# IOPB SCHOOL
# ON
# QUANTUM INFORMATION

Date:- 9-13 Feb 2016

CHIRANJIB MUKHOPADHYAY ; HRI ALLAHABAD

# SCHEDULE FOR SCHOOL

## 9 FEBRUARY

8:30-9:15 → Registration
9:15-9:30 → Inauguration

9:30-11:00 → "Non locality arguments"- Sujit Chowdhury

11:30-13:00 → "Pre Quantum Information Theory"- Goutam Paul

14:30-16:00 → "Quantum circuits & simple Quantum algorithms"- Jozef Gruska

16:30-18:00 → "Pre Quantum Cryptology"- Goutam Paul

## 10 FEBRUARY

9:30-11:00 → "Death & rebirth of Classical Crypto in a Quantum World"- Goutam Paul

11:30-13:00 → "Advanced Quantum Algorithms": Jozef Gruska

14:30-16:00 → "Quantum Information Theory"- Sibashis Ghosh

16:30-18:00 → "Quantum Correlations"- Debasis Sarkar

## 11 FEBRUARY

09:30-11:00 → "Quantum Uncertainty Principle & Joint measurement" Guruprasad Kar

11:30-13:00 → "Quantum Information Theory"- Sibashis Ghosh

14:30-16:00 → "Quantum Correlations" Debasis Sarkar

16:30-18:00 → "Joint measurement, steering & nonlocality" - Guruprasad Kar

## 12 FEBRUARY

09:30-11:00 → "Quantum Thermodynamics": Sibashis Ghosh

11:30-13:00 → "Is the wavefunction a part of reality"- Guruprasad Kar

14:30-16:00 → "Quantum Games"- Colin Benjamin

16:30-18:00 → "Quantum Thermodynamics"- Sibashis Ghosh

## 13 FEBRUARY

09:30-10:30 - "Is the Wavefunction part of reality ?"- Guruprasad Kar

11:00-12:30 → "Optical Quantum Information"- Anirban Pathak

12:30-13:15 → "Experimental Optical Quantum Information"- Anindita Banerjee

14:30-16:00 → "Semidefinite Programming": Ramij Rahman

16:30-18:00 → "Semidefinite Programming Tutorial"- Ramij Rahman

DAY- 1

09:30- 11:00

LECTURE - 1

TOPIC :- NON-LOCALITY ARGUMENTS

LECTURER :- SUJIT CHOWDHURY (IOP BHUBANESWAR)

- Nonlocality : i) Special Relativity, ii) Resource } Motivation
- QM is a statistical theory.
- Consider spin $\frac{1}{2} \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$; measure $\sigma_z \rightarrow 50\% \uparrow, 50\% \downarrow$ probability.
- What if there is a hidden variable theory finer than QM?
- On a statistical level - HVT predictions must match experimentally with QM.

for 2+ correlated systems - local HVT models get tough....

Bell Expt :- Conditional Probabilities $p(a,b|A,B,P)$ → these are what we observe.

Ontic HVT :- $\lambda$ = ontic variable $\in \Lambda$ (Ontic State Space) & $p_P(\lambda)$ is a prob distrib. $\forall$ prep procedure P. Knowing preparation P may not let us know $\lambda$ precisely - so it's a probability distribution over $\lambda$'s. ∴ Prob $(a,b|A,B,P) = \int_\Lambda p(a,b|A,B,P,\lambda)\, p_P(\lambda)\, d\lambda$ → Summing over all $\lambda$'s.

Cavalcanti Wiseman Found Phys. 42 1329 (2012) → Review Article
Rob Spekkens Phys Rev A (2005)

Deterministic model $\Rightarrow p(a,b|A,B,\lambda) \in \{0,1\}\ \forall\ a,b,A,B$.

$a = f(A,B,P,\lambda)$; $b = g(A,B,P,\lambda)$ in a deterministic model.

Implies $P(b|A,a,B,P,\lambda) = P(b|A,B,P,\lambda)$. A model satisfies locality if

Bayes Thm says $p(a,b|A,B,P,\lambda) = p(a|A,B,P,\lambda)\, p(b|A,a,B,P,\lambda)$.

Determinism means $P(b|A,a,B,P,\lambda) = P(b|A,B,P,\lambda)$ ∴ Hence

$p(a,b|A,B,P,\lambda) = p(a|A,B,P,\lambda)\, P(b|A,B,P,\lambda)$; Now locality means

$p(a|A,B,P,\lambda) = p(a|A,P,\lambda)\ \forall\ a,A,B$ & Similarly $p(b|A,B,P,\lambda) = p(b|B,P,\lambda)$

$\therefore P(a,b|A,B,P,\lambda) = p(a|A,P,\lambda)\, p(b|B,P,\lambda)$ for local deterministic models.

## BELL NONLOCALITY ARGUMENTS

Alice can measure A or A′; Bob can measure B or B′. {all dichotomic observables}
Alice & Bob are spacelike separated.

**Bell Theorem**

$$|\langle AB\rangle + \langle AB'\rangle + \langle A'B\rangle - \langle A'B'\rangle|_{LRT} \leq 2$$

To Prove this one needs Assumption:- $p(\lambda|A,B,P) = p(\lambda)$ (free will assumption)

Brunner RMP 86, 839 (2014)

Bayes Thm:- $p(AB|\lambda) = \dfrac{p(\lambda|AB)\,P(AB)}{P(\lambda)} \Rightarrow P(AB|\lambda) = P(AB)$ ∴ Measurement settings can be chosen freely.


Spin measurement strategy

for this & state $= \dfrac{|01\rangle + |10\rangle}{\sqrt{2}}$

$|\langle AB\rangle + \langle AB'\rangle + \langle A'B\rangle - \langle A'B'\rangle| = 2\sqrt{2}$ → violating local realism

$2\sqrt{2}$ is the maximal possible violation (Tsirelson)

Bell Thm:- Local Realism ⊁ Quantum Mechanics

If you want a deterministic theory of QM → it's nonlocal

Special Relativity ?? No-Signalling?

NO-SIGNALLING:- $p(a|A,B,\rho) = p(a|A,\rho)\ \forall\ a,A,B$
$p(b|A,B,\rho) = p(b|B,\rho)\ \forall\ b,A,B$ if A & B are causally separated (spacelike)

Violation of locality ≠ Superluminal Signalling

Bohm model → Local but non-reality but no-signalling.

Locality → Ontological Concept; No-Signalling Operational Concept

Locality implies signal locality but not the converse

?? IDEA:- Non Signalling with Lieb-Robinson in Quantum Lattice models ??

A model is Predictable iff

$$p(a,b|A,B,\rho) \in \{0,1\}\ \forall\ a,b,A,B$$

for predictable models → Nonlocality ≡ Nosignalling.

PREDICTABILITY + NO-SIGNALLING ⇒ BELL THEOREM (Proof)

$p(a,b|A,B,\rho,\lambda) = p(a,b|A,B,\rho)$ from Predictability

$p(a,b|A,B,\rho) = p(a|A,B,\rho)\ p(b|A,a,B,\rho)$

∵ Predictability implies $p(b|A,a,B,\rho) = p(b|A,B,\rho)$ ∴ Hence $p(a,b|A,B,\rho) = p(a|A,B,\rho)\,p(b|A,B,\rho)$
But this is precisely the locality assumption. ---- (Proved)

✓ Bell Violation + No-Signalling ⇒ True Randomness.

Good Resource for generating truly random numbers.
Classically → be satisfied with pseudo-random numbers.

* "Randomness Certified by Bell Theorem" - Ref.

NON-LOCALITY WITHOUT INEQUALITY ⇒ GHZ states $\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)$

Bell nonlocality as a measure of Entanglement ⇒ fewer # of measurements needed than complete state tomography.

Hardy PRL 68, 2981 (1992) → NLWI with only 2 qubits.
Consider $P(++|A,B,\rho) > 0$; $P(+-|A,B,\rho) = P(+-|A,B,\rho) = P(--|A,B,\rho) = 0$

Goal :- Show that this four outcomes are impossible with Local Realism but NOT QM.

$$\int_{\Lambda} p(+|A,\beta,\lambda)\, p(+|B,\beta,\lambda)\, d\lambda > 0$$

$\therefore \Rightarrow$ a subset $\Lambda' \subset \Lambda$ s.t. $p(+|A,\beta,\Lambda') > 0$ & $p(+|B,\beta,\Lambda') > 0$

but from other conditions $\Rightarrow \nexists$ subset s.t. $p(+|A,\beta,\Lambda')$ or $p(+|B,\beta,\Lambda')$ is non-zero.

Contradiction for the last Hardy Conditi

But in QM $\Rightarrow$ take the state in Any pure non-maximally entangled state

HW:- Check all four Hardy Conditions are satisfied by them; but no maximally entangled state satisfy the Hardy Paradox ($q_s$ = success probability of Hardy Paradox = 0.09.. show)

$A = |\omega_1^+\rangle\langle\omega_1^+| - |\omega_1\rangle\langle\omega_1|$

$B = |\omega_2^+\rangle\langle\omega_2^+| - |\omega_2\rangle\langle\omega_2|$

$A' = |u_1\rangle\langle u_1| - |v_1\rangle\langle v_1|$

$B' = |u_2\rangle\langle u_2| - |v_2\rangle\langle v_2|$

Cabello → Success Probability 11%
(Look up)

$$|\omega_1\rangle = \frac{a|v_1\rangle + b|u_1\rangle}{\sqrt{|a|^2 + |b|^2}} \qquad |\omega_2\rangle = \frac{a|v_2\rangle + c|u_2\rangle}{\sqrt{|a|^2 + |c|^2}}$$

LECTURE-2

11:30-13:00

# PRE QUANTUM INFORMATION THEORY

GOUTAM PAUL, ISI KOLKATA

OUTLINE:-

1) MEASUREMENT OF INFORMATION
2) MEASURES OF INFORMATION FLOW
3) QUANTUM INFORMATION

# MEASURES OF INFORMATION

## UNCERTAINTY

$A \to P_1$ ; $B \to P_2$ independently ; so- $A \cap B \to$ Probability $P_1P_2$ ; Information = $I = I_1 + I_2$

$\Rightarrow -\log P_i$ is tentatively a good measure.

**Average Information :-** $= \sum_i P_i I(P_i) = -\sum_i P_i \log P_i = H(\vec{P}) \to$ Shannon Entropy $\left(\vec{P} = \{P_1, \ldots, P_n\}\right)$

Joint Entropy $H(AB)$ ; Conditional Entropy $H(A|B)$ ; Marginal Entropy $H(B)$

$$H(A|B) = H(AB) - H(B) \rightsquigarrow \text{Chain Rule}$$

$$H(Y|X) = \sum_x P(x)\, H(Y|X=x) = \sum_x P(x) \sum_y \left(-P(y|x) \log P(y|x)\right) = \sum_{x,y} P(x,y) \log P(y|x)$$

$H(XY) \leq H(X) + H(Y) \rightsquigarrow$ Sub-additivity

$H(Y|X) \leq H(Y) \rightsquigarrow$ Conditioning reduces uncertainty

**Mutual Information :-** $I(X;Y) = H(X) + H(Y) - H(X,Y) = \sum_x \sum_y P(x,y) \log \frac{P(x,y)}{P(x)P(y)} = H(X) - H(X|Y) = H(Y) - H(Y|X)$ ∴ Mutual Information is symmetric.

## COMPRESSIBILITY

If I can compress/summarize the data - we've extracted information out of it.

**Kraft Inequality** :- ∃ an instantaneous code over an r-ary alphabet with codeword lengths $l_1, \ldots, l_n$ iff

$\sum_{i=1}^{n} r^{-l_i} \leq 1$ → Necessary + Sufficient Condition

Say 10 → Goodnews, 101 → Badnews

After first two codeword arrives → I'm still not sure ∴ We want prefix-free codewords.

↓

Instantaneous Code

## ENGINEERING OPTIMIZATION

Choosing $r \to \infty$ makes Kraft trivial - But not very practical

We want to minimize the length of average codeword $\sum_i P_i l_i$ s.t. $\sum_{i=1}^{n} r^{-l_i} \leq 1$ gives $l_i^* = -\log_r P_i$

$L^* = \sum_i l_i P_i = \sum_i P_i l_i^* = H(X)$ ..... COOL !!!

Idea :- Quantum version of Kraft Inequality for Entangled pairs ?? DON'T KNOW

# ENTROPY & DATA COMPRESSION

for Integer choice of data compression codeword lengths $H(X) \leq L^* \leq H(X)+1$

for Supersymbols with n-symbols at a time $H(X) \leq L_n^* \leq H(X) + \frac{1}{n} \rightarrow$ is achievable for stationery distribution as $n \to \infty$

Huffman:- Explicit Coding Algorithm

Shannon's noiseless Source Coding Theorem

# RANDOMNESS

More randomness → more information ; less randomness → less information

But Entropy is a measure of randomness.

PROB:- Maximizing $\left(-\sum_i p_i \log p_i\right)$ s.t. $\sum p_i = 1$ What's that prob. distribution ?

Ans:- Uniform Distribution → Connection to Randomness

# ENCRYPTION

Encodings would be such that it looks random to the eavesdropper.

Goal :→ $H(C) > H(P)$ [C = Encrypted Text ; P :- Plain Text]

But $H(P|C)$ may be $<$ $H(P)$ . Example :- a, b, c plaintexts (0.5, 0.3, 0.2 → probabilities)

3 possible ciphers :- U, V, W & two possible keys U, V, W

Encryption under $K_1$ : U, V, W
Encryption under $K_2$ : U, W, V
} $p(U) = 0.5$, $p(V) = p(W) = 0.25$

$p(a|U) = 0$, $p(b|V) = 0.6$, $p(c|W) = 0.4$ } (Say)

$H(P) = 1.485$ ; $H(P|C) = 0.485$ (Check)

PERFECT SECRECY:- (INFORMATION THEORETIC) $H(P|C) = H(P)$ → Hard to achieve

Equivalently $p(P|C) = p(P)$ → necessary for this is $H(K) \geq H(P)$ → i.e. length of secret key must be greater than length of plain text..... Impractical

Our aim :- Practically go as close as possible.

# MEASURES OF INFORMATION FLOW

## CHANNEL CAPACITY

### DISCRETE CHANNEL

What is a channel ?

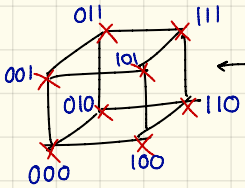
- Input alphabet $X$
- Output alphabet $Y$
- Probability Transisition Matrix $p(y|x)$

Informational Channel Capacity $C = \max_{p(x)} I(X;Y)$

i.e. maximal amount of information I can transmit through a channel

Strategy:- add redundancy at source end → Partial Information at the receiver end = Exact information sent by sender if no redundancy. Example:- Bit-flip → Send in 2 bits → error is much lesser. Suppose $A \equiv 000$, $B \equiv 111$ ∴ Now: Democratic Vote means error probability $= \frac{1}{p_{error}^2} < \frac{1}{p_{error}}$

Geometrically:




← in the Boolean Hypercube ∴ Flipping one bit → a dist. Flipping all 3 bits → a $\sqrt{3}$ dist.

↙ Hamming Distance → Metric ✓✓

(M,n) Code

- An index set $\{1,\dots,M\}$ + an encoding fn + a decoding function $Y^n$

Error Probability Conditional given index $i$

$$\epsilon_i = Pr\left[D(Y^n) \neq i \mid X^n = C(i)\right] = \sum_{D(y^n) \neq i} p(y^n|c_i)$$

∴ Maximum Error Probability $\epsilon_{max} = \max_{i \in \{1,2,\dots M\}} \epsilon_i$

Rate $R = \frac{\log_2 M}{n}$ bits per transmission

R is Achievable if ∃ a sequence $([2^{nR}], n)$ codes s.t. $\epsilon_{max} \to 0$ as $n \to \infty$.

OPERATIONAL CHANNEL CAPACITY = supremum of all achievable rates.

