/burl@stx null def /BU.S /burl@stx null def def /BU.SS currentpoint /burl@lly exch def /burl@llx exch def burl@s

量子计算的优势与局限*

查尔斯 · 本内特（CHARLES H. BENNETT）†，伊桑 · 伯恩斯坦（ETHAN BERNSTEIN）‡，吉尔 · 布拉萨（GILLES BRASSARD）§，AND 乌梅什 · 瓦齐拉尼（UMESH VAZIRANI）¶

摘要. 近年来，量子计算受到了广泛关注。一系列研究成果 [4, 15, 16] 表明，量子计算机在某些问题上比经典概率计算机更强大。继 Shor 的研究指出，整数分解与离散对数提取可在量子多项式时间内求解之后，自然而然地引出一个问题：**是否所有的 NP 问题都可以在量子多项式时间内高效求解？**

我们证明：相对于从所有可能性中均匀随机选取的预言机，必然（以概率 1）存在一个预言机，使得 **NP** 类问题无法在时间 $o(2^{n/2})$ 内由量子图灵机解决。此外，我们还证明：对于均匀随机选取的置换预言机，必然（以概率 1）有 **NP** ∩ **co-NP** 类问题无法在时间 $o(2^{n/3})$ 内被量子图灵机解决。前一个下界是紧的，因为 Grover 的最新工作 [13] 展示了如何在时间 $O(2^{n/2})$ 内，利用任意预言机接受 **NP** 类语言。

Key words. 量子图灵机，量子预言机图灵机，量子多项式复杂度

MSC codes. 68Q05, 68Q15, 03D10, 03D15

1. 引言. 量子计算复杂性是一个令人振奋的新领域，它触及理论计算机科学和量子物理学的基础。20 世纪八十年代初，费曼 [12] 指出在经典计算机上对量子力学进行直接模拟时，其模拟开销在系统规模和模拟时长上均呈指数增长；由此他提出了两个核心问题：这种指数开销是否不可避免？是否有可能设计出通用量子计算机？Deutsch[9] 提出了量子图灵机（QTM）的通用模型。Bernstein 和 Vazirani 证明了存在一种高效的通用 QTM[4]；随后姚期智 [17] 进一步证明了：由 Deutsch[11] 引入的量子电路模型与量子图灵机在相差多项式时间下等价。

量子图灵机的计算能力已被多位研究者深入探索。Deutsch 与 Jozsa [10] 的早期工作展示了如何利用 QTM 的量子力学特性解决某些问题；随后 Berthiaume 和 Brassard 的研究 [5, 6] 证明，存在某些预言机，使得 QTM 能在多项式时间内以确定性接受一些语言，而若经典概率图灵机要以**确定性**输出正确答案，则在某些输入上必需指数时间。另一方面，这些问题相对于相同的预言机属于 **BPP**[1]，因而在经典意义下仍可高效求解。量子计算的 **BPP** 类比是 **BQP**[5]。Bernstein 和 Vazirani [4] 证明了 **BPP** ⊆ **BQP** ⊆ **PSPACE**，这表明，若不解决 **P** $\stackrel{?}{=}$ **PSPACE**

*编辑部收到日期：1996 年 3 月 21 日；修订后接受日期：1996 年 12 月 2 日。

†IBM T. J. Watson 研究中心，美国纽约州约克镇高地 (bennetc@watson.ibm.com)。

‡微软公司，美国华盛顿州雷德蒙（ethanb@microsoft.com）。本作者的研究受美国国家科学基金会（NSF）资助，资助号：CCR-9310214。

§蒙特利尔大学信息与运筹学系，加拿大魁北克省蒙特利尔市（brassard@iro.umontreal.ca）。本作者的研究部分受加拿大自然科学与工程研究委员会（NSERC）和魁北克省 FCAR 项目资助。

¶加州大学伯克利分校计算机科学系，美国加利福尼亚州伯克利市（vazirani@cs.berkeley.edu）。本作者的研究受 NSF 资助，资助号：CCR-9310214。

[1]**BPP** 是指一类判定问题（语言），可由概率图灵机在多项式时间内解决，并且对所有输入，其错误概率均有界于 1/3. 通过标准的放大技术——重复运行算法 k 次并对结果进行多数投票——可以将错误概率指数级地降低。

等重大未决问题，就无法给出 **BQP** $\neq$ **BPP** 的决定性证明。他们还给出了首个证据：存在某个预言机，使得受限于运行时间为 $n^{o(\log n)}$ 的经典概率机器无法以小错误率解决 **BQP** 中的问题。由于 **BPP** 被视为所有 "高效可计算" 语言的类，这一结果从模型无关的角度提供了量子计算机相对于经典计算机更强大内在能力的证据。

Simon 强化了这一证据，他构造了一个预言机，使得即便允许经典概率机器运行 $2^{n/2}$ 步，也无法模拟 **BQP**[2]。此外，Simon 的论文还引入了一项关键新技术，该技术成为 Shor 提出多项式时间量子算法的核心组成部分。Shor 给出了整数分解和离散对数问题的多项式时间量子算法。这两个问题已被广泛研究，其 presumed intractability 构成了现代密码学的基石。鉴于上述成果，自然而然地提出了一个关键问题：

NP $\subseteq$ **BQP**？ 即量子计算机能否在多项式时间内解决**NP**-完全问题？[3]

在本文中，我们通过证明以下结果来回答上述问题：相对于均匀随机选取的预言机 [3]，以概率 1，**NP** 中的问题无法被量子图灵机在时间 $o(2^{n/2})$ 内解决。我们还证明：相对于以均匀随机方式选取的置换预言机，以概率 1，**NP** $\cap$ **co-NP** 中的问题无法被量子图灵机在时间 $o(2^{n/3})$ 内解决。前一界限是紧的，因为 Grover [13] 的最新工作展示了如何在时间 $O(2^{n/2})$ 内在量子计算机上针对任意预言机接受 **NP**。文献 [7] 给出了 Grover 算法的详细分析。

这些预言机结果的意义何在？我们需要强调：它们并不排除 **NP** $\subseteq$ **BQP** 的可能性。这些结果确立了：不存在**仅基于黑盒 (black-box) 的方法**，能够利用量子图灵机的某些独特量子力学特性来高效解决 NP 完全问题。Grover 的工作则清楚地表明，这种黑盒方法最多只能将经典所需时间加速至其平方根量级。

一种理解预言机的方式是将其视为一种特殊的子程序调用，其调用仅需耗费一个时间单位。在量子图灵机的语境中，子程序调用提出了一个经典计算中没有对应的问题：子程序在返回其计算结果时不得在任何多余的比特中留下残留信息，否则携带不同残余信息的计算路径将无法相互干涉。对于确定性子程序，这一要求易于满足，因为任何经典确定性计算都可以以可逆方式进行，从而仅保留输入和答案。然而，对于更一般的情况——即是否可以将一个 **BQP** 机器用作子程序——这一点仍有待解答。

---

[2] **BQP** 是指一类判定问题（语言），可由量子图灵机在多项式时间内解决，并且对所有输入，其错误概率均有界于 1/3 ——详见文献 [4] 以获取形式定义。我们在第 4 节证明，正如 BPP 的情况一样，通过相应的放大技术，BQP 机器的错误概率也可以被指数级地缩小。

[3] 实际上，甚至不能确定是否 **BQP** $\subseteq$ $\mathbf{BPP}^{\mathbf{NP}}$；也就是说，我们尚不清楚非确定性加上随机性是否足以模拟量子图灵机。实际上，Bernstein 和 Vazirani 的结果 [4] 比上述表述更强。他们实际上证明了，相对于某个 oracle，递归傅里叶采样问题可以在 **BQP** 中解决，但甚至不能被 Arthur-Merlin 游戏 [1] 在时间界 $n^{o(\log n)}$ 内解决（这为 "在概率计算上叠加非确定性是否有用" 提供了负面证据）。他们还猜想，递归傅里叶采样甚至无法在未相对化的多项式时间层次结构中解决。

