UNIVERSITI PUTRA MALAYSIA

THE DISCRETE PHASE SPACE FOR 3-QUBIT AND 2-QUTRIT SYSTEMS BASED ON GALOIS FIELD

MAZLINDA BINTI ZAINY
FS 2009 39

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

THE DISCRETE PHASE SPACE FOR 3-QUBIT AND 2-QUTRIT SYSTEMS BASED ON GALOIS FIELD

By

MAZLINDA BINTI ZAINY

November 2009

Chair: Hishamuddin B. Zainuddin, PhD
Faculty: Science

Generally, quantum states are abstract states that carry probabilistic information of position and momentum of any dynamical physical quantity in quantum system. E.P.Wigner (1932) had introduced a function that can determine the combination of position and momentum simultaneously, and it was the starting point to define a phase space probability distribution for a quantum mechanical system using density matrix formalism. This function named as Wigner Function. Recently, Wootters (1987) has developed a discrete phase space analogous to Wigner's ideas. The space is based on Galois field or finite field. The geometry of the space is represented by $N \times N$ point, where N denoted the number of elements in the field and it must be a prime or a power of a prime numbers. In this work, we study the simplest way to compute the binary operations in finite field in order to form such a discrete space. We developed a program using Mathematica software to solve the binary operation in the finite field for the case of 3-qubit and 2-qutrit systems. The program developed should also be extendible for the higher number of qubit and qutrit. Each state is defined by a line $aq + bp = c$ and parallel lines give equivalent states. The results show that, there are 9 set of parallel lines for the 3-qubit system and 10 sets of parallel lines for 2-qutrit system. These complete set of parallel lines called a ‘striation’.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

RUANG FASA DISKRIT UNTUK SISTEM *3*-QUBIT DAN *2*-QUTRIT BERDASARKAN MEDAN GALOIS

Oleh

MAZLINDA BINTI ZAINY

November 2009

Pengerusi: Hishamuddin B. Zainuddin, PhD

Fakulti: Sains

Secara amnya, keadaan-keadaan kuantum adalah keadaan abstrak yang membawa maklumat kebarangkalian berkaitan kedudukan dan momentum suatu kuantiti fizikal dinamik di dalam sistem kuantum. E.P.Wigner (1932) telah memperkenalkan suatu fungsi yang dapat menentukan kombinasi kedudukan dan momentum secara serentak, dan keadaan ini adalah suatu permulaan untuk menjelaskan taburan kebarangkalian ruang fasa untuk sistem kuantum mekanik dengan menggunakan formalisasi ketumpatan matrik. Fungsi tersebut dinamakan Fungsi Wigner. Baru-baru ini, daripada analogi idea Wigner, Wootters (1987) telah membina suatu ruang fasa yang diskrit. Ruang fasa ini adalah berdasarkan medan terhingga atau medan galois. Struktur geometri fasa ruang ini diwakili oleh titik $N \times N$, di mana N ini menandakan bilangan elemen dalam medan ini dan ianya mesti nombor perdana atau kuasa nombor perdana. Dalam penyelidikan ini, kami mengkaji cara yang paling mudah untuk mengira operasi dedua dalam medan terhingga yang dapat digunakan untuk menghasilkan struktur fasa ruang yang diskrit. Kami telah bangunkan satu program menggunakan perisian Mathematica untuk menyelesaikan operasi dedua dalam medan terhingga untuk sistem *3*-qubit and *2*-qutrit. Program yang dibina juga harus disambungkan untuk bilangan qubit dan qutrit yang tinggi. Setiap keadaan kuantum dalam ruang fasa ini ditakrifkan oleh garis yang dipunyai oleh persamaan $aq + bp = c$, dan garis yang selari memberikan keadaan-keadaan kuantum yang sama. Hasil kajian menunjukkan , terdapat 9 set garis yang selari untuk sistem *3*-qubit dan 10 set garis yang selari untuk sistem *2*-qutrit. Set garis-garis selari ini dikenali sebagai “jaluran”.

