \mathcal{B}_k \subset S;\ (j,n) \neq (k,m)\} \tag{4.89}$$

For any vector $|\mathcal{B}_j; n\rangle \in S$ and any angle $a \in \mathcal{A}$ the subdegree $\zeta(a|j,n)$ is the cardinality of the set $\{|\mathcal{B}_k; m\rangle|\ \mathcal{B}_k \subset S;\ [v_{jk}(n,m)]^2 = a\ \}$. If $\zeta(a|j,n)$ does not depend on $|\mathcal{B}_j; n\rangle$, S is called regular scheme.

In the view of the above discussion we consider a power of prime dimensional system $d = p^n$. Let S be the complete set of mutually unbiased bases in $\mathcal{H}_d$, therefore $|S| = d(d+1)$. We calculate the left hand side ($L.H.S$) and the right hand side ($R.H.S$) of Eq. (4.88) for $Q = 0, 1, 2$. In the case that $Q = 0$,

$$L.H.S = \frac{1}{d^2(d+1)^2}([(d)(d+1)][(d)(d+1)]) = 1. \tag{4.90}$$

$$R.H.S = \frac{(d-1)!0!}{(d-1)!} = 1 = L.H.S\ \ . \tag{4.91}$$

In the case that $Q = 1$,

$$L.H.S = \frac{1}{d^2(d+1)^2}([(d)(d+1)(d)(d)(1/d)] + [(d)(d+1)]) = \frac{1}{d}. \tag{4.92}$$

$$R.H.S = \frac{(d-1)!1!}{(d)!} = \frac{1}{d} = L.H.S\ \ . \tag{4.93}$$

In the case that $Q = 2$,

$$L.H.S = \frac{1}{d^2(d+1)^2}([(d)(d+1)(d)(d)(1/d^2)] + [(d)(d+1)]) = \frac{2}{d(d+1)}. \tag{4.94}$$

$$R.H.S = \frac{(d-1)!2!}{(d+1)!} = \frac{2}{d(d+1)} = L.H.S \ . \tag{4.95}$$

Eqs. (4.90,4.91,4.92,4.93,4.94,4.95) show that mutually unbiased bases are complex projective 2-design and form WBE-sequence set.

Regardless the value of (j, n), the absolute value of the overlap $v_{jk}(n, m)$ where $(j, n) \neq (k, m)$ takes only the values 0 with multiplicity $d-1$ and $d^{-1/2}$ with multiplicity d^2. Therefore, the set of mutually unbiased bases is a regular scheme with angle set $\{0, \frac{1}{d}\}$ where $\zeta(0|j, n) = d - 1$, and $\zeta(\frac{1}{d}|j, n) = d^2$.

Analogously, we consider a system with dimension $d = p_1 p_2$; p_1, p_2 are prime numbers. Let S be the complete set of weak mutually unbiased bases in $\mathcal{H}_d$. The cardinality of this set is $d\psi(d)$. We calculate the left hand side $(L.H.S)$ and the right hand side $(R.H.S)$ of Eq. (4.88) for $Q = 0, 1, 2$. In the case that $Q = 0$,

$$L.H.S = \frac{1}{d^2\psi^2(d)}([d\psi(d)][d\psi(d)]) = 1. \tag{4.96}$$

$$R.H.S = \frac{(d-1)!0!}{(d-1)!} = 1 = L.H.S \ . \tag{4.97}$$

In the case that $Q = 1$,

$$\begin{aligned} L.H.S &= \frac{1}{d^2\psi^2(d)}([\frac{1}{p_1}(p_1 d)(p_1\psi(d))] + [\frac{1}{p_2}(p_2 d)(p_2\psi(d))] + [\frac{1}{d}(d^2)(d\psi(d))] + [(d)\psi(d)]) \\ &= \frac{1}{d}. \end{aligned} \tag{4.98}$$

$$R.H.S = \frac{(d-1)!1!}{(d)!} = \frac{1}{d} = L.H.S \quad . \tag{4.99}$$

In the case that $Q = 2$,

$$\begin{aligned} L.H.S &= \frac{1}{d^2\psi^2(d)}([\frac{1}{p_1^2}(p_1 d)(p_1\psi(d))] + [\frac{1}{p_2^2}(p_2 d)(p_2\psi(d))] + [\frac{1}{d^2}(d^2)(d\psi(d))] + [(d)\psi(d)]) \\ &= \frac{4}{d\psi(d)}. \end{aligned} \tag{4.100}$$

$$R.H.S = \frac{(d-1)!2!}{(d+1)!} = \frac{2}{d(d+1)} \neq L.H.S \quad . \tag{4.101}$$

Eqs. (4.96,4.97,4.98,4.99,4.100,4.101) show that the equality holds only for $Q = 0, 1$, and hence weak mutually unbiased bases are complex projective 1-design and form WBE-sequence set.

Using the definition of weak mutually unbiased bases we find that the absolute value of the overlap $v_{jk}(n, m)$ for all $k \in \mathcal{Z}_d$ and $(j, n) \neq (k, m)$ takes only the values $0, p_1^{-1/2}, p_2^{-1/2}, d^{-1/2}$. Regardless the value of (j, n), $v_{jk}(n, m)$ take the value 0 with multiplicity $d - 1 + p_1(d - p_1) + p_2(d - p_2)$, $p_1^{-1/2}$ with multiplicity p_1^2, $p_2^{-1/2}$ with multiplicity p_2^2, and $d^{-1/2}$ with multiplicity d^2. Therefore, the set of weak mutually unbiased bases is a regular scheme with angle set $\{0, \frac{1}{p_1}, \frac{1}{p_2}, \frac{1}{d}\}$ where $\zeta(0|j, n) = d - 1 + p_1(d - p_1) + p_2(d - p_2)$, $\zeta(\frac{1}{p_1}|j, n) = p_1^2$, $\zeta(\frac{1}{p_2}|j, n) = p_2^2$, and $\zeta(\frac{1}{d}|j, n) = d^2$.

4.10 Summary

In this chapter we have introduced the concept of weak mutually unbiased bases. As an example, we have presented an explicit construction of weak mutually unbiased bases. We have proved that this construction is tomo-

graphically complete. We have illustrated this fact by doing quantum tomography for two systems one of them is pure state system and the other is mixed state system. We have shown that weak mutually unbiased bases are intimately related to the finite geometry $\mathcal{Z}_d \times \mathcal{Z}_d$. Finally we have presented weak mutually unbiased bases in the view of complex projective t-designs.

Chapter 5

Quantum cryptography

In the previous chapter we have introduced the concept of weak mutually unbiased bases. We have used the complete set of weak mutually unbiased bases for quantum tomography. Here we use this set to derive a new quantum cryptography protocol by modifying the (one-way) 'prepare and measure' protocol BB84 [2]. The set of weak mutually unbiased bases is used to prepare and measure qudits of d-dimensional systems where $d = p_1 p_2$; p_1, p_2 are prime numbers. We also generalize the two-way quantum cryptography protocol [82] to work with qudits of odd dimensional systems rather than qubits. We analyze the security of both protocols against the intercept and resend attack.

