arXiv:2602.17647v1 [quant-ph] 19 Feb 2026

伪确定性量子算法

HugoAaronson TomGur Jiawei Li剑桥大学 奥斯汀得克萨斯大学

2026年2月20日

摘要

我们开始系统地研究伪确定性量子算法。这类量子算法对于任何输入，都能以高概率输出一个典范解。我们聚焦于查询复杂度模型，主要贡献包括以下复杂度分离；这些结果需要专门针对伪确定性设计的新下界技术：

- 我们展示了一个问题——避免一个加密字符串（AOES）——其经典随机查询复杂度为 $O(1)$，但对伪确定性量子算法而言却是最难的（查询复杂度为 $\Omega(N)$）。
- 我们提出一个问题——量子锁定估计（QL-Estimation）。对于该问题，伪确定性量子算法相较于经典伪确定性算法可实现指数级加速（$Q(\log(N))$ vs. $\Theta(\sqrt{N})$），而其随机化查询复杂度为 $O(1)$。

作为对这些分离结果的补充，我们证明，对于任意全问题 R，伪确定性量子算法相较于确定性算法至多具有五次方优势，即 $\mathrm{D}(R) = \tilde{O}(\mathrm{psQ}(R)^5)$。在算法方面，我们找出了一类只需少量额外开销即可实现伪确定性的量子搜索问题，其中包括 Grover 搜索、元素互异性、三角形查找、 k-和以及图碰撞。

1 引言

由 Gat 和 Goldwasser 发起的伪确定性算法研究 [GG11], 关注的是这样一类随机化算法：对于每个输入，它们都会输出一个典范解。也就是说，若随机化算法 $\mathcal{A}$ 能够解决搜索问题 $R \subseteq \mathcal{X} \times \mathcal{Y}$，并且存在函数 $f : \mathcal{X} \to \mathcal{Y}$，使得对任意输入 $X \in \mathcal{X}$，输出 $\mathcal{A}(X)$ 以高概率为 $f(X)$，那么就称该算法是伪确定性的。

伪确定性算法利用随机化的计算能力，同时保持确定性算法可预测的输出行为。这与完全随机化算法形成鲜明对比，后者多次运行可能会返回截然不同的输出。在过去十年中，伪确定性算法受到广泛关注，并已应用于理论计算机科学的多个领域 [GGR13，GGH18，GGH19，GGMW20，DPV21，DPWV22，CDM23，CLO+23，BKKS23，GGS23]。

在量子情形下，Goldwasser、Impagliazzo、Pitassi 和 Santhanam [GIPS21] 在研究 FIND1 问题时[1]，首次在查询复杂度模型中考察了伪确定性算法。尽管FIND1 可以通过随机采样用 $O(1)$ 次查询解决，但他们证明，对于FIND1 而言，任何经典或量子的伪确定性算法都需要 $\Omega(\sqrt{N})$ 次查询。 —

量子伪确定性的真正独特之处，在于测量所带来的随机性。许多实现指数级量子加速的量子算法（例如傅里叶采样），都会对横跨指数多个候选解的叠加态进行测量，这一步似乎不可避免。这为重新审视现有的量子优势提供了一个新视角：

> 量子加速何时能够以伪确定性方式实现？量子优势又在何时本质上需要输出熵？

这个问题也将量子伪确定性与可认证随机性联系起来：如果能够证明，给定伪确定性要求，某个问题的量子优势 R 无法保留，那么任何能够高效解决该问题的量子设备（可能是不可信的）$\mathcal{A}$ 都必须 R产生一定的熵。一系列研究 [BBF+21、AH23、YZ24] 在标准复杂性假设下表明，傅里叶采样 [Aar10], 、随机线路采样以及 Yamakawa–Zhandry 算法 [YZ24] 无法实现伪确定性[2]。

受上述问题启发，我们开始系统研究量子伪确定性。我们探究伪确定性量子算法的基本性质，展示揭示量子伪确定性优势与局限的复杂度分离，并找出一大类能够由高效伪确定性量子算法解决的问题，其中包括 Grover 搜索、元素互异性、三角形查找、k-和以及图碰撞。

1.1 我们的结果

我们从查询复杂度模型开始。除非另有说明，我们用 N 表示搜索问题的输入长度。对于搜索问题 R，我们分别用 $\mathrm{D}(R)$ 、 $\mathrm{psQ}(R)$ 和 $\mathrm{Q}(R)$ 表示确定性查询复杂度、伪确定性量子查询复杂度和量子查询复杂度。我们将算法$\mathcal{A}$ 在获得输入 X 的查询访问时的输出记为$\mathcal{A}^X$。

1.1.1 查询复杂度分离

我们首先研究伪确定性量子查询算法、随机化算法和经典伪确定性算法之间的关系。

量子伪确定性的困难性。我们的首个结果表明，并非所有问题都存在高效的伪确定性量子算法。我们给出了经典随机查询复杂度与量子伪确定性查询复杂度之间的最大分离。

定理 1.1. 存在一个搜索问题 R ，其经典随机复杂度为 $O(1)$，而其伪确定性量子查询复杂度为$\Omega(N)$。

[1]Find1 问题的输入是一个字符串 $X \in \{0,1\}^N$，并承诺 X 的汉明重量至少为$N/2$，目标是输出一个满足 $X_i = 1$ 的索引 i 。[2] 对于量子可认证随机性，这些研究实际上证明了定量上更强的结论：任何能完成这些任务的高效量子算法都必须生成大量的最小熵。

定理 1.1 改进了由FIND1 问题给出的分离，其中伪确定性量子下界为Ω(√N)。我们通过避免一个加密字符串 (AOES)问题获得了这一更强的分离。非正式地说，输入编码 m 个异或 构件实例；它们共同加密一个隐藏串 $b \in \{0,1\}^m$，其中 b_i 是第 i个异或 实例的解。目标是输出任意 m比特串，它不等于 b。经典随机算法可通过盲采样以常数概率成功，而任何伪确定性算法都必须在多次运行中始终避开b，这实际上迫使其至少学习 b的一个比特。

量子伪确定性的力量。我们的第二个结果表明，伪确定性量子算法可能远强于其经典对应算法。我们证明，在一项经典随机化算法仍能轻松完成的任务上，伪确定性量子算法与伪确定性经典算法之间存在指数分离。为了确保这种分离确有意义，我们需要确认量子算法并非只是在引入经典计算无法获得的解。为此，我们定义了“规范化”的概念。直观地说，量子算法会将随机化算法中以相当高概率出现的某个解固定为典范解，从而将其从随机解规范化为伪确定性解。

定义1.2。 设 $R \subseteq X \times Y$ 是一个搜索问题，其随机化算法为 A，并设 $f: X \to Y$ 是一个函数。若对于任意 $X \in X$，A^X 输出 $f(X)$ 的概率大于其输出错误解的概率，则称 f规范化 A。等价地，

$$\forall X \in \mathcal{X} : \mathbb{P}_{\mathcal{A}}[\mathcal{A}^X = f(X)] > \mathbb{P}_{\mathcal{A}}[(X, \mathcal{A}^X) \notin R].$$

如果由 B 计算的函数 f 将算法 A 正规化，则称伪确定性算法 B 将算法 A 正规化。

现在我们陈述一个定理，展示伪确定性算法中的量子优势。

定理 1.3。 存在一个搜索问题 R，使得

1. 存在一个针对 R 的随机化经典算法 A，使用 $O(\log N)$ 次查询；*2.* 存在一个量子伪确定性算法 B，其查询复杂度为 $O(\log N)$，并将算法 A 正规化；*3.* 任意针对 R 的经典伪确定性算法都需要 $\Omega(\sqrt{N})$ 次查询。

—

对于在伪确定性算法的背景下展示具有概念意义的量子优势所需的条件，我们有两点说明。首先请注意，如果不要求该问题对随机化算法来说是容易的（条目 1），那么这种分离就会变得毫无意义，因为它根本不必涉及伪确定性（例如 Simon 问题就有唯一解）。相比之下，定理 1.3 展示了另一种形式的量子优势：除了加速搜索之外，量子算法还能比经典伪确定性算法更高效地打破对称性（通过消除输出随机性）。此外，我们还要求这样的量子伪确定性算法将某个经典算法正规化。这是因为我们不希望量子算法通过输出一个经典算法无法获取的新解来投机取巧。

1.1.2 量子伪确定性的基本性质。

接下来，我们给出一些定理，展示伪确定性量子算法的两项基本性质：全问题的最大加速幅度受到限制；以及利用 Find1 问题的完备性，可以得到一般性的伪确定性量子查询复杂度上界。

全问题的确定性模拟。我们证明，对于全问题，伪确定性量子算法无法实现相对于经典算法的指数级加速。具体而言，全问题的伪确定性量子算法可以由确定性算法模拟，开销为五次方。

定理 1.4。 设 $R \subseteq \{0,1\}^N \times Y$ 是一个全搜索问题，则 $\mathsf{D}(R) = O(\mathsf{psQ}(R)^5 \log(N))$。

相比之下，在经典设置中， [GGR13] 证明了，全问题的伪确定性经典算法可以通过确定性算法模拟，但会产生四次方开销$\mathsf{D}(R) = O(\mathsf{psR}(R)^4 \log(N))$。我们对 定理 1.4 的证明沿用了 [GGR13], 的策略，但面临一个新的挑战；也就是说，我们在证明 定理 1.4 时的主要技术贡献是一个引理（引理 3.1），该引理给出了伪确定性量子算法可能输出数量的上界；而这一步在经典情形中是平凡的。

一般的伪确定性量子查询上界。 我们还注意到， [GIPS21], 中的完全性结果指出， FIND1 问题是伪确定性经典查询复杂度的完全 问题，这一结果可以扩展到量子情形。将其与以下事实结合：$\mathsf{psQ}(\text{FIND1}) = \Theta(\sqrt{N})$ [GIPS21],[3] 我们推导出任意问题的伪确定性量子查询复杂度的一般上界，该上界通过其随机化查询复杂度和验证复杂度给出（即，验证输入-解对是否属于某个关系的确定性查询复杂度）。

定理 1.5。 对于任何搜索问题 R，若其随机化查询复杂度为 $\mathsf{R}(R)$，验证复杂度为 $\mathsf{V}(R)$，则有 $\mathsf{psQ}(R) = O((\mathsf{R}(R) + \mathsf{V}(R)) \cdot \sqrt{N})$。

这意味着，对于任何伪确定性量子查询复杂度问题，若其下界大于 $\Omega(\sqrt{N})$，则该问题要么具有较高的随机化查询复杂度，要么难以验证。例如，在我们构造的最难伪确定性问题AOES (定义 4.2) 中，其随机化查询复杂度为 $O(1)$，但验证起来非常困难。

1.1.3 使量子算法具有伪确定性。

在 [GIPS21], 中，人们注意到，将格罗弗算法融入二分搜索，可以得到一种用于FIND1 的伪确定性量子算法，该算法可在$\tilde{\Theta}(\sqrt{N})$ 次查询中返回第一个非零索引。

我们进一步拓展这一思路，并将其推广，从而为一大类 k-子集查找 问题 [CE05]构造伪确定性量子算法。这里，输入 $X \in \Sigma^N$ 由 N个元素组成，目标是找到一个包含 k 个元素且满足某个谓词的子集。为了使二分搜索方法适用，我们引入一个温和的条件 `Prunable`；直观而言，该条件要求缩小搜索域不会增加查询成本。我们证明，对于 `Prunable`问题，任何子集查找量子算法都可以转化为伪确定性算法，且对 k的依赖仅为近线性。

~定理 1.6。 设 R 是一个 k子集查找问题。如果 R 是 `Prunable`，那么 $\mathsf{psQ}(R) = O(k \cdot \mathsf{Q}(R))$。

我们注意到，许多自然的 k子集查找任务都是 `Prunable`，例如 k互异性、三角形查找和 k和问题。然而，我们发现，对于具有全局结构的 k子集查找问题，例如 Find1（将其解释为 1-子集查找问题时），这一条件可能不成立。

[3]一个 $\tilde{O}(\sqrt{N})$ 上界 FIND1 在 [GIPS21]中已有非正式描述。我们进行了更仔细的分析，并证明可以避免这一对数项。详情请参阅 第 5 节 和 定理 5.1 。

1.1.4 超越查询复杂度模型

最后，我们研究标准查询复杂度模型之外的伪确定性量子算法；具体而言，我们考察具有量子输入的搜索问题，以及白盒设置。

量子输入搜索问题。我们考虑另一类搜索问题，其输入是一个量子态。此处，查询复杂度定义为求解该问题所需的输入态副本数。伪确定性可能有助于解决如下问题：在输入态的支撑集中找到一个计算基元素、找到与输入态正交的态，等等。然而，我们证明，若输入域是连通连续空间，则不可能存在伪确定性算法。

