DISCRETE QUANTUM THEORIES AND COMPUTING

Yu-Tsung Tai

(戴淯琮)

Submitted to the faculty of the University Graduate School
in partial fulfillment of the requirements
for the degree
Doctor of Philosophy
in the Department of Mathematics
and the Department of Computer Science,
Indiana University
July 1, 2018

Accepted by the Graduate Faculty, Indiana University, in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Doctoral Committee

Amr A. Sabry (عمرو صبري), PhD

Gerardo Ortiz, PhD

Dylan Paul Thurston, PhD

Andrew J. Hanson, PhD

Shouhong Wang (汪守宏), PhD

Defense Date

DEDICATION

I would like to dedicate my thesis to my parents, Cheng-Tien Tai (戴振沺) and Feng-Ming Chang (張鳳鳴). Thanks for encouraging me to study abroad and all your support during my Ph.D. study.

ACKNOWLEDGMENTS

Thank Prof. Gerardo Ortiz, Prof. Amr Sabry (عمرو صبري), and Prof. Andrew Hanson for publishing three papers [1, 2, 3] with me, and enormous other things. These papers become the main part of my thesis, especially most of Chapter 3 is based on “Geometry of discrete quantum computing”[1] and “Discrete quantum theories”(DQT) [2]; most of Chapter 4 is based on “Quantum Interval-Valued Probability: Contextuality and the Born Rule”(QIVPM) [3]. Together with Prof. Dylan Thurston and Prof. Shouhong Wang (汪守宏), thank you for getting together to understand what I did and passing my dissertation proposal Spring 2017. Also, thank Prof. Dylan Thurston for serving in my advisory committee and my Tier 3 committee, with other advisory committee members passing my Computer Science qualifying exam Spring 2016. Especially, my survey of real computation in the qualifying exam inspires me the comparison of quantum computer and analog computer in Chapter 1. Chapter 1 also contains the motivation in my application for Rethinking Foundations of Physics 2017 workshop reviewed by Prof. Amr Sabry (عمرو صبري). Thank Prof. Lawrence Moss for inviting me to present our results in the interdisciplinary logic seminar and theory seminar in Computer Science, co-chairing my Tier 3 committee, writing an assessment letter for me, and drawing my attention on Prof. Abramsky’s paper [4], which inspired me to merge quantum probability with discrete quantum theories. Thank John Gardiner for inspiring discussion on the difficulties merging them [5]. These results are improved and motivated the transition from DQT to QIVPM in Sec. 3.9. Thank Prof. Tom Lewis for helping me organize the unpublished deterministic quantum algorithms in the term paper for SLST-T501 Academic Writing course as presented in Sec. 3.4. Thank Traci Nagle for

going through the literature review about finite precision measurement and contextuality discussed for CSCI-Y790 Writing and Editing course as presented in Sec. 2.5. Also, thank Elizabeth “Betsy” Merceron and Kexin “Casey” Chen (谌可心) for teaching me English in general so that others can understand me more easily.

Many people in both department of Mathematics and Computer Science need to do something more to make my double-major works smoothly. I need to thank all of them, especially directors of graduate study in Mathematics, especially Prof. Christopher Judge and Prof. Matthias Weber; directors of Ph.D. study in Computer Science, especially Prof. Yuqing Melanie Wu (吴愈青) and Prof. Funda Ergun.

Thank Meng-Wei Chen (陳孟瑋) as my best friend and roommate in Bloomington. Thank Hao-Chun Lee (李浩君) and Hsien-Ching Kao (高憲慶) for discussing what I did in the prospective of a general Ph.D. in Physics, and working later in more computational industry.

Finally, thank Jin-Ru Yang (楊謹如) for everything could not be written here.

PREFACE

- The latest version of this thesis is in GitHub:

https://github.com/yuttai/Contextuality-and-Nonlocality-in-Discrete-Quantum-Theory/blob/master/dissertation.pdf

- Its source code is typeset using LyX [6] in:

https://github.com/yuttai/Contextuality-and-Nonlocality-in-Discrete-Quantum-Theory/blob/master/dissertation.lyx

- Any address and comments can be left in the Issue part of the GitHub Repository:

https://github.com/yuttai/Contextuality-and-Nonlocality-in-Discrete-Quantum-Theory/issues

Yu-Tsung Tai

(戴淯琮)

DISCRETE QUANTUM THEORIES AND COMPUTING

Our primary research interest is to build a quantum computing model characterizing realistic quantum computers. While most of the quantum computing models based on uncomputable numbers, that is, the continuum of real numbers, most of the classical computers in our daily life are digital instead of analog computers. This highlight the necessity to investigate discrete models for quantum theory and computing. Specifically, we start from replacing the continuum of complex numbers by the discrete finite fields. Although we have fruitful results on their geometric implications and computing powers, their probability models are still not completely satisfactory. To address this issue, we further exploited quantum interval-valued probability, and proved an imprecise version of foundational results such as the Gleason and Kochen-Specker theorems.

Amr A. Sabry (عمرو صبري), PhD

Gerardo Ortiz, PhD

Dylan Paul Thurston, PhD

Andrew J. Hanson, PhD

Shouhong Wang (汪守宏), PhD

CONTENTS

Chapter 1

INTRODUCTION

This marriage of quantum mechanics and computer science first envisioned and popularized by Feynman has created an awkward, but opportune, moment. The embarrassing dilemma was concisely described by Aaronson with the following three statements [7, 8]:

(i) Textbook quantum mechanics is correct.

(ii) There does not exist an efficient classical factoring algorithm.

(iii) The extended Church-Turing thesis —that probabilistic Turing machines can efficiently simulate any physically realizable model of computation —is correct [9, 10].

There is overwhelming evidence to support each of these statements. The theoretical framework of quantum mechanics (i) has withstood decades of experimental confirmation. Entire industries are founded on the assumption (ii) that algorithms like RSA are secure and they also have withstood years of attempted attacks [11, 12]. Finally the entire field of complexity theory in computer science which has also withstood years of field testing rests, in essence, on assumption (iii) [13, 14]. And yet at least one of these three statements *must be false*! Indeed if there is a corresponding efficient classical factoring algorithm, then we concede (ii). If it is correct Shor's efficient factoring algorithm is realizable, and we can prove there is no efficient classical factoring algorithm, we concede (iii). Otherwise, if we cannot implement Shor's algorithm no matter how hard we try, textbook quantum mechanics, i.e., (i) may need to be improved by a better theory. It is unlikely that there will be a simple resolution to this awkward situation. It is more likely that the resolution will emerge from deep and careful analyses of the foundations of each field.

When we check the compatibility between quantum mechanics and computer science, we found their fundamental assumptions are different. On one hand, the quantum theory is based on infinitely precise real and complex numbers. Its prediction could fit the physical reality by utilizing error analysis technique although these prediction cannot be completely faithful because of the measurement precision. On the other hand, current computers mostly perform digital computation, except some analog chips communicating with physical world [15]. While the computability of digital parts is faithfully characterized by its theoretical model, the Turing machine [16], the computability of analog chips in reality is far weaker than the theoretical prediction of real computation [17, 18, 19, 20]. One of the reason behind this gap is also due to measurement precision, and some of their computability difference cannot be compensated by error analysis technique. All these problems for classical computation could potentially apply to quantum computation. Because we are agnostic about whether the physical reality is ultimately discrete or continuous, we tried to develop two different types of quantum theories and computing models to address these issues. Since the discrete classical computing model faithfully represents digital computers, we first tried to build discrete quantum theories and computing by considering quantum theories and computing over finite fields in Chapter 3. Since error analysis technique cannot always compensate the inevitable problem of measurement precision, we then incorporate the idea of finite precision measurement into the quantum theory in Chapter 4, and hope it could describe the physical reality and computability more faithful.

Chapter 2

CONVENTIONAL QUANTUM THEORY AND COMPUTING

The part of conventional quantum theory (CQT) used by quantum circuit model is described by the following:

(i) D orthonormal basis vectors for a Hilbert space of dimension D,

(ii) the normalized D complex probability amplitude coefficients describing the contribution of each basis vector,

(iii) a set of probability-conserving unitary matrix operators that suffice to describe all required state transformations of a quantum circuit,

(iv) and a measurement framework.

In Sec. 2.1, we focus on the discrete geometric issues raised by the properties (i) and (ii) given above for CQT. In Sec. 2.2, we introduce the important issues of (iv) and the foundations of quantum probability space. In Sec. 2.4, we address the property (iii) by describing product and entangled n-qubit states and unitary matrices in quantum circuit model.

2.1 GEOMETRICAL STRUCTURE OF STATES

There are many things that are assumed in CQT, such as the absence of zero norm states for non-zero vectors, and the decomposition of complex amplitudes into a pair of ordinary real numbers. One also typically assumes the existence of a D-dimensional Hilbert space with an orthonormal basis, allowing us to write *pure* states in general as Hilbert space vectors with an Hermitian inner product:

$$|\Psi\rangle \quad = \quad \sum_{i=0}^{D-1} \alpha_i \, |i\rangle \ . \tag{2.1}$$

Here $\alpha_i \in \mathbb{C}$ are complex probability amplitudes, $\vec{\alpha} \in \mathbb{C}^D$, and the $\{|i\rangle\}$ is an orthonormal basis of states obeying $\langle i|k\rangle = \delta_{ik}$.

The meaning of this is that any state $|\Phi\rangle = \sum_{i=0}^{D-1} \beta_i \, |i\rangle$ can be projected onto another state $|\Psi\rangle$ by writing

$$\langle \Phi|\Psi\rangle \quad = \quad \sum_{i=0}^{D-1} \beta_i^* \alpha_i \, , \tag{2.2}$$

thus quantifying the proximity of the two states. (Here * denotes complex conjugation.) This is one of many properties we take for granted in continuum quantum mechanics that challenge us in defining a discrete quantum geometry. To facilitate the transition to DQT carried out in later sections, we concern ourselves first with the properties of the simplest possible abstract state object in CQT, the single qubit state.

2.1.1 TWO-DIMENSIONAL HILBERT SPACE

A state in a two-dimensional Hilbert space, known as a qubit, already provides access to a wealth of geometric information and context. When we write the single qubit state as $|\psi_1\rangle = \alpha_0 \, |0\rangle + \alpha_1 \, |1\rangle$, a convenience for computing probability and relative state properties is the normalization condition

$$\|\psi_1\|^2 = |\alpha_0|^2 + |\alpha_1|^2 = \alpha_0^*\alpha_0 + \alpha_1^*\alpha_1 = 1\,, \tag{2.3}$$

which identifies α_0 and $\alpha_1 \in \mathbb{C}$ as probability amplitudes and implies the conservation of probability in the closed world spanned by $\{|0\rangle\,, |1\rangle\}$. Note that we distinguish for future use the *norm* $\|\cdot\|$ of a vector from the *modulus* $|\cdot|$ of a complex number. Continuing, we see that if we want only the irreducible state descriptions, we must supplement the process of computing Eq. (2.3) by finding a way to remove the distinction between states that differ only by an overall phase transformation $\mathrm{e}^{\mathrm{i}\theta}$, that is, $\alpha_0\,|0\rangle + \alpha_1\,|1\rangle$ and $\mathrm{e}^{\mathrm{i}\theta}\alpha_0\,|0\rangle + \mathrm{e}^{\mathrm{i}\theta}\alpha_1\,|1\rangle$ are representing the same physical state. This can be accomplished by the Hopf fibration [21, 22, 23, 24, 25, 26], which can be written down as follows: let $\alpha_0 = x_0 + \mathrm{i}y_0$ and $\alpha_1 = x_1 + \mathrm{i}y_1$. Then Eq. (2.3) becomes the condition that the four real variables describing a qubit denote a point on the three-sphere $\mathbf{S}^3$ (a 3-manifold) embedded in $\mathbb{R}^4$:

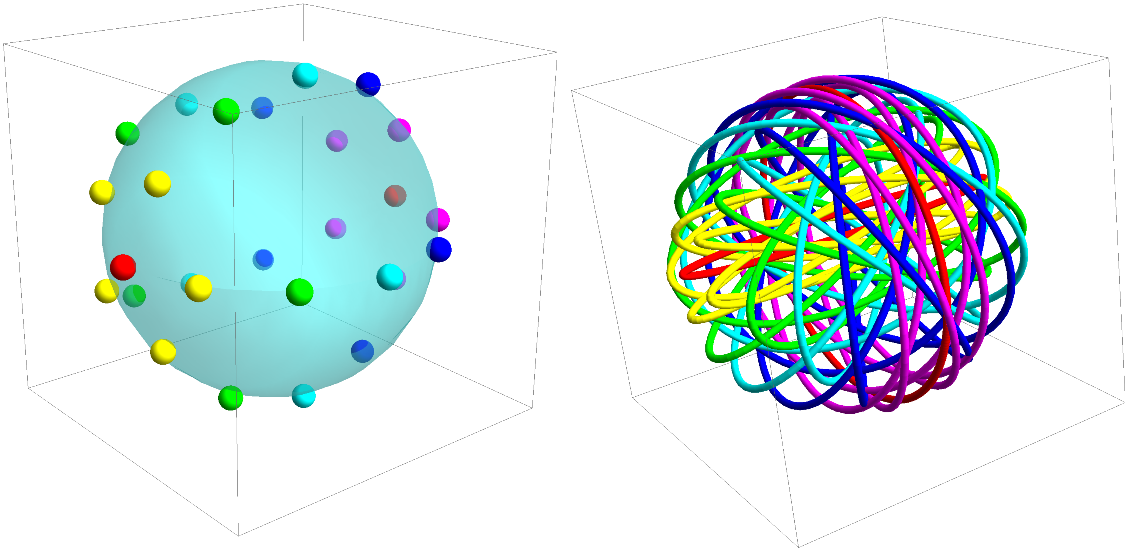
$${x_0}^2 + {y_0}^2 + {x_1}^2 + {y_1}^2 = 1\,. \tag{2.4}$$

We can reduce 3 degrees of freedom in Eq. (2.4) to 2 degrees of freedom by effectively removing $\mathrm{e}^{\mathrm{i}\theta}$ (“fibering out by the circle $\mathbf{S}^1$”). The standard form of this maps (“the Hopf fibration”) is

$$\begin{aligned} X &= 2\,\mathrm{Re}\;\alpha_0\alpha_1^* = 2x_0x_1 + 2y_0y_1\,, \\ Y &= 2\,\mathrm{Im}\;\alpha_0\alpha_1^* = 2x_1y_0 - 2x_0y_1\,, \\ Z &= |\alpha_0|^2 - |\alpha_1|^2 = {x_0}^2 + {y_0}^2 - {x_1}^2 - {y_1}^2\,. \end{aligned} \tag{2.5}$$

By denoting the three-dimensional vector (X, Y, Z) as $\hat{a}$, Eq. (2.4) implies these transformed coordinates obeying

$$\|\hat{a}\|^2 = X^2 + Y^2 + Z^2 = \left(|\alpha_0|^2 + |\alpha_1|^2\right)^2 = 1 \tag{2.6}$$



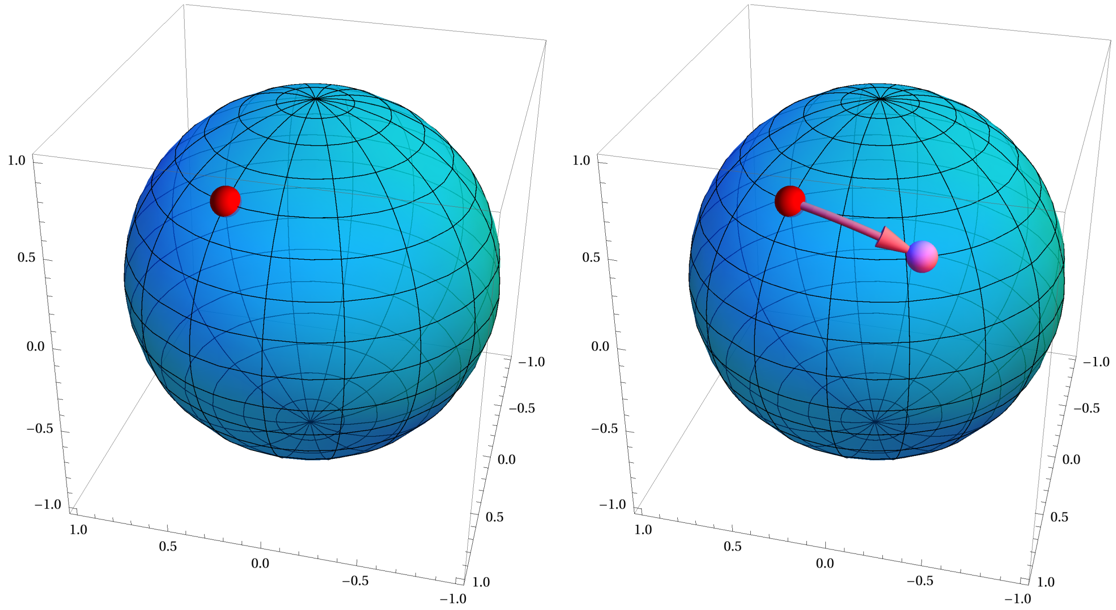
(a) (b)

Figure 2.1: (a) The two-sphere $\mathbf{S}^2$ represented by Eq. (2.6), which is the irreducible space of one-qubit states, along with a representative set of points on the sphere. Each single point on the sphere in (a) corresponding to a circle in (b), and a whole family of circles (the paths of $\mathrm{e}^{\mathrm{i}\theta}$) on the three-sphere $\mathbf{S}^3$ represents the Hopf fibration, Eq. (2.5). Although $\mathbf{S}^3$ cannot be directly embedded in $\mathbb{R}^3$, three-sphere $\mathbf{S}^3$ can be regarded as attaching two three-dimensional ball on two sides of two-sphere $\mathbf{S}^2$. In this way, each circle in $\mathbf{S}^3$ can be represented as a circle in the three-dimensional ball as shown in (b). Moreover, points in (a) are color coded corresponding to circles in (b), e.g., one pole contains the red elliptical circle that would become an infinite-radius circle by a slightly different way to represent $\mathbf{S}^3$ in $\mathbb{R}^3$, and the opposite pole corresponds to the large perfectly round red circle at the equator.

and therefore have only two remaining degrees of freedom describing all possible distinct one-qubit quantum states. In Fig. 2.1, we illustrate schematically the family of circles *each one of which is collapsed to a point* (ϕ, ψ) on the surface $X^2 + Y^2 + Z^2 = 1$ by the Hopf map.