5.1 Introduction

The security of the current cryptography systems is based on the great difficulty of factorizing a large integer number into its prime factors. Peter

Shor [83] presented a quantum computer based algorithm (known as Shor's algorithm) that factorizes a large integer exponentially faster than other algorithms. As a result, classical cryptography systems became threatened and as soon as quantum computers are feasible, classical cryptography systems could collapse. On the contrary, the security of quantum cryptography protocols is based on the uncertainty principle of quantum mechanics, and hence quantum cryptography contributes to the field of cryptography with an important advantage as it offers a mechanism for eavesdropper detection. Quantum cryptography is classified into two main categories, 'Prepare and measure' based quantum cryptography and entanglement based quantum cryptography. Although there is a lot of work regarding the entanglement based protocols [84, 85, 86, 87, 88], this chapter is dedicated to the 'Prepare and measure' based protocols, in particular [2, 82]. Based on the idea of conjugate coding [89], the pioneering work of quantum cryptography and the 'Prepare and measure' based protocols was the BB84 protocol. It was proposed by Bennett and Brassard where the two legitimate users (by convention we call them Alice and Bob) use four non-orthogonal quantum states to prepare and measure qubits (two dimensional systems). This protocol was modified to use six non-orthogonal quantum states rather than four [90]. Also BB84 protocol was extended in the sense that it uses larger alphabets [91] or it deals with systems of dimensions higher than two [92, 93, 94]. In 1992, Bennett noticed that the eavesdropper (by convention we call her Eve) can be detected using only two non-orthogonal states, and hence BB84 protocol was modified to work with two non-orthogonal states rather than four [95]. We note that BB84 based protocols were surveyed in [3]. BB84 protocols can be

called one-way nondeterministic protocols because the states are transmitted in one direction from Alice to Bob, and some of the states are discarded when Alice and Bob use different bases to prepare and measure the states, respectively. Based on the 'Ping-Pong' (PP) protocol [52], another 'Prepare and measure' based protocols were proposed where the states travel in the two ways between Alice and Bob, and none of the states are discarded. such protocols are called two-way deterministic protocols. The first two-way deterministic protocol without entanglement was presented by Lucamarini and Mancini [82] where the qubits are prepared in one of four non-orthogonal quantum states and encoded using the operators $\mathcal{I}, \mathscr{Z}\mathscr{X}$. After that [96, 97] modified it such that the qubits are prepared in one of six non-orthogonal quantum states. Recently [98, 99] extended this protocol to work with qudits rather than qubits. In section (5.2) we discuss in details the BB84 protocol, then we modify this protocol to work with qudits using the weak mutually unbiased bases presented in chapter (4). In section (5.3) we describe the two-way deterministic protocol [82] that work with qubits then we generalize it to work with qudits. Although there are different forms of attacks that Eve can use [100, 101, 102], we analyze our proposed protocols only against the intercept and resend attack which gives a guide to the security of these protocols against other forms of attack.

5.2 One-way nondeterministic cryptography protocols

One-way nondeterministic cryptography protocols are dealing with states that travel in one way from Alice to Bob. They are called nondeterministic because Alice and Bob do not take into account the states where they use different bases. Here we discuss the BB84 protocol, and then we present our proposed protocol that works with d-level quantum systems.

5.2.1 BB84 protocol

BB84 protocol allows the two legitimate users Alice and Bob to share a secret key, and detect any attempt of eavesdropping with high probability. The protocol considers that there are two channels between Alice and Bob. The first is quantum channel and the second is public (classical) channel. Eavesdropper (Eve) has full access to the quantum channel, and can listen (without interfering) to the public channel. To make the key information totally random to Eve, Alice uses two mutually unbiased bases to prepare qubits. Alice may use the position states $|X;m\rangle$ and the momentum states $|P;m\rangle$ to prepare qubits. Let $|X;0\rangle, |P;0\rangle$ be encoded as (stand for) 0, and $|X;1\rangle, |P;1\rangle$ be encoded as 1. The following steps show how Alice and Bob share a secret key.

(1) Alice creates randomly a string of bits.

(2) Alice randomly chooses the encoding bases, prepares the states according to these bases, and then transmits the states through the quantum

channel one at a time to Bob.

(3) Bob randomly chooses a basis to measure each state in.

(4) Alice and Bob announce publicly the bases they used to prepare and measure the states in.

(5) In the case that Alice and Bob use different bases, Bob gets totally random results; so they ignore the states corresponding to these bases and take into account only the states corresponding to the matched bases. The bits corresponding to these states form the shared (sifted) key.

Table (5.1) summarizes the above steps.

Table 5.1: Summary of the BB84 quantum cryptography protocol. In this table, X denotes the basis $\{|X;0\rangle, |X;1\rangle\}$ and P denotes the basis $\{|P;0\rangle, |P;1\rangle\}$

A string of randomly bits	1	0	0	0	1	1	0	1
Alice's states (qubits)	$\|P;1\rangle$	$\|X;0\rangle$	$\|P;0\rangle$	$\|P;0\rangle$	$\|X;1\rangle$	$\|X;1\rangle$	$\|P;0\rangle$	$\|X;1\rangle$
Bob's random bases	X	X	P	X	X	P	P	P
Bob's results	1	0	0	1	1	0	0	1
Shared key		0	0		1		0	

Now let us assume that Eve intercepts the states transmitted by Alice, measures them, and resends these states to Bob according to her measurements. Eve uses the same basis as Alice with probability $\frac{1}{2}$, and in this case Bob will get the right value of the qubit, i.e. Eve will not be detected at all. In the case that Eve uses a basis different from the basis that Alice uses, Bob still has the chance to get the right value of the qubit with probability $\frac{1}{2}$, and

hence Eve has the chance to be undetected with probability $\frac{1}{2}$. Therefore, the probability of detecting Eve P_d is calculated as

$$P_d = \frac{1}{2}(1-1) + \frac{1}{2}(1-\frac{1}{2}) = \frac{1}{4} \tag{5.1}$$

Table (5.2) shows the case that there is an Eavesdropping on the quantum channel. It also shows that after the public discussion between Alice and

Table 5.2: Summary of the BB84 quantum cryptography protocol in the case that there is an Eavesdropping on the quantum channel. In this table, X denotes the basis $\{|X;0\rangle, |X;1\rangle\}$ and P denotes the basis $\{|P;0\rangle, |P;1\rangle\}$

A string of randomly bits	1	0	0	0	1	1	0	1
Alice's states (qubits)	$\|P;1\rangle$	$\|X;0\rangle$	$\|P;0\rangle$	$\|P;0\rangle$	$\|X;1\rangle$	$\|X;1\rangle$	$\|P;0\rangle$	$\|X;1\rangle$
Eve's random bases	P	P	P	X	X	P	X	X
Eve's retransmitted states	$\|P;1\rangle$	$\|P;1\rangle$	$\|P;0\rangle$	$\|X;1\rangle$	$\|X;1\rangle$	$\|P;1\rangle$	$\|X;0\rangle$	$\|X;1\rangle$
Bob's random bases	X	X	P	X	X	P	P	P
Bob's results	1	0	0	1	1	1	1	1
Shared key		0	0		1		$\underline{1}$	

Bob, they detect that the underlined bit should be 0; however its value is 1, and hence they detect the Presence of Eve. We note that only a small part of the sifted key is revealed during the public discussion.

