arXiv:2603.05920v1 [quant-ph] 6 Mar 2026

量子电路后接稀疏经典后处理的经典可模拟性

Yasuhiro Takahashi[1, 2, *] Masayuki Miyamoto[1, 2] Noboru Kunihiro[1, 2]
[1]茨城筑波大学系统与信息工程研究所，邮编305-8573，日本[2] 筑波大学筑波高等研究所，邮编305-8577，日本

摘要

我们研究多项式规模量子电路 C_n 作用于 n 个量子比特后，再对 m个比特进行稀疏经典后处理（SCP）时的经典可模拟性，其中 $m \leq n \leq \text{poly}(m)$。SCP由一个非零布尔函数 f_m 描述，该函数可在多项式时间内经典计算且是稀疏的，即具有峰值傅里叶谱。首先，我们给出关于 C_n 的充要条件，使得对于任意SCP f_m，C_n 后接 f_m 均可经典模拟。这一刻画推广了Van den Nest的结果，并表明多种量子电路后接SCP均可经典模拟。例如，IQP 电路、Clifford Magic电路以及Simon 算法的量子部分，尽管这些电路单独而言难以经典模拟。随后，我们考虑 C_n 具有常数深度 d的情况。尽管对于任意SCP f_m，C_n 后接 f_m 不太可能可经典模拟，但我们证明，可以通过一种多项式时间概率算法对其进行模拟，该算法可调用作用于 $n+1$ 个量子比特的对易量子电路。每个这样的量子电路至多包含 $\deg(f_m)$个对易门，且每个对易门至多作用于 2^d+1个量子比特，其中$\deg(f_m)$是 f_m的傅里叶次数。这有助于更好地理解量子电路在常数深度下后接SCP时的模拟难度。

1 引言

1.1 背景与主要结果

量子计算的一个核心挑战是阐明量子计算机与经典计算机之间的计算差距 [10]。实现这一目标的一种富有成效的方法是研究量子计算模型的经典可模拟性 [8]。特别地，由于著名的快速量子算法，例如Simon算法和Shor算法 [18, 17], 依赖于经典后处理，因此自然要考察一种基于量子电路并后接经典后处理的模型。Van den Nest研究了后接稀疏经典后处理（SCP）的Simon型量子电路，该后处理简化了原算法中的非稀疏后处理，并证明此类计算是可经典模拟的 [23]。这里，若描述经典后处理的布尔函数具有峰值傅里叶谱，则称该经典后处理是稀疏的。然而，正如我们在第3节中所讨论的，后接SCP的常数深度量子电路不太可能是可经典模拟的。这与Simon型情形形成鲜明对比，表明后接SCP的量子电路的经典可模拟性对底层量子电路的结构高度敏感。因此，为了阐明可经典模拟的量子计算与不可经典模拟的量子计算之间的边界，有必要研究后接SCP的一般量子电路的经典可模拟性。

在本文中，我们研究一种计算模型的经典可模拟性。该模型由一个作用于 n 个量子比特的多项式规模量子电路 C_n 和一个非零布尔函数 $f_m : \{0,1\}^m \to$ 组成

*ya.takahashi@cs.tsukuba.ac.jp

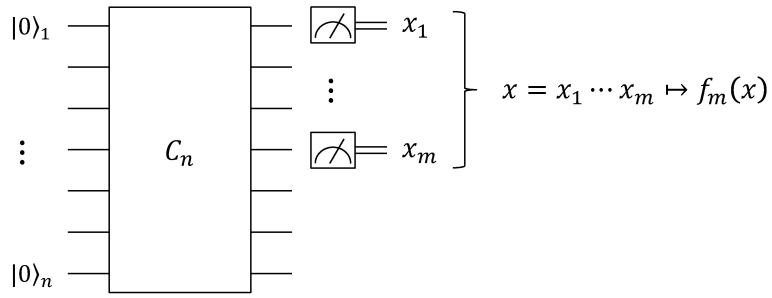


图1： C_n 后接 f_m。量子电路 C_n 作用于初始态 $|0^n\rangle$，对顶部的 m 个量子比特在计算基下进行测量，得到经典测量结果 $x = x_1 \cdots x_m \in \{0, 1\}^m$，并将非零布尔函数 f_m 作用于 x，得到输出 $f_m(x) \in \{0, 1\}$。

{0,1}，它是一个 SCP，其中 $m \leq n \leq \text{poly}(m)$。具体而言， C_n 作用于初始态$|0^n\rangle$，对 m 个量子比特进行计算基测量，并由 f_m 处理测量得到的经典测量结果。我们假设 f_m 可在多项式时间内经典计算，且是稀疏的，即具有峰值傅里叶谱；这里，f_m 的傅里叶稀疏度由 m 中某个已知多项式上界：

$$|\{s \in \{0,1\}^m \mid \widehat{f_m}(s) \neq 0\}| \leq \text{poly}(m),$$

其中傅里叶系数为

$$\widehat{f_m}(s) = \frac{1}{2^m} \sum_{x \in \{0,1\}^m} f_m(x)(-1)^{s \cdot x}.$$

整体计算， C_n 后接 f_m，如图1所示。如果存在一个多项式时间概率算法，能够以指数小的错误概率，将该计算输出为 1 的概率近似到 n的多项式小加性误差范围内，且给定C_n 的经典描述以及一个用于计算 f_m [5, 23]的多项式时间经典算法，则称该计算可经典模拟。本文中，对于其他更一般的计算模型，也采用相同的可模拟性概念。

关于量子电路后接经典后处理，已有多项研究。据我们所知，Van den Nest 首先研究了量子电路后接 SCP [23]；然而，该研究仅限于具有特定结构的量子电路，其结构类似于 Simon 算法的量子部分。Bravyi 等人研究了相关模型 [5], ，但其设定不涉及 SCP。除这些研究外，还有若干工作考察了量子电路后接受限形式的经典后处理。Slote 研究了 $\text{AC}^0 \circ \text{QNC}^0$ [19], 模型，该模型由 QNC^0 量子电路后接 AC^0 函数构成。其中，QNC^0 量子电路是常数深度量子电路，而 AC^0 函数是由具有无界扇入的常数深度经典电路计算的布尔函数。Anshu 等人 [1] 和 Ghosh 等人 [7]进一步拓展了这一研究方向。Takahashi 等人研究的模型可以视为 QNC^0 量子电路后接一个作用于任意数量输入的与函数 [22], ，尽管他们没有明确提及经典后处理。尽管已有这些研究，先前仍没有工作分析一般量子电路后接 SCP 时的经典可模拟性，而这正是本文关注的重点。