# SHANNON NOISY CODING THEOREM

- All rates below capacity are achievable
- $\forall R < C \ \exists$ a sequence of codes such that $\epsilon_{max} \to 0$ as $n \to \infty$
- Informational Capacity = Operational Capacity

} → 3 VERSIONS

LECTURE - 3 | 14:30 - 16:00

# QUANTUM CIRCUITS
# &
# SIMPLE QUANTUM ALGORITHMS

JOZEF GRUSKA
MASARYK UNIVERSITY

Quantum Operations → Reversible

i.e. outputs uniquely determine the inputs

Example :-

$(a,b) \to a+b$ ..... NON-REVERSIBLE

$(a,b) \to (a+b, a-b)$ ..... REVERSIBLE

$a \to f(a)$ may be irreversible but $a \to (0, f(a))$ is surely reversible

3 Reversible Classical Gate → NOT, XOR, TOFFOLI

## TIMELINE

1970: Landauer Reversibility ⇒ Minimal Energy Computation
1973: Bennett Universal Reversible Touring Machine

1984: BB84 Protocol
1985: Deutsch → Universal Quantum Touring Machine
1994: Shor Algorithm
1995: Quantum Error Correction
1996: Quantum Fault Tolerance

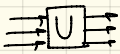
$|\psi\rangle, |\phi\rangle$ are perfectly distinguishable iff $\langle\phi|\psi\rangle = 0$

Quantum Register:- Any ordered sequence of n qubits → quantum n-qubit register

## QUANTUM GATES

Classical models:-
- finite automata
- Turing Machines
- Cellular Automata

Quantum Process:-
- Unitary Based Quantum Circuits
- " " Cellular Automata
- " " Finite Automata
- " " Touring Machine
- Measurement based Quantum Computation → No Classical Analogue



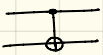
Quantum Unitary Gate (Preserves Inner Pdt)

Rotation Gates:- $R_x(\theta) = \begin{pmatrix} \cos\theta & i\sin\theta \\ -i\sin\theta & \cos\theta \end{pmatrix}$ $R_{\vec{n}}(\theta) = e^{-i\frac{\vec{n}\cdot\vec{\sigma}}{2}}$ in general

Computational Basis → $\{|0\rangle, |1\rangle\}$ ; Hadamard Basis → $\{|+\rangle, |-\rangle\}$

$\hat{\sigma}_x$ → Bit-flip
$\hat{\sigma}_z$ → changes sign → phase flip
$\hat{\sigma}_y$ → bit-phase flip

CNOT:- or XOR



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

# UNIVERSAL SET OF GATES

If every unitary operation can be approximated in terms of all

- CNOT + all 1-qubit gates
- Three gates:

$$\text{CNOT}, H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \sigma_z^{1/4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

CNOT is difficult to implement because it entangles previously non-entangled gates.

CNOT in Computational Basis → $\begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$ → diff in Bell Basis.

for the CNOT gate → Hamiltonian $H = \frac{\pi k}{2}\begin{pmatrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&1&-1 \\ 0&0&-1&1 \end{pmatrix} = \frac{\pi k}{2} V$ ⇝ Now; $e^{-i\frac{\hat{H}t}{\hbar}} =$

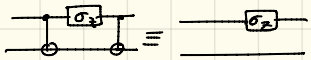
$$= \sum_{k=0}^{\infty} \frac{\left(-i\frac{\pi}{2}\right)^k V^k t^k}{k!} = \mathbb{1} + \frac{1}{2}\sum_{k=1}^{\infty} \frac{(-\pi i t)^k}{k!} V$$ ; for $t = 1$ → Gives the CNOT gate.

INVERSE CNOT →⊕→

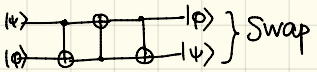
$$|0\rangle|1\rangle \xrightarrow{H} \underbrace{|+\rangle|-\rangle}_{\text{each}} \xrightarrow{\text{CNOT}} |+\rangle|+\rangle \xrightarrow{H} |1\rangle$$

SWAP GATE : ⨯ A(U) GATE: 


Identities Btwn Gates

Example: 


Generalized CNOT-Gates



## Hadamard Gates :-

$|0\rangle$ $|0\rangle$ $|0\rangle$ — $H_n$ — $|\varphi\rangle$ where $H_n(|x\rangle) = \frac{1}{\sqrt{2^n}} \sum (-1)^{x.y} |y\rangle$

## Simple Quantum Algorithms

Quantum Parallelism :- If $f = \{0,1,\ldots,2^n-1\} \Rightarrow \{0,1,\ldots,2^n-1\}$

the $f: (x,b) \rightarrow (x, b \oplus f(x))$, $\exists$ a unitary $U$ s.t. $U(|x\rangle|0\rangle) = |x\rangle|f(x)\rangle$

Let $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|0\rangle$

With a single application - $U_f|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle \rightarrow$ All $2^n$ Values of f are computed

Now

If we measure on 2nd Register in comp basis $\left[K_y = |\{x | f(x) = y\}|\right]$

$|\varphi_y\rangle = \frac{1}{\sqrt{K_y}} \sum_{\{x | f(x) = y\}} |x\rangle|y\rangle$ With Prob $= \frac{K_y}{2^n} \rightarrow$ Linear Resource (Key to Shore Algorithm)

$V_f$ operators :- $V_f|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$ where $X = \{0,1,\ldots,2^n-1\}$ can be expressed as

$U_f: |x,b\rangle \longrightarrow |x, b \oplus f(x)\rangle$ & an ancilla in $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ as follows

$U_f\left|x, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\rangle = \frac{1}{\sqrt{2}}(|x, 0\oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle) = (-1)^{f(x)}|x\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$

## DEUTSCH PROBLEM - RANDOMIZED SOLUTION

Given $f: \{0,1\} \rightarrow \{0,1\}$ as a Black Box → Our Task :- Is f constant or Balanced ? (Sholay Coin Toss)

Classical → 2 calls of f is needed.

Quantum → 1 call is sufficient → ALGO 1 :- (Success Prob = $\frac{1}{2}$)

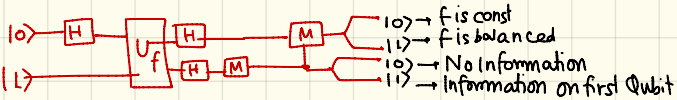
$U_f: \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$

If f is constant → Output $= \frac{1}{\sqrt{2}}(|0',0'\rangle + (-1)^{f(0)}|0',1'\rangle)$

If f is Balanced → Output $= \frac{1}{\sqrt{2}}(|p s'\rangle + (-1)^{f(0)}|1',1'\rangle)$

Now measure in Dual Basis → 50% chance that we'll end up with perfectly distinguishable states.

## CIRCUIT




## DETERMINISTIC SOLUTION

Finally, do one measurement 100% success

## Even-Odd Problem

$f: \{0,1\}^2 \to \{0,1\}$ is even if range of f has even # of ones / odd if range of f has odd # of ones.

Classically → We need 4 calls.

Quantum Mechanically → After 2 calls → Diff States but not distinguishable.

## DEUTSCH-JOZSA PROBLEM

Deutsch-Josza → (Look up Vijwal's QM-2 Notes)

$f: \{0,1\}^n \to \{0,1\}$ → Task: Is f balanced or Constant?

$$|0^{(n)}\rangle \xrightarrow{H_n} |\Phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

$$V_f|\varphi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} |i\rangle = |\Phi_1\rangle \rightarrow \text{Value of f transfered into the amplitudes.}$$

This can be utilized thru the power of quantum superposition & a proper observable.

$$\alpha = \frac{1}{2^n} \sum_i \sum_j (-1)^{f(i)} \langle i|j\rangle = \frac{1}{2^n} \sum_i (-1)^{f(i)} \quad \text{Because } \langle i|j\rangle = \delta_{ij}$$

Now, f is balanced if $\alpha = 0$ ⟶ Measurement of $|\varphi_1\rangle$ wrt D always give outcome b.

If f is constant → $\alpha = \pm 1$ ⟶ Measurement of $|\varphi_1\rangle$ wrt D always gives outcome a.

DEUTSCH-JOZSA CLASSICAL RANDOM ALGORITHM → Also doable :)

## SIMON PROBLEM

$f: \{0,1\}^n \to \{0,1\}^n$ such that either $f$ is 1-to-1 or $f$ is 2-to-1 & $\exists$ a single $0 \neq s \in \{0,1\}^n$ such that $\forall x \neq x' \left(f(x) = f(x) \Leftrightarrow x' = x \oplus s\right)$.

Exponential for all possible Classical Algorithms ; Polynomial for Quantum Algorithm

1. Apply Hadamard to first register with Initial $|0\rangle^n$
2. Apply $U_f$ to compute $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x, f(x)\rangle$
3. Apply Hadamard on first register
4. Observe the resulting state to get a pair $(y, f(x))$

Repeat these steps again & again $n$ - times.

If $\exists$ some $s \neq 0^{(n)}$ s.t. $\forall x \neq x' \left(f(x) = f(x') \Leftrightarrow x' = x \oplus s\right)$

In such a case $\rightarrow$ $\forall y, x$; $|y, f(x)\rangle$ & $|y, f(x \oplus s)\rangle$ are identical. Their total amplitude $\alpha(x,y)$ has value $= 2^{-n}\left((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}\right)$ $\therefore$ If $y \cdot s = 0 \bmod 2$ then $|\alpha(x,y)| = 2^{-n+1}$ otherwise $\alpha(x,y) = 0$

If $f(0) \neq f(s)$ then $f$ is one-to-one. If else $\rightarrow$ two-to one.

SHOR'S ALGORITHM $\rightarrow$ Next day

LECTURE - 4 16:30-18:00

# PRE-QUANTUM CRYPTOGRAPHY

GAUTAM PAUL
ISI KOLKATA

Shannon → Communication Theory of Secrecy Systems
Bell System Journal Technology (1949)

What is Cryptology ?

Targets :- 1) Confidentiality
2) Data Integrity (Ensures authenaity of the data)
3) Authentication (Ensures authencity of the source of the data)
4) Non-Repudiation (Can't deny the data)

# CONFIDENTIALITY

Cryptosystem = $\{P, C, K, \mathcal{E}, \mathcal{D}\}$

$P$ = finite set of possible plaintexts; $C$ = finite set of possible ciphertexts
$K$ = finite set of keys with . Encryption fn $e_k \in \mathcal{E}$ $(P \to C)$ & decryption fn $d_k \in \mathcal{D}(C \to P)$

Goal of Adversary :- Any of the following

1. Secret Disclosure
2. Distinguishing Attack
3. Transformations on the ciphertext to produce meaningful changes in the plaintext (Malleability)

Passive Adversary → Only monitors the communication channel.
Active " → Add, delete or Change the Data in Channel.

## ATTACK MODELS

CIPHERTEXT ONLY ATTACK → Attacker knows certain ciphertexts
KNOWN PLAINTEXT ATTACK → The attacker knows $(M_1, C_1) \ldots\ldots (M_t, C_t) \Rightarrow$ Target :- find the key $M^*$ corresponding to a new ciphertext $C^*$

CHOSEN PLAINTEXT ATTACK → The attacker chooses a few $\{M_i, C_i\}$ and then model the Black-Box as an Oracle.

CHOSEN CIPHERTEXT ATTACK → Attacker has temporary control over decryption devices

## CRYPTOGRAPHIC SECURITY

Kerckhoff (1883) :- The Security of a cipher relies only the secrecy of the keys _ you can bring the algos to open source

Rationale :-
- ⊙ Easy to maintain secrecy of a secret key than an algorithm
- ⊙ Easy to change a compromised key than a compromised algorithm
- ⊙ For many pairs of communicating parties → $O(n^2)$ different algorithms needed for mutual secret communications → Impractical
- ⊙ If ∃ a serious algorithmic vulnerabilities → Experts can point it out if it's open domain
- ⊙ Public Design enables establishment of standards

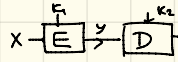
# SECURITY MODELS

**Perfect Secrecy** :- Can't be broken even with ∞ computation resource.

**Computational Secrecy** :- Best known algo for breaking the algorithm requires at least n-operations where n is some specified very large number.

**Provable Secrecy** :- The cryptosystem is as difficult to break as some well known & hard problem (RSA & Factorization)

# SYMMETRIC KEY CRYPTOGRAPHY

most general scenario → 

; By Definition $E_{k_1}^{-1} = D_{k_2}$

Symmetric Key Cryptography ⟹ $K_1 = K_2 = K$

## BLOCK CIPHER

Message is divided into fixed group of bits (Blocks)

Each Block is Encrypted by the same key

Length of Block publicly known

### KEY DESIGN CRITERIA

Good Diffusion + Good Confusion

- Diffusion: dissipation of redundancy in statistics of plaintext in the statistics of ciphertext
- Confusion: Making the statistical relation between a key & corresponding ciphertext as complex as possible

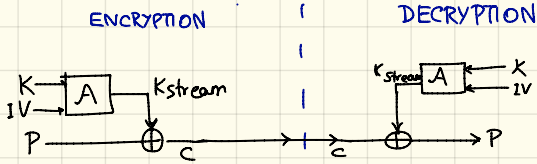
Example :- Caesar Cipher (Most well known)

- Primitive Shift Cipher
- Affine Cipher
- Vigenère Cipher
- Hill Cipher
- Permutation / Transposition Cipher

## STREAM CIPHER

Consider data is a stream of bits.

Real time Encryption




Why XOR ? → Same # of 0 & 1 in output → bitwise XOR ≡ modulo 2 addition

for security keystream size = message size → Impractical

ONE TIME PAD

Practical Solution :- Have a Keystream Generator, Have a secret key ↓ These together generate pseudo random keystream

SEED = SECRET KEY → SHORT ; Keystream Generator → Long Keystream } → Best of both worlds...

Real Challenge :- Good Random Number Generation

- Substitution Cipher
- Permutation + Substition (Good modern Block Cipher) (Iterated Block Cipher)
- DES, AES } → Roughly this substitution + Permutation paradigm

SYMMETRIC KEY :- ADVANTAGES :- Fast. Very High Security

BUT If one user is compromised → everything compromised.

Plus; How to distribute the Secret Key in the first place?

## ASYMMETRIC / PUBLIC KEY CRYPTOGRAPHY

$K_1$: Public ; $K_2$ = Secret & the receiver will publish $K_1$ publicly.

No key sharing problem.....

for n users with Symmetric Key → need $\binom{n}{2} = \mathcal{O}(n^2)$ secret keys
for n users with asymmetric key → need only $2n$ secret keys } Advantages

So; what's the Rub ? Speed goes down .....

Can we get best of both worlds ?

## FURTHER

Is the data unchanged? → Hash Function

Is the data unread ? → Quantum Tracing (No Cloning)

## NON-REPUDIATION

A ← $E_{K_1}$ B } → Digital Signature → Alice will apply $D(k_2)$ on a document M | $S = D_{k_2}(M)$ (Signature)

A: $K_1, K_2$ (Public, Private)

Now Alice claims anybody can verify the signature $E_{k_1}(S) = E_{k_1}(D_{k_2}(M)) = M$

Public Verifiability

OTHER FACETS :-
- Broadcast Encryption
- Secret Sharing
- Zero-knowledge Proof
- Identify Friend / Foe
- Key Establishment

DAY - 2

LECTURE - V

09:30 - 11:00

# DEATH & REBIRTH OF CLASSICAL CRYPTOGRAPHY IN A QUANTUM WORLD

GOUTAM PAUL

ISI KOLKATA

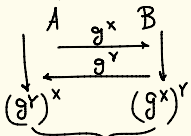
---

## Asymmetric / Public Key Cryptography

1) Diffie Hellmann → 2) RSA

### Diffie Hellmann

$\mathcal{G}$ = Common multiplicative group (generator $g$)




Alice doesn't knows $Y$
Bob doesn't knows $X$
} $g$ is known to everybody

Knowing $(g, g^x, g^y) \rightarrow g^{xy}$ is hard to predict

$\equiv$ Discrete logarithm problem

Hard to Solve

## KNAPSACK

$S = \{a_1 \dots a_n\}$ → Given A : Goal ⇒ find a subset $T \subseteq S$ s.t. $\sum_{i \in T} a_i = A$

⇓

Difficult (bcz # of subsets of a set scales exponentially.

## Goldwasser - Micali

Given X, N find y such that $x = y^2 \bmod N$ (Quadratic Residue)

↓

Hardness Number Theoretically ≡ Factoring

ElGamal Based on discrete logarithm

Elliptic Curve Cryptography (1985) → Much faster than RSA

## Paillier (1999)

Given X, N ∃ a y such that $x = y^N \bmod N$ → find y (extension of quadratic residue)

## Cramer Shoup (1998)

Discrete Logarithm based

## RSA

Key Generation Based on → Factoring into Primes is hard.

