arXiv:2601.15393v1 [quant-ph] 21 Jan 2026

计算双向量子容量

J. J. Meyer，[1]J. Rizzo，[1]A. Raza，[1]L. Leone，[2,1]S. Jerbi，[1,3]以及 J. Eisert[1,3,4]
达勒姆复杂量子系统中心，柏林自由大学，德国柏林 *14195*[2]工业工程系，萨勒诺大学，意大利菲夏诺（*SA*）*84084*[3]柏林亥姆霍兹材料与能源中心，德国柏林 *14109*[4]弗劳恩霍夫海因里希·赫兹研究所，德国柏林 *10587*（日期：2026 年 1 月 23 日）

量子信道容量是量子信息论的基础。然而，其定义并不限制发送方和接收方所使用的计算资源。在这项工作中，我们开启了对计算量子容量的研究。这些容量刻画了在施加这样一个自然要求时，能够可靠传输的信息量：编码和解码必须具备计算效率。我们聚焦于计算双向量子容量，并展示它与该信道 Choi 态的计算可蒸馏纠缠密切相关。这一联系使我们能够展示一种显著的计算容量分离。在标准密码学假设下，存在一个具有多项式复杂度的量子信道，其计算双向量子容量为零，而其无界版本却接近最大值。此外，我们还证明，当信道复杂度超出多项式范围时，计算量子容量会从接近最大值骤然转变为零。我们的结果表明，对计算效率的自然要求可以彻底改变量子通信的极限。

量子信息论致力于探究以量子系统作为信息载体来完成任务的潜力与局限。其基本框架主要在 20 世纪 90 年代形成，之后又得到完善或严格化；它是量子技术赖以建立的概念与数学支柱之一 [1–5]。量子信道容量是这一框架的核心，它衡量量子比特通过噪声量子信道进行可靠传输的速率，甚至还能限定量子纠错所需的开销 [6]。研究发现，量子容量由正则化相干信息给出，体现了该量本质上的渐近特性[2–5]。这反映出，在传送量子信息时

在发送方通过信道的多个副本向接收方传输信息时，可以采用日益复杂的编码与解码程序。

在这项工作中，我们对这一图景提出质疑，并得出了出人意料且可能令人惊讶的结论。我们的做法是采用这样一个前提：此类通信任务中的所有步骤都必须使用多项式资源来完成。这是计算机科学和量子计算中的一项基础性认识：只有当步骤总数随输入规模以多项式增长时，任务才被认为是可行的，或称“高效”的。因此，自然应要求只使用多项式数量的副本，并且在编码与解码过程中只实施多项式数量的量子门。

受这一推理启发，我们开始研究计算双向量子容量，即严格遵守这些多项式约束条件下的双向量子容量。由此，我们在计算量子信息论 [7–11], 中确立了一个新的方向，确保所计算的容量能够在操作上实现。我们发现，它与 Choi 态的计算可蒸馏纠缠密切相关，这与传统的无约束情形相呼应，同时也体现了双分体情景中纠缠的资源属性。这一洞见

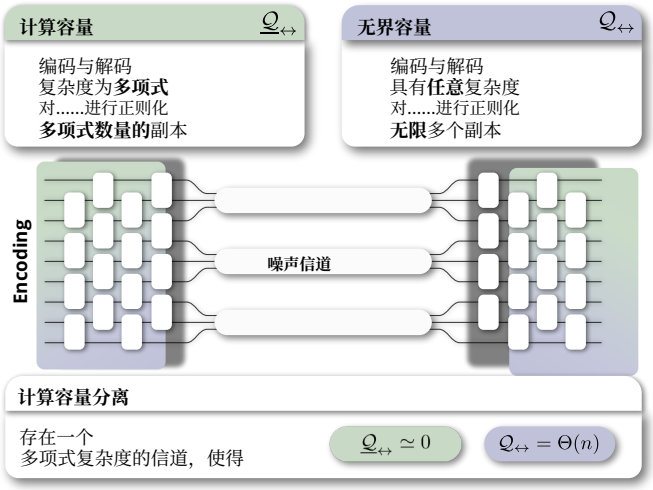


图 1. 计算双向量子容量刻画了在所涉及的操作具有多项式复杂度时，借助双向经典通信进行量子信息传输的极限。与传统的无界情形相比，差异可能相当显著：正如我们所展示的，存在一种信道，其无界量子容量几乎达到最大值，但计算双向量子容量却趋于零。

为评估计算双向量子容量提供了一种定量工具。尤为重要的是，它带来了一个引人注目的分离结果：在标准密码学假设下，存在计算复杂度为多项式且具有物理意义的量子信道，其计算双向量子容量为零，而其传统的、不受限制的双向量子容量则随系统规模增长。这一现象可被视为量子信息中一种计算受限容量。更进一步，我们证明，广义退相位

信道的计算双向量子容量会随其 Choi 秩发生明显的转变。在 Choi 秩为多项式的情形下，我们给出一种计算高效的协议，可实现近乎最优的量子容量；而一旦 Choi 秩变为超多项式，计算容量便可能降为零。

我们的工作的要旨是，要全面理解量子通信理论，就必须重新审视其基本前提，并考虑这些前提可能隐含要求的超多项式——因而不合理的——资源。自量子通信理论和量子计算问世以来，三十多年已经过去，这两个领域应当更加充分地融合，而且应当明确，高效操纵量子信息的概念对二者都至关重要。

