Discrete Quantum Theories

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

(1) School of Informatics and Computing
(2) Department of Physics
(3) Mathematics Department

Indiana University

July 2nd, 2013

Quantum Computing

- Opportunity to re-examine the foundations of quantum mechanics;
- Can provide executable interpretations of quantum mechanics;
- Physics is computational;
- Computation is physical;
- We are striving for a precise mathematical model that quantifies the actual cost (i.e., resources) needed to perform a physical quantum computation;
- Our framework is that of finite-resource quantum computing and finite-resource quantum measurement.

Conventional Quantum Theory

The underlying mathematical structure is a Hilbert space. Let's decompose this structure into its basic ingredients: (This is slightly simplified.)

- Start with the field $\mathbb{R}$ of real numbers;
- Extend it to the field $\mathbb{C}$ of complex numbers;
- Define a vector space over $\mathbb{C}$;
- Define an inner product over the above vector space.

Add postulates defining states, composition, evolution, and measurement. (More about this later.)

Quantum Theories

Conventional wisdom is that each of the ingredients of the Hilbert space is necessary for the formulation of quantum mechanics. But the literature contains several variants of conventional quantum theory:

- Instead of $\mathbb{R}$, one could use the *p*-adic numbers;
- Instead of $\mathbb{C}$, one could use the quaternions $\mathbb{H}$;
- Instead of a vector space, one could use a projective space;
- Instead of infinite fields, one could use finite fields.

Explore the finite field approach in depth

Relevance for Computer Science

- Computer science's starting point is that $\mathbb{R}$ is uncomputable;
- Real numbers are explicitly rejected as an appropriate foundation for computation. The intuitive reason is that one must account for resources;
- Turing's original paper is titled "On computable numbers . . . ";
- Early papers on "Quantum Complexity Theory" (e.g., Bernstein and Vazirani 1997) spend considerable time proving that quantum computing can be done with finite approximations of the real numbers.

Relevance for Physics

- In the words of Rolf Landauer (our emphasis):

  > *. . . the real world is unlikely to supply us with unlimited memory or unlimited Turing machine tapes. Therefore, continuum mathematics is not executable, and physical laws which invoke that can not really be satisfactory . . .*

- Is the universe a computational engine ? Crucially, is it a computational engine with finite resources ?
- The conservation laws (e.g., of energy, mass, information, etc.) suggest the conservation of computational resources;
- Is it possible that extremely large discrete quantum theories that contain only computable numbers are at the heart of our physical universe?

Technical Outline

- Vector spaces over unrestricted finite fields.
  Schumacher and Westmoreland's modal quantum theory or Chang et al. Galois field quantum mechanics.

- Vector spaces over *i*-extended finite fields ($\mathbb{F}_p$ with $p \equiv 3 \pmod 4$).
  Discrete theories with no inner product that are suitable for simple deterministic problems, e.g, Deutsch algorithm.

- Vector spaces over locally orderable fields: $\mathbb{F}_p$ with p is an element of the sequence:

$$3, 7, 23, 71, 311, 479, 1559, 5711, 10559, 18191, \ldots$$

  Discrete theories with a subspace on which there is an inner product; conventional quantum theory emerges as the primes chosen as a basis for computation and/or measurement increase.

Theories over unrestricted finite fields

Modal Quantum Theory (I)

- Ignore complex numbers and ignore the inner product and define a vector space over an unrestricted field;
- Focus is $\mathbb{F}_2$, the field of booleans;
- Scalars: $a \in \{0, 1\}$;
- Scalar addition (exclusive-or):

$$0 + a = a \qquad a + 0 = a \qquad 1 + 1 = 0$$

- Scalar multiplication (conjunction):

$$0 * a = 0 \qquad a * 0 = 0 \qquad 1 * 1 = 1$$

Modal Quantum Theory (II)

- One qubit system: 2-dimensional vector space;
- Four vectors:

$$\bullet = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |+\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

- Three states: the zero vector is considered un-physical;
- Evolution described by invertible maps.

Modal Quantum Theory (III)

Evolution described by invertible maps. There are exactly 6 such maps:

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

$$S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad S^\dagger = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$D_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad D_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Notes: maps do not include Hadamard and are generally not unitary.