The resulting manifold is the two-sphere $\mathbf{S}^2$ (a 2-manifold) embedded in $\mathbb{R}^3$. If we choose one of many possible coordinate systems describing $\mathbf{S}^3$ via Eq. (2.4) such as

$$(x_0, y_0, x_1, y_1) = (\cos{(\theta + \phi)} \cos\psi,\ \sin{(\theta + \phi)} \cos\psi,\ \cos{(\theta - \phi)} \sin\psi,\ \sin{(\theta - \phi)} \sin\psi)\ , \tag{2.7}$$



(a)

(b)

Figure 2.2: (a) The conventional Bloch sphere with a unique state represented by the point at the red sphere. (b) The geodesic shortest-distance arc connecting two one-qubit quantum states.

where $0 \leq \psi \leq \frac{\pi}{2}$, with $0 \leq \theta + \phi < 2\pi$ and $0 \leq \theta - \phi < 2\pi$, we see that

$$(X, Y, Z) = (\cos(2\phi)\sin(2\psi)\,,\ \sin(2\phi)\sin(2\psi)\,,\ \cos(2\psi))\ . \tag{2.8}$$

Thus the one-qubit state is independent of θ, and we can choose $\theta = \phi$ without loss of generality, reducing the form of the unique one-qubit states to $|\psi_1\rangle = \mathrm{e}^{2\mathrm{i}\phi}\cos\psi\,|0\rangle + \sin\psi\,|1\rangle$, and an irreducible state can be represented as a point on a sphere called the Bloch sphere, as shown in Fig. 2.2(a).

Thus the geometry of a single qubit reduces to transformations among points on $\mathbf{S}^2$, which can be parametrized in an infinite one-parameter family of transformations, one of which is the geodesic or minimal-length transformation. Explicitly, given two one-qubit states denoted by points $\hat{a}$ and $\hat{b}$ on $\mathbf{S}^2$, the shortest rotation carrying $\hat{a}$ to $\hat{b}$ is the SLERP (spherical linear interpolation) [27, 28]

$$S\left(\hat{a}, \hat{b}, t\right) = \hat{a}\,\frac{\sin((1-t)\omega)}{\sin\omega} + \hat{b}\,\frac{\sin(t\omega)}{\sin\omega}\,, \tag{2.9}$$

where $\hat{a}\cdot\hat{b} = \cos\omega$. Figure 2.2(b) illustrates the path traced by a SLERP between two irreducible one-qubit states on the Bloch sphere. Because states in CQC are defined by infinite precision real numbers, it is not possible, even in principle, to make an exact state transition as implied by Fig. 2.2(b). In practice, one has to be content with approximate, typically exponentially expensive, transitions from state to state.

2.1.2 D-DIMENSIONAL HILBERT SPACE

The irreducible states in a D-dimensional Hilbert space are encoded in a similar family of geometric structures known technically as the complex projective space $\mathbb{C}\mathbf{P}^{D-1}$. We obtain these structures starting with the D initially unnormalized complex coefficients of the D-dimensional basis $|\Psi\rangle = \sum_{i=0}^{D-1} \alpha_i\, |i\rangle$. We then follow the analog of the two-dimensional procedure: Conservation of probability requires that the norm of the vector $\vec{\alpha}$ be normalized to unity:

$$\langle\Psi|\Psi\rangle = \|\vec{\alpha}\|^2 = \sum_{i=0}^{D-1} |\alpha_i|^2 = 1\,. \tag{2.10}$$

Thus the initial equation for the geometry of a quantum state describes a *topological sphere* $\mathbf{S}^{2D-1}$ embedded in $\mathbb{R}^{2D}$. To see this, remember that we can write the real and imaginary parts of α_i as $\alpha_i = x_i + \mathrm{i}y_i$, so

$$\sum_{i=0}^{D-1} |\alpha_i|^2 = \sum_{i=0}^{D-1} {x_i}^2 + {y_i}^2 = 1 \tag{2.11}$$

describes the locus of a $2D$-dimensional real unit vector in $\mathbb{R}^{2D}$, which is by definition $\mathbf{S}^{2D-1}$, the $(2D-1)$-sphere.

This $\mathbf{S}^{2D-1}$ in turn is ambiguous up to the usual overall phase, inducing an $\mathbf{S}^1$ symmetry action, and identifying $\mathbf{S}^{2D-1}$ as an $\mathbf{S}^1$ bundle, whose base space is the $(D-1)$-complex-dimensional projective space $\mathbb{C}\mathbf{P}^{D-1}$. There are thus $2D-2$ irreducible real degrees of freedom ($D-1$ complex degrees of freedom) for a quantum state with a D-dimensional basis, $\{|i\rangle \mid i = 0, \ldots, D-1\}$.

In summary, the full space of a D-dimensional quantum state, including its overall phase defining its relationship to other quantum states, is the topological space $\mathbf{S}^{2D-1}$. For an isolated system, the overall phase is not measurable, and eliminating the phase dependence in turn corresponds to identifying $\mathbf{S}^{2D-1}$ as a circle bundle over the base space $\mathbb{C}\mathbf{P}^{D-1}$, and therefore $\mathbb{C}\mathbf{P}^{D-1}$ defines the $2D-2$ intrinsic, irreducible, degrees of freedom of the isolated D-dimensional state's dynamics. In mathematical notation, this would be written $\mathbf{S}^1 \hookrightarrow \mathbf{S}^{2D-1} \to \mathbb{C}\mathbf{P}^{D-1}$**TODO. Citation?**. For $D = 2$, the single qubit, we have $2 - 1 = 1$, and the base space of the circle bundle is $\mathbb{C}\mathbf{P}^1 = \mathbf{S}^2$, the usual Bloch sphere. Note that only for $D = 2$ is this actually a sphere-like geometry due to an accident of low-dimensional topology.

2.1.3 EXPLICIT GENERALIZATION OF THE HOPF FIBRATION CONSTRUCTION

For a two-dimensional system, we could easily solve the problem of reducing the full unit-norm space to its irreducible components $\hat{a} = (X, Y, Z)$ characterizing the Bloch sphere. We have just argued that essentially the same process is possible for D-dimensional system: in the abstract argument, we simply identify the family of coefficients $\{\alpha_i\}$ as being the same if they differ only by an overall phase $\mathrm{e}^{\mathrm{i}\theta}$. However, in practice this is not a construction that is easy to realize in a practical computation. We now outline an explicit algorithm for accomplishing the reduction to the irreducible D-dimensional state space $\mathbb{C}\mathbf{P}^{D-1}$; this construction will turn out to be useful for the validation of our discrete results to follow below.

Given a normalized pure state $|\Psi\rangle = \sum_{i=0}^{D-1} \alpha_i \, |i\rangle$, a natural quantity characterizing an D-

dimensional system is its *density matrix*, $\rho = |\Psi\rangle\langle\Psi|$, or

$$\rho = \begin{pmatrix} |\alpha_0|^2 & \alpha_0\alpha_1^* & \cdots & \alpha_0\alpha_{D-1}^* \\ \alpha_1\alpha_0^* & |\alpha_1|^2 & \cdots & \alpha_1\alpha_{D-1}^* \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{D-1}\alpha_0^* & \cdots & \alpha_{D-1}\alpha_{D-2}^* & |\alpha_{D-1}|^2 \end{pmatrix} . \tag{2.12}$$

We can now use the complex generalization of the classical Veronese coordinate system for projective geometry to remove the overall phase ambiguity $\mathrm{e}^{\mathrm{i}\theta}$ from the D-dimensional states. If we take a particular weighting of the elements of the density matrix ρ, we can construct a *unit vector* of real dimension D^2 with the form:

$$\hat{a} = \left(|\alpha_i|^2, \ldots, \sqrt{2}\,\mathrm{Re}\;\alpha_i\alpha_j^*, \ldots, \sqrt{2}\,\mathrm{Im}\;\alpha_i\alpha_j^*, \ldots\right) , \tag{2.13}$$

where

$$\hat{a}\cdot\hat{a} = \sum_{i=0}^{D-1}\left(|\alpha_i|^2\right)^2 + \sum_{i=0}^{D-1}\sum_{\substack{j=0\\ j\neq i}}^{D-1}\left(\mathrm{Re}\;\alpha_i\alpha_j^*\right)^2 + \left(\mathrm{Im}\;\alpha_i\alpha_j^*\right)^2 = \left(\sum_{i=0}^{D-1}|\alpha_i|^2\right)\left(\sum_{j=0}^{D-1}|\alpha_j|^2\right) = 1 \, .$$

This construction gives an explicit embedding of the $(D-1)$-dimensional complex, or $(2D-2)$-dimensional real, object in a real space of dimension D^2. However, this is somewhat subtle because the vector is of unit length, so technically the embedding space is a sphere of dimension $D^2 - 1$ embedded in $\mathbb{R}^{D^2}$. For example, the two-dimensional irreducible states could be represented in a four-dimensional embedding, but the magnitude of every coordinate would be one; furthermore, the object embedded in the resulting $\mathbf{S}^3$ is indeed $\mathbf{S}^2$ because we can fix one complex coordinate to be unity, and let one vary, giving a total of two irreducible dimensions. In fact one must choose *two* coordinate patches, one covering one pole of $\mathbf{S}^2$ with coordinates $\alpha_0 = 1 + \mathrm{i}0$ and $\alpha_1 = x_1 + \mathrm{i}y_1$, and the other patch covering the other pole of $\mathbf{S}^2$ with coordinates $\alpha_0 = x_0 + \mathrm{i}y_0$ and $\alpha_1 = 1 + \mathrm{i}0$.

TODO. Explain the last part more clear or add a picture.

We finally see that the irreducible D-dimensional state space $\mathbb{C}\mathbf{P}^{D-1}$ is described by D projectively equivalent coordinates, one of which can always be scaled out to leave $(D-1)$ actual (complex) degrees of freedom. We must choose, in turn, D different local sets of complex variables defined by taking the value $\alpha_k = 1$, with $k = 0, \dots, D-1$, and allowing the remaining $D-1$ complex (or $2D-2$ real) variables to run free. No single set of coordinates will work, since the submanifold including $\alpha_k = 0$ is undefined and another coordinate system must be chosen to cover that coordinate patch. This is a standard feature of the topology of non-trivial manifolds such as $\mathbb{C}\mathbf{P}^{D-1}$ (see any textbook on geometry [29]).

2.2 QUANTUM PROBABILITY

A *probability space* is a mathematical abstraction specifying the necessary conditions for reasoning coherently about collections of uncertain events [30, 31, 32, 33]. In the quantum case, the events of interest are specified by *projection operators* P satisfying the condition $P^2 = P$. These include the empty projector $\mathbb{0}$, the identity projector $\mathbb{1}$, projectors of the form $|\Phi\rangle\langle\Phi|$ where $|\Phi\rangle$ is a pure quantum state (an element of a Hilbert space $\mathscr{H}$), sums of *orthogonal* projectors P_0 and P_1 with $P_0 P_1 = \mathbb{0}$, and products of *commuting* projectors P_0 and P_1 with $P_0 P_1 = P_1 P_0$. In a quantum probability space [34, 35, 36, 37, 4], each event P_i is mapped to a probability $\mu(P_i)$ using a probability measure $\mu : \mathscr{E} \to [0, 1]$, where $\mathscr{E}$ is the set of all events, (i.e., projectors on a given Hilbert space), subject to the following constraints: $\mu(\mathbb{0}) = 0$, $\mu(\mathbb{1}) = 1$, $\mu(\mathbb{1} - P) = 1 - \mu(P)$, and for each pair of *orthogonal* projectors P_0 and P_1:

$$\mu(P_0 + P_1) = \mu(P_0) + \mu(P_1) \ . \tag{2.14}$$

Given a Hilbert space $\mathscr{H}$ of dimension d and a probability assignment for every projector P, we can define the expectation value of an observable $\mathbf{O}$ having spectral decomposition $\mathbf{O} = \sum_{i=1}^{d} \lambda_i P_i$, with eigenvalues $\lambda_i \in \mathbb{R}$, as [31, 38]:

$$\langle \mathbf{O} \rangle_{\mu} = \sum_{i=1}^{d} \lambda_i \mu \left(P_i\right) \ , \tag{2.15}$$

where the subscript μ might be omitted if it is clear according to the context.

A conventional quantum probability measure can easily be constructed using the Born rule if one knows the current pure unnormalized quantum state $|\Phi\rangle \in \mathscr{H}$; then the Born rule induces a probability measure μ_{Φ}^{B} defined as

$$\mu_{\Phi}^{B}(P) = \frac{\langle \Phi | P | \Phi \rangle}{\langle \Phi | \Phi \rangle} \, . \tag{2.16}$$

If $|\Phi\rangle$ is normalized, Eq. (2.16) could be simplified as $\mu_{\Phi}^{B}(P) = \langle \Phi | P | \Phi \rangle$. For mixed states $\rho = \sum_{j=1}^{N} q_j \left|\Phi_j\right\rangle \left\langle \Phi_j\right|$, where $\left|\Phi_j\right\rangle \in \mathscr{H}$, $q_j > 0$, and $\sum_{j=1}^{N} q_j = 1$, the generalized Born rule induces a probability measure μ_{ρ}^{B} defined as $\mu_{\rho}^{B}\left(P\right) = \mathrm{Tr}\left(\rho P\right) = \sum_{j=1}^{N} q_j \mu_{\Phi_j}^{B}\left(P\right)$ [39, 40, 38].

As an example, consider a three-dimensional Hilbert space with orthonormal basis $\{|0\rangle, |1\rangle, |2\rangle\}$ and an observable $\mathbf{O}$ with spectral decomposition $\mathbf{O} = |0\rangle\langle 0| + 2\ |1\rangle\langle 1| + 3\ |2\rangle\langle 2|$, i.e., $\lambda_i = i$ and $P_i = |i-1\rangle\langle i-1|$. Two fragments of valid probability measures μ_1 and μ_2 that can be associated with this space are defined in Table 2.1.

By the Born rule, the first probability measure corresponds to the quantum system being in the pure state $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and the second corresponds to the quantum system being in the state $\rho = \frac{|0\rangle\langle 0| + |2\rangle\langle 2|}{2}$. The expectation values of the observable $\mathbf{O}$, $\langle \mathbf{O} \rangle_{\mu_{1,2}}$, are 1.5 in the first case and 2 in the second.

The quantum probability postulates assume a mathematical idealization in which quantum states and measurements are both infinitely precise, i.e., *sharp*. In an actual experimental setup with an

Table 2.1: Two fragments of valid probability measures μ_1 and μ_2.

$\lvert\Psi\rangle$	$\mu_1\left(\lvert\Psi\rangle\langle\Psi\rvert\right)$	$\mu_2\left(\lvert\Psi\rangle\langle\Psi\rvert\right)$
$\lvert 0\rangle$	$\frac{1}{2}$	$\frac{1}{2}$
$\lvert 1\rangle$	$\frac{1}{2}$	0
$\lvert 2\rangle$	0	$\frac{1}{2}$
$\lvert +\rangle = \frac{\lvert 0\rangle + \lvert 1\rangle}{\sqrt{2}}$	1	$\frac{1}{4}$
$\lvert \mathrm{i}\rangle = \frac{\lvert 0\rangle + \mathrm{i}\lvert 1\rangle}{\sqrt{2}}$	$\frac{1}{2}$	$\frac{1}{4}$
$\lvert +'\rangle = \frac{\lvert 0\rangle + \lvert 2\rangle}{\sqrt{2}}$	$\frac{1}{4}$	$\frac{1}{2}$
$\lvert \mathrm{i}'\rangle = \frac{\lvert 0\rangle + \mathrm{i}\lvert 2\rangle}{\sqrt{2}}$	$\frac{1}{4}$	$\frac{1}{2}$
$\lvert +''\rangle = \frac{\lvert 1\rangle + \lvert 2\rangle}{\sqrt{2}}$	$\frac{1}{4}$	$\frac{1}{4}$
$\lvert \mathrm{i}''\rangle = \frac{\lvert 1\rangle + \mathrm{i}\lvert 2\rangle}{\sqrt{2}}$	$\frac{1}{4}$	$\frac{1}{4}$

ensemble of quantum states that would ideally be identical, but are not actually identically prepared, with imperfections and inaccuracies in measuring devices, an experimenter might not be able to determine that the probability of an event P is precisely 0.5. To address this issue, we investigate the cardinal probability in Sec. 3.7 and the interval-valued probability in Chapter 4.

The quantum expectation value can also used to decide whether a state is entangled or not for multipartite systems as we describe in the following section.

2.3 THE GEOMETRY OF ENTANGLEMENT

Entanglement may be regarded as one of the main characteristics distinguishing quantum from classical mechanics. Entanglement involves quantum correlations such that the measurement outcomes in one subsystem are related to the measurement outcomes in another one. To discuss entanglement, we consider a D-dimensional quantum system composed of n-qubit subsystems, i.e., $D = 2^n$. A pure state of the total system $\lvert\Psi\rangle$ is said to be entangled if it cannot be written as a product of states of each subsystem [41, 31, 38]. That is, a state $\lvert\Psi\rangle$ is entangled if $\lvert\Psi\rangle \neq \lvert\psi_1\rangle \otimes \cdots \otimes \lvert\psi_j\rangle \otimes \cdots \otimes \lvert\psi_n\rangle$, where $\left|\psi_j\right\rangle$ refers to an arbitrary state of the j-th qubit, and $\otimes$ represents the tensor product. This is equivalent to saying that if one calculates the reduced density operator ρ_j of the j-th subsystem by tracing out all the other subsystems,

$$\rho_j = \mathrm{Tr}_{\{1,\cdots,j-1,j+1,\cdots,n\}}\left(\rho\right) , \tag{2.17}$$

with $j = 1, \cdots, n$ and $\rho = |\Psi\rangle\langle\Psi|$, the normalized state $|\Psi\rangle$ is entangled if and only if at least one subsystem state is *mixed*, i.e., $\mathrm{Tr}_j\left(\rho_j^2\right) < 1$ [31, 38].

