Quantum Effects in Zero-Error Communication and Non-Commutative Graphs

Runyao Duan

Centre for Quantum Computation and Intelligent Systems (QCIS)

University of Technology, Sydney (UTS), Australia

and

Tsinghua University, Beijing, China.

Partly supported by ARC DP and NSFC

This talk is mainly based on arXiv:0906.2527 (Topic 1) and joint work arXiv:1002.2514 with S. Severini (UCL) and A. Winter (Univ. of Bristol and CQT at NUS) (Topic 2).

Operator Spaces, Quantum Probability and Applications

Wuhan University, Wuhan, China

June 4-10, 2012

“The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.”

----Claude Elwood Shannon, 1948

1. **Exactly (zero-error):** $\forall m, \quad m = \widehat{m}$
2. **Approximately (small-error):** $\forall m, \quad m \approx \widehat{m}$
3. **Unambiguously (no mistake):** $\forall m, \quad m = \widehat{m} \text{ or } m = ?$

Why Zero-Error?

1. In some critical applications no error can be tolerated.

"Even a decision with tiny probability of error may lead to fatal consequence!"

2. Only a finite number of uses of channel are available but high reliability is required.

Game: Answer 100 questions with "Yes", "No", or "Disclaim".

Rules: Correct +10$; Mistake -1000$; Disclaim -1$ (per Q).

It is much better to say "I don't know" than to make a possible false guess.

3. Far-reaching connections with Graph theory, Combinatorics, Communication complexity, and Quantum entanglement theory.

Culmination: "The Strong Perfect Graph Theorem."
(Chudnovsky, Robertson, Seymour, and Thomas, 2006)

4. Many new and interesting unsolved problems.

"Zero-Error Information Theory" (Korner&Orlitsky,1998)

Overview of Talk

Topic 1: Some striking quantum effects in zero-error communication via noisy quantum channels.

(i). Entanglement between different uses enables perfect transmission of classical information.

(ii). Both zero-error classical and quantum capacities are strongly super-additive, intuitively, 1+0>>1.

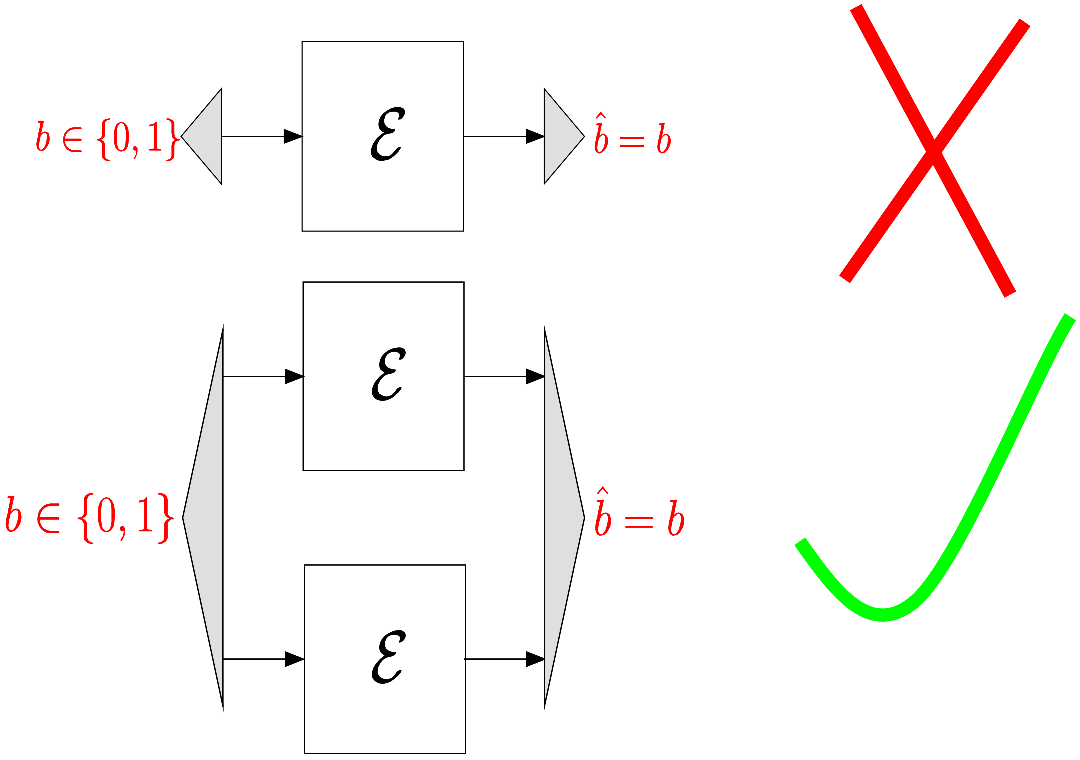
(iii). Classical feedback can boost the zero-error capacity from zero to positive.