计算信息论。尽管我们进入了量子通信这一新的概念领域，但很大程度上仍沿用参考文献 [10], 的符号体系，该文研究了假设检验中的计算约束。在计算（量子）信息论中，我们根据一个尺度变量 $n \in \mathbb{N}$来量化实现操作和协议的复杂度。因此，我们始终处理对象的序列，例如量子态、信道或希尔伯特空间。为使符号简洁，我们约定，索引n 表示一列对象，其中 $n \in \mathbb{N}$， ρ_n 例如表示量子态序列（ρ_n）$_{n\in\mathbb{N}}$。

为了衡量量子信道 Φ 的复杂度，我们固定如下计算模型：通过访问任意多个处于 $|0\rangle$ 态矢量中的辅助系统，来实现对输入量子态的操作。所有操作均由所选系统中的基本二局部门组成，随后进行测量；测量要么投影到 $|0\rangle$，要么忽略该系统。这类门的数量就是信道的复杂度 $C(\Phi)$。请注意，在此模型中，偏迹是一种免费操作。

上述概念使我们能够定义量子信息处理任务的门约束版本。我们使用的最重要任务是纠缠蒸馏：我们的任务是使用复杂度有界的 LOCC（局部操作与经典通信）映射，从共享的资源态中蒸馏出最大纠缠态。令 $\mathrm{LOCC}(A|B;G)$ 表示相对于双部系统 A， B 、复杂度至多为 G 的 LOCC 映射集合，并令 ϕ 为一个纠缠比特（最大纠缠量子比特态）。那么，在误差有界的条件下，可蒸馏的最大纠缠量为 [12]

$$E_D^{\epsilon}(\rho^{A,B};G) = \log 2 \times \max\big\{m \in \mathbb{N} \,\big|\, \exists \Phi \in \mathrm{LOCC}(A|B;G)\colon F(\Phi[\rho^{A,B}], \phi^{\otimes m}) \geq 1-\epsilon\big\}. \tag{1}$$

这里， $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ 是量子保真度 [13]。

为了得到一个能够体现利用多项式资源可以蒸馏出多少纠缠的本质的量，我们对上述量进行多项式正则化。相关数学背景见参考文献 [10], ，此处仅提及要点。在这种设定下，我们关注这些量在可忽略项以内的渐近标度，即比任何多项式都更快趋于零的项，记作 $\mathrm{negl}(n)$。我们用记号 $f \simeq g$ 表示 $f-g$ 是一个可忽略函数，并用相关的序关系 $\gtrsim$和 $\lesssim$表示。现在给出量子态 $\rho^{A_n,\ B_n}_n$ [10]的计算可蒸馏纠缠定义（另请参见参考文献 [7–9, 11]中的类似概念）：

$$\underline{E}_D(\rho_n^{A_n,B_n}) :\simeq \lim_{\epsilon\to 0}\lim_{\ell\to\infty}\liminf_{k\to\infty}\frac{1}{n^k}E_D^{\epsilon}((\rho_n^{A_n,B_n})^{\otimes n^k}; n^{k\ell}). \tag{2}$$

记号 $:\simeq$表示，右侧应被理解为函数空间中的一个对象；该空间是从通常的函数空间中对等价关系 $f \simeq g$ 取商后得到的。文献 [10] 证明，这构成了一个度量空间，进而使我们能够合理地讨论其中涉及的极限；这些极限被视为函数的极限，而非逐点极限。极限 $k\to\infty$将副本数取为任意大的多项式，从而使我们能够忽略某些修正项。极限 $\ell\to\infty$ 将门的数量取为任意大的多项式，确保我们能够实现所有多项式复杂度操作。极限 $\epsilon\to 0$ 是可蒸馏纠缠定义中的标准组成部分。

最后，如果对于所有多项式复杂度的POVM效应 $C(\Lambda_n) \leq O(\mathrm{poly}(n))$以及所有 $m_n \leq O(\mathrm{poly}(n))$，我们都有：那么，我们就认为两个量子态 ρ_n 和 σ_n 在计算上不可区分， $\rho_n \approx_c \sigma_n$。

$$|\operatorname{Tr}[\Lambda_n\rho_n^{\otimes m_n}] - \operatorname{Tr}[\Lambda_n\sigma_n^{\otimes m_n}]| \leq \mathrm{negl}(n). \tag{3}$$

计算双向量子容量。现在我们转而定义计算双向量子容量。为此，我们先回顾标准定义。两个量子信道 Φ 和 Ψ之间的最坏情形信道保真度定义为

$$F(\Phi,\Psi) := \inf_{\psi} F((\mathbb{I}\otimes\Phi)[\psi], (\mathbb{I}\otimes\Psi)[\psi]), \tag{4}$$

其中， F是量子态的保真度，辅助系统的维度与输入系统相同。为了涵盖局部操作与经典通信（LOCC）操作，我们将使用量子组合这一概念。对我们而言，只需该概念能够表示一种输入和输出均为量子信道的映射，并能够模拟自适应计算。我们用符号 $\Phi^{[m]}$ 表示代表对基本信道 Φ进行 m 次独立调用的组合。现在用 $\mathbb{I}_d$ 表示一个 d 维恒等信道。量子信道的单次双向量子容量定义为 [12]

$$\mathcal{Q}_{\leftrightarrow}^{\epsilon}(\Phi) := \log\max\big\{d\in\mathbb{N}\,\big|\, \exists\mathcal{L}: F(\mathcal{L}[\Phi], \mathbb{I}_d) \geq 1-\epsilon\big\},$$