The reduced density operator could be expressed explicitly by the expectation value of the Pauli operators. Therefore, we can decide whether a system is entangled or not by examining these expectation values. Let σ_η^j be the Pauli operators acting on the j-th spin [31],

$$\sigma_\eta^j = \overbrace{\sigma_0 \otimes \cdots \otimes \sigma_0 \otimes \underbrace{\sigma_\eta}_{j^{\text{th}}\text{ factors}} \otimes \sigma_0 \otimes \cdots \otimes \sigma_0}^{n\text{ factors}} , \tag{2.18}$$

and $\left\langle\sigma_\eta^j\right\rangle$ be the corresponding expectation value, $\left\langle\sigma_\eta^j\right\rangle = \left\langle\Psi\middle|\sigma_\eta^j\middle|\Psi\right\rangle$, where $\eta = x$, y, and z, and

$$\begin{aligned} \sigma_0 &= |0\rangle\langle 0| + |1\rangle\langle 1| \ , \quad & \sigma_x &= |1\rangle\langle 0| + |0\rangle\langle 1| \ , \\ \sigma_y &= \mathrm{i}\,|1\rangle\langle 0| - \mathrm{i}\,|0\rangle\langle 1| \ , & \sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1| \ . \end{aligned} \tag{2.19}$$

For example, given a normalized two-qubit system $|\Psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$, some of its expectation values are

$$\begin{aligned} \langle\sigma_0^1\rangle &= |\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \, , \\ \langle\sigma_x^1\rangle &= \alpha_{00}\alpha_{10}^* + \alpha_{01}\alpha_{11}^* + \alpha_{10}\alpha_{00}^* + \alpha_{11}\alpha_{01}^* \, , \\ \langle\sigma_y^1\rangle &= -\alpha_{00}\alpha_{10}^*\mathrm{i} - \alpha_{01}\alpha_{11}^*\mathrm{i} + \alpha_{10}\alpha_{00}^*\mathrm{i} + \alpha_{11}\alpha_{01}^*\mathrm{i} \, , \\ \langle\sigma_z^1\rangle &= |\alpha_{00}|^2 + |\alpha_{01}|^2 - |\alpha_{10}|^2 - |\alpha_{11}|^2 \ . \end{aligned} \tag{2.20}$$

Then, the reduced density operator ρ_1 can be expressed by these expectation values as following:

$$\begin{aligned}\rho_1 =& \mathrm{Tr}_{\{2\}}\left(|\Psi\rangle\langle\Psi|\right)\\ =& \left(\left|\alpha_{00}\right|^2 + \left|\alpha_{01}\right|^2\right)|0\rangle\langle 0| + \left(\alpha_{00}\alpha_{10}^* + \alpha_{01}\alpha_{11}^*\right)|0\rangle\langle 1|\\ &+ \left(\alpha_{10}\alpha_{00}^* + \alpha_{11}\alpha_{01}^*\right)|1\rangle\langle 0| + \left(\left|\alpha_{10}\right|^2 + \left|\alpha_{11}\right|^2\right)|1\rangle\langle 1|\\ =& \frac{\left\langle\sigma_0^1\right\rangle\sigma_0 + \left\langle\sigma_x^1\right\rangle\sigma_x + \left\langle\sigma_y^1\right\rangle\sigma_y + \left\langle\sigma_z^1\right\rangle\sigma_z}{2}\,.\end{aligned} \tag{2.21}$$

In general, the reduced density operator ρ_j of the j-th subsystem can always be expressed as

$$\rho_j = \frac{1}{2}\sum_{\eta=0,x,y,z}\left\langle\sigma_\eta^j\right\rangle\sigma_\eta\,, \tag{2.22}$$

and its coefficients can be summarized as the vector

$$X_j = \left(\left\langle\sigma_x^j\right\rangle, \left\langle\sigma_y^j\right\rangle, \left\langle\sigma_z^j\right\rangle\right) \in \mathbb{R}^3 \tag{2.23}$$

that allows a geometric representation of each reduced state in $\mathbb{R}^3$, satisfying $0 \le \left\|X_j\right\| \le 1$. Since $\mathrm{Tr}_j\left(\rho_j^2\right) = \frac{1}{2}\left(1 + \left\|X_j\right\|^2\right)$, the state $|\Psi\rangle$ is entangled if $\left\|X_j\right\| < 1$ for at least one j, represented by a point *inside* the corresponding local Bloch sphere embedded in $\mathbb{R}^3$. One may therefore consider $|\Psi\rangle$ to be maximally entangled if $\left\|X_j\right\| = 0$ for all j. On the other hand, the state $|\Psi\rangle$ is unentangled (i.e., a product state) if $\left\|X_j\right\| = 1$ for all j, corresponding to points lying on the surface of the Bloch spheres.

A natural geometric measure of multipartite entanglement is obtained by defining the *purity of a state relative to a set of observables* [42, 43]. **TODO. Since we have the word "observables" here, we may need to discuss measurement before this subsection.** If the set is chosen to be the set of *all local observables*, i.e., corresponding to each of the subsystems that compose the actual system, one recovers the standard notion of entanglement for multipartite systems. For example, if the system consists of n qubits, we obtain a measure of conventional entanglement by calculating the purity relative to the semi-simple Lie algebra $\mathfrak{h}$ spanned by $\left\{\sigma_x^1, \sigma_y^1, \sigma_z^1, \ldots, \sigma_x^n, \sigma_y^n, \sigma_z^n\right\}$,

$$P_{\mathfrak{h}} = \frac{1}{n}\sum_{j=1}^{n}\sum_{\eta=x,y,z}\left\langle\sigma_\eta^j\right\rangle^2 = \frac{1}{n}\sum_{j=1}^{n}\left\|X_j\right\|^2 . \tag{2.24}$$

Since the norm of the geometric representation state $\left\|X_j\right\|$ defined in Eq. (2.23) is between 0 and 1, we have $0 \leq P_{\mathfrak{h}} \leq 1$, where $\frac{1}{n}$ in Eq. (2.24) is just a normalization factor. All the product states of the form $|\Psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$, have maximum purity (i.e., $P_{\mathfrak{h}} = 1$). Other states such as the Greenberger-Horne-Zeilinger state $|\Psi\rangle = |\mathsf{GHZ}_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes \cdots \otimes |0\rangle + |1\rangle \otimes \cdots \otimes |1\rangle\right)$ are (maximally) entangled relative to the set of local observables (i.e., $P_{\mathfrak{h}} = 0$).

Different entanglement measures are obtained when an algebra $\mathfrak{h}$ different from the local observables is chosen. An obvious example, in particular, is given by the set of all observables. In this case, the purity takes its maximum value independently of the pure quantum state [42, 43], expressing the fact that any state is a generalized coherent state of the Lie algebra of all observables.

2.4 QUANTUM CIRCUIT MODEL

TODO. Further explain σ_η^j used as a quantum circuit, control not, the Deutsch quantum black box [31], and maybe Deutsch Algorithm...

2.5 HIDDEN VARIABLE MODEL AND QUANTUM CONTEXTUALITY

TODO. Explain enough background knowledge to support the discussion about contextuality in the end of Sec. 3.2. I have typed some literature review in writing course, but I need to decide whether it could be used or not before finish Sec. 2.2.

Chapter 3

QUANTUM THEORIES AND COMPUTING OVER FINITE FIELDS

3.1 FUNDAMENTALS OF FINITE FIELDS

3.1.1 BACKGROUND

A field $\mathbb{F}$ is an algebraic structure consisting of a set of elements equipped with the operations of addition, subtraction, multiplication, and division [44, 45, 46]. Fields may contain an infinite or a finite number of elements. The rational $\mathbb{Q}$, real $\mathbb{R}$, and complex numbers $\mathbb{C}$ are examples of infinite fields, while the set $\mathbb{F}_3 = \{0, 1, 2\}$, under multiplication and addition modulo 3, is an example of a finite field.

There are two distinguished elements in a field, the addition identity 0, and the multiplication identity 1. Given the field $\mathbb{F}$, the closed operations of addition, "$+$," and multiplication, "$*$," satisfy the following set of axioms:

1. $\mathbb{F}$ is an Abelian group under the addition operation $+$ (additive group);

2. The multiplication operation $*$ is associative and commutative. The field has a multiplicative identity and the property that every nonzero element has a multiplicative inverse;

3. Distributive laws: For all $a, b, c \in \mathbb{F}$

$$\begin{aligned} a * (b + c) &= a * b + a * c\,, && (3.1) \\ (b + c) * a &= b * a + c * a\,. && (3.2) \end{aligned}$$

From now on, unless specified, we will omit the symbol $*$ whenever we multiply two elements of a field.

Finite fields of q elements, $\mathbb{F}_q = \{0, \dots, q - 1\}$, will play a special role in this work. A simple explicit example is $\mathbb{F}_3$ with the following addition and multiplication tables:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

3.1.2 CYCLIC PROPERTIES OF FINITE FIELDS

The characteristic of a field is the least positive integer m such that $m = 1 + 1 + 1 + \cdots + 1 = 0$, and if no such m exists we say that the field has characteristic zero (which is the case for $\mathbb{R}$ for example). It turns out that if the characteristic is non-zero, it must be a prime p. For every prime p and positive integer r there is a finite field $\mathbb{F}_{p^r}$ of size $q = p^r$ and characteristic p, which is unique up to field isomorphism [21, 44]. The exponent r is known as the *degree* of the field over its prime subfield[1] [47]. If the characteristic p is an arbitrary prime number, we call the field *unrestricted*.

For every $a \in \mathbb{F}_q$, $a \neq 0$, then $a^{q-1} = 1$, implying the Frobenius endomorphism (also a consequence of Fermat's little theorem) $a^q = a$, which in turn permits us to write the multiplicative inverse of any non-zero element in the field as $a^{-1} = a^{q-2}$, since $a^{q-2}a = a^{q-1} = 1$. Every subfield of the field $\mathbb{F}_q$, of size $q = p^r$, has $p^{r'}$ elements with some r' dividing r, and for a given r' it is

[1] Fields $\mathbb{F}_q$ where q is a power of a prime p, i.e., $q = p^r$, are known as Galois fields.

unique.

3.2 MODAL QUANTUM THEORY

Recently, Schumacher and Westmoreland [48, 49] and Chang et al. [50, 51] defined versions of quantum theory over *unrestricted* finite fields, which they call modal quantum theories (MQT) or Galois field quantum theories. Such theories retain several key quantum characteristics including notions of superposition, interference, entanglement, and mixed states, along with time evolution using invertible linear operators, complementarity of incompatible observables, exclusion of local hidden variable theories, impossibility of cloning quantum states, and the presence of natural counterparts of quantum information protocols such as superdense coding and teleportation. These modal theories are obtained by collapsing the Hilbert space structure over the field of complex numbers to that of a vector space over an *unrestricted* finite field. In the resulting structure, all non-zero vectors represent valid quantum states, and the evolution of a closed quantum system is described by *arbitrary* invertible linear maps.

Specifically, consider a one-qubit system with basis vectors $|0\rangle$ and $|1\rangle$. In conventional quantum theory, there exists an infinite number of states for a qubit of the form $\alpha_0 |0\rangle + \alpha_1 |1\rangle$, with α_0 and α_1 elements of the underlying field of complex numbers subject to the normalization condition $|\alpha_0|^2 + |\alpha_1|^2 = 1$. Moving to a finite field immediately limits the set of possible states as the coefficients α_0 and α_1 are now drawn from a finite set. In particular, in the field $\mathbb{F}_2 = \{0, 1\}$ of booleans, there are exactly four possible vectors: the zero vector, the vector $|0\rangle$, the vector $|1\rangle$, and the vector $|0\rangle + |1\rangle = |+\rangle$. Since the zero vector is considered non-physical, a one-qubit system can be in one of only three states. The dynamics of these one-qubit states is realized by any invertible linear map, i.e., by any linear map that is guaranteed never to produce the zero vector from a valid state. There are exactly 6 such maps, and their matrix representation with respect to the standard basis are:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \qquad S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} , \qquad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} , \tag{3.3a}$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} , \qquad S^\dagger = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} , \qquad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} . \tag{3.3b}$$

For example,

$$S\left|0\right\rangle = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \left|+\right\rangle , \quad S\left|+\right\rangle = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \left|0\right\rangle . \tag{3.4}$$

This set of maps is clearly quite impoverished compared to the full set of one-qubit unitary maps in conventional quantum theory. In particular, it does not include the Hadamard transformation. However, this set also includes non-unitary maps such as S and $S^\dagger$ that are not allowed in conventional quantum computation.

Measurement in the standard basis is fairly straightforward: measuring $\left|0\right\rangle$ or $\left|1\right\rangle$ deterministically produces the same state while measuring $\left|+\right\rangle$ nondeterministically produces $\left|0\right\rangle$ or $\left|1\right\rangle$ with no assigned probability distribution. When measuring an arbitrary state $\left|\phi\right\rangle \in \{\left|0\right\rangle, \left|1\right\rangle, \left|+\right\rangle\}$ in other bases $\{\left|\psi_0\right\rangle, \left|\psi_1\right\rangle\}$, we first represents $\left|\phi\right\rangle$ as the linear combination of the basis vectors $\beta_0 \left|\psi_0\right\rangle + \beta_1 \left|\psi_1\right\rangle$, where β_0 and β_1 are elements in the field $\mathbb{F}_2$. If β_i is zero, measuring $\left|\phi\right\rangle$ is impossible to produce $\left|\psi_i\right\rangle$; otherwise, measuring $\left|\phi\right\rangle$ is possible to produce $\left|\psi_i\right\rangle$. Since only possibility and impossibility is predicted by the theory, modal quantum theories are named after these "modal" concepts.

Notice that the measurement process is complicated by the fact that the possibility to produce a basis vector $\left|\psi_i\right\rangle$ depending on the measurement basis. For example, measuring $\left|+\right\rangle$ is possible to produce $\left|0\right\rangle$ in the standard basis $\{\left|0\right\rangle, \left|1\right\rangle\}$ but is impossible to produce $\left|0\right\rangle$ in another basis $\{\left|+\right\rangle, \left|0\right\rangle\}$. In contrast, when measuring a state $\left|\phi\right\rangle$ in CQT, the probability to produce a basis vector $|\psi_i\rangle$ is completely determined by $|\psi_i\rangle$ and $|\phi\rangle$ no matter $|\psi_i\rangle$ is in which measurement basis. This phenomena of the measurement basis dependence in CQT only exists when discussing quantum contextuality. Despite this kind of "supercontextuality" of MQT, its computational model, modal quantum computing (MQC), having "supernatural" computational power is also far from conventional quantum computing as we will describe next.

3.3 MODAL QUANTUM COMPUTING

To understand the computational implications of the modal quantum theory defined over the field $\mathbb{F}_2$ of booleans, we developed a quantum computing model and established its correspondence to a classical model of logical programming with a feature that has quantum-like behavior [52]. In a conventional logic program, answers produced by different execution paths are collected in a sequence with *no* interference. However, in this modal quantum computing model over $\mathbb{F}_2$, these answers may interfere destructively with one another.

Our computations with this "toy" modal quantum theory showed that it possesses "supernatural" computational power. For example, one can solve a black box version of the UNIQUE-SAT problem [53] in a way that outperforms conventional quantum computing. The classical UNIQUE-SAT problem (also known as USAT or UNAMBIGUOUS-SAT**TODO. Add citation about where these two names come from.**) is the problem of deciding whether a given boolean formula has a satisfying assignment, assuming that it has at most one such assignment [54]. This problem is, in a precise sense [55], just as hard as the general satisfiability problem and hence all problems in the NP complexity class. Our black-box version of the UNIQUE-SAT problem replaces the boolean formula with an arbitrary black box. Solutions to this generalized problem can be used to solve an unstructured database search of size N using $O(\log N)$ black box evaluations by binary search on the database. This algorithm then outperforms the known asymptotic bound $O\left(\sqrt{N}\right)$ for unstructured database search in conventional quantum computing.

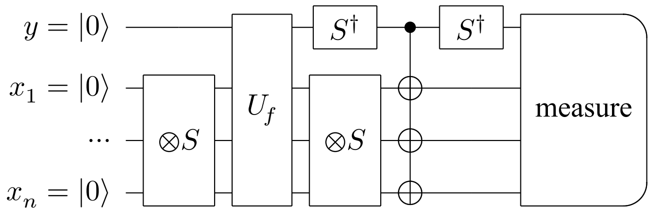


Figure 3.1: Circuit for black box UNIQUE-SAT in modal quantum theory over the field $\mathbb{F}_2$. For further notation see text.

We can prove the unreasonable power of the arbitrary-function UNIQUE-SAT starting with a classical function $f : \mathsf{Bool}^n \to \mathsf{Bool}$ that takes n bits and returns at most one `true` result. To build a quantum algorithm, f is first represented as the Deutsch quantum black box U_f with [56, 31]

$$U_f\,|y\rangle\,|\overline{x}\rangle = |y \oplus f(\overline{x})\rangle\,|\overline{x}\rangle = \begin{cases} |y\rangle\,|\overline{x}\rangle\ , & \text{if } f(\overline{x}) = \texttt{false}\,; \\ \\ |\mathsf{not}\,(y)\rangle\,|\overline{x}\rangle\ , & \text{if } f(\overline{x}) = \texttt{true}\,, \end{cases} \tag{3.5}$$

where $\overline{x}$ denotes a sequence $x_1, x_2, \ldots, x_n$ of n bits, $\oplus$ is exclusive disjunction, and 0 and 1 are identified as `false` and `true`, respectively. Then, we can give an algorithm (see Fig. 3.1) taking as input such a classical function that decides, deterministically and in a constant number of black box evaluations, whether f is satisfiable or not:

CASE I: f IS UNSATISFIABLE; THE MEASUREMENT DETERMINISTICALLY PRODUCES $|0\rangle\,|\overline{0}\rangle$. TODO. This part use $|\overline{a}\rangle = |a_1\rangle \ldots |a_n\rangle$ while previous parts use $|\Psi\rangle = |\psi_1\rangle \cdots |\psi_j\rangle \cdots |\psi_n\rangle$. Moreover, bar is heavily used in QIVPM discussion later, so maybe not using bar here????The state is initialized to $|0\rangle\,|\overline{0}\rangle$, with $|\overline{0}\rangle = |0\rangle\,|0\rangle \cdots |0\rangle$, i.e., the tensor product of n $|0\rangle$ states. As Eq. (3.4), applying the map S to each qubit in the second component of the state produces $|0\rangle\,|\overline{+}\rangle$ where $|\overline{+}\rangle$ denotes the sequence $|+\rangle \ldots |+\rangle$ of length n. Applying U_f to the entire state has no effect since U_f is the identity when f is unsatisfiable. Applying S to each qubit in the second component of the state produces $|0\rangle\,|\overline{0}\rangle$. Applying $S^\dagger$ to the first component leaves the state unchanged. As the first component of the state is 0, applying the map σ_0 (which is the identity) leaves the state unchanged.**TODO. Control-not need to be defined and explained in Sec. ??** Applying $S^\dagger$ to the first component leaves the state unchanged. Measuring the state will deterministically produce $|0\rangle\left|\overline{0}\right\rangle$.

