Discrete Quantum Theories and Computing

Yu-Tsung Tai

Department of Mathematics and Department of Computer Science
Indiana University, Bloomington

Dilemma of quantum computing?

- Textbook quantum mechanics is correct.
- There does not exist an efficient classical factoring algorithm.
- The extended Church-Turing thesis —that probabilistic Turing machines can efficiently simulate any physically realizable model of computation —is correct.

Check the compatibility of Quantum Mechanics and Computer Science.

Quantum Mechanics is based on continuous. How about Computer Science?

	Discrete	Continuum
Theoretical Model	Turing machine	BCSS machine
Physical Realization	Digital Computer	Analog Computer
How the models realize?	Reliably	Not Reliably: 1. The quality might be quantized.. 2. The precision of an analog computer is low.

Build a more faithful Quantum Computing model?

Our Quantum Models	Quantum Theories and Computing over Finite Fields	Quantum Interval-Valued Probability Measures

Conventional Quantum Theory

Conventional Quantum Theory

i. D orthonormal basis vectors for a Hilbert space of dimension D.

ii. D complex probability amplitude coefficients describing the contribution of each basis vector.

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

iv. A measurement framework.

Pure State

- A pure state can be represented as a D-dimensional vector, $|\Psi\rangle = \sum_{i=0}^{D-1} \alpha_i |i\rangle$, where $\{|0\rangle, |1\rangle \dots, |D-1\rangle\}$ form an orthonormal basis.
- Given two states $|\Psi\rangle = \sum_{i=0}^{D-1} \alpha_i |i\rangle$ and $|\Phi\rangle = \sum_{i=0}^{D-1} \beta_i |i\rangle$, their inner product

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

satisfying the following properties:

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.

Mixed State

- A mixed state is the weighted average of the density matrices of pure states

$$\rho = \sum_{j=1}^{N} q_j |\Phi_i\rangle\langle\Phi_i| \ ,$$

where $|\Phi_i\rangle$ are normalized, $q_j > 0$, and $\sum_{j=1}^{N} q_j = 1$.

Probability Space

Abstraction

- Sample space Ω.
- Event Space 2^{Ω}.
- Probability measure $\mu: 2^{\Omega} \rightarrow [0,1]$
  - $\mu(\emptyset) = 0$.
  - $\mu(\Omega) = 1$.
  - For any event E,
    $$\mu(\bar{E}) = 1 - \mu(E) .$$
  - For disjoint events E_0 and E_1,
    $\mu(E_0 \cup E_1) = \mu(E_0) + \mu(E_1)$.

Example

- Sending a particle to a beam splitter with the split beams $|0\rangle$, $|1\rangle$, and $|2\rangle$.
- Sample space $\Omega_0 = \{|0\rangle, |1\rangle, |2\rangle\}$.
- Event Space 2^{Ω_0}.
- Probability measure $\mu_0: 2^{\Omega_0} \rightarrow [0,1]$.

Probability Space

Example

- Sending a particle to a beam splitter with the split beams $|0\rangle$, $|1\rangle$, and $|2\rangle$.
- Sample space $\Omega_0 = \{|0\rangle, |1\rangle, |2\rangle\}$.
- Event Space 2^{Ω_0}.
- Probability measure $\mu_0 : 2^{\Omega_0} \to [0,1]$.

Another Example

- Sending the same particle to a beam splitter with the split beams $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, and $|2\rangle$.
- Sample space $\Omega_1 = \{|+\rangle, |-\rangle, |2\rangle\}$.
- Event Space 2^{Ω_1}.
- Probability measure $\mu_1 : 2^{\Omega_1} \to [0,1]$.

When the particle is the same, the probability of the same event is the same: $\mu_0(\{|2\rangle\}) = \mu_1(\{|2\rangle\})$.
So does their complement: $\mu_0(\{|0\rangle, |1\rangle\}) = \mu_1(\{|+\rangle, |-\rangle\})$

Glue Classical Event Spaces to a Quantum Event Space

- When the particle is the same, the probability of the same event is the same: $\mu_0(\{|2\rangle\}) = \mu_1(\{|2\rangle\})$.
  So does their complement: $\mu_0(\{|0\rangle, |1\rangle\}) = \mu_1(\{|+\rangle, |-\rangle\})$
- Consider
  $$\varphi(E) = \sum_{|j\rangle \in E} |j\rangle\langle j|$$
  Then,
  $\varphi(\{|0\rangle, |1\rangle\}) = |0\rangle\langle 0| + |1\rangle\langle 1| = |+\rangle\langle +| + |-\rangle\langle -| = \varphi(\{|+\rangle, |-\rangle\})$
- The quantum event of a classical event E is the projector $\varphi(E)$, and the set of all projectors on a given Hilbert space is called a quantum event space $\mathcal{E}$.