The information that Eve can leak for one qubit is measured by Shannon information (I_E) [91]. The general form of Shannon information is

$$I_E = 1 + H(P_0, ..., P_{d-1}), \tag{5.2}$$

where d is the system dimension and $H(P_0, ..., P_{d-1})$ denotes the entropy which is defined as

$$H(P_0, ..., P_{d-1}) = \sum_{j=0}^{d-1} P_j log_d P_j, \tag{5.3}$$

P_j is the probability of the outcome j. Therefore, in the case of BB84 protocol (where qubits are used), the information that Eve can leak is

$$I_E = 1 + H(P_0, P_1) = \frac{1}{2}[1 + (1)log_2(1) + (0)log_2(0)] + \frac{1}{2}[1 + 2 \times \frac{1}{2} log_2(\frac{1}{2})] = \frac{1}{2}. \tag{5.4}$$

5.2.2 One-way nondeterministic protocol with qudits

BB84 protocol was generalized to work with qudits rather than qubits in [92, 93, 94]. The more mutually unbiased bases are used, the better security the legitimate users can get. However, the existence of a complete set of mutually unbiased bases for systems with composite dimensions has not been proved yet. Up to now, only $p_1 + 1$ mutually unbiased bases can be constructed for systems with dimensions $d = p_1 p_2$, where $p_1 < p_2$ [49]. This leads to the following.

$$P_d = \frac{1}{p_1 + 1}(1 - 1) + \frac{p_1}{p_1 + 1}(1 - \frac{1}{d}) = \frac{d - 1}{p_2(p_1 + 1)} \tag{5.5}$$

$$
\begin{aligned}
I_E &= 1 + H(P_0, ..., P_{d-1}) \\
&= \frac{1}{p_1+1}[1 + (1)log_d(1) + (d-1)(0)log_d(0)] \\
&+ \frac{p_1}{p_1+1}[1 + (d)(\frac{1}{d})log_d(\frac{1}{d})] = \frac{1}{p_1+1}.
\end{aligned} \tag{5.6}
$$

Here we generalize the BB84 protocol to work with qudits of composite dimensions using a complete set of the weak mutually unbiased bases introduced in chapter (4). As we mentioned earlier, for a d-dimensional system where $d = p_1 p_2$ and p_1, p_2 are prime numbers the weak mutually unbiased bases can be written as

$$T = T_0 \cup ... \cup T_{p_2}; \tag{5.7}$$

such that

$$T_u = \{|\mathcal{B}_j^{(1)}; \tilde{n}_1\rangle \otimes |\mathcal{B}_{j+u}^{(2)}; \tilde{n}_2\rangle \mid j \in \mathcal{Z}_{p_1+1}\}; \tag{5.8}$$

where $|\mathcal{B}_j^{(1)}; \tilde{n}_1\rangle$ are mutually unbiased bases in $\mathcal{H}_{p_1}$ and $|\mathcal{B}_{j+u}^{(2)}; \tilde{n}_2\rangle$ are mutually unbiased bases in $\mathcal{H}_{p_2}$, and $u \in \mathcal{Z}_{p_2+1}$. Let $|\mathcal{B}_{u,j}; n\rangle$ denote the bases that belong to T_u, therefore T_u can be written as

$$T_u = \{|\mathcal{B}_{u,j}; n\rangle \mid j \in \mathcal{Z}_{p_1+1}\}. \tag{5.9}$$

Chapter (4) shows that the absolute value of the overlap of any two vectors $|\mathcal{B}_{u,j}; n\rangle, |\mathcal{B}_{u',k}; m\rangle$ in two different weak mutually unbiased bases falls in one of the three categories where $\langle \mathcal{B}_{u,j}; n|\mathcal{B}_{u',k}; m\rangle = 0$ or $p_1^{-1/2}$ in the first category, $\langle \mathcal{B}_{u,j}; n|\mathcal{B}_{u',k}; m\rangle = 0$ or $p_2^{-1/2}$ in the second category, and $\langle \mathcal{B}_{u,j}; n|\mathcal{B}_{u',k}; m\rangle = d^{-1/2}$ in the third category.

Proposition 5.2.1. *Let $|\mathcal{B}_{u,j};n\rangle$ be a basis in a complete set of the weak mutually unbiased bases. Therefore, the other bases $|\mathcal{B}_{u',k};m\rangle$ are partitioned such that, there are p_1 bases $|\mathcal{B}_{u',k};m\rangle$ where $|\langle\mathcal{B}_{u,j};n|\mathcal{B}_{u',k};m\rangle|$ falls in the first category, p_2 bases $|\mathcal{B}_{u',k};m\rangle$ where $|\langle\mathcal{B}_{u,j};n|\mathcal{B}_{u',k};m\rangle|$ falls in the second category, and d bases $|\mathcal{B}_{u',k};m\rangle$ where $|\langle\mathcal{B}_{u,j};n|\mathcal{B}_{u',k};m\rangle|$ falls in the third category.*

Proof. $|\langle\mathcal{B}_{u,j};n|\mathcal{B}_{u',k};m\rangle|$ falls in the first category when $j \neq k$ and $j+u = k+u' \pmod{(p_2+1)}$. Let $j+u = k+u' \pmod{(p_2+1)}$, then $k = j+h;\ 0 < h < p_1+1$. Since $j+u = k+u' \pmod{(p_2+1)}$, then $u' = u-h \pmod{(p_2+1)}$. Therefore, given a basis $|\mathcal{B}_{u,j};m\rangle$ there exists p_1 bases $|\mathcal{B}_{u',k};m\rangle$ such that $|\langle\mathcal{B}_{u,j};n|\mathcal{B}_{u',k};m\rangle|$ falls in the first category. $|\langle\mathcal{B}_{u,j};n|\mathcal{B}_{u',k};m\rangle|$ falls in the second category when $j = k$ and $j+u \neq k+u' \pmod{(p_2+1)}$, there are p_2 such cases. Since the number of the bases $|\mathcal{B}_{u',k};m\rangle$ other than the basis $|\mathcal{B}_{u,j};n\rangle$ is $\psi(d)-1$, then the number of the bases $|\mathcal{B}_{u',k};m\rangle$ such that $|\langle\mathcal{B}_{u,j};n|\mathcal{B}_{u',k};m\rangle|$ falls in the third category is d. □

Now we assume that Alice prepares the qudit in one (randomly chosen) basis of the complete set of weak mutually unbiased bases, and Bob randomly chooses one basis of this set to measure the qudit in. Consider the case where Alice and Bob use the same basis $|\mathcal{B}_{u,j};n\rangle$, and Eve uses another different basis $|\mathcal{B}_{u',k};m\rangle$. According to the definition of weak mutually unbiased bases, Bob will get the right value of the qudit with probability $1/p_1$ if $|\langle\mathcal{B}_{u,j};n|\mathcal{B}_{u',k};m\rangle|$ belong to the first category, $1/p_2$ if $|\langle\mathcal{B}_{u,j};n|\mathcal{B}_{u',k};m\rangle|$ belong to the second category, and $1/d$ if $|\langle\mathcal{B}_{u,j};n|\mathcal{B}_{u',k};m\rangle|$ belong to the third category. Therefore, according to proposition (5.2.1), the probability

of detecting the presence of Eve P_d is

$$\begin{aligned} P_d &= \frac{1}{(p_1+1)(p_2+1)}[(1-1)+p_1(1-\frac{1}{p_1})+p_2(1-\frac{1}{p_2})+(d)(1-\frac{1}{d})] \\ &= \frac{p_1+p_2+d-3}{(p_1+1)(p_2+1)}. \end{aligned} \tag{5.10}$$

The information that Eve can leak I_E is

$$\begin{aligned} I_E &= 1+H(P_0,...,P_{d-1}) \\ &= \frac{1}{(p_1+1)(p_2+1)}[1+(1)log_d(1)+(d-1)(0)log_d(0)] \\ &+ \frac{p_1}{(p_1+1)(p_2+1)}[1+(p_1)(\frac{1}{p_1})log_d(\frac{1}{p_1})+(d-p_1)(0)log_d(0)] \\ &+ \frac{p_2}{(p_1+1)(p_2+1)}[1+(p_2)(\frac{1}{p_2})log_d(\frac{1}{p_2})+(d-p_2)(0)log_d(0)] \\ &+ \frac{d}{(p_1+1)(p_2+1)}[1+(d)(\frac{1}{d})log_d(\frac{1}{d})] \\ &= \frac{1}{(p_1+1)(p_2+1)}[1+p_2+(p_2-p_1)log_d(\frac{1}{p_2})]. \end{aligned} \tag{5.11}$$

