Quantum Advantage for Shared Randomness Generation

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

[1]Physics and Applied Mathematics Unit, Indian Statistical Institute, 203 B.T. Road, Kolkata 700108, India.

[2]School of Physics, IISER Thiruvanathapuram, Vithura, Kerala 695551, India.

[3]International Centre for Theory of Quantum Technologies (ICTQT), University of Gdańsk, 80-308 Gdańsk, Poland.

[4]S.N. Bose National Center for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700098, India.

[5]Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong.

Sharing correlated random variables is a resource for a number of information theoretic tasks such as privacy amplification, simultaneous message passing, secret sharing and many more. In this article, we show that to establish such a resource called shared randomness, quantum systems provide an advantage over their classical counterpart. Precisely, we show that appropriate albeit fixed measurements on a shared two-qubit state can generate correlations which cannot be obtained from any possible state on two classical bits. In a resource theoretic set-up, this feature of quantum systems can be interpreted as an advantage in winning a two players co-operative game, which we call the 'non-monopolize social subsidy' game. It turns out that the quantum states leading to the desired advantage must possess non-classicality in the form of quantum discord. On the other hand, while distributing such sources of shared randomness between two parties via noisy channels, quantum channels with zero capacity as well as with classical capacity strictly less than unity perform more efficiently than the perfect classical channel. Protocols presented here are noise-robust and hence should be realizable with state-of-the-art quantum devices.

1 Introduction

Present day quantum technology is getting increasingly sophisticated with the aim to control individual quantum systems, enabling them in different practical tasks that otherwise are not possible in classical world. This approach already finds several practical applications, such as secure communication [1–4], quantum imaging [5–8], quantum metrology [9–12], and more excitingly promises opportunities for Near-Term Quantum Computing Systems [13–18]. Thus, it is important to explore and identify more and more instances where quantum theory can exhibit advantage over the corresponding classical systems. In this work, we report such a novel quantum advantage. We consider the computational scenario of generating correlated random variables between distant parties, also known as *shared randomness.*

Shared randomness (SR) is known to be an important resource in a number of applications, *viz* privacy amplification [22–24], simultaneous message passing [25], secret sharing and secret key generation protocol [26, 27], classical simulation of quantum nonlocal statistics [28, 30, 51], Bayesian game theory [31–34], and communication complexity [35]. Among spatially separated parties, shared randomness can not be established free of cost. It requires the distant parties to have access to noiseless communication channels, which, in Shannon theory, are considered to be expensive [36]. Alternatively, one can ask whether sharing multipartite quantum systems provide any advantage over the correlated classical systems for shared randomness generation or not. A similar question can also be asked concerning the advantage of using noisy quantum communication channels over classical ones. In this work, we find affirmative answers to both of these questions by identifying new instances where quantum theory yields provable advantage over its classical counterpart. Importantly, the quantum advantage sustains even in presence of noise and hence is achievable with the present day imperfect quantum devices.

To demonstrate the advantage of using quantum sources, we take resort to the language of resource theory. In the recent past, researchers in quantum information community have successfully applied this framework to identify, characterize, and quantify different useful resources [37–48]. Such a framework is operationally motivated. Firstly, it identifies the free states that are *useless* for performing certain tasks and specifies the free operations that are unable to produce any resource from free states and hence are allowed to be implemented at no cost. Given these sets of free states and operations, the framework aims to find the resource conversion conditions (either necessary or sufficient, sometimes both), commonly phrased as monotones, that characterize possible transformations among the resource states under free operations.

In this article, we consider the resource theory of shared randomness. At the outset, it is worth mentioning that our framework is distinct from the well known resource theory of local operations with shared randomness (LOSR) [49, 50]. In the present work, shared randomness is not considered as a free resource, which is the case in the resource theory of LOSR. Here, we aim to quantify the resource for generating shared randomness between distant parties by performing local operations on their subsystems. In that respect, the works of Toner *et al.*[51] and Bowles *et al.*[30] are noteworthy, where it has been shown that nonlocal correlations obtained from a bipartite entangled state can be simulated with shared randomness when assisted with classical communication. While in [51] it requires infinite amount of shared randomness, the authors in [30] propose a simulation of nonlocal states with finite shared randomness and finite communication. The present article establishes the utility of shared randomness even outside the nonlocality paradigm. First, we identify the set of correlations that can be obtained from a shared 2-faced classical coin (henceforth called *two-2-coin*) under the free local operations. Secondly we observe that, within the proposed resource theoretic framework, every two-2-coin state can be freely obtained from its quantum analogue, namely the two-2-quoin which corresponds to a two-qubit quantum system with Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$. Lastly, the quantum advantage is established by a set inclusion relation, which involves identifying two-d-coin states that can be obtained from a two-2-quoin under free operation but cannot be obtained from any two-2-coin state.

We also show that the quantum advantage for generating shared randomness translates to higher success probability of winning a two-player co-operative game, namely the 'non-monopolize social subsidy' game with quantum resource, when compared to that of corresponding classical strategies. More precisely, the players can achieve optimal payoff when assisted with two-2-quoin states, whereas their payoffs remain suboptimal with two-2-coin states. Further, we show that *better than classical* payoff necessitates use of two-2-quoin states with non-zero discord – an intriguing non-classical feature present in bipartite quantum systems even when the states are not entangled [52, 53]. We then consider the scenario where one wishes to establish shared randomness with a distant party. We show that a quantum channel can exhibit advantage over the corresponding classical channels. Such an advantage is quite remarkable, as there exist *no-go* results [60, 61] that limit the utilities of quantum systems as information carrier. Recall that in Shannon theory, efficacy of a classical channel is characterized by its capacity, quantified as the mutual information optimized over probability distributions of the input variables [36]. In quantum scenario, different quantities of interest are used to characterize the utility of a quantum channel. For instance, while quantum capacity of a quantum channel denotes the highest rate of transmitting quantum information [64–66], its classical capacity [62, 63] characterizes utility of transferring classical information. In shared randomness distribution, a quantum channel can show advantage over a classical channel even when its classical capacity is much less than that of the classical channel. At this point, it seems natural to think that such advantage requires the noisy quantum channels to possess non-zero quantum capacity. However, it turns out that the quantum advantage persists even when the quantum channel has zero quantum capacity. Evidently, these instances of noise robust advantage of quantum strategies should be realizable with the state-of-the-art quantum devices.

2 Results

2.1 Resource theory of shared randomness

The framework of resource theory provides a novel approach to quantify the resources of shared randomness. The generic framework of any resource theory characterizes the followings: the class of free states or non-resources, the set of free operations, and resource conversion conditions (either necessary or sufficient, sometimes both) that are commonly phrased as monotones [67].

Free resources

A source of shared randomness 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 as each of the shared variables follows an independent probability distribution and consequently information of one does not provide any knowledge about the other. Unlike the resource theories of quantum entanglement [39] or quantum coherence [46] the set $\mathcal{F}_{SR}$ of free states does not form a convex set in this case.

In an operational theory, shared randomness between Alice and Bob can be obtained from a shared bipartite system by performing local measurement on their respective parts. The state space of such a system, in a convex operational theory, is given by $\Omega_A \otimes \Omega_B$, where Ω_K be the convex compact marginal state space embedded in some real vector space V_K; $K \in \{A,B\}$ [68–70]. For instance, the state space of d-level classical system is the d-simplex embedded in $\mathbb{R}^{d-1}$, whereas for d-level quantum system it is $\mathcal{D}(\mathbb{C}^d) \subset \mathbb{R}^{d^2-1}$; $\mathcal{D}(\mathcal{H})$ denotes the set of density operators acting on the Hilbert space $\mathcal{H}$ associated with the system. While considering the state space for a composite system by taking tensor product of component state space of the subsystems, it is important to note that the choice of tensor product is unique for simplex, which is not the case for other convex sets [71–74].

