

My Adventures in the Quantum Wonderland

Man-Duen Choi

Math Dept. , University of Toronto

June 2008 of GPOTS

**With fond memories of the
beautiful Cincinnati campus,
as in 2006 and 1986**

Introduction

- Originally, Quantum Information was a sub-field of Quantum Mechanics.
- Quantum Information has risen as an important field in connection with physics, computer Science and mathematics .
- The first quantum computer in real functioning was built in 1998.
- In 2006, there was a benchmarking of a 12-qubit computer.

Units of Information

--- Bits vs Qubits

- a **bit** (binary integer) is the base of conventional computer memory.
- 1-bit is read as either a zero or a one with probability in the real interval $[0, 1]$.
- Thus, a 3-bit corresponds to an element in $\{0, 1\} \times \{0, 1\} \times \{0, 1\} = 2^3$, which can be viewed as 8 vertices of a solid cube.
- When $n = 30$, we get $2^{30} = 1$ giga

- To get a setting of a possible non-commutative generalization, we associate each 1-bit with a rank-1 diagonal 2 X 2 projection matrix. i.e..

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

- Each 3-bit corresponds to a rank-1 diagonal 8 X 8 projection matrix, as the tensor product of three 2 X 2 matrices where each is

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

- A ***qubit*** (quantum bit) is a unit of quantum computer memory.
- Physically, a 1-qubit is a superposition of the spherical surface (called the Bloch sphere), because an electron can move freely to any direction from the origin of \mathbf{R}^3 .
- Mathematically, each 1-qubit is regarded as an element in

$$S^2 \simeq \left\{ \frac{1}{2} \begin{pmatrix} 1-x & y+iz \\ y-iz & 1+x \end{pmatrix} \quad \text{with } x^2 + y^2 + z^2 = 1 \right\}$$

= {all rank-1 2 X 2 projection matrices}

= {one-dimensional complex linear subspaces of \mathbf{C}^2 }.

An ***n-qubit*** is regarded as a 1-dimensional complex linear subspace of the dim 2^n Hilbert space, which can also be identified as a rank-1 projection in the form as a $2^n \times 2^n$ complex matrix.

➤ It has been well understood in quantum mechanics, many n-qubits are not realizable in terms of n units of 1-qubits because of the sophisticated effect of ***quantum entanglement*** of the superposition of the Bloch sphere.

➤ However, this sort of physical explanations may be incomprehensible for experts in computer science.

➤ For the sake of better understanding, it may be desirable to interpret all physical features by means of the simple language of pure mathematics.

Specifically, with respect to a fixed decomposition of the Hilbert space $\mathbf{C}^{2^n} = \bigotimes \mathbf{C}^2$ as the tensor product of n pieces of \mathbf{C}^2 , we write $M_{2^n} = \bigotimes M_2$ as the canonical tensor product of n copies of M_2 . Then, it is mathematically obvious that many one-dimensional complex linear subspaces of $\bigotimes \mathbf{C}^2$ cannot be expressed as the tensor product of n pieces of 1-dimensional complex linear subspaces of \mathbf{C}^2 ; equivalently, many rank-1 projections in $\bigotimes M_2$ need not be of the form of tensor product of n pieces of rank-1 2×2 projections.

As a sort of non-commutative probability, the random position of an n -qubit can be regarded as a *density matrix*, to be defined as a convex combination of rank-1 projections in M_{2^n} .

Definition: A *density matrix* is a positive semi-definite matrix of trace 1.

Thus each 2×2 density matrix is expressible in the form

$$\frac{1}{2} \begin{pmatrix} 1-x & y+iz \\ y-iz & 1+x \end{pmatrix}$$

with $x^2 + y^2 + z^2 \leq 1$; and so all 2×2 density matrices together fill up the solid sphere with S^2 as boundary.

Nevertheless, for the case $n > 2$, there is no geometrical picture for the collection of all $n \times n$ density matrices. We need a rigorous mathematical approach to understand positive semi-definite matrices.

