• 量子信息专栏 •

经典、量子及其混合场景下的经典关联生成协议

林小蝶[1]，魏朝晖[2,3*]

(1. 清华大学交叉信息研究院 北京 海淀区 100084；2. 清华大学丘成桐数学科学中心 北京 海淀区 100084；
3. 北京雁栖湖应用数学研究院 北京 海淀区 100084)

【摘要】在信息处理任务中，多方共享的随机变量和量子纠缠都是重要的计算资源，其中共享的随机变量也被称为经典关联。经典关联生成问题研究的是生成目标关联所需消耗的最少随机性或量子纠缠的数量。该文综述性地介绍了在经典场景、量子场景以及经典、量子混合场景下的经典关联生成协议。其中，非负秩和半正定秩分别刻画了生成目标关联所需共享的最少随机性与量子纠缠的量。基于这一结果，事先共享量子纠缠相比于事先共享随机性展示出了指数级优势。考虑到近期可实现的量子设备规模有限，经典、量子混合场景下的经典关联生成协议是一个现实的选择。在可操控的量子系统大小有限的前提之下，可用k区块半正定秩来量化完成经典关联生成任务所需通讯的最少经典比特。在这一混合协议中，量子资源仍能表现出相对经典资源而言的巨大优越性。由此可见，经典关联生成问题提供了一个新的视角来对比量子资源和经典资源之间的差别。

关 键 词 通讯复杂度； 关联复杂度； 关联生成； 混合协议； 量子优势
中图分类号 TN911.2 **文献标志码** A doi:10.12178/1001-0548.2022187

Classical, Quantum and Quantum-Classical Hybrid Protocols for Generating Classical Correlations

LIN Xiaodie[1] and WEI Zhaohui[2,3*]

(1. Institute for Interdisciplinary Information Sciences, Tsinghua University Haidian Beijing 100084;
2. Yau Mathematical Sciences Center, Tsinghua University Haidian Beijing 100084;
3. Yanqi Lake Beijing Institute of Mathematical Sciences and Applications Haidian Beijing 100084)

Abstract Shared randomness and quantum entanglement are important resources for many information processing tasks, where the former is also called classical correlation. In the classical correlation generation problem, we study the minimum amount of shared randomness or quantum entanglement needed to produce a target classical correlation. Here we review classical protocol, quantum protocol, and classical and quantum hybrid protocols for generating classical correlations. First, in classical protocol and quantum protocol the minimum amount of shared randomness and quantum entanglement required are characterized by nonnegative rank and positive semidefinite rank, respectively. Based on these results, sharing prior quantum entanglement shows exponentially advantage over sharing prior randomness in such a task. Second, since it is hard to access large-scale quantum system in the near future, classical-quantum hybrid protocol is also introduced to produce large scale classical correlations. When the size of manipulable quantum systems is limited, the minimum amount of extra classical resources needed to generate a target classical correlation is characterized by the concept of k-block positive semidefinite rank. In classical-quantum hybrid protocols, it turns out that quantum resources still enjoy huge advantages over classical resources. Therefore, the classical correlation generation problem provides a new insight to compare the computational power of quantum and classical resources.

Key words communication complexity; correlation complexity; correlation generation; hybrid protocol; quantum advantage

在信息处理任务中，分隔各地的不同参与方常常需要协同完成计算任务。在这一过程中，多方之间共享计算资源往往是不可或缺的，如随机变量或量子纠缠，其中前者也被称作经典关联 (classical

收稿日期：2022－06－13；修回日期：2022－09－27
基金项目：国家自然科学基金重点项目 (61832015)；科技部重点研发计划 (2018YFA0306703，2021YFE0113100)
作者简介：林小蝶 (1996－)，女，博士生，主要从事量子信息、通讯复杂度方面的研究.
*通信作者：魏朝晖，E-mail：weizhaohui@gmail.com

correlation)。因此，如何高效地制备这些共享计算资源是一个重要问题。本文将介绍近期在经典关联生成这一任务上的一系列进展。经典关联生成问题主要研究的是：为了生成一个目标共享经典关联，最少需要涉及多少数量的初始共享随机性或者量子纠缠？本文主要讨论两方参与的情形，并将介绍经典场景、量子场景以及量子、经典混合场景下的经典关联生成协议[1-3]。

考虑这样一个具体的场景：分隔两地的 Alice 和 Bob 二人想要从目标经典关联$\boldsymbol{P}=(X,Y)$中进行采样，即二人各自输出随机变量X和Y，使得(X,Y)的联合概率分布与$\boldsymbol{P}$完全一致。那么，对于一个任意的经典关联$\boldsymbol{P}$，如何刻画生成其所需要的最小代价？