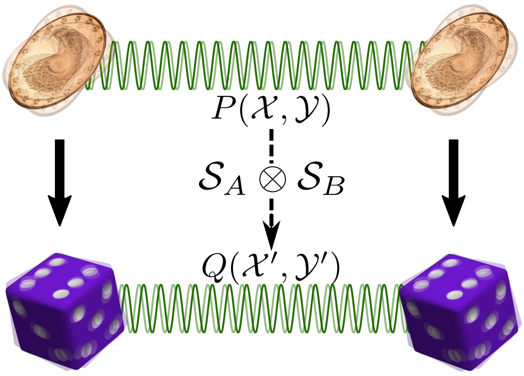
$P(\mathcal{X},\mathcal{Y})$
$\mathcal{S}_A \otimes \mathcal{S}_B$
$Q(\mathcal{X}',\mathcal{Y}')$

Figure 1: [Color on-line] **Resource theory of shared randomness processing.** By performing free operations (local stochastic operations) on two-2-coin states $\mathfrak{C}(2)$ one can obtain only a proper subset $\mathfrak{S}_C(2\mapsto d)$ of two-d-coin state space $\mathfrak{C}(d)$. Such a transformation can never increase classical mutual information of the coin state. For instance, the transformation $\mathcal{C}_{1/2}(2)\mapsto\mathcal{C}_{1/6}(6)$ is not allowed under free operations, where $\mathcal{C}_{1/6}(6):=1/6\sum_{f=1}^{6}\mathbf{ff}\in\mathfrak{C}(6)$.

Free operations

The set of free operations for SR consists of all possible local product operations $L_A\otimes L_B$ applied by Alice and Bob on their respective parts of the joint system. 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. Note that cardinality of $\mathcal{X}$ and $\mathcal{X}'$ can be different in general (see Fig.1). In the quantum scenario, the allowed operations are local unitary operations and/or local measurements generally described by a positive operator valued measure (POVM) [75]. At this point, a comparison with the resource theory of quantum entanglement is worth mentioning. In entanglement theory classical communication is considered as free, but it bears a cost in the present scenario as it can create a non-product joint distribution, *i.e.*, a resourceful state, starting from a product one. In any operational theory, if Alice and Bob initially share a joint state $\omega_{AB}\in\Omega_A\otimes\Omega_B$ of the product from, *i.e.*, $\omega_{AB}=\omega_A\otimes\omega_B$, then a free operation on it can never result in an SR resource between them.

Resource monotone

A necessary condition of state conversion from a distribution $P(\mathcal{X},\mathcal{Y})$ to another $Q(\mathcal{X}',\mathcal{Y}')$ is given by $I(Q)\le I(P)$, 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, $H(\mathcal{X}):=-\sum_{x\in\mathcal{X}}p(x)\log_2 p(x)$. Importantly, mutual information is a faithful resource quantifier, as it takes zero value for every free state while non-zero for all the resourceful states. In the subsequent section, however, we will see that it can not sufficiently characterize the possible resource conversions.

Two-2-coin state space

Consider that Alice and Bob share a pair of 2-faced classical coins (two-2-coin), *i.e.*, $\mathcal{X}\equiv\{\text{head}(\mathtt{h}),\ \text{tail}(\mathtt{t})\}\equiv\mathcal{Y}$. A generic state of this system is described by a column vector $\mathcal{C}(2)\equiv(p(\mathtt{hh}),p(\mathtt{ht}),p(\mathtt{th}),p(\mathtt{tt}))^\intercal\in\mathfrak{C}(2)$; with $\mathfrak{C}(2)$ denoting the set of all two-2-coin states. A state $\mathcal{C}(2)\equiv(x,y,z,1-x-y-z)^\intercal$ is isomorphic to the vector $\mathcal{V}\equiv(x,y,z)^\intercal\in\mathbb{R}^3$

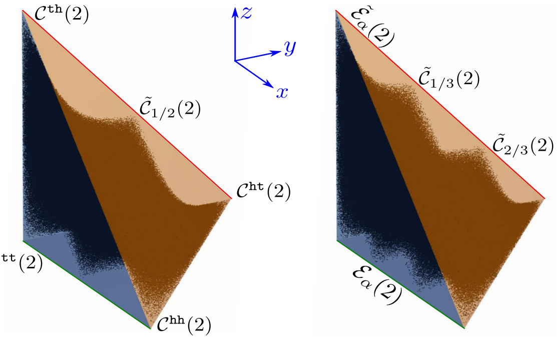

Figure 2: [Color on-line] **Two-2-coin state space $\mathfrak{C}(2)$.** All the four vertices are the free states. Green (red) line denotes the α-correlated (α-anti-correlated) edges. The remaining four edges consist of free states only. Dots in the left [right] figure denote the states obtained from $\mathcal{C}_{1/2}(2)$ [$\mathcal{C}_{1/3}(2)$] by applying randomly generated local stochastic maps. Action of such maps on α-correlated (or α-anti-correlated) edge generate the whole state space $\mathfrak{C}(2)$ (see Lemma 1).

with $x, y, z \geq 0$ & $x + y + z \leq 1$, forming a convex subset $\mathbf{T}$ in the positive octant (see Fig.2). All the four vertices (0-faces) $\mathcal{C}^{\mathtt{hh}}(2)$, $\mathcal{C}^{\mathtt{ht}}(2)$, $\mathcal{C}^{\mathtt{th}}(2)$, and $\mathcal{C}^{\mathtt{tt}}(2)$ are free states. We call the states $\mathcal{C}_{\alpha}(2) := (\alpha, 0, 0, 1-\alpha)^{\intercal} \equiv \alpha\ \mathtt{hh} + (1-\alpha)\mathtt{tt}$ as α-correlated. Whenever $\alpha \notin \{0,1\}$, $\mathcal{C}_{\alpha}(2)$ contains shared randomness even though they are obtained by convex mixing of two free states, hence implies non-convexity of $\mathcal{F}_{SR}$. The α-correlated states live in one of the edges (1-faces) of $\mathbf{T}$ and we call it α-correlated edge, which will be denoted as $\mathcal{E}_{[\alpha]}(2) := \{\mathcal{C}_{\alpha}(2);\ \alpha \in [0,1]\}$. Under free operations, this edge can be transferred into the α-anti-correlated edge $\tilde{\mathcal{E}}_{[\alpha]}(2) \equiv \{\tilde{\mathcal{C}}_{\alpha}(2) := \alpha\ \mathtt{ht} + (1-\alpha)\mathtt{th};\ \alpha \in [0,1]\}$. In fact, every $\mathcal{C}_{\alpha}(2)$ is connected to the corresponding $\tilde{\mathcal{C}}_{\alpha}(2)$ by local permutation, a free operation that keeps the mutual information invariant. The remaining four edges of $\mathbf{T}$ contain only free states. Except these states, no other state residing on any of the four 2-faces of $\mathbf{T}$ is free. However, the volume (3-face) of $\mathbf{T}$ contains both free and resource states.

Consider a state $\mathcal{C}_{\Delta}(2) := (1/3, 0, 1/3, 1/3)^{\intercal}$ residing on one of the 2-faces of $\mathbf{T}$. The state $\mathcal{C}_{\Delta}(2)$ can be obtained from $\mathcal{C}_{1/2}(2)$ under free operation. The two possible free operations allowing this transformation are given by,

$$\left\{ \begin{pmatrix} 0 & 2/3 \\ 1 & 1/3 \end{pmatrix} \otimes \begin{pmatrix} 1/3 & 1 \\ 2/3 & 0 \end{pmatrix};\ \begin{pmatrix} 2/3 & 0 \\ 1/3 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1/3 \\ 0 & 2/3 \end{pmatrix} \right\}.$$

The reverse transformation $\mathcal{C}_{\Delta}(2) \mapsto \mathcal{C}_{1/2}(2)$ is not possible under free operations as the former has lesser mutual information than the latter. Importantly, such a transformation may not be possible even if the initial state has more mutual information than the targeted one. For instance, none of the states $\mathcal{C}_{\alpha}(2)$ can be obtained from $\mathcal{C}_{1/2}(2)$ whenever $\alpha \notin \{0, 1/2, 1\}$, though $I(\mathcal{C}_{1/2}(2)) \geq I(\mathcal{C}_{\alpha}(2))$, with strict inequality holding for $\alpha \in [0, 1/2) \cup (1/2, 1]$. It establishes insufficiency of mutual information in characterizing the possible state conversions. It furthermore proves non-convexity of the set of states obtained from a given resource under the free operations.

2.2 Quantum advantage

In this section we will present our main result which establishes quantum advantage in shared randomness processing. To this aim, we first introduce a quantum analogue of the two-2-coin.

