IOP Publishing Journal of Physics A: Mathematical and Theoretical
J. Phys. A: Math. Theor. **47** (2014) 115305 (20pp) doi:10.1088/1751-8113/47/11/115305

Discrete quantum theories

Andrew J Hanson[1], **Gerardo Ortiz**[2], **Amr Sabry**[1] **and Yu-Tsung Tai**[3]

[1] School of Informatics and Computing, Indiana University, Bloomington, IN 47405, USA
[2] Department of Physics, Indiana University, Bloomington, IN 47405, USA
[3] Department of Mathematics, Indiana University, Bloomington, IN 47405, USA

E-mail: hansona@indiana.edu

Received 7 September 2013, revised 8 September 2013
Accepted for publication 7 February 2014
Published 3 March 2014

Abstract

We explore finite-field frameworks for quantum theory and quantum computation. The simplest theory, defined over unrestricted finite fields, is unnaturally strong. A second framework employs only finite fields with no solution to $x^2 + 1 = 0$, and thus permits an elegant complex representation of the extended field by adjoining $\mathrm{i} = \sqrt{-1}$. Quantum theories over these fields recover much of the structure of conventional quantum theory except for the condition that vanishing inner products arise only from null states; unnaturally strong computational power may still occur. Finally, we are led to consider one more framework, with further restrictions on the finite fields, that recovers a local transitive order and a locally-consistent notion of inner product with a new notion of *cardinal probability*. In this framework, conventional quantum mechanics and quantum computation emerge locally (though not globally) as the size of the underlying field increases. Interestingly, the framework allows one to choose *separate* finite fields for system description and for measurement: the size of the first field quantifies the resources needed to describe the system and the size of the second quantifies the resources used by the observer. This resource-based perspective potentially provides insights into quantitative measures for actual computational power, the complexity of quantum system definition and evolution, and the independent question of the cost of the measurement process.

Keywords: finite fields, modal quantum theory, discrete quantum computation, cardinal probability, discrete Deutsch–Jozsa algorithm, discrete Grover algorithm, quantum measurement resources
PACS numbers: 03.67.−a, 03.67.Ac, 03.65.Ta, 02.10.De

1. Introduction

The means by which quantum computing[4] extends the capacity of classical computing frameworks deeply involves both the laws of physics and the mathematical principles of computation. Richard Feynman and Rolf Landauer [1, 2], among others, have strongly advocated the careful study of quantum computation to understand its mechanisms and the source of its computational features. Our purpose here is exploit the consequences of replacing complex continuous numbers by finite complex fields in the quantum computation framework[5]; in particular, we show how a number of subtle properties of quantum computing can be teased apart, step by step, as we explore the implications of *discrete quantum theories* in a systematic fashion.

We observe that the traditional mathematical framework of complex number fields in quantum mechanics is, in principle, not amenable to numerical computation with finite resources. Since theories based on finite fields are, in principle, always computable with finite resources, a universe that was in some way a computational engine (a non-trivial philosophical hypothesis) could actually have a fundamental basis in finite fields, with conventional quantum mechanics emerging as a limiting case. This is another mechanism by which the frameworks we present could conceivably be relevant to our understanding of the laws of physics. Specifically, we can quantify the resources needed for problems of a given complexity by identifying the size of the required discrete field. The cost of such resources, clearly exposed by using discrete fields, is concealed by the properties of real numbers in conventional quantum computations.

After a review of finite fields in section 2, we proceed with a sequence of finite-field approaches that lead more and more closely to the properties of conventional quantum computing. In section 3, we examine previously-introduced quantum theories defined over unrestricted finite fields and show in section 4 that this approach leads to theories with such bizarre powers that they are probably unphysical. Although a version of quantum theory defined over a two-valued field can express simple algorithms such as quantum teleportation, it is so weak that it cannot express Deutsch's algorithm. This quantum theory is, however, also so powerful that it can be used to solve an unstructured database search of size N using $O(\log(N))$ steps, which outperforms the known asymptotic bound $O(\sqrt{N})$ in conventional quantum computing.

Next, in section 5, we improve on this by showing that for finite fields of order p^2, with the prime p of the form $4\ell + 3$ (ℓ a non-negative integer), the complex numbers have extremely compelling and natural discrete analogues that permit a great many of the standard requirements of quantum computing to be preserved. Under suitable conditions, we have amplitude-based partitions of unity, unitary transformations, and entanglement [4], as well as solutions to deterministic quantum algorithms such as the algorithms of Deutsch, Simon, and Bernstein–Vazirani [5, 6], though still with some bothersome shortcomings. Because of the modular nature of arithmetic in the finite complex field, it is not possible to define an inner product in the usual sense, and we show in section 6 that this leads to excessive computational power for the unstructured database search problem for certain database sizes.

We are led, in sections 7 and 8, to develop a framework with further restrictions on p that *locally* recovers the structure and expected properties of conventional quantum theory. Section 7 locally recovers the inner product space and section 8 locally recovers a notion

[4] We use the phrase 'conventional quantum theory' where necessary to distinguish the usual quantum theory and quantum computing paradigm using (continuous) complex numbers from discrete quantum theory. Alternative terminology in the literature includes 'actual,' 'standard,' and 'ordinary' quantum theory.

[5] Our approach is complementary to other attempts to re-formulate quantum mechanics starting with alternative number systems such as the p-adic numbers, See, for example, [3].

of probability. The development in both sections exploits the fact that longer sequences of *ordered* numbers appear in the quadratic residues (numbers with square roots in the field) as the size of the field increases. Discrete quantum computations whose calculations are confined to numbers in this ordered sequence resemble conventional quantum computations. The size of the field p plays an important role in describing the resources needed for the computation as larger problem sizes require a larger field size to represent all intermediate numerical values. A significant feature of our framework is that the resources needed for the measurement process can be separated from the resources needed by the evolution of the system being modeled. This interplay between the resources used by the system under study and the resources used for the observation process is a significant concept that is nonexistent in conventional quantum computing and is exposed by our careful accounting of resources.

