Quantum and Classical Hybrid Generations for Classical Correlations

Xiaodie Lin, Zhaohui Wei, and Penghui Yao

***Abstract*—We consider two-stage hybrid protocols that combine quantum resources and classical resources to generate classical correlations shared by two separated players. Our motivation is twofold. First, in the near future, the scale of quantum information processing is quite limited, and when quantum resource available is not sufficient for certain tasks, a possible way to strengthen the capability of quantum schemes is introducing extra classical resources. We analyze the mathematical structures of these hybrid protocols, and characterize the relation between the amount of quantum resources and classical resources needed. Second, a fundamental open problem in communication complexity theory is to describe the advantage of sharing prior quantum entanglement over sharing prior randomness, which is still widely open. It turns out that our quantum and classical hybrid protocols provide new insight into this important problem.**

***Index Terms*—Near-term quantum computing, hybrid protocols, correlation generation, quantum advantage.**

I. Introduction

SUPPOSE two separated parties, Alice and Bob, aim to output random variables X and Y, such that (X, Y) is distributed exactly according to a target joint probability distribution P. As shared randomness, sometimes we call P a *classical correlation*. Then an important problem is, what is the minimum cost of generating an arbitrary classical correlation? For the convenience of later discussion, we give a formal definition for the task we consider in this paper.

Definition I.1: Suppose $P = (P_{xy})$ is a joint probability distribution on X and Y, where $x \in X$ and $y \in Y$. If in a protocol, the probability that Alice outputs x and Bob outputs y is exactly P_{xy} for any $x \in X$ and $y \in Y$, we say Alice and Bob sample or generate P.

Actually this problem has been systematically studied [1]–[3]. Generally, P is not a product distribution, thus in order to sample P, Alice and Bob can share a seed correlation (X', Y') and each applies a local operation on the corresponding subsystem without communication. The minimum *size* of this seed distribution, i.e., half of the total number of bits, is defined to be the *randomized correlation complexity* of P, denoted $\mathsf{R}(P)$. Alternatively, the two parties can also share a *quantum* state σ as a seed state, on which the two parties apply local quantum operations without communication to generate P. More specifically, suppose $P = (P_{xy})$, then it holds that $P_{xy} = \mathtt{tr}((E_x \otimes F_y)\sigma)$, where $x \in X$, $y \in Y$, and $\{E_x\}$ and $\{F_y\}$ are the kraus operators of Alice and Bob's local quantum operations respectively. In this case, the minimum size of the quantum seed state σ, i.e., half of the total number of qubits, is called the *quantum correlation complexity*, denoted $\mathsf{Q}(P)$.

Instead of sharing seed states, Alice and Bob can also generate a correlation from scratch by communication only. When communicating quantum information, the minimum number of qubits exchanged between Alice and Bob, initially sharing nothing, to generate P at the end of the protocol is defined as the *quantum communication complexity* of P, denoted $\mathsf{QComm}(P)$. Similarly, one can also define the *randomized communication complexity* of P, denoted $\mathsf{RComm}(P)$, as the minimum number of bits exchanged to generate P. It turns out that for any P, the correlation complexity and the communication complexity are always the same, namely $\mathsf{QComm}(P) = \mathsf{Q}(P)$ and $\mathsf{RComm}(P) = \mathsf{R}(P)$ [1]. Therefore, we can simply use the notations Q and R to denote the quantities in quantum and classical settings respectively. In this paper, when generating classical correlations by quantum procedures, we will mainly focus on the setting with seed states.

In fact, the full characterizations for $\mathsf{Q}(P)$ and $\mathsf{R}(P)$ have been achieved [1], [2] for any classical correlation P. That is, for any classical correlation P,

$$\mathsf{R}(P) = \lceil \log_2 \mathtt{rank}_+(P) \rceil, \tag{1}$$

and

$$\mathsf{Q}(P) = \lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P) \rceil. \tag{2}$$

Here for any nonnegative matrix $P \in \mathbb{R}_+^{n \times m}$, $\mathtt{rank}_+(P)$ is the nonnegative rank, which is defined as the minimum number r such that P can be decomposed as the summation of r nonnegative matrices of rank 1. And $\mathtt{rank}_{\mathtt{psd}}(P)$ is the

Manuscript received July 30, 2020; revised July 21, 2021; accepted October 14, 2021. Date of publication October 27, 2021; date of current version December 23, 2021. The work of Xiaodie Lin and Zhaohui Wei was supported in part by the National Key Research and Development Program of China, Grant 2018YFA0306703 and in part by the National Natural Science Foundation of China, Grant No. 20181311604. This work was supported in part by the Zhongguancun Haihua Institute for Frontier Information Technology. The work of Penghui Yao was supported in part by the National Key R&D Program of China 2018YFB1003202, in part by the National Natural Science Foundation of China (Grant No. 61972191), in part by the Program for Innovative Talents and Entrepreneur in Jiangsu, in part by the Fundamental Research Funds for the Central Universities 0202/14380068, and in part by the Anhui Initiative in Quantum Information Technologies Grant No. AHY150100. *(Corresponding author: Zhaohui Wei.)*

Xiaodie Lin is with the Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China (e-mail: linxd19@mails.tsinghua.edu.cn).

Zhaohui Wei was with the Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China. He is now with the Yau Mathematical Sciences Center, Tsinghua University, Beijing 100084, China (e-mail: weizhaohui@gmail.com).

Penghui Yao is with the State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu 210023, China (e-mail: pyao@nju.edu.cn).

Communicated by M. Mosonyi, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2021.3123401

positive semi-definite rank (PSD-rank), which is the minimum r such that there are $r \times r$ positive semi-definite matrices C_x, $D_y \in \mathbb{C}^{r\times r}$, satisfying that $P(x,y) = \mathtt{tr}(C_x D_y)$, for all x and y [4], [5].

It can be shown that the gap between nonnegative ranks and PSD-ranks can be huge, and this, therefore, reveals the remarkable advantage of quantum schemes in generating classical correlations. For example, consider the following $2^n \times 2^n$ matrix $M \in \mathbb{R}_+^{2^n\times 2^n}$ with rows and columns indexed by n-bit strings a and b, and real nonnegative entries $M_{ab} := (1 - a^\intercal b)^2$, where $a^\intercal b$ is the mod 2 inner product between a and b. Then we have the following conclusions.

Fact I.2 ([4]): It holds that $\mathtt{rank}_+(M) = 2^{\Omega(n)}$ and $\mathtt{rank}_{\mathtt{psd}}(M) = O(n)$.

Though quantum advantage can be huge, and meanwhile extraordinary progress has been achieved on physical implementation of quantum computation, it is still widely believed that the availability of large-scale quantum computers is still far [6], [7]. As a consequence, in the near future the scale of quantum information processing, especially the scale of entanglement, is quite limited, say dozens or hundreds of qubits. For the convenience of later discussions, we now introduce the following definition.

Definition I.3: Suppose the largest bipartite quantum system that we can fully manipulate experimentally has s qubits in each subsystem, then we say our *quantum capability* is s qubits.

For some realistic classical correlations P, it is possible that $\lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P)\rceil$, the necessary size of a shared seed quantum state that produces P according to [2], exceeds our quantum capability. In this situation, a natural question is, can we design a proper quantum and classical hybrid protocol to generate P in such a way that, it not only fulfills the task completely but also fully exploits the potential of our quantum capability? In this manuscript, by looking into the rich mathematical structures of quantum and classical hybrid protocols, we will give a positive answer to the above question.