2.2.1 Two-2-quoin state space

The quantum analogue of two-2-coin state, which we call two-2-quoin and denoted as $\mathcal{Q}(2)$, corresponds to the states of a two-qubit quantum system. The state space is given by $\mathfrak{Q}(2) \equiv \mathcal{D}(\mathbb{C}_A^2 \otimes \mathbb{C}_B^2)$, where subsystems A and B are held by Alice and Bob, respectively. From the two-2-quoin states, Alice and Bob can prepare any state of $\mathfrak{C}(2)$ by applying local POVMs on their respective parts of the joint system. Therefore, the former can always replace the latter for any shared randomness processing task. From these shared classical and quantum 2-level coins, one can obtain shared d-level classical coin states by performing suitable stochastic operations and measurements, respectively. The following proposition establishes quantum advantage in generating shared randomness with higher outcomes.

Proposition 1. *Let $\mathfrak{S}_C(2 \mapsto d)$ denote the set of two-d-coin states in $\mathfrak{C}(d)$ that are freely simulable (i.e., can be obtained under allowed free operations) with states from $\mathfrak{C}(2)$. Similarly, $\mathfrak{S}_Q(2 \mapsto d)$ denotes the subset of $\mathfrak{C}(d)$ freely simulable from states in $\mathfrak{Q}(2)$. It holds that $\mathfrak{S}_C(2 \mapsto d) \subset \mathfrak{S}_Q(2 \mapsto d)$, for $d > 2$.*

Sketch of the proof. First we observe that both the sets $\mathfrak{S}_C(2 \mapsto d)$ and $\mathfrak{S}_Q(2 \mapsto d)$ are non-convex, and for any state $\mathcal{C}(2 \mapsto d) \in \mathfrak{S}_J(2 \mapsto d)$, with $J \in \{C, Q\}$, we have $I(\mathcal{C}(2 \mapsto d)) \leq 1$. Then we argue that $\forall\ \mathcal{C}(2 \mapsto d) \in \mathfrak{S}_C(2 \mapsto d)$, it also lies in $\mathfrak{S}_Q(2 \mapsto d)$. Note that a $2-$coin state $\mathcal{C}(2) \equiv (p, q, r, 1-p-q-r)^\intercal$ can be obtained from a two-qubit state, $\rho_{AB} = p\,|00\rangle\langle 00| + q\,|01\rangle\langle 01| + r\,|10\rangle\langle 10| + (1-p-q-r)\,|11\rangle\langle 11|$ by performing local measurement in computational basis. Furthermore, corresponding to every $2 \times d$ stochastic matrix, applied locally on $\mathcal{C}(2)$ there is a $d-$outcome POVM acting locally on the part of ρ_{AB}, which implies that $\mathfrak{S}_C(2 \mapsto d) \subseteq \mathfrak{S}_Q(2 \mapsto d)$. Proof of the strict set inclusion relation is deferred till the end of Theorem 1 and Theorem 2 (see Remark 1). Rather, we now show that the strict set inclusion can be rendered as quantum advantage in a practical two-player game.

2.2.2 Non-monopolizing social subsidy game

The game $\mathbb{G}(n)$ involves two employees Alice & Bob working in an organization and n different restaurants $r_1, \cdots, r_n$. On every working day, each of the employees buys beverage from the restaurant chosen at her/his will. The organization has a reimbursement policy to pay back the beverage bill. For this purpose, each day's bill is accounted for a long time to calculate the probability $P(ij)$ of Alice visiting r_i restaurant and Bob r_j restaurant. Events (ij) where each employee ends up in different restaurants $(i \neq j)$ are considered for reimbursement / payoff[1]. Now it may be the case that the employees pick their favorite restaurants which happen to be different and become regular visitors. But this will leave the other restaurants out of business. To circumvent this situation a sub-clause is added to the subsidy rule which says that the payoff will be defined as $\$\mathcal{R}(n) = \$\min_{i \neq j} P(ij)$, maximizing over all possible strategies with a source of shared randomness with fixed local level, allowed by any physical theory. We further assume that the per day expense for each of the employees is \$1. 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 a bipartite state with subsystems described by two-level systems, independent of the number of restaurants. They can choose local strategies from the set of free operations. Following result bounds their achievable payoff.

[1] This condition mimics the physical distancing norm which people need to follow during the unfortunate pandemic of COVID-19.

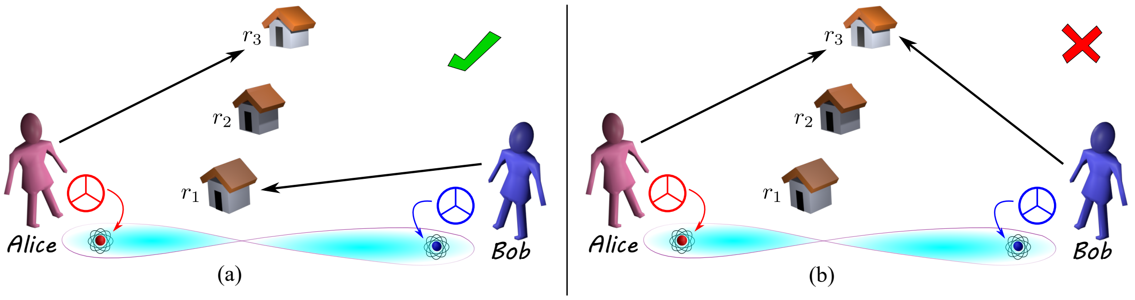

Figure 3: [Color on-line] **Non-monopolizing social subsidy game.** The choice of restaurants, as in figure (a), is permissible by the organization to obtain a subsidy on the beverage costs of the employees, while the situation depicted in figure (b) will not be entertained. Although a two-2-coin state is unable to accomplish all possible combinations similar to (a), a shared two-2-quoin can do so.

Proposition 2. *The maximum payoff achieved in the game $\mathbb{G}(n)$ by two spatially separated employees is bounded from above and below by the following expression-*

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

.

Proof. The lower bound is achieved, on an average, when a uniformly randomized local strategy is followed by each of the employees. For maximal payoff, there are $n(n-1)$ different cases where the employees' bills get reimbursed. Since minimum probability of these events will be considered for reimbursement, the optimal payoff will be achieved if they choose these cases with equal probability, *i.e.*, with probability $\frac{1}{n(n-1)}$. Note that the payoff of the employees will be zero if both the employees decide to go to the same restaurant every day. Thus, the lower bound in the above proposition assumes rational employees who want to maximize their payoff. ■

At this point, we define a specific kind of bipartite shared randomness, namely *not-α-correlated* coin, which in a special case saturates the upper bound of the payoff in the $\mathbb{G}(n)$ game.

Definition 1. *A two-d-coin state is said to be 'not-α-correlated' if $p(\mathbf{ff}) = 0$ and $p(\mathbf{ff}') \neq 0$, $\forall\ \mathbf{f}, \mathbf{f}' \in \{1, \cdots, d\}$, and $\mathbf{f} \neq \mathbf{f}'$.*

In the rest of the manuscript, we will depict them as $\mathcal{C}_{\neq\alpha}(d) \in \mathfrak{C}(d)$. The maximum achievable payoff in $\mathbb{G}(n)$ is assured if the employees share a particular not-α-correlated coin state $\mathcal{C}^{eq}_{\neq\alpha}(n)$, where $p(\mathbf{ff}') = 1/n(n-1)$, $\forall\ \mathbf{f}, \mathbf{f}' \in \{1, \cdots, n\}$, & $\mathbf{f} \neq \mathbf{f}'$. What follow next are the two Lemmas regarding simulability of different sets of classical coin states using free operations.