We note that the conventional mathematical framework based on the real numbers allows one to distinguish states whose measurement outcomes differ by infinitesimally small probabilities, e.g., 10^{-100} versus 0. In the proposed framework of discrete quantum computing, the finite size of the field implies a maximum precision for measurement: a 'small' field represents limited resources with which it becomes impossible to distinguish states whose measurement outcomes differ by an amount less than the resolution afforded by the field. It is possible, however, to discriminate between such states at the cost of moving to a larger field, i.e., by investing more resources in the measurement process. We formalize this approach to measurement using the novel notion of *cardinal probability*, with numerical labels corresponding to 'more probable, the same, or less probable,' rather than a percentage-based likelihood measure. In cardinal probability, relative outcomes are associated with intervals of ambiguity that get smaller and more precise as the size of the field increases.

Finally, in section 9, we apply our discrete quantum theory to the study of two representative algorithms, the deterministic Deutsch–Jozsa algorithm and the probabilistic Grover algorithm [5, 6]. The first algorithm highlights the role played by the size of the field p in determining the actual resources required for computation as the number of input bits n increases, a concept nonexistent in conventional quantum computing. The second algorithm highlights, in addition, the dependence of the precision of measurement (via cardinal probabilities) on the size of the field, another nonexistent concept in conventional quantum computing.

2. Fundamentals of finite fields

A field $\mathbb{F}$ is an algebraic structure consisting of a set of elements equipped with the operations of addition, subtraction, multiplication, and division [7, 8]. 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:

(i) $\mathbb{F}$ is an Abelian group under the addition operation $+$ (additive group);
(ii) The multiplication operation $*$ is associative and commutative. The field has a multiplicative identity and the property that every non-zero element has a multiplicative inverse;
(iii) Distributive laws: For all $a, b, c \in \mathbb{F}$

$$a * (b + c) = a * b + a * c \tag{1}$$

$$(b + c) * a = b * a + c * a. \tag{2}$$

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

Finite fields of q elements, $\mathbb{F}_q = \{0, \ldots, q-1\}$, 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

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 (Lagrange's theorem), which is unique up to field isomorphism. The exponent r is known as the *degree* of the field over its prime subfield [9][6]. 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 unique. Notice that a fundamental difference between finite fields and infinite fields with characteristic 0 is one of topology: finite fields induce a compact structure because of their modular arithmetic, permitting *wrapping around*, while that is not the case for fields of characteristic zero. This feature may lead to fundamental physical consequences.

3. Modal quantum theory

Recently, Schumacher and Westmoreland [10] and Chang *et al* [11] defined versions of quantum theory over *unrestricted* finite fields, which they call modal quantum theories 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 1-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 1-qubit system can be in one of only three states. The dynamics of these

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

1-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 six such maps:

$$X_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad S^\dagger = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

This set of maps is clearly quite impoverished compared to the full set of 1-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 $|0\rangle$ or $|1\rangle$ deterministically produces the same state while measuring $|+\rangle$ nondeterministically produces $|0\rangle$ or $|1\rangle$ with no assigned probability distribution. In other bases, the measurement process is complicated by the fact that the correspondence between $|\Psi\rangle$ and its *dual* $\langle\Psi|$ is basis-dependent, and that the underlying finite field is necessarily cyclic. For example, in $\mathbb{F}_2$, addition $(+)$ and multiplication $(*)$ are modulo 2: $\langle +|+\rangle = (1 * 1) + (1 * 1) = 1 + 1 = 0$. Hence, the dual of $|+\rangle$ is not $\langle +|$ if $|+\rangle$ is part of the basis.

4. 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 [12]. 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 [13] in a way that outperforms conventional quantum computing. The classical `UNIQUE-SAT` problem (also known as `USAT` or `UNAMBIGUOUS-SAT`) is the problem of deciding whether a given Boolean formula has a satisfying assignment, assuming that it has at most one such assignment [14]. This problem is, in a precise sense [15], 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 $O(\sqrt{N})$ for unstructured database search in conventional quantum computing.

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. Then we can give an algorithm (see figure 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 $|0\rangle|\overline{0}\rangle$. 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. Applying the map S (defined in the previous section) 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

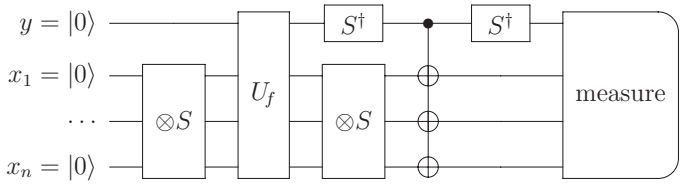

Figure 1. Circuit for black box `UNIQUE-SAT` in modal quantum theory over the field $\mathbb{F}_2$. U_f is a Deutsch quantum black box [5] with $U_f|y\rangle|\bar{x}\rangle = |y + f(\bar{x})\rangle|\bar{x}\rangle$, where $\bar{x}$ denotes a sequence $x_1, x_2, \ldots, x_n$ of n bits. For further notation see text.

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 X_0 (which is the identity) leaves the state unchanged. Applying $S^\dagger$ to the first component leaves the state unchanged. Measuring the state will deterministically produce $|0\rangle|\overline{0}\rangle$.

Case II: f is satisfiable; the measurement produces some state other than $|0\rangle|\overline{0}\rangle$. 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 $|0\rangle|\overline{+}\rangle$ 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 $|+\rangle|\overline{a}\rangle + \Sigma_{\overline{x}}|0\rangle|\overline{x}\rangle = |+\rangle|\overline{a}\rangle + |0\rangle|\overline{+}\rangle$, 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 $|+\rangle|\overline{S(a)}\rangle + |0\rangle|\overline{0}\rangle$. Applying $S^\dagger$ to the first component produces: $|1\rangle|\overline{S(a)}\rangle + |0\rangle|\overline{0}\rangle$. Applying X_b, where b is the first component of the state, to each qubit in the second component produces $|1\rangle|\overline{\mathsf{not}(S(a))}\rangle + |0\rangle|\overline{0}\rangle$. Applying $S^\dagger$ to the first component produces $|+\rangle|\overline{\mathsf{not}(S(a))}\rangle + |0\rangle|\overline{0}\rangle$. For the measurement of $|+\rangle|\overline{\mathsf{not}(S(a))}\rangle + |0\rangle|\overline{0}\rangle$ to be guaranteed to never be $|0\rangle|\overline{0}\rangle$, we need to verify that $|+\rangle|\overline{\mathsf{not}(S(a))}\rangle$ has one occurrence $|0\rangle|\overline{0}\rangle$. 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 $|0\ldots\rangle$.