- Choose two large primes p & q

- $N = pq$
- Take $\phi(N) = (p-1)(q-1)$ (Euler Totient Function)
- Choose $e \in \mathbb{Z}^+$ such that $\gcd(e, \phi(N)) = 1$ } $a^{-1} \bmod N$ exists iff $\gcd(a, N) = 1$ (Fermat Little Thm. Corollary)
- Compute $d$ such that $ed = 1 \pmod{\phi(N)}$ }

**KEY DISTRIBUTION**

Public Key → $\{N, e\}$
Private Key → $\{N, d\}$

**ENCRYPTION**

Ciphertext
$C = M^e \bmod N$

**DECRYPTION**

Plaintext
$M = C^d \bmod N$
$= (M^e \bmod N)^d \bmod N$
$= M^{1 + \bmod(\phi(N))}$ } Euler Theorem
$= M$ .... (Verified)

To attack → attacker must know $d$ or $\phi(N)$ → If he knows $\phi(N)$ → Use extended Euclid → Cracked!

But knowing $N$ → finding $\phi(N)$ is factoring → If you can factor $N$ → DONE!

## QUANTUM ATTACKS ON CLASSICAL ALGORITHMS

$f(x) = f(x+r)$ $\forall$ $x = \{0, 1, 2, \ldots, M-1\}$ → finding the exact period is hard classically

QM:- Create $\frac{1}{\sqrt{M}} \sum_x |x\rangle |f(x)\rangle$

Measure the last $m$ bits:- for an output $y = f(x_0)$ with smallest $x_0$ (out of many inputs possible).

Take the Quantum Fourier Transform

Easy to Solve

ORDER FINDING PROBLEM → find order of an element $a$ given $N \in \mathbb{Z}[>2]$ & $a \in \mathbb{Z}_N^*$
Classically Hard, but Quantum Period Finding Helps

## Order Finding → Factoring

$a^r \equiv 1 \bmod N \;\therefore N \mid a^r - 1 \rightsquigarrow$ if $r$ is even $N \mid (a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1)$

$\therefore$ either $N \mid (a^{\frac{r}{2}} - 1)$ or $N \mid (a^{\frac{r}{2}} + 1)$ or $N = pq$ s.t. $p \mid a^{\frac{r}{2}} - 1$, $q \mid a^{\frac{r}{2}} + 1$

But $a^{\frac{r}{2}} \equiv 1 \bmod N$ is contradiction since $r$ is defined to be the smallest integer such that $a^r \equiv 1 \bmod N$ → Similarly second

Only left is the third possibility....

if $N \mid a^{\frac{r}{2}} + 1 \rightarrow \gcd(N, a^{\frac{r}{2}} - 1)$ gives the factor of $N$

Fastest Classical Algorithm $\rightsquigarrow O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$

Shor Algorithm $\rightsquigarrow O((\log N)^2 (\log\log N)(\log\log\log N)) \rightsquigarrow$ Cubic Scaling

Record → 56153 (PRL 2012)

## QUANTUM KEY DISTRIBUTION

Goal:- Share Secret Key in QM → Then use Classical Key

This is the Only thing Quantum in Quantum Cryptography

Semi Quantum QKD: Boyer, Kenigsberg, Mor (PRL 2007) → Alice is Quantum

→ Bob is Semiquantum (Only can measure in $\{|0\rangle, |1\rangle\}$ not $|+\rangle, |-\rangle$)

→ Same Security as BB84

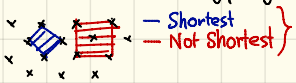
## NON-QKD QUANTUM CRYPTOGRAPHY

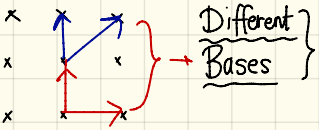
- Quantum Commitment
- Quantum Secure multiparty Communication
- Position Based Quantum Cryptography

# POST-QUANTUM CRYPTOGRAPHY

## Public Key Cryptography (Classical) Not Vulnerable to Quantum Algorithms

- Lattice-based cryptography (e.g. NTRU)




- Multivariate Cryptography (Rainbow)
- Hash-based Cryptography (Lamport, Merkle)
- Code-Based Cryptography → Decrypting a linear code is hard (McEliece, Niederreiter)
  - Encryption → Noise Added
  - Decryption → Noise Dropped

- Supersingular ECC

LECTURE - 6

11:30 - 13:00 Day - 2

# SEMINAL QUANTUM ALGORITHMS

JOZEF GRUSKA

## Integer Factorization

Classically Hard Problem.....

Modulo Operation ; Euclid GCD Algorithm

↓

$\gcd(0,n)=n$

$\gcd(m,n) = \gcd(n \bmod n, m)$ for $m>0$

e.g. $\gcd(296,555) = \gcd(296,259) = \gcd(37,259) = \gcd(0,37) = 37$

## RSA Cryptosystem

- Choose large primes $p$ & $q$ (How to ensure $p$ & $q$ are prime ? → New deterministic algo exists)
- compute $n = pq$; $\varphi(n) = (p-1)(q-1)$
- Choose a large $d$ s.t. $\gcd(d, \varphi(n)) = 1$
- compute $e = d^{-1} \pmod{\varphi(n)}$

Public key :- $(n,e)$ Private Key $\rightarrow (n,d)$

Gardner :- Sci Am 1977 $\rightarrow$ RSA Challenge

## RSA Signature

What happens if we first apply $c = w^d$, then $c^e$? $\rightarrow$ Digital Signature...

## Reductions of the Factorization Problem

(1) Lemma :- $a^2 \equiv 1 \pmod n$ solving is $\equiv$ factorization

$(a^2-1) \equiv 0 \bmod n \;\therefore\; (a-1)(a+1) \equiv 0 \bmod n$

(2) finding period of a function $f_{n,x}(k) = x^k \bmod n$ $\rightarrow$ Period is the smallest integer $r$ s.t. $f_{n,x}(k+r) = f_{n,x}(k)$ i.e smallest $r$ s.t. $x^r \equiv 1 \bmod n$

SHOR ALGORITHM SCHEME $\rightarrow$ All steps are easy except period finding.

STEP-1 :- for given $n$, $q = 2^d$ & create state

$$\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |n,a,q,x,0\rangle \Big\} \rightarrow \text{Can be done using Hadamard Transform}$$

$$\& \; \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |n,a,q,x,a^x \bmod n\rangle$$

STEP-2 :- By measuring the last register the states collapse into $\frac{1}{\sqrt{A+1}} \sum_{j=0}^{A} |n,a,q,jr+l,y\rangle$ or shortly $\frac{1}{\sqrt{A+1}} \sum_{j=0}^{A} |jr+l\rangle$ where $A$ is the largest integer such that $l + Ar \leq q$ ($r$ = period of $a^x \bmod n$ & $l$ is the offset

STEP-3 :- In case $A = \frac{q}{r} - 1$ ; resulting state has the form $\sqrt{\frac{r}{q}} \sum_{j=0}^{\frac{q}{r}-1} |jr+l\rangle$

STEP-4 :- By Applying Quantum Fourier Transform

$$\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{\frac{2\pi i l j}{r}} \left|j \tfrac{q}{r}\right\rangle$$

Step 5 :- By measuring the resulting state we get $c = \frac{jq}{r}$ & if $\gcd(j, r) = 1 \rightarrow$ very likely that from $c$ & $q$ we can find the period $r$.

## Discrete Fourier Transform

$$DFT(a) = A_n a$$

$$A_n = \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \\ 1 & & \omega & & \\ \vdots & & & \ddots & \\ & & & & \end{bmatrix}$$

## Quantum Fourier Transform

$$\{f(0), f(1), \ldots, f(q-1)\} \xrightarrow{QFT} \{\bar{f}(0), \bar{f}(1), \ldots, \bar{f}(q-1)\}$$

$$\bar{f}(c) = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} e^{\frac{2\pi i}{q} ac} f(a)$$

## Quantum Version of FT ≡ Unitary Transfn

$$F_q = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 & & \\ 1 & \omega & & \\ 1 & \omega & \omega^4 & \\ & & & \ddots \end{pmatrix}$$

$$|0\rangle \xrightarrow{QFT_q} \frac{1}{\sqrt{q}} \sum_{i=0}^{q-1} |i\rangle$$

## Quantum Parallelism

If $f: \{0, 1, \ldots, 2^n - 1\} \Rightarrow \{0, 1, \ldots, 2^n - 1\}$ then the mapping $f: (x, b) \Rightarrow (x, b \oplus f(x))$ where $x, b \in \{0, 1, \ldots, 2^n - 1\}$

In one step $2^n$ values of $f$ are 'computed'

## Impact of Projective Measurements

Measuring Second register in the standard basis $\rightarrow |\phi\rangle$ collapses into one of the states

$$|\phi_y\rangle = \frac{1}{\sqrt{k_y}} \sum_{\{x | f(x) = y\}} |x\rangle |y\rangle \text{ where}$$

- $y$ is in the range of values of function $f$
- $k_y = |\{x | f(x) = y\}|$

## Shor Algorithm :- Phase - 1

Given $n \in \overbrace{\mathbb{Z}}^{m \text{ bit}}$ Choose a $n^2 \leq q = 2^d \leq 2n^2$ (This can always be done)

Application of Hadamard to the 4th register $\Rightarrow \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |n, a, q, x, 0\rangle$

Now use Quantum parallelism. Compute $a^x \bmod n \ \forall x$ in one step to get $\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x, a^x \bmod n\rangle$

Now measure on the last register. Let $y$ be the value obtained i.e. $y = a^l \bmod n$ for smallest $(l, y)$ with this property. If $r$ is the period of $f_{n,a}$ then the measurement actually selects the sequence of $x$'s values (in the fourth register)

## SHOR ALGORITHM - SECOND PHASE

Consider spl. case $\rightarrow r \mid q \Rightarrow A = \frac{q}{r} - 1$ & last state $= |\varphi_l\rangle = \sqrt{\frac{r}{q}} \sum_{j=0}^{q/r-1} |jr + l, y\rangle$ & after $QFT_q$ is applied to $|\varphi_l\rangle$ we get: $QFT_q(|\varphi_I\rangle) = \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \frac{r}{q} \sum_{j=0}^{q/r-1} e^{\frac{2\pi i c(jr+l)}{q}} |c\rangle$

$= \frac{\sqrt{r}}{q} \sum_{c=0}^{q-1} e^{\frac{2\pi i l y c}{q}} \left( \sum_{j=0}^{q/r-1} e^{\frac{2\pi i j c r}{q}} \right) |c\rangle = \sum_{c=0}^{q-1} \alpha_c |c\rangle \rightarrow$ If $c$ is a multiple of $\frac{q}{r}$ then $e^{\frac{2\pi i j c r}{q}} = 1$

If $c$ is not a multiple of $\frac{q}{r}$ then $\sum_{j=0}^{\frac{q}{r}-1} e^{\frac{2\pi i j c r}{q}} = 0 \rightsquigarrow$ Can't get such $c$ by measurement (otherwise amplitude $= 0$)

This implies $\alpha_c = \begin{cases} \frac{1}{\sqrt{r}} e^{\frac{2\pi i l y j}{r}} & \text{if } c \text{ is a multiple of } q/r \\ 0 & \text{otherwise} \end{cases}$

$\Rightarrow |\varphi_{out}\rangle = QFT_q |\varphi_l\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{\frac{2\pi i l y j}{r}} |j \frac{q}{r}\rangle \rightarrow$ Trouble making offset now appears on the phase exponent only.

## SHOR ALGORITHM - THIRD PHASE

### Period Extraction

If $\gcd(\lambda, r) = 1$ then from $q$ we can determine $r$ by dividing $q$ with $\gcd(c, q)$. Since $\lambda$ is chosen randomly; $\gcd(\lambda, r) = 1$ is $> \Omega\left(\frac{1}{\log\log r}\right) \therefore \mathcal{O}(\log\log r) \ldots$ (solution time)

General Case when $A \neq \frac{q}{r} - 1 \rightarrow$ Use continuous fractions

Key Idea :- Quantum Fourier Transform

## Analysis of SHOR ALGORITHM

# of Steps: $O(\log \log \log N)$

Quantum Fourier Transform: Efficient Implementation

↓

Since each such state are pdt states

↓

NOT ~~that~~ hard to implement

## HIDDEN SUBGROUP PROBLEM

Related to Calculation of discrete logarithm problem

PROBLEM :- Given a group Group $G$, finite set $R$ & an efficiently computable fn $f: G \to R$

And Promised that $\exists$ a subgroup $G_0 \subseteq G$ s.t. $f$ is constant & distinct on the cosets of $G$ defined by $G_0$

Task :→ Find a generating set for $G_0$ (in a polynomial time (in $\log |G|$) wrt the # of calls to the oracle for $f$ & in the overall polynomial time)

↓

Hidden Subgroup Problem

OPEN :- IS THERE ANY EFFICIENT ALGORITHM FOR NON-ABELIAN HIDDEN SUBGROUP PROBLEM ?

# GROVER SEARCH PROBLEM

Sorting :- Classically $O(N)$

Quantum $O(\sqrt{N})$

LECTURE - 7

14:30 - 16:00

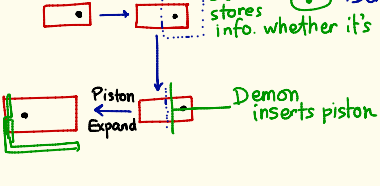
# QUANTUM INFORMATION THEORY

Sibasish Ghosh

---

Benefit of Going Quantum : ↗ More Efficient Storage
↘ More Efficient Coding & Compression

## Szilard Engine




} Full Conversion of heat → work ??
} Erasing Information cost energy (Landauer) $k_B T \ln 2$

## Benett's Resolution of Maxwell Demon

Damon has memory whether fast / slow → system is converted to original state iff this memory is erased

Requires $k_B T \ln 2$ work to erase each bit of information ← Resolution of Maxwell Demon

## Noisy Quantum Systems

Stern-Gerlach output state $|\alpha|^2 |\uparrow\rangle\langle\uparrow| + |\beta|^2 |\downarrow\rangle\langle\downarrow|$ } → Mixed state

Properties :- i) $\rho \geq 0$ ii) $\mathrm{Tr}(\rho) = 1$ iii) $\rho^2 \leq \rho$ [= → pure state]

## Reduced Density Matrix

$$|\psi\rangle = \sum_i \sum_j \lambda_{ij} |i\rangle_A \otimes |j\rangle_B \rightarrow \rho_A = \mathrm{tr}_B \left( |\psi\rangle\langle\psi| \right) = \sum_m \langle m_B | \sum_{i,j} \lambda_{ij} |i_A\rangle \otimes |j\rangle_B \sum_{i',j'} \lambda_{i'j'} \langle i_A | \otimes \langle j_B | m_B \rangle$$

$$= \sum_m \sum_{i,j,i',j'} \lambda_{ij} \lambda_{i'j'} \langle m_B | j_B \rangle |i_A\rangle\langle i'_A| \otimes \langle j'_B | m_B \rangle = \sum_{i,j,i',j'} \lambda_{ij} \lambda_{i'j'} \delta_{j'm} \delta_{jm} \lambda_{ij} \lambda_{i'j'} |i\rangle\langle i'|$$

## POVM vs. PVM

POVM → $M = \{E_j\}$ such that $\sum_j E_j = \mathbb{1}$

POVM ≡ PVM in Higher Dimension

$|\psi_1\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$ ; $|\psi_2\rangle = \cos\frac{\theta}{2}|0\rangle - \sin\frac{\theta}{2}|1\rangle$ ⟶ Task:- Somebody prepared this state either in $|\psi_1\rangle$ & $|\psi_2\rangle$ find out which is it?

Inconclusive to distinguish btwn them.....(using PVM's).

Distinguishable using a 3-element POVM

$E_1 = X|\psi_1^\perp\rangle\langle\psi_1^\perp|$ ; $E_2 = X|\psi_2^\perp\rangle\langle\psi_2^\perp|$ ; $E_3 = \mathbb{1} - E_1 - E_2$ where $0 < x < 1$ & $E_3 \geq 0$ → This condition gives

If $E_1$ clicks → inputstate must be $|\psi_2\rangle$
If $E_2$ clicks → " " " $|\psi_1\rangle$
If $E_3$ clicks → " may be either $|\psi_1\rangle$ or $|\psi_2\rangle$.

⇒ Unambiguous discrimination of non-orthogonal States.

Post measurement State $= \mathrm{Tr}_A\left[\frac{\langle\psi_i|(\rho\otimes|0\rangle_A\langle 0|)|\psi_i\rangle_A\langle\psi_i|}{\langle\psi_i|(\rho\otimes|0\rangle_A\langle 0|)|\psi_i\rangle}\right]$ → Initial correlations nothing Changes

↓ Not always is the post measurement state of the Lüders type.

Most general measurement → POVM

DYNAMICS → Schrödinger Eqn → Unitary dynamics. But difficult to get Unitary Dynamics.