These properties do NOT hold for classical memoryless channels.

Topic 2: A notion of non-commutative graph and a quantum Lovasz theta function.

Intuitive Meaning of Quantum Effect (i)

There is a class of quantum noisy channels of which a single use cannot transmit classical information exactly yet two uses can.



Entangled encoding enables perfect transmission of classical information.

This is NOT true for classical memoryless channels (Shannon, 1956).

Some Related Works

1. Basic Properties of zero-error capacity of quantum channels: Medeiros et al, arXiv, 2006; Beigi and Shor,arXiv, 2007. No entangled input states are allowed.

2. Entanglement between different uses enables perfect transmission of classical information (for multi-user quantum channels): Duan and Shi, PRL, 2008.

3. Super-activation of quantum capacity: Smith and Yard, Science, 2008.

4. Disprove the celebrated additivity conjecture: Hastings, Nat. Phys., 2009.

5. Strong Non-additivity of the private classical capacity: Li, Winter, Zou, and Guo, 2009; Smith and Smolin, arXiv, 2009.

6. Classical feedback increases the classical capacity of quantum channels : Smith and Smolin, 2009; (strong evidences provided in Bennett, Devetak, Shor, Smolin, PRL, 2006)

Classical Discrete Memoryless Channels (CDMC)

General Form of CDMC: $\mathcal{N}=(\mathcal{X},\{p(y|x)\},\mathcal{Y})$

Input letters: $\mathcal{X}=\{x_1,\cdots,x_n\}.$

Output letters: $\mathcal{Y}=\{y_1,\cdots,y_m\}.$

Transition Probability Matrix: $\sum_{y\in\mathcal{Y}} p(y|x)=1, \forall x\in\mathcal{X}, p(y|x)\geq 0.$

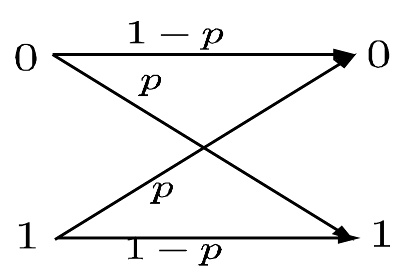
X: a probability distribution over input letters $\mathcal{X}$

Y: a probability distribution over output letters $\mathcal{Y}$

A positive linear transformation between probability distributions!

Binary Symmetric Channel:

Input letters $\{0,1\}$



Output letters $\{0,1\}$

Classical states vs. Quantum states

Pure states:

A finite set

$\mathcal{X} = \{1, \cdots, d\}$

$\text{Bit}: \{0, 1\}$

A finite-dimensional Hilbert space

$\mathcal{H} = \text{span}\{|1\rangle, \cdots, |d\rangle\}.$

$\text{Quantum Bit: } \alpha_0|0\rangle + \alpha_1|1\rangle$

$|\alpha_0|^2 + |\alpha_1|^2 = 1.$

Mixed (general) states:

$\mathcal{P}(\mathcal{X})$: probability distributions over $\mathcal{X}$.

$X \in \mathcal{P}(\mathcal{X}).$

Mixed bit: $(p, 1-p)$.

$\mathcal{B}(\mathcal{H})$: bounded linear operators over $\mathcal{H}$.

$\rho \in \mathcal{B}(\mathcal{H}), \rho \geq 0, \text{tr}\rho = 1.$

Mixed Qubit: $\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1| + a|0\rangle\langle 1| + a^*|1\rangle\langle 0|.$

Some Dirac notations:

$|\psi\rangle$: a column vector; $\langle\varphi|$: a row vector;

$\langle\psi|\varphi\rangle$: inner product between $|\psi\rangle$ and $|\varphi\rangle$; a scalar.

$|\psi\rangle\langle\varphi|$: outer product between $|\psi\rangle$ and $|\varphi\rangle$; a matrix.

$\langle\psi|A|\varphi\rangle$: inner product between $|\psi\rangle$ and $A|\varphi\rangle$.

$A^\dagger$: complex conjugate of A.

Composite Systems and Quantum Entanglement

Two classical systems: X £ Y = f(x; y) : x 2 X; y 2 Yg.

Two bits: f00, 01, 10, 11g

Two quantum systems: $\mathcal{H}_1 \otimes \mathcal{H}_2 = \mathrm{span}\{|k,l\rangle : |k\rangle \in \mathcal{H}_1, |l\rangle \in \mathcal{H}_2\}.$

Two qubits: jÃi = a_{00}j00i + a_{01}j01i + a_{10}j10i + a_{11}j11i .