关联复杂度 (correlation complexity) 和通讯复杂度 (communication complexity) 是与此相关的两个量。对于两体的共享经典随机变量$\boldsymbol{P}'=(X',Y')$，可将其大小size$(\boldsymbol{P}')$定义为$(\lceil\log_2\mathcal{X}\rceil+\lceil\log_2\mathcal{Y}\rceil)/2$，其中$\mathcal{X}$和$\mathcal{Y}$分别是随机变量$X'$和$Y'$采样集合的大小；对于两体的量子态$\sigma\in\mathcal{H}_A\otimes\mathcal{H}_B$，其大小size$(\sigma)$则定义为$(\lceil\log_2 D_A\rceil+\lceil\log_2 D_B\rceil)/2$，其中$D_A$和$D_B$分别对应希尔伯特空间 (Hilbert space)$\mathcal{H}_A$和$\mathcal{H}_B$的维度。对于经典关联生成问题，Alice 和 Bob 可以共享一个关联种子$\boldsymbol{P}'=(X',Y')$，并且每个人都可以在自己的系统上进行本地操作 (local operation, LO) 以最终生成目标经典关联$\boldsymbol{P}$。称$\boldsymbol{P}$的随机关联复杂度 (randomized correlation complexity) 为最小的size$(\boldsymbol{P}')$，记作$R(\boldsymbol{P})$。若 Alice 和 Bob 共享的是量子态σ，并且他们通过在自己的系统上进行本地量子操作，最终通过量子测量成功生成目标经典关联$\boldsymbol{P}$。那么称$\boldsymbol{P}$的量子关联复杂度 (quantum correlation complexity) 为最小的size(σ)，记作$Q(\boldsymbol{P})$。

除了共享关联种子以外，Alice 和 Bob 还可以利用通讯的方式来生成目标经典关联$\boldsymbol{P}$。在协议的一开始，Alice 和 Bob 并不共享任何资源，而是在协议的执行过程中通过进行相互间的通讯，最终协同生成目标经典关联$\boldsymbol{P}$。若 Alice 和 Bob 进行的是经典通讯，则称$\boldsymbol{P}$的随机通讯复杂度 (randomized communication complexity) 为二者交换的最少比特数，记作RComm$(\boldsymbol{P})$；若 Alice 和 Bob 进行的是量子通讯，则称$\boldsymbol{P}$的量子通讯复杂度 (quantum communication complexity) 为二者交换的最少量子比特数，记作QComm$(\boldsymbol{P})$。有研究结果证明，对于任意的量子态ρ，其量子关联复杂度和量子通讯复杂度总是相等的，也即$Q(\boldsymbol{P})=\mathrm{QComm}(\boldsymbol{P})$且$R(\boldsymbol{P})=\mathrm{RComm}(\boldsymbol{P})$[1]。因此，下文将直接使用$R$和$Q$的记号，不对关联复杂度和通讯复杂度进行严格的区分。

1　预备知识

给定自然数n，$[n]$表示集合$\{1,2,\cdots,n\}$。矩阵$\boldsymbol{A}=[\boldsymbol{A}(x,y)]$表示其$x$行$y$列的元素为$\boldsymbol{A}(x,y)$。对于矩阵$\boldsymbol{A}$，$\boldsymbol{A}^{\mathrm{T}}$表示其转置，$\boldsymbol{A}^{\dagger}$表示其共轭转置。若矩阵$\boldsymbol{A}$满足性质$\boldsymbol{A}^{\dagger}=\boldsymbol{A}$，则称$\boldsymbol{A}$为厄米特 (Hermitian) 矩阵。若一个厄米特阵$\boldsymbol{A}$的所有特征值都是非负的，则称$\boldsymbol{A}$为半正定 (positive semidefinite, PSD) 矩阵。

对任意非负矩阵$\boldsymbol{P}\in\mathbb{R}_+^{n\times m}$, $\mathrm{rank}_+(\boldsymbol{P})$为$\boldsymbol{P}$的非负秩 (nonnegative rank)，其定义为使得$\boldsymbol{P}$能分解为r个秩 (rank) 为 1 的非负矩阵的最小r。此外，$\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P})$为$\boldsymbol{P}$的半正定秩 (PSD-rank)。若$\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P})$为$r$，则存在半正定矩阵$\boldsymbol{C}_x,\boldsymbol{D}_y\in\mathbb{C}^{r\times r}$满足$\boldsymbol{P}(x,y)=\mathrm{tr}(\boldsymbol{C}_x\boldsymbol{D}_y)$，且$r$是满足这一半正定分解的最小值[4-5]。对于$\boldsymbol{P}$的$k$区块半正定秩 ($k$-block PSD-rank)，它是半正定秩的扩展，记作$\mathrm{rank}_{\mathrm{psd}}^{(k)}(\boldsymbol{P})$。若$\mathrm{rank}_{\mathrm{psd}}^{(k)}(\boldsymbol{P})$为$r$，则存在半正定矩阵$\boldsymbol{C}_x=\mathrm{diag}(\boldsymbol{C}_x^1,\boldsymbol{C}_x^2\cdots,\boldsymbol{C}_x^r),\boldsymbol{D}_y=\mathrm{diag}(\boldsymbol{D}_y^1,\boldsymbol{D}_{y,}^2\cdots,\boldsymbol{D}_y^r)\in\mathbb{C}^{kr\times kr}$满足：

$$\boldsymbol{P}(x,y)=\mathrm{tr}(\boldsymbol{C}_x\boldsymbol{D}_y)=\sum_{l=1}^{r}\mathrm{tr}(\boldsymbol{C}_x^l\boldsymbol{D}_y^l)$$

式中，$\boldsymbol{C}_x^l,\ \boldsymbol{D}_y^l\in\mathbb{C}^{k\times k}$。要求$r$是满足这一$k$区块半正定分解的最小值[6-9]。