尽管如此，我们考虑一个量子版本的FIND1 ，我们称之为均匀支持查找：在支撑集中找出一个计算基元素，该支撑集属于输入态 $|\psi\rangle$，其中 $|\psi\rangle$ 被承诺为一个均匀叠加，其叠加范围为一个基子集。我们证明均匀支持查找 的查询复杂度为 $\Theta(d)$，其中 d是 $|\psi\rangle$的维数（定理 6.6）。

白盒设置。最后，我们给出在白盒（图灵机）设置下，哪些问题存在高效伪确定性量子算法的刻画。

定理 1.7。 搜索问题 R 存在伪确定性量子多项式时间算法，当且仅当 R 它可 P-归约[4] 到某个有界错误量子多项式时间中的判定问题。

我们在 定理 1.7 的 附录 A中证明该定理；它是对经典对应结果的推广，见 [GGR13]。直观来说，定理 1.7 指出，任意搜索问题 R 存在高效伪确定性量子算法，当且仅当它存在一个 搜索到判定的 归约到有界错误量子多项式时间。换言之，搜索问题的任何（超多项式）伪确定性量子优势，本质上都源自某个判定问题的量子优势。

1.2 技术

本节将简要介绍我们用于证明 定理 1.1 和 定理 1.3中查询复杂度分离的技术。在这两种情况下，关键都在于证明伪确定性量子算法或经典算法的查询复杂度下界，这需要新的技术。这是因为缺乏证明伪确定性下界的工具，而且多项式方法等成熟技术无法直接应用。

随机化量子算法与伪确定性量子算法之间存在最大分离。与伪确定性算法相比，随机化算法的一项典型优势是能够输出随机字符串。我们考虑以下问题，称为避免一个加密字符串（AOES），它利用了这一优势。AOES 的输入由并行的 m 个异或问题实例构成，其中 m 是一个很大的常数。令 N 为输入总长度， N/m 为每个异或实例的输入长度。这些异或实例编码了一个秘密字符串 $b \in \{0,1\}^m$，其中 b_i 是第 i 个异或实例的值。目标是输出任意一个不等于 b 的 m 比特字符串。

通过以准确率 $1 - 1/2^m$ 随机采样一个 m 比特串，即可轻松解决 AOES。然而，不难证明，任何确定性算法都无法做得更好，除非使用 N/m

[4] P-归约指确定性多项式时间图灵归约。

次查询来解决第一个异或实例，然后输出任意一个首位不匹配的字符串。直观地说，任何能够始终避免输出 b 的伪确定性算法，都必须掌握有关这些异或实例的一些信息。另一方面，异或对于量子查询算法而言是最难的，即任何针对长度为异或的量子查询算法 n 在少于 $n/2$ 次查询的情况下，表现都不会优于随机猜测 [FGGS98，BBC+01]。

为将直觉转化为证明，我们给出一个从异或到 AOES 的新随机化 归约。具体而言，我们证明：如果存在一个针对 AOES 的零错误量子算法$\mathcal{B}_{N,\ m}$ 其查询复杂度为 q，那么就存在一个针对异或的量子算法$\mathcal{A}^{N/m}$，它调用$\mathcal{B}$ 一次，并且对于每个输入 $X \in \{0,\ 1\}^{N/m}$，

$$\mathbb{P}\left[\mathcal{A}^X = \mathsf{XOR}(X)\right] \geq \frac{1}{2} + \frac{1}{2^{m+1}}.$$

为证明这一点，设$\mathcal{B}$ 是 AOES 问题的求解器，设 $X \in \{0,\ 1\}^{N/m}$ 是我们要解决的异或实例。我们分两步构造一个随机 AOES 实例 $Z = (Z_1,\ \ldots,\ Z_m)$。首先，我们生成一个 m 均匀随机字符串 $Y_1,\ \ldots,\ Y_m \in \{0,\ 1\}^{N/m}$。然后，对每个位置 $i \in [m]$，我们以概率 $1/2$取 $Z_i = Y_i$，并以概率 $1/2$取 $Z_i = Y_i \oplus X$。

从较高层面来看，$Y_1, \ldots, Y_m$可以视为一次性密码本，而 X嵌入在 AOES 实例 Z 中的一个随机位置子集中。关键的观察是，从 AOES 求解器 $\mathcal{B}$ 的角度来看，Z 是均匀随机的；它对 X以及 X 嵌入在 Z中的位置一无所知。我们可以证明，当将 X 嵌入到 Z 中由$\mathcal{B}$决定的某个位置子集中时，就能确定性地恢复异或实例 X 的解。当$\mathcal{B}$ 是 AOES 的零错误算法时，我们的随机化归约的整体成功率为 $1/2+1/2^{m+1}$；鉴于异或问题的困难性，任何严格大于 $1/2$的值都足够。

最后，对于任何用于 AOES 的伪确定性算法$\mathcal{B}$，我们都可以通过进行 $O(m)$次重复运行并选取出现最频繁的输出，将其错误率降至$1/2^{2m}$。随后，我们可以将这个错误率极低的 AOES 算法代入随机化归约，仍能在异或问题上获得非零优势。请注意，虽然随机采样算法的错误率为 $1/2^m$，但无法通过重复运行进一步降低该错误率。

指数级伪确定性量子优势。我们构造了一个称为量子锁定估计（QL-估计）的问题，该问题对随机化算法以及量子伪确定性算法而言很容易，但对经典伪确定性算法而言很难。

设 $N = 2^n$。为简便起见，我们有时以自然方式将值 $x \in [N]$ 解释为一个 n 比特串，反之亦然。回想一下，在 Simon 问题 [Sim97], 中，输入是一个函数f：$[N] \to [N]$，它被承诺编码一个秘密字符串 s，使得 $f(x) = f(y) \Leftrightarrow (x = y) \vee (x = y \oplus s)$。在汉明问题中，给定输入字符串 $X \in \{0,1\}^N$，目标是输出 X 的汉明重量的估计，加性误差不超过 $N/10$。

在 QL-估计问题中，输入只是一个二元组 (f, X)，其中 f 是 Simon 问题的一个实例，X 是汉明问题的一个实例。承诺 f 编码某个字符串 s，该字符串被承诺为 $X(|s - \|X\|_{\mathsf{hw}}| \leq 0.09 \cdot N)$ 的汉明重量的有效估计。目标是输出 X 的汉明重量的估计，加性误差不超过 $N/10$。

经典随机算法可以用 $O(1)$次查询估计汉明重量，而量子算法可以计算出秘密字符串 s，根据该问题的承诺，它是一个有效解。事实上，该量子算法典范化了这一特定估计 s，而这只是经典随机算法可能合理产生的众多不同汉明重量估计之一。[5] 我们将此视为一种“锁与钥匙”构造，其中汉明问题

[5]为确保满足规范化条件（定义1.2），我们需要对经典随机采样算法稍作调整，使其使用 $O(\log N)$ 次查询。更多详情请参见 4.2 节。

锁住了一个对伪确定性经典算法隐藏的典范解，而钥匙则是 Simon 问题，只有量子算法才能访问它。

要证明伪确定性经典算法的下界，一个有用的方法是先通过敏感度论证，重新审视汉明问题的伪确定性难度。假设对于某个字符串X（其中 $\|X\|_{\mathsf{hw}} = N/2$），某个算法的伪确定性输出为 t。令 X' 为伪确定性输出是 t的字符串中汉明重量最小的字符串。该算法在 X' 处是敏感的，因为翻转 X' 的任意一个 1 比特，都会得到一个伪确定性输出不是 t 的字符串（因为它的汉明重量会更小），这意味着要区分 X' 与任何此类字符串，需要很大的查询复杂度。

然而，高敏感度也意味着量子查询复杂度很大，因此，我们必须修改论证来处理量子算法易于解决的 QL-估计 问题。假设 $\mathcal{A}$ 是一个用于求解QL-估计的经典伪确定性算法。证明的关键在于论证：如果 $\mathcal{A}$ 在任何地方的敏感度都次线性，那么它就必须近似地求出 Simon 问题中的秘密字符串 s（见引理 4.18）。为此，我们采用了与汉明的证明类似的技巧：在那些经$\mathcal{A}$处理后产生相同输出的字符串中，找出汉明重量最小的字符串 X'；然后翻转其中的 1 比特。这里的分析更为微妙，因为问题中的汉明部分和 Simon 部分并不独立；Simon 见证与汉明输入相互耦合，因此标准的乘积分布论证或解耦论证并不适用。

最后，我们证明了近似求解 Simon 问题与精确求解该问题同样困难，因此得出结论：$\mathcal{A}$ 必须使用 $\Omega(\sqrt{N})$ 次查询。

1.3 论文结构

在第 2 节中，我们建立查询模型，定义伪确定性经典/量子算法，并回顾关键的预备知识（包括 Find1 和信息论工具）。第 3 节证明基础性结果，包括全搜索问题中的五次关系，以及量子伪确定性中 Find1 的完备性。第 4 节给出我们的主要分离结果：4.1 节引入 AOES，以获得随机化量子查询复杂度与伪确定性量子查询复杂度之间的最大差距；4.2 节定义QL-估计，从而在保持随机化算法易于求解的同时，分离伪确定性量子算法与伪确定性经典算法。第 5 节展示如何以较小的额外开销，使一大类量子子集查找算法具备伪确定性。最后，第 6 节研究量子输入搜索问题中的伪确定性，证明拓扑限制以及量子 Find1 类比的紧确界。

2 预备知识

在查询复杂度模型中，若算法 A 在获得输入 $X \in \mathrm{X}$ 的查询访问后，输出 $Y \in \mathrm{Y}$，使得 $(X,Y) \in R$ 以至少 $2/3$ 的概率成立，则称算法 A 解决了搜索问题 $R \subseteq \mathrm{X} \times \mathrm{Y}$。我们将算法 A 在获得输入 X 的查询访问后输出的结果记为 A^X。除非另有说明，输入集合是二进制字符串的子集，$\mathrm{X} \subseteq \bigcup_{N\in\mathbb{N}}\{0,1\}^N$。在这种情况下，算法可以显式访问输入长度 $N \in \mathbb{N}$，其中 $X \in \{0,1\}^N$。这里的复杂度度量是对黑盒预言机进行的查询次数。若搜索问题没有其他参数，我们将定义 $\mathrm{X}_N := \mathrm{X} \cap \{0,1\}^N$，表示搜索问题中输入长度为 N 的子集。当输入长度可由上下文明确得知时，我们会省略下标，只写 X。

定义 2.1 (伪确定性算法)。 对于搜索问题 $R \subseteq X \times Y$，若存在函数 $f : X \to Y$，使得对于所有 $X \in X$，$A(X)$ 的输出以至少 $2/3$ 的概率为 $f(X)$，且 f 的输出始终是该搜索问题的一个解，则称算法 A 是伪确定性的。这里，输出 $f(X)$ 称为规范解或伪确定性解。等价地，

$$\exists f : \mathcal{X} \to \mathcal{Y}, \forall X \in \mathcal{X} \left((X, f(X)) \in R \wedge \mathbb{P}[\mathcal{A}(X) = f(X)] \geq \frac{2}{3} \right).$$

在经典设置中，对黑盒的一次查询由算法指定一个索引 $i \in [N]$，然后算法接收值 X_i。对于具有经典输入的量子算法，算法是由酉算子组成的电路，一次查询就是对预言机酉算子 U_X 的一次使用，其作用表示为

$$\forall i \in [N], j \in \{0,1\} : U_X |i\rangle \otimes |j\rangle = |i\rangle \otimes |j \oplus X_i\rangle .$$

定义 2.2 （查询复杂度度量）。 对于搜索问题 $R \subseteq X \times Y$，我们记查询设置下的以下复杂度度量。

- $\mathsf{D}(R)$ 是求解 R 的确定性查询复杂度。
- $\mathsf{R}(R)$ 是求解 R 的随机化经典查询复杂度。
- $\mathsf{Q}(R)$ 是求解 R 的随机化有界错误量子查询复杂度。
- $\mathsf{psR}(R)$ 是求解 R 的伪确定性有界错误经典查询复杂度。
- $\mathsf{psQ}(R)$ 是求解 R 的伪确定性有界错误量子查询复杂度。

这里，有界错误意味着任何算法必须以至少 $2/3$ 的概率成功。我们类似地为布尔函数 $f : X \to \{0,1\}$ 定义D、R、Q。

2.1 Find1 问题

我们定义 FIND1 问题，并回顾来自 [GIPS21] 的现有完备性与量子下界结果。

定义 2.3 (FIND1)。 对于满足 $\sum_j X_j \geq N/2$ 的输入 $X \in \{0,1\}^N$，FIND1 问题的一个解是满足 $X_i = 1$ 的下标 i。

