Quantum t-design

by

Mohammad Derakhshani

(20236816)

An essay
presented to the University of Waterloo
in fulfillment of the
requirement for the degree of
Master of Science
in
Mathematics

under the guidance of

Prof. Debbie Leung

Waterloo, Ontario, Canada, 2008

Abstract

The Classical notions of Computation are rapidly entering Quantum Computation. People try to find Quantum counterparts for Classical concepts.

In this essay, we will discuss about classical t-design, the quantum counterpart, Mutual Unbiased bases and a new technique for evaluating the expectation of a polynomial over Haar measure.

Acknowledgements

I would like to thank my advisor Prof. Debbie Leung and Prof. Andris Ambainis for introducing me to this the area and their guidance. Also I would like to thank Abhinav Bahadur for our joint work on the problem and my essay reader, Prof. Ashwin Nayak for his comments.

Mohammad Derakhshani
August 24, 2008

Contents

List of Figures

Chapter 1

Introduction

For a long time, algorithm and computation were equivalent to what we know today as classical computation. The fundamental model of classical computation is Turing machine. Informally speaking, Turing machine is a mathematical model for computation with a head, an infinite tape, and a finite transition table. The head reads a symbol written on a cell of the infinite tape and is able to alter the content of the cell and move right or left according to the finite transition table stored internally. In the late 1960s and early 1970s [12, 8] people observed that it seemed Turing machine model of computation is as strong as other models of computations. It is strong in the sense that if a particular problem can be solved efficiently in one model of computation also it can be efficiently solved in the Turing machine model. The strong Church-Turing thesis hypothesized this observation:

> Any algorithmic process which can be performed on any hardware can be simulated efficiently using a Universal Turing machine.

In the mid 1970s, Robert Solovay and Volker Strassen found a randomized algorithm to test whether an integer is prime or coprime. This algorithm used randomness as an essential resource. At that time there was no deterministic version for primality test; so it was proposed that computers with a random number generator as a resource would be able to solve problems more efficiently. This was the first challenge to the strong Church-Turing thesis. The result was a modification to the strong Church-Turing thesis:

> Any algorithmic process can be simulated efficiently using a probabilistic Turing machine.

The probabilistic Turing machine is a Turing machine which chooses among possible transitions based on some probability distribution. Informally speaking, it is a Turing machine with access to a random number generator.

The unpredicted modification to Church-Turing thesis left some people in doubt. How could we be sure that this version of Church-Turing thesis would not need a new

modification to cover new things? With this motivation in mind some people began to investigate to find a model of computation which is guaranteed to be able to efficiently simulate any other model of computations. To give the most fundamental answer to this question we should think about laws of the world in which a real Turing machine can operate. The Turing machine fully works in the classical world of physics. Considering the fact that a process which inherently is not a classical phenomenon might not be simulated efficiently using classical physics, Feynman proposed the notion of Quantum Computation. Deutsch introduced the notion of a Universal Quantum Computer and proposed a problem which was solved more efficiently on a Quantum Computer.

For a long time, People work on Classical Algorithms and in general Classical Computation and so there are a variety of concepts and techniques built to deal with a problem in Classical Computation. A lot of problems were studied in Classical Computation. In theory part of Quantum Computing, one trend is to study the same problems once studied in Classical Computation. Counterpart concepts of the classical problems are firstly defined and then studied in Quantum Computation, e.g, Quantum Complexity classes.

In this essay the concept of t-design and its quantum counterpart will be studied. We will deal with the definition of the classical t-design, mutually unbiased bases and the concept of Cubature formula in integration, and then we will define quantum t-design and will cover a few related topics including an alternative proof on the formula related to the expectation of monomials over the Haar-measure which is my small contribution.

1.1 Mathematical Formalism of Quantum Computing

The Quantum Mechanical laws governing the world of Quantum Computing can largely be expressed in terms of Linear Algebra. In this chapter we are going to build up the preliminaries needed for this essay.

The notion of a classical bit in a quantum computer is substituted by the notion of a quantum bit. A classical bit's state is either 0 or 1. A quantum bit, say $|\psi\rangle$, can be in any linear combination of two base states, let's say $|0\rangle$ and $|1\rangle$, which can be realized using two distinct states of a quantum system, e.g., spins of an electron. We show this linear superposition using the following notation:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{where } |\alpha|^2 + |\beta|^2 = 1$$

If a device measures $|\psi\rangle$ to read its value, the outcome will be $|0\rangle$ with probability of $|\alpha|^2$ or $|1\rangle$ with probability of $|\beta|^2$. All quantum states can be seen as elements of a Hilbert space.

1.1.1 Hilbert Space

Definition 1.1.1. *An Inner product space is a vector space V defined over a field $\mathbb{F}$ with an inner product. The inner product function $\langle\cdot|\cdot\rangle : V \times V \mapsto \mathbb{F}$ has the following properties:*

1. $\langle v|u\rangle = \overline{\langle u|v\rangle}$
2. $\langle av|u\rangle = a\langle v|u\rangle$
3. $\langle v + w|u\rangle = \langle v|u\rangle + \langle w|u\rangle$
4. $\langle v|v\rangle \geq 0$
5. $\langle v|v\rangle = 0$ *if and only if* $v = 0$.

Definition 1.1.2. *A Hilbert space is a real or complex inner product space where the norm function* $\|\cdot\| : V \mapsto \mathbb{R}$ *defined by*

$$\|x\| = \sqrt{\langle x, x\rangle}$$

We can combine two Hilbert spaces to get a larger one. This combination can be expressed in terms of the direct sum or the tensor operation. If we are given two Hilbert spaces H_1 and H_2 with inner products $\langle\cdot|\cdot\rangle_1$ and $\langle\cdot|\cdot\rangle_2$ then we can define a new Hilbert space $H = H_1 \otimes H_2$ to be the vector space with vectors of the form

$$\sum_j \alpha_j \psi_1^j \otimes \psi_2^j, \quad \text{where } \psi_1^j \in H_1 \text{ and } \psi_2^j \in H_2$$

And, the inner product of H will be defined as

$$\langle \phi_1 \otimes \phi_2 | \psi_1 \otimes \psi_2\rangle = \langle \phi_1|\psi_1\rangle_1 \langle \phi_2|\psi_2\rangle_2$$

This expansion of Hilbert spaces using tensor operation gives us a very strange and powerful tool known as entanglement. We can make states of the form $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2$. Suppose we give Alice the part corresponding to the first Hilbert space and Bob the second part. Then if Alice measures her Qubit and gains $|0\rangle$ (or $|1\rangle$), the part of Bob collapses to $|0\rangle$ (or $|1\rangle$). This notion will be covered later.

1.1.2 Quantum Sates

The world of Quantum bits is Hilbert space, and any normalized element in the Hilbert state can represent a Quantum state or Quantum bit.

If $|\psi_i\rangle \in \mathcal{H}$ for $i = 1, \ldots, n$ then any linear combination of them given by

$$|\psi\rangle = \alpha_1|\psi_1\rangle + \cdots + \alpha_n|\psi_n\rangle$$

lies in the Hilbert space H.

We represent the elements of the Hilbert space $\mathcal{H}$ by "ket" vectors $|\cdot\rangle$. The "bra" vectors will represent the duals of elements of $\mathcal{H}$, e.g., $\langle\psi| = |\psi\rangle^*$ where $|\psi\rangle \in \mathcal{H}$. The "braket" notation $\langle\phi|\psi\rangle$ stands for the inner product of $|\phi\rangle$ and $|\psi\rangle$.