But Open System ≡ Larger Isolated System + Environment

$\rho^{out} = \mathrm{tr}_E\left[e^{-i\frac{\hat{H}_{tot}}{\hbar}t}(\rho\otimes|0\rangle_A\langle 0|)\,e^{+i\frac{\hat{H}_{tot}}{\hbar}t}\right]$ → CPTP map

$= \sum_j A_j(t)\,\rho\,A_j^\dagger(t)$ .... $\{A_j\}$ → Kraus Operators ; $\sum_j A_j^\dagger(t)A_j(t) = \mathbb{1}$

Reverse question :- given a CPTP evolution ≡ Unitary Operation on a larger Hilbert Space

$\mathcal{N}$ (True)

Explicit Construction of Unitary :- Look up ☺

This unitary may not be unique for a given CPTP map

↓

Interaction Hamiltonian also not unique

Kraus Operators are also not unique

↓

See Mark Wilde for Proof

$\{A_i = \sum_j u_{ij} B_j$ say → then $U$ is an isometry $\}$

then $\{B_j\}$'s are also perfectly good Kraus Operators

Non Unitary Character :- $\mathcal{N}$ is a linear map

1) $\mathcal{N}$ is Hermiticity Preserving $\{\mathcal{N}(A)\}^\dagger = \mathcal{N}(A)$ $\forall$ $A^\dagger = A$
2) $\mathcal{N}$ is trace preserving $Tr[\mathcal{N}(A)] = Tr[A]$
3) $\mathcal{N}$ is positivity preserving
4) $\mathcal{N}$ is Completely Positive $(\mathcal{N} \otimes \mathbb{1}_A)\, B \geq 0$ $\quad \forall\ B \geq 0$

3) is a spl. case of 4)

linear → bcz this is Quanta ☺

Hermiticity & Trace Preserving → Since should map density matrices into density matrices

CP → Required to map every bipartite density matrix to a bonafide density matrix

Ensures $\rho_{AB} \xrightarrow{\Lambda_A \otimes \mathbb{1}_B} \sigma_{AB}$ is still a density matrix.

Example :- (TRANSPOSE) → NOT a CPTP map because it violates complete positivity

$$\rho_S \to \sum_{i,j} \rho_{ij} |i\rangle\langle j| \xrightarrow{\mathcal{N}} \sum_{i,j} \rho_{ji} |i\rangle\langle j|$$

$\mathcal{N}_{ij,kl} = \delta_{il}\delta_{jk}$

$(\mathcal{N}(A)^\dagger)_{ij} = A^\dagger_{ji} = A_{ji} = (\mathcal{N}(A))_{ij}$ → Hermiticity Preserving

But take $\rho_{AB} = |\phi^+\rangle\langle\phi^+|_{AB}$ → $\mathcal{N}(\rho_{AB}) < 0$ → Violates Complete Positivity

↓

Transpose ≡ Going Backward in time is not possible

# HUGSTON - JOZSA - WOOTTERS THEOREM

Every mixed state $\rho$ has infinitely many pure state ensemble representation

A mixed state has infinitely many pure state representation

Example:- $\rho = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) = \frac{1}{2}\left(|+\rangle\langle +| + |-\rangle\langle -|\right) = \frac{1}{2}\left(|\nearrow\rangle\langle\nearrow| + |\nwarrow\rangle\langle\nwarrow|\right) \ldots\ldots$

Tomorrow:- Quantum Channels & Channel Capacity

LECTURE - 8 | 16:30 - 18:00

# QUANTUM CORRELATIONS

Debasis Sarkar
Calcutta University

---

1935 :- Einstein, Podolski, Rosen (EPR Paradox)

1952 :- EPR Interms of Bohm's Spin $\frac{1}{2}$ Representation $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$

1957 :- Gleason's Theorem

1964 :- Bell's Paper → Local HVT's incompatible with Quantum Mechanics

1968 : Kochen Specker → $\begin{Bmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{Bmatrix} \begin{Bmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{Bmatrix}$ Now assume $A_k = B_l$ for some $k \& l$

↓ (some observable common to both sets)

1993 RMP Mer - min

$[A_k, A_l] = [B_r, B_l] = 0$

↓

With 117 vectors → This will give you a contradiction.

↓

Where's the rub ? Value of $A_k$ = Value of $B_l$ always (assumed)

Contextuality !

Moral :- Hidden-Variables must not be non-contextual.

Common to all these things ⇒ Composite Quantum Systems

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$$

$|\Psi\rangle_{ABC} = |\chi\rangle_A \otimes |\xi\rangle_B \otimes |\eta\rangle_C$ is the one possibility.

Now linearity implies $|\chi_1\rangle \otimes |\xi_1\rangle \otimes |\eta_1\rangle + |\chi_2\rangle \otimes |\xi_2\rangle \otimes |\eta_2\rangle$ is also legit

But this is ← state Entangled in general

# ENTANGLEMENT

If $\rho_{ABC} = \sum_i \omega_i \rho_i^A \otimes \rho_i^B \otimes \rho_i^C$ → Then Separable ; Otherwise Entangled

$(0 \le \omega_i \le 1 \;\&\; \sum_i \omega_i = 1)$

Physical Realization → Separable States can be prepared locally

FOR BIPARTITE PURE STATES

$|\psi\rangle_{AB} = \sum_{i,j} \alpha_{ij} |i\rangle_A \otimes |j\rangle_B$ → from Singular Value Decomposition Theorem one can always write this as $= \sum_{k=1}^{N} |k_A\rangle \otimes |k_B\rangle$ in some other basis → (Schmidt Decomposition)

If $N=1$ → Separable

But for multipartite states → no unique Schmidt Decomposition → Can't be done

Bipartite Systems:- Q) Is it Entangled ?
Q) If yes - How much Entanglement ?

Entanglement Quantification in terms of Teleportation Protocol

Compare States in terms of their Entanglement ... → Take Singlet (Original Benett Protocol) → 100% Exact Teleportation ; But take some other initial state → inexact teleportation → In terms of fidelity wrt target

Suppose we have a state like $a|00\rangle + b|11\rangle$ ..... allowed operation = LOCC

Under LOCC → $\rho^{\otimes n} \longrightarrow \sigma^{\otimes m}$ $[m < n]$ (Entanglement concentration) $m = n\,(S(\rho_A))$ → Benett et al ...

$\rho$: Less Entangled ; $\sigma$: highly entangled

Schumacher Noiseless Data Compression Theorem → Allows the reverse process

$\Rightarrow S(\rho_A)$ = Entanglement of a pure bipartite state → Easily Calculable

What about mixed Bipartite States ?

Two Defns → 1) Distillable Entanglement
2) Entanglement of formation
} ≠ for mixed states

$EOF(\rho_{AB}) = \inf \sum_i p_i E(|\psi_i\rangle_{AB})$ over all pure state decompositions $\rho_{AB} = \sum_i p_i |\psi^i_{AB}\rangle\langle\psi^i_{AB}|$

Distillable Entanglement $= \lim_{n\to\infty} \frac{m}{n}$

But these optimizations are hard to do :(

PROPERTIES A GOOD MEASURE OF ENTANGLEMENT MUST SATISFY

- Vanishes for Separable State
- LU-invariant
- Monotone decreasing under LOCC
- Additivity, Convexity, Continuity → NOT Necessary but desirable (like Sixpack abs :))

Hastings → EoF is not additive (Recent Result)

One good candidate with all those properties → Squashed Entanglement (Winter)

↓

But notoriously hard to calculate (Winter :))

LOG-NEGATIVITY / CONCURRENCE (2x2) → Easy to Calculate

↓ Easy to Calculate

$\sim \log |N|$

N = Negativity

↓ (under Partial Transpose)

Additive but not convex (Plenio)

↓ EoF = Simple fn of Concurrence

Squashed Entanglement → Depends on Quantum Mutual Information ... So Good for Channels

DETECTION OF ENTANGLEMENT

Prob:- Given $\rho_{AB}$ is it entangled / separable ?

Initially people thought → Bell Violation ≡ Entanglement

But for Werner States $p|\phi^-\rangle\langle\phi^-| + \frac{(1-p)}{4}\mathbb{1}_4$ → if $p > \frac{1}{3}$ → Entangled

Possible to have no Bell Violation even with Entanglement | But $p > 0.707\ldots$ → Bell Violation


## PARTIAL TRANSPOSE

If you have an operator which is +ve but not CP → Will Serve as a detector (Hahn-Banach)

(e.g. Transpose Operator)

$\tilde{\rho}_A = (\rho_{AB})^{T_B}$ = Partial Transpose on B
$\tilde{\rho}_B = (\rho_{AB})^{T_A}$ = Partial Transpose on A

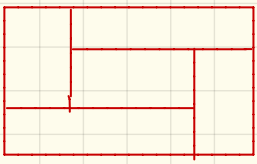
If all eigenvalues of $\tilde{\rho}_A$ are $\geq 0$ → PPT states
If at least one -ve eigenvalue → NPT states → Entangled for sure

But does PPT ⇒ Separable ?

2×2, 2×3 ⟶ true

for higher dimensional states ⟶ False → ∃ Bound Entangled State (Entangled but not distillable)

### Example of a PPT Entangled State in 3×3 systems



$|0\rangle \otimes \frac{|1\rangle \pm |2\rangle}{\sqrt{2}}$ $\quad \frac{|0\rangle \pm |2\rangle}{\sqrt{2}} \otimes |2\rangle$

$|2\rangle \otimes \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ $\quad |1\rangle \otimes |1\rangle$

$\frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \otimes |0\rangle$

→ Unextendible Product Basis

⇓

Implies Existence of Bound Entangled States

Here $\rho = \left[\mathbb{1} - \sum_{i=1}^{5} |\phi_i\rangle\langle\phi_i|\right]$ ⟶ Bound Entanglement

EoF > 0 But Distillable Entanglement = 0

### Reduction Criteria Violation ⟹ Distillable

$U \otimes U^*$ invariant states ≡ $\mathbb{1} + \beta P^+$ [Isotropic States] where $P^+_{d-1} = \sum_{i=0}^{d-1} \frac{|ii\rangle}{\sqrt{d}}$

Either Separable / Distillable

Definite form of Entanglement available

$U \otimes U$ invariant states ≡ $1 + \beta V$ [Werner States] → Satisfies Reduction Criteria → Can be Bound Entangled

$\rho_{AB}$ → if you find $|\psi\rangle$ of rank=2 and $\langle\psi|\underbrace{\rho_{AB}^{T_A}}_{\text{(Partial Transpose)}}|\psi\rangle < 0 \rightarrow$ Distillable

$> 0 \rightarrow$ One copy undistillable

⋮

Similarly n-copy undistillability

Tomorrow :- Multipartite Entanglement, Non Classical Correlations Beyond Entanglement

DAY-3

LECTURE 9 09:30 - 11:00

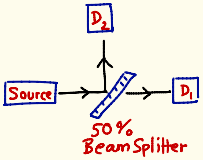
# QUANTUM FOUNDATIONS - UNCERTAINTY PRINCIPLE

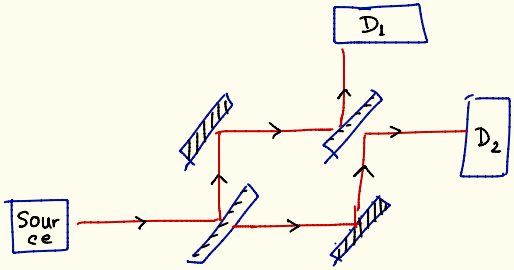
Guruprasad Kar

ISI Kolkata

---

## DETECTING A HIGHLY SENSITIVE BOMB WITHOUT EXPLODING ONE



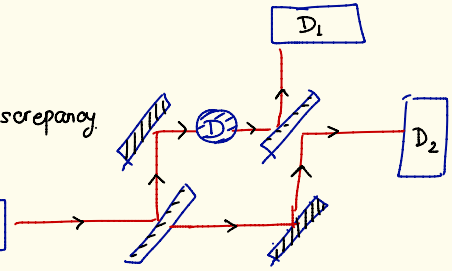

Classically I expect 50% of photons to be detected in $D_1$ & 50% in $D_2$

Quantum Mechanically (Experimentally) → all of the photons in either in $D_1$ or in $D_2$

Conclusion:- Collapsed !!!

QM was born to explain this kind of discrepancy

What happens when a detector D is placed?



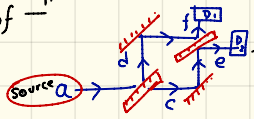

Ans:- Interference Pattern is lost

Back to Classical 50-50 kind of mixture

## How the Beam Splitter Works ?

$|u\rangle \xrightarrow{BS} \sqrt{T}\,|x\rangle + \underbrace{i\sqrt{R}}_{\text{Phase Change of } \frac{\pi}{2}}\,|y\rangle$ $\quad [R+T=1]$ $\{|x\rangle, |y\rangle$ correspond to different output paths$\}$

$|v\rangle \xrightarrow{BS} i\sqrt{R}\,|x\rangle + \sqrt{T}\,|y\rangle$ $\Big\}$

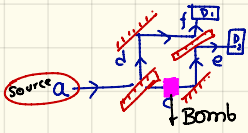



Take $R=T=\frac{1}{2}$

$$|a\rangle \xrightarrow{BS_1} \frac{1}{\sqrt{2}}(|c\rangle + i|d\rangle) \xrightarrow{BS_2} \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(i|e\rangle + |f\rangle) + \frac{i}{\sqrt{2}}(|e\rangle + i|f\rangle)\right] = i|e\rangle$$

$\therefore$ All the particles will be collected in the detector $D_2$

Now on one arm → ⊣ a very sensitive Bomb at $D_1$ → No Blast but detection




If Bomb is there

$$|a\rangle \to \frac{1}{\sqrt{2}}(|c\rangle + i|d\rangle) \to \frac{1}{\sqrt{2}}|\text{☆}\rangle + i\frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(i|e\rangle + |f\rangle)\right]$$

$$\downarrow$$

$$\frac{1}{\sqrt{2}}|\text{☆}\rangle - \frac{1}{2}|e\rangle + \frac{1}{2}i|f\rangle$$

So; Probability of Explosion = 50% → Failwe

Probability of detection in $D_1$ = 25% → Success

Probability of detection in $D_2$ = 25% → No Conclusion

Can we make success probability 100% ? (Experimentally 73%)

Theoretically yes - using photon polarization.