CASE II: f IS SATISFIABLE; THE MEASUREMENT PRODUCES SOME STATE OTHER THAN $|0\rangle\left|\overline{0}\right\rangle$. Assume the function f is satisfiable at some input $a_1, a_2, \ldots, a_n$ denoted $\overline{a}$, and where $|\overline{a}\rangle = |a_1\rangle \ldots |a_n\rangle$. In the second step, the state becomes $|0\rangle\left|\overline{+}\right\rangle$ as above. We can write this state as $|0\rangle|\overline{a}\rangle + \Sigma_{\overline{x}\neq\overline{a}}|0\rangle|\overline{x}\rangle$. Applying U_f produces $|1\rangle|\overline{a}\rangle + \Sigma_{\overline{x}\neq\overline{a}}|0\rangle|\overline{x}\rangle$. We can rewrite this state as $|+\rangle|\overline{a}\rangle + \Sigma_{\overline{x}}|0\rangle|\overline{x}\rangle = |+\rangle|\overline{a}\rangle + |0\rangle\left|\overline{+}\right\rangle$, where the summation is now over all vectors (notice that $|0\rangle|\overline{a}\rangle + |0\rangle|\overline{a}\rangle$ is the zero vector). Applying S to each qubit in the second component produces $|+\rangle\left|\overline{S(a)}\right\rangle + |0\rangle\left|\overline{0}\right\rangle$. Applying $S^\dagger$ to the first component produces: $|1\rangle\left|\overline{S(a)}\right\rangle + |0\rangle\left|\overline{0}\right\rangle$. Applying control-not gate, which applying σ_0 or σ_x on the second component depending on the first component of the state, and produces

$$|1\rangle\left(\sigma_x\left|\overline{S(a)}\right\rangle\right) + |0\rangle\left(\sigma_0\left|\overline{0}\right\rangle\right) = |1\rangle\left|\overline{\mathsf{not}\,(S(a))}\right\rangle + |0\rangle\left|\overline{0}\right\rangle\ . \tag{3.6}$$

Applying $S^\dagger$ to the first component produces $|+\rangle\left|\overline{\mathsf{not}\,(S(a))}\right\rangle + |0\rangle\left|\overline{0}\right\rangle$. For the measurement of $|+\rangle\left|\overline{\mathsf{not}\,(S(a))}\right\rangle + |0\rangle\left|\overline{0}\right\rangle$ to be guaranteed to never be $|0\rangle\left|\overline{0}\right\rangle$, we need to verify that $|+\rangle\left|\overline{\mathsf{not}\,(S(a))}\right\rangle$ has one occurrence $|0\rangle\left|\overline{0}\right\rangle$. **TODO. The following need to be rewritten.**This can be easily proved as follows. Since each a_i is either 0 or 1, then each $S(a_i)$ is either $+$ or 1, and hence each $\mathsf{not}\,(S(a_i))$ is either $+$ or 0. The result follows since any state with a combination of $+$ and 0, when expressed in the standard basis, would consist of a superposition containing the state $|0\ldots\rangle$.

3.4 DISCRETE QUANTUM THEORY (I)

3.4.1 COMPLEXIFIED FINITE FIELDS

Our next objective is to develop more realistic discrete quantum theory variants that exclude "supernatural" algorithms such as the one presented above. Our first such plausible framework [57] is based on complexifiable finite fields. To incorporate complex numbers for quantum amplitudes, we exploit the fact that the polynomial $x^2 + 1$ is *irreducible* ($x^2 + 1 = 0$ has no solution) over a prime field $\mathbb{F}_p$ with p odd if and only if p is of the form $4\ell + 3$, with ℓ a non-negative integer [21, 44, 46]. For example, when $p = 3$, x could be 0 or ± 1. Since $0^2 + 1 \neq 0$ and $(\pm 1)^2 + 1 \neq 0$, none of the element in $\mathbb{F}_3$ solves $x^2 + 1 = 0$, and $x^2 + 1$ is irreducible over $\mathbb{F}_3$. In contrast, $2^2 + 1 = 0$ over $\mathbb{F}_5$ so that $x^2 + 1$ is reducible.

Since $x^2 + 1 = 0$ has no solution in any field $\mathbb{F}_p$ with $p = 4\ell + 3$, we can extend $\mathbb{F}_p$ to a field $\mathbb{F}_{p^2}$ whose elements can be viewed as discrete complex numbers with the real and imaginary parts in $\mathbb{F}_p$. Therefore, every element in $\mathbb{F}_{p^2}$ can be expressed as $a + b\mathrm{i}$ with $a, b \in \mathbb{F}_p$, and a $\mathbb{F}_{p^2}$ is called a complexified finite field. Since the multiplicative group of any finite field is cyclic [21], there is a generator $g \in \mathbb{F}_{p^2}$ such that every non-zero element $a + b\mathrm{i}$ can also be represented as the power of a generator, i.e., $a + b\mathrm{i} = g^j$ for some j. For example, $1 - \mathrm{i}$ is a generator in $\mathbb{F}_{3^2}$ means a particular element $1 + \mathrm{i} \in \mathbb{F}_{3^2}$ can be expressed as $1 + \mathrm{i} = 1 - 3\mathrm{i} - 3 + \mathrm{i} = (1 - \mathrm{i})^3$. All possible choices of generators in $\mathbb{F}_{3^2}$ is listed in Table 3.1.

In Table 3.1, one can notice that $(a + b\mathrm{i})^3 = a - b\mathrm{i}$. In general, the p-th power $(a + b\mathrm{i})^p = a - b\mathrm{i}$ is called the *Frobenius automorphism* acts like complex conjugation $(a + b\mathrm{i})^* = a - b\mathrm{i}$ [21, 58, 44]. Then, we define the *field norm* $\mathsf{N}(\cdot) : \mathbb{F}_{p^2} \to \mathbb{F}_p$ as an element $a + \mathrm{i}b$ multiplying its complex conjugation $(a + b\mathrm{i})^*$ [59],

$$\mathsf{N}(a + \mathrm{i}b) = (a + b\mathrm{i})(a + b\mathrm{i})^* = (a + b\mathrm{i})^{p+1} = a^2 + b^2 \,, \tag{3.7}$$

Table 3.1: Generators in $\mathbb{F}_{3^2}$

j	$(1+\mathrm{i})^j$	$(1-\mathrm{i})^j$	$(-1+\mathrm{i})^j$	$(-1-\mathrm{i})^j$
0	1	1	1	1
1	$1+\mathrm{i}$	$1-\mathrm{i}$	$-1+\mathrm{i}$	$-1-\mathrm{i}$
2	$-\mathrm{i}$	i	i	$-\mathrm{i}$
3	$1-\mathrm{i}$	$1+\mathrm{i}$	$-1-\mathrm{i}$	$-1+\mathrm{i}$
4	-1	-1	-1	-1
5	$-1-\mathrm{i}$	$-1+\mathrm{i}$	$1-\mathrm{i}$	$1+\mathrm{i}$
6	i	$-\mathrm{i}$	$-\mathrm{i}$	i
7	$-1+\mathrm{i}$	$-1-\mathrm{i}$	$1+\mathrm{i}$	$1-\mathrm{i}$

where the square root in the usual definition of norm is avoided because, unlike the continuous case, the square root does not always exist. For example, the field norm of every generator g in Table 3.1 is the same number $\mathsf{N}(g) = g^{3+1} = -1$. In fact, these four generators are the only elements in $\mathbb{F}_{3^2}$ whose field norm is $-1 \in \mathbb{F}_3$. Generally, given any $c \in \mathbb{F}_p$, let $\mathsf{N}^{-1}(\{c\})$ denote the set of element whose field norm is c, i.e., $\mathsf{N}^{-1}(\{c\}) = \big\{\alpha \in \mathbb{F}_{p^2} \bigm| \mathsf{N}(\alpha) = c\big\}$. The set $\mathsf{N}^{-1}(\{c\})$ is the discrete analog of phase-equivalence under the modulus-preserving transformation $z \to \mathrm{e}^{\mathrm{i}\phi}z$, and the number of its elements is characterized by the following proposition.

Proposition 3.4.1. *Given any $c \in \mathbb{F}_p$, the number of elements in $\mathsf{N}^{-1}(\{c\})$ is $p+1$, i.e., there are always $p+1$ elements in $\mathbb{F}_{p^2}$ whose field norm is c.*

Proof. To prove Proposition 3.4.1, we start by proving $\mathsf{N}^{-1}(\{c\})$ is non-empty. Consider a special case of the field norm $\mathsf{N}(.)$, namely the real quadratic map $Q(e) = e^2$ taking an arbitrary element $e \in \mathbb{F}_p$ to its square in the field. Since $(\pm 1)^2 = 1$, the image of $Q(e)$ has only $\frac{p+1}{2}$ elements in $\mathbb{F}_p$, including the zero element. We let A be the image of the map $Q(e)$ in $\mathbb{F}_p$, and note that the set A_c resulting from displacing an element $x = b^2$ of A to $c - x = c - b^2$ with $c \in \mathbb{F}_p$ also has $\frac{p+1}{2}$ elements because the result is simply a cyclic shift of element labels. We now observe that for any non-zero $c \in \mathbb{F}_p$, the sum of the elements in two sets A and A_c is $\frac{p+1}{2} + \frac{p+1}{2} = p+1$, which is greater than the size p of $\mathbb{F}_p$, and so there must be at least one common element such that

$a^2 = c - b^2$. Thus every element $c \in \mathbb{F}_p$ is the field norm of some element $\alpha = a + b\mathrm{i} \in \mathbb{F}_{p^2}$ such that $\mathsf{N}(\alpha) = a^2 + b^2 = c$, and $\mathsf{N}^{-1}(\{c\})$ is non-empty.

We then want to show for all non-zero $c \in \mathbb{F}_p$, the size of $\mathsf{N}^{-1}(\{c\})$ is always the same. Given a particular non-zero $c_0 \in \mathbb{F}_p$ and $\alpha_0 \in \mathbb{F}_{p^2}$ with $\mathsf{N}(\alpha_0) = c_0$, consider the map $f(\alpha) = \alpha_0\alpha$. When $\mathsf{N}(\alpha) = 1$, we have [44]

$$\mathsf{N}(f(\alpha)) = \mathsf{N}(\alpha_0\alpha) = \mathsf{N}(\alpha_0)\,\mathsf{N}(\alpha) = c_0 \tag{3.8}$$

so that $f(\alpha) \in \mathsf{N}^{-1}(\{c_0\})$. Since $\mathsf{N}(a + b\mathrm{i}) = 0$ only for $a = b = 0$, α_0 is non-zero, and f is actually a bijection between $\mathsf{N}^{-1}(\{1\})$ and $\mathsf{N}^{-1}(\{c_0\})$. This means the number of elements in $\mathsf{N}^{-1}(\{1\})$ and $\mathsf{N}^{-1}(\{c_0\})$ are the same. Because c_0 can be any non-zero element, the number of elements in the equivalence classes $\mathsf{N}^{-1}(\{c\})$ is always the same.

We can now compute the size of the equivalence class of complex unit-modulus phases corresponding to the Hopf fibration circle. **TODO. Explain the Hopf fibration circle here... ?** Since $\mathbb{F}_{p^2}$ has $p^2 - 1$ non-zero values, and the map $\mathsf{N}(\alpha)$ distributes these equally across the domain of $p - 1$ non-zero elements $c \in \mathbb{F}_p$, there are $\frac{p^2-1}{p-1} = p + 1$ (non-zero) domain elements in $\mathbb{F}_{p^2}$ for each (non-zero) image element in $\mathbb{F}_p$. We illustrate this graphically in Figure 3.2. Thus the Hopf circle always has size $p + 1$, corresponding essentially to a discrete projective line, and that is the size of each equivalence class of the map $\mathsf{N}(\alpha)$ for non-vanishing α, including in particular the map to the unit norm value $c = 1 \in \mathbb{F}_p$. □

3.4.2 VECTOR SPACES

In this section we want to build a theory of discrete vector spaces that approximates as closely as possible the features of conventional quantum theory. Such a structure would ideally consist of the following: (i) a vector space over the field of complex numbers, and (ii) an inner product $\langle\Phi|\Psi\rangle$ associating to each pair of vectors a complex number, and satisfying the following properties:

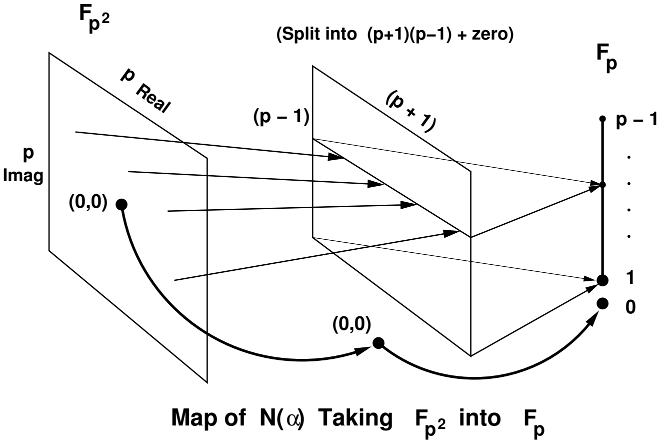

F_{p^2}
(Split into (p+1)(p−1) + zero)
F_p
p Real
(p + 1)
(p − 1)
p − 1
p Imag
(0,0)
1
0
(0,0)
Map of N(α) Taking F_{p^2} into F_p

Figure 3.2: Sketch of the map from $\mathbb{F}_{p^2}$ to $\mathbb{F}_p$ using $\mathsf{N}\left(\alpha\right)$, showing the decomposition of $\mathbb{F}_{p^2}$ into the zero element $(0,0)$ and the $p^2-1=\left(p+1\right)\left(p-1\right)$ non-zero elements that map onto the $p-1$ non-zero elements of $\mathbb{F}_p$ with multiplicity $p+1$.

(A) $\langle\Phi|\Psi\rangle$ is the complex conjugate of $\langle\Psi|\Phi\rangle$;

(B) $\langle\Phi|\Psi\rangle$ is conjugate linear in its first argument and linear in its second argument;

(C) $\langle\Psi|\Psi\rangle$ is always non-negative and is equal to 0 only if $|\Psi\rangle$ is the zero vector.

It turns out that a vector space defined over a finite field cannot have an inner product satisfying the properties above. However, we will introduce an Hermitian "dot product" satisfying some of those properties.

We are interested in the vector space $\mathscr{H}$ of dimension D defined over the complexified field $\mathbb{F}_{p^2}$. Let $|\Psi\rangle=\begin{pmatrix}\alpha_0 & \alpha_1 & \dots & \alpha_{D-1}\end{pmatrix}^T$ and $|\Phi\rangle=\begin{pmatrix}\beta_0 & \beta_1 & \dots & \beta_{D-1}\end{pmatrix}^T$ represent vectors in $\mathscr{H}$, with numbers α_i and β_i drawn from $\mathbb{F}_{p^2}$, and where $\left(\cdot\right)^T$ is the transpose.

Definition 3.4.1 (Hermitian dot product)**.** Given vectors $|\Phi\rangle$ and $|\Psi\rangle\in\mathscr{H}$, it can be shown [58] the Hermitian dot product is always reducible to the form

$$\langle\Phi|\Psi\rangle=\sum_{i=0}^{D-1}\beta_i^p\alpha_i\,. \tag{3.9}$$

Two vectors $|\Phi\rangle$ and $|\Psi\rangle\in\mathscr{H}$ are said to be orthogonal if $\langle\Phi|\Psi\rangle=0$. This product satisfies conditions (A) and (B) for inner products but violates condition (C) since in every finite field there always exists a non-zero vector $|\Psi\rangle$ such that $\langle\Psi|\Psi\rangle = 0$. The reason is that addition in finite fields eventually "wraps around" (because of their cyclic or modular structure), allowing the sum of non-zero elements to be zero. The fraction of non-zero vectors satisfying $\langle\Psi|\Psi\rangle = 0$ decreases with the order p.

For any vector $|\Psi\rangle = \begin{pmatrix}\alpha_0 & \alpha_1 & ... & \alpha_{D-1}\end{pmatrix}^T$, the Hermitian dot product $\langle\Psi|\Psi\rangle$ is equal to $\sum_{i=0}^{D-1} \mathsf{N}\left(\alpha_i\right)$, which is the sum of the field norms for the complex coefficients. For convenience, we now extend the field norm to include vector arguments by defining

$$\mathsf{N}\left(|\Psi\rangle\right) = \langle\Psi|\Psi\rangle = \sum_{i=0}^{D-1} \mathsf{N}\left(\alpha_i\right) . \tag{3.10}$$

Although the field norm of a vector can vanish for non-vanishing vectors, if a vector $|\Psi\rangle$ has a non-vanishing field norm c, its field norm can be utilized to normalize $|\Psi\rangle$. Recalled in Sec. 3.4.1, we defined $\mathsf{N}^{-1}\left(\{c\}\right)$ to be the set of element whose field norm is c. Given any $\alpha \in \mathsf{N}^{-1}\left(\{c\}\right)$, the field norm of $\frac{|\Psi\rangle}{\alpha}$ is

$$\mathsf{N}\left(\frac{|\Psi\rangle}{\alpha}\right) = \frac{\mathsf{N}\left(|\Psi\rangle\right)}{\mathsf{N}\left(\alpha\right)} = \frac{c}{c} = 1 , \tag{3.11}$$

i.e., $\frac{|\Psi\rangle}{\alpha}$ is normalized. However, since the size of $\mathsf{N}^{-1}\left(\{c\}\right)$ is $p+1$, we cannot identify a "unique" normalized for any given vector.

