非定域性蒸馏可优于纠缠蒸馏

Peter Høyer卡尔加里大学 计算机科学系卡尔加里，加拿大 hoyer@ucalgary.ca

Jibran Rashid计算机科学系 工商管理学院卡拉奇，巴基斯坦 jrashid@iba.edu.pk

Razeen Ud Din数学科学系 工商管理学院卡拉奇，巴基斯坦 ruddin@iba.edu.pk

arXiv:2603.00940v1 [quant-ph] 1 Mar 2026

摘要——**鉴于我们的目标是最大化 CHSH违背，我们比较纠缠蒸馏与非定域性蒸馏的最优策略。当共享态的副本数趋于无穷时，纠缠蒸馏必定能够通过生成一个贝尔态而奏效。对于数量较少的态副本，我们证明，非定域性蒸馏能够取得更高的 CHSH 值，即使最优纠缠蒸馏需要通信也是如此。非定域性蒸馏不仅优于纠缠蒸馏，在量子资源估算的多项指标上也展现出更高的资源效率。**

关键词—**非局域性蒸馏、纠缠蒸馏、量子资源估算、稀疏态制备、量子密钥分发**

I. 引言

提纯纠缠、关联和信道等资源的协议在量子信息领域发挥着重要作用。它们能够将多个噪声资源副本集中起来，得到更纯净或更强的资源版本。一个自然的问题是，能以多高的效率生成更强的资源。本文探讨通过纠缠蒸馏提纯非定域关联的可能性，并考察由此得到的界限是否总是优于直接进行非定域性蒸馏。

纠缠和非局域性是量子信息论中既不同又相关的资源 [1]。纠缠指复合量子系统无法独立描述的性质，而非局域性则指纠缠系统表现出的、无法通过经典方式生成的关联。二者都是量子通信和计算的重要资源。然而，并非所有纠缠态都表现出非局域性 [2]。一些纠缠态可以由局域隐变量模型描述，因此不表现出非局域性。这一区别表明，尽管非局域性是纠缠的一种体现，但它并非同一种现象。

量子信息理论中的纠缠蒸馏协议 [3] 可以从多个弱纠缠态或噪声态副本中提取最大纠缠贝尔态。鉴于贝尔态作为纠缠单位的重要性，这些协议对于量子通信任务至关重要，例如量子隐形传态和量子密钥分发（QKD）；在这些任务中，高质量的纠缠是实现安全、可靠信息传输的关键。

有些纠缠态无法提纯（即束缚纠缠），这一事实凸显了资源转换 [4]的根本局限。Lo 和 Popescu [5]构造了适用于双体纯态、采用单向通信的最优纠缠提纯协议。

Peres [6]通过指出，对某个态的多个副本进行集体测量，即使单个副本只产生局域关联，也能导致 CHSH违背，从而开创了非定域性蒸馏的研究。Liang 和 Doherty [8] 给出了通过集体测量对 n个双量子比特纯态副本实现 CHSH违背的界限。

假设只能获得少数几个含噪纠缠态副本，我们要探讨的问题是：最优纠缠提纯协议是否也能作为最优的非定域性蒸馏协议。在通常考虑的纠缠提纯框架中，假设可以随时获得许多相同的含噪纠缠态副本。如果副本数量足够多，就能通过该协议获得多个完美贝尔态副本。因此，比较纠缠提纯率与非局域性浓缩协议的提纯率这一问题便不会出现。如果可用副本数量少到甚至无法确定性地获得一个完美贝尔态，那么目前尚不清楚纠缠提纯和非定域性蒸馏这两者中，哪一种能最大化 CHSH [7] 违背。我们在此表明，尽管纠缠提纯需要通信，但当态的副本数量足够少、噪声足够大时，非定域性蒸馏能够达到更高的 CHSH 值。

A. 主要结果

我们的核心贡献是证明某些现有非定域性蒸馏协议的最优性，并将其性能与最优纠缠蒸馏协议进行比较。对于纯态，尽管目前已知的最佳协议尚未被证明是最优的，定理1表明，它们的表现已经可以优于纠缠蒸馏。

定理*1*： 对于双体纯态，非定域性蒸馏能够达到比最优纠缠蒸馏协议更高的 CHSH 值（针对 $n = 2$ 和 3）。

对于混合态，据我们所知，目前尚无适用于少数副本的最优纠缠蒸馏协议。我们在定理 2 中证明，

对于给定的混合态，最佳非定域性蒸馏协议可以达到与纯态协议相同的值。因此，非定域性蒸馏在混合态下也能取得更好的效果。

定理 *2*：针对混合态的最优非局域性提纯协议，能够使 $n=2$ 达到比最优纠缠提纯协议更高的 CHSH 值。方程 6 中该状态的 $n=3$ 个副本的一个界限为

$$V \leq 2\sqrt{1+\left(1-24p^2+80p^3-120p^4+96p^5-32p^6\right)}.$$

下一节中，我们将阐述不同的蒸馏框架，并在第三节证明定理 1 和定理 2。

II. 蒸馏综述

我们先简要回顾 Lo 和 Popescu [5]提出的纯态最优提纯协议。

A. 纯态的最优纠缠蒸馏

设状态 $|\psi\rangle$和 $|\phi\rangle$为如下给出的贝尔态

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right) \quad \text{and} \quad |\phi\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle+|10\rangle\right).$$