首先，我们给出关于 C_n 的一个充要条件，使得对于任意 SCP f_m， C_n 后接 f_m 都可经典模拟。为此，我们利用由 C_n 定义的某些实数的经典可近似性。这里，“经典可近似”与上述经典可模拟性的定义含义相同，即该量可由多项式时间概率算法以多项式小的加性误差进行近似

错误以及 ，且错误概率为指数小。对于任意 $s = s_1 \cdots s_m \in \{0,1\}^m$，我们定义 e

$$Z(s) = \bigotimes_{j=1}^{m} Z_j^{s_j},$$

它是作用于 m 已测量量子比特的酉操作。其中， $Z_j^0 = I$ 和 $Z_j^1 = Z_j$，其中Z_j 表示作用于第 j 个量子比特上的泡利-Z 操作。令 I_{n-m} 表示作用于$n-m$ 未测量量子比特的恒等操作。我们的第一个结果如下所述:

定理 1。 令 C_n 为作用于 n 个量子比特、并初始化为 $|0^n\rangle$ 的任意多项式规模量子电路，令 m 为满足 $m \le n \le \mathrm{poly}(m)$ 的任意整数。以下各项等价:

(1) 对于任意 *SCP* f_m， C_n 后接 f_m 是可经典模拟的。

(2) 对于任意 $s \in \{0,1\}^m \mid \{0^m\}$，泡利期望值

$$\langle 0^n | C_n^\dagger (Z(s) \otimes I_{n-m}) C_n | 0^n \rangle$$

是经典可近似的。

定理1表明，多种量子电路在后接 SCP 后都可经典模拟。一个主要例子是 C_n 具有与 Simon 算法量子部分相似结构的情形。这包括 IQP 电路 [16], ，它们被视为展示量子霸权的候选方案 [8] ，因为人们认为，从它们的输出概率分布中进行经典采样在计算上难以实现。利用 CT 态和 ECS 操作的性质 [23], ，我们可以证明定理1 中的条件（2）对这些电路成立。因此，根据定理 1，对于任意 SCP f_m， C_n 后接 f_m 均可经典模拟。这一结果重现了 Van den Nest 的结论，同时明确说明了其对 IQP 电路的适用性；此前的工作 [23]并未正式讨论这一点。此外，定理1 也可直接应用于 C_n为 Clifford Magic 电路的情形 [24], ，这是另一种重要的量子霸权模型。与前一个例子一样，条件（2）成立，因此对于任意 SCP f_m， C_n 后接 f_m 均可经典模拟。值得注意的是， [23]中的原始论证并不能直接推出 Clifford Magic 电路的这一结果，因此定理1 构成了对先前工作的实质性扩展。

接下来，我们考虑 C_n 是常数深度量子电路的情形，这是与量子霸权相关的另一种模型 [8]。正如我们在第 3 节讨论的，对于任意 SCP f_m， C_n 后接 f_m 不太可能是可经典模拟的。不过，我们证明，如果为多项式时间概率算法增加访问对易量子电路的能力，它就可以被模拟。为此，对于任意定义在 m 个比特上的非零实值布尔函数 h_m ，我们将其傅里叶次数 deg(h_m) 定义为

$$\max\{|s| \mid \widehat{h_m}(s) \neq 0, s \in \{0,1\}^m\},$$

其中 $|s|$ 表示 s的汉明重量。此外，对于任意酉操作 U，我们将其支撑集 supp(U) 定义为 U 以非平凡方式作用于其上的量子比特集合。我们的第二个结果如下所述:

定理 2. 设 C_n 是作用于 n个初始化为 $|0^n\rangle$的量子比特上的任意多项式规模常数深度量子电路 d ，且 m 是满足 $m \le n \le \mathrm{poly}(m)$的任意整数。那么，对于任意 *SCP* f_m， C_n 后接 f_m 可由一种多项式时间概率算法模拟，该算法可访问满足以下条件的、作用于 $n+1$ 个量子比特的对易量子电路:

- 每个对易量子电路中的对易门数量最多为 $\deg(f_m)$。
- 每个对易门作用的量子比特数至多为

$$1 + \max\{|\mathrm{supp}(C_n^\dagger (Z_j \otimes I_{n-m}) C_n)| \mid 1 \le j \le m\}.$$

由于 $\deg(f_m) \le m$ ，且第二个条件中的最大支撑集规模至多为 2^d，定理 2 中出现的每个对易量子电路至多由 m 个对易门组成。此外，这些电路是 (2^d+1)-局部的，也就是说，每个对易门至多作用于2^d+1 个量子比特。定理 2 首次证明，对易量子电路足以模拟后接 SCP 的常数深度量子电路。因此，该定理为模拟这一计算模型所需的量子资源确立了一个非平凡的上界，从而让我们更清楚地理解模拟后接 SCP 的常数深度量子电路的难度。

1.2 技术概述

定理 $\Rightarrow$中的蕴含关系（1）$\Rightarrow$（2）可通过将 f_m 视为奇偶函数直接得出，因为它能筛选出单个傅里叶系数。因此，证明的核心在于证明（2） $\Rightarrow$ $\Rightarrow$（1）。在假设（2）成立的情况下，对于任意 SCP f_m，我们构造一个多项式时间概率算法，用于近似 C_n 后接 f_m 的输出为 1 的概率。该概率记作 $p(C_n, f_m)$，可表示为

$$p(C_n, f_m) = \sum_{x\in\{0,1\}^m} f_m(x)p_m(x),$$

其中， p_m 是 C_n 在$\{0,1\}^m$上的输出概率分布。一个关键步骤是将该概率变换到傅里叶域。具体而言，通过应用普朗歇尔定理 [14]以及量子电路与其输出概率分布的傅里叶系数之间的一般关系（这是对 [20], 中所示关系的略微扩展），我们证明，近似 $p(C_n, f_m)$ 可归约为近似以下数值

$$p'(C_n, f_m) = \sum_{s\in\{0,1\}^m} \widehat{g_m}(s)\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle,$$

其中，对于任意 $x \in \{0,1\}^m$， $g_m(x) = (-1)^{f_m(x)}$ 。由于 f_m 是稀疏的， g_m 也稀疏，这意味着 $p'(C_n, f_m)$ 可表示为

$$\sum_{s\in L} \widehat{g_m}(s)\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle,$$

