Strong advantage of quantum systems (as communication resource) over the classical counterparts

Manik Banik

IMSc, Chennai, India

YouQu-2017, HRI, Allahabad

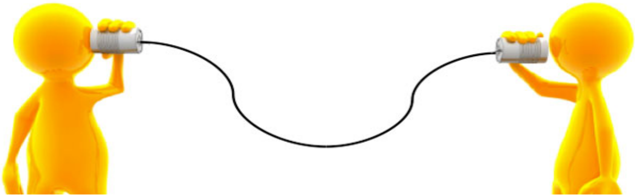
Figure: Maria (IMSc)

Figure: Andris (LU, Latvia)

Figure: Ashutosh (LU, Latvia)

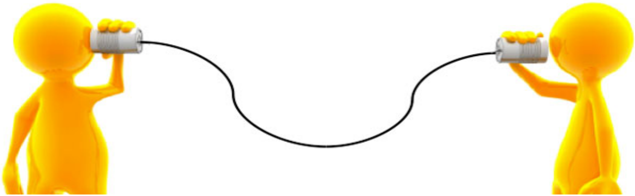
"Prithibi-ta naki choto hote hote...."

A naive view:

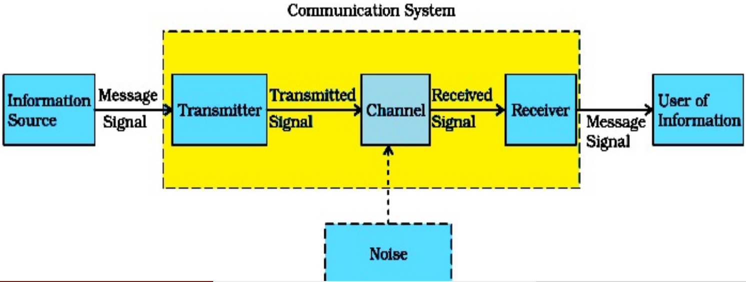


Communication process –in a nutshell

A naive view:



An engineer's view:



Communication media

Sender must encode her/his information in some physical system: particle, radiation field, laser pulse etc.

Classical System

Finite dim system describe by simplex: d-dim classical system $\Rightarrow$ associated with $(d-1)$-simplex

1-simplex $\rightarrow$ line segment

2-simplex $\rightarrow$ triangle

3-simplex $\rightarrow$ tetrahedron

Quantum system

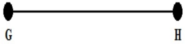
d-dim quantum system is associated Hilbert space $\mathbb{C}^d$

State$\Rightarrow$ $\mathcal{D}(\mathbb{C}^d)$

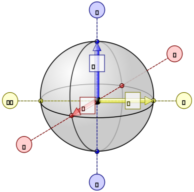
$\mathcal{D}(\mathbb{C}^d)$ $\Rightarrow$ Set of density operators: a convex set

Classical Vs Quantum: Example

♣ For example, consider a two level Classical system: a two-faced classical coin
⇒ Its states space is 1-simplex, i.e., a line segment



⇒ Note that it has only two 'pure'/'extremal' points
♣ Correspondingly, state space of a two level quantum is a Bloch sphere in $\mathbb{R}^3$



⇒ It has infinite (actually uncountably many) 'pure' states

Holevo's theorem: a limitative theorem (Prob. of Inf. Trans. 9: 177-183)

- **Let the sender (say, Alice) has a letter (classical random variable) x taking values from an alphabet set $x \in \mathcal{X} \equiv \{x_1, x_2, ..., x_n\}$ with corresponding probabilities $\{p_1, p_2, ..., p_n\}$.**
- **Alice encodes the letters in some quantum states: $x \to \rho_x$; and gives this state to Bob**
- **Bob's aim: guess the value of x; for that he performs a measurement on the state and obtains a classical outcome $y \in \mathcal{Y}$**
- **Amount of "accessible information", i.e., the amount of information that Bob can get about the variable $\mathcal{X}$, is the maximum value of the mutual information $I(\mathcal{X} : \mathcal{Y})$**

Holevo's theorem

$$\mathbf{I}(\mathcal{X} : \mathcal{Y}) \leq \mathbf{S}(\rho) - \sum_{\mathbf{i}} \mathbf{p_i} \mathbf{S}(\rho_{\mathbf{i}}); \quad \rho = \sum_{\mathbf{i}} \mathbf{p_i} \rho_{\mathbf{i}}$$

A more general limitative theorem: Frenkel and Weiner (Commun. Math. Phys. 340, 563 (2015))

- A random variable x is revealed to Alice only
- She is allowed to send a quantum d-level system or a classical d-state system for communication
- Bob recovers the value of x by specifying a value y and a reward value $f(x,z)$ is given to the team
- Whatever the probability distribution of x and the reward function f are, there is no quantum advantages
- Proof technique: Frenkel and Weiner have actually proved that

$$\mathcal{P}_{Q^d}^{m\to n} = \mathcal{P}_{C^d}^{m\to n}, \quad \text{for arbitrary} \quad m,n;$$

where $\mathcal{P}_S^{m\to n} := \{P(x\in\mathcal{X}|y\in\mathcal{Y})\}$ is the set of conditional probability distribution generated by sending a system S.

