Quantum Advantage in Shared Randomness Processing

Some Sankar Bhattacharya

Department of Computer Science
The University of Hong Kong

Young Researchers' Forum on Quantum Information 2020
NTHU, Taiwan

Talk based on

arXiv:2001.01889

in Collaboration with Tamal Guha, Mir Alimuddin, Sumit Raut, Amit Mukherjee and Manik Banik.

Shared Randomness (SR)

A source of SR is specified by a bipartite probability distribution

$$P(\mathcal{X}, \mathcal{Y}) \equiv \{p(x, y) \mid x \in \mathcal{X}, y \in \mathcal{Y}\}.$$

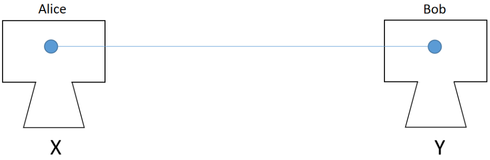
In an operational theory an SR resource between Alice and Bob can be obtained from a shared bipartite system

Shared Randomness (SR)

A source of SR is specified by a bipartite probability distribution

$$P(\mathcal{X},\mathcal{Y}) \equiv \{p(x,y) \mid x \in \mathcal{X}, y \in \mathcal{Y}\}.$$

In an operational theory an SR resource between Alice and Bob can be obtained from a shared bipartite system



by performing local measurement on their respective parts.

Resource Theory of SR

Free resource

$P(\mathcal{X},\mathcal{Y}) = P(\mathcal{X})Q(\mathcal{Y})$

- Let $\mathcal{F}_{SR}$ denotes the set of all free states.
- The set $\mathcal{F}_{SR}$ is not convex.

Resource Theory of SR

Free resource

$P(\mathcal{X},\mathcal{Y}) = P(\mathcal{X})Q(\mathcal{Y})$

- Let $\mathcal{F}_{SR}$ denotes the set of all free states.
- The set $\mathcal{F}_{SR}$ is not convex.

Free operations

$L_A \otimes L_B$

- For classical systems: tensor product of local stochastic matrices $\mathcal{S}_A \otimes \mathcal{S}_B$.
- In quantum scenario: local unitary operations and/or local measurements generally described by a positive operator valued measure (POVM).

Resource Theory of SR

Free resource

$P(\mathcal{X}, \mathcal{Y}) = P(\mathcal{X})Q(\mathcal{Y})$

- Let $\mathcal{F}_{SR}$ denotes the set of all free states.
- The set $\mathcal{F}_{SR}$ is not convex.

Free operations

$L_A \otimes L_B$

- For classical systems: tensor product of local stochastic matrices $\mathcal{S}_A \otimes \mathcal{S}_B$.
- In quantum scenario: local unitary operations and/or local measurements generally described by a positive operator valued measure (POVM).

Resource monotones

$I(P(\mathcal{X}, \mathcal{Y})) := H(\mathcal{X}) + H(\mathcal{Y}) - H(\mathcal{X}, \mathcal{Y})$

- $I(Q(\mathcal{X}', \mathcal{Y}')) \leq I(P(\mathcal{X}, \mathcal{Y}))$ necessary for conversion $P \to Q$.
- But not sufficient.

Classical Two-2-coin

$\mathcal{C}(2) \equiv (p(\mathtt{hh}), p(\mathtt{ht}), p(\mathtt{th}), p(\mathtt{tt}))^\intercal \in \mathfrak{C}(2).$

Example: Classical vs Quantum

Classical Two-2-coin

$\mathcal{C}(2) \equiv (p(\mathtt{hh}), p(\mathtt{ht}), p(\mathtt{th}), p(\mathtt{tt}))^\intercal \in \mathfrak{C}(2)$.

Quantum Two-2-quoin

$\mathcal{Q}(2)$, corresponds to the states of a two-qubit quantum system.
The state space $\mathfrak{Q}(2) \equiv \mathcal{D}(\mathbb{C}^2_A \otimes \mathbb{C}^2_B)$

Example: Classical vs Quantum

Classical Two-2-coin

$\mathcal{C}(2) \equiv (p(\mathtt{hh}), p(\mathtt{ht}), p(\mathtt{th}), p(\mathtt{tt}))^{\intercal} \in \mathfrak{C}(2)$.

Quantum Two-2-quoin

$\mathcal{Q}(2)$, corresponds to the states of a two-qubit quantum system.
The state space $\mathfrak{Q}(2) \equiv \mathcal{D}(\mathbb{C}_A^2 \otimes \mathbb{C}_B^2)$

- From the two-2-quoin states Alice and Bob can prepare any states of $\mathfrak{C}(2)$ by applying local POVMs on their respective parts of the joint system.

