Quantum information theory with functional analysis techniques: Lecture 1

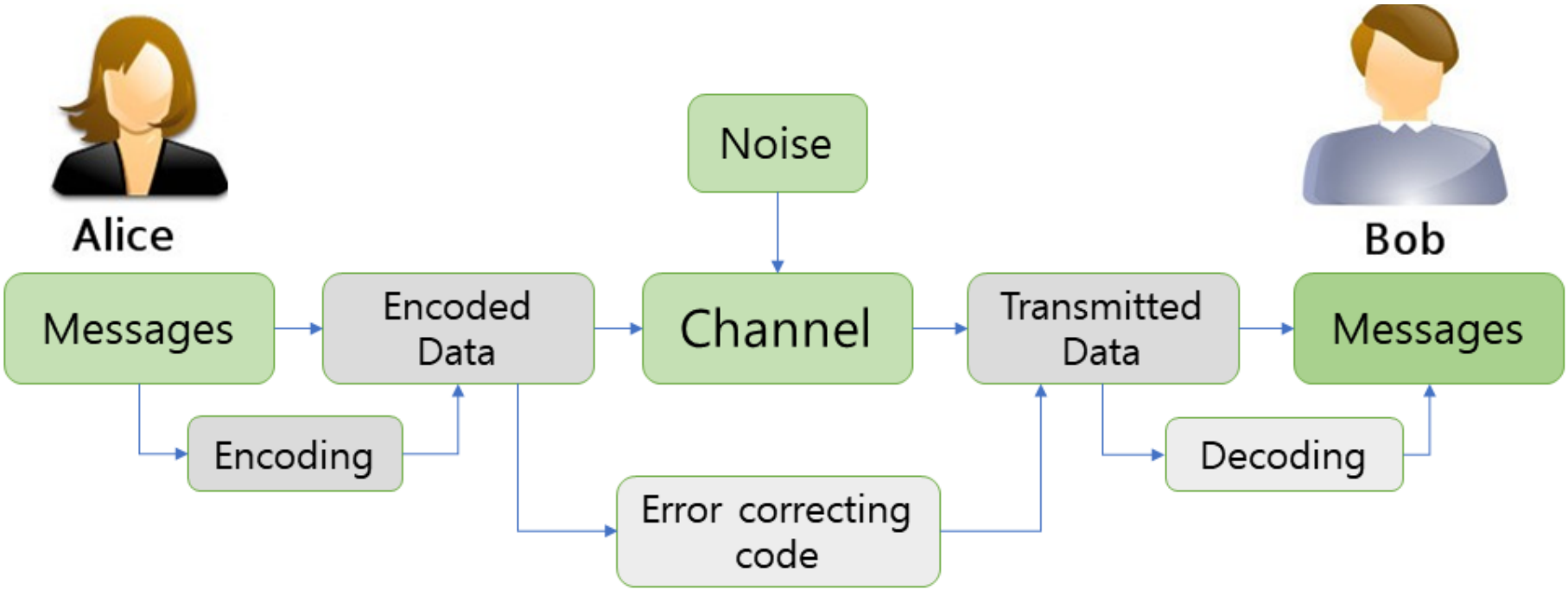
Hun Hee Lee
Seoul National University

SNU, December 18th - 21st, 2018

Table of contents

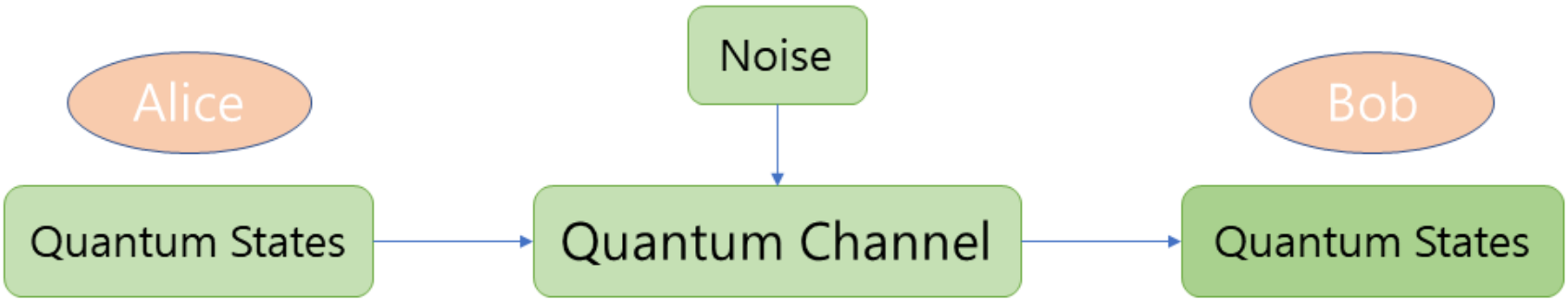
Alice and Bob

- Information theory studies the quantification, storage, and communication of information, which was originally proposed by Claude E. Shannon in 1948 (from Wikipedia).



Alice and Bob: continued

- Information theory has a quantum counterpart called Quantum Information Theory (shortly, QIT).



- QIT serves as a background theory for Quantum Computing(양자컴퓨팅)/Quantum Cryptography(양자암호)

Quantum Computer

Quantum Computer: continued

- Quantum computers are machines that can run quantum algorithms, such as Shor's quantum integer factorization, '94 and Grover's quantum search, '96.
- (**Existing quantum computers**)
  by Google, IBM, Intel, Rigetti, D-wave.
- (**Reference on the current status**):
  John Preskill, Quantum Computing in the NISQ era and beyond, arXiv:1801.00862.

Quantum information theory for functional analysts

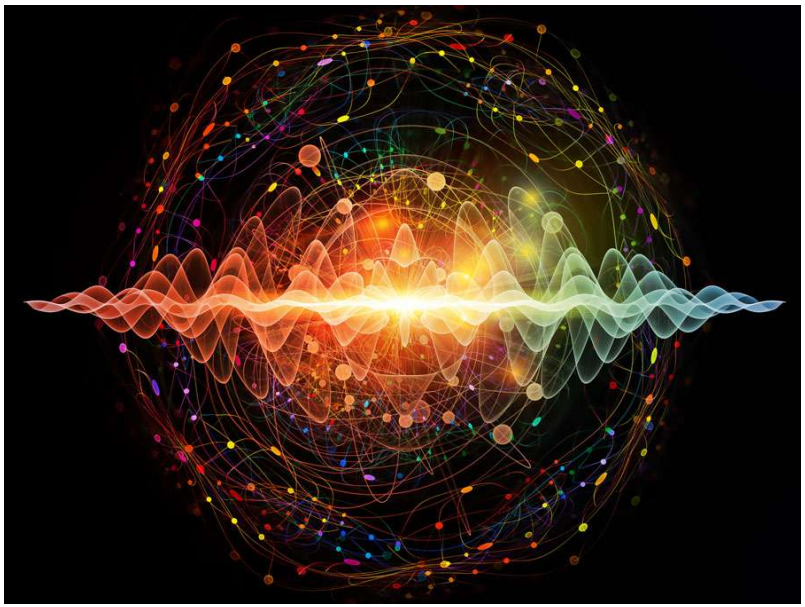
- Traditionally QIT preferred finite dimensional Hilbert spaces, so that linear algebras and matrix analysis were the main tools.
- Recently, many branches of functional analysis are being crucially used in QIT including Banach/operator space theory, operator system theory and quantum probability, which we will see in this series of lectures.

Postulates of Quantum Mechanics I

(P1)

Any *isolated* physical system is associated to a complex Hilbert space $\mathcal{H}$ called the state space

- The state of the system is described by a unit vector $\psi \in \mathcal{H}$, which is called the state vector.
- When $\dim\mathcal{H} = 2$ the system is called a qubit system.



Postulates of Quantum Mechanics II

Remark

We assume that $\mathcal{H}$ is finite dimensional unless specified.

Bra-ket notation

For $h \in \mathcal{H}$, $A \in B(\mathcal{H})$

- vector $|h\rangle \in \mathcal{H}$, functional $\langle h| \in \mathcal{H}^*$;
- $A|h\rangle \in \mathcal{H}$, $\langle h|A \in \mathcal{H}^*$ and $\langle h|A|h\rangle \in \mathbb{C}$.
- When $\mathcal{H} = \ell^2(I)$ we denote the canonical basis by $|i\rangle$, $i \in I$ and $|i\rangle\langle j|$ refers to the matrix unit in $B(\mathcal{H})$ usually denoted by e_i and e_{ij} in mathematics.

Postulates of Quantum Mechanics III

(P2)

A *discrete time* evolution of a closed quantum system is described by a unitary transformation, i.e. $|h\rangle \in \mathcal{H} \mapsto U|h\rangle \in \mathcal{H}$ for some $U \in \mathcal{U}(\mathcal{H})$.

Postulates of Quantum Mechanics IV

(P3)

We could *"read out"* quantum states only by quantum measurements.

- A quantum measurement is a family of operators $\{M_i\}_{i\in I} \subseteq B(\mathcal{H})$ satisfying $\sum_{i\in I} M_i^* M_i = I_{\mathcal{H}}$.
- The index $i \in I$ refers to the measurement outcome and we say that the probability $p(i)$ of the outcome being i after we apply the measurement to the state ψ is given by $\|M_i|\psi\rangle\|^2 = \langle\psi|M_i^* M_i|\psi\rangle$.

- $\sum_{i\in I} p(i) = \langle\psi| \sum_{i\in I} M_i^* M_i|\psi\rangle = \langle\psi|I_{\mathcal{H}}|\psi\rangle = \|\psi\|^2 = 1.$

Postulates of Quantum Mechanics V

(P3)-related

- $\{P_i = M_i^* M_i\}_{i \in I}$ is called a POVM (positive operator valued measure).
- (**Ex**) A POVM on $\mathcal{H} = \mathbb{C}^2$: $\{M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}$.
  The state $|\psi\rangle = a|0\rangle + b|1\rangle$ collapses into $\frac{a}{|a|}|0\rangle$ with prob. $|a|^2$ and into $\frac{b}{|b|}|1\rangle$ with prob. $|b|^2$ after the above measurement.
- After applying the measurement to the state ψ with the outcome i the state collapses to another state $\frac{M_i|\psi\rangle}{\|M_i|\psi\rangle\|}$.

