Quantum Advantage in Shared Randomness Processing

Tamal Guha[1], Mir Alimuddin[1], Sumit Rout[2], Amit Mukherjee[3], Some Sankar Bhattacharya[4], Manik Banik[5,*]

1– Physics and Applied Mathematics Unit, Indian Statistical Institute, 203 B.T. Road, Kolkata 700108, India.
2– Integrated Science Education and Research Centre, Visva Bharati University, Santiniketan 731235, India.
3– S.N. Bose National Center for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700098, India.
4– Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong.
5– School of Physics, IISER Thiruvanathapuram, Vithura, Kerala 695551, India.

Abstract: Randomness appears both in classical stochastic physics and in quantum mechanics. Here we address a computational scenario of shared randomness processing where a quantum source manifest clear-cut precedence over the corresponding classical counterpart. To this aim we formulate a *resource theory* framework for shared randomness processing. The advantage is operationally viable as it is manifested in the optimal payoff of a game involving two players. In distributing shared randomness between distant parties, we also exhibit advantage of noisy quantum channel (with sub-optimal classical capacity) over a perfect classical channel. Surprisingly, the advantage persists even when the channel has zero quantum capacity. The noisy channel examples facilitate noise-robust empirical setups to verify the obtained quantum advantage.

Motivation

One of the central motives in quantum information theory is to identify advantageous applications of quantum rules in practical tasks. Quantum advantages are, however, hard to find and even harder to establish. For instance, exponential speed-up by quantum computing for a range of problems, such as factoring, sustains under the assumption (yet to be proved) that no efficient classical algorithm is possible for them.

Here we consider the task of processing shared randomness which has already been established as an important resource for a range of problems, starting from Privacy amplification and Secure key generation, Simultaneous message passing model, Simulating nonlocal correlation, Random access codes, Communication complexity to Bayesian game theory. We established that quantum theory provably yields resource reduction over classical stochastic physics in shared randomness processing.

Principal Contributions

- Formulate a resource theory of Shared Randomness (SR)
- Establish quantum advantage in SR processing
- Show that Quantum Discord is necessary for the desired advantage
- Demonstrate advantage of noisy quantum channel in SR distribution

Resource theory of SR

The framework of resource theory provides a novel approach to quantify different physical resources. Generic framework of any such theory identifies: (i) class free states, (ii) class of free operations, and (iii) resource conversion conditions (monotones).

Free states: A source of SR is specified by a bipartite probability distribution $P(\mathcal{X},\mathcal{Y}) \equiv \{p(x,y) \mid x \in \mathcal{X}, y \in \mathcal{Y}\}$, where $\mathcal{X}$ and $\mathcal{Y}$ are the parts of the shared variable accessible by spatially separated parties Alice and Bob, respectively. Probability distributions of the product form $P(\mathcal{X},\mathcal{Y}) = P(\mathcal{X})Q(\mathcal{Y})$ are considered as free resources/states.

