Project Number: PH-PKA-SH05

The Discrete Wigner Function Formulation of Quantum Bits and Its Applications

A Major Qualifying Project Report

Submitted to the Faculty

of the

WORCESTER POLYTECHNIC INSTITUTE

In partial fulfillment of the requirements for the

Degree of Bachelor of Science

by

Michael Holmes

and

Warren Schudy

April 26, 2005

APPROVED:

1. Discrete Wigner Function
2. Quantum Computation
3. Quantum Tomography

Professor Padmanabhan K. Aravind,
Major Advisor

Abstract

Wigner (1932) showed how to introduce a phase space distribution of quantum systems possessing one or more continuous degrees of freedom. Gibbons *et. al.* (2004) [4] developed a discrete version of the Wigner function which is used to describe systems with discrete coordinates, such as systems of qubits. The discrete version for a single qubit uses a phase space based on the eigenvalues of the Pauli Z and X operators. For n qubits, the phase space is a $2^n \times 2^n$ grid. Lines in phase space are defined by the arithmetic of Galois Fields. The association of lines with eigenstates of observables is partly arbitrary, with different choices corresponding to different *quantum nets*.

We discuss how two 1-qubit discrete Wigner functions can be combined to form a single 2-qubit discrete Wigner function (DWF). If the 1-qubit DWFs use different quantum nets, a straightforward direct product produces the 2-qubit DWF. We discuss several open questions regarding combining DWFs that are important for applications.

Arbitrary quantum computations can be built using single-qubit rotations and the controlled-not gate. Arbitrary rotation matrices which can be applied to the single qubit DWF are developed. We give formulae for the effects of simple quantum gates on 2-qubit Wigner functions. Applications of the DWF to quantum state reconstruction and superdense coding are also discussed.

Acknowledgements

The authors would like to thank the project advisor, P.K. Aravind, for his excellent support. This project would not have been possible without the paper by Gibbons, Hoffman and Wootters [4] upon which most of Chapter 3 is based. We would also like to thank each other for putting up with each others' quirks and warts.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In 1932 E.P. Wigner introduced a phase space description of quantum systems, now known as the Wigner function. The Wigner function is a real function defined on the phase space of one or more particles that gives the probability of finding the particle(s) to have each combination of position and momentum – but these *quasi-probabilities* can be negative! A comprehensive review of the Wigner function and its applications may be found in the article by Hillery *et. al.* [6]. In 1982 Feynman [3] used a form of the Wigner function to describe a 2-state system (qubit). Recently, Wootters [11] extended Feynman's idea and developed a discrete phase space analog of the Wigner function for any number of qubits. Gibbons, Hoffman and Wootters (2004) [4] give a formal treatment of the discrete Wigner function.

The discrete Wigner function (DWF) representation of quantum states is based on a finite phase space and therefore uses a finite set of real elements to describe a state. Quantum bits, or qubits, are 2-state quantum systems and form the basis of quantum computation and quantum information. One may represent systems of any number of qubits using the discrete Wigner function. In this work we follow the approach of Wootters [11] and Gibbons *et. al.* [4] who develop a formal description of qubits using the discrete Wigner function.

Gibbons *et. al.* [4] define the DWF for a single qubit on a discrete phase space grid with 2×2 points. For higher dimensional systems of qubits the phase space has $2^n \times 2^n$ points, where n is the number of qubits. The phase space is described mathematically using Galois fields. Physically measurable probabilities may be found using a DWF by summing over lines in the phase space. Lines are associated with eigenstates of measurable operators. There are $2^n + 1$ sets of lines,

with 2^n lines in each set.

An important problem in quantum mechanics and quantum information theory is the determination of an unknown quantum state from measurements on many identical copies of the state. This problem is sometimes called *state reconstruction* or *quantum tomography*. One challenge in quantum tomography is the selection of a set of measurements to make on the copies that provide a reliable estimate of the quantum state with the minimum number of measurements. The Wigner function is a useful tool for solving state reconstruction problems. Quantum tomography has been experimentally verified for a single mode of the quantized electromagnetic field in a cavity, a system with one continuous degree of freedom. Certain measurements have been developed that give probabilities of finding the system in strips in phase space at arbitrary orientations, from which the Wigner function can be found. The book by Leonhardt [8] gives theoretical and experimental details. Wootters [11] and Gibbons *et. al.* [4] developed a discrete version of the continuous Wigner function for modeling systems of qubits. This report focuses on the DWF.

Recently many works have focused on the application of the DWF to problems in quantum information theory. The DWF has been used to analyze quantum teleportation in arbitrary dimensions and in the continuous limit by Koniorczyk *et. al.* [7]. Paz *et. al.* [10] used the DWF in the analysis of error correction and state retrodiction for up to 3 qubits. It is hoped that the DWF will lead to useful visualizations and insights involving quantum computations. The field of quantum information theory is still very active, and these hopes have yet to be fully realized.

The report is arranged as follows:

Chapter 2 introduces the necessary quantum mechanics needed to understand qubits. The continuous Wigner function is described; many of its properties carry over to the discrete version. The chapter concludes with an informal description of the 1-qubit discrete Wigner function motivated by analogy to the continuous Wigner function.

Chapter 3 gives a formal description of the discrete Wigner function following the work of Gibbons *et. al.* [4]. The necessary mathematics of Galois fields are discussed, along with the application of Galois fields to the discrete phase space. The theoretical framework connecting the phase space based on Galois Fields to the quantum systems of qubits is then developed, with examples of 1- and 2-qubit

DWFs. The connection between the discrete phase space and quantum systems is used to develop the discrete Wigner function rigorously. Finally, we present an alternative construction for the 2-qubit DWF.

Chapter 4 discusses the interesting problem of converting two 1-qubit DWFs into one 2-qubit DWF and vice versa. We discuss how a naïve formula for combining two 1-qubit DWFs does not work. We then present a modified formula which does work for certain quantum nets. We also discuss the reduction of Wigner functions analogous to the partial trace of density matrices.

Chapter 5 contains applications of the DWF. Formulae for arbitrary rotations of a 1-qubit DWF are derived. We present formulae for the effect of simple unitary operators (quantum gates) on the 2-qubit DWF. We discuss how the discrete Wigner function can be used to obtain a solution to the problem of state reconstruction in quantum tomography. Finally, the quantum communication protocol *superdense coding* is illustrated using the DWF.

Chapter 2

Basics of Qubits and the Wigner Function

This chapter describes qubits and introduces the Wigner function. We will discuss a few equivalent ways of representing a qubit including the familiar state vector notation, the pseudospin vector, and the density operator formulation. The continuous Wigner function is discussed, those properties of it being highlighted that are necessary for understanding the discrete version. We end the chapter with a pedagogic discussion of the single qubit discrete Wigner function. A formal discussion of the discrete Wigner function follows in Ch. 3.

2.1 Bloch Sphere Description of 1 qubit

A quantum bit (qubit) is any two-state quantum system. Examples of 2-state quantum systems include a spin $\frac{1}{2}$ particle, the horizontal and vertical polarizations of a photon and the ground and first excited state of an electron in an atom. A general state of a qubit is expressed as a superposition of the orthonormal standard basis states, $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{2.1}$$

where a and b are complex numbers. 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 $|1\rangle$ state, respectively. The ability of a qubit to be a linear combination, or superposition, of states allows it to be much more versatile than a classical bit.

Equation (2.1) may be rewritten in the form

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{2.2}$$

where the normalization of the state is guaranteed by $\cos^2 + \sin^2 = 1$. The angles θ and ϕ represent the state of the qubit by a point on the surface of a unit sphere known as the Bloch sphere. The state in Eqn (2.2) represents a spin-half particle whose spin is definitely up along the direction θ, ϕ. For example, the pure state $|\psi\rangle = \frac{1}{2}|0\rangle + i\frac{\sqrt{3}}{2}|1\rangle$ is definitely spin-up along the direction defined by $\theta = \frac{2\pi}{3}$ and $\phi = \frac{\pi}{2}$.

The standard observables for a qubit are the usual Pauli operators (or matrices). They are Hermitian and thus represent observables. We write the Pauli matrices as

$$X \equiv \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y \equiv \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z \equiv \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.3}$$

The eigenvalues of each Pauli operator are +1 and -1. The standard basis kets $|0\rangle$ and $|1\rangle$ are the eigenvectors of the Z operator. To emphasize the connection with the Z operator, we sometimes denote $|0\rangle$ by $|\uparrow\rangle$ and $|1\rangle$ by $|\downarrow\rangle$. Basis vectors span the space and therefore one may write the eigenvectors of X and Y as linear combinations of $|0\rangle$ and $|1\rangle$. The eigenvectors of X are $|x_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|x_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$; the subscripts of + and - denote the eigenvalue signature. Similarly, the eigenvectors of Y may be written as $|y_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|y_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$.

The X, Y and Z bases have the property that if a qubit is in an eigenstate of one basis and is projected onto another basis, the probability of finding it to be either up or down is $\frac{1}{2}$. Such a set of bases is termed *mutually unbiased*. This can be usefully generalized to any number of dimensions. A set of bases in a N-dimensional Hilbert space is mutually unbiased if each basis is orthonormal and for any $|\psi_i\rangle$ and $|\phi_j\rangle$ from *different* bases, $|\langle\psi_i|\phi_j\rangle|^2 = \frac{1}{N}$. The discrete Wigner function is based on mutually unbiased bases.

The Pauli matrices may be written in a more compact form if we let $\vec{\sigma} = (X, Y, Z)$. This simpler form allows one to write the following identity for vectors

$\vec{a}$ and $\vec{b}$ (whose components are complex numbers and not operators)

$$(\vec{\sigma}\cdot\vec{a})(\vec{\sigma}\cdot\vec{b}) = \vec{a}\cdot\vec{b}I + i(\vec{a}\times\vec{b})\cdot\vec{\sigma} \tag{2.4}$$

where I is the identity matrix. A useful property is that one may express any general Hermitian operator (observable) A as a linear combination $A = aI + bX + cY + dZ$ of the Pauli operators and the identity I, with real coefficients a, b, c and d.

The Pauli operators can also be defined by the way they act on the vectors of the standard basis:

$$\begin{aligned} Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle; \qquad X|0\rangle = |1\rangle, X|1\rangle = |0\rangle; \\ Y|0\rangle = i|1\rangle, Y|1\rangle = -i|0\rangle \end{aligned} \tag{2.5}$$

The Z operator is often called the phase-flip operator, since it leaves the magnitude of the coefficients in front of $|0\rangle$ and $|1\rangle$ unchanged but changes the sign (phase) in front of the $|1\rangle$ term. The X operator is often called the bit-flip operator, since it swaps $|0\rangle$ and $|1\rangle$. The Y operator is a combination of the previous two, since $Y = iXZ$. One may also express the Pauli operators in outer product form:

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| \qquad Y = i|1\rangle\langle 0| - i|0\rangle\langle 1| \qquad Z = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{2.6}$$

The Hermitian operator $\vec{\sigma}\cdot\hat{n}$ represents the spin of a spin $\frac{1}{2}$ particle along the $\hat{n}$ direction. Using the Bloch sphere description for a qubit, the direction of the unit vector $\hat{n}$ is specified by the spherical angles (θ, ϕ). One may now confirm that the state in Eqn (2.2) is an eigenstate of $\vec{\sigma}\cdot\hat{n}$ with eigenvalue $+1$ and so represents a spin up state along θ, ϕ. The orthogonal eigenstate of $\vec{\sigma}\cdot\hat{n}$ has eigenvalue -1 and is represented by the unit vector that points in the opposite direction of $\hat{n}$. One may see this by replacing (θ, ϕ) by $(\pi - \theta, \phi + \pi)$ and checking that the two states are orthogonal. Alternatively, one may verify that the new state is an eigenvector of $\vec{\sigma}\cdot\hat{n}$ with eigenvalue -1.

2.1.1 Density Operator

A very useful and important way of representing the state of a qubit is by using the density operator. For a 2-level pure state $|\psi\rangle$ (pure states are discussed below),

the density operator ρ is defined as

$$\rho = |\psi\rangle\langle\psi| \tag{2.7}$$

Let us take $|\psi\rangle$ to be given by Eqn (2.2). Using Eqn (2.6), the completeness relation for a 2-level system, $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, and Eqn (2.7), one finds that ρ takes the following form

$$\rho = \frac{1}{2}(I + \vec{s}\cdot\vec{\sigma}) \tag{2.8}$$

where $\vec{s} = (\sin(\theta)\cos(\phi), \sin(\theta)\sin(\phi), \cos(\theta))$ is the *pseudospin vector*. This vector completely describes the state of the qubit.

A generalization of quantum states, called mixed states, is often useful. In the context of mixed states, the ordinary quantum states described previously in this report, or in elementary quantum mechanics, are called pure states. A pure state is one in which there is a direction along which the probability of finding the spin of the qubit to be up is equal to 1. Elementary quantum mechanics deals exclusively with pure states. A *mixed* state is one in which the state of the qubit is not completely known, that is, there is no direction in space along which spin of the qubit is definitely up. A mixed state has definite probabilities of being in some mixture of pure states $|\psi_i\rangle$, with corresponding probabilities p_i that sum to unity. Therefore, one may write the density operator in more general terms, that incorporates both mixed and pure states, as a weighted sum of pure states $|\psi_i\rangle$ with probabilities p_i as their weighting factors

$$\rho = \sum_{i=1}^{n} p_i \, |\psi_i\rangle \, \langle\psi_i| \tag{2.9}$$

There is no requirement that the $|\psi_i\rangle$ be orthogonal, so the number of states being mixed can exceed the dimensionality of the Hilbert space (2 for qubits). The reader should be aware that the probabilities involved here are not the same as the ordinary quantum mechanical probabilities. A system with a 50% probability of being in the up or down along Z eigenstates is entirely different from a system in the $|X_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ eigenstate.

Using Eqn (2.8) for the density operators of the pure states $|\psi_i\rangle$ in Eqn (2.9), one may express the pseudospin vector of a mixture as a weighted sum of the

pseudospin vectors for the pure states

$$\vec{s}_{mix} = \sum_i p_i \vec{s}_i \tag{2.10}$$

with weights p_i for each pure state pseudospin vector $\vec{s}_i$. A mixed state pseudospin vector has less than unit length, whereas a pure state pseudospin vector has unit length. This is easily verified by finding the norm of Eqn (2.10), since the p_is are all less than 1, and sum to unity for a mixed state. Also note that a completely mixed state has a pseudospin vector of length 0; it is at the origin of the Bloch sphere with a density matrix of $\rho = I/2$.

Representing a point on the interior of the Bloch sphere may be done in an infinite number of ways, using any number of unit vectors with the appropriate weighing factors. This means that Eqn (2.10) is not a unique representation of a mixed state. Typically one uses the simpler method of writing the mixed state pseudospin vector in terms of a pair of orthogonal states whose pseudospin vectors are parallel (one parallel, one anti-parallel) to the mixed states pseudospin vector, denoted $\vec{s}$. If the pseudospin vector directed parallel to $\vec{s}$ is $\vec{s}_1$ with probability p, then the pseudospin vector of the orthogonal state is directed along $-\vec{s}_1$ with probability $(1-p)$. The pseudospin vector of the mixture may then be written as

$$\vec{s} = p\vec{s}_1 - (1-p)\vec{s}_1 = (2p-1)\vec{s}_1 \tag{2.11}$$

with $p \geq \frac{1}{2}$. Geometrically, Eqn (2.11) corresponds to representing the mixed state pseudospin vector as a weighted sum of two orthogonal states which correspond to diametrically opposite points on the Bloch sphere. These orthogonal states are weighted by probabilities $(1+s)/2$ and $(1-s)/2$, where s is the length of the mixed state pseudospin vector.