Alice 和 Bob 在空间上彼此分隔的实验室中共享n 个该纯态的副本

$$|\Psi\rangle=\sqrt{p}\,|\psi\rangle+\sqrt{1-p}\,|\phi\rangle. \tag{1}$$

该态 $|\Psi\rangle$的施密特分解为

$$|\Psi\rangle=\left(\frac{\sqrt{p}+\sqrt{1-p}}{\sqrt{2}}\right)|00\rangle+\left(\frac{\sqrt{p}-\sqrt{1-p}}{\sqrt{2}}\right)|11\rangle.$$

对于 $n=3$, $|\Psi\rangle^{\otimes n}$ 的施密特分解可表示为

$$\begin{aligned}|\Phi\rangle_{AB}=\ & \sqrt{\lambda_1}\,|000\rangle_A\,|000\rangle_B+\sqrt{\lambda_2}\,|001\rangle_A\,|001\rangle_B\\ &+\sqrt{\lambda_3}\,|010\rangle_A\,|010\rangle_B+\sqrt{\lambda_4}\,|100\rangle_A\,|100\rangle_B\\ &+\sqrt{\lambda_5}\,|011\rangle_A\,|011\rangle_B+\sqrt{\lambda_6}\,|101\rangle_A\,|101\rangle_B\\ &+\sqrt{\lambda_7}\,|110\rangle_A\,|110\rangle_B+\sqrt{\lambda_8}\,|111\rangle_A\,|111\rangle_B,\end{aligned}$$

其中系数 λ_i 为

$$\lambda_1=\left(\frac{\sqrt{p}+\sqrt{1-p}}{\sqrt{2}}\right)^6,\ \lambda_8=\left(\frac{\sqrt{p}-\sqrt{1-p}}{\sqrt{2}}\right)^6,$$

$$\lambda_2=\lambda_3=\lambda_4=\left(\frac{\sqrt{p}+\sqrt{1-p}}{\sqrt{2}}\right)^4\left(\frac{\sqrt{p}-\sqrt{1-p}}{\sqrt{2}}\right)^2,$$

$$\lambda_5=\lambda_6=\lambda_7=\left(\frac{\sqrt{p}+\sqrt{1-p}}{\sqrt{2}}\right)^2\left(\frac{\sqrt{p}-\sqrt{1-p}}{\sqrt{2}}\right)^4,$$

与 $\lambda_i\geq\lambda_{i+1}$ 和 $\sum_{i=1}^{8}\lambda_i=1$。这里，下标 A 和B 分别表示 Alice 和 Bob 持有的状态 $|\Phi\rangle_{AB}$。从 $|\Phi\rangle_{AB}$ 中成功提纯出贝尔态 $|\psi\rangle$ 的最优概率 p_{succ} 由方程 2 确定。如果提纯协议失败，所得状态就是乘积态。因此，我们可以将 3 个副本得到的 CHSH 值 V_{ED} 确定为加权平均

$$V_{ED}=2\sqrt{2}p_{\text{succ}}+2(1-p_{\text{succ}}).$$

B. 纯态的非定域性蒸馏

近期关于非定域性蒸馏的大量研究都聚焦于盒子世界框架 [9], [10], [11], [12]。对于方程 1 中纯态 $|\Psi\rangle$ 的n 个副本，Liang 和 Doherty [8] 给出的非局域性蒸馏已知最佳 CHSH 界 V_{ND} 为

$$V_{ND}=2\sum_{n=1}^{\lfloor d/2\rfloor}\sqrt{\left(\lambda_{2n-1}^2+\lambda_{2n}^2\right)^2+4\lambda_{2n}^2\lambda_{2n-1}^2}, \tag{3}$$

其中 λ_i 为施密特系数， d 为该态的维数。对于 $n=1$, 已知该界是最优的 [13], , 但对于 $n>1$, 尚未证明其最优性。对于 $n=1$，达到该界的可观测量为

$$\begin{aligned}A_0&=Z\\ A_1&=X\\ B_0&=\frac{(1-2p)}{\sqrt{1+(1-2p)^2}}Z+\frac{1}{\sqrt{1+(1-2p)^2}}X\\ B_1&=\frac{(1-2p)}{\sqrt{1+(1-2p)^2}}Z-\frac{1}{\sqrt{1+(1-2p)^2}}X.\end{aligned} \tag{4}$$