Modal Quantum Theory (IV)

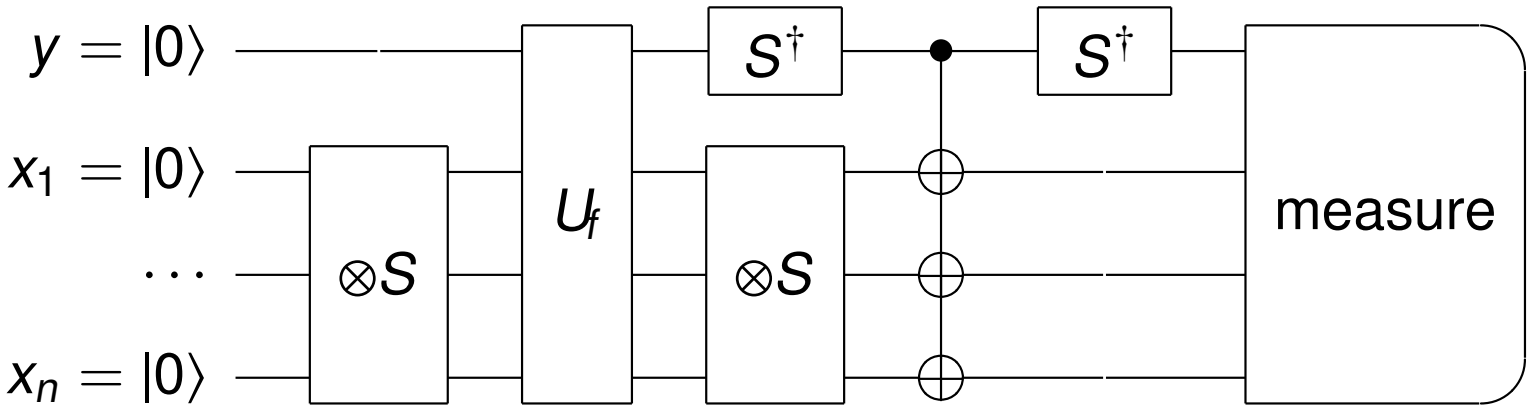
- Measuring $|0\rangle$ deterministically produces 0;
- Measuring $|1\rangle$ deterministically produces 1;
- Measuring $|+\rangle$ non-deterministically produces 0 or 1 with no probability distribution.

A Toy Theory

Schumacher and Westmoreland present modal quantum theories as toy theories:

- Retain some quantum characteristics: Superposition, interference, entanglement, mixed states, complementarity of incompatible observables, exclusion of hidden variable theories, no-cloning, etc.
- Can implement elementary quantum algorithms such as superdense coding and teleportation;
- Cannot implement richer quantum algorithms: there is no Hadamard.

A Surprising Development (Hanson, Ortiz, Sabry, Willcock)



- This circuit can be used to solve the unstructured database search in $O(\log N)$ outperforming the known asymptotic bound of $O(\sqrt{N})$ of Grover's algorithm;
- Our conclusion: these theories are "unreasonable".

Analysis

- Not enough expressiveness: Need to enrich the operations (e.g., include Hadamard);
- Too much expressiveness: Need to restrict the operations (e.g., all transformations must be unitary);
- Enriching is easy: use larger, extended, fields;
- Restriction is more difficult: need an inner product to even define what it means to be unitary.

Theories over *i*-extended finite fields

Enriching

- Need fields with more structure, specifically "discrete complex numbers";
- Fields $\mathbb{F}_{p^2}$ where $p \equiv 3 \pmod 4$ have elements α that behave like the complex numbers. (E.g. complex conjugation is α^p.)
- Example: $\mathbb{F}_{3^2}$ has 9 elements:

$$\begin{array}{cccc} 0 & & & \\ 1 & -1 & i & -i \\ 1+i & -1+i & 1-i & -1-i \end{array}$$

  These are all the complex numbers one can form using the integers modulo 3 as real and imaginary coefficients;
- Check $(1+i)^3 = 1 + 3i - 3 - i = -2 + 2i = 1 - i \pmod 3$.