其中 $\mathcal{L}$是一个 LOCC 梳（相对于输入端和输出端），用于表示编码和解码。双向量子容量随后通过正则化定义为

$$\mathcal{Q}_{\leftrightarrow}(\Phi) := \lim_{\epsilon\to 0}\lim_{m\to\infty}\frac{1}{m}\mathcal{Q}_{\leftrightarrow}^{\epsilon}(\Phi^{[m]}). \tag{5}$$

沿袭前一节的论述，我们通过对单次设置施加门限制，再进行多项式正则化，定义双向量子容量的计算版本。

定义 1（计算双向量子容量）。我们将量子信道 Φ的 G-复杂度单次双向量子容量定义为

$$\begin{aligned}\mathcal{Q}^{\epsilon}_{\leftrightarrow}(\Phi;G) \coloneqq \log\max\{d\in\mathbb{N}\,|\\ \exists\mathcal{L}: C(\mathcal{L})\leq G, F(\mathcal{L}[\Phi],\mathbb{I}_d)\geq 1-\epsilon\},\end{aligned} \tag{6}$$

其中 $\mathcal{L}$ 是一个局部操作与经典通信梳。信道 Φ_n 的计算双向量子容量定义为

$$\underline{\mathcal{Q}}_{\leftrightarrow}(\Phi) :\simeq \lim_{\epsilon\to 0}\lim_{\ell\to\infty}\liminf_{k\to\infty}\frac{1}{n^k}\mathcal{Q}^{\epsilon}_{\leftrightarrow}(\Phi_n^{[n^k]};n^{k\ell}). \tag{7}$$

高效可延展信道的容量。本节旨在通过为一大类信道建立容量公式，为我们的分离结果奠定基础。我们将紧密遵循文献 [14]，并特别关注相关操作的计算效率。我们从一个定义开始。

定义 2（高效可延展性）。如果存在一个多项式复杂度的局部操作与经典通信映射 $\mathcal{L}^{A_n,\ A'_nB_n}_{n}C(\mathcal{L}^{A_n,\ A'_nB_n}_{n})\leq O(\mathrm{poly}(n))$，其中局部操作与经典通信是相对于二分划分 A_n, A'_nB_n 而言，且存在一个量子态 $\sigma^{A'_n,\ B_n}_{n}$，使得量子信道 $\Phi_n^{A_n\to B_n}$可高效拉伸

$$\Phi_n^{A_n\to B_n}[X^{A_n}] = \mathcal{L}_n^{A_n,A'_nB_n}[X^{A_n}\otimes\sigma_n^{A'_n,B_n}]. \tag{8}$$

量子态 $\sigma^{A'_n,\ B_n}_{n}$无需具有多项式复杂度。我们进一步将量子信道称为高效 Choi 可拉伸，如果该信道的 *Choi* 态 $\sigma_n^{A'_nB_n}=J_{\Phi_n}$ 可以高效拉伸。

下文中，通常会省略对子系统的精确标识，因为上下文已足以明确其含义。参考文献 [14] 已证明，所谓的传态协变性蕴含 Choi 可延展性。为验证高效 Choi 可延展性，我们将证明一个类似的结果，并着重说明这种蕴含关系能够保持计算效率。所引用的传态校正酉算子出现在广义量子传态协议 [12, 第 3.3 节2],中；就我们的目的而言，只需知道这些操作是单局域的。

引理 3（高效 Choi 可拉伸性）。考虑一个量子信道 Φ_n: $\mathcal{H}_n\to\mathcal{K}_n$ 其多项式复杂度为 $C(\Phi_n)\leq O(\mathrm{poly}(n))$，且 $\log\dim\mathcal{H}_n\leq O(\mathrm{poly}(n))$。若该信道具有传态协变性，即对于任意传态校正酉算子 U_i，均存在一个酉算子 V_i，使得

$$\Phi_n[U_iXU_i^\dagger] = V_i\Phi_n[X]V_i^\dagger, \tag{9}$$

该信道是高效 *Choi* 可拉伸的。

证明推迟到文末给出。现在让我们分析高效可拉伸信道的容量。首先给出一个适用于所有量子信道的可达性结论，它在量子通信的背景下，为 Choi 态的计算可蒸馏纠缠赋予了直接的操作意义。

引理 4（计算双向量子容量的下界）。考虑一个量子信道 Φ_n，其 *Choi* 态为 J_{Φ_n}。那么，计算双向量子容量的下界为

$$\underline{\mathcal{Q}}_{\leftrightarrow}(\Phi_n)\gtrsim\underline{E}_D(J_{\Phi_n}). \tag{10}$$

证明。制备最大纠缠态是一种高效操作。将其中一半通过给定信道发送后，双方各自获得一份 Choi 态，并在其上执行最优的高效蒸馏协议。获得蒸馏出的纠缠比特后，双方通过常规量子隐形传态传输所需信息。量子隐形传态是高效的，因此该协议也是高效的，从而证明了所给不等式。□