作用在希尔伯特空间$\mathcal{H}$上的量子态ρ是迹 (trace) 为 1 的半正定算子。若该算子秩为 1，则其为纯态，可写作$\rho=|\psi\rangle\langle\psi|$，其中$|\psi\rangle$是模为 1 的向量。对于量子态$\rho\in\mathcal{H}_A$，$|\psi\rangle\in\mathcal{H}_A\otimes\mathcal{H}_B$，若有$\mathrm{tr}_{\mathcal{H}_B}(|\psi\rangle\langle\psi|)=\rho$，则称$|\psi\rangle$是$\rho$的一个纯化 (purification)。其中，$\mathrm{tr}_{\mathcal{H}_B}$代表在$\mathcal{H}_B$空间上的部分迹 (partial trace)。对任意的量子态而言，总可以对其进行纯化操作。

对于任意的两体纯态$|\psi\rangle_{AB}$，总存在$\mathcal{H}_A,\mathcal{H}_B$上的标准正交基$\{|i_A\rangle\},\{|i'_B\rangle\}$使得$|\psi\rangle_{AB}=\sum_i\sqrt{p_i}|i_A\rangle\otimes|i'_B\rangle$。其中$p_i$为非负实数，满足$\sum_i p_i=1$。该分解为施密特分解 (Schmidt decomposition)，$\sqrt{p_i}$为施密特系数 (Schmidt coefficient)，非零施密特系数的数目定义为施密特秩 (Schmidt rank)，记作$\mathrm{S-rank}(|\psi\rangle)$。更详细的量子信息基础介绍可参考文献 [10]。

2　经典场景

在经典场景中，Alice 和 Bob 通过仅共享关联

种子$\boldsymbol{P}'=(X',Y')$或仅进行经典通讯，并在各自拥有的子系统上进行本地操作，使得二人最终输出的联合概率分布(X,Y)与目标经典关联$\boldsymbol{P}$一致。文献 [1] 将这一任务所需的最小代价，即所需的最小 size$(\boldsymbol{P}')$或所交换的最少比特数，与$\mathrm{rank}_+(\boldsymbol{P})$建立了联系，并给出了$R(\boldsymbol{P})=\lceil\log_2\mathrm{rank}_+(\boldsymbol{P})\rceil$这一精确刻画。下文给出简要的证明思路。

根据$\mathrm{rank}_+(\boldsymbol{P})$的定义，可将经典关联$\boldsymbol{P}$分解为$\boldsymbol{P}_{x,y}=\sum_{i=1}^{r}q_i\boldsymbol{a}_i(x)\boldsymbol{b}_i(y)$，其中$\{q_i\},\boldsymbol{a}_i,\boldsymbol{b}_i$均为概率分布，且$r=\mathrm{rank}_+(\boldsymbol{P})$。则 Alice 和 Bob 可通过从共享的$\{q_i\}$中采样$i$，然后各自从$\boldsymbol{a}_i,\boldsymbol{b}_i$中采样$x,y$，并将其输出。由于其输出$(x,y)$的概率与$\boldsymbol{P}_{x,y}$一致，则说明$R(\boldsymbol{P})\leqslant\lceil\log_2\mathrm{rank}_+(\boldsymbol{P})\rceil$。

对于$R(\boldsymbol{P})$的下界，考虑二者进行经典通讯的场景，即尝试证明$\lceil\log_2\mathrm{rank}_+(\boldsymbol{P})\rceil\leqslant\mathrm{RComm}(\boldsymbol{P})$。假设经典关联$\boldsymbol{P}$是通过$r$轮的通讯协议$\boldsymbol{M}=(M_1,M_2,\cdots,M_r)$生成的，其中随机变量$M_i$是第$i$轮传输的信息。Alice 和 Bob 各自拥有私有随机变量r_A和r_B，不失一般性，假设由 Alice 开始传输信息M_1。则有：

$$\begin{aligned}\boldsymbol{P}(x,y)=&\sum_m\Pr_{r_A,r_B}[M=m]\\&\Pr_{r_A,r_B}[X=x,Y=y|M=m]\end{aligned}\tag{1}$$

将$\Pr_{r_A,r_B}[M=m]$展开，即为：

$$\begin{aligned}&\Pr_{r_A,r_B}[M=m]=\\&\Pr_{r_A}[M_1=m_1]\Pr_{r_B}[M_2=m_2|M_1=m_1]\times\\&\cdots\Pr[M_r=m_r|M_1\cdots M_{r-1}=m_1\cdots m_{r-1}]\end{aligned}\tag{2}$$

这里最后的概率是基于r_A还是基于r_B取决于最后一轮由谁通讯。此外，由于给定信息m后，Alice 和 Bob 的输出是相互独立的，条件概率为：

$$\begin{aligned}&\Pr_{r_A,r_B}[X=x,Y=y|M=m]=\\&\Pr_{r_A}[X=x|M=m]\Pr_{r_B}[Y=y|M=m]\end{aligned}\tag{3}$$