Lemma 1. *Under the action of free operations, any coin state of $\mathfrak{C}(2)$ can be obtained from the α-correlated edge $\mathcal{E}_{[\alpha]}(2)$, i.e., $\mathcal{E}_{[\alpha]}(2)$ freely simulates the state space $\mathfrak{C}(2)$.*

Proof. A state $\mathcal{C}(2) \in \mathfrak{C}(2)$ can most generally be expressed as,

$$\begin{aligned} \mathcal{C}(2) &= (x, y, z, 1-x-y-z)^{\intercal}, \\ 0 \leq x \leq 1; \quad & 0 \leq y \leq 1-x; \quad 0 \leq z \leq 1-x-y. \end{aligned} \tag{1}$$

The range of y is determined by the value of x, *i.e.*, $\forall\ x \in [0,1]$ the value of y lies within $[0, 1-x]$. Similarly, the range of z is specified by x and y. Even though the variables specify each other's range, their values are mutually random, *i.e.*, the variables fix the range of each other but not the exact value. We wish to show that by applying local stochastic operations on $\mathcal{C}_\alpha(2) \in \mathcal{E}_{[\alpha]}(2)$ Alice and Bob can prepare any vector of the form of Eq.(1). We therefore can write

$$\begin{aligned}
\mathcal{K} &:= \mathcal{S}_A^{2\mapsto 2} \otimes \mathcal{S}_B^{2\mapsto 2} \ \times \ \mathcal{C}_\alpha(2) \\
&= \begin{pmatrix} a_1 & 1-a_1 \\ a_2 & 1-a_2 \end{pmatrix}^{\mathsf{T}} \otimes \begin{pmatrix} b_1 & 1-b_1 \\ b_2 & 1-b_2 \end{pmatrix}^{\mathsf{T}} \times \begin{pmatrix} \alpha \\ 0 \\ 0 \\ 1-\alpha \end{pmatrix} \\
&= \begin{pmatrix} a_1 b_1 \alpha + a_2 b_2 (1-\alpha) \ \ [:= k_1] \\ a_1\alpha + a_2(1-\alpha) - k_1 \ [:= k_2] \\ b_1\alpha + b_2(1-\alpha) - k_1 \ \ [:= k_3] \\ 1 - \sum_{i=1}^{3} k_i \end{pmatrix} = \begin{pmatrix} k_1 \\ k_2 \\ k_3 \\ 1 - \sum k_i \end{pmatrix},
\end{aligned}$$

where $a_1, a_2, b_1, b_2 \in [0,1]$. Since action of a local stochastic matrix $\mathcal{S}_A \otimes \mathcal{S}_B$ on $\mathcal{C}_\alpha(2)$ always result in a probability vector, therefore constraints as of Eq.(1) among k_1, k_2, and k_3 are always satisfied. Now, for every fixed values of $a_2, b_2 \in [0,1]$, $\exists\ \alpha, a_1, b_1 \in [0,1]$ s.t. k_1 can take all values in $[0,1]$. Since the values of a_2 and b_2 can be chosen randomly, they are independent of each other and also k_1 is independent of them. Consequently, k_2 and k_3 are independent of k_1 and also of each other. This completes the proof. ■

Lemma 2. *None of the coin states $\mathcal{C}_{\neq\alpha}(n)$ are freely simulable from $\mathcal{E}_{[\alpha]}(2)$, whenever $n > 2$.*

Proof. A generic stochastic operation $\mathcal{S}^{2\mapsto n}$ mapping a two-level probability vector into an n level probability vector is of the form

$$\begin{pmatrix} u_{11} & u_{21} & \cdots & 1 - \sum_{i=1}^{n-1} u_{i1} \\ u_{12} & u_{22} & \cdots & 1 - \sum_{i=1}^{n-1} u_{i2} \end{pmatrix}^{\mathsf{T}},$$

where $u_{ij} \in [0,1]$ and $\sum_{i=1}^{n-1} u_{ij} \leq 1$. Action of local operations by Alice and Bob on their respective parts of the coin state $\mathcal{C}_\alpha(2)$ yield a two-n-coin state,

$$\begin{aligned}
\mathcal{C}(n) \ &= \ \mathcal{S}_A^{2\mapsto n} \otimes \mathcal{S}_B^{2\mapsto n} \ \times \ \mathcal{C}_\alpha(2) \\
&= \begin{pmatrix} a_{11} & a_{21} & \cdots & 1 - \sum_{i=1}^{n-1} a_{i1} \\ a_{12} & a_{22} & \cdots & 1 - \sum_{i=1}^{n-1} a_{i2} \end{pmatrix}^{\mathsf{T}} \otimes \\
&\quad \begin{pmatrix} b_{11} & b_{21} & \cdots & 1 - \sum_{i=1}^{n-1} b_{i1} \\ b_{12} & b_{22} & \cdots & 1 - \sum_{i=1}^{n-1} b_{i2} \end{pmatrix}^{\mathsf{T}} \times \begin{pmatrix} \alpha \\ 0 \\ 0 \\ 1-\alpha \end{pmatrix}.
\end{aligned}$$

Whenever $\alpha \in \{0,1\}$, the initial state is free and hence the final one. To get the final state as $\mathcal{C}_{\neq\alpha}(n)$ (see Definition1), we require $\alpha a_{i1} b_{i1} + (1-\alpha) a_{i2} b_{i2} = 0,\ \forall\ i \in \{1, ..., n\}$. Since $\alpha \in (0,1)$, therefore $a_{ij} b_{ij} = 0,\ \forall\ i \in \{1, ..., n\}\ \&\ \forall\ j \in \{1,2\}$. Presence of anti-correlated terms in $\mathcal{C}_{\neq\alpha}(n)$ demands, $\alpha a_{i1} b_{k1} + (1-\alpha) a_{i2} b_{k2} \neq 0,\ \forall\ i,k \in \{1, ..., n\}\ \&\ i \neq k$. Therefore, for every $(i, k \neq i)$ pair $\exists$ at-least one $j \in \{1,2\}$ s.t. $a_{ij} b_{kj} \neq 0 \implies a_{ij} \neq 0$ and $b_{kj} \neq 0$. Similarly, for the corresponding reverse pair, $(k, i \neq k)$ $\exists$ at-least one $j' \in \{1,2\}$ s.t. $a_{kj'} b_{ij'} \neq 0 \implies a_{kj'} \neq 0$ and $b_{ij'} \neq 0$. Now j and j' should be different, otherwise a correlated term of the resulting coin state will become non-vanishing. Since $j, j' \in \{1,2\}$, the requirement $j \neq j'$ can not be satisfied whenever $i, k \in \{1, ..., n\}$, with $n > 2$. This completes the proof. ■

These two Lemmas lead us to the following result, describing the limitation of the shared classical coins in achieving the maximum payoff in the game $\mathbb{G}(n)$.

Theorem 1. *Given any coin state from $\mathfrak{C}(2)$, the payoff $\mathcal{R}(n)$ is always suboptimal for all $n > 2$.*

Proof. Contrary to the hypothesis, let us assume that there exist a two-2-coin state $\mathcal{C}^n_{win}(2)$ that provides perfect success in $\mathbb{G}(n)$. Since perfect success of $\mathbb{G}(n)$ requires the two-n-coin state $\mathcal{C}^{eq}_{\neq\alpha}(n)$, this implies that $\mathcal{C}^{eq}_{\neq\alpha}(n)$ can be obtained from $\mathcal{C}^n_{win}(2)$ under free operation. Invoking Lemma 1 we can say that the state $\mathcal{C}^{eq}_{\neq\alpha}$ can be obtained freely from $\mathcal{E}_{[\alpha]}(2)$. This, however, contradicts Lemma 2. ■

At this point one can ask for maximum payoff $\mathcal{R}^{\mathfrak{C}(m)}_{\max}(n)$ that can be achieved in $\mathbb{G}(n)$ given an assistance from $\mathfrak{C}(m)$. This turns out to be an optimization problem. Given a two-m-coin, $\mathcal{C}(m) \equiv (p(\mathbf{11}), \cdots, p(\mathbf{1m}), \cdots, p(\mathbf{mm}))^{\intercal}$ Alice and Bob can obtain some two-n-coin states $\mathcal{C}(n) \equiv (q(\mathbf{11}), \cdots, q(\mathbf{1n}), \cdots, q(\mathbf{nn}))^{\intercal}$ by applying local stochastic maps (free operation), *i.e.*, $\mathcal{C}(n) = \mathcal{S}_A^{m\mapsto n} \otimes \mathcal{S}_B^{m\mapsto n} \cdot \mathcal{C}(m)$. We therefore have

$$\begin{aligned}
\mathcal{R}^{\mathfrak{C}(m)}_{\max}(n) \quad = \quad & \underset{\substack{\mathcal{C}(m)\in\mathfrak{C}(m)\\ \mathcal{S}_A^{m\mapsto n}\otimes\mathcal{S}_B^{m\mapsto n}}}{\text{maximize}} \; q(\mathbf{i} \neq \mathbf{j}) \\
& \text{subject to} \;\; q(\mathbf{i} \neq \mathbf{j}) \leq \;\; q(\mathbf{i}' \neq \mathbf{j}') \\
& \mathbf{i} \neq \mathbf{i}' \text{ and/or } \mathbf{j} \neq \mathbf{j}'.
\end{aligned} \tag{2}$$

Here $\mathcal{S}^{m\mapsto n}_{A/B}$ is a stochastic map mapping m-level probability vectors into n-level ones. While calculating $\mathcal{R}^{\mathfrak{C}(m)}_{\max}(n)$, for $m = 2$, Lemma 1 allows us to restrict the optimization over the edge $\mathcal{E}_{[\alpha]}(2)$, instead of the full two-2-coin state space $\mathfrak{C}(2)$. In Table 1 we list maximum payoffs for a few cases. There we also provide the optimal coin states of $\mathfrak{C}(m)$ and the applied free operations on it that maximize $\mathcal{R}^{\mathfrak{C}(m)}_{\max}(n)$. Our next result establishes quantum advantage of shared randomness generation in non-monopolize social subsidy game.