5. Discrete quantum theory (I)

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 [16] is based on complexifiable finite fields. To incorporate complex numbers for quantum amplitudes, we exploit the fact that the polynomial $x^2 + 1 = 0$ is *irreducible* (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. In other words, $x^2 + 1 = 0$ is irreducible over $\mathbb{F}_3, \mathbb{F}_7, \mathbb{F}_{11}, \mathbb{F}_{19}, \ldots$. We achieve our goal by observing that any field in this family is extensible to a field $\mathbb{F}_{p^2}$ whose elements can be viewed as discrete complex numbers with the real and imaginary parts in $\mathbb{F}_p$. In the field $\mathbb{F}_{p^2}$, the Frobenius automorphism of an element α (defined as α^p) represents the usual definition of complex conjugation[7].

[7] The simplest example is the field $\mathbb{F}_{3^2}$ with nine elements,

$$0, 1, -1, \mathrm{i}, 1 + \mathrm{i}, -1 + \mathrm{i}, -\mathrm{i}, 1 - \mathrm{i}, -1 - \mathrm{i}.$$

(These are all the complex numbers one can form using the integers modulo 3 as real and imaginary coefficients.) Similarly, the field $\mathbb{F}_{7^2}$ has 49 elements of the form $\alpha = a + i\,b$ where a, b are integers in the range $[-3, 3]$ and addition and multiplication are modulo 7.

The next task is to examine the consequences when we attempt to construct d-dimensional vector spaces over the complexified fields $\mathbb{F}_{p^2}$ [4]. (For readability, instead of writing column vectors, we will often use the vector notation $|\Psi\rangle = (\alpha_0\alpha_1 \ldots \alpha_{d-1})^T$ and $|\Phi\rangle = (\beta_0\beta_1 \ldots \beta_{d-1})^T$, where $(.)^T$ is the transpose of the *row* vector $(.)$.) It can be shown [17] that, given two vectors

$$|\Psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle \ , \ |\Phi\rangle = \sum_{i=0}^{d-1} \beta_i |i\rangle, \tag{3}$$

with scalars α_i and β_i drawn from the field elements, and orthonormal basis $\{|i\rangle\}$, the Hermitian dot product is always reducible to the form

$$\langle\Phi|\Psi\rangle = \sum_{i=0}^{d-1} \beta_i^p \alpha_i. \tag{4}$$

This product satisfies conditions A and B below, but not C, because in a finite field, addition can 'wrap around,' making the concepts of positive and negative meaningless and allowing the sum of non-zero elements to be zero:

(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.

With just conditions A and B, it is possible to recover unitary operators, and thus recover much of the relevant structure of Hilbert spaces over the field of complex numbers. The failure of condition C, however, plays havoc with the traditional notions of ordered probabilities as well as the geometric notions of ordered distances and angles, whose lengths and cosines, respectively, are normally expressed using the inner product [18]. In a separate development, we explore the geometry of these finite fields and define a discrete version of the Hopf fibration extending the Bloch sphere to n-qubits, as well as determining discrete measures for the relative sizes of the entangled, maximally entangled, and unentangled discrete states [4].

6. Discrete quantum computing (I)

Given a complexified finite field $\mathbb{F}_{p^2}$ and its Hermitian dot product (equation (4)) 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 [5] algorithm, 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 and Bernstein–Vazirani, perform as desired [19]. Algorithms such as Grover's search will not work in the usual way because we lack (the notion of) ordered angles and probability in general.

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 figure 2, which is a variant of the one in figure 1. Unlike the modal quantum theory 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'

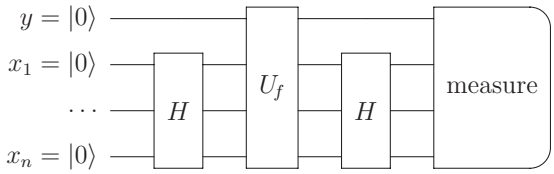

Figure 2. Circuit for black box `UNIQUE-SAT` in discrete quantum computing.

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.

7. Discrete quantum theory (II): inner product space

We next discuss an approach using finite complexifiable fields that conditionally resolves the inner product condition (C), which is violated by the theory just presented. A possible path is suggested by the work of Reisler and Smith [20]. 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 [20] suggested by recent number theory resources [21].

Let us first note that the range of the quadratic map, $\{x^2 \text{ modulo } p | x \in \mathbb{F}_p\}$, 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.

As a concrete example, consider a finite field in which the sequential elements $0, 1, 2, 3, \ldots, k-1$ 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., $S_x(k) = x-(k-1)/2, \ldots, x-2, x-1, x, x+1, x+2, \ldots, x+(k-1)/2$, 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 [21][8]. The nth element of that sequence (which must be prime) is the least number such that

[8] For computational purposes, this sequence is preferable to the one proposed by Reisler and Smith [20] 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 $8\Pi_{i=1}^{m} q_i - 1$, 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, 2 042 039, ...

Table 1. Number k of transitively ordered elements for a given field $\mathbb{F}_p$.

p	3	7	23	71	311	479	1559	5711	10 559	18 191	...
k	**2**	**3**	**5**	**7**	**11**	**13**	**17**	**19**	**23**	**29**	...
$\pi(k)$	1	2	3	4	5	6	7	8	9	10	...

Table 2. Allowed probability amplitudes for different vector space dimensions d and $k = 11$.