Actually, the similar problem has already happened in conventional quantum theory. For example, assume we want to normalize $|\Psi\rangle = |0\rangle + |1\rangle$. Its inner product with itself is $\langle\Psi|\Psi\rangle = 2$. Since $\left(\pm\sqrt{2}\right)^2 = 2$, both $\frac{|\Psi\rangle}{\sqrt{2}}$ and $\frac{|\Psi\rangle}{-\sqrt{2}}$ are normalized and representing the same state $|\Psi\rangle$. In this case, we systematically choose dividing the positive square root as "the" normalized vector $|\Psi\rangle$ for in conventional quantum theory. In discrete case, we can also systematically choose the *principal inverse field norm* by utilizing a generator $g \in \mathbb{F}_{p^2}$ discussed in Sec. 3.4.1. Because g is a generator, any non-zero element $c \in \mathbb{F}_p \setminus \{0\}$ can be expressed as $g^{(p+1)k}$ where k is an integer and

Table 3.2: Inverse field norm over $\mathbb{F}_{3^2}$ with respect to the generator $1-\mathrm{i}$

$c = g^{(p+1)k}$	$(p+1)\,k$	k	$\mathsf{N}^{-1}\left(g^{(p+1)k}\right) = g^k$
-1	4	1	$1-\mathrm{i}$
1	0	0	1

$0 \leq k < p-1$, so we can define the principal inverse field norm $\mathsf{N}^{-1}\left(g^{(p+1)k}\right)$ as g^k. For example, the inverse field norm over $\mathbb{F}_{3^2}$ with respect to the generator $1-\mathrm{i}$ is shown in Table 3.2. Given the non-normalized state $|\Psi\rangle = |0\rangle + |1\rangle$, since its field norm is $\mathsf{N}\left(|\Psi\rangle\right) = \mathsf{N}\left(1\right) + \mathsf{N}\left(1\right) = -1$, it can be normalized as

$$\frac{|\Psi\rangle}{\mathsf{N}^{-1}\left(-1\right)} = \frac{|0\rangle + |1\rangle}{1-\mathrm{i}} = \left(1+\mathrm{i}\right)|0\rangle + \left(1+\mathrm{i}\right)|1\rangle\ . \tag{3.12}$$

3.4.3 IRREDUCIBLE DISCRETE D-DIMENSIONAL STATES: GENERALIZED DISCRETE BLOCH SPHERE

In the one-qubit state with coefficients in $\mathbb{F}_{p^2}$, the discrete analog of the Bloch sphere is constructed by exact analogy to the continuous case: we first require that the coefficients of the single qubit basis obey

$$\mathsf{N}\left(|\psi_1\rangle\right) = \mathsf{N}\left(\alpha_0\right) + \mathsf{N}\left(\alpha_1\right) = 1 \tag{3.13}$$

in the discrete field. We show that there are $p\left(p^2-1\right)$ such values later in the general theorem, Proposition 3.4.2. Given this requirement, which is similar in form to the conservation of probability, but not as useful due to the lack of orderable probability values, we can immediately conclude that the discrete analog of the Hopf fibration is again

$$\begin{aligned}
X &= 2\,\mathrm{Re}\,\alpha_0\alpha_1^* = 2x_0x_1 + 2y_0y_1\,, \\
Y &= 2\,\mathrm{Im}\,\alpha_0\alpha_1^* = 2x_1y_0 - 2x_0y_1\,, \qquad (3.14) \\
Z &= \mathsf{N}\left(\alpha_0\right) - \mathsf{N}\left(\alpha_1\right) = {x_0}^2 + {y_0}^2 - {x_1}^2 - {y_1}^2\,.
\end{aligned}$$

but now with all computations in $\pmod{p}$. At this point one simply writes down all possible discrete values for the complex numbers (α_0, α_1) satisfying Eq. (3.13) and enumerates those that project to the same value of (X, Y, Z). This equivalence class is the discrete analog of the circle in the complex plane that was eliminated in the continuous case. In Proposition 3.4.1, we show that $p + 1$ discrete values of (α_0, α_1) with unit norm map to the same point under the Hopf map Eq. (3.14)**TODO. Does Proposition 3.4.1 really show this?**; we may think of these as discrete circles or projective lines of equivalent, physically indistinguishable, complex phase. The surviving $p\,(p-1)$ values of (α_0, α_1) correspond to irreducible physical states of the discrete single qubit system. Thus, for example, choosing the underlying field to be $\mathbb{F}_{3^2}$, there are exactly 6 single-qubit state vectors to populate the Bloch sphere; the four equivalent phase-multiples mapping to each of the six points on the $\mathbb{F}_{3^2}$ Bloch sphere are collapsed and regarded as physically indistinguishable. In Figure 3.3, we plot the irreducible states on the Bloch sphere for $p = 3$, 7, and 11. Note that the Cartesian lengths of the real vectors corresponding to the points on the Bloch sphere vary considerably due to the nature of discrete fields; we have artificially normalized them to a “continuous world” unit radius sphere for conceptual clarity.

3.4.3.1 COUNTING STATES ON THE DISCRETE BLOCH SPHERE

We have the unique opportunity in the finite-field approach to quantum computing to precisely identify and enumerate the physical states. In the conventional theory, as we have seen in Sec. 2.1.3, we employ a generalized Hopf fibration on the normalized states to project out a circle of phase-

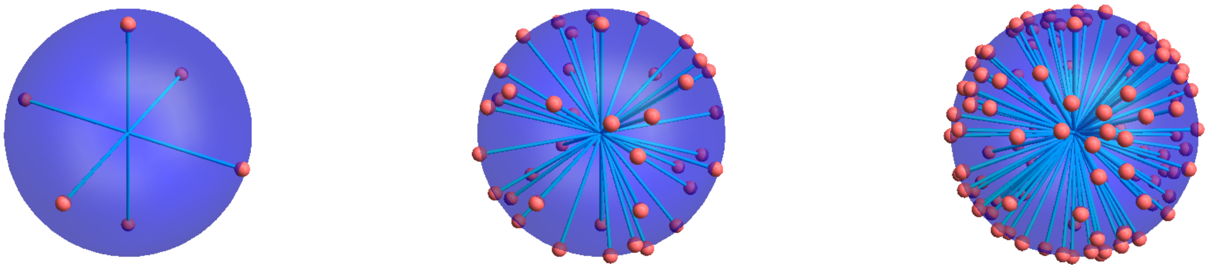


Figure 3.3: Schematically normalized plots of the elements of the discrete Bloch sphere, the irreducible single-qubit (two-dimensional) state vectors with unit norm over the field $\mathbb{F}_{p^2}$. We show the results for $p = 3$, 7, and 11. For example, in $\mathbb{F}_{3^2}$, there are 24 vectors of unit norm, but only the 6 inequivalent classes appear in the plot. The $p + 1 = 4$ equivalent vectors in each class differ only by a complex discrete phase.

equivalent states, yielding the generalized Bloch sphere.

In the introduction to this subsection, we sketched the counting of the irreducible single-qubit discrete states. To count the number of inequivalent discrete states for the general n-qubit case with coefficients in $\mathbb{F}_{p^2}$, we first must find the set of unit-norm states, and then determine the equivalence classes of unit-norm states under discrete phase transformations; we can then enumerate the list of states on the discrete generalized Bloch sphere. By executing computer searches of these spaces, we discovered an hypothesis for a closed-form solution for the counting of the states, and find a rigorous proof of the enumeration.

This process of describing the discrete D-dimensional irreducible states can again be understood geometrically by following the discrete analog of the Hopf fibration. First, we construct the discrete version of the quadratic unit-length form that automatically annihilates the distinction among states differing only by a discrete phase,

$$\hat{a} = \Big(\mathsf{N}\left(\alpha_i\right), \ldots, \sqrt{2}\,\mathrm{Re}\;\alpha_i\alpha_j^*, \ldots, \sqrt{2}\,\mathrm{Im}\;\alpha_i\alpha_j^*, \ldots\Big) \ , \tag{3.15}$$

where

$$\hat{a} \cdot \hat{a} = \left(\sum_{i=0}^{D-1} \mathsf{N}\left(\alpha_i\right) \right)^2 = 1\,. \tag{3.16}$$

From Proposition 3.4.1, we know that $p + 1$ elements of this discrete $\mathbf{S}^{2D-1}$ structure map to the *same point* in $\hat{a}$**TODO. Does Proposition 3.4.1 really show this?**. Each set of $p + 1$ redundant points is, geometrically speaking, the *discrete Hopf fibration circle* living above each *irreducible* point of the D-dimensional state description. These $p + 1$ points are interpretable as the p finite points plus the single point at infinity of the projective discrete line (see, e.g., [60]).

The next part of this argument is the determination of the unit-norm states, effectively the space of allowed discrete partitions of unity; we cannot exactly call these "probability-conserving" sectors of the state coefficients since we do not have a well defined notion of probability, but we do have a well-defined notion of partition of unity. Compared to the total number p^{2D} of possible complex integer state vectors that could be chosen, the number of unit-norm states is given by the following proposition. This unit-norm state structure is the discrete analog of $\mathbf{S}^{2D-1}$.

Proposition 3.4.2. *The number of unit-norm states described by a D-dimensional vector* $(\alpha_0, \dots, \alpha_{D-1})$ *with coefficients* $\alpha_i \in \mathbb{F}_{p^2}$ *is* $p^{D-1}\left(p^D - (-1)^D\right)$.

Proof. Proposition 11.27 in Grove [58] provides the count of the zero-norm states $\zeta\left(D, p\right) = p^{D-1}\left(p^D + (-1)^D\,(p-1)\right)$. Since there are p^2 elements $\alpha \in \mathbb{F}_{p^2}$, we must have $\left(p^2\right)^D = p^{2D}$ possible values of a D-dimensional vector $(\alpha_0, \dots, \alpha_{D-1})$. There are $p^2 - 1$ non-zero values of $\alpha \in \mathbb{F}_{p^2}$, and we showed in Proposition 3.4.1 that $\mathsf{N}\left(\alpha\right)$ maps exactly $p+1$ values in that set to each of the $p - 1$ non-zero values in $\mathbb{F}_p$. Therefore, the *unit-norm case* has a count of domain elements that is $\frac{1}{p-1}$ of the total number of non-zero-norm cases,

$$\frac{p^{2D} - \zeta\left(D, p\right)}{p-1} = \frac{p^{2D} - p^{2D-1} - (-1)^D\, p^{D-1}\,(p-1)}{p-1} = p^{D-1}\left(p^D - (-1)^D\right)\,. \tag{3.17}$$

□

Finally, we repeat the last step of the D-dimensional continuous Hopf fibration process for discrete D-dimensional states, eliminating the discrete set of $p+1$ equivalent points that map to the same point $\hat{a}$ on the generalized Bloch sphere. Dividing the tally $p^{D-1}\left(p^D-(-1)^D\right)$ of unit norm states by the $p+1$ elements of each phase-equivalent discrete circle, we find

$$\frac{p^{D-1}\left(p^D-(-1)^D\right)}{p+1} \tag{3.18}$$

as the total count of unique irreducible states in a discrete D-dimensional configuration. The resulting object is precisely the discrete version of $\mathbb{C}\mathbf{P}^{D-1}$, which we might call a *discrete complex projective space* or $\mathbf{D}\mathbb{C}\mathbf{P}^{D-1}$.

3.4.4 GEOMETRY OF ENTANGLED STATES

To discuss entanglement, we consider a D-dimensional quantum system composed of n-qubit subsystems, i.e., $D=2^n$ as usual. Without regard to uniqueness, an n-qubit state with discrete complex coefficients in $\mathbb{F}_{p^2}$ will have the total possible space of coefficients with dimension $p^{2\times 2^n}$ (including the null state). Imposing the condition of a length-one norm in $\mathbb{F}_p$, this number is reduced to $p^{2^n-1}\left(p^{2^n}-1\right)$. The ratio of all the states to the unit-norm states is asymptotically p:

$$\frac{p^{2^n+1}}{p^{2^n}-1}\to p\,, \tag{3.19}$$

so there are roughly p sets of coefficients, for any number of qubits n, that are discarded for each retained unit-length state vector. A factor of $p+1$ more states are discarded in forming the discrete Bloch sphere of irreducible states. Selected plots of the full space compared to both the unit-norm space and the irreducible space for a selection of complexified finite fields are shown in Figure 3.4 for 1, 2, 3, and 4 qubits.

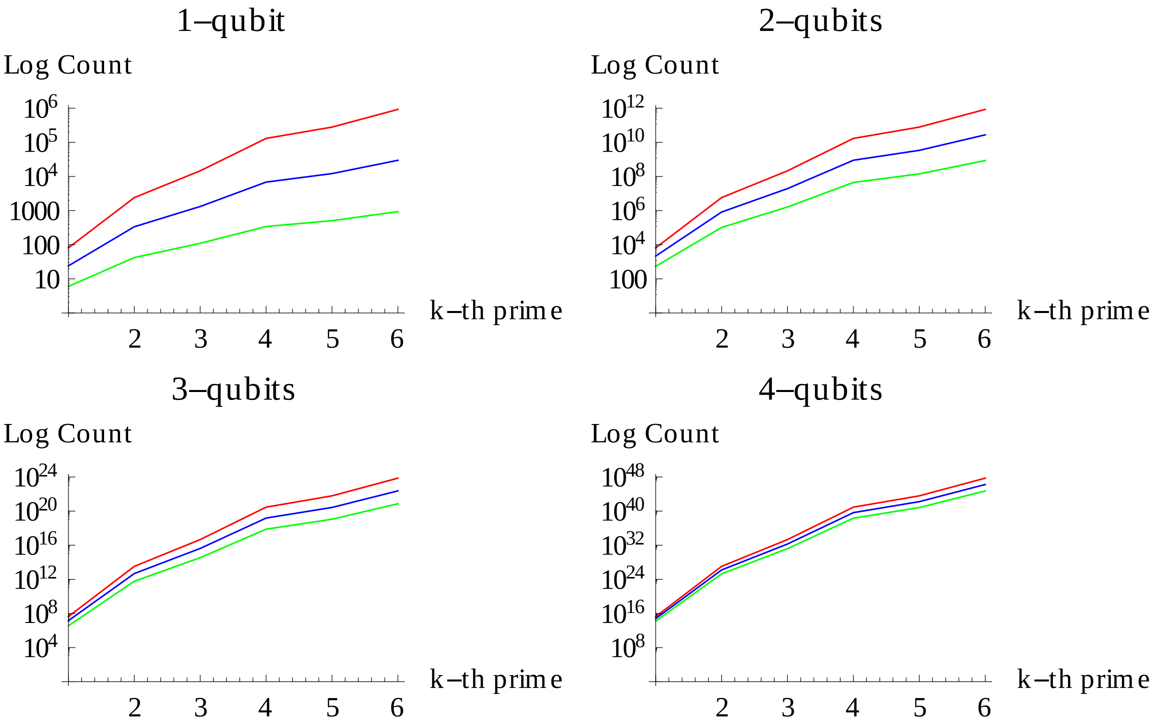


Figure 3.4: Logarithmic plot of the number of discrete unnormalized states (top, in red), vs the number of normalized discrete states (middle, in blue), vs the irreducible states (bottom, in green) for the first 6 $\mathbb{F}_{p^2}$-compatible primes, (3, 7, 11, 19, 23, 31), for the number of qubits 1, 2, 3, and 4.

3.4.4.1 UNENTANGLED VS ENTANGLED DISCRETE STATES

For a given p and the corresponding complexified field $\mathbb{F}_{p^2}$, the n-qubit discrete quantum states with coefficients in $\mathbb{F}_{p^2}$ can be classified by their degree of entanglement to a level of precision that is unavailable in the continuous theory. We look first at the unentangled n-qubit states, which are direct product states of the form

$$|\Psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_j\rangle \otimes \cdots \otimes |\psi_n\rangle \ . \tag{3.20}$$

Without regard to normalization, there are $\left(p^4\right)^n$ possible unentangled states out of the total of $p^{2\times 2^n}$ states noted above. When we normalize the individual product states to unit norm, the norm of the entire n-qubit state becomes the product of those unit norms, and is automatically normalized to one. We have already seen that each single-qubit normalized state in the tensor product Eq. (3.20) has precisely $p\,(p-1)$ irreducible components due to $D=2$ case in Eq. (3.18).

3.4.4.2 COMPLETELY UNENTANGLED STATES AND THE DISCRETE BLOCH SPHERE

In effect, the irreducible states for unentangled n-qubit configurations reduce to a single Bloch sphere for each one-qubit component $|\psi_j\rangle$, and thus the whole set of states is defined by an n-tuple of discrete Bloch sphere coordinates. Since each Bloch sphere in $\mathbb{F}_{p^2}$ has $p\,(p-1)$ distinct irreducible components, we have

$$\textbf{Count of Unentangled States} = p^n\,(p-1)^n \ . \tag{3.21}$$

According to Eq. (3.18), we know that the total number of irreducible states (points in the generalized $\mathbf{D}\mathbb{C}\mathbf{P}^{2^n-1}$ Bloch sphere) for an n-qubit state is $\frac{p^{2^n-1}(p^{2^n}-1)}{p+1}$, and so the number of states containing some measure of entanglement is

$$\textbf{Count of Entangled States} = \frac{p^{2^n-1}\,(p^{2^n}-1)}{p+1} - p^n\,(p-1)^n \ . \tag{3.22}$$

Therefore a very small fraction of the unit norm states are unentangled.

3.4.4.3 MAXIMAL ENTANGLEMENT

Equation (2.24) for $P_{\mathfrak{h}}$ includes a normalization factor $\frac{1}{n}$. In the discrete case, this normalization factor is undefined when $p \mid n$. Equation (2.24) also includes a summation of n terms. In the discrete case, certainly when $p \mid n$ but also in other cases, this summation may vanish in the field even if the individual summands are non-zero. These anomalies are irrelevant for the classification of unentangled states as this computation is performed by directly checking the possibility of direct decomposition into product states, disregarding equation (2.24).

For maximally entangled states, the purity calculation in conventional quantum mechanics using equation (2.24) produces 0. Given the above observations, in a discrete field, equation (2.24) may be undefined or may report a purity of 0 even for partially entangled states. For example, the normalized 5-qubit state $|\Psi\rangle = (1-\mathrm{i})\left(|00\rangle + |11\rangle\right) \otimes |000\rangle$ has $P_{\mathfrak{h}} = 0$ for $p = 3$, and is not maximally entangled because only the first two qubits are entangled. In the discrete case, we therefore check for maximally entangled states using the following equations [5],

$$\forall j, \forall \eta \in \{x, y, z\}\, , \left\langle \sigma_\eta^j \right\rangle^2 = 0\, , \tag{3.23}$$

which avoids the normalization factor and simply checks that each summand is 0.

We now implement these procedures to enumerate the maximally entangled states for the specific cases for $n = 2, 3$ and compare these to the counts for product states. We have verified explicitly in Eq. (3.21) that the numbers of unit-norm product states for $n = 2$, $p = \{3, 7, 11, 19, ...\}$ are

$$(p+1)p^2(p-1)^2 = \{144, 14\,112, 145\,200, 2339\,280, ...\}\, , \tag{3.24}$$

and for general n, $(p+1)p^n(p-1)^n$. The irreducible state counts are reduced by $(p+1)$, giving

$$p^2(p-1)^2 = \{36, 1764, 12\,100, 116\,964, ...\}\, , \tag{3.25}$$

and in general for n-qubits, there are $p^n\,(p-1)^n$ instances of pure product states.

Performing the computation using equation (3.23), we find the numbers of maximally entangled states for two qubits to be

$$p\left(p^2-1\right)(p+1) = \{96, 2688, 15\,840, 136\,800, ...\}\ . \tag{3.26}$$

The irreducible state counts for maximal entanglement are reduced by $(p+1)$, giving, for $n=2$,

$$p\left(p^2-1\right)=\{24,336,1320,6840,...\}\ . \tag{3.27}$$

For three qubits, there are $p^3\left(p^4-1\right)(p+1)$ (total) and $p^3\left(p^4-1\right)$ (irreducible) instances of pure maximally entangled states, while the general formula for 4-qubit states remains unclear.

Therefore, the ratio of maximally entangled to product states is

$$\frac{\textbf{Max entangled}}{\textbf{Product}}=\frac{p+1}{p\left(p-1\right)}\text{ and }\frac{\left(p^2+1\right)\left(p+1\right)}{\left(p-1\right)^2} \tag{3.28}$$

for $n=2$ and 3, respectively.