将式 (2) 和式 (3) 代入式 (1)，整理可得：

$$\begin{aligned}&\boldsymbol{P}(x,y)=\\&\sum_m\left(\Pr_{r_A}[X=x|M=m]\prod_{i\in[r]:\mathrm{odd}}\Pr_{r_A}[M_i=m_i|M_{i-1}=m_{i-1}]\right)\times\\&\left(\Pr_{r_B}[Y=y|M=m]\prod_{i\in[r]:\mathrm{even}}\Pr_{r_B}[M_i=m_i|M_{i-1}=m_{i-1}]\right)\end{aligned}$$

给定m，第一个括号中的乘积项只与x有关，第二个括号中的乘积项只与y有关，因此每一个求和项对应一个秩为 1 的矩阵。此外，由于矩阵中的元素对应概率的乘积，因此该矩阵为非负矩阵。换句话说，可以将$\boldsymbol{P}$分解为2^c项秩为 1 的非负矩阵之和，c为传输的总比特数。由此得证，$\lceil\log_2\mathrm{rank}_+(\boldsymbol{P})\rceil\leqslant\mathrm{RComm}(\boldsymbol{P})$。

3 量子场景

3.1 量子关联复杂度$Q(\boldsymbol{P})$

在量子场景中，Alice 和 Bob 可通过仅共享量子纠缠或仅进行量子通讯，即传输量子比特，并在各自拥有的系统上进行本地操作来生成经典关联$\boldsymbol{P}$。值得注意的是，在量子场景下，如果能制备形如$\rho=\sum_{x,y}\boldsymbol{P}(x,y)|x\rangle\langle x|\otimes|y\rangle\langle y|$的量子态，则 Alice 和 Bob 可通过在各自的子系统上进行计算基下的测量得到$\boldsymbol{P}$。一个值得关注的结果是文献 [2] 将$\boldsymbol{P}$的关联复杂度$Q(\boldsymbol{P})$与$\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P})$关联起来，并给出了与经典场景类似的精确刻画，即$Q(\boldsymbol{P})=\left\lceil\log_2\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P})\right\rceil$。

该结果的证明基于如下引理[2]：对量子态$\rho\in\mathcal{H}_A\otimes\mathcal{H}_B$，$Q(\rho)=\min_{\mathcal{H}_{A_1},\mathcal{H}_{B_1}}\lceil\log_2\mathrm{S}-\mathrm{rank}(|\psi\rangle)\rceil$，其中$|\psi\rangle\in\mathcal{H}_{A_1}\otimes\mathcal{H}_A\otimes\mathcal{H}_B\otimes\mathcal{H}_{B_1}$是$\rho$的纯化。基于这一引理，下文给出$Q(\boldsymbol{P})=\left\lceil\log_2\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P})\right\rceil$的简要证明。

首先，尝试给出$Q(\boldsymbol{P})$的上界。令$r=\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P})$，$\rho=\sum_{x,y}\boldsymbol{P}(x,y)|x\rangle\langle x|\otimes|y\rangle\langle y|$。若存在$\rho$的纯化$|\psi\rangle$满足$S-\mathrm{rank}(|\psi\rangle)\leqslant r$，结合如上引理，则有$Q(\boldsymbol{P})\leqslant\left\lceil\log_2\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P})\right\rceil$。考虑半正定矩阵$\boldsymbol{C}_x,\boldsymbol{D}_y\in\mathbb{C}^{r\times r}$使得对任意$x\in X,y\in Y$，$\boldsymbol{P}(x,y)=\mathrm{tr}(\boldsymbol{C}_x\boldsymbol{D}_y)$都成立。令$|v_x^i\rangle$为$\sqrt{\boldsymbol{C}_x^{\mathrm{T}}}$的第$i$列向量，$|w_y^i\rangle$为$\sqrt{\boldsymbol{D}_y}$的第$i$列向量。定义$|\psi\rangle\in\mathcal{H}_A\otimes\mathcal{H}_A\otimes\mathcal{H}_{A_1}\otimes\mathcal{H}_B\otimes\mathcal{H}_B\otimes\mathcal{H}_{B_1}$为如下形式：

$$|\psi\rangle=\sum_{i=1}^{r}\left(\sum_x|x\rangle\otimes|x\rangle\otimes|v_x^i\rangle\right)\otimes\left(\sum_y|y\rangle\otimes|y\rangle\otimes|w_y^i\rangle\right)$$

显而易见，$S-\mathrm{rank}(|\psi\rangle)\leqslant r$，并可验证$|\psi\rangle$是$\rho$的一个纯化。因此，Alice 和 Bob 可以在计算基下测量各自的第一部分系统，并抛弃后面两部分的系统，最终生成$\boldsymbol{P}$。

此外，对于$Q(\boldsymbol{P})$的下界，上面的引理意味着：存在ρ的纯化$|\psi\rangle$满足$S-\mathrm{rank}(|\psi\rangle)=r$且$\mathrm{Q}(\boldsymbol{P})=r$。因此，只要证明$r\geqslant\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P})$，即可完成论证。令：

$$|\psi\rangle=\sum_{i=1}^{r}\left(\sum_x|x\rangle\otimes|v_x^i\rangle\right)\otimes\left(\sum_y|y\rangle\otimes|w_y^i\rangle\right)$$