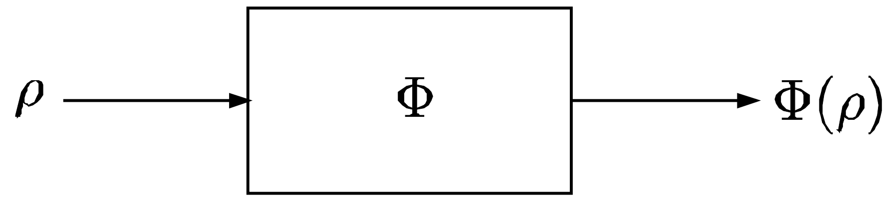
ja_{00}j^2 + ja_{01}j^2 + ja_{10}j^2 + ja_{11}j^2 = 1.

Entangled states (Non-factorable states): $|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle.$

$$|\Phi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Entangled state is a valuable resource for quantum information processing.

Quantum Memoryless Noisy Channels



Any quantum channel $\Phi: B(H_{d_1}) \to B(H_{d_2})$ has the following Kraus representation:

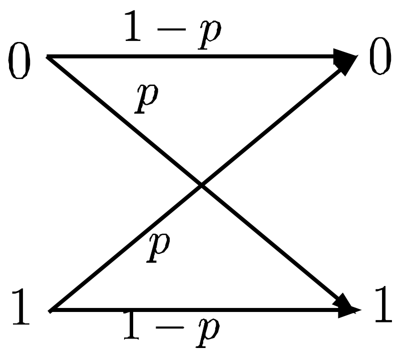
$$\Phi(\rho) = \sum_{k=1}^{N} E_k \rho E_k^{\dagger}.$$

1. E_k are linear operators from H_{d_1} to H_{d_2}, i.e., $d_2 \times d_1$ matrices, represent ambient noises applied to ρ.

2. $\sum_{k=1}^{N} E_k^{\dagger} E_k = I_{d_1}$ to guarantee trace-preserving, i.e., $tr(\Phi(\rho)) = tr(\rho)$.

The most general form of physically realizable operations allowed by quantum mechanics.

Classical DMC as Special Quantum Channels



$$\Phi(\rho) = \mathrm{tr}(\rho|0\rangle\langle 0|)\rho_0 + \mathrm{tr}(\rho|1\rangle\langle 1|)\rho_1;$$

$$\rho_0 = (1-p)|0\rangle\langle 0| + p|1\rangle\langle 1|;$$

$$\rho_1 = (1-p)|1\rangle\langle 1| + p|0\rangle\langle 0|.$$

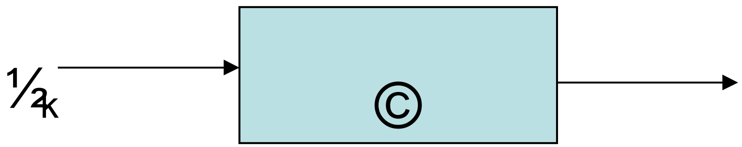
$$\mathcal{N} = (\mathcal{X}, \{p(y|x)\}, \mathcal{Y})$$

$$\Phi(\rho) = \sum_{x\in\mathcal{X}} \mathrm{tr}(|x\rangle\langle x|\rho)\rho_x,$$

$$\rho_x = \sum_{y\in\mathcal{Y}} p(y|x)|y\rangle\langle y|.$$

Criterion for Distinguishability

Definition: Two states ρ_0 and ρ_1 are said to be exactly distinguishable if there exists a quantum channel(operation) Φ such that $\Phi(\rho_0) = |0\rangle\langle 0|$ and $\Phi(\rho_1) = |1\rangle\langle 1|$.



$\Phi(\rho_k) = |k\rangle\langle k|;\ k = 0; 1$

Theorem: Two states ρ_0 and ρ_1 are exactly distinguishable if and only if they are orthogonal, i.e., $\rho_0 \perp \rho_1$, or equivalently $\rho_0\rho_1 = 0$.

Definition of Zero-Error Capacity

The one-shot zero-error capacity (or quantum independent number) of a quantum channel $\mathcal{E}$, denote as $\alpha(\mathcal{E})$, is the maximum integer n that there exists states $\rho_1, \cdots, \rho_n$ such that $\mathcal{E}(\rho_1), \cdots, \mathcal{E}(\rho_n)$ are pairwise orthogonal (thus distinguishable). (Medeiros et al, 2006; Beigi and Shor, 2007).

A single use of $\mathcal{E}$ can transmit $\alpha(\mathcal{E})$ messages exactly.

The (asymptotic) zero-error classical capacity of $\mathcal{E}$, denoted by $\Theta(\mathcal{E})$, is defined as follows:

$$\Theta(\mathcal{E}) = \sup_{k\geq 1}[\alpha(\mathcal{E}^{\otimes k})]^{\frac{1}{k}}.$$

A single use of $\mathcal{E}$ can asymptotically transmit $\Theta(\mathcal{E})$ messages exactly.