Alternatively, the form of Eqn (2.9) is reminiscent of an eigenvalue expansion of ρ, except that the $|\psi_i\rangle$ need not be orthogonal. Any density operator can be diagonalized, determining two pure states that can be mixed to form a particular density operator.

As previously noted, the density operator is another way of representing a quantum state. The following properties of density operators are useful:

1. ρ is Hermitian
2. $\mathrm{Tr}(\rho) = 1$, normalization

3. $\mathrm{Tr}(\rho^2) \leq 1$, equal only for pure states
4. ρ has eigenvalues λ_i, such that $0 \leq \lambda_i \leq 1$ and $\sum_{i=1}^{n} \lambda_i = 1$. The eigenvalues correspond to the probability weight associated with the expansion of the mixed states in terms of orthogonal pure states.
5. The expectation of an observable A in the state ρ is $\langle A \rangle = \mathrm{Tr}(\rho A)$
6. For a unitary transformation U such that $|\psi'\rangle = U|\psi\rangle$, $\rho' = U\rho U^\dagger$

All of the above properties for a 2-level system follow from Eqn (2.9). Alternatively, one may use the pseudospin vector to verify the above properties. From Eqn (2.8), one immediately sees that property 1 is true, as must be the case as it represents an observable quantity. Property 2 follows directly from Eqn (2.8), while properties 3 and 4 are both satisfied as a consequence of the fact that the pseudospin vector has a length on the interval $0 \leq |\vec{s}| \leq 1$. Property 4 is also satisfied directly by property 3, since the eigenvalues λ_i are equivalent to the probabilities p_i in Eqn (2.9). As previously noted, a general observable may be written as a linear combination of the identity and the Pauli matrices, thus one may express a general observable A as $A = aI + \vec{b}\cdot\vec{\sigma}$, where a is a real scalar and $\vec{b}$ is a real vector. From this and by using property 5, one has $\langle A \rangle = \mathrm{Tr}(\rho A) = a + \vec{b}\cdot\vec{s}$. The last property follows for pure states from the definition of the density operator in Eqn (2.7) and for mixed states from Eqn (2.9) and linearity arguments.

Property 6 can also be considered in light of the pseudospin vector. From [9], a general unitary operator is defined with parameters the unit vector $\hat{n}$ and the angle θ as

$$U = e^{-i\hat{n}\cdot\vec{\sigma}\frac{\theta}{2}} = \cos\left(\frac{\theta}{2}\right) - i(\hat{n}\cdot\vec{\sigma})\sin\left(\frac{\theta}{2}\right) \tag{2.12}$$

with the last equality in Eqn (2.12) following from expansion of the exponential as a power series. When one operates on a state described by the pseudospin vector $\vec{s}$, the new pseudospin vector $\vec{s}'$ is found to be

$$\vec{s}' = (\hat{n}\cdot\vec{s})\hat{n} + [\vec{s} - (\hat{n}\cdot\vec{s})\hat{n}]\cos\theta + (\hat{n}\times\vec{s})\sin\theta \tag{2.13}$$

where we have used property 6 that says $\rho' = U\rho U^\dagger$ along with Eqn (2.12) and Eqn (2.4). Equation (2.13) then relates the pseudospin vector $\vec{s}' = \mathrm{Tr}(\rho'\vec{\sigma})$ to the old one $\vec{s} = \mathrm{Tr}(\rho\vec{\sigma})$, where we have used property 5 to write the pseudospin vectors. There is a nice geometrical interpretation to Eqn (2.13), that the $\vec{s}'$ is obtained by rotating $\vec{s}$ in a positive sense (counterclockwise) about the unit vector

$\hat{n}$ by the angle θ. The derivation of Eqn (2.13) demonstrates the homomorphism between SU(2) and SO(3) by showing how the unitary transformation $U(\hat{n}, \theta)$ in the 2-dimensional complex space leads to a rotation in a 3-dimensional real space [5]. The mapping is homomorphic since the two distinct unitary operators $U(\hat{n}, \theta)$ and $U(\hat{n}, \theta + 2\pi)$ are negatives of each other, but both map onto the same rotation in 3-dimensional real space.

Now that we have a good understanding of the standard quantum mechanical description of qubits, we may proceed to the Wigner function formulation of qubits in phase space.

2.2 Continuous Wigner Function

The quantum state of a moving particle subject to a position-dependent force can be represented by a weighted sum of eigenkets in many different bases, including position, momentum, or energy. In 1932, E.P. Wigner [6] introduced a formulation of a quantum state that puts position and momentum on an equal footing, as in a Hamiltonian phase space. Unlike a classical system, a quantum system in phase space cannot have definite simultaneous eigenstates for position and momentum since the operators do not commute. Therefore, a delta-function like Wigner function that is large in one neighborhood and zero elsewhere is not physically possible.

The Wigner function is designed so that when it is integrated between parallel lines in phase space associated with the position operator $\hat{q}$ or momentum operator $\hat{p}$, the result is the probability of measuring the corresponding observable to have the corresponding range of eigenvalues. For a particle moving in one dimension the continuous Wigner function is defined as:

$$\mathrm{W}(x, p) = \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{(i\,p\,r)}\, \psi(x - \frac{r}{2})\, \psi^*(x + \frac{r}{2})\, \mathrm{d}r \tag{2.14}$$

where q and p are the particle's position and momentum, r is a dummy variable of integration and ψ is the particle's position wave function. The Wigner function is normalized, giving unity when integrated over all q and p. Unlike a ordinary probability distribution, W(q, p) can take positive and negative values, and is therefore known as a quasi-probability function. Having negative probabilities seems counter-intuitive, but the negative probabilities arise in intermediate steps;

the final answers are always positive and less than or equal to 1 as probabilities should be. Feynman [3] discusses negative probabilities in his 1982 article in which he introduces an analog of the Wigner function to describe a 2-state system. When integrated over the momentum, $\mathrm{W}(q,p)$ gives the probability that the particle is at q. Likewise, when integrated over position $\mathrm{W}(q,p)$ gives the probability of the particle having momentum p. Fortunately, these and all other measurable probabilities are positive.

$$\int_{-\infty}^{\infty} \mathrm{W}(q,p)\,\mathrm{d}x = |\psi(p)|^2 \qquad \int_{-\infty}^{\infty} \mathrm{W}(q,p)\,\mathrm{d}p = |\psi(x)|^2 \tag{2.15}$$

One may also integrate an area between parallel lines in phase space. Two parallel lines in the phase space may be described by the linear equations $aq+bp=c$ and $aq+bp=d$, where a, b, c and d are real constants. When integrated over the infinite strip between these two parallel lines in phase space, the Wigner function gives the probability of measuring the operator $a\hat{q}+b\hat{p}$ to be between c and d. Wootters [11] also gives an important property of the Wigner function, the property of translational covariance. An analogous property plays an important role in the development of the discrete Wigner function. A state $|\psi\rangle$ that undergoes a unitary transformation U in which the systems position is translated by an amount q_0 and its momentum is shifted by p_0 is represented by $|\psi'\rangle = U|\psi\rangle$. Translational covariance requires that the Wigner function of $|\psi'\rangle$, W', be equivalent to the Wigner function of the translated coordinates

$$\mathrm{W}'(q,p) = \mathrm{W}(q-q_0, p-p_0) \tag{2.16}$$

It can be shown that the definition of the continuous Wigner function given here is, in fact, translationally covariant.

2.3 1-Qubit Discrete Wigner Function

This section introduces and motivates the discrete Wigner function, or DWF, for 1 qubit. We take a qualitative approach to favor readability and intuition; a rigorous discussion of DWFs for any number of qubits follows in the next chapter. To introduce the DWF, we consider several properties of the continuous WF that the discrete version must have: non-commuting operators, normalization, and the correspondence of measurements to sums over lines.

The continuous Wigner function exists in a phase space comprised of the non-commuting observables position $\hat{q}$ and momentum $\hat{p}$. For the discrete version, we base our phase space on two non-commuting observables, the Pauli X and Z operators. The horizontal axis of the continuous Wigner function is labeled with different eigenvalues of the position operator. For the DWF, the horizontal axis is labeled by eigenvalues of the Z operator. Similarly, the vertical axis is labeled by the $\hat{p}$ operator in the continuous case and the X operator in the discrete case. Since the Pauli operators have only 2 eigenvalues instead of an infinite number, the resulting phase space is a 2×2 grid instead of a continuous 2-dimensional space. In the continuous case, the probability of measuring a certain position is equal to the integral over a column in phase space. In the discrete case, the probability of measuring the particle to be spin up or spin down along the z-axis is equal to the sum of the Wigner function over the corresponding column. Sums along rows correspond to momentum probabilities in the continuous case and x-component spin measurements in the discrete case. We adapt the convention of labeling the eigenvalues corresponding to the vertical and horizontal as: $+1$ eigenvalue of Z is $\uparrow$, the -1 eigenvalue of Z is $\downarrow$, $+1$ eigenvalue of X is $\rightarrow$ and the -1 eigenvalue of X is $\leftarrow$. The phase space is shown below in Fig 2.1.

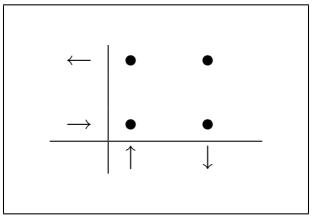

Figure 2.1: 1-qubit eigenstate assignments of the X and Z operators.

We continue to the next property the discrete Wigner function should have: normalization. In the continuous case, the double integral of the Wigner function over the phase space must be unity. We require the discrete Wigner function to have an analogous property: the double sum over the Wigner function must be unity. In other words the sum over all Wigner elements must be unity, where the Wigner elements are the (real) values assumed at each of the points in phase space by a quantum state.

As an example, the 1-qubit Wigner function for a particle spin down along X is shown in Fig 2.2. The reader should verify that the sums along rows and columns for the example Wigner functions are the expected ones for a particle that is spin

down along the x-axis. Also note that summing all the elements gives unity, as required by the normalization condition.

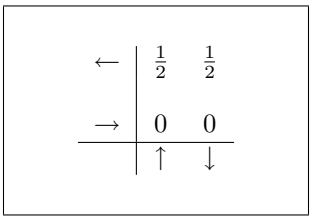

Figure 2.2: Wigner function for spin down along X.

Having discussed the probabilities of measuring eigenvalues of Z and X, it is natural to ask about Y. To motivate the solution, consider another property of the continuous Wigner function. When the Wigner function is integrated over a line in phase space $aq + bp = c$, the result is the probability density of measuring the observable $a\hat{q} + b\hat{p}$ to have eigenvalue c. There are two obvious lines in our phase space we have yet to consider: the two diagonals. In the discrete case the operator that is associated with the diagonals is not $Z + X$, but rather $ZX = iY$. In a later chapter, we develop a formalism that finds the operators that correspond to each line algorithmically.

An obvious question remains: which diagonal should be assigned to Y-up, and which to Y-down? There is no unique way to answer this question. We will arbitrarily assign the state $|y+\rangle$ to the diagonal line which contains the origin (0,0); the remaining state $|y-\rangle$ is assigned to the other diagonal line. Understanding how rotations in real 3-dimensional space act to shift the elements in the phase space will allow us to verify this assignment. A rotation acts to shift the DWF elements so as to correspond to measurements made to the rotated state. A rotation of π about z-axis will exchange the probabilities of measuring X and Y while leaving the Z measurement unchanged. In terms of the DWF elements, this rotation can be modeled by exchanging the two rows of the DWF, whereby exchanging the measurement probabilities of X and Y and leaving the Z measurement unchanged. The assignment of the diagonals to the Y basis can be shown to be consistent with rotations about the X and Z axes. This construction therefore strongly suggests the assignment to be correct.

The last property of the continuous Wigner function that should be extended to the discrete version is translational covariance. The unitary operator Z is associated with a vertical translation in the discrete phase space, analogous to the

unitary operator $e^{-\frac{i}{\hbar}p_0\hat{q}}$ for the continuous Wigner function. The X operator is associated with horizontal translations. Chapter 3 discusses translational covariance in great detail.

The 2×2 phase space contains 6 lines, which correspond to measuring the 6 eigenstates of the Pauli operators. These lines may be grouped into 3 sets of 2 lines each that correspond to the eigenstates of one of the Pauli operators. Each set of lines is known as a *striation*, with the 3 striations containing all 6 lines in the phase space given in Fig 2.3. When we develop the formalism in following chapters, these lines will be given in a more rigorous way. For now the figure just serves to give the lines that when summed along, give corresponding measurement probabilities.

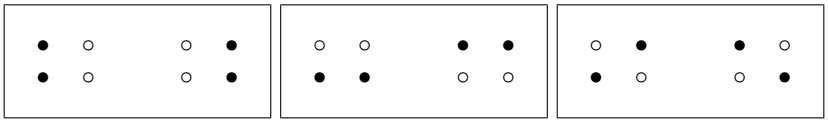

Figure 2.3: 1-Qubit Striation Diagrams. Each box contains a striation set. The associated bases from left to right for each striation are Z, X, and Y

The DWF gives a complete description of a qubit, and is used in tomography. Making measurements with the 3 Pauli operators, X, Y, and Z, is adequate to obtain a complete description of a qubit. This is because the Pauli operators constitute a complete and minimal set of observables for a qubit. This means that leaving one measurement out will not give enough information to specify the state, while measuring with all of them will completely determine the state. These operators are also all mutually conjugate with their eigenstates forming a set of mutually unbiased bases, where making a measurement of any eigenstate with respect to another basis will return a value of $\frac{1}{2}$. For example, if a system is prepared in the up along z state, and one makes a measurement in the Y basis, one will get the probability of the system having spin up along y as $\frac{1}{2}$. Likewise, the probability of finding the system with spin down along y is $\frac{1}{2}$. Looking at Fig 2.2, one sees that the probabilities of finding the state in an eigenstate of Y or Z is $\frac{1}{2}$. The DWF thus expresses the mutually conjugate property of the Pauli bases nicely.

2.3.1 Mapping Between Pseudospin Vector and the DWF

Using the notion of striations, let us return to describing a state in phase space. We will now write down our form for the discrete Wigner function in matrix notation, with each element corresponding to a point in phase space. This is simply a compact way of displaying the Wigner function; matrix operations such as trace and multiplication do not give useful results. The Wigner matrix W is defined by

$$\mathrm{W} = \begin{pmatrix} w_{10} & w_{11} \\ w_{00} & w_{01} \end{pmatrix} \tag{2.17}$$

The elements in the Wigner matrix all have subscripts which denote spin orientations for the X and Z operators. An element is labeled with the subscripts with the convention w_{xz}, where the 0 denotes spin up and the 1 denotes spin down along the corresponding axis. This labeling is used for convenience.