可对任意$x\in X$，定义$r\times r$的半正定矩阵$\boldsymbol{C}_x$，其i行j列的元素$\boldsymbol{C}_x(i,j)=\langle v_x^i|v_x^j\rangle$；定义$r\times r$的半正定矩阵$\boldsymbol{D}_y$，其$i$行$j$列的元素$\boldsymbol{D}_y(i,j)=\langle w_y^j|w_y^i\rangle$。可验证$|\psi\rangle$在$\mathcal{H}_A\otimes\mathcal{H}_B$上的约化密度矩阵：

$$\rho = \mathrm{tr}_{\mathcal{H}_{A_1}\otimes\mathcal{H}_{B_1}}(|\psi\rangle\langle\psi|) = \sum_{x,y}|x\rangle\langle x|\otimes|y\rangle\langle y|\left(\sum_{i,j=1}^{r}\langle v_x^j|v_x^i\rangle\langle w_y^j|w_y^i\rangle\right) = \sum_{x,y}|x\rangle\langle x|\otimes|y\rangle\langle y|\mathrm{tr}(\boldsymbol{C}_x\boldsymbol{D}_y)$$

因此，$\boldsymbol{C}_x$和$\boldsymbol{D}_y$是$\boldsymbol{P}$的一个半正定分解，有$r\geqslant\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P})$。由此得证。

3.2　随机、量子关联复杂度$R(\boldsymbol{P})$与$Q(\boldsymbol{P})$的对比

由于量子可模拟经典行为，有$Q(\boldsymbol{P})\leqslant R(\boldsymbol{P})$。此外，Alice 和 Bob 可直接共享经典关联$\boldsymbol{P}$，从而平凡地生成$\boldsymbol{P}$。因此，对于$\boldsymbol{P}$的关联复杂度有如下这一简单关系：

$$Q(\boldsymbol{P})\leqslant R(\boldsymbol{P})\leqslant \mathrm{size}(\boldsymbol{P})$$

那么一个自然的问题就是，$Q(\boldsymbol{P})$与$R(\boldsymbol{P})$之间的差距有多大？根据前文介绍的结果，这一问题等价于刻画非负矩阵$\boldsymbol{P}$的$\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P})$和$\mathrm{rank}_{+}(\boldsymbol{P})$之间的差距。以下展示两个极具代表性的例子。

一个是欧式距离矩阵 (Euclidean distance matrix, EDM)：给定n个互不相同的实数$c_1,c_2,\cdots,c_n$，其对应的 EDM 为$n\times n$的对称非负矩阵$\boldsymbol{Q}$，该矩阵i行j列的元素为$\boldsymbol{Q}(i,j)=(c_i-c_j)^2$。有研究结果证明，存在欧氏距离矩阵$\boldsymbol{Q}_1$满足$\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{Q}_1)=2$，且$\mathrm{rank}_{+}(\boldsymbol{Q}_1)\geqslant 2\sqrt{n}-2$[11]。换言之，若要生成经典关联$\boldsymbol{P}_1=\boldsymbol{Q}_1/\|\boldsymbol{Q}_1\|_1$，在量子场景下，Alice 和 Bob 只需要传输 1 量子比特；而若在经典场景下，Alice 和 Bob 需要传输的比特数为$O(\log_2 n)$量级。随着n的增大，生成关联$\boldsymbol{P}$所需的量子比特和经典比特数之间的差距可以达到任意大。

此外，考虑一个$2^n\times 2^n$的非负矩阵$\boldsymbol{M}$，其i行j列的元素为$\boldsymbol{M}(i,j)=(1-i^{\mathrm{T}}j)^2$。这里$i$和$j$是长度为$n$的比特串，$i^{\mathrm{T}}j$是$i$和$j$模 2 的内积。对于该矩阵而言，有$\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{M})=O(n)$，且$\mathrm{rank}_{+}(\boldsymbol{Q}_2)=2^{\Omega(n)}$[4]。即，若 Alice 和 Bob 想要生成经典关联$\boldsymbol{P}_2=\boldsymbol{M}/\|\boldsymbol{M}\|_1$，在量子场景下，二人所需传输的量子比特数为$O(\log_2 n)$量级；而在经典场景下，二人所需传输的经典比特数为$\Omega(n)$量级。在这一任务中，量子和经典之间的差距甚至达到了指数级别。因此，关联复杂度提供了区分量子和经典资源能力的一个视角。

4　量子、经典混合场景

在纯经典、量子的场景对比中，量子展示了极大的优势。但从目前的实验水平看来，距离实现大规模的量子计算这一目标，仍有相当长的路要走[12-13]。对于近期可实现的量子设备，其能操作的量子系统规模有限，通常为几十个量子比特。因此，对于需要更多量子比特才能完成的任务而言，一个亟待解决的问题就是：如何在可操作的量子资源有限的情况下，既能充分利用现有的量子资源，又能顺利完成任务？

出于这一需求，文献 [3] 研究了量子、经典混合场景下的经典关联生成问题。定义量子能力 (quantum capability) 为可完全操控的量子比特数的一半。考虑如下场景：Alice 和 Bob 想要生成经典关联$\boldsymbol{P}$，且二人具有的量子能力为s，但$s<\left\lceil\log_2\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P})\right\rceil$，也即二人不能通过纯量子协议直接生成经典关联$\boldsymbol{P}$，必须引入额外的经典计算资源才有可能完成任务。在这种情况下，一个有趣的问题是，在充分利用现有量子资源的前提下，他们该如何完成这一任务？同时，他们需要额外引入的经典资源最少是多少？