其中

$$L = \{s \in \{0,1\}^m \mid \widehat{g_m}(s) \neq 0\}$$

且 $|L|$ 以某个已知的关于 m的多项式为上界。为计算该求和，我们采用 Kushilevitz-Mansour 算法 [9] ，以高效识别 g_m的显著傅里叶系数。随后，我们利用切尔诺夫–霍夫丁界近似每个 $\widehat{g_m}(s)$，并依据假设(2)近似每个泡利期望值。由于项数 $|L|$ 受多项式界约束，总加性误差仍保持为多项式小量。

为证明定理2，其中 C_n 是常数深度为 d 、作用于 n 个量子比特上的量子电路，我们近似 $p(C_n,\ f_m)$ ，方法是利用前述关于(2) $\Rightarrow$ (1)的证明。具体而言，只需近似每个泡利期望值

$$\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle,$$

但在这种设定下，我们改用一种多项式时间概率算法，该算法能够访问作用于 $n+1$ 个量子比特上的对易量子电路，并满足对易门数量以及每个对易门作用的量子比特数量的条件。事实上，我们改编了 Ni 等人 [11] 的构造，以近似计算 $|\langle 0^n|C_n|0^n\rangle|^2$。更具体地说，我们利用如下分解

$$\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle = \langle 0^n| \prod_{1\le j\le m: s_j=1} (C_n^\dagger(Z_j\otimes I_{n-m})C_n)|0^n\rangle.$$

每个操作 $V_j = C_n^\dagger(Z_j \otimes I_{n-m})C_n$ 都可以视为对易量子电路中的一个门，因为所有 $\{V_j\}$ 彼此对易。将这些门纳入一个使用单个辅助量子比特的哈达玛测试后，我们可以构造一个作用于 $n+1$ 个量子比特上的对易量子电路。测量辅助量子比特并得到 0 的概率为

$$\frac{1 + \langle 0^n | \prod_{j:s_j=1} (C_n^\dagger (Z_j \otimes I_{n-m}) C_n) | 0^n \rangle}{2}.$$

通过应用切尔诺夫–霍夫丁界，只需访问作用于 $n+1$ 个量子比特上的对易量子电路，即可高效近似每个泡利期望值。该构造直接满足定理2的条件：对易量子电路中的对易门数量为 $|s|$，其上界为 $\deg(g_m) = \deg(f_m)$，且每个对易门作用的量子比特数至多为

$$1 + \max\{|\mathrm{supp}(C_n^\dagger (Z_j \otimes I_{n-m}) C_n)| \mid 1 \le j \le m\}.$$

结合这些要素，即可得到定理 2中所述的模拟。

2 预备知识

2.1 量子电路

我们使用量子态的标准记号和量子电路的标准图示 [12]。量子电路由基本门组成，每个门都属于门集$\{H,\ T,\ CZ\}$，其中

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix},\ CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

该门集对于量子计算是近似通用的。我们定义 $S = T^2$、 $Z = T^4$ 和 $X = HZH$。有时我们使用 CCZ 门，其中

$$CCZ = |00\rangle\langle 00| \otimes I + |01\rangle\langle 01| \otimes I + |10\rangle\langle 10| \otimes I + |11\rangle\langle 11| \otimes Z,$$

它可以精确分解为上述基本门的常数个门。对于任意酉操作 U，我们将 U 的支撑集定义为 $\mathrm{supp}(U)$，即 U 非平凡作用于其上的量子比特集合。

量子电路的复杂度度量是其规模和深度。规模是电路中基本门的数量。为定义深度，我们将电路视为由基本门组成的一组层 1、.....、d，其中同一层中的门作用于两两不相交的量子比特集合，并且第 j 层中的任何门都在第 $j+1$ 层中的任何门之前应用。深度是 d [6] 可能取到的最小值。每一层 j 都由可并行执行的门组成，因为它们作用于两两不相交的量子比特集合。

我们研究一族一致的多项式规模量子电路$\{C_n\}_{n\ge 1}$，其中每个C_n 有 n 个输入量子比特，初始状态为 $|0^n\rangle$。一致性意味着函数 $1^n \mapsto C_n$ 可由多项式时间经典图灵机计算，其中 C_n 是 C_n [13]的经典描述。执行 C_n后，我们在计算基（即 Z基）下测量 m个量子比特，其中 $m \le n$。不失一般性，我们假设被测量的量子比特是最前面的 m 个量子比特，即电路图中最上方的 m个量子比特。 C_n 在 $\{0,1\}^m$ 上的输出概率分布 p_m 定义为

$$p_m(x) = \langle 0^n | C_n^\dagger (|x\rangle\langle x| \otimes I_{n-m}) C_n | 0^n \rangle,$$

其中，表示量子电路的符号也表示其在 Z 基下的矩阵表示，而 I_{n-m} 是作用于 $n-m$ 个未测量量子比特的恒等操作。对于任意 $s = s_1 \cdots s_m \in \{0,1\}^m$，我们定义

$$Z(s) = \bigotimes_{j=1}^{m} Z_j^{s_j},$$

它是作用于 m 已测量量子比特的酉操作。这里，$Z_j^0 = I$ 和 $Z_j^1 = Z_j$，其中 Z_j 表示作用于第 j 个量子比特的 Pauli-Z 操作。

2.2 布尔函数的傅里叶展开

设 $f_m : \{0,1\}^m \to \mathbb{R}$ 是定义在 m 位上的任意实值布尔函数。那么，f_m 可以唯一表示为基函数的 $\mathbb{R}$-线性组合：

$$f_m(x) = \sum_{s \in \{0,1\}^m} \widehat{f_m}(s)(-1)^{s \cdot x},$$

$\widehat{\ }$称为 f_m [14]的傅里叶展开。这里，$f_m(s)$称为f_m 的傅里叶系数，符号“$\cdot$”表示两个 m位字符串模 2 的内积，即

$$s \cdot x = \bigoplus_{j=1}^{m} s_j x_j$$

对于任意 $s = s_1 \cdots s_m$和 $x = x_1 \cdots x_m \in \{0,1\}^m$，其中 $\oplus$表示模 2 加法。成立：

$$\widehat{f_m}(s) = \frac{1}{2^m} \sum_{x \in \{0,1\}^m} f_m(x)(-1)^{s \cdot x}$$