The proposed protocol has a lower 'key construction' rate than the protocol adopted in [92, 93, 94] because it keeps one qudit out of $(p_1+1)(p_2+1)$ qudits while the other protocol keeps one qudit out of (p_1+1) qudits. However comparing Eq. (5.10) with Eq. (5.5) and Eq. (5.11) with Eq. (5.6) we find that the proposed protocol is more secure against the intercept and resend attack. The previous statement is true for all dimensions d where $d = p_1p_2$ and p_1, p_2 are prime numbers where $p_1 < p_2$ because

$$p_2(p_2-3) > -p_2-1. \tag{5.12}$$

Adding $d + p_2 d$ to both sides

$$d + p_2 d + p_2^2 - 3p_2 > d + p_2 d - p_2 - 1. \tag{5.13}$$

Dividing both sides by $p_2(p_1 + 1)(p_2 + 1)$

$$\frac{p_2(p_1 + p_2 + d - 3)}{p_2(p_1 + 1)(p_2 + 1)} > \frac{(d-1)(p_2 + 1)}{p_2(p_1 + 1)(p_2 + 1)}. \tag{5.14}$$

Therefore,

$$\frac{(p_1 + p_2 + d - 3)}{(p_1 + 1)(p_2 + 1)} > \frac{(d-1)}{p_2(p_1 + 1)}. \tag{5.15}$$

Also

$$\frac{1}{(p_1+1)(p_2+1)}[1+p_2+(p_2-p_1)log_d(\frac{1}{p_2})] = \frac{1}{p_1+1}+\frac{(p_2-p_1)log_d(\frac{1}{p_2})}{(p_1+1)(p_2+1)} < \frac{1}{p_1+1}. \tag{5.16}$$

Tables (5.3,5.4) consider quantum systems with different composite dimensions. Table (5.3) shows a comparison between the proposed protocol and the general BB84 protocol from the point of view of the probability of detecting Eve, and table (5.4) shows a comparison between the two protocols from the point of view of the information that Eve can leak. Table (5.4) also shows that the information that Eve can leak in the proposed protocol depends on the difference between p_2 and p_1 as well as the system dimension (this explains why the information that Eve can leak goes up from dimension 14 to dimension 15).

Table 5.3: A comparison between the proposed protocol (with $\psi(d)$ weak mutually unbiased bases) and the general BB84 protocol (with p_1+1 mutually unbiased bases) from the point of view of the probability of detecting Eve. In this table quantum systems with dimension d where $d = 6, 10, 14, 15, 21, 35$ are considered.

d	Proposed protocol	General BB84 protocol
6	0.667	0.556
10	0.778	0.6
14	0.833	0.619
15	0.833	0.7
21	0.875	0.714
35	0.917	0.81

Table 5.4: A comparison between the proposed protocol (with $\psi(d)$ weak mutually unbiased bases) and the general BB84 protocol (with p_1+1 mutually unbiased bases) from the point of view of the information that Eve can leak. In this table quantum systems with dimension d where $d = 6, 10, 14, 15, 21, 35$ are considered.

d	Proposed protocol	General BB84 protocol
6	0.282	0.333
10	0.217	0.333
14	0.18	0.333
15	0.2	0.25
21	0.17	0.25
35	0.144	0.167

5.3 Two-way deterministic cryptography protocols

Two way quantum cryptography protocols started with the 'Ping-Pong' protocol [52]. Later this protocol has been presented to provide a secure communication either with entanglement [103] or without entanglement [82, 104, 105]. Here we discuss the protocol adopted in [82] then we present our perspective to generalize this protocol to work with qudits of odd prime dimensions.

5.3.1 Two-way deterministic cryptography protocols with qubits

Here we consider that Alice and Bob use the two bases $|X;m\rangle, |P;m\rangle$ in $\mathcal{H}_2$. First Bob prepares the qubit in one of the four states $|X;0\rangle, |X;1\rangle, |P;0\rangle, |P;1\rangle$. After that the qubit is transmitted to Alice who decides randomly the mode in which she will use the qubit. Alice has two modes to choose from. The first mode is the control mode where Alice chooses randomly one of the bases $|X;m\rangle, |P;m\rangle$ to measure the qubit in then she sends the qubit back to Bob. The second mode is the encoding mode where Alice acts on the qubit either with the operator $\mathcal{I}$ which encodes the qubit as 0, or with the operator $i\sigma_y = \sigma_z\sigma_x$ which encodes the qubit as 1. We note that $\sigma_y, \sigma_x, \sigma_z$ are the Pauli operators discussed in chapter (2). The operator $i\sigma_y$ inverts the qubit irrespective of the state it is prepared in as shown in table (5.5)

Then the qubit is transmited back to Bob who measures it in the same

Table 5.5: The action of the operator $i\sigma_y$ on the states $|X;0\rangle$, $|X;1\rangle$, $|P;0\rangle$, $|P;1\rangle$.

	$\|X;0\rangle$	$\|X;1\rangle$	$\|P;0\rangle$	$\|P;1\rangle$
$i\sigma_y$	$-\|X;1\rangle$	$\|X;0\rangle$	$\|P;1\rangle$	$-\|P;0\rangle$

basis he prepared the qubit in. After that Alice declares publicly the working mode. In the case that Alice decides to work in the control mode, both Alice and Bob reveal the basis they use to measure and prepare the qubit in.

In the encoding mode, Bob decodes each qubit as 0 if it remains unchanged, and 1 if it is inverted.

In the control mode, the qubits are used to detect the presence of Eve. Eve uses the two bases $|X;m\rangle, |P;m\rangle$ to measure qubits. If she uses the correct basis (i.e. she uses the same basis that Bob used to prepare the qubit in), she will not be detected. If she uses a basis different from the basis used by Bob, she can stay undetected with probability $\frac{1}{2}$ in the forward path (on Alice's side), and with probability $\frac{1}{2}$ in the backward path (on Bob's side). Therefore, the probability of detecting Eve P_d is

$$P_d = \frac{1}{2} \times (0) + \frac{1}{2} \times (1 - \frac{1}{2} \times \frac{1}{2}) = \frac{3}{8} \tag{5.17}$$

5.3.2 Two-way deterministic cryptography protocols with qudits of two bases

In this subsection we generalize the two-way deterministic protocol to work with odd prime dimensional qudits rather than qubits. The position states $|X;m\rangle$ and the momentum states $|P;m\rangle$ are shifted by the same value under

the action of the operators $X^{\alpha}Z^{\alpha}$ as

$$(\mathscr{X}^{\alpha}\mathscr{Z}^{\alpha})|X;m\rangle = \Omega(m\alpha)|X;m+\alpha\rangle$$
$$(\mathscr{X}^{\alpha}\mathscr{Z}^{\alpha})|P;m\rangle = \Omega(-m\alpha)|P;m+\alpha\rangle, \tag{5.18}$$

where $m, \alpha \in \mathcal{Z}_d$. Eqs. (5.18) show that we can use the operators $\mathcal{I}, XZ, ..., X^{d-1}Z^{d-1}$ to encode the qudits as $0, 1, ..., d-1$. We modify the two-way deterministic cryptography protocol with qubits as follows.