本论文的最终结果展示了如何将任意 **BQP** 机器改造为一个*整洁* **BQP** 机器，其最终叠加态几乎完全由仅包含输入和单比特答案的工作带格局（tape configuration）组成。由于这种整洁 **BQP** 机器可以安全地用作子程序，我们由此证明了 $\mathbf{BQP}^{\mathbf{BQP}} = \mathbf{BQP}$. 该结果也为我们随后给出的预言机量子机定义提供了正当性。

2. 预言机量子图灵机. 在本节及下一节中，我们在不失一般性的前提下假设对每个磁带，图灵机的字母表为 $\{0,1,\#\}$，其中 "#" 表示空白符号。最初，除输入带之外，所有磁带均为空白，输入带上仅有被空白符号包围的实际输入。我们用 Σ 表示集合 $\{0,1\}$。

在经典环境中，预言机常被非正式地描述为一种以单位时间代价计算某布尔函数 $A\colon \Sigma^* \to \Sigma$ 的设备。它允许我们提出诸如 "如果 A 可由图灵机高效计算，那么还有哪些函数（或语言）也能被图灵机高效计算?" 之类的问题。在量子环境中，可以提出等价的问题，只要我们为预言机 QTM 给出恰当的定义，并证明有界误差的 QTM 可以复合（第 4 节将对此予以说明）。

一个预言机 QTM 拥有一条特殊的 *查询磁带*，除了一段连续的非空白单元格，其他所有单元格最初均为空白。在规范化（well-formed）[4]的预言机 QTM 中，图灵机规则允许这一非空白区间增长或收缩，但不允许其被分割[5]。预言机 QTM 有两个区分的内部状态：*前查询状态* q_q 与*后查询状态* q_a。当机器进入前查询状态时即执行一次查询。如果查询串为空，则不作任何操作，机器直接进入后查询状态且格局不变；如果查询串非空，则可写为 $x \circ b$，其中 $x \in \Sigma^*$，$b \in \Sigma$，符号 "$\circ$" 表示串拼接。此时，对预言机 A 的调用使得状态控制器进入后查询状态，同时查询带上的内容由 $|x \circ b\rangle$ 变为 $|x \circ \big(b \oplus A(x)\big)\rangle$，其中 "$\oplus$" 表示按位异或（模 2 加法）。查询过程中，除查询磁带和状态控制器以外，预言机 QTM 的其他部分均保持不变。

若目标位 $|b\rangle$ 初始为 $|0\rangle$，则其最终态为 $|A(x)\rangle$，正如经典预言机机；反之若目标位已处于 $|A(x)\rangle$，则调用预言机会将其复位为 $|0\rangle$。这一 "逆计算"（*uncompute*）能力对于保证不同计算路径的相干干涉至关重要。利用上述性质，可以看出：只要限制机器在进入前查询状态与离开后查询状态时的演化为酉演化，预言机 QTM 的整体演化即为酉操作。

量子计算机的威力源于其能够执行计算路径的相干叠加。同样地，量子预言机的强大能力也来源于其对叠加态查询的支持。例如，当查询磁带处于状态 $|\psi \circ 0\rangle = \sum_x \alpha_x |x \circ 0\rangle$，其中 α_x 为复系数，对应于目标位保持 $|0\rangle$ 的任意查询叠加时，可调用预言机 A。在此情况下，查询之后，查询串将处于纠缠态 $\sum_x \alpha_x |x \circ A(x)\rangle$. 将目标位 b 置于叠加态也是十分有用的。例如，在 Grover 算法中使用的条件相

[4]指图灵机的迁移函数满足酉性（即线性、保范及正交条件），保证整体演化为酉变换

[5]即始终保持为一个连贯的区块，而非若干不相邻的区块。这一限制可以在不损失一般性的情况下做出，而且可以通过允许只有那些在写入查询磁带之前确保不违反规则的机器才能使用。

位翻转操作，可通过将目标位 b 置于非经典叠加态 $\beta = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ 后，执行查询来实现。可以验证：当查询磁带处于状态 $x \circ \beta$ 时，若 $A(x) = 0$，预言机调用将保持包括查询磁带在内的整个机器态不变；若 $A(x) = 1$，则保持态不变但引入相位因子 -1。

通常，可将布尔预言机视为对 Σ^* 上输入输出长度保持一致函数。这可通过将预言机对二元组 (x, i) 的输出作为函数值的第 i 位来轻松实现。二元组 (x, i) 可通过任意合适的函数编码为二进制串。置换预言机是指这样的输入输出长度保持函数：对于每个 $n \geq 0$ 都在 Σ^n 上作用为置换的预言机。从此，在不引起歧义时，我们将用 $A(x)$ 表示与预言机 A 相关联的长度保持函数，而非产生它的布尔函数。

令 $\mathbf{BQTime}(T(n))^A$ 表示由某个预言机 QTM M^A 以至少 2/3 的概率接受且运行时间不超过 $T(n)$ 的语言集合。该运行时间上界适用于每个具体输入，而不仅限于平均情况。注意，M^A 是否为 **BQP** 机器可能依赖所使用的预言机 A——因此 M^A 可能是 **BQP** 机器，而 M^B 则未必。

注：上述对任意布尔函数的量子预言机定义对于本文目标已足够，但量子计算机执行一般酉变换的能力提示了更广义的定义，在其他上下文中也可能有用。例如，已有研究在计算学习理论 [8] 和针对经典查询的信息隐藏 [14] 中考虑过执行更一般非布尔值酉变换的预言机。

最广义地，一个量子预言机可以定义为一种设备，当调用时，会对查询带的当前内容 $|z\rangle$ 应用一个固定的酉变换 U，将其替换为 $U|z\rangle$。这样的预言机 U 必须定义在一个可数无限维的希尔伯特空间上，例如由二进制基向量

$$|\epsilon\rangle, |0\rangle, |1\rangle, |00\rangle, |01\rangle, |10\rangle, |11\rangle, |000\rangle, \ldots$$

所张成，其中 ϵ 表示空串。显然，只要预言机图灵机规范（well-formed），使用此类一般的酉预言机依然会产生酉演化。自然地，这些预言机可以将输入映射为输出的叠加，反之亦然，且不必保持长度不变。然而，为了遵循“单个机器周期不应在磁带上产生无限变化”的原则，可能需要要求 $U|z\rangle$ 对除有限多个基向量之外的所有基向量具有零振幅。（甚至可以坚持要求上述限制的统一且可有效验证的版本。）对于 U 的另一个自然约束是要求其为对合变换（involution），即 $U^2 = I$，这样一次预言机调用的效果就可以通过对同一预言机的再次调用来撤销。这对于保证不同计算路径之间能够正确干涉可能至关重要。注意，本文所考虑的计算经典布尔函数的特殊酉变换情形，恰好就是一个对合变换。

3. 在量子图灵机上模拟非确定性的难度. 量子图灵机的计算能力源于其维护和操作指数级大叠加态的能力。人们很容易想尝试利用这种“指数并行性”来模拟非确定性。然而，量子力学的形式化理论对这种并行性的作用范围施加了固有

的约束[6]。本节将探讨其中的一些约束。

为了说明为什么量子干涉只能对 **NP** 问题实现二次加速而非指数加速，不妨考虑区分空预言机（$\forall_x\, A(x)=0$）与仅包含一个长度为 n 的随机未知串 y 的预言机（即 $A(y)=1$ 且 $\forall_{x\neq y}\, A(x)=0$）的问题。我们要求：在空预言机情况下，计算机绝不应回答“是”；在非空预言机情况下，希望最大化其回答“是”的“成功概率”。经典计算机的最优策略是随机查询若干不同的 n 位串：一次查询后的成功概率为 $1/2^n$，k 次查询后的成功概率为 $k/2^n$。那么，量子计算机如何在保持整体演化酉性、并且在非空预言机的计算中，对所有查询空位置的计算路径都与空预言机情况下完全相同的情况下取得更好表现呢？直接的量子模拟算法是：从 2^n 条计算路径的均等叠加态出发，在每条路径上查询一个不同的串，最后通过测量查询结果来判断是否发现了非空位置。这一策略的成功概率仍为 $1/2^n$，与经典计算机相同。然而，这并非利用量子并行性的最佳方式。我们的目标应该是最大化两者之间的态向量分离度：经过 k 次查询与空预言机交互后的态向量 $|\psi_k\rangle$ 与经过 k 次查询并在未知位置 y 存在非空预言机交互后的态向量 $|\psi_k(y)\rangle$。