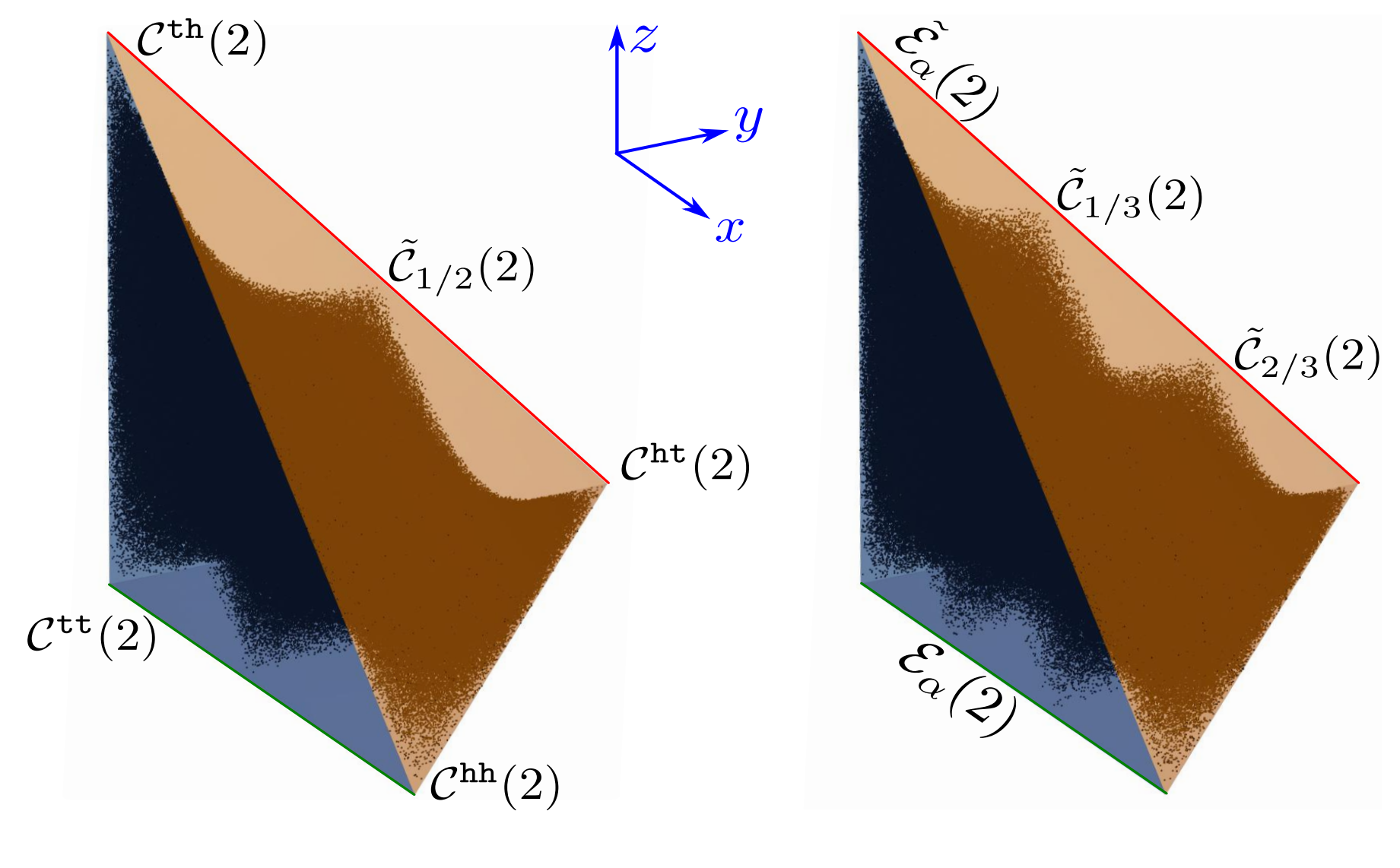


Fig.1: Two-2-coin state space $\mathfrak{C}(2)$. A generic state is described as $\mathcal{C}(2) \equiv (p(\mathtt{hh}), p(\mathtt{ht}), p(\mathtt{th}), p(\mathtt{tt}))^{\intercal} \equiv (x,y,z,1-x-y-z)^{\intercal}$, isomorphic to the vector $(x,y,z)^{\intercal} \in \mathbb{R}^3$ with $x,y,z \geq 0$ & $x+y+z \leq 1$.

Free operations: Local product operations $L_A \otimes L_B$ applied by Alice and Bob on their respective parts. For classical systems such operations are most generally described by tensor product of local stochastic matrices $\mathcal{S}_A \otimes \mathcal{S}_B$, where $\mathcal{S}_A$ maps Alice's local probability vector $P(\mathcal{X})$ into a new probability vector $P'(\mathcal{X}')$ and $\mathcal{S}_B$ does the similar on Bob's part. In quantum case, free operations are product CPTP maps $\Lambda_A \otimes \Lambda_B$.

Resource monotones: A necessary condition of state conversion from a distribution $P(\mathcal{X},\mathcal{Y})$ to another $Q(\mathcal{X}',\mathcal{Y}')$ is given by $I(Q) \leq I(P)$, where $I(P)$ is the classical mutual information defined as $I(P) := H(\mathcal{X}) + H(\mathcal{Y}) - H(\mathcal{X},\mathcal{Y})$, with $H(\mathcal{X})$ being the Shannon entropy, $H(\mathcal{X}) := -\sum_{x\in\mathcal{X}} p(x)\log_2 p(x)$.