Summing the entries of the W matrix gives unity, $1 = \sum_{i,j} w_{ij}$, which is the normalization requirement. Summing two of the entries in the matrix that define a line will give the probability of the measurement outcome associated with that line. An element of W represents a joint probability, for example the element w_{10} gives the joint probability of measuring the +1 eigenvalue for Z and -1 for X, but since these operators do not commute, one cannot have a definite value for this joint probability. Individual elements can be negative, but summing along any line will give legitimate probabilities, i.e. a value between 0 and 1. Summing along the columns gives the spin up and spin down probabilities along z, whereas summing along the rows gives the spin up and down probabilities along x. Summing along the diagonals gives the probabilities of measuring spin up and down along y. One may write the probabilities $P(i)$ associated with summing along each line as

$$\begin{aligned} P(x+) &= w_{00} + w_{01} & \qquad P(x-) &= w_{10} + w_{11} \\ P(z+) &= w_{00} + w_{10} & \qquad P(z-) &= w_{01} + w_{11} \\ P(y+) &= w_{00} + w_{11} & \qquad P(y-) &= w_{01} + w_{10} \end{aligned} \tag{2.18}$$

It is helpful to relate this to the pseudo-spin vector $\vec{s}$. Recall that this vector describes the direction of spin of the state and is defined as $\vec{s} = (s_x, s_y, s_z)$, where each component of $\vec{s}$ is the projection of $\vec{s}$ along its corresponding coordinate axis. Each component of the pseudo-spin vector may be expressed in terms of the

eigenvalues λ associated with the spin operators multiplied by the corresponding probability P of the state being in each eigenstate $|\lambda\rangle$. For example the s_i component ($i = x, y, z$) is given by:

$$s_i = (+1)P(i+) + (-1)P(i-) \tag{2.19}$$

since the Pauli matrices all have eigenvalues of $(+1)$ and (-1).

The components of $\vec{s}$ can be found using Eqn (2.18) and Eqn (2.19). The normalization condition that the elements in W sum to unity gives another relation. The normalization equation and the equations for the components of $\vec{s}$ may be cast as a matrix equation relating the pseudospin components to the matrix entries of W:

$$\begin{pmatrix} 1 \\ s_x \\ s_y \\ s_z \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \begin{pmatrix} w_{00} \\ w_{01} \\ w_{10} \\ w_{11} \end{pmatrix} \tag{2.20}$$

We label the vector containing the components of $\vec{s}$ and a 1 as $\vec{S}$, and term it the *density coefficient vector*. The $\vec{S}$ vector is just the components of the pseudospin vector, with the normalization of the Wigner elements also included. The column vector containing the Wigner elements will be denoted $\vec{W}$, as opposed to just W which will always be used to denote a Wigner matrix. The 4×4 matrix containing 1s and -1s is known as a Hadamard matrix, which has the property that any pair of rows or any pair of columns is orthogonal. Solving the above equation for the ws in terms of the components of $\vec{s}$, we arrive at the following relations:

$$\begin{aligned} w_{00} &= \frac{1}{4}(1 + s_x + s_y + s_z) \\ w_{01} &= \frac{1}{4}(1 + s_x - s_y - s_z) \\ w_{10} &= \frac{1}{4}(1 - s_x - s_y + s_z) \\ w_{11} &= \frac{1}{4}(1 - s_x + s_y - s_z) \end{aligned} \tag{2.21}$$

The above equations give the relation between the Wigner function elements and the pseudospin components. Using Eqn (2.21), we may find the discrete Wigner function if we know $\vec{s}$, or we may determine $\vec{s}$ from the discrete Wigner

function. Once the components of $\vec{s}$ are known, we may also determine the density operator. One may put Eqn (2.21) into Eqn (2.17) to write W explicitly in terms of the components of $\vec{s}$ as

$$\mathrm{W} = \frac{1}{4}\begin{pmatrix} 1 - s_x - s_y + s_z & 1 - s_x + s_y - s_z \\ 1 + s_x + s_y + s_z & 1 + s_x - s_y - s_z \end{pmatrix} \tag{2.22}$$

One may also rewrite the density operator $\rho = \frac{1}{2}(I + \vec{s}\cdot\vec{\sigma})$ in terms of w's by replacing the pseudospin components with their corresponding Wigner elements as

$$\rho = \begin{pmatrix} w_{00} + w_{10} & \frac{(-1+i)}{2}\alpha + \frac{(1+i)}{2}\beta \\ \frac{(-1-i)}{2}\alpha + \frac{(1-i)}{2}\beta & w_{01} + w_{11} \end{pmatrix} \tag{2.23}$$

where $\alpha \equiv -w_{00} + w_{10}$ and $\beta \equiv w_{01} - w_{11}$.

An Example

We illustrate the mapping from $\vec{s}$ the discrete Wigner function with an example. (The mapping from density matrices to the pseudo-spin vector can be found using $s_i = \mathrm{Tr}(\rho\sigma_i)$). Consider a particle prepared in the spin up state along y. The vector $\vec{s}$ then has components $s_y = 1$ and $s_x = s_z = 0$. Substituting this into Eqn (2.22), the W matrix is found to be

$$\mathrm{W} = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$$

By summing along the diagonal points starting at the bottom left, we can find the probability of finding the spin up along y. As the particle was prepared in this state, the probability is 1, as it should be. Also notice that the probabilities along the x and z directions give $\frac{1}{2}$ for up and down. This is in accordance with the Pauli operators being mutually unbiased. We may also map to the density operator for this state directly from the above W via Eqn (2.23) giving

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$$

which is the same as finding the density matrix for spin up along y using $\rho = |y+\rangle\langle y+|$, the example just illustrates how given a W, one may find a ρ. Now that we have ρ we can also find $\vec{s}$ using $s_i = \mathrm{Tr}(\rho\sigma_i)$ giving what we expect, that

$s_x = s_z = 0$ and $s_y = 1$.

2.3.2 One-Qubit Operations using the DWF

Using the DWF representation of a qubit, one may reformulate many useful operations from elementary quantum mechanics such as inner products, expectation values, and measurements.

Overlap of 2 States

The overlap of two arbitrary states $|\psi_1\rangle$ and $|\psi_2\rangle$, is denoted as $\langle\psi_1|\psi_2\rangle$. Representing the states as density matrices, $\rho_1 = |\psi_1\rangle\langle\psi_1|$ and $\rho_2 = |\psi_2\rangle\langle\psi_2|$, one can show that $\mathrm{Tr}(\rho_1\rho_2) = |\langle\psi_1|\psi_2\rangle|^2$. Writing the density matrices in terms of their respective pseudospin vectors, as in Eqn (2.8), $\vec{s}_1$ and $\vec{s}_2$, one can also show that $\mathrm{Tr}(\rho_1\rho_2) = \frac{1}{2}(1 + \vec{s}_1 \cdot \vec{s}_2)$. One may then use Eqn 2.20 to write the pseudospin vectors in terms of their respective DWF elements, along with the normalization condition for the Wigner elements. We let the Wigner elements for $\vec{s}_1$ and $\vec{s}_2$ be a_{ij} and b_{ij} respectively, with $(i, j = 0, 1)$. After some algebra one has the following relation:

$$|\langle\psi_1|\psi_2\rangle|^2 = 2\sum_{i,j} a_{ij}b_{ij} \tag{2.24}$$

This equation holds for states that may or may not be pure states. In Ch. 3, we prove a generalization of this for any number of qubits.

Expectation values

In terms of density matrices, the expectation value for an arbitrary observable A is given by $\langle A\rangle = \mathrm{Tr}(A\rho)$, where ρ is the state of interest. In order to express the expectation value of A in terms of DWF elements, we need to first consider the spectral decomposition of A, which is $A = \lambda_1|\psi_1\rangle\langle\psi_1| + \lambda_2|\psi_2\rangle\langle\psi_2| = \lambda_1\rho_1 + \lambda_2\rho_2$, with each term containing the eigenvalue (λ) and its corresponding eigenstate (ρ). Using the spectral decomposition and the linearity of the trace, one can represent A as

$$\langle A\rangle = \mathrm{Tr}A\rho = \lambda_1\mathrm{Tr}(\rho\rho_1) + \lambda_2\mathrm{Tr}(\rho\rho_2) \tag{2.25}$$

Labeling the elements of the DWFs for ρ, ρ_1, ρ_2 as a, b, and c, respectively, one may use Eqn (2.24) to find

$$\langle A \rangle = \lambda_1(2\sum_{i,j} a_{ij}b_{ij}) + \lambda_2(2\sum_{i,j} a_{ij}c_{ij}) = 2\sum_{i,j} a_{ij}A_{ij} \tag{2.26}$$

with $A_{ij} = \lambda_1 b_{ij} + \lambda_2 c_{ij}$ $(i, j = 0, 1)$. The A_{ij} is the Wigner representation of the observable A. Thus to find an expectation value using the DWF, first find the Wigner representation of the observable, then find the overlap of the observable with the state of interest.

Measurements

Projective measurements on quantum systems may be written in terms of density operators. For a measurement operator M_m, corresponding to measurement of state m, and an initial state ρ, the state after measurement ρ_m is defined as [9]

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\mathrm{Tr}(M_m^\dagger M_m \rho)} \tag{2.27}$$

where the denominator is the required normalization for the new state. One may also rewrite Eqn (2.27) in terms of the DWF. We can use Eqn (2.23) to express ρ in terms of its Wigner elements, and once the numerator is found, one may get the proper normalization using the normalization condition for DWFs $1 = \sum_{i,j} w_{ij}$, where the w_{ij} are the elements of the measured DWF. Unfortunately, the formula one arrives at is quite messy, and is best implemented using mathematical software, such as Maple.

Chapter 3

Formalism

This chapter introduces the discrete Wigner function for n-qubits in a rigorous fashion. To help illustrate the theory, examples with one and two qubits are provided. Appendix B discusses some examples of the theory for a 3-qubit system.

This chapter is based on Gibbons *et. al.* [4]. That paper covers a more general case (arbitrary prime powers, not just powers of 2), but given the central importance of qubits, we limit our discussion to qubits. We refer readers seeking the generalization to the paper by Gibbons *et. al.* [4].

3.1 Galois Fields

To extend the discrete Wigner function to 2-qubit systems, we need the notion of a line in phase space. In the continuous case, lines can be defined by $aq + bp = c$. To make this work for qubits, we need some sort of numbers to associate with the rows and columns of the phase space for a system of qubits. An obvious choice is arithmetic modulo 2^n, where n is the number of qubits. A few example lines in the 4×4 phase space modulo four are shown in Fig 3.1.

There is a big problem with defining lines this way: two distinct lines can intersect at more than one point! This would prevent us from associating lines with mutually unbiased bases. To discover what went wrong, consider the following proof that non-parallel lines in two real dimensions intersect at exactly one point. Consider two non-parallel non-vertical lines defined by $y = m_1 x + b_1$ and $y = m_2 x + b_2$. To find the point of intersection, simply subtract one equation from the other and solve for x, yielding $x = \frac{-b_1 - b_2}{m_1 - m_2}$. This gives the unique intersection point.

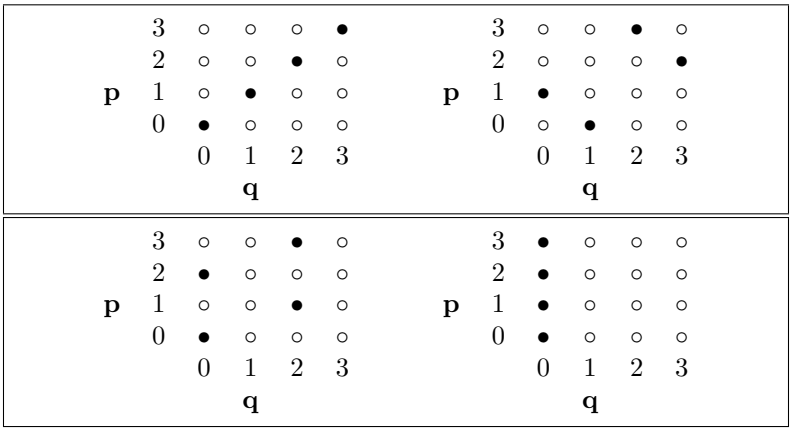

Figure 3.1: Some lines in arithmetic modulo 4. The horizontal axis is the q axis and the vertical axis is the p axis. From left to right and top to bottom the lines satisfy the equations $q - p = 0$, $q + p = 1$, $q + 2p = 0$, and $q = 0$. Note that the first two lines are not parallel yet do not intersect. The third and fourth lines are not parallel yet intersect at two points.

What went wrong with the modular case? There is no unique multiplicative inverse in arithmetic modulo 4, so the division in the above proof does not extend to the modular arithmetic case. What we need is a mathematical structure that satisfies the familiar properties of addition and multiplication, but has only 2^n elements. Such a structure is called a Galois Field, after its inventor. Here are the properties satisfied by all fields, including Galois Fields, where a, b, c are arbitrary elements of the field, and 0 and 1 are fixed additive and multiplicative identities respectively.

1. $a + 0 = a$ 0 is the additive identity
2. $1a = a$ 1 is the multiplicative identity
3. $a + (b + c) = (a + b) + c$ addition is associative
4. $a + b = b + a$ addition is commutative
5. $ab = ba$ multiplication is commutative
6. $a(bc) = (ab)c$ multiplication is associative
7. $a(b + c) = ab + ac$ addition distributes over multiplication
8. $a + (-a) = 0$ where $-a$ is additive inverse
9. $a * a^{-1} = 1 \quad a \neq 0$ where a^{-1} is multiplicative inverse

Examples of fields include the rationals, reals, and complex numbers. It turns out that one can construct fields over finite sets of objects, not just infinite ones.

However, such fields exist if and only if the number of objects is equal to a prime power: p^n, where p is prime and n is an integer. There is really only one distinct Galois field of any particular order, for it can be shown that all Galois fields of the same order are isomorphic to each other.

If the exponent n is 1, the Galois field is simply arithmetic modulo p. For higher exponents, the Galois fields (denoted $GF(N)$) are more complicated. The addition and multiplication tables for $GF(2)$ are defined in Table 3.1.

Phase space points used to define the discrete Wigner function are elements of a Galois Field. For a state space dimension $N = 2^n$, where n is the number of qubits, the phase space is defined on $GF(N)$, with elements of 0 and the $2^n - 1$ powers of a primitive element, which we take to be ω. The primitive element and its powers are solutions to the primitive polynomial, which is of degree n, and cannot be factored into a product of lesser degree polynomials using elements of the prime field.

A similar extension technique allows one to generalize the real numbers to complex numbers. One can define the complex numbers by introducing the primitive polynomial $x^2 + 1 = 0$, which cannot be solved with real numbers. The solution to this polynomial is defined to be the primitive element $i = \sqrt{-1}$.

The trace of any element within the field $GF(N)$ is defined as:

$$\mathrm{tr}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}} \tag{3.1}$$

To differentiate the Galois Field trace from the matrix trace, the former is denoted $\mathrm{tr}(x)$ with a lower-case t while the latter is denoted $\mathrm{Tr}(x)$ with an upper-case T. The trace is linear:

$$\mathrm{tr}(x + y) = \mathrm{tr}(x) + \mathrm{tr}(y) \tag{3.2}$$

since the expansion of $(x + y)^{2^i}$, contains the terms x^{2^i}, y^{2^i} and cross terms with an even coefficient in front and therefore equal to 0 mod 2. It can be shown that the trace is always a member of the primitive field $GF(p)$. In particular, when dealing with qubits, the trace is always either 0 or 1.

The basis of a field is a set of field elements: $E = \{e_1, e_2, \cdots, e_n\}$ such that any field element can be expressed as a linear combination of the basis:

$$x = \sum_i^n x_i e_i \tag{3.3}$$

The x_i are restricted to be elements of $GF(p)$ in general, or 0 or 1 for the $GF(2^n)$ we are concerned with when discussing qubits. For every field basis there exists a unique dual basis which is important for assigning bases for the horizontal and vertical directions in phase space. The unique dual basis $E' = \{e'_1, e'_2, \cdots, e'_n\}$ is defined by:

$$\mathrm{tr}(e'_i e_j) = \delta_{ij} \tag{3.4}$$

where δ_{ij} is the Kronecker delta.

The special case of one qubit ($n = 1$) is quite simple. $GF(2)$ is simply arithmetic modulo 2:

x	$\mathrm{tr}(x)$
0	0
1	1

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	1
1	1	1

Table 3.1: $GF(2)$ tables. These tables give the trace, addition and multiplication for $GF(2)$.