Remarks: If measure in bits, we have $C_0(\mathcal{E}) = \log_2 \Theta(\mathcal{E})$. But $\Theta(\mathcal{E})$ is more convenient and intuitive. Sometimes we are also interested in $Q_0(\mathcal{E})$, the zero-error quantum capacity of $\mathcal{E}$.

Classical Case: Shannon Capacity of a Graph

Given a CDMC $\mathcal{N} = (\mathcal{X}, \{p(y|x)\}, \mathcal{Y})$

The reachable set of an input letter x: $R(x) = \{y \in \mathcal{Y} : p(y|x) > 0\}.$

x and x' are adjacent (or confusable): $x \sim x' \Leftrightarrow R(x) \cap R(x') \neq \emptyset.$

The confusability graph is given as follows:

$$G(\mathcal{N}) = (V, E), V = \mathcal{X}, E = \{(x, x') : x \sim x'\}.$$

We also have $G(\mathcal{N}_0 \otimes \mathcal{N}_1) = G(\mathcal{N}_0) \otimes G(\mathcal{N}_1).$

Theorem (Shannon, 1956): The zero-error capacity of a CDMC is completely determined by the independent number of its confusability graph.

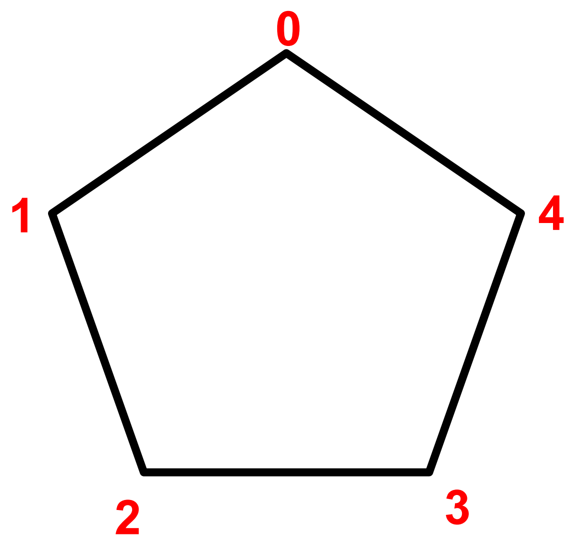
One-shot zero-error capacity: $\alpha(\mathcal{N}) = \alpha(G(\mathcal{N})).$

Asymptotic zero-error capacity: $\Theta(\mathcal{N}) = \sup_{k \geq 1} [\alpha(G(\mathcal{N}^{\otimes k}))]^{\frac{1}{k}}.$

A connection between zero-error information theory and graph theory!

A Classic Example: Pentagon Channel

The Pentagon Channel C_5 (Shannon,1956):



$$\alpha(C_5) = 2, \text{ code}: \{0, 2\}$$

$$\alpha(C_5^{\otimes 2}) = 5, \text{ code}: \{00, 12, 24, 31, 43\}$$

$$\text{Thus } \Theta(C_5) \geq \sqrt{5}.$$

In 1979 (23 years later!) it was finally confirmed by Lovasz using the celebrated theta function named after him that

$$\Theta(C_5) = \sqrt{5}.$$

The zero-error capacity of other odd cycles C_{2n+1} and their graph complements for n>2 are still widely open!!!

Quantum Case: Feasibility of Zero-Error Communication

A subset $S \subset \mathcal{B}(\mathcal{H})$ is said to **be extendible** if the orthogonal complement $S^{\perp}$ (in the sense of Hilbert-Schmidt) contains **an element with matrix rank one.** Otherwise S is said to **be an unextendible bases (UB).**

$$\mathcal{E}(\rho) = \sum_{k=1}^{N} E_k \rho E_k^{\dagger}, \quad \sum_{k=1}^{N} E_k^{\dagger} E_k = I_d.$$

Lemma 1: $\alpha(\mathcal{E}) > 1$ **iff** $\mathcal{K}(\mathcal{E}) = \mathrm{span}\{E_k^{\dagger} E_j\}$ **is extendible.**

Proof. K(E) is extendible is equivalent to the existence of a rank-one matrix jÃ$_0$ihÃ$_1$j such that tr(E$_k^y$E$_j$ jÃ$_0$ihÃ$_1$j) = 0, or equivalently,

hÃ$_0$jE$_k^y$E$_j$ jÃ$_1$i = 0;

which is exactly E(jÃ$_0$ihÃ$_0$j) ? E(jÃ$_1$ihÃ$_1$j).

Remark 1. The same result has been obtained previously (Beigi and Shor, 2007), but the connection with UB was not mentioned there.

Remark 2. The zero-error capacity of E is completely determined by the matrix subspace K(E).

Characterization of $K(E)$

Question Given a matrix subspace S on $B(H_d)$, when there is a quantum channel E such that $S = K(E)$?

Lemma 2 Given a matrix subspace S on $B(H_d)$, there is a quantum channel E such that $S = K(E)$ iff S satisfies i) $S^\dagger = S$ and ii) $I_d \in S$.