在为所有信道确立计算双向容量的下界后，我们给出一个适用于所有可高效拉伸的信道的上界。

引理 5（计算双向容量的上界）。考虑一个量子信道 Φ_n，它可高效拉伸为 $\Phi_n[X]=\mathcal{L}_n[X\otimes\sigma_n]$。那么，计算双向量子容量的上界为

$$\underline{\mathcal{Q}}_{\leftrightarrow}(\Phi_n)\lesssim\underline{E}_D(\sigma_n). \tag{11}$$

证明。这直接源自文献 [14], ，其中证明了，实现通过 m 个信道副本传输的双向局部操作与经典通信梳 $\mathcal{L}_0$，可以与实现该信道的 m 局部操作与经典通信操作 $\mathcal{L}_n$ 组合，从而得到一个作用于 m 个资源态 $\mathcal{L}'_n[\sigma_n^{\otimes m}]$的复合局部操作与经典通信映射 $\mathcal{L}'_n$。重要的是，$\mathcal{L}'_n$ 的复杂度满足

$$C(\mathcal{L}'_n)\leq C(\mathcal{L}_0)+mC(\mathcal{L}_n), \tag{12}$$

如果所有相关操作的复杂度均为多项式，且我们使用多项式数量的副本，那么该复杂度就是多项式。由于蒸馏纠缠比特与传输量子比特是等价的，这意味着双向量子容量至多等于在对 $\mathcal{L}'$ 具有完全控制权时所能实现的可蒸馏纠缠。□

对于高效的 Choi 可拉伸信道，这些条件彼此一致，因此我们能够完全刻画其计算双向量子容量。

定理 6（双向容量的刻画）。考虑一个量子信道 Φ_n，其可高效 *Choi*-延展为 $\Phi_n[X]=\mathcal{L}_n[X\otimes J_{\Phi_n}]$。那么，计算双向量子容量为

$$\underline{\mathcal{Q}}_{\leftrightarrow}(\Phi_n)\simeq\underline{E}_D(J_{\Phi_n}). \tag{13}$$

证明。 由上述两个引理可立即得到。 □

计算容量与无界容量的分离。现在我们转而描述前文提到的显著分离。对于比特串 $x \in \{0,1\}^n$ 上给定的概率分布 $p(x)$，记 $Z^x = Z^{x_1} \otimes Z^{x_2} \otimes \cdots \otimes Z^{x_n}$，以定义广义退相位信道如下

$$\mathcal{D}_p[\rho] \coloneqq \sum_{x\in\{0,1\}^n} p(x) Z^x \rho Z^x. \tag{14}$$

我们注意到，上述信道是泡利信道，因此 可高效地进行 *Choi* 拉伸 [14]。其高效性直接源于以下事实：只需将标准量子隐形传态协议中的最大纠缠态替换为该泡利信道的 Choi 态，即足以对其进行模拟 [15]。这一联系使我们能够推导出双向量子容量的以下公式，另见文献。 [12, 16]。

引理 7 （退相干量子信道的双向量子容量）。 考虑广义退相位信道D_p。则

$$\mathcal{Q}_{\leftrightarrow}(\mathcal{D}_p) = E_D(J_{\mathcal{D}_p}) = D(p \,\|\, u). \tag{15}$$

我们注意到，与文献 [17], 的结果类似，对于这类信道，量子容量与强逆私密容量之间的所有容量实际上都相等。

证明概要。 正如文献 [14], 所指出的，导致我们得到 定理 6的推理同样适用于无界情形，并表明无界双向量子容量与 Choi 态的可蒸馏纠缠相等。随后，我们通过在最大纠缠输入态矢量上计算单副本相干信息来给出双向量子容量的下界，该态矢量的熵等于分布 p 的熵，因为不同的泡利算子会将最大纠缠态映射为相互正交的态。接着，我们使用 Rains 界对可蒸馏纠缠给出上界，其中以完全退相干信道的 Choi 态作为候选态。通过认识到，对于任意分布 p，$\mathcal{D}_p[\rho] = \mathcal{T}[\rho \otimes p]$ 存在一个映射 $\mathcal{T}$，它只需测量经典寄存器，并在输入寄存器上施加相应的泡利算子，即可得到相匹配的上界。由此，我们通过数据处理得出结论。完整证明见文末材料。

□

在无界情形下确定了广义退相位信道的容量后，我们可以利用计算双向量子容量的公式，证明存在显著差距。

定理 8 (计算容量分离)。 假设量子安全的一对一单向函数存在，则对于所有 $\delta > 0$，存在一个多项式复杂度为 $\mathcal{D}_n$ 的量子信道，使得

$$\underline{Q}_{\leftrightarrow}(\mathcal{D}_n) \simeq 0, \textit{ but } Q_{\leftrightarrow}(\mathcal{D}_n) = n\log 2 - \Omega(n^\delta). \tag{16}$$

证明概要。 我们利用这样一个事实：与通过计算不可区分的分布定义的信道相关联的 Choi态继承了这种计算不可区分性。随后我们证明，在该定理的密码学假设下，存在一个与均匀分布计算不可区分且熵为n^δ的分布，由此证明无界双向量子容量的结论。最后，我们通过证明计算可蒸馏纠缠具有计算平滑性质来完成证明；该性质使我们能够利用 Choi 态的计算不可区分性，得出计算可蒸馏纠缠至多等于完全退相干信道的 Choi 态的计算可蒸馏纠缠，而后者为零。完整证明详见文末材料。