3.5 DISCRETE QUANTUM COMPUTING (I)

Given a complexified finite field $\mathbb{F}_{p^2}$ and its Hermitian dot product (Eq. (3.9)) much of the structure of conventional quantum computing can be recovered. For example, the smallest field $\mathbb{F}_{3^2}$ is already rich enough to express the standard Deutsch-Jozsa algorithm [61, 31, 38], which requires only normalized versions of vectors or matrices with the scalars 0, 1, and -1. Similarly, other deterministic quantum algorithms (algorithms for which we may determine the outcome with certainty), such as Simon's [62, 40, 38] and Bernstein-Vazirani [63, 40], perform as desired. In the following subsection, we will present the discrete Deutsch algorithm as an example. However, this quantum computing model is still different from the conventional one. On one hand, algorithms such as Grover's search [64, 40, 38] will not work in the usual way because we lack (the notion of) ordered angles and probability in general. On the other hand, this computational model still leads to excessive computational power for the unstructured database search problem for certain database sizes.

Table 3.3: Possible f for Deutsch black box U_f

Input	f_1	f_2	f_3	f_4
`false`	`false`	`false`	`true`	`true`
`true`	`false`	`true`	`false`	`true`
constant or balanced?	constant	balanced	balanced	constant

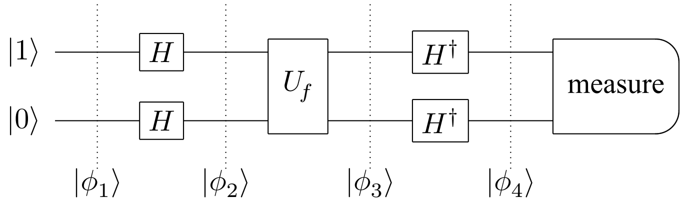


Figure 3.5: Quantum Circuit for Deutsch Algorithm.

3.5.1 DISCRETE DEUTSCH ALGORITHM

Although having no realistic application, the Deutsch algorithm is the first quantum algorithm which outperforms any possible classical algorithm for the Deutsch problem [56, 31, 40]. The Deutsch problem is to decide whether a function $f : \{\texttt{false}, \texttt{true}\} \to \{\texttt{false}, \texttt{true}\}$ is constant or balanced. As listed in Table 3.3, we have only 4 different f: 2 of them are constant while another 2 are balanced. Similar to our UNIQUE-SAT algorithm in Sec. 3.3, we start by representing f as a Deutsch black box U_f in the middle of the quantum circuit, Figure 3.5. To explain why this circuit solves the Deutsch problem, we then compute the state in each step explicitly, and express the Dirac bracket notation with its matrix representation in computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ parallelly. **TODO. We typeset U_f either directly or use macro \uf, but the definition of \uf has a negative space between U and f which is different from U_{f}... I need to understand whether the negative space is necessary or not, or whether the negative space has any semantic meaning...**

First, a 2-qubit pure state is initialized to $|\phi_1\rangle = |1\rangle |0\rangle = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$.

Second, on both initialized qubits, we apply the Hadamard matrix $H = \frac{1}{\alpha} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ over $\mathbb{F}_{p^2}$, where $\alpha = \mathsf{N}^{-1}(2)$ is the principal inverse field norm which is used to replace the square root $\sqrt{2}$ in the conventional Hadamard matrix $\frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)$ as discussed in Sec. 3.4.2. The second step produces

$$|\phi_2\rangle = (H \otimes H)\,|\phi_1\rangle = \left[\frac{1}{\alpha}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}\right] \otimes \left[\frac{1}{\alpha}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right] = |-\rangle\,|+\rangle \ ,$$

where

$$|+\rangle = \frac{1}{\alpha}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{|0\rangle + |1\rangle}{\alpha}\,, \qquad\qquad |-\rangle = \frac{1}{\alpha}\begin{pmatrix}1\\ -1\end{pmatrix} = \frac{|0\rangle - |1\rangle}{\alpha}\,. \tag{3.29}$$

Third, the Deutsch black box U_f is applied to the state $|\phi_2\rangle$. According to Eq. (3.5), these Deutsch black box will be used to apply exclusive disjunction on the first qubit, where we respectively identify `false` and `true` as 0 and 1 as usual. Since our first qubit is $|-\rangle$, the value $f\,(x)$ could be moved outside as a phase no matter $f\,(x)$ is `false` or `true`:

$$\begin{aligned} U_f\,|-\rangle\,|x\rangle &= \tfrac{1}{\alpha}\left[|0 \oplus f\,(x)\rangle\,|x\rangle - |1 \oplus f\,(x)\rangle\,|x\rangle\right] \\ &= \begin{cases} \tfrac{1}{\alpha}\left[|0\rangle\,|x\rangle - |1\rangle\,|x\rangle\right] \ , & \text{if } f\,(x) = \texttt{false} = 0\,; \\ \tfrac{1}{\alpha}\left[|1\rangle\,|x\rangle - |0\rangle\,|x\rangle\right] \ , & \text{if } f\,(x) = \texttt{true} = 1\,, \end{cases} \\ &= (-1)^{f(x)}\,|-\rangle\,|x\rangle \ . \end{aligned} \tag{3.30}$$

Then, $|\phi_3\rangle$ can be evaluated as follow:

$$\begin{aligned} |\phi_3\rangle &= U_f\,|-\rangle\,|+\rangle = \tfrac{1}{\alpha}\left[U_f\,|-\rangle\,|0\rangle + U_f\,|-\rangle\,|1\rangle\right] \\ &= \tfrac{1}{\alpha}\left[(-1)^{f(0)}\,|-\rangle\,|0\rangle + (-1)^{f(1)}\,|-\rangle\,|1\rangle\right] \\ &= \begin{cases} (-1)^{f(0)}\,|-\rangle\,|+\rangle \ , & \text{if } f\,(0) = f\,(1) \ ; \\ (-1)^{f(0)}\,|-\rangle\,|-\rangle \ , & \text{if } f\,(0) \neq f\,(1) \ . \end{cases} \end{aligned} \tag{3.31}$$

Finally, $|\phi_4\rangle$ can then be obtained by applying the Hermitian conjugate of Hadamard matrix

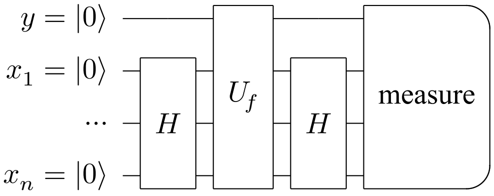


Figure 3.6: Circuit for black box UNIQUE-SAT in discrete quantum computing.

$H^\dagger = \frac{1}{\alpha^*} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix} \right)$ on both qubits. If $f(0) = f(1)$, i.e., f is constant, we have

$$|\phi_4\rangle = (-1)^{f(0)} \left[\frac{1}{\alpha^*} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\alpha} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right] \otimes \left[\frac{1}{\alpha^*} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\alpha} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] = (-1)^{f(0)} |1\rangle |0\rangle \ ;$$

if $f(0) \neq f(1)$, i.e., f is balanced, we have

$$|\phi_4\rangle = (-1)^{f(0)} \left[\frac{1}{\alpha^*} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\alpha} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right] \otimes \left[\frac{1}{\alpha^*} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\alpha} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right] = (-1)^{f(0)} |1\rangle |1\rangle \ .$$

Hence, we can decide whether f is constant or balanced by measuring $|\phi_4\rangle$ in the computational basis.

3.5.2 PARTIAL UNIQUE-SAT ALGORITHM

It is possible, in some situations, to exploit the cyclic behavior of the field to creatively cancel probability amplitudes and solve problems with what again appears to be “supernatural” efficiency. We illustrate this behavior with the algorithm in Fig. 3.6, which is a variant of the one in Fig. 3.1. Unlike the modal quantum algorithm, the new algorithm does not always succeed deterministically using a constant number of black box evaluations. We can, however, show that supernatural behavior occurs if the characteristic p of the field divides $2^N - 1$. For a database of fixed size N, matching the conditions becomes less likely as the size of the field increases. Nevertheless, for a *given* field, it is always possible to expand any database with dummy records to satisfy the divisibility property.

Physically, we are taking advantage of additional interference processes that happen because of the possibility of "wrapping around" due to modular arithmetic. We do not know, in general, whether this version of discrete quantum computing actually enables the rapid solution of NP-complete problems.

3.6 DISCRETE QUANTUM THEORY (II): INNER PRODUCT SPACE

We next discuss an approach using finite complexifiable fields that conditionally resolves the inner product condition (C) discussed in Sec. 3.4.2, which is violated by the theory just presented. A possible path is suggested by the work of Reisler and Smith [65]. The general idea is that while the cyclic properties of arithmetic in finite fields make it impossible to *globally* obtain the desired properties of the conventional Hilbert space inner product, it *is* possible to recover them *locally*, thereby restoring, with some restrictions, all the usual properties of the inner product needed for conventional quantum mechanics and conventional quantum computing. As the size of the discrete field becomes large, the size of the locally valid computational framework grows as well, leading to the *effective emergence of conventional quantum theory*. We next briefly outline such a context for local orderable subspaces of a finite field, and introduce an improvement on the original method [65] suggested by recent number theory resources [66].

Let us first note that the range of the quadratic map, $\{x^2 \bmod p \mid x \in \mathbb{F}_p\}$, is always one-half of the non-zero elements of $\mathbb{F}_p$, and is the set of elements with square roots in the field. This is the set of *quadratic residues*, and the complementary set (the other half of the non-zero field elements) is the set of *quadratic non-residues*. For example, in $\mathbb{F}_7$, the elements $\{1, 2, 4\}$ are considered positive as they have the square roots $\{1, 3, 2\}$ respectively; the remaining elements $\{3, 5, 6\}$ do not have square roots in the field. What is interesting is that if we have an uninterrupted sequence of numbers that are all quadratic residues, then we can define a *transitive order*, with $a > c$ if $a > b$ and $b > c$, provided $a - b$, $b - c$, and $a - c$ are all quadratic residues.**TODO. Should we remove the quadratic residue part? Since we never use take the square roots of numbers in order range later, whether they**

p	3	7	23	71	311	479	1559	5711	10559	18191	…
k	2	3	5	7	11	13	17	19	23	29	…
$\pi(k)$	1	2	3	4	5	6	7	8	9	10	…

Table 3.4: Number k of transitively ordered elements for a given field $\mathbb{F}_p$.

are the quadratic residues or not doesn't really matter...

As a concrete example, consider a finite field in which the sequential elements 0, 1, 2, 3, …, and $k-1$ are all quadratic residues (including 0). Then any sequence of odd length k and centered around an arbitrary $x \in \mathbb{F}_p$, i.e., $S_x(k) = x - \frac{k-1}{2}$, …, $x-2$, $x-1$, x, $x+1$, $x+2$, …, $x + \frac{k-1}{2}$, is *transitively ordered*. Indeed, we have $(x+1) - x = 1$ which is a quadratic residue and hence $x+1 > x$. Similarly, $x - (x-1) = 1$ and hence $x > x-1$. Also $(x+1) - (x-1) = 2$ which is a quadratic residue and hence $x+1 > x-1$. Clearly this process may be continued to show that the sequence $S_x(k)$ is transitively ordered. We can construct examples using the sequence A000229 in the encyclopedia of integer sequences [66][2]. The nth element of that sequence (which must be prime) is the least number such that the nth prime is the *least* quadratic non-residue for the given element. The first few elements of this sequence are listed in the top row of Table 3.4. The next row lists the number k of transitively ordered consecutive elements in that field, and $\pi(k)$ in the bottom row is the prime counting function (the number of primes up to k).

As an example, consider the field $\mathbb{F}_{23}$. Looking at the squares of the numbers $\mathbb{F}_{23} = \{0, \ldots, 22\}$ modulo 23, we find the 2-centered uninterrupted sequence $S_2(5) = \{0, 1, 2, 3, 4\}$, followed by 5, which is both the smallest quadratic non-residue and the size of the uninterrupted sequence of quadratic residues (including 0) of interest. In particular, it is possible to construct a total order for the elements $S_0(5) = \{-2, -1, 0, 1, 2\}$ in the fields $\mathbb{F}_{23}$, $\mathbb{F}_{71}$, $\mathbb{F}_{311}$, etc., but not in the smaller fields

[2] For computational purposes, this sequence is preferable to the one proposed by Reisler and Smith [65] because it produces smaller primes. Their work showed that a sufficient condition on finite fields to produce sequences of quadratic residues is to further constrain the underlying prime numbers to be of the form $8\prod_{i=1}^{m} q_i - 1$, where q_i is the ith odd prime. While all such primes are of the form $4\ell + 3$, the set is severely restricted to astronomical numbers because the first few such primes are 7, 23, 839, 9239, 2042039, …

	allowed probability amplitudes $F^D\left(k\right)$
$D=1$	$F^1\left(11\right)=\{0,\pm 1,\pm 2,\pm \mathrm{i},\pm 2\mathrm{i},(\pm 1\pm \mathrm{i}),(\pm 1\pm 2\mathrm{i}),(\pm 2\pm \mathrm{i})\}$
$D=2$	$F^2\left(11\right)=\{0,\pm 1,\pm \mathrm{i},(\pm 1\pm \mathrm{i})\}$
$D=3$	$F^3\left(11\right)=\{0,\pm 1,\pm \mathrm{i}\}$
$D=4$	$F^4\left(11\right)=\{0,\pm 1,\pm \mathrm{i}\}$
$D=5$	$F^5\left(11\right)=\{0,\pm 1,\pm \mathrm{i}\}$
$D\geq 6$	$F^D\left(11\right)=\{0\}$

Table 3.5: Allowed probability amplitudes for different vector space dimensions D and $k=11$.

$\mathbb{F}_3$ and $\mathbb{F}_7$.

Given a D-dimensional vector space over $\mathbb{F}_{p^2}$ where p is one of the primes above, it is possible to define a *region* over which an inner product and norm can be identified. Let the length of the sequence of quadratic residues be k. The region of interest includes all vectors $|\Psi\rangle=\sum_{i=0}^{D-1}\alpha_i\,|i\rangle=\begin{pmatrix}\alpha_0 & \alpha_1 & ... & \alpha_{D-1}\end{pmatrix}^T$, for which $D<p-\frac{k-1}{2}$ and each α_i satisfies

$$D\,\mathsf{N}\left(\alpha_i\right)=D\,\left(a_i^2+b_i^2\right)\leq\frac{k-1}{2}\,, \tag{3.32}$$

with a_i and b_i drawn from the set $S_0\left(k\right)$. Consider, for example, $\mathbb{F}_{311^2}$ ($p=311$, $k=11$). We find that we can trade off the dimension D of the vector space against the range of probability amplitudes available for each α_i in Table 3.5.

We can now verify, by using Table 3.5, that for any vector $|\Psi\rangle$ in the selected region the value of $\langle\Psi|\Psi\rangle$ is ≥ 0 and vanishes precisely when $|\Psi\rangle$ is the zero vector. Thus, in the selected region, condition (C) is established. Although the set of vectors defined over that region is not closed under addition, and hence the set is not a vector subspace, we can still have a theory by restricting our computations. In other words, *as long as our computation remains within the selected region*, we may pretend to have an inner product space. The salient properties of conventional quantum mechanics emerge, but the price to be paid is that the state space is no longer a vector space. This is basically a rigorous formulation of Schwinger's intuition (See, in particular, Chapter 1, Section 1.16. in [67]).

Readers with backgrounds in computer science or numerical analysis will notice, significantly, that this model for discrete quantum computing is reminiscent of practical computing with a classic microprocessor having only integer arithmetic and a limited word length. We cannot perform a division having a fractional result at all, since there are no fractional representations; we do have the basic constants zero and one, as well as positive and negative numbers, but multiplications or additions producing results outside the integer range wrap around modulo the word length and typically yield nonsense. This implies that, for the local discrete model, we must accept an operational world view that *has no awareness of the value of* p, and depends on having set up in advance an environment with a field size, analogous to the word size of a microprocessor, that happily processes *any* calculation we are prepared to perform. This is the key step, though it may seem strange because we are accustomed to arithmetic with real numbers: we list the calculations that must be performed in our theory, discover an *adequate size of the processor word* —implying a possibly ridiculously large value of p chosen as described above —and from that point on, we calculate necessarily valid values within that processor, never referring in any way to p itself in the sequel.

3.7 DISCRETE QUANTUM THEORY (II): CARDINAL PROBABILITY

The final issue that must be addressed in the discrete theory put forward in Section 3.6 concerns measurement. To recap, within the theory, states are D-dimensional vectors with complex discrete-valued amplitudes drawn from a totally-ordered range, $F^D(k)$, in the underlying finite field. These states possess, by construction, having field norms in the non-negative integers, all in the ordered range of Eq. (3.32), and hence potentially produce probabilities that can be ordered. We start by applying the measurement framework of conventional quantum computing to these states; we then systematically expose and isolate the parts that rely on infinite precision real numbers and replace them by finite approximations. Our point is that, although the mathematical framework of conventional quantum mechanics relies on infinite precision probabilities, it is impossible in practice to measure exact equality of real numbers —we can only achieve an approximation within measurement accuracy. Significantly, when we use finite fields, this measurement accuracy will be encoded in the size of the finite field used for measurements.

Although we can measure on every projector and observable as discussed in Sec. 2.2, our previous quantum circuits in Figures 3.1, 3.5, and 3.6 always measure in the computational basis $\{|0\rangle, |1\rangle, \ldots, |D-1\rangle\}$ in a D-dimensional Hilbert space, because measuring in other basis is the same as applying a quantum gate and measuring in the computational basis. Following this idea, we can simplify the Born rule for pure states, Eq. (2.16), as

$$\mu_{\Psi}^{B}\left(|i\rangle\langle i|\right) \equiv \mu_{\Psi}^{B}\left(i\right) = \frac{\langle\Psi|i\rangle\,\langle i|\Psi\rangle}{\langle\Psi|\Psi\rangle} = \frac{\left|\langle i|\Psi\rangle\right|^{2}}{\langle\Psi|\Psi\rangle} = \frac{\left|\alpha_{i}\right|^{2}}{\langle\Psi|\Psi\rangle}\,, \tag{3.33}$$

called the probability of measuring i, where $|\Psi\rangle = \sum_{i=0}^{D-1} \alpha_i \, |i\rangle = \begin{pmatrix}\alpha_0 & \alpha_1 & \ldots & \alpha_{D-1}\end{pmatrix}^T$.