下一个定理确立了 Find1 问题对于伪确定性查询算法的完备性。

定理2.4（[GIPS21] 定理3，Find1的完备性）。设 r、q、v 是满足以下条件的函数：对于任意 $f \in \{r, q, v\}$，均有 $f(\Theta(N)) = \Theta(f(N))$。设 R 是一个搜索问题，对于输入规模为 N 的实例，解可通过 $v(N)$ 次查询进行验证，其有界误差随机查询复杂度至多为 $r(N)$，且 R 的有界误差伪确定性查询复杂度至少为 $q(N)$。那么，Find1 的伪确定性查询复杂度至少为 $\Omega(q(N)/(r(N) + v(N)))$。

我们还需要以下关于 Find1 问题的伪确定性量子复杂度下界。

定理 2.5 （[GIPS21] 定理 4，量子下界）。针对 FIND1 的伪确定性量子查询复杂度至少为 $\Omega(\sqrt{N})$。

2.2 熵

对于随机变量 $\mathbf{X}$，令 $|\mathbf{X}|$ 表示 $\mathbf{X}$ 的支撑集大小。全文中，所有对数均以 2 为底。

定义 2.6 （香农熵）。 对于具有概率分布 $(p_x)_x$ 的随机变量 $\mathbf{X}$ ， $\mathbf{X}$ 的香农熵定义为

$$H(\mathbf{X}) = -\sum_x p_x \log(p_x).$$

定义 2.7（冯·诺伊曼熵）。 设 ρ 为具有一组特征值$(p_x)_x$的混合量子态，则 ρ的冯·诺伊曼熵定义为

$$S(\rho) = H(p) = -\sum_x p_x \log(p_x).$$

注 2.8。 注意，对于支撑在 n 个元素上的分布以及维数为 n 的量子态，相应熵概念的最大值均为 $\log(n)$。该最大值分别由均匀分布和最大混合态达到。

我们将两个随机变量 $\mathbf{X}$、$\mathbf{Y}$ 的联合熵记为 $H(\mathbf{X},\mathbf{Y})$。我们将条件熵记为 $H(\mathbf{X}|\mathbf{Y}) = H(\mathbf{X},\mathbf{Y}) - H(\mathbf{Y})$。

定义 2.9。 两个随机变量 $\mathbf{X}$、$\mathbf{Y}$ 之间的互信息为 $I(\mathbf{X},\mathbf{Y}) = H(\mathbf{X}) + H(\mathbf{Y}) - H(\mathbf{X},\mathbf{Y}) = H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y})$。

引理 2.10 （Holevo界，定理 12.1 [NC16]）。 对于量子态系综 $(\rho_x)_{x\in[n]}$以及概率分布 $\mathbf{X} = (p_x)_{x\in[n]}$ 和 *POVM* $\{L_y\}_{y\in[m]}$。若 *POVM* 作用于量子态 $\rho = \sum_x p_x\rho_x$时的输出分布为 $\mathbf{Y} = \{\mathrm{Tr}(L_y\rho)\}_{y\in[m]}$ 则有以下结论：

$$I(\mathbf{X},\mathbf{Y}) \le S(\rho) - \sum_{p_x} S(\rho_x).$$

引理 2.11 （Fano不等式，框 12.2 [NC16]）。 两个经典随机变量 $\mathbf{X}$、$\mathbf{Y}$ 之间的条件熵 $H(\mathbf{X}|\mathbf{Y}) = H(\mathbf{X},\mathbf{Y}) - H(\mathbf{Y})$ 满足以下上界：

$$H(\mathbf{X}|\mathbf{Y}) \le H(e, 1-e) + e\log(|\mathbf{X}| - 1).$$

其中，e 是任何根据$\mathbf{X}$的值来估计$\mathbf{Y}$的算法所能达到的最小错误率 .

3 伪确定性量子查询复杂度的基本原理

本节将确立伪确定性量子算法的两项基本性质：全搜索问题中确定性算法与量子伪确定性算法之间的关系，以及 Find1 问题对于量子伪确定性的完备性。

3.1 全搜索问题的最大五次加速

我们证明，对于任何全搜索问题，伪确定性量子算法相较于经典算法都无法实现超多项式加速，正如定理 1.4所述，下面我们将重述该定理。

定理 1.4。L 设 $R \subseteq \{0,1\}^N \times Y$ 为一个全搜索问题，则 $\mathsf{D}(R) = O(\mathsf{psQ}(R)^5 \log(N))$.

该结果是对以下文献中经典对应结果的推广： [GGR13，定理 4。1],其证明了存在一种四次关系，即任意全搜索问题的经典伪确定性查询复杂度与确定性查询复杂度之间的关系。该证明首先表明，伪确定性输出的数量以上界为 $2^{q(N)+1}$，然后分别计算 $q(N)+1$ 规范输出的各个比特，并使用伪确定性算法分别计算。这些比特中的每一个——即一个全布尔函数——都可以根据全布尔函数的确定性查询复杂度与随机化查询复杂度之间的关系，以多项式开销确定性地计算出来。

我们采用类似的策略来证明定理 1.4。首先，我们需要给出伪确定性量子算法可能输出数量的上界，随后便可以用有界数量的比特对规范输出进行编码。事实证明，这一步比经典情形更具挑战性。利用经典与量子信息论中的工具，我们证明了以下引理，该引理本身可能也具有独立的意义。

引理 3.1。 设 A 是一个针对搜索问题 $R \subseteq \{0,1\}^N \times \{0,1\}^\ell$ 的伪确定性量子查询算法，其查询复杂度为 q。令 $f_{\mathcal{A}}: \{0,1\}^N \to \{0,1\}^\ell$ 表示将 $\{0,1\}^N$ 中的元素映射到 A 的规范输出的函数。那么，可能的输出数量 $|\mathrm{Im}(f_{\mathcal{A}})|$ 为 $O((2N)^{3q/2})$。

证明。 令 $m = |\mathrm{Im}(f_{\mathcal{A}})|$，并设输入为 $X \in \{0,1\}^N$；对于所有 $i \in [q]$，寄存器 B_i 和 C_i 分别表示输入以及向预言机输出的内容 X。回顾一下，量子预言机表示为酉算子 U_X，其作用如下：

$$U_X : |a\rangle \otimes |b\rangle \mapsto |a\rangle \otimes |b \oplus X_a\rangle .$$

酉算子 $(V_i)_{i\in[q]}$ 在寄存器 B_i 中准备输入至预言机，同时不影响之前的寄存器，

$$\begin{aligned} V_i : |j_1\rangle_{B_1} \otimes |X_{j_1}\rangle_{C_1} \otimes \ldots \otimes |j_{i-1}\rangle_{B_{i-1}} \otimes |X_{j_{i-1}}\rangle_{C_{i-1}} \otimes |0\rangle \mapsto \\ |j_1\rangle_{B_1} \otimes |X_{j_1}\rangle_{C_1} \otimes \ldots \otimes |j_{i-1}\rangle_{B_{i-1}} \otimes |X_{j_{i-1}}\rangle_{C_{i-1}} \otimes \sum_{j=1}^{N} a_{i,j_1,\ldots,j_{i-1},X_{j_1},\ldots,X_{j_{i-1}},j} |j\rangle \end{aligned}$$

该算法一般可表示为算法 1。

算法 1 一般伪确定性量子算法

输入： $X \in \{0,1\}^N$。

1: 在其他寄存器中准备状态 $|0\rangle$ 。2: 对于 $k = 1 \ldots q$ 执行3: 在寄存器 $B_1C_1 \ldots B_{k-1}C_{k-1}B_k$ 上应用 V_i。4: 将 U_X 应用于寄存器 B_kC_k。5: 结束循环6: 在寄存器 $B_1C_1 \ldots B_qC_q$ 上执行 POVM，并输出结果。

TPOVM 测量前的最终态维数为 $(2N)^q$，因为它可以表示为，

$$\sum_{(j_1,\ldots,j_q)\in[N]^q} a_{1,j_1} |j_1\rangle \otimes |X_{j_1}\rangle \otimes \ldots a_{q,j_1,\ldots,j_{q-1},X_{j_1},\ldots,X_{j_{q-1}},j_q} |j_q\rangle \otimes |X_{j_q}\rangle .$$

该表达式存在于一个线性子空间中，其中最多有 $(2N)^q$ 个线性无关基态（由每个 $(j_1$、……、$j_q) \in [N]^q$ 和 X_{j_i} 定义）。添加辅助量子比特或额外的工作空间也不会改变这一点。

现在我们调用 Holevo界。给定 $|\mathrm{Im}(f_{\mathcal{A}})| = m$，令 X 为一个随机变量，它在集合 $L = \{X_1, \ldots, X_m\}$ 上均匀分布；对集合中的每个元素应用 $f_{\mathcal{A}}$ 后，其输出各不相同 $\forall i, j \in [m]: f_{\mathcal{A}}(X_i) = f_{\mathcal{A}}(X_j) \implies i = j$。令 Y 为随机变量，表示以随机变量 X 为输入时 A 的输出。若输入枚举为 $(X_t)_{t\in[m]}$，且输入 X_t 时的最终态为 ρ_t，那么 Holevo界（引理 2.10，针对系综 $(\rho_t)^{t\in[m]}$，且分布在 $[m]$上均匀）给出以下结论，

$$\begin{aligned} I(\mathbf{X}:\mathbf{Y}) &\leq S\left(\sum_{t=1}^{m}\frac{1}{m}\rho_t\right) - \sum_{t=1}^{m}\frac{1}{m}S(\rho_t) \\ &\leq S\left(\sum_{t=1}^{m}\frac{1}{m}\rho_t\right) \\ &\leq \log\left(\dim\left(\sum_{t=1}^{m}\frac{1}{m}\rho_t\right)\right) \\ &\leq q\log(2N). \end{aligned}$$

第二行成立是因为每个 $S(\rho_t)$ 都是非负的。第三行则由维数为 d(注 2.8) 下状态的最大熵得出。

左侧可以如下界定，

$$\begin{aligned} I(\mathbf{X}:\mathbf{Y}) &= H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y}) \\ &= \log(m) - H(\mathbf{X}|\mathbf{Y}) \\ &\geq \log(m) - H\left(\frac{1}{3},\frac{2}{3}\right) - \frac{1}{3}\log(m) \\ &\geq \frac{2}{3}\log(m) - 2. \end{aligned}$$

第三行由 Fano不等式（引理 2.11）得出。

因此，$q\log(2N) \geq I(\mathbf{X}:\mathbf{Y}) \geq \frac{2}{3}\log(m) - 2$，这意味着 $m = O((2N)^{3q/2})$.

□

现在我们可以用与经典情形类似的搜索到判定归约来证明定理 1.4 （[GGR13，定理 4。1]）。请注意，其复杂度与经典情形不同：在经典情形中，将随机化判定问题转化为确定性判定问题会带来三次方的复杂度开销（$\forall f$: $D(f) = O(R(f)^3)$），而在量子情形下，这种开销是四次方的（$\forall f$: $D(f) = O(Q(f)^4)$ 。

定理 1.4 的证明。固定一个查询复杂度为 $\mathrm{psQ}(R)$ 的伪确定性量子算法 A。对于每个 X，A 都存在一个规范输出 Y_X 。根据引理 3.1，我们可以用 $d = O(\mathrm{psQ}(R)\log(N))$ 比特对该输出进行编码。接着我们可以定义 d 全布尔函数 $(f_i)_i^d$，其中对所有 $i \in [d]$: $f_i(X) = (Y_X)_i$，也就是说，f_i输出 i 的第 Y_X 位。

我们使用以下事实来联系判定问题的确定性查询复杂度与量子查询复杂度。

定理 3.2 (定理 2 [ABK+21])。 对于任意全布尔函数 f，确定性查询复杂度与量子查询复杂度的关系如下：

$$\mathsf{D}(f_i) = O(\mathsf{Q}(f_i)^4)$$

我们还注意到，对于所有 $i \in [d]$，$\mathsf{Q}(f_i) = O(\mathsf{psQ}(R))$，由此可得

$$\mathsf{D}(R) = O\left(\sum_{i=1}^{d} \mathsf{D}(f_i)\right) = O(d \cdot \mathsf{psQ}(R)^4) = O(\mathsf{psQ}(R)^5 \log(N)).$$

□

3.2 一般伪确定性量子查询上界

我们通过任意问题的随机化查询复杂度和验证复杂度，给出了该问题的一般量子伪确定性查询上界。

定理 1.5。 对于任意搜索问题 R，若其随机化查询复杂度为 $\mathsf{R}(R)$，验证复杂度为 $\mathsf{V}(R)$，则有 $\mathsf{psQ}(R) = O((\mathsf{R}(R) + \mathsf{V}(R)) \cdot \sqrt{N})$。