Particularly, we first consider the case that the only restriction on our capability to manipulate quantum states is the scale, which means we can require any quantum states whenever we want as long as their size is within our means, which may depend on the classical messages exchanged. Then we prove that if a hybrid protocol has to be utilized to generate a large classical correlation P, the protocol can be fully characterized by a concept called *k-block positive semi-definite ranks*, which was recently studied by [8]–[11] and is essentially a generalization of the concept of PSD-ranks. More specifically, in our setting this concept exactly reveals the relation between the amount of classical resources needed and the quantum resources available. Particularly, by looking into the rich mathematical structures of the concept of k-block positive semi-definite ranks, we prove that the shortage of one single qubit may require a huge amount of classical resources to compensate, thus providing new evidence of quantum advantage in generating classical correlations. Furthermore, we also consider another setting with more rigorous restrictions on our freedom of exploiting quantum resources, i.e., in addition to the restricted quantum scale, only one single quantum state that is independent of classical messages is provided for the players. Based on the idea of entanglement transformation, we show that the second model actually has similar power to the first one.

Apart from the applications in near-term quantum computers, the trade-off between classical resources and quantum resources is also an important topic in quantum resource theories. Quantum resource theories are a versatile framework to compare the amount of various quantum resources, such as entanglement and coherence in various computational or communication tasks. Readers may refer to [12] for an excellent survey. In fact, the trade-off between classical communication and quantum communication in quantum resource theories has been systematically studied in [13], [14], where Hsieu and Wilde provided a tight achievable rate region for the trade-off between classical communication, quantum communication, and entanglement for processing information in the Shannon-theoretic setting.

Meanwhile, our results are also related to a famous open problem in quantum communication complexity theory. Quantum communication complexity was introduced by Yao in [15], which investigates the advantage and limits of the communication complexity models when the players are allowed to exchange quantum messages. Dozens of examples have been discovered that exhibit the advantage of quantumness (see [16] and references therein) as well as numerous methods proving the lower bounds on quantum communication complexity have been established [17]. In the model introduced by Yao, the players may share classical random strings independent of the input before exchanging messages. This is named as the Yao's model. Thanks to Newman's theorem [18], we know that the shared randomness can only save at most $O(\log n)$ bits communication, where n is the length of the inputs. Cleve and Buhrman in [19] introduced another model where the players are allowed to preshare arbitrary bipartite quantum states, which is named as the Cleve-Buhrman model. Using quantum teleportation [20], we may assume that the players in the Cleve-Buhrman model only exchange classical messages while the communication cost increases by at most factor 2 compared with the Cleve-Buhrman model exchanging qubits.

A fundamental problem in communication complexity is how much communication can be saved if the players share entanglement. In other words, what is the largest separation between the Yao's model and the Cleve-Buhrman model? The role of entanglement in quantum computing has always been a core topic in the theory of quantum computation, which is studied in various models of computation. In particular, it has been shown in a very recent breakthrough result [21] that multi-prover interactive proof systems with sharing entanglement are able to decide the Halting problem, while the ones without sharing entanglement are in NEXP [22]. However, little is known about the power of entanglement in communication complexity. Indeed, till now we do not have any nontrivial upper bound on the separation between the Yao's model and the Cleve-Burhman model. Meanwhile, we are not aware of any example that exhibits a super-constant separation between these two models as well. In this paper, our results provide more facts on the power of entanglement in the context of classical correlation generation, which show that sharing entanglement can save the classical communication significantly. Although our model is not about computing functions, we hope that our results shed new light on this widely open problem.

II. The Hybrid Protocols

Recall that for convenience we define the size of a bipartite distribution as half of the total number of bits. Similarly, the size of a bipartite quantum state is half of the total number of qubits.

Suppose our quantum capability is s qubits. We now consider a target classical correlation $P \in \mathbb{R}_+^{n\times m}$ with $s < \lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P)\rceil$. Clearly, we cannot generate P using a purely quantum scheme according to [2].

Therefore, we turn to analyze the possibility to combine quantum power and classical power together. To make the hybrid protocol valuable, we hope the extra classical cost needed will be dramatically smaller than that of a pure classical protocol. In the meantime, as in principle we have different ways to combine quantum subprotocols and classical ones to design hybrid protocols, we now analyze two main possibilities as below.

A. The Classical-Quantum Hybrid

Suppose the target classical correlation can be expressed as a linear combination of two other ones, i.e., $P = \frac{1}{2}P_1 + \frac{1}{2}P_2$, where P_1 and P_2 are nonnegative matrices. Then one can easily construct examples with $\mathtt{rank}_{\mathtt{psd}}(P_1) < \mathtt{rank}_{\mathtt{psd}}(P)$ and $\mathtt{rank}_{\mathtt{psd}}(P_2) < \mathtt{rank}_{\mathtt{psd}}(P)$, which inspires us to design the following natural hybrid protocol. Assume $P = \sum_{i\in I} p_i P_i$, where $\{p_i\}$ is a probability distribution on $i \in I$, and for any $i \in I$, $P_i \in \mathbb{R}_+^{n\times m}$ is a classical correlation with $\lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P_i)\rceil \leq s$, then Alice and Bob can produce a sampling of P as below. They first sample a shared output $i \in I$ classically according to the probability distribution $\{p_i\}$, then one of them prepares a bipartite quantum state ρ_i that can serve as a seed state to produce P_i and sends half of the qubits to the other party by quantum communication, which is within the quantum capability. After that, they generate a classical correlation P_i by performing local measurements on ρ_i like in a purely quantum protocol. Since $\sum_{i\in I} p_i P_i = P$, overall the hybrid protocol generates exactly the target classical correlation P.

Since in the first stage of the protocol Alice and Bob sample $i \in I$, we call this a *classical-quantum hybrid protocol*. Here the classical cost is $c = \lceil \log_2 |I|\rceil$ bits, and the quantum cost is $q = \max_i \mathsf{size}(\rho_i)$ qubits, where $\mathsf{size}(\rho_i)$ is the size of ρ_i. Since it holds that $q \leq s$, the current hybrid protocol can generate the target correlation P within the quantum capability. Below is a simple example that demonstrates this idea.

Let

$$P = \frac{1}{2^k}\begin{bmatrix} P_1 & & & \\ & P_2 & & \\ & & \ddots & \\ & & & P_{2^k}\end{bmatrix}, \tag{3}$$

where $2^k \cdot P \in \mathbb{R}_+^{2^k n\times 2^k m}$ is a block diagonal matrix, and for the convenience of later discussion, we denote it by $\mathrm{diag}(P_1, P_2, \ldots, P_{2^k})$. For each $i \in [2^k]$, suppose $P_i \in \mathbb{R}_+^{n\times m}$ is a classical correlation satisfying $\mathtt{rank}_{\mathtt{psd}}(P_i) = 2^s$. Then it can be seen that P, as a classical correlation, cannot be produced using a purely quantum protocol, as the current quantum capability s is smaller than $\lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P)\rceil = k + s$. However, we can generate it using a hybrid protocol, where in the first stage it takes them classical communication of k bits to sample $i \in [2^k]$, then they consume a shared quantum state of size s qubits to generate the corresponding P_i. As long as they adjust the output labels properly, the overall output will be exactly a sample of P.