对于这些测量，四个CHSH关联函数的取值为

$$\langle\Psi|\,A_0\otimes B_0\,|\Psi\rangle=\ \langle\Psi|\,A_0\otimes B_1\,|\Psi\rangle=\frac{(1-2p)^2}{\sqrt{2-4p+4p^2}}$$

$$\langle\Psi|\,A_1\otimes B_0\,|\Psi\rangle=-\langle\Psi|\,A_1\otimes B_1\,|\Psi\rangle=\frac{1}{\sqrt{2-4p+4p^2}}$$

从而得到CHSH界

$$V=2\sqrt{(1+(1-2p)^2)}. \tag{5}$$

对于 $n=3$ 非局域性界为

$$V_{ND}=2\sum_{n=1}^{4}\sqrt{\left(\lambda_{2n-1}^2+\lambda_{2n}^2\right)^2+4\lambda_{2n}^2\lambda_{2n-1}^2},$$

然而，相应的测量结果目前仅通过数值方法得到验证。

C. 混合态的非定域性蒸馏

鉴于我们没有混合态的规范表示，受纯态分析的启发，我们考虑混合态

$$\rho=p\,|\psi\rangle\langle\psi|+(1-p)\,|\phi\rangle\langle\phi| \tag{6}$$

其中，CHSH 值为

$$\mathrm{Tr}(M\rho)=\mathrm{Tr}((pM+(1-p)M')\,|\psi\rangle\langle\psi|)$$

其中,

$$\begin{aligned}M&=A_0\otimes B_0+A_0\otimes B_1+A_1\otimes B_0-A_1\otimes B_1\\ M'&=A_0\otimes B_0'+A_0\otimes B_1'+A_1\otimes B_0'-A_1\otimes B_1'\end{aligned}$$

以及 $B_i'=XB_iX$。令

$$N=pM+(1-p)M' \tag{7}$$

$$p_{\text{succ}} = \min_{1\le r\le 2} \frac{2}{r}\left(\lambda_{2-r+1} + \lambda_{2-r+2} + \cdots + \lambda_8\right) = \min\left\{1, 6\left(\frac{\sqrt{p}+\sqrt{1-p}}{\sqrt{2}}\right)^2\left(\frac{\sqrt{p}-\sqrt{1-p}}{\sqrt{2}}\right)^2 + 2\left(\frac{\sqrt{p}-\sqrt{1-p}}{\sqrt{2}}\right)^6\right\} \quad (2)$$

使用方程4中给出的相同可观测量，我们得到

$$\begin{aligned}\mathrm{Tr}(A_0\otimes B_0\rho) = \quad & \mathrm{Tr}(A_0\otimes B_1\rho) = \frac{(1-2p)^2}{\sqrt{2-4p+4p^2}}\\ \mathrm{Tr}(A_1\otimes B_0\rho) = -\,& \mathrm{Tr}(A_1\otimes B_1\rho) = \frac{1}{\sqrt{2-4p+4p^2}},\end{aligned}$$

这会得到与纯态相同的 CHSH界，即，

$$V = 2\sqrt{1+(1-2p)^2}.$$

我们在定理 2 中证明， ρ的两个副本的界与 $n=1$的相同。值得注意的是，纯态情形似乎也具有类似性质，尽管尚未得到证明。

对于状态 ρ的 $n=3$ 个副本，我们在第三节证明了以下界

$$2\sqrt{1+(1-24p^2+80p^3-120p^4+96p^5-32p^6)},$$

但请注意，目前尚不清楚该界是否紧致。图 2 展示了混合态的一个、两个和三个副本对应的界。

III. 纠缠与非局域性提纯的比较

我们现在证明的定理1中达到的数值，可以在图 1 中直观地看到。

定理1的证明 分别使用 II-A节和II-B节中的纠缠蒸馏和非定域性蒸馏协议，对于 $n=2$ ，我们得到

$$\begin{aligned}V_{ED} &= 2+4(2\sqrt{2}-2)t+2\left(\frac{\sqrt{p}+\sqrt{1-p}}{\sqrt{2}}\right)^4\\ &\le 2\sqrt{1+4t} = V_{ND} \text{ for } p\in[0.5,0.85],\end{aligned}$$

其中

$$t = \left(\frac{\sqrt{p}+\sqrt{1-p}}{\sqrt{2}}\right)^2\left(\frac{\sqrt{p}-\sqrt{1-p}}{\sqrt{2}}\right)^2.$$

这表明，对于区间 $p\in[0.5,0.85]$，非定域性蒸馏取得的值高于纠缠蒸馏。图1（左）展示了这一比较。

类似地，对于 $n=3$ ，我们有

$$\begin{aligned}V_{ED} &= 2+6(2\sqrt{2}-1)t+2\left(\frac{\sqrt{p}-\sqrt{1-p}}{\sqrt{2}}\right)^6\\ &\le (4\sqrt{2})t+2(\sqrt{1+4t})r = V_{ND} \text{ for } p\in[0.5,0.746],\end{aligned}$$

其中

$$r = \left(\frac{\sqrt{p}+\sqrt{1-p}}{\sqrt{2}}\right)^4+\left(\frac{\sqrt{p}-\sqrt{1-p}}{\sqrt{2}}\right)^4.$$