从均匀叠加态

$$|\psi_0\rangle \;=\; \frac{1}{\sqrt{2^n}}\sum_x |x\rangle,$$

出发，可见在一次查询后，通过将态演化为

$$|\psi_1(y)\rangle \;=\; \frac{1}{\sqrt{2^n}}\sum_x (-1)^{\delta_{x,y}}|x\rangle \;=\; |\psi_0\rangle \;-\; \frac{2}{\sqrt{2^n}}\,|y\rangle,$$

能最大化两态的分离度。这相当于仅对非空位置的分量施加相位翻转。随后检测查询后态是否与 $|\psi_0\rangle$ 一致，可获得成功概率

$$1-\left|\langle\psi_0|\psi_1(y)\rangle\right|^2 \approx \frac{4}{2^n}.$$

约为经典值的四倍左右。因此，如果仅允许一次查询，量子并行性虽能带来适度改进，但仍极有可能失败，因为与非空预言机交互后的态向量与与空预言机交互后的态向量几乎相同。要在一次查询后产生显著差异，唯一办法是在查询前将初始叠加态的大量权重集中到 y 项上，但由于该位置未知，这无法实现。

在一次查询后达到最大分离度后，如何通过后续查询进一步扩大这种分离度？各种策略皆可设想，但一种被 Grover [13] 称为“关于平均值的翻转”的方法效果最佳：先执行一个与预言机无关的酉变换，将相位差转换为幅度差，使 y 项与其他项同号但幅度约增大三倍。随后交替进行与预言机的相位翻转和与预言机无关的相位–幅度转换，令 $|\psi_0\rangle$ 与 $|\psi_k(y)\rangle$ 之间的距离随 k 线性增长，当 $k<\sqrt{N}/2$

[6]在量子计算中的这种指数并行性，与经典概率计算所产生的覆盖指数大域的概率分布表面上类似；不同之处在于，经典概率计算的计算路径是通过一系列随机选择（每步一次）来决定的，而在量子力学中，多条计算路径可以相消干涉，因此必须在每一步跟踪整个叠加态以准确模拟系统。

时约为 $2k/\sqrt{2^n}$。这导致成功概率呈二次增长——对于小 k 约为 $4k^2/2^n$。定理 3.5 的证明表明，此方法在本质上是最优的：对于相对于随机预言机提出解答 NP 类型问题的尝试，任何量子算法相较于经典算法在成功概率上都无法超过此二次因子。

3.1. 量子搜索的下界. 有时我们通过计算目标与模拟叠加态之间的欧几里得距离[7] 来度量模拟的准确性。文献 [4] 中的以下定理表明，模拟的准确性至多比该欧几里得距离差 4 倍。

THEOREM 3.1. *若两个单位长度叠加态在欧几里得距离 ε 内，则观察这两个叠加态所得的分布的全变差距离[8] 最多为 4ε。*

DEFINITION 3.2. *令 $|\phi_i\rangle$ 为在输入 x 下，预言机 QTM M^A 于时间 i 的叠加态。记 $q_y\big(|\phi_i\rangle\big)$ 为 $|\phi_i\rangle$ 中对预言机在字符串 y 上发出查询的格局的幅度平方和，我们称其为态 $|\phi_i\rangle$ 的 y 项查询幅度。*

Remark 3.3 (译者注). 记在第 i 步使用预言机 A 时的全局叠加态为 $|\phi_i\rangle = \sum_C \alpha_C^{(i)} |C\rangle$, 定义3.2用

$$q_y\big(|\phi_i\rangle\big) \;=\; \sum_{\substack{\{C|\text{格局}C\text{中}\\ \text{查询带字符串为}y\}}} \big|\langle C|\phi_i\rangle\big|^2$$

来衡量算法在第 i 步对某个字符串 y 的 “关注度”。

THEOREM 3.4. *令 $|\phi_i\rangle$ 为在输入 x 下，预言机 QTM M^A 于时刻 i 的叠加态。取任意 $\varepsilon > 0$，令集合 $F \subseteq [0, T-1] \times \Sigma^*$ 包含一些 “时刻-查询串” 对，使得 $\sum_{(i,y)\in F} q_y\big(|\phi_i\rangle\big) \;\le\; \frac{\varepsilon^2}{T}$. 现在，假设将对每个查询 $(i,y) \in F$ 的回答修改为任意固定的 $a_{i,y}$ (这些回答无需与预言机一致)。令 $|\phi_i'\rangle$ 为上述修改后，在相同输入 x 与预言机情形下，机器 M 于时间 i 的叠加态。则*

$$\big\|\, |\phi_T\rangle - |\phi_T'\rangle \,\big\| \;\le\; \varepsilon.$$

Proof. 令 U 为 M^A 的酉时间演化算符。令 A_i 表示如下预言机：若 $(i,y) \in F$ 则 $A_i(y) = a_{i,y}$，否则 $A_i(y) = A(y)$。令 U_i 为 M^{A_i} 的酉时间演化算符。记 $|\phi_i\rangle$ 为输入 x 下，机器 M^A 于时间 i 的叠加态，并定义

$$|E_i\rangle \;=\; U_i\,|\phi_i\rangle \;-\; U\,|\phi_i\rangle$$

---

[7] 欧几里得距离 (Euclidean distance)：若 $|\phi\rangle = \sum_x \alpha_x|x\rangle$ 且 $|\psi\rangle = \sum_x \beta_x|x\rangle$，则定义为 $\big(\sum_x |\alpha_x - \beta_x|^2\big)^{1/2}$.

[8] 全变差距离 (total variation distance)：两个分布 D 与 D' 之间的全变差距离定义为 $\sum_x |D(x) - D'(x)|$.

为在第 i 步中由替换预言机引入的误差态。于是

$$\begin{aligned}|\phi_T\rangle = U\,|\phi_{T-1}\rangle &= U_T\,|\phi_{T-1}\rangle - |E_{T-1}\rangle \\ &= U_T\,U_{T-1}\,|\phi_{T-2}\rangle - U_T\,|E_{T-2}\rangle - |E_{T-1}\rangle \\ &\vdots \\ &= U_T\,U_{T-1}\cdots U_1\,|\phi_0\rangle \;-\; \sum_{i=0}^{T-1} U_{T-1}\cdots U_i\,|E_i\rangle.\end{aligned}$$

由于各 U_i 均为酉算符，

$$\big\|\,U_{T-1}\cdots U_i\,|E_i\rangle\big\| = \big\|\,|E_i\rangle\big\|.$$

而所有 $|E_i\rangle$ 的幅度平方和恰等于 $\sum_{(i,y)\in F} q_y(|\phi_i\rangle)$，因而至多为 ε^2/T。在最坏情况下，这些误差态可能构成相长干涉，但其和的幅度平方最多为它们各自幅度平方和的 T 倍，即 ε^2。因此

$$\big\|\,|\phi_T\rangle - |\phi'_T\rangle\big\| \;\le\; \varepsilon.$$

□

Remark 3.5 (译者注). 在量子查询模型里，算法每一步都可能把查询寄存器置于若干字符串的叠加; 对于某个具体字符串 y，在第 i 步上出现在叠加中的“概率权重”就是 $q_y\big(|\phi_i\rangle\big)$。把所有时间步 i 对同一 y 的 $q_y\big(|\phi_i\rangle\big)$ 相加，就得到算法一生中“关注” y 的总量。如果这个总量很小（集合 F 中的元素），直觉上说算法几乎没花注意力在 y 身上，因此它也就难以察觉你对 y 回答的篡改。

Corollary 3.6. *令 A 为字母表 Σ 上的任意预言机。对每个 $y\in\Sigma^*$，设 A_y 为任意满足 $\forall_{x\neq y}\,A_y(x)=A(x)$ 的预言机。记 $|\phi_i\rangle$ 为输入 x 下 M^A 于时间 i 的叠加态，$|\phi_i^{(y)}\rangle$ 为输入 x 下 M^{A_y} 于时间 i 的叠加态。则对任意 $\varepsilon>0$，存在集合 $S\subseteq\Sigma^*$，$\mathbf{card}(S)\le 2T^2/\varepsilon^2$，使得对所有 $y\notin S$ 都有*

$$\big\|\,|\phi_T\rangle - |\phi_T^{(y)}\rangle\big\| \;\le\; \varepsilon.$$

Proof. 由于每个 $|\phi_i\rangle$ 都为单位长度，且 $\sum_{i=0}^{T-1}\sum_y q_y(|\phi_i\rangle)\le T$，令

$$S=\Big\{\,y:\sum_{i=0}^{T-1} q_y(|\phi_i\rangle)\ge\frac{\varepsilon^2}{2T}\Big\}.$$