- In fact, if we think of n-bits as the special subclass of commutative n-qubits, then the commutative counterpart of density matrices are precisely the collection of diagonal matrices with non-negative diagonal entries summing up to one.
- While the setting of diagonal matrices looks too trivial to be useful, the non-commutative matrix theory turns out to be indispensable for quantum information beyond physical interpretation.
- In the theory of quantum information, a ***quantum channel*** is a communication channel which can transmit quantum information. We will explain why a quantum channel should be viewed as a trace-preserving completely positive linear map.

Notations

M_n = the algebra of all $n \times n$ complex matrices

M_n^h = the real space of all $n \times n$ hermitian matrices

M_n^+ = the cone of all $n \times n$ positive semidefinite matrices.

Def: A linear map $\Phi : M_n \rightarrow M_m$ is a *positive linear map* when $\Phi(M_n^+) \subseteq M_m^+$.

Φ is ***completely positive*** when Φ is of the form

$$\Phi(A) = \sum V_j^* A V_j \text{ for all } A \text{ in } M_n .$$

Structural problem

- In many natural setup, the positive linear maps are considered as the natural morphisms.
- The main question: Are there any tractable structure theory for positive linear maps?
- Must each positive linear map (restricted to real symmetric matrices) be realized as a completely positive linear map?

The simplest counter-example of a positive linear map that does not have completely positive effect

The promised counter-example

is a linear map

$\phi: M_3 \rightarrow M_3$ such that

$$\phi \left(\begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{bmatrix} \right) = \begin{bmatrix} \alpha_{11} & -\alpha_{12} & -\alpha_{13} \\ -\alpha_{21} & \alpha_{22} & -\alpha_{23} \\ -\alpha_{31} & -\alpha_{32} & \alpha_{33} \end{bmatrix} + \begin{bmatrix} \alpha_{33} & 0 & 0 \\ 0 & \alpha_{11} & 0 \\ 0 & 0 & \alpha_{22} \end{bmatrix}$$

For the sake of a better structure theory, we need to get full information of the structure of special classes of positive linear maps.

Notation: Each linear map $\Phi : M_n \longrightarrow M_k$ can be extended to a linear map

$$\Phi \otimes id_p : M_n \otimes M_p \longrightarrow M_k \otimes M_p \quad .$$

Definition. Φ is said to be *p-positive* when $\Phi \otimes id_p$ is a positive linear map.

Definition. Φ is said to be *completely positive* when Φ is a *p*-positive linear map for each positive integer *p*.

The following is the key result for completely positive linear maps on matrix algebras.

Theorem (Choi [7]): *Let $\Phi : M_n \longrightarrow M_k$ be a linear map. Then the following are equivalent:*

(a) Φ is completely positive.

(b) $[\Phi(E_{ij})]_{i,j} \in (M_n(M_k))^+ = (M_n \otimes M_k)^+ .$

(c) Φ can be written as

$$\Phi(X) = \sum A_j^* X A_j$$

with $n \times k$ matrices A_j for all $X \in M_n$.

The following is the basic structure theorem.

Theorem (Choi [5]): *All p -positive linear maps from $M_n \longrightarrow M_k$ are completely positive when $p \geq n$ or $p \geq k$.*

Nevertheless, various integers p provide distinct classes of linear maps as elaborated in

Example(Choi [5]): The map $\Phi(A) = (n - 1)(\text{trace}A)I_n - A$ is an $(n-1)$ -positive linear map from M_n to M_n , but it is not n -positive.

Now, we are ready to carry out the full exploration of quantum information.

Let H_s be the system Hilbert space and let H_e be the environment Hilbert space. (Usually, $\dim H_e \geq \dim H_s < \infty$.)

Definition: A *quantum channel* (alias, *quantum operation*) is a linear map $\Phi : L(H_s) \longrightarrow L(H_s)$ satisfying the conditions:

- (i) Φ is trace preserving: i.e., $\text{trace}(\Phi(X)) = \text{trace}X$ for all X .
- (ii) $\Phi \otimes id : L(H_s) \otimes L(H_e) \longrightarrow L(H_s) \otimes L(H_e)$ is a positive linear map.