Postulates of Quantum Mechanics VI

(P4)

The state space of a composite physical systems is the Hilbert space tensor product of the component state spaces.

- (**Ex**) Suppose we have the system A and B with the state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, then the composite system, which we denote by AB, has the state space $\mathcal{H}_A \otimes_2 \mathcal{H}_B$, which we denote by $\mathcal{H}_{AB}$.
- (**Def**) A state vector $|\psi\rangle \in \mathcal{H}_{AB}$ is called separable if $|\psi\rangle = |a\rangle \otimes |b\rangle$ for some $|a\rangle \in \mathcal{H}_A$ and $|b\rangle \in \mathcal{H}_B$. A non-separable state vector in $\mathcal{H}_{AB}$ is called entangled.

Extended Postulates I

- A state vector $h \in \mathcal{H} \Rightarrow$ an operator $|h\rangle\langle h|$ acting on $\mathcal{H}$, which we call a pure state.

(P1')

A *"state"* of a system is described by a mixed state

$$\rho = \sum_{i \geq 1} p_i |h_i\rangle\langle h_i|, \ \sum_i p_i = 1, \ p_i \geq 0,$$

which we interpret as the pure states $|h_i\rangle\langle h_i|$ being "mixed" with "probability" p_i.

- The state ρ is nothing but a positive matrix with trace 1 by spectral decomposition, which we call a density matrix.
- We denote the set of all density matrices on $\mathcal{H}$ by $\mathcal{D}(\mathcal{H})$.

Extended Postulates II

(P2')

Evolution on a closed system is given by unitary conjugations, i.e. $\rho \mapsto U\rho U^*$.

(P3')

For a POVM $(P_i)_{i\in O}$ we have

$$\text{the } \textit{"probability"} \text{ of outcome } i = \mathrm{Tr}(P_i\rho) = \langle \rho, P_i \rangle.$$

Extended Postulates III

Embedding of a quantum state

When a physical system, say A with the state space $\mathcal{H}_A$, is *"open"* we assume that it interacts with another system E (with the state space $\mathcal{H}_E$) called "environment". In this case we think the original system is "embedded" in the composite system AE by an isometry

$$V : |\psi\rangle \in \mathcal{H}_A \mapsto |\psi\rangle \otimes |\varphi\rangle \in \mathcal{H}_A \otimes_2 \mathcal{H}_E$$

for a fixed state vector $\varphi \in \mathcal{H}_E$. In the density operator level this becomes

$$\rho \in \mathcal{D}(\mathcal{H}_A) \mapsto \rho \otimes |\varphi\rangle\langle\varphi| \in \mathcal{D}(\mathcal{H}_A \otimes_2 \mathcal{H}_E).$$

Extended Postulates IV

Reduction

A density matrix $\sigma \in \mathcal{D}(\mathcal{H}_{AE})$ can be reduced to a density matrix σ_A by taking partial trace over the system E, i.e.

$$\sigma_A = I_A \otimes \mathrm{Tr}_E(\sigma) \text{ (simply denoted by } \mathrm{Tr}_E(\sigma)).$$

Purification

- For a density matrix $\rho \in \mathcal{D}(\mathcal{H}_A)$, a state vector $|v\rangle \in \mathcal{H}_{AB}$ is called a purification of ρ if $\mathrm{Tr}_B(|v\rangle\langle v|) = \rho$.
- The spectral decomposition $\rho = \sum_{k=1}^{d_A} \lambda_k |x_k\rangle\langle x_k|$ with an ONB $\{|x_k\rangle\}$ of $\mathcal{H}_A$ gives us the canonical purification $|v\rangle = \sum_{k=1}^{d_A} \sqrt{\lambda_k}|x_k\rangle \otimes |x_k\rangle \in \mathcal{H}_A \otimes_2 \mathcal{H}_A$.

Extended Postulates V

(P2") Quantum channels as generalized quantum evolutions

Evolution on an open quantum system is given by

$$\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B),\ \rho \mapsto (I_B \otimes \mathrm{Tr}_E)(U(\rho \otimes \rho_E)U^*)$$

for some environment $\mathcal{H}_E$, a state ρ_E on $\mathcal{H}_E$ and a unitary $U : \mathcal{H}_{AE} \to \mathcal{H}_{BE}$, which is nothing but a completely positive and trace-preserving linear map. We call it a quantum channel. We may also write (which is called the Stinespring representation)

$$\Phi(\rho) = I_B \otimes \mathrm{Tr}_E[V\rho V^*]$$

for the isometry

$$V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E,\ |\psi\rangle \mapsto U(|\psi\rangle \otimes |\varphi\rangle).$$

Extended Postulates VI

Remark

We "think" quantum channels describe all possible "noises" in quantum world!

Theory of completely positive maps I

Completely positive maps

(**Def**) A linear map $T : B(\mathcal{H}) \to B(\mathcal{K})$ is called completely positive (shortly, CP) if $I_n \otimes T : M_n(B(\mathcal{H})) \to M_n(B(\mathcal{K}))$ is positive for all $n \geq 1$.

Theory of completely positive maps II

Lemma

1. For a positive matrix $P \in B(\mathcal{H})$ the following map is CP.

$$T : \mathbb{C} \to B(\mathcal{H}),\ \alpha \mapsto \alpha \cdot P.$$

2. Let $T : B(\mathcal{H}) \to B(\mathcal{K})$ be a (completely) positive map. Then, the adjoint (via trace duality)

$$T^* : B(\mathcal{K}) \to B(\mathcal{H})$$

given by $\langle T^* Y, X \rangle := \langle Y, TX \rangle$, $X \in B(\mathcal{H})$, $Y \in B(\mathcal{K})$ is also (completely) positive.

3. The trace functional $B(\mathcal{H}) \to \mathbb{C},\ X \mapsto \mathrm{Tr}(X)$ is CP.

(Proof)

Theory of completely positive maps III

Various characterizations of completely positive maps

Let $T : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ be a linear map. Then, T.F.A.E.

1. T is CP.
2. T is n-positive, $(n = \dim\mathcal{H}_A = d_A)$ i.e. $I_n \otimes T : M_n(B(\mathcal{H}_A)) \to M_n(B(\mathcal{H}_B))$ is positive.
3. The Choi matrix $C_T = \sum_{i=1}^{n} T(|i\rangle\langle j|) \otimes |i\rangle\langle j| \in B(\mathcal{H}_B \otimes_2 \mathcal{H}_A)$ is positive.
4. (Kraus representation) $\exists\ \exists\ \{A_j : j \in J\} \subseteq B(\mathcal{H}_A, \mathcal{H}_B)$ such that $T(X) = \sum_{j\in J} A_j X A_j^*$.
5. (Stinespring representation) $\exists\ \mathcal{H}_C$ and $A \in B(\mathcal{H}_A, \mathcal{H}_{BC})$ such that $T(X) = \mathrm{Tr}_C(AXA^*)$.

(Proof)

Theory of completely positive maps IV

Choi rank

- (**Def**) The rank of the Choi matrix C_T is called the Choi rank.
- We may take $|J| = \dim \mathcal{H}_C =$ the Choi rank.

Quantum channels = CP trace preserving (CPTP) maps

A CP map T satisfies trace preserving property if and only if

- (Choi matrix) $\mathrm{Tr}_B(C_T) = I_A$.
- (Kraus representation) $\sum_{j \in J} A_j^* A_j = I_A$.
- (Stinespring representation) $A^* A = I_A$, i.e. an isometry.

Including Classical into Quantum I

Classical states

- (**Def**) Classical states are probability distributions on a finite set I.
- The set of all probability distributions on I will be denoted by $\mathcal{P}(I)$
- A classical state $(p_i)_{i\in I}$ can be understood as a quantum state acting on $\ell^2(I)$ as a diagonal matrix, namely $\mathrm{diag}(p_i)$.

Including Classical into Quantum II

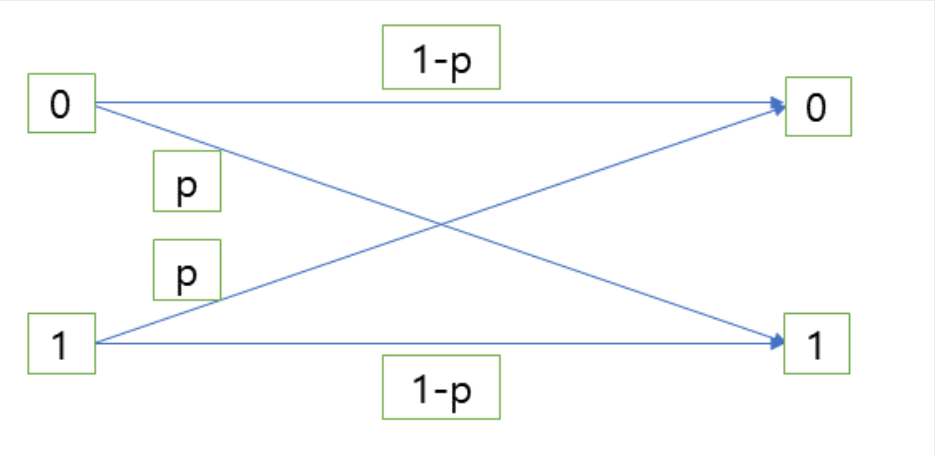
Classical channels

(**Def**) A classical (discrete and memoryless) channel consists of the input set **A**, the output set **B** and the map

$$\Phi : \mathbf{A} \to \mathcal{P}(\mathbf{B}),\ x \mapsto (p(y|x))_{y \in \mathbf{B}}.$$

Example: Binary symmetric channel

$\mathbf{A} = \mathbf{B} = \{0, 1\}$, $0 \leq p \leq 1$: the flipping probability



Including Classical into Quantum III

Correlation set

(**Notation**) We denote the set of all classical channels from **A** into **B** by $\mathcal{P}(\mathbf{B}|\mathbf{A})$.

Remarks

- The ideal situation for communication is "Alice and Bob agree on what was sent" $\Rightarrow$ Channels represents all possible noises.
- We assume that the relationship between the output $y \in \mathbf{B}$ given the input $x \in \mathbf{A}$ is described probabilistically, or more precisely by its "conditional probability" $p(y|x)$.

