arXiv:2301.08348v1 [cs.CC] 19 Jan 2023

量子 EL 定理

Samuel Epstein*

2023年1月23日

摘要

本文证明了 EL 定理的一个量子版本。该定理指出，秩较大的非奇异投影，其像空间中必定存在简单的量子态。由此可知，对于冯·诺依曼熵足够大的量子源，若不使用简单的量子态，就无法进行通信。

1 引言

量子信息论研究通过量子信道进行通信的极限。在Holevo (1973)中，Holevo 界得到了证明，它给出了两个能够制备并测量混合态的参与方之间共享的经典信息量上限。Holevo 界指出，从 n 个经典信息比特中，最多只能获取 n 个量子比特的信息。Schumacher 定理 Schumacher (1995)给出了存在可靠压缩方案的充要条件，该方案能够以高保真度压缩并解压缩量子消息。

关于量子算法潜力的文献浩如烟海，其中最著名的当属 Shor 因数分解算法。一个相对较新的领域将算法与量子力学结合起来：算法信息论（AIT）与量子信息论的交叉领域。这一新领域中已有若干有趣的研究成果。例如，在 Epstein(2021b)中，研究表明，对纯量子态施加量子测量（即正算子值测度）时，绝大多数测量结果都是毫无意义的随机噪声。

这项研究计划旨在为算法信息论（AIT）中的定义和定理寻找量子对应概念，其核心概念是柯尔莫哥洛夫复杂度的量子版本 $\mathbf{K}(x)$。对于混合量子态或纯量子态的算法信息含量，已有若干种不同的定义可用于衡量。本文将采用 $\mathbf{K}(|\psi\rangle)$ 的定义，见 Vitanyi (2000)：若不存在一个简单的（就其经典编码而言）纯量子态能与 $|\psi\rangle$ 具有较高的量子保真度，则称纯量子态 $|\psi\rangle$是复杂的。本文的结果也适用于量子算法熵，G´acs (2001)。在 Epstein (2019) 中，定义了算法信息和随机缺陷的量子对应概念。此外，还证明了关于酉变换的守恒不等式

本文证明了一个量子 EL 定理。在算法信息论中，EL 定理 Levin (2016); Epstein(2019) 指出，不包含简单成员的字符串集合与停机序列之间具有较高的互信息。该定理有许多应用，其中包括所有抽样方法都会产生离群值 Epstein (2021a) 。量子 EL 定理指出，秩较大的非奇异投影，其像空间中必定包含简单的量子纯态。这里的“非奇异”是指该投影的编码与停机序列之间的信息量较低。

*samepst@jptheorygroup.org

量子 EL 定理可用于处理量子信息论中的开放问题。在 G´acs (2001) 中，曾提出如下评论。

备注。 (G´acs(2001)). 对量子描述复杂度问题的研究，或许有助于理解冯·诺依曼熵问题及其与量子信息论中编码任务的关系。

本文的定理有助于回应这一观点。

论断。随着量子源相关的冯·诺依曼熵增大，无损量子编码投影算子的秩也会增大，因此其像中必定包含算法量子复杂度更低的纯态。

2 相关工作

关于算法信息论的历史和基础，请读者参阅教材 Downey 和 Hirschfeldt（2010）以及 Li 和 Vit´anyi（2008）。目前有几种定义用于刻画量子态的算法内容。Berthiaume 等人（2001）将量子态的复杂度定义为能够以给定保真度近似该量子态的最小量子图灵机的规模。Mora 和 Briegel（2005）将量子态的算法复杂度定义为通过量子门制备该量子态的编码的最小长度。G´acs（2001）通过量子态乘以一个通用下半可计算半密度矩阵后所得结果的负对数来度量该量子态的算法熵。Vitanyi（2000）将纯量子态的熵定义为一个初等近似态的经典复杂度加上其保真度的负对数。Benatti 等人（2006）证明了 Brudno 定理的量子版本。Nies 和 Scholz（2019）引入了无限量子自旋链的随机性，称为量子 Martin L¨of 随机序列。Benatti 等人（2014）给出了算法熵的一个无限版本。

3 约定

字符串 $x \in \{0,1\}^*$ 的长度为 $\|x\|$。对于正实值函数 f，使用 $<^+ f$、$>^+ f$ 和 $=^+ f$ 分别表示 $< f + O(1)$、$> f + O(1)$ 和 $= f \pm O(1)$。$x \in \{0,1\}^*$ 的编码为 $1^{\|x\|}0x$。对于非负实值函数 f，术语 $<^{\log} f$、$>^{\log} f$ 和 $=^{\log} f$ 分别表示术语 $<f+O(\log(f+1))$、$>f-O(\log(f+1))$ 和 $=f\pm O(\log(f+1))$。