If the dimesion of $\mathcal{H}$ is n then we can choose an orthonormal basis for $\mathcal{H}$, say $\{|i\rangle\}_{i=1}^{n}$. Then any state like $|\phi\rangle$ can be uniquely expressed as a linear superposition of the elements of this basis. Let's have $|\phi\rangle = \alpha_1|1\rangle + \cdots + \alpha_n|n\rangle$. If we measure $|\phi\rangle$ in the same basis the outcome of the measurement will be $|i\rangle$ with the probability of $|\alpha_i|^2$. Since the sum of the probabilities should be one we have

$$\sum_{i=1}^{n} |\alpha_i|^2 = 1$$

1.1.3 Quantum Operations

The Quantum Mechanical laws describe two kinds of operations:

1. Unitary Transformation
2. Measurements

Definition 1.1.3. *The state of an isolated quantum system evolve according to a Unitary Linear map. A system in the state $|\psi\rangle$, after evolving according to a unitary map U, evolves to the state corresponding to $U|\psi\rangle$.*

The famous Pauli matrices $\sigma_x, \sigma_y, \sigma_z$ are unitary matrices defined by

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

Definition 1.1.4. *Quantum Projective measurements are described by a collection $\{M_m\}$ of measurement operators each of which describes the projection of the state onto a subspace. These operators satisfy in the following equation:*

$$\sum_{m} M_m^\dagger M_m = I$$

If a pure state $|\psi\rangle$ is measured the probability of observing the outcome m will be

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

and the state of the system after the measurement will be

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

1.1.4 Entanglement

Let $\{|h_i\rangle\}$ be the basis of the Hilbert space $\mathcal{H}$, and $\{|k_j\rangle\}$ be the basis of the Hilbert space $\mathcal{K}$ then $\{|h_i\rangle \otimes |k_j\rangle\}$ is the basis for the Hilbert space $\mathcal{H} \otimes \mathcal{K}$. In $\mathcal{H} \otimes \mathcal{K}$ we can have any state in the linear combination of $\{|h_i\rangle \otimes |k_j\rangle\}$ in the form of

$$|\psi\rangle = \sum_{ij} \alpha_{ij}|h_i\rangle|k_j\rangle, \text{where } \textstyle\sum_{ij} |\alpha_{ij}|^2 = 1$$

This tensor product composition gives us the entanglement property which is not seen in classical physics.

Definition 1.1.5. *Entanglement is a quantum mechanical phenomomen in which two quatum systems are linked together such that no description is adequate to describe the behaviour of one of them without considering the other one. This entanglement can be preserved between two or more objects although they become spatially far separated.*

Suppose we prepare $|\psi\rangle$ in the following state

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum_i |h_i\rangle|k_i\rangle$$

and then give the half corresponding to $\mathcal{H}$ to Alice and the other half corresponding to $\mathcal{K}$ to Bob. Then upon Alice measures her qubit and get $|h_i\rangle$ for some i Bob's state will collapse to the state with the same index $|k_i\rangle$.

1.1.5 Density Matrix

Definition 1.1.6. *A density matrix is a Hermition positive-semidefinite matrix of trace one that describes the state of a quantum system. For a pure state $|\psi\rangle$ the density matrix representation is defined by*

$$|\psi\rangle\langle\psi|$$

.

Consider a random generator generating a number from the set $\{1, \ldots, n\}$ where the number i is picked with probability of p_i. Now suppose Alice uses this random number generator, and upon receiving i from this random number generator makes a state $|\psi_i\rangle$ and sends that state to Bob without telling him the number i. Therefore the state of the quantum system Bob receives will be

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$$

Intuitively speaking, Bob's quantum state is a mixed state.

Definition 1.1.7. *A* **mixed state** *is an ensemble* (p_i, ρ_i)*. That is a probability distribution over density operators. So the density matrix of the system can be described by*

$$\rho = \sum_i p_i \rho_i$$

Density matrix representation is another representation for quantum systems. If we apply the unitary evolution U on the system of the state of $|\psi\rangle$, the state of the system will evolve to $U|\psi\rangle$. Similarly the density matrix evolution of this system can be represented by

$$|\psi\rangle\langle\psi| \mapsto U|\psi\rangle\langle\psi|U^\dagger$$

Just by studying the definition of a mixed state it can be seen that in the general case the unitary evolution U of a system with the density matrix ρ can be described by

$$\rho \mapsto U\rho U^\dagger$$

Chapter 2

Discrete Design

2.1 Block Design

Definition 2.1.1. *A block design $\mathcal{D}$ with parameters (v, b, r, k, λ) consists of a point set V of v points and block set $\mathcal{B}$ with b blocks, where each of the blocks is a k-subset of V, such that the following conditions hold:*

1. *each point lies on exactly r blocks.*
2. *each pair of points lies on exactly λ blocks.*

The above design is called a 2-design.

Example 2.1.2. *The following is a block design with parameters $(v, b, r, k, \lambda) = (7, 7, 3, 3, 1)$.*

$$\{0, 1, 3\}$$
$$\{1, 2, 4\}$$
$$\{2, 3, 5\}$$
$$\{3, 4, 6\}$$
$$\{4, 5, 0\}$$
$$\{5, 6, 1\}$$
$$\{6, 0, 2\}$$

The parameters of a design are not independent. Let's take a pair (x, α) where $x \in V$ and $\alpha \in \mathcal{B}$ such that x lies on α. If we first choose x then α, we have v choices for x and r choices for α such that α contains x. If we first choose α then x, we have b choices for α and k choices for x such that x lies on α. Therefore we have the following equality:

$$vr = bk \tag{2.1}$$

Now let's take (x, y, α) where $x \neq y \in \alpha$. Similarly by choosing x, y in $v(v-1)$ ways we will have λ ways to choose α. Conversely by choosing α in b ways we will have $k(k-1)$ ways to choose x, y. Therefore we have the following equality:

$$v(v-1)\lambda = bk(k-1) \tag{2.2}$$

From the above two equality we can conclude that

$$(v-1)\lambda = r(k-1) \tag{2.3}$$

2.2 Classical t-design

Definition 2.2.1. *Generalized t-design is a class of k-subsets of point set V such that the number of blocks, say b_i, that contain any chosen i-subset of V is independent of the choice of the i-subset for all $i = 1, \ldots, t$.*

Again the parameters of the design are not independent. The following equations will hold [3]:

$$b_i = b_t \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}, \text{for } i = 0, \ldots, t \tag{2.4}$$

With the above definition we can conclude that the prior defined block design is 2-design. Design theory has very important applications in other fields such as Code Design.

Suppose the machine A_1 is a random number generator which generates uniformly independent numbers $x_1, x_2, \ldots, x_k$ from the set $V = \{1, 2, \ldots, n\}$. The machine A_2 uses a pre-determined t-design on the set V whose block size is k. This machine picks a number from the set $\{1, 2, \ldots, b\}$ where b is the block size. Then it will output the elements of the k-th block. We are given these two oracles one of the first type and the other of the second type, but we do not know which is which. We want to find out which oracle is of which type.

By running machine A we are allowed to uniformly at random pick t elements of its k-set output and read those elements. It can be shown that using the described procedure it is not possible to distinguish between A_1 and A_2.

Later we will define the notion of Quantum t-design which has some similarities with the above problem.

2.3 Mutually Unbiased Basis

One of the very basic principles of Quantum Mechanics is that position and momentum are two complementary observables. That is if we know one of them with certainty, we

cannot know anything about the other one. This arises from the fact that their corresponding operators are not commutative. We can see Mutually Unbiased Basis from the same viewpoint.

Definition 2.3.1. *Two quantum mechanical observables are called complementary if and only if precise knowledge of one of them implies zero knowledge of the other one that is all possible outcomes are possible with equal probability.*

There is a one-to-one correspondence between non-degenerate complementary observables and mutually unbiased bases.

Definition 2.3.2. *Suppose $x_1, x_2 \ldots, x_d$ and $y_1, y_2 \ldots, y_d$ are two orthogonal bases in $\mathbb{C}^d$. If there is a constant γ such that for all choices of $i, j = 1, 2, \ldots, d$ the norm of inner product of x_i and x_j is γ we say they are unbiased:*

$$\langle x_i|y_j\rangle\langle y_j|x_i\rangle = \gamma, \textit{ for all } i, j = 1, 2, \ldots, d$$

A set of orthonormal bases is mutually unbiased if each pair of bases is unbiased.