For $GF(2^2)$ the primitive polynomial is taken as: $\pi(x) = x^2 + x + 1$. The field elements are then: $GF(2^2)$=$\{0,1,\omega,\omega^2\}$. Note that $\omega^2 = -\omega - 1 = \omega + 1$, since $-1 = 1 \bmod 2$. Also note that $\omega^3 = 1$, which is useful when finding the trace. We arbitrarily choose the field basis $(\omega, 1)$ which has a unique dual of $(1, \omega^2)$. Arithmetic in $GF(4)$ is shown in Table 3.2. The addition and multiplication

n	ω^n	$\mathrm{tr}(\omega^n)$
0	1	0
1	ω	1
2	$\omega + 1$	1

$+$	0	1	ω	ω^2
0	0	1	ω	ω^2
1	1	0	ω^2	ω
ω	ω	ω^2	0	1
ω^2	ω^2	ω	1	0

$\times$	0	1	ω	ω^2
0	0	0	0	0
1	0	1	ω	ω^2
ω	0	ω	ω^2	1
ω^2	0	ω^2	1	ω

Table 3.2: $GF(4)$ tables. These tables give the trace, addition and multiplication for $GF(4)$.

tables for $GF(2^3)$ are given in Appendix B.

3.2 Lines in Discrete Phase Space

Now that we have defined Galois fields, we can use the equation for a line $ap+bq = c$ to generate lines in a phase space labeled by a Galois field. There are N vertical

lines which are solutions to the equation $q = c_i$. Non-vertical lines have $b \neq 0$, so we can without loss of generality choose $b = 1$, yielding $a_j q + 1p = c_i$. There are N possible values of a_j, and N possible values of c_i, resulting in N^2 non-vertical lines. Together with the vertical lines, there are $N^2 + N$ lines in $N + 1$ families of N parallel lines each. For lines in this discrete phase space we define two lines to be *parallel* if they do not intersect. Two different lines in the same family clearly cannot intersect, since otherwise $aq + bp = c_1$ and $aq + bp = c_2$, contradicting $c_1 \neq c_2$. Two lines from different families always intersect at exactly one point. Two lines of the form $a_j q + 1p = c_i$ and $a_k q + 1p = c_l$ intersect at $q = \frac{c_l - c_i}{a_k - a_j}$, which is well-defined since the lines are from different families so $a_k \neq a_j$.

Figures 3.2 and 3.3 show the family of striations for 1 and 2 qubits respectively.

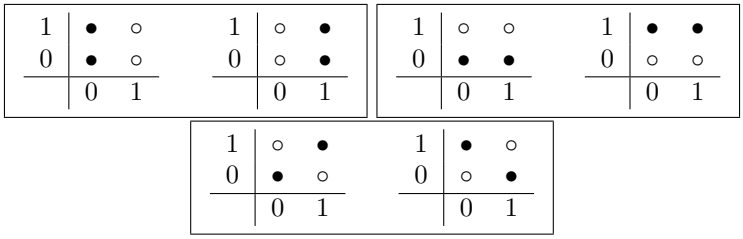

Figure 3.2: 1 Qubit Striation Diagrams. Each box contains a striation set. The associated bases from left to right for each striation are Z, X, and Y. The horizontal and vertical axes correspond to q and p respectively. The equations are $q = c$, $p = c$, and $p + q = c$ respectively, where $c \in \{0, 1\}$.

3.3 Translational Covariance and Quantum Nets

We begin the theoretical development of the n-qubit DWF, with $N = 2^n$ states. To connect the Galois field phase space to the world of qubits, we need to associate translations in the phase space labeled by Galois Field (GF) elements with unitary operators in the quantum world. A *translation vector* in the Galois world is a pair of GF elements $(\delta q, \delta p)$ that can be added to a point in GF phase space (q, p), yielding $(q + \delta q, p + \delta p)$. Given a basis E for q, and a basis F for p, one expands δq and δp in the basis, so $\delta q = \sum_{i=1}^{n} q_i e_i$ and $\delta p = \sum_{i=1}^{n} p_i f_i$. The *translation operator* corresponding to $(\delta q, \delta p)$, $T_{(\delta q, \delta p)}$, is defined by:

$$T_{(\delta q, \delta p)} = X^{q_1} Z^{p_1} \otimes X^{q_2} Z^{p_2} \cdots \otimes X^{q_n} Z^{p_n} \tag{3.5}$$

This equation satisfies a desirable property of a translation operator, in that

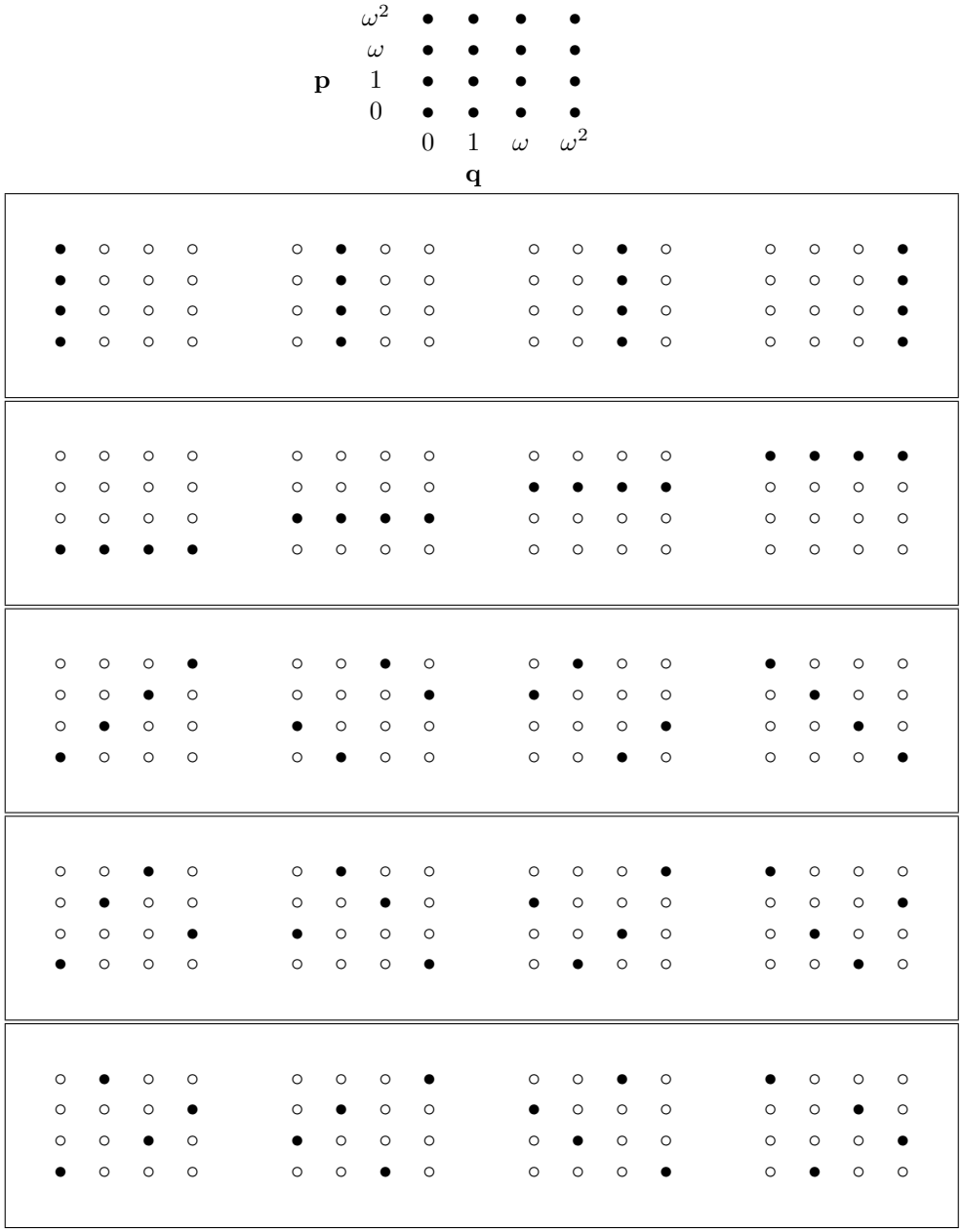

Figure 3.3: 2 Qubit Striation Diagrams. Each box contains a striation set. The equations are $q = c$, $p = c$, $p + q = c$, $\omega^2 p + q = c$, and $\omega p + q = c$ respectively, where $c \in \{0, 1, \omega, \omega^2\}$.

the translation operator corresponding to a sum of translation vectors is equal to the product of corresponding translation operators, up to an unimportant phase factor.

We will define the quantum state associated with each line, $|\lambda\rangle$, by insisting that the eigenstates associated with lines in phase space be translationally covariant:

$$|\lambda + (\delta q, \delta p)\rangle = e^{i\theta} T_{(\delta q, \delta p)} |\lambda\rangle \tag{3.6}$$

where θ is a real phase factor. $\lambda + (\delta q, \delta p)$ denotes the line λ with each point shifted by the translation vector $(\delta q, \delta p)$. T is the quantum-mechanical unitary operator that corresponds to $(\delta q, \delta p)$.

Alternatively, in operator form, with $Q(\lambda) \equiv |\lambda\rangle\langle\lambda|$:

$$Q(\lambda + (\delta q, \delta p)) = T_{(\delta q, \delta p)} Q(\lambda) T^{\dagger}_{(\delta q, \delta p)} \tag{3.7}$$

Gibbons *et. al.* [4] showed that the Galois Field bases for the two axes cannot be chosen independently. If the basis associated with the horizontal axis is taken as $E = \{e_1, e_2, \cdots, e_n\}$, then the basis associated with the vertical axis $F = \{f_1, f_2, \cdots, f_n\}$ must satisfy the following relation:

$$f_i = \alpha e'_i \tag{3.8}$$

where α is an element of $GF(N)$ and e'_i is the dual of e_i.

For each line, there are $N-1$ non-trivial translation vectors that leave the line unchanged. Using Eqn (3.6), we find:

$$|\lambda\rangle = e^{i\theta} T_{(\delta q, \delta p)} |\lambda\rangle \tag{3.9}$$

This is just an eigenvalue equation for $|\lambda\rangle$! The quantum mechanical translation operators corresponding to translation vectors that leave a line invariant commute (requiring this is what led to Eqn 3.8), so one can simultaneously diagonalize them. This gives the states that can be assigned to each striation.

Translational covariance does not, however, specify which eigenstate to assign to which line. It turns out that the choice of which eigenstate to assign to one of the lines in a striation is completely arbitrary, but translational covariance then determines the assignment of the remaining lines to the remaining eigenstates.

3.3.1 Example: 1 Qubit

For the case of $n = 1$, this theory becomes quite simple. Consider the family of vertical lines $q = c$. This has an associated invariance translation vector of $(0, 1)$. The corresponding translation operator is simply the Pauli Z operator. Therefore, the vertical lines are associated with Z-eigenstates. Similarly, horizontal lines are associated with X-eigenstates.

The diagonals are a bit more interesting. Both diagonal lines can be expressed in the form $q+p = c$, with associated invariance vector $(1, 1)$. Therefore, the translation operator is $XZ = -iY$, so the corresponding lines must be Y-eigenstates.

3.3.2 Example: 2 Qubits

Now we consider the case for $n = 2$. We choose for E the field basis $(e_1, e_2) = (\omega, 1)$ which has the dual basis $(e'_1, e'_2) = (1, \omega^2)$. Using Eqn (3.8) we can take $\alpha = \omega$ yielding $(f_1, f_2) = (\omega, 1)$. Now we may use Eqn (3.5) to determine which operators to associate with each striation. First let us give the invariance translation vectors for each striation set. The invariance translation vectors are given in Table 3.3 for the 5 striations for a system of 2-qubits. The invariance operators send points in a line in the striation into other points in the line.

Basis	Invariance Operators
0	$(0,1), (0,\omega), (0,\omega^2)$
1	$(1,0), (\omega,0), (\omega^2,0)$
2	$(1,1), (\omega,\omega), (\omega^2,\omega^2)$
3	$(1,\omega), (\omega,\omega^2), (\omega^2,1)$
4	$(1,\omega^2), (\omega,1), (\omega^2,\omega)$

Table 3.3: 2-Qubit Invariance Operators. The basis numbers correspond to the order of the striations in Fig 3.3.

We will discuss a few examples to make the use of Eqn (3.5) clear. In the following examples, we will find the invariance translation operators using the line that contains the point $(0, 0)$, and then see which translation vectors result in landing on points within the line, as one can see from Fig (3.3). For each example there will be three invariance vectors, since there are four points on a line, and we start at the origin.

Example: $q = c$

This first example is quite straightforward and instructive, and will display the method to be follow in the later examples. For this line the three invariance translation vectors corresponding to three separate vectors $(\delta q, \delta p)$ are $(0,1)$, $(0,\omega)$, $(0,\omega^2)$. Expanding each of these in terms of the basis and the dual we get $(0,1) = (0e_1 + 0e_2, 0f_1 + 1f_2)$, $(0,\omega) = (0e_1 + 0e_2, 1f_1 + 0f_2)$ and $(0,\omega^2) = (0e_1 + 0e_2, 1f_1 + 1f_2)$. For $GF(2^2)$, Eqn (3.5) becomes $T_{(\delta q,\delta p)} = X^{q_1}Z^{p_1} \otimes X^{q_2}Z^{p_2}$. We then have $T_{(0,1)} = X^0Z^0 \otimes X^0Z^1 = I \otimes Z$, $T_{(0,\omega)} = X^0Z^1 \otimes X^0Z^0 = Z \otimes I$ and $T_{(0,\omega^2)} = X^0Z^1 \otimes X^0Z^1 = Z \otimes Z$. From Eqn (3.9) we know that we can simultaneously diagonalize the operators we have just found to find the basis that we want to associate with the striations that are defined by $q = c$. One can show that the three operators just found all commute with each other. We list this set of operators as $\{IZ, ZI, ZZ\}$, which we have now shown correspond to the striations for $q = c$. When discussing commuting sets, we often omit the direct product symbol; for example IZ is short for $I \otimes Z$. Since the third operator is the product of the first two, if one simultaneously diagonalizes the first two operators, the resulting eigenvectors automatically satisfy the eigenvalue equation for the third operator. These eigenvectors are obvious and are the standard basis vectors in Hilbert space dimension $N = 4$: $|\uparrow\uparrow\rangle$, $|\uparrow\downarrow\rangle$, $|\downarrow\uparrow\rangle$, $|\downarrow\downarrow\rangle$.

Example: $\omega p + q = c$

In this case the three invariance translation operators are $(1,\omega^2)$, $(\omega,1)$ and (ω^2,ω). Writing them in terms of the field bases we have $(1,\omega^2) = (0e_1+1e_2, 1f_1+1f_2)$, $(\omega,1) = (1e_1+0e_2, 0f_1+1f_2)$ and $(\omega^2,\omega) = (1e_1+1e_2, 1f_1+0f_2)$. We then find that the translation operators for these vectors are $T_{(1,\omega^2)} = Z \otimes XZ = -iZ \otimes Y$, $T_{(\omega,1)} = X \otimes Z$ and $T_{(\omega^2,\omega)} = XZ \otimes X = -iY \otimes X$. We can ignore the phase in two of the terms, and then have the set of operators $\{ZY, XZ, YX\}$, which correspond to the striations for $\omega p + q = c$. One can check that the three operators just found do indeed commute, and also that the third is the product of the first two. We can then simultaneously diagonalize the first two operators to find the eigenvectors which will be associated with this striation.