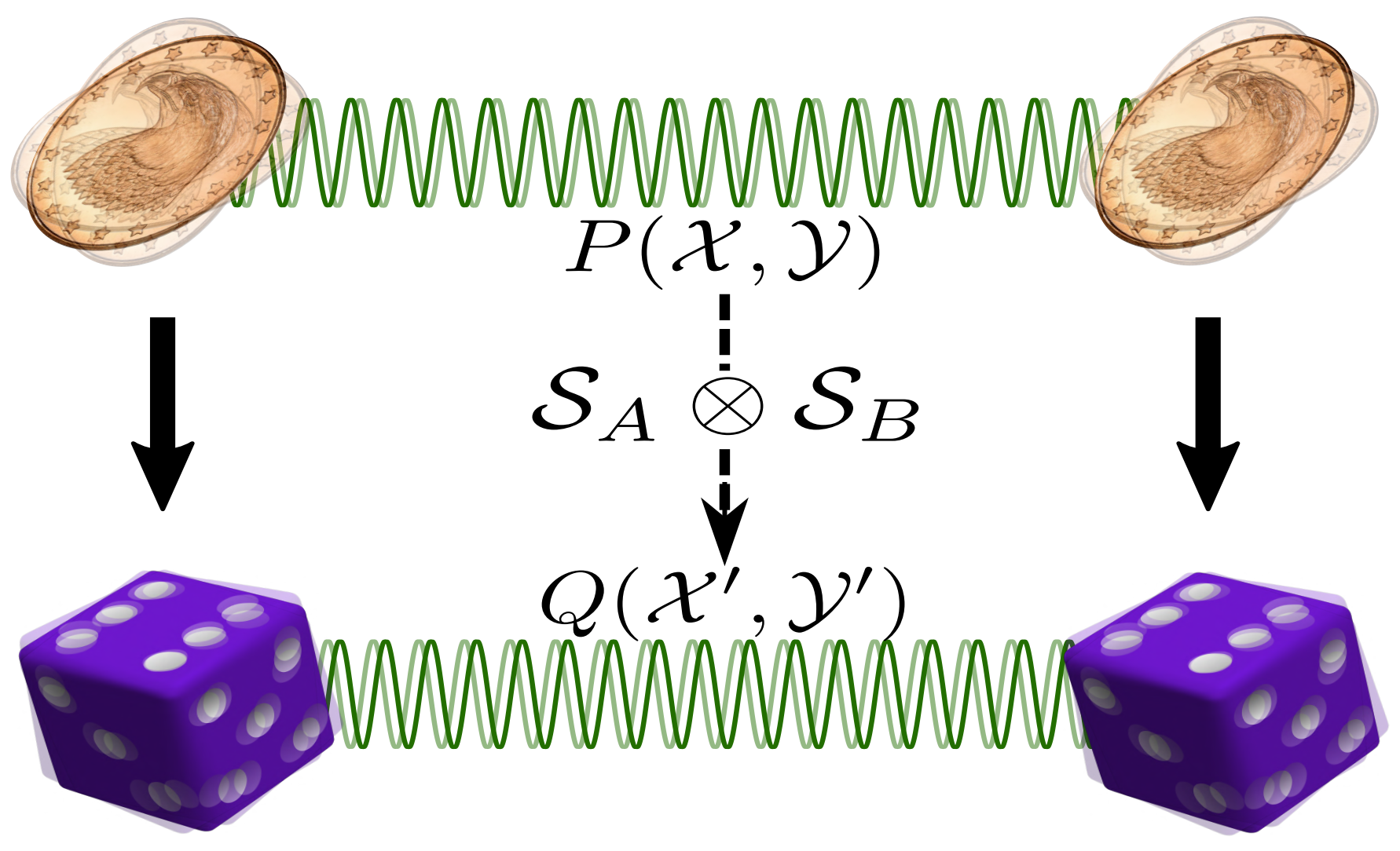

$P(\mathcal{X},\mathcal{Y})$
$\mathcal{S}_A \otimes \mathcal{S}_B$
$Q(\mathcal{X}',\mathcal{Y}')$