Now suppose H_1 and H_2 are two hermitian $d \times d$ matrices whose eigenbases B_1 and B_2 are Mutually Unbiased. Let quantum qubit $|\psi\rangle$ be prepared in an eigenbasis of H_1, i.e., $|\psi\rangle = b_{1i} \in B_1$. If we measure observable H_1 following by measuring H_2 we will get one of the eigenbasis of H_2, say b_{2j} with probability $\langle b_{1i}|b_{2j}\rangle = 1/d$. That means observables H_1 and H_2 are two complementary observables. Conversely eigenbases of two arbitrary complementary observable H_1 and H_2 are mutually unbiased provided that the eigenbases are non-degenerate.

Mutually Unbiased Bases also plays a role in Quantum Tomography. The Quantum Tomography is the process of reconstructing quantum state using measurement on many state copies. We are given a source of unknown quantum state $|\psi\rangle$. Using a large number of measurements for an observable $H = \sum_{b\in B} x_b|b\rangle\langle b|$ we can find all the statistics $\mathrm{Tr}(\rho|b\rangle\langle b|)$ for all the eigenvalues of H. The question is how many distinct observables are needed to be measured to reconstruct $|\psi\rangle$. It is found that at least $d + 1$ distinct observables should be measured. Also the lower bound $d + 1$ is enough when we use $d + 1$ non-degenerate pairwise complementary observables. A simple example of this process is when Pauli Matrices $\sigma_x, \sigma_y, \sigma_z$ are used as observables to reconstruct a 2×2 density matrix.

Consider the following example for a set of 3 Mutually Unbiased Bases in the Hilbert space of dimension 2.

$$\begin{aligned}
B_1 &= \{|0\rangle, |1\rangle\}, \\
B_2 &= \{|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}\}, \\
B_2 &= \{|+i\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, |-i\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}\}
\end{aligned}$$

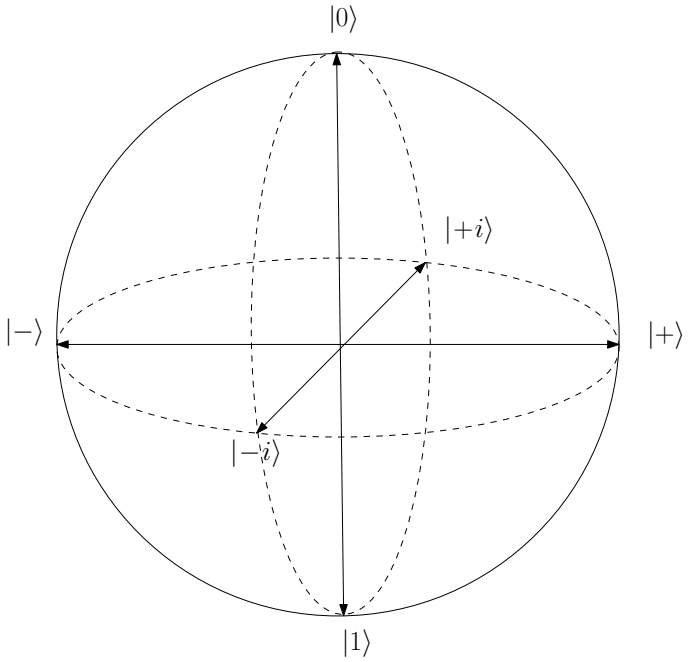

Figure 2.1: A set of 3 Mutually Unbiased Bases in the Hilbert space of dimension 2.

Since for each x_i and y_j chosen from distinct bases we have $|\langle x_i|y_j\rangle| = \frac{1}{\sqrt{2}}$ using the interpretation above the corresponding angle is $\frac{\pi}{4}$. Figure 2.1 shows that on the Bloch sphere the angles are double.

Now we will have a few properties. Since $x_1, x_2, \ldots, x_d$ forms a basis we have $|y_j\rangle = \sum_i \langle x_i|y_j\rangle|x_i\rangle$. So we have

$$\langle y_j|y_j\rangle = \sum_i |\langle x_i|y_j\rangle|^2 = d\gamma$$

Therefore $\gamma = \frac{1}{d}$. One interpretation of $|\langle x_i|y_j\rangle|^2$ is the angle between the lines spanned by x_i and y_j. In the above example it can be seen that 3 is maximal. It is suggested that in a Hilbert space of dimension d there are at most $d+1$ mutually-unbiased bases. Later we will come back to this and show some construction for special cases.

Mutually Unbiased Basis was introduced by Schwinger [14]. Suppose B_1 and B_2 are two unbiased bases. If a state $|\psi\rangle$ is prepared as a state of B_i and then measured in basis B_j where $i \neq j$ no information about $|\psi\rangle$ is revealed. This is one of the key ideas in BB84 QKD protocol where as long as the choice of basis in unknown no one can gain any information about the key.

2.3.1 Constructions

One fundamental question to be answered is how many mutually unbiased bases in dimension d we can have. This problem is solved partially for prime power dimensions. In

general Let's define MUB : $\mathbb{N} \mapsto \mathbb{N}$ as the following:

$$\text{MUB}(n) = \max\{|\mathcal{B}| : \mathcal{B} \text{ is the set of MUBs in } \mathbb{C}^n\}$$

Then the following properties are known:

- MUB$(p^r) = p^r + 1$ for prime number p.
- MUB$(n) \leq n + 1$
- MUB$(mn) \geq \min\{\text{MUB}(m), \text{MUB}(n)\}$
- MUB$(d^2) \geq N(d)$, where $N(d)$ is the number of mutually orthogonal Latin squares of size $d \times d$.

There are different constructions for mutually unbiased basis. We will discuss a few of them here. By giving these construction the truth of the above facts will be shown.

For add prime power dimension we have the following construction given by Wootters and Fields [16]. Let p be any odd prime number, and , w_p be the pth root of unity $\exp(2\pi i/p)$. For a and b in $\text{GF}(p^k)$ define $|\psi_b^a\rangle$ as the following:

$$|\psi_b^a\rangle = \frac{1}{\sqrt{p^k}} \sum_{x \in \text{GF}(p^k)} w_p^{\text{Tr}(ax^2+bx)} |x\rangle$$

where $\text{Tr}(z)$ for $z \in \text{GF}(p^k)$ is defined as

$$\text{Tr}(z) = z^{p^0} + z^{p^1} + \cdots + z^{p^{d-1}}$$

Theorem 2.3.3. *For any odd prime p, the sets*

$$B_a = \{|\psi_b^a\rangle | b \in \text{GF}(p^k)\}, \textit{where } a \in \text{GF}(p^k)$$

with the computational basis form a set of $d + 1$ *mutually unbiased bases.*

Proof. We have

$$\langle \psi_b^a | \psi_{b'}^{a'} \rangle = \frac{1}{p^k} \left| \sum_{x \in \text{GF}(p^k)} w_p^{\text{Tr}((a'-a)x^2+(b-b')x)} \right|$$

If $|\psi_b^a\rangle$ and $|\psi_{b'}^{a'}\rangle$ are from the same basis then $a = a'$ and that means

$$\langle \psi_b^a | \psi_{b'}^a \rangle = \frac{1}{p^k} \left| \sum_{x \in \text{GF}(p^k)} w_p^{\text{Tr}((a'-a)x^2} \right|$$

Therefore if $b = b'$ we have $\langle \psi_b^a | \psi_{b'}^a \rangle = 1$ and if $b \neq b'$ we have $\langle \psi_b^a | \psi_{b'}^a \rangle = 0$.