ACKNOWLEDGEMENTS

Alhamdulillah, praise to Allah S.W.T. for giving me the strength, patience and enable me to complete this work.

First of all, I would like to express gratitude to my supervisor, Associate Professor Dr. Hishamuddin Zainuddin for his invaluable support, encouragements, supervision throughout this research work. His moral support and continues guidance enabled me to complete my work.

I would also like to thank my co-supervisors, Associate Professor Dr. Jumiah Hassan for her willingness to help and guide me in this research.

I wish to thanks my family for their support, encouragement, patience and kindness throughout my study.

Finally, my sincere thanks go to my research friends Abu, Risya and Ain, who always shared their research experience with me. May Allah bless all of you.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

$\mathbb{C}$	Complex numbers
$\mathbb{R}$	Real Numbers
$\mathbb{Q}$	Rational Numbers
$\lvert\psi\rangle$	Vector in Hilbert space
$\lvert e_k\rangle$	Basis vectors
$\lvert 0\rangle, \lvert 1\rangle$	2-level basis states in quantum bit
$\lvert a\rvert^2$	Modulus of a power of 2
$\lvert b\rvert^2$	Modulus of b power of 2
$\langle\psi\rvert$	Dual vector in Hilbert space, *bra*
$\langle\psi_1\vert\psi_2\rangle$	Inner product in Hilbert space
ρ_ψ	Density operators
$\lvert\psi\rangle\langle\psi\rvert$	Outer product in Hilbert space
N	Field Elements
$N\times N$	Discrete phase space of *N* points
$2N\times 2N$	Discrete phase space of *2N* points
2^n	Field elements of power of prime numbers
$2^n\times 2^n$	Discrete phase space of power of prime numbers
F	Field
F_N	Finite Field with *N* elements
$F_N[x]$	Polynomial Rings
$+$	Addition operation

$\cdot$	Multiplication operation
α	Elements representations
$\vert\lambda\rangle$	superposition of these three basis states of general qutrit
$a \equiv b(\bmod m)$	a congruent to b modulo m
$R/(m)$	Residue class ring modulo m
$Z/(p)$	Residue class ring of integers modulo prime numbers
$F[x]/(f(x))$	Residue class ring of polynomial ring modulo the polynomial
p	Prime numbers
$\geq$	Bigger than or equal
$>$	Bigger than

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Quantum Computation and Quantum Information

Quantum computation (QC) and quantum information (QI) are nowadays active research fields in science and technology. The basic ideas of the fields come from four disciplines namely quantum mechanics, computer science, information theory and cryptography. According to Nielsen & Chuang, 2000, quantum computation and quantum information is the study of the information processing tasks that can be accomplished using quantum mechanical system. It is expected that the nature of quantum information processing will be significantly different given that quantum mechanics is altogether different from classical mechanics which govern the traditional information theory. It is crucial to mention the remarkable development of quantum factoring algorithm by Peter W. Shor (1997) giving an exponential speed-up of prime factorization by a clever use of quantum superposition and interference. This has led to an explosive development in the area of quantum computing and quantum information. One particular interesting problem is to look for experimental realization of computers operating according to quantum mechanics can be exponentially faster than classical computers in specific tasks. In popular literature, we read claims that quantum information will contribute a method to secure the communications channels, data storage, speedup the computational task and many more.

The key ingredient in quantum information processing is the description of quantum states. The simplest being quantum bit or qubits used in the bulk of quantum computation and quantum information literature. Qubit provides the information of the state in two-level quantum system. The two-level quantum system can be realised as the elementary state of a spin $\frac{1}{2}$ particle or equivalently as the horizontal and vertical polarization states of a photon or even the ground and first excited state of an electron in an atom, ignoring higher energy states in the manipulation.