Polarization Rotator :- $|H\rangle \longrightarrow \cos\left(\frac{\pi}{2N}\right)|H\rangle + \sin\left(\frac{\pi}{2N}\right)|V\rangle$

Probability of passing through the polarization = $\cos^2\left(\frac{\pi}{2N}\right)$

After many iterations → $|H\rangle$ becomes $|V\rangle$ & nothing passes through

Probability of passing through after n-iterations $P_N = \left(\cos^2\frac{\pi}{2N}\right)^N$

$= \left(1 - \sin^2\frac{\pi}{2N}\right)^N \to 1$ as $N \to \infty$

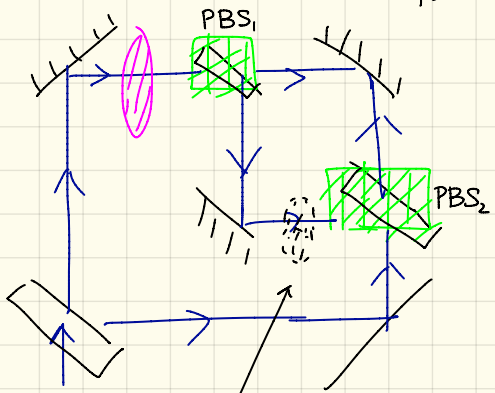
NOW WE INTRODUCE A POLARIZATION BEAM SPLITTER

Transmits horizontally polarized photons, reflects vertical polarized photons

$\left(\cos\alpha|H\rangle + \sin\alpha|V\rangle\right)|a\rangle \xrightarrow{PBS} \cos\alpha|Hb\rangle + \sin\alpha|Vc\rangle$

But this splitter ≡ measurement on polarization state of the photon

No Interference Pattern ←




$|H\rangle|a\rangle \longrightarrow \left(\cos\frac{\pi}{2N}|H\rangle + \sin\frac{\pi}{2N}|V\rangle\right)|a\rangle$

↓ PBS1

↓ PBS2

after N cycles → eventually vertically polarized

But if there is a Bomb

↓

Horizontal Polarization when $N \to \infty$

∴ 100% Successful Prediction

# UNCERTAINTY PRINCIPLE & JOINT MEASUREMENT

Version 1:- (Preparation Uncertainty) → Usual Uncertainty Relation

Version 2:- (Measurement Uncertainty) → Impossible to simultaneously measure $\hat{x}$ & $\hat{p}$

Version 3:- (Disturbance Uncertainty) → Impossible to measure with disturbing the system

Self Adjoint $\hat{A}$ determines projector $E_A(X)$ $\forall$ Bord Set (Measurable) $X$

s.t.
- $E_A(X) = E_A(X)^\dagger = (E_A(X))^2$
- $E_A(\mathbb{R}) = \mathbb{1}$
- $E_A(X_1 \cup X_2) = E_A(X_1) + E_A(X_2)$ if $X_1 \cap X_2 = \Phi$

Then spectral decomposition

$$\hat{A} = \int a\, E_A(da) \quad \& \quad \hat{E}_A(X) = \int_X E_A(da)$$

Quantum Probability $p_A^\rho(X) = \mathrm{Tr}[\rho E_A(X)]$ → Probability that measurement of $\hat{A}$ gives result $\in X$

## Position & Momentum

$$\hat{Q} = \int q\, E_Q(dq) \quad \& \quad E_Q(X) = \int_X E_Q(dq)$$

$E_Q(X)\,\psi(q) = \psi(q)$ if $q \in X$
$= 0$ otherwise

No Eigenvalue interpretation for continuous dim

$\hat{Q}$ acts as a multiplication operator $\hat{Q}\psi(q) = \int q'\psi(q)\, E_Q(dq') = q\psi(q)$

Momentum operator $\hat{P}\psi(q) = -ik\frac{\partial \psi}{\partial q}$

Fourier Transform $F[\psi(x)] = \tilde{\psi}(p) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{ipx}{\hbar}} \psi(x)\, dx$ & similarly $\tilde{F}[\tilde{\psi}(p)] = \psi(x)$ (Inverse Fourier Transform)

**Dispersion :-**

$$\Delta|\psi|^2 = \left( \int_{-\infty}^{\infty} x^2 |\psi(x)|^2 dx - \left\{ \int_{-\infty}^{\infty} x |\psi(x)|^2 dx \right\}^2 \right)$$

$$\Delta|\bar{\psi}|^2 = \left( \int_{-\infty}^{\infty} p^2 |\bar{\psi}(p)|^2 dp - \left\{ \int_{-\infty}^{\infty} p |\bar{\psi}(p)|^2 dp \right\}^2 \right)$$

$$\Delta(\hat{Q},\psi) = \Delta|\psi|^2 \Big\} \rightarrow \Delta(\hat{Q},\psi) = \Delta|\psi|^2 ; \quad \Delta(\hat{P},\psi) = \Delta(-\hbar F^{-1}\hat{Q}F,\psi) = \Delta(\hbar\hat{Q},\bar{\psi}(p)) = \hbar\Delta|\bar{\psi}|^2$$

$$\text{i.e. } \Delta(\hat{Q},\psi)\Delta(\hat{P},\psi) = \hbar\Delta|\psi|^2\Delta|\bar{\psi}|^2 \geq \frac{\hbar}{2} \rightarrow \text{Preparation Uncertainty Relation}$$

This is well established

**Support Property** → This is essential for measurement uncertainty

If $\text{supp}\{\psi\} = \{x \in \mathbb{R}, \psi(x) \neq 0\}$ is closed & bounded - then its Fourier Transform is nowhere Zero

i.e. $\text{supp}(\bar{\psi})$ is $\mathbb{R}$.

**Complementarity:-**

Contradicts support ...

**Proof:-**

Assume $\langle\psi|E_Q(X)|\psi\rangle = \langle\psi|E_P(Y)|\psi\rangle = 1$

$$\int_X |\psi|^2 dx = 1 \qquad \int_Y |\psi|^2 dy = 1$$

Contradicts the theorem.

**POSITION & MOMENTUM DO NOT ADMIT SIMULTANEOUSLY SHARP JOINT MEASUREMENT**

**Proof:-**

Assume $E_{Q,P}(X \times Y)$ exists

$$E_{Q,P}(X \times Y) \leq E_Q(X)$$
$$E_{Q,P}(X \times Y) \leq E_Q(Y)$$

Now assume $\exists$ a vector $\phi : \langle\phi|E_{Q,P}(X \times Y)|\phi\rangle = 1$

$\Rightarrow \langle\phi|E_Q(X)|\phi\rangle = \langle\phi|E_P(Y)|\phi\rangle = 1$

$\therefore E_Q(R-X) \wedge E_P(R-Y) \neq 0 \Big\} \rightarrow$ Fleming Result

$E_Q(X) \wedge E_P(Y) = E_Q(R-X) \wedge E_P(Y) = E_Q(X) \wedge E_P(R-Y) = 0$

$\therefore$ Perfect Joint measurement of $\hat{x}$ and $\hat{p}$ is not possible .. (Proved)

LECTURE - 10 11:30 - 13:00

# QUANTUM INFORMATION THEORY

Sibasish Ghosh

IMSc Chennai

---

Why 'Quantum' Information Theory ?

**Efficiency** : Classical Information Theory → N signals → need N bits.
Quantum Information → N different orthogonal states pairwise orthogonal

But non-orthogonal states → Quantum is advantageous (Schumacher Data Compression Theorem)

## Encoding 'Quantum' Information

for $\rho$ in d-dimensional state $\mathcal{H}_d \longrightarrow S(\rho)$ qubits required

- Encoding Classical Information in quantum states $\Longrightarrow$ Superdense Coding

$\{00, 01, 10, 11\}$ → Classically 2 bits required.

Quantum Mechanically → A & B share entangled state $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$

⊙ Alice applies one of $\mathbb{1}, \sigma_x, \sigma_y, \sigma_z$ to her qubit
↓
⊙ Alice sends her qubit to Bob
↓
⊙ Now Bob has 4 mutually orthogonal states $\left\{\frac{|01\rangle \pm |10\rangle}{\sqrt{2}}, \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}\right\}$
↓
⊙ Now Bob can perform measurement on them to find Alice's message

Variants :- ① Noisy Channel
② Initially Mixed State

Quantum Teleportation → Send information about unknown qubit to Bob → finally the information about unknown state at Alice is destroyed (No-Cloning isn't Violated)

## Holevo Bound

$|\psi\rangle = \sum_j \alpha_j |j\rangle$ → so $\exists$ ∞-ly many such superpositions → so can we encode one-bit with each such superposition? → Infinite Classical Information storable in one qubit

↓

NO; nonorthogonal states can't be distinguished so decoding not possible.

↓

Upper limit → only $\log_2 d$ bits can be extracted.

↓

Capacity :- Holevo Bound

## SCHUMACHER COMPRESSION

Quantum Version of Shannon's data compression Theorem

Coin Toss with N runs with head probability = P { HT.... H.... } → $2^N$ such sequences } → # of sequences with NP heads N(1-P) tails } → Typical Sequences

↓

$< 2^n$

$|\psi_{x_1}\rangle, |\psi_{x_2}\rangle, \ldots$ ($p(x_1)$, $p(x_2)$) → Corresponds to $\rho_{avg} = \sum_i p(x_i) |\psi_{x_i}\rangle\langle\psi_{x_i}|$

How to store information about N-copies of this ensemble

↓

Q: How to store minimally without making any error.

Write $\rho = \sum_j q_j |\phi_j\rangle\langle\phi_j| \rightarrow$ Spectral decomposition $\{|\psi_i\rangle$'s may not be orthogonal, but $|\phi_j\rangle$'s are$\}$

Now; Shannon's data compression limit $= H(Y) = H(\vec{q}) = -\sum_j q_j \log_2 q_j$

$= -\mathrm{tr}(\rho \log_2 \rho)$

$= S(\rho)$ per copy

for $n$ copies in asymptotic limit $n \to \infty$

($n \to \infty$ because typicality arguments hold only for Law of Large Numbers $\leftarrow$ large $n$)

Moral :- von Neumann Entropy $\equiv$ # of qubits required to store the information per copy asymptotically

But $\{|\psi_x\rangle\}$ are not orthogonal $\Rightarrow$ so; $S(\rho) \neq -\sum_x p_x \log(p_x) = H(X)$

It can be shown $S(\rho) \leq H(X)$ $\therefore$ Qubits offer advantage over bits

One can show this scheme is optimal .... (Keeping Typical States, but throw out Others)

Data Compression for Mixed State Encoding

$\mathcal{E} = \{p_x, \rho_x \mid x \in X\}$ with $\rho = \sum_x p_x \rho_x \rightarrow$ Holevo Bound :- $S(\rho) - \sum_{x \in X} p_x S(\rho_x) = \chi(\mathcal{E})$

But is this quantity attainable in an asymptotic compression scheme $\rightarrow$ OPEN!

## MUTUAL INFORMATION VS. THE HOLEVO BOUND

$\chi(\mathcal{E})$ tells us how much, on average, the von Neumann Entropy $S(\rho)$ (with $\rho = \sum_x p_x \rho_x$) is reduced once we know which preparation was chosen to prepare $\rho$.

$\therefore$ We have to maximize the mutual information between input & output

$\Rightarrow$ Holevo Bound $\rightarrow$ Upper Limit of the Mutual Information (Accessible Information) $\downarrow$ Tight for $n \to \infty$ asymptotic limit

Proof :- Nielsen Chuang $\rightarrow$ Use strong subadditivity for Von Neumann Entropy

## Attainability

$\mathcal{E} = \{|\psi_1\rangle, p(|\psi_1\rangle)=\frac{1}{2}, |\psi_2\rangle, p(|\psi_2\rangle)=\frac{1}{2}\} \rightarrow I_{acc} = 1 - |\langle\psi_1|\psi_2\rangle| = 1$ if $\langle\psi_1|\psi_2\rangle$ = Orthogonal

Holevo Bound $\chi(\mathcal{E}) \geq I_{acc}$ with equality for $\langle\psi_1|\psi_2\rangle = 0$ or $1$

for 2qubit $\rightarrow I_{acc}(\mathcal{E}^{(2)}) = 1 - |\langle\psi_1|\psi_2\rangle|^2$ & $\chi(\mathcal{E}^{(2)}) = H\left(\left(1+\frac{\langle\psi_1|\psi_2\rangle|^2}{2}\right), 1-\frac{|\langle\psi_1|\psi_2\rangle|^2}{2}\right)$

↓ gap btwn $I_{acc}$ & Holevo Bound goes down

↓ Intuitively see why Holevo Bound is asymptotically attainable

# CAPACITIES OF QUANTUM CHANNELS

How to compare performance of Classical & Quantum Noisy Channels?

## Classical Capacity of Quantum Channels

Classical Information Source → Encode in density matrix → Send thru Quantum Channel → Decode

Sending only finitely many states $\rho_x$ is not sufficient (e.g. for teleportation we need to send an entire subspace of the Input Hilbert Space $H_1$)

## Quantum Capacity of Quantum Channels

Signal States $\{\rho_x\}$ with prob $\{p_x\}$ → Encode by a CP map → Send through Channel → Decode

One shot classical capacity $C_{1,1} = \sup_{\{p_x, \rho_x\}} I_{max}(X;Y)$

Holevo - Schumacher - Westmoreland (1997) :- $C_{1,\infty}$ = Capacity per single use of channel for infinite # of usages $\therefore C_{1,1} \leq C_{1,\infty}$

$C_{E,\infty}$ → Input allowed to be Entangled → $C_{E,\infty} \geq C_{1,\infty}$

Equality if Channel Capacities Additive ⇒ This is not yet known

DENSE CODING CAPACITY :-

$C_E(\mathcal{N}_{qm})$ → no exact form known but $C_E(\mathcal{N}_{qm}) \geq C_{1,1}, C_{1,\infty}, C_{E,\infty}$

Ref :- Bennett, Shor, Smolin, Thapliyal

↓

Exact Formula known for only in cases where $\infty$ amt of shared entanglement allowed.

LECTURE - 11 14:30 - 16:00

# QUANTUM CORRELATIONS

Debasis Sarkar
Calcutta University

TODAY :- MULTIPARTITE QUANTUM ENTANGLEMENT & QUANTUM CORRELATIONS BEYOND ENTANGLEMENT

For pure bipartite states → Entanglement dynamics under LOCC is reversible.

But in general (for mixed states) → Entanglement dynamics under LOCC is irreversible

↓

Extend LOCC to PPT Operations (Operations which preserve PPT-ness)

$\rho(PPT) \xrightarrow{\Lambda} \sigma(PPT)$

↓

Even then Irreversible

Plenio/Brandao (2010): Under non-entangling operations → (non-entangling asymptotically)
(Science, Commun. Math. Phys.)

↓

Reversible Entanglement Dynamics

LOCAL DISTINGUISHABILITY ⇒ May not be possible even for globally orthogonal states (e.g. UPB-s)

## MULTIPARTITE ENTANGLEMENT FOR PURE STATES

Q:- (i) How to quantify entanglement?
(ii) What are maximally entangled states?

↓

If we require them as states whose bipartite cuts are completely mixed (ρ ∝ I)

↓ Not possible for N ≥ 3

Gilad Gour:- Avg. Bipartite Entanglement wrt all the cuts maximum.

## Geometric Measure:-

Most acceptable = $\min_{\sigma \in Sep} D(\rho, \sigma)$ for some distance measure $D$ & pure states $\rho$ & $\sigma$

Recent :- PRL, 111, 110502 (2013), PRL 115, 150502 (2015) → Barbara Kraus et al

We have to look closely at LOCC itself (Ref:- Eric Chitambar → "All you wanted to know about LOCC but were afraid to ask").

① LOCC Provides protocols with which entangled states can be manipulated.
② LOCC Provides Ordering.
③ For pure bipartite case → we have definite result regarding convertibility of LOCC

Single Copy Case → Lo/ Popescu Phys Rev A 63, 022301 (2001)

No. of Schmidt Coefficients can never increase.

Nielsen Criteria let $|\psi\rangle \to \{\lambda_i\}$ Schmidt Coefficient
$|\Phi\rangle \to \{\mu_i\}$ ,, ,,

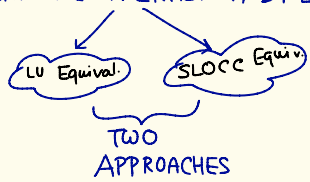
Then $|\psi\rangle \xrightarrow{SLOCC} |\Phi\rangle \iff \vec{\lambda} \succ \vec{\mu}$ ..(Nielsen Criterion)

Then :- Catalysis → $|\psi\rangle \otimes |\chi\rangle \xrightarrow{LOCC} |\Phi\rangle \otimes |\chi\rangle$ may be possible even if $|\psi\rangle \overset{LOCC}{\not\to} |\Phi\rangle$

↓

Under PPT Operations :- Winter → Condition for Existence of Catalytic State.

MULTIPARTITE CONVERTIBILITY BY LOCC




SLOCC ⇒ Dür Vidal Cirac ⇒ GHZ ⟷ W isn't possible

But for 4 qubits → ∞-ly many inequivalent classes under SLOCC

↓ Frank Verstraete vs. Gilad Gour

$\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$ → Bell Basis States

Example :- $a|\psi^+\psi^+\rangle + b|\psi^-\psi^-\rangle + c|\phi^+\phi^-\rangle + d|\phi^-\phi^-\rangle$ → If $a \neq b \neq c \neq d$ → SLOCC inequivalent all of them

Multipartite $|\psi\rangle \xrightarrow{\text{LOCC}} |\phi\rangle \rightarrow$ what's the condition ?

Consider $M_a(|\psi\rangle) \rightarrow$ all states accessible from $|\psi\rangle$; $M_s(|\psi\rangle) \rightarrow$ all states that can reach $|\psi\rangle$

Consider $\text{Vol}\{M_a|\psi\rangle\} = V_a|\psi\rangle$ & $\text{Vol}\{M_s|\psi\rangle\} = V_s|\psi\rangle$ with some suitable Volume measure.

Barbara Kraus :- Volume in LU-eqvt. classes.

If $M_s$ is very large $\rightarrow$ the state is not very 'powerful'. However if $M_a$ is very large $\rightarrow$ the state is very 'valuable' $\Longrightarrow$ Operationally meaningful Definition for multipartite Entanglement.

$$E_a = \sup_{V_a} V_a|\psi\rangle \;\&\; E_s = \sup_{V_s}(1 - V_s|\psi\rangle)$$

} Two Possible Entanglement measure

If $M_s(|\psi\rangle) = \text{null}$ implies $V_s = 0 \rightarrow$ we call maximally entangled states } [Ref arXiv 1510.09164]

Monogamy $\rightarrow$ If A & B are maximally entangled then A & C aren't entangled.
(PRA, 92, 062340 (2015)) $\rightarrow$ Reference

## CORRELATION MEASURES BEYOND ENTANGLEMENT

Discord $\rightarrow$ (Olliviers Zurek)

Mutual Information $\longrightarrow J(A,B) = S(A) - \min_{\{\Pi_j\}} \sum_j p_j S(A|j)$

$I(A;B) = H(A) + H(B) - H(AB)$

$I(A;B) = J(A;B)$ Classically but not in QM always $\therefore$ Discord $= I(A;B) - J(A;B)$

If they are equal then CQ states

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|_A \otimes \rho_j^B$$

* Discord may increase under LOCC
* Set of CQ states is not convex - so geometrically very hard
  ↓
  Exact Analytical Result is hard to get in general

Geometric Discord

$$D(\rho) = \min_{\chi \in CQ} D(\rho, \chi)$$ → a tight lower bound is found recently. (Swapan Rana)

[D = Suitable Distance measure]

Is Discord a good resource ?