□

计算容量的急剧转变。 现在，除了计算容量与无界容量之间的差距外，我们还将展示另一种显著现象：广义退相位信道的计算容量会随着相关概率分布支撑集的大小，从接近最大值急剧降至零。对于任意子集 $S_n \subseteq \{0,1\}^n$，定义 u_{S_n} 为 S_n 上比特串的均匀分布，并简记为$\mathcal{D}_{S_n} = \mathcal{D}_{u_{S_n}}$。采用这一记号，我们可以证明如下结论。

定理 9 （计算容量的急剧转变）。考虑量子信道 $\mathcal{D}_{S_n}$。那么，对于任意满足 $|S_n| \le O(\text{poly}(n))$ 的 S_n，有

$$\underline{\mathcal{Q}}_{\leftrightarrow}(\mathcal{D}_{S_n}) \gtrsim n\log 2 - \omega(\log n) \tag{17}$$

在这种情况下，这是近乎最优的，因为 $\mathcal{Q}_{\leftrightarrow}(\mathcal{D}_{S_n}) = n\log 2 - O(\log n)$。然而，假设量子安全的一对一单向函数存在，则存在一个子集 S'_n，满足$|S'_n| = \omega(\text{poly}(n))$，使得

$$\underline{\mathcal{Q}}_{\leftrightarrow}(\mathcal{D}_{S'_n}) \simeq 0. \tag{18}$$

证明概要。我们给出一种协议，可达到定理陈述中的计算容量；只要 $|S_n| \le O(\text{poly}(n))$，该协议就是高效的。协议首先应用 Hadamard 门，使我们处理比特翻转 X^x而非相位翻转 Z^x。接着，我们利用这一事实：该广义比特翻转信道的 Choi 态是最大纠缠态的混合态，其中每个副本都带有一个未知的校正 X^x。Alice 和 Bob 应用一个随机 Clifford，使得 X^x 映射为 $X^{\pi(x)}$，其中 $\pi(x)$ 是一个均匀随机且不同于恒等元的比特串。然后，他们测量前 $m = \omega(\log n)$ 个比特；我们证明，这些信息足以在 $\pi(S_n)$ 中可靠地找到 $\pi(x)$，并且只要 $|S_n| \le O(\text{poly}(n))$，这一过程就是高效的。随后，Alice 和 Bob 撤销 $X^{\pi(x)}$，剩下 $n - \omega(\log n)$ 个纠缠比特。对于 $|S_n| = \omega(\text{poly}(n))$ 的过渡是定理 8 的推论，因为注意到本证明中使用的分布具有所需的形式即可。完整证明见附录。

□

展望。 在这项工作中，我们挑战了既有的量子通信观念，接受所有步骤

都必须高效，才能最终得到有意义的量子容量概念。我们希望本项工作有助于倡导一种高效的量子信息论范式，承认归根结底只有高效的协议才能付诸实施，从而让量子计算与量子通信的概念更加紧密地联系在一起。

致谢。 本项目获得了 BMFTR（QR.N、DAQC、QSol、MuniQC-Atoms、Hybrid++）、BMWK（EniQmA）、慕尼黑量子谷（K- 8）、卓越集群（ML4Q 和 MATH+）、Berlin Quantum、QuantERA（HQCC）、量子旗舰计划（MillenionandPasquans2）以及欧洲研究委员会（DebuQC）的资助。

[1] C. H. Bennett、D. P. DiVincenzo、J. A. Smolin 和 W. K. Wootters，《混合态纠缠与量子纠错》，Phys. Rev. A 54，3824（1996）。[2] S. Lloyd，《噪声量子信道的容量》，Phys. Rev. A 55，1613（1997）。[3] I. Devetak，《量子信道的私有经典容量与量子容量》，IEEE Trans. Inf. Th. 51，44（2005）。[4] M. M. Wilde，《量子信息论》（剑桥大学出版社，剑桥，2013）。[5] J. Watrous，《量子信息理论》，第 1 版（剑桥大学出版社，2018）。[6] O. Fawzi、A. M¨uller-Hermes 和 A. Shayeghi，《容错量子计算空间开销的下界》，LIPIcs，第 215 卷，ITCS 2022 215，68:1，2202.00119。[7] S. Aaronson、A. Bouland、B. Fefferman、S. Ghosh、U. Vazirani、C. Zhang 和 Z. Zhou，《量子伪纠缠》（2022），arXiv:2211.00747。[8] R. Arnon、Z. Brakerski 和 T. Vidick，《计算纠缠理论》（2023），arXiv:2310.02783。[9] L. Leone、J. Rizzo、J. Eisert 和 S. Jerbi，《有限计算资源下的纠缠理论》，Nature Phys. 21，1847（2025）。[10] J. J. Meyer、A. Raza、J. Rizzo、L. Leone、S. Jerbi 和 J. Eisert，《计算相对熵》（2025），arXiv:2509.20472。[11] ´A. Y´ang¨uez、T. A. Hahn 和 J. Kochanowski，《高效量子测量：计算最大散度与测量 Rényi 散度及其应用》（2025），arXiv:2509.21308。[12] S. Khatri 和 M. M. Wilde，《量子通信理论原理：一种现代方法》（2020），arXiv:2011.04672。[13] 因我们约定 log 表示自然对数，所以会出现因子 log 2；这是因为需要将比特转换为奈特。[14] S. Pirandola、R. Laurenza、C. Ottaviani 和 L. Banchi，《无中继量子通信的基本极限》，Nature Comm. 8，15043（2017）。[15] G. Bowen 和 S. Bose，《作为退极化量子信道的量子隐形传态、相对熵与经典容量》，Phys. Rev. Lett. 87，267901。[16] M. M. Wilde、M. Tomamichel 和 M. Berta，《量子信道私有通信的反向界》，IEEE Trans. Inf. Theory 63，1792（2017）。[17] L. Lami 和 M. M. Wilde，《玻色退相位信道量子容量与私有容量的精确解》，Nature Phot. 17，525。[18] A. Srinivasan 和 Y. Shah，CSC 2426：密码学基础——密码学，第4讲：Goldreich–Levin 与计算不可区分性，《课程讲义》，多伦多大学（2023 年）。[19] A. Gu、L. Leone、K. Goodenough 和 S. Khatri，《通过搅乱实现恒定开销的纠缠蒸馏》（2025 年），arXiv:2502.09483。