Remaining Lines

One can use the method just outlined to find the rest of the commuting sets. Upon simultaneous diagonalization of the first two operators in each set, one can find the four eigenvectors of each set. The results are summarized in Table 3.4. The commuting sets are each labeled in terms of a basis number labeled 0 to 4. The striations for 2 qubits are given in Fig 3.3. The commuting sets are numbered from top to bottom in the figure with basis 0 corresponding to the 1st striation, basis 1 to the second striation, and so on. The operators in the commuting set for a striation are equivalent to the invariance translation vectors. One can verify that the bases given in Table 3.4 form a set of mutually unbiased bases.

Basis	Eigenvectors			
0 {ZI,IZ,ZZ}	$\|0_1\rangle$=1000	$\|0_2\rangle$=0100	$\|0_3\rangle$=0010	$\|0_4\rangle$=0001
1 {XI,IX,XX}	$\|1_1\rangle$=1111	$\|1_2\rangle$=1$\bar{1}$1$\bar{1}$	$\|1_3\rangle$=11$\bar{1}\bar{1}$	$\|1_4\rangle$=1$\bar{1}\bar{1}$1
2 {YI,IY,YY}	$\|2_1\rangle = 1i\bar{i}\bar{1}$	$\|2_2\rangle = 1\bar{i}i1$	$\|2_3\rangle = 1i\bar{i}1$	$\|2_4\rangle = 1\bar{i}\bar{i}\bar{1}$
3 {XY,YZ,ZX}	$\|3_1\rangle = 1\bar{1}ii$	$\|3_2\rangle = 11\bar{i}i$	$\|3_3\rangle = 11i\bar{i}$	$\|3_4\rangle = 1\bar{1}\bar{i}\bar{i}$
4 {YX,ZY,XZ}	$\|4_1\rangle = 1i\bar{1}i$	$\|4_2\rangle = 1\bar{i}1i$	$\|4_3\rangle = 1i1\bar{i}$	$\|4_4\rangle = 1\bar{i}\bar{1}\bar{i}$

Table 3.4: 2-qubit mutually unbiased bases from [1]. The rows contain the simultaneous eigenstates for the given basis with eigenvalue signatures of $++,+-,-+,--$ with respect to the first 2 observables in a commuting set. The numbers following a ket in each row are *abcd*, which are the coefficients for the unnormalized state $a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$. A bar over a number means the number is negative and $i = \sqrt{-1}$.

3.3.3 2-Qubit Quantum Net

One needs to associate each eigenstate in Table 3.4 with a particular line in the corresponding striation of Fig 3.3. This choice is completely arbitrary, and each separate choice is known as a *quantum net*. We will associate the vertical and horizontal lines in a way similar to the single qubit DWF. The choice is shown in Fig 3.4.

We have made our choice for the first two striation sets in Fig 3.3, but what about the other three remaining bases? One can choose to associate a particular eigenstate of a commuting set with any line in a striation, but upon doing so the other eigenstates are fixed by the shift operators. For each of the bases given in Table 3.4 one may apply a shift operator to one of the eigenvectors to produce a new eigenvector within the same basis. The phase space defined on $GF(2^2)$ has 4 basic translation operators out of which any other translation operator can be

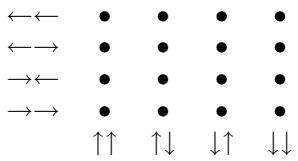

Figure 3.4: Phase Space Labels for a System of 2 Qubits. The arrows are defined as $\uparrow$ = spin up along z, $\downarrow$ = spin down along z, $\rightarrow$ = spin up along x, $\leftarrow$ = spin down along x. Qubit one is always the leftmost arrow, qubit two is always the rightmost arrow. Each phase space point is labeled by the horizontal and vertical arrows with which it is aligned.

built up. These basic translation vectors each correspond to a unitary operator in the state space and are given with their corresponding unitary operators as $(1,0) \leftrightarrow I \otimes X$, $(\omega,0) \leftrightarrow X \otimes I$, $(0,1) \leftrightarrow I \otimes Z$ and $(0,\omega) \leftrightarrow Z \otimes I$. There are many different ways in which one can shift from one eigenvector in a basis to another eigenvector in a basis. Table 3.5 gives one of the ways for each basis of shifting from the first eigenstate to the other eigenstates in a basis. One can check that the unitary operators corresponding to the shift operators given in the table do indeed shift to the correct eigenstate.

Basis	1 & 2	1 & 3	1 & 4
0	$(1,0)$	$(\omega,0)$	$(\omega^2,0)$
1	$(0,1)$	$(0,\omega)$	$(0,\omega^2)$
2	$(0,1)$	$(\omega,0)$	(ω^2)
3	$(1,0)$	$(\omega,0)$	$(\omega^2,0)$
4	$(\omega,0)$	$(\omega^2,0)$	$(1,0)$

Table 3.5: 2-Qubit Shift Operators. The columns are labeled with the eigenvalue signatures corresponding to the eigenvectors one can shift between with the corresponding shift vector.

Following the choice of Gibbons *et. al.* [4], we use the association of the eigenstates for each basis to lines in the striations given in Fig 3.5. We chose this quantum net because it leads to an elegant crossing formula as discussed in Ch. 4.

There are of course many other choices of quantum nets one may use. One possible quantum net is the one for which each ++ eigenstate is associated with the line that passes through the origin $(0,0)$ of phase space. The line passing through the origin is called the ray. This choice was proposed by our advisor, Aravind [2], and it turns out that it gives a simple form for the *Cnot* gate (in Ch.

1	2	3	4	4	4	4	4	3	4	1	2	1	2	3	4
1	2	3	4	3	3	3	3	4	3	2	1	4	3	2	1
1	2	3	4	2	2	2	2	1	2	3	4	2	1	4	3
1	2	3	4	1	1	1	1	2	1	4	3	3	4	1	2

3	2	4	1
4	1	3	2
1	4	2	3
2	3	1	4

Figure 3.5: 2-Qubit Striations with Associated Eigenstates. From left to right the associated mutually unbiased bases are 0, 1, 2, 3, and 4. The numbers arranged in the grids correspond to eigenvalue signatures for the corresponding basis vectors with the convention that $1 = ++$, $2 = +-$, $3 = -+$ and $4 = --$.

5) as well as for the reduction formula (Ch. 4). Unless specified, we will use the choice of quantum net given in Fig 3.5, denoted *Wootters's net*. Occasionally we will refer to *Aravind's net*.

3.4 The Wigner Function

We return to the development of the DWF theory for a $N = 2^n$-state system. The elements of $GF(N)$ will furnish the labels for the two axes of the phase space. Here we define the DWF by associating a number with each point in phase space; later we prove that these numbers are real. This section follows Gibbons's *et. al.* paper [4], section 5 closely.

With the lines λ in phase space associated with quantum states $|\lambda\rangle$ and corresponding density operators $Q(\lambda) = |\lambda\rangle\langle\lambda|$, we are prepared to define the Wigner function. We would like a sum along a line to give the probability of measuring the corresponding eigenstate. That is, for a quantum state ρ with corresponding Wigner function W, we insist that, for any line λ:

$$\mathrm{Tr}(\rho Q(\lambda)) = \sum_{\alpha \in \lambda} W_\alpha \tag{3.10}$$

It is useful to invert this equation, to find W_β as a function of ρ. To do this, we sum the above equation over the $N + 1$ lines λ containing an arbitrary point β.

$$\sum_{\lambda \ni \beta} \mathrm{Tr}(\rho Q(\lambda)) = \sum_{\lambda \ni \beta} \sum_{\alpha \in \lambda} W_\alpha \tag{3.11}$$

The sum on the right-hand side contains W_β exactly $N + 1$ times (one for each line), and every other point exactly once. Subtracting the sum of the Wigner

function over every point in phase space from both sides:

$$\sum_{\lambda \ni \beta} \mathrm{Tr}(\rho Q(\lambda)) - \sum_{\gamma} W_\gamma = \sum_{\lambda \ni \beta} \sum_{\alpha \in \lambda} W_\alpha - \sum_{\gamma} W_\gamma \tag{3.12}$$

Using the linearity of trace on the LHS, and the analysis of the double sum discussed earlier on the RHS:

$$\mathrm{Tr}\left(\sum_{\lambda \ni \beta} Q(\lambda)\rho\right) - \sum_{\gamma} W_\gamma = (N + 1 - 1)W_\beta \tag{3.13}$$

Use the fact that parallel lines form a complete orthonormal basis, so for any line Λ:

$$\sum_{\lambda \| \Lambda} Q(\lambda) = I \tag{3.14}$$

and therefore, using Eqn (3.10):

$$\sum_{\gamma} W_\gamma = \sum_{\lambda \| \Lambda} \sum_{\alpha \in \lambda} W_\alpha = \sum_{\lambda \| \Lambda} \mathrm{Tr}(\rho Q(\lambda)) = \mathrm{Tr}(\rho I) \tag{3.15}$$

Solving Eqn (3.13) for W_β using Eqn (3.15):

$$W_\beta = \frac{1}{N} \mathrm{Tr}\left(\rho\left(\sum_{\lambda \ni \beta} Q(\lambda) - I\right)\right) \tag{3.16}$$

The quantity multiplying ρ in the argument of the trace is given a special name:

$$A_\beta \equiv \sum_{\lambda \ni \beta} Q(\lambda) - I \tag{3.17}$$

The following fact is useful for proving statements about the A operators:

$$\mathrm{Tr}\left(\sum_{\lambda \ni \beta} Q(\lambda)\right) = N + 1 \tag{3.18}$$

Several properties follow from this and the properties of the Q operators:

$$A_\beta = A_\beta^\dagger \tag{3.19}$$

$$\mathrm{Tr} A_\beta = 1 \tag{3.20}$$

$$\sum_{\alpha \in \lambda} A_\alpha = N Q(\lambda) \tag{3.21}$$

Another equation that can be derived from Eqn (3.17) is:

$$\mathrm{Tr}(A_\alpha A_\beta) = \sum_{\lambda \ni \beta} \sum_{\Lambda \ni \alpha} \mathrm{Tr}(Q(\lambda)Q(\Lambda)) - 2(N+1) + N \tag{3.22}$$

To evaluate the double sum, note that since the bases are mutually unbiased, $\mathrm{Tr}(Q(\lambda)Q(\Lambda))$ is 1 if the lines are the same, 0 if the lines are parallel, and $\frac{1}{N}$ if the lines are not parallel. If the points are the same, $N+1$ terms in the double sum have $\lambda = \Lambda$, contributing $N+1$, and the remaining $N(N+1)$ terms contribute $1/N$ each, totaling $N+1$. The right side of Eqn (3.22) works out to $2(N+1) - 2(N+1) + N = N$.

If the points are different, one term in the double sum will involve the same line, N involve two parallel lines, and the remaining $N(N+1)$ involve intersecting lines. In this case, the total is $1 + N + 1 - 2(N+1) + N = 0$. Therefore:

$$\mathrm{Tr}(A_\alpha A_\beta) = N\delta_{\alpha\beta} \tag{3.23}$$

According to Gibbons *et. al.* [4], Eqn (3.23) shows that the A operators form a complete set in the space of $N \times N$ matrices. This means that ρ can be expressed as a linear combination of the A's:

$$\rho = \sum_\alpha b_\alpha A_\alpha \tag{3.24}$$

Multiplying by A_β, and taking the trace:

$$\mathrm{Tr}(A_\beta \rho) = \sum_\alpha b_\alpha \mathrm{Tr}(A_\beta A_\alpha) = N b_\beta \tag{3.25}$$

Comparing this to the formula for W (Eqn 3.16), we see that $b_\alpha = W_\alpha$, so

$$\rho = \sum_\alpha W_\alpha A_\alpha \tag{3.26}$$

We have therefore shown how to convert from ρ to W (Eqn 3.16) and vice versa (Eqn 3.26). Note that nowhere in this derivation did we assume that ρ was a density operator. The Wigner representation works fine for any operator at all. For Hermitian ρ, Eqn 3.16, combined with the fact that Hermitian operators can be expressed as a sum of projectors with real weights, shows that W_α is real.

It is useful to be able to construct a Wigner function for a pure or mixed state from a set of measurement probabilities. Using Eqn (3.16), one finds:

$$W_\beta = \frac{1}{N}\sum_{\lambda \ni \beta} \mathrm{Tr}(\rho Q(\lambda)) - \frac{1}{N}\mathrm{Tr}(\rho) \tag{3.27}$$

$$= \frac{1}{N}\left[\sum_{\lambda \ni \beta} P(|\lambda\rangle) - 1\right] \tag{3.28}$$

where $P(|\lambda\rangle)$ denotes the probability of finding the system in the state corresponding to the line λ.

A corollary of this equation is that Wigner elements cannot be more negative than $\frac{-1}{N}$. This is an unobtainable lower bound; Wootters [11] states that for 1 qubit the most negative element is -0.183. An interesting problem is finding the most negative obtainable Wigner element for any number of qubits.

Using the expansion of ρ in terms of A, it is easy to show that, if ρ_1 and ρ_2 can be expressed using Wigner elements W and V respectively, the squared overlap is:

$$\mathrm{Tr}(\rho_1\rho_2) = N\sum_\alpha W_\alpha V_\alpha \tag{3.29}$$

This leads to a way to determine if a DWF corresponds to a pure or mixed state. A state with density operator ρ is pure iff it has an eigenvalue of 1. Together with the normalization condition that all eigenvalues add up to 1, this shows that a state is pure iff the sum of squares of eigenvalues is 1. Identifying the trace with the sum of eigenvalues and using Eqn (3.29), we can characterize how mixed a state is by:

$$M \equiv \sum_\alpha W_\alpha^2 \tag{3.30}$$

For a pure state, $M = 1/N$ while for a mixed state, $0 \leq M < 1/N$.

3.4.1 1-qubit Wigner Function Example

For this example we will consider the state $|y+\rangle$. We want to write the discrete Wigner function for this state, and we may do so by using Eqn (3.28). Let us begin by finding the value of the Wigner element at the origin, i.e. $(0,0)$. There are three lines that pass through this point and correspond to the states $|\uparrow\rangle$, $|\rightarrow\rangle$ and $|y+\rangle$. For the state under consideration, $|y+\rangle$, we may find the probabilities of measuring the three states whose lines pass through this point. The respective probabilities of measuring the $|y+\rangle$ state to be in the states whose lines pass

through $(0,0)$ are: $P(|\uparrow\rangle) = 1/2$, $P(|\rightarrow\rangle) = 1/2$ and $P(|y+\rangle) = 1$. We can now use these probabilities and employ Eqn (3.28), where the Hilbert space dimension is of course $N = 2$. We then find for the state $|y+\rangle$:

$$\begin{aligned} W_{(0,0)} &= \frac{1}{2}\left[\sum_{\lambda \ni (0,0)} P(|\lambda\rangle) - 1\right] = \frac{1}{2}\left[P(|\uparrow\rangle) + P(|\rightarrow\rangle) + P(|y+\rangle) - 1\right] \\ &= \frac{1}{2}\left[\frac{1}{2} + \frac{1}{2} + 1 - 1\right] = \frac{1}{2} \end{aligned} \tag{3.31}$$

In this way one can also find the other values of the Wigner elements at the remaining three points. Upon performing these calculations, one arrives at the following representation of the state $|y+\rangle$ in terms of the DWF:

$$W_{y+} = \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix} \tag{3.32}$$

3.5 Alternate Construction for 2-qubit DWF

This section describes an alternate way to determine how to convert between the Wigner representation and the standard density matrix representation using Hadamard matrices. As an accident of history, some of our later results were derived from this representation, since we encountered it first.