在量子、经典混合场景中，主要考虑先进行经典操作，后根据经典结果给定量子态的经典−量子混合协议；以及先给定固定的量子态 (与经典信息无关)，而后才进行经典操作的量子−经典混合协议。

4.1　经典−量子混合协议

在经典−量子混合协议中，Alice 和 Bob 可以先从概率分布$\{p_i\}$中采样i，后根据采样结果i制备量子态ρ_i，最后基于量子态ρ_i生成目标经典关联$\boldsymbol{P}$。假设$\boldsymbol{P}$可分解为$\boldsymbol{P}=\sum_{i\in I}p_i\boldsymbol{P}_i$，其中$\{p_i\}$是$i\in I$的概率分布，$\boldsymbol{P}_i$是一个经典关联，并满足$\left\lceil\log_2\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P}_i)\right\rceil\leqslant s$。那么，Alice 和 Bob 就可以从$\{p_i\}$中采样$i$，随后制备$\boldsymbol{P}_i$。因为$\left\lceil\log_2\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P}_i)\right\rceil\leqslant s$，制备$\boldsymbol{P}_i$是在量子能力范围之内的。这样，Alice 和 Bob 输出X和Y的联合概率分布就与$\boldsymbol{P}$的分布一致，也即完成了目标经典关联$\boldsymbol{P}$的生成。结合这一发现，文献 [3] 将量子能力为s时所需交换的经典比特数c与$\mathrm{rank}_{\mathrm{psd}}^{(2^s)}(\boldsymbol{P})$建立联系，并给出了$c=\left\lceil\log_2\mathrm{rank}_{\mathrm{psd}}^{(2^s)}(\boldsymbol{P})\right\rceil$这一结论。下面给出这一结果的简要证明。

首先证明 Alice 和 Bob 所需交换的经典比特数的下界。假设二人所需的最小量子比特数为c，则$\boldsymbol{P}$可分解为$\boldsymbol{P}(x,y)=\sum_{i=1}^{2^c}p_i\boldsymbol{P}_i(x,y)$，其中$\{p_i\}$是$i\in[2^c]$上的概率分布，且有$\left\lceil\log_2\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P}_i)\right\rceil\leqslant s$。令$\boldsymbol{P}_i$对应的半正定分解为$\boldsymbol{P}_i(x,y)=\mathrm{tr}(\boldsymbol{C}_x^i\boldsymbol{D}_y^i)$，其中

$\boldsymbol{C}_x^i, \boldsymbol{D}_y^i \in \mathbb{C}^{2^s \times 2^s}$为半正定矩阵。定义半正定矩阵 $\boldsymbol{C}_x = \mathrm{diag}(p_1\boldsymbol{C}_x^1, p_1\boldsymbol{C}_x^2, \cdots, p_{2^c}\boldsymbol{C}_x^{2^c})$，$\boldsymbol{D}_y = \mathrm{diag}(\boldsymbol{D}_y^1, \boldsymbol{D}_y^2, \cdots, \boldsymbol{D}_y^{2^c})$。则简单验证可得，$\boldsymbol{P}(x,y) = \mathrm{tr}(\boldsymbol{C}_x\boldsymbol{D}_y)$。因此，有$\left\lceil \log_2 \mathrm{rank}_{\mathrm{psd}}^{(2^s)}(\boldsymbol{P}) \right\rceil \leqslant c$。

此外，令 $r = \mathrm{rank}_{\mathrm{psd}}^{(2^s)}(\boldsymbol{P})$。则有半正定矩阵 $\boldsymbol{C}_x = \mathrm{diag}(\boldsymbol{C}_x^1, \boldsymbol{C}_x^2, \cdots, \boldsymbol{C}_x^r)$，$\boldsymbol{D}_y = \mathrm{diag}(\boldsymbol{D}_y^1, \boldsymbol{D}_y^2, \cdots, \boldsymbol{D}_y^r)$满足$\boldsymbol{P}(x,y) = \mathrm{tr}(\boldsymbol{C}_x\boldsymbol{D}_y)$。其中，对所有的$i \in [r]$，半正定矩阵$\boldsymbol{C}_x^i, \boldsymbol{D}_y^i \in \mathbb{C}^{2^s \times 2^s}$。定义$\boldsymbol{Q}_i(x,y) = \mathrm{tr}(\boldsymbol{C}_x^i\boldsymbol{D}_y^i)$，经典关联$\boldsymbol{P}_i = \boldsymbol{Q}_i / \|\boldsymbol{Q}_i\|_1$。当$p_i = \|\boldsymbol{Q}_i\|_1$时，根据$2^s$区块半正定秩的定义，有$p_i > 0$。这意味着可将$\boldsymbol{P}$分解为 $\boldsymbol{P} = \sum_{i=1}^{r} p_i\boldsymbol{P}_i$，并对所有的$i \in [r]$有$\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P}_i) \leqslant 2^s$。由此，Alice 和 Bob 可通过交换$\lceil \log_2 r \rceil$个经典比特来生成经典关联$\boldsymbol{P}$，即有$c \leqslant \left\lceil \log_2 \mathrm{rank}_{\mathrm{psd}}^{(2^s)}(\boldsymbol{P}) \right\rceil$。由此得证，$c = \left\lceil \log_2 \mathrm{rank}_{\mathrm{psd}}^{(2^s)}(\boldsymbol{P}) \right\rceil$。