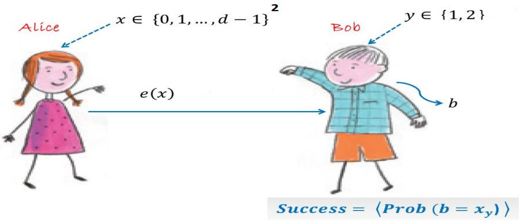
♣ **Holevo and Frenkel-Weiner results give enough reason for quantum physicists to worry about**

♣ **Does the story end here?**

- Quantum advantages have been established by Ambainis et al. in a class of communication tasks called Random Access Codes (RAC) [Theory of Computing, pp. 376-383, 1999; Journal of the ACM 49, 496 (2002)].
- Actually this task was first proposed by Stephen Wiesner in the name of Conjugate coding[SIGACT News, vol. 15, issue 1, pp. 78-88, 1983].
- Quantum-RAC finds applications in quantum finite automata [Nayak, arXiv:quant-ph/9904093], quantum communication complexity [Klauck, arXiv:quant-ph/0106160; Aaronson, arXiv:quant-ph/0402095; Gavinsky et al, arXiv:quant-ph/0511013], network coding [Hayashi et al, arXiv:quant-ph/0601088], locally decodable codes [Kerenidis & Wolf, arXiv:quant-ph/0208062; Wehner, arXiv:quant-ph/0403140; Ben-Aroya, arXiv:0705.3806] and quantum state learning [Aaronson, arXiv:quant-ph/0608142]
- Recently Tavakoli et al have studied d-level QRAC [Phys. Rev. Lett. 114, 170502 (2015)].

- Spekkens et al. have introduced a variant of QRAC, called Parity-Oblivious Multiplexing to establish operational usefulness of preparation contextuality[Phys. Rev. Lett. 102, 010401 (2009)].
- Further studies on this topic have been done by Banik et al. [Phys. Rev. A 92, 030103(Rapid) 2015]and by Chailloux et al.[New Journal of Physics (18) 045003, 2016].
- Recently we have studied parity oblivious QRAC for d-level system[arXiv:1607.05490 (quant-ph)].
- And our study has been further extended by Armin Tavakoli [arXiv:1609.09301 (quant-ph)]
- And a related study by Ambainis et al.[arXiv:1510.03045(quant-ph)].

Random Access Codes (RAC), the task



Alice: given n-dit string $x = x_1 ... x_n$ chosen uniformly at random from $\{0, 1, ..., d-1\}^n$

Bob's task: guess y^{th} bit of Alice string, y chosen uniformly at random from $\{1, ..., n\}$

- **Alice:** can send information, $[x \mapsto e(x)]$ to Bob.
- **Restriction:** Alice is allowed to transfer no more than 1-dit information.
- We will call it $[(n, d) \to 1]$ RAC

Optimal classical success

A. Ambainis, D. Kravchenko, and A. Rai [arXiv:1510.03045 (quant-ph)]

$[(n, d) \to 1]$ RAC

- **the strategy "majority-encoding-identity-decoding" is an optimal classical strategy**
- **However, a closed analytical formula is hard to derive for general values of parameters n and d**

Analytic expressions

- $[(2, d) \to 1]$ **RAC** $\implies P^C_{2,d} = \frac{1}{2}(1 + \frac{1}{d})$
- $[(3, d) \to 1]$ **RAC** $\implies P^C_{3,d} = \frac{1}{3}(1 + \frac{3}{d} - \frac{1}{d^2})$

♣ **Different QRACs:**

- $[(2,2)\rightarrow 1]$ **QRAC** $\Longrightarrow P^{Q}_{2,2}=\frac{1}{2}(1+\frac{1}{\sqrt{2}})$ [Ambainis et al.]
- $[(3,2)\rightarrow 1]$ **QRAC** $\Longrightarrow P^{Q}_{3,2}=\frac{1}{2}(1+\frac{1}{\sqrt{3}})$ [Chuang]
- **no** $[(n,2)\rightarrow 1]$ **QRAC with** $P^{Q}_{n,2}>\frac{1}{2}$**, for** $n\geq 4$ [Hayashi et al.]
- $[(2,d)\rightarrow 1]$ **QRAC** $\Longrightarrow P^{Q}_{2,d}=\frac{1}{2}(1+\frac{1}{\sqrt{d}})$ [Tavakoli et al.]
- $[(3,d)\rightarrow 1]$ **QRAC** $\Longrightarrow P^{Q}_{3,d}>P^{C}_{3,d}$ [Tavakoli et al.]

All this results establish quantum supremacy of d-level quantum systems over the corresponding d-state classical systems.

We ask another question: Can a d-level quantum system $\succ$ d'-level classical system, with $d<d'$?