As pointed out before, examples of P_i exist such that $\mathtt{rank}_+(P_i) \gg 2^s$, i.e., when sampling P_i quantum schemes enjoy remarkable advantage over classical ones. If this is the case, though we cannot produce P using a purely quantum scheme directly, such a hybrid protocol may still decrease the amount of classical resources dramatically.

Due to the above example, we are tempted to consider the following realistic problem. Still assume our quantum capability is known to be s, and the target classical correlation P satisfies $s < \lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P)\rceil$. Then if we choose to generate P using a classical-quantum hybrid protocol, what is the minimum amount of extra classical resources needed? Or, to put it another way, given an arbitrary classical correlation P, what is the minimum number m such that P can be expressed as the summation of m nonnegative matrices with PSD-rank not larger than 2^s? To answer this question, we will utilize the concept of k-block positive semi-definite rank, which is essentially a generalization of the concept of PSD-rank and has been studied by [8]–[11].

Definition II.1: A *k-block positive semi-definite factorization* of a nonnegative matrix $P \in \mathbb{R}_+^{n\times m}$ is a collection of positive semi-definite matrices $C_i = \mathrm{diag}(C_i^1, \ldots, C_i^r), D_j = \mathrm{diag}(D_j^1, \ldots, D_j^r) \in \mathbb{C}^{kr\times kr}$ that satisfy

$$P_{ij} = \mathtt{tr}(C_i D_j) = \sum_{l=1}^{r} \mathtt{tr}(C_i^l D_j^l),\ i = 1, \ldots, n,\ j = 1\ldots, m,$$

where $C_i^l, D_j^l \in \mathbb{C}^{k\times k}$ for each i, j, and l. And the k-block positive semi-definite rank, denoted $\mathtt{rank}_{\mathtt{psd}}^{(k)}(P)$, is defined as the smallest integer r for which such a k-block positive semi-definite factorization exists.

We now prove that the question asked above is perfectly answered by the concept of 2^s-block semi-definite ranks, where the corresponding optimal classical-quantum hybrid protocol is exactly characterized by an optimal 2^s-block positive semi-definite factorization.

Theorem II.2: Suppose the quantum capability is s qubits. Then the minimum amount of classical communication needed in a classical-quantum hybrid protocol producing P is exactly $\lceil \log_2 \mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P)\rceil$ bits.

Proof: Suppose the minimal classical cost is c bits. Then we have a factorization $P(x, y) = \sum_{i=1}^{2^c} p_i P_i(x, y)$, where $\{p_i\}$ is a probability distribution on $i \in [2^c]$, and each correlation P_i can be generated by quantum communication of $\lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P_i)\rceil \leq s$ qubits with a purely quantum protocol. Suppose a positive semi-definite factorization of P_i is $P_i(x,y) = \mathtt{tr}(C_x^i D_y^i)$, where without loss of generality C_x^i, D_y^i can be chosen as positive semi-definite matrices of size $2^s \times 2^s$ for any $x \in [n], y \in [m]$. Let $C_x = \mathrm{diag}(p_1 C_x^1, \ldots, p_{2^c} C_x^{2^c})$ and $D_y = \mathrm{diag}(D_y^1, \ldots, D_y^{2^c})$. Then it can be seen that C_x and D_y are block diagonal positive semi-definite matrices with each block of size $2^s \times 2^s$, and furthermore, $P(x,y) = \mathtt{tr}(C_x D_y)$ for any $x \in [n], y \in [m]$. Therefore, it holds that $\mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P) \leq 2^c$, i.e., $\lceil \log_2 \mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P) \rceil \leq c$.

On the other hand, suppose $r = \mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P)$. Then one can find block diagonal positive semi-definite matrices C_x and D_y of block size $2^s \times 2^s$ such that $P(x,y) = \mathtt{tr}(C_x D_y)$ for any $x \in [n], y \in [m]$. That is to say, we can suppose $C_x = \mathrm{diag}(C_x^1, \ldots, C_x^r)$ and $D_y = \mathrm{diag}(D_y^1, \ldots, D_y^r)$, where C_x^i and D_y^i are positive semi-definite matrices of size $2^s \times 2^s$ for any $i \in [r]$. Define P_i to be the classical correlation $Q_i / \|Q_i\|_1$, where $Q_i \in \mathbb{R}_+^{n \times m}$ and $Q_i(x,y) = \mathtt{tr}(C_x^i D_y^i)$ for any $x \in [n], y \in [m]$. Note that this is well-defined: If we let $p_i = \|Q_i\|_1$, then $p_i > 0$ according to the definition of 2^s-block diagonal positive semi-definite rank. Then it is not hard to see that $P = \sum_{i=1}^r p_i P_i$, and for each $i \in [r]$, it holds that $\mathtt{rank}_{\mathtt{psd}}(P_i) \leq 2^s$. Therefore, one can design a classical-quantum hybrid protocol to generate P corresponding to this factorization, where the cost of classical communication is $\lceil \log_2 r \rceil$, implying that $c \leq \lceil \log_2 \mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P) \rceil$. □

In real-life implementations of sampling $P \in \mathbb{R}_+^{n \times m}$, we often allow a small deviation of ϵ, which suggests us to consider approximate samplings of classical correlations.

Definition II.3: Suppose $P = (P_{xy})$ is a joint probability distribution on X and Y, where $x \in X$ and $y \in Y$. $0 < \epsilon < 1$ is a small positive number. If in a protocol, P'_{xy}, the probability that Alice outputs x and Bob outputs y, satisfies that $\sum_{xy} |P_{xy} - P'_{xy}| \leq \epsilon$ for any $x \in X$ and $y \in Y$, we say Alice and Bob sample or generate P approximately.

Accordingly, we need to consider an approximate version of k-block positive semi-definite rank, that is,

$$\mathtt{rank}_{\mathtt{psd},\epsilon}^{(k)}(P) \equiv \min\{\mathtt{rank}_{\mathtt{psd}}^{(k)}(Q) :\ Q \in \mathbb{R}_+^{n \times m} \text{ is a probability distribution and } \|P - Q\|_1 \leq \epsilon\}, \tag{4}$$

where $\|P - Q\|_1$ is the 1-norm of $P - Q$, i.e., the summation of the absolute values of all entries of $P - Q$. Then it can be seen that when tolerating a small additive error ϵ, the cost of optimal classical-quantum protocol that samples P approximately is characterized by the corresponding approximate k-block positive semi-definite rank.

We now know that given the quantum capability s qubits, suppose $s < \lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P) \rceil$, then in order to design a proper classical-quantum hybrid protocol generating P, estimating $\mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P)$ is crucial. In the rest of the current section, we will focus on the characterization of $\mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P)$.

Firstly, according to the properties of ranks and PSD-ranks, we immediately have the following lower bounds for $\mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P)$ and $\mathtt{rank}_{\mathtt{psd},\epsilon}^{(2^s)}(P)$.