对于任意 $s \in \{0,1\}^m$。f_m 的傅里叶稀疏度定义为其非零傅里叶系数的数量

$$|\{s \in \{0,1\}^m \mid \widehat{f_m}(s) \neq 0\}|.$$

我们称 f_m 为稀疏的，如果其傅里叶稀疏度被$\sim m$ 中的某个已知多项式所上界（尽管满足 $f_m(s) \neq 0$ 的 $s \in \{0,1\}^m$ 集合不一定已知）。此外，对于任意非零布尔函数 f_m，我们将其傅里叶次数 $\deg(f_m)$ 定义为

$$\max\{|s| \mid \widehat{f_m}(s) \neq 0, s \in \{0,1\}^m\},$$

其中 $|s| = \sum_{j=1}^{m} s_j$，是 s 的汉明重量。为保持一般性，我们考虑实值函数，但主要关注取值为 $\{0, 1\}$ 的函数 $f_m : \{0, 1\}^m \to \{0, 1\}$。稀疏布尔函数的一个简单例子是奇偶函数

$$f_m(x) = \bigoplus_{j=1}^{m} x_j.$$

$\widehat{\ }$在这种情况下，$\{s \in \{0, 1\}^m \mid f_m(s) \neq 0\} = \{0^m, 1^m\}$ 且 $\deg(f_m) = m$。

2.3 量子电路后接 SCP

设 C_n 是作用于 n 个量子比特上的任意多项式规模量子电路，且 $f_m : \{0, 1\}^m \to \{0, 1\}$ 是任意一个非零、稀疏且可在多项式时间内经典计算的布尔函数，其中 $m \leq n \leq \mathrm{poly}(m)$。我们将 f_m 视为稀疏经典后处理（SCP），并考虑以下计算模型，称为 C_n 后接 f_m：

1. 对初始化为 $|0^n\rangle$ 的 C_n 个量子比特 n 执行操作。

2. 对状态 $C_n|0^n\rangle$ 中的 m 个量子比特进行测量，测量基为 Z；其中，第 j 个量子比特的经典测量结果为 $x_j \in \{0,\ 1\}$，对任意 $1 \le j \le m$ 均成立。

3. 将 f_m 应用于测量的经典测量结果 $x = x_1 \cdots x_m \in \{0,1\}^m$。

该计算的输出为 $f_m(x) \in \{0,1\}$。

设 p_m 为上述所描述的 C_n 的输出概率分布。C_n后接 f_m 的输出以概率 $\sum_{x:f_m(x)=0} p_m(x)$ 为 0，以概率 $\sum_{x:f_m(x)=1} p_m(x)$ 为 1。因此，我们可以将 C_n 后接 f_m 时输出为 1 的概率表示为

$$p(C_n, f_m) = \sum_{x\in\{0,1\}^m} f_m(x)p_m(x).$$

这可以看作 f_m 在概率分布 p_m下的期望值。整体计算 C_n 后接 f_m，若存在一个多项式时间概率算法，能够以指数小的错误概率，在给定 $p(C_n, f_m)$ 的情况下，以多项式小加性误差近似 n，并且给定 C_n 的经典描述以及一个用于计算 f_m [5, 23]的多项式时间经典算法，则称其为可经典模拟。更具体地说，对于任意多项式 $q(n)$，存在一个多项式时间概率算法，以大于 $1 - 1/\exp(n)$的概率输出一个实数 A，使得

$$|p(C_n, f_m) - A| \le \frac{1}{q(n)}.$$

该定义同样适用于实数：若存在一个多项式时间概率算法，能以指数小的错误概率、以多项式小加性误差逼近某个实数，则称该实数为经典可逼近的。在第5节中，我们引入一种计算模型，它通过赋予概率算法对某些量子资源的访问权限来扩展经典计算。若 $p(C_n, f_m)$ 能被该模型中的算法以与上述相同的精度和成功概率逼近，则称该计算在此扩展模型中是可模拟的。

3 后接SCP的一般量子电路

3.1 后接SCP的常数深度量子电路的困难性

作为定理1所给刻画的动机，我们首先讨论后接SCP的常数深度量子电路的经典可模拟性。设 C_n 是作用于 n个量子比特、并初始化为 $|0^n\rangle$的任意常数深度多项式规模量子电路。就我们的目的而言，只需考虑 $m = n$ 且 f_n 为奇偶函数的情形，即

$$f_n(x) = \bigoplus_{j=1}^{n} x_j,$$

这是一个稀疏布尔函数的简单示例。

要对 C_n 后接 f_n进行经典模拟（如第 2.3 节所述），我们需要近似计算概率

$$p(C_n, f_n) = \sum_{x\in\{0,1\}^n} f_n(x)p_n(x) = \sum_{x\in\{0,1\}^n} \left(\bigoplus_{j=1}^{n} x_j\right) p_n(x).$$

由于有

$$\bigoplus_{j=1}^{n} x_j = \frac{1}{2} - \frac{1}{2}(-1)^{|x|}$$

and $p_n(x) = \langle 0^n|C_n^\dagger|x\rangle\langle x|C_n|0^n\rangle$，上述概率可表示如下 :

$$\begin{aligned} p(C_n, f_n) &= \sum_{x\in\{0,1\}^n} \left(\frac{1}{2} - \frac{1}{2}(-1)^{|x|}\right) p_n(x) \\ &= \frac{1}{2} - \frac{1}{2}\sum_{x\in\{0,1\}^n} (-1)^{|x|}\langle 0^n|C_n^\dagger|x\rangle\langle x|C_n|0^n\rangle \\ &= \frac{1}{2} - \frac{1}{2}\sum_{x\in\{0,1\}^n} \langle 0^n|C_n^\dagger Z(1^n)|x\rangle\langle x|C_n|0^n\rangle = \frac{1}{2} - \frac{1}{2}\langle 0^n|C_n^\dagger Z(1^n)C_n|0^n\rangle, \end{aligned}$$

其中，最后一个等式是由于 $\sum_{x\in\{0,\ 1\}^n} |x\rangle\langle x| = I_n$。

这个恒等式意味着，如果 C_n 后接 f_n 可经典模拟，那么泡利期望值

$$\langle 0^n|C_n^\dagger Z(1^n)C_n|0^n\rangle$$

必须是经典可近似的。具体而言，存在一种多项式时间概率算法，能够以指数小的错误概率将该值近似到多项式小加性误差。虽然目前尚无形式化的复杂性理论困难性证明，但人们普遍认为，当 C_n 是一个一般的常数深度量子电路 [11]时，这种近似是难以实现的；Bravyi 等人证明，在特定结构假设（例如几何约束）下，相关量可以在准多项式时间甚至多项式时间内进行经典近似 [4, 3], 但这些算法关键依赖于所假设的结构，人们认为它们无法推广到一般情形。