则显然 $\mathbf{card}(S)\le 2T^2/\varepsilon^2$，且对任意 $y\notin S$ 都有 $\sum_{i=0}^{T-1} q_y(|\phi_i\rangle)<\frac{\varepsilon^2}{2T}$。由定理 3.3 可得 $\big\|\,|\phi_T\rangle - |\phi_T^{(y)}\rangle\big\|\le\varepsilon$。 □

Remark 3.7 (译者注). 一个运行 T 步、错误容限 ϵ（随意篡改某些查询答案，但整台量子计算机最终“跑偏”的最大幅度，ϵ 越小相当于我们要求算法几乎“一毫不差”地重现原输出）的量子算法，真正“盯着看”的地址只有多项式级别 $\frac{T^2}{\epsilon^2}$

这么少（“真正有可能影响算法结果的查询字符串”集合的大小上界反比于 ϵ^2）；对于其他指数量级级的大多数地址，它几乎看不见，也就无法利用它们去做 NP-式的“猜测并验证”。T 越大，算法有更多时间分配注意力，可能关注的地址上限随 T^2 抬升。

证明数学细节：A 是论文中默认的“真实预言机”，可看作一个将二进制串映射到 $\{0,1\}$ 的布尔函数，A_y 是对 A 做了一次点修改 (single-bit perturbation) 的派生预言机：它在查询字符串 y 处的值被替换成一个（可由证明者任取的）固定比特 (例如取反)，其余输入上保持与 A 完全一致。通过比较使用 A 与使用 A_y 得到的量子态距离，可量化算法对字符串 y 的“敏感度”。记在第 i 步使用预言机 A 时的全局叠加态为 $|\phi_i\rangle = \sum_C \alpha_C^{(i)} \big|C\big\rangle$，使用 A_y 时的叠加态为 $|\phi_i^{(y)}\rangle = \sum_C \beta_C^{(i)} \big|C\big\rangle$. 仅当格局 C 包含查询 y 并处于后查询状态时，$\alpha_C^{(i)}$ 与 $\beta_C^{(i)}$ 才可能不同。

推论3.6把那些在 T 步运行中累计关注度至少为 $\varepsilon^2/(2T)$ 的所有字符串都收录在 S 中。由于每一步对所有字符串的查询关注度之和为 1，T 步总和不超过 T，故算关注度的贡献立刻给出 $|S| \times \frac{\varepsilon^2}{2T} \le T \implies |S| \le \frac{2T^2}{\varepsilon^2}$，即至多有 $2T^2/\varepsilon^2$ 个字符串可能属于 S。接着，对任意 $y \notin S$，我们把所有关于 y 的查询打包为 $F = \big\{(i,y) \mid 0 \le i < T\big\}$. 由于累积关注度 $\sum_{(i,y)\in F} q_y\big(|\phi_i\rangle\big) < \varepsilon^2/T$，它满足定理 3.4 的前提条件，因此无论如何篡改这些查询的预言机答案，算法最终态与原态之间的欧几里得距离都不会超过 ε。

最后值得一提的是，常数 2 并非神秘之数，作者只是想在证明的时候给不等式放缩留点余量，任何大于 1 的常数 c 都可替代，只需在定义 $S = \left\{ y : \sum_i q_y(|\phi_i\rangle) \ge \frac{\varepsilon^2}{cT} \right\}$ 时做相应更改，并将上界写为 $|S| \le cT^2/\varepsilon^2$。若想用 $c = 1$，也完全可行。

Remark 3.8 (译者注). 定理 3.4 告诉我们：如果一个量子算法在整个运行过程中“关注”某个候选输入 y 的总幅度非常小，那么就算你在所有涉及 y 的查询上把预言机的答案随意篡改，算法最终的量子态也只会发生最多 ϵ 的微小偏移；推论3.6 进一步说明：对于任何给定的预言机和运行时间 T，真正能显著影响算法输出的候选输入至多只有大约 $\frac{T^2}{\epsilon^2}$ 个，换句话说，大多数位置对算法来说几乎是“隐身”的。这就是 BBBV 这篇论文里著名的 hybrid argument 的核心结论，也是他们证明量子搜索至多得到平方级加速的关键工具。

THEOREM 3.9. 对于任何 $T(n) = o(2^{n/2})$，**相对于**随机预言机，以概率 1，**BQTime**$(T(n))$ 不包含 **NP**。

Proof. 回顾第 2 节：预言机可被视为一个长度保持函数，我们下面以 $A(x)$ 表示。令 $\mathcal{L}_A = \{\, y : \exists x\ A(x) = y\}$。显然 $\mathcal{L}_A \in \mathbf{NP}^A$。设 $T(n) = o(2^{n/2})$。我们将证明：对任何运行时间至多 $T(n)$ 的有界误差预言机 QTM M^A，以概率 1，M^A 不接受语言 $\mathcal{L}_A$。此处概率取自对（长度保持的）预言机 A 的选择。由于可数多个发生概率为 1 事件的交集仍以概率 1 发生，遂可断言：以概率 1，没有有界误

差预言机 QTM 能在时间 $T(n)$ 内接受 $\mathcal{L}_A$。

由于 $T(n)=o(2^{n/2})$，我们可以选取足够大的 n，使得 $T(n)\leq\frac{2^{n/2}}{20}$。我们将证明：对于任意固定长度不等于 n 的输入上的预言机回答方式，M 在输入 1^n 上给出错误答案的概率至少为 $1/8$。此处概率取自对 (接受输入长度为 n 的) 预言机的随机选择。

我们固定一个长度为 n 以外的输入字符串上的任意长度保持函数 f，其定义在字母表 Σ 上。令 $\mathcal{C}$ 表示所有在这些（长度不是 n 的）输入上与该函数 f 一致的预言机的集合。令 $\mathcal{A}$ 表示 $\mathcal{C}$ 中使得 1^n 没有原像的那些预言机（即 $1^n\notin\mathcal{L}_A$）。若对长度为 n 的输入，预言机回答在 Σ^n 上均匀随机地选取，那么预言机落入 $\mathcal{A}$ 的概率至少为 $1/4$。这是因为 1^n 没有原像的概率为 $\left(\frac{2^n-1}{2^n}\right)^{2^n}$，对充分大的 n 而言该值至少为 $1/4$。令 $\mathcal{B}$ 表示 $\mathcal{C}$ 中使得 1^n 有唯一原像的那些预言机。同样地，随机选择一个预言机落入 $\mathcal{B}$ 的概率为 $\left(\frac{2^n-1}{2^n}\right)^{2^n-1}$，这至少为 $1/e$。

给定一个属于 $\mathcal{A}$ 的预言机 A，我们可以将其在某一个输入（如 y）上的回答修改为 1^n，从而得到一个属于 $\mathcal{B}$ 的预言机 A_y。我们将证明，对于大多数 y，M^A 在输入 1^n 上的接受概率几乎等于 M^{A_y} 在输入 1^n 上的接受概率。另一方面，M^A 必须拒绝 1^n，而 M^{A_y} 必须接受 1^n，因此 M 不可能同时接受 $\mathcal{L}_A$ 和 $\mathcal{L}_{A_y}$。通过以下更细致地展开证明可以发现，当预言机在长度为 n 的字符串上是均匀随机函数、在其他所有输入上任意时，M 在输入 1^n 上失败的概率至少为 $1/8$：