Including Classical into Quantum IV

Classical channels as quantum channels

For a classical channel $\Phi : \mathbf{A} \to \mathcal{P}(\mathbf{B}),\ x \mapsto (p(y|x))_{y\in\mathbf{B}}$ we can associate a quantum channel

$$\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B),\ e_{xx'} \mapsto \delta_{x,x'}\mathrm{diag}(p(y|x))_{y\in\mathbf{B}}.$$

We use the same symbol Φ by abuse of notation and this is usually called as a classical-classical channel.

Examples of quantum channels I

Classical-quantum channel

(**Def**) A classical-quantum channel is a map

$$\Phi : \mathbf{A} \to \mathcal{D}(\mathcal{H}_{\mathbf{B}}),\ x \mapsto \rho_x,$$

where the associated quantum channel is

$$\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B),\ e_{xx'} \mapsto \delta_{x,x'}\rho_x.$$

We sometimes call it a classical-quantum coding.

Examples of quantum channels II

Quantum-classical channel and quantum measurement

- Let $\{M_i\}_{i\in I} \subseteq B(\mathcal{H})$ be a quantum measurement. Then, we can associate two types of quantum channels.
- The first one is

$$\Psi : B(\mathcal{H}) \to B(\mathcal{H}), \quad \rho \mapsto \sum_i \mathrm{Tr}(M_i \rho M_i^*) \frac{M_i \rho M_i^*}{\mathrm{Tr}(M_i \rho M_i^*)},$$

  which describes the after-effect of measurement as in (P3').
- The second one is the following "quantum-classical channel":

$$\Phi : B(\mathcal{H}) \to \mathcal{P}(I) \subseteq B(\ell^2(I)), \ \rho \mapsto \sum_i \mathrm{Tr}(M_i \rho M_i^*) |i\rangle\langle i|.$$

- $\Psi = \Phi$ when M_i's have 1 dimensional orthogonal ranges with $\dim\mathcal{H} = |I|$.

Examples of quantum channels III

Further examples of quantum channels

- (Random unitary channel) For a family of unitaries $\{U_i\}_{i\in I} \subseteq B(\mathcal{H})$ we consider

$$\Phi : B(\mathcal{H}) \to B(\mathcal{H}),\ X \mapsto \frac{1}{|I|}\sum_{i\in I} U_i X U_i^*.$$

- (Isometry channel) For an isometry $V : \mathcal{H}_A \to \mathcal{H}_B$

$$\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B),\ X \mapsto VXV^*.$$

Examples of quantum channels IV

Further examples of quantum channels 2

- (Replacement channel) For a fixed state $\rho \in B(\mathcal{H}_B)$

$$\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B),\ X \mapsto \mathrm{Tr}(X)\rho.$$

  When $\rho = \frac{I_A}{d_A}$, we call it the completely depolarizing channel.
- (Completely dephasing channel)

$$\Phi : B(\mathcal{H}) \to B(\mathcal{H}),\ X \mapsto \sum_{i=1}^{\dim\mathcal{H}} X_{ii}|i\rangle\langle i|.$$

Examples of quantum channels V

More on completely depolarizing channel

- (Discrete Weyl operators) For $\mathcal{H} = \ell^2_n = \ell^2(\mathbb{Z}_n)$ with $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$. We define two operators on $\mathcal{H}$ as follows: $U := \sum_{c \in \mathbb{Z}_n} |c+1\rangle\langle c|$ and $V := \sum_{c \in \mathbb{Z}_n} z^c |c\rangle\langle c|$, where $z = \exp(\frac{2\pi i}{n})$.
- For $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n$ we also define

$$W_{a,b} : U^a V^b.$$

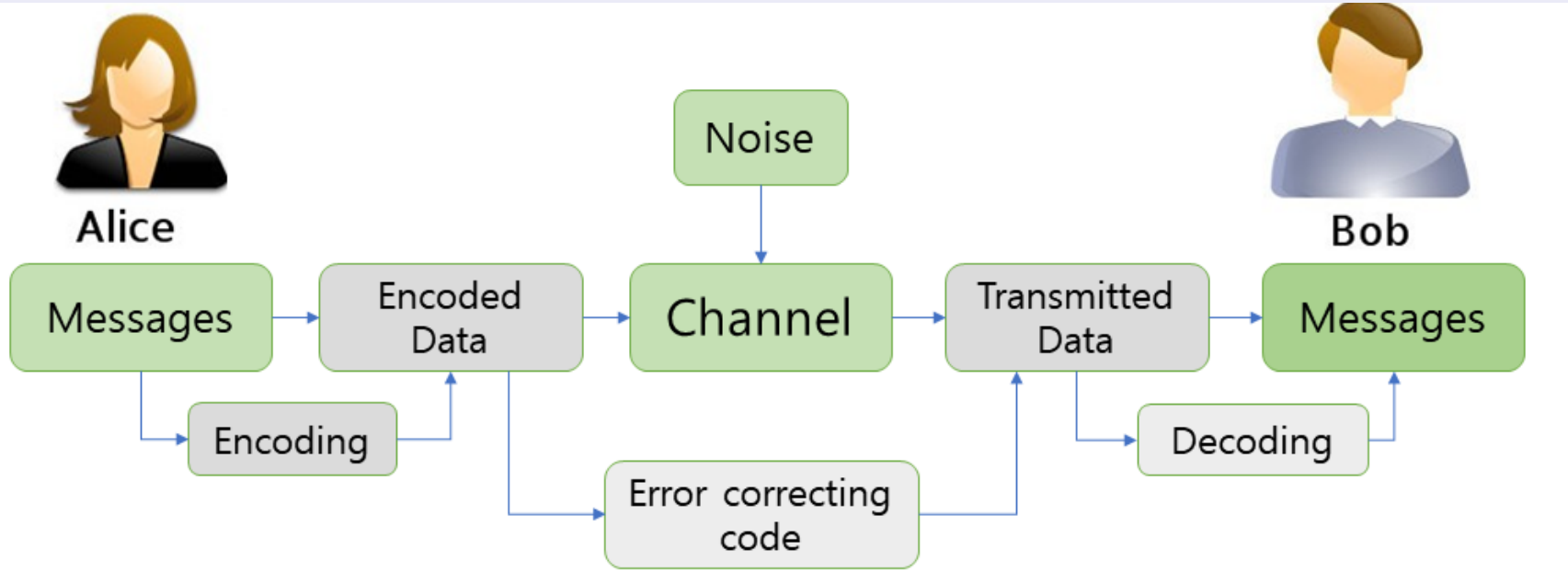
- (Completely depolarizing channel) For $X \in B(\mathcal{H})$ we have

$$\frac{1}{n^2} \sum_{a,b \in \mathbb{Z}_n} W_{a,b} X W_{a,b}^* = \frac{\mathrm{Tr}(X)}{n} I_{\mathcal{H}}.$$

In other words, completely depolarizing channels are random unitary channels.

Basic concepts of information theory I

Communication Scenario



Alice and Bob are communicating using a classical channel

$$\Phi : \mathbf{A} \to \mathcal{P}(\mathbf{B}),\ x \mapsto (p(y|x))_{y \in \mathbf{B}}.$$

Basic concepts of information theory II

Classical state as a random source

A classical state in Alice side will be a probability distribution on **A**(or a random variable with **A**-values) describing randomly arriving messages.

The Shannon entropy

(**Def**) The Shannon entropy $H(X)$ of random variable $X : (\Omega, P) \to \{1, \cdots, n\}$ is defined by

$$H(X) := -\sum_{i=1}^{n} p_i \log p_i = H(p_1, \cdots, p_n),$$

where $p_i = P(X = i)$ satisfying $p_i \geq 0$, $\sum_{i=1}^{n} p_i = 1$.

Basic concepts of information theory III

Exercise

In the above case we have

$$0 \leq H(X) \leq \log n.$$

The Shannon entropy: interpretation

- The Shannon entropy $H(X) = -\sum_{i=1}^{n} p_i \log p_i$ is understood as the average information after we learn the value of X or the average uncertainty before we learn the value of X.
- High probability $\approx$ less surprise $\approx$ less valuable information.
- (**Ex**) Uniform distribution $(\frac{1}{n}, \cdots, \frac{1}{n}) \Rightarrow$ max entropy $\log n$
  Point mass $(1, 0, \cdots, 0) \Rightarrow$ min entropy 0.

Basic concepts of information theory IV

The Source coding theorem

- Let X be a random message source (i.e. a prob. dist. p on I). For $n \in \mathbb{N}$, $\alpha > 0$, $0 < \delta < 1$ an (n, α, δ)-coding for X refers to an encoding $f : I^n \to \{0,1\}^{\lfloor \alpha n \rfloor}$, a decoding $g : \{0,1\}^{\lfloor \alpha n \rfloor} \to I^n$ such that $P(\{A \in I^n : g(f(A)) = A\}) > 1 - \delta$, where $P = p \times \cdots \times p$, which means we use X independently n-times.
- (**Shannon's source coding theorem**)
  - If $\alpha > H(X)$, then $\exists$ (n, α, δ)-coding for X eventually for $n \in \mathbb{N}$.
  - If $\alpha < H(X)$, then $\exists$ (n, α, δ)-coding for X at most finitely many $n \in \mathbb{N}$.
- (**Meaning of entropy**) We can say that we need $H(X)$-bits per one letter to encode a random message from X in average.

Basic concepts of information theory V

Joint entropy and mutual information

For two random variables $\begin{cases} X : (\Omega, P) \to \{1, \cdots, n\}, \\ Y : (\Omega, P) \to \{1, \cdots, m\} \end{cases}$ we can associate another random variable $(X, Y) : (\Omega, P) \to \{1, \cdots, n\} \times \{1, \cdots, m\}$.

- The entropy $H(X, Y)$ of (X, Y) is called the joint entropy of X and Y.
- The mutual information of X and Y is defined by

$$I(X; Y) := H(X) + H(Y) - H(X, Y).$$

- $I(X; Y)$ quantifies the "information that X and Y share". In other words, how much knowing one of these variables reduces uncertainty about the other.

Basic concepts of information theory VI

Channel capacity

(**Def**) The channel capacity $C(\Phi)$ of a given channel Φ is defined by

$$C(\Phi) := \sup_{\text{prob. dist. } X \text{ on } A} I(X;Y).$$

- (**Ex**) Binary symmetric channel: $C(\Phi) = 1 - H(p, 1-p)$, where $H(p, 1-p)$ is the binary entropy function.