Bob prepares the qudit in one of the $2d$ states (position and momentum states) then sends the qudit to Alice. Alice decides randomly the operation mode (control mode or encoding mode) then sends the qudit back to Bob. In the control mode, Alice measures the qudit in the position basis or the momentum basis. In the encoding mode, Alice encodes the qudit using one of the d operators $\mathscr{X}^{\alpha}\mathscr{Z}^{\alpha}$ where $\alpha \in \mathcal{Z}_d$. In some sense, this technique of encoding is similar to the blind encoding adopted in [106]. Bob gets the value α by applying a projective measurement to a qudit along the same basis used in preparing this qudit. The qudits which are used in the control mode are used to detect the presence of Eve. Eve measures the qudits along the position basis or the momentum basis. Therefore, with probability $\frac{1}{2}$ Eve estimates the correct basis (hence she will not be detected), and with probability $\frac{1}{2}$ she uses the wrong basis. In the case that Eve uses the wrong basis, she has the chance to be undetected on Alice's side with probability $\frac{1}{d}$ and on Bob's side with probability $\frac{1}{d}$, and hence the probability to be

undetected on both sides is $\frac{1}{d^2}$. The probability of detecting Eve is

$$P_d = \frac{1}{2} \times (0) + \frac{1}{2} \times (1 - \frac{1}{d} \times \frac{1}{d}) = \frac{d^2 - 1}{2d^2}. \tag{5.19}$$

As d increases, the probability of detecting eve tends to $\frac{1}{2}$,

$$P_{d\to\infty} = lim_{d\to\infty} \frac{d^2 - 1}{2d^2} = \frac{1}{2}. \tag{5.20}$$

5.3.3 Two-way deterministic cryptography protocols with qudits of d bases

In this subsection we prove that there are d bases of which the states are shifted by the same value α under the action of the operators $\mathscr{X}^\alpha \mathscr{Z}^\alpha$. We find these bases, and we prove that if d is prime, then these bases are mutually unbiased.

Since

$$\mathscr{X}^\alpha \mathscr{Z}^\alpha |X; m\rangle = \Omega(m\alpha)|X; m + \alpha\rangle \tag{5.21}$$

Then

$$U\mathscr{X}^\alpha \mathscr{Z}^\alpha |X; m\rangle = \Omega(m\alpha)U|X; m + \alpha\rangle, \tag{5.22}$$

where U is any unitary operator. Therefore,

$$U\mathscr{X}^\alpha \mathscr{Z}^\alpha U^\dagger U|X; m\rangle = \Omega(m\alpha)U|X; m + \alpha\rangle \tag{5.23}$$

Eq. (5.23) shows that, if there exists unitary transformation U such that

$$U\mathscr{X}^{\alpha}\mathscr{Z}^{\alpha}U^{\dagger} = \mathscr{X}^{\alpha}\mathscr{Z}^{\alpha}, \tag{5.24}$$

then the states $U|X;m\rangle$ are shifted by the value α under the action of the operators $\mathscr{X}^{\alpha}\mathscr{Z}^{\alpha}$. The following proposition finds such d unitary transformations.

Proposition 5.3.1. *In the case that d is prime, the states* $\mathcal{S}(1-\mu,-\mu|\mu,\mu+1)|X;m\rangle$ *are shifted by the same value* α *under the action of the operators* $\mathscr{X}^{\alpha}\mathscr{Z}^{\alpha}$ *where* $\mu,\alpha\in\mathcal{Z}_d$*. Furthermore, the bases* $\mathcal{S}(1-\mu,-\mu|\mu,\mu+1)|X;m\rangle$ *are mutually unbiased.*

Proof. Since

$$\mathscr{D}(\alpha,\beta) = \Omega(-2^{-1}\alpha\beta)\mathscr{Z}^{\alpha}\mathscr{X}^{\beta} = \Omega(2^{-1}\alpha\beta)\mathscr{X}^{\beta}\mathscr{Z}^{\alpha}. \tag{5.25}$$

Then

$$\mathscr{D}(\alpha,\alpha) = \Omega(2^{-1}\alpha^2)\mathscr{X}^{\alpha}\mathscr{Z}^{\alpha}. \tag{5.26}$$

Therefore, using Eq. (5.25) we can write Eq.(5.24) as

$$\mathcal{S}(\kappa,\lambda|\mu,\nu)\mathscr{D}(\alpha,\alpha)[\mathcal{S}(\kappa,\lambda|\mu,\nu)]^{\dagger} = \mathscr{D}(\alpha,\alpha) \tag{5.27}$$

But

$$\mathcal{S}(\kappa,\lambda|\mu,\nu)\mathscr{D}(\alpha,\alpha)[\mathcal{S}(\kappa,\lambda|\mu,\nu)]^{\dagger} = \mathscr{D}(\alpha\nu+\alpha\lambda,\alpha\mu+\alpha\kappa). \tag{5.28}$$

Then using Eqs. (5.27,5.28)

$$\alpha\nu + \alpha\lambda = \alpha, \alpha\mu + \alpha\kappa = \alpha. \tag{5.29}$$

Therefore,

$$\nu + \lambda = \mu + \kappa = 1. \tag{5.30}$$

Since

$$\kappa\nu - \lambda\mu = 1, \tag{5.31}$$

then using Eq. (5.30,5.31) we get

$$\kappa = 1 - \mu, \lambda = -\mu, \nu = 1 + \mu. \tag{5.32}$$

Therefore, there are d symplectic transformations $\mathcal{S}(1-\mu, -\mu|\mu, \mu+1)$ such that the states $\mathcal{S}(1-\mu, -\mu|\mu, \mu+1)|X; m\rangle$ are shifted by the same value α under the action of the operators $\mathscr{X}^{\alpha}\mathscr{Z}^{\alpha}$; $\mu, \alpha \in \mathcal{Z}_d$.

Now we prove that the bases $\mathcal{S}(1-\mu, -\mu|\mu, \mu+1)|X; m\rangle$; $0 \leq \mu < d$ are mutually unbiased. Let $|X(1-\mu, -\mu|\mu, \mu+1); m\rangle = \mathcal{S}(1-\mu, -\mu|\mu, \mu+1)|X; m\rangle$. In the case that $\mu = 0$, $|X(1-\mu, -\mu|\mu, \mu+1); m\rangle = |X(1, 0|0, 1); m\rangle = |X; m\rangle$ (because $\mathcal{S}(1, 0|0, 1) = \mathcal{I}$).

Bandyopadhyay et al. [54] showed that for any orthonormal bases $|X; m\rangle$, if there exists an operator V such that

$$V|X; m\rangle = \theta|X; m + j\rangle, \tag{5.33}$$

where $m, j \in \mathcal{Z}_d$ and $|\theta| = 1$, therefore the eigenstates of the operator V and

$|X;m\rangle$ are mutually unbiased bases. Since $|X;m\rangle$ are the eigenstates of the operator $\mathscr{Z}$ then $|X(1-\mu,-\mu|\mu,\mu+1);m\rangle;\ 0<\mu<d$ are the eigenstates of the operator $\mathcal{S}(1-\mu,-\mu|\mu,\mu+1)\mathscr{Z}[\mathcal{S}(1-\mu,-\mu|\mu,\mu+1)]^{\dagger}$. But the operator $\mathcal{S}(1-\mu,-\mu|\mu,\mu+1)\mathscr{Z}[\mathcal{S}(1-\mu,-\mu|\mu,\mu+1)]^{\dagger}$ is a displacement operator that shifts the state $|X;m\rangle$ by the value μ. Therefore, $|X;m\rangle$ and each of the bases $|X(1-\mu,-\mu|\mu,\mu+1);m\rangle$ where $\mu>0$ are mutually unbiased. Now we need to prove that the bases $|X(1-\mu,-\mu|\mu,\mu+1);m\rangle$ where $\mu>0$ are mutually unbiased. Let $0<\mu_1,\mu_2<d;\ \mu_1\neq\mu_2$, then

$$\begin{aligned}&|\langle X(1-\mu_1,-\mu_1|\mu_1,\mu_1+1);m_1|X(1-\mu_2,-\mu_2|\mu_2,\mu_2+1);m_2\rangle|\\&=|\langle X;m_1|[\mathcal{S}(1-\mu_1,-\mu_1|\mu_1,\mu_1+1)]^{\dagger}\mathcal{S}(1-\mu_2,-\mu_2|\mu_2,\mu_2+1)|X;m_2\rangle|\end{aligned}\tag{5.34}$$