♣ **Protocol:**

- **Consider the computational Basis:** $\mathcal{B}_C := \{|l\rangle\}_{l=0}^{d-1}$
- **Consider the Fourier Basis:** $\mathcal{B}_F := \{|e_l\rangle\}_{l=0}^{d-1}$**;** **where** $|e_l\rangle := \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kl}|l\rangle$ **and** $\omega = \exp(\frac{2\pi i}{d})$**.**
- **Also consider the operators** $X := \sum_{k=0}^{d-1}|k+1\rangle\langle k|$ **and** $Z := \sum_{k=0}^{d-1}\omega^k|k\rangle\langle k|$
- **Consider the quantum state** $|\psi_{00}\rangle := \frac{1}{N_{2,d}}(|0\rangle + |e_0\rangle) \in \mathbb{C}^d$**, where** $N_{2,d} = \sqrt{2+2/\sqrt{d}}$ **is the normalization factor.**

- **Alice: given a random string $x_1x_2 \in \{0, ..., d'-1\}^2$, where $d' > d$**
- **Alice's encoding:**

$$x_1x_2 \to |\psi_{x_1,x_2}\rangle := \mathcal{G}(x_1, x_2, X, Z)|\psi_{00}\rangle \in \mathbb{C}^d$$

where

$$\mathcal{G}(x_1, x_2, X, Z) = \begin{cases} X^{x_1}Z^{x_2}, & \text{if both } x_1, x_2 \leq d' \\ \mathbf{1}, & \text{otherwise.} \end{cases}$$

- **Bob's decoding:**

First letter $\Rightarrow$ performs measurement in the basis $\mathcal{B}_C$

$\Rightarrow$ **on obtaining outcome $l \in \{1, .., d-1\}$, he answers l**

$\Rightarrow$ **otherwise answers $\{0, d, d+1, ..., d'-1\}$ randomly**

Second letter $\Rightarrow$ performs measurement in the $\mathcal{B}_F$ basis

$\Rightarrow$ **follow the similar protocol like first letter**

Quantum protocol: Success probability

- **If we play the $[(2,d') \to 1]$ RAC with a quantum system of dimension d like the above protocol then the success probability becomes**

$$P^Q_{res} = \frac{d'-r}{2d'}\left(1+\frac{1}{\sqrt{d'-r}}\right),$$

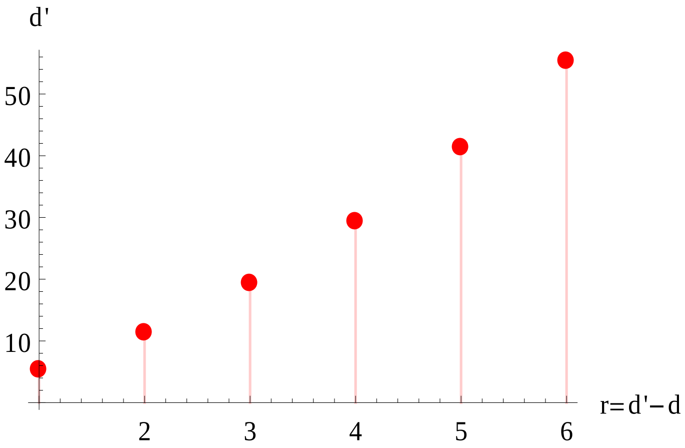
where $r = d' - d$.

- **Corresponding Classical probability is $P^C_{2,d'} = \frac{1}{2}\left(1+\frac{1}{d'}\right)$.**

We have $P^Q_{res} > P^C_{2,d'}$ if $d' > r^2 + 3r + 1$

- **Therefore quantum protocol gives advantage for $d \geq 6$ and $r \in \{1, ..., \lfloor\frac{1}{2}(-3+\sqrt{4d'+5})\rfloor\}$, where $\lfloor a \rfloor$ is the greatest integer less then or equal to a.**

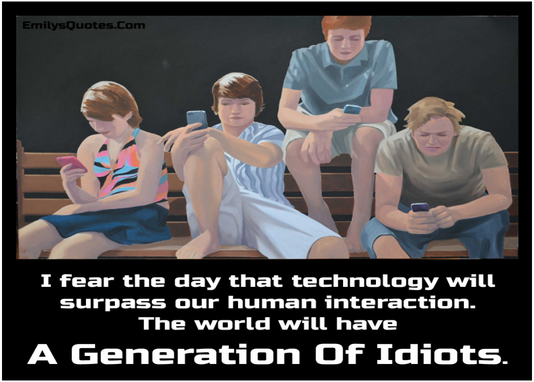
Quantum protocol: Success probability....



Concluding Remarks

- **Continuity of quantum theory provides an enormous power to encode infinite information in a finite level quantum systems.**
- **But, Holevo and Frenkel-Weiner like theorems put severe limitation on the information storage capacity of such systems.**
- **However, in RAC, PO-RAC like tasks quantum supremacy have been established as communication resource.**
- **Our work establishes a stronger quantum supremacy.**
- **Optimality of our task or introducing some new tasks showing such quantum supremacy may be interesting research problem.**

Thanks for your patience..



Questions, Comments !!