Remarks:

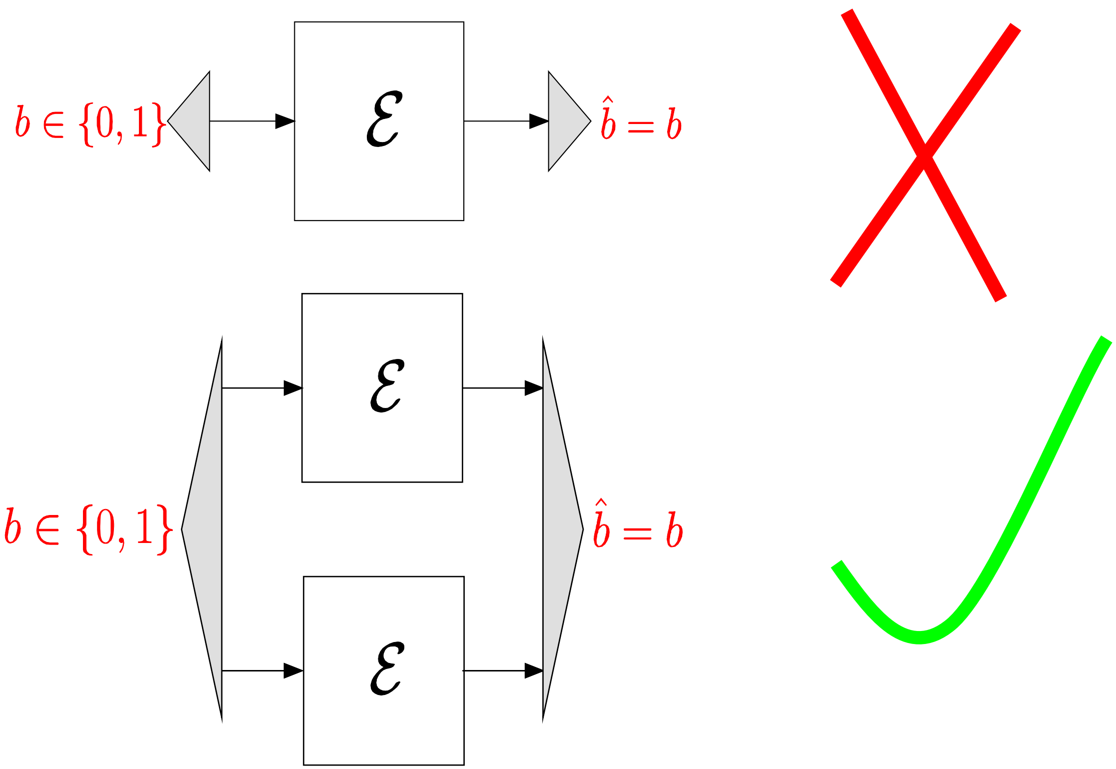
1.Lemma 2 greatly simplifies the study of zero-error capacity of quantum channels.

2.It suggests a non-commutative version of classical graphs.

3. Any subspace S satisfying the conditions i) and ii) is precisely an operator system in operator algebras.

Quantum Effect (i)

Theorem 1 There is quantum channel E such that ®(E) = 1 and £(E) > 1.



For any classical discrete memoryless channel N, £(N) = 1 i®®(N) = 1. (1956, Shannon).

Quantum Effect (i) (cont.)

Proof Outline:

1. We only need to construct two quantum channels E_0 and E_1 such that ®(E_0) = ®(E_1) = 1 and ®(E_0 - E_1) > 1. Choose E = E_0 © E_1. Then ®(E) = 1 and ®($E^{-\ 2}$) > 1:

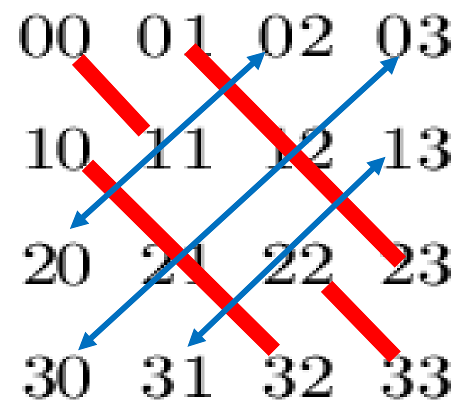
2. By Lemmas 1 and 2, the problem is reduced to ¯nd two matrix subspaces S_0 and S_1 such that a) S_0 and S_1 are unextendible; b) S_0 - S_1 is extendible; c) there are quantum channels E_0 and E_1 such that S_0 = K(E_0) and S_1 = K(E_1).

3. S_0 and S_1 satisfy a) and b) can be constructed easily by employing the techniques in previous works (Duan and Shi, 2008). Part c) is equivalent to further enforce S_0 and S_1 satisfy S_k^y = S_k and I_d 2 S_k, k = 0; 1.