In chapter (2) we have shown that

$$\mathcal{S}(\kappa_2,\lambda_2|\mu_2,\nu_2)\mathcal{S}(\kappa_1,\lambda_1|\mu_1,\nu_1)=\mathcal{S}(\kappa,\lambda|\mu,\nu),\tag{5.35}$$

where

$$\begin{pmatrix}\kappa_1 & \lambda_1\\ \mu_1 & \nu_1\end{pmatrix}\begin{pmatrix}\kappa_2 & \lambda_2\\ \mu_2 & \nu_2\end{pmatrix}=\begin{pmatrix}\kappa & \lambda\\ \mu & \nu\end{pmatrix}.\tag{5.36}$$

Since $[\mathcal{S}(1-\mu_1,-\mu_1|\mu_1,\mu_1+1)]^{\dagger}\mathcal{S}(1-\mu_1,-\mu_1|\mu_1,\mu_1+1)=\mathcal{I}$ then using Eqs. (5.35,5.36)

$$[\mathcal{S}(1-\mu_1,-\mu_1|\mu_1,\mu_1+1)]^{\dagger}=\mathcal{S}(\mu_1+1,\mu_1|-\mu_1,1-\mu_1).\tag{5.37}$$

Therefore, using Eqs. (5.35,5.36,5.37) we prove that

$$\begin{aligned}&|\langle X(1-\mu_1,-\mu_1|\mu_1,\mu_1+1);m_1|X(1-\mu_2,-\mu_2|\mu_2,\mu_2+1);m_2\rangle|\\&=|\langle X;m_1|X(1+\mu_1-\mu_2,\mu_1-\mu_2|\mu_2-\mu_1,\mu_2-\mu_1+1);m_2\rangle|\end{aligned}\tag{5.38}$$

Let $\mu=\mu_2-\mu_1$, then Eq. (5.38) can be written as

$$\begin{aligned}&|\langle X(1-\mu_1,-\mu_1|\mu_1,\mu_1+1);m_1|X(1-\mu_2,-\mu_2|\mu_2,\mu_2+1);m_2\rangle|\\&=|\langle X;m_1|X(1-\mu,-\mu|\mu,\mu+1);m_2\rangle|.\end{aligned}\tag{5.39}$$

Since the bases $|X;m_1\rangle$ and each of the bases $|X(1-\mu,-\mu|\mu,\mu+1);m_2\rangle;\ 0<\mu<d$ are mutually unbiased then

$$|\langle X(1-\mu_1,-\mu_1|\mu_1,\mu_1+1);m_1|X(1-\mu_2,-\mu_2|\mu_2,\mu_2+1);m_2\rangle|=d^{-1/2}.\tag{5.40}$$

This completes the proof. □

Using the d bases $|X(1-\mu,-\mu|\mu,\mu+1);m\rangle$ (where $0\leq\mu<d$) in our two-way deterministic protocol, the probability of detecting Eve is calculated as follows

$$P_d=\frac{1}{d}\times(0)+\frac{d-1}{d}\times(1-\frac{1}{d}\times\frac{1}{d})=\frac{(d-1)(d^2-1)}{d^3}.\tag{5.41}$$

Comparing Eq. (5.41) with Eq. (5.19), it is seen that for $d>2$ the probability of detecting Eve using d mutually unbiased bases is better than the probability of detecting Eve using two mutually unbiased bases. Eq. (5.41)

shows that as $d \to \infty$, the probability of detecting Eve tends to 1.

$$P_{d\to\infty} = lim_{d\to\infty}\frac{(d-1)(d^2-1)}{d^3} = 1. \tag{5.42}$$

5.4 Summary

In this chapter we presented two quantum cryptography protocols. The first one is one-way nondeterministic protocol that generalizes the BB84 protocol to work with qudits with dimension $d = p_1 p_2$; p_1, p_2 are prime numbers. We have used the weak mutually unbiased bases to prepare and measure the qudits. The second protocol is two-way deterministic that generalizes the two-way deterministic protocol with qubits to work with qudits. We have analyzed the two protocols against the intercept and resend attack.

Chapter 6

Conclusion and future work

6.1 Conclusion

We have considered finite quantum systems where the variables are defined in $\mathcal{Z}_d$. The $\mathcal{Z}_d \times \mathcal{Z}_d$ phase space is near-linear geometry if d is a prime number, otherwise $\mathcal{Z}_d \times \mathcal{Z}_d$ is not near-linear geometry and this leads to two important concepts which generalize the near-linear geometry. The first concept is, two lines may have more than one point in common, i.e $\mathcal{Z}_d \times \mathcal{Z}_d$ where d is not prime has geometrical redundancy (Eq. (3.20)). The second concept is, the existence of sublines with d_j points where d_j is a divisor of d. We have proved important properties of lines that emphasize the differences in $\mathcal{Z}_d \times \mathcal{Z}_d$ in the cases that $\mathcal{Z}_d$ is a field or a ring (proposition (3.2.1)).

We considered the case $d = p_1 p_2$ where $p_1,\ p_2$ are prime numbers (however, the generalization to a product of many prime numbers is also possible). Then we presented the concept of factorizing a line in $\mathcal{Z}_d \times \mathcal{Z}_d$ into two component lines in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$ and $\mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$, correspondingly. The concept of

factorizing lines led us to an explicit construction of all maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ (Eqs. (3.32,3.33)). It also led us to clarify the relation between the number of common points between two lines in $\mathcal{Z}_d \times \mathcal{Z}_d$, and their first and second component lines in $\mathcal{Z}_{p_1} \times \mathcal{Z}_{p_1}$ and $\mathcal{Z}_{p_2} \times \mathcal{Z}_{p_2}$, Correspondingly (proposition (3.3.2)).

Motivated by the properties of the finite geometry of $\mathcal{Z}_d \times \mathcal{Z}_d$, we have introduced the concept of weak mutually unbiased bases that weakens the concept of mutually unbiased bases. Two bases in $\mathcal{H}_d$ where $d = p_1 p_2$, are called weak mutually unbiased, if the absolute value of the overlap of any vector in the first basis and any vector in the second basis is equal to $d^{-1/2}$ or alternatively to one of the $p_j^{-1/2}$, 0 (where p_j is a divisor of d and p_j is not equal to 1 or d). Eqs. (4.52,4.62) have shown an explicit construction of a complete set of weak mutually unbiased bases. This construction is based on forming the tensor product of the $p_1 + 1$ mutually unbiased bases in $\mathcal{H}_{p_1}$ and the $p_2 + 1$ mutually unbiased bases in $\mathcal{H}_{p_2}$ to get the $\psi(d)$ weak mutually unbiased bases in $\mathcal{H}_d$.

We have shown the duality between the maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ and the weak mutually unbiased bases in $\mathcal{H}_d$, in the sense that there is a correspondence between the properties of the maximal lines and the properties of the bases. Tables (3.1,4.2,3.2,4.3,3.3,4.8,3.4,4.9) present explicitly this duality.

We have studied the concept of weak mutually unbiased bases in the context of complex projective t-designs. We proved that a complete set of weak mutually unbiased bases is a complex projective 1-design with angle set $\{0, 1/p_1, 1/p_2, 1/d\}$ and form WBE-sequence set. We have also shown that a set of weak mutually unbiased bases is a regular scheme.

As an application of weak mutually unbiased bases, we have proved that, using a complete set of such bases in tomography experiments can lead us to reconstruct the density matrix of an arbitrary quantum system; i.e. we have proved that, the set of weak mutually unbiased bases is tomographically complete.