	Allowed probability amplitudes $F^d(k)$
$d = 1$	$F^1(11) = \{0, \pm1, \pm2, \pm\mathrm{i}, \pm2\mathrm{i}, (\pm1 \pm \mathrm{i}), (\pm1 \pm 2\mathrm{i}), (\pm2 \pm \mathrm{i})\}$
$d = 2$	$F^2(11) = \{0, \pm1, \pm\mathrm{i}, (\pm1 \pm \mathrm{i})\}$
$d = 3$	$F^3(11) = \{0, \pm1, \pm\mathrm{i}\}$
$d = 4$	$F^4(11) = \{0, \pm1, \pm\mathrm{i}\}$
$d = 5$	$F^5(11) = \{0, \pm1, \pm\mathrm{i}\}$
$d \geqslant 6$	$F^d(11) = \{0\}$

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 1. 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 $\mathbb{F}_3$ 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 $|\Psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle = (\alpha_0 \alpha_1 \ldots \alpha_{d-1})^T$, for which $d < p - \frac{k-1}{2}$ and each α_i satisfies

$$d\,|\alpha_i|^2 = d\left(a_i^2 + b_i^2\right) \leqslant \frac{k-1}{2}\,, \tag{5}$$

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

We can now verify, by using table 2, that for any vector $|\Psi\rangle$ in the selected region the value of $\langle\Psi|\Psi\rangle$ is $\geqslant 0$ 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 [22].

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.

8. Discrete quantum theory (II): cardinal probability

The final issue that must be addressed in the discrete theory put forward in section 7 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, absolute squares having values in the positive integers, and squared projections on the bases in the non-negative integers, all in the ordered range of equation (5), 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.

8.1. Theory

In conventional quantum theory, given an observable $\mathcal{O}$ with eigenvalues λ_i, $i = 0, \ldots, d-1$, and orthonormal eigenvectors $|i\rangle$ (i.e., $\mathcal{O}|i\rangle = \lambda_i|i\rangle$), the probability of measuring the (non-degenerate) eigenvalue λ_i in a system characterized by the state $|\Psi\rangle$ is given by:

$$P_\Psi(\lambda_i) \equiv P_\Psi(i) = \frac{|\langle i|\Psi\rangle|^2}{\langle\Psi|\Psi\rangle} = \frac{|\alpha_i|^2}{\langle\Psi|\Psi\rangle}\,, \tag{6}$$

where $|\Psi\rangle = (\alpha_0\alpha_1 \ldots \alpha_{d-1})^T$ in the eigenbasis of $\mathcal{O}$, that is the measurement basis. Hereafter, we will simplify by calling $P_\Psi(i)$ the probability of measuring λ_i.

The fundamental property of conventional quantum theory is that a complete set of states such as $\{|i\rangle\}$ induces a partition of unity in the (real-valued) probabilities, so that

$$\sum_{i=0}^{d-1} P_\Psi(i) = 1\,, \tag{7}$$

and, more importantly for our treatment, for any given system, there is a *precise ordering* of the set $\{P_\Psi(i)\}$. In general, this ordering can be expressed as a sequence of equalities and inequalities of the following form,

$$P_\Psi(a) \preceq P_\Psi(b) \preceq \cdots \preceq P_\Psi(y) \preceq P_\Psi(z)\,, \tag{8}$$

where we adopt the symbol '$\preceq$' to denote *either* equal ($=$) *or* less-than ($<$), but *never* less-than-or-equal ($\leqslant$). We observe that *in practical measurements*, these formal properties are

meaningless, since, statistically, a poor measurement could reverse the apparent order of the strictly increasing theoretical inequalities; more significantly, distinguishing *formally equal* probabilities from a (>) or (<) ordering is impossible with an observer that has only finite resources.

We now show that, while formal achievement of the conventional quantum probability ordering of equation (8) is not possible in a world with finite resources modeled by our discrete quantum theory, we can define a context for the definition of probabilities, *cardinal probability*, that is consistent with the just-noted properties of probability measurement in conventional quantum theory. That is, in a theory with cardinal probability, *inequalities* in the conventional probability relations equation (8) can be preserved with appropriate resources (in the form of a sufficiently large choice of the field), while *equalities* cannot be guaranteed in the theory, and in fact can be represented as *inequalities of any order*. The *set* of discrete theories obeying these properties is defined as a single equivalence class of cardinal probability theories.

In order to study the explicit properties of a discrete theory, we examine states of the form

$$|\Psi_m\rangle = \left(\alpha_0^m \alpha_1^m \dots \alpha_{d-1}^m\right)^T,$$

where the coefficients must be discrete complex numbers α_i^m in the field representing the resources needed by the computation, and the label m is the 'starting value' of the discrete norm-squared,

$$m = \langle\Psi_m|\Psi_m\rangle = \sum_{i=0}^{d-1} \left|\alpha_i^m\right|^2.$$

(We drop the superscript m on the coefficients when there is no ambiguity.)

One might hope to construct a probability object corresponding exactly to the conventional quantum theory by finding a common factor that eliminated the diverse denominators $\sqrt{m}$ that would be used to normalize all the states to unity in the conventional theory. This would require rescaling

$$\frac{\langle\Psi_{m_1}|\Psi_{m_1}\rangle}{m_1} = \frac{\langle\Psi_{m_2}|\Psi_{m_2}\rangle}{m_2} = 1\,,$$

for any two vectors $|\Psi_{m_1}\rangle$ and $|\Psi_{m_2}\rangle$, to the form

$$\langle\Psi_{m_1}|\Psi_{m_1}\rangle \prod_{i\neq 1} m_i = \langle\Psi_{m_2}|\Psi_{m_2}\rangle \prod_{i\neq 2} m_i = \prod_i m_i \equiv \mu. \tag{9}$$

Can we succeed in imposing such a restriction? To determine the answer, let us define an *integer-valued* normalization for each of a set of states we wish to compare: let

$$|\Psi_m\rangle \to \left|\overline{\Psi}_m\right\rangle = \nu_m|\Psi_m\rangle = (x_m + \mathrm{i}\, y_m)|\Psi_m\rangle,$$

where, from equation (9), we would *like* to have

$$\langle\overline{\Psi}_m|\overline{\Psi}_m\rangle = \prod_i m_i = \mu\,,$$

or

$$|\overline{\Psi}_m\rangle = \left(\prod_{m_i\neq m} \sqrt{m_i}\right)|\Psi_m\rangle$$

for *any* value of m.