Lemma 2.3.4. *Suppose $\mathbb{F}_q$ is a finite field of odd characteristic. Let $\mathcal{X}$ be a non-trivial additive character of $\mathbb{F}_q$. Let $P(X)\mathbb{F}_q[X]$ be a polynomial of degree 2. Then*

$$\left|\sum_{x\in\mathbb{F}_q}\mathcal{X}(P(x))\right| = \sqrt{q}$$

For a proof you can refer to [11]

If $a \neq a$, $|\psi_b^a\rangle$ and $|\psi_{b'}^{a'}\rangle$ are from distinct bases. Now using the above lemma we have

$$\begin{aligned}\langle\psi_b^a|\psi_{b'}^{a'}\rangle &= \frac{1}{p^k}\left|\sum_{x\in\mathrm{GF}(p^k)} w_p^{\mathrm{Tr}((a'-a)x^2+(b'-b)x}\right| \\ &= \frac{1}{\sqrt{d}}\end{aligned}$$

□

In dimension 3 the above construction gives us the following bases

$$\begin{aligned}B_0 &= \{\frac{1}{\sqrt{3}}(1,1,1), \frac{1}{\sqrt{3}}(1,w_3,w_3^2), \frac{1}{\sqrt{3}}(1,w_3^2,w_3)\}, \\ B_1 &= \{\frac{1}{\sqrt{3}}(1,w_3,w_3), \frac{1}{\sqrt{3}}(1,w_3^2,1), \frac{1}{\sqrt{3}}(1,1,w_3^2)\}, \\ B_2 &= \{\frac{1}{\sqrt{3}}(1,w_3^2,w_3^2), \frac{1}{\sqrt{3}}(1,w_3,1), \frac{1}{\sqrt{3}}(1,1,w_3)\}.\end{aligned}$$

So B_0, B_1, B_2 with the computational basis form four mutually unbiased bases.

The above construction only works for odd prime power dimensions. For dimensions of the power of 2 we have the following construction:

Let $G(4,n)$ be a finite Galois ring with Teichmuller set $\mathcal{T}_n$ Then define

$$|\psi_a^b\rangle = 2^{-n/2}\sum_{x\in\mathcal{T}_n} w_4^{\mathrm{Tr}(a+2b)x}|x\rangle$$

Theorem 2.3.5. *For any prime of 2, say 2^n, the sets*

$$B_a = \{|\psi_b^a\rangle | b \in \mathcal{T}_n(p^k)\}, \textit{where } a \in \mathcal{T}_n$$

with the computational basis form a set of $2^n + 1$ mutually unbiased bases.

For a proof, refer to [2].

In dimension 4 the above constructing gives us the following bases:

$$\begin{aligned}
B_0 &= \{\frac{1}{2}(1,1,1,1), \frac{1}{2}(1,1,-1,-1), \frac{1}{2}(1,-1,-1,1), \frac{1}{2}(1,-1,1,-1)\},\\
B_1 &= \{\frac{1}{2}(1,-1,i,-i), \frac{1}{2}(1,-1,i,i), \frac{1}{2}(1,1,i,-i), \frac{1}{2}(1,1,-i,i)\},\\
B_2 &= \{\frac{1}{2}(1,-i,-i,-1), \frac{1}{2}(1,-i,i,1), \frac{1}{2}(1,i,i,-1), \frac{1}{2}(1,i,-i,1)\},\\
B_3 &= \{\frac{1}{2}(1,-i,-1,-i), \frac{1}{2}(1,-i,1,i), \frac{1}{2}(1,i,1,-i), \frac{1}{2}(1,i,-1,i)\},
\end{aligned}$$

The above four bases together with the computational basis are 5 MUBs in $\mathbb{C}^4$.

2.4 Cubature

In mathematics integration plays an important role, and that is to evaluate

$$\int_a^b f(x)dx$$

In some cases carrying out numerical integration is the only option in evaluating an integration. There are a few reasons to evaluate an integration using numerical methods:

- The value of integrand, $f(x)$, is only known at specific points, for example, via sampling.
- It is difficult to find an antiderivative, for example when $f(x) = exp(x^2)$
- Computing a numerical approximation for a known antiderivative is hard, for example when the antiderivative is given as an infinite series.

To overcome these issues a number of numerical quadrature techniques were introduced. The main idea behind them is interpolating. Simpson's rule is one of them:

$$\int_a^b f(x)dx \approx \frac{(b-a)}{6}\left(f(a) + 4f(\frac{a+b}{2}) + f(b))\right)$$

There is a generalization to these approximation integrations to higher dimensions.

Definition 2.4.1. *Let μ be a measure on $\mathbb{R}^n$ with finite moments. A cubature formula of degree t for μ is a set of points $F = \{\overrightarrow{p_a}\} \in \mathbb{R}^n$ and a weight function $\overrightarrow{p_a} \mapsto w_a \in \mathbb{R}$ such that*

$$\int P(\overrightarrow{x})d\mu = \sum_{a=1}^{N} w_a P(\overrightarrow{p_a})$$

for some polynomial P of degree at most t. Also we refer to $\sum_{a=1}^{N} w_a P(\overrightarrow{p_a})$ using the notation $P(F)$.

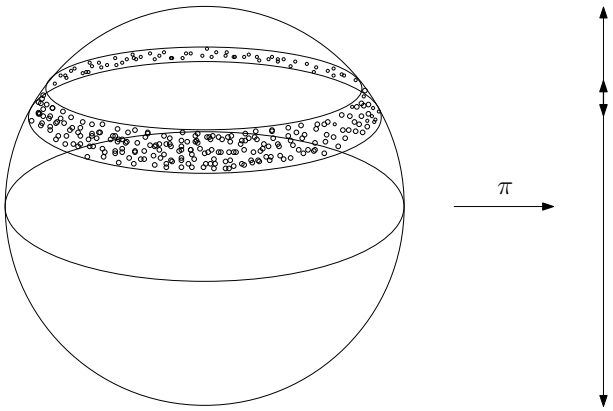

Figure 2.2: Archimedes' hat-box theorem

In the above definition if $n = 1$, then F is also called a quadrature formula which is the same notion discussed in the numerical integration section. There is motivation to determine how many points are needed for a given formula and a given degree t to make the cubature formula as simple as possible. We will discuss later about equal-weight formula under the name of *t-designs*.

2.5 Connection between Quadrature and Cubature

The main question to be answered in this section is to show a connection between quadrature on the interval $[-1, -1]$ and cubature on the unit sphere S^2, both with uniform measure.

Let's define π to be the orthogonal projection from S^2 to the z coordinate. Then according to Archimedes' hat-box theorem for any interval $I \in [a, b]$ the area of $\pi^{-1}(I)$ is proportional to the length of I [10]. We can conclude that if F is a t-cubature formula on S^2, then $\pi(F)$ is a t-cubature on $[-1, 1]$.

Using this conclusion we can derive a few well-known quadrature formula using cubature formula on S^2. The vertices of a regular octahedron form a 3-design on S^2. Figure 2.3 shows that by projecting this formula we get Simpson's rule If we project the same set of points using a different projection we get 2-point Gauss-Legendre quadrature shown in figure 2.4.

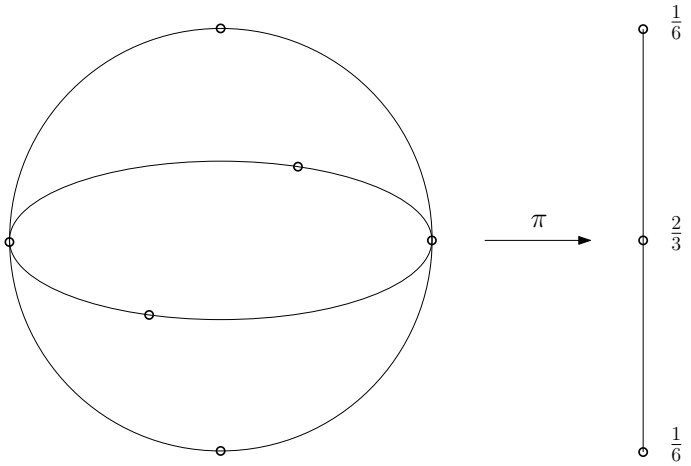

Figure 2.3: Simpson's rule: If the vertices of a regular octahedron which form a 3-design on S^2 is projected on $[-1, 1]$ in the above way, we will get the familiar Simpson's rule.

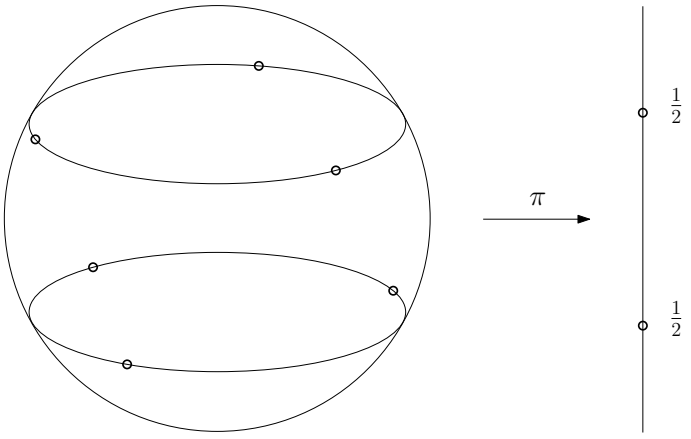

Figure 2.4: 2-point Gauss-Legendre rule: Using a different projection of the vertices of a regular octahedron on $[-1, 1]$ we will get the 2-point Gauss-Legendre rule.

