Discrete Quantum Theories

Andrew J. Hanson* Gerardo Ortiz† **Amr Sabry*** Yu-Tsung Tai‡

(*) School of Informatics and Computing
(†) Department of Physics
(‡) Mathematics Department

Indiana University

(To appear in **J. Phys. A: Math. Theor.**, 2014)

Colloquiumfest
University of Saskatchewan
February 28-March 1, 2014

Our Origins: 1853

An Investigation of the Laws of Thought, on which are Founded the Mathematical Theories of Logic and Probabilities, G. Boole, 1853.

Opening sentence of Chapter 1:

> *The design of the following treatise is to investigate the fundamental laws of those operations of the mind by which reasoning is performed; . . .*

A few chapters later:

> ***Proposition IV.*** *That axiom of metaphysicians which is termed the principle of contradiction, and which affirms that it is impossible for any being to possess a quality, and at the same time not to possess it, is a consequence of the fundamental law of thought, whose expression is* $x^2 = x$.

Our Origins: 1936

On Computable Numbers, with an Application to the Entscheidungsproblem, A. Turing, 1936.

Opening sentence of Sec. 1:

> *We have said that the computable numbers are those whose decimals are calculable by finite means . . . the justification lies in the fact that the human memory is necessarily limited.*

Sec. 9:

> *I think it is reasonable to suppose that they can only be squares whose distance from the closest of the immediately previously observed squares does not exceed a certain fixed amount.*

Mathematical Models vs. Nature

Feynman, Girard, and others: Revisit our abstract models of computation and logical frameworks in view of the advances in physics.

> *In other terms, what is so good in logic that quantum physics should obey? Can't we imagine that our conceptions about logic are wrong, so wrong that they are unable to cope with the quantum miracle?*

> *Instead of teaching logic to nature, it is more reasonable to learn from her. Instead of interpreting quantum into logic, we shall interpret logic into quantum (Girard 2007).*

Quantum Mechanics vs. Quantum Computing

Quantum computing ...

- Opportunity to re-examine the foundations of quantum mechanics;
- Can provide executable interpretations of quantum mechanics;
- Physics is computational;
- Computation is physical;
- A precise mathematical model that quantifies the actual cost (i.e., resources) needed to perform a physical quantum process;

Relevance for Computer Science

- Turing's original paper is titled "On computable numbers . . . ";
- 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.
- 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.

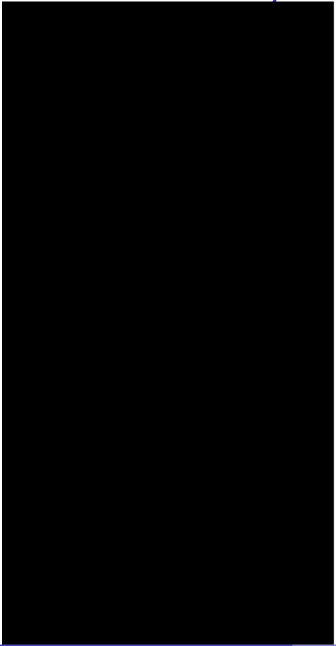
Relevance for Physics

- 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?

Relevance for Physics



25 March 1999
revised 19 September 1999
quant-ph/9905080

FINITE PRECISION MEASUREMENT NULLIFIES THE KOCHEN-SPECKER THEOREM

David A. Meyer

Project in Geometry and Physics
Department of Mathematics
University of California/San Diego
La Jolla, CA 92093-0112
dmeyer@chonji.ucsd.edu

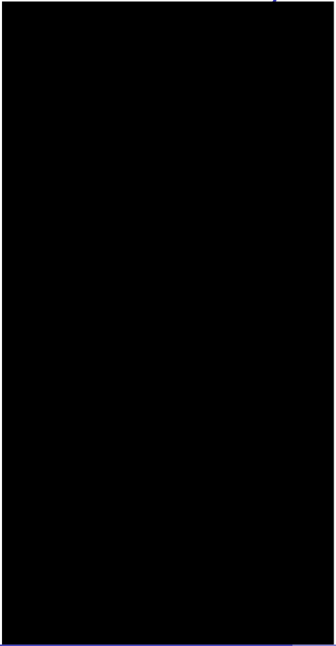
and Institute for Physical Sciences
Los Alamos, NM

ABSTRACT

Only finite precision measurements are experimentally reasonable, and they cannot distinguish a dense subset from its closure. We show that the rational vectors, which are dense in S^2, can be colored so that the contradiction with hidden variable theories provided by Kochen-Specker constructions does not obtain. Thus, in contrast to violation of the Bell inequalities, no quantum-over-classical advantage for information processing can be derived from the Kochen-Specker theorem alone.