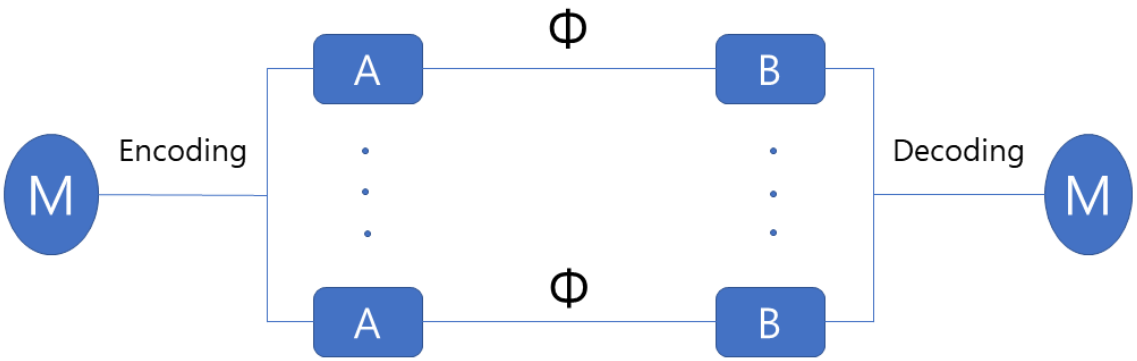
Basic concepts of information theory VII

Multiple use of channels

- (**Scenario**) Use the same channel Φ repeatedly (n-times) and independently to send a message from $M = \{1, \cdots, N\}$.
- More precisely, we consider the classical channel

$$\Phi^n : \mathbf{A}^n \to \mathcal{P}(\mathbf{B}^n),\ (x_1, \cdots, x_n) \mapsto \Phi(x_1) \times \cdots \times \Phi(x_n),$$

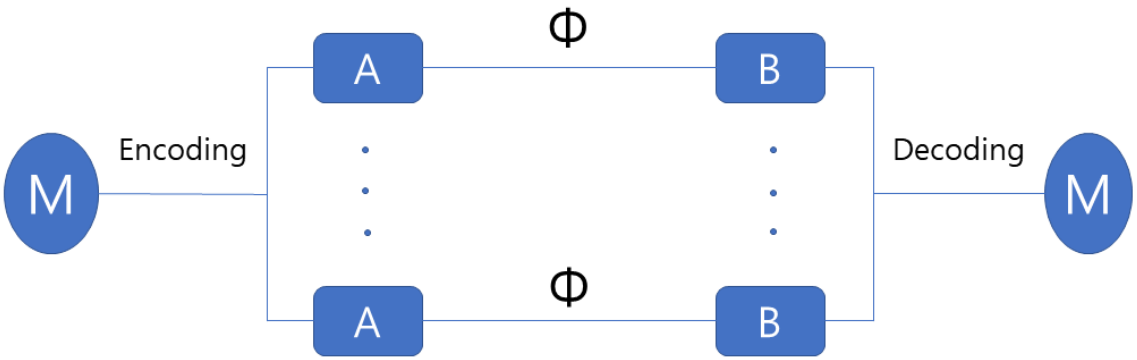
where the latter means the product of measure, which implies that we are assuming independency.



Basic concepts of information theory VIII

Codings

- (**Def**) An (N, n)-coding for the channel Φ consists of encoding $f : M = \{1, \cdots, N\} \to \mathbf{A}^n$ and decoding $g : \mathbf{B}^n \to M$.
- We define the transmission rate to be $\dfrac{\log N}{n}$.
- We also define the maximum error probability $P_{e,\max} := \max\limits_{1 \le i \le N} P(g(Y^n) \neq i | X^n = f(i))$.



Basic concepts of information theory IX

Shannon's channel coding theorem

- (**Def**) We say that $R > 0$ is an achievable rate if $\exists$ (N, n)-coding's whose transmission rate is R such that $\lim_{n\to\infty} P_{e,\max} = 0$.
- This means that we can send R-bits per one use of the channel in average.
- (**Shannon's channel coding theorem**)

$$C(\Phi) = \sup R.$$

Basic concepts of information theory X

Zero error capacity

- (**Def**) We say that an (N, n)-coding is zero error if $P_{e,\max} = 0$.
- The zero error capacity $C_0(\Phi)$ of a channel Φ is the supremum of $R > 0$ such that $\exists$ a zero error (N, n)-coding for Φ.
- The one-shot zero error capacity $C_0^1(\Phi)$ of a channel Φ is the supremum of $R > 0$ such that $\exists$ a zero error $(N, 1)$-coding for Φ.

Thank you for your attention!

Quantum information theory with functional analysis techniques: Lecture 2

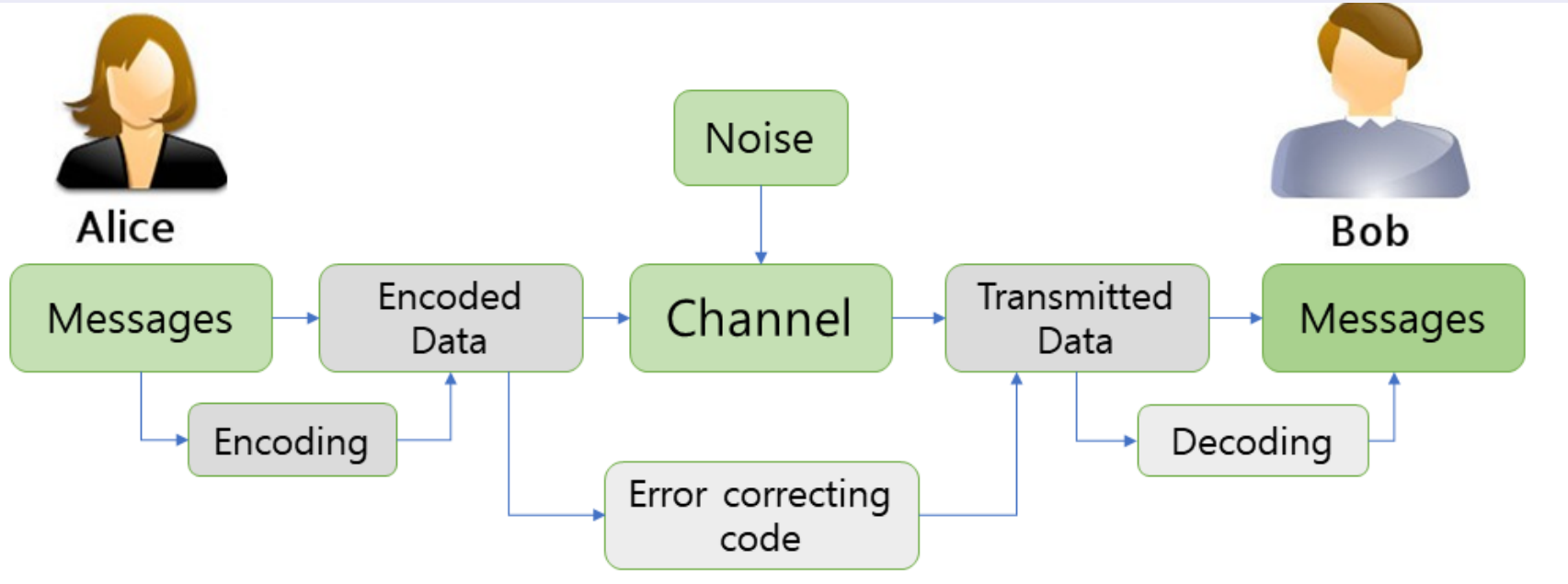
Hun Hee Lee
Seoul National University

SNU, December 18th - 21st, 2018

Table of contents

Basic concepts of quantum information theory I

Communication Scenario



Alice and Bob are communicating using a quantum channel

$$\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B).$$

Basic concepts of quantum information theory II

The von Neumann entropy

(**Def**) For a quantum state $\rho = \sum_{i=1}^{n} p_i |h_i\rangle\langle h_i| \in B(\mathcal{H})$ we define the von Neumann entropy by

$$S(\rho) := -\sum_{i=1}^{n} p_i \log p_i.$$

Basic concepts of quantum information theory III

Comparing quantum states: fidelity

- (**Def**) For quantum state $\rho, \sigma \in B(\mathcal{H})$ we define the fidelity $F(\rho, \sigma)$ by

$$F(\rho, \sigma) := \mathrm{Tr}[(\rho^{\frac{1}{2}} \sigma \rho^{\frac{1}{2}})^{\frac{1}{2}}].$$

- We always have $0 \leq F(\rho, \sigma) \leq 1$.
- $F(\rho, \sigma) = 1 \Leftrightarrow \rho = \sigma$.
- $F(\rho, \sigma) = 0 \Leftrightarrow \rho\sigma = 0$, i.e. orthogonal ranges.
- Fidelity measures how close the two quantum states are.

Basic concepts of quantum information theory IV

Comparing input/output quantum states: channel fidelity

- (**Def**) For a quantum state $\rho \in B(\mathcal{H})$ with the canonical purification $|u\rangle \in \mathcal{H} \otimes_2 \mathcal{H}$ and a quantum channel $\Phi : B(\mathcal{H}) \to B(\mathcal{H})$ we define the channel fidelity $F(\Phi, \rho)$ by

$$F(\Phi, \rho) := F(|u\rangle\langle u|, \Phi \otimes I_{\mathcal{H}}(|u\rangle\langle u|)).$$

Basic concepts of quantum information theory V

Recall: The Source coding theorem

- Let X be a random message source (i.e. a prob. dist. p on I). For $n \in \mathbb{N}$, $\alpha > 0$, $0 < \delta < 1$ an (n, α, δ)-coding for X refers to an encoding $f : I^n \to \{0,1\}^{\lfloor \alpha n \rfloor}$, a decoding $g : \{0,1\}^{\lfloor \alpha n \rfloor} \to I^n$ such that $P(\{A \in I^n : g(f(A)) = A\}) > 1 - \delta$, where $P = p \times \cdots \times p$, which means we use X independently n-times.
- (**Shannon's source coding theorem**)
  - If $\alpha > H(X)$, then $\exists$ (n, α, δ)-coding for X eventually for $n \in \mathbb{N}$.
  - If $\alpha < H(X)$, then $\exists$ (n, α, δ)-coding for X at most finitely many $n \in \mathbb{N}$.
- (**Meaning of entropy**) We can say that we need $H(X)$-bits per one letter to encode a random message from X in average.