Chapter 3

Quantum t-design

3.1 Introduction

Formerly, we talked about cubature formulas for evaluating integrations. Intuitively speaking, the idea of cubature formulas can be extended to the Quantum world in which integrand is a quantum state picked from some special measure. Suppose we have two quantum machines C and D. Machine C upon running outputs t copies of a quantum state $|\psi\rangle$ picked up from a continues probability distribution, while machine D outputs t copies of a quantum state $|\psi_i\rangle$ where i is chosen from a discrite probability distribution. Suppose D acts in a way that its output cannot be distinguished from the output of C. That means if one is given one of the two machines as an oracle, knowing the probability distribution of C, cannot determine which machine is given to him or her using any possible Quantum Operation on the output of the machine he or she is possessed.

Formally speaking, what we want is a disjoint probability distribution over quantum states $(p_i, |\phi_i\rangle)$ such that

$$\sum_i p_i(|\phi_i\rangle\langle\phi_i|)^{\otimes t} = \int_\psi (|\psi\rangle\langle\psi|)^{\otimes t} d\psi$$

The integration in the right hand side is over Haar measure. Intuitively speaking, Haar measure is a uniform measure over $\mathbb{C}S^{d-1}$. For example, when the dimension of the space is 2, picking up states from Haar measure is equivalent to picking uniformly up states from the Block sphere (for more detail refer to the appendix).

To understand the space over which the integration is taken we have to study the space spanned by all states of the form $|\psi\rangle^{\otimes t}$. Let's call this space H_{sym}.

Suppose $\text{SWAP}_{i,j}$ is the operator acting on any state from $\mathcal{H}$ swaps the ith qubit with the jth qubit. Since $\text{SWAP}_{i,j}|\psi\rangle^{\otimes t} = |\psi\rangle^{\otimes t}$, $\text{SWAP}_{i,j} H_{\text{sym}} = H_{\text{sym}}$. So we can conclude that H_{sym} is the simultaneous eigenspace corresponding to $+1$ eigenvalue of $\text{SWAP}_{i,j}$ for all $i, j = 1, \ldots, t$.

The eigenvectors corresponding to the eigenvalue $+1$ of the SWAP operator can be easily determined.

For example, let the dimension of the space be $d = 2$ and suppose we are working with $t = 2$ copies, then the eigenbasis of SWAP operator and similarly H_{sym} are the normalized version of the following vectors:

$$|00\rangle, |11\rangle, |01\rangle + |10\rangle$$

We can easily generalized the above example for $d = 2$ and any t. Let $|b_n\rangle$ be defined as the following:

$$|b_n\rangle = \frac{1}{\sqrt{\binom{t}{n}}} \left(\sum_{\text{The number of 0s in } \{r_1, \ldots, r_t\} \text{ is } n} |r_1 r_2 \ldots r_t\rangle \right)$$

Then $\{|b_n\rangle\}_{n=0}^{t}$ is an eigenbasis of the SWAP operator and H_{sym}. This result can be easily generalized for any dimension d. Let's define

$$|b_{i_1,i_2,\ldots,i_d}\rangle = \frac{1}{\sqrt{\binom{t}{i_1,i_2,\ldots,i_d}}} \left(\sum_{\forall j : 1 \leq j \leq d \text{ the number of } j\text{s in } r_1, \ldots, r_d \text{ is } i_j} |r_1 r_2 \ldots r_t\rangle \right)$$

It is clear that for all $r, s = 1, \ldots, t$ we have $\text{SWAP}_{r,s}|b_{i_1,i_2,\ldots,i_d}\rangle = |b_{i_1,i_2,\ldots,i_d}\rangle$. If the sequences $i_1, i_2, \ldots, i_d$ and $j_1, j_2, \ldots, j_t$ differ in just one location, i.e., $i_m \neq j_m$, then all terms in corresponding sums of $|b_{i_1,i_2,\ldots,i_d}\rangle$ and $|b_{j_1,j_2,\ldots,j_t}\rangle$ will be different and so the terms are orthonormal to each other. Since the number of terms in the sum is $\binom{t}{i_1,i_2,\ldots,i_d}$ so $|b_{i_1,i_2,\ldots,i_d}\rangle$ is normalized.

Theorem 3.1.1. *$\{|b_{i_1,i_2,\ldots,i_d}\rangle\}$ is an eigenbasis for the simultaneous $+1$ subspace for all $\text{SWAP}_{i,j}$, where $i, j = 1, \ldots, t$. Similarly it forms a basis for H_{sym}.*

Proof. The key points of the above theorem were discussed. □

Corollary 3.1.2. *One important result of this theorem is that the dimension of H_{sym} is the number of non-negative integer solutions to the following equation:*

$$i_1 + i_2 + \cdots + i_d = t$$

Therefore the dimension of H_{sym} is $\binom{t+d-1}{t}$.

Theorem 3.1.3. *Let H_{sym} be the subspace spanned by all t-tensor states $|\psi\rangle^{\otimes t}$. Then we have*

$$\int_{\psi} |\psi\rangle\langle\psi|^{\otimes t} d\psi = \frac{I}{M}$$

Where $\frac{I}{M}$ is just the completely mixed state over H_{sym} and so M is the dimension of the H_{sym} evaluated above to be $\binom{t+d-1}{t}$.

Proof. [1] □.

Definition 3.1.4. *A probability distribution over quantum states $(p_i, |\phi_i\rangle)$ is a complex projective t-design if*

$$\sum_i p_i (|\phi_i\rangle\langle\phi_i|)^{\otimes t} = \int_\psi (|\psi\rangle\langle\psi|)^{\otimes t} d\psi$$

where the integrand $|\psi\rangle$ is taken from the Haar measure.

In the earlier work on this topic another definition, which is proved to be equivalent, for complex projective t-design was used.

Let $P(x_1, x_2, \ldots, x_d, y_1, y_2, \ldots y_d)$ be a polynomial of degree at most t in variables $x_1, x_2, \ldots x_d$ and degree at most t in variables $y_1, y_2, \ldots y_d$. For a quantum state $|\psi\rangle = \sum_{j=1}^{d} \alpha_j |j\rangle$ we define

$$P(\psi) = P(\alpha_1, \alpha_2, \ldots, \alpha_d, \alpha_1^*, \alpha_2^*, \ldots, \alpha_d^*)$$

The alternative definition for the complex projective t-design is given bellow:

Definition 3.1.5. *If for any arbitrary polynomial $P(x_1, x_2, \ldots x_d, y_1, y_2, \ldots y_d)$ of degree at most t in variables $x_1, x_2, \ldots x_d$ and degree at most t in variables $y_1, y_2, \ldots, y_d$ the following equation holds*

$$\int_\psi P(\psi) d\psi = \sum_i p_i P(\phi_i) \tag{3.1}$$

then, the probability distribution over quantum states $(p_i, |\phi_i\rangle)$ is a complex projective t-design.

3.2 Properties

Theorem 3.2.1. *The two given definitions, 3.1.5 and 3.1.4, for complex projective t-design are equivalent.*

Proof. It suffices to study the case in which P is a monomial since then we can take sum over different monomials to prove the theorem for the general case.

Let a probability distribution over $(p_i, |\phi_i\rangle)$ be a complex projective t-design according to the second definition. Therefore the equation (3.1) holds for each monomial of degree at most t in terms of the first d variables and degree at most t in terms of the second d variables.