Fact II.4: For any nonnegative matrix $P \in \mathbb{R}_+^{n \times m}$ and any integer $k \geq 1$, it holds that

$$\mathtt{rank}_{\mathtt{psd}}^{(k)}(P) \geq \frac{\mathtt{rank}_{\mathtt{psd}}(P)}{k},\quad \mathtt{rank}_{\mathtt{psd},\epsilon}^{(k)}(P) \geq \frac{\mathtt{rank}_{\mathtt{psd},\epsilon}(P)}{k}, \tag{5}$$

and

$$\mathtt{rank}_{\mathtt{psd}}^{(k)}(P) \geq \frac{\mathtt{rank}(P)}{k^2},\quad \mathtt{rank}_{\mathtt{psd},\epsilon}^{(k)}(P) \geq \frac{\mathtt{rank}_{\epsilon}(P)}{k^2}, \tag{6}$$

where $\mathtt{rank}_{\mathtt{psd},\epsilon}(P)$ and $\mathtt{rank}_{\epsilon}(P)$ are the approximate PSD-rank and the approximate rank of P, respectively, i.e., $\mathtt{rank}_{\mathtt{psd},\epsilon}(P) \equiv \min\{\mathtt{rank}_{\mathtt{psd}}(Q) :\ Q \in \mathbb{R}_+^{n \times m}$ is a probability distribution and $\|P - Q\|_1 \leq \epsilon\}$ and $\mathtt{rank}_{\epsilon}(P) \equiv \min\{\mathtt{rank}(Q) :\ Q \in \mathbb{R}_+^{n \times m}$ is a probability distribution and $\|P - Q\|_1 \leq \epsilon\}$.

Proof: We only prove the exact cases here, and the approximate cases are similar. Suppose $r = \mathtt{rank}_{\mathtt{psd}}^{(k)}(P)$, then there exist block diagonal positive semi-definite matrices $C_i, D_j \in \mathbb{C}^{kr \times kr}$ such that $P_{ij} = \mathtt{tr}(C_i D_j)$. Since C_i and D_j also form a positive semi-definite factorization of P, we have $\mathtt{rank}_{\mathtt{psd}}(P) \leq kr$, which is exactly Eq.(5). Besides, according to the structures of classical-quantum hybrid protocols, we have $P = \sum_{i=1}^r P_i$, and $\mathtt{rank}_{\mathtt{psd}}(P_i) \leq k$ for any $i \in [r]$. Together with the fact that $\sqrt{\mathtt{rank}(A)} \leq \mathtt{rank}_{\mathtt{psd}}(A)$ holds for any nonnegative matrix A [23], we have

$$\mathtt{rank}(P) \leq \sum_{i=1}^{r} \mathtt{rank}(P_i) \leq r k^2, \tag{7}$$

which completes the proof for Eq.(6). □

The above two lower bounds can be tight on some specific cases. For example, let P be the classical correlation in Eq.(3), then it holds that $\mathtt{rank}_{\mathtt{psd}}(P) = 2^{s+k}$ and $\mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P) \leq 2^k$, where the second fact comes from that we can decompose P into the summation of 2^k classical correlations with each corresponding to one P_i. Hence $\mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P) \leq \mathtt{rank}_{\mathtt{psd}}(P)/2^s$, and combined with Eq.(5) this means that actually $\mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P) = \mathtt{rank}_{\mathtt{psd}}(P)/2^s = 2^k$. Furthermore, if one chooses P_i such that $\mathtt{rank}(P_i) = \mathtt{rank}_{\mathtt{psd}}(P_i)^2 = 2^{2s}$ for any $i \in [2^k]$, then we have $\mathtt{rank}(P) = 2^{2s+k}$, and $\mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P) = \mathtt{rank}(P)/2^{2s}$, implying that Eq.(6) can also be tight. However, later we will see that in some cases these relations can be very loose.

We next turn to upper bounds for $\mathtt{rank}_{\mathtt{psd}}^{(k)}(P)$. It turns out that $\mathtt{rank}_{\mathtt{psd}}^{(k)}(P)$ can be upper bounded by generalizing the idea in the example of Eq.(3), and utilizing the notion of *combinatorial rectangle* proposed by Yao [24], which plays a key role in communication complexity theory. Suppose $X \subseteq [n]$ and $Y \subseteq [m]$, then $X \times Y$ pins down a submatrix of P, called a combinatorial rectangle. Then we define a *partition* of P to be a series of nonzero combinatorial rectangles, where there is no overlap between any two of them and the union of all combinatorial rectangles contains all nonzero entries of P. If each combinatorial rectangle, which is regarded as a classical correlation after normalization, can be produced quantumly within the quantum capability, then P can be generated by a classical-quantum protocol as a probability mixture of these combinatorial rectangles. Naturally, in this situation, we are interested in the optimal partition of P, which has the minimum number of combinatorial rectangles with each within the quantum capability. For this, we make the following definition.

Definition II.5: Let $P \in \mathbb{R}_{+}^{n\times m}$ be a classical correlation. Define the k-**partition number** of P, denoted $C^k(P)$, as the minimum number of combinatorial rectangles that form a partition of P with the property that each combinatorial rectangle has PSD-rank at most k. For convenience, we call these combinatorial rectangles a k-**partition** of P.

Then we have the following proposition.

Proposition II.6: For any nonnegative matrix $P \in \mathbb{R}_{+}^{n\times m}$ and any integer $k \geq 1$, it holds that

$$\mathtt{rank}_{\mathtt{psd}}^{(k)}(P) \leq C^k(p). \tag{8}$$

Proof: Suppose $t = C^k(P)$, and $\{P_1, P_2, \ldots, P_t\}$ is an optimal k-**partition** of P. Define the weight of the i-th combinatorial rectangle to be the summation of all its entries, denoted w_i. Then $\sum_{i=1}^{t} w_i = 1$, and $\{w_i, i \in [t]\}$ is a valid probability distribution.

We expand the size of each P_i to be $n \times m$ by adding zero entries with the positions of all nonzero entries the same as in P, which does not change its PSD-rank. For any $i \in [t]$ suppose an optimal positive semi-definite factorization of P_i is $P_i(x, y) = \mathtt{tr}(C_x^i D_y^i)$, where C_x^i, D_y^i are $k \times k$ positive semi-definite matrices for any $x \in [n], y \in [m]$. Let $C_x = \mathrm{diag}(w_1 C_x^1, \ldots, w_t C_x^t)$ and $D_y = \mathrm{diag}(D_y^1, \ldots, D_y^t)$. Then it can be seen that $P(x, y) = \mathtt{tr}(C_x D_y)$ for any $x \in [n]$, $y \in [m]$. Therefore, it holds that $\mathtt{rank}_{\mathtt{psd}}^{(k)}(P) \leq C^k(p)$. □

We now consider a specific example of this upper bound. Again we go back to the one in Eq.(3), and we already know that in this case $\mathtt{rank}_{\mathtt{psd}}^{(2^s)}(P) \leq 2^k$ according to our previous discussions, which is actually also what Eq.(8) implies in this example. This means that the amount of classical resources needed to perform a classical-quantum hybrid generating P is at most k bits. In the meantime, note that $\mathtt{rank}_{\mathtt{psd}}(P) = 2^{s+k}$, that is to say, a purely quantum scheme producing P needs a shared quantum state of size $s+k$ qubits. Therefore, it can be said that the k-bit classical resource involved in the classical-quantum protocol works quite efficiently, in the sense that it fulfills completely the task of the remaining k-qubit quantum resource in a purely quantum scheme.

However, this is not always the case: It is possible that the effect of one single qubit needs a large amount of classical resources to compensate! Before exhibiting such an example, we would like to remark that this can be regarded as another angle to reveal the remarkable advantage of quantum resources over classical resources in generating correlations. Our example will be based on *Euclidean distance matrices* that have been extensively studied [25]–[27].