根据这一等价刻画，可以比较量子资源和经典资源之间的差别。在 3.2 节定义的欧氏距离矩阵$\boldsymbol{Q}_1$对应的经典关联$\boldsymbol{P}_1$，有$\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P}_1) = 2$，$\mathrm{rank}_{+}(\boldsymbol{P}_1) \geqslant 2\sqrt{n} - 2$。这里定义$\boldsymbol{P}_2 = \boldsymbol{P}_1 \otimes \boldsymbol{P}_1$，结合半正定秩的性质：$\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{A} \otimes \boldsymbol{B}) \leqslant \mathrm{rank}_{\mathrm{psd}}(\boldsymbol{A})\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{B})$[14]，简单可得$\mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P}_2) = 4$。因此，若通过执行纯量子协议来生成经典关联$\boldsymbol{P}_2$，Alice 和 Bob 需要传输的量子比特数为 2。当量子能力$s = 1$时，由于所需的量子系统超过了目前可操控的量子比特数，考虑用经典−量子混合协议来生成$\boldsymbol{P}_2$。对于这一经典关联，有研究结果表明$\mathrm{rank}_{\mathrm{psd}}^{(2)}(\boldsymbol{P}_2) \geqslant \log_2 n$[3]。即，缺少 1 个量子比特的代价需要用$\Omega(\log_2\log_2 n)$规模的经典比特来弥补。因此，在经典−量子混合场景中，同样可以看到量子资源相对经典资源的优势。

4.2 量子−经典混合协议

在经典−量子混合协议中，Alice 和 Bob 拥有在看到经典采样i后再对应选择共享量子态ρ_i的自由度，即他们可以随意要求不同的初始共享量子态ρ_i。但在某些时候，这一自由度仍是不易实现的。因此，这里考虑一个更为严格的场景，即 Alice 和 Bob 只能在协议一开始获得一个固定的量子态，该量子态与经典信息无关，而后二人才能进行经典操作，或在该量子态上进行本地操作以达成目的。在这一限制之下，前文提出的经典−量子混合协议就自然失效了。同样限制 Alice 和 Bob 具有的量子能力为s。由于这里是先有的量子态，而后才介入经典操作，故考虑量子−经典混合协议来处理这一经典关联生成问题。

为了解决该问题，文献 [3] 将共享的量子态设定为纯态。对于任意的关联，若其能被$\mathbb{C}^d \otimes \mathbb{C}^d$上的混态生成，那么一定存在$\mathbb{C}^d \otimes \mathbb{C}^d$上的纯态同样可以生成这一关联[15]。因此，共享量子态为纯态这一假定依然发挥了量子能力范围内该有的作用。

此外，文献 [16] 曾用优超 (majorization) 这一概念刻画了将一个量子纯态通过本地操作和经典通讯 (local operation and classical communication, LOCC) 来转化成另一个量子纯态的充分必要条件。假设$|\psi\rangle$和$|\phi\rangle$是两个$d \times d$的两体量子纯态，λ_ψ和λ_ϕ是其对应的施密特系数的平方组成的向量。那么，$|\psi\rangle$可以通过 LOCC 的方式被转化成$|\phi\rangle$，当且仅当$|\phi\rangle$优超$|\psi\rangle$[17]。由于任意$2^n \times 2^n$的量子纯态都优超n对 Einstein-Podolsky-Rosen (EPR) 态组成的复合系统$|n-\mathrm{EPR}\rangle = (1/\sqrt{2}(|00\rangle + |11\rangle))^{\otimes n}$，所以$|n-\mathrm{EPR}\rangle$可以通过 LOCC 的方式制备任意$2^n \times 2^n$的量子纯态。

结合以上两个事实，Alice 和 Bob 可以首先共享s对 EPR 态，这里的s为受限的量子能力。然后，与经典−量子混合协议类似地，考虑$\boldsymbol{P} = \sum_{i \in I} p_i\boldsymbol{P}_i$这一分解,其中$\{p_i\}$是$i \in I$的概率分布，$\boldsymbol{P}_i$是一个经典关联，并满足$\left\lceil \log_2 \mathrm{rank}_{\mathrm{psd}}(\boldsymbol{P}_i) \right\rceil \leqslant s$。这样，Alice 和 Bob 就可以从概率分布$\{p_i\}$中采样$i$，随后用 LOCC 的方式将$s$对 EPR 态转化成$\rho_i$，并依据$\rho_i$来制备$\boldsymbol{P}_i$。这样，考虑 Alice 和 Bob 输出随机变量X和Y的整体行为，其概率分布与经典关联$\boldsymbol{P}$一致，也即完成了量子−经典混合协议下的经典关联$\boldsymbol{P}$的生成。

在这一过程中引入的经典通讯只存在于将s对 EPR 态转化成ρ_i这一部分，根据文献 [16] 的结果，该步骤所需的经典比特数至多为$2^s - 1$。因此，对于量子−经典混合协议下的经典关联$\boldsymbol{P}$的生成问题而言，给定量子能力s，其所需要传输的经典比特数至多为$\left\lceil \log_2 \mathrm{rank}_{\mathrm{psd}}^{(2^s)}(\boldsymbol{P}) \right\rceil + 2^s - 1$。