A 2-qubit discrete Wigner function physically corresponds to a system containing 2 spin-$\frac{1}{2}$ particles with a Hilbert space dimension of $N = 4$. A 2-qubit pure state may be represented as a state vector, a density operator or a discrete Wigner function. The state vector of a 2-qubit state can be represented as

$$|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \tag{3.33}$$

The kets correspond to direct products (tensor products) of the standard 1-qubit basis vectors. The first number in a ket corresponds to the first qubit, and the second number to the second qubit, i.e. $|01\rangle = |0_1 1_2\rangle = |0_1\rangle \otimes |1_2\rangle$, where the 1 and 2 subscripts denote qubit 1 and 2. The subscripts will not be included henceforth. The coefficients are in general complex and obey the normalization condition $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

A general density operator for a 2-qubit system requires $4^2 - 1 = 15$ independent parameters, with the -1 coming from normalization. A general density matrix for

a system of 2 qubits is found by taking a tensor product of two 1-qubit density matrices. The general 2-qubit density matrix is defined as:

$$\begin{aligned}\rho &= \frac{1}{4}(I + s_{1x}XI + s_{1y}YI + s_{1z}ZI + s_{2x}IX + s_{2y}IY + s_{2z}IZ + \\ &\quad c_{xx}XX + c_{xy}XY + c_{xz}XZ + c_{yx}YX + c_{yy}YY + c_{yz}YZ + \\ &\quad c_{zx}ZX + c_{zy}ZY + c_{zz}ZZ)\end{aligned} \tag{3.34}$$

where I, X,Y, and Z are the one-qubit identity and Pauli spin operators, except for the first I after the parenthesis, which is a 4×4 identity matrix. The notation XI is shorthand for the tensor product of the operators, i.e. $XI = X \otimes I$. We use this shorthand often in this report. The coefficients in the expansion of ρ may be found by multiplying ρ by the operator corresponding to the coefficient and taking the trace, for example, $c_{xz} = \mathrm{Tr}(\rho XZ)$. The coefficients labeled s_{ni}, where n is 1 or 2 and i is x, y, or z are the spin components for the individual qubits, when the other qubit is ignored. It is convenient to represent the coefficients of ρ in a column vector $\vec{S}$. To save space $\vec{S}$ is written below transposed:

$$\vec{S}^T = (1, s_{1x}, s_{1y}, s_{1z}, s_{2x}, s_{2y}, s_{2z}, c_{xx}, c_{xy}, c_{xz}, c_{yx}, c_{yy}, c_{yz}, c_{zx}, c_{zy}, c_{zz}) \tag{3.35}$$

Equation (3.35) is useful when manipulating the 2-qubit Wigner function, as is explained shortly.

Now that we have a good understanding of the eigenstate associations and the phase space structure, let us discuss representing states with the discrete Wigner function. The discrete Wigner function representation for 2 qubits is given as a 4×4 matrix. The elements are expressed as:

$$W = \begin{pmatrix} w_{1100} & w_{1101} & w_{1110} & w_{1111} \\ w_{1000} & w_{1001} & w_{1010} & w_{1011} \\ w_{0100} & w_{0101} & w_{0110} & w_{0111} \\ w_{0000} & w_{0001} & w_{0010} & w_{0011} \end{pmatrix} \tag{3.36}$$

The entries in W are labeled with the convention $w_{x_1x_2z_1z_2}$, with the subscripts on the x's and z's representing qubit 1 and qubit 2, respectively. The x's and z's are either 0 (spin up) or 1 (spin down) with the columns associated with the Pauli Z operator and the rows associated with the Pauli X operator. The elements of the W matrix correspond to discrete phase space points, which may be formed into 5 sets of striations for the $(2^2+1) = 5$ sets of commuting operators, with each

set containing $(2^2 - 1) = 3$ operators. It is again convenient to write the entries of W as a column vector $\overrightarrow{W}$ with its elements arranged in lexicographic order. To save space, $\overrightarrow{W}$ is shown in Eqn (3.37) transposed:

$$\begin{aligned}\overrightarrow{W}^T = (&w_{0000}, w_{0001}, w_{0010}, w_{0011}, w_{0100}, w_{0101}, w_{0110}, w_{0111},\\ &w_{1000}, w_{1001}, w_{1010}, w_{1011}, w_{1100}, w_{1101}, w_{1110}, w_{1111})\end{aligned} \tag{3.37}$$

In Sec 2.3.1 we were able to easily map between the density coefficients and the Wigner elements. We would again like to do such a mapping for a system of 2-qubits. The mapping between the elements of the Wigner matrix (Eqn 3.37) and the density matrix coefficients (Eqn 3.35) can be found as follows. Each density matrix coefficient, denoted η_i, can be calculated as

$$\eta_i = (+1)P(i+) + (-1)P(i-) \tag{3.38}$$

Equation (3.38) is essentially the same as Eqn (2.19) from Ch. 2. The 2-qubit case is a bit more involved since the probabilities of measuring the density coefficient η_i to be up or down each correspond to summing over 8 Wigner elements as opposed to 2. For instance if we are to find the total probability of finding qubit 1 to have spin up along z we need to sum the 8 Wigner elements that correspond to the lines $\uparrow\uparrow$ and $\uparrow\downarrow$. Likewise if we want to find the total probability of finding qubit 2 to have spin up along z we need to sum the 8 Wigner elements corresponding to the lines $\uparrow\uparrow$ and $\downarrow\uparrow$. In Eqn (3.34) each η_i is multiplied by an operator which belongs to one of the 5 commuting sets. To get the probability of measuring each η_i to be either up or down one needs to sum over a particular set of lines; which set of lines to sum over is determined by the quantum net. When considering the η_i's which correspond to the first two operators in a commuting set it is easy to see which elements to sum over, since the eigenvalue signatures of $++$, $+-$, etc were developed for the first two operators. Since the third operator in each set is either equal to the product of the first two (bases 0 to 3) or the negative of the product (bases 4 to 5), one can easily calculate the eigenvalue for the third operator from the eigenvalues of the first two.

It is a bit easier to write the formula for each η_i in terms of the lines within a striation. We can then re-write Eqn (3.38) as

$$\eta_i = (+1)\sum_{i+} \lambda^m_{i+} + (-1)\sum_{i-} \lambda^m_{i-} \tag{3.39}$$

where the λ's correspond to the lines within a basis labeled by $m \in \{0, 1, 2, 3, 4\}$. Each sum is over the elements from 2 lines, which represent the +1 or -1 eigenvalue signature for the η_i. For the η_i that corresponds to the third operator in a commuting set, make sure the +1 or -1 for the set results from multiplying the three lines for the η_i's corresponding to a commuting set. For example, the reader can verify that for the coefficient c_{zz} associated with basis 0 we have $c_{zz} = (+1)\{\lambda_1^0 + \lambda_4^0\} + (-1)\{\lambda_2^0 + \lambda_3^0\}$. After finding each coefficient of ρ in terms of the elements W, one may relate the two using the column vector forms of each. The equation relating them is given by Eqn (3.40), where the $\vec{S}$ is given by Eqn (3.35) and the $\overrightarrow{W}$ is given by Eqn (3.37).

$$\vec{S} = H\overrightarrow{W} \tag{3.40}$$

Using this process one can arrive at the 16×16 Hadamard matrix which is given in Appendix A.1. The 16×16 Hadamard matrix is used for manipulating the 2-qubit discrete Wigner function; this is why we write $\vec{S}$ and $\overrightarrow{W}$ as column vectors. Using the inverse of Eqn (3.40), we can determine a Wigner function for a given ρ.

Manipulations on 2-qubit systems using the DWF are best done using a computer program such as Maple. Applications of the 2-qubit DWF are given in Ch. 5.

Chapter 4

Discrete Wigner Function Crossing and Reducing

4.1 Introduction

Often in physics one must combine two subsystems to form a single composite system. In quantum mechanics, the density matrix of a composite system is obtained by taking the direct product of the density matrices of the component subsystems, while the density matrices of the individual subsystems are obtained from that of the composite by taking the partial trace [9]. The direct product of 1-qubit Wigner functions looks promising as a way to form a combined Wigner function, but we show that regardless of what quantum net one uses, the direct product of Wigner functions cannot be made to yield the DWF of the combined system.

When combining two qubits, we discovered that if one uses different quantum nets for the two qubits being crossed, the direct product does give the correct Wigner function for the two qubits considered together. The same crossing formula can be considered from an equivalent perspective, using the same quantum net for both qubits, but negating a spin component before doing the direct product. We discuss both viewpoints. From this crossing formula, we derive a similar reduction formula.

4.2 Naïve Crossing

In this section, we discuss how the simple direct product might work, and why it does not.

The combination formulae for the A operators and the W Wigner function elements are intimately related. Consider one qubit with a density matrix $\rho^{(1)}$ and a second with density matrix $\rho^{(2)}$. Using Eqn (3.26), and our knowledge of how to cross density matrices, we can find the combined density matrix $\rho^{(1,2)}$:

$$\rho^{(1)} = \sum_{\alpha} W_\alpha A^{(1)}_\alpha \tag{4.1}$$

$$\rho^{(2)} = \sum_{\beta} V_\beta A^{(2)}_\beta \tag{4.2}$$

$$\rho^{(1,2)} = \sum_{\alpha}\sum_{\beta} W_\alpha V_\beta A^{(1)}_\alpha \otimes A^{(2)}_\beta \tag{4.3}$$

If one were to identify $W_\alpha V_\beta$ with the two-qubit Wigner coefficients and $A^{(1)}_\alpha \otimes A^{(2)}_\beta$ with the 2-qubit A operators, Eqn (4.3) would be an expansion for the two qubit Wigner function.

Unfortunately, the A operators are not arbitrary Hermitian operators, so this identification of the $A^{(1,2)}$ might not be legitimate. The A operators must be related to the density matrices for the mutually unbiased bases discussed previously via Eqn (3.17).

We will next show that there is no quantum net where the naïve direct product formula Eqn (4.3) correctly computes the 2-qubit DWF. Consider the Wigner functions for $|x+\rangle \otimes |y+\rangle$, $|y+\rangle \otimes |z+\rangle$, and $|z+\rangle \otimes |x+\rangle$ produced by the naïve crossing formula (Eqn 4.3):

←←	0	0	0	0	←←	0	0	1/4	0	←←	0	0	0	0
←→	0	0	0	0	←→	0	0	1/4	0	←→	1/4	1/4	0	0
→←	0	1/4	0	1/4	→←	1/4	0	0	0	→←	0	0	0	0
→→	1/4	0	1/4	0	→→	1/4	0	0	0	→→	1/4	1/4	0	0
	↑↑	↑↓	↓↑	↓↓		↑↑	↑↓	↓↑	↓↓		↑↑	↑↓	↓↑	↓↓
	$\|x+\rangle$	⊗	$\|y+\rangle$			$\|y+\rangle$	⊗	$\|z+\rangle$			$\|z+\rangle$	⊗	$\|x+\rangle$	

(4.4)

Here are the lines for the $\{XY, YZ, ZX\}$ basis from Table 3.5:

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{array} \tag{4.5}$$

We want to show that no association of the above lines to the eigenstates of the $\{XY, YZ, ZX\}$ basis is consistent with Eqn (4.4). Comparing the supposed $|x+\rangle \otimes |y+\rangle$ Wigner function to the lines, one sees that lines 1 and 3 must be associated with $+XY$ eigenstates. From the supposed $|y+\rangle \otimes |z+\rangle$ Wigner function, one sees that lines 2 and 3 must be associated with $+YZ$. Since the Pauli operators satisfy $X \cdot Y = iZ$, $(X \otimes Y) \cdot (Y \otimes Z) = -Z \otimes X$, one can determine the ZX eigenvalue for each line by multiplying the XY and YZ eigenvalues. Table 4.1 summarizes these results.

Line	XY	YZ	ZX
1	+	-	+
2	-	+	+
3	+	+	-
4	-	-	-

Table 4.1: The eigenvalues associated with the lines under naïve crossing.

Now consider the $|z+\rangle \otimes |x+\rangle$ Wigner function. Comparing it to Table 3.5, one sees that lines 3 and 4 are associated with $ZX+$. This is inconsistent with the association of $ZX+$ with lines 1 and 2 in Table 4.1. We therefore conclude that for the 1-qubit quantum net we chose, no 2-qubit quantum net will allow the naïve crossing formula (Eqn 4.3) to work. The cause of this problem is the fact that the Pauli operators satisfy $X \cdot Y = iZ$, not $X \cdot Y = Z$, so for the fourth and fifth bases, the third operator is the negative of the product of the first two. If one instead uses the 1-qubit quantum net where the Y-eigenstates have line assignments swapped, a similar problem occurs with the $\{IY, YI, YY\}$ basis.

4.3 Spin Component Flipping

Gibbons *et. al.* [4] note that their quantum net has the special property that:

$$A^{(1,2)} = A^{(1)} \otimes \bar{A}^{(2)} \tag{4.6}$$

where the overbar indicates complex conjugation. They mention this as a reason to prefer their choice of net.

Complex conjugating a density matrix negates the y-component of the spin while leaving the x and z-components unchanged. We generalized their result in two ways. We discovered that a negation of the x or z-component of the spin would also allow an analogous cross-product of A operators. We also found the crossing formula for the W that goes with Eqn (4.6).

To negate the y spin-component of a 1-qubit Wigner function, use:

$$V'_{00} = 1/2 - V_{11} \tag{4.7}$$
$$V'_{01} = 1/2 - V_{10} \tag{4.8}$$
$$V'_{10} = 1/2 - V_{01} \tag{4.9}$$
$$V'_{11} = 1/2 - V_{00} \tag{4.10}$$

where V_{ij} is the original Wigner function and V'_{ij} is the flipped WF.

Consider density matrices $\rho^{(1)}$ and $\rho^{(2)}$, expanded as Wigner functions using Eqn 3.26:

$$\rho^{(1)} = \sum_\alpha W_\alpha A^{(1)}_\alpha \tag{4.11}$$
$$\rho^{(2)} = \sum_\beta V_\beta A^{(2)}_\beta \tag{4.12}$$

One can also express the result of flipping a component of the spin of $\rho^{(2)}$, denoted $\rho'^{(2)}$ as a Wigner function:

$$\rho'^{(2)} = \sum_\beta V'_\beta A^{(2)}_\beta \tag{4.13}$$

Do the inverse of the spin-flip to both sides:

$$\rho^{(2)} = \sum_\beta V'_\beta A'^{(2)}_\beta \tag{4.14}$$

where $A'^{(2)}$ denotes the A operator with its spin component flipped. Combining:

$$\rho^{(1,2)} = \sum_\alpha \sum_\beta W_\alpha V'_\beta A^{(1)}_\alpha \otimes A'^{(2)}_\beta \tag{4.15}$$

We identify $W_\alpha V'_\beta$ with the the 2-qubit Wigner function, and $A^{(1)}_\alpha \otimes A'^{(2)}_\beta$ with the

2-qubit A operator.

It turns out that the A operators defined here do correspond to a legitimate quantum net if the x, y, or z component of the spin is flipped. Reflection of the spin along other axes, such as $\hat{x} + \hat{y}$, do not seem to correspond to quantum nets. We tested various crossing formulae by calculating the resulting A operators. We then verified numerically that the Q operators derived from the A operators formed mutually unbiased bases.

Another way to think of the spin-flip is that one must use different quantum nets for the two Wigner functions being crossed. Since the choice of quantum net for a 1-qubit system amounts to deciding which X, Y, and Z eigenstates to assign to each line, negating the y-component of the spin is equivalent to swapping which Y-eigenstate to associate with which line, with similar remarks applying to X and Z.