(Remark: We will take $y_m = 0$ in general; replacing a square by a sum of squares in the norm-squared value of $|\overline{\Psi}_m\rangle$ adds a few more cases with exact solutions, but fails to make a difference in the general case.)

Then we need to show that

$$\langle\overline{\Psi}_m|\overline{\Psi}_m\rangle = m\,(x_m)^2 = \mu \tag{10}$$

either does or does not have a solution for all m in any chosen set $\{|\overline{\Psi}_m\rangle\}$. The resulting condition is obviously

$$m_1\,(x_1)^2 = m_2\,(x_2)^2 = m_3\,(x_3)^2 = \cdots. \tag{11}$$

Since every m is a sum of at least four squares, even for a single qubit state, by Lagrange's four-square theorem there is some complexified integer field that can produce any arbitrary integer as the value of m. Assume $m_1 = 2$ and $m_2 = 3$. Then $x_2/x_1 = \sqrt{2/3}$; but there are no integer values of (x_1, x_2) that can satisfy that equation, so it is impossible in the integer domain to satisfy equation (11) in general.

This no-go theorem leads us inevitably to consider a *set* of values of $\mu_m = m\,(x_m)^2$ that defines *approximate* norm-squared values that are close enough so that the values of the *scaled* probabilities based on the set $\{|\overline{\Psi}_m\rangle\}$ obey the *cardinal order* of equation (8) with the following variant of equation (6):

$$\bar{P}_{\overline{\Psi}_m}(i) = (x_m)^2|\alpha_i|^2.$$

We notice that m itself does not appear, and that, since each $\alpha_i \to x_m\alpha_i$, the original expression is now re-weighted by $(x_m)^2$. The important point is now that as long as the inequalities of equation (8) are preserved, and the violation of exact equalities does not violate the inequalities, we have a valid instance of a cardinal probability theory.

Since the ordering requirements typically refer to *sets* of comparisons, possibly with different states, we introduce the notation

$$\bar{P}(i) = \{\bar{P}_{\overline{\Psi}_m}(i)\}/\!/\{\mu_m\} \tag{12}$$

that expands to

$$\{(x_{m_1})^2|\alpha_i^{m_1}|^2, (x_{m_2})^2|\alpha_i^{m_2}|^2, \ldots\}/\!/\{\mu_{m_1}, \mu_{m_2}, \ldots\}.$$

This expression represents a *realization* of the set of cardinal probabilities $\bar{P}_{\overline{\Psi}_m}(i)$ with respect to the approximate normalizations $\mu_m = \langle\overline{\Psi}_m|\overline{\Psi}_m\rangle = m\,(x_m)^2$.

The set $\{\mu_m\}$ represents the scale with respect to which we are going to compare cardinal probabilities of states $\{|\overline{\Psi}_m\rangle\}$ during the measurement process. The number of resources required by the observer corresponds precisely to the characteristic of the field used to define the scale via the set $\{\mu_m\}$. One can intuitively picture the elements of $\{\mu_m\}$ as a set of *rulers* that are 'equal' to within a certain precision; to get more precision, one needs to buy a more expensive set of rulers. Alternatively, one can visualize the precision of the rulers to be controlled by a set of interactive dials or sliders, with the precision (as well as the cost of the resources) increasing progressively as the values are increased.

8.2. Scale determination

We begin with some simple examples of scale determination. Let $p = 311$, $k = 11$, and $d = 2$. The permitted range of coefficients is $S_0(11) = \{-5, \ldots, -1, 0, 1, \ldots, 5\}$; given the dimension $d = 2$, the allowed probability amplitude coefficients are $F^2(11) = \{0, \pm1, \pm\mathrm{i}, (\pm1 \pm \mathrm{i})\}$ (see table 2 above). Consider a single state $|\Psi_3\rangle = 1|0\rangle + (1+\mathrm{i})|1\rangle$. In this case there is no need to scale the state, i.e., we can take $x_m = 1$ and calculate $|1|^2 = 1$, $|(1+\mathrm{i})|^2 = 2$ and the norm-squared $\langle\Psi_3|\Psi_3\rangle = 3$ (which is in the allowed range). The probability of measuring λ_0 is $1/\!/3$ and that of measuring λ_1 is $2/\!/3$. These results *can* be used to infer that the probability of measuring λ_1 is greater than the probability of measuring λ_0 but they *cannot* be used to conclude that the former event is exactly twice as likely as the second.

Table 3. Norms-squared and probabilities for 1-qubit states $|\Psi_m\rangle$ in $F^2(11)$.

$\text{Norm}^2 = m$	$\langle\Psi_1\|\Psi_1\rangle = 1$	$\langle\Psi_2\|\Psi_2\rangle = 2$	$\langle\Psi_3\|\Psi_3\rangle = 3$	$\langle\Psi_4\|\Psi_4\rangle = 4$
Prob. of λ_0	$\|\langle 0\|\Psi_1\rangle\|^2 = 1/\!/1$	$\|\langle 0\|\Psi_2\rangle\|^2 = 1/\!/2$	$\|\langle 0\|\Psi_3\rangle\|^2 = 1/\!/3$	$\|\langle 0\|\Psi_4\rangle\|^2 = 2/\!/4$
Prob. of λ_1	$\|\langle 1\|\Psi_1\rangle\|^2 = 0/\!/1$	$\|\langle 1\|\Psi_2\rangle\|^2 = 1/\!/2$	$\|\langle 1\|\Psi_3\rangle\|^2 = 2/\!/3$	$\|\langle 1\|\Psi_4\rangle\|^2 = 2/\!/4$

Table 4. A failing choice (left) and a successful choice (right) for the rescaling of the system $\{|\Psi_1\rangle,\ |\Psi_2\rangle,\ |\Psi_3\rangle,\ |\Psi_4\rangle\}$ to realize a cardinal probability system consistent with conventional quantum mechanical probabilities.