Each entry of the density matrix of $\sum_i p_i (|\phi_i\rangle\langle\phi_i|)^{\otimes t}$ is an expectation of a monomial over $|\phi_i\rangle$s, and the corresponding entry in $\int_\psi (|\psi\rangle\langle\psi|)^{\otimes t}$ is also an expectation of the same monomial over the Haar measure. By taking polynomial P the monomial showing up in this entry, we can conclude that the corresponding entry in $\sum_i p_i (|\phi_i\rangle\langle\phi_i|)^{\otimes t}$ and $\int_\psi (|\psi\rangle\langle\psi|)^{\otimes t}$ are equal. Therefore our probability distribution is a complex projective t-design according to the first definition.

The other direction is quite the same as the first direction [1]. □

Theorem 3.2.2. *Suppose X is a finite subset of $\mathbb{C}S^{d-1}$. Then the following statements are equivalent:*

1. *X is a uniform t-design.*
2. *For all $|\psi\rangle \in \mathcal{H}$ and all $0 \leq k \leq t$ we have*

$$\frac{\langle\psi|\psi\rangle^k}{\binom{d+k-1}{k}} = \frac{1}{|X|}\sum_{|\phi\rangle\in X}|\langle\psi|\phi\rangle|^{2k}$$

3. *For all $0 \leq k \leq t$ we have*

$$\frac{1}{|X|^2}\sum_{|\psi\rangle,|\phi\rangle\in X}|\langle\psi|\phi\rangle|^{2k} = \frac{1}{\binom{d+k-1}{k}}$$

Proof. To show that 1 implies 2, we use theorem 3.1.3. Since X is a uniform t-design, all $p_i = \frac{1}{|X|}$. Therefore

$$\sum_i \frac{1}{|X|}(|\phi_i\rangle\langle\phi_i|)^{\otimes t} = \int_\psi (|\psi\rangle\langle\psi|)^{\otimes t}d\psi$$

Using theorem 3.1.3 we have

$$\begin{aligned}\frac{I}{M} &= \int_\psi (|\psi\rangle\langle\psi|)^{\otimes t}d\psi \\ &= \sum_i \frac{1}{|X|}(|\phi_i\rangle\langle\phi_i|)^{\otimes t}\end{aligned}$$

Here according to the theorem 3.1.3, I is the identity operator in H_{sym} space. Therefore for an arbitrary $|\psi\rangle \in \mathcal{H}$ we have

$$\begin{aligned}\frac{\langle\psi|\psi\rangle^k}{M} &= \langle\psi|^{\otimes t}\frac{I}{M}|\psi\rangle^{\otimes t} \\ &= \langle\psi|^{\otimes t}\left(\sum_i \frac{1}{|X|}(|\phi_i\rangle\langle\phi_i|)^{\otimes t}\right)|\psi\rangle^{\otimes t} \\ &= \sum_i \frac{1}{|X|}\langle\phi_i|\psi\rangle^k\langle\psi|\phi_i\rangle^k \\ &= \sum_i \frac{1}{|X|}|\langle\phi_i|\psi\rangle|^{2k}\end{aligned}$$

Now recall that $M = \binom{d+k-1}{k}$. So (1) implies (2).

The prove that (2) implies (3) we use (2), $|X|$ times with all possible values of elements of X for $|\psi\rangle$, then summing up the results will imply (3).

The proof that (3) implies (1) is a little bit tricky. The trick is to define

$$|v\rangle = \frac{1}{|X|}\sum_{|\psi\rangle\in X} |\psi\rangle^{\otimes k} \otimes \overline{|\psi\rangle}^{\otimes k} - \int_{\psi} |\psi\rangle^{\otimes k} \otimes \overline{|\psi\rangle}^{\otimes k} d|\psi\rangle$$

Then, it can be shown that $\langle v|v\rangle = 0$, and that means $|v\rangle = 0$. So X is a t-design.

3.3 Equivalence of MUBs and 2-designs

The importance of the above theorem is that it gives us a framework to study t-designs better, and a tool to check whether a given set of quantum states is a t design.

Theorem 3.3.1. *The states corresponding to a mutually-unbiased bases in a Hilbert space $\mathcal{H}$ of dimension d form a 2-design X in $\mathbb{C}S^{d-1}$.*

Proof. We use the theorem 3.2.2. Let X be the set of all the states corresponding to the mutually-unbiased bases. Then X has $d(d+1)$ elements, for $k=1$ we have

$$\begin{aligned}\frac{1}{|X|^2}\sum_{|\psi\rangle,|\phi\rangle\in X} |\langle\psi|\phi\rangle|^{2k} &= \frac{1}{d^2(d+1)^2}\left(2\binom{d+1}{2}\binom{d}{1}\binom{d}{1}\frac{1}{d} + \binom{d+1}{1}\binom{d}{1}\right)\\ &= \frac{1}{d}\\ &= \frac{1}{\binom{d+1-1}{1}}\end{aligned}$$

For $k=2$ we have

$$\begin{aligned}\frac{1}{|X|^2}\sum_{|\psi\rangle,|phi\rangle\in X} |\langle\psi|\phi\rangle|^{2k} &= \frac{1}{d^2(d+1)^2}\left(2\binom{d+1}{2}\binom{d}{1}\binom{d}{1}\frac{1}{d^2} + \binom{d+1}{1}\binom{d}{1}\right)\\ &= \frac{2}{d(d+1)}\\ &= \frac{1}{\binom{d+2-1}{2}}\end{aligned}$$

Therefore according to the thorem 3.2.2, X is a 2-design [9].

□

3.4 Polynomials Over Haar-measure

We call a monomial $P = \prod_{j=1}^{d} x_j^{c_j}(x_j^*)^{e_j}$ balanced if $c_j = e_j$ for all $j = 1, \ldots, d$. We have the following theorem:

Theorem 3.4.1. *For any unbalanced monomial P*

$$\int_{\psi} P(\psi)d\psi = 0$$

and the Haar-expectation of any balanced monomial of the form $P = \prod_{j=1}^{d} x_j^{c_j}(x_j^*)^{c_j}$ is

$$\int_{\psi} P(\psi)d\psi = \frac{c_1! \cdots c_d!}{(d+t-1)\cdots(d+1)d} \qquad \textit{where } t = \textstyle\sum_j c_j.$$

This theorem is provided and proved in [1]. Before this paper was officially published I found a simpler proof for this theorem, and presented it in our research meetings with one of the authors of this paper. The following proof gives us more intuition.

The idea of the proof lies in the proof of the equivalence of the two definitions of quantum t-design. That is to evaluate $\int_{\psi} P(\psi)d\psi$ we can look at the proper entry in the density matrix of $\int_{\psi}(|\psi\rangle\langle\psi|)^{\otimes t}d\psi$. Now note that for any density matrix ρ we have $\rho_{ij} = \langle i|\rho|j\rangle$ where $\{|k\rangle\}$ is an eigenbasis for the space in which ρ exists. Now note that $\int_{\psi}(|\psi\rangle\langle\psi|)^{\otimes t}d\psi$ lies in H_{sym} and we have evaluated the eigenbasis of H_{sym} before. So what we will do is to evaluate $\langle v|\int_{\psi}(|\psi\rangle\langle\psi|)^{\otimes t}d\psi|u\rangle$ for some $|u\rangle$ and $|v\rangle$ which are two elements of the eigenbasis of H_{sym}.