Definition II.7 (Euclidean Distance Matrix): Given n distinct real numbers $c_1, \ldots, c_n$, the corresponding Euclidean distance matrix (EDM) is the $n \times n$ symmetric and nonnegative matrix $Q(c_1, \ldots, c_n)$ whose (i, j)-th entry $q_{i,j}$ is defined by

$$q_{ij} = (c_i - c_j)^2,\ i, j = 1, \ldots, n.$$

Fact II.8: [27] There exist n distinct real numbers $c_1, \ldots, c_n$ such that $\mathtt{rank}(Q_1) = 3, \mathtt{rank}_{\mathtt{psd}}(Q_1) = 2$ and $\mathtt{rank}_{+}(Q_1) \geq 2\sqrt{n} - 2$, where $Q_1 = Q(c_1, \ldots, c_n)$.

We choose such a Q_1 with $q_{i,j} > 0$ for any $i \neq j$, and let $\tilde{Q}_1 = Q_1/\|Q_1\|_1$, then $\tilde{Q}_1$ is a classical correlation with $\mathtt{rank}_{+}(\tilde{Q}_1) \geq 2\sqrt{n} - 2$. The above fact indicates that when generating $\tilde{Q}_1$, a quantum scheme enjoys remarkable advantage over any classical ones, as the cost of the former can be only one single qubit, while the latter needs classical resources of $\Omega(\log n)$ bits.

We now consider $\tilde{Q}_2 = \tilde{Q}_1 \otimes \tilde{Q}_1$, which is a classical correlation of size $n^2 \times n^2$, and similarly for any positive integer k, we define $\tilde{Q}_k = \tilde{Q}_1^{\otimes k}$. Since $\mathtt{rank}_{\mathtt{psd}}(A \otimes B) \leq \mathtt{rank}_{\mathtt{psd}}(A) \cdot \mathtt{rank}_{\mathtt{psd}}(B)$ for any nonnegative matrices A and B, we have that $\mathtt{rank}_{\mathtt{psd}}(\tilde{Q}_2) \leq 4$ (actually it is not hard to see that $\mathtt{rank}_{\mathtt{psd}}(\tilde{Q}_2) = 4$), thus a purely quantum scheme only needs a quantum seed of size 2 qubits to generate $\tilde{Q}_2$. To study classical-quantum hybrid protocols generating $\tilde{Q}_2$, we now assume that $s = 1$, i.e., our quantum capability is only one qubit, thus we cannot generate $\tilde{Q}_2$ using a purely quantum scheme directly. Then we turn to classical-quantum hybrid protocols to produce $\tilde{Q}_2$, and we are interested in the minimum classical resources needed. According to Theorem II.2, we have to estimate $\lceil \log_2 \mathtt{rank}_{\mathtt{psd}}^{(2)}(\tilde{Q}_2) \rceil$. We now prove the following conclusion.

Theorem II.9: $\mathtt{rank}_{\mathtt{psd}}^{(2)}(\tilde{Q}_2) \geq \log n$. As a consequence, when the quantum capability is only one qubit, a classical-quantum hybrid protocol needs at least $\Omega(\log\log n)$ bits of classical communication to sample $\tilde{Q}_2$.

Proof: Denote the (i, j)-entry of $\tilde{Q}_1$ by $\tilde{q}_{i,j}$, i.e., $\tilde{q}_{i,j} = \tilde{Q}_1(i, j)$. Then

$$\tilde{Q}_2 = \tilde{Q}_1 \otimes \tilde{Q}_1 = \begin{bmatrix} 0 & \tilde{q}_{1,2}\tilde{Q}_1 & \ldots & \tilde{q}_{1,n}\tilde{Q}_1 \\ \tilde{q}_{2,1}\tilde{Q}_1 & 0 & \ldots & \tilde{q}_{2,n}\tilde{Q}_1 \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{q}_{n,1}\tilde{Q}_1 & \tilde{q}_{n,2}\tilde{Q}_1 & \ldots & 0 \end{bmatrix}. \tag{9}$$

For the convenience of later discussion, we call $\tilde{q}_{i,j}\tilde{Q}_1$ the (i, j)-th block of $\tilde{Q}_2$ when $i \neq j$, and apparently for any $i \in [n]$ the (i, i)-th block is a zero matrix as $\tilde{q}_{i,i} = 0$. For any other matrix M with the same size $n^2 \times n^2$, we also use this term to address the corresponding submatrix of M with exactly the same position. Suppose $\tilde{Q}_2 = \sum_{k=1}^{r} P_k$, where P_k is a nonnegative matrix and $\mathtt{rank}_{\mathtt{psd}}(P_k) \leq 2$ for any $k \in [r]$. Then we need to prove that $r \geq \log n$.

Suppose $r < \log n$. We claim that for any $i \neq j$, there must be an integer $k_0 \in [r]$ such that the (i, j)-th block of P_{k_0} has PSD-rank 2. This can be proved as below. Suppose this is not the case, i.e., for any $k \in [r]$, the PSD-rank of the (i, j)-th block of P_k is 1, then according to the fact that for any PSD-rank-1 nonnegative matrix A it holds that $\mathtt{rank}_{+}(A) = 1$, the summation of the (i, j)-th blocks of all P_k has a nonnegative rank smaller than $\log n$. However, this summation is actually $\tilde{q}_{i,j}\tilde{Q}_1$, whose nonnegative rank is at least $2\sqrt{n} - 2$, much larger than $\log n$, which is a contradiction. Therefore, for any block, there exists $k \in [r]$ such that this block of P_k has PSD-rank 2.

We now fix an arbitrary $k \in [r]$, and focus on the blocks of P_k which have PSD-rank 2. Suppose the (i, j)-th and the (i', j')-th blocks, denoted $P_k^{(i,j)}$ and $P_k^{(i',j')}$, have PSD-rank 2, then it holds that [5]

$$\begin{aligned}&\texttt{rank}_{\texttt{psd}}\left(\begin{bmatrix} P_k^{(i,j)} & * \\ 0 & P_k^{(i',j')} \end{bmatrix}\right)\\ =&\texttt{rank}_{\texttt{psd}}\left(\begin{bmatrix} P_k^{(i,j)} & 0 \\ * & P_k^{(i',j')} \end{bmatrix}\right) = 4, \qquad (10)\end{aligned}$$

where the star can be any $n \times n$ nonnegative matrix. Since $\texttt{rank}_{\texttt{psd}}(P_k) = 2$, this means that the locations of the blocks of P_k with PSD-rank 2 have to be well-organized, and the patterns in Eq.(10) cannot exist. Let $A = \{i \in [n] : \exists j \in [n]$ such that the (i, j)-th block has PSD-rank 2$\}$, $B = \{j \in [n] : \exists i \in [n]$ such that the (i, j)-th block has PSD-rank 2$\}$, and call the set $A \times B$ a *position rectangle*. Then, it can be seen that this position rectangle covers all the positions of the blocks of P_k with PSD-rank 2. Note also that the position rectangle does not contain any diagonal blocks, since the observation given by Eq.(10) implies that $A \cap B = \emptyset$.

We now consider the corresponding position rectangles for all P_k. It can be seen that these rectangles may have overlap, but they need to cover all the off-diagonal blocks of $\tilde{Q}_2$, because of the fact that for each off-diagonal block there exists a $k_0 \in [r]$ such that the corresponding block of P_{k_0} has PSD-rank 2. Therefore, r should be at least the minimum number of monochromatic-1 rectangles needed to cover all the 1s in the communication matrix of the inequality function, which means $r \geq \log n$ [28]. This is contradicted by the assumption $r < \log n$. This completes the proof. □

Therefore, to compensate for a single-qubit shortage of quantum resource in generating $\tilde{Q}_2$, one has to consume classical resources of $\log \log n$ bits roughly. Note that here n could be any positive integer, making a sharp difference from the example in Eq.(3).