令 A_y 为满足 $A_y(y)=1^n$ 且对所有 $z\neq y$ 有 $A_y(z)=A(z)$ 的预言机。由推论 3.6 可知，存在一个至多包含 $338T^2(n)$ 个字符串的集合 S，使得 M^{A_y} 在输入 1^n 上的第 i 步叠加态与 M^A 在输入 1^n 上的第 i 步叠加态之间的范数最大为 $\epsilon=1/13$。结合定理 3.1，我们可以推得：M^{A_y} 和 M^A 在输入 1^n 上的接受概率之差最多为 $4\epsilon=1/13\times4<1/3$。由于 M^{A_y} 应以至少 $2/3$ 的概率接受 1^n，而 M^A 应以至少 $2/3$ 的概率拒绝 1^n，因此我们可以得出结论：M 必然无法同时接受 $\mathcal{L}_A$ 和 $\mathcal{L}_{A_y}$。

因此，对于每一个使得 M 能正确判断 $1^n\in\mathcal{L}_A$ 的预言机 $A\in\mathcal{A}$，我们通过仅修改 A 在某一输入上的回答为 1^n，可以将其映射到至少 $(2^n-\mathbf{card}(S))\geq2^{n-1}$ 个不同的预言机 $A_f\in\mathcal{B}$，这些预言机上 M 无法正确判断 $1^n\in\mathcal{L}_{A_f}$。另一方面，任意给定的 $A_f\in\mathcal{B}$ 最多只能是 2^n-1 个 $A\in\mathcal{A}$ 的像，因为 A 在该位置原本可选择的候选回答有 2^n-1 个。因此，M 在 $\mathcal{B}$ 上失败的预言机数量至少是 M 在 $\mathcal{A}$ 上成功预言机数量的一半。记 a 为 M 在 $\mathcal{A}$ 上失败的预言机数量，则 M 至少在 $a+\frac{1}{2}(\mathbf{card}(\mathcal{A})-a)$ 个预言机上失败。因此，M 无法正确判断 $1^n\in\mathcal{L}_A$ 的概率至少为 $\frac{1}{2}\Pr[\mathcal{A}]\geq\frac{1}{8}$.

于是可知，对于均匀随机选择的预言机 A，M 判定 $1^n\in\mathcal{L}_A$ 的正确性概率为 0。 □

Remark 3.10 (译者注). 我们的目标是说明：若从所有长度保持预言机中均匀

随机选取 A，则任何运行时间 $T(n) = o(2^{n/2})$ 的有界误差量子预言机图灵机 M^A 都几乎必定无法判定由该预言机派生的语言 $\mathcal{L}_A = \{y : \exists x\, A(x) = y\}$，从而得到 $\mathbf{NP}^A \not\subseteq \mathbf{BQTime}(o(2^{n/2}))^A$ 以概率 1 成立。做法是先 “固定外壳”：把 A 在所有长度 $\neq n$ 的输入上的值冻结成任意长度保持函数，方便后续计数。设 $\mathcal{C}$ 为所有与该外壳一致的预言机集合；再对长度 n 区段的映射在 Σ^n 上均匀随机填充，由每个地址有 2^n-1 个值可选，可得 1^n 无前像的概率 $\left((2^n-1)/2^n\right)^{2^n} \geq 1/4$，记满足此性质的预言机集合为 $\mathcal{A}$；同理，1^n 有且仅有唯一前像的概率 $\left((2^n-1)/2^n\right)^{2^n-1} \geq 1/e$，对应集合记为 $\mathcal{B}$。显然 $\mathcal{A}$ 中的预言机使 $1^n \notin \mathcal{L}_A$（应答为 NO），而 $\mathcal{B}$ 中的预言机使 $1^n \in \mathcal{L}_A$（应答为 YES）。现在取任意 $A \in \mathcal{A}$ 并任选地址 y，把 $A(y)$ 改成 1^n 得到 $A_y \in \mathcal{B}$；对 “冷门” 地址——即不在推论 3.6 所界定的至多 $338T^2(n)$ 个 “热点” 中的 y——定理 3.4告诉我们，从 A 切换到 A_y 只会把 M 的最终量子态欧氏距离改变至多 $\varepsilon = 1/13$，再由定理 3.1 把态距乘以系数 4 得到两世界在输入 1^n 上的接受概率差 $< 4/13 < 1/3$；然而 BQP 定义要求 YES 实例接受率 $\geq 2/3$、NO 实例 $\leq 1/3$，二者须至少相差 $1/3$，故 M 必在 $\mathcal{A}$ 或 $\mathcal{B}$ 世界判错。由于可替换的冷门地址至少 $2^n - 338T^2(n) \geq 2^{n-1}$ 个，而任一固定 A_y 至多对应 $2^n - 1$ 个原始 A（地址 y 上选 $2^n - 1$ 个其他值），把所有成功 A 与其映射出的 $(A, y) \mapsto A_y$ 计为 “对象–盒子” 对应：对象总数 $\geq s \cdot 2^{n-1}$（s 个 A、每个 $\geq 2^{n-1}$ 个 y）；而每个盒子（某一 A_y）最多容纳 $2^n - 1$ 个对象。鸽巢原理得 $|\text{失败}\mathcal{B}\text{-预言机 s}| \geq \frac{s \cdot 2^{n-1}}{2^n-1} \geq \frac{s}{2}$. 即若 M 在 $\mathcal{A}$ 上成功的预言机数为 s，则它在 $\mathcal{B}$ 上失败的预言机数至少 $s/2$；结合 $\Pr[\mathcal{A}] \geq 1/4$ 得到 M 在长度 n 场景下出错概率 $\geq 1/8$。因为不同长度段的填充是独立的，这些 “单长出错” 事件在 $n = 1, 2, \ldots$ 上独立且概率和发散，第二 Borel–Cantelli 引理说明 M 以概率 1 会在无限多个 n 上把输入 1^n 判错；而判定语言必须在所有输入上正确，故 M 几乎必定不是 $\mathcal{L}_A$ 的判定器。把结论对可数多台量子机取并（可数并的补集仍为测度 1），即可断言：以概率 1 的预言机 A 满足 $\mathcal{L}_A \notin \mathbf{BQTime}(o(2^{n/2}))^A$，从而完成定理所需的随机 - 预言机分离。

注： 定理 3.4 及其推论 3.6 揭示了由酉演化所施加的对 “量子并行性” 的限制。上述定理3.9其余部分的证明，在精神上类似于用随机预言机区分 **BPP** 与 **NP** 的标准技术 [3]。例如，这些技术可用于证明：相对于一个随机预言机 A，任何经典概率图灵机都无法在时间 $o(2^n)$ 内识别语言 $\mathcal{L}_A$。然而，量子图灵机可以更快地识别该语言，达到平方级提速，即在时间 $O(\sqrt{2^n})$ 内完成，使用的是 Grover 算法。这也解释了为何在证明上述定理时，必须对标准技术做出实质性的修改。

接下来的结果关于相对于一个随机置换预言机的 $\mathbf{NP} \cap \mathbf{co\text{-}NP}$。它需要一个更为细致的论证；理想情况下，我们希望在断言 $A^{-1}(1^n)$ 被探测的总查询幅度较小时，直接应用定理 3.4。然而，这恰恰是我们一开始就要证明的东西。

THEOREM 3.11. 对于任何 $T(n) = o(2^{n/3})$，相对于一个随机置换预言机，以

概率 1，$\mathbf{BQTime}(T(n))$ 不包含 $\mathbf{NP}\cap\mathbf{co\text{-}NP}$。

Proof. 对于任意置换预言机 A，令 $\mathcal{L}_A=\{\,y:A^{-1}(y)\text{ 的第一个比特是}1\,\}$。显然，该语言属于 $(\mathbf{NP}\cap\mathbf{co\text{-}NP})^A$。设 $T(n)=o(2^{n/3})$。我们将证明，对于任何运行时间不超过 $T(n)$ 的有界误差预言机 QTM M^A，以概率 1，M^A 不会接受语言 $\mathcal{L}_A$。其中的概率是对随机选择的置换预言机 A 取的。由于 QTM 的数量是可数的，而可数多个概率为 1 的事件的交集仍为概率 1，我们可得出结论：以概率 1，不存在任何有界误差预言机 QTM 能在时间 $T(n)$ 内接受 $\mathcal{L}_A$。

由于 $T(n)=o(2^{n/3})$，我们可以取足够大的 n，使得 $T(n)\le\frac{2^{n/3}}{100}$。我们将证明：对于任意固定预言机在长度不等于 n 的输入上的回答方式，M 在输入 1^n 上出错的概率至少为 $1/8$。此处概率是对预言机在长度为 n 的输入上的置换方式的随机选择所取的。