5 结 束 语

随着量子计算和量子信息的兴起，越来越多的研究工作聚焦于对比量子资源和经典资源在计算能力上的差距[17-20]。本文从经典关联生成问题入手，首先介绍了完成该任务的经典协议和量子协议的完整数学刻画。通过将经典协议所需的经典资源与非负秩建立联系，并将量子协议所需的量子资源与半正定秩对标，把该问题转化为对比非负矩阵的非负秩与半正定秩的问题。在此基础之上，本文介绍了

两个区分量子和经典资源计算能力的例子，其中，事先共享量子纠缠甚至能比事先共享随机性有指数级的优势。

此外，针对近期量子设备规模，本文还介绍了量子、经典混合场景下的经典关联生成问题。根据在协议中提供初始共享量子态的时间点，分别讨论了经典−量子混合协议和量子−经典混合协议。与纯经典协议和纯量子协议类似，在量子、经典混合场景下，其所需的经典比特数与k区块半正定秩相关。在这一量子、经典混合场景中，仍然可以看到量子相对经典的优势。因此，经典关联生成问题是对比量子资源和经典资源之间计算能力的一个极佳视角。

总体而言，经典关联生成问题中蕴含着丰富的数学结构。并且由于其与半正定秩的性质密切相关，而半正定秩的研究尚处于初期阶段，因此该问题仍有极大的探讨空间，希望后续能有更丰富的研究结果诞生。

参 考 文 献

[1] ZHANG S. Quantum strategic game theory[C]// Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. New York: Association for Computing Machinery, 2012: 39-59.

[2] JAIN R, SHI Y, WEI Z, et al. Efficient protocols for generating bipartite classical distributions and quantum states[J]. IEEE Transactions on Information Theory, 2013, 59(8): 5171-5178.

[3] LIN X, WEI Z, YAO P. Quantum and classical hybrid generations for classical correlations[J]. IEEE Transactions on Information Theory, 2021, 68(1): 302-310.

[4] FIORINI S, MASSAR S, POKUTTA S, et al. Linear vs. semidefinite extended formulations: Exponential separation and strong lower bounds[C]//Proceedings of the 44th Annual ACM Symposium on Theory of Computing. [S.l.]: ACM, 2012: 95-106.

[5] FAWZI H, GOUVEIA J, PARRILO P A, et al. Positive semidefinite rank[J]. Mathematical Programming, 2015, 153(1): 133-177.

[6] FAWZI H. On representing the positive semidefinite cone using the second-order cone[J]. Mathematical Programming, 2019, 175(1): 109-118.

[7] AVERKOV G. Optimal size of linear matrix inequalities in semidefinite approaches to polynomial optimization[J]. SIAM Journal on Applied Algebra and Geometry, 2019, 3(1): 128-151.

[8] SAUNDERSON J. Limitations on the expressive power of convex cones without long chains of faces[J]. SIAM Journal on Optimization, 2020, 30(1): 1033-1047.

[9] SOH Y S, VARVITSIOTIS A. A non-commutative extension of Lee-Seung's algorithm for positive semidefinite factorizations[EB/OL]. (2021-06-01). http://arxiv.org/abs/2016.00293.

[10] NIELSEN M A, CHUANG I L. Quantum computation and quantum information: 10th anniversary edition[M]. Cambridge: Cambridge University Press, 2010.

[11] SHITOV Y. Euclidean distance matrices and separations in communication complexity theory[J]. Discrete & Computational Geometry, 2019, 61(3): 653-660.

[12] ARUTE F, ARYA K, BABBUSH R, et al. Quantum supremacy using a programmable superconducting processor[J]. Nature, 2019, 574(7779): 505-510.

[13] PRESKILL J. Quantum computing in the NISQ era and beyond[J]. Quantum, 2018, 2: 79.

[14] LEE T, WEI Z, DE WOLF R. Some upper and lower bounds on PSD-rank[J]. Mathematical Programming, 2017, 162(1): 495-521.

[15] SIKORA J, VARVITSIOTIS A, WEI Z. Minimum dimension of a Hilbert space needed to generate a quantum correlation[J]. Physical Review Letters, 2016, 117(6): 060401.

[16] NIELSEN M A. Conditions for a class of entanglement transformations[J]. Physical Review Letters, 1999, 83(2): 436.

[17] AARONSON S, ARKHIPOV A. The computational complexity of linear optics[C]//Proceedings of the 43rd Annual ACM Symposium on Theory of Computing. [S. l.]: ACM, 2011: 333-342.

[18] KING J, YARKONI S, RAYMOND J, et al. Quantum annealing amid local ruggedness and global frustration[J]. Journal of the Physical Society of Japan, 2019, 88(6): 061007.

[19] AARONSON S, CHEN L. Complexity-theoretic foundations of quantum supremacy experiments[EB/OL]. (2016-12-26). https://arxiv.org/abs/1612.05903.

[20] BOULAND A, FEFFERMAN B, NIRKHE C, et al. On the complexity and verification of quantum random circuit sampling[J]. Nature Physics, 2019, 15(2): 159-163.

编　辑　蒋　晓