1.2 Quantum State

Here we briefly describe the general concept of quantum state used to describe a quantum system, most of which are available in standard quantum mechanic text books. Quantum state is represented by a ray in a Hilbert space. For our purposes, we simply use a vector in Hilbert space denoted by $|\psi\rangle$, and the projection onto a ray will be understood implicitly. Equipped with the vector space are basis kets $|e_k\rangle$, for which the vector $|\psi\rangle$ can be written as linear combination of the basis states in the following way:

$$|\psi\rangle = \sum_k c_k |e_k\rangle \quad , \qquad c_k \in \mathbb{C} \tag{1.2.1}$$

Each vector $|\psi\rangle$ has a conjugate dual known as *bra*, denoted by $\langle\psi|$. Thus, an inner product structure $\langle\psi_1|\psi_2\rangle$ is available for use to describe measurement results in scalar form.

As an example, $|0\rangle$ and $|1\rangle$ form basis states for quantum bit. Just as classical bit, qubit also can be in basis state $|0\rangle$ or $|1\rangle$, but qubit has the extra possibility that it can be in both basis states simultaneously. With this special property called superposition, qubits can be more powerful in quantum information processing than the classical bits. The superposition qubit is represented as the linear combination of $|0\rangle$ and $|1\rangle$ i.e.

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad , \quad a,b \in \mathbb{C} \qquad (1.2.2)$$

Normalization requires $\langle\psi|\psi\rangle = 1$, thus giving $|a|^2 + |b|^2 = 1$. The values $|a|^2$ and $|b|^2$ give the probabilities of measuring the $|0\rangle$ and $|1\rangle$ states respectively.

It is possible to associate the states $|\psi\rangle$ with operators formed from outer products, namely the density operators i.e.

$$\rho_\psi = |\psi\rangle\langle\psi| \quad . \qquad (1.2.3)$$

The advantage of using density operators instead of merely ket vectors is that they can also describe what is known as mixed states for statistical ensembles. In this work, however we will not consider mixed states at all but the density operators play an important role in another alternative description of quantum states namely the phase space description.

1.3 Discrete Wigner Function (DWF) and Discrete Phase Space

Generally, the measurement outcomes of a quantum system are described by a probability distribution. In the usual quantum mechanics formalism, such probability distributions are often restricted to either one based on position representation or on momentum representation. Apart from the conditions of the Heisenberg uncertainty principle, there is no real reason for such a restriction. It is in this context that Wigner Function was introduced by E.P. Wigner (1932) in defining a state in quantum mechanical system in the full phase space formalism. The Wigner function acts in some respect like a probability distribution, but it differs from a probability distribution in that it can take negative values (Gibbons et.al., 2004). Note that the original Wigner function employs continuous variables of position and momentum equivalent to an infinite dimensional Hilbert space description of states. In practice, often we would like to make simpler (partial) description of a quantum system and uses only a finite dimensional Hilbert space, particularly in the field of quantum information. It is then natural to ask whether a phase space description exists for such finite dimensional systems. The answer is in the affirmative as demonstrated by Wootters and earlier works in quantum optics. Instead of defining the function in continuous phase space, one develops the discrete version of phase space and hence define discrete Wigner function. In principal, the properties of discrete phase space are analogous to the continuous phase space. The discrete phase space is mathematically constructs using Galois field or known as finite field. Thus, with finite set of elements, the phase space can be pictured by an array of $N \times N$ points. The geometry is like that of the ordinary phase plane where momentum represents the vertical axis and position represents the horizontal axis.

Intrigued by this development, it is interesting to see how far can the discrete phase space formalism be extended particularly beyond the examples have often been shown in the literature, and whether there are complications arising in the construction of higher dimensional discrete phase spaces. Throughout this research, the study has focused on explicit construction for three-qubit and two-qutrit systems. We have developed a program to compute the binary operations of the appropriate discrete field and have constructed accordingly a set of parallel lines (striations) in the discrete phase space for the *3*-qubit and *2*-qutrit systems that can lead to identifying the discrete Wigner function.