考虑以下定义 $\{0,1\}^n$ 上随机置换的方法：令 $x_0,x_1,\ldots,x_{T+1}$ 是从 $\{0,1\}^n$ 中独立均匀随机抽取的字符串序列。从满足 $\pi(x_0)=1^n$ 的所有置换中均匀随机选择初始置换 π_0。然后依次构造 $\pi_i=\pi_{i-1}\cdot\tau$，其中 τ 是将 x_{i-1} 与 x_i 对调的置换，即 $\pi_i(x_i)=\pi_{i-1}(x_{i-1})$，$\pi_i(x_{i-1})=\pi_{i-1}(x_i)$，其他保持不变。显然，每个 π_i 都是 $\{0,1\}^n$ 上的一个置换。

考虑一列置换预言机 A_i，满足当 $y\notin\{0,1\}^n$ 时 $A_i(y)=A_j(y)$，当 $y\in\{0,1\}^n$ 时 $A_i(y)=\pi_i(y)$。记 $|\phi_i\rangle$ 为 $M^{A_{T(n)}}$ 在输入 1^n 时的第 i 步叠加态，$|\phi'_i\rangle$ 为 $M^{A_{T(n)-1}}$ 在输入 1^n 时的第 i 步叠加态。根据构造，以概率恰为 $1/2$，字符串 1^n 恰好属于两个语言 $L_{A_{T(n)}}$ 和 $L_{A_{T(n)-1}}$ 中的一个。我们将证明 $\mathbb{E}\big[\,\||\phi_{T(n)}\rangle-|\phi'_{T(n)}\rangle\|\,\big]\le 1/50$，这里的期望是对预言机的随机选择所得。由 Markov 不等式可得 $P\big(\||\phi_{T(n)}\rangle-|\phi'_{T(n)}\rangle\|\le 2/25\big)\ge 3/4$。应用定理3.1，若 $\||\phi_{T(n)}\rangle-|\phi'_{T(n)}\rangle\|\le 2/25$，则 $M^{A_{T(n)}}$ 与 $M^{A_{T(n)-1}}$ 在输入 1^n 上的接受概率之差至多为 $8/25<1/3$，因而要么两者均接受，要么两者均拒绝，故它们在输入 1^n 上给出相同答案的概率至少为 $3/4$。另一方面，构造中有 $P[\text{first bit of }x_{T(n)-1}\neq\text{first bit of }x_{T(n)}]=1/2$，即字符串 1^n 恰好属于这两种语言之一的概率为 $1/2$，因此以至少 $1/4$ 的概率，$M^{A_{T(n)}}$ 或 $M^{A_{T(n)-1}}$ 会在输入 1^n 上给出错误答案。由于 $A_{T(n)}$ 与 $A_{T(n)-1}$ 独立同分布，故 $M^{A_{T(n)}}$ 在输入 1^n 上出错的概率至少为 $1/8$。

为了界定 $\mathbb{E}\big\|\,|\phi\rangle-|\phi_{T(n)}\rangle\big\|$，我们证明 $|\phi_{T(n)}\rangle$ 和 $|\phi'_{T(n)}\rangle$ 均近似于某一固定的叠加态 $|\psi_{T(n)}\rangle$。为定义该叠加态，令机器 M 在输入 1^n 上运行 $T(n)$ 步，并在第 i 步调用不同的预言机 A_i 来回答查询；记 $|\psi_i\rangle$ 为由此得到的第 i 步叠加态。考虑时刻-字符串对集合 $S=\{(i,x_j):\,j\ge i,\ 0\le i\le T(n)\}$. 易核查，上述模拟过程中与 $M^{A_{T(n)}}$ 和 $M^{A_{T(n)+1}}$ 的预言机查询仅在 S 上有所差异。我们断言：对于 S 中任一对 (i,x_j)，其期望查询幅度至多为 $1/2^n$，因为当 $j\ge i$ 时，可将 x_j 理解为在第 j 步之后随机选取，且此前所有对预言机的查询叠加已写入查询带中。令

α 为 S 上所有时-串对的查询幅度之和，则

$$\mathbb{E}[\alpha] \le \mathbf{card}(S)/2^n = \binom{T(n)+1}{2}/2^n \le \frac{T(n)^2}{2^n}$$

当 $T(n) \ge 4$。令随机变量 ε 满足 $\alpha = \varepsilon^2/(2T(n))$。由定理 3.3 得 $\big\| |\phi\rangle - |\phi_{T(n)}\rangle \big\| \le \varepsilon$ 且 $\big\| |\phi\rangle - |\phi'_{T(n)}\rangle \big\| \le \varepsilon$. 我们已示

$$\mathbb{E}\big[\varepsilon^2/T(n)\big] = \mathbb{E}[\alpha] \le \frac{T(n)^2}{2^n}$$

又有 $\mathbb{E}\big[\varepsilon/\sqrt{2T(n)}\big]^2 \le \mathbb{E}\big[\varepsilon^2/(2T(n))\big]$. 因此

$$\mathbb{E}[\varepsilon] = \sqrt{2T(n)}\,\mathbb{E}\big[\varepsilon/\sqrt{2T(n)}\big] \le \sqrt{2T(n)\,\mathbb{E}[\varepsilon^2/(2T(n))]} \le \sqrt{\frac{2}{100^3}} < \frac{1}{100}.$$

于是

$$\mathbb{E}\big\| |\phi\rangle - |\phi_{T(n)}\rangle \big\| \le \mathbb{E}[\varepsilon] < \frac{1}{100}, \quad \mathbb{E}\big\| |\phi\rangle - |\phi'_{T(n)}\rangle \big\| \le \mathbb{E}[\varepsilon] < \frac{1}{100},$$

从而

$$\mathbb{E}\big\| |\phi_{T(n)}\rangle - |\phi'_{T(n)}\rangle \big\| < \frac{1}{50}.$$

最后，很容易得出结论：对于一个均匀随机选择的排列预言机 A，M 以概率 0 判断 $1^n \in \mathcal{L}_A$。 □

注： 根据 Grover 算法，我们知道定理 3.9 中的常数 “1/2” 是无法改进的。另一方面，目前并无证据表明定理 3.11中的常数 “1/3” 是根本性的。定理3.11也很有可能在将 1/3 替换为 1/2 的情况下仍然成立（尽管现有的证明方法可能无法适用）。

COROLLARY 3.12. **相对于一个随机置换预言机，以概率 1 存在一个量子单向置换函数。给定该预言机，不仅在量子图灵机上，在经典确定性机器上也可以高效地计算该排列。但在量子机器上求逆该置换却需要指数时间。**

Proof. 设 A 是一个任意的置换预言机，且 A^{-1} 可以在量子图灵机上以 $o(2^{n/3})$ 时间计算，则判定定理 3.11 中定义的语言 $\mathcal{L}_A$ 同样是容易的。而我们已经在定理 3.11 的证明中说明：当 A 是均匀随机选择的 permutation 预言机时，这一事件发生的概率为 0。 □

4. 使用有界误差量子图灵机作为子程序. 子程序调用或预言机调用的概念在经典计算中提供了一种简单且实用的抽象。然而，在将该抽象应用于量子计算之前，必须考虑一些微妙的细节。例如，假设子程序计算某函数 f，我们希望将其作用于字符串 x 的调用视作在某个指定位置 “魔法般地” 写下 $f(x)$（实际上是进行异或以保证酉性）。在量子算法中，这种抽象仅在子程序能够清除其所有中间计算痕迹、并仅在磁带上留下最终答案时才是有效的。

这是因为，如果子程序是在多个 x 的叠加态上调用的，那么不同的 x 值将导致辅助工作带中产生不同的工作内容，这将阻碍不同计算路径之间的干涉。而由于擦除通常不是酉操作，辅助工作带内容一般不能被事后移除。