附录

定理 3 的证明。定理 3。事实是， Φ_n 是 Choi 可拉伸的，这一点已在参考文献 [14]中证明。下面只需论证， V_i 必然具有多项式复杂度。由于 Φ_n 在我们的计算模型中具有多项式复杂度，因此存在一个具有多项式复杂度的酉扩张 W_n ，使得

$$\Phi_n[X] = \mathrm{Tr}_{\mathrm{anc}}[W_i(|0\rangle\langle 0|_{\mathrm{anc}} \otimes X)W_i^\dagger]. \tag{19}$$

利用扩张，我们得到等式

$$\begin{aligned} & V_i\Phi_n[X]V_i^\dagger \\ &= V_i\,\mathrm{Tr}_{\mathrm{anc}}[W_i(|0\rangle\langle 0|_{\mathrm{anc}} \otimes X)W_i^\dagger]V_i^\dagger \\ &= \mathrm{Tr}_{\mathrm{anc}}[(Q_i \otimes V_i)W_i(|0\rangle\langle 0|_{\mathrm{anc}} \otimes X)W_i^\dagger(Q_i \otimes V_i)^\dagger], \end{aligned} \tag{20}$$

其中，我们用到了这样一个事实： V_i 仅作用于未被迹掉的系统，而 Q_i 是任意酉算子。类似地，从另一个方向可得

$$\begin{aligned} & \Phi_n[U_iXU_i^\dagger] \\ &= \mathrm{Tr}_{\mathrm{anc}}[W_i(|0\rangle\langle 0|_{\mathrm{anc}} \otimes U_iXU_i^\dagger)W_i^\dagger] \\ &= \mathrm{Tr}_{\mathrm{anc}}[\tilde{U}_iW_i(|0\rangle\langle 0|_{\mathrm{anc}} \otimes X)W_i^\dagger\tilde{U}_i^\dagger], \end{aligned} \tag{21}$$

其中$\tilde{U}_i^\dagger = W_i(\mathbb{I} \otimes U_i)W_i^\dagger$。由于两个表达式必须相等，因此必定存在某个 Q_i 使得

$$W_i(\mathbb{I} \otimes U_i)W_i^\dagger = Q_i \otimes V_i. \tag{22}$$

因此， V_i 可以实现为

$$V_i = \mathrm{Tr}_{\mathrm{anc}}[W_i(\mathbb{I} \otimes U_i)W_i^\dagger], \tag{23}$$

我们得到上界 $C(V_i) \le C(U_i) + 2C(W_i)$ $=C(U_i)$ $+ 2C(\Phi_n)$。根据假设， $C(\Phi_n) \le O(\mathrm{poly}(n))$。传态校正酉算子始终是单局域算子；当 $\log\dim\mathcal{H}_n \le O(\mathrm{poly}(n))$ 时，可以高效实现，而这由假设可知成立。因此， $C(V_i)$ $\le O(\mathrm{poly}(n))$，证毕。 □

定理 7 的证明。 正如文献 [14], 中所观察到的，导致我们得到 定理 6 的推理在无界情形下同样成立，这就证明了

$$\mathcal{Q}_{\leftrightarrow}(\mathcal{D}_p) = E_D(J_{\mathcal{D}_p}). \tag{24}$$

为确立双向容量的精确值，我们沿用文献 [17]，通过在最大纠缠输入态矢量上计算相干信息，为双向量子容量给出下界

$$\gamma^{A,B} = \frac{1}{2^n}\sum_{x,x'\in\{0,1\}^n} |x,x\rangle\langle x',x'|. \tag{25}$$

这得到

$$\begin{aligned} \mathcal{Q}_{\leftrightarrow}(\mathcal{D}_p) &\ge \mathcal{Q}(\mathcal{D}_p) \ge S(\mathcal{D}_p[\gamma^A]) - S((\mathcal{D}_p \otimes \mathbb{I})[\gamma^{AB}]) \\ &= n\log 2 - S(J_{\mathcal{D}_p}). \end{aligned} \tag{26}$$