An explicit construction for d=4

Let S_0 be a matrix subspace spanned by the following matrix bases:

$$
\begin{aligned}
F_1 &= |0\rangle\langle 0| + |1\rangle\langle 1|;\\
F_2 &= |2\rangle\langle 2| + |3\rangle\langle 3|;\\
F_3 &= |2\rangle\langle 0| - |0\rangle\langle 2|;\\
F_4 &= |3\rangle\langle 0| + |0\rangle\langle 3|;\\
F_5 &= |1\rangle\langle 3| + |3\rangle\langle 1|;\\
F_6 &= \cos\theta|0\rangle\langle 1| + \sin\theta|2\rangle\langle 3| - |1\rangle\langle 2|;\\
F_7 &= \cos\theta|1\rangle\langle 0| + \sin\theta|3\rangle\langle 2| - |2\rangle\langle 1|;\\
F_8 &= \sin\theta|0\rangle\langle 1| - \cos\theta|2\rangle\langle 3| + \sin\theta|1\rangle\langle 0| - \cos\theta|3\rangle\langle 2|;
\end{aligned}
$$

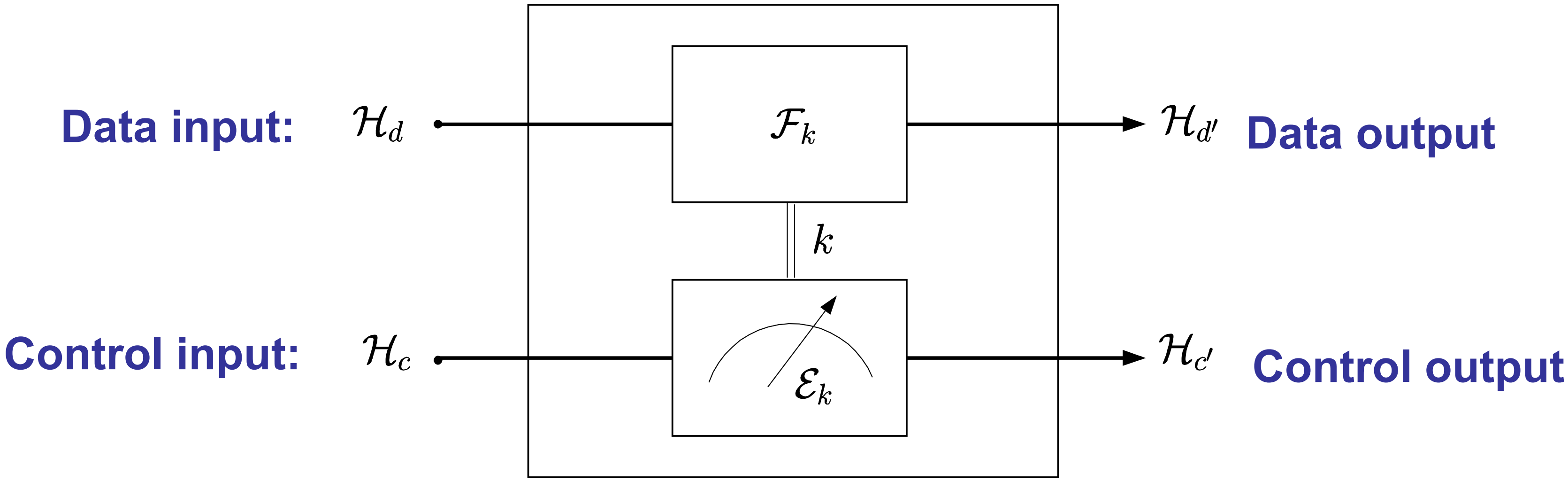


where $0 < \theta < \pi/2$ is a parameter. Let $U = |0\rangle\langle 0| - |1\rangle\langle 1| + |2\rangle\langle 2| - |3\rangle\langle 3|$, and let $S_1 = US_0^{\perp}$, where $S_0^{\perp}$ is the orthogonal complement via Hilbert-Schmidt inner product. (Construction based on: Duan and Shi, 2008)

a) and b) need a tedious but routine calculation. (details omitted)

c) is by inspection.