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

Proof. Let the two-2-quoin state $\mathcal{Q}_{\texttt{singlet}}(2) := |\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB})$ is shared between the players. Both of them perform the same three outcome Trine-POVM $\mathcal{M}^{\mathrm{T}} \equiv \left\{\Pi_k := \frac{2}{3}|\psi_k\rangle\langle\psi_k|\right\}$, 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 $\mathbb{G}(4)$, they consider the SIC-measurement $\mathcal{M}^{\mathrm{S}} \equiv \{\frac{1}{2}|0\rangle\langle 0|, \frac{1}{2}|\psi_k\rangle\langle\psi_k| \mid k = 0, 1, 2\}$, where $|\psi_k\rangle = \sqrt{\frac{1}{3}}|0\rangle + e^{i\frac{2k\pi}{3}}\sqrt{\frac{2}{3}}|1\rangle$. This leads to the coin state $\mathcal{C}^{eq}_{\neq\alpha}(4)$, resulting in the optimum payoff in $\mathbb{G}(4)$. This completes the proof. ■

Remark 1. *Theorem 1 and Theorem 2 together provide a proof for the second part of the Proposition 1 for $d = 3, 4$. According to Theorem 1, $\mathcal{C}^{eq}_{\neq\alpha}(d) \notin \mathfrak{S}_C(2 \mapsto d)$ whenever $d > 2$. In fact, from Lemma 2 we can say that $\mathcal{C}_{\neq\alpha}(d) \notin \mathfrak{S}_C(2 \mapsto d)$. On the other hand, Theorem 2 tells that $\mathcal{C}^{eq}_{\neq\alpha}(d) \in \mathfrak{S}_Q(2 \mapsto d)$ for $d = 3, 4$ and hence proves the second part of the Proposition 1. For higher values of d, consider the two-2-quoin state $\mathcal{Q}_{\texttt{singlet}}(2)$ and consider the same d outcome POVM $\mathcal{M}^{(d)} \equiv \left\{\Pi_k := \frac{2}{d}|\psi_k\rangle\langle\psi_k|\right\}$ for Alice and Bob, where $|\psi_k\rangle := \cos(k-1)\theta_d|0\rangle + \sin(k-1)\theta_d|1\rangle$; $k \in \{1, \cdots, d\}$ and $\theta_d = 2\pi/d$. This leads to a state $\mathcal{C}_{\neq\alpha}(d)$ and completes the proof of Proposition 1 for arbitrary $d > 2$.*

Table 1: Maximum payoff in $\mathbb{G}(n)$ given a coin state from $\mathfrak{C}(m)$. Coin states $\mathcal{C}(m)$ and the free operations $\mathcal{S}_A^{m\mapsto n} \otimes \mathcal{S}_B^{m\mapsto n}$ yielding maximum success $\mathcal{R}_{\max}^{\mathfrak{C}(m)}(n)$ are not unique in general. $\mathcal{R}^{\max}(n)$ is the maximum payoff of the game $\mathbb{G}(n)$ achievable if there is no limitation on the amount of shared randomness.

$\mathcal{R}_{\max}^{\mathfrak{C}(m)}(n)$	$\mathcal{C}(m)$	$\mathcal{S}_A^{m\mapsto n}$	$\mathcal{S}_B^{m\mapsto n}$	$\mathcal{R}^{\max}(n)$
$\mathcal{R}_{\max}^{\mathfrak{C}(2)}(3) = \frac{1}{8}$	$\mathcal{C}_{1/2}(2)$	$\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$	$\frac{1}{6}$
$\mathcal{R}_{\max}^{\mathfrak{C}(2)}(4) = \frac{1}{15}$	$\mathcal{C}_{1/2}(2)$	$\begin{pmatrix} \frac{1}{5} & \frac{1}{3} \\ \frac{1}{5} & \frac{1}{3} \\ \frac{2}{5} & 0 \\ \frac{1}{5} & \frac{1}{3} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{3} & \frac{1}{5} \\ \frac{1}{3} & \frac{1}{5} \\ 0 & \frac{2}{5} \\ \frac{1}{3} & \frac{1}{5} \end{pmatrix}$	$\frac{1}{12}$
$\mathcal{R}_{\max}^{\mathfrak{C}(3)}(4) = \frac{2}{27}$	$\mathcal{C}_{\neq\alpha}^{eq}(3)$	$\begin{pmatrix} 0 & \frac{2}{3} & 0 \\ 0 & 0 & \frac{2}{3} \\ \frac{2}{3} & 0 & 0 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$	$\begin{pmatrix} 0 & \frac{2}{3} & 0 \\ 0 & 0 & \frac{2}{3} \\ \frac{2}{3} & 0 & 0 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$	$\frac{1}{12}$

Note that for higher d values the state $\mathcal{C}_{\neq\alpha}^{eq}(d)$ can not be obtained from $\mathcal{Q}_{\texttt{singlet}}(2)$ and hence perfect payoff in $\mathbb{G}(d)$ can not be obtained even when a coin state from $\mathfrak{Q}(2)$ is given as an assistance. Optimal classical vs quantum payoff(s) for the generic case $\mathbb{G}(d)$, we leave here as an open question.

2.3 Noise-robust quantum advantage

The quantum advantage established above considers a two-qubit perfect entangled state. However, entanglement is extremely fragile under noise and hence the advantage obtained with such a perfect state seems impossible to archive in a practical scenario. Thus, a more realistic question is whether the advantage manifested by quantum systems is robust to noise or not. To this aim, let us consider a noisy two-2-quoin $\mathcal{Q}_p(2) := p|\psi^-\rangle_{AB}\langle\psi^-| + (1-p)\frac{\mathbb{I}}{2} \otimes \frac{\mathbb{I}}{2}$ (i.e., a mixture of the singlet state and white noise)[2]. Note that $\mathcal{R}_{\max}^{\mathfrak{C}(2)}(3) = 1/8$ and $\mathcal{R}_{\max}^{\mathfrak{C}(2)}(4) = 1/15$ (see Table 1). Any quantum strategy providing a greater payoff can be considered advantageous over the classical resources. With the two-2-quoin state $\mathcal{Q}_p(2)$, if we follow the same strategy as discussed in Theorem 2, they can be used to demonstrate advantage over the classical strategies for $p > 1/4$ and $p > 1/5$ in the games $\mathbb{G}(3)$ and $\mathbb{G}(4)$. At this point, it is noteworthy that the state $\mathcal{Q}_p(2)$ is not even entangled whenever $p \leq 1/3$. This raises another fundamentally important question: which quantum feature does underpin the aforementioned advantage in shared randomness generation? Next, we make an attempt to provide a partial answer to this question. Recall that, a bipartite state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is called classically correlated (CC) if it has a diagonal representation in some orthogonal product basis, *i.e.* $\rho_{AB} = \sum_{a,b} p_{ab}|a\rangle_A\langle a| \otimes |b\rangle_B\langle b|$, where $\{|a\rangle_A\}$ is an

[2] Here we deal with a subclass ($p \in [0,1]$) of Werner states, for which $-\frac{1}{3} \leq p \leq 1$

orthogonal basis for $\mathcal{H}_A$ & $\{|b\rangle_B\}$ for $\mathcal{H}_B$ and $p_{ab} \geq 0$, & $\sum_{ab} p_{ab} = 1$. These states do *not* possess quantum discord – a non-classical feature present in the correlation of bipartite quantum states [52, 53]. Besides the entangled, all the separable states, which are not CC, exhibit non-zero quantum discord. For instance, the two-2-quoin $\mathcal{Q}_p(2)$ has non-zero quantum discord for $p \in (0, 1]$, whereas it is separable whenever $p \leq 1/3$.