Although a division required in Eq.(3.33) cannot be performed within an ordered region, we could follow the standard Mathematics and Computer Science procedure [21, 44, 68, 69] to define the result of a discrete Born rule as an order pair

$$\mu_{\Psi}^{C}\left(i\right) = \mathsf{N}\left(\alpha_{i}\right) \mathbin{/\!\!/} \mathsf{N}\left(|\Psi\rangle\right)\,. \tag{3.34}$$

3.8 DISCRETE QUANTUM COMPUTING (II)

We now examine two particularly important types of examples within the discrete theory of the previous section: the first is the deterministic Deutsch-Jozsa algorithm [**NCbook**, **Mermin**], which determines the balanced or unbalanced nature of an unknown function with a single measurement step ($O(1)$), and the second is the (normally) probabilistic Grover algorithm [**NCbook**, **Mermin**, **Grover**], determining the result of an unstructured search in $O(\sqrt{N})$ time. In the following, we use

k to denote the upper bound of the ordered range of integers needed to perform a given calculation; this in turn is assumed to be implemented using a choice of a finite prime number p that supports calculation in the range of k.

3.8.1 DISCRETE DEUTSCH-JOZSA ALGORITHM: DETERMINISTIC

To examine the Deutsch-Jozsa algorithm in the discrete theory of the previous section, we assume we are given a classical function $f : \mathsf{Bool}^n \to \mathsf{Bool}$, and are told that f is either constant or balanced [**NCbook**, **Mermin**]. The algorithm is expressed in a space of dimension $D = 2^{n+1}$: it begins with the $n+1$ qubit state $|1\rangle\,|\overline{0}\rangle$ where the overline denotes a sequence of length n. A straightforward calculation [**NCbook**] shows that the final state is [**HadamardNote**]

$$\sum_{\overline{z}\in\{0,1\}^n}\sum_{\overline{x}\in\{0,1\}^n}(-1)^{f(\overline{x})+\overline{x}\cdot\overline{z}}\left(|0\rangle\,|\overline{z}\rangle-|1\rangle\,|\overline{z}\rangle\right) \;,$$

and that its norm-squared is 2^{n+1}. To make sure that the algorithm works properly, we note that all the probability amplitudes involved in the calculation are in the range $-2^n,\dots,2^n$ and therefore, by Eq. (3.32), we get the following constraint on the size of the ordered region in the finite field:

$$2^{n+1}\left(2^n\right)^2 \le \frac{k-1}{2} \quad\Leftrightarrow\quad k \ge 2^{3n+2}+1 \;.$$

Now we need to choose a prime number p that supports calculation in the range of k. Assume that k is the least prime satisfying $k \ge 2^{3n+2}+1$, and let p be the $\pi(k)$th element of the sequence A000229 [66]. We argue that no prime less than this value of p can support calculation in the ordered range of k, and that this p is sufficient to support such calculation. In particular, since k is the least quadratic non-residue of p, every number less than k is a quadratic residue, and thus $0, 1, 2, 3, \dots, 2^{3n+2}$ are all quadratic residues. Hence the numbers $-2^n,\dots,2^n$ are all inside the ordered range $S_0(k)$. On the other hand, if we choose any prime smaller than p, there is a quadratic

p	...	422231	...	196265095009	...		...		...
k	...	**37**	...	**131**	...	**257**	...	**32771**	...
$\pi\left(k\right)$	...	12	...	32	...	55	...	3513	...

Table 3.6: Extension of transitively ordered elements.

non-residue smaller than k, and we also know that the least quadratic non-residue is a prime [46]. Thus, there is a quadratic non-residue in $0, 1, 2, 3, \ldots, 2^{3n+2}$, and therefore, for this smaller p, there would be a number in $-2^n, \ldots, 2^n$ that is not in the ordered range $S_0\left(k\right)$.

When f is constant, the cardinal probability of measuring $\left|0\right\rangle\left|\overline{0}\right\rangle$ or $\left|1\right\rangle\left|\overline{0}\right\rangle$ is $\left(2^n\right)^2 + \left(2^n\right)^2 = 2^{2n+1} \mathbin{/\!\!/} 2^{2n+1}$; i.e., the cardinal probability of measuring any other state is $0 \mathbin{/\!\!/} 2^{2n+1}$. When f is balanced, the cardinal probability of measuring $\left|0\right\rangle\left|\overline{0}\right\rangle$ or $\left|1\right\rangle\left|\overline{0}\right\rangle$ is $0 \mathbin{/\!\!/} 2^{2n+1}$. Therefore, if we find that the post-measurement state is either $\left|0\right\rangle\left|\overline{0}\right\rangle$ or $\left|1\right\rangle\left|\overline{0}\right\rangle$, we know f is constant; otherwise, f is balanced.

For a single qubit Deutsch problem, the absolute maximum probability amplitude is 2 and $D = 2^{1+1} = 4$, so we want to have

$$k \quad \geq \quad 2^{3\cdot 1+2} + 1 = 2^5 + 1 = 33 \; .$$

The least prime satisfying the above condition is $k = 37$, and thus

$$\begin{aligned} \pi\left(37\right) &= 12 \\ p &= 422231 \; , \end{aligned}$$

where the prime counting function $\pi\left(k\right)$ is taken from the extended elements in Table 3.6.

For the 2-qubit Deutsch-Jozsa, the computation is already quite challenging. Now the absolute maximum probability amplitude is 4 and $D = 2^{2+1} = 8$, so we need

$$k \;\geq\; 2^{3\cdot 2+2} + 1 = 2^{8} + 1 = 257\;.$$

Because 257 is a prime, we can pick

$$\begin{aligned} k &= 257 \\ \pi\,(257) &= 55\;. \end{aligned}$$

The actual value of p is already outside the range of the published tables.

These examples illustrate that the value of p plays an essential role: its size grows with the numerical range of the intermediate and final results of the algorithms being implemented. Therefore, we naturally recover a deterministic measure of the intrinsic resources required for a given level of complexity; this measure is normally completely hidden in computations with real numbers, and explicitly exposing it is one of the significant achievements of our discrete field analysis of quantum computation. This solves the conundrum that the conventional Deutsch-Jozsa algorithm mysteriously continues to work for larger and larger input functions without any apparent increase in resources. Our analysis of this problem reveals that as the size of the input increases, it is necessary to increase the size of p and hence the size of the underlying available numeric coefficients. This observation does not fully explain the power of quantum computing over classical computing, but at least it explains that some of the power of quantum computing depends on increasingly larger precision in the underlying field of numbers.

3.8.2 DISCRETE GROVER SEARCH: NONDETERMINISTIC

As an example of how to apply our cardinal probability framework to a nondeterministic algorithm, consider the $N \times N$ “diffusion” and “phase rotation” matrices for searching an unstructured database of size $N = 2^n$ using Grover's algorithm [**Grover**]:

$$\Delta = \begin{pmatrix} 1-\frac{N}{2} & 1 & 1 & ... & 1 \\ 1 & 1-\frac{N}{2} & 1 & ... & 1 \\ 1 & 1 & 1-\frac{N}{2} & ... & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & ... & 1-\frac{N}{2} \end{pmatrix},$$

$$R = \begin{pmatrix} -1 & 0 & 0 & ... & 0 \\ 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & ... & 1 \end{pmatrix},$$

where we have eliminated, in matrix Δ, the scaling factor $2/N$ to enforce the requirement that all matrix coefficients in our framework are integer-valued. Note that we have chosen the "marked" element in matrix R to be in the first position. In the standard algorithm, the transformation ΔR is repeated j times, where

$$j = round\left(\frac{\pi}{4\arccos\sqrt{1-\frac{1}{N}}} - \frac{1}{2}\right) \approx round\left(\frac{\pi}{4}\sqrt{N}\right) .$$

In our context, we must choose a prime number that is large enough to ensure that all the numbers that occur during the calculation and after measurement are within the transitively-ordered subrange.

Let f be the function we want to search, and let $\overline{t}$ be the target, i.e., $f\left(\overline{x}\right) = 1$ if and only if $\overline{x} = \overline{t}$. Because the probability amplitudes of $\left|\overline{x}\right\rangle$ are all the same for $\overline{x} \neq \overline{t}$, we can let a_l be the probability amplitude of $\left|\overline{t}\right\rangle$, with b_l the probability amplitude of each of the other possibilities, which are all the same. We begin at $l = 0$ with the information-less state, the normalization scaled to integer values as usual, which we can write as

$$\begin{pmatrix} a_0 \\ b_0 \\ \vdots \\ b_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} .$$

Applying the operators ΔR, and denoting by a_l and b_l the two unique elements of the N-dimensional column vector describing the evolving process, we find the following recurrence relation for the successive coefficients:

$$\begin{aligned} a_0 &= 1 \\ b_0 &= 1 \\ a_{l+1} &= \left(\frac{N}{2} - 1\right) a_l + (N-1)\, b_l \\ b_{l+1} &= (-1)\, a_l + \left(\frac{N}{2} - 1\right) b_l \, . \end{aligned}$$

We also know $|a_j| > |b_j|$, so we can estimate an upper bound for the maximum cardinal probability as

$$\max \mathsf{N}\left(a_j\right) \leq 2 \left(\frac{N}{2}\right)^{2j+1} .$$

By applying Eq. (3.32) with $D = N = 2^n$, we can estimate k using

$$k \geq 8 \left(\frac{N}{2}\right)^{2j+2} + 1 \, .$$

If we pick a prime k satisfying the above condition, then choosing the $\pi(k)$th prime in the sequence represented by Table 3.4 guarantees that every number we need for the computation is within the transitively ordered range $F^D(k)$.

For the 2-qubit Grover search, we have $N = D = 4$ and $j = 1$, with the maximum cardinal probability

$$\max \mathsf{N}\left(a_j\right) \leq 2 \left(\frac{4}{2}\right)^{2+1} = 16 \, ,$$

so we need

$$k \;\geq\; 8\left(\frac{4}{2}\right)^{2\cdot 1+2} + 1 = 8\cdot 2^4 + 1 = 129\ .$$

The least prime k satisfying the above condition is $k = 131$, and so

$$\begin{aligned}\pi\left(131\right) &= 32 \\ p &= 196265095009\ .\end{aligned}$$

When $p = 196265095009$, we assume that $f\left(\overline{x}\right) = 1$ if and only if $|\overline{x}\rangle = |0\rangle|0\rangle$, and so the final state is $(4, 0, \cdots, 0)^T$ with norm-squared of 16. Then, the cardinal probability of obtaining $|0\rangle|0\rangle$ as the post-measurement state is $16 \mathbin{/\!/} 16$, and it is $0 \mathbin{/\!/} 16$ for the rest of the states.

For the 3-qubit Grover search, we have $N = D = 8$ and $j = 2$, with an upper bound $\max \mathsf{N}\left(a_j\right) \leq 2\left(\frac{8}{2}\right)^{4+1} = 2048$ on the cardinal probability. Thus

$$k \;\geq\; 8\left(\frac{8}{2}\right)^{6} + 1 = 32769\ .$$

The nearest prime greater than this number is 32771, so we can pick

$$\begin{aligned}k &= 32771 \\ \pi(32771) &= 3513\ ,\end{aligned}$$

and so if we use the 3513th prime, we can implement Grover's algorithm for a database of size 8.

Continuing with the 3-qubit Grover example, we show how the cardinal probabilities evolve to single out the target state. First, assume that $f\left(\overline{x}\right) = 1$ if and only if $|\overline{x}\rangle = |0\rangle|0\rangle|0\rangle$. The initial information-less 8-dimensional state vector evolves under the application of ΔR as follows:

$$\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} 10 \\ 2 \\ \vdots \\ 2 \end{pmatrix} \rightarrow \begin{pmatrix} 44 \\ -4 \\ \vdots \\ -4 \end{pmatrix} .$$

These states have differing norm-squared, so we multiply the first and second states by 16 and 4, respectively, to force them to have the same value of 2048. The now-consistently-normalized states become

$$\begin{pmatrix} 16 \\ 16 \\ \vdots \\ 16 \end{pmatrix} \rightarrow \begin{pmatrix} 40 \\ 8 \\ \vdots \\ 8 \end{pmatrix} \rightarrow \begin{pmatrix} 44 \\ -4 \\ \vdots \\ -4 \end{pmatrix} .$$

Therefore, the cardinal probabilities of measuring $|0\rangle|0\rangle|0\rangle$ in each state are

$$256 \,/\!\!/\, 2048 \qquad 1600 \,/\!\!/\, 2048 \qquad 1936 \,/\!\!/\, 2048 \;,$$

while the cardinal probabilities of measuring the other states become

$$256 \,/\!\!/\, 2048 \qquad 64 \,/\!\!/\, 2048 \qquad 16 \,/\!\!/\, 2048 \;.$$

We may thus conclude that the cardinal probability of measuring the satisfying assignment of f increases as we apply the diffusion Δ and phase rotation R matrices repeatedly.

Clearly, the required size of k increases systematically with the problem size, and the corresponding size of the required prime number p defining the discrete field increases in the fashion illustrated in Tables 3.4 and 3.6.

3.9 TOWARD DISCRETE QUANTUM PROBABILITY

When people tried to define quantum probability over finite fields, people tended to treat the original Born rule as an axiom, and tried to modify it to get a discrete Born rule [48, 50, 2, 70]. However, any modified Born rule could hardly work on the whole vector space, since there is no inner product on the whole vector space over finite fields. Instead of treating the Born rule as an axiom, the Born rule can actually be deduced from a set of abstract definitions and axioms according to Gleason's theorem. Although we might hope to deduce a discrete Born rule directly from a similar set of definitions and axioms, no discrete Born rule satisfies certain properties motivated by Gleason's theorem with infinitely precise real-number probability [5]. Since the state spaces are now discrete and finite, this suggests us to consider a discrete Born rule mapping to finite number of intervals called interval-valued probability [71, 3]. To adopting the idea of interval-valued probability step-by-step, before attempting to study quantum interval-valued probability over finite fields, we will first review the classical interval-valued probability, and extend it with the conventional quantum theory.

Chapter 4

TOWARD A QUANTUM MEASUREMENT THEORY WITH ERROR: QUANTUM INTERVAL-VALUED PROBABILITY

4.1 CLASSICAL INTERVAL-VALUED PROBABILITY

In the classical setting, there are several proposals for "imprecise probabilities" [72, 73, 74, 71, 75, 33]. Although these proposals differ in some details, they all share the fact that the probability $\bar{\mu}(E)$ of an event E is generalized from a single *real number* to an *interval* $[l, r]$, where l intuitively corresponds to the strength of evidence for the event E and $1 - r$ corresponds to the strength of evidence against the same event. Given a sample space Ω and a set of intervals $\mathcal{I}$, similar to a classical probability measure $\mu : 2^{\Omega} \rightarrow [0, 1]$, a classical interval-valued probability measure (IVPM) $\bar{\mu} : 2^{\Omega} \rightarrow \mathcal{I}$ needs to satisfy some coherent axioms. By satisfying the convexity axiom [76, 73, 74, 33], Shapley proved that there is always a classical probability measure consistent with the classical IVPM $\bar{\mu}$ [76, 73, 33]. Given any random variable, its expectation value with respect to classical probability measures consistent with $\bar{\mu}$ is consistent with its Choquet integral [77, 73, 33] with respect to $\bar{\mu}$ [78, 73, 33].

4.2 QUANTUM INTERVAL-VALUED PROBABILITY

The quantum extension, quantum interval-valued probability measure (QIVPM) $\bar{\mu} : \mathcal{E} \rightarrow \mathcal{I}$, is a generalization of both classical IVPMs $\bar{\mu} : 2^{\Omega} \rightarrow \mathcal{I}$ and conventional quantum probability measures $\mu : \mathcal{E} \rightarrow [0, 1]$ [3], because QIVPMs reduce to classical IVPMs when the space of quantum events $\mathcal{E}$ is restricted to mutually commuting events, and reduces to conventional quantum probability measures when mapping to infinitely precise uncountable intervals $\mathcal{I}_{\infty} = \{[x, x] \mid x \in [0, 1]\}$. While Shapley and Gleason both proved there must be a "state" consistent with any given QIVPM in the reduced cases, in general there exists a QIVPM such that no state is consistent with it. However, we found a class of QIVPMs such that all QIVPMs in this class are consistent with a non-empty "ball" of quantum states whose radius is defined by the maximal length of the intervals, and recovers the original Gleason theorem asymptotically. Similarly, the conventional quantum expectation value and the classical Choquet integral are together generalized to the quantum interval-valued expectation value. This is used to prove an imprecise Kochen-Specker theorem [79, 80, 36, 41, 38] which suggests a possible resolution of the Meyer-Mermin debate on the impact of finite-precision measurement on the Kochen-Specker theorem [81, 82].

Chapter 5

FURTHER QUESTIONS

When people proved the original Gleason theorem, people usually exploited the geometrical structure of real 3-dimensional Hilbert space [35, 41, 83, 84]. Since our finite-precision extension of the Gleason theorem only applies on a class of QIVPMs, we might want to ask how to modify these geometrical arguments to have a Gleason-type theorem for general QIVPMs. We will further study the tensor product structure among QIVPMs which is essential for defining product and entangled states, and serves the basis to discuss quantum nonlocality [85, 36, 41, 38] and quantum computing with QIVPMs. Finally, we want to improve the discrete quantum theories to consider QIVPMs over finite fields in future research.

BIBLIOGRAPHY

[1] Andrew J. Hanson, Gerardo Ortiz, Amr Sabry, and Yu-Tsung Tai. “Geometry of discrete quantum computing”. In: *J. Phys. A: Math. Theor.* 46.18 (2013), p. 185301. Erratum “Corrigendum: Geometry of discrete quantum computing”. In: *J. Phys. A: Math. Theor.* 49.3 (Dec. 2016), p. 039501.

[2] Andrew J. Hanson, Gerardo Ortiz, Amr Sabry, and Yu-Tsung Tai. “Discrete quantum theories”. In: *J. Phys. A: Math. Theor.* 47.11 (2014), p. 115305.

[3] Yu-Tsung Tai, Andrew J. Hanson, Gerardo Ortiz, and Amr Sabry. *Quantum Interval-Valued Probability: Contextuality and the Born Rule*. Dec. 25, 2017. arXiv: `1712.09006 [quant-ph]`.

[4] Samson Abramsky. “Big toy models: Representing physical systems as Chu spaces”. In: *Synthese* 186.3 (2012), pp. 697–718.

[5] John Gardiner. “Notes on Quantum Mechanics over a Finite Field”. In: *Research Experience for Undergraduates. Research Reports*. Ed. by Chris Connell. Indiana University, Bloomington, 2014, pp. 5–18.

[6] The LyX Team. *LyX 2.3.0 - The Document Processor [Computer software and manual]*. Internet: http://www.lyx.org. Retrieved June 27, 2018, from http://www.lyx.org. 2018.

[7] Scott Aaronson and Alex Arkhipov. “The Computational Complexity of Linear Optics”. In: *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*. STOC ’11. San Jose, California, USA: ACM, 2011, pp. 333–342.