Hermitian Dot Product

- Let $|\Psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle$ and $|\Phi\rangle = \sum_{i=0}^{d-1} \beta_i |i\rangle$;
- Define $\langle \Phi \mid \Psi \rangle = \sum_{i=0}^{d-1} \beta_i^p \alpha_i$;
- $\langle \Phi \mid \Psi \rangle$ is the complex conjugate of $\langle \Psi \mid \Phi \rangle$; YES
- $\langle \Phi \mid \Psi \rangle$ is conjugate linear in its first argument and linear in its second argument; YES
- $\langle \Psi \mid \Psi \rangle \geq 0$ and is equal to 0 only if $|\Psi\rangle$ is the zero vector. NO: in fact $\geq$ makes no sense in a finite field in the first place

An Improvement

- Can implement more algorithms (e.g., Deutsch algorithm)
- Previous supernatural algorithm does not always work (only when the size of the field divides $2^N - 1$)
- For a fixed database, matching the supernatural conditions becomes less likely as the size of the field increases
- For a fixed field, one can always pad the database with dummy records to achieve the supernatural efficiency

Analysis

- Theory is still unreasonable;
- We need a proper metric, trigonometric, and geometric constructions;
- We can, however, already develop discrete counterparts of the Hopf fibration, the Bloch sphere and count entangled and unentangled states: Hanson, Ortiz, Sabry, Tai, "Geometry of Discrete Quantum Computing", *J. Phys. A: Math. Theor. 46 (2013)*.)
- Number of unentangled n-qubit states (purity 1): $p^n(p-1)^n$;
- Number of maximally entangled n-qubit states (purity 0): $p^{n+1}(p-1)(p+1)^{n-1}$.

Theories over locally-ordered finite fields

Inner Product

- Let's look again at the missing property we need: $\langle \Psi \mid \Psi \rangle \geq 0$ and is equal to 0 only if $|\Psi\rangle$ is the zero vector;
- For that to even make sense, we need a sensible notion of $\geq$ in a finite field;
- We need a relation that is reflexive, anti-symmetric, transitive, and total;
- Impossible on the entire field but possible on a subset of the elements.

Local Order

- Reisler and Smith 1969 propose to define $a > b$ if $(a - b)$ is a quadratic residue;
- Is only transitive if the field has an uninterrupted sequence of quadratic residues;
- Reisler and Smith propose fields $\mathbb{F}_p$ with p of the form $8\Pi_{i=1}^{m} q_i - 1$ where q_i is the i^{th} odd prime;
- A better sequence is the sequence A000229 whose n^{th} element is the least number such that the n^{th} prime is the least quadratic non-residue for the given element.
- Good news: there are an infinite number of such fields.

Example

- The sequence A000229 starts with $3, 7, 23, 71, 311, \ldots$;
- The third element is 23; the third prime is 5; we say $p = 23$ and $k = 5$
- There are 5 elements $\{0, 1, 2, 3, 4\}$ that are quadratic residues: check $5^2 = 25 = 2 \pmod{23}$ and $7^2 = 49 = 3 \pmod{23}$;
- Because we deal with differences, any sequence of 5 elements centered around an arbitrary field element is totally ordered.

Local Inner Product

- Given a d-dimensional vector space, we can define a region where an inner product can be defined
- Example $p = 311$ and $k = 11$
- Allowed probability amplitudes:

$d = 1$	$\{0, \pm 1, \pm 2, \pm i, \pm 2i, (\pm 1 \pm i), (\pm 1 \pm 2i), (\pm 2 \pm i)\}$
$d = 2$	$\{0, \pm 1, \pm i, (\pm 1 \pm i)\}$
$d = 3$	$\{0, \pm 1, \pm i\}$
$d = 4$	$\{0, \pm 1, \pm i\}$
$d = 5$	$\{0, \pm 1, \pm i\}$
$d \geq 6$	$\{0\}$

Emergence of Conventional Quantum Theory

- Replace the Hilbert space with a local inner product subspace;
- Not closed under vector addition or scalar multiplication;
- But as long as all the probability amplitudes remain within the selected region, we may pretend to have a full inner product space.
- In a numerical computation on a microprocessor, as long as the numbers are within the range of the hardware, we can pretend to have conventional arithmetic.

Deutsch-Jozsa

- Common presentations state it is exponentially faster than any classical algorithm;
- . . . and in fact, it takes constant time !
- Our analysis shows that the size of the field must increase: one must pay for the extra precision;
- For an input function $2^n \to 2$, we need $k > 2^{3n+2}$;
- For a single qubit, $k = 37$;
- For two qubits, $k = 257$.