这证明，对于 $p\in[0.746,0.904]$ 非定域性蒸馏再次优于纠缠蒸馏。图1（中）展示了这一比较，而（右）展示了 $n=4$ 的情况，此时纠缠蒸馏总是更优。□

现在，我们使用方程 6 中的混合态进行提纯，以证明定理 2。对于 $n=1$和 2，我们得到的界与纯态情形下方程 5 中的值相同。

定理 2 的证明 注意到，混合态的 n 个副本在方程 7 中对应的算符 N 的平方为

$$N^2 = 4\mathbb{1}\otimes\tilde{K} + (2A)\otimes\tilde{L}, \quad (8)$$

其中 $A = A_1A_0 - A_0A_1$ 且

$$\tilde{K} = \sum_{x,y\in\{0,1\}^n} K[x,y]\cdot\frac{1}{2}\left(B_0^xB_0^y + B_1^xB_1^y\right), \quad (9)$$

$$\tilde{L} = \sum_{x,y\in\{0,1\}^n} L[x,y]\cdot\frac{1}{2}\left(B_0^xB_1^y - B_1^yB_0^x\right). \quad (10)$$

这里我们有 $B_0^x = X^xB_0X^x$ 和 $B_1^x = X^xB_1X^x$ ，其中 $X^x = \otimes_{i=1}^n X^{x_i}$。一般而言，我们还有 $K=L$ ，其针对 $n=1$, 2 和 3 的显式形式如下。

1）对于 $n=1$，我们有

$$K = L = \begin{bmatrix}a & b\\ b & a\end{bmatrix}.$$

其中我们固定

$$\begin{aligned}a &= \frac{p^2+(1-p)^2}{2} \text{ and}\\ b &= p(1-p).\end{aligned}$$

2）对于 $n=2$，我们有

$$K = L = \begin{bmatrix}a & b & b & c\\ b & a & c & b\\ b & c & a & b\\ c & b & b & a\end{bmatrix},$$

其中我们固定

$$\begin{aligned}a &= \frac{(p^2+(1-p)^2)^2}{4},\\ b &= \frac{p(1-p)(p^2+(1-p)^2)}{2} \text{ and}\\ c &= p^2(1-p)^2.\end{aligned}$$

3) 对于 $n=3$，我们有

$$K = L = \begin{bmatrix}a & b & b & c & b & c & c & d\\ b & a & c & b & c & b & d & c\\ b & c & a & b & c & d & b & c\\ c & b & b & a & d & c & c & b\\ b & c & c & d & a & b & b & c\\ c & b & d & c & b & a & c & b\\ c & d & b & c & b & c & a & b\\ d & c & c & b & c & b & b & a\end{bmatrix},$$

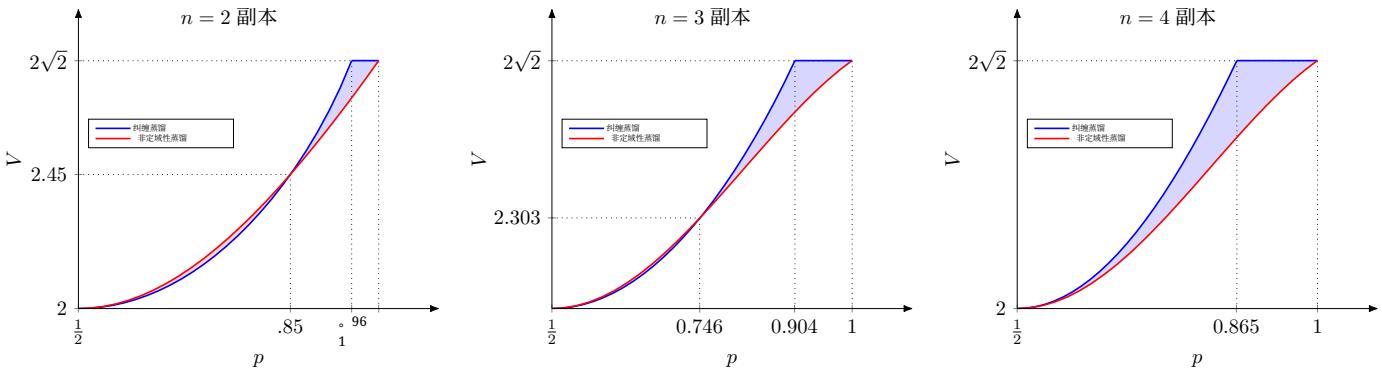


图 1. 对纯态而言， $n = 2,3$ 和 4 个副本的纠缠蒸馏与非定域性蒸馏比较。结果表明，在特定的 p 范围内，非定域性蒸馏优于纠缠蒸馏，但这一优势在副本数超过三个后消失。