Any odd number of space inversions (combined between the two qubits) along the three axes forms a quantum net. There are therefore $8 \cdot 8/2 = 32$ possible 2-qubit quantum nets that are formed using cross products of this form. However, there are $4^{4+1} = 1024$ different quantum nets, so there are quantum nets that do not have a crossing formula of this type. For example, a choice of quantum net that looks obvious at first is the one where the $++$ eigenstate is associated with the line passing through the origin – Aravind's net (see Sec 3.3.3). However, with this type of net, crossing is more complicated. With this quantum net, the $Z \otimes X$ eigenstate has a DWF of:

$$W = \frac{1}{8} \begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \tag{4.16}$$

Note that this cannot be expressed as the direct product of 2×2 matrices.

4.4 Reduction

The crossing formula for the A operators leads naturally to a formula for calculating the reduced density matrix for 1 of the 2 qubits. The reduced density matrix

for the first qubit can be expressed as follows:

$$\mathrm{Tr}^{(2)}(\rho) = \sum_{\alpha}\sum_{\beta} W_{\alpha\beta}\mathrm{Tr}^{(2)}(A_\alpha \otimes A'_\beta) \quad (4.17)$$

$$= \sum_{\alpha} A_\alpha \sum_{\beta} W_{\alpha\beta} \quad (4.18)$$

The sum over β can be identified with the Wigner coefficient W_α for the reduced system. Similarly,

$$\mathrm{Tr}^{(1)}(\rho) = \sum_{\alpha}\sum_{\beta} W_{\alpha\beta}\mathrm{Tr}^{(1)}(A_\alpha \otimes A'_\beta) \quad (4.19)$$

$$= \sum_{\beta} A'_\beta \sum_{\alpha} W_{\alpha\beta} \quad (4.20)$$

This produces a 1-qubit DWF, but for the wrong quantum net. One needs to flip the spin (Eqn 4.10) to get the Wigner function in terms of the correct A operators. Therefore, computing the reduced density matrix over the second qubit requires summing the Wigner function in 4 sets of 4, and then flipping the spin of the resulting 1-qubit DWF.

Aravind's net has a complicated crossing formula, but the reduction formula is surprisingly simple. Using Aravind's net and performing the reduction using brute-force computer aided algebra using the methods of Sec 3.5, one can show:

$$W^{(1)} = \begin{pmatrix} w_{1000} + w_{1001} + w_{1100} + w_{1101} & w_{1010} + w_{1011} + w_{1110} + w_{1111} \\ w_{0000} + w_{0001} + w_{0100} + w_{0101} & w_{0010} + w_{0011} + w_{0110} + w_{0111} \end{pmatrix} \quad (4.21)$$

$$W^{(2)} = \begin{pmatrix} w_{0100} + w_{0110} + w_{1100} + w_{1110} & w_{0101} + w_{0111} + w_{1101} + w_{1111} \\ w_{0000} + w_{0010} + w_{1000} + w_{1010} & w_{0001} + w_{0011} + w_{1001} + w_{1011} \end{pmatrix} \quad (4.22)$$

The result for the first qubit is the same as for Wootters's net. For Aravind's net, reduction over the second qubit is analogous to the first – no spin-flip required.

4.5 Future Work

Spin component flipping does not seem to be sufficient for handling 3 qubits crossed together. We do not understand in any deep way why the spin-component inversion trick makes crossing work, so we cannot predict what generalization of spin-component negation might work for more qubits.

Aravind's quantum net has a complicated crossing formula, but some other

formulae are simpler than Wootters. In particular, the reduction formula for Aravind's quantum net is very simple, and the *Cnot* gate (see Ch. 5) is also simpler. We do not understand why. Understanding these issues would help one choose an appropriate quantum net that is convenient for calculations.

Chapter 5

Applications

5.1 Arbitrary Rotations of 1-Qubit DWF

Applying gates to qubits is equivalent to acting on the qubits with unitary operators. Arbitrary rotations for a qubit are represented here in the form of unitary operators, which we apply to the discrete Wigner function. We will use the column vector form of the 1-qubit Wigner function

$$\overrightarrow{W} = \begin{pmatrix} w_{00} \\ w_{01} \\ w_{10} \\ w_{11} \end{pmatrix} \tag{5.1}$$

along with what will be called the arbitrary gate matrix G, to find the new matrix form of the DWF W' of the rotated state in phase space. We will use Eqn (2.13), which we reproduce here:

$$\vec{s}' = (\hat{n} \cdot \vec{s})\hat{n} + [\vec{s} - (\hat{n} \cdot \vec{s})\hat{n}]cos\theta + (\hat{n} \times \vec{s})sin\theta$$

to relate the rotated to non-rotated pseudospin vectors. This equation can be written as $\vec{s}' = \mathbf{r}\vec{s}$ where $\mathbf{r}$ is a 3×3 orthogonal matrix. We can then augment that matrix to a 4×4 rotation matrix called R, where we do not give explicit

expressions for the components of **r** since they are rather cumbersome.

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & r_{11} & r_{12} & r_{13} \\ 0 & r_{21} & r_{22} & r_{23} \\ 0 & r_{31} & r_{32} & r_{33} \end{pmatrix} \tag{5.2}$$

Equation (5.2) may then be used to relate the density coefficient vectors $\vec{S}$ and $\vec{S}'$ by $\vec{S}' = R\vec{S}$. This may then be used to relate the rotated DWF, $\overrightarrow{W}' = H^{-1}\vec{S}'$, to the original DWF $\vec{W} = H^{-1}\vec{S}$ by $\overrightarrow{W}' = H^{-1}RH\overrightarrow{W}$, where H is the 4×4 Hadamard matrix given in Eqn (2.20). One can write the relation more compactly as

$$\overrightarrow{W}' = G\overrightarrow{W} \tag{5.3}$$

with $G \equiv H^{-1}RH$. The G matrix acts on the DWFs as a unitary operator would act on state vectors. It turns out that G contains a lot of terms and does not simplify nicely. One can limit the rotations to those that correspond only to rotations about the x, y, and z axes with corresponding rotation matrices G_x, G_y, and G_z, respectively. These matrices are easier to write than the general form and are given, for a rotation by θ about each axis, by

$$G_x = \begin{pmatrix} \frac{1}{2}(1+\cos\theta) & \frac{1}{2}(1-\cos\theta) & -\frac{1}{2}\sin\theta & \frac{1}{2}\sin\theta \\ \frac{1}{2}(1-\cos\theta) & \frac{1}{2}(1+\cos\theta) & \frac{1}{2}\sin\theta & -\frac{1}{2}\sin\theta \\ \frac{1}{2}\sin\theta & -\frac{1}{2}\sin\theta & \frac{1}{2}(1+\cos\theta) & \frac{1}{2}(1-\cos\theta) \\ -\frac{1}{2}\sin\theta & \frac{1}{2}\sin\theta & \frac{1}{2}(1-\cos\theta) & \frac{1}{2}(1+\cos\theta) \end{pmatrix} \tag{5.4}$$

$$G_y = \begin{pmatrix} \frac{1}{2}(1+\cos\theta) & -\frac{1}{2}\sin\theta & \frac{1}{2}\sin\theta & \frac{1}{2}(1-\cos\theta) \\ \frac{1}{2}\sin\theta & \frac{1}{2}(1+\cos\theta) & \frac{1}{2}(1-\cos\theta) & -\frac{1}{2}\sin\theta \\ -\frac{1}{2}\sin\theta & \frac{1}{2}(1-\cos\theta) & \frac{1}{2}(1+\cos\theta) & \frac{1}{2}\sin\theta \\ \frac{1}{2}(1-\cos\theta) & \frac{1}{2}\sin\theta & -\frac{1}{2}\sin\theta & \frac{1}{2}(1+\cos\theta) \end{pmatrix} \tag{5.5}$$

$$G_z = \begin{pmatrix} \frac{1}{2}(1+\cos\theta) & \frac{1}{2}\sin\theta & \frac{1}{2}(1-\cos\theta) & -\frac{1}{2}\sin\theta \\ -\frac{1}{2}\sin\theta & \frac{1}{2}(1+\cos\theta) & \frac{1}{2}\sin\theta & \frac{1}{2}(1-\cos\theta) \\ \frac{1}{2}(1-\cos\theta) & -\frac{1}{2}\sin\theta & \frac{1}{2}(1+\cos\theta) & \frac{1}{2}\sin\theta \\ \frac{1}{2}\sin\theta & \frac{1}{2}(1-\cos\theta) & -\frac{1}{2}\sin\theta & \frac{1}{2}(1+\cos\theta) \end{pmatrix} \tag{5.6}$$

Note that each of the G_i $(i = x, y, z)$ matrices have the same diagonal terms with a trace of $2(1+\cos(\theta)) = 4\cos^2(\frac{\theta}{2})$. Note also that all of the rotation matrices

contain the same four elements: $\frac{1}{2}(1+\cos(\theta))$, $\frac{1}{2}(1-\cos(\theta))$, $\frac{1}{2}\sin(\theta)$ and $-\frac{1}{2}\sin(\theta)$. As an example of using the rotation matrices, consider a rotation about the x axis by $\frac{\pi}{2}$ on the 1-qubit Wigner function for the $|\uparrow\rangle$ state. Setting $\theta = \frac{\pi}{2}$ in G_x we have for $\overrightarrow{W}'$

$$\overrightarrow{W}' = \frac{1}{2}\begin{pmatrix} 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{1}{2} \\ \frac{1}{2} \\ 0 \end{pmatrix}$$

The resulting Wigner vector corresponds to the state $|y-\rangle$, which is what one would expect from such an operation. One can easily check that other obvious rotations, such as those for $\theta = \pi$, give the expected results.

One may write any arbitrary rotation as the product of three rotations about 2 perpendicular axes [5]. For example a rotation of α about z followed by a rotation of β about y followed by a rotation γ about z may be used to form any rotation. These three angles are the Euler angles and the rotation can be expressed as the product $R = R_z(\gamma)R_y(\beta)R_z(\alpha)$.

5.2 2-Qubit DWF Gates

One may define the outcome of applying a gate (unitary operator) to a quantum system in terms of the discrete Wigner function. For a 4-level system we develop the quantum gates XI, IX, ZI, IZ, YI, IY, and $Cnot$. We also discuss the $Hadamard, S$, and T gates, but these gates have complicated Wigner function representations so we omit them.

To find the new Wigner functions that are formed by the unitary operators (gates) we need to first see how the 4-level density operator changes. One may find the new density operator as follows: $\rho' = |\psi'\rangle\langle\psi'| = U|\psi\rangle\langle\psi|U^\dagger = U\rho U^{-1}$ where the U is a unitary operator which acts as a gate. We are interested in finding the resulting Wigner function W' as the result of a gate. We can represent the original density matrix in terms of the original Wigner elements by writing the density matrix as a column vector, $\vec{\rho}$, that can be related to the density coefficient

vector $\vec{S}$. We write $\vec{\rho}$ as follows:

$$\vec{\rho} = \begin{pmatrix} \rho_{11} \\ \rho_{12} \\ \vdots \\ \rho_{44} \end{pmatrix} \tag{5.7}$$

$\vec{\rho}$ can be related to $\vec{S}$ using Eqn (3.34) by writing $\vec{\rho} = J\vec{S} = JH\overrightarrow{W}$ where J is a 16×16 matrix that picks out the correct components of $\vec{S}$ and is given in Appendix A.2.

Using $\vec{\rho} = JH\overrightarrow{W}$ and a function that takes $\vec{\rho}$ from a 16×1 column vector into the 4×4 ρ matrix, one can write ρ in terms of the original Wigner elements, thus being able to write ρ' in terms of the original Wigner elements. Now that we have ρ' in terms of the w's, we can obtain the new density coefficient vector $\vec{S}'$ utilizing the inverse of J. We can write ρ' as a column vector $\vec{\rho}'$ and then relate $\vec{S}'$ to it by $\vec{S}' = J^{-1}\vec{\rho}'$. Once that $\vec{S}'$ is known, it is easy to find the new Wigner function that is obtained from the given unitary operator by $\overrightarrow{W}' = H^{-1}\vec{S}'$. This construction gives W' in terms of the elements of the original Wigner function, W.

We will now look at specific examples of quantum gates on the DWF, which may be understood by recalling the translation operators in the discrete phase space. The DWF for an arbitrary 2-qubit state has the form given in Eqn (5.8). It is a useful exercise to look at this and to see how each gate should transform using the phase space translation vector. Gates that can be expressed as products of Pauli operators (e.g. $I \otimes Y$) look the same in any quantum net since they correspond to translation operators.

$$W = \begin{pmatrix} w_{1100} & w_{1101} & w_{1110} & w_{1111} \\ w_{1000} & w_{1001} & w_{1010} & w_{1011} \\ w_{0100} & w_{0101} & w_{0110} & w_{0111} \\ w_{0000} & w_{0001} & w_{0010} & w_{0011} \end{pmatrix} \tag{5.8}$$

IX gate

When the state in Eqn (5.8) is acted on by the gate IX, equivalent to a translation in phase space by $(1, 0)$, one obtains the state in Eqn (5.9).

$$\begin{pmatrix} w_{1101} & w_{1100} & w_{1111} & w_{1110} \\ w_{1001} & w_{1000} & w_{1011} & w_{1010} \\ w_{0101} & w_{0100} & w_{0111} & w_{0110} \\ w_{0001} & w_{0000} & w_{0011} & w_{0010} \end{pmatrix} \tag{5.9}$$

XI gate

When the state in Eqn (5.8) is acted on by the gate XI, equivalent to a translation in phase space by $(\omega, 0)$, one obtains the state in Eqn (5.10).

$$\begin{pmatrix} w_{1110} & w_{1111} & w_{1100} & w_{1101} \\ w_{1010} & w_{1011} & w_{1000} & w_{1001} \\ w_{0110} & w_{0111} & w_{0100} & w_{0101} \\ w_{0010} & w_{0011} & w_{0000} & w_{0001} \end{pmatrix} \tag{5.10}$$

IZ gate

When the state in Eqn (5.8) is acted on by the gate IZ, equivalent to a translation in phase space by $(0, 1)$, one obtains the state in Eqn (5.11).

$$\begin{pmatrix} w_{1000} & w_{1001} & w_{1010} & w_{1011} \\ w_{1100} & w_{1101} & w_{1110} & w_{1111} \\ w_{0000} & w_{0001} & w_{0010} & w_{0011} \\ w_{0100} & w_{0101} & w_{0110} & w_{0111} \end{pmatrix} \tag{5.11}$$

ZI gate

When the state in Eqn (5.8) is acted on by the gate ZI, equivalent to a translation in phase space by $(0, \omega)$, one obtains the state in Eqn (5.12).

$$\begin{pmatrix} w_{0100} & w_{0101} & w_{0110} & w_{0111} \\ w_{0000} & w_{0001} & w_{0010} & w_{0011} \\ w_{1100} & w_{1101} & w_{1110} & w_{1111} \\ w_{1000} & w_{1001} & w_{1010} & w_{1011} \end{pmatrix} \tag{5.12}$$

IY gate

When the state in Eqn (5.8) is acted on by the gate IY, equivalent to a translation in phase space by $(1, 1)$, one obtains the state in Eqn (5.13).

$$\begin{pmatrix} w_{1001} & w_{1000} & w_{1011} & w_{1010} \\ w_{1101} & w_{1100} & w_{1111} & w_{1110} \\ w_{0001} & w_{0000} & w_{0011} & w_{0010} \\ w_{0101} & w_{0100} & w_{0111} & w_{0110} \end{pmatrix} \tag{5.13}$$

YI gate

When the state in Eqn (5.8) is acted on by the gate YI, equivalent to a translation in phase space by (ω, ω), one obtains the state in Eqn (5.14).

$$\begin{pmatrix} w_{0110} & w_{0111} & w_{0100} & w_{0101} \\ w_{0010} & w_{0011} & w_{0000} & w_{0001} \\ w_{1110} & w_{1111} & w_{1100} & w_{1101} \\ w_{1010} & w_{1011} & w_{1000} & w_{1001} \end{pmatrix} \tag{5.14}$$

***Cnot*, *Hadamard*, $\frac{\pi}{4}$ and $\frac{\pi}{8}$ gates**

The *Cnot* (controlled-not) gate is defined by the matrix in the Z-basis:

$$Cnot = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{5.15}$$

We discovered that using the quantum net proposed by Wootters (which we have been using unless otherwise noted) in this case did not lead to a simple formula for the *Cnot* gate. If one instead uses Aravind's net and acts upon the state in Eqn (5.8) with the *Cnot* gate, one gets the elegant form shown in Eqn (5.16):

$$\begin{pmatrix} w_{0100} & w_{0101} & w_{0111} & w_{0110} \\ w_{1000} & w_{1001} & w_{1011} & w_{1010} \\ w_{1100} & w_{1101} & w_{1111} & w_{1110} \\ w_{0000} & w_{0001} & w_{0011} & w_{0010} \end{pmatrix} \tag{5.16}$$

The Wigner function transforms in a more complicated manner under the *Hadamard* gate and the $\frac{\pi}{8}$ gate as one may show. One may obtain the result of operating on a 2-qubit state by any unitary operator using the construction explained at the beginning of the section. It is necessary to use a computer for

this, as there are many terms involved. We used the math program Maple to determine the effect of these gates on Wigner functions, but the result was too complicated to usefully report here. The $\frac{\pi}{4}$ is denoted by S and the $\frac{\pi}{8}$ gate is denoted T. The forms of the $Hadamard$, S and T gates are as follows

$$Hadamard = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{5.17}$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{5.18}$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix} \tag{5.19}$$

For details on the use of these gates see [9].