对于字符串 $x, y \in \{0,1\}^*$，算法 T在输入 x和辅助输入 y上的输出记为$T_y(x)$。当且仅当对于字符串 $x, y, s \in \{0,1\}^*, \neq \emptyset$，若 $T_y(x)$ 停机，则 $T_y(xs)$ 不停机时，算法 T是前缀无关的。存在一个通用前缀无关算法 U，使得对于所有前缀无关算法T，都存在一个 $t \in \{0,1\}^*$，并且对于所有 $x, y \in \{0,1\}^*$，$U_y(tx) = T(x)$。利用这个 U定义柯尔莫哥洛夫复杂度，其中 $\mathrm{K}(x|y) = \min\{\|p\| : U_y(x) = p\}$。以 $y \in \{0,1\}^*$为条件时，$x \in \{0,1\}^*$的通用概率为 $\mathrm{m}(x|y) = \sum\{2^{-\|p\|} : U_y(p) = x\}$。根据编码定理，我们有 $-\log \mathrm{m}(x|y) =^+ \mathrm{K}(x|y)$。我们用 $\mathrm{I}(x;\mathcal{H}) = \mathrm{K}(x) - \mathrm{K}(x|\mathcal{H})$ 表示停机序列 $\mathcal{H} \in \{0,1\}^\infty$ 关于 $x \in \{0,1\}^*$所包含的信息量。

我们用 $\mathcal{H}_n$ 表示一个具有 n 维的希尔伯特空间，其由基 $|\beta_1\rangle, \ldots, |\beta_n\rangle$张成。量子比特是希尔伯特空间 $\mathcal{H}_2$中的单位向量，该空间由向量 $|0\rangle, |1\rangle$张成。为了对 n 个量子比特建模，我们使用 $\mathcal{H}_{2^n}$中的一个单位向量，该空间由基向量 $|x\rangle$张成，其中 x 是一个大小为 n的字符串。

长度为 n 的纯量子态 $|\psi\rangle$ 是 $\mathcal{H}_{2^n}$ 中的单位向量。其在对偶空间中的对应元素记作 $\langle\phi|$。矩阵 A 的共轭转置为 A^*。用 Tr 表示矩阵的迹。投影矩阵是特征值位于 $\{0,1\}$ 中的厄米矩阵。

如果纯量子态的值是具有有理数系数的复数，那么它们就是初等的，因此可以用有限字符串表示。因此，初等量子态 $|\phi\rangle$ 可以编码为字符串 $\langle|\phi\rangle\rangle$ ，并赋予柯尔莫哥洛夫复杂度 $\mathrm{K}(|\phi\rangle)$ 和算法概率 $\mathrm{m}(|\phi\rangle)$。它们分别等于对状态进行编码的字符串的复杂度和算法概率。更一般地，如果复矩阵 A 的元素是具有有理数系数的复数，并且可以编码为 $\langle A\rangle$，那么该矩阵就是初等的，且具有柯尔莫哥洛夫复杂度 $\mathrm{K}(A)$ 和算法概率 $\mathrm{m}(A)$。

4 量子投影

纯态的简单性依据其经典信息含量来衡量。这与Vitanyi (2000)中的定义类似，不同之处在于使用的是经典图灵机而非量子图灵机。

定义 1（量子纯态复杂度）。对于 n 量子比特态 $|\phi\rangle$，$\mathrm{H}(|\phi\rangle) = \min\{\mathrm{K}(|\psi\rangle) - \log |\langle\phi|\psi\rangle|^2 : |\psi\rangle$ 是一个初等纯态$\}$。

如果一个概率分布的支撑集有限，且其所有取值都是有理数，则称其为初等概率。字符串 x 相对于初等概率测度 Q 的随机性亏损为 $\mathrm{d}(x|Q) = \lfloor -\log Q(x) \rfloor - \mathrm{K}(x|\langle Q\rangle)$。字符串的随机性为 $\mathrm{Ks}(x) = \min_Q\{\mathrm{K}(Q) + 3\log \mathrm{d}(x|Q)\}$。

引理 1 (Epstein (2021a); Levin (2016)). $\mathbf{Ks}(x) <^{\log} \mathbf{I}(x;\mathcal{H})$。