Theorem 3. *Classically correlated bipartite quantum states will not provide any advantage in shared randomness generation.*

Proof. Without loss of any generality, we can consider the computational basis and hence can represent a two-qubit CC state as $\rho_{AB} = \sum_{u,v} p_{uv}\ |uv\rangle_{AB}\langle uv|;\ u,v \in \{0,1\},\ p_{uv} \geq 0$ & $\sum_{u,v} p_{uv} = 1$. To obtain a two-d-coin state $\mathcal{C}(d)$, Alice and Bob perform some d-outcome POVMs $\{\mathcal{M}_i^A | \sum_{i=1}^d \mathcal{M}_i^A = \mathbb{I}\}$ and $\{\mathcal{M}_i^B | \sum_{i=1}^d \mathcal{M}_i^B = \mathbb{I}\}$ on their respective subsystems. Probability of clicking the POVM elements $\mathcal{M}_i^A \otimes \mathcal{M}_j^B$ on the state ρ_{AB} is given by,

$$p(ij) \quad = \quad \sum_{u,v=0}^{1} p_{uv}\ \langle u|\mathcal{M}_i^A|u\rangle\langle v|\mathcal{M}_j^B|v\rangle. \tag{3}$$

Obviously, $\langle\psi|\mathcal{M}_i^X|\psi\rangle \geq 0$, & $\sum_{i=1}^d \langle\psi|\mathcal{M}_i^X|\psi\rangle = 1,\ \forall\ |\psi\rangle;\ X \in \{A, B\}$. This fact leads us to construct stochastic matrices $\mathcal{S}_X^{2\to d}$, with the elements,

$$\left[\mathcal{S}_X^{2\to d}\right]_{kl} = \langle l|\mathcal{M}_k^X|l\rangle, \text{where } l \in \{0,1\}. \tag{4}$$

Evidently, action of $\mathcal{S}_A^{2\to d} \otimes \mathcal{S}_B^{2\to d}$ on a classical coin $\mathcal{C}_p(2) \equiv p_{00}\ \mathtt{hh} + p_{01}\ \mathtt{ht} + p_{10}\ \mathtt{th} + p_{11}\ \mathtt{tt}$ will produce the same probability statistics of Eq.[3]. Therefore, any $\mathcal{C}(d)$ coin state generated from any *zero-discord* two-qubit state, can be freely simulated from a properly chosen $\mathcal{C}(2)$ coin state. Hence, the quantum advantage in shared randomness generation necessarily requires the $\mathcal{Q}(2)$ states to have non-zero discord. ■

The above theorem is quite important, as it establishes a fundamentally new application of quantum discord [52, 53]. Notably, several other results have been derived to establish a connection between quantum discord and entanglement transformations [54–56], coherence resources [57], remote state preparations [58], random access codes [59] etc. Our result finds a utility of quantum discord in the generation of shared randomness. It would be interesting to explore further quantitative connections between the measure of discord with the quantum advantage obtained in the noisy scenario. The noisy scenario becomes even more interesting if we consider distribution of sources (classical or quantum) to establish shared randomness between two parties.

2.3.1 Quantum advantage in distributing SR

In the non-monopolize social subsidy game, we have considered that both the shared randomness and the strategies of the players are assisted by the referee. Let us consider now a scenario where a paired-coin (bipartite state) is prepared by one of the players who wish to distribute, through some communication channel, its one part to the other player to maximize their payoff. Distribution of the coin state $\mathcal{C}_{1/2}(2)$ in its exact form requires a perfect binary channel of capacity 1-bit. In quantum scenario, a communication channel can be most generally described by completely positive trace preserving maps [75]. Let Alice prepare a two-2-quoin state $\mathcal{Q}(2) = \rho_{AB} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ in her laboratory and then she sends the B part to Bob through a qubit channel Λ. They end up with a two-2-quoin state $\mathcal{Q}'(2) = \mathbf{I} \otimes \Lambda[\rho_{AB}]$, where $\mathbf{I}$ denotes the identity map (*i.e.* noiseless process) on the A part. Then they obtain a classical shared coin from $\mathcal{Q}'(d)$ by applying allowed free operations as suggested by the referee. In the following, we analyze two familiar noisy qubit channels for achieving better payoff in $\mathbb{G}(n)$.

Qubit phase-flip channel: Its action on an arbitrary state $\rho \in \mathcal{D}(\mathbb{C}^2)$ is given by, $\Lambda^z_p(\rho) := p\ \rho + (1-p)\ \sigma_z \rho \sigma_z$, where $p \in [0,1]$. If Alice sends one part of the coin state $\mathcal{Q}_{\psi^-}(2) = |\psi^-\rangle\langle\psi^-|$ to Bob through Λ^z_p then they end up sharing the state $\mathcal{Q}^z_p(2) = \mathbf{I}_2 \otimes \Lambda^z_p[\mathcal{Q}_{\psi^-}(2)] = p\ \mathcal{Q}_{\psi^-}(2) + (1-p)\ \mathcal{Q}_{\psi^+}(2)$. Applying the same Trine-POVM as in Theorem 2, the probabilities $p(ij) = \mathrm{Tr}\left[(\Pi_i \otimes \Pi_j).\mathcal{Q}^z_p(2)\right]$ can be represented as a 3×3 matrix

$$\mathcal{P}^z_p(3) \equiv \begin{pmatrix} 0 & \mu & \mu \\ \mu & (1-p)\ \mu & p\ \mu \\ \mu & p\ \mu & (1-p)\ \mu \end{pmatrix},$$

where $\mu = 1/6$. Since the maximum payoff for $\mathbb{G}(3)$ with a perfect classical channel is $1/8$, the Λ^z_p channel is advantageous whenever $\beta > 3/4$. For the $\mathbb{G}(4)$ case, following the same SIC-POVM strategy we have,

$$\mathcal{P}^z_p(4) \equiv \begin{pmatrix} 0 & 3\nu & 3\nu & 3\nu \\ 3\nu & \nu' & (1+2p)\nu & (1+2p)\nu \\ 3\nu & (1+2p)\nu & \nu' & (1+2p)\nu \\ 3\nu & (1+2p)\nu & (1+2p)\nu & \nu' \end{pmatrix},$$

where $\nu = 1/36$ and $\nu' = (1-p)/9$. In this case maximum classical payoff is $1/15$ which means Λ^z_p is advantageous for cases with more noise, *i.e.* whenever $p > 7/10$.

Qubit depolarizing channel: Its action is given by, $\Lambda^D_p(\rho) := p\ \rho + (1-p)\ \frac{\mathbb{I}}{2}$. If Alice prepares $\mathcal{Q}_{\psi^-}(2)$, then they end up sharing the state $\mathcal{Q}^D_p(2) = p\ \mathcal{Q}_{\psi^-}(2) + (1-p)\ \frac{\mathbf{I}}{2} \otimes \frac{\mathbf{I}}{2}$. A straightforward calculation, in this case, yields

$$\mathcal{P}^D_p(3) = \begin{pmatrix} \eta & \eta' & \eta' \\ \eta' & \eta & \eta' \\ \eta' & \eta' & \eta \end{pmatrix} \quad \& \quad \mathcal{P}^D_p(4) = \begin{pmatrix} \delta & \delta' & \delta' & \delta' \\ \delta' & \delta & \delta' & \delta' \\ \delta' & \delta' & \delta & \delta' \\ \delta' & \delta' & \delta' & \delta \end{pmatrix},$$

where $\eta = (1-p)/9$, $\eta' = (2+p)/18$, $\delta = (1-p)/16$. and $\delta' = (3+p)/48$. Therefore, the channel Λ^D_p is advantageous in $\mathbb{G}(3)$ [$\mathbb{G}(4)$] whenever $p > 1/4$ [$p > 1/5$]. Importantly, Λ^D_p is an entanglement breaking channel whenever $p \leq 1/3$ [76]. Therefore, the channel exhibits advantage in shared randomness distribution even when its quantum capacity is zero [64–66]. Also recall that classical capacity of qubit depolarizing channel is given by $\chi(\Lambda^D_p) = 1 - H\left(\frac{1+p}{2}\right)$, where $H(x) := -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy [77]. Therefore, quantum advantage is tangible even when the classical capacity of the quantum channel is much less than unity.