Choi 态的熵可直接计算为

$$\begin{aligned} S(J_{\mathcal{D}_p}) &= (\mathcal{D}_p \otimes \mathbb{I})[\gamma^{A_n,B_n}] \\ &= S\left(\sum_{x\in\{0,1\}^n} p(x)Z^x\gamma^{A_n,B_n}Z^x\right) = S(p), \end{aligned} \tag{27}$$

因为所有量子态 $Z^x\gamma Z^x$ 彼此正交。注意到 $n\log 2 - S(p) = D(p\,\|\,u)$，即可确定下界。为证明上界，我们使用 Rains 界关于可蒸馏纠缠的结果，该结果断言 $E_D(\rho^{A,B}) \le \min_{\sigma^{A,B}\in\mathrm{PPT}} D(\rho^{A,B}\,\|\,\sigma^{A,B})$，其中相对熵是在所有正部分转置（PPT）态上取最小值。PPT 态的一个特例是最大经典关联态，即完全退相干信道的 Choi 态，

$$\bar{\gamma} = \frac{1}{2^n}\sum_{x\in\{0,1\}^n} |x,x\rangle\langle x,x| = J_{\mathcal{D}_u}. \tag{28}$$

现在我们利用这样一个事实：我们可以将广义退相位信道实现为 $\mathcal{D}_p[\rho] = \mathcal{T}[\rho \otimes p]$，其中 $\mathcal{T}$只需在计算基下测量经典寄存器，并在获得结果 x 后对输入寄存器实施 Z^x 。于是，我们有

$$\begin{aligned} E_D(J_{\mathcal{D}_p}) &\le D(J_{\mathcal{D}_p}\,\|\,J_{\mathcal{D}_u}) \\ &= D((\mathbb{I}\otimes\mathcal{D}_p)[\gamma]\,\|\,(\mathbb{I}\otimes\mathcal{D}_u)[\gamma]) \\ &= D(\mathbb{I}\otimes\mathcal{T})[\gamma\otimes p]\,\|\,(\mathbb{I}\otimes\mathcal{T})[\gamma\otimes u]) \\ &\le D(\gamma\otimes\,\|\,\gamma\otimes u) = D(p\,\|\,u). \end{aligned} \tag{29}$$

这里，我们将上述模拟论证与相对熵的数据处理性质结合起来，从而完成引理的证明。下面的评论源于我们直接给出了量子容量的下界，并且基于可蒸馏纠缠得到的上界同样适用于强逆私有容量 [16]这一事实。

□

证明定理 8。首先考虑与两个经典分布 p_n和 q_n 相关联的广义退相位信道，其中这两个分布在计算上不可区分。在这种情况下，相关信道的 Choi 态也具有计算不可区分性

$$p_n \approx_c q_n \;\Rightarrow\; J_{\mathcal{D}_{p_n}} \approx_c J_{\mathcal{D}_{q_n}}. \tag{30}$$

这是因为我们可以通过以下方式实现信道 $\mathcal{D}_{p_n}$：借助分布 p_n ，先在计算基下对其进行测量，得到结果 x，随后对输入量子态实施 Z^x 。输入最大纠缠态（该态可高效制备）后，我们便得到 Choi 态。因此，任何用于区分Choi态的协议都可以用来区分这些分布，从而导出矛盾。接下来，我们需要用到以下事实：根据定理陈述中关于单向函数存在性的假设，存在一个定义在长度为 n 的比特串上的经典分布p_n ，它在计算上与均匀分布 u_n 不可区分，但在同一

时间满足

$$D(p_n \,\|\, u_n) = n\log 2 - \Omega(n^\delta). \tag{31}$$

这里我们采用一种基于 Goldreich-Levin定理的标准构造（例如参见文献 [18]）。值得注意的是，该定理使我们能够构造一个伪随机生成器 $G\colon \{0,1\}^m \to \{0,1\}^{m+1}$，使得分布$\{G(x)\}_{x\leftarrow u_m}$ 在计算上与均匀分布 u_{m+1}不可区分；也就是说，它将 m比特的均匀分布扩展1比特。随后，我们可以递归地应用这一构造，在同一关于求逆单向函数的困难性假设下，将扩展量增至任意多项式(m)比特（参见文献 [18]中的推论1）。由于我们希望得到一个定义在 n 比特上的伪随机分布 p_n，因此对任意 $\delta > 0$，都可以选择$m = n^\delta$，并将 u_m 多项式地扩展至n 比特。该构造只使用 n^δ 比特随机性，因此给出了 p_n的熵的所需上界。我们需要的最后一个要素是证明，可高效蒸馏的纠缠 E_D 具有计算平滑性质 [10]。确实，考虑任意量子态 $\tilde{\rho}^{A_n}{}_n{}^{B_n}$，它在计算上与 $\rho^{A_n}{}_n{}^{B_n}$不可区分。那么，式（1）中单次可蒸馏纠缠定义的目标函数为

$$F(\Phi[\rho^{AB}, \phi^{\otimes m}] = \mathrm{Tr}[\Phi[\rho^{AB}]\phi^{\otimes m}] = \mathrm{Tr}[\rho^{AB}\Phi^\dagger[\phi^{\otimes m}]]. \tag{32}$$