	Failing choice				Successful choice			
Actual $\{P_{\Psi_m}(0), P_{\Psi_m}(1)\}$	m	x	$\mu = mx^2$	$\{\bar{P}_{\bar{\Psi}_m}(0), \bar{P}_{\bar{\Psi}_m}(1)\}$	m	x	$\mu = mx^2$	$\{\bar{P}_{\bar{\Psi}_m}(0), \bar{P}_{\bar{\Psi}_m}(1)\}$
$\{1, 0\}$	1	4	16	$\{16, 0\}$	1	16	256	$\{256, 0\}$
$\{1/2, 1/2\}$	2	3	18	$\{9, 9\}$	2	12	288	$\{144, 144\}$
$\{1/3, 2/3\}$	3	2	12	$\{4, 8\}$	3	9	243	$\{81, 162\}$
$\{1/2, 1/2\}$	4	2	16	$\{8, 8\}$	4	8	256	$\{128, 128\}$

Now let us consider a more interesting example that involves several representative 1-qubit states,

$$
\begin{aligned}
|\Psi_1\rangle &= 1|0\rangle \\
|\Psi_2\rangle &= 1|0\rangle + 1|1\rangle \\
|\Psi_3\rangle &= 1|0\rangle + (1+\mathrm{i})|1\rangle \\
|\Psi_4\rangle &= (1-\mathrm{i})|0\rangle + (1+\mathrm{i})|1\rangle,
\end{aligned}
$$

as explicit examples of each m. (There are of course many equivalent vectors representing the same physical state, a miniature local version of the traditional Bloch sphere mapping [4].) Table 3 presents the bare analogues of norms-squared and probabilities for the $|\Psi_m\rangle$ representing the properties of the four unique norms, $m = 1,\ 2,\ 3,$ and 4. (In larger fields, these numbers do not necessarily form a sequence.)

We will introduce a deterministic construction to identify approximate choices for $\{\mu_1, \mu_2, \mu_3, \mu_4\}$ in a moment. But first let us give a clear heuristic example of the nature of the problem and the process by which we can converge towards solutions. In table 4, we show two guesses for the values of $\{x_1, x_2, x_3, x_4\}$. The first is extremely simple, but the numbers do not quite have enough power to avoid a conflict with the required order corresponding to the real-valued probabilities $P_{\Psi_m}(0) = (1, 1/2, 1/3, 1/2)$ and $P_{\Psi_m}(1) = (0, 1/2, 2/3, 1/2)$. The second choice, still constructed from integers that are quite small, achieves the required ordering and is our first example of an instance of a cardinal probability system for $\{|\Psi_1\rangle,\ |\Psi_2\rangle,\ |\Psi_3\rangle,\ |\Psi_4\rangle\}$.

To extend this heuristic framework toward a deterministic computation, we now propose specific criteria to select the set of normalizations $\{\mu_1, \mu_2, \mu_3, \mu_4\}$ with respect to which we can compare cardinal probabilities. The method relies on introducing the notion of *square root* of a number drawn from a finite field. In conventional quantum computing, it is possible to re-weight the four states above so that all have a norm-squared of 24 as follows:

$$
\begin{aligned}
|\Psi_1\rangle &= 2\sqrt{6}\ (1|0\rangle) \\
|\Psi_2\rangle &= 2\sqrt{3}\ (1|0\rangle + 1|1\rangle) \\
|\Psi_3\rangle &= 2\sqrt{2}\ (1|0\rangle + (1+\mathrm{i})|1\rangle) \\
|\Psi_4\rangle &= \sqrt{6}\ ((1-\mathrm{i})|0\rangle + (1+\mathrm{i})|1\rangle).
\end{aligned}
$$

However, it is impossible to achieve this re-weighting precisely in a discrete theory because the square roots cannot be calculated exactly in finite fields. We can, however, produce successively

more accurate approximations of square roots with bigger and bigger fields using a prescription suggested by Reisler and Smith [20].

We denote the approximate square root of $m > 0$ in a finite field $\mathbb{F}_p$ by $\sqrt[\prime]{m}$. This approximate square root is calculated by taking the usual square root of the smallest element in the ordered range $S_0(k)$ that is greater than m and that is a quadratic residue. For example, in a field with more than 8 positive ordered elements, $S_0(k \geqslant 19)$, we have:

$$\begin{aligned}\sqrt[\prime]{2} &= \sqrt{4} = 2\\ \sqrt[\prime]{3} &= \sqrt{4} = 2\\ \sqrt[\prime]{6} &= \sqrt{9} = 3.\end{aligned}$$

Even though these approximations are crude, they can be used to re-weight the vectors above to get probabilities $\bar{P}_{\overline{\Psi}_m}(i)$ whose relationships approximate the ideal mathematical (but uncomputable using finite resources) probabilities. In more detail, the re-weighted vectors become:

$$\begin{aligned}\left|\overline{\Psi}_1\right\rangle &= 6(1|0\rangle)\\ \left|\overline{\Psi}_2\right\rangle &= 4(1|0\rangle + 1|1\rangle)\\ \left|\overline{\Psi}_3\right\rangle &= 4(1|0\rangle + (1+\mathrm{i})|1\rangle)\\ \left|\overline{\Psi}_4\right\rangle &= 3((1-\mathrm{i})|0\rangle + (1+\mathrm{i})|1\rangle),\end{aligned}$$

with $\{\mu_m\} = \{36,\ 32,\ 48,\ 36\}$, and the probabilities become:

$$\begin{aligned}\bar{P}_{\overline{\Psi}_1}(0) &= 36 \qquad & \bar{P}_{\overline{\Psi}_1}(1) &= 0\\ \bar{P}_{\overline{\Psi}_2}(0) &= 16 \qquad & \bar{P}_{\overline{\Psi}_2}(1) &= 16\\ \bar{P}_{\overline{\Psi}_3}(0) &= 16 \qquad & \bar{P}_{\overline{\Psi}_3}(1) &= 32\\ \bar{P}_{\overline{\Psi}_4}(0) &= 18 \qquad & \bar{P}_{\overline{\Psi}_4}(1) &= 18,\end{aligned}$$

which we express as

$$\begin{aligned}\bar{P}(0) &= \{36, 16, 16, 18\}/\!/\{36, 32, 48, 36\}\\ \bar{P}(1) &= \{0, 16, 32, 18\}/\!/\{36, 32, 48, 36\}.\end{aligned}$$

In comparison with the exact probabilities, we see that $\bar{P}_{\overline{\Psi}_3}(0)$ and $\bar{P}_{\overline{\Psi}_2}(0)$ collapse to a single value and $\bar{P}_{\overline{\Psi}_4}(0)$ is approximated in a way that makes it larger than $\bar{P}_{\overline{\Psi}_2}(1)$. If we only concern ourselves with how the actual probabilities are related by the $\preceq$ relation, then our approximation is adequate.