3.2 定理 1 中 (1) $\Rightarrow$ $\Rightarrow$ (2) 的证明1

首先，我们给出概率 $p(C_n, f_m)$的一种表示，这有助于证明定理 1:

引理 1. 设 C_n 是一个任意的多项式规模量子电路，作用于 n 个量子比特，初态为 $|0^n\rangle$； f_m : $\{0,1\}^m \to \{0,1\}$ 是一个作用于 m 位的任意 *SCP*，其中 $0 < m \le n$。那么，概率 $p(C_n, f_m)$ 可以表示为

$$p(C_n, f_m) = \frac{1}{2} - \frac{1}{2}\sum_{s\in\{0,1\}^m} \widehat{g_m}(s)\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle,$$

其中，对于任意 $x \in \{0,1\}^m$，有 $g_m(x) = (-1)^{f_m(x)}$。

证明。 设 p_m 是 C_n 在 $\{0,1\}^m$ 上的输出概率分布。简单计算可得以下 $\mathbb{E}_x[g_m(x)p_m(x)]$, 的表示，这就是普朗歇尔定理 [14]:

$$\begin{aligned} \frac{1}{2^m}\sum_{x\in\{0,1\}^m} g_m(x)p_m(x) &= \frac{1}{2^m}\sum_{x\in\{0,1\}^m} \left(\sum_{s\in\{0,1\}^m} \widehat{g_m}(s)(-1)^{s\cdot x}\right)\left(\sum_{t\in\{0,1\}^m} \widehat{p_m}(t)(-1)^{t\cdot x}\right) \\ &= \frac{1}{2^m}\sum_{s,t\in\{0,1\}^m} \widehat{g_m}(s)\widehat{p_m}(t)\sum_{x\in\{0,1\}^m} (-1)^{(s+t)\cdot x} = \sum_{s\in\{0,1\}^m} \widehat{g_m}(s)\widehat{p_m}(s), \end{aligned}$$

其中 $s + t$ 是 s 与 t 模2的按位加法。因此，我们可以将 $p(C_n, f_m)$表示如下:

$$\begin{aligned} p(C_n, f_m) &= \sum_{x\in\{0,1\}^m} f_m(x)p_m(x) = \sum_{x\in\{0,1\}^m} \left(\frac{1}{2} - \frac{1}{2}(-1)^{f_m(x)}\right) p_m(x) \\ &= \frac{1}{2} - \frac{1}{2}\sum_{x\in\{0,1\}^m} g_m(x)p_m(x) = \frac{1}{2} - \frac{2^m}{2}\sum_{s\in\{0,1\}^m} \widehat{g_m}(s)\widehat{p_m}(s). \end{aligned}$$

利用恒等式 $p_m(x) = 0^n|C_n^\dagger(|xx|\otimes I_{n-m})C_n|0^n$和$\sum_{x\in\{0,1\}^m}|xx| = I_m$，对于任意 $s\in\{0,1\}^m$，我们得到 C_n 与 $\widehat{p_m}(s)$之间的如下关系，这是 [20]中所示关系的略微扩展版本：

$$\begin{aligned}\widehat{p_m}(s) &= \frac{1}{2^m}\sum_{x\in\{0,1\}^m} p_m(x)(-1)^{s\cdot x} = \frac{1}{2^m}\sum_{x\in\{0,1\}^m}\langle 0^n|C_n^\dagger(|x\rangle\langle x|\otimes I_{n-m})C_n|0^n\rangle(-1)^{s\cdot x}\\ &= \frac{1}{2^m}\sum_{x\in\{0,1\}^m}\langle 0^n|C_n^\dagger(Z(s)|x\rangle\langle x|\otimes I_{n-m})C_n|0^n\rangle = \frac{1}{2^m}\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle.\end{aligned}$$

因此，

$$p(C_n,f_m) = \frac{1}{2} - \frac{2^m}{2}\sum_{s\in\{0,1\}^m}\widehat{g_m}(s)\widehat{p_m}(s) = \frac{1}{2} - \frac{1}{2}\sum_{s\in\{0,1\}^m}\widehat{g_m}(s)\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle,$$

这就是所需的关系。 □

利用引理 1，我们证明定理 ⇒ 1 中的 (2) 如下引理所示：

引理 2. 设 C_n 是一个作用于 n 个量子比特、初态为$|0^n\rangle$的任意多项式规模量子电路，且 m 是满足 $m\le n\le \mathrm{poly}(m)$ 的任意整数。我们假设，对于任意 *SCP*f_m，C_n 后接 f_m 是可经典模拟的。那么，对于任意 $s\in\{0,1\}^m\setminus\{0^m\}$，泡利期望值

$$\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle$$

是经典可近似的。

证明。 固定任意 $s\in\{0,1\}^m\setminus\{0^m\}$。我们定义一个布尔函数 $h_m^s\colon\{0,1\}^m\to\{0,1\}$，定义如下：

$$h_m^s(x) = s\cdot x = \frac{1}{2} - \frac{1}{2}(-1)^{s\cdot x},$$

其可在多项式时间内进行可经典计算。根据该函数的表示，

$$\widehat{h_m^s}(t) = \begin{cases}\frac{1}{2} & \text{if } t = 0^m,\\ -\frac{1}{2} & \text{if } t = s,\\ 0 & \text{otherwise.}\end{cases}$$

我们可以使用以下关系进行验证：对于任意 $t\in\{0,1\}^m$，

$$\widehat{h_m^s}(t) = \frac{1}{2^m}\sum_{x\in\{0,1\}^m} h_m^s(x)(-1)^{t\cdot x} = \frac{1}{2^{m+1}}\sum_{x\in\{0,1\}^m}(-1)^{t\cdot x} - \frac{1}{2^{m+1}}\sum_{x\in\{0,1\}^m}(-1)^{(s+t)\cdot x}.$$

因此，

$$|\{t\in\{0,1\}^m \mid \widehat{h_m^s}(t)\neq 0\}| = 2,$$

这意味着 h_m^s 是稀疏的。

我们可以将 h_m^s 视为一个 SCP。根据引理 2，C_n 后接 h_m^s 是可经典模拟的，这意味着 $p(C_n, h_m^s)$ 是经典可近似的。根据引理 1，

$$p(C_n,h_m^s) = \frac{1}{2} - \frac{1}{2}\sum_{t\in\{0,1\}^m}\widehat{g_m^s}(t)\langle 0^n|C_n^\dagger(Z(t)\otimes I_{n-m})C_n|0^n\rangle,$$