So far

- As the superpositions get denser and denser and the states get closer and closer to each other, the needed resources must increase;
- These resources are captured by the size of the underlying field;
- These resources are not apparent if one uses real numbers;
- Complexity theorists went to great length to formalize the needed precision if one uses real numbers (basically T steps require $O(\log T)$ bits of precision)

Measurement

- Key insight: The observer has resources that are independent from the resources needed to model the system;
- An observer that uses “few” resources will get crude information about the system;
- An observer that uses “many” resources will get precise information about the system;
- The notions of “few” and “many” can be formalized by comparing the size of the field used by the observer vs. the size of the field used to model the system;
- A new insight on measurement: what happens when two quantum systems with different underlying field sizes interact?

Example (I)

- Given these four 1-qubit states:

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

- All amplitudes are in the required range of $p = 311$, $k = 11$, and $d = 2$;
- Now consider the probabilities of observing various outcomes by an observer.
- Let's first calculate what an observer with infinite resources will see.

Example (II)

- Normalize using infinite precision numbers

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

- Probabilities of measuring 0: 1, 1/2, 1/3, and 1/2
- Probabilities of measuring 1: 0, 1/2, 2/3, and 1/2
- But this assumes the observer has enough resources to probe the state enough to distinguish the amplitudes
- Mathematically, how do we compute these square roots in finite fields?

Example (III)

- Another idea based on Reisler and Smith 1969
- Approximate square roots calculation in finite fields
- Round up to the next quadratic residue
- In a field with $k > 19$:

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

- Observed amplitudes:

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

Example (IV)

- Observed probabilities of measuring 0:

$$\{36, 16, 16, 18\} \not\parallel \{36, 32, 48, 36\}$$

- Observed probabilities of measuring 1:

$$\{0, 16, 32, 18\} \not\parallel \{36, 32, 48, 36\}$$

- Exact probabilities of measuring 0: 1, 1/2, 1/3, and 1/2
- Exact probabilities of measuring 1: 0, 1/2, 2/3, and 1/2
- Relative order is preserved but exact ratios ($16 * 3 \neq 36$) and exact equality are not ($16 \neq 18$)

Example (V)

- In a field with $k > 1230$, a better approximation of the square roots:

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

- Observed amplitudes:

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

Example (VI)

- Observed probabilities of measuring 0:

$$\{2500, 1296, 900, 1250\} \not\parallel \{2500, 2592, 2700, 2500\}$$

- Observed probabilities of measuring 1:

$$\{0, 1296, 1800, 1250\} \not\parallel \{2500, 2592, 2700, 2500\}$$

- Exact probabilities of measuring 0: 1, 1/2, 1/3, and 1/2;
- Exact probabilities of measuring 1: 0, 1/2, 2/3, and 1/2;
- $16 * 3$ vs. 36 is now $900 * 3$ vs. 2500; better approximations using more resources

Cardinal Probabilities

- Given several probabilistic events $e_1, e_2, \ldots$;
- Define a set of "rulers" $\mu_1, \mu_2, \ldots$ that are "equal" to within some precision;
- Measure each event with its own ruler;
- If the rulers are infinitely accurate, the measurement results can be directly compared; one can say "twice as likely"
- Otherwise, one can only speak of "at least as likely as"

Conclusions

- A simple finite field (e.g., booleans) is sufficient for teleportation, superdense coding, etc. Only thing needed is (constructive and destructive) superposition
- Finite fields that can be extended with i are sufficient for deterministic algorithms such as Deutsch's algorithm. In addition to superpositions, we need limited geometric notions (e.g., orthogonality).
- The above theories are, as far as we know, at odds with our present understanding of physical reality.
- Finite fields with locally-ordered elements are rich enough for conventional quantum theory to emerge as the size of the field increases.

Conclusions

- Accurate accounting of resources used during evolution using the size of the field used to represent the evolving amplitudes. The *precision* of the numeric approximations provided by the underlying number system, which is completely hidden in the real number system, is exposed as an explicit computational resource.
- Novel accounting of the resources used by the observer to extract information from the system
- Novel counting of the number of irreducible states, the relative sizes of the unentangled and entangled states, including maximally entangled states, i.e., those with zero purity.