我们的证明是对 [GIPS21 定理 3], 的直接推广。该定理通过构造从任意问题到 *Find1* 的完备性的一般归约，证明了 Find1（针对经典伪确定性查询复杂度）。我们注意到，同一归约在量子情形下也适用，随后将其与 $O(\sqrt{N})$ 上界结合起来，该上界由 Find1 [GIPS21]给出（另见 定理 5.1）。我们在 B 节中给出定理 1.5 的完整证明。

4 查询复杂度分离

本节中，我们证明伪确定性量子算法的两个查询复杂度分离结果。在4.1 节中，我们提出一个对经典随机化算法而言微不足道、但对伪确定性量子算法而言最难的问题。在4.2 节中，我们给出一个对经典随机化算法和伪确定性量子算法都很容易、但对经典伪确定性算法而言很难的问题。

4.1 伪确定性量子算法的一个最难问题 s

我们定义避免一个加密字符串（AOES）问题，并证明其伪确定性量子查询复杂度为 $\Omega(N)$，而对标准随机化算法而言则完全微不足道。我们证明了定理 1.1 所述的分离结果，定理重述如下。

定理 1.1. 存在一个搜索问题 R，其经典随机化复杂度为 $O(1)$，而其伪确定性量子查询复杂度为 $\Omega(N)$。

我们使用异或$_N$ 问题作为基本构件，因为异或$_N$ 对量子查询算法而言（渐近地）是最难的问题。这里，对于 $a, b \in \{0,1\}$：$a \oplus b$ 是两个比特的异或；对于字符串 $X, Y \in \{0,1\}^r$，$X \bigoplus Y$ 是两个字符串的按位异或。我们将 $\mathrm{XOR}(X)$ 写作字符串 X 中每个比特的异或。

这里，XOR_N 的输入是一个长度为 N 的字符串，输出是该字符串中每个比特的异或$_N$。当长度可由上下文明确时，我们将这个问题记作不带下标的 XOR。如下引理所述，对于 XOR 的量子算法而言，如果查询次数少于 $N/2$，就无法比随机猜测获得任何优势。

引理 4.1 ([FGGS98，BBC+01])。 假设 $\mathcal{A}$ 是一个针对异或问题的量子算法，并且它比随机猜测具有优势。换言之，若存在 p，$\delta \in \mathbb{R}$ 使得对于任意$X \in \{0,1\}^N$，

$$\mathbb{P}[\mathcal{A}^X = 1 | (\mathsf{XOR}(X) = 1)] \geq p + \delta,$$

and

$$\mathbb{P}[\mathcal{A}^X = 1 | (\mathsf{XOR}(X) = 0)] \leq p.$$

那么，A 的查询复杂度至少为 $\binom{N+1}{2}$ 。 ——

现在我们定义避免单个加密字符串（AOES）问题。非正式地说，AOES 的输入使用 m 个独立的异或实例来加密一个字符串 $b \in \{0,1\}^m$，目标是避免输出该加密字符串 b。直观来说，由于异或问题对于量子算法而言是最难的问题，因此字符串 b 无法被解密，量子算法也就无法避开它。请注意，参数 m 控制着量子伪确定性查询复杂度与经典随机查询复杂度之间的权衡。取 m 为一个较大的常数，即可获得最大的分离。

定义 4.2 (避免单个加密字符串 (AOES))。 设 $m \in \mathbb{N}$。在 AOES_m 问题中，我们可以访问 m 个不同字符串 X_1、.....、 $X_m \in \{0,1\}^{N/m}$ 的预言机。对于每个 $i \in [m]$，定义b_i =异或(X_i)。

目标是输出一个字符串 $x \in \{0,1\}^m$，使得 $x \neq b$。

当问题的参数可由上下文明确时，我们省略 AOES 的下标。我们还假设 m 整除 N，否则可以使用标准的填充论证。我们首先指出，对于较小的 m，AOES 对随机化算法来说很容易，而对确定性算法来说很难

命题 4.3。 以下关于AOES_m的复杂度的结论成立。

- $R(\mathrm{AOES}_m) = O(1)$;
- $D(\mathrm{AOES}_m) = \Theta(N/m)$。

证明。 第一项可通过从字符串 $x \in \{0,1\}^m$ 中均匀随机抽样得到；该字符串成为有效解的概率为 $1 - 1/2^m$。第二项的上界可通过使用 N/m 次查询计算$b_1 =$ 异或(X_1)并输出 $(1 \oplus b_1)0^{m-1}$得到。

我们使用标准的对手论证来证明该下界。假设存在一个用于 AOES 的确定性算法 $\mathcal{A}$，它进行 $q = N/m - 1$ 次确定性查询。每当 $\mathcal{A}$查询一个比特时，我们将该比特设为 0。在 $\mathcal{A}$ 输出一个解 $x \in \{0,1\}^m$ 之后，每个字符串 X_i 中至少有一个比特未被 $\mathcal{A}$查询。因此，可以将这些剩余比特设置为使得对所有 $i \in [m]$ 均有异或$(X_i) = x_i$，这意味着 $\mathcal{A}$ 是错误的。 □

我们表明，任何针对AOES的伪确定性量子算法都无法比平凡的确定性算法好太多。

定理 4.4 （AOES 的 psQ 下界）。 设 $m \in [N]$。任何针对AOES_m 的伪确定性量子算法都需要 $\Omega(N/m^2)$ 次查询。

注意，通过将 m 在 定理 4.4 中设为一个足够大的常数，我们便得到 定理 1.1。我们证明 定理 4.4 分两步进行。我们首先将一个零错误量子算法针对AOES转化为一个量子算法，用于异或 问题且具有某种 非零 优势。然后，我们将该零错误算法替换为一个伪确定性算法。

下面的引理表明，只需获取一个用于 AOES 的算法的单个样本，就足以提取有关某个字符串的异或的非零信息。

引理4.5。 如果存在一个用于 $\mathrm{AOES}_{N,\ m}$ 查询复杂度为q的零错误量子算法 B，那么就存在一个用于 异或$_{N/m}$ 的量子算法 A，它调用 B 一次，并且对每个输入 $X \in \{0,1\}^{N/m}$，

$$\mathbb{P}\left[\mathcal{A}^X = \mathsf{XOR}(X)\right] \geq \frac{1}{2} + \frac{1}{2^{m+1}}.$$

归约。 我们利用 $\mathcal{B}$ 构造一个用于 $\mathcal{A}$ 的 异或$_{N/m}$算法。在该算法中，我们将 异或 实例 X 编码为一个AOES_m随机化实例；从$\mathcal{B}$的视角来看，该实例与均匀随机实例在信息论上不可区分。如果 $\mathcal{B}$ 的输出满足某些条件，我们就能确定无误地恢复 X 的奇偶性。算法$\mathcal{A}$ 的伪代码见 算法 2。

算法 2 由算法B^X 构造的用于异或$_{N/m}$ 的算法A （该算法针对 $\mathrm{AOES}_{N,\ m}$）

Uniformly sample an index set $I \subseteq [m]$ and strings $Y_1, \cdots Y_m \in \{0,1\}^{N/m}$.
For all $j \in [m]$: Let $Z_j = \begin{cases} Y_j & \text{if } j \in I \\ Y_j \oplus X & \text{otherwise} \end{cases}$
Run algorithm $\mathcal{B}$ on $(Z_1, \cdots, Z_m)$, get the outcome $a = (a_1, \cdots, a_m)$.
if $\exists t \in \{0,1\}, \forall j \in [m] : a_j = \begin{cases} \mathsf{XOR}(Y_j) & \text{if } j \in I \\ \mathsf{XOR}(Y_j) \oplus t & \text{otherwise} \end{cases}$ **then**
    Output $1 \oplus t$.
else
    Output a uniformly random bit.
end if

分析。现在我们证明算法$\mathcal{A}$的正确性。为简单起见，我们定义以下比特

$$x^* = \mathsf{XOR}(X),\ \forall j \in [m] : y_j = \mathsf{XOR}(Y_j),\ z_j = \mathsf{XOR}(Z_j).$$

执行完算法$\mathcal{A}$的前三步后，我们得到（a_1， $\cdots$ a_m），它是 AOES 实例（Z_1， $\ldots$， Z_m）的一个有效解。现在，我们定义以下集合

$$J := \{j \in [m] : a_j = z_j\}.$$

请注意，$\mathcal{A}$ 无法直接计算 J，因为当 $j \notin I$时，$\mathcal{A}$ 不知道z_j 的值。尽管如此，$\mathcal{A}$ 总能测试 J 是否等于 I，如下述命题所示。

命题 4.6。 当且仅当 算法 2 满足以下条件： $I = J$。

证明。 对于一个方向，若 $I = J$，则对任意 $j \in [m]$，都有

$$a_j = \begin{cases} z_j & \text{if } j \in I \\ z_j \oplus 1 & \text{otherwise} \end{cases}.$$

现在，如果 $j \in I$，将 z_j 替换为 y_j；否则替换为 $(y_j \oplus x^*)$，即可得到

$$a_j = \begin{cases} y_j & \text{if } j \in I \\ y_j \oplus x^* \oplus 1 & \text{otherwise} \end{cases}.$$

因此，取 算法 2 即可满足该条件： $t = x^* \oplus 1$。

另一方面，若 算法 2 中的条件成立，我们可以将该条件中的 y_j 替换为 z_j，或将$z_j \oplus x^*$替换为 $j \in I$，或将 $j \notin I$ 替换为相应的项；此时有

$$a_j = \begin{cases} z_j & \text{if } j \in I \\ z_j \oplus x^* \oplus t & \text{otherwise} \end{cases}.$$

我们断言 $x^* \oplus t = 1$；否则，对于所有 $j \in [m]$，都有 $a_j = z_j$，这与 a 是 AOES 实例的有效解这一事实矛盾。因此，根据 J 的定义，我们有 $I = J$。

□

命题 命题 4.6 的证明立即推出以下推论。

断言 4.7。 算法 $\mathcal{A}$ 在 算法 2 中总是给出正确答案。

证明。 在 命题 4.6 的证明中，我们证明了若 算法 2 中的条件成立，则必有 $x^* \oplus t = 1$。因此，$x^* = t \oplus 1$ 是正确答案。 □

断言 4.8。 算法 2 中的条件以概率 $1/2^m$得到满足。

证明。由命题 4.6，只需证明 $I = J$ 以概率 $1/2^m$发生。注意，I的选取与 Y_1、……、Y_m独立，并且 Y_1、……、Y_m是均匀随机的。因此，I也与 $(Z_1, \ldots\ldots, Z_m)$ 独立。由于集合 J仅取决于 $(Z_1, \ldots\ldots, Z_m)$ 和 B 的内部随机性，I 和 J 也相互独立。因此，I 以概率 $1/2^m$ 等于 J。 □

结合 断言 4.7 和 断言 4.8，$\mathcal{A}$的整体成功概率为

$$\frac{1}{2^m} + \frac{1}{2}(1 - \frac{1}{2^m}) = \frac{1}{2} + \frac{1}{2^{m+1}},$$

由此得证引理 4.5。

最后，我们证明可以将AOES 在 引理 4.5 中的零错误算法替换为伪确定性算法，并且只需少量增加查询复杂度。

引理 4.9. 若存在一个用于 $\mathrm{AOES}_{N,\,m}$ 查询复杂度为 q 的伪确定性量子算法 $\mathcal{B}$，则存在一个用于异或$_{N/m}$ 的量子算法 $\mathcal{A}$，其查询复杂度为 $O(q \cdot m)$，使得对于每个输入 $X \in \{0,1\}^{N/m}$，

$$\mathbb{P}\left[\mathcal{A}^X = \mathsf{XOR}(X)\right] \geq \frac{1}{2} + \frac{1}{2^{m+2}}.$$

证明。 给定这样一个伪确定性算法$\mathcal{B}$，我们可以构造一个新算法 $\mathcal{B}'$，让它重复运行 $\mathcal{B}^X$ $100m$ 次，并输出这些重复运行中最常见的结果（若出现并列，则任意选择）。根据 Chernoff 界，$\mathcal{B}'$ 的错误概率小于 $\frac{1}{2^{m+2}}$。

由于用于AOES 的零错误算法在 引理 4.5中只调用一次，因此我们可以用$\mathcal{B}'$替换它，并且整体错误概率至多增加 $\frac{1}{2^{m+2}}$。 □

结合 引理 4.9 与 引理 4.1，我们得出 定理 4.4。

备注 4.10. 证明 定理 4.4 时，唯一用到伪确定性性质的地方是 引理 4.9中的重复技巧。相比之下，针对AOES的平凡随机采样算法的错误概率为 $1/2^m$；然而，我们无法通过重复来降低这一错误概率。