其中 $g_m^s(x) = (-1)^{h_m^s(x)} = (-1)^{s\cdot x}$ 对任意 $x\in\{0,1\}^m$。由 g_m^s 的表示可知，

$$\widehat{g_m^s}(t) = \begin{cases}1 & \text{if } t = s,\\ 0 & \text{otherwise.}\end{cases}$$

我们可以利用如下关系验证这一点：对任意 $t \in \{0,1\}^m$,

$$\widehat{g_m^s}(t) = \frac{1}{2^m} \sum_{x\in\{0,1\}^m} g_m^s(x)(-1)^{t\cdot x} = \frac{1}{2^m} \sum_{x\in\{0,1\}^m} (-1)^{(s+t)\cdot x}.$$

因此,

$$p(C_n, h_m^s) = \frac{1}{2} - \frac{1}{2}\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle.$$

由于 $p(C_n,\ h_m^s)$ 是经典可近似的，泡利期望值

$$\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle$$

也可以经典近似。至此，引理的证明完成。 □

3.3 定理 ⇒ 1 中 (2) ⇒ (1) 的证明

为证明定理 ⇒ 1 中 (2) ⇒ (1)，根据引理 1，只需证明以下引理:

引理 3。 设 C_n 是一个作用于 n 个量子比特、以$|0^n\rangle$ 初始化的任意多项式规模量子电路，且 m 是满足 $m \le n \le \mathrm{poly}(m)$ 的任意整数。我们假设，对于任意 $s \in \{0,1\}^m \mid \{0^m\}$，泡利期望值

$$\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle$$

是经典可近似的。那么，对于任意 *SCP* f_m,

$$p'(C_n, f_m) = \sum_{s\in\{0,1\}^m} \widehat{g_m}(s)\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle$$

是经典可近似的，其中 $g_m(x) = (-1)^{f_m(x)}$ 对任意 $x \in \{0,1\}^m$均成立。

我们固定任意一个 SCP f_m，并考虑 $g_m(x) = (-1)^{f_m(x)}$。首先注意到，对于任意 $s \in \{0,1\}^m$，值 $\widehat{g_m}(s)$ 是经典可近似的。这是切尔诺夫–霍夫丁界的一个简单应用，可表述如下 [11]: 设 $X_1, \ldots, X_K$ 为独立同分布实值随机变量，满足 $X_j \in [-1, 1]$，且对任意 $1 \le j \le K$有 $E = \mathbb{E}X_j$。那么，对于任意多项式 $q(m)$,

$$\mathrm{Prob}\left[\left|\frac{1}{K}\sum_{j=1}^{K} X_j - E\right| \le \frac{1}{q(m)}\right] \ge 1 - 2e^{-\frac{K}{4q(m)^2}}.$$

事实上，我们固定任意一个 $s \in \{0,1\}^m$，并将 X_j 定义为如下实值随机变量

$$X_j = g_m(x)(-1)^{s\cdot x},$$

其中 $x \in \{0,1\}^m$ 是均匀随机选取的。成立的是 $X_j \in [-1, 1]$，并且

$$E = \mathbb{E}X_j = \frac{1}{2^m} \sum_{x\in\{0,1\}^m} g_m(x)(-1)^{s\cdot x} = \widehat{g_m}(s).$$

我们选取足够大的 $K = \mathrm{poly}(m)$，并对 K 个独立采样的输入 $x \in \{0,1\}^m$计算 $g_m(x)(-1)^{s\cdot x}$。根据切尔诺夫–霍夫丁界， $\widehat{g_m}(s)$可由这些值的平均值以多项式小加性误差和指数小的错误概率近似。由于 f_m 可在多项式时间内经典计算， g_m亦然。这可总结为如下引理:

引理 4. 存在一个多项式时间概率算法，对任意 $s \in \{0,1\}^m$以及多项式 $q(m)$，输出一个实数 $A(s)$，使得以大于 $1-1/\exp(m)$的概率，

$$|\widehat{g_m}(s) - A(s)| \leq \frac{1}{q(m)}.$$

注意到，由于 $m \leq n \leq \text{poly}(m)$，类似的论证表明，当分别将$q(m)$ 和 $\exp(m)$ 替换为 $q(n)$ 和 $\exp(n)$ 时，该引理仍然成立。

另一个观察是，值 $p'(C_n, f_m)$ 可以表示为多项式多个项之和。事实上，很容易证明 g_m 是稀疏的：

引理 5。 函数 g_m 是稀疏的，其中 $g_m(x) = (-1)^{f_m(x)}$ 对任意 $x \in \{0,1\}^m$.

Pro。 对于任意 $x \in \{0,1\}^m$，有 $g_m(x) = 1 - 2f_m(x)$。因此，对于任意 $s \in \{0,1\}^m$ ，

$$\begin{aligned}\widehat{g_m}(s) &= \frac{1}{2^m}\sum_{x\in\{0,1\}^m} g_m(x)(-1)^{s\cdot x} = \frac{1}{2^m}\sum_{x\in\{0,1\}^m}(1-2f_m(x))(-1)^{s\cdot x} \\ &= \frac{1}{2^m}\sum_{x\in\{0,1\}^m}(-1)^{s\cdot x} - 2\widehat{f_m}(s).\end{aligned}$$

因此，

$$\widehat{g_m}(s) = \begin{cases} 1-2\widehat{f_m}(s) & \text{if } s = 0^m, \\ -2\widehat{f_m}(s) & \text{otherwise.}\end{cases}$$

$\widehat{\ }$这意味着，对于任意 $s \in \{0,1\}^m \setminus \{0^m\}$， $\widehat{g_m}(s) \neq 0$ 当且仅当 $f_m(s) \neq 0$。由于

$$|\{s \in \{0,1\}^m \mid \widehat{f_m}(s) \neq 0\}|$$

由 m 中某个已知多项式所上界，因此

$$|\{s \in \{0,1\}^m \mid \widehat{g_m}(s) \neq 0\}|.$$

更具体地说，

$$|\{s \in \{0,1\}^m \mid \widehat{g_m}(s) \neq 0\}| \leq |\{s \in \{0,1\}^m \mid \widehat{f_m}(s) \neq 0\}| + 1,$$

这就完成了该引理的证明。 □

根据引理 5， $p'(C_n, f_m)$ 可以表示为

$$p'(C_n, f_m) = \sum_{s\in L}\widehat{g_m}(s)\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle,$$