Fig.2: Free operations on two-2-coin states $\mathfrak{C}(2)$ generates only a proper subset $\mathfrak{S}_C(2 \mapsto d)$ of two-d-coin state space $\mathfrak{C}(d)$. For instance, the transformation $\mathcal{C}_{1/2}(2) \mapsto \mathcal{C}_{1/6}(6)$ is not allowed under free operations, where $\mathcal{C}_{1/6}(6) := 1/6\sum_{f=1}^{6} \mathbf{ff} \in \mathfrak{C}(6)$.

Quantum advantage

- $\mathfrak{S}_C(2 \mapsto d)$: the subset of $\mathfrak{C}(d)$ that can be obtained from from $\mathfrak{C}(2)$ under free operations
- $\mathfrak{S}_Q(2 \mapsto d)$: the subset of $\mathfrak{C}(d)$ that can be obtained from from $\mathfrak{Q}(2)$ under free operations

Theorem 1: $\mathfrak{S}_C(2 \mapsto d) \subset \mathfrak{S}_Q(2 \mapsto d)$, for $d > 2$.

Non-monopolizing social subsidy game.– The game $\mathbb{G}(n)$ involves two employees Alice & Bob working in an organization and n there are different restaurants $r_1, \cdots, r_n$ where the employees have their beverages. The organization have a subsidy rule which returns back the beverages bill $\$\mathcal{R}(n) = \$\min_{i\neq j} P(ij)$ to the employees, where $P(ij)$ is the probability of Alice visiting r_i restaurant and Bob r_j restaurant [assuming per day expense $1 for each of the employees].

Since the reimbursement policy encourages total trade to be distributed among all the restaurants we call it 'non-monopolizing subsidy' rule. The employees are non-communicating and possess no pre-shared randomness. However, they may be assisted with some shared coin state (either classical or quantum) along with the local strategies belonging to the set of free operations. Following result bounds their achievable payoff.

Theorem 2: $\frac{1}{n^2} \leq \mathcal{R}(n) \leq \frac{1}{n(n-1)}$.

Theorem 3: Given any coin state from $\mathfrak{C}(2)$ the payoff $\mathcal{R}(n)$ is always suboptimal for $n > 2$.

Theorem 4: The optimum payoff in $\mathcal{R}(n)$ can be obtained from a coin state in $\mathfrak{Q}(2)$, for $n = 3,4$.

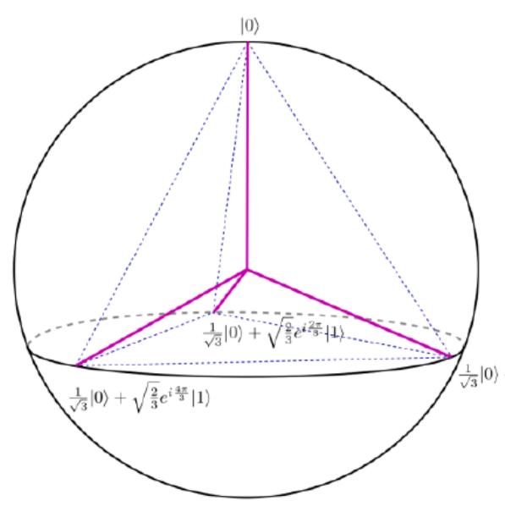
For $n = 3,4$ the $\mathcal{R}(n)$ will be achieved with the following SR:

$$\mathcal{C}^{eq}_{\neq\alpha}(3) = \left(\overset{\overset{11}{\downarrow}}{0}, \overset{\overset{12}{\downarrow}}{1/6}, \overset{\overset{13}{\downarrow}}{1/6}, \overset{\overset{21}{\downarrow}}{1/6}, \overset{\overset{22}{\downarrow}}{0}, \overset{\overset{23}{\downarrow}}{1/6}, \overset{\overset{31}{\downarrow}}{1/6}, \overset{\overset{32}{\downarrow}}{1/6}, \overset{\overset{33}{\downarrow}}{0}\right)^{\mathrm{T}}$$