事实上，我们对 定理 4.4 的证明意味着，要将 $1/2^m$ 的错误概率降至远低于该值，对于 AOES 而言极其困难，即使使用标准量子算法也是如此。

4.2 指数级伪确定性量子优势

本节中，我们定义了一个问题——量子锁定估计（QL-Estimation），经典算法很难以伪确定性的方式解决该问题，但伪确定性量子算法和随机化经典算法则能轻松解决。

定理 1.3。 存在一个搜索问题 R ，使得

1. 存在一个针对 R 的经典随机化算法 *A*，其使用 $O(\log N)$ 次查询；*2.* 存在一个量子伪确定性算法 *B*，其查询复杂度为 $O(\log N)$ ，可以将 *A* 规范化；*3.* 对于 R 的任何经典伪确定性算法都需要 $\Omega(\sqrt{N})$ 次查询。

—

该 QL-估计 问题可以看作一种 锁钥 构造。我们首先选择汉明 问题——计算字符串汉明重量的估计值——作为“锁”，因为它对经典随机化算法而言很容易，但对任何伪确定性经典算法而言都很困难。然后加入一把“钥匙”，即 Simon 问题 [Sim97], ，将其作为具有指数级量子优势的搜索问题，并且“钥匙”问题的唯一解是“锁”问题的有效解。将这些结合起来，锁钥承诺问题的输入是一对 (f, X)。如果钥匙问题在输入 f 上的解是锁问题在输入 X 上的一个解，并且任何整体上的有效解都是锁问题在输入 X上的一个解，则这种形式的输入满足承诺（因此是有效输入）。这意味着量子算法可以获得秘密字符串；我们知道，该字符串是这个问题的伪确定性解，而该问题在经典伪确定性意义下很难。

在本节中，除非另有说明， $N = 2^n$。我们先介绍以下必要的定义。

定义 4.11 (Simon 问题)。该问题的输入是一个函数 $f\colon \{0,1\}^n \to \{0,1\}^n$，并承诺它是一个二对一或一对一函数，且存在一个秘密字符串 $s \in \{0,1\}^n$ ，使得

$$\forall x, y \in \{0,1\}^n : f(x) = f(y) \iff x = y \oplus s \quad or \quad x = y.$$

给定对该函数的预言机访问，目标是输出秘密字符串 s。特殊情况 $s = 0^n$意味着 f 是长度为 n的字符串的一个置换。

稍微滥用一下记号，我们将 $s \in \{0,1\}^n$ 视情况视为字符串或 n 位二进制数。对于 $s \in \{0,1\}^n$，我们用 $\mathcal{F}_s$ 表示在 $\{0,1\}^n$上编码秘密字符串 s的 Simon 函数集合，即所有满足以下条件的函数 $f\colon \{0,1\}^n \to \{0,1\}^n$：对于任意互不相同的$x$， $y \in \{0,1\}^n$，当且仅当 $x = y$或 $x = y \oplus s$时， $f(x) = f(y)$。我们将使用以下 Simon 问题查询复杂度的标准界。

定理 4.12([Sim97])。 任何解决 *Simon* 问题的经典随机算法都需要 $\Omega(2^{n/2})$次查询，而存在一种解决 *Simon* 问题的量子算法，只需使用 $O(n)$ 次查询。

事实上，我们需要 以下关于 Simon 问题难度的更强结论 .

引理 4.13。 给定一个函数 $f \in \mathcal{F}_s$ ，并承诺秘密字符串 s 属于两个互不相交的集合 $S_1, S_2 \subseteq \{0,1\}^n$之一，那么任何经典随机算法都需要进行$\Omega(\sqrt{\min(|S_1|, |S_2|)})$次查询，才能确定 s 属于 S_1 还是 S_2。

证明。 以二分之一的概率，让秘密字符串 s 从 S_1中均匀抽取；以二分之一的概率，让 s 从 S_2中均匀抽取。然后，让 f 从$\mathcal{F}_s$中均匀抽取。

根据 Yao 极小极大原理，只需考虑在上述输入分布下，至多进行 $t = o(\sqrt{\min(|S_1|, |S_2|)})$ 次查询的任意确定性算法$\mathcal{A}$ 。不失一般性，我们假设$\mathcal{A}$ 一旦发现 f发生碰撞，就立即停止并输出答案。利用对称性，我们可以通过合并节点来简化$\mathcal{A}$ 的决策树，使每个非叶节点只有两个子节点：一个表示发现了碰撞，另一个表示没有发现碰撞。

如果对 u的祖先节点进行的查询尚未排除 f 的秘密字符串为 t的可能性，我们就称节点 u 处的字符串 t 仍然存活$alive$ 。在根节点处， S_1 和 S_2 中的所有字符串都仍然存活，而深度为 d 处的一次查询最多可以$kill$ $d-1$ 个字符串。利用对称性，$\mathcal{A}$ 从未发现碰撞的概率为$1 - o(1)$。并且，在条件为到达一个未发生碰撞的叶节点 u 时， S_1 和S_2 中的大多数字符串在 u处仍然存活。因此，无论 $\mathcal{A}$ 在 u处输出 S_1 还是 S_2 ，$\mathcal{A}$ 出错的概率都至少为 $\frac{1}{2} - o(1)$。这说明$\mathcal{A}$并不正确，因此至少需要 $\Omega(\sqrt{\min(|S_1|, |S_2|)})$ 次查询。 □

现在，我们正式陈述汉明重量近似问题的一个版本，并将其记为汉明问题。

定义 4.14 （汉明问题）。给定一个比特串 $X \in 01^N$，目标是输出 X 的汉明重量近似值，其加性误差范围为 $N/10$；也就是说，

$$\textsc{Hamming} = \{(X, t) \in \{0,1\}^N \times \mathbb{N} : |\|X\|_{\mathsf{hw}} - t| \le N/10\} .$$

由于我们允许汉明问题的解与实际汉明重量相差一个范围，因此可以通过随机采样算法，用 O（1）次查询轻松解决。然而，汉明问题已被证明是经典伪确定性算法最难解决的问题 [GGR13]。我们在此重现该证明，因为其中包含一些有助于稍后证明 QL-估计问题下界的有用思路。

定理 4.15 （ [GGR13]的推论 3.2）。 $\mathsf{psR}(\text{汉明问题}) = \Omega(N)$。

证明。 现在设 $\mathcal{A}$ 是一个用于汉明问题的伪确定性算法。令 $X^* \in \{0,1\}^N$ 为某个固定字符串，其汉明重量为 $N/2$，并令 $t := \mathcal{A}^{X^*}$。接着，我们选取一个字符串 $Y \in \{0,1\}^N$，使得在所有满足$\mathcal{A}$ 以至少 $2/3$ 的概率输出 t 的字符串中，它的汉明重量最小（若有并列，则任意选取）。 Y 的汉明重量至少为 $3N/10$。

现在考虑将 Y 中的一个“1”翻转为“0”后得到的字符串集合 $\mathcal{E}_Y$，即

$$\mathcal{E}_Y := \{X \in \{0,1\}^N : \exists i \in [N], X_i = 0 \wedge Y_i = 1 \wedge (X_j = Y_j, \forall j \neq i)\}.$$

根据定义，对于任意字符串 $Y\prime \in \mathcal{E}_Y$，我们有 $\mathcal{A}^Y \neq \mathcal{A}^{Y'}$；我们还知道 $|\mathcal{E}_Y| \ge 3N/10$。因此，要区分 Y 与 $\mathcal{E}_Y$ 中的所有字符串，$\mathcal{A}$ 需要 $\Omega(N)$ 次查询。 □

现在我们陈述 QL-估计问题，其中 Simon 问题是“钥匙”，而汉明是“锁”。

定义4.16 (QL-估计问题。 输入是一个二元组 (f, X)，其中 $f: \{0,1\}^n \to \{0,1\}^n$ 且 $X \in \{0,1\}^N$，其中 $N = 2^n$。这里，(f, X) 承诺满足以下条件。

- $f \in F_s$ 对于字符串 $s \in \{0,1\}^n$，即 f 是一个有效的 *Simon* 实例，其编码了秘密字符串 s；
- $\big|\|X\|_{\text{汉明重量}} - s\big| \le 0.09 \cdot N$，即， s 的值是汉明 实例 X的有效解

.

目标是在距离 X的汉明重量 $N/10$ 范围内输出一个整数 $t \in [N]$ 。

在这种情况下，对输入（f， X）QL-估计的一次查询，可以是对 f 或对 X 的查询，而用于QL-估计的算法的查询复杂度，是对输入任一部分进行查询的总次数。我们证明，QL-估计对经典随机算法而言很容易，并且存在一个量子伪确定性算法将其规范化；但该问题对经典伪确定性算法而言很难。这立即推出定理 1.3。

定理 4.17。令 $N = 2^n$ 为QL-估计中的长度参数，则QL-估计的复杂度满足以下结论。

1. R(QL-Estimation) $= O(1)$；2. psQ(QL-Estimation) $= O(\log N)$；
3. psR(QL-Estimation) $= \Omega(\sqrt{N})$。

此外，存在一个用于QL-估计的经典随机算法 A，其查询复杂度为 $O(\log N)$；还存在一个伪确定性量子算法 B，其查询复杂度为 $O(\log(N))$，使得 B 将 A 规范化。

上界与规范化。第一个上界成立，因为经典随机算法可以通过采样直接求解汉明部分，并通过随机采样以 $O(1)$次查询忽略 Simon 问题。对于第二个上界，请注意，伪确定性量子算法也可以使用 $O(\log N)$次查询求解 QL-估计：先在 Simon 问题中根据给定的 f 求解秘密字符串 s ，然后输出 s 作为汉明重量的估计。

关于规范化的最后一点说明（定义1.2），我们将量子算法$\mathcal{B}$ 取为求解并输出秘密字符串 s 的算法，如上所述。然而，我们需要构造一个修改后的随机化算法$\mathcal{A}$，如下所述：

1. 对 X 进行 $10^6 \cdot \log N$ 次查询，并令$\hat{t}$ 为 X汉明重量的最佳估计。
2. O在范围 $I := [\hat{t} - 0.095N,\ \hat{t} + 0.095N]$内输出一个均匀随机整数 .

根据 Chernoff 界，$|\hat{t} - \|X\|_{\mathsf{hw}}| \le 0.005N$为 $(1 - o(1/N))$ 的概率是。在这种情况下，$\mathcal{A}$ 总是输出一个正确的解，并且根据 QL-估计问题的承诺，我们有 $s \in I$ 。因此，$\mathcal{B}$ 的规范输出 s 将以 $\Omega(1/N)$ 的概率由$\mathcal{A}$ 输出。这说明$\mathcal{B}$ 规范化了$\mathcal{A}$

伪确定性下界。为了证明任意经典伪确定性算法的 $\Omega(\sqrt{N})$ 下界，我们声称，任何用于 QL-估计的亚线性伪确定性经典算法都必须近似地 解决底层的 Simon 问题，这意味着根据 Simon 问题的经典困难性可得一个下界。

引理 4.18。 设 A 是一个用于QL-估计 的伪确定性经典算法，使用$o(N)$ 次查询。对于任意满足 $\|X^*\|_{\mathsf{hw}} = N/2$ 的字符串 $X^* \in \{0,1\}^N$，以及任意取值介于 $0.41N$ 和 $0.59N$ 之间的字符串 $s \in \{0,1\}^n$，对于任意 *Simon* 函数 $f \in \mathcal{F}_s$，A 在输入(f, X^*) 上的规范输出都是某个满足 $|s - t| \le 0.01N$ 的 t。

证明。 取 $\mathcal{A}$ X^*, s 作为满足 引理 4.18 陈述中条件的对象，并考虑任意一个 $f \in \mathcal{F}_s$ 并令 t 为 $\mathcal{A}$ 在输入 (f, X^*) 上的规范输出。根据 $\mathcal{A}$的正确性，我们有 $2N/5 \le t \le 3N/5$。

接着，我们选取一个字符串 Y_{low}，使得在$\mathcal{A}^{(f,\cdot)}$ 输出 t的条件下，其汉明重量最小（若有并列，则任意选择）。 Y_{low} 的汉明重量至少为 $2N/5 - N/10 = 3N/10$。我们声称 $\|Y_{\mathsf{low}}\|_{\mathsf{hw}} = s - 0.09N$。

反设不然，即 $\|Y_{\mathsf{low}}\|_{\mathsf{hw}} > s - 0.09N$，我们定义集合$\mathsf{E}_{\mathsf{low}}$，它由将 Y_{low}中任意一个“1”翻转为“0”所得到的字符串组成。对于任意字符串 $Y' \in \mathsf{E}_{\mathsf{low}}$，我们有 $\|Y'\|_{\mathsf{hw}} \geq s - 0.09N$，因此$(f, Y')$是QL-估计问题的一个有效输入。回顾可知， t 是A在输入(f, Y_{low})上的规范输出，并令 t' 为A在输入(f, Y')上的规范输出。根据 Y_{low}的定义，我们有 $t \neq t'$。我们知道 $|\mathsf{E}_{\mathsf{low}}| \geq 3N/10$，这意味着A至少需要$\Omega(N)$次查询才能将 Y_{low}与$\mathsf{E}_{\mathsf{low}}$中的所有字符串区分开来。这与A使用 $o(N)$次查询的假设相矛盾。因此，我们得出结论：$\|Y_{\mathsf{low}}\|_{\mathsf{hw}} = s - 0.09N$。