Proof. Recall the definition of $|b_{i_1,i_2,\ldots,i_d}\rangle$:

$$|b_{i_1,i_2,\ldots,i_d}\rangle = \frac{1}{\sqrt{\binom{t}{i_1,i_2,\ldots,i_d}}}\left(\sum_{\forall j\,:\,1\le j\le d \text{ the number of } j\text{s in } r_1,\ldots,r_d \text{ is } i_j} |r_1 r_2 \ldots r_t\rangle\right)$$

Just using the above definition we get

$$\langle b_{c_1,c_2,\ldots,c_d}|\psi^{\otimes t}\rangle = \frac{1}{\sqrt{\binom{t}{c_1,\ldots,c_d}}}\binom{t}{c_1,\ldots,c_d}\prod_{i=1}^{d}\langle i|\psi\rangle^{c_i} = \sqrt{\binom{t}{c_1,\ldots,c_d}}\prod_{i=1}^{d}\psi_i{}^{c_i} \quad (3.2)$$

Since

$$\int_{\psi}(|\psi\rangle\langle\psi|)^{\otimes t}d\psi = \frac{I}{M}$$

we have

$$\begin{aligned}\int_{\psi}\langle b_{c_1,c_2,\ldots,c_d}|\psi^{\otimes t}\rangle\langle\psi^{\otimes t}|b_{e_1,e_2,\ldots,e_d}\rangle d\psi &= \langle b_{c_1,c_2,\ldots,c_d}|\frac{I}{M}|b_{e_1,e_2,\ldots,e_d}\rangle \\ &= \frac{1}{M}\langle b_{c_1,c_2,\ldots,c_d}|b_{e_1,e_2,\ldots,e_d}\rangle \\ &= \frac{1}{M}\delta_{c_1,e_1}\delta_{c_2,e_2}\cdots\delta_{c_d,e_d} \qquad (3.3)\end{aligned}$$

By using the equations (3.2) and (3.3) we get

$$\int_\psi \sqrt{\binom{t}{c_1,\ldots,c_d}} \prod_{i=1}^{d} {\psi_i}^{c_i} \sqrt{\binom{t}{e_1,\ldots,e_d}} \prod_{i=1}^{d} \psi_i^{*e_i} d\psi = \int_\psi \langle b_{c_1,c_2,\ldots,c_d} | \psi^{\otimes t} \rangle \langle \psi^{\otimes t} | b_{e_1,e_2,\ldots,e_d} \rangle d\psi$$
$$= \frac{1}{M} \delta_{c_1,e_1} \delta_{c_2,e_2} \cdots \delta_{c_d,e_d}$$

Therefore if $c_j \neq e_j$ we have

$$\int_\psi \prod_{i=1}^{d} {\psi_i}^{c_i} \psi_i^{*e_i} d\psi = 0$$

and

$$\int_\psi \prod_{i=1}^{d} {\psi_i}^{c_i} \psi_i^{*e_i} d\psi = \binom{t}{c_1,\ldots,c_d} \int_\psi \langle b_{c_1,c_2,\ldots,c_d} | \psi^{\otimes t} \rangle \langle \psi^{\otimes t} | b_{e_1,e_2,\ldots,e_d} \rangle d\psi$$
$$= \frac{1}{\binom{t+d-1}{t}\binom{t}{c_1,\ldots,c_d}}$$
$$= \frac{c_1! \cdots c_d!}{(d+t-1)\cdots(d+1)d}$$

3.5 Future work

3.5.1 Efficient Construction

For Quantum 2-designs, construction with $O(d^2)$ states is known where d is the dimension of the space. For an arbitrary t in dimension d, a construction by $O(t^d)$ states was found by Hayashi [7]. The problem is $O(t^d)$ is only efficient when the dimension d which is the power of the polynomial in $O(t^d)$ is fixed. So for the cases when d is much larger than t we have to look for other constructions.

3.5.2 Approximate Construction of t-design

One solution to this issue is to find inexact approximate t-design. Intuitively speaking, that is a discrete distribution over $(p_i, |\phi_i\rangle)$ with the property that the construction it gives us is close enough to what we want.

The notion of closeness to an ideal t-design can be defined in many different ways using many different norms. The one chosen in the [1] uses l_∞ norm:

Definition 3.5.1. *A probability distribution over quantum states $(p_i, |\phi_i\rangle)$ is an ϵ-approximate t-design if*

$$(1-\epsilon) \int_\psi (|\psi\rangle\langle\psi|)^{\otimes t} d\psi \leq_\infty \sum_i p_i (|\phi_i\rangle\langle\phi_i|)^{\otimes t} \leq_\infty (1+\epsilon) \int_\psi (|\psi\rangle\langle\psi|)^{\otimes t} d\psi$$

and

$$\sum_i p_i(|\phi_i\rangle\langle\phi_i|)^{\otimes t} = \int_\psi (|\psi\rangle\langle\psi|)^{\otimes t} d\psi$$

In the above definition $A \leq_\infty B$ means $B-A$ is a positive semidefinite, and $\| A \|_\infty \leq \| B \|_\infty$. For more detail on ∞-norm refer to the appendix.

For a fixed constant t and for every $d \geq 2t$ [1] gives a construction of an $O(\frac{1}{d^{1/3}})$-approximate t-design.

Appendix A

Mathematical preliminaries

A.1 Measure Theory

In studying the set theory, to be able to compare the volume of subsets of a set, we define a mathematical model to formally assign a value to each subset based on its volume. Specially when the universal set is not discrete, such model becomes very useful.

Definition A.1.1. *A subset Σ of the power set of a set X is a σ-algebra if and only if it has the following properties:*

1. *Σ is non-empty.*
2. *If $E \in \Sigma$ then $E^c \in \Sigma$.*
3. *If $E_1, E_2, E_3, \ldots$ is a countably sequence of sets in Σ, then $\bigcup_i E_i \in \Sigma$.*

The above properties can be summarized: Σ contains X, Σ is closed under complements, and Σ is closed under countable unions.

Definition A.1.2. *A measure μ is a function defined on a σ-algebra Σ over a set X and takes values from the interval $[0, \infty]$ such that the following properties hold:*

- *The measure of the empty set is zero:*

$$\mu(\{\}) = 0$$

- *Countable additivity: if $E_1, E_2, E_3, \ldots$ is a countable sequence of pairwise disjoint sets in Σ, then the measure of the union of them is equal to the sum of the measures of each of them:*

$$\mu\left(\bigcup_{i=1}^{\infty} E_i\right) = \sum_{i=1}^{\infty} \mu(E_i)$$

One can simply interpret probability distribution over events as a measure. In that case the measure function should satisfy $\mu(X) = 1$.

Definition A.1.3. *A probability measure is a measure $\mu : X \mapsto [0, 1]$ where $\mu(X) = 1$.*

Now we define the Haar measure which was used for evaluating expectation of a polynomial. Consider the case when $\mathcal{H}$ is a Hilbert space of dimension 2. Each normalized $|\psi\rangle \in \mathcal{H}$ by ignoring its phase can be visualize in the Bloch sphere. If we talk about expectation of a function $f(\cdot)$ over Haar-measure, $\int_\psi f(\psi)d\mu(\psi)$, what we mean is the expectation of $f(\psi)$ when $|\psi\rangle$ moves uniformly on the Block sphere. The idea of moving uniformly over Block sphere can guide us to understand Haar-measure when when $\mathcal{H}$ has the arbitrary dimension d.

Definition A.1.4. *Let G be a locally compact group. Then a left invariant Haar measure on G is a measure μ which satisfies the following properties:*

- *$\mu(aE) = \mu(E)$ for every $a \in G$ and every measurable E over G.*
- *$\mu(A) > 0$ for every non-empty open set A over G.*
- *$\mu(A) < 1$ for every compact set K over G.*

A.2 Topology

Definition A.2.1. *A metric space M is a space for which a metric function $d : M \times M \mapsto \mathbb{R}$ is defined such that*

1. $d(x, y) \geq 0$.
2. $d(x, y) = 0$ *if and only if* $x = y$.
3. $d(x, y) = d(y, x)$.
4. $d(x, y) \leq d(x, z) + d(z, y)$.

We show the metric space M with the metric function d as the pair (M, d).

Definition A.2.2. *In the metric space (M, d), the ball $B_r(x)$ for any positive real r and $x \in M$ is defined as*

$$B_r(x) = \{y \in M : d(x, y) < r\}$$

Definition A.2.3. *A set O in a metric space (M, d) is called open if for each $x \in O$ there is a neighbourhood set $B_r(x)$ for some positive real r, such that $B_r(x) \subseteq O$.*

Definition A.2.4. *A set C in a metric space (M, d) is called closed if its complement set is open.*

Definition A.2.5. *A subset K of the Euclidean space $\mathbb{R}^n$ is called compact if it is closed and bounded.*

A.3 Group Theory

The definition of compactness and openness used in the definition A.1.4 are given in the Topology section of the appendix. For deeper understanding of group theory, a classical group theory textbook [4] can be used.