Classical and Quantum Probability Measure

Classical Probability measure

- $\mu: 2^{\Omega} \to [0,1]$
- $\mu(\emptyset) = 0.$
- $\mu(\Omega) = 1.$
- For any event E,
$$\mu(\bar{E}) = 1 - \mu(E)\,.$$
- For disjoint events E_0 and E_1 ($E_0 \cap E_1 = \emptyset$),
$$\mu(E_0 \cup E_1) = \mu(E_0) + \mu(E_1)\,.$$

Quantum Probability measure

- $\mu: \mathcal{E} \to [0,1]$
- $\mu(\mathbb{0}) = 0$, where $\mathbb{0}$ is the zero projector.
- $\mu(\mathbb{1}) = 1$, where $\mathbb{1}$ is the identity projector.
- For any projector P,
$$\mu(\mathbb{1} - P) = 1 - \mu(P)\,.$$
- For orthogonal projectors P_0 and P_1 ($P_0 P_1 = \mathbb{0}$),
$$\mu(P_0 + P_1) = \mu(P_0) + \mu(P_1)\,.$$

Fix an orthonormal basis Ω, consider the restricted $\varphi: 2^{\Omega} \to \mathcal{E}$. Then, $\varphi^{*}\mu: 2^{\Omega} \to [0,1]$ defined by $(\varphi^{*}\mu)(E) = \mu\big(\varphi(E)\big)$ is a classical probability measure and called the pullback of μ by $\varphi: 2^{\Omega} \to \mathcal{E}$.

Observables and Expectation Values

- A quantum probability measure $\mu : \mathcal{E} \to [0,1]$.
- A observable $\mathbf{O}$ diagonalizable by an orthonormal basis $\Omega = \{|0\rangle, |1\rangle, \dots, |D-1\rangle\}$with spectral decomposition $\mathbf{O} = \sum_{i=1}^{D-1} \lambda_i |i\rangle\langle i|$.
- The expectation value is $\langle \mathbf{O} \rangle_\mu = \sum_{i=1}^{D-1} \lambda_i \mu(|i\rangle\langle i|)$.
- The pullback of $\mathbf{O}$ by $\varphi: 2^\Omega \to \mathcal{E}$ is the random variable $\varphi^* \mathbf{O}: 2^\Omega \to \mathcal{E}$ defined by $\varphi^* \mathbf{O} = \sum_{i=1}^{D-1} \lambda_i \mathbf{1}_{\{|i\rangle\}}$, where $\mathbf{1}_{\{|i\rangle\}}$ is the indicator function.
- The pullback preserves the expectation value

$$\langle \mathbf{O} \rangle_\mu = \int (\varphi^* \mathbf{O}) \, d(\varphi^* \mu)$$

Gleason's Theorem

Theorem (Gleason's) When dimension $d \geq 3$, given a quantum probability measure $\mu: \mathcal{E} \rightarrow [0,1]$, there exists a unique mixed state ρ such that

$$\mu(P) = \mathrm{Tr}(\rho P) \,.$$

- If we follow the same interpretation that $\mu(P)$ is the probability of the particle in the split beams in P, does ρ represent the state of the particle sending to the beam splitter?

Born Rule

- Let $\mu_{\Phi}^{\mathrm{B}}(P)$ denote the quantum probability measure created by the particle in the unnormalized pure state $|\Phi\rangle$. It should satisfy:
  - $P|\Phi\rangle = |\Phi\rangle$ if and only if $\mu_{\Phi}^{\mathrm{B}}(P) = 1$.
  - $\mu_{\Phi}^{\mathrm{B}}(P) = \mu_{U|\Phi\rangle}^{\mathrm{B}}\left(UPU^{\dagger}\right)$ for unitary U.
- Then, $\mu_{\Phi}^{\mathrm{B}}(P) = \dfrac{\langle \Phi|P|\Phi \rangle}{\langle\Phi|\Phi\rangle}$ is called the Born rule.
- When $|\Phi\rangle$ is normalized, $\mu_{\Phi}^{\mathrm{B}}(P) = \langle \Phi \mid P \mid \Phi \rangle$.
- For a mixed state $\rho = \sum_{j=1}^{N} q_j |\Phi_i\rangle\langle\Phi_i|$,
  $\mu_{\rho}^{\mathrm{B}}(P) = \sum_{j=1}^{N} q_j \mu_{\Phi_j}^{\mathrm{B}}(P) \; = \mathrm{Tr}(\rho P)$.