3 Discussion

Considerable effort has been made by researchers in quantum information and foundations community to identify a list of practical instances where application of quantum rules provide advantage over the classical physics. The present work, where we establish quantum advantage in generating higher degrees of shared randomness quantified within a suitably formulated resource theoretic framework, is an addition to this list. We also show precedence of quantum channel over its classical counterpart in distributing shared randomness. Such advantage is quite relevant if we recall some of the fundamental no-go results that limit the advantage of using quantum systems in classical information processing. For instance, Holevo's theorem limits the classical capacity of a quantum channel [60] whereas the recent no-go result by Frenkel and Weiner [61] limits classical information storage capacity in a quantum system. However, in the present work, it is established that a class of noisy qubit channels with imperfect classical capacity can surpass noiseless classical channels in distributing shared randomness. Moreover, the quantum advantage turns out to be robust to extreme noise that can erase its most prominent quantum signature, the quantum capacity. A discussion of our Proposition 1 in connection with the seminal Bell's theorem is worth mentioning. Recall that Bell's theorem establishes a non-classical feature for quantum correlations, in the sense that some of these cannot have a classical (local realistic) description [78]. In the same spirit, our results also point out a non-classical feature of quantum correlations in a setting where appropriate albeit fixed measurements are performed locally on a shared bipartite state. Precisely, a two-2-quoin can yield correlated random variables that cannot be obtained from a two-2-coin. Note that, while Bell's theorem involves more than one measurement on each part of the spatially separated systems and hence requires the assumption of 'measurement independence' [79, 80], our result only invokes a fixed measurement on each side and thus is free of this particular assumption. On the other hand, unlike Bell's theorem, the depiction of non-classical correlations in the present work requires the local dimension of the systems to be known.

Our work raises a number of important questions regarding the utility of non-classical origin of randomness, which will be of interest to the broader community of researchers in quantum foundations and quantum information. First, a class of monotones, completely characterizing the (im)possibility of conversion between two shared randomness resources, is still missing. Second, the advantage of two-2-quoins and noisy qubit channels in the generation and distribution of higher level shared randomness, demonstrated in this work, necessitate further characterization of quantum resources providing such preeminence. Our work serves as a stepping stone towards unveiling the rich potentiality of accomplishing quantum advantage in shared randomness generation from higher level systems and multipartite scenarios.

Acknowledgement: We gratefully acknowledge the discussions with Guruprasad Kar. MA acknowledges support from the CSIR project 09/093(0170)/2016- EMR-I. SR acknowledges support by the Foundation for Polish Science (IRAP project, ICTQT, contract no. MAB/2018/5, co-financed by EU within Smart Growth Operational Programme). SSB is supported by the National Natural Science Foundation of China through grant 11675136, the Foundational Questions Institute through grant FQXiRFP3-1325, the Hong Kong Research Grant Council through grant 17300918, and the John Templeton Foundation through grant 60609, Quantum Causal Structures. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation. MA and MB acknowledge support through the research grant of INSPIRE Faculty fellowship of MB from the Department of Science and Technology, Government of India.

References

[1] L. Jiang, J. M. Taylor, N. Khaneja, and M. D. Lukin, "Optimal approach to quantum communication using dynamic programming," Proceedings of the National Academy of Sciences **104**, 17291–17296 (2007).

[2] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate," Optics Express **16**, 18790 (2008).

[3] S. Wengerowsky, *et. al.*"Entanglement distribution over a 96-km-long submarine optical fiber," Proceedings of the National Academy of Sciences **116**, 6684–6688 (2019).

[4] J. Yin, *et. al.*,"Entanglement-based secure quantum cryptography over 1, 120 kilometres," Nature **582**, 501–505 (2020).

[5] Si-Hui Tan, Baris I. Erkmen, Vittorio Giovannetti, Saikat Guha, Seth Lloyd, Lorenzo Maccone, Stefano Pirandola, and Jeffrey H. Shapiro, "Quantum illumination with gaussian states," Phys. Rev. Lett. **101**, 253601 (2008).

[6] R. Schneider, *et.* al., "Quantum imaging with incoherently scattered light from a free-electron laser," Nature Physics **14**, 126–129 (2017).

[7] Shahaf Asban, Konstantin E. Dorfman, and Shaul Mukamel, "Quantum phase-sensitive diffraction and imaging using entangled photons," Proceedings of the National Academy of Sciences **116**, 11673–11678 (2019), https://www.pnas.org/content/116/24/11673.full.pdf .

[8] T. Gregory, P.-A. Moreau, E. Toninelli, and M. J. Padgett, "Imaging through noise with quantum illumination," Science Advances **6**, eaay2652 (2020).

[9] C. F. Roos, M. Chwalla, K. Kim, M. Riebe, and R. Blatt, "'designer atoms' for quantum metrology," Nature **443**, 316–319 (2006).

[10] J. Appel, P. J. Windpassinger, D. Oblak, U. B. Hoff, N. Kjaergaard, and E. S. Polzik, "Mesoscopic atomic entanglement for precision measurements beyond the standard quantum limit," Proceedings of the National Academy of Sciences **106**, 10960–10965 (2009).

[11] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone, "Advances in quantum metrology," Nature Photonics **5**, 222–229 (2011).

[12] Gershon Kurizki, Patrice Bertet, Yuimaru Kubo, Klaus Mølmer, David Petrosyan, Peter Rabl, and Jörg Schmiedmayer, "Quantum technologies with hybrid systems," Proceedings of the National Academy of Sciences **112**, 3866–3873 (2015).

[13] S.-S. Li, G.-L. Long, F.-S. Bai, S.-L. Feng, and H.-Z. Zheng, "Quantum computing," Proceedings of the National Academy of Sciences **98**, 11847–11848 (2001).

[14] Mikkel V. Larsen, Xueshi Guo, Casper R. Breum, Jonas S. Neergaard-Nielsen, and Ulrik L. Andersen, "Deterministic generation of a two-dimensional cluster state," Science **366**, 369–372 (2019).

[15] Abhinav Kandala, Kristan Temme, Antonio D. Córcoles, Antonio Mezzacapo, Jerry M. Chow, and Jay M. Gambetta, "Error mitigation extends the computational reach of a noisy quantum processor," Nature **567**, 491–495 (2019).

[16] C. Flühmann, T. L. Nguyen, M. Marinelli, V. Negnevitsky, K. Mehta, and J. P. Home, "Encoding a qubit in a trapped-ion mechanical oscillator," Nature **566**, 513–517 (2019).

[17] Frank Arute, *et. al.*"Quantum supremacy using a programmable superconducting processor," Nature **574**, 505–510 (2019).

[18] Raúl García-Patrón, Jelmer J. Renema, and Valery Shchesnovich, "Simulating boson sampling in lossy architectures," Quantum **3**, 169 (2019).

[19] P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (IEEE Comput. Soc. Press).

[20] L. K. Grover; A fast quantum mechanical algorithm for database search, Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing. STOC '96.

Philadelphia, Pennsylvania, USA: Association for Computing Machinery: 212–219 (1996)

[21] D. R. Simon; On the Power of Quantum Computation, Journal on Computing, **26**(5), 1474–1483 (1997)

[22] C. H. Bennett, G. Brassard, and J. Robert, "Privacy amplification by public discussion," SIAM Journal on Computing **17**, 210–229 (1988).

[23] C.H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer, "Generalized privacy amplification," IEEE Trans. Inf. Theory **41**, 1915–1923 (1995).

[24] I. Newman and M. Szegedy, "Public vs. private coin flips in one round communication games (extended abstract)," (ACM Press, 1996).

[25] L. Babai and P.G. Kimmel, "Randomized simultaneous messages: solution of a problem of yao in communication complexity," (IEEE Comput. Soc).