Dakic et al (2012) Claim → Discord necessary & sufficient for Remote State Preparation
↓
Disputed

Ref: Zwolak / Zurek Sci Rep 2013; 3; 1729, Streltsov - Zurek PRL 2013 'QD Cannot be Shared'

Discord ≡ Information Lost when a Composite Quantum System is Disassembled

CRITERIA FOR NON-CLASSICAL CORRELATIONS (MODI)

Necessary Condition

- ⊙ $C(\rho_A \otimes \rho_B) = 0$ for pdt states
- ⊙ Invariance Under Local Unitary
- ⊙ Classical States have zero quantum correlations
- ⊙ For Pure Bipartite State $= S(\rho_A)$

Reasonable Condition

- ⊙ Additivity
- ⊙ Symmetry under interchange
- ⊙ Convexity

Measurement Induced Nonlocality → $N(\rho) = \max \| \rho - \Pi(\rho) \|$

max over all PVM's that preserve density matrix of the first party.

↓
But this is nonzero even for Classical Values.

MIN is good to calculate.

↓

But set of all MIN = 0 is non-convex.

## LOCAL QUANTUM UNCERTAINTY

We need to build a measure which is not affected by classical mixing.

LQU = minimum over all local maximally informative (i.e. non-degenerate spectrum) of state information

- Vanishes ∀ CQ states
- LU invariant
- Reduces to $S(\rho_A)$ for pure bipartite states.

Geometrically LQU = min Hellinger distance btwn the state & the state after a least-disturbing root-of-unity local unitary operation applied on the qubit.

LECTURE - 12 16:30 - 18:00

# QUANTUM FOUNDATIONS - UNCERTAINTY PRINCIPLE

Guruprasad Kar

ISI Kolkata

---

Meaning of $E_Q(X) \wedge E_P(Y) = 0$ $\rightsquigarrow$ There is no non-trivial projection operator P such that $P \leq E_Q(X)$ & $P \leq E_P(Y)$

## Generalized Observables

Heisenberg never quantified unsharp measurements / error-disturbances
We would $\left(\frac{1}{0}\right)$

POVM $F: X \longrightarrow F(X)$

$F(X) \geq 0$
$F(\mathbb{R}) = \mathbb{1}$ (Trace Condition)
$F(X_1 \cup X_2) = F(X_1) + F(X_2)$ if $X_1 \cap X_2 = \phi$

} But no idempotency $F^2 \neq F$

And Born Rule $p_F^\rho(X) = Tr[\rho F(X)]$

Naimark Dilation Thm $\equiv$ POVM in a low dimensional Hilbert Space $\Longleftrightarrow$ PVM in higher dim Hilbert Space.

## Unsharp Position & Momentum Observables

$f(x')$, $g(y')$ are pdf-s

$$E_Q^f(X) = \int f(x')\, E_Q(x+x')\, dx' \quad \text{where } f(x') \geq 0 \ \& \ \int_{-\infty}^{\infty} f(x')dx' = 1$$

$$E_P^g(Y) = \int g(y')\, E_P(y+Y)\, dy' \quad \text{where } g(y') \geq 0 \ \& \ \int_{-\infty}^{\infty} g(y')\, dy' = 1$$

describing the probability distribution of the unsharp measurement [$f(x), g(Y)$ are $\delta$-functions for sharp measurements]

Now Born Probability $p^f_{\psi,Q}(x) = \langle\psi| E^f_Q |\psi\rangle$

Now; $\mathrm{Var}\left(E^f_Q(x), \psi\right) = \Delta(\hat{Q}_f, \psi) = \int \left(x - \int x\, dp^f_{\psi,Q}(x)\right)^2 dp^f_{\psi,Q}(x)$

$= \mathrm{Var}\left(E_Q, \psi\right) + \mathrm{Var}(f)$ [HW :- Verify this]

Similarly $\mathrm{Var}\left(E^g_P, \psi\right) = \underbrace{\mathrm{Var}\left(E_P, \psi\right)}_{\text{Due to Sharp measurement}} + \underbrace{\mathrm{Var}(g)}_{\text{Measure of Unsharpness}}$

But we still have no relation between $f$ and $g$.

## Joint Position & Momentum Measurement

Choose $f = |\phi|^2$ & $g = |\tilde{\phi}|^2$

$U_{qp} = e^{i(p\hat{Q} - q\hat{P})} \rightsquigarrow$ unitary evolution operator for

$$X \times Y \longrightarrow E(X \times Y) = \int_{X \times Y} |U_{qp}\phi \times U_{qp}\phi| \, dq\, dp$$

$$E(X \times Y) \leq E(X \otimes \mathbb{R}) = E^f_Q(X)$$
$$E(X \times Y) \leq E(\mathbb{R} \otimes Y) = E^g_P(Y)$$

$\therefore$ Uncertainty due to unsharpness $= \Delta(\hat{Q}, \phi)$ ; Uncertainty due to unsharpness of momentum operator $= \Delta(\hat{P}, \phi)$ $\therefore \Delta(\hat{Q}, \phi)\, \Delta(\hat{P}, \phi) = \hbar\, \Delta|\phi|^2\, \Delta|\tilde{\phi}|^2 \geq \frac{\hbar}{2}$

↓

This is exclusively due to unsharpness of the measurement itself

↓

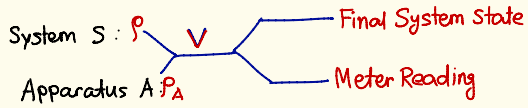
Not State-dependent → NOT Preparation Uncertainty

**Wigner Function** → Not a proper probability function

↓

Can be negative → We have to convolute it with another function to get positive

## QUANTUM MEASUREMENT PROCESS




Measurement : $(\mathcal{H}_A, \mathcal{Z}, \rho_A, V, f)$ & Interaction $V := U_{SA}(\rho \otimes \rho_A) U_{SA}^{\dagger}$ } final joint state of system & apparatus

$$\mathrm{Tr}[\rho F^{\rho_A, \mathcal{Z}V}] = \mathrm{Tr}[V(\rho \otimes \rho_A) \mathbb{1} \otimes \mathcal{Z}(f^{-1}(X))]$$

Now; measurement of B if $F^{\rho_A, \mathcal{Z}V}(X) = E_B(X)$

Example :- Discrete Observable → $E_k = |k\rangle\langle k|$

$A = \sum_k a_k E_k$ ; Apparatus Hilbert Space $\mathcal{H}_A = \mathbb{L}^2(\mathbb{R})$

$U = \sum E_k e^{i\lambda a_k \hat{P}_A}$ → momentum of apparatus

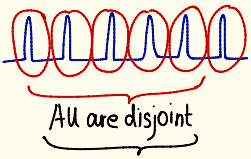
[By Spectral Decomposition $f(A) = \sum f(a_k) E_k$]

$$\therefore U(|\psi\rangle \otimes |\phi\rangle) = \sum E_k |\psi\rangle e^{i\lambda a_k \hat{P}_A} |\phi\rangle$$

$$= \sum E_k |\psi\rangle \phi(x - \lambda a_k) \quad [\text{Shift}]$$

Now if $|a_{k+1} - a_k| \geq \frac{\delta}{\lambda}$ $\forall k$ & $\phi$ is supported in $(-\frac{\delta}{2}, \frac{\delta}{2})$

Then $\Phi_{\lambda a_k}$ has mutually disjoint supports $I_k = \left(a_k - \frac{\delta}{2\lambda}, a_k + \frac{\delta}{2\lambda}\right)$




$$E(X) = \sum \langle \Phi_{\lambda a_k} | E^{Q_A}(\lambda I_k) | \Phi_{\lambda a_k} \rangle E_k$$

$$= \sum_{k \in X} \langle \Phi_{\lambda a_k} | E^{Q_A}(\lambda I_k) | \Phi_{\lambda a_k} \rangle E_k = E^A(X) \text{ for perfect}$$

projective measurement.

# Von Neumann Model

System wave function: $\psi$, apparatus wave function $\phi$; Measurement interaction $U = e^{\left(-\frac{i}{\hbar}\lambda \hat{Q} \otimes \hat{P}_A\right)}$

$$U\psi(q)\phi(x) = \psi(q)\phi(x-\lambda q)$$

**Measured Observable:-**

$$E(X) = \iint |\phi(q'-\lambda q)|^2 \chi_{\lambda X}(q')\, dq'\, E_Q(dq) = E^f_Q(X)$$

$= 1$ if $q' \in \lambda X$
$= 0$ else

Variance of $q \to f(q) = \lambda |\phi(-\lambda q)|^2$

## JOINT POSITION-MOMENTUM (ARTHUR KELLY MODEL)

Initial $\Psi_0 = \psi(q) \otimes \Phi_1(f_1) \otimes \Phi_2(f_2)$ (System, First Apparatus, Second Apparatus)

$$U = e^{-\frac{i}{\hbar}\left[\lambda \hat{Q} \otimes \hat{P}_1 \otimes \mathbb{1}_2 - \mu \hat{P} \otimes \mathbb{1}_2 \otimes \hat{Q}_2\right]}$$

Now →

$$\Psi = U\Psi_0 = \psi(q+\mu f_2)\, \Phi_1\left(f_1 - \lambda q - \frac{\lambda\mu}{2} f_2\right) \Phi_2(f_2)$$

Actually measured observable $G(X \times Y)$

↓

$$\langle \Psi | G(X \times Y) | \Psi \rangle = \langle \Psi | \mathbb{1} \otimes E_{Q_1}(\lambda X) \otimes E_{P_2}(\mu Y) | \Psi \rangle$$

$$G(X \times Y) = \langle \Phi_1 \otimes \Phi_2 |\, U^\dagger E_{Q_1}(\lambda X) \otimes E_{P_2}(\mu Y)\, U\, | \Phi_1 \otimes \Phi_2 \rangle$$

after 'some' calculation → $G(X \times \mathbb{R}) = E^f_Q(X)$

$G(\mathbb{R} \times Y) = E^g_P(Y)$

and finally $f(q) = f_0 \; |\Phi_2^M|^2(q)$, $g(p) = g_0 \; |\tilde{\Phi}_1^M|^2(p)$ } Unsharpnesses $f_0$ & $g_0$ become even more unsharp

## Uncertainty Relation for Arthur-Kelly

$$\text{Var}(f) = \frac{1}{\lambda^2}\text{Var}(\hat{Q}_1, \hat{\Phi}_1) + \frac{M^2}{4}\text{Var}(\hat{Q}_2, \Phi_2)$$
$$\text{Var}(g) = \frac{1}{M^2}\text{Var}(\hat{P}_2, \Phi_2) + \frac{\lambda^2}{4}\text{Var}(\hat{P}_1, \Phi_1)$$

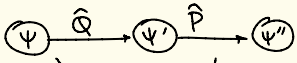
$$\text{Var}(f).\text{Var}(g) = \frac{1}{4}\text{Var}(\hat{Q}_1, \Phi_1)\text{Var}(\hat{P}_1, \Phi_1) + \frac{1}{4}\text{Var}(\hat{Q}_2, \Phi_2)\text{Var}(\hat{P}_2, \Phi_2)$$
$$+ \frac{1}{\lambda^2 M^2}\text{Var}(\hat{Q}_1, \Phi_1)\text{Var}(\hat{P}_2, \Phi_2) + \frac{\lambda^2 M^2}{16}\text{Var}(\hat{Q}_2, \Phi_2)\text{Var}(\hat{P}_1, \Phi_1)$$

This is due to measurement

NOW; $X = \text{Var}(\hat{Q}_1, q_1)\text{Var}(\hat{P}_2, p_2)$ (some scaling)

$$\therefore \text{Var}(f).\text{Var}(g) = \frac{1}{4}\left(\frac{\hbar^2}{4} + \frac{\hbar^2}{4}\right) + \underbrace{\text{Last two terms}}_{\text{Due to measurement}}$$
$$\geq \frac{\hbar^2}{8} + \frac{\hbar^2}{16}\left(X + \frac{1}{X}\right)$$
$$\geq \frac{\hbar^2}{4} \longrightarrow \text{This is the Arthurs Kelly model}$$

## ERROR-DISTURBANCE RELATIONS




Goal $\Rightarrow$ Relate error $\epsilon_Q$ & disturbance $\eta_P$
Sequential measurement

Error:- $D(\Psi, Q'; f) = \sqrt{\langle (q' - f)^2 \rangle}$

Now calibration error $\Delta_c(Q, Q') = \lim_{\epsilon \to 0} \sup \{ D(\Psi, Q'; f) \mid \Psi, f; D(\Psi, Q', f) \leq \epsilon \}$

Now $Q'$ and $P'$ are marginal observables of some joint measurement $M$ then

$$\Delta_c(Q, Q')\,\Delta_c(P, P') \geq \frac{\hbar}{2}$$ [Bush, Lahti, Werner]

HW :- Show that this holds true for Covariant Joint Position & Momentum measurement

THEOREM (Werner)

If M be any joint measurement $\Delta_c(Q,Q')$ & $\Delta_c(P,P')$, then $\exists$ a covariant joint measurement $\overline{M}$ such that

$$\Delta_c(Q,Q^{f'}) \leq \Delta_c(Q,Q')$$
$$\Delta_c(P,P^{f'}) \leq \Delta_c(P,P') \qquad f' = |\alpha|^2,\ g' = |\tilde{\alpha}|^2$$

$$\Rightarrow \Delta_c(Q,Q')\,\Delta_c(P,P') \geq \Delta_c(Q,Q^{f'})\,\Delta_c(P,P^{f}) \geq \frac{\hbar^2}{4}$$

It can be shown $\epsilon(Q,Q') \geq \Delta_c(Q,Q')$ and $\eta(P,P') \geq \Delta_c(P,P')$

$\Rightarrow$ Error-Disturbance Relation $\epsilon(Q,Q')\ \eta(P,P') \geq \frac{\hbar}{2}$

DAY-4

LECTURE 13 09:30-11:00

# QUANTUM THERMODYNAMICS

SIBASHIS GHOSH

IMSc Chennai

FOCUS :- Thermalization in Quantum Systems (Not Thermal Machines)

Ref:- Popescu, Short, Winter Nat Phys (2006)

Put a system in a Heat Bath → maximum entropy state = Thermal State

$$\rho_{th} = \frac{e^{-\beta H}}{Tr(e^{-\beta H})}$$

Q:- How does the Quantum System get Thermalized ?

In open system dynamics $\xrightarrow[\text{Bath}]{\text{Heat}}$ $\frac{d\rho}{dt} = i[H,\rho] + \underbrace{\mathcal{L}[\rho]}_{\text{Lindbladian}} \xrightarrow[\text{time}]{\text{In } t\to\infty} \rho_{th}$

(Markovian Dynamics)

Q:- If $\mathcal{H}_S \otimes \mathcal{H}_E$ is total Hilbert Space but $\exists$ constraints such that effectively the Hilbert Space $\mathcal{H}_R \subseteq \mathcal{H}_S \otimes \mathcal{H}_E$. Now if I take equal a-priory probable state $= \mathcal{E}_R = \frac{\mathbb{1}_R}{d_R}$ in $\mathcal{H}_R$.

Concentrate on state of the system.

$Tr_E\, \mathcal{E}_R = \Omega_S \rightarrow$ The State to which the system equilibriates.

Start with an arbitrary pure state $|\phi\rangle_{SE}$ s.t. $\rho_S = Tr_E |\phi\rangle\langle\phi|$

Target :- if $D(\rho_S, \Omega_S) \leq \epsilon \rightarrow$ Thermalization (Trace Distance)

i.e. $\text{Prob}\left[\| \rho - \Omega_S \|_1 > \eta\right] < \eta'$ → Very improbable to go far apart from equilibrium state

(condition → effective dimension $d_{eff}^{environment} \gg d_{system}$)

If H is two-level → $\rho_{th} = \begin{bmatrix} p & 0 \\ 0 & \tilde{p} \end{bmatrix}$ Where $p = \frac{e^{-\beta E_0}}{e^{-\beta E_1} + e^{-\beta E_0}}$ & $\tilde{p} = 1 - p$

$\rho \xrightarrow{N} \rho_{th} \Rightarrow \rho_{th} = \frac{1}{2}(\mathbb{1} + \underbrace{\vec{n}_{th}} \cdot \vec{\sigma})$

↓

Pin map → Every map gets pinned to one target state

Q:- Can you give me a Hamiltonian Which takes ($t \to \infty$ limit) ⟶ ??