Example: Classical vs Quantum

Classical Two-2-coin

$\mathcal{C}(2) \equiv (p(\mathtt{hh}), p(\mathtt{ht}), p(\mathtt{th}), p(\mathtt{tt}))^\intercal \in \mathfrak{C}(2)$.

Quantum Two-2-quoin

$\mathcal{Q}(2)$, corresponds to the states of a two-qubit quantum system.
The state space $\mathfrak{Q}(2) \equiv \mathcal{D}(\mathbb{C}_A^2 \otimes \mathbb{C}_B^2)$

- From the two-2-quoin states Alice and Bob can prepare any states of $\mathfrak{C}(2)$ by applying local POVMs on their respective parts of the joint system.
- $\mathfrak{C}(2)$ can always replace $\mathfrak{Q}(2)$ for generating any binary-outcome distributions.

Example: Classical vs Quantum

Classical Two-2-coin

$\mathcal{C}(2) \equiv (p(\mathtt{hh}), p(\mathtt{ht}), p(\mathtt{th}), p(\mathtt{tt}))^{\intercal} \in \mathfrak{C}(2)$.

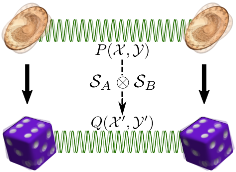
Quantum Two-2-quoin

$\mathcal{Q}(2)$, corresponds to the states of a two-qubit quantum system.
The state space $\mathfrak{Q}(2) \equiv \mathcal{D}(\mathbb{C}^2_A \otimes \mathbb{C}^2_B)$

- From the two-2-quoin states Alice and Bob can prepare any states of $\mathfrak{C}(2)$ by applying local POVMs on their respective parts of the joint system.
- $\mathfrak{C}(2)$ can always replace $\mathfrak{Q}(2)$ for generating any binary-outcome distributions.

Quantum advantage??

Simulating higher outcomes: Towards quantum advantage



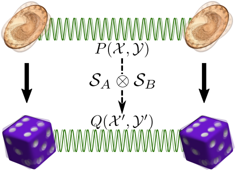
- Classical coins: $\mathfrak{C}(m) \longrightarrow \mathfrak{C}(n)$

$$\Big[\underbrace{S_A^{m\to n}}_{n\times m} \otimes \underbrace{S_B^{m\to n}}_{n\times m}\Big] \times \underbrace{C(m)}_{m^2\times 1} = \underbrace{C'(n)}_{n^2\times 1} \in \mathfrak{S}_C(m\to n)$$

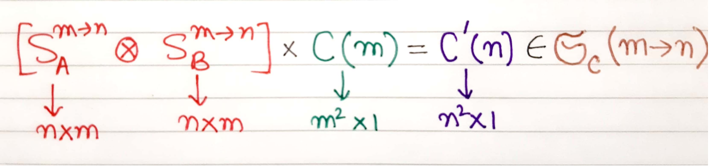
$\mathfrak{S}_C(m \mapsto n) \subset \mathfrak{C}(n)$ that are freely simulable from $\mathfrak{C}(m)$.

- Quoins: Similarly, $\mathfrak{S}_Q(m \mapsto n) \subset \mathfrak{C}(n)$ freely simulable from $\mathfrak{Q}(m)$.

Simulating higher outcomes: Towards quantum advantage



- Classical coins: $\mathfrak{C}(m) \longrightarrow \mathfrak{C}(n)$

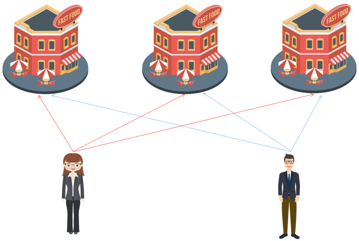


$\mathfrak{S}_C(m \mapsto n) \subset \mathfrak{C}(n)$ that are freely simulable from $\mathfrak{C}(m)$.

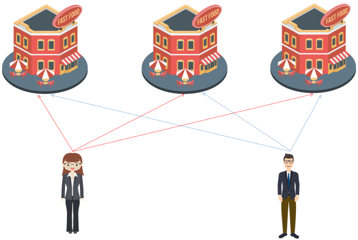
- Quoins: Similarly, $\mathfrak{S}_Q(m \mapsto n) \subset \mathfrak{C}(n)$ freely simulable from $\mathfrak{Q}(m)$.