1.4 Objectives

The objectives of this study can be succintly posed as:

- To identify the discrete fields for the *3*-qubit and *2*-qutrit systems and develop a Mathematica program to compute their binary operations.
- To form the set of striations in the discrete phase space for *3*-qubit and *2*-qutrit systems.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Wigner function distribution is used to define the arbitrary state in quantum system. The function has the property that can determine the position and momentum variables of the state in quantum system simultaneously. Many researchers have proposed to generalize Wigner function in discrete phase space in order to determine the arbitrary state in finite dimensional quantum system.

In 1974, Buot apply a discrete Weyl transform to one-dimensional periodic lattice of N, where N is odd number. This application directly will generate a Wigner function defined on a phase space with $N \times N$ array of points.

Hannay and Berry in 1980 has directly adapted the continuous Wigner function to a periodic lattice. With that adaption, they defined discrete Wigner function on a $2N \times 2N$ phase space.

The discrete phase space represented by $2N \times 2N$ array of points for a system with N orthogonal states is the most famous version to define discrete Wigner function.

2.2 Discrete Phase Space Based on Finite Fields

A Wigner-function formulation of finite-state quantum was proposed by Wootters (1987). He presented the Wigner function in discrete phase space, where the phase space is a two-dimensional vector space over the finite field with N (must be a prime number) elements. The space is like ordinary Cartesian plane that can be pictured as an $N \times N$ array of point. Each point in phase space was labeled by a pair coordinates, each taking values in finite field (from 0 to $N-1$). He specified that, the Wigner function in discrete system must be closely analogous as continuous Wigner function. Therefore, he applied the basic laws of quantum mechanics to transform the function from the continuous to discrete system.

2.3 Qubits in Discrete Phase Space

The initial idea to describe 2-level states of quantum system using Wigner function was proposed by Feynman (1982). This idea correlated well with the idea of a qubit system, where a qubit is a unit of quantum computation and quantum information that has 2-level state of quantum system. Wootters (2003) investigate Feynman idea's and extend it to any number of qubit system. He proposed to develop the phase space based on the finite field with 2^n elements. The discrete phase space that represented by $2^n \times 2^n$ array of points will perform as a medium to define discrete Wigner function. Besides that, this discrete Wigner function can act as a real function to define a quantum state of a system of *n* qubits in the phase space.

Later, Gibbons *et al.* (2004) describe the construction of discrete phase space of two-qubits system technically and proposed the notion of lines in this discrete space. They have used as much as the property in continuous phase space to apply in the discrete phase space that they proposed. They also investigated the physical interpretation in the discrete phase where they applied a pure quantum state to each line in space. This condition they called as quantum net. They notice perfect correlation of the sets parallel lines in phase space with a complete set of mutually unbiased bases. They defined the construction of the phase space such that it will generate complete sets of MUBs.

However, to date there are still having no evidence that discrete phase space has the same property with respect to the law of physics like continuous phase does. But the description of discrete phase space has been found useful in a variety of problem in quantum information.

2.4 Outlook & Motivation

None from the above literature highlighted or explicitly discuss the construction of discrete phase space of *3*-qubit and *2*-qutrit systems as the construction gets more difficult. It is also interesting to note that these systems will have direct usage in quantum information; for example a GHZ state is a 3-qubit state and qutrit entanglement requires at least two qutrits. In this research, we developed a program by using Mathematica software, to solve two binary operations in order to develop a discrete phase space for both systems. With the computation of the linear equation

$aq + bp = c$, we identify the set of parallel lines in the discrete phase space for both systems also.