在一种特殊情形中，即函数 f 可被确定性地高效计算时，我们可以设计子程序，使其可逆地清除辅助工作带内容——具体做法是先计算 $f(x)$，将 $f(x)$ 拷贝到安全存储区，再逆计算 $f(x)$ 以移除辅助工作带内容 [2]。然而，当 f 是由一个 **BQP** 机器计算时，情形则更加复杂。这是因为，只有部分计算路径会输出正确答案 $f(x)$，因此若我们将 $f(x)$ 拷贝至安全区域后再逆计算 $f(x)$，那么具有不同 $f(x)$ 值的计算路径将不再互相干涉，我们也不会执行第一部分的逆计算。接下来我们展示，如果在将 $f(x)$ 拷贝至安全存储区并逆计算 $f(x)$ 之前提升 **BQP** 机器的成功概率，那么最终叠加态的大部分权重将集中在只包含输入 x 和答案 $f(x)$ 的干净磁带上。由于这样的整洁的 **BQP** 机器可以被安全地用作子程序，这就允许我们证明 $\mathbf{BQP}^{\mathbf{BQP}} = \mathbf{BQP}$. 该结果也正好为我们关于预言机量子机器的定义提供了合理性依据。

增强程序正确性的证明见定理 4.13 与 4.14。该证明总体框架与经典情形相同，只是我们在处理诸如循环等简单编程结构时需要更加小心。因此，我们借用了文献 [4] 中为此目的开发的机制，并在本节开头给出了相关引理与定理的陈述。本节的主要新贡献体现在定理 4.13 与 4.14 的证明中，读者也可选择直接跳至这些证明部分。

4.1. 一些关于量子图灵机的编程原语. 在本小节中，我们将介绍一些来自 [4] 的定义、引理与定理。

回忆一个 QTM M 由三元组 (Σ, Q, δ) 定义，其中：Σ 是带有标识空白符号 $\#$ 的有限字母表，Q 是带有标识初始状态 q_0 和终止状态 $q_f \neq q_0$ 的有限状态集合，而 δ，即量子转移函数，是如下形式的函数：

$$\delta \,:\, Q \times \Sigma \to \tilde{\mathbb{C}}^{\Sigma \times Q \times \{L,R\}}$$

其中 $\tilde{\mathbb{C}}$ 表示其实部与虚部都可以在时间多项式于 n 内逼近到 2^{-n} 精度的复数集合。

Definition 4.1. *一个 QTM 的最终格局是任意处于状态 q_f 的格局。若 QTM M 在输入 x 上运行，在时间 T 时叠加态仅包含最终格局，且在任意时间 $< T$ 时叠加态均不包含最终格局，则称 M 在输入 x 上以运行时间 T 停机。M 在时间 T 的叠加态称为其在输入 x 上的最终叠加态。一个多项式时间的 QTM 是指对任意输入 x 都能在其长度的多项式时间内停机的良构 QTM。*

Definition 4.2. *若 QTM M 在所有输入串上均以某个叠加态停机，且该叠加态中每个格局的读写头都停在同一单元上，则称 M 是行为良好的。若该单元始终是起始单元，则称该 QTM 为静止型的 (stationary)。*

我们称一个 QTM M 处于标准形式（*normal form*），若所有从终止状态 q_f 的跃迁都会导向特殊状态 q_0，被扫描单元格中的符号保持不变，且读写头向右移动。形式上：

DEFINITION 4.3. 一个 $QTM\ M = (\Sigma, Q, \delta)$ 处于标准形式，当且仅当

$$\forall \sigma \in \Sigma \quad \delta(q_f, \sigma) = |\sigma\rangle|q_0\rangle|R\rangle$$

THEOREM 4.4. 若 f 是一个从字符串映射到字符串的函数，且 f 可以在确定性多项式时间内计算，且 $f(x)$ 的长度仅依赖于 x 的长度，则存在一个多项式时间、稳定的、标准形式的 QTM，当输入为 x 时，它输出 $f(x)$，其运行时间仅依赖于 x 的长度。

若 f 是一个一一映射，且 f 与 f^{-1} 均可在确定性多项式时间内计算，且 $f(x)$ 的长度仅依赖于 x 的长度，则存在一个多项式时间、稳定的、标准形式的 QTM，当输入为 x 时，它输出 $f(x)$，其运行时间仅依赖于 x 的长度。

DEFINITION 4.5. 一个 k 轨多轨图灵机是其字母表 Σ 形如 $\Sigma_1 \times \Sigma_2 \times \cdots \times \Sigma_k$ 的图灵机，并在每个 Σ_i 中有特殊空白符 $\#$，使得 Σ 中的空白符为 $(\#, \ldots, \#)$。我们通过指定每条“轨道”上的字符串（以 *';'* 分隔）来指定输入，并可选地指定轨道内容的对齐方式。

LEMMA 4.6. 设任意 $QTM\ M = (\Sigma, Q, \delta)$ 与任意集合 Σ'，则存在 $QTM\ M' = (\Sigma \times \Sigma', Q, \delta')$，使得 M' 的行为与 M 完全一致，同时保持其第二轨道不变。

LEMMA 4.7. 设任意 $QTM\ M = (\Sigma_1 \times \cdots \times \Sigma_k, Q, \delta)$ 以及排列 $\pi : [1,k] \to [1,k]$，则存在 $QTM\ M' = (\Sigma_{\pi(1)} \times \cdots \times \Sigma_{\pi(k)}, Q, \delta')$，使得 M' 的行为与 M 完全一致，除了其轨道按照 π 进行了重排。

LEMMA 4.8. 若 M_1 与 M_2 是在相同字母表下的良行为（*well-behaved*）、标准形式 QTM，则存在一个标准形式的 $QTM\ M$，其计算过程依次执行 M_1 与 M_2。

LEMMA 4.9. 设 M 是一个良行为、标准形式的 QTM。则存在一个标准形式的 $QTM\ M'$，使得对输入 $x;k$，当 $k > 0$ 时，M' 在其第一轨道上运行 M 共 k 次。

DEFINITION 4.10. 如果量子图灵机 M_1 和 M_2 具有相同的字母表，那么我们说 M_2 反转 M_1 的计算，若满足以下条件：对于任意使 M_1 停机的输入 x，记 c_x 和 ϕ_x 分别为 M_1 在输入 x 时的初始格局和最终叠加态。那么 M_2 在输入叠加态 ϕ_x 时会停机，最终叠加态完全由格局 c_x 构成。注意，为了让 M_2 能反转 M_1，M_2 的最终状态必须等于 M_1 的初始状态，反之亦然。

LEMMA 4.11. 若 M 是一个对所有输入均停机的正规形式 QTM，则存在一个正规形式的 $QTM\ M'$，它以慢因子 5 反转 M 的计算过程。

接下来，回顾一下类 **BQP** 的定义。

DEFINITION 4.12. 设 M 是一个静态、正规形式的多带量子图灵机，其最后一带的字母表为 $\{\#, 0, 1\}$。我们称 M 接受 输入 x，当且仅当它在起始单元格的最后一带上以符号 1 停机。否则我们称 M 拒绝 输入 x。

若 M 对语言 $\mathcal{L} \subseteq (\Sigma - \#)^*$ 的每个字符串 $x \in \mathcal{L}$ 以至少 p 的概率接受，且对每个 $x \in (\Sigma - \#)^* - \mathcal{L}$ 以至少 p 的概率拒绝，则称 M 以概率 p 接受语言 $\mathcal{L}$。我们定义类 ***BQP*** (有界误差量子多项式时间) 为：存在某个多项式时间 QTM 以概率 2/3 接受的语言集合。更一般地，我们定义类 ***BQTime***$(T(n))$ 为：存在某个 QTM 其在任意长度为 n 的输入上运行时间至多为 $T(n)$，并以概率 2/3 接受的语言集合。

4.2. 放大与子程序调用.