5.3 Quantum Tomography

In quantum tomography, or quantum state estimation, the problem is to determine an unknown quantum state of which a large number of identical copies are given. Both the continuous and discrete Wigner function can be determined by quantum tomography. The continuous case has been discussed extensively in the book by Leonhardt [8]; the discrete case is discussed here.

To determine the DWF of a 2-qubit system by quantum tomography, one divides the copies of the system into 5 groups. A measurement of a pair of commuting observables is carried out on each of these groups, the observables being the ones shown in the first column of Table 5.1 (only the first pair of observables in each triplet need to be measured). The measurements are used to estimate the probabilities of measuring each state $|\lambda\rangle$.

Using Eqn (3.28) from Ch. 3 ($W_\beta = \frac{1}{N}\left[\sum_{\lambda \ni \beta} P(|\lambda\rangle) - 1\right]$), one can construct the WF from the measured probabilities. For example, consider a system where both qubits are up along z. The probability of measuring both qubits up along z is one and the probability of measuring any other pair of z eigenstates is zero. The probability of measuring any pair of eigenvalues in any of the other bases is $\frac{1}{4}$. Therefore, the elements along the Z-up-up axis are $\frac{1}{4}(1 + 4 \cdot \frac{1}{4} - 1) = \frac{1}{4}$, and all others are $\frac{1}{4}(0 + 4 \cdot \frac{1}{4} - 1) = 0$. This fits what one expects.

	++	+-	-+	--
X_1, X_2	37/76	13/76	1/76	25/76
Y_1, Y_2	13/76	13/76	1/76	49/76
Z_1, Z_2	4/76	16/76	40/76	16/76
X_1Y_2, Y_1Z_2	9/76	13/76	45/76	9/76
Y_1X_2, Z_1Y_2	37/76	13/76	25/76	1/76

Table 5.1: Example Probabilities for Quantum Tomography

For a more complicated example, consider the probabilities in Table 5.1. The Wigner elements can be found again using Eqn (3.28). For example, the lower-left Wigner element is obtained as $w_{0000} = \frac{1}{4}\left[37/76 + 13/76 + 4/76 + 45/76 + 13/76 - 1\right] = 9/76$. The complete Wigner function can be found in Table 5.2.

$\leftarrow\leftarrow$	-3/76	10/76	12/76	6/76
$\leftarrow\rightarrow$	-3/76	6/76	4/76	-6/76
$\rightarrow\leftarrow$	1/76	-6/76	0/76	18/76
$\rightarrow\rightarrow$	9/76	6/76	24/76	-2/76
	$\uparrow\uparrow$	$\uparrow\downarrow$	$\downarrow\uparrow$	$\downarrow\downarrow$

Table 5.2: Wigner Function for Example Quantum Tomography

Using Eqn (3.26) ($\rho = \sum_\alpha W_\alpha A_\alpha$), one can find ρ. Diagonalizing ρ yields the original state $|\psi\rangle = \frac{1}{\sqrt{19}}\left(|\uparrow\uparrow\rangle + 2\,|\uparrow\downarrow\rangle + (3+i)\,|\downarrow\uparrow\rangle - 2i\,|\downarrow\downarrow\rangle\right)$.

5.4 Superdense Coding

It is not immediately obvious how much information one can transmit using a qubit. By preparing a qubit in one of the two Z-eigenstates and giving it to another person, one can easily transmit 1 classical bit using 1 qubit. However, it is possible to do better. A scheme called superdense coding allows one to transmit two classical bits by transmitting 1 qubit – if the parties are already in possession of a pair of entangled qubits [9].

Suppose Alice is trying to send 2 classical bits to Bob. A third party prepares a pair of entangled qubits in the singlet state and sends one each to Alice and

Bob. The singlet state's discrete Wigner function is shown below.

$$\begin{array}{cccccc} \leftarrow\leftarrow & 0 & 0 & 0 & 0 \\ \leftarrow\rightarrow & 0 & 1/4 & 1/4 & 0 \\ \rightarrow\leftarrow & 0 & 1/4 & 1/4 & 0 \\ \rightarrow\rightarrow & 0 & 0 & 0 & 0 \\ & \uparrow\uparrow & \uparrow\downarrow & \downarrow\uparrow & \downarrow\downarrow \end{array} \tag{5.20}$$

If the first bit Alice wants to send is a 1, she applies the X gate to her qubit, otherwise she does nothing. If the second bit Alice wants to send is a 1, she applies the Z gate to her qubit, otherwise she does nothing. As mentioned earlier in this chapter, applying the X gate to the first qubit swaps the first two and last two columns of the Wigner function. If Alice applies the X gate, the resulting Wigner function is:

$$\begin{array}{cccccc} \leftarrow\leftarrow & 0 & 0 & 0 & 0 \\ \leftarrow\rightarrow & 1/4 & 0 & 0 & 1/4 \\ \rightarrow\leftarrow & 1/4 & 0 & 0 & 1/4 \\ \rightarrow\rightarrow & 0 & 0 & 0 & 0 \\ & \uparrow\uparrow & \uparrow\downarrow & \downarrow\uparrow & \downarrow\downarrow \end{array} \tag{5.21}$$

Similarly, the Z gate swaps the first and last pair of rows of the Wigner function. Regardless of what Alice sends, the resulting Wigner function is of the form:

$$\begin{array}{cccccc} \leftarrow\leftarrow & d & b & b & d \\ \leftarrow\rightarrow & c & a & a & c \\ \rightarrow\leftarrow & c & a & a & c \\ \rightarrow\rightarrow & d & b & b & d \\ & \uparrow\uparrow & \uparrow\downarrow & \downarrow\uparrow & \downarrow\downarrow \end{array} \tag{5.22}$$

where all of a, b, c, d are 0 except for one which is $1/4$. Nonzero a, b, c, d correspond respectively to sending 00, 01, 10, 11. These states correspond to the famous Bell basis, but we do not need that for this analysis, so we do not prove it here.

One can easily verify that the Bell states are all pure and mutually orthogonal

using Eqn (3.29):

$$|\langle\psi_1|\psi_2\rangle|^2 = \mathrm{Tr}(\rho_1\rho_2) = N\sum_\alpha W_\alpha V_\alpha \tag{5.23}$$

where $|\psi_1\rangle$ and $|\psi_2\rangle$ have Wigner elements W_α and V_α respectively.

Alice then physically gives her qubit to Bob. Bob then makes a measurement on the two qubits in the Bell basis. Since these states are orthogonal, a measurement can differentiate the states with perfect reliability. Bob thereby deduces the two bits Alice sent.

Chapter 6

Conclusions

This report showed how the discrete Wigner function (DWF) can be developed in a manner analogous to the continuous Wigner function. The DWF representation for n qubits is defined on a discrete phase space of $2^n \times 2^n$ points. The values of the DWF at the phase space points are always real, but they can be negative. Summing along a line in phase space gives the probability of measuring the associated eigenstate. Galois Fields provide the discrete analog of real numbers essential for the construction of the discrete Wigner function.

One difficulty delaying the application of the DWF is the difficulty in combining 1-qubit DWFs to make a many-qubit DWF. Since different quantum nets have different crossing formulae, this problem is closely related to the problem of choosing an appropriate quantum net. We discussed how two 1-qubit DWFs can be combined using a simple direct product if the 1-qubit DWFs use different quantum nets. It remains to be discovered why this works and how to combine 3 or more qubits.

The DWF can be used to visualize quantum computations. We discussed how to express arbitrary rotations of a single qubit using the DWF. We showed how various 2-qubit gates, including IX, IY, and IZ, and the controlled-not gate, can be expressed using the DWF. These gates allow any quantum computation using 2 qubits to be visualized without complex numbers. Once crossing formulae are discovered for an arbitrary number of qubits, the controlled-not and 1-qubit gates can be combined to simulate any quantum computation.

In quantum tomography, the DWF can be used to easily determine the state of a large number of identically prepared systems. The DWF naturally produces a set of mutually unbiased bases which provide the most accurate reconstruction

possible for a given number of measurements. The DWF also eases the calculations involved in reconstructing the state from the measurements.

The DWF provides a valuable tool for visualizing 2-qubit quantum computations without complex numbers. Once crossing formulae for more qubits are developed, the DWF will be a valuable tool for many qubits.

Appendix A

2-Qubit 16×16 Matrices

A.1 2-Qubit Hadamard Matrix

The Hadamard matrix for 2 qubits relating $\vec{S}$ to $\overrightarrow{W}$ by $\vec{S} = H\overrightarrow{W}$ using Wootters's quantum net.

$$H = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
-1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\
-1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\
-1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
-1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1
\end{pmatrix} \tag{A.1}$$

A.2 2-Qubit J Matrix

The J matrix relates the density vector $\vec{\rho}$ to the density coefficient vector $\vec{S}$ by $\vec{\rho} = J\vec{S}$. The J matrix makes finding gate operations on 2 qubits easy.

$$J = \frac{1}{4}\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & -i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -i & 0 \\
0 & 1 & -i & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -i & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -i & 0 & -i & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & 0 & -i & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & -i & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & i & 0 & 0 & 0 \\
0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & i & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -i & 0 & i & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 1 & -i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & i & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & 0 & i & -1 & 0 & 0 & 0 & 0 \\
0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -i & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -i & 0 \\
1 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix} \tag{A.2}$$

Appendix B

3 Qubit Arithmetic Tables

The primitive polynomial is taken as: $\pi(x) = x^3 + x^2 + 1$. The field elements are then: $GF(2^3) = \{0,1,\omega,\omega^2,\omega^3,\omega^4,\omega^5,\omega^6\}$. Note that $\omega^3 = \omega^2 + 1$. Also note that $\omega^7 = 1$. It turns out that there are 7 field bases $\{e_i\}$ in $GF(2^3)$ that have a dual basis $\{e'_i\}$ that may be multiplied by an element α of $GF(2^3)$ to get $f_i = \alpha e'_i = e_i$. The field bases with their dual and multiplicative factor to return the original basis are also given below:

n	ω^n	$tr(\omega^n)$
0	1	1
1	ω	1
2	ω^2	1
3	$\omega^2 + 1$	0
4	$\omega^2 + \omega + 1$	1
5	$\omega + 1$	0
6	$\omega^2 + \omega$	0

basis	dual	α
$(1, \omega, \omega^3)$	$(\omega^2, \omega^3, \omega^5)$	ω^5
$(1, \omega^2, \omega^6)$	$(\omega^4, \omega^6, \omega^3)$	ω^3
$(1, \omega^4, \omega^5)$	$(\omega, \omega^5, \omega^6)$	ω^6
$(\omega, \omega^2, \omega^4)$	$(\omega, \omega^2, \omega^4)$	1
$(\omega, \omega^5, \omega^6)$	$(1, \omega^4, \omega^5)$	ω
$(\omega^2, \omega^3, \omega^5)$	$(1, \omega, \omega^3)$	ω^2
$(\omega^3, \omega^4, \omega^6)$	$(\omega^6, 1, \omega^2)$	ω^4

The following table shows addition in $GF(8)$.

$+$	0	1	ω	ω^2	ω^3	ω^4	ω^5	ω^6
0	0	1	ω	ω^2	ω^3	ω^4	ω^5	ω^6
1	1	0	ω^5	ω^3	ω^2	ω^6	ω	ω^4
ω	ω	ω^5	0	ω^6	ω^4	ω^3	1	ω^2
ω^2	ω^2	ω^3	ω^6	0	1	ω^5	ω^4	ω
ω^3	ω^3	ω^2	ω^4	1	0	ω	ω^6	ω^5
ω^4	ω^4	ω^6	ω^3	ω^5	ω	0	ω^2	1
ω^5	ω^5	ω	1	ω^4	ω^6	ω^2	0	ω^3
ω^6	ω^6	ω^4	ω^2	ω	ω^5	1	ω^3	0

The following table shows multiplication in $GF(8)$.

$\times$	0	1	ω	ω^2	ω^3	ω^4	ω^5	ω^6
0	0	0	0	0	0	0	0	0
1	0	1	ω	ω^2	ω^3	ω^4	ω^5	ω^6
ω	0	ω	ω^2	ω^3	ω^4	ω^5	ω^6	1
ω^2	0	ω^2	ω^3	ω^4	ω^5	ω^6	1	ω
ω^3	0	ω^3	ω^4	ω^5	ω^6	1	ω	ω^2
ω^4	0	ω^4	ω^5	ω^6	1	ω	ω^2	ω^3
ω^5	0	ω^5	ω^6	1	ω	ω^2	ω^3	ω^4
ω^6	0	ω^6	1	ω	ω^2	ω^3	ω^4	ω^5

Bibliography

[1] P.K. Aravind, Z. Naturforsch **58a**, 2212 (2003).

[2] P.K. Aravind, personal communication (2004).

[3] R. Feynman, "Negative Probabilities" in *Quantum Implications: Essays in Honour of David Bohm*, edited by B. Hiley and D. Peat (Routledge, London, 1987).

[4] K.S. Gibbons, M.J. Hoffman, and W.K. Wootters, Phys.Rev A70, 062101 (2004) quant-ph/0401155

[5] H. Goldstein, C. Poole, and J. Safko, *Classical Mechanics, 3rd Edition*, (Addison Wesley, San Francisco, 2002).

[6] M. Hillery, R.F. OConnell, M.O. Scully, and E.P. Wigner, Phys. Rep. **106**, 123 (1984).

[7] M. Koniorczyk, V. Buzek, J. Janszky, Phys. Rev A64, 034301 (2001).

[8] U. Leonhardt, *Measuring the Quantum State of Light*, (Cambridge University Press, Cambridge, 1997).

[9] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, 2000).

[10] J.P. Paz, A.J. Roncaglia and M. Saraceno, "Qubits in phase space: Wigner function approach to quantum error correction and the mean king problem", quant-ph/0410117

[11] W.K. Wootters, quant-ph/0306135.