↓

Append some ancilla to the system.

↓

for a finite dimensional ancilla → $\beta$ itself changes → Not compatible with Classical Thermo dynamics

## Proof of $\text{Prob}\left[\| \rho - \Omega_S \|_1 > \eta\right] < \eta'$

Theorem :- For a randomly chosen state $|\Phi\rangle \in \mathcal{H}_R$ & $\epsilon > 0$ The distance $\| \text{Tr}_E (|\Phi\rangle\langle\Phi|) - \Omega_S \|_1$

$\text{Prob}\left[\| \rho - \Omega_S \|_1 > \eta\right] < \eta'$ Where $\eta = \epsilon + \sqrt{\frac{d_S}{d_{eff}^{env.}}}$, $\eta' = 2e^{-C d_R \epsilon^2}$

Proof:- Probabilitic Theoretic Result → Levy's Lemma → Given a fn $f: S^d \to \mathbb{R}$ & a point $\Phi \in S^d$ chosen with uniform probability, then $\text{Prob}\ |f(\Phi) - \langle f \rangle| \leq e^{-\frac{2C(d+1)\epsilon^2}{\eta^2}}$ Where $\eta = \sup_{\Phi} |\vec{\nabla} f|$ & $C = \frac{1}{18\pi^3}$

(Ref:- Millman) $\left[\langle f \rangle = \int_{\Phi \in S^d} f(\Phi)\, d\Phi\right]$

Here $|\Phi\rangle \in \mathcal{H}_R$ → Any pure state representible here interms of $2d_R - 1$ dimensional Hypersphere $S^{2d_R - 1}$

Now define $f(\Phi) = \| \text{Tr}_E |\Phi\rangle\langle\Phi| - \Omega_S \|_1$ (Trace 1-norm)

Now using levy's Lemma requires finding out Lipschutz Constant $\eta = 2$.. (HW)

Now we get $\text{Prob}\left[\left| \| \rho_S - \Omega_S \|_1 - \langle \| \rho_S - \Omega_S \|_1 \rangle \right| \geq \varepsilon\right] \leq 2 \exp\left(\frac{\quad}{\eta}\right)$

$\Rightarrow \text{Prob}\left[\|\rho_S - \Omega_S\|_1 \right] \geq \langle \|\rho_S - \Omega_S\|_1 \rangle + \varepsilon] \leq 2\exp(-c\, d_R \varepsilon^2)$

The average $\langle \|\rho_S - \Omega_S\|_1 \rangle \leq \sqrt{d_S}\, \langle \|\rho_S - \Omega_S\|_2 \rangle$

$$\sqrt{d_S} \int_{\varphi \in S^{2d_R-1}} d\varphi \, \|\text{Tr}_R |\varphi\rangle\langle\varphi| - \Omega_S\|_2 \xrightarrow[\text{some calculation}]{\text{After}} \leq \sqrt{d_S} \sqrt{\int d\varphi \, \|\text{Tr}_R |\varphi\rangle\langle\varphi| - \Omega_S\|_2^2}$$

but $\langle \rho_S \rangle = \int_{\varphi \in S^{2d_R-1}} d\varphi \, \text{Tr}_E |\varphi\rangle\langle\varphi| = \Omega_S$

finally $\leq \sqrt{d_S} \cdot \sqrt{\langle \text{Tr}\, \rho_S^2 \rangle - \text{Tr}\, \Omega_S^2}$

What is $\langle \text{Tr}\, \rho_S^2 \rangle$ ? This is $\leq \text{Tr}\langle \rho \rangle^2 + \text{Tr}\, \langle \rho_E \rangle^2$

$= \text{Tr}(\Omega_S)^2 + \text{Tr}\langle \rho_E \rangle^2$

But $\langle \rho_E \rangle = \Omega_E \therefore \langle \text{Tr}\, \rho_S^2 \rangle \leq \text{Tr}(\Omega_S)^2 + \text{Tr}(\Omega_E)^2$

Now $d_{\text{eff}} = \frac{1}{\text{Tr}(\Omega_E)^2} \rightarrow$ Then $\langle \|\rho_S - \Omega_S\|_1 \rangle \leq \sqrt{\frac{d_S}{d_E^{\text{eff}}}}$

Thus $\rightarrow \text{Tr}\left( \|\rho_S - \Omega_S\|_1 \geqslant \varepsilon + \sqrt{\frac{d_S}{d_E^{\text{eff}}}} \right)$ has prob $\leq 2\exp(-c\, d_R \varepsilon^2]$

$\therefore$ (Proved)

## Sanity Check

$\mathcal{H}_R = \mathcal{H}_S \otimes \mathcal{H}_E \rightarrow d_{\text{eff}} = \frac{1}{\text{Tr}_E\, \Omega^2} = d_E \longrightarrow$ expected

Now $\sqrt{\frac{d_S}{d_E^{\text{eff}}}} \leq \sqrt{\frac{d_S}{d_R}}$ $\quad \Omega_E = \sum_k \lambda_k |\varphi_k\rangle\langle\varphi_k| \rightarrow$ Spectral Decomposition

Proof :- 2 line (HW)

i.e. avg $\langle \|\rho_S - \Omega_S\|_1 \rangle$ is small if $d_{\text{eff}} \gg d_S$

Levy's Lemma + This $\longrightarrow$ Thermalization }

## Implications of This Theorem

### Reconciling with standard Stat Mech

Assume Energy of the system E is given $\rightarrow$ Temp $\beta$ given

$H_{\text{tot}} = H_S \otimes \mathbb{1} + \mathbb{1} \otimes H_R + \underbrace{H_{\text{int}}}_{\text{Weak enough interaction}}$ & assume dense energy spectrum

$\Omega_S^{(\epsilon)} = Tr_\epsilon \, \epsilon_R \overset{\text{can be shown}}{=\!=} \frac{e^{-\beta H_S}}{Tr(e^{-\beta H_S})}$ → All Previous Results valid for This also

Thermal Canonical Equilibriation Principle → Start from arbitrary state subject to these constraints - Thermalizes

Models with spins :- N spins ..... Show that these bounds can be sharpened

↓

(no interaction) in external $\vec{B}$ field → Next Lecture

LECTURE 14 11:30 - 13:00

# JOINT MEASUREMENT, STEERING & NONLOCALITY

GURUPRASAD KAR

ISI KOLKATA

---

Today :- Spin Case (No $\infty$ - dimensional ado)

Mantra:- Existence/Nonexistence of joint measurement has something to say about steering

Spin along two different directions $\longrightarrow$ do not admit joint measurement (other than trivially for $+\hat{n}$ & $-\hat{n}$ directions)

$$\hat{n}.\vec{\sigma} = (+)\tfrac{1}{2}\left[\mathbb{1}+\hat{n}.\vec{\sigma}\right] + (-)\tfrac{1}{2}\left[\mathbb{1}-\hat{n}.\vec{\sigma}\right]$$

Unsharp Spin Observable $F(a) = \frac{1}{2}\left[\mathbb{1} + \vec{a}.\vec{\sigma}\right] \quad |\vec{a}| \leq 1$

$$= \frac{1+|a|}{2}\,\frac{\mathbb{1}+\vec{a}.\vec{\sigma}}{2} + \frac{1-|a|}{2}\,\frac{\mathbb{1}-\vec{a}.\vec{\sigma}}{2}$$

$\frac{1+|a|}{2}$ : Degree of Reality

$\frac{1-|a|}{2}$ : Degree of Unsharpness

When $|a| = 1$ Then $\longrightarrow$ Reduces to Sharp spin measurement
When $|a| < 1$ Then $\longrightarrow$ POVM measurement

Q:- What's the condition that we can find four POVM's whose marginals $\Rightarrow$ diff direction spin measurement

Consider $\begin{cases} F_1, \mathbb{1}-F_1 \\ F_2, \mathbb{1}-F_2 \end{cases}$ Constraint :- Find 4 POVM's such that & each element $F_{ij} > 0$ $\quad F_{12} + F_{\bar{1}2} + F_{1\bar{2}} + F_{\bar{1}\bar{2}} = \mathbb{1}$

Demo $F_{1\bar{2}} \to F_1$ gives $+1$, $F_2$ gives $-1$

Then → Marginality Conditions :- Constraint

i) $F_{12} + F_{\bar{1}2} = F_2$

ii) $F_{12} + F_{1\bar{2}} = F_1$

iii) $F_{\bar{1}2} + F_{\bar{1}\bar{2}} = \mathbb{1} - F_1 = F_{\bar{1}}$

iv) $F_{1\bar{2}} + F_{\bar{1}\bar{2}} = F_{\bar{2}} = \mathbb{1} - F_2$

Consider $F(a_i) = \frac{1}{2}\left[\mathbb{1} + \vec{a}_i \cdot \vec{\sigma}\right] \quad [i = 1,2]$

for joint observables to exist → must exist some $\gamma$ $F(c)$ s.t.

$$0 \le \gamma F(c) \le \mathbb{1}$$
$$\gamma F(c) \le F(a_1)$$
$$\gamma F(c) \le F(a_2)$$
$$F(a_1) + F(a_2) - \gamma F(c) \le \mathbb{1}$$

[Proof Hint :- Use $\alpha F(\vec{a}) \le \beta F(\vec{b}) \Rightarrow (\alpha\vec{a} - \beta\vec{b}) \cdot \vec{\sigma} \le (\beta - \alpha) \Rightarrow |\beta\vec{b} - \alpha\vec{a}| \le \beta - \alpha$]

Now we get $|\gamma c| \le \gamma$; $|a_1 - \gamma c| \le 1-\gamma$; $|a_2 - \gamma c| \le 1-\gamma$ ; $|a_1 + a_2 - \gamma c| \le \gamma$

$S(a,r)$ is a closed ball with centre $\vec{a}$ & radius $r$

$\gamma c \in S(a_1, 1-\gamma) \cap S(a_2, 1-\gamma) \cap S(a_1+a_2, \gamma) \cap S(0,\gamma)$

Now: If This is $\phi$ ↓ $\gamma \le 1 - \frac{1}{2}|a_1 - a_2|$

If this is $\phi$ ↓ $\gamma \ge \frac{1}{2}|a_1 + a_2|$

$1 - \frac{1}{2}|a_1 - a_2| \ge \frac{1}{2}|a_1 + a_2| \Rightarrow |a_1 + a_2| + |a_1 - a_2| \le 2$

Paul Busch (1988)

Now; if $a_1 = \lambda \hat{a}_1$ & $a_2 = \lambda \hat{a}_2$ then $\lambda(\underbrace{|\hat{a}_1 + \hat{a}_2| + |\hat{a}_1 - \hat{a}_2|}_{\text{Maximum} = 2\sqrt{2}}) \le 2$

$\therefore \lambda \le \frac{1}{\sqrt{2}}$

## What about Higher Dimensional Case?

Two observables $P, 1-P$
$Q, 1-Q$
Unsharp counterpart $\longrightarrow$ $E = \frac{1+\lambda}{2} P + \frac{1-\lambda}{2}(\mathbb{1}-P)$

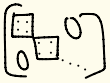
$F = \frac{1+\lambda}{2} Q + \frac{1-\lambda}{2}(\mathbb{1}-Q)$

**Thm:** $\exists$ an orthonormal basis s.t. $H = \bigoplus_{\alpha=1}^{k} H_\alpha$ [$H_\alpha$ = at most 2-dim]

s.t. $\mathbb{P} = \sum_{\alpha=1}^{k} P^{(\alpha)}$ ; $Q = \sum_{\alpha=1}^{k} Q^{(\alpha)}$

↓ Can they be diagonalized?

↓ Can be block diagonalized



Separable into different blocks

$\therefore$ Still $\lambda_{opt} = \frac{1}{\sqrt{2}}$ ... Wow!

What is $\lambda_{opt}$ for any theory?

* Classically $\lambda_{opt} = 1$
* Quantum Mechanics $= \frac{1}{\sqrt{2}}$
* PR Box $= \frac{1}{2}$
* Any Non-Signalling GPT with state space → compact convex subset of a finite dimensional vector space.

## BELL INEQUALITY

Conditions (Any one of them will do)

① LOCALITY $p(ij|AB) = \int p_\lambda(i|A)\, p_\lambda(j|B)\, d\lambda\, p(\lambda)$ [Bell '64]

② EXISTENCE $p(ijmn|ABCD)$ exists (Fine '82)

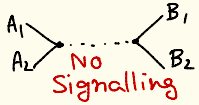
## ③ ON ONE SIDE JOINT MEASUREMENT EXISTS + NO-SIGNALLING

i.e. $p(ijm|A_1A_2B_1)$ & $p(ijn|A_1A_2B_2)$ exist & $p(ij|A_1A_2;B_1) = p(ij|A_1A_2;B_2) \rightarrow$ No signaling

Where $p(ij|A_1A_2;B_1) = \sum_m p(ijm|A_1A_2B_1)$ [Andersson et al '2005]

## ② ≡ ③ Proved Equivalence ⟶ Wolfe

Outlining the Derivation of Bell Inequality on the assumption of joint measurement on one side & no signalling constraint




ASSUMPTION :- ① $A_1, A_2$ jointly measurement (dichotomic) ② No Signalling

$$p[v(A)=v(A_2);B] = p[v(A_1)=v(A_2)=v(B)] + p[v(A_1)=v(A_2)=-v(B)]$$

$$\geq \left| p[v(A_1)=v(A_2)=v(B)] - p[v(A_1)=v(A_2)=-v(B)] \right|$$

$$= \frac{1}{2}\left| p[v(A_1)=v(B)] - p[v(A_1)=-v(B)] + p[v(A_2)=v(B)] - p[v(A_2)=-v(B)] \right|$$

$$= \frac{1}{2}|E(A_1,B)+E(A_2,B)|$$

Thus, for $B=B_1$

$$p[v(A_1)=v(A_2);B_1] \geq \frac{1}{2}|E(A_1,B_1)+E(A_2,B_1)|$$

Similarly $p[v(A_1)=-v(A_2);B_2] \geq \frac{1}{2}|E(A_1,B_2)-E(A_2,B_2)|$

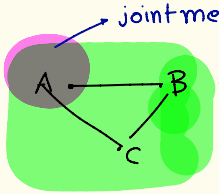
∴ Hence; Using Triangle Inequality →

$$|E(A_1,B_1)+E(A_2,B_1)|+|E(A_1,B_2)-E(A_2,B_2)| \leq 2$$

$$\Rightarrow |E(A_1,B_1)+E(A_1,B_1)+E(A_1,B_2)-E(A_2,B_2)| \leq 2 \rightarrow \text{Bell Inequality}$$

Stupid Question?

Multipartite Scenario




Possible to get a Bell-like Inequality ????
(in terms of $A_1, A_2, B_1, B_2, C_1, C_2$)
just assuming joint measurement on one of many parties?

for a general no signalling theory

$$E(A_1,B_1) + E(A_2,B_1) + E(A_1,B_2) - E(A_2,B_2) \leq \frac{2}{\lambda_{opt}}$$

∴ for PR Box ⟶ Bound = 4
for QM ⟶ " $= 2\sqrt{2}$
for Class Mech ⟶ " $= 2$

Reverse Question :- Does impossibility of joint measurement imply Bell Violation ?

↓

YES ! → Wolfe

Q :- How to optimize $\lambda_{opt}$ for specific measurement direction ?

→ Some LPP Problem

↓

কিছু একটা লেখে

So; does measurement incompatibility necessarily lead to Nonlocality?

↓

Yes for incompatible observable with binary outcome

↓

In general :- Open ! (Necessarily leads to steering → this is known)

# STEERING

A & B share a singlet

Alice can now fool Bob into preparing a desired ensemble.

↓

Without Entanglement → Alice can't fool Bob

Even with entanglement ⟶ may not be done.

If Joint measurement exists ⟶ Alice can cheat without using entanglement.

CHECK SLIDES FOR DETAILED CALCULATIONS

LECTURE - 15 14:30 - 16:00

# QUANTUM GAMES

COLIN BENJAMIN

NISER BHUBANESWAR

---

What is a Game ?

Some competitive activity played with definite rules.