[26] D. Gavinsky, T. Ito, and G. Wang, "Shared randomness and quantum communication in the multi-party model," (2012), arXiv:1210.1535 [quant-ph] .

[27] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," IEEE Trans. Inf. Theory **39**, 1121–1132 (1993).

[28] G. Brassard, R. Cleve, and A. Tapp, "Cost of exactly simulating quantum entanglement with classical communication," Phys. Rev. Lett. **83**, 1874–1877 (1999).

[29] B. F. Toner and D. Bacon, "Communication cost of simulating bell correlations," Phys. Rev. Lett. **91**, 187904 (2003).

[30] J. Bowles, F. Hirsch, M. T. Quintino, and N. Brunner, "Local hidden variable models for entangled quantum states using finite shared randomness," Phys. Rev. Lett. **114**, 120401 (2015).

[31] R. J. Aumann, "Correlated equilibrium as an expression of bayesian rationality," Econometrica **55**, 1 (1987).

[32] N. Brunner and N. Linden, "Connection between bell nonlocality and bayesian game theory," Nat. Commun. **4**, 2057 (2013).

[33] Arup Roy, Amit Mukherjee, Tamal Guha, Sibasish Ghosh, Some Sankar Bhattacharya, and Manik Banik, "Nonlocal correlations: Fair and unfair strategies in bayesian games," Phys. Rev. A **94**, 032120 (2016).

[34] M. Banik, S. S. Bhattacharya, N. Ganguly, T. Guha, A. Mukherjee, A. Rai, and A. Roy, "Two-qubit pure entanglement as optimal social welfare resource in bayesian game," Quantum **3**, 185 (2019).

[35] C. L. Canonne, V. Guruswami, R. Meka, and M. Sudan, "Communication with imperfectly shared randomness," IEEE Trans. Inf. Theory **63**, 6799–6818 (2017).

[36] C. E. Shannon, "A mathematical theory of communication," Bell System Technical Journal **27**, 379–423 (1948).

[37] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513–577 (2005).

[38] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, "Reference frames, superselection rules, and quantum information," Rev. Mod. Phys. **79**, 555–609 (2007).

[39] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," Rev. Mod. Phys. **81**, 865–942 (2009).

[40] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, "The classical-quantum boundary for correlations: Discord and related measures," Rev. Mod. Phys. **84**, 1655–1707 (2012).

[41] F. G. S. L. Brandão, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, "Resource theory of quantum states out of thermal equilibrium," Phys. Rev. Lett. **111**, 250404 (2013).

[42] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, P. Joshi, W. Kłobus, and A. Wójcik, "Quantifying contextuality," Phys. Rev. Lett. **112**, 120401 (2014).

[43] Á. Rivas, S. F Huelga, and M. B. Plenio, "Quantum non-markovianity: characterization, quantification and detection," Rep. Prog. Phys. **77**, 094001 (2014).

[44] V. Veitch, S. A. H. Mousavian, D. Gottesman, and J. Emerson, "The resource theory of stabilizer quantum computation," New J. Phys. **16**, 013009 (2014).

[45] R. Gallego and L. Aolita, "Resource theory of steering," Phys. Rev. X **5**, 041008 (2015).

[46] A. Winter and D. Yang, "Operational resource theory of coherence," Phys. Rev. Lett. **116**, 120404 (2016).

[47] Eric Chitambar and Gilad Gour, "Quantum resource theories," Rev. Mod. Phys. **91**, 025001 (2019).

[48] Elie Wolfe, David Schmid, Ana Belén Sainz, Ravi Kunjwal, and Robert W. Spekkens, "Quantifying bell: the resource theory of nonclassicality of common-cause boxes," Quantum **4**, 280 (2020).

[49] D. Schmid, D. Rosset and F. Buschemi; The type-independent resource theory of local operations and shared randomness, Quantum, **4**, 262 (2020)

[50] D. Rosset, D. Schmid and F. Buschemi; Type-Independent Characterization of Space-like Separated Resources, Phys. Rev. Lett. **125**, 210402 (2020)

[51] B. F. Toner and D. Bacon; Communication Cost of Simulating Bell Correlations, Phys. Rev. Lett. **91**, 187904 (2003)

[52] Harold Ollivier and Wojciech H. Zurek, "Quantum discord: A measure of the quantumness of correlations," Phys. Rev. Lett. **88**, 017901 (2001).

[53] L Henderson and V Vedral, "Classical, quantum and total correlations," Journal of Physics A: Mathematical and General **34**, 6899–6905 (2001).

[54] D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani, and A. Winter; Operational interpretations of quantum discord, Phys. Rev. A **83**, 032324 (2011)

[55] V. Madhok and A. Datta; Interpreting quantum discord through quantum state merging, Phys. Rev. A **83**, 032323 (2011)

[56] A. Streltsov, H. Kampermann, and D. Bruß; Linking Quantum Discord to Entanglement in a Measurement, Phys. Rev. Lett. **106**, 160401 (2011)

[57] V. Madhok and A. Datta; Role of quantum discord in quantum communication, arXiv: 1107.0994[quant-ph] (2011)

[58] B. Dakic *et. al.*; Quantum discord as resource for remote state preparation, Nature Physics volume 8, pages666–670(2012)

[59] T. K. C. Bobby and T. Paterek; Separable states improve protocols with finiterandomness, New J. Phys. **16**, 093063 (2014)

[60] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," Problems of Information Transmission **9**, 177–183 (1973).

[61] P. E. Frenkel and M. Weiner, "Classical information storage in an n-level quantum system," Commun. Math. Phys. **340**, 563–574 (2015).

[62] A.S. Holevo, "The capacity of the quantum channel with general signal states," IEEE Trans. Inf. Theory **44**, 269–273 (1998).

[63] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," Phys. Rev. A **56**, 131–138 (1997).

[64] S. Lloyd, "Capacity of the noisy quantum channel," Phys. Rev. A **55**, 1613–1622 (1997).

[65] P. W. Shor, "The quantum channel capacity and coherent information," Lecture notes,MSRIWorkshop on Quantum Computation **-**, – (2002).

[66] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," IEEE Trans. Inf. Theory **51**, 44–55 (2005).

[67] F. G. S. L. Brandão and G. Gour, "Reversible framework for quantum resource theories," Phys. Rev. Lett. **115**, 070503 (2015).

[68] L. Hardy, "Quantum theory from five reasonable axioms," (2001), arXiv:quant-ph/0101012 [quant-ph] .

[69] J. Barrett, "Information processing in generalized probabilistic theories," Phys. Rev. A **75**, 032304 (2007).

[70] G. Chiribella, G. M. D'Ariano, and P. Perinotti, "Informational derivation of quantum theory," Phys. Rev. A **84**, 012311 (2011).

[71] I. Namioka and R.Phelps, "Tensor products of compact convex sets," Pac. J. Math **31**, 469–480 (1969).

[72] G. P. Barker, "Monotone norms and tensor products," Linear and Multilinear Algebra **4**, 191–199 (1976).

[73] G. P. Barker, "Theory of cones," Linear Algebra Its Appl **39**, 263–291 (1981).

[74] G. Aubrun, L. Lami, C. Palazuelos, and M. Plavala, "Entangleability of cones," (2019), arXiv:1911.09663 [math.FA] .

[75] K. Kraus, *States, Effects, and Operations Fundamental Notions of Quantum Theory*, edited by K. Kraus, A. Böhm, J. D. Dollard, and W. H. Wootters (Springer Berlin Heidelberg, 1983).

[76] R. F. Werner, "Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model," Phys. Rev. A **40**, 4277–4281 (1989).

[77] C. King, "The capacity of the quantum depolarizing channel," IEEE Transactions on Information Theory **49**, 221–229 (2003).

[78] John S. Bell, "On the problem of hidden variables in quantum mechanics," Rev. Mod. Phys. **38**, 447–452 (1966).

[79] Michael J. W. Hall, "Local deterministic model of singlet state correlations based on relaxing measurement independence," Phys. Rev. Lett. **105**, 250404 (2010).

[80] Jonathan Barrett and Nicolas Gisin, "How much measurement independence is needed to demonstrate nonlocality?" Phys. Rev. Lett. **106**, 100406 (2011).