其中

$$L = \{s \in \{0,1\}^m \mid \widehat{g_m}(s) \neq 0\}$$

并且 $|L|$由 m中的某个多项式上界，可表示为 $q_L(n)$ 因为$m \leq n \leq \text{poly}(m)$。我们注意到 $q_L(n)$ 是已知的，因为根据 SCP 的定义，用来上界 f_m 的傅里叶稀疏度的多项式是已知的，并且引理 5证明中的不等式成立。关键在于，几乎所有重要的 L 元素都可以通过使用（某个版本的）Kushilevitz-Mansour 定理高效地获得：

定理 3 ([9])**.** 存在一种多项式时间概率算法，对于任意 $h : \{0,1\}^m \to \{-1,1\}$，若其可在多项式时间内经典计算，且多项式 $\theta(m)$，则输出 $\widetilde{L}$ *puts* $L \subseteq \{0,1\}^m$，使得以大于 $1 - 1/\exp(m)$ 的概率，对于任意 $s \in \{0,1\}^m$,

- *If* $s \in \widetilde{L}$, *then* $|\widehat{h}(s)| > 1/(2\theta(m))$.

- 若 $s \notin \widetilde{L}$，则 $|\widehat{h}(s)| < 1/\theta(m)$。
- $|\widetilde{L}| < 4\theta(m)^2$。

注意，由于 $m \le n \le \mathrm{poly}(m)$，类似的论证表明，当分别用 $\theta(n)$ 和 $\exp(n)$ 替换 $\theta(m)$ 和 $\exp(m)$ 时，定理仍然成立。

在证明引理 3之前，在引理的假设下，对于任意多项式$p(n)$，我们描述一种多项式时间概率算法，它以指数小的错误概率，对 $p'(C_n, f_m)$ 进行近似，且加性误差为 $1/p(n)$：

1. 对函数 g_m 应用定理3 中的 Kushilevitz–Mansour 算法，使用阈值多项式 $\theta(n) = 3p(n)q_L(n)$，得到集合 $L \subseteq \{0,1\}^m$，其中包含 g_m的显著傅里叶系数。

2. 对每个 $s \in L$，将引理 4 中的算法应用于指标 s，使用精度多项式 $q(n) = 24p(n)\theta(n)^2$，得到 $A(s)$ 对 $\widehat{g_m}(s)$的近似值。

3. 对每个 $s \in L$，若 $s = 0^m$，则令 $B(s) = 1$。否则，对索引 3 应用引理中假设的算法 s，精度多项式取 $r(n) = 12p(n)\theta(n)^2$，得到泡利期望值 $B(s)$ 的一个近似值

$$\langle 0^n | C_n^\dagger (Z(s) \otimes I_{n-m}) C_n | 0^n \rangle.$$

4. 输出该值

$$\sum_{s \in \widetilde{L}} A(s)B(s).$$

我们如下证明引理 3，从而完成定理1的证明：

*Pro*引理 *3*的证明。 只需证明，以大于 $1 - 1/\exp(n)$ 的概率，

$$|p'(C_n, f_m) - \sum_{s \in \widetilde{L}} A(s)B(s)| \le \frac{1}{p(n)}.$$

上述算法第 1 步中得到的集合 L满足：以大于$1 - 1/\exp(n)$ 的概率，对于任意 $s \in \{0,1\}^m$，

- 若 $s \in \widetilde{L}$，则 $|\widehat{g_m}(s)| > 1/(2\theta(n))$.
- 若 $s \notin L$，则 $|\widehat{g_m}(s)| < 1/\theta(n)$。
- $|\widetilde{L}| < 4\theta(n)^2$。

此外，对于每个 $s \in L$，以大于 $1 - 1/\exp(n)$ 的概率，

$$|\widehat{g_m}(s) - A(s)| \le \frac{1}{q(n)}.$$

此外，对于每个 $s \in L$ （包括 $0^m \in L$ 的情况），以大于$1 - 1/\exp(n)$ 的概率，

$$|\langle 0^n | C_n^\dagger (Z(s) \otimes I_{n-m}) C_n | 0^n \rangle - B(s)| \le \frac{1}{r(n)}.$$

因此，以大于 $1 - 1/\exp(n)$ 的概率，上述所有关系将同时成立。接下来，我们将分析以该事件为条件的误差。

我们可以如下界定以下量:

$$\left|p'(C_n,f_m)-\sum_{s\in\widetilde{L}}A(s)B(s)\right|\le\left|p'(C_n,f_m)-\sum_{s\in\widetilde{L}}\widehat{g_m}(s)\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle\right|$$
$$+\left|\sum_{s\in\widetilde{L}}\widehat{g_m}(s)\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle-\sum_{s\in\widetilde{L}}\widehat{g_m}(s)B(s)\right|$$
$$+\left|\sum_{s\in\widetilde{L}}\widehat{g_m}(s)B(s)-\sum_{s\in\widetilde{L}}A(s)B(s)\right|.$$

上述不等式右边第一项的上界如下:

$$\left|p'(C_n,f_m)-\sum_{s\in\widetilde{L}}\widehat{g_m}(s)\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle\right|$$
$$=\left|\sum_{s\in L\setminus\widetilde{L}}\widehat{g_m}(s)\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle\right|$$
$$\le\sum_{s\in L\setminus\widetilde{L}}|\widehat{g_m}(s)||\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle|<\frac{q_L(n)}{\theta(n)}=\frac{1}{3p(n)},$$

~ ~因为对任意 $s\in L\setminus L$，有
$L\subseteq L$，$|\widehat{g_m}(s)|<1/\theta(n)$,

$$|\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle|\le 1$$

对任意 $s\in\{0,1\}^m$，以及 $|L|\le q_L(n)$。

第二项的上界如下:

$$\left|\sum_{s\in\widetilde{L}}\widehat{g_m}(s)\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle-\sum_{s\in\widetilde{L}}\widehat{g_m}(s)B(s)\right|$$
$$\le\sum_{s\in\widetilde{L}}|\widehat{g_m}(s)||\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle-B(s)|<\frac{4\theta(n)^2}{r(n)}=\frac{1}{3p(n)},$$

因为对任意 $s\in\{0,1\}^m$ 以及 $|\widetilde{L}|<4\theta(n)^2$，有 $|\widehat{g_m}(s)|\le 1$。