Although we do not know whether the bound in Theorem II.9 is optimal, we can strengthen this conclusion in the following different ways. Indeed, the first corollary below shows that when n is large, even if the quantum capability is qutrit, i.e., only one dimension smaller than 2 qubits, any classical-quantum hybrid protocol that produces $\tilde{Q}_2$ still needs a large amount of classical resources.

Corollary II.10: $\texttt{rank}_{\texttt{psd}}^{(3)}(\tilde{Q}_2) \geq \log n$.

Proof: The proof is almost the same as the previous theorem, except that now the blocks $P_k^{(i,j)}$ and $P_k^{(i',j')}$ introduced above can have PSD-rank 2 or 3, but the patterns in Eq.(10) still cannot exist. Therefore, the proof still works. □

At the same time, the following corollary implies that for any positive integer k, there always exist classical correlations P such that the cost of a purely quantum scheme to sample P is k qubits, but if the quantum capacity is $k-1$ qubits, i.e., a shortage of one single qubit for a purely quantum scheme, then in any classical-quantum hybrid protocol sampling P a large amount of classical resources have to be needed.

Corollary II.11: For any positive integer $k \geq 2$, $\texttt{rank}_{\texttt{psd}}^{(2^{k-1})}(\tilde{Q}_k) \geq \log n$.

Proof: We prove it by induction. First, according to Theorem II.9, we know that it is true when $k = 2$. We suppose it holds when $k = i_0$, i.e., $\texttt{rank}_{\texttt{psd}}^{(2^{i_0-1})}(\tilde{Q}_{i_0}) \geq \log n$, and we now focus on $\texttt{rank}_{\texttt{psd}}^{(2^{i_0})}(\tilde{Q}_{i_0+1})$. Since $\tilde{Q}_{i_0+1}$ can be expressed in a similar way as Eq.(9), for convenience we also use the term of the (i, j)-th block to address the corresponding submatrix, except that now it is not $\tilde{q}_{i,j}\tilde{Q}_1$, but $\tilde{q}_{i,j}\tilde{Q}_{i_0}$. Again we suppose $\tilde{Q}_{i_0+1} = \sum_{k=1}^{r} P_k$, where P_k is a nonnegative matrix and $\texttt{rank}_{\texttt{psd}}(P_k) \leq 2^{i_0}$ for any $k \in [r]$. And we need to prove that $r \geq \log n$.

Suppose $r < \log n$. Then for any $i \neq j$, there must be an integer $k_0 \in [r]$ such that the (i, j)-th block of P_{k_0}, denoted $P_{k_0}^{(i,j)}$, has PSD-rank larger than 2^{i_0-1}. If this is not true, then $\sum_{k=1}^{r} P_k^{(i,j)}$, which is actually $\tilde{q}_{i,j}\tilde{Q}_{i_0}$, can be a summation of $r < \log n$ nonnegative matrices with each having PSD-rank not larger than 2^{i_0-1}, contradicted with the assumption that $\texttt{rank}_{\texttt{psd}}^{(2^{i_0-1})}(\tilde{Q}_{i_0}) \geq \log n$.

Then again we fix a $k \in [r]$ and look at the blocks of P_k with PSD-rank larger than 2^{i_0-1}. By a similar observation as Eq.(10), we know that these special blocks of P_k also appear in a similar pattern as the blocks with PSD-rank 2 in the decomposition of $\tilde{Q}_2$, and their positions can also be covered by a position rectangle. Therefore, a similar argument proves that we must have $r \geq \log n$. □

In fact, according to the above proof, we can generalize the conclusion in Corollary 2.2 further, which may have independent interests.

Corollary II.12: Assume M is an $n \times n$ nonnegative matrix such that $M_{ii} = 0$ for any $i \in [n]$ and $M_{ij} > 0$ for any $i \neq j$. Then for any positive integer $k \geq 2$, it holds that $\texttt{rank}_{\texttt{psd}}^{(2^{k-1})}(M^{\otimes k}) \geq \log n$.

Note that when the nonnegative matrix M satisfies that $M_{ii} = 0$ for any $i \in [n]$ and $M_{ij} > 0$ for any $i \neq j$, we must have that $\texttt{rank}_{+}(M) \geq \log n$ [29], which is necessary to apply the technique in Theorem II.9.

Clearly, the above facts reveal the rich mathematical structure of classical-quantum hybrid protocols and k-block positive semi-definite rank.

B. The Quantum-Classical Hybrid

In classical-quantum hybrid protocols, the major restriction on exploiting quantum power is the size of available quantum states. Within the quantum capability, we have the freedom to control and manipulate any quantum state whenever we need it. Particularly, when producing a classical correlation, with respect to the classical sampling result i in the first stage, we are able to ask for any corresponding quantum state ρ_i. However, sometimes this kind of freedom is still expensive to us. For this, we now consider a new hybrid protocol with more rigorous restrictions, that is, only one quantum state independent of classical messages is available for the players, and thus the classical-quantum hybrid protocols introduced above do not work any more. Since the quantum state available is fixed (independent of the involved classical resource), we can choose its preparation as the first action, and hence call the new protocol a *quantum-classical hybrid* one.

Suppose we need to generate a target classical correlation P, and the only quantum state provided has size s with $s < \lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P) \rceil$. Then one may think of utilizing it in the following natural way. Based on the shared state, Alice and Bob produce a classical correlation P'. After sampling x' and y' according to P', both of them make two proper local classical samplings accordingly, which generate their outputs x and y, hoping that the final output is exactly distributed corresponding to the target P. However, it can be argued that, this is not possible in general. Indeed, since the second stage is a classical local sampling for each party, each operation can be regarded as a special form of local quantum operations. Therefore, each party can merge this special local quantum operation into the local quantum operation he/she performs when producing P', resulting in a valid composite quantum operation. Then if the above protocol is possible, based on the original seed quantum state of size s, Alice and Bob are able to generate P directly by local quantum operations, which indicates $s \geq \lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P) \rceil$, leading to a contradiction.

Due to this observation, one may wonder, with such a rigorous restriction on the quantum resource available, whether or not quantum can make essential contributions in this task? It turns out that the answer to this question is again affirmative. To explain why this is the case, we first recall two useful facts.

First, if we choose all bipartite quantum states ρ_i involved in a classical-quantum hybrid protocol to be pure, we still have the same power in generating classical correlations, even if the quantum capability is unchanged [30]. Second, we also need the following well-known result by Nielsen.

Fact II.13: [31] $|\Psi\rangle$ and $|\Phi\rangle$ are two $d \times d$ bipartite pure quantum states, and λ_Ψ and λ_Φ are the vectors of their squared Schmidt coefficients respectively. Then $|\Psi\rangle$ can be transformed to $|\Phi\rangle$ using local operations and classical communication (LOCC) if and only if λ_Ψ is majorized by λ_Φ.

Suppose $\lambda_\Psi = (\lambda_{\Psi,1}, \ldots, \lambda_{\Psi,d})$ and $\lambda_\Phi = (\lambda_{\Phi,1}, \ldots, \lambda_{\Phi,d})$ are real d-dimensional vectors. We say λ_Ψ is majorized by λ_Φ if for any $k \in [d]$, i.e.,

$$\sum_{i=1}^{k} \lambda^{\downarrow}_{\Psi,i} \leq \sum_{i=1}^{k} \lambda^{\downarrow}_{\Phi,i},$$

with equality holding when $k = d$, and here the ↓ indicates the descending order of the entries.