Basic concepts of quantum information theory VI

The quantum source coding theorem

- Let $\rho \in \mathcal{D}(\mathcal{H})$ with $\mathcal{H} = \ell^2(I)$. For $n \in \mathbb{N}$, $\alpha > 0$, $0 < \delta < 1$ an (n, α, δ)-quantum coding for ρ refers to quantum channels $\Phi : B(\mathcal{H}^{\otimes n}) \to B((\mathbb{C}^2)^{\lfloor \alpha n \rfloor})$ and $\Psi : B((\mathbb{C}^2)^{\lfloor \alpha n \rfloor}) \to B(\mathcal{H}^{\otimes n})$ such that $F(\Psi \circ \Phi, \rho^{\otimes n}) > 1 - \delta$.
- (**Schumacher's quantum source coding theorem**)
  - If $\alpha > H(\rho)$, then $\exists$ (n, α, δ)-Q-coding for X eventually for $n \in \mathbb{N}$.
  - If $\alpha < H(\rho)$, then $\exists$ (n, α, δ)-Q-coding for X at most finitely many $n \in \mathbb{N}$.
- (**Meaning of entropy**) We can say that we need $H(\rho)$-qubits to quantum-encode a "quantum message from ρ" in average.

Basic concepts of quantum information theory VII

Joint entropy and mutual information for quantum states

For two quantum states $\rho_A \in B(\mathcal{H}_A)$ and $\rho_B \in B(\mathcal{H}_B)$ we assume that there is a quantum state $\rho \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ which reduces to ρ_A and ρ_B. We call ρ "a joint distribution" of ρ_A and ρ_B.

- The joint entropy $S(A, B)$ is given by $S(\rho)$ when we fixed a "joint distribution" ρ.
- The quantum mutual information $I_q(A, B)$ by

$$I_q(A, B) := S(A) + S(B) - S(A, B).$$

Classical capacity of quantum channels I

Recall: channel capacity

(**Def**) The channel capacity $C(\Phi)$ of a given channel Φ is defined by

$$C(\Phi) := \sup_{\text{prob. dist. } X \text{ on } A} I(X;Y).$$

Classical capacity of quantum channels II

The Holevo capacity

Let $\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ be a quantum channel.

- (**Def**) The Holevo capacity of Φ is defined by

$$\chi(\Phi) := \sup_{\text{prob. dist. } (p_i)_{i=1}^n, \text{ states } (\rho_i)_{i=1}^n \text{ on } \mathcal{H}_A} I_q(A;B),$$

  where A represents the classical state $(p_i)_{i=1}^n$, B represents the quantum state $\sum_{i=1}^n p_i \Phi(\rho_i)$ with a specific joint distribution

$$\rho = \sum_{i=1}^n p_i |i\rangle\langle i| \otimes \Phi(\rho_i).$$

- The collection of states $(\rho_i)_{i=1}^n$ refers to the classical-quantum encoding $i \mapsto \rho_i$.

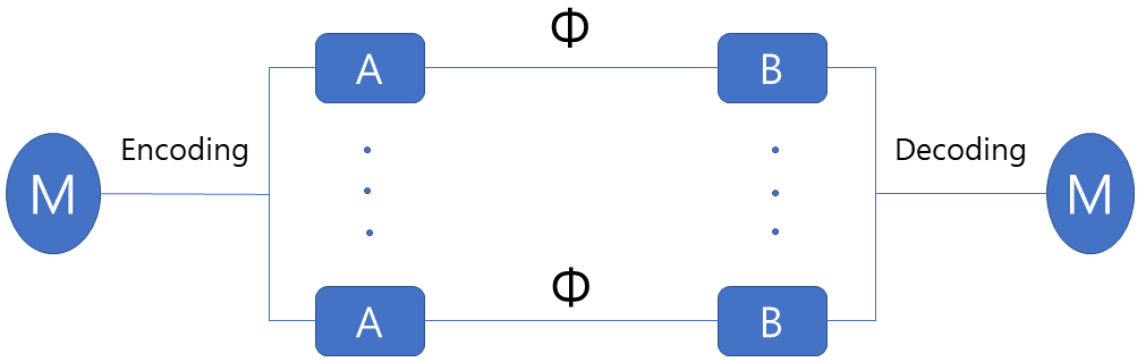
Classical capacity of quantum channels III

Multiple use of quantum channels

- (**Scenario**) Use the same quantum channel Φ repeatedly (n-times) and independently to send a message from $M = \{1, \cdots, N\}$.
- More precisely, we consider the quantum channel

$$\Phi^{\otimes n} : B(\mathcal{H}_A^{\otimes n}) \to B(\mathcal{H}_B^{\otimes n}),\ (\rho_1, \cdots, \rho_n) \mapsto \Phi(\rho_1) \otimes \cdots \otimes \Phi(\rho_n).$$

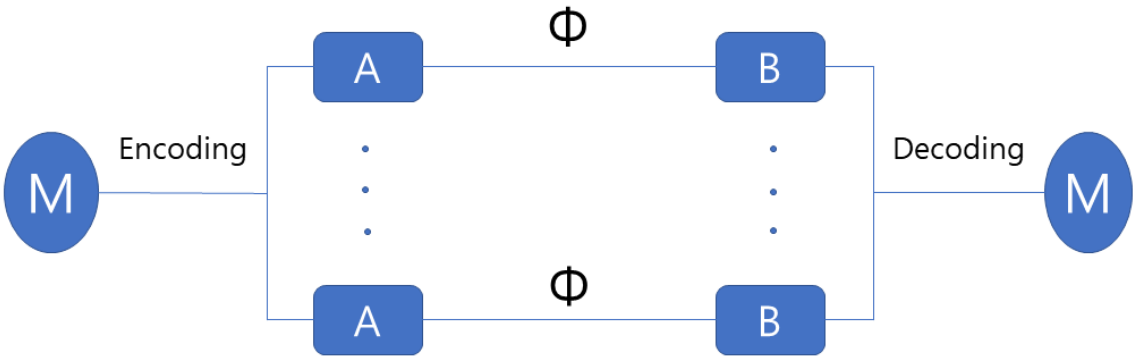
- Independency is being reflected by taking tensor product.



Classical capacity of quantum channels IV

Quantum codings

- (**Def**) An (N, n)-quantum coding for the quantum channel Φ consists of classical-quantum encoding $f : M = \{1, \cdots, N\} \to \mathcal{D}(\mathcal{H}_A^{\otimes n})$ and quantum-classical decoding given by a POVM $\{P_k\}_{k=0}^{N}$ acting on $\mathcal{H}_B^{\otimes n}$.
- We define the transmission rate to be $\dfrac{\log N}{n}$.
- We also define the maximum error probability $P_{e,\max} := \max_{1 \le i \le N} [1 - \mathrm{Tr}(\Phi^{\otimes n}(\rho_i) P_i)]$.



Classical capacity of quantum channels V

Channel quantum coding theorem

- (**Def**) We say that $R > 0$ is an achievable rate if $\exists$ (N, n)-quantum coding's whose transmission rate is R such that $\lim_{n\to\infty} P_{e,\max} = 0$.
- This means that we can send R-bits per one use of the quantum channel in average.
- (**Holevo-Schumacher–Westmoreland theorem**)

$$C(\Phi) := \sup R = \lim_{n\to\infty} \frac{\chi(\Phi^{\otimes n})}{n}.$$

Classical capacity of quantum channels VI

Additivity of Holevo Capacity

The "regularized" quantity $\lim_{n\to\infty} \frac{\chi(\Phi^{\otimes n})}{n}$ is a new quantum phenomenon, which leads us to the following question.

- (**Additivity Conjecture for** χ)
  For any quantum channel Φ we have

$$\chi(\Phi \otimes \Phi) = 2\chi(\Phi).$$

- (**Hastings, 2008**) There is a quantum channel Φ such that

$$\chi(\Phi \otimes \Phi) > 2\chi(\Phi).$$

- (**Rem**) The above can be interpreted as "repeated use of Φ will increase classical information transmission"!

Brief history of Banach space theory (A. Pietsch) I

The beginning

- 1920 (Birth): Thesis by S. Banach
- 1920 – 1932 (Youth): Monographs by Dunford/Schwarz and Hille-Yoshida
- 1932 – 1958 (Post-Banach): Uniform boundedness principle, Hahn-Banach thm, Open mapping thm

Brief history of Banach space theory (A. Pietsch) II

Modern Banach space theory, 1958 –

Grothendieck - tensor norms, **Dvoretzky** - local theory

Local theory of Banach spaces, 1970 –

- (**Q1**) Can we distinguish Banach spaces upto (bi-continuous) linear isomorphisms?
- The above is usually quite difficult. Even the statement $L^p \not\simeq L^q$ for $1 < p < q < \infty$ is not easy to prove.
- Banach space theorists started to look at (arbitrary) finite dimensional subspaces of a given (infinite dimensional) Banach space in the hope that it tells us the "global" structure.
  - Closed subspaces of Hilbert space are again Hilbert spaces.
  - $L^p(\mathbb{R}), 1 \leq p < \infty$ contains a closed subspace isomorphic to ℓ^2.
- (**Q2**) Can we embed a B-sp. X into another B-sp. Y isomorphically?

Local theory of Banach spaces and QIT I

Dvoretzky's Theorem and QIT

- (**Thm, Dvoretzky, '61**) For each $k \in \mathbb{N}$ and $\varepsilon > 0$ there is $N = N(k, \varepsilon)$ such that any N-dim Banach space X contains a k-dim'l subspace E which is $(1+\varepsilon)$-isomorphic to ℓ_k^2.
- (**Thm, Dvoretsky-Milman, '71**) The above holds for a random subspace E with high probability. Here, the probability is the canonical translation invariant measure on the Grassmanian manifold

$$Gr(k, \mathbb{R}^N) \cong O(N)/(O(k) \times O(N-k)),$$

  which is a homogeneous space of quotient type.
- (**Additivity violation of Holevo capacity**) One approach is based on a refinement of the above theorem, which uses concentraion of measure phenomenon, a then popular technique in Banach space local theory.