CHAPTER 3

THEORY

3.1 Qubit and Qutrit

Earlier in Chapter 1, we have introduced qubit as the state of a two-level quantum system, which is the simplest. The next simplest system will be a three-level system whose states we called qutrits. Similar to the qubit, a qutrit is analogous to the unit of classical information, “trit”. The basis states of a qutrit is denoted by $|0\rangle$, $|1\rangle$ and $|2\rangle$. The general qutrit state is a superposition of these three basis states given by

$$|\lambda\rangle = a|0\rangle + b|1\rangle + c|2\rangle, \qquad a,b,c \in \mathbb{C} \tag{3.1.1}$$

One could generalize this further to a *d*-level system, where the states are generally known as qudits but our interest here will be limited to qubits and qutrits. We would however consider higher-dimensional systems by combining a few qubits or qutrits. The total Hilbert space will be the tensor product of the Hilbert spaces of the individual qubit or qutrit. For example, a two-qubit system will be described by a tensor product of two two-dimensional Hilbert spaces giving a total Hilbert space of dimension four.

While states of (multiple) qubit(s) or qutrit(s) can be a superposition of the basis states, on measurement, only one of the basis states will be the output. The measurement values corresponding to eigenvalues of the basis states thus they pose as the candidate points of the discrete phase space we are looking for. Note however that these points are required to obey some algebraic properties just like the points of the usual phase space do.

The specific mathematical concept needed to construct the discrete phase space is that of Galois field or finite field. This concept required the number of the elements in finite field is a power of a prime. The dimension of the state space are thus given in this form, $N = 2^n$ and $N = 3^n$, where n represents the number of qubits and qutrits while 2 and 3 are prime numbers showing the system levels. Besides that, *n*-qubit and *n*-qutrit are able to represent 2^n and 3^n different basis states simultaneously. To systematically introduce these finite fields, we begin with the mathematical concept of rings, in which finite field share their same properties albeit with a further algebraic structure.

3.2 Rings

Ring is an algebraic structure with several operations with importance in introducing finite fields. The set of integers is the most familiar example that shares the same properties used in ring. Hence, the set all integers is a ring with usual definition of addition and multiplication. The following definition will formally define a ring.

Definition: The set *R* together with two binary operations $+$ and $\cdot$ (called addition and multiplication) is called a ring if the following axioms hold for every selection of elements $a, b, c \in R$ (McCoy & Janusz, 2001).

P_1: commutative law of addition

$a + b = b + a$

P_2: associative law of addition

$(a + b) + c = a + (b + c)$

P_3: Existence of a zero

There is an element $0 \in R$ such that $a + 0 = a$ for every $a \in R$

P_4: Existence of additive inverses

If $a \in R$ there exists an $x \in R$ such that $a + x = 0$

P_5: Associative law of multiplication

$(ab)c = a(bc)$

P_6: Distributive laws

$a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

On top of these, we could also have the following properties which are also obeyed by the ring of integers.

P_7: Commutative law of multiplication

$ab = ba$

P_8: Existence is an identity for multiplication

There is an element $e \in R$ such that $ea = ae = a$ for all $a \in R$

However, the set *R* is not required to have either of the properties P_7 and P_8 to be a ring. Without these two properties the set *R* can still be identified as a ring, but later these two properties are important in determining the concept of a field. A ring R that has the multiplication property P$_7$ is called a commutative ring.

3.3 Finite Field/Galois Field

Generally, a commutative ring F is said to be a field if every nonzero element of F has a multiplicative inverse in F. Like a ring, a set F of field is closed under the addition and multiplication operations and it also satisfies the axioms P$_1$ – P$_8$

The familiar examples of a field is the field of real numbers $\mathbb{R}$, the field of rational numbers $\mathbb{Q}$, and the field of complex numbers $\mathbb{C}$. These types of field have infinite number of elements. However, it is possible for a field to have a finite number of elements and such a field is called finite field.

In honor of the founder of finite field theory Évariste Galois, the finite field also called Galois field. There exists a finite field F of order N *if* and only if p is a prime power, $N = p^n$ where prime number p called the characteristic of F and n is a positive integer. If $n = 1$, then F is called a prime field. If $n > 1$, then F is called an extension field. The order of a finite field is the number of elements in that field.

For any prime power N, there is essentially only one finite field of order N, which means that any two finite fields of order N are structurally the same except that the