类似地，我们可以令 Y_{hi} 为使 $\mathcal{A}^{(f,\cdot)}$ 输出 t 的汉明重量最大的字符串。由对称性可得 $\|Y_{\mathsf{hi}}\|_{\mathsf{hw}} = s + 0.09N$。由于 t 是 Y_{hi} 和 Y_{low} 的有效解，因此有 $|t - (s - 0.09N)| \leq N/10$ 和 $|t - (s + 0.09N)| \leq N/10$。这意味着 $|s - t| \leq 0.01N$。 □

现在我们可以证明经典伪确定性算法的下界了。

定理 *4.17* 的证明，第 *3* 项。 定义集合

$$S_1 = \{s : 0.4N \leq s \leq 0.45N\},\ S_2 = \{s : 0.55N \leq s \leq 0.6N\}.$$

我们知道 $|S_1| = |S_2| = N/20 = \Omega(N)$。

假设秘密字符串 s 承诺属于以下两种情况之一： S_1， S_2，目标是区分这两种情况，引理 4.13 表明，该任务的随机化查询复杂度仍为 $\Omega(\sqrt{N})$。

现在，设 A 是任意一个用于 QL-估计、查询复杂度为 $o(N)$ 的经典伪确定性算法。给定一个 Simon 函数 $f \in \mathsf{F}_s$，且 s 属于 S_1 或 S_2，我们可以对某个满足 $\|X^*\|_{\mathsf{hw}} = N/2$ 的 X^* 运行 $\mathsf{A}^{(f,X^*)}$，并将其伪确定性解记为 t。根据引理 4.18，必有 $t \leq 0.46N$ 或 $t \geq 0.54N$，据此我们可以判断 $s \in S_1$ 还是 $s \in S_2$。因此，A 的查询复杂度为 $\Omega(\sqrt{N})$。

□

5 Ps小开销的伪确定性量子优势

本节中，我们将展示一大类量子查询算法可以通过一种基于二分搜索的方法，以较小的开销实现伪确定性。首先，我们将在第 5.1 节中介绍一种渐近开销为零的伪确定性格罗弗算法。随后，我们将在第 5.2 节中将这一思路推广到更广泛的一类算法。

记号。对于任意索引集 $I \subseteq [N]$，令 $X|_I \in \{0,1\}^{|I|}$为 X 限制于 I 中索引的子序列。对于任意两个元素元组 $X = (x_1, \ldots, x_t)$ $Y = (y_1, \ldots, y_\ell)$，我们将$X \circ Y = (x_1, \ldots, x_t, y_1, \ldots, y_\ell)$记作它们的串接。

5.1 热身：格罗弗算法

我们先介绍 [GIPS21] 给出的一个非正式结果：通过二分搜索，Grover 算法可以实现伪确定性，但查询复杂度会增加对数级开销。我们通过更细致的分析证明，可以避免这一开销。其结果如定理 2.5 所述，即使输入中的大多数比特为 1，也给出了 $\Omega(\sqrt{N})$ 的下界。

令 格罗弗 表示这样一个量子查询算法：对于输入 $X \in \{0,1\}^N \setminus \{0^N\}$，其输出$i \in [N]$满足 $X_i = 1$，并且使用 $O(\sqrt{N})$ 次查询。我们在算法 3中正式介绍伪确定性 Grover 算法。

算法 3：针对 $N = 2^n$ 个元素的伪确定性格罗弗搜索 1：令 L $\leftarrow 1$，R $\leftarrow N$ 2：对于 $k = 0 \ldots n-1$，执行 3：Cur $\leftarrow \lfloor$(L $+$R)/2$\rfloor$，$I \leftarrow$ {L，L $+1$，...，Cur} 4：运行 Grover($X|_I$) $k+2$ 次。5：如果至少一次 Grover 调用返回了一个满足 $X_i = 1$ 的索引 $i \in I$：则 6：R $\leftarrow$Cur 7：否则 8：L $\leftarrow$ Cur $+1$ 9：结束如果 10：结束循环 11：输出 L

定理 5.1。 对于 $N > 1$，存在一种查询复杂度为 $O(\sqrt{N})$ 的伪确定性量子算法；输入 $X \in \{0,1\}^N \setminus \{0^N\}$ 时，它以至少 $2/3$ 的概率输出满足 $X_i = 1$ 的最小索引 $i \in [N]$。

证明。 在此证明中，不失一般性，我们假设 $N = 2^n$ 对于某个 $n \in \mathbb{N}$ 否则，我们可以通过补齐输入来实现，代价是增加常数次查询。我们考虑 算法 3中给出的算法。首先注意到，算法 3的查询复杂度上界为

$$\sum_{k=0}^{n-1}(k+2)O\left(\sqrt{N/2^{k+1}}\right) = O\left(\sqrt{N}\sum_{k=0}^{n-1}\frac{k+2}{\sqrt{2^{k+1}}}\right) = O(\sqrt{N}).$$

令 i_0 为满足 $X_{i_0} = 1$ 的最早下标（根据输入的承诺，该下标存在）。算法结束时，L 的值等于 i_0，当且仅当在算法的每个阶段都有 $i_0 \in [L, R-1]$。假设格罗弗算法的某次迭代在 $i_0 \in I$ 时接受，那么集合 I 的每次重新赋值都会使 I 的大小减半，同时仍包含 i_0。因此，算法在经过 n 次迭代后终止时，$L = i_0$，$R = i_0 + 1$，且 $I = \{i_0\}$。

算法 3 中的二分搜索 可能失败，当且仅当存在某一步 $k \in [n-1]$，使得所有 $k+2$ 次 Grover 算法重复运行都未能在 $X|_I$ 中找到一个现存的“1”，其中 $i_0 \in I$。在每个阶段，如果确实找到一个 1，那么 i_0 在 I 下一步仍然成立。Grover 算法在步骤 k 中所有 $k+2$ 次迭代均失败的概率上界为 $1/3^{k+2}$。对所有 k应用并集界，可得错误概率的上界为 $\sum_{k=0}^{n-1} \frac{1}{3^{k+2}} < 1/6$。 □

5.2 Prunable可剪枝问题

现在，我们将上一节中的想法推广，并介绍一类更广泛的问题，使得对于该类中的任意问题，都可以通过较小的额外开销将其量子算法转化为伪确定性算法。具体而言，我们考虑这样一类问题：寻找输入的一个小子集（即见证），使其具有某种特定性质。

定义 *5.2*（*k*-子集查找 [CE05]）。设 $k, N \in \mathbb{N}$。k-子集查找问题由关系 $R \subseteq \Sigma^k \times [N]^k$ 定义。给定对输入 $X \in \Sigma^N$ 的预言机访问，任务是找到一对 (Y, I)，使得 $I \subseteq [N]$ 的大小为 k，且 $X|_I = Y$，满足 $(Y, I) \in R$；如果不存在这样的数对，则输出 $\perp$。

现在我们描述一个较弱的条件，并据此将一类问题称为 Prunable。在这个条件下，对于 k-子集查找问题 R 的算法 $\mathcal{A}$ ，只需付出较小的额外开销，就能将其改造为伪确定性算法。粗略地说，如果对于每个 $I \subseteq [N]$ ，都存在一种算法，在仅限于使用 I 中的索引时，能够为 R 找到一个子集，且其查询复杂度不超过为 R 查找子集所需的查询复杂度，那么问题 R 就是 Prunable 。

定义 5.3 (Prunable)。令由 $R \subseteq \Sigma^k \times [N]^k$ 定义的搜索问题为一个k-子集查找问题的实例，并令 A 为求解 R 的 R 次查询量子算法。对于任意索引集 $I \subseteq [N]$，定义一个新的 k- 子集查找问题 $R|_I := R \cap (\Sigma^k \times I^k)$。

我们称 R 是 Prunable ，若对于任意索引集 $I \subseteq [N]$，都存在一个算法 A_I ，它以 O 次$(\mathsf{Q}(R))$ 次查询求解$R|_I$ 。

˜定理 1.6。令 R 为一个 k-子集查找问题。若 R 是 Prunable，则 $\mathsf{psQ}(R) = O(k \cdot \mathsf{Q}(R))$。

证明。考虑算法 4中给出的算法。该算法通过迭代逐步构造出按字典序最大的、能够解决该搜索问题的子集。假设已经找到子集中的前 $\ell - 1$个元素，并令 T 为这些 $\ell - 1$ 个元素对应的索引集合。算法通过二分搜索，找到满足问题 $R|_I$ 仍有 i 有效解的最大索引 $I = T \cup \{i,\ i+1 \ldots,\ N\}$。然后， X_i 被选为该子集中的第 ℓ个元素。

算法 4 使用随机化量子算法 R 的伪确定性算法，用于 a Prunable 问题

1：令 $\mu \leftarrow 10\log(k\log(N))$ 2：令 $Y \leftarrow ()$ $T \leftarrow \emptyset$, $Next \leftarrow 1$3：对于 $\ell = 1, \ldots, k$，执行 4：令 $L \leftarrow Next$, $R \leftarrow N$5：当 $L < R$ 时，执行 6：Cur $\leftarrow \lceil (L+R)/2 \rceil$, $I \leftarrow T \cup \{\text{Cur}, \text{Cur} + 1, \ldots, N\}$ 7：运行 $\mathsf{A}_I(X)$ 共 μ 次。8：如果 A_I 的任一次迭代找到 $R|_I$ 的解，则 9：$L \leftarrow$Cur 10：否则 11：$R \leftarrow$ Cur $-1$12：结束 if 13：结束 while 14：$Y \leftarrow Y \circ X_L$15：$T \leftarrow \{L\} \cup T$16：$Next \leftarrow L + 1$17：结束 for 18：输出 (Y, T)

算法 4 仅在存在某个步骤时才可能失败 $\ell \in [k]$ ，使得在二分搜索的某一步中， $R|_I$存在一个解，但所有 $\mu = 10\log(k\log(N))$ 次重复运行$\mathcal{A}_I$都未能找到解。注意，对于每个 $\ell \in [k]$，二分搜索需要进行 $O(\log(N))$ 次$\mathcal{A}_I$迭代 k 。因此，根据 $k \cdot \log(N)$ 次迭代的并集界，失败概率至多为

$$\frac{k\log(N)}{3^{10\log(k\log(N))}} = \frac{k\log(N)}{(k\log(N))^{10\log(3)}} = o(1).$$

同样，根据 Prunable 条件，$\mathcal{A}_I$ 的每次重复运行需要 $O(Q)$ 次查询。因此，˜的查询算法 4 复杂度的上界为 $k \cdot \log N \cdot \mu \cdot Q = O(k \cdot Q)$。

□

由此结果，我们立即得到以下用于下列问题的伪确定性量子查询算法，这些问题满足 Prunable。

定义 5.4. k-互异性 是这样一个问题：给定输入 $X \in [m]^N$，找出 $i_1, \ldots, i_k$，使得 X在每个索引处取值相同。

存在 一个 $\tilde{O}(N^{3/4})$ 查询量子算法，用于求解 k-互异性问题 [Bel12，定理 8].

推论 5.5. 存在一 存在一个 $\tilde{O}(N^{3/4}k)$ 查询伪确定性量子算法，用于求解 k-互异性问题 s.

定义 5.6。 三角形 是一个图问题：给定一个具有 *over* n 个顶点的图，寻找一个包含3 个顶点的完全子图。

存在一个 $\tilde{O}(n^{5/4})$ 查询量子算法，用于求解三角形 邻接矩阵模型中的[Gal14，定理 1。1]。

推论 5.7。该 存在一个 $\tilde{O}(n^{5/4})$ 查询伪确定性量子算法，用于求解三角形 .