1999 Physics and Astronomy Classification Scheme: 03.65.Bz, 03.67.Hk, 03.67.Lx.
American Mathematical Society Subject Classification: 81P10, 03G12, 68Q15.
Key Words: quantum computation, Kochen-Specker theorem, hidden variable theories,

Relevance for Physics



A Kochen-Specker Theorem for Imprecisely Specified Measurements

N. David Mermin
Laboratory of Atomic and Solid State Physics, Cornell University, Ithaca, NY 14853-2501

A recent claim that finite precision in the design of real experiments "nullifies" the impact of the Kochen-Specker theorem, is shown to be unsupportable, because of the continuity of probabilities of measurement outcomes under slight changes in the experimental configuration.

PACS numbers: 03.65.Bz, 03.67.Hk, 03.67.Lx

The Kochen-Specker (KS) theorem is one of the major no-hidden-variables theorems of quantum mechanics. It exhibits a finite set of finite-valued observables with the following property: there is no way to associate with each observable in the set a particular one of its eigenvalues so that the eigenvalues associated with every subset of mutually commuting observables obey certain algebraic identities obeyed by the observables themselves [1]. Such a set of observables is traditionally called uncolorable.

The physical significance of an uncolorable set of observables stems from the fact that a simultaneous measurement of a mutually commuting set must yield a set of simultaneous eigenvalues, which are constrained to obey the algebraic identities obeyed by the observables themselves. So any attempt to assign every observable in a KS uncolorable set a preexisting *noncontextual* value (a "hidden variable") that is simply revealed by a measurement, will necessarily assign to at least one mutually commuting subset of observables a set of values specifying results that quantum mechanics forbids.

The term "noncontextual" emphasizes that the disagreement with quantum mechanics only arises if the value associated with each observable is required to be independent of the choice of the other mutually commuting observables with which it is measured. *Contextual* value assignments in full agreement with all quantum mechanical constraints can, in fact, be made. The import of the KS theorem is that there exist sets of observables — "uncolorable sets" — for which any assignment of preexisting values must be contextual if all the outcomes specified by those values are allowed by the laws of quantum mechanics. The theorem prohibits noncontextual hidden-variable theories that agree with all the quantitative predictions of quantum mechanics.

Meyer [2] and Kent [3] have questioned the relevance of the KS theorem to the outcomes of real imperfect laboratory experiments, by constructing some clever noncontextual assignments of eigenvalues to every observable in a dense subset of observables, whose closure contains the

they note that observables measured in an actual experiment cannot be specified with perfect precision so, in Kent's words, "no Kochen-Specker-like contradiction can rule out hidden variable theories indistinguishable from quantum theory by finite precision measurements. . . ." [3]

I show below that this plausible-sounding but not entirely sharply formulated intuition dissolves under close scrutiny [4]. First I describe how the KS conclusion that quantum mechanics requires any assignment of preexisting values to be contextual can be deduced directly from the data, even when one is not sure precisely which observables are actually being measured. Then I identify where the intuition of Meyer and Kent goes astray.

At first glance it is not evident that either a KS uncolorable set or a Meyer-Kent (MK) dense colorable set of observables is relevant when one cannot specify to more than a certain high precision what observables are actually being measured. As traditionally viewed, the KS theorem merely makes a point about the formal structure of quantum mechanics, telling us that there is no consistent way to interpret *the theory* in terms of the statistical behavior of an ensemble, in each individual member of which every observable in the theory has a unique noncontextual value waiting to be revealed by any appropriate measurement. Upon further reflection, however, there emerges a straightforward way to apply the result of the KS theorem to measurements specified with high but imperfect precision, which makes it evident that the theorem and its various descendants remain entirely relevant to imperfect experiments, while the ingenious constructions of Meyer and Kent do not.

Let us first rephrase the implications of the KS theorem in the ideal case of perfectly specified measurements. The theorem gives a finite uncolorable set of observables, each with a finite number of eigenvalues. Because the number of possible assignments of noncontextual values to observables in the set is finite, no matter what probabilities are used to associate such values with the observables, the assignment must give nonzero probability to at least

A Game

- I get to pick a secret real number $r \in \mathbb{R}$;
- I will answer any yes/no questions about it? E.g., is it ≥ 5?
- Gleason says you can recover the secret based on the observations.
- Meyer says there is a catch: this can only be done if the observations can have infinite precision
- Mermin says there is no catch etc.
- Kochen-Specker is a generalization of this idea which says the secret must depend on the experimental setup (i.e., on who is asking the questions).