Am J. Phys. → Quantum Tic Tac Toe / Quantum Chess

Von Neumann

↓

Game ≡ Decision making

↓

Rigorous Branch of Mathematics underlying real conflicts among irrational human beings

Biology:- Axelrod "Evolution of Cooperation"

↓

Introduce game theory in Biology. (1970s)

↓

Evolutionary Game Theory

Quantum Game Theory ⇒ Important algorithms.

El Ferrol Bar Problem → Which Restaurant shall I go to avoid the crowd ? (Minority Game)

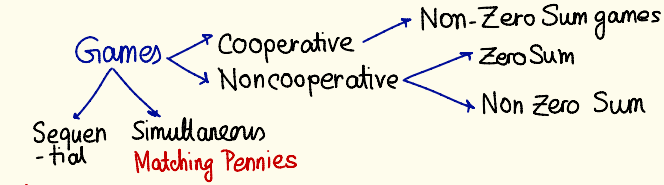
↓

Application in Statistical Physics (Certain Phase Transitions)

Player:- Game Theory is about logical players interested only in winning.

Actions:- The set of all choices available to a player.

Payoff:- With Each Action, we associate with a reward. Optimal Strategy:- Which action to take to maximize my payoff




## Von Neumann Cake Division (Minimax)

CHOOSER

CUTTER

| | Half 'c' | Half 'c' |
|---|---|---|
| Sm a ll | Big Piece | |

Payoff Matrix

Von Neumann → Best Strategy = Half the cake minus the crumb

Cuttermaximin (maximum row minimum)
Chooser minimax (minimum row maximum)

## Prisoner's Dilemma

Nash Eqbm. → No player can unilaterally change his/her strategy & do better.

| A \ B | Snitch | Don't |
|---|---|---|
| Snitch | 3,3 | 0,6 |
| Don't | 6,0 | 1,1 |

Nash Eqbm. Strategy
Pareto Optimal Strategy

## Matching Pennies (Zero Sum)

| A \ B | H | T |
|---|---|---|
| H | 1,-1 | -1,1 |
| T | -1,1 | 1,-1 |

→ There is no Nash Equilibrium for pure strategy.
Maximin
Minimax

Random Strategy → Choose 50% H, 50% T randomly.
↓
Mixed Strategy

Pure Strategy:- Same Strategy each time.
Mixed Strategy:- Diff Strategy diff time.

Matching Pennies :- Unique mixed strategy NE

↓

$X$ = Prob of Alice playing H
$Y$ = " " Bob " H

$$\Pi_A(x,y) = \begin{pmatrix} x \\ 1-x \end{pmatrix}^T \begin{pmatrix} (a_1,b_1) & (a_2,b_2) \\ (a_3,b_3) & (a_4,b_4) \end{pmatrix} \begin{pmatrix} y \\ 1-y \end{pmatrix}$$

↓

NE when $\Pi_A(x^*,y^*) - \Pi_A(x,y^*) \geq 0$ & $\Pi_B(x^*,y^*) - \Pi_B(x^*,y) \geq 0$

For the Payoff matrix → this reads → $2(x^*-x)(2y^*-1) \geq 0$
$2(y^*-y)(-2x^*+1) \geq 0$

↓

Unique NE $\equiv (x^*,y^*) = \left(\frac{1}{2},\frac{1}{2}\right)$

At Nash Eqn Payoff $\Pi_A = \Pi_B = 0$

## Penny Flip

P & Q have a single penny → initially H → Q → P → Q

| | FF | FN | NF | NN |
|---|---|---|---|---|
| F | + − | − + | − + | + − |
| N | − + | + − | + − | − + |

No Pure Strategy NE; but mixed strategy NE. (HW :- What's the NE?)

## QUANTUM GAMES

Superposed Initial States
Quantum Entanglement of Initial States

## Quantum Penny Flip

$P \rightarrow$ Classical moves ($X$ or $\mathbb{1}$)
$Q \rightarrow$ Quantum moves (Hadamard)

$$|0\rangle \xrightarrow{Q\ H} \frac{|0\rangle+|1\rangle}{\sqrt{2}} \xrightarrow[X \text{ or } \mathbb{1}]{P} \frac{|0\rangle+|1\rangle}{\sqrt{2}} \xrightarrow{Q\ H} |0\rangle \rightsquigarrow Q \text{ always wins.}$$

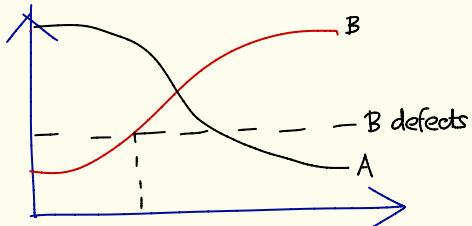
## Quantum Prisoner's Dilemma

- $|\psi_{in}\rangle = |00\rangle$
- Generate Entanglement via $\hat{J}(\gamma) = \cos\frac{\gamma}{2}\,\hat{\mathbb{1}}\otimes\hat{\mathbb{1}} + i\sin\left(\frac{\gamma}{2}\right)\hat{\sigma}_x\otimes\hat{\sigma}_x$
- $|\psi_{fin}\rangle = \hat{J}^{\dagger}(\gamma)\,(\hat{A}\otimes\hat{B})\,\hat{J}(\gamma)\,|00\rangle$

Quantum Payoff for Alice/Bob $\rightarrow \langle \$ \rangle = \sum_{i,j=1}^{2} \$_{ij}\,|\langle ij|\psi_{fin}\rangle|^2$

↓

Eisert Miracle $\rightarrow \hat{M}\left(\frac{\pi}{2}, \frac{\pi}{2}, 0\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$




Solid → Bob plays Miracle moves
Dashed → Bob Defects

**General Q:-**
How much resource (Coherence/Entanglement.) one needs to improve the winning strategy by some given amount?

**Van Enk:-** Does this solve the Original Prisoner's Dilemma.

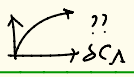
???

**Take the Penny Flip Game (Q = Quantum, P = Classical)**

Q's prob of winning for optimal classical strategy $= p$ .. (Say) [When P & Q are both Classical]
Now instead of Hadamard → Q applies a map $\Lambda$ s.t. $\Lambda$ creates $\delta C$ amount of coherence
[for Hadamard $\delta C = 1 \Rightarrow$ maximally coherent output] & prob of winning $= \tilde{p}$ .. (Say)
[$\tilde{p} = 1$ for Hadamard] Then ($\tilde{p} - p = \delta p$ .. (Say))

$\delta P = (\ )\,\delta C$ ?? for any general map $\Lambda$ ?

or any other final relation? $f(\delta P, \delta C_\Lambda) = 0$ ??



Non-Local Games $\Rightarrow$ XOR/CHSH Game

Parrondo Game

Two losing Strategies combined $\rightarrow$ Winning Strategy

Ref:- Asturian Paradox

$\downarrow$

Martin Van Baeyer Am J. Phys. 72 710 (2004)
Review on Parrondo Games

History dependent Parrondo Game $\rightarrow$ Look up...

Quantum Parrondo Game $\longrightarrow$ Physica A (2003).

LECTURE 16 16:30 - 18:00

# QUANTUM THERMODYNAMICS

SIBASHIS GHOSH

JMSc Chennai

---

In Last Lecture → start with any state $\rho_S$ → end up with a very high prob very near the thermal state subject to $d_{eff}$ (env.) $\gg$ d system.

Can We do Better ? (Better values of $\eta$ and $\eta'$ ?)

YES $\Rightarrow$ FOR SPECIFIC MODELS

**Thm :- (Modification of Morning Thm) [Statement Only]**

Assume $\exists$ some bounded +ve operator $X_R$ on $\mathcal{H}_R$ satisfying $0 \le X_R \le \mathbb{1}_R$ [POVM Elements] such that with $\tilde{\mathcal{E}}_R = X_R^{1/2}\, \mathcal{E}_R\, X_R^{1/2}$, we have

$$\mathrm{Tr}(\tilde{\mathcal{E}}_R) = \mathrm{Tr}(\mathcal{E}_R X_R) \ge 1-\delta$$

High Chance on equiprobable states $\mathcal{E}_R$ to get this measurement outcome

For a randomly chosen state $|\psi\rangle \in \mathcal{H}_R$ & $\varepsilon > 0$

$$\mathrm{Prob}\left[ \| \rho_S - \Omega_S \|_1 \ge \tilde{\eta} \right] \le \tilde{\eta}'$$

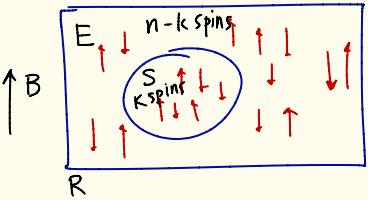
Where $\tilde{\eta} = \varepsilon + \sqrt{\frac{d_S}{d_{eff}}} + 4\sqrt{\delta}$

and $\tilde{\eta}' = 2\exp\left[-c\, d_R\, \varepsilon^2\right]$ $\qquad \tilde{\Omega}_E = \mathrm{Tr}_S(\tilde{\mathcal{E}}_R)$

$$\tilde{d}_E^{eff} = \frac{1}{\mathrm{Tr}\,\tilde{\Omega}_E^2}$$

Example :-

## SPIN SYSTEM




$R \equiv np$ spins in $\uparrow$
$\equiv n(1-p)$ spins in $\downarrow$ } Say

$d_S = 2^k$ ; $d_E = 2^{n-k}$ $\Rightarrow$ What can I say about $d_R$ ?

$$d_R = \binom{n}{np} = \frac{n!}{(np)!\,nq!}$$

$$\geq \frac{2^{nH(p)}}{n+1}$$ [H(p) = 2 point Shannon Entropy] (for large n)

Now using Thm 1 (Manning) $\longrightarrow$

$$\text{Prob}\left[\| \rho_S - \Omega_S \|_1 \geq \eta\right] \leq \eta'$$

Where $\eta = \varepsilon + \sqrt{\frac{d_S}{d_{eff}}}$, $\eta' = \exp\left[-c d_R \varepsilon^2\right]$

$$\sqrt{\frac{d_S}{d_{eff}}} \leq \sqrt{\frac{d_S^2}{d_R}} \leq d_S \frac{\sqrt{n+1}}{2^{\frac{nH(p)}{2}}} = \frac{2}{\sqrt{n+1}}\, 2^{-(nH(p) - 2k)/2}$$ and $\varepsilon = d_R^{-\frac{1}{3}} \leq \frac{(n+1)^{1/3}}{2^{\frac{nH(p)}{3}}} \ll 1$ for $n \to \infty$

$$\therefore \text{Prob}\left[\|\rho_S - \Omega_S\|_1 \geq d_R^{-\frac{1}{3}} + \sqrt{\frac{2^k}{d_{eff}}}\right] \leq 2e^{-c d_R^{1/3}}$$

Putting this expression $\rightarrow$ (for n = very large) $\Rightarrow$ $\|\rho_S - \Omega_S\|_1 \to 0$ in the large n limit.

[Valid subject to $n \gg k$]

Moral :- For arbitrary pure state $\in \mathcal{H}_R$ $\longrightarrow$ it WILL Thermalize ... (For This Specific System)

Popescu, Short, Winter $\longrightarrow$ arXiv version $\rightarrow$ 2005

so; $d_{eff} \ll d_{env}$ but so long as $d_{eff} \gg d_S$ $\rightarrow$ Thermalization is safe. ☺

# THERMAL MACHINES

What happens if we go from Classical → Quantum Engines

Popescu et al PRL (2010) — Smallest Possible Refrigerator

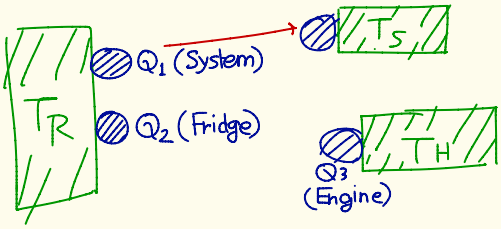
Claim :- 1) It can be done
2) Even Better → it can go to $T \to 0$ limit

Q :- Smallest Hilbert Space dimension in which I can construct a refrigerator ?

Two Qubit Model | Qubit Qutrit with n-n interaction | Single Qutrit system

POPESCU, LINDEN } 3 models

Today :- Only the two-qubit model




$T_R$ = room temp
$T_H$ = Bath temp (Hot)
} $T_R < T_H$

Free Hamiltonian $H_0 = E_1 |1\rangle\langle 1| + E_2 |2\rangle\langle 2|$ (Assume $E_1 < E_2$)

$|i\rangle\langle i|$ = excited state of i-th qubit ($i = 1, 2$)
Ground State Energy for both qubits = 0 .. (assume)

∴ Thermal State of First Qubit = $\tau_1 = \frac{e^{-\beta E_1 |1\rangle\langle 1|}}{Tr\left[e^{-\beta E_1 |1\rangle\langle 1|}\right]}$

Similarly for the second qubit $\tau_2 = r_1 |0\rangle\langle 0| + (1-r_1)|1\rangle\langle 1|$ $\left\{ r_1 = \frac{1}{1+e^{-\beta E_1}};\ r_2 = \frac{e^{-\beta E_1}}{1+e^{-\beta E_1}} \right\}$

∴ Joint State → $\tau_1 \otimes \tau_2$ ∴ When Refrigeration occurs → The system achieves some steady state temp $T_i^S$ & the new $\tau_f$ of the first qubit = $r_i^S |0\rangle\langle 0| + (1-r_i^S)|1\rangle\langle 1|$

Clearly here $r_i^S > r_i$ $\left[\because \rho_f^1 \prec \rho_{init}^1\right]$

$$\therefore \tau_1 \otimes \tau_2 = \begin{bmatrix} r_1 r_2 & & & \\ & r_1 \tilde{r}_2 & \bigcirc & \\ & \bigcirc & \tilde{r}_1 r_2 & \\ & & & \tilde{r}_1 \tilde{r}_2 \end{bmatrix} \quad \tilde{r}_i = 1 - r_i \ (i = 1, 2)$$

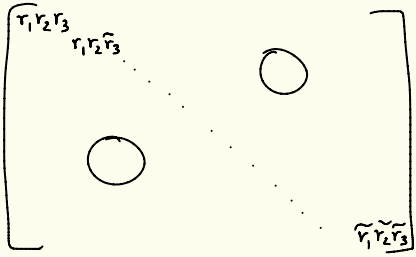
Now if $E_1 < E_2$ implies $r_1 > r_2$

∴ Here coefft of $|01\rangle$ has higher energy than $|10\rangle$ $\xrightarrow{\text{Swap}}$ .... ≡ Cooling

Caveat :- Applying this unitary Swap is not free → Idea :- Use free Energy

Add a third qubit which is at contact with a high temp bath ($E_3 = E_2 - E_1$)

Joint State of the system $\tau_1 \otimes \tau_2 \otimes \tau_3$

$=$ 


Check:-
Verify that coefft of $|010\rangle$ = coefft of $|101\rangle$
$[r_1 \tilde{r}_2 r_3 = \tilde{r}_1 r_2 \tilde{r}_3]$

Now can I cool ? (Not forbidden now !)

Won't be using SWAP, rather will use an interaction

$H_{int} = g(|010\rangle\langle 101| + |101\rangle\langle 010|)$ ; Assume $E_i \gg g$ → Will not change eigenvalues & eigenvectors significantly.

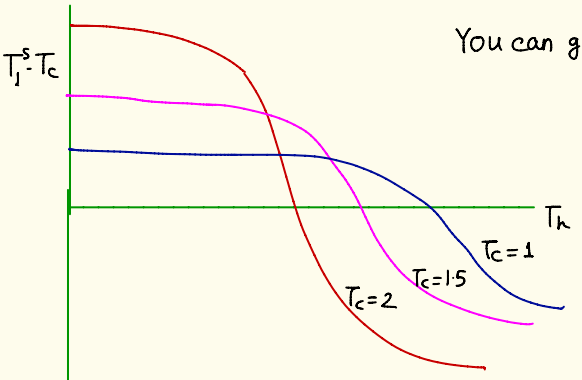
What happens to free coherence constraints? Study!

**Phenomenological model:-**
With probability $p_i$ per unit time → the i-th qubit goes back to original state

Now I want a dynamics for this

Master Equation :- $\frac{\partial \rho}{\partial t} = -i[H_0 + H_{int}, \rho] + \sum_{i=1}^{3} p_i \underbrace{(\tau_i \otimes Tr_i \rho - \rho)}_{\text{Lindblad term}}$

Approach:- Look at the steady state solution & corresponding steady state temperature
↓
Doable analytically, but boring hard calculation → done numerically.




You can go $T \to 0$ → Efficiency = Carnot Efficiency

DAY-5

LECTURE 17 09:30-11:00

# Is Wavefunction a part of the Reality ?

Guruprasad Kar
ISI Kolkata