定义 5.8。 k-和 是这样一个问题：通过查询访问形式为 $X \in [m]^N$ 的输入，判断是否存在一个大小为 k 、元素之和为某个固定整数 t 的子集。

定理 1 中存在一个通用的 $O(N^{k/(k+1)})$ 查询量子算法，用于 k-子集查找，见 [CE05]。 k-和 是一个特殊情形，因此可得以下结论。

推论 5.9。 对于k-SUM 问题，存在一个 $\tilde{O}(N^{k/(k+1)} \cdot k)$ 次查询的伪确定性量子算法。

定义 5.10。 图碰撞 是这样一个问题：给定一个 G 上的无向图（具有 n个顶点），以及对一组布尔值$\{x_v | v \in G\}$的查询访问，确定是否存在两个顶点 v、 v'，它们由一条边 $x_v = x_{v'} = 1$连接。

根据 $O(t^{1/6} \cdot \sqrt{n})$ 次查询量子算法，存在一个用于图碰撞 问题的量子算法，其图的树宽为 t ，由 [ABI+13]中的定理 1 得出。

推论 5.11。 当树宽为 t时，对于图碰撞 问题，存在一个 $\tilde{O}(t^{1/6} \cdot \sqrt{n})$ 次查询的伪确定性量子算法。

注 5.12。 注意，最后一个结果是由以下事实得出的：任意子图的树宽至多等于原图的树宽，因此该问题是 Prunable。

具有全局结构的问题的局限性。Find1 问题是一个无法通过该定理实现伪确定性的问题示例。特别是，在二分搜索过程中，输入位中多数为 1 的承诺不再成立。非正式地说，如果一个高效的随机化／量子查询算法 $\mathcal{A}$ 高度利用了问题的全局结构 R，那么我们的二分搜索方法可能会失败，而且很可能， R 根本不存在任何高效的伪确定性算法。

现在我们再介绍一个量子算法的例子，由于其“全局结构”，它无法变为伪确定性算法。

定义 5.13。 固定一个图 $G=(V,E)$，并提供对一个函数的预言机访问 $f\colon V\to\{0,1\}$，使得当 $f(v)=1$ 时，顶点 $v\in V$ 被标记。目标是输出一个标记顶点。

f 的击中时间定义为随机游走在到达由 f 标记的顶点时终止，其长度的期望值。

与经典随机游走相比，量子游走算法实现了二次加速。

定理 5.14([Sze04, AGJK20])。 对于量子算法，在击中时间为 HT 的图上寻找标记顶点需要 $\tilde{O}(\sqrt{HT})$ 次查询。

然而，伪确定性地实现这一点并不可行，因为对整个图成立的承诺（击中时间较小）在取子图后并不一定成立。考虑图 G 是由 n 个顶点构成的完全图，且大多数顶点都被标记。这可归约为 $\sqrt{N}$ FindGIPS1 [的下界21]。

我们注意到，尽管寻找标记顶点的量子游走算法无法实现伪确定性，但使用该算法作为子程序的算法（例如 k-差异性 [Bel12] ）可以实现伪确定性，因为该问题是 `Prunable`。

6 量子搜索问题与连续域

我们将搜索问题的概念扩展到量子输入。为此，考虑一个搜索问题$R\subseteq\mathcal{X}\times\mathcal{Y}$。这里，$\mathcal{X}$ 是一个纯态集合，

$$\mathcal{X}\subseteq\bigcup_{d\in\mathbb{N}}\mathcal{S}(\mathbb{C}^d),$$

并且$\mathcal{S}(\mathbb{C}^d)$表示维度为 $d\in\mathbb{N}$ 的纯态集合，这些纯态表示为归一化向量$|\psi\rangle\in\mathbb{C}^d$，满足$\langle\psi|\psi\rangle=1$。在此设定中，我们考虑这样的算法：显式接收维度$d\in\mathbb{N}$，并通过预言机访问获取未知量子态 $|\psi\rangle\in\mathcal{S}(\mathbb{C}^d)$的副本。在这个模型中，量子算法是作用于 $|\psi\rangle\langle\psi|^{\otimes t}$ 上的一个POVM，而 t 的值就是该算法的查询复杂度（即未知量子态 $|\psi\rangle$的副本数）。

形式上，POVM表示为一组半正定矩阵$\{M_y\}_{y\in\mathcal{Y}}$，它们作用于$(\mathbb{C}^d)^{\otimes t}$，并且$\sum_{y\in\mathcal{Y}}M_y=I$，其中 I 是$(\mathbb{C}^d)^{\otimes t}$上的单位矩阵。对于输入 $|\psi\rangle\in\mathcal{S}(\mathbb{C}^d)$，观察到输出 $y\in\mathcal{Y}$ 的概率为$\mathrm{Tr}(M_y|\psi\rangle\langle\psi|^{\otimes t})$。

H此处，我们将伪确定性视为与定义 2.1中的概念相同 .

备注 6.1。本节重点讨论将量子纯态映射为经典字符串的搜索问题；不过，也可以考虑输入为混合态、酉算子或量子信道的情形。

当量子算法的输出本身是量子态时，伪确定性的概念就会变得棘手。在大多数此类任务中，允许输出近似结果（例如量子态层析），但对同一输入重复运行算法会得到不同的近似结果。这表明，对于这些问题，似乎无法立即给出一个既能保持其基本性质的伪确定性定义。

在此，我们考虑输入为量子态的搜索问题，并证明伪确定性解的数量以有效输入集合的连通分支数量为上界。为此，我们需要如下定义。

定义 6.2. 设 $d \in \mathbb{N}$。考虑一个量子查询算法 A，其输入为量子态$|\phi\rangle \in S(\mathbb{C}^d)$，且其输出空间为 Y。

我们将 $g_{\mathcal{A}}$： $S(\mathbb{C}^d) \to \Delta_{\mathcal{Y}}$ 定义为一个映射，它将纯态映射到该算法下的输出分布。这里， $\Delta_{\mathcal{Y}}$ 是 Y 上的概率单纯形。等价地，

$$\forall |\phi\rangle \in \mathcal{S}(\mathbb{C}^d), \forall y \in \mathcal{Y} : g_{\mathcal{A}}\left(|\phi\rangle\right)_y \coloneqq \mathbb{P}\left[\mathcal{A}^{|\phi\rangle} = y\right].$$

引理 6.3. 设 $d \in \mathbb{N}$。对于任何输入为 d 维纯态的算法 A， $g_{\mathcal{A}}$ 是一个连续映射。

证明。 设 $\mathcal{Y}$ 为算法 $\mathcal{A}$ 的输出空间，其中 $s = |\mathcal{Y}|$，且 $\mathcal{A}$ 的查询复杂度为$t > 0$。$\mathcal{A}$ 由一个 s 结果 POVM 描述，其输入为量子态 $|\phi\rangle\langle\phi|$ 的 t 个副本。该 POVM 表示为 s 个半正定矩阵 $\{M_1, \ldots, M_s\}$，满足 $\sum_{j=1}^{s} M_j = I$。 $g_{\mathcal{A}}$ 的输出如下:

$$\forall y \in \mathcal{Y} : g_{\mathcal{A}}\left(|\phi\rangle\right)_y \coloneqq \mathbb{P}[\mathcal{A}^{|\phi\rangle} = y] = \mathrm{Tr}\left(M_y \, |\phi\rangle \, \langle\phi|^{\otimes t}\right).$$

映射 $|\phi\rangle \mapsto |\phi\rangle\langle\phi|^{\otimes t}$ 关于 $|\phi\rangle$ 的分量是多项式，因此连续；与固定矩阵相乘以及求迹也都是连续的。这意味着对于每个 $y \in \mathcal{Y}$，映射 $|\phi\rangle \mapsto g_{\mathcal{A}}(|\phi\rangle)_y$ 必定连续。因此， $g_{\mathcal{A}}$ 是连续的。

□

推论 6.4. 设 s、$d \in \mathbb{N}$。假设 A 是一个伪确定性算法，其输入是集合 $S \subseteq S(\mathbb{C}^d)$ 中的一个元素，其输出是 $[s]$ 中的一个元素。设 $f_{\mathcal{A}}$： $S \to [s]$ 为根据 A 将输入状态映射到其伪确定性解的函数（由伪确定性的定义，该解存在且唯一）。则可能的输出的个数 $|\mathrm{Im}(f_{\mathcal{A}})|$ 至多为 S 的连通分支个数。

证明。 只需证明：对于 S 的任意连通分支，当输入限制在该分支内时，伪确定性解的个数为 1。因此，不失一般性，我们假设 S 是连通的。

由于伪确定性函数任一给定输出的概率要么小于$1/3$，要么大于 $2/3$，因此 $\forall j \in [s]$: $g_{\mathcal{A}}(\cdot)_j$ 将连通空间 S 映射到$[0, 1/3] \cup [2/3, 1]$ 的一个子集。由 引理 6.3，该函数是连续的，因此 $\mathrm{Im}(g_{\mathcal{A}}(\cdot)_j)$ 是一个连通空间。

由于 $[0, 1/3]$ 和 $[2/3, 1]$ 是 $[0, 1/3] \cup [2/3, 1]$的仅有的连通子集，对于每个 $j \in [s]$，要么 $g_{\mathcal{A}}(\cdot)_j$ 将 S 中的所有元素映射到 $[0, 1/3]$ （此时 j 永远不会是伪确定性解），要么将 S 中的所有元素映射到 $[2/3, 1]$ （此时 j 始终是伪确定性输出）。由于伪确定性要求$\mathcal{A}$ 以至少 $2/3$的概率输出唯一解，因此在整个输入集合 S上， $j \in [s]$ 中恰有一个值是伪确定性解。

□

这意味着，任何定义域为固定维度的全部量子态集合的伪确定性算法，都只能输出一个常数值。更一般地，根据同样的拓扑论证，对于量子态、酉算子、量子信道或经典分布，如果其定义域是这类对象的全集，就不存在非平凡的伪确定性算法。

这排除了连通域上的非平凡算法，表明非连通性是非平凡性的必要条件。为说明这一点，我们现在引入 Find1 问题的一个量子类比——均匀支持查找，其输入域是非连通的。

定义 6.5 (均匀支持查找). 输入为 $|x\rangle \in S(\mathbb{C}^d)$，即一个被承诺为某些基态子集上的均匀叠加的量子态，任务是输出一个下标 $a \in [d]$，使得 $\langle a|x\rangle \neq 0$。

等价地，每个输入 $|x\rangle$ 都具有 $|x\rangle = \frac{1}{\sqrt{|J|}} \sum_{j\in J} |j\rangle$ 的形式，其中 $J \subseteq [d]$，而输出为某个 $j_0 \in J$。

注意，这些叠加态构成了$\mathcal{S}(\mathbb{C}^d)$ 的一个离散、因而不连通的子集。

定理 6.6。 均匀支持查找 的查询复杂度为 $\Theta(d)$.

证明。 我们首先证明上界。这是因为，当在计算基下对定义在集合 $J \subseteq [d]$ 上的状态进行测量时，以概率 $1/|J| \geq 1/d$ 得到支撑集中的最小元素。因此，可以在计算基下测量该状态的 $t = cd$ 个副本，然后输出这些测量结果中的最小索引。测得最小索引的概率由下式给出，其中 $c \geq$ln(3)。

$$1 - (1 - 1/|J|)^t \geq 1 - (1 - 1/d)^{cd} \geq 1 - e^{-c} \geq 2/3$$

为了证明下界，我们考虑一个伪确定性算法$\mathcal{A}$，并注意到，算法区分两个状态的概率至多为它们的迹距离。考虑量子态 $|y\rangle$，其支撑集大小为 $d-1$，仅缺少基元素 k。假设$\mathcal{A}$ 在 $|y\rangle$ 上的伪确定性输出为 $j \neq k$。该状态可表示为

$$|y\rangle = \sum_{\ell\in[d]\setminus\{k\}} \frac{1}{\sqrt{d-1}} |\ell\rangle .$$

现在考虑状态

$$|z\rangle = \sum_{\ell\in[d]\setminus\{j\}} \frac{1}{\sqrt{d-1}} |\ell\rangle ,$$

其支撑集大小为 $d-1$，仅缺少基元素 j。$\mathcal{A}$ 在$|z\rangle$ 上的伪确定性输出不能是 j。 t份 $|y\rangle$与 $|z\rangle$之间的迹距离为:

$$\begin{aligned}
\frac{1}{2}\| |y\rangle\langle y|^{\otimes t} - |z\rangle\langle z|^{\otimes t} \|_1 &= \sqrt{1 - |\langle y|z\rangle|^{2t}} \\
&= \sqrt{1 - \left(1 - \frac{1}{d-1}\right)^{2t}} \\
&\leq \sqrt{1 - \left(1 - \frac{2t}{d-1}\right)} \\
&= \sqrt{\frac{2t}{d-1}}
\end{aligned}$$