A special class of quantum channels



$$\mathcal{E} = \sum_{k=1}^{N} \mathcal{E}_k \otimes \mathcal{F}_k;$$

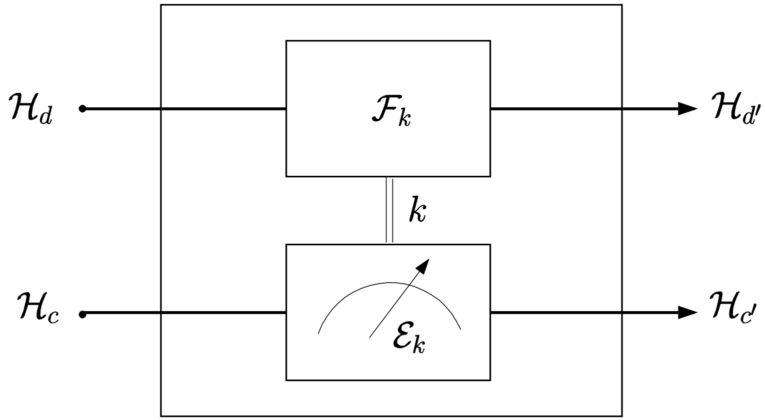
where both $\mathcal{E}_k$ and $\mathcal{F}_k$ are super-operators. Usually we choose $\{\mathcal{F}_k\}$ to be a set of quantum operations and $\{\mathcal{E}_k\}$ is a quantum measurement, i.e., $\sum_{k=1}^{N} \mathcal{E}_k$ is trace-preserving.

A special class of quantum channels (cont.)

Data input:

Alice:

Control input:



Data output

Bob

Control output

$$\mathcal{E} = \sum_{k=1}^{N} \mathcal{E}_k^{(control)} \otimes \mathcal{F}_k^{(data)};$$

Basic Property: If the receiver Bob can distinguish between $\{\mathcal{E}_k\}$, he will be able to infer the hidden measurement outcome k. Thus the net effect of the channel $\mathcal{E}$ will reduce to one of $\{\mathcal{F}_k\}$. In the case that $\mathcal{F}_k$ has a large amount of classical or quantum capacity, $\mathcal{E}$ will also have large capacity.

A generalization of the retro-correctible channels (Bennett, Devtak, Shor, Smolin, 2006)

Quantum effect (ii): Strong Super-additivity

Theorem 2. There is quantum channel $\mathcal{E}$ with input state space $\mathcal{B}(\mathcal{H}_2 \otimes \mathcal{H}_d)$ such that $C^{(0)}(\mathcal{E}) = 0$ and $Q^{(0)}(\mathcal{I}_2 \otimes \mathcal{E}) = \log_2 d \gg C^{(0)}(\mathcal{I}_2) + C^{(0)}(\mathcal{E}) = 1$, where $\mathcal{I}_2$ is the noiseless qubit channel.

$$0 + 1 \gg 1$$

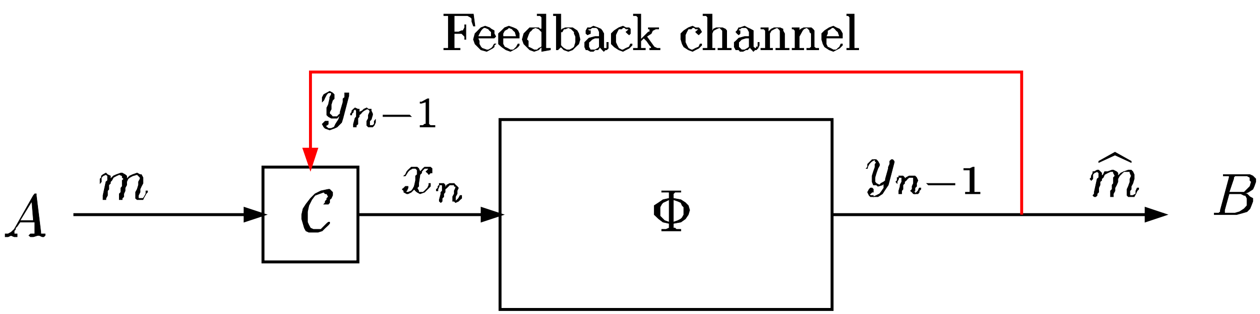
Proof Ideas. The crucial point is to construct the following channel:

$$\mathcal{E} = \frac{1}{\sqrt{N}} \sum_{k=1}^{N} (\mathcal{E}_{k0} \otimes I_d + \mathcal{E}_{k1} \otimes U_k)$$

where $\mathcal{E}_{k0} = \{|k\rangle\langle\psi^*_{k0}|\}$, $\mathcal{E}_{k1} = \{|k\rangle\langle\psi^*_{k1}|\}$, $\{|\psi_{k0}\rangle, |\psi_{k1}\rangle\}$ is an orthogonal basis for $\mathcal{H}_2$, "$*$" is the complex conjugate according to $\{|0\rangle, |1\rangle\}$, and $\{U_k\}$ is a set of unitary operations on $\mathcal{H}_d$.

Quantum effect (iii): Auxiliary resources

We can further show that auxiliary resources such as shared entanglement (more later), classical and quantum feedbacks can either simplify the feasibility problem greatly, or increase the capacity dramatically.



$$x_n = f(m, y_{n-1})$$

Communication with a classical feedback channel

Theorem 3. There is a quantum channel E from $B(H_2)$ to $B(H_2 \otimes H_4)$ such that $C^{(0)}(E) = 0$ and $C^{(0)}_{cf\,b}(E)$ ¸ $Q^{(0)}_{cf\,b}(E) > 0$, where \cfb means classical feedback.