$$\mathcal{C}^{eq}_{\neq\alpha}(4) = \left(\overset{\overset{11}{\downarrow}}{0}, \overset{\overset{12}{\downarrow}}{1/12}, \overset{\overset{13}{\downarrow}}{1/12}, \overset{\overset{14}{\downarrow}}{1/12}, \overset{\overset{21}{\downarrow}}{1/12}, \overset{\overset{22}{\downarrow}}{0}, \overset{\overset{23}{\downarrow}}{1/12}, \overset{\overset{24}{\downarrow}}{1/12}, \overset{\overset{31}{\downarrow}}{1/12}, \overset{\overset{32}{\downarrow}}{1/12}, \overset{\overset{33}{\downarrow}}{0}, \overset{\overset{34}{\downarrow}}{1/12}, \overset{\overset{41}{\downarrow}}{1/12}, \overset{\overset{42}{\downarrow}}{1/12}, \overset{\overset{43}{\downarrow}}{1/12}, \overset{\overset{44}{\downarrow}}{0}\right)^{\mathrm{T}}$$

Quantum Protocol: Share the state $\mathcal{Q}_{\mathtt{singlet}}(2) := |\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB})$ and perform same TRINE/ SIC measurement.

TRINE POVM


$|0\rangle$
$\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}e^{i\frac{2\pi}{3}}|1\rangle$
$\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}e^{i\frac{4\pi}{3}}|1\rangle$
$\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$

SIC POVM

Perfection should not be the enemy of your achievement

Instead of the perfect two-2-quoin $\mathcal{Q}_{\mathtt{singlet}}(2)$ if they share imperfect $\mathcal{Q}_{\mathrm{p}}(2) := p\,|\psi^-\rangle\langle\psi^-| + (1-p)\frac{\mathbf{I}}{2}\otimes\frac{\mathbf{I}}{2}$, the quantum advantage persists if $p > 1/4$ and $p > 1/5$ for $n = 3$ and $n = 4$, respectively.

Theorem 5: Non-zero discord is necessary for advantage over classical coins in $\mathbb{G}(n)$ game for $n = 3,4$.

SR distribution: Let Alice prepares $\mathcal{Q}_{\mathtt{singlet}}(2)$ and sends one part to Bob through some noisy channel.

Qubit de-phasing channel $\Lambda^z_\beta(\rho) := \beta\rho + (1-\beta)\sigma_z\rho\sigma_z$ is advantageous over the noiseless classical binary channel for $\beta > 3/4$ and $\beta > 7/10$ while playing the games $\mathbb{G}(3)$ and $\mathbb{G}(4)$.

For de-polarizing channel $\Lambda^D_p(\rho) := p\rho + (1-p)\mathbb{I}/2$ the advantage can be obtained for $p > 1/4$ and $p > 1/5$, respectively. Note that, Λ^D_p is an entanglement breaking channel whenever $\beta \leq 1/3$. Therefore a quantum channel can exhibit advantage in SR distribution even when its quantum capacity is zero. Classical capacity of qubit de-polarizing channel is given by $\chi(\Lambda^D_p) = 1 - H\left(\frac{1+p}{2}\right)$. Therefore, the advantage is tangible even when the quantum channel is largely imperfect.

Concluding remarks

- In SR distribution advantages of quantum channels have been shown. Such advantage is quite remarkable when analyzed from the perspective of the no-go results of Holevo and Frenkel-Weiner that put limits on the classical information processing through quantum systems
- The imperfect channel examples facilitate noise robust empirical setup to verify the obtained quantum advantage. The present work thus reckons an important novel element in the list of quantum preeminences.
- Our work also leaves a number of important questions for future research. First of all, the class of monotones, completely characterizing the resource conversion is still missing
- It also serves as a stepping stone towards the rich potentiality of accomplishing quantum advantage in randomness processing for higher dimensional and multipartite scenarios.

"If it were necessary to give the briefest possible definition of imperialism, we should have to say that imperialism is the monopoly stage of capitalism."— **Vladimir Lenin**

Use Quantum Break Monopoly

[arXiv:2001.01889]

manik11ju@gmail.com
manik.banik@iisertvm.ac.in