Entanglement, Pauli Operators, and Purity

- A state $|\Psi\rangle$ is entangled if $|\Psi\rangle \neq |\psi_1\rangle \otimes \cdots \otimes |\psi_j\rangle \otimes \cdots \otimes |\psi_n\rangle$.
- $\sigma_0 = |0\rangle\langle 0| + |0\rangle\langle 0|$, $\sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|$, $\sigma_y = \mathbb{i}|1\rangle\langle 0| - \mathbb{i}|0\rangle\langle 1|$, $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$.
- $\sigma_\eta^j = \sigma_0 \otimes \cdots \otimes \sigma_0 \otimes \sigma_\eta \otimes \sigma_0 \otimes \cdots \otimes \sigma_0$, where σ_η is the j-th factor.
- The purity $P_{\mathfrak{h}} = \frac{1}{n}\sum_{j=1}^{n} \sum_{\eta=x,y,z} \left\langle \sigma_\eta^j \right\rangle^2$ is a measure of entanglement
- If $P_{\mathfrak{h}} = 1$, the state is a product state.
- When $P_{\mathfrak{h}} = 0$, the state is called maximally entangled.

Quantum Theories and Computing over Finite Fields

Modal Quantum Theory and Computing No Deutsch’s algorithm

- Replace Complex Numbers by $\mathbb{F}_2$
- A n-qubit state is a non-zero vector in $\mathbb{F}_2^{2^n}$.
- Since unitary matrices aren’t defined, the dynamics is realized by the group of any invertible linear map.
- However, since $\mathbb{F}_2$ only has two elements 0 and 1, we cannot express the Hadamard transformation $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$, and any algorithm based on it including Deutsch’s algorithm.

Modal Quantum Theory and Computing Has UNIQUE-SAT algorithm

- Since the dynamics is realized by the group of any invertible linear map, it also includes some maps which cannot be used on CQT like
$$S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } S^\dagger = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$
- Even if this theory only predicts whether an result is possible or impossible, we can use the above matrices to construct a circuit solving UNIQUE-SAT efficiently.

Discrete Quantum Theory (I)

- Replace Complex Numbers by $\mathbb{F}_{p^2} = \left\{a + b\mathbb{i} \middle| a, b \in \mathbb{F}_{p^2}\right\}$.
- A pure state can be represented as a D-dimensional vector, $|\Psi\rangle = \sum_{i=0}^{D-1} \alpha_i |i\rangle$, where $\{|0\rangle, |1\rangle \dots, |D-1\rangle\}$ form an orthonormal basis.
- Given two states $|\Psi\rangle = \sum_{i=0}^{D-1} \alpha_i |i\rangle$ and $|\Phi\rangle = \sum_{i=0}^{D-1} \beta_i |i\rangle$, their Hermitian dot product

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

- Although the Hermitian dot product looks familiar, it doesn't have positive definite.
- This theory only predicts whether an result is possible or impossible.

Discrete Quantum Theory (I): State Counting

- The total count of unique irreducible state in D-dimensional space is
$$\frac{p^D(p^D-(-1)^D)}{p+1}\,.$$
- For n-qubit system, the number of product state is $p^n(p-1)^n$.
- The maximal entangled state is defined to satisfy
$$\forall j, \forall \eta \in \{x,y,z\}, \left\langle \sigma_\eta^j \right\rangle^2 = 0\,.$$
- The number of maximal entangled state for two-qubit and three-qubit systems are $p(p^2-1)$ and $p^3(p^4-1)$, respectively.

Discrete Quantum Computing (I)

- We can express Deutsch's algorithm.
- We may have UNIQUE-SAT algorithm depending on the relation between the prime p and the size of Boolean expression.