For example, if Alice and Bob share s Einstein-Podolsky-Rosen (EPR) pairs, i.e., a pair of qubits which are in a maximally entangled state, then as a whole bipartite pure state the corresponding vector of Schmidt coefficients is $\lambda_{s-EPR} = (2^{-s}, 2^{-s}, \ldots, 2^{-s})$. Then, for any $2^s \times 2^s$ pure quantum state $|\Phi\rangle$, it is easy to check that λ_{s-EPR} is majorized by λ_Φ.

With the above two facts, we can design a quantum-classical hybrid protocol to generate a target classical correlation P as below. Suppose that an optimal classical-quantum hybrid protocol that generates P corresponds to a decomposition $P = \sum_{i \in I} p_i P_i$, and for any $i \in I$, P_i can be produced quantumly using a bipartite quantum state ρ_i within quantum capability s. According to the above discussion, we can assume that all ρ_i are pure. Then in a quantum-classical hybrid protocol, Alice and Bob first share s EPR pairs, which is within quantum capability. Next, they sample an integer $i \in I$ classically with respect to the distribution $\{p_i\}$. After obtaining the shared i, they transform the s EPR pairs into ρ_i using LOCC. According to Fact II.13, this can be fulfilled with certainty, though needs some classical communication. Then they are able to sample P_i by performing local quantum operations on ρ_i. It is not hard to see that the overall output will be exactly a sampling of P, as in a classical-quantum hybrid protocol.

It can be seen that the resources consumed in a quantum-classical hybrid protocol are quite similar to those in the corresponding classical-quantum hybrid protocol, except some extra classical communication is needed in the part that transforms s EPR pairs into ρ_i, which turns out to be at most $2^s - 1$ bits [31]. Therefore, we have the following conclusion.

Proposition II.14: Suppose P is a classical correlation with $\mathtt{rank}_{\mathtt{psd}}(P) > 2^s$, where s is the quantum capability. Then the classical communication needed in a quantum-classical hybrid protocol to sample P is at most $\lceil \log_2 \mathtt{rank}^{(2^s)}_{\mathtt{psd}}(P) \rceil + 2^s - 1$ bits.

Consider the facts that for state-of-the-art technologies s is still quite small, and that classical communication is relatively cheap, the performance of a quantum-classical hybrid protocol is comparable with that of the corresponding classical-quantum protocol, though it suffers from more rigorous restriction to access quantum resources.

III. The Advantage of Shared Entanglement Over Shared Randomness in Communication Complexity

As mentioned in the Introduction, in communication complexity theory a fundamental open problem is to exhibit and prove the advantage of shared entanglement over shared randomness in computing Boolean functions. Though hybrid protocols for generating classical correlations deal with a different and simpler task, it turns out that they provide us an angle to look into the advantage of shared entanglement over shared randomness in communication protocols.

For this, we now consider and compare the following two specific settings that sample a classical correlation P. In the two settings, Alice and Bob first share two different computational resources of the same size (number of bits or qubits) respectively: one is entangled quantum state, and the other is public randomness. We set the amount of shared resources in such a way that to fulfill the task, they may need more computational resources, which we supposed to be quantum communication. Therefore, we can see that one of the two settings is actually a purely quantum protocol, while the other is a classical-quantum hybrid protocol. We compare the amount of quantum communication needed in the second stage. Clearly, this is a reasonable way to compare the computational power of the shared entanglement and public randomness involved in the first stage.

More specifically, suppose $P \in \mathbb{R}_+^{n \times m}$ is the target classical correlation. And we let the common size of the initially shared resources be $\lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P) \rceil$ bits or qubits. Then in the purely quantum protocol, the quantum communication needed in the second stage is zero, as the shared quantum state in the first stage is already sufficient to sample P. As a result, to compare the two settings, the remaining problem is estimating how much quantum communication is needed in classical-quantum hybrid protocols. For convenience, we denote this quantity by t qubits.

We immediately have two trivial lower and upper bounds for t. First, if $\mathtt{rank}_{\mathtt{psd}}(P) < \mathtt{rank}_+(P)$, which is usually the case, then $t > 0$. Second, Alice and Bob can choose to throw away the shared randomness and generate P from scratch in the second stage, and the corresponding cost is $\lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P) \rceil$ qubits. Therefore, it holds that

$$t \leq \lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P) \rceil. \tag{11}$$

Actually, we can prove the following result, which provides a nontrivial lower bound for t.

Lemma III.1: In a classical-quantum hybrid protocol that generates $P \in \mathbb{R}_+^{n\times m}$, suppose the costs of the first and the second stages are c bits and s qubits respectively. Then it holds that

$$2s + c \geq \lceil \log_2 \mathtt{rank}(P) \rceil. \tag{12}$$

Proof: According to the structures of classical-quantum hybrid protocols, we have $P = \sum_{i=1}^{2^c} P_i$, and $\mathtt{rank}_{\mathtt{psd}}(P_i) \leq 2^s$ for any $i \in [2^c]$. Then using the relation $\mathtt{rank}_{\mathtt{psd}}(A) \geq \sqrt{\mathtt{rank}(A)}$ for any nonnegative matrix A, it holds that $\mathtt{rank}(P_i) \leq 2^{2s}$. In the meantime, we also have that

$$\mathtt{rank}(P) \leq \sum_{i=1}^{2^c} \mathtt{rank}(P_i) \leq 2^{2s+c}, \tag{13}$$

which concludes the proof. □

Recall that in our setting we set c to be $\lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P) \rceil$, hence the above lemma implies the following fact.

Corollary III.2:

$$t \geq \frac{1}{2}\left(\lceil \log_2 \mathtt{rank}(P) \rceil - \lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P) \rceil\right). \tag{14}$$

Note that there exists nontrivial nonnegative matrices P such that $\mathtt{rank}_{\mathtt{psd}}(P) = \sqrt{\mathtt{rank}(P)}$ [32]. If we choose such P as our target classical correlation, the result given by Corollary III.2 is actually

$$t \geq \frac{1}{2}\lceil \log_2 \mathtt{rank}_{\mathtt{psd}}(P) \rceil - \frac{1}{2}. \tag{15}$$

This indicates that the trivial upper bound in Eq.(11) can be tight up to a factor of $1/2$.

IV. Conclusion

Motivated by the fact that the scale of near-term quantum computing is quite limited, in this paper we propose two kinds of hybrid protocols that combine classical power and quantum power to generate large-scale classical correlations. By looking into the connections between these two models, we show that their performances are close, thus we can choose to focus on the more flexible one of them, i.e., the model of classical-quantum hybrid protocols. Particularly, we show that this kind of protocol can be fully characterized by the concepts of k-block positive semi-definite rank and k-block positive semi-definite factorization. By specific examples, we show that hybrid protocols have rich mathematical structures, which, from two different viewpoints, indicate the remarkable quantum advantage in generating classical correlations. Indeed, we witness the cases where in order to compensate for a shortage of one single qubit, a large amount of classical resources have to be consumed. Meanwhile, by comparing two specific settings with the same amount but different kinds of beforehand shared resources, we may gain a better understanding of the different power of shared entanglement and public randomness in communication complexity theory.