Definition A.3.1. *A non-empty set G with a binary operation $\cdot$ on G is called a group if the following properties hold:*

1. $a(bc) = (ab)c$ *for all* $a, b, c \in G$.
2. *There exist a identity element* $e \in G$ *such that* $ea = a$ *for all* $a \in G$.
3. *For every* $a \in G$ *there exist an inverse* $a^{-1} \in G$ *such that* $a^{-1}a = e$.

Definition A.3.2. *An abelian group, is a group $(G, *)$ with the property that the group operation $*$ is commutative that is for all $a, b \in G$ we have $a * b = b * a$.*

Definition A.3.3. *The system $(\mathcal{F}, +, \cdot)$ where $\mathcal{F}$ is a nonempty set and $+, \cdot$ are binary operations on $\mathcal{F}$ is called* **field** *if the following properties hold:*

1. $\mathcal{F}$ *is an abelian group respect to the additive group operation* $+$.
2. $\mathcal{F} \setminus \{0\}$ *is an abelian group respect to the multiplicative group operation* $\cdot$.
3. *The multiplicative operation $\cdot$ distributes over the additive operation $+$:*

$$x(y + z) = xy + sz$$

Definition A.3.4. *A manifold is a space in which neighbourhood of each point resembles the Euclidean space, but the global structure may be more complicated.*

Let S^{d-1} be the sphere of unit vectors in the complex vector space $\mathbb{C}^d$. Two vectors $u, v \in S^{d-1}$ are called equivalent $u \equiv v$ if and only if $u = e^{i\theta}v$ for some real θ. Note that if S^1 is the Block sphere and if $u \equiv v$ then u and v have the same representation in the Block sphere. Let $\mathbb{C}S^{d-1}$ be the quotient manifold $S^{d-1}/\equiv$.

Definition A.3.5. *The system $(R, +, \cdot)$ where R is a nonempty set and $+, \cdot$ are binary operations on R is called* **ring** *if the following properties hold:*

1. R *is an abelian group respect to the additive group operation* $+$.
2. $(R, \cdot)$ *is a monoid with identity* 1 *that is*

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$
$$1 \cdot a = a \cdot 1 = a$$

3. *The multiplicative operation $\cdot$ is distributive over the additive operation $+$:*

$$x(y+z) = xy + xz$$
$$(y+z)x = yx + zx$$

Each field is a ring with two more properties. A field is a commutative ring with an multiplicative inverse for every non zero element.

Definition A.3.6. *Let R be a ring. A left* **ideal** *I of R is a nonempty subset $I \subset R$ with the following properties:*

1. *$x - y \in I$ for all $x, y \in I$*
2. *$r \cdot x \in I$ for all $a \in I$ and $r \in R$.*

Definition A.3.7. *A quotient ring is a ring that is the quotient of a ring A and one of its ideals I, denoted A/I. In general, a quotient ring is a set of equivalence classes where $[x] = [y]$ if and only if $x - y$ in I.*

Definition A.3.8. *A finite field or* **Galois field** *is a field that contains finitely many elements. A finite field with q elements is denoted by $\mathrm{GF}(q)$.*

Definition A.3.9. Galois Ring *is a finite ring isomorphic to the quotient ring $\mathbb{Z}_{p^k}[X]/(P)$ where p is a prime and P is a unitary polynomial with the property that $P \mod p$ is an irreducible polynomial with coefficients in $\mathrm{GF}(p)$. We denote $\mathrm{GR}(p^k, m)$ the Galois ring isomorphic to $\mathbb{Z}_{p^k}[X]/(P)$ where P has degree m*

Definition A.3.10. *The set of roots of $X^{p^m-1} - 1$ is a cyclic multiplicative group of order $p^m - 1$. By adding 0 to this we get the set $\mathcal{T} = \{0, \zeta, \ldots, \zeta^{p^m-1}\}$ where ζ is a generator of the cyclic group. We call this set the* **Tiechmuller set** *[6].*

Definition A.3.11. Characteristic of a field *is the smallest number n such that adding up the identity of the field n-times to itself gives zero of the field. Therefore*

$$\underbrace{1 + 1 + \cdots + 1}_{n} = 0$$

For any finite field of q elements for some prime number p we have $q = p^k$. In a finite fields with p^k elements where p is a prime, $\mathrm{GF}(p^k)$, the characteristic is p.

If $\mathbb{F}$ is a field of Characteristic p, then the following map is an automorphism of the field $\mathbb{F}$ and fixes elements in the prime field $\mathbb{Z}_p$:

$$\sigma : x \mapsto x^p$$

For a field $\mathbb{F}$ subfield of $\mathcal{E}$ when $|\mathcal{E} : \mathbb{F}| = d$ we define the trace of an element of $\mathbb{F}$ relative to the extension $\mathcal{E}/\mathbb{F}$ in the following way:

$$\mathrm{Tr}_{\mathcal{E}/\mathbb{F}}(z) = z + \sigma(z) + \cdots + \sigma^{d-1}(z)$$

If $z \in \mathcal{E}$ then $\mathrm{Tr}_{\mathcal{E}/\mathbb{F}}(z)$ is fixed by σ and lies in $\mathbb{F}$.

A.4 Archimedes' Hat-Box theorem

Theorem A.4.1. *If two parallel planes of distant h cut of a sphere of radios r into a slice, then the aria of the surface of the slice enclosed by the two planes is equal to the area of a slice on a cylinder of radius r produced by the same two planes perpendicular to its axis.*

Therefore the surface of the slice is $2\pi h$.

A.5 Operator Norm

Definition A.5.1. *In the Hilbert space $\mathcal{H}$, the spectral norm or the operator norm of an operator A is defined as*

$$\| A \| = \max\{\| Au \| : u \in \mathcal{H}, \| u \| = 1\}$$

By the above definition $\| A \|$ is the largest singular value of the operator A. This norm also is called ∞-norm and can be shown by $\| A \|_\infty$ [15].

List of References

[1] Andris Ambainis and Joseph Emerson. Quantum t-designs: t-wise independence in the quantum world. In *CCC '07: Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity*, pages 129–140, Washington, DC, USA, 2007. IEEE Computer Society. 17, 18, 21, 22, 23

[2] Somshubhro Bandyopadhyay, P. Oscar Boykin, Vwani Roychowdhury, and Farrokh Vatan. A new proof for the existence of mutually unbiased bases. 12

[3] Thomas Beth, Dieater Jungnickel, and Hanfried Lenz. *Design theory*. Cambridge University Press, New York, NY, USA, 1986. 8

[4] Prabir Bhattacharya, S. K. Jain, and S. R. Nagpaul. *Basic Abstract Algebra*. Cambridge University Press, 1994. 26

[5] Christoph Dankert. Efficient simulation of random quantum states and operators. 2005.

[6] Marc P. C. Fossorier, Tom Høholdt, and Alain Poli, editors. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 15th International Symposium, AAECC-15, Toulouse, France, May 12-16, 2003, Proceedings*, volume 2643 of *Lecture Notes in Computer Science*. Springer, 2003. 27

[7] A. Hayashi, T. Hashimoto, and M. Horibe. Reexamination of optimal quantum state estimation of pure states. *Physical Review A*, 72:032325, 2005. 22

[8] Mika Hirvensalo. *Quantum computing*. Springer-Verlag New York, Inc., New York, NY, USA, 2001. 1

[9] Andreas Klappenecker and Martin Roetteler. Mutually unbiased bases are complex projective 2-designs. 2005. 20

[10] Greg Kuperberg. Numerical cubature from archimedes' hat-box theorem. *SIAM J. Numer. Anal.*, 44(3):908–935, 2006. 14

[11] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge, revised edition, 1994. 12

[12] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, October 2000. 1

[13] Walter Rudin. *Real and complex analysis, 3rd ed.* McGraw-Hill, Inc., New York, NY, USA, 1987.

[14] Julian Schwinger. Unitary operator bases. *The National Acad- emy of Sciences of the USA*, page 46:570579, 1960. 10

[15] John Watrous. Theory of quantum information. Lecture Notes in CPSC 519/619 Quantum Computation, pages 2–5, 2006. 28

[16] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191:363–381, May 1989. 11