Our main result: $\mathfrak{S}_C(2 \mapsto d) \subset \mathfrak{S}_Q(2 \mapsto d)$, for $d > 2$

Quantum advantage: Non-monopolizing social subsidy game $\mathbb{G}(3)$

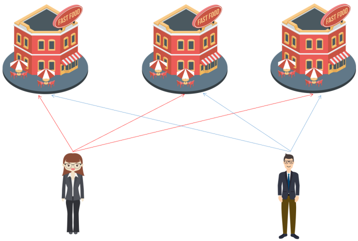


Quantum advantage: Non-monopolizing social subsidy game $\mathbb{G}(3)$



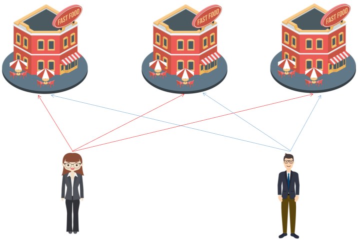
- On every working day each of the employees buys beverage from the restaurant chosen at her/his will.
- Each day's bill is accounted for a long time to calculate the probability $P(\mathbf{ff}')$ of Alice visiting $\mathbf{f}$ restaurant and Bob $\mathbf{f}'$ restaurant.

Quantum advantage: Non-monopolizing social subsidy game $\mathbb{G}(3)$



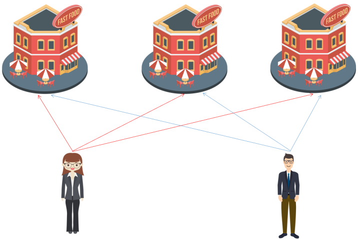
- On every working day each of the employees buys beverage from the restaurant chosen at her/his will.
- Each day's bill is accounted for a long time to calculate the probability $P(\mathbf{ff'})$ of Alice visiting $\mathbf{f}$ restaurant and Bob $\mathbf{f'}$ restaurant.
- Events $(\mathbf{ff'})$ where each employee ends up in different restaurants $(\mathbf{f} \neq \mathbf{f'})$ are considered for reimbursement (payoff). [Different Choice]

Quantum advantage: Non-monopolizing social subsidy game $\mathbb{G}(3)$



- On every working day each of the employees buys beverage from the restaurant chosen at her/his will.
- Each day's bill is accounted for a long time to calculate the probability $P(\mathbf{ff}')$ of Alice visiting $\mathbf{f}$ restaurant and Bob $\mathbf{f}'$ restaurant.
- Events $(\mathbf{ff}')$ where each employee ends up in different restaurants $(\mathbf{f} \neq \mathbf{f}')$ are considered for reimbursement (payoff). [Different Choice]
- The minimum probability of the events where each employee ends up in different restaurants are eligible for reimbursement (payoff). [No Favorites]

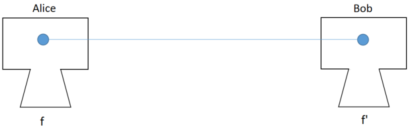
Quantum advantage: Non-monopolizing social subsidy game $\mathbb{G}(3)$



- On every working day each of the employees buys beverage from the restaurant chosen at her/his will.
- Each day's bill is accounted for a long time to calculate the probability $P(\mathbf{ff}')$ of Alice visiting $\mathbf{f}$ restaurant and Bob $\mathbf{f}'$ restaurant.
- Events $(\mathbf{ff}')$ where each employee ends up in different restaurants $(\mathbf{f} \neq \mathbf{f}')$ are considered for reimbursement (payoff). [Different Choice]
- The minimum probability of the events where each employee ends up in different restaurants are eligible for reimbursement (payoff). [No Favorites]
- Assuming per day expense 1 unit for each, the payoff is

$$\mathcal{R}(n) = \min_{\mathbf{f}\neq\mathbf{f}'} p(\mathbf{ff}').$$

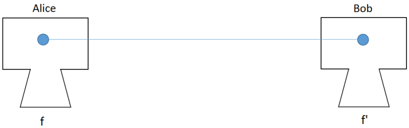
Quantum advantage: Non-monopolizing social subsidy game



Optimal source: 'anti-correlated' two-d-coin state

$\mathcal{C}_{\neq\alpha}(d) := (p|p(\mathbf{ff}) = 0 \ \& \ p(\mathbf{ff}') \neq 0, \ \forall \ \mathbf{f}, \mathbf{f}' \in \{1, \cdots, d\}, \ \& \ \mathbf{f} \neq \mathbf{f}').$

Quantum advantage: Non-monopolizing social subsidy game



Optimal source: 'anti-correlated' two-d-coin state

$\mathcal{C}_{\neq\alpha}(d) := (p|p(\mathbf{ff}) = 0 \ \& \ p(\mathbf{ff}') \neq 0, \ \forall \ \mathbf{f}, \mathbf{f}' \in \{1, \cdots, d\}, \ \& \ \mathbf{f} \neq \mathbf{f}')$.