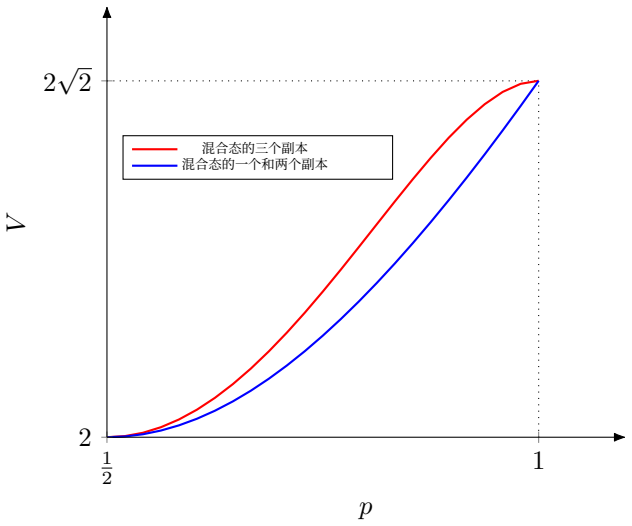


图 2. 混合态 ρ的一个、两个和三个副本的非定域性蒸馏界。

其中我们设

$$\begin{aligned} a &= \frac{(p^2+(1-p)^2)^3}{8}, \\ b &= \frac{p(1-p)((p^2+(1-p)^2))^2}{4}, \\ c &= \frac{p^2(1-p)^2(p^2+(1-p)^2)}{2} \text{ and} \\ d &= p^3(1-p)^3. \end{aligned}$$

我们有 $\left\|\tilde{K}\right\| \leq 1$、 $\|4\mathbb{1}\| = 4$ 和 $\|2A\| \leq 4$。为了界定 $\left\|\tilde{L}\right\|$，令 $C_{xy} = B_0^x B_1^y - B_1^y B_0^x$，于是，对于 $n = 1$，我们有

$$\begin{aligned} \tilde{L} &= \sum_{x,y\in\{0,1\}} L[x,y]\cdot\frac{1}{2}C_{xy} \\ &= \frac{a}{2}C_{00} + \frac{b}{2}C_{01} + \frac{b}{2}C_{10} + \frac{a}{2}C_{11}. \end{aligned}$$

我们可以将该表达式重新表述为

$$\tilde{L} = \frac{a}{2}C_{00} - \frac{b}{2}C_{00} - \frac{b}{2}C_{11} + \frac{a}{2}C_{11} + \frac{b}{2}\sum_{x,y\in\{0,1\}} C_{xy}.$$

利用循环性质，我们有

$$\begin{aligned} B_0^0 B_1^1 - B_1^1 B_0^0 &= B_0 X B_1 X - X B_1 X B_0 \\ &= X B_1 X B_0 - X B_1 X B_0 = 0 \end{aligned}$$

类似地， $B_0^1 B_1^0 - B_0^0 B_1^1 = 0$。注意到求和项 $\left\|\frac{b}{2}\sum_{x,y\in\{0,1\}} C_{xy}\right\|$ 消失，因此得到界

$$\left\|\tilde{L}\right\| \leq 2|a-b| = (1-2p)^2.$$

最后，结合所有部分可得

$$\begin{aligned} \left\|N^2\right\| &\leq \|4\mathbb{1}\|\cdot\left\|\tilde{K}\right\| + \|2A\|\cdot\left\|\tilde{L}\right\| \\ &\leq 4 + 4(1-2p)^2, \end{aligned}$$

这就得到了所需结论

$$\|N\| \leq 2\sqrt{(1+(1-2p)^2)}.$$

在 $n = 2$ 的情况下，我们同样通过注意到 L 来对其进行界定：

$$\begin{aligned} \tilde{L} &= \sum_{x,y\in\{0,1\}^2} L[x,y]\cdot\frac{1}{2}C_{xy} \\ &= \frac{a-b}{2}\left(C_{0000}+C_{0011}+C_{0101}+C_{0110}\right) \\ &\quad + \frac{c-b}{2}\left(C_{0000}+C_{0011}+C_{0101}+C_{0110}\right) \\ &\quad + \frac{b}{2}\sum_{x,y\in\{0,1\}^2} C_{xy}, \end{aligned}$$

由此得到

$$\left\|\tilde{L}\right\| \leq 4|a-b| + 4|c-b| = (1-2p)^2.$$

这给出了与 $n = 1$ 情况相同的界，即，

$$\|N\| \leq 2\sqrt{(1+(1-2p)^2)}.$$

˜对于 $n = 3$，我们可以将 L 表示为

$$\tilde{L} = L_1 + \frac{b}{2} \sum_{x,y \in \{0,1\}^3} C_{xy},$$

其中 L_1 由下式给出

$$\begin{bmatrix} a-b & 0 & 0 & c-b & 0 & c-b & c-b & d-b \\ 0 & a-b & c-b & 0 & c-b & 0 & d-b & c-b \\ 0 & c-b & a-b & 0 & c-b & d-b & 0 & c-b \\ c-b & 0 & 0 & a-b & d-b & c-b & c-b & 0 \\ 0 & c-b & c-b & d-b & a-b & 0 & 0 & c-b \\ c-b & 0 & d-b & c-b & 0 & a-b & c-b & 0 \\ c-b & d-b & 0 & c-b & 0 & c-b & a-b & 0 \\ d-b & c-b & c-b & 0 & c-b & 0 & 0 & a-b \end{bmatrix}.$$