[8] Matthew A. Broome, Alessandro Fedrizzi, Saleh Rahimi-Keshari, Justin Dove, Scott Aaronson, Timothy C. Ralph, and Andrew G. White. "Photonic Boson Sampling in a Tunable Circuit". In: *Science* 339.6121 (2013), pp. 794–798. eprint: `http://science.sciencemag.org/content/339/6121/794.full.pdf`.

[9] Ethan Bernstein and Umesh Vazirani. "Quantum Complexity Theory". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1411–1473. eprint: `http://dx.doi.org/10.1137/S0097539796300921`.

[10] P. Kaye, R. Laflamme, and M. Mosca. *An Introduction to Quantum Computing*. Oxford University Press, 2007.

[11] Dan Boneh. "Twenty years of attacks on the RSA cryptosystem". In: *Notices of the AMS* 46.2 (Feb. 1999), pp. 203–213.

[12] Wikipedia. *RSA Factoring Challenge — Wikipedia, The Free Encyclopedia*. [Online; accessed 12-November-2016]. 2016.

[13] Scott Aaronson. "Guest Column: NP-complete Problems and Physical Reality". In: *SIGACT News* 36.1 (Mar. 2005), pp. 30–52.

[14] Gualtiero Piccinini. *Physical Computation. A mechanistic account*. Oxford University Press (OUP), June 2015.

[15] Hans Camenzind. *Designing Analog Chips*. Virtualbookworm.com Publishing, Mar. 31, 2005. 244 pp.

[16] A. M. Turing. "On Computable Numbers, with an Application to the Entscheidungsproblem". In: *Proceedings of the London Mathematical Society* s2-42.1 (Jan. 1937), pp. 230–265. Erratum "On Computable Numbers, with an Application to the Entscheidungsproblem. A Correction". In: *Proceedings of the London Mathematical Society* s2-43.6 (Jan. 1938), pp. 544–546.

[17] Hava T. Siegelmann. *Neural Networks and Analog Computation*. Birkhäuser Boston, Dec. 1, 1998. 204 pp.

[18] Martin Ziegler. "Real Computability and Hypercomputation". Habilitationsschrift. University of Paderborn, 2007.

[19] K. Weihrauch. *Computable Analysis: An Introduction*. Texts in Theoretical Computer Science. An EATCS Series. Springer Berlin Heidelberg, 2012.

[20] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. SpringerLink : Bücher. Springer New York, Dec. 6, 2012.

[21] M. Artin. *Algebra*. Prentice Hall, 1991.

[22] Allen Hatcher. *Algebraic Topology*. Cambridge University Pr., 2001. 556 pp.

[23] Rémy Mosseri and Rossen Dandoloff. "Geometry of entangled states, Bloch spheres and Hopf fibrations". In: *Journal of Physics A: Mathematical and General* 34.47 (2001), p. 10243.

[24] Andrew J. Hanson. *Visualizing Quaternions*. Elsevier LTD, Oxford, Jan. 11, 2006. 600 pp.

[25] I. Bengtsson and K. Zyczkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, 2007.

[26] Wikipedia contributors. *Hopf fibration — Wikipedia, The Free Encyclopedia*. [Online; accessed 3-March-2018]. 2017.

[27] Ken Shoemake. "Animating Rotation with Quaternion Curves". In: *Proceedings of the 12th Annual Conference on Computer Graphics and Interactive Techniques*. SIGGRAPH '85. New York, NY, USA: ACM, 1985, pp. 245–254.

[28] Wikipedia contributors. *Slerp — Wikipedia, The Free Encyclopedia*. [Online; accessed 3-March-2018]. 2018.

[29] Marcel Berger and Bernard Gostiaux. *Differential Geometry: Manifolds, Curves, and Surfaces*. Graduate Texts in Mathematics. Springer New York, 1988.

[30] Andrei Nikolaevich Kolmogorov. *Foundations of the Theory of Probability*. English. Trans. from the German by Nathan Morrison. New York: Chelsea Publishing Company, 1950.

[31] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. New York, NY, USA: Cambridge University Press, 2000.

[32] Robert B. Griffiths. *Consistent quantum theory*. Cambridge University Press, 2003.

[33] Michel Grabisch. *Set functions, games and capacities in decision making*. Theory and Decision Library C 46. Springer International Publishing, 2016.

[34] George W. Mackey. "Quantum Mechanics and Hilbert Space". In: *The American Mathematical Monthly* 64.8 (1957), pp. 45–57.

[35] Andrew Gleason. "Measures on the Closed Subspaces of a Hilbert Space". In: *Indiana Univ. Math. J.* 6 (4 1957), pp. 885–893.

[36] Michael Redhead. *Incompleteness, Nonlocality, and Realism: A Prolegomenon to the Philosophy of Quantum Mechanics*. Oxford University Press, 1987.

[37] Hans Maassen. "Quantum probability and quantum information theory". In: *Quantum information, computation and cryptography*. Springer, 2010, pp. 65–108.

[38] Gregg Jaeger. *Quantum Information*. Springer New York, Apr. 3, 2007.

[39] Max Born. "On the Quantum Mechanics of Collisions". English. In: *Quantum Theory and Measurement*. Trans. by John Archibald Wheeler and Wojciech Hubert Zurek. Princeton University Press, 1983, pp. 52–55.

[40] N. David Mermin. *Quantum Computer Science*. Cambridge University Press, 2007.

[41] Asher Peres. *Quantum Theory: Concepts and Methods*. Fundamental Theories of Physics. Springer, Sept. 30, 1995. 464 pp.

[42] Howard Barnum, Emanuel Knill, Gerardo Ortiz, and Lorenza Viola. “Generalizations of entanglement based on coherent states and convex sets”. In: *Physical Review A* 68.3 (Sept. 2003), p. 032308.

[43] Howard Barnum, Emanuel Knill, Gerardo Ortiz, Rolando Somma, and Lorenza Viola. “A Subsystem-Independent Generalization of Entanglement”. In: *Physical Review Letters* 92.10 (10 Mar. 2004), p. 107902.

[44] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, Inc., 2004.

[45] G. L. Mullen and C. Mummert. *Finite Fields and Applications*. American Mathematical Society, Rhode Island, 2007.

[46] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford, 2006.

[47] I. Stewart. *Galois theory*. Chapman and Hall/CRC, Boca Raton, 2004.

[48] Benjamin Schumacher and Michael D. Westmoreland. “Modal Quantum Theory”. In: *Foundations of Physics* 42.7 (2012), pp. 918–925.

[49] Benjamin Schumacher and Michael D. Westmoreland. *Non-contextuality and free will in modal quantum theory*. Oct. 26, 2010. arXiv: `1010.5452v1 [quant-ph]`.

[50] Lay Nam Chang, Zachary Lewis, Djordje Minic, and Tatsu Takeuchi. “Galois Field Quantum Mechanics”. In: *Modern Physics Letters B* 27.10 (2013), p. 1350064. eprint: `http://www.worldscientific.com/doi/pdf/10.1142/S0217984913500644`.

[51] Lay Nam Chang, Zachary Lewis, Djordje Minic, and Tatsu Takeuchi. “Quantum $\mathbb{F}_{un}$: the $q = 1$ limit of Galois field quantum mechanics, projective geometry and the field with one element”. In: *Journal of Physics A: Mathematical and Theoretical* 47.40 (2014), p. 405304.

[52] Roshan P. James, Gerardo Ortiz, and Amr Sabry. *Quantum Computing over Finite Fields*. Jan. 19, 2011. arXiv: `1101.3764v1 [quant-ph]`.

[53] Jeremiah Willcock and Amr Sabry. *Solving UNIQUE-SAT in a Modal Quantum Theory*. Feb. 17, 2011. arXiv: `1102.3587v1 [quant-ph]`.

[54] Christos H. Papadimitriou. *Computational Complexity*. Addison-Wesley Publishing Company, Dec. 11, 1993.

[55] L. G. Valiant and V. V. Vazirani. "NP is as easy as detecting unique solutions". In: *Theoretical Computer Science* 47 (1986), pp. 85–93.

[56] David Deutsch. "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer". In: *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 400.1818 (July 1985), pp. 97–117.

[57] Andrew J. Hanson, Gerardo Ortiz, Amr Sabry, and Jeremiah Willcock. *The Power of Discrete Quantum Theories*. Apr. 8, 2011. arXiv: `1104.1630v1 [quant-ph]`.

[58] Larry C. Grove. *Classical Groups and Geometric Algebra*. Fields Institute Communications. American Mathematical Society, 2002.

[59] Wikipedia contributors. *Field norm — Wikipedia, The Free Encyclopedia*. `https://en.wikipedia.org/w/index.php?title=Field_norm&oldid=804256096`. [Online; accessed 21-April-2018]. 2017.

[60] V. I. Arnold. *Dynamics, Statistics and Projective Geometry of Galois Fields*. Cambridge University Press, 2010.

[61] David Deutsch and Richard Jozsa. "Rapid Solution of Problems by Quantum Computation". In: *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 439.1907 (1992), pp. 553–558. eprint: `http://rspa.royalsocietypublishing.org/content/439/1907/553.full.pdf`.

[62] D. R. Simon. “On the Power of Quantum Computation”. In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. SFCS ’94. Washington, DC, USA: IEEE Computer Society, 1994, pp. 116–123.

[63] Ethan Bernstein and Umesh Vazirani. “Quantum Complexity Theory”. In: *Proceedings of the Twenty-fifth Annual ACM Symposium on Theory of Computing*. STOC ’93. San Diego, California, USA: ACM, 1993, pp. 11–20. Updated Version “Quantum Complexity Theory”. In: *SIAM Journal on Computing* 26.5 (1997), pp. 1411–1473. eprint: `http://dx.doi.org/10.1137/S0097539796300921`.

[64] Lov K. Grover. “A Fast Quantum Mechanical Algorithm for Database Search”. In: *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*. STOC ’96. Philadelphia, Pennsylvania, USA: ACM, 1996, pp. 212–219.

[65] Donald L Reisler and Nicholas M Smith. *Geometry Over a Finite Field*. Tech. rep. AD0714115. Defense Technical Information Center, Jan. 1969.

[66] N. J. A. Sloane and Simon Plouffe. *The Encyclopedia of Integer Sequences*. Academic Press, San Diego, 2005.

[67] Julian Schwinger. *Quantum Mechanics*. Ed. by Berthold-Georg Englert. Physics and astronomy online library. Springer-Verlag GmbH, Feb. 27, 2003.

[68] The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. Institute for Advanced Study: `https://homotopytypetheory.org/book`, 2013.

[69] Stephen Wolfram. *An Elementary Introduction To The Wolfram Language*. Wolfram Media Inc, Jan. 14, 2016. 328 pp.

[70] David Ellerman. “Quantum mechanics over sets: a pedagogical model with non-commutative finite probability theory as its quantum probability calculus”. In: *Synthese* (2016), pp. 1–34.

[71] Kenneth David Jamison and Weldon A. Lodwick. *Interval-Valued Probability Measures*. Tech. rep. 213. Center for Computational Mathematics, University of Colorado Denver, 2004.

[72] Glenn Shafer. *A Mathematical Theory of Evidence*. Princeton University Press, Apr. 11, 1976. 314 pp.

[73] Itzhak Gilboa and David Schmeidler. "Additive representations of non-additive measures and the Choquet integral." In: *Annals of Operations Research* 52.1–4 (1994), pp. 43–65.

[74] Massimo Marinacci. "Limit Laws for Non-additive Probabilities and Their Frequentist Interpretation". In: *Journal of Economic Theory* 84.2 (Feb. 1999), pp. 145–195.

[75] Peter J. Huber and Elvezio M. Ronchetti. *Robust Statistics*. English. 2nd ed. Wiley Series in Probability and Statistics. John Wiley & Sons Inc., Mar. 6, 2009. 354 pp.

[76] Lloyd S. Shapley. "Cores of convex games". In: *International Journal of Game Theory* 1.1 (1971), pp. 11–26.

[77] Gustave Choquet. "Theory of capacities". In: *Annales de l'institut Fourier* 5 (1954), pp. 131–295.

[78] Joachim Rosenmüller. "On core and value". In: *Operations Research-Verfahren. Methods of operations research* 9 (1971), pp. 84–104.

[79] John S. Bell. "On the Problem of Hidden Variables in Quantum Mechanics". In: *Rev. Mod. Phys.* 38.3 (3 July 1966), pp. 447–452.

[80] S. Kochen and E. Specker. "The Problem of Hidden Variables in Quantum Mechanics". In: *Indiana Univ. Math. J.* 17 (1 1968), pp. 59–87.

[81] David Meyer. "Finite Precision Measurement Nullifies the Kochen-Specker Theorem". In: *Phys. Rev. Lett.* 83 (19 Nov. 1999), pp. 3751–3754.

[82] N. David Mermin. *A Kochen-Specker Theorem for Imprecisely Specified Measurement*. Dec. 16, 1999. arXiv: `quant-ph/9912081v1 [quant-ph]`.

[83] Fred Richman and Douglas Bridges. “A Constructive Proof of Gleason’s Theorem”. In: *Journal of Functional Analysis* 162.2 (1999), pp. 287–312.

[84] Jan Hamhalter. *Quantum Measure Theory*. Vol. 134. The Fundamental Theories of Physics. Springer Science & Business Media, Oct. 31, 2003. 420 pp.

[85] J. S. Bell. “On the Einstein Podolsky Rosen Paradox”. English. In: *Physics. Physique. физика. An International journal for selected articles which deserve the special attention of physicists in all fields.* 1 (3 Nov. 1964), pp. 195–200.

Yu-Tsung Tai
LinkedIn : https://www.linkedin.com/in/yu-tsung-tai-9aa30551
GitHub : https://github.com/yuttai

EDUCATION

Indiana University Bloomington (IUB) (GPA: 3.802/4.0) **2010 – Present**

- Ph.D. double-major in Mathematics and Computer Science (expected) November 2018
- Master of Science in Computer Science May 2016
- Master of Arts in Mathematics December 2012

National Taiwan University (NTU) (GPA: 3.68/4.0) **2002 – 2006**

- Bachelor of Science in Mathematics (Rank: 4/48) June 2006

PUBLICATIONS

[1] Y.-T. Tai, A. J. Hanson, G. Ortiz and A. Sabry, "Quantum interval-valued probability: Contextuality and the Born rule," *Phys. Rev. A*, vol. 97, no. 5, p. 052121, May 2018.

[2] A. J. Hanson, G. Ortiz, A. Sabry and Y.-T. Tai, "Discrete Quantum Theories," *J. Phys. A: Math. Theor.*, vol. 47, p. 115305, 2014.

[3] A. J. Hanson, G. Ortiz, A. Sabry and Y.-T. Tai, "Geometry of Discrete Quantum Computing," *J. Phys. A: Math. Theor.*, vol. 46, p. 185301, 2013. Erratum "Corrigendum: Geometry of Discrete Quantum Computing," *J. Phys. A: Math. Theor.*, vol. 49, p. 039501, 12 2016.

CONFERENCES AND SEMINARS

Quantum Interval-Valued Probability: Contextuality and the Born Rule

- Talk in Interdisciplinary Logic Seminar, IUB August 2017
- Poster Session in Contextuality: Conceptual Issues, Operational Signatures, and Applications, Perimeter Institute for Theoretical Physics July 2017

Introduction to Discrete Quantum Theories and Computing

- Talk in Theory Seminar, Department of Computer Science, IUB March 2017

Real Computation

- Talk in Theory Reading Group, Department of Computer Science, IUB Feb 2016

TEACHING EXPERIENCE

Taught with Full Responsibility

- MATH-T101 Mathematics for Elementary Teachers I, IUB Fall 2017
- MATH-M216 Calculus II (Online), Indiana University East Summer 2012

Designed and Edited Online Courses, Data Science Program, IUB

- Basic Linear Algebra and Calculus with Python (Designer) Summer 2017 – Spring 2018
- Machine Learning with Python (Editor) Fall 2016 – Spring 2018
- Introduction to C++ (Designer) Summer 2016 – Fall 2017

Taught Recitation Sessions, IUB

- MATH-M211 Calculus I Fall 2016
- MATH-M212 Calculus II Summer 2014, Fall 2014, Fall 2015
- CSCI-B501 Theory of Computing Spring 2015

Assisted and Graded, IUB

- CSCI-B609 Topics in Algorithms and Computing Theory (AlphaGo) Spring 2018
- INFO-I231 Introduction to the Mathematics of Cybersecurity Spring 2017
- CSCI-B503 Algorithms Design and Analysis Spring 2016
- MATH-M119 Brief Survey of Calculus I Fall 2013, Spring 2014
- MATH-M303 Linear Algebra for Undergraduates Spring 2013
- MATH-M118 Finite Mathematics Fall 2010, Fall 2012
- MATH-M301 Linear Algebra and Applications Spring 2012
- MATH-M365 Introduction to Probability and Statistics Fall 2011
- MATH-M120 Brief Survey of Calculus II Spring 2011
- MATH-S312 Honors Course in Calculus IV Spring 2011

Taught Mini-Courses in NTU Math Camps

- There is No Formula for General Quintic Equations in Terms of Radicals 2005
- Game Theory 2004

RESEARCH APPOINTMENTS

- Research Assistant, Department of Computer Science, IUB July 2018 – Present
- Research Assistant, Kelley School of Business, IUB May 2016
- Research Assistant, Department of Computer Science, IUB Summer 2015
- Research Associate, Department of Computer Science, IUB Summer 2013
- Research Assistant, Department of Economics, NTU January 2008 – July 2009

TECHNICAL SKILLS

- Programming Languages:
  Python (with NumPy, matplotlib, and SymPy), Mathematica, Visual Basic for Application, HTML, C/C++, LaTeX, MATLAB, Isabelle, Agda, Scheme, SQL
- Platforms:
  Microsoft Windows (7, 10, 8, XP, 98, 95, 3.1), Cygwin, Red Hat Linux, MS-DOS 6.22
- Office and Project Management Softwares:
  Microsoft Outlook, Microsoft PowerPoint, Microsoft Excel, Microsoft Word,
  Adobe Acrobat, Adobe Dreamweaver CC, Adobe Captivate 9,
  LyX, ShareLaTeX, Trello, Google Docs, Google Sheets, Slack, emacs
- Version Control Systems:
  Git, Apache Subversion
- Integrated Development Environments:
  Eclipse, PyCharm, Visual Studio 2013
- Fluency of Languages:
  Chinese (Native), English (Fluent), Japanese (Beginning), French Reading (Beginning)

AWARDS AND HONORS

- Studying Abroad Scholarship, Ministry of Education, Taiwan, R.O.C. 2010 – 2012
- Presidential Award, NTU Spring 2005, Fall 2005, Spring 2006
- Distinction Award, 1st Taiwan Mathematical Contest of Modeling for Undergraduate Students September 2003

CLUB ACTIVITIES

- Account Administrator of ptt2.cc 2006 – 2009
- NTU Go Club 2002 – 2006