Open Problems and Recent Progresses

Problem 1: There are quantum channels E_0 and E_1 such that $C^{(0)}(E_0) = C^{(0)}(E_1) = 0$ and $C^{(0)}(E_0 \otimes E_1) > 0$.

Problem 2: There are quantum channels E_0 and E_1 such that $C^{(0)}(E_0) = C^{(0)}(E_1) = 0$ and $Q^{(0)}(E_0 \otimes E_1) > 0$.

Note added: In their independent work (arXiv: 0906.2547) Cubitt, Chen, and Harrow have obtained some interesting results about zero-error capacity that partially overlap our main Result 1. Most notably, they have resolved the above open problem 1 (and in a later work problem 2). **However, explicit constructions are still unknown.**

Non-Commutative Graphs and Zero-Error Communication

We can introduce more notions of capacities for zero-error communication by consider the type of information (quantum or classical) we are interested in or the auxiliary resources that might be available (classical feedback, quantum feedback, and shared entanglement, etc).

Entanglement-assisted zero-error classical capacity of quantum channels: Alice and Bob can make use of (pre-shared) entanglement for communication

One-shot ent-assisted zero-error classical capacity: $\alpha_E(\mathcal{E})$

Asymptotic ent-assisted zero-error classical capacity : $\Theta_E(\mathcal{E})$

In bits, $C_{0,E}(S) = \log_2 \Theta_E(S)$

Key observation: All these quantities only depend on $\mathcal{K}(\mathcal{E})$. In general, almost known quantities of zero-error communication only depends on $\mathcal{K}(\mathcal{E})$. Thus we can focus on non-commutative graphs rather than actual channels.

A quantum Lovasz theta function

Let S be a non-commutative graph (operator system) over a d-dimensional Hilbert space. A direct (somehow native) generalization of Lovasz theta function is the following:

$$\vartheta(S) = \sup_{I_d+X\geq 0, X\in S^\perp} ||I_d + X||.$$

Not well-behaved:

$$\vartheta(I_d) = d,\ \vartheta(\mathcal{B}(\mathcal{H}_d)) = 1,\ \text{but}\ \vartheta(I_d \otimes \mathcal{B}(\mathcal{H}_d)) = d^2.$$

A "correct" version (similar to the idea of completely bounded norm):

$$\tilde{\vartheta}(S) = \sup_{n\geq 1} \vartheta(S \otimes \mathcal{B}(\mathcal{H}_n)).$$

Duan, Severini, and Winter, 2010, arXiv: 1002.2514; also ISIT 2011.

A Quantum Lovasz theta function

$\tilde{\vartheta}(\cdot)$ **satisfies a number of natural properties that we are expecting for a "Quantum Lovasz theta function":**

Theorem (Duan, Severini, and Winter, 2010): Let S, S_0, S_1 be non-commutative graphs (operator systems). Then the following hold:

1. Semi-definite programming characterization. In particular, we have

$$\tilde{\vartheta}(S) = \min ||\mathrm{Tr}_A Y||, \text{ st } Y \in S \otimes \mathcal{B}(\mathcal{H}_{A'}), Y \geq \Phi, \quad \text{where } |\Phi\rangle = \sum_{k=1}^{d} |k\rangle_A |k\rangle_{A'}.$$

2. Multiplicativity under tensor product: $\tilde{\vartheta}(S_0 \otimes S_1) = \tilde{\vartheta}(S_0) \times \tilde{\vartheta}(S_1).$

3. Upper bound for ent-assisted zero-error capacity: $C_{0,E}(S) \leq \log_2 \tilde{\vartheta}(S).$

4. Consistent with Lovasz theta function for classical graphs: $\tilde{\vartheta}(G) = \vartheta(G).$

Combining 3 and 4, we have:

$$C_0(G) \leq C_{0,E}(G) \leq \log_2 \vartheta(G).$$

The first inequality can be strict (Leung et al, 2011), and the second inequality was obtained independently by Beigi (arXiv: 1002.2488).

Some Questions

1. Is it true that $\tilde{\vartheta}(S_0 \cap S_1) \leq \tilde{\vartheta}(S_0) \times \tilde{\vartheta}(S_1)$? This is true for classical G_0 and G_1.

2. Do we have the equality $C_{0,E}(S) = \log_2 \tilde{\vartheta}(S)$ for general non-commutative graph S? In particular, do we have $C_{0,E}(G) = \log_2 \vartheta(G)$ for any classical graph G?

3. A more complete theory for non-commutative graphs? (For instance, how to define natural notions of perfect graphs, chromatic number, etc. (Duan, Severini, Winter, and Paulsen, work in progress).

Thank you for your attention!