If we desire an even more accurate approximation, we can proceed as follows: we choose a larger field for measurement in which the ordered ranged is scaled by 100 so that the square roots get one additional digit of precision. Specifically, in a field with more than 625 positive ordered elements, we have

$$\begin{aligned}\sqrt[\prime]{200} &= \sqrt{225} = 15\\ \sqrt[\prime]{300} &= \sqrt{324} = 18\\ \sqrt[\prime]{600} &= \sqrt{625} = 25\ ,\end{aligned}$$

giving a better approximation of the square roots (scaled by 10). Using these approximations, the four vectors become:

$$\begin{aligned}\left|\overline{\Psi}_1\right\rangle &= 50(1|0\rangle)\\ \left|\overline{\Psi}_2\right\rangle &= 36(1|0\rangle + 1|1\rangle)\\ \left|\overline{\Psi}_3\right\rangle &= 30(1|0\rangle + (1+\mathrm{i})|1\rangle)\\ \left|\overline{\Psi}_4\right\rangle &= 25((1-\mathrm{i})|0\rangle + (1+\mathrm{i})|1\rangle)\end{aligned}$$

with $\{\mu_m\} = \{2500,\ 2592,\ 2700,\ 2500\}$, and the probabilities become:

$$\begin{aligned}
\bar{P}_{\overline{\Psi}_1}(0) &= 2500 \qquad & \bar{P}_{\overline{\Psi}_1}(1) &= 0 \\
\bar{P}_{\overline{\Psi}_2}(0) &= 1296 \qquad & \bar{P}_{\overline{\Psi}_2}(1) &= 1296 \\
\bar{P}_{\overline{\Psi}_3}(0) &= 900 \qquad & \bar{P}_{\overline{\Psi}_3}(1) &= 1800 \\
\bar{P}_{\overline{\Psi}_4}(0) &= 1250 \qquad & \bar{P}_{\overline{\Psi}_4}(1) &= 1250.
\end{aligned}$$

In comparison with the exact probabilities, we see that the increase in precision has reestablished the distinction between $\bar{P}_{\overline{\Psi}_3}(0)$ and $\bar{P}_{\overline{\Psi}_2}(0)$. The two probabilities $\bar{P}_{\overline{\Psi}_4}(0)$ and $\bar{P}_{\overline{\Psi}_2}(1)$ are now relatively closer but they are still, however, not equal. A moment's reflection shows that these two values can *never* be equal as $(\sqrt{2})^2$ can never be precisely 2 no matter how many digits of the actual $\sqrt{2}$ we maintain.

9. 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 [5, 6], 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 [5, 6, 23], 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.

9.1. 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 [5, 6]. 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, as in section 4. A straightforward calculation [5] shows that the final state is[9]

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

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 $-2^n, \ldots, 2^n$ and therefore, by equation (5), we get the following constraint on the size of the ordered region in the finite field:

$$2^{n+1}\,(2^n)^2 \leqslant \frac{k-1}{2} \quad \Leftrightarrow \quad k \geqslant 2^{3n+2} + 1.$$

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 $k \geqslant 2^{3n+2}+1$, and let p be the $\pi(k)$th element of the sequence A000229 [21]. 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 $0, 1, 2, 3, \ldots, 2^{3n+2}$ are all quadratic residues. Hence the numbers $-2^n, \ldots, 2^n$ are all inside the ordered range $S_0(k)$. On the other hand, if we choose any prime smaller than

[9] Note that the algorithm in [5] makes use of the Hadamard matrix. We have eliminated the factor $1/\sqrt{2}$ to ensure that all quantities are expressed in terms of integers. Also notice that the positioning of the initial qubit state $|1\rangle$ is reversed from [5].

Table 5. Extension of transitively ordered elements.

p	...	422 231	...	196 265 095 009	...		...		...
k	...	**37**	...	**131**	...	**257**	...	**32 771**	...
$\pi(k)$	...	12	...	32	...	55	...	3513	...

p, there is a quadratic non-residue smaller than k, and we also know that the least quadratic non-residue is a prime [8]. 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 $S_0(k)$.

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

$$k \geqslant 2^{3\times 1+2} + 1 = 2^5 + 1 = 33.$$

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

$$\pi\ (37) = 12$$
$$p = 422\,231,$$

where the prime counting function $\pi(k)$ is taken from the extended elements in table 5.

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

$$k \geqslant 2^{3\times 2+2} + 1 = 2^8 + 1 = 257.$$

Because 257 is a prime, we can pick

$$k = 257$$
$$\pi\ (257)\ = 55.$$

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.

9.2. 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 [23]:

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

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

where we have eliminated, in matrix D, 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 DR is repeated j times, where

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

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 $\bar{t}$ be the target, i.e., $f(\bar{x}) = 1$ if and only if $\bar{x} = \bar{t}$. Because the probability amplitudes of $|\bar{x}\rangle$ are all the same for $\bar{x} \neq \bar{t}$, we can let a_l be the probability amplitude of $|\bar{t}\rangle$, 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 DR, 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 that $|a_j| > |b_j|$, so we can estimate an upper bound for the maximum cardinal probability as

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

By applying equation (5) with $d = N = 2^n$, we can estimate k using

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

If we pick a prime k satisfying the above condition, then choosing the $\pi(k)$th prime in the sequence represented by table 1 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

$$\max |a_j|^2 \leqslant 2\left(\frac{4}{2}\right)^{2+1} = 16\,,$$

so we need

$$k \geqslant 8\left(\frac{4}{2}\right)^{2\times 1+2} + 1 = 8 \times 2^4 + 1 = 129.$$

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

$$\pi\,(131) = 32$$
$$p = 196\,265\,095\,009.$$

When $p = 196\,265\,095\,009$, we assume that $f(\bar{x}) = 1$ if and only if $|\bar{x}\rangle = |0\rangle|0\rangle$, and so the final state is $(4, 0, \ldots, 0)^T$ with norm-squared of 16. Then, the cardinal probability of obtaining $|0\rangle|0\rangle$ as the post-measurement state is $16/\!/16$, and it is $0/\!/16$ for the rest of the states.