这里，第三行由伯努利不等式得出。要使迹距离为 Ω(1)，从而能够区分这两种情况，我们必须有 $t = \Omega(d)$。 □

致谢

感谢 Rahul Santhanam、Igor Oliveira 和 Scott Aaronson 就伪确定性问题进行的有益讨论。

参考文献

[Aar10] Scott Aaronson。BQP与多项式层次。载于 Leonard J. Schulman（编），《第42届ACM计算理论研讨会论文集》，STOC 2010，美国马萨诸塞州剑桥，2010年6月5日至8日，第141–150页。ACM，2010。 doi:10.1145/1806689.1806711。[ABI+13] Andris Ambainis、Kaspars Balodis、Janis Iraids、Raitis Ozols 和 Juris Smotrovs。图碰撞的参数化量子查询复杂度。CoRR，abs/1305.1021，2013。网址： http://arxiv.org/abs/1305.1021, arXiv:1305.1021。[ABK+21] Scott Aaronson、Shalev Ben-David、Robin Kothari、Shravas Rao 和 Avishay Tal。次数与近似次数，以及Huang灵敏度定理的量子推论。载于 Samir Khuller 和 Virginia Vassilevska Williams（编），《STOC '21：第53届ACM SIGACT计算理论研讨会》，意大利虚拟活动，2021年6月21日至25日，第1330–1342页。ACM，2021。 doi:10.1145/3406325.3451047。[AGJK20] Andris Ambainis、Andr´as Gily´en、Stacey Jeffery 和 Martins Kokainis。量子游走在寻找标记顶点方面的二次加速。载于 Konstantin Makarychev、Yury Makarychev、Madhur Tulsiani、Gautam Kamath 和 Julia Chuzhoy（编），《第52届ACM SIGACT 计算理论研讨会论文集》，STOC 2020，美国伊利诺伊州芝加哥，2020年6月22日至26日，第412–424页。ACM，2020。 doi:10.1145/3357713.3384252。[AH23] Scott Aaronson 和 Shih-Han Hung。通过量子优越性获得可认证随机性。载于 Barna Saha 和 Rocco A. Servedio（编），《第55届ACM计算理论研讨会论文集》，STOC 2023，美国佛罗里达州奥兰多，2023年6月20日至23日，第933–944页。ACM，2023。 doi:10.1145/3564246.3585145。[BBC+01] Robert Beals、Harry Buhrman、Richard Cleve、Michele Mosca 和 Ronald de Wolf。基于多项式的量子下界。ACM学报，48(4):778–797，2001。 doi:10.1145/502090.502097。[BBF+21] Roozbeh Bassirian、Adam Bouland、Bill Fefferman、Sam Gunn 和 Avishay Tal。关于通过傅里叶采样或随机电路采样获得可认证随机性。arXiv预印本 arXiv:2111.14846，2021。[Bel12] Aleksandrs Belovs。用于k-互异性的基于学习图的量子算法。载于《第53届IEEE计算机科学基础研讨会》，FOCS 2012，美国新泽西州新不伦瑞克，2012年10月20日至23日，第207–216页。IEEE计算机学会，2012。 doi:10.1109/FOCS.2012.18。[BKKS23] Vladimir Braverman、Robert Krauthgamer、Aditya Krishnan 和 Shay Sapir。数据流中伪确定性计数的下界。载于 Kousha Etessami、Uriel Feige 和 Gabriele Puppis（编），《第50届自动机、语言与编程国际研讨会》，ICALP 2023，2023年7月10日至14日，德国帕德博恩，LIPIcs第261卷，第30:1–30:14页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2023。网址： https://doi.org/10.4230/LIPIcs.ICALP.2023.30, doi:10.4230/LIPICS.ICALP.2023.30。

[CDM23] Arkadev Chattopadhyay、Yogesh Dahiya 和 Meena Mahajan。搜索问题的查询复杂度。《电子计算复杂性讨论会》，TR23-039，2023年。网址：https://eccc.weizmann.ac.il/report/2023/039，arXiv:TR23-039。[CE05] Andrew M. Childs 和 Jason M. Eisenberg。子集查找的量子算法。《量子信息与计算》，5(7):593–604，2005年。doi:10.26421/QIC5.7-7。[CLO+23] Lijie Chen、Zhenjian Lu、Igor C. Oliveira、Hanlin Ren 和 Rahul Santhanam。素数的多项式时间伪确定性构造。载于：第64届IEEE计算机科学基础年会，FOCS 2023，美国加利福尼亚州圣克鲁斯，2023年11月6日至9日，第1261–1270页。IEEE，2023年。doi:10.1109/FOCS57990.2023.00074。[DPV21] Peter Dixon、Aduri Pavan 和 N. V. Vinodchandran。承诺问题与伪确定性相遇。CoRR，abs/2103.08589，2021年。网址：https://arxiv.org/abs/2103.08589，arXiv:2103.08589。[DPWV22] Peter Dixon、Aduri Pavan、Jason Vander Woude 和 N. V. Vinodchandran。伪确定性：承诺与下界。载于 Stefano Leonardi 和 Anupam Gupta（编），STOC '22：第54届ACM SIGACT计算理论研讨会，意大利罗马，2022年6月20日至24日，第1552–1565页。ACM，2022年。doi:10.1145/3519935.3520043。[FGGS98] Edward Farhi、Jeffrey Goldstone、Sam Gutmann 和 Michael Sipser。量子计算确定奇偶性的速度限制。《物理评论快报》，81(24):5442，1998年。[Gal14] François Le Gall。通过组合论证改进三角形查找的量子算法。载于：第55届IEEE计算机科学基础年会，FOCS 2014，美国宾夕法尼亚州费城，2014年10月18日至21日，第216–225页。IEEE计算机学会，2014年。doi:10.1109/FOCS.2014.31。[GG11] Eran Gat 和 Shafi Goldwasser。具有唯一答案的概率搜索算法及其密码学应用。《电子计算复杂性讨论会》，TR11-136，2011年。网址：https://eccc.weizmann.ac.il/report/2011/136，arXiv:TR11-136。[GGH18] Shafi Goldwasser、Ofer Grossman 和 Dhiraj Holden。伪确定性证明。载于 Anna R. Karlin（编），第9届理论计算机科学创新会议，ITCS 2018，2018年1月11日至14日，美国马萨诸塞州剑桥，LIPIcs第94卷，第17:1–17:18页。Schloss Dagstuhl - 莱布尼茨信息学中心，2018年。网址：https://doi.org/10.4230/LIPIcs.ITCS.2018.17，doi:10.4230/LIPICS.ITCS.2018.17。[GGH19] Michel X. Goemans、Shafi Goldwasser 和 Dhiraj Holden。双重高效的伪确定性证明。CoRR，abs/1910.00994，2019年。网址：http://arxiv.org/abs/1910.00994，arXiv:1910.00994。[GGMW20] Shafi Goldwasser、Ofer Grossman、Sidhanth Mohanty 和 David P. Woodruff。伪确定性数据流。载于 Thomas Vidick（编），第11届理论计算机科学创新会议，ITCS 2020，2020年1月12日至14日，美国华盛顿州西雅图，LIPIcs第151卷，第79:1–79:25页。Schloss Dagstuhl - 莱布尼茨信息学中心，2020年。网址：https://doi.org/10.4230/LIPIcs.ITCS.2020.79，doi:10.4230/LIPICS.ITCS.2020.79。

[GGR13] Oded Goldreich、Shafi Goldwasser 和 Dana Ron。论伪确定性算法的可能性与局限性。载于 Robert D. Kleinberg（编），理论计算机科学创新，ITCS '13，美国加利福尼亚州伯克利，2013年1月9日至12日，第127–138页。ACM，2013年。 doi:10.1145/2422436.2422453。[GGS23] Ofer Grossman、Meghal Gupta 和 Mark Sellke。伪确定性近似计数的紧空间下界。载于：第64届IEEE计算机科学基础年会，FOCS 2023，美国加利福尼亚州圣克鲁斯，2023年11月6日至9日，第1496–1504页。IEEE，2023年。 doi:10.1109/FOCS57990.2023.00091。[GIPS21] Shafi Goldwasser、Russell Impagliazzo、Toniann Pitassi 和 Rahul Santhanam。NP搜索问题的伪确定性查询复杂度。载于 Valentine Kabanets（编），第36届计算复杂性会议，CCC 2021，2021年7月20日至23日，加拿大安大略省多伦多（线上会议），LIPIcs第200卷，第36:1–36:22页。Schloss Dagstuhl - 莱布尼茨信息学中心，2021年。 doi:10.4230/LIPIcs.CCC.2021.36。[NC16] Michael A. Nielsen 和 Isaac L. Chuang。《量子计算与量子信息》（十周年纪念版）。剑桥大学出版社，2016年。网址：https://www.cambridge.org/de/academic/subjects/physics/quantum-physics-quantum-information-and-quantum-computation/quantum-computation-and-quantum-information-10th-anniversary-edition?format=HB。[Sim97] Daniel R. Simon。论量子计算的能力。《SIAM计算学报》，26(5):1474–1483，1997年。 doi:10.1137/S0097539796298637。[Sze04] Mario Szegedy。基于马尔可夫链的算法的量子加速。载于：第45届计算机科学基础研讨会（FOCS 2004），2004年10月17日至19日，意大利罗马，论文集，第32–41页。IEEE计算机学会，2004年。 doi:10.1109/FOCS.2004.53。[YZ24] Takashi Yamakawa 和 Mark Zhandry。无需结构的可验证量子优势。《ACM学报》，71(3):20，2024年。 doi:10.1145/3658665。

定理 1.7 的证明

定理 1.7。 当且仅当 R 可 P-归约到某个有界错误量子多项式时间判定问题时，搜索问题 R 才存在伪确定性量子多项式时间算法。

证明。 对于“若”方向，我们假设这样的 P-归约存在。给定搜索问题 R的一个输入，我们将该归约用作算法，并对其输出运行有界错误量子多项式时间算法。该解是伪确定性的，因为对于 $R : X$的单个输入，该归约总会归约到相同的有界错误量子多项式时间判定问题实例，因为此类归约都是确定性的；设其将输入归约为有界错误量子多项式时间判定问题的一系列输入 $(Y_j)_j$。由于该有界错误量子多项式时间问题是一个判定问题，对输入 $(Y_j)_j$ 的解在对该算法进行多次重复运行时R都相同。

对于另一个方向，假设算法$\mathcal{A}$ 是针对该搜索问题的伪确定性量子算法。我们按如下方式定义集合 R' ，

$$(x, i, b) \in R' \iff \mathbb{P}[\mathcal{A}(x)_i = b] > \frac{2}{3}.$$

根据定义，集合 R' 属于有界错误量子多项式时间，因此，求解 R 可 P-归约到判定 R'。 □

B 定理定理 1.5

定理 1.5。 对于任意随机化查询复杂度为$\mathsf{R}(R)$ 、验证复杂度为$\mathsf{V}(R)$的搜索问题 R ，有 $\mathsf{psQ}(R) = O((\mathsf{R}(R) + \mathsf{V}(R)) \cdot \sqrt{N})$。

证明。 我们构造一个从 R 到 Find1 的归约。令$\mathcal{V}$ 为一个经典确定性算法，它以查询复杂度 $\mathsf{V}(R)$ 验证 R 的任意解；令 $\mathcal{R}$ 为一个经典随机算法，它以查询复杂度 $\mathsf{R}(R)$ 求解 R 。

不失一般性，$\mathcal{R}$ 是带重数的确定性算法上的均匀分布，其中$\mathcal{R}$ 支撑集中的每个确定性算法最多进行 $\mathsf{R}(R)$ 次查询。此外，对于任意输入X，从$\mathcal{R}$中随机抽取的算法在输入 X 上成功的概率至少为 $2/3$。

如果我们从$\mathcal{R}$的支撑集中随机抽取 $100N$ 个确定性算法，就得到一个新的随机算法$\mathcal{R}'$。根据 Chernoff 界，对于任意给定的 X，在$\mathcal{R}'$ 中的算法至少有 0.49 的比例失败的概率至多为 $2e^{-N}$。因此，对所有可能的输入 $X \in \{0,1\}^N$应用并集界后，随机选取的$\mathcal{R}'$ 也是 R 的有效随机算法的概率为 $1 - o(1)$。此外，$\mathcal{R}'$ 的支撑集大小为 $100N$。

我们现在通过将其归约为输入字符串$Z \in \{0,1\}^{100N}$上的一个 Find1 实例，来求解输入为 $X \in \{0,1\}^N$ 的 R 。具体而言，对任意 $i \in [100N]$，若 $\mathcal{R}'$ 的支撑集中第 i 个确定性算法能为 X 产生正确解，则 Z_i 为 1。注意， Z_i 可通过 $(\mathsf{R}(R) + \mathsf{V}(R))$ 次对字符串 X 的查询来计算。此外，Find1 实例 Z 的任一解都会导出 R 在实例 X 上的某个确定解。

最后，鉴于事实 $\mathsf{psQ}(\textsc{Find1}) = \Theta(\sqrt{N})$ [GIPS21], 我们得到一个针对 R 的伪确定性量子算法，其具有 $O((\mathsf{R}(R) + \mathsf{V}(R)) \cdot \sqrt{N})$ 次查询。

□

[6]P-归约是指 到一个确定性多项式时间图灵归 约。