定理 1（量子 EL 定理）。固定一个 n 量子比特希尔伯特空间。设 P 是一个秩为 $> 2^m$ 的初等投影。那么，相对于 (n,m)，$\min_{|\phi\rangle\in\mathrm{Image}(P)} \mathrm{H}(|\phi\rangle) <^{\log} 3(n-m) + \mathrm{I}(\langle P\rangle; \mathcal{H})$。

证明。我们假设 P 的秩为 2^m。设 Q 是实现编码 P 的随机性 $\mathrm{Ks}(P)$ 的初等概率测度。我们可以假设，Q 支持集中的每个字符串都编码一个秩为 2^m 的投影。我们按照 Λ 在 n 量子比特空间上的均匀分布，抽取 N 个相互独立的纯态。对于支持集 Q 中的每个纯态 $|\psi_i\rangle$ 和投影 R，$\langle\psi_i| R |\psi_i\rangle$ 的期望值为

$$\int \langle\psi_i| R |\psi_i\rangle \, d\Lambda = \mathrm{Tr}R \int |\psi_i\rangle \langle\psi_i| \, d\Lambda = 2^{-n}\mathrm{Tr}RI = 2^{m-n}.$$

令随机变量 $X_R = \frac{1}{N}\sum_{i=1}^N \langle\psi_i| R |\psi_i\rangle$ 表示随机纯态在投影 R 上的平均投影大小。由于 $\langle\psi_i| R |\psi_i\rangle \in [0,1]$ 的期望为 2^{m-n}，根据 Hoeffding 不等式，

$$\Pr(X_R \le 2^{m-n-1}) < \exp\left[-N2^{-2(m-n)-1}\right]$$

令 $d = \mathbf{d}(P|Q)$。因此，如果我们设定 $N = d2^{2(m-n)+1}$，就能找到 N 个基本的 n 量子比特，使得 $Q(\{R: X_R \leq 2^{m-n-1}\}) \leq \exp(-d)$，其中 X_R 现在是一个固定值，而不是随机变量。因此 $X_P > 2^{m-n-1}$，否则就能构造一个 Q 期望检验 t，使得 $t(R) = \exp d$。这是矛盾的，因为

$$1.44d <^+ \log(P) <^+ \mathbf{d}(P|Q) <^+ d,$$

对于足够大的 d，我们可以不失一般性地假设这一点。因此存在 i 使得$\langle\psi_i| P |\psi_i\rangle \geq 2^{m-n-1}$。因此 $|\phi\rangle = P|\psi_i\rangle / \sqrt{\langle\psi_i| P |\psi_i\rangle}$属于 P的像，且 $|\langle\psi_i|\phi\rangle|^2 = \langle\psi_i| P |\psi_i\rangle \geq 2^{m-n-1}$。初等态 $|\psi_i\rangle$ 的经典柯尔莫哥洛夫复杂度为 $\mathbf{K}(|\psi_i\rangle) <^{\log} \log N + \mathbf{K}(Q,d) <^{\log} 2(m-n) + \mathbf{Ks}(P)$。因此，根据引理 1，

$$\begin{aligned}
&\min\{\mathbf{H}(|\psi\rangle) : |\psi\rangle \in \mathrm{Image}(P)\} \\
&\leq \mathbf{H}(|\phi\rangle) \\
&<^{\log} \mathbf{K}(|\psi_i\rangle) + |\langle\psi_i|\phi\rangle|^2 \\
&<^{\log} 3(n-m) + \mathbf{Ks}(P) \\
&<^{\log} 3(n-m) + \mathbf{I}(P;\mathcal{H}).
\end{aligned}$$

□

4.1 可计算投影

定理 1 以初等描述的投影为对象，并且可以推广到任意可计算投影。对于矩阵 M，令 $\|M\| = \max_{i,j} |M_{i,j}|$为最大范数。若程序$p \in \{0,1\}^*$ 输出一列秩为 ℓ 的投影 $\{P_i\}_{i=1}^{\infty}$，且满足 $\|P - P_i\| \leq 2^{-i}$，则称该程序计算秩为 ℓ 的投影 P。对于可计算投影算子 P，$\mathbf{I}(P;\mathcal{H}) = \min\{\mathbf{K}(p) - \mathbf{K}(p|\mathcal{H}) : p$ 是一个计算 $P\}$的程序。

Lem理 2 (Epstein (2022))。对于部分可计算的 f，$\mathbf{I}(f(a);\mathcal{H}) <^+ \mathbf{I}(a;\mathcal{H}) + \mathbf{K}(f)$.