The maximum achievable payoff in $\mathbb{G}(n)$ is assured if the employees share the particular 'anti-correlated' coin state $\mathcal{C}^{eq}_{\neq\alpha}(n)$, where
$p(\mathbf{ff}') = 1/n(n-1), \ \forall \ \mathbf{f}, \mathbf{f}' \in \{1, \cdots, n\}, \ \& \ \mathbf{f} \neq \mathbf{f}'$.

$$\mathcal{C}(2) \longrightarrow^{?} \mathcal{C}^{eq}_{\neq\alpha}(n)$$
$$\mathcal{Q}(2) \longrightarrow^{?} \mathcal{C}^{eq}_{\neq\alpha}(n)$$

Payoff

$$\mathcal{R}(n) = \min_{\mathbf{f}\neq\mathbf{f}'} p(\mathbf{ff}') \leq \frac{1}{n(n-1)}$$

.

Classical Strategy

Lemma 2: Sub-optimality of classical resource

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

Classical Strategy

Lemma 2: Sub-optimality of classical resource

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

α-correlated states

$\mathcal{C}_\alpha(2) := (\alpha, 0, 0, 1-\alpha)^\intercal \equiv \alpha\ \mathtt{hh} + (1-\alpha)\mathtt{tt};\ \alpha \in [0,1]$

- $\mathcal{C}_\alpha(2)$ can freely simulate any state in $\mathfrak{C}(2)$.
- $\mathcal{C}_\alpha(2)$ can not simulate any $\mathcal{C}_{\neq\alpha}(n)$, for $n > 2$.

Classical Strategy

Lemma 2: Sub-optimality of classical resource

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

α-correlated states

$\mathcal{C}_\alpha(2) := (\alpha, 0, 0, 1-\alpha)^\intercal \equiv \alpha\ \mathtt{hh} + (1-\alpha)\mathtt{tt};\ \alpha \in [0,1]$

- $\mathcal{C}_\alpha(2)$ can freely simulate any state in $\mathfrak{C}(2)$.
- $\mathcal{C}_\alpha(2)$ can not simulate any $\mathcal{C}_{\neq\alpha}(n)$, for $n > 2$.

$$\mathcal{R}_{\max}^{\mathfrak{C}(2)}(3) = 1/8$$

and

$$\mathcal{R}_{\max}^{\mathfrak{C}(2)}(4) = 1/15$$

Quantum advantage

Optimality of Quantum resource

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

Optimal Quantum Strategy

- Let the two-2-quoin state $\mathcal{Q}_{\mathtt{singlet}}(2) := |\psi^-{}_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|01_{AB}\rangle - |10_{AB}\rangle\right)$ is shared between the employees.

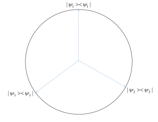
Quantum advantage

Optimality of Quantum resource

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

Optimal Quantum Strategy

- Let the two-2-quoin state $\mathcal{Q}_{\texttt{singlet}}(2) := |\psi^-{}_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|01_{AB}\rangle - |10_{AB}\rangle\right)$ is shared between the employees.
- Both of them perform the same three outcome trine-POVM $\mathcal{M} \equiv \left\{\Pi_k := \frac{2}{3}|\psi_k\rangle\langle\psi_k|\right\}$, where $|\psi_k\rangle := \cos(k-1)\theta_3|0\rangle + \sin(k-1)\theta_3|1\rangle$; $k \in \{1, 2, 3\}$, $\theta_3 = 2\pi/3$.



- This strategy leads to the coin state $\mathcal{C}^{eq}_{\neq\alpha}(3)$ yielding the optimum payoff in $\mathbb{G}(3)$.
- To obtain the optimum payoff in $\mathbb{G}(4)$ consider the qubit SIC-POVM in above protocol instead of the trine-POVM.

Quantum advantage

A necessary condition

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

- Measurement statistics for any local POVMs performed on zero discordant states can be simulated by the local operations on the shared classical $2-$coin states.
- *Non-monopolizing social subsidy* game turns out to be operationally useful for detecting presence of quantum discord.

Quantum advantage: SR distribution through noisy channels

- Instead of having SR resources as assistance let us assume that Alice and Bob share a communication channel (either classical or quantum) for establishing SR aiming to achieve better payoff in $\mathbb{G}(n)$.