Acknowledgment

The authors thank Xun Gao and Zhengfeng Ji for helpful comments.

References

[1] S. Zhang, “Quantum strategic game theory,” in *Proc. 3rd Innov. Theor. Comput. Sci. Conf. (ITCS)*, 2012, pp. 39–59.

[2] R. Jain, Y. Shi, Z. Wei, and S. Zhang, “Efficient protocols for generating bipartite classical distributions and quantum states,” *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 5171–5178, Aug. 2013.

[3] R. Jain, Z. Wei, P. Yao, and S. Zhang, “Multipartite quantum correlation and communication complexities,” *Comput. Complex.*, vol. 26, p. 199, Mar. 2017.

[4] S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary, and R. de Wolf, “Linear vs. semidefinite extended formulations: Exponential separation and strong lower bounds,” in *Proc. 44th Symp. Theory Comput. (STOC)*, 2012, pp. 95–106.

[5] H. Fawzi, J. Gouveia, P. A. Parrilo, R. Z. Robinson, and R. R. Thomas, “Positive semidefinite rank,” *Math. Program.*, vol. 153, no. 1, pp. 133–177, Oct. 2015.

[6] F. Arute *et al.*, “Quantum supremacy using a programmable superconducting processor,” *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[7] J. Preskill, “Quantum computing in the NISQ era and beyond,” *Quantum*, vol. 2, p. 79, Aug. 2018.

[8] H. Fawzi, “On representing the positive semidefinite cone using the second-order cone,” *Math. Program.*, vol. 175, nos. 1–2, pp. 109–118, May 2019.

[9] G. Averkov, “Optimal size of linear matrix inequalities in semidefinite approaches to polynomial optimization,” *SIAM J. Appl. Algebra Geometry*, vol. 3, no. 1, pp. 128–151, Jan. 2019.

[10] J. Saunderson, “Limitations on the expressive power of convex cones without long chains of faces,” *SIAM J. Optim.*, vol. 30, no. 1, pp. 1033–1047, Jan. 2020.

[11] Y. S. Soh and A. Varvitsiotis, “A non-commutative extension of Lee-Seung’s algorithm for positive semidefinite factorizations,” 2021, *arXiv:2106.00293*.

[12] E. Chitambar and G. Gour, “Quantum resource theories,” *Rev. Mod. Phys.*, vol. 91, Apr. 2019, Art. no. 025001. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.91.025001

[13] M.-H. Hsieh and M. M. Wilde, “Trading classical communication, quantum communication, and entanglement in quantum Shannon theory,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4705–4730, Sep. 2010.

[14] M.-H. Hsieh and M. M. Wilde, “Entanglement-assisted communication of classical and quantum information,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4682–4704, Sep. 2010.

[15] A. C.-C. Yao, “Quantum circuit complexity,” in *Proc. IEEE 34th Annu. Found. Comput. Sci.*, Nov. 1993, pp. 352–361.

[16] D. Gavinsky, “Bare quantum simultaneity versus classical interactivity in communication complexity,” in *Proc. 52nd Annu. ACM SIGACT Symp. Theory Comput.*, New York, NY, USA, Jun. 2020, p. 401, doi: 10.1145/3357713.3384243.

[17] T. Lee and A. Shraibman, *Lower Bounds in Communication Complexity*. Hanover, MA, USA: Now, 2009.

[18] I. Newman, “Private vs. common random bits in communication complexity,” *Inf. Process. Lett.*, vol. 39, no. 2, pp. 67–71, 1991. [Online]. Available: http://www.sciencedirect.com/science/article/pii/002001909190157D

[19] R. Cleve and H. Buhrman, "Substituting quantum entanglement for communication," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 2, pp. 1201–1204, Aug. 1997.

[20] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, p. 1895, Mar. 1993.

[21] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, "MIP*=RE," 2020, *arXiv:2001.04383*.

[22] L. Babai, L. Fortnow, and C. Lund, "Nondeterministic exponential time has two-prover interactive protocols," in *Proc. 31st Annu. Symp. Found. Comput. Sci.*, vol. 1, Oct. 1990, pp. 16–25.

[23] J. Gouveia, P. A. Parrilo, and R. R. Thomas, "Lifts of convex sets and cone factorizations," *Math. Oper. Res.*, vol. 38, no. 2, pp. 248–264, May 2013.

[24] A. C.-C. Yao, "Some complexity questions related to distributive computing (preliminary report)," in *Proc. 11th Annu. ACM Symp. Theory Comput. (STOC)*, 1979, pp. 209–213.

[25] M. M. Lin and M. T. Chu, "On the nonnegative rank of Euclidean distance matrices," *Linear Algebra Appl.*, vol. 433, no. 3, pp. 681–689, Sep. 2010.

[26] P. Hrubeš, "On the nonnegative rank of distance matrices," *Inf. Process. Lett.*, vol. 112, no. 11, pp. 457–461, Jun. 2012.

[27] Y. Shitov, "Euclidean distance matrices and separations in communication complexity theory," *Discrete Comput. Geometry*, vol. 61, no. 3, pp. 653–660, Apr. 2019.

[28] E. Kushilevitz and N. Nisan, *Communication Complexity*. Cambridge, U.K.: Cambridge Univ. Press, 1997.

[29] S. Fiorini, V. Kaibel, K. Pashkovich, and D. O. Theis, "Combinatorial bounds on nonnegative rank and extended formulations," *Discrete Math.*, vol. 313, no. 1, pp. 67–83, Jan. 2013.

[30] J. Sikora, A. Varvitsiotis, and Z. Wei, "Minimum dimension of a Hilbert space needed to generate a quantum correlation," *Phys. Rev. Lett.*, vol. 117, no. 6, Aug. 2016, Art. no. 060401.

[31] M. A. Nielsen, "Conditions for a class of entanglement transformations," *Phys. Rev. Lett.*, vol. 83, no. 2, p. 436, 1999.

[32] T. Lee, Z. Wei, and R. de Wolf, "Some upper and lower bounds on PSD-rank," *Math. Program.*, vol. 162, nos. 1–2, pp. 495–521, Mar. 2017.

Xiaodie Lin received the B.Eng. degree from Sun Yat-sen University, Guangdong, China, in 2019. She is currently pursuing the Ph.D. degree with the Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China. Her research interests include quantum information, quantum computation, and computational complexity.

Zhaohui Wei received the Ph.D. degree in computer science from Tsinghua University, Beijing, China, in 2009. Before he joined the Institute for Interdisciplinary Information Sciences, Tsinghua University, as an Assistant Professor, in 2018, he worked with the Centre for Quantum Technologies, Singapore, as a Research Fellow. In 2021, he moved to the Yau Mathematical Sciences Center, Tsinghua University. His research interests include quantum information theory, computational complexity, communication complexity, and quantum foundations.

Penghui Yao received the Ph.D. degree in computer science from the Centre for Quantum Technologies (CQT), National University of Singapore, in 2013. He spent one year at CQT as a Research Associate, one year at the Centrum Wiskunde and Informatica, The Netherlands, as a Post-Doctoral Researcher, one year at the Institute for Quantum Computing, University of Waterloo, Waterloo, ON, Canada, as a Post-Doctoral Researcher, and one and a half years at the Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD, USA, as a Hartree Post-Doctoral Fellow. He is currently an Associate Professor with the Department of Computer Science, Nanjing University, China. His research interests include communication complexity, information theory, computational complexity, and Fourier analysis.