Discrete Quantum Theory (II)

- Recall when $|\Psi\rangle = \sum_{i=0}^{D-1} \alpha_i |i\rangle$ is not normalized, $\mu_\Psi^{\mathrm{B}}(|i\rangle\langle i|) = \frac{\langle\Psi|i\rangle\langle i|\Psi\rangle}{\langle\Psi|\Psi\rangle} = \frac{\alpha_i^* \alpha_i}{\sum_{i=0}^{D-1} \alpha_i^* \alpha_i}$.
- When α_i is an element in finite fields, the division doesn't make sense, but $\alpha_i^* \alpha_i$ and $\sum_{i=0}^{D-1} \alpha_i^* \alpha_i$ could make sense as long as we don't wrap around $1 + 1 + \cdots + 1 = 0$.
- To not wrap around, we restrict computation in a small region.
- To not divide, we replace the division by // and get the cardinal probability $\mu_\Psi^{\mathrm{C}}(i) = \alpha_i^* \alpha_i // \sum_{i=0}^{D-1} \alpha_i^* \alpha_i$.

Discrete Quantum Computing (II)

- UNIQUE-SAT could not perform because the vectors cannot inside a small region during the whole computation.
- Neither does Shor's algorithm.
- It can perform probabilistic Grover search algorithm.
- It is not clear how to define mixed states on the cardinal probability.

Quantum Probability Measures over Finite Fields

Quantum Probability Measure

- $\mu: \mathcal{E} \to [0,1]$
- $\mu(\mathbb{0}) = 0.$
- $\mu(\mathbb{1}) = 1.$
- For any projector P,
$$\mu(\mathbb{1} - P) = 1 - \mu(P)\,.$$
- For orthogonal projectors P_0 and P_1 ($P_0 P_1 = \mathbb{0}$),
$$\mu(P_0 + P_1) = \mu(P_0) + \mu(P_1)\,.$$

Quantum Probability Measure over Finite Fields

- Let $\mathcal{E}_{p^2}$ denote the set of projectors which can be expressed as the sum of 1-dimensional projectors on $\mathbb{F}_{p^2}$.
- $\mu: \mathcal{E}_{p^2} \to [0,1]$
- $\mu(\mathbb{0}) = 0.$
- $\mu(\mathbb{1}) = 1.$
- For any projector P,
$$\mu(\mathbb{1} - P) = 1 - \mu(P)\,.$$
- For orthogonal projectors P_0 and P_1 ($P_0 P_1 = \mathbb{0}$),
$$\mu(P_0 + P_1) = \mu(P_0) + \mu(P_1)\,.$$

Quantum Probability Measures over Finite Fields (QPMFF)

- When $D = 3$ and $p = 7$, there is only one QPMFF.
- For $D \geq 3$ except $p = D = 3$, there is no Born rule satisfying:
  - $\mu_{\Phi}^{\mathrm{F}}: \mathcal{E}_{p^2} \to [0,1]$ is a quantum probability measure.
  - $P|\Phi\rangle = |\Phi\rangle$ if and only if $\mu_{\Phi}^{\mathrm{F}}(P) = 1$.
  - $\mu_{\Phi}^{\mathrm{F}}(P) = \mu_{U|\Phi\rangle}^{\mathrm{F}}\left(UPU^{\dagger}\right)$ for unitary U.

From Infinitely Precise to Finite-Precision

Classical Probability Measure

- $\mu: 2^{\Omega} \to [0,1]$
- $\mu(\emptyset) = 0.$
- $\mu(\Omega) = 1.$
- For any event E,
  $$\mu(\Omega \backslash E) = 1 - \mu(E).$$
- For disjoint events E_0 and E_1,
  $$\mu(E_0 \cup E_1) = \mu(E_0) + \mu(E_1).$$

Classical Interval-Valued Probability Measure (IVPM)

- $\overline{\mu}: 2^{\Omega} \to \mathcal{I} = \{[\ell_i, r_i] \subseteq [0,1]\}$
- $\overline{\mu}(\emptyset) = [0,0].$
- $\overline{\mu}(\Omega) = [1,1].$
- For any event E, if $\overline{\mu}(E) = [\ell, r]$, then $\overline{\mu}(\Omega \backslash E) = [1,1] - \overline{\mu}(E) = [1 - r, 1 - \ell].$
- For disjoint events E_0 and E_1, if $\overline{\mu}(E_0) = [\ell_0, r_0]$ and $\overline{\mu}(E_1) = [\ell_1, r_1]$, then
  $$\overline{\mu}(E_0 \cup E_1) \subseteq \overline{\mu}(E_0) + \overline{\mu}(E_1)$$
  $$= [\ell_0 + \ell_1, r_0 + r_1].$$