THEOREM 4.13. 如果量子图灵机 M 以概率 2/3 在时间 $T(n) > n$ 内接受语言 $\mathcal{L}$，且 $T(n)$ 为时间可构造函数，那么对于任意 $\varepsilon > 0$，存在一个 QTM M'，它以概率 $1 - \varepsilon$ 接受语言 $\mathcal{L}$，其运行时间为 $cT(n)$，其中 c 是 $\log(1/\varepsilon)$ 的多项式，但与 n 无关。

Proof. 令 M 为一个静态量子图灵机，它在时间 $T(n)$ 内接受语言 $\mathcal{L}$。

我们将构造一个机器，它独立运行 M 的 k 份拷贝，并对这 k 个答案进行多数投票。在任意输入 x 上，M 会有某个最终叠加态 $\sum_i \alpha_i x_i$。若我们记 A 为那些 x_i 给出正确答案 $M(x)$ 的 i 的集合，则有 $\sum_{i \in A} |\alpha_i|^2 \geq 2/3$。现在对输入 x 独立运行 M 共 k 次，将会产生叠加态 $\sum_{i_1,\ldots,i_k} \alpha_{i_1} \cdots \alpha_{i_k} x_{i_1} \cdots x_{i_k}$。那么，多数路径给出正确答案 $M(x)$ 的概率就是那些 $|\alpha_{i_1}|^2 \cdots |\alpha_{i_k}|^2$ 之和，其中 $\{i_1, \ldots, i_k\}$ 的多数属于 A。但这就像是对独立硬币掷 k 次，每次成功概率为 2/3，然后取多数的过程。因此存在某个常数 b，使得当 $k = b\log(1/\varepsilon)$ 时，正确答案出现多数的概率至少为 $1 - \varepsilon$。

所以，我们将构造一台机器来执行以下步骤。

1. 计算 $n = T(|x|)$。
2. 写出 k 份输入 x 的副本，每份之间间隔 $2n$ 个空格单元，并在其他磁道上写下 k 与 n。
3. 在运行 M 的机器上循环 k 次，每次向右移动 n 步。
4. 计算 k 个答案中的多数值，并将其写回到起始单元。

我们通过为上述四个步骤中的每一步构造一个 QTM，并将它们拼接在一起来构造出所需的 QTM。

由于步骤 1、2 和 4 涉及的函数都是易于计算的，其输出长度仅依赖于 k 和 x 的长度，因此我们可以使用良态（well-behaved）、标准形式的 QTM 来实现它们，这些 QTM 可由定理 4.4 构造，它们的运行时间也仅依赖于 k 和 x 的长度。

因此，我们通过构造一个 QTM 来运行给定机器 k 次，从而完成证明。首先，使用定理 4.4，我们可以构造一个静态的、标准形式的 QTM，它将整数 k 和 n 在其工作磁道上向右拖动一个单元格。如果我们在这个 QTM 的末尾添加一个单步操作并应用引理 4.9，我们就能构造一个良态、标准形式的 QTM，该 QTM 向右移动 n 个单元，同时将 k 和 n 一并拖动。将该机器拼接在 M 之后，再应用引理 4.9 可得一个标准形式的 QTM，它在输入的 k 个副本上运行 M。最后，我们可以拼接一个机器，用于将 k 和 n 返回到起始单元，这可以通过围绕一个将 k 和 n 向左移动一步的 QTM，再次应用引理 4.9 两次来完成。 □

QTM 的输出磁带上的额外信息可以通过将所需的输出复制到另一条磁道上，然后运行该 QTM 的反向过程来擦除。如果在最终叠加态中的每一个格局中输出都是相同的，那么该反向过程将精确恢复输入。不幸的是，如果输出在不同格局中有所不同，那么保存该输出将阻止这些格局在机器反转时发生干涉，因而输入将无法恢复。我们展示了，在大多数最终叠加态中情况是相同的，因此该反向过程必须将我们引回接近输入的位置。

Proof. 设 $M = (\Sigma, Q, \delta)$ 为一个静态的、正规形式的 QTM，其在时间 $T(n)$ 内接受语言 $\mathcal{L}$。

根据定理 4.13，在以 $\log 1/\varepsilon$ 的多项式为因子的速度下降的代价下（但该因子与 n 无关），我们可以假设 M 以至少 $1 - \varepsilon/2$ 的概率在每个输入上接受 $\mathcal{L}$。

然后我们可以通过运行 M、将答案复制到另一条轨道上，并运行 M 的反向机来构造期望的 M'。复制过程可以通过一个简单的两步 QTM 实现，该机先向左移动一步再向右移回来，同时将答案写入一条干净的轨道。根据引理 4.11，我们可以构造一个正规形式的 QTM M^R 来反转 M。最后，使用引理 4.6 和 4.7 中的合适方式，我们可以将复制机与 M 和 M^R 对接起来，构造出期望的静态 QTM M'。

为了验证 M' 拥有所需性质，考虑 M' 在一个长度为 n 的输入 x 上的运行。M' 首先在 x 上运行 M，产生某个最终叠加态 $\sum_y \alpha_y |y\rangle$。然后它将在每个格局的起始单元的额外轨道上写入 0 或 1，并在此叠加态 $\phi = \sum_y \alpha_y |y\rangle|M(x)\rangle$ 上运行 M^R。如果我们直接在 $\phi = \sum_y \alpha_y |y\rangle|M(x)\rangle$ 上运行 M^R，在 $T(n)$ 步之后将得到一个仅包含最终格局的叠加态，其输出为 $x; M(x)$。显然，$\langle\phi|\phi'\rangle$ 是实数，并且由于 M 的接受概率至少为 $1 - \varepsilon/2$，故 $\langle\phi|\phi'\rangle \geq \sqrt{1-\varepsilon}$. 因为 M^R 的酉演化保持内积不变，所以 M' 的最终叠加态中必须包含一个内部积为 $\langle x|M(x)\rangle$ 的项，并且该值为实数，且至少为 $1 - \varepsilon/2$。因此，M' 的最终叠加态中关于 $x; M(x)$ 的项的平方幅度至少为 $(1 - \varepsilon/2)^2 \geq 1 - \varepsilon$。 □

推论 4.15 $\mathbf{BQP}^{\mathbf{BQP}} = \mathbf{BQP}$。

参考文献

[1] L. Babai and S. Moran, *Arthur-merlin games: a randomized proof system, and a hierarchy of complexity classes*, Journal of Computer and System Sciences, 36 (1988), pp. 254–276.

[2] C. H. Bennett, *Logical reversibility of computation*, IBM journal of Research and Development, 17 (1973), pp. 525–532.

[3] C. H. Bennett and J. Gill, *Relative to a random oracle a, \bfp^a≠\bfnp^a≠co-\bfnp^a with probability 1*, SIAM Journal on Computing, 10 (1981), pp. 96–113.

[4] E. Bernstein and U. Vazirani, *Quantum complexity theory*, in Proceedings of the twenty-fifth annual ACM symposium on Theory of computing, 1993, pp. 11–20.

[5] A. Berthiaume and G. Brassard, *The quantum challenge to structural complexity theory.*, in SCT, Citeseer, 1992, pp. 132–137.

[6] A. Berthiaume and G. Brassard, *Oracle quantum computing*, Journal of modern optics, 41 (1994), pp. 2521–2535.

[7] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, *Tight bounds on quantum searching*, Fortschritte der Physik: Progress of Physics, 46 (1998), pp. 493–505.

[8] N. H. Bshouty and J. C. Jackson, *Learning dnf over the uniform distribution using a quantum example oracle*, in Proceedings of the eighth annual conference on Computational learning theory, 1995, pp. 118–127.

[9] D. Deutsch, *Quantum theory, the church–turing principle and the universal quantum computer*, Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 400 (1985), pp. 97–117.

[10] D. Deutsch and R. Jozsa, *Rapid solution of problems by quantum computation*, Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences, 439 (1992), pp. 553–558.

[11] D. E. Deutsch, *Quantum computational networks*, Proceedings of the royal society of London. A. mathematical and physical sciences, 425 (1989), pp. 73–90.

[12] R. P. Feynman, *Simulating physics with computers*, in Feynman and computation, cRc Press, 2018, pp. 133–153.

[13] L. K. Grover, *A fast quantum mechanical algorithm for database search*, in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, pp. 212–219.

[14] J. Machta, *Phase information in quantum oracle computing*, arXiv preprint quant-ph/9805022, (1998).

[15] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, in Proceedings 35th annual symposium on foundations of computer science, Ieee, 1994, pp. 124–134.

[16] D. R. Simon, *On the power of quantum computation*, SIAM journal on computing, 26 (1997), pp. 1474–1483.

[17] A. C.-C. Yao, *Quantum circuit complexity*, in Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science, IEEE, 1993, pp. 352–361.