Local theory of Banach spaces and QIT II

Minimum output entropy (MOE)

- (**Def**) For a quantum channel $\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ we define the minimum output entropy $S_{\min}(\Phi)$ by

$$S_{\min}(\Phi) := \min_{\rho \in \mathcal{D}(\mathcal{H}_A)} S(\Phi(\rho)).$$

- (**Remark**) Recall the completely depolarizing channel on $\mathcal{H}_B$ written as a ramdom unitary channel $Y \mapsto \frac{1}{|J|} \sum_{j \in J} U_j Y U_j^*$. Then we can associate another quantum channel

$$\Psi : B(\ell^2(J) \otimes \mathcal{H}_A) \to B(\mathcal{H}_B),\ |j\rangle\langle k| \otimes X \mapsto \delta_{j,k} U_j Y U_j^*.$$

Then, we have the following:

$$\chi(\Psi) = \log d_B - S_{\min}(\Phi).$$

Local theory of Banach spaces and QIT III

Additivity Conjecture for MOE

- (**Additivity Conjecture for** $S_{\min}$)
  For any quantum channel Φ we have

$$S_{\min}(\Phi \otimes \Phi) = 2S_{\min}(\Phi).$$

- (**Hastings, 2008**) There is a quantum channel Φ such that

$$S_{\min}(\Phi \otimes \Phi) < 2S_{\min}(\Phi).$$

Zero error capacity of a classical channel I

Recall: Zero error capacity

- (**Def**) An (N, n)-coding for the channel Φ consists of encoding $f : M = \{1, \cdots, N\} \to \mathbf{A}^n$ and decoding $g : \mathbf{B}^n \to M$.
- We define the transmission rate to be $\dfrac{\log N}{n}$.
- We also define the maximum error probability $P_{e,\max} := \max\limits_{1 \le i \le N} P(g(Y^n) \neq i | X^n = f(i))$.
- (**Def**) We say that an (N, n)-coding is zero error if $P_{e,\max} = 0$.
- (**Def**, Shannon '56) The one-shot zero error capacity $C_0^1(\Phi)$ of a channel Φ is the supremum of $R > 0$ such that $\exists$ a zero error $(N, 1)$-coding for Φ.
- (**Rem**) In other words, $N = 2^{C_0^1(\Phi)}$ is the maximal number of different inputs that Alice can send through Φ so that Bob knows exactly which input was sent.

Zero error capacity of a classical channel II

Confusability graph

- (**Def**) For a classical channel $\Phi : \mathbf{A} \to \mathcal{P}(\mathbf{B}),\ x \mapsto (p(y|x))_{y\in\mathbf{B}}$ the confusability graph $G = (V, E)$ is given by

$$V = \mathbf{A}, \quad E = \{(x, x') : \exists y \in \mathbf{B} \text{ s.t. } p(y|x)p(y|x') \neq 0\}$$

- (**Ex**) Binary symmetric channel
- (**Def**) For a graph $G = (V, E)$ (no loop, un-directed) we say that a subset $S \subseteq V$ is called independent if for all $u, v \in S$ we have $(u, v) \notin E$. The independence number $\alpha(G)$ is the maximal cardinality of independent subsets of V.
- (**Thm**) Let G be the confusability graph of a classical channel Φ, then we have

$$\log \alpha(G) = C_0^1(\Phi).$$

Zero error capacity of a classical channel III

Zero error capacity: asymptotic version

- (**Prop**) The zero error capacity of a classical channel $\Phi : \mathbf{A} \to \mathcal{P}(\mathbf{B})$ can be calculated by $C_0(\Phi) = \lim_{n\to\infty} \frac{C_0^1(\Phi^n)}{n}$, where Φ^n refers to n-times independent use of Φ.
- (**Prop**) Let G be the confusability graph of a classical channel Φ, then the confusability graph of Φ^n is the strong graph product $G \boxtimes \cdots \boxtimes G$($n$-times).
- (**Def**) For two graphs $G_i = (V_i, E_i)$, $i = 1, 2$ we define the strong graph product $G_1 \boxtimes G_2 = (V, E)$ by $V := V_1 \times V_2$ and

$$E := \{(x_1, x_2) \sim (x_1', x_2') : x_1 \simeq x_1', x_2 \simeq x_2', (x_1, x_2) \neq (x_1', x_2')\}.$$

  Here, $x \simeq x'$ means that $x \sim x'$ or $x = x'$.
- Computing $C_0(\Phi)$ is usually very difficult!

Zero error capacity of quantum channels I

One-shot zero error capacity of quantum channels

(**Def**) For a a quantum channel $\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ we define the one-shot zero error capacity $C_0^1(\Phi)$ as follows:

$$C_0^1(\Phi) := \max\{d : \exists \text{ perfectly distinguishable } \{\rho_1, \cdots, \rho_d\} \subseteq \mathcal{D}(\mathcal{H}_S) \text{ s.t. } \{\Phi(\rho_1), \cdots, \Phi(\rho_d)\} \text{ is perfectly distinguishable}\}.$$

Distinguishing quantum states

(**Def**) We say that $\{\rho_1, \cdots, \rho_d\} \subseteq \mathcal{D}(\mathcal{H})$ is perfectly distinguishable if $\exists$ a quantum measurement $\{M_1, \cdots, M_k\}$ with $k \geq d$ s.t.

$$\mathrm{Tr}(M_j \rho_i M_j^*) = \delta_{ij} \text{ for } 1 \leq i, j \leq d.$$

Zero error capacity of quantum channels II

Lemma

$P, Q \in B(\mathcal{H})$: positive matrices.

- $\mathrm{Tr}(P) \Rightarrow P = 0$.
- T.F.A.E.
  1. $\langle P, Q \rangle = \mathrm{Tr}(PQ) = 0$,
  2. $PQ = 0$,
  3. $\mathrm{ran}P \perp \mathrm{ran}Q$.

More on distinguishability

- (**Prop**) $\{\rho_1, \cdots, \rho_d\} \subseteq \mathcal{D}(\mathcal{H})$ is perfectly distinguishable iff $\rho_i \rho_j = 0$ for all $i \neq j$. (proof)
- When $\rho_i = |v_i\rangle\langle v_i|$, i.e. pure states, then perfectly distinguishability is the same as $v_i \perp v_j$ for all $i \neq j$.

Zero error capacity of quantum channels III

One-shot zero error capacity of quantum channels: repeatition

(**Def**) For a a quantum channel $\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ we define the one-shot zero error capacity $C_0^1(\Phi)$ by

$$C_0^1(\Phi) := \max\{d : \exists\ v_1, \cdots, v_d \text{ orthonormal in } \mathcal{H}_A \\ \text{s.t. } \Phi(|v_i\rangle\langle v_i|)\Phi(|v_j\rangle\langle v_j|) = 0,\ \forall i \neq j\}.$$

Remark

In the above we are using the fact that we may assume that the quantum encodings are done by pure states. (why?)

Zero error capacity of quantum channels IV

One-shot zero error capacity and operator systems

- (**Def**) A subspace $\mathcal{S} \subseteq B(\mathcal{H})$ is called an operator system if (1) $I_{\mathcal{H}} \in \mathcal{S}$ and (2) $X \in \mathcal{S} \Rightarrow X^* \in \mathcal{S}$.
- (**Def**) For a quantum channel $\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ with the Kraus representation $\Phi(X) = \sum_{j\in J} A_j X A_j^*$ we define the associated operator system $\mathcal{S}_\Phi$ by

$$\mathcal{S}_\Phi := \text{span}\{A_i^* A_j : i, j \in J\}.$$

  This definition does not depend on the choice of Kraus representations.
- (**Thm**) For a quantum channel $\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ we have

$$C_0^1(\Phi) := \max\{d : \exists\ v_1, \cdots, v_d \text{ orthonormal in } \mathcal{H}_A \\ \text{s.t. } \mathrm{Tr}(|v_i\rangle\langle v_j| X) = 0, \forall X \in \mathcal{S}_\Phi,\ \forall i \neq j\}.$$

- Thus, $C_0^1(\Phi)$ depends only on the associated operator system!

Zero error capacity of quantum channels V

Graphs and operator systems

- From the previous theorem we might guess graphs and operator systems have some relationship.
- (**Def**) For a graph $G = (V, E)$ with $|V| = n$ we can associate an operator system $\mathcal{S}_G \subseteq B(\ell^2(V))$ given by

$$\mathcal{S}_G := \text{span}(\{|i\rangle\langle i| : i \in V\} \cup \{|i\rangle\langle j| : (i,j) \in E\}).$$

- (**Prop**) Let $\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ be a quantum channel and G is the confusability graph of Φ. Then we have $\mathcal{S}_\Phi = \mathcal{S}_G$. (proof)
- (**Remark**) For this reason we call operator systems ($\subseteq M_n$) as non-commutative graphs! Many concepts of graph theory are being transferred to operator system setting.

Thank you for your attention!

Quantum information theory with functional analysis techniques: Lecture 3

Hun Hee Lee
Seoul National University

SNU, December 18th - 21st, 2018

Table of contents

Tensor norms of Banach spaces I

Preliminaries

- X, Y, Z: Banach spaces
  $B(X, Y)$: linear maps from X into Y with operator norm
  $B(X \times Y, Z)$: bilinear maps from $X \times Y$ into Z with the norm

$$\|T\| := \sup_{x \in B_X, y \in B_Y} \|T(x, y)\|_Z, \ T \in B(X \times Y, Z),$$

  where B_X refers to the unit ball of X.

Tensor norms of Banach spaces II

Algebraic correspondence

For finite dimensional X, Y we have

$$\begin{array}{ccccc} X^* \otimes Y^* & \cong & (X \otimes Y)^* & \cong & B(X, Y^*) \cong B(X \times Y, \mathbb{C}) \\ \phi \otimes \psi & \mapsto & \phi \otimes \psi & \mapsto & S \qquad\qquad \mapsto T, \end{array}$$

where $\langle S(x), y\rangle = \langle x \otimes y, \phi \otimes \psi\rangle = \phi(x)\psi(y) = T(x, y)$ for $x \in X$ and $y \in Y$.

Tensor norms of Banach spaces III

Injective tensor norm of Banach spaces

Assume that X, Y are finite dimensional Banach spaces.