$\|L_1\|$ 可由以下式子界定

$$\|L_1\| \leq 8|a-b| + 24|c-b| + 8|d-b|,$$

最终得到

$$\|N\| \leq 2\sqrt{1 + (1 - 24p^2 + 80p^3 - 120p^4 + 96p^5 - 32p^6)}.$$

□

图 2 绘出了定理 2 中达到的混合态界。 $n = 3$ 的界是否为紧界尚未可知。

A. 蒸馏的量子资源估算

比较不同蒸馏协议时，需要考虑的一个因素是其实现所需的资源。由于相干时间有限且可用的贝尔态数量有限，对于 NISQ 硬件而言，确定这些资源尤为重要。量子资源估算 [14]–[16]使我们能够在假设特定硬件特性的情况下，确定运行量子协议所需的量子比特和量子门数量、处理时间及其他资源。不同量子资源估算器的示例包括 pyLIQTR [17], Qualtran [18], BenchQ [19] 和 Azure Quantum Resource Estimator [20]。

量子态制备是量子计算的重要组成部分，而且可能比其经典对应过程更加复杂。事实上，已知某些 n量子比特态只能通过规模为 $\Omega(2^n)$ 的电路制备 [21]。Gleinig 和 Hoefler [22]构建了一种利用稀疏性、从而渐近地提高稀疏态制备效率的算法。

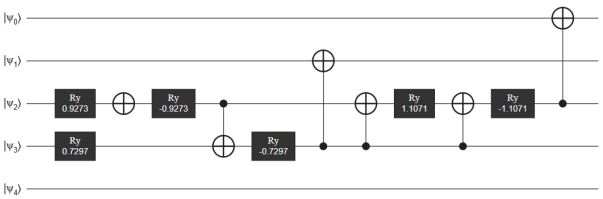
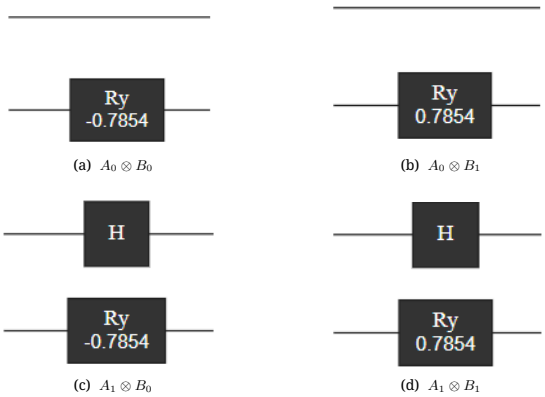


图 3. 制备两个初始量子态 $|\Psi\rangle$副本的电路。第五个量子比特是用于纠缠蒸馏过程的辅助量子比特。

使用我们对稀疏态算法 [23],的实现，我们估算了 $n = 2$ 纯态情况下非局域性提纯和纠缠提纯所需的量子资源。整个过程可分为以下三个阶段。

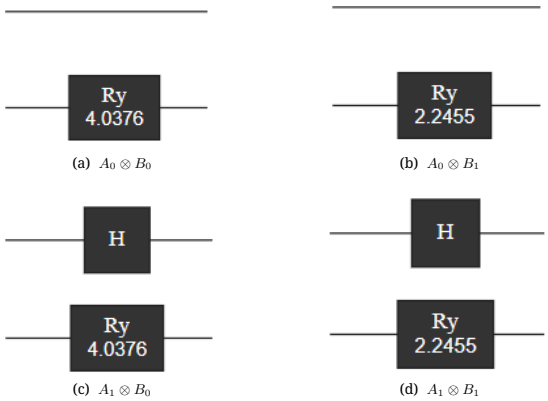
制备 $\mapsto$蒸馏 $\mapsto$测量

尽管在实际的提纯场景中，态是作为输入提供的，但在模拟中我们需要在第1阶段制备这些态。图3中的电路对应于非局域性提纯和纠缠蒸馏的态制备电路。第3阶段的测量（图4和图5）对两种协议也产生了相对相似的电路。



(a) $A_0 \otimes B_0$ (b) $A_0 \otimes B_1$ (c) $A_1 \otimes B_0$ (d) $A_1 \otimes B_1$

图4. 纠缠蒸馏的最优测量电路。最优CHSH测量在各方的第一个量子比特上执行（图 6 中的量子比特 0 和 3），因为贝尔对是在这两个量子比特之间生成的。



(a) $A_0 \otimes B_0$ (b) $A_0 \otimes B_1$ (c) $A_1 \otimes B_0$ (d) $A_1 \otimes B_1$