Quantum advantage: SR distribution through noisy channels

- Instead of having SR resources as assistance let us assume that Alice and Bob share a communication channel (either classical or quantum) for establishing SR aiming to achieve better payoff in $\mathbb{G}(n)$.
- Optimal classical channel: perfect binary classical channel (unit classical capacity) which gives $\mathcal{R}^{\mathfrak{C}(2)}_{\max}(3) = 1/8$ and $\mathcal{R}^{\mathfrak{C}(2)}_{\max}(4) = 1/15$.

Quantum advantage: SR distribution through noisy channels

- Instead of having SR resources as assistance let us assume that Alice and Bob share a communication channel (either classical or quantum) for establishing SR aiming to achieve better payoff in $\mathbb{G}(n)$.
- Optimal classical channel: perfect binary classical channel (unit classical capacity) which gives $\mathcal{R}^{\mathfrak{C}(2)}_{\max}(3) = 1/8$ and $\mathcal{R}^{\mathfrak{C}(2)}_{\max}(4) = 1/15$.

Quantum advantage

- Noisy quantum channel: qubit de-polarizing channel $\Lambda^{D}_{\beta}(\rho) := \beta\rho + (1-\beta)\mathbb{I}/2$.

Quantum advantage: SR distribution through noisy channels

- Instead of having SR resources as assistance let us assume that Alice and Bob share a communication channel (either classical or quantum) for establishing SR aiming to achieve better payoff in $\mathbb{G}(n)$.
- Optimal classical channel: perfect binary classical channel (unit classical capacity) which gives $\mathcal{R}^{\mathfrak{C}(2)}_{\max}(3) = 1/8$ and $\mathcal{R}^{\mathfrak{C}(2)}_{\max}(4) = 1/15$.

Quantum advantage

- Noisy quantum channel: qubit de-polarizing channel $\Lambda^D_\beta(\rho) := \beta\rho + (1-\beta)\mathbb{I}/2$.
- classical capacity $\chi(\Lambda^D_\beta) = 1 - H\left(\frac{1+\beta}{2}\right)$

Quantum advantage: SR distribution through noisy channels

- Instead of having SR resources as assistance let us assume that Alice and Bob share a communication channel (either classical or quantum) for establishing SR aiming to achieve better payoff in $\mathbb{G}(n)$.
- Optimal classical channel: perfect binary classical channel (unit classical capacity) which gives $\mathcal{R}^{\mathfrak{C}(2)}_{\max}(3) = 1/8$ and $\mathcal{R}^{\mathfrak{C}(2)}_{\max}(4) = 1/15$.

Quantum advantage

- Noisy quantum channel: qubit de-polarizing channel $\Lambda^D_\beta(\rho) := \beta\rho + (1-\beta)\mathbb{I}/2$.
- classical capacity $\chi(\Lambda^D_\beta) = 1 - H\left(\frac{1+\beta}{2}\right)$
- Λ^D_β has zero quantum capacity whenever $\beta \leq 1/3$.

Quantum advantage: SR distribution through noisy channels

- Instead of having SR resources as assistance let us assume that Alice and Bob share a communication channel (either classical or quantum) for establishing SR aiming to achieve better payoff in $\mathbb{G}(n)$.
- Optimal classical channel: perfect binary classical channel (unit classical capacity) which gives $\mathcal{R}^{\mathfrak{C}(2)}_{\max}(3) = 1/8$ and $\mathcal{R}^{\mathfrak{C}(2)}_{\max}(4) = 1/15$.

Quantum advantage

- Noisy quantum channel: qubit de-polarizing channel $\Lambda^D_\beta(\rho) := \beta\rho + (1-\beta)\mathbb{I}/2$.
- classical capacity $\chi(\Lambda^D_\beta) = 1 - H\left(\frac{1+\beta}{2}\right)$
- Λ^D_β has zero quantum capacity whenever $\beta \leq 1/3$.
- Better than classical payoff can be obtained for $\beta > 1/4$ in $\mathbb{G}(3)$ and $\beta > 1/5$ in $\mathbb{G}(4)$, while quantum capacity is zero and classical capacity much less than unity.

Summary

- In this work we establish advantage of quantum sources of shared randomness.
- Quantum discord is necessary for such an advantage.
- The obtained quantum advantage is operationally perceivable as it is demonstrated through a game.
- We also show precedence of quantum channel over its classical counterpart in distributing shared randomness between two distant parties.

Future Directions

- The class of monotones, completely characterizing the (im)possibility of conversion between two shared randomness resources, is still missing.
- Further characterization of quantum resources providing advantage in SR processing and distribution.
- Higher dimensional and multipartite scenarios.