- (**Def**) We define the injective norm $\|\cdot\|_\varepsilon$ on $X \otimes Y$ by

$$\|z\|_\varepsilon := \sup_{\phi \in B_{X^*}, \psi \in B_{Y^*}} |\langle z, \phi \otimes \psi \rangle|$$

  for $z \in X \otimes Y$. We write the corresponding Banach space as $X \otimes_\varepsilon Y$ and call it the injective tensor product of X and Y.

- (**Prop**) We have an isometric identification

$$X^* \otimes_\varepsilon Y^* \cong B(X \times Y, \mathbb{C}) \cong B(X, Y^*).$$

Tensor norms of Banach spaces IV

γ_2 tensor norm and its trace dual γ_2^*

Assume that X, Y are finite dimensional Banach spaces.

- (**Def**) We define the γ_2-norm $\|\cdot\|_{\gamma_2}$ on $X \otimes Y$ by

$$\|z\|_{\gamma_2} := \inf \|A\| \cdot \|B\|$$

for $z \in X \otimes Y$ and the infimum is taken for all possible factorization $S_z : X \xrightarrow{A} \mathcal{H} \xrightarrow{B} Y^*$ of the corresponding linear map for some Hilbert space $\mathcal{H}$.

- (**Def**) We define the γ_2^*-norm $\|\cdot\|_{\gamma_2^*}$ on $X \otimes Y$ by

$$\|z\|_{\gamma_2^*} := \sup |\langle z, w \rangle|$$

for $z \in X \otimes Y$, where the supremum is taken over all $w \in X^* \otimes Y^*$ with $\|w\|_{\gamma_2} \leq 1$. Note that we are using trace duality here.

Tensor norms of Banach spaces V

Grothendieck's theorem and γ_2^*-norm on ℓ^1-spaces

- (**Prop**) For $n, m \in \mathbb{N}$ and $z = (z_{ij})_{1\le i\le n, 1\le j\le m} \in \ell_n^1 \otimes \ell_m^1$ we have

$$\|z\|_{\gamma_2^*} = \sup_{d\in\mathbb{N}, u_i, v_j \in B_{\ell_d^2}} \left| \sum_{1\le i\le n, 1\le j\le m} z_{ij} \langle u_i, v_j \rangle \right|.$$

- (**Thm, Grothendieck, '53**)
  There are universal constants $K_G^{\mathbb{R}}$ and $K_G^{\mathbb{C}}$ such that for any $n, m \in \mathbb{N}$, $z_1 \in \ell_n^1(\mathbb{R}) \otimes \ell_m^1(\mathbb{R})$ and $z_2 \in \ell_n^1(\mathbb{C}) \otimes \ell_m^1(\mathbb{C})$ we have

$$\|z_1\|_{\gamma_2^*} \le K_G^{\mathbb{R}} \|z_1\|_{\ell_n^1(\mathbb{R})\otimes_\varepsilon \ell_m^1(\mathbb{R})} \text{ and } \|z_2\|_{\gamma_2^*} \le K_G^{\mathbb{C}} \|z_2\|_{\ell_n^1(\mathbb{C})\otimes_\varepsilon \ell_m^1(\mathbb{C})}.$$

Tensor norms of operator spaces I

Operator space

- Recall that any Banach space X is isometrically embedded in $C(\Sigma)$ for a compact Hausdorff space Σ.
- (**Def**) An operator space E is a closed subspace of $B(\mathcal{H})$ for some Hilbert space $\mathcal{H}$.
- (**Ex**)
  1. Any closed subspaces of C^*-algebras are operator spaces.
  2. D_n, R_n, C_n: the spaces of diagonal, (1st) row, (1st) column matrices in M_n, respectively
  3. We also have that $D_n \cong \ell_n^\infty$ as commutative C^*-algebras.

Tensor norms of operator spaces II

Ruan's abstract characterization of operator spaces

- For an operator space $E \subseteq B(\mathcal{H})$ we may equip a natural norm $\|\cdot\|_n$ on $M_n(E)$ as a subspace of $M_n(B(\mathcal{H})) \cong B(\ell_n^2 \otimes_2 \mathcal{H})$ for any $n \geq 1$. We call $(M_n(E), \|\cdot\|_n)_{n\geq 1}$ an operator space structure (shortly, o.s.s. (or a matricial norm structure) on E.
- (**Ruan's theorem**)
  Let E be a Banach space with matricial norm structure $(M_n(E), \|\cdot\|_n)_{n\geq 1}$ satisfying the following.
  (R1) $\|x \oplus y\|_{n+m} = \max\{\|x\|_n, \|y\|_m\}$ for $x \in M_n(E)$, $y \in M_m(E)$.
  (R2) $\|\alpha x \beta\|_n \leq \|\alpha\| \cdot \|x\|_n \cdot \|\beta\|$ for $x \in M_n(E)$ and $\alpha, \beta \in M_n$.

  Then, there is an isometric embedding $E \hookrightarrow B(\mathcal{H})$ for some Hilbert space $\mathcal{H}$.

Tensor norms of operator spaces III

Completely bounded maps and duality

- (**Def**) A linear map $T : E \to F$ between operator spaces is called completely bounded (shortly, cb) if

$$\|T\|_{cb} := \sup_{n \geq 1} \|I_n \otimes T : M_n(E) \to M_n(F)\| < \infty.$$

  We denote the space of all cb-maps by $CB(E, F)$ endowed with cb-norm.

- (**Def**) For an operator space E we define its dual operator space E^* by the Banach space E^* equipped with the o.s.s. given by

$$M_n(E^*) := CB(E, M_n)$$

  via the canonical identification.

- (**Ex**) $\ell_n^1 = (\ell_n^\infty)^*$ has a canonical o.s.s.

Tensor norms of operator spaces IV

Injective tensor norm of operator spaces

Assume that E, F are finite dimensional operator spaces.

- (**Def**) We define the injective norm $\|\cdot\|_\varepsilon$ on $E \otimes F$ by

$$\|z\|_{\min} := \|S_z\|_{CB(E,F^*)}$$

for $z \in E \otimes F$ and its corresponding linear map $S_z : E \to F^*$. We write the corresponding Banach space as $E \otimes_{\min} F$ and call it the injective tensor product of E and F.

- (**Prop**) We have an isometric identification $E^* \otimes_{\min} F^* \cong CB(E, F^*) \cong CB(E \times F, \mathbb{C})$, where the space $CB(E \times F, \mathbb{C})$ of cb-bilinear maps is equipped with the norm $\|T\|_{cb} := \sup_{d \in \mathbb{N}, x=(x_{ij}) \in B_{M_d(E)}, y=(y_{kl}) \in B_{M_d(F)}} \|T(x_{ij}, y_{kl})\|_{M_{d^2}}$ for $T \in CB(E \times F, \mathbb{C})$.

Tensor norms of operator spaces V

Comparing two injective norms and Grothendieck's theorem

(**Prop**) Let $z = (z_{ij})_{1\le i\le n, 1\le j\le m} \in \ell_n^1(\mathbb{R}) \otimes \ell_m^1(\mathbb{R})$. Then,

$$\begin{aligned}
\|z\|_{\ell_n^1 \otimes_{\min} \ell_m^1} &= \sup_{d\in\mathbb{N},\, A_i, B_j \in B_{M_d}} \|\sum_{i=1}^n \sum_{j=1}^m z_{ij} A_i \otimes B_j\|_{M_{d^2}} \\
&= \sup_{d\in\mathbb{N},\, A_i, B_j \in B_{M_d},\, |\phi\rangle, |\psi\rangle \in B_{\ell_d^2 \otimes_2 \ell_d^2}} |\sum_{i=1}^n \sum_{j=1}^m z_{ij} \langle \phi | A_i \otimes B_j | \psi \rangle| \\
&= \sup_{d,\, A_i, B_j,\, |\phi\rangle, |\psi\rangle} |\sum_{i=1}^n \sum_{j=1}^m z_{ij} \langle \phi | A_i \otimes I_d \cdot I_d \otimes B_j | \psi \rangle| \\
&\le \sup_{d\in\mathbb{N},\, u_i, v_j \in B_{\ell_d^2}} |\sum_{i=1}^n \sum_{j=1}^m z_{ij} \langle u_i, v_j \rangle| \\
&= \|z\|_{\gamma_2^*} \le K_G^{\mathbb{R}} \|z\|_{\ell_n^1(\mathbb{R}) \otimes_\varepsilon \ell_m^1(\mathbb{R})}.
\end{aligned}$$

Correlation sets and two player games I

Recall: Classical channels

(**Def**) A classical (discrete and memoryless) channel consists of the input set **A**, the output set **B** and the map

$$\Phi : \mathbf{A} \to \mathcal{P}(\mathbf{B}),\ x \mapsto (p(y|x))_{y \in \mathbf{B}}.$$

Recall: Correlation set

(**Notation**) We denote the set of all classical channels from **A** into **B** by $\mathcal{P}(\mathbf{B}|\mathbf{A})$. In other words,

$$\mathcal{P}(\mathbf{B}|\mathbf{A}) = \{(p(y|x))_{x \in \mathbf{A},\, y \in \mathbf{B}} : p(y|x) \geq 0,\ \sum_{y} p(y|x) = 1\}.$$

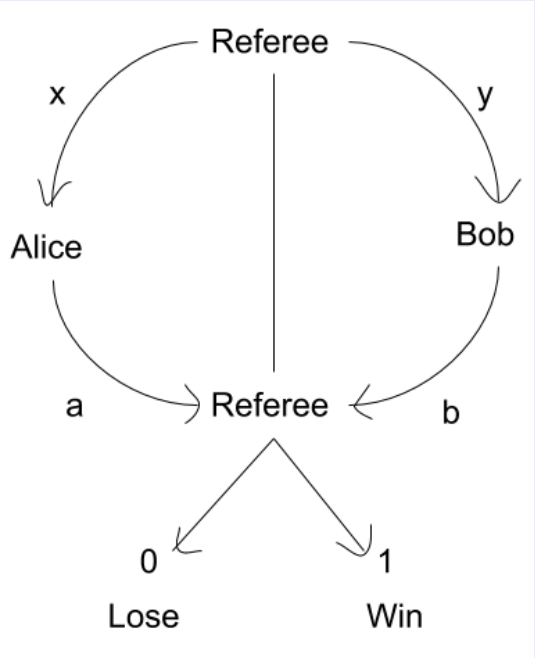
When we have two input sets **X**, **Y** and two output sets **A**, **B**, we simply write

$$\mathcal{P}(\mathbf{AB}|\mathbf{XY}) = \mathcal{P}(\mathbf{A} \times \mathbf{B}|\mathbf{X} \times \mathbf{Y}).$$

Correlation sets and two player games II

Two player games

- Alice and Bob plays a game against the referee.
- (1) The referee sends inputs $x \in \mathbf{X}$ and $y \in \mathbf{Y}$ to Alice and Bob respectively. (2) Alice and Bob use their own "strategy" and return their output $a \in \mathbf{A}$ and $b \in \mathbf{B}$ to the referee. (3) The referee declares "win" or "lose" according to the "rule".