图 5. 方程 4 给出的最优非局域性蒸馏测量电路。

关键区别出现在第 2 阶段的纠缠蒸馏过程中（图 6）。这是整个过程中最耗费资源的主要任务；即使不考虑参与方之间通信的需求，这一点也成立。这是意料之中的，因为这项任务对应于提纯量子态所需的工作。然而，非定域性蒸馏并没有类似的任务需要执行。这凸显了与非定域性蒸馏相比，纠缠蒸馏对实验资源的需求显著更高。

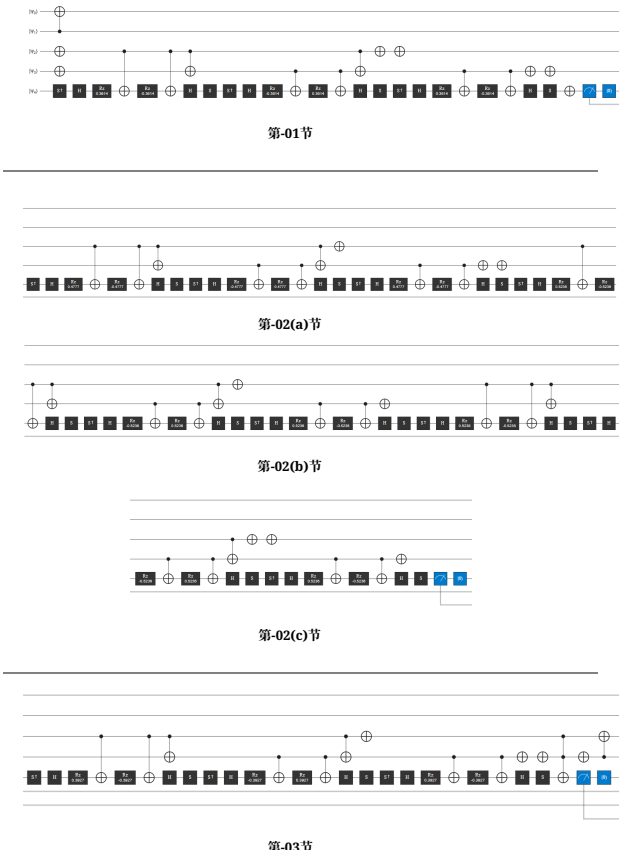


图6. 从两个噪声态副本生成贝尔态的纠缠蒸馏电路。该电路分为三个部分，分别对应对辅助量子比特（量子比特4）的三次测量。

表 I 使用 Azure资源估算器对两个 $|\Psi\rangle$ 副本进行非定域性蒸馏与纠缠蒸馏的资源需求

	资源指标			
	逻辑量子比特	逻辑深度 T态数量		运行时间（秒）
非定域性蒸馏	15	63	150	0.00025
纠缠蒸馏	18	512	500	0.00225

表 I 展示了使用 $|\Psi\rangle$ 的两个副本实施非定域性和纠缠蒸馏协议所需的资源。比较结果显然表明，非定域性蒸馏所需的资源显著更少。

IV. 讨论

对于纯态和混合态的非定域性蒸馏及其相应测量，一般情况下仍有待证明其最优性界。有人批评我们的比较，理由是纠缠蒸馏过程中需要通信。如果参与者可以通信，Alice 只需将自己的输入告知 Bob，反之亦然，因此就没有必要进行蒸馏。然而，纠缠蒸馏过程中传递的比特不包含关于参与者输入的任何信息，它仅用于提纯量子态。因此，既然非定域性蒸馏能够胜过纠缠蒸馏——尽管后者需要通信——这恰恰进一步支持了这样一种观点：纠缠和非局域性是不同的资源。

最近，Sun 等人 [24] 已表明，纠缠蒸馏可用于提升量子密钥分发中密钥的可蒸馏性。利用非局域性蒸馏更优的性能，是否也有可能获得更高的密钥率？设备无关量子密钥分发使 Alice 和 Bob 即使在生成密钥所用的物理设备不可信的情况下，也能成功共享密钥。

Farkas 等人 [25] 已表明，对 Werner 态进行测量可得到某些非定域关联，而这些关联要么无法用于密钥生成，要么需要新的协调技术。因此，非定域关联并不必然意味着设备无关量子密钥分发协议具有保密性。同时，已知即使非局域性任意小，设备无关量子密钥分发速率也可能无界 [26]。因此，密钥的保密性取决于生成过程中双方共享的非定域关联结构。我们提出在这些协议中使用非局域性蒸馏作为一种可能的协调技术。最后，这种技术或可提供一些实例，表明经典量子协议与量子协议在密钥协商中可容忍的噪声极限并不相同 [27]。