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

$$k \geqslant 8\left(\frac{8}{2}\right)^{6} + 1 = 32\,769.$$

The nearest prime greater than this number is 32 771, so we can pick

$$k = 32\,771$$
$$\pi\,(32\,771) = 3513\,,$$

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 $f(\bar{x}) = 1$ if and only if $|\bar{x}\rangle = |0\rangle|0\rangle|0\rangle$. The initial information-less eight-dimensional state vector evolves under the application of DR as follows:

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

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

$$256/\!/2048 \quad 1600/\!/2048 \quad 1936/\!/2048\,,$$

while the cardinal probabilities of measuring the other states become

$$256/\!/2048 \quad 64/\!/2048 \quad 16/\!/2048.$$

We may thus conclude that the cardinal probability of measuring the satisfying assignment of f increases as we apply the diffusion D 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 1 and 5.

10. Conclusions

Since conventional quantum theory is defined over uncomputable complex numbers, it is natural to explore alternative versions of quantum theory based on finite fields. Examining the computational and physical consequences of such computable frameworks can yield new insights into the power and capacity of quantum computing. We have described a path through several variants of discrete quantum theories, starting with unrestricted discrete fields (modal theories), then advancing to a more reasonable framework based on complexifiable discrete fields (discrete quantum theory I), which supports unnaturally efficient deterministic quantum algorithms. We conclude with a still more plausible discrete theory (discrete quantum theory II), from which conventional quantum computing and conventional quantum theory emerge in a local sense. Note that as the number of restrictions on the discrete fields increases, the frequency of possibly unreasonable efficiency decreases. As long as we do not perform measurements or the quantum algorithm is of a deterministic nature, as in Deutsch's problem, we do not need to invoke any statistical postulates. This situation is an exception, since conventional quantum mechanics requires probabilistic components describing information extracted by measurement from the systems being studied. This measurement process is problematic in any discrete quantum theory. To resolve the measurement problem in our nondeterministic situations, we have introduced the notion of cardinal probability. With this approach, we see that the issues surrounding transitively-ordered probability, intrinsically troublesome in quantum theory for discrete fields, show signs of being resolvable locally. Interestingly, our framework allows us to define distinct finite fields for system description and for measurement. These finite fields distinguish the resources needed to describe the system from the resources used by the observer. Additional work is in progress on the interaction between the geometrical properties of finite fields and discrete quantum computing, and we hope to be able to make more definitive statements about probability measures based on the properties of discrete geometry. Our investigation leaves open the question of whether conventional quantum mechanics is physical, or whether perhaps extremely large discrete quantum theories that contain only computable numbers are at the heart of our physical universe.

References

[1] Feynman R P 1982 *Int. J. Theor. Phys.* **21** 467
[2] Landauer R 1996 *Phys. Lett.* A **217** 188
[3] Vladimirov V S and Volovich I V 1989 *Commun. Math. Phys.* **123** 659
Brekke L and Freund P G O 1993 *Phys. Rep.* **233** 1
[4] Hanson A J, Ortiz G, Sabry A and Tai Y-T 2013 *J. Phys. A: Math. Theor.* **46** 185301
[5] Nielsen M A and Chuang I L 2010 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[6] Mermin N D 2007 *Quantum Computer Science* (Cambridge: Cambridge University Press)
[7] Mullen G L and Mummert C 2007 *Finite Fields and Applications* (Providence, RI: American Mathematical Society)
[8] Hardy G H and Wright E M 2006 *An Introduction to the Theory of Numbers* (Oxford: Oxford University Press)
[9] Stewart I 2004 *Galois Theory* (Boca Raton, FL: Chapman and Hall)
[10] Schumacher B and Westmoreland M D 2012 *Found. Phys.* **42** 918
[11] Chang L N, Lewis Z, Minic D and Takeuchi T 2013 *Mod. Phys. Lett.* B **27** 1350064
[12] James R P, Ortiz G and Sabry A 2011 arXiv:1101.3764
[13] Willcock J and Sabry A 2011 arXiv:1102.3587v1
[14] Papadimitriou C H 1994 *Computational Complexity* (Reading, MA: Addison Wesley)
[15] Valiant L G and Vazirani V V 1986 *Theor. Comput. Sci.* **47** 85
[16] Hanson A, Ortiz G, Sabry A and Willcock J 2011 arXiv:1104.1630
[17] Grove L C 2002 *Classical Groups and Geometric Algebra* (Providence, RI: American Mathematical Society) (see, in particular, chapter 10)
[18] It is possible to recover many features of geometry in finite fields. See Wildberger N J 2005 *Divine Proportions: Rational Trigonometry to Universal Geometry* (Sydney: Wild Egg)
[19] Hanson A J, Ortiz G, Sabry A and Tai Y-T 2013 unpublished
[20] Reisler D L and Smith N M 1969 Geometry over a finite field *DTIC Technical Report AD0714115* (McLean, VA: Research Analysis Corp.) available from DTIC.mil, Accession Number: AD0714115
[21] Sloane N J A and Plouffe Simon 1995 *The Encyclopedia of Integer Sequences* (San Diego, CA: Academic) (http://oeis.org/A000229)
[22] Schwinger J 2001 *Quantum Mechanics* (Berlin: Springer) (see, in particular, chapter 1, section 1.16)
[23] Grover L K 2001 *Am. J. Phys.* **69** 769