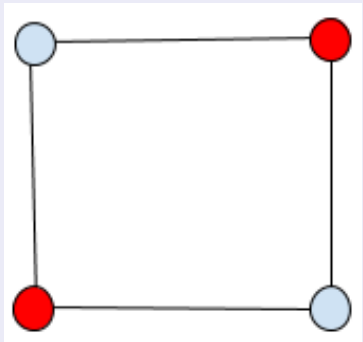
Correlation sets and two player games III

Two player games: formal definition

- (**Def**) A two player one-round game $G = (\mathbf{X}, \mathbf{Y}, \mathbf{A}, \mathbf{B}, \pi, V)$ consists of input sets $\mathbf{X}, \mathbf{Y}$ and output sets $\mathbf{A}, \mathbf{B}$ for Alice and Bob, respectively, a initial prob. dist. π on $\mathbf{X} \times \mathbf{Y}$ and the rule function

$$V : \mathbf{A} \times \mathbf{B} \times \mathbf{X} \times \mathbf{Y} \to \{0, 1\}.$$

- (**Ex**) Graph coloring game for a graph (V, E)
  - Alice and Bob want to claim that they have c-coloring of (V, E).
  - $\mathbf{X} = \mathbf{Y} = V$, $\mathbf{A} = \mathbf{B} = \{1, \cdots, c\}$, Winning $\Leftrightarrow \begin{cases} x \sim y \Rightarrow a \neq b \\ x = y \Rightarrow a = b \end{cases}$.



Correlation sets and two player games IV

More on correlation sets

- (**Def**) With input sets $\mathbf{X}$, $\mathbf{Y}$ and output sets $\mathbf{A}$, $\mathbf{B}$ we define the classical correlation set $\mathcal{P}_{\mathcal{C}}(\mathbf{AB}|\mathbf{XY}) \subseteq \mathbb{R}_+^{\mathbf{ABXY}} = \mathbb{R}_+^{\mathbf{A}\times\mathbf{B}\times\mathbf{X}\times\mathbf{Y}}$ by

$$\mathcal{P}_{\mathcal{C}}(\mathbf{AB}|\mathbf{XY}) := \mathrm{Conv}\{P \times Q : P \in \mathcal{P}(\mathbf{A}|\mathbf{X}), Q \in \mathcal{P}(\mathbf{B}|\mathbf{Y})\}.$$

  In other words, they are "local distributions with shared randomness".

- (**Def**) We also define the quantum correlation set $\mathcal{P}_{\mathcal{Q}}(\mathbf{AB}|\mathbf{XY}) \subseteq \mathbb{R}_+^{\mathbf{ABXY}}$ by

$$\begin{aligned}&\mathcal{P}_{\mathcal{Q}}(\mathbf{AB}|\mathbf{XY})\\ &:= \{(\langle\psi|A_x^a \otimes B_y^b|\psi\rangle)_{x,y,a,b} : d \in \mathbb{N},\ |\psi\rangle \in B_{\ell_d^2 \otimes_2 \ell_d^2},\\ &\qquad\qquad (A_x^a)_a, (B_y^b)_b \text{ POVMs on } \ell_d^2,\ \forall x, y\}.\end{aligned}$$

- $\mathcal{P}_{\mathcal{C}}(\mathbf{AB}|\mathbf{XY}) \subseteq \mathcal{P}_{\mathcal{Q}}(\mathbf{AB}|\mathbf{XY}) \subseteq \mathcal{P}(\mathbf{AB}|\mathbf{XY}) \subseteq \mathbb{R}^{\mathbf{ABXY}}$: convex sets.

Correlation sets and two player games V

Bell functionals and Bell inequality

- (**Def**) A linear functional $M = (M_{xy}^{ab})_{x,y,a,b}$ of $\mathbb{R}^{\mathbf{ABXY}}$ is called a Bell functional.
- (**Def**) For a Bell functional $M = (M_{xy}^{ab})_{x,y,a,b}$ we define its classical value $\omega(M)$ by $\omega(M) := \sup_{P \in \mathcal{P}_{\mathcal{C}}(\mathbf{AB}|\mathbf{XY})} |\sum_{x,y,a,b} M_{xy}^{ab} p(a,b|x,y)|$.

  We also define its quantum (or entangled) value $\omega^*(M)$ by

$$\omega^*(M) := \sup_{P \in \mathcal{P}_{\mathcal{Q}}(\mathbf{AB}|\mathbf{XY})} |\sum_{x,y,a,b} M_{xy}^{ab} p(a,b|x,y)|.$$

- Any inequality of the form $\omega(M) \leq C$ is called a Bell inequality.
- We always have $\omega(M) \leq \omega^*(M)$. The situation $\omega(M) < \omega^*(M)$ is called a Bell inequality violation.

XOR games and Bell's/Grothendieck's inequality I

Values of games

(**Def**) A two player one-round game $G = (\mathbf{X}, \mathbf{Y}, \mathbf{A}, \mathbf{B}, \pi, V)$ give rise to a Bell functional

$$G_{xy}^{ab} := \pi(x, y)V(a, b, x, y),$$

which allows us to define classical/quantum values of G, namely $\omega(G)$ and $\omega^*(G)$.

XOR games and Bell's/Grothendieck's inequality II

XOR games

- (**Def**) A two player one-round game $G = (\mathbf{X}, \mathbf{Y}, \mathbf{A}, \mathbf{B}, \pi, V)$ is called an XOR game if $\mathbf{A} = \mathbf{B} = \{0, 1\}$ and V is of the following form:

$$V(a, b, x, y) = \frac{1}{2}(1 + (-1)^{a \oplus b \oplus c_{xy}})$$

  for some $c_{xy} \in \{0, 1\}$, where $\oplus$ means the binary addition. In other words, V depends on x, y and the parity of a and b.
- (**Ex**) CHSH game: $\mathbf{X} = \mathbf{Y} = \mathbf{A} = \mathbf{B} = \{0, 1\}$ and $c_{xy} = xy$, the binary product.

XOR games and Bell's/Grothendieck's inequality III

Note that

$$\sum_{x,y,a,b} \pi(x,y)V(a,b,x,y)p(a,b|x,y)$$

$$= \sum_{x,y,a,b} \pi(x,y)\frac{1+(-1)^{a\oplus b\oplus c_{xy}}}{2}p(a,b|x,y)$$

$$= \frac{1}{2} + \frac{1}{2}\sum_{x,y} \pi(x,y)(-1)^{c_{xy}}(p(0,0|x,y) + p(1,1|x,y)$$

$$- p(0,1|x,y) - p(1,0|x,y))$$

$$= \frac{1}{2} + \frac{1}{2}\beta(G;P)$$

The last sum $\beta(G;P)$ in the above looks better to deal with. By extreme point argument we propose the following definition.

XOR games and Bell's/Grothendieck's inequality IV

Classical bias of games

- (**Def**) We define classical bias $\beta(G)$ by

$$\beta(G) := \sup_{P \in \mathcal{P}_C(\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y})} |\beta(G;P)|.$$

- We actually have

$$\begin{aligned}
&\beta(G) \\
&:= \sup_{\substack{A \in \mathcal{P}(\mathbf{A}|\mathbf{X}) \\ B \in \mathcal{P}(\mathbf{B}|\mathbf{Y})}} |\sum_{x,y} \pi(x,y)(-1)^{c_{xy}} (A(0|x) - A(1|x))(B(0|y) - B(1|y)| \\
&= \sup_{\substack{a \in B_{\ell^\infty(X,\mathbb{R})} \\ b \in B_{\ell^\infty(Y,\mathbb{R})}}} |\sum_{x,y} \pi(x,y)(-1)^{c_{xy}} a_x b_y| \\
&= \|(\pi(x,y)(-1)^{c_{xy}})_{x,y}\|_{\ell^1(X,\mathbb{R}) \otimes_\varepsilon \ell^1(Y,\mathbb{R})}
\end{aligned}$$

XOR games and Bell's/Grothendieck's inequality V

Quantum bias of games and its upper bound

- (**Def**) We define quantum (or entangled) bias $\beta^*(G)$ by

$$\beta^*(G) := \sup_{P \in \mathcal{P}_{\mathcal{Q}}(\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y})} |\beta(G;P)|.$$

- We may check that

$$\begin{aligned}
&\beta^*(G) \\
&= \sup_{d\in\mathbb{N}, A\in B_{\ell^\infty}(X,M_d), B\in B_{\ell^\infty}(Y,M_d)} |\sum_{x,y} \pi(x,y)(-1)^{c_{xy}} A_x \otimes B_y| \\
&= \|(\pi(x,y)(-1)^{c_{xy}})_{x,y}\|_{\ell^1(X)\otimes_{\min}\ell^1(Y)}
\end{aligned}$$

- (**Thm, Tsirelson, 87**) For any XOR game G we have

$$\beta^*(G) \leq K_G^{\mathbb{R}} \beta(G).$$

XOR games and Bell's/Grothendieck's inequality VI

Three-player XOR games and unbounded violation

- We may extend the concept of XOR games for $n \geq 3$ players.
- (**Thm, Junge et al, 08**) There is $C > 0$ s.t. for any n there is a three-player XOR game G with input set size n^2 such that

$$\beta^*(G) \geq C \frac{\sqrt{n}}{\log^{3/2} n} \beta(G).$$

Thus, we can say that tripartite Bell inequality may have unbounded violation!

Thank you for your attention!