在对 式（2） 进行正则化以获得计算可蒸馏纠缠时，我们注意到，POVM效应 $\Phi^\dagger[\phi^{\otimes m}]$ 的复杂度始终是多项式级的，因为最大纠缠态 ϕ 可以高效制备，且 Φ是一个高效的局部操作与经典通信映射。因此，计算不可区分性意味着：对于输入 $\rho^{A_n}{}_n{}^{B_n}$时能保证保真度至少为 $1-\epsilon$ 的任何协议，也必须保证对于 $\tilde{\rho}^{A_n}{}_n{}^{B_n}$的保真度为 $1-\epsilon-\mathrm{negl}(n)$。当 n 足够大时，我们总有该可忽略项为 $\le \epsilon$；取最终极限 $\epsilon \to 0$后，即可恢复

$$\underline{E}_D(\rho_n^{A_n,B_n}) = \underline{E}_D(\tilde{\rho}_n^{A_n,B_n}). \tag{33}$$

由于在所有计算不可区分的量子态中，$\tilde{\rho}^{A_n}{}_n{}^{B_n}$的选取是任意的，因此我们得到所需的计算平滑性质

$$\underline{E}_D(\rho_n^{A_n,B_n}) = \min_{\tilde{\rho}_n^{A_n,B_n} \approx_c \rho_n^{A_n,B_n}} \underline{E}_D(\tilde{\rho}_n^{A_n,B_n}). \tag{34}$$

因此，我们可以推知

$$\underline{E}_D(J_{\mathcal{D}_{p_n}}) \simeq \underline{E}_D(J_{\mathcal{D}_{u_n}}) \simeq 0, \tag{35}$$

后一个等式成立，是因为与均匀分布相关联的完全退相干信道的 Choi 态 u_n不含纠缠。由这些结果，定理陈述即可由定理 7在无界情形下的容量公式，以及定理 6中计算容量与可蒸馏纠缠之间的联系推出。

□

定理 9 的证明。我们将证明当 $|S_n| = O(\mathrm{poly}(n))$ 时，Choi 态 $J_{\mathcal{D}_{S_n}}$ 的可蒸馏纠缠具有可达性。首先，Alice 和 Bob 可以对各自的所有量子比特施加一层 Hadamard 门，将定义 $\mathcal{D}_{S_n}$ 中的算子 Z^x 转换为比特翻转X^x。接着，我们可以将 Choi 态视为如下形式的量子态的均匀混合：$(X^x \otimes \mathbb{I})\,|\gamma\rangle$，其中 $|\gamma\rangle$ 是最大纠缠态矢量，$x \in S_n$。我们的策略是，在不扰动过多量子比特的前提下，找出 x。为此，与参考文献 [19]，类似，Alice 和 Bob 随机均匀地选取一个 Clifford 操作 C_π；Alice 在 Choi 态的自己一半上实施 C_π，Bob 在自己一半上实施 C_π^T，从而实现比特串 $x \mapsto \pi$ 的一个置换 x，使得 $\pi(x)$ 在除全零比特串外的所有比特串上均匀分布。由于 Clifford 操作可在多项式时间内实现，因此通信成本也是多项式级的。像 $\pi(x)$ 这样的映像具有均匀性，这是 Clifford 群结构的结果：这意味着，对于x、$x' \neq 0$，概率 $C_\pi X^x C_\pi^\dagger = X^{x'}$ 在与将 x 映射到 x'的 Clifford 算子进行左右乘法后保持不变，由此可证明所诱导的比特串置换是均匀的。随后，Alice 和 Bob 分别测量经过上述变换的 Choi 态各自一半中的前 m 个量子比特，得到测量结果 y_A 和 y_B，其中 $y = y_A + y_B$ 等于$y = \pi(x)|_m$的前 m 个比特。我们声称，已知 y 足以以高概率从集合 $\pi(S_n)$ 中识别出 $\pi(x)$。为说明这一点，考虑到对于 $x \neq x'$，我们有

$$\mathop{\mathbb{P}}_{C_\pi}\left[\pi(x)|_m = \pi(x')|_m\right] = \frac{2^{n-m}-1}{2^n-1} \le 2^{-m}. \tag{36}$$

这个界只需通过计数得出：统计在前 m 比特上具有固定模式的比特串数量（不包括全零比特串）即可。并集界表明，发生碰撞、从而无法可靠识别 $\pi(S_n)$ 内比特串的概率至多为 $|S_n|^2 2^{-m}$。我们注意到，失败情形可以并入可蒸馏纠缠定义中的 ϵ参数，这意味着我们只需保证失败概率为 $O(\epsilon/n^k)$，其中 n^k 是可用副本的数量。只要选择

$$m = \log\frac{|S_n|^2}{\mathrm{negl}(n)} = \omega(\log n) \tag{37}$$

需要测量许多比特。根据观测结果 y，Alice 随后在 $\pi(S_n)$ 中进行搜索；当 $|S_n| = O(\mathrm{poly}(n))$ 时，该搜索可以高效地精确完成。在可靠地从 $\pi(S_n)$ 中识别出 $\pi(x)$ 后，Alice 应用算子 $X^{\pi(x)}$，此时 Alice 和 Bob 共享 $n-m = n-\omega(\log n)$ 个纠缠比特，从而证明了可达性结论。无界情形下相应的可达性是定理 7 的直接推论。定理 8 的一部分内容是证明存在一个信道，其 $|S_n| = \omega(\mathrm{poly}(n))$ 计算容量趋于零；其中指出，构造中使用的伪随机分布具有 u_S 的形式，适用于某个集合 S。 □