We gave two examples of using weak mutually unbiased bases in quantum tomography. The first example is for a quantum system in pure state, and the second example is for a quantum system in mixed state. In both examples, we started with the probabilities corresponding to the weak mutually unbiased bases, and we ended with the reconstruction of the density matrix of the quantum system. Tables (4.4, 4.5) show samples of these probabilities. According to the redundancy associated with weak mutually unbiased bases (Eq. (4.70)), the probabilities must obey the constraint of (Eq. (4.72)). Tables (4.6,4.7) show that the probabilities considered in the two examples obey this constraint.

Another application of weak mutually unbiased bases is its use in quantum cryptography with quantum systems of dimension d where $d = p_1 p_2$. We have modified the BB84 protocol such that weak mutually unbiased bases are used to prepare and measure qudits. The security analysis of the proposed protocol against intercept and resend attack showed that it gives better performance than the protocol adopted in [92, 93, 94], regarding the probability of detecting Eve and the information that Eve can leak (compare Eq. (5.10) with Eq. (5.5) and Eq. (5.11) with Eq. (5.6)).

For quantum systems with dimension d where d is odd prime, we have proved that the states of d bases are shifted by the same value α under

the action of the operators $X^{\alpha}Z^{\alpha}$. We have used this result to generalize the two-way deterministic cryptography protocol to work with qudits rather than qubits. We have analyzed this protocol against the intercept and resend attack, Eq. (5.41) shows the probability of detecting Eve according to this attack.

6.2 Future work

In this work we have studied the duality between the maximal lines in $\mathcal{Z}_d \times \mathcal{Z}_d$ and the weak mutually unbiased bases, We can extend this study to find the dual concept of sublines as well.

Another aspect of our future work is to analyze the proposed quantum cryptography protocols against various types of eavesdropper attacks. It would be interesting to study the tradeoff between the construction rate and the security in the one-way protocol as well as the tradeoff between the system dimension and the security in the two-way protocol.

References

Bibliography

[1] M.A. Nielsen and I.L. Chuang, Quantum computing and quantum information, Cambridge University Press, Cambridge (2000)

[2] C.H. Bennett and G. Brassard, Proceedings of the IEEE Intl. Conf. Computers, Systems, and Signal Processing, 175 (1984)

[3] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys., Vol. 74, No. 1 (2002)

[4] W. K. Wooters, Ann. Phys. (NY), 176:1 (1987)
W. K. Wooters and B. D. Fields, Ann. Phys. (NY), 191:363 (1989)

[5] A. Vourdas, Rep. Prog. Phys., 67:267 (2004)

[6] I.J. Good, IEEE Trans. Computers, C-20:310 (1971)

[7] H. Weyl, Theory of Groups and Quantum Mechanics, New York: Dover, (1950)

[8] J. Schwinger, Nat. Acad. Sci., 46:570 (1960)

[9] J. Schwinger, Quantum Kinematics and Dynamics, New York: Benjamin, (1970)

[10] R. Balian and C. Itzykson, C R Acad. Science, 303:773 (1986)

[11] M. L. Mehta, J. Math Phys., 28:781 (1987)

[12] D. Galetti and A. F. R. de Toledo-Piza, Physica A, 149:267 (1988)

[13] J. C. Varilly and J. M. Gracia-Bondia, Ann. Phys. (NY), 190:107 (1989)
H. Figueroa, J. M. Gracia-Bondia, and J. C. Varilly, J. Math. Phys., 31:2664 (1990)

[14] A. Vourdas, Phys. Rev. A, 41:1653 (1990)
A. Vourdas, Phys. Rev. A, 43:1564 (1991)

[15] T. Lulek, Acta Phys. Polon. A, 82:377 (1992)
T. Lulek, Rep. Math. Phys., 34:71 (1994)

[16] V. S. Varadarajan, Lett. Math. Phys., 34:319 (1995)

[17] U. Leonhardt, Phys. Rev. Lett., 74:4101 (1995)
U. Leonhardt, Phys. Rev. A, 53:2998 (1996)

[18] G. Hadzitaskos and J. Tolar, Int. J. Theor. Phys., 32:517 (1993)
J. Tolar and G. Hadzitaskos, J. Phys. A, 30:2509 (1997)

[19] T. Hakioglu, J. Phys. A, 31:6975 (1998)

[20] A. Vourdas and C. Bendjaballah, Phys. Rev. A, 47:3523 (1993)
A. Vourdas, J. Phys. A, 36:5645 (2003)

[21] A. Vourdas, J. Phys. A, 29:4275 (1996)
A. Vourdas, Rep. Math. Phys., 40:367 (1997)
A. Vourdas, J. Opt. B-Quantum Semiclass. Opt., 5:S581 (2003)

[22] R.T. Perry, The temple of quantum computing, Riley Perry, (2010)

[23] L. Auslander and R. Tolimieri, Bull. Am. Math. Soc., 1:847 (1979)

[24] P. Feinsilver, Monatshefte fr Mathematik, 104:89 (1987)
L.D. Faddeev, Lett. in Math. Phys., 34:249 (1995)
A. Ballesteros, F.J. Herranz and P. Parashar, J. Phys. A: Math. Gen, 30:L149 (1997)

[25] A. Vourdas and C. Banderier, J. Phys. A: Math. Theor., 43:042001 (2010)

[26] E. Wigner, Phys. Rev., 40:749 (1932)

[27] A. Royer, Phys. Rev. A, 15:449 (1977)

[28] M. V. Berry, Phil. Trans. R. Soc., 287:237 (1977)

[29] N. L. Balazs and B. K. Jennings, Phys. Rep., 104:347 (1984)

[30] M. Hillery, R. F. OConnell, M. O. Scully and E. Wigner, Phys. Rep., 106:121 (1984)

[31] H. W. Lee, Phys. Rep., 259:147 (1995)

[32] V. Buzek and P. L. Knight, Prog. Opt., 34:1 (1995)

[33] K. Vogel and H. Risken, Phys. Rev. A, 40:2847 (1989)

[34] D. T. Smithey, M. Beck, M. G. Raymer and T. Faridani, Phys. Rev. Lett., 70:1244 (1993)

[35] U. Leonhardt, Measuring the Quantum State of Light, Cambridge University Press (1995)

[36] A. Wunsche, Phys. Rev. A, 54:5291 (1996)

[37] A. Wunsche, J. Mod. Opt., 44:2293 (1997)

[38] A. Wunsche, J. Mod. Opt., 47:33 (2000)

[39] D. Leibfried, D. M. Meekhof, B. E. King, C. Monroe, W. M. Itano and D. J. Wineland, Phys. Rev. Lett., 77:4281 (1996)

[40] C. Kurtsiefer, T. Pfau and J. Mlynek, Nature, 386:150 (1997)

[41] G. Breitenbach, S. Schiller and J. Mlynek, Nature, 387:471 (1997)

[42] M. Koniorczyk, V. Buek and J. Janszky, Phys. Rev. A, 64:034301 (2001)

[43] L. Mita, R. Filip and A. Furusawa, Phys. Rev. A, 82:012322 (2010)

[44] A. Casado, S. Guerra and J. Placido, J. Phys. B, 41:045501 (2008)

[45] X. Shao-hua, S. Bin, L. Jin and S. Ke-hui, Physica Scripta, 79:025002 (2009)

[46] A. Luis and J. Perina, J. Phys. A, 31:1423 (1998)

[47] A. O. Pittenger and M. H. Rubin, J. Phys. A, 38:6005 (2005)

[48] J. H. McClellan and T. W. Parks, IEEE Trans. Audio Electroacoust., 20:66 (1972)

R. Yarlagadda, IEEE Trans. Acoustics Speech Signal Proc., 25:586 (1977)

B. W. Dickinson and K. Steiglitz, IEEE Trans. Acoustics Speech Signal

Proc., 30:25 (1982)

R. Tolimieri, Adv. Appl. Math., 5:56 (1984)

[49] I. Bengtsson, AIP Conference Proceedings, 889:40 (2006)