推论 1。固定一个 n 量子比特希尔伯特空间。设 P 是一个秩为 $> 2^m$的可计算投影。那么，相对于 (n,m)，$\min_{|\phi\rangle \in \mathrm{Image}(P)} \mathbf{H}(|\phi\rangle) <^{\log} 3(n-m) + \mathbf{I}(P;\mathcal{H})$。

证明。设 p 是一个计算 P的程序。存在一个定义简单的算法 A，给定 p时，它会输出 P_n，使得 $\min_{|\psi\rangle \in \mathrm{Image}(P)} \mathbf{H}(|\psi\rangle) =^+ \min_{|\psi\rangle \in \mathrm{Image}(P_n)} \mathbf{H}(|\psi\rangle)$。因此，根据引理 2，可得 $\mathbf{I}(P_n;\mathcal{H}) <^+ \mathbf{I}(P;\mathcal{H})$。由定理 1 即得该推论。 □

5 量子数据压缩

量子源由一组纯量子态 $\{|\psi_i\rangle\}$ 及其对应的概率 $\{p_i\}$组成，其中 $\sum_i p_i = 1$。这些纯态不一定彼此正交。发送方 Alice 想将这些纯态发送给接收方 Bob。令 $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ 为与该量子源关联的密度矩阵。令 $S(\rho)$ 为 ρ的冯·诺依曼熵。根据 Schumacher 压缩，Schumacher (1995)，当 $n \to \infty$趋于极限时，Alice 可以将 n 个量子比特压缩为 $S(\rho)n$个量子比特，并将这些量子比特发送给 Bob，同时使保真度趋近于 1。例如，如果消息由 n 个光子偏振态组成，我们可以将初始量子比特压缩为 $nS(\rho)$ 个光子。Alice

不能将初始量子比特压缩为 $n(S(\rho)-\delta)$ 个量子比特，否则保真度将趋近于 0。量子比特通过投影消息到秩为 $nS(\rho)$ 的典型子空间来压缩，所用投影算子为 P。该投影通过一次量子测量实现，该测量由 P 和第二个投影算子 $(\mathbf{1}-P)$ 组成，后者将状态投影到垃圾态。

本文的结果表明，随着 $S(\rho)$ 增大， P 的取值范围内必定存在简单态。若不使用简单量子态，就无法传输具有足够大 $S(\rho)$ 的量子源。

参考文献

F. Benatti, T. Kr¨uger, M. M¨uller, R. Siegmund-Schultze, and A. Szko la. 熵与量子柯尔莫哥洛夫复杂度：量子布鲁德诺定理。《数学物理通讯》, 265(2), 2006. F. Benatti, S. K. Oskouei, and A. S. Deh Abad. 无限维希尔伯特空间中的盖奇量子算法熵。《数学物理杂志》, 55(8), 2014. A. Berthiaume, W. van Dam, and S. Laplante. 量子柯尔莫哥洛夫复杂度。《计算机与系统科学杂志》,63(2), 2001.R. G. Downey and D.R. Hirschfeldt. 算法随机性与复杂度。可计算性理论与应用。施普林格纽约，2010。S. Epstein. 算法不可克隆定理。《IEEE信息论汇刊》, 65(9), 2019. S. Epstein. 关于集合的算法概率。 *CoRR*, abs/1907.04776, 2019. S. Epstein. 离群值定理再探。 *CoRR*, abs/2203.08733, 2022. Samuel Epstein. 所有抽样方法都会产生离群值。《IEEE信息论汇刊》, 67(11):7568–7578, 2021a. doi: 10.1109/TIT.2021.3109779. Samuel Epstein. 关于量子测量的算法内容。 *CoRR*, abs/2102.03905,2021b.
URLhttps://arxiv.org/abs/2102.03905。P. G´acs. 量子算法熵。《物理学杂志A：数学与一般》, 34(35), 2001. A. Holevo. 量子通信信道传输信息量的界。《信息传输问题》, 9, 1973. L. A. Levin. 元素最低复杂度的奥卡姆界。《纯粹与应用逻辑年刊》,167(10):897–900, 2016.M. Li andP. Vit´anyi. 《柯尔莫哥洛夫复杂度及其应用导论》。施普林格出版公司，第三版，2008。C. Mora and H. Briegel. 量子态的算法复杂度与纠缠。《物理评论快报》,95,2005.

A. Nies 和 V. Scholz. 量子 Martin-L¨of 随机性。arXiv 电子预印本，arXiv:quant-ph/1709.08422, 2019. B. Schumacher. 量子编码。《物理评论 A》，51, 1995. P. Vitanyi. 单个纯量子态中信息定量定义的三种方法。载于《第15届 IEEE 计算复杂性年度会议论文集》，2000。