From the structure theorems mentioned in this section, it follows that Φ is completely positive and

$$\Phi(X) = \sum A_j^* X A_j$$

and $\sum A_j A_j^* = I$. Thus, we have established the theoretical settings of quantum channels, ready for all sort of practical uses of programming

Error Correction

- There arise several new and important questions about the intrinsic structure of completely positive linear maps. In particular, the notion of error correction plays an important role in the structure theory.
- The terminology *error correction* may be misleading. It could be called *information re-storage* or *quantum inversion channel*.
- Namely, given a trace preserving completely positive linear map $\Phi : M_n \rightarrow M_n$, how can we proceed to find a trace preserving completely positive linear map Ψ so that $\Psi \circ \Phi$ is the identity map?
- Or, in many cases, one may like to get a projection P (as large as possible) so that $P\Psi(\Phi(X))P = PXP$.

Error Corrections

- If there was a missing page in a book, how could you get the full meaning of the book?
- How could you check whether the incoming message is complete/accurate ?
- The bank sent out all information, how to ensure the right persons to get the right messages?

Mathematical meanings of certain results related to error corrections.

- Let $\Phi : M_n \rightarrow M_n$, and $\Psi : M_n \rightarrow M_n$ be trace preserving completely positive linear maps such that $\Psi \circ \Phi$ is the identity map. Then, both Ψ and Φ are $*$ -automorphisms induced by unitary matrices.
- Each unital complete positive linear map is induced by the compression of a $*$ -representation (Stinespring Theorem). Thus an easy representation will provide uncountably many different messages (of different kinds of information).

Non-commutative harmonic analysis in the easy setting of the Stinespring Theorem

- **Theorem** (Ando, Arveson): If the numerical range of an operator T is a subset of the closed unit disc, then T can be dilated to

$$\begin{bmatrix} 0 & 2I \\ 0 & 0 \end{bmatrix}$$

The proof is non-constructive. Major Problem:

Given T , how to get concrete A, B, C so that

$$\begin{bmatrix} T & A \\ B & C \end{bmatrix}$$

Is unitarily equivalent to

$$\begin{bmatrix} 0 & 2I \\ 0 & 0 \end{bmatrix}$$

Higher-Rank Numerical Ranges

- There is a down-to-earth problem:
- If T is an $n \times n$ matrix and if $PTP = \lambda P$ for some scalar λ and some projection P , then what can be said about T ?
- **Definition:** Let T be an $n \times n$ matrix. For each positive integer k , ***the rank- k numerical range*** of T is the subset of the complex plane given by

$$\Lambda_k(\sigma) = \{ \lambda \in \mathbb{C} : PTP = \lambda P \text{ for some } P \in \mathfrak{P}_k \},$$

where \mathfrak{P}_k is the set of all rank- k projections in M_n .

The case $k = 1$ yields the familiar numerical range $W(T)$ for the $n \times n$ matrix T :

$$\Lambda_1(T) = W(T) = \{x^*Tx : x \in \mathbf{C}^n, \quad \|x\| = 1\}.$$

It is clear that

$$\Lambda_1(T) \supseteq \Lambda_2(T) \supseteq \dots \supseteq \Lambda_n(T).$$

Recently, H. Woederman, C.K. Li and N.S. Sze have proved the remarkable result: each $\Lambda_k(T)$ is convex set.

The meaning of 0 in $\Lambda_2(T)$

By definition, there exists a rank-2 projection P such that $PTP = 0$.

In practice, what is the algorithm to check whether any given $n \times n$ matrix T is a dilation of the 2×2 zero matrix.

In particular, what is the spectrum of an $n \times n$ normal matrix N to be a dilation of the 2×2 zero matrix?

Normal Dilations

- Here is a simple question of unknown depth in matrix theory:
- Which normal matrices are of the form

- $$N = \begin{bmatrix} O & A \\ B & C \end{bmatrix}$$

- ---What can be said about the spectrum of N ?

- Hard Question: Which matrices can be dilated to a normal matrix with prescribed eigenvalues?
- Equivalently, with prescribed complex numbers α_j , how to describe all matrices of the form $\sum \alpha_j A_j$ with positive semi-definite A_j such that $\sum A_j = I$? (Non-commutative resolution of identity)