[50] I.D. Ivanovic, J. Phys. A, 14:3241 (1981)

[51] M. S. Zubairy, Phys. Rev. A, 54:4368 (1998)

T. Durt, Cosmos 2, World Scientific Singapore, 21-48 (2006)

Z. Zhang, Y. Liu and D. Wang, Phys. Lett. A, 372:28 (2007)

[52] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett., 69:2881 (1992)

[53] L. Vaidman, Y. Aharonov and D. Albert, Phys. Rev. Lett., 58:1385 (1987)

B. G. Englert and Y. Aharonov, Phys. Lett. A, 284:1 (2001)

P. Aravind, Zeitschrift fr Naturforschung, 58:2212 (2003)

[54] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury and F. Vatan, Algorithmica, 34(4):512 (2002)

[55] I. Bengtsson, W. Bruzda, A. Ericsson, J. Larsson, W. Tadej and K. Zyczkowskiin, J. Math. Phys., 48:052106 (2007)

S. Brierley and S. Weigert, Phys. Rev. A, 79:052316 (2009)

S. Brierley, S. Weigert and I. Bengtsson, Quantum Info. and Comp., 10:0803 (2010)

[56] S. Chowla, P. Erdos, and E.G. Strauss, Canadian J. Math., 12:204 (1960)

T. Beth, D. Jungnickel and H. Lenz., 'Design theory, Encyclopedia of

Mathematics and Its Applications', vol. 1, Cambridge University Press, (1999)

[57] C. Godsil and A. Roy, European Journal of Combinatorics, 30:246 (2009)

[58] P. Butterley and W. Hall, Phys. Lett. A, 369:5 (2007)
S. Brierley and S. Weigert, Phys. Rev. A, 79:052316 (2009)

[59] T. Durt, B.G. Englert, I. Bengtsson and K. Zyczkowski, Int. J. Quantum Comp., 8:535 (2010)

[60] J.W.P. Hirchfeld, 'Projective geomtries over finite fields', Oxford Univ. Press, Oxford, (1979)
J.W.P. Hirchfeld and J.A. Thas, 'General Galois geometries', Oxford Univ. Press, Oxford, (1991)
L.M. Batten, 'Combinatorics of finite geometries', Cambridge Univ. Press, Cambridge, (1997)

[61] O. Albouy, J. Phys. A, 42:072001 (2009)

[62] T. M. Apostol, 'Introduction to Analytic Number Theory', Berlin: Springer, (1976)

[63] S. Chaturvedi, Phys. Rev. A, 65:044301 (2002)

[64] K. Gibbons, M.J. Hoffman and W. Wootters, Phys. Rev. A, 70:062101 (2004)
A. Klappenecker and M. Rotteler, Lect. Notes Comp. Science, 2948:137 (2004)

[65] C. Archer, J. Math. Phys., 46:022106 (2005)
A. Klimov, L. Sanchez-Soto and H. de Guise, J. Phys. A, 38:2747 (2005)
J.L. Romero, G. Bjork, A.B. Klimov and L.L. Sanchez-Soto, Phys. Rev. A, 72:062310 (2005)

[66] M.R. Kibler and M. Planat, Intern. J. Mod. Phys. B, 20:1802 (2006)
M. Saniga and M. Planat, J. Phys. A, 39:435 (2006)
A. Vourdas, J. Math. Phys., 47:092104 (2006)

[67] P. Sulc and J. Tolar, J. Phys. A,40:15099 (2007)
A. Vourdas, J. Phys. A, 40:R285 (2007)

[68] J. Tolar and G. Chadzitaskos, J. Phys. A, 42:245306 (2009)

[69] J. M. Renes, R. Blume-Kohout, A. J. Scott and C. M. Caves, J. Math. Phys., 45:2171 (2004)

[70] D. M. Appleby, J. Math. Phys., 46:052107 (2005)

[71] S. T. Flammia, J. Phys. A: Math. Gen., 39:13483 (2006)

[72] A. J. Scott and M. Grassl, J. Math. Phys., 51:042203 (2010)

[73] T. Beth, D. Jungnickel and H. Lenz, 'Design Theory', Cambridge University Press, Cambridge, (1993)

[74] H. Havlicek, 'Divisible designs, Laguerre geometry, and beyond', Lectures in Summer School on Combinatorial Geometry and Optimisation, pp 159, (Brescia, Italy), (2004)

[75] A. Roy and A. J. Scott, J. Math. Phys., 48:072110 (2007)

[76] G. M. Connell and D. Gross, Quantum Inform. Comput., 8:734 (2008)

[77] S. G. Hogar, Eur. J. Comb., 5:29 (1984)

[78] G. Zauner, Int. J. Quantum Inform., 9:445 (2011)

[79] A. Klappenecker and M. Rotteler, Proceedings of the IEEE International Symposium on Information Theory (ISIT'05), pages 1740-1744 (2005)

[80] L. R. Welch, IEEE Trans. on Information Theory, IT-20:397 (1974)

[81] J.L. Massey and T. Mittelholzer, Sequences II: Methods in Communications, Security and Computer Sciences, pages 6378 (1993)

[82] M. Lucamarini and S. Mancini2, Phys. Rev. Lett., 94:140501 (2005)

[83] P. W. Shor, Proceedings of the 35th Symposium on Foundations of Computer Science, IEEE Computer Society, Los Alamitos, California, pp. 124134 (1994)

[84] A. K. Ekert, Phys. Rev. Lett., 67:661 (1991)

[85] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter and A. Zeilinger, Phys. Rev. Lett., 84:4729 (2000)

[86] I. Devetak and A.Winter, Proc. R. Soc. Lond. A, Math. Phys. Sci., pp. 207235 (2005)

[87] K. Horodecki, D. Leung and H.-K. Lo, J. Oppenheim, Phys. Rev. Lett., 96:070501 (2006)

[88] G. Gordona and G. Rigolinb, Optics Communications, 283:184 (2010)

[89] S. Wiesner, Sigact News, 15:78 (1983)

[90] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A, 59:42384248 (1999)

[91] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A, 61:062308 (2000)

[92] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett., 85:33133316 (2000)

[93] M. Bourennane, A. Karlsson, G. Bjork, N. Gisin and N. J. Cerf, J. Phys. A: Math. Gen., 35:10065 (2002)

[94] N. J. Cerf, M. Bourennane, A. Karlsson, G. Bjork and N. Gisin, Phys. Rev. Lett, 88:127902 (2002)

[95] C. H. Bennett, Phys. Rev. Lett., 68:3121 (1992)

[96] J.S. Shaari ,M. Lucamarini and M.R.B. Wahiddin, Phys. Lett. A, 358:8590 (2006)

[97] F. A. A. El-Orany, Phys. Lett. A, 374:1097 (2010)

[98] A. Eusebi and S. Mancini, Quant. Inf. Comp., 9:950 (2009)

[99] A. Eusebi and S. Mancini, Int. J. Quant. Inf., 9:1209 (2011)

[100] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. Niu and A. Peres, Phys. Rev. A, 56:1163 (1997)

[101] D. Brub, Phys. Rev. Lett., 81:3018 (1998)

[102] D. Brub and C. Macchiavello, Phys. Rev. Lett., 88:127901 (2002)

[103] K. Bostrom and T. Felbinger, Phys. Rev. Lett., 89:187902 (2002)

[104] C. Qing-Yu and L. Bai-Wen, Chin. Phys. Lett., 21:601 (2004)

[105] F. G. Deng and G. L. Long, Phys. Rev. A, 69:52319 (2004)
F. G. Deng and G. L. Long, ibid., 70:012311 (2004)

[106] J.S. Shaari, S. Mancini and M.R.B. Wahiddin, Phys. Lett. A, 372:1963 (2008)