参考文献

[1] N. Brunner、N. Gisin 和 V. Scarani，《纠缠与非局域性是不同的资源》，*NJP*，第 7 卷，第 88 页，2005 年。[2] N. Brunner、D. Cavalcanti、S. Pironio、V. Scarani 和 S. Wehner，《贝尔非定域性》，*RMP*，第 86 卷，第 419–478 页，2014 年。[3] C. Bennett、H. Bernstein、S. Popescu 和 B. Schumacher，《通过局域操作浓缩部分纠缠》，*PRA*，第 53 卷，第 2046 页，1996 年。[4] C. H. Bennett、G. Brassard、S. Popescu、B. Schumacher、J. A. Smolin 和 W. K. Wootters，《通过有噪信道提纯噪声纠缠并实现忠实隐形传态》，*PRL*，第 76 卷，第 722 页，1996 年。[5] H. Lo 和 S. Popescu，《通过局域操作浓缩纠缠：超越均值》，*PRA*，第 63 卷，第 022301 页，2001 年。[6] A. Peres，《量子非定域性的集体检验》，*PRA*，第 54 卷，第 4 页，1996 年。[7] J. Clauser、M. Horne、A. Shimony 和 R. Holt，《检验局域隐变量理论的实验方案》，*PRL*，第 23 卷，第 880 页，1969 年。[8] Y. Liang 和 A. Doherty，《通过集体测量实现更强的贝尔不等式违背》，*PRA*，第 73 卷，第 052116 页，2006 年。[9] D. Dukaric 和 S. Wolf，《非局域性蒸馏的上限》，*arXiv* 预印本 *arXiv:0808.3317*，2008 年。[10] J. Allcock、N. Brunner、M. Pawłowski 和 V. Scarani，《从信息因果性中恢复量子与非量子关联边界的一部分》，*PRA*，第 80 卷，第 040103 页，2009 年。[11] P. Høyer 和 J. Rashid，《非定域性蒸馏的最优协议》，*PRA*，第 82 卷，第 042118 页，2010 年。[12] M. Forster，《非定域性蒸馏协议的界限》，*PRA*，第 83 卷，第 062114 页，2011 年。[13] N. Gisin 和 A. Peres，《任意大自旋的贝尔不等式最大违背》，*PLA*，第 162 卷，第 15–17 页，1992 年。[14] E. Hansen、S. Joshi 和 H. Rarick，《量子乘法算法的资源估算》，载于*2023*年 *IEEE* 量子计算与工程国际会议 *(QCE)*，第 2 卷。IEEE，2023 年，第 199–202 页。[15] N. Quetschlich、M. Soeken、P. Murali 和 R. Wille，《利用资源估算开发量子计算应用》，*arXiv* 预印本，卷号 arXiv:2402.12434，2024 年。

[16] W. van Dam、M. Mykhailova 和 M. Soeken，《使用 Azure Quantum 资源估算器评估容错量子计算的性能》，载于*SC'23* 高性能计算、网络、存储与分析国际会议研讨会论文集。ACM，2023 年。[17] K. O. 等，《PyLIQTR（林肯实验室量子算法测试与研究）》，https://github.com/isi-usc-edu/pyLIQTR，2023 年。[18] 谷歌，《Qualtran 文档》，https://qualtran.readthedocs.io/en/ latest/，2023 年。[19] Z. AI，《BenchQ：容错量子计算的资源估算》，https://github.com/zapatacomputing/benchq，2023 年。[20] 《量子资源估算器》，https://github.com/microsoft/qdk/tree/main/source/resource estimator。[21] E. Knill，《量子电路近似》，*arXiv* 预印本 *quant- ph/9508006*，未发表，1995 年。[22] N. Gleinig 和 T. Hoefler，《一种高效的稀疏量子态制备算法》，载于*2021* 年第 *58* 届 *ACM/IEEE* 设计自动化会议 *(DAC)*。IEEE，2021 年，第 433–438 页。[23] R. U. Din，《量子稀疏态制备算法实现》，2025 年，https://github.com/Razeen-ud-din/Quantum-Resource-Estimation-for-Distillation。[24] S. Sun、K. Goodenough、D. Bhatti、K. Azuma 和 D. Elkouss，《通过纠缠蒸馏和经典优势蒸馏增强密钥的可蒸馏性》，*PRA*，第 112 卷，第 052602 页，2025 年 11 月。 [在线]。网址：https://link.aps.org/doi/10.1103/95k8-3zxd [25] M. Farkas、J. Haah、D. Elkouss 和 V. B. Scholz，《贝尔非定域性不足以保障标准设备无关量子密钥分发协议的安全性》，*PRL*，第 127 卷，第 5 期，第 050503 页，2021 年。[26] L. Wooltorton、P. Brown 和 R. Colbeck，《具有任意小非局域性的设备无关量子密钥分发》，*PRL*，第 132 卷，第 21 期，第 210802 页，2024 年。[27] N. Gisin 和 S. Wolf，《经典与量子密钥协商的联系：是否存在“束缚信息”？》，载于密码学进展——*CRYPTO 2000*，《计算机科学讲义》系列，2000 年 8 月，第 482–500 页。