Relevance for Mathematics

- Equality is not a static relationship; it is a process with computational content;
- Homotopy Type Theory (HoTT) with the univalence axiom is a serious look at equality, identity, and equivalence from a computational perspective.
- A proposition is a statement that is susceptible to proof
- The question of whether two elements of a type (set or space) are equal is clearly a proposition
- Reversible physical laws and computational algorithms that conserve resources are examples of these “equality processes” modeled by paths in appropriate topological spaces.

Relevance to Science

Implications (**Scott Aaronson, Umesh Vazirani, and others**)

One of these wild claims must be true!:

- the extended Church-Turing thesis is false, or
- quantum physics is false, or
- there is an efficient classical algorithm for factoring

Relevance to Science

Implications (**Scott Aaronson, Umesh Vazirani, and others**)

One of these wild claims must be true!:

- the extended Church-Turing thesis is false, or
- quantum physics is false, or
- there is an efficient classical algorithm for factoring

If quantum physics is correct then there is an efficient quantum algorithm for factoring (Shor). If there is no efficient classical algorithm for factoring then the extended Church-Turing thesis is false.

Technical Outline I

Goal: revisit quantum mechanics assuming everything is finite.

- 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.)

Technical Outline II

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.

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)

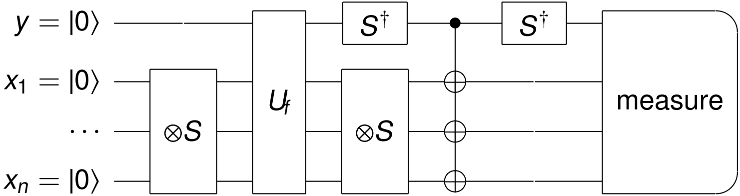
- Measuring $|0\rangle$ deterministically produces 0;
- Measuring $|1\rangle$ deterministically produces 1;
- Measuring $|+\rangle$ non-deterministically produces 0 or 1 with no probability distribution.

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;
- With $\mathbb{R}$, we can require operations to be continuous: vectors that are “close” to each other must remain “close”.
- Restriction is more difficult: what does it mean to be “close” in finite fields; what does it mean to be unitary if we don’t have an inner product?

Theories over *i-extended* finite fields

Enriching

- Need fields with more structure, specifically "discrete complex numbers";
- Complex numbers allow some notion of continuity (reflections in 2D).
- 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:

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

  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 $\langle\Psi \mid \Phi\rangle$;
- $\langle\Phi \mid \Psi\rangle$ is conjugate linear in its first argument and linear in its second argument;
- $\langle\Psi \mid \Psi\rangle \geq 0$ and is equal to 0 only if $|\Psi\rangle$ is the zero vector.

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;
- $\langle\Psi \mid \Psi\rangle \geq 0$ and is equal to 0 only if $|\Psi\rangle$ is the zero vector.

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.

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:

$$\begin{array}{c|l} d = 1 & \{0, \pm 1, \pm 2, \pm i, \pm 2i, (\pm 1 \pm i), (\pm 1 \pm 2i), (\pm 2 \pm i)\} \\ d = 2 & \{0, \pm 1, \pm i, (\pm 1 \pm i)\} \\ d = 3 & \{0, \pm 1, \pm i\} \\ d = 4 & \{0, \pm 1, \pm i\} \\ d = 5 & \{0, \pm 1, \pm i\} \\ d \geq 6 & \{0\} \end{array}$$

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 $2^n \rightarrow 2$, 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:

$$\{36, 16, 16, 18\} \mathbin{/\!\!/} \{36, 32, 48, 36\}$$

- Observed probabilities of measuring 1:

$$\{0, 16, 32, 18\} \mathbin{/\!\!/} \{36, 32, 48, 36\}$$

- 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:

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

- Observed amplitudes:

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

Example (VI)

- Observed probabilities of measuring 0:

$$\{2500, 1296, 900, 1250\} \mathbin{/\!\!/} \{2500, 2592, 2700, 2500\}$$

- Observed probabilities of measuring 1:

$$\{0, 1296, 1800, 1250\} \mathbin{/\!\!/} \{2500, 2592, 2700, 2500\}$$

- 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 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; this is modeled by the size of the underlying field;
- 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;
- Finite trigonometry; finite geometry; finite Hopf fibrations, etc.
- 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.