第三项的上界如下:

$$\left|\sum_{s\in\widetilde{L}}\widehat{g_m}(s)B(s)-\sum_{s\in\widetilde{L}}A(s)B(s)\right|\le\sum_{s\in\widetilde{L}}|\widehat{g_m}(s)-A(s)||B(s)|\le\frac{1}{q(n)}\sum_{s\in\widetilde{L}}|B(s)|$$
$$\le\frac{1}{q(n)}\sum_{s\in\widetilde{L}}\left(\left|\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle-B(s)\right|+\left|\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle\right|\right)$$
$$\le\frac{1}{q(n)}\sum_{s\in\widetilde{L}}\left(\frac{1}{r(n)}+1\right)<\frac{4\theta(n)^2}{q(n)}\left(\frac{1}{r(n)}+1\right)=\frac{1}{6p(n)}\left(\frac{1}{r(n)}+1\right)<\frac{1}{3p(n)},$$

因为不失一般性，我们可以假设 $1/r(n)<1$。因此，

$$\left|p'(C_n,f_m)-\sum_{s\in\widetilde{L}}A(s)B(s)\right|<\frac{1}{3p(n)}+\frac{1}{3p(n)}+\frac{1}{3p(n)}=\frac{1}{p(n)},$$

这就是所需的关系。 □

定理 1 的应用

4.1 CT 态和ECS 操作

我们将定理 1 应用于各种用于执行经典难题的量子电路。应用定理 1的一个关键步骤，是验证多项式规模量子电路 C_n 满足定理 1中的条件 (2)，或者更具体地说，满足对于任意 $s \in \{0,1\}^m \setminus \{0^m\}$，泡利期望值

$$\langle 0^n | C_n^\dagger (Z(s) \otimes I_{n-m}) C_n | 0^n \rangle$$

是经典可近似的。为此，我们引入计算易处理（CT）态和可高效计算的稀疏（ECS）操作 [23], ，其中我们的 ECS 概念是针对当前情形定制的受限版本。

令 $|\varphi\rangle$ 为 n 个量子比特上的任意量子态，并令p_φ 为定义在$\{0,1\}^n$ 上的概率分布，其定义为$p_\varphi(x) = |\langle x|\varphi\rangle|^2$。那么，如果满足以下两个条件， $|\varphi\rangle$ 就是 CT 态:

- 概率分布p_φ 可在多项式时间内进行经典采样。
- 对于任意 $x \in \{0,1\}^n$，内积$\langle x|\varphi\rangle$ 均可在多项式时间内经典计算。

乘积态是 CT 态的一个例子。我们指出，为简单起见，我们要求对概率分布进行采样和计算内积时达到完美精度；但其中可能涉及无理数，因此只需要求指数级精度。以下 ECS 操作的定义也采用相同的约定。

令 U 为作用于 n 个量子比特上的任意操作，且该操作既是酉的又是厄米的。若存在多项式 $s(n)$，使得对于任意 $x \in \{0,1\}^n$， $U|x\rangle$ 是至多 $s(n)$ 个计算基态的线性组合，则称 U 是稀疏的。对于稀疏操作 U （与 $s(n)$ 相关联），我们定义函数

$$\beta_j : \{0,1\}^n \to \mathbb{C},\ \gamma_j : \{0,1\}^n \to \{0,1\}^n$$

对每个 $1 \le j \le s(n)$，定义如下：对于任意 $x \in \{0,1\}^n$，考虑 U 中由 x 索引的列，并从上到下遍历该列。

- 如果第 j 个非零元素存在:
  - $\beta_j(x)$ 是该元素的值。– $\gamma_j(x)$ 是该元素的行索引。

如果第 j 个非零项不存在:

- $\beta_j(x) = 0$.
- $\gamma_j(x) = 0^n$.

若稀疏操作 U 对任意 $1 \le j \le s(n)$ 都满足函数 β_j 和 γ_j 可在多项式时间内经典计算，则称其为 ECS。特别地，具有 $s(n) = 1$ 的 ECS 操作称为高效可计算保基操作。

高效可计算保基操作保持 CT 态的类别如下:

定理4 （[23]）。设 $|\varphi\rangle$ 是 n 个量子比特上的任意 *CT* 态，且 U 是 n 个量子比特上的任意高效可计算保基操作。那么， $U|\varphi\rangle$ 是 *CT* 态。

以下定理是 [23], 中结果针对我们经典可近似性背景的专门化版本:

定理 5 ([23])。 设 U 是作用于 n 个量子比特上的任意酉操作，满足 $U|0^n\rangle$ 是 *CT*，并且 O 是满足 $||O|| \leq 1$的任意厄米操作，其中 $||O||$ 是 O的特征值绝对值的最大值。设 V 是作用于 n 个量子比特上的任意酉操作，满足 $V^\dagger OV$ 是 *ECS*。则，实数

$$\langle 0^n|U^\dagger V^\dagger OVU|0^n\rangle$$

是经典可近似的。

4.2 IQP 电路与 Simon 算法的量子部分

我们考虑作用于 n 个量子比特上的以下量子电路，这些量子比特初始化为 $|0^n\rangle$ [23]:

1. 对量子比特 Q的某个子集施加哈达玛门。2. 在 n 个量子比特上施加一个用于实现高效可计算保基操作的多项式规模量子电路 D_n 。3. 对量子比特 R的某个子集施加哈达玛门。

特殊情形 $Q = R = \{1,\ldots,n\}$ 如图 2 (a) 所示。例如，当 $Q = R =\{1,\ldots,n\}$， $m = n$和 D_n 由 Z-对角门（如 Z、 CZ和 CCZ门）组成时，该量子电路就归结为 IQP 电路。IQP 电路作为展示量子计算优势的候选方案，已得到广泛研究。此外，Simon 算法的量子部分是具有 $Q = R = \{1,\ldots,n/2\}$ 和 $m = n/2$[1]的部分。

令 C_n 为这种形式的任意多项式规模量子电路，即 $C_n = H_R D_n H_Q$，其中 H_Q 和 H_R 分别是在量子比特 Q 和量子比特 R 上的 H 门层。我们可以证明，对于任意 $s \in \{0,\ 1\}^m \mid 0^m\}$，

$$\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle = \langle 0^n|H_Q D_n^\dagger H_R(Z(s)\otimes I_{n-m})H_R D_n H_Q|0^n\rangle$$

是经典可近似的。事实上，乘积态 $H_Q|0^n\rangle$ 是一个 CT 态，因此根据定理 4， $D_n H_Q|0^n\rangle$ 也同样是一个 CT 态。此外，由于 $HZH = X$ 和 $H^2 = I$，操作 $H_R(Z(s)\otimes I_{n-m})H_R$ 可以表示为 X 和 I的张量积，这显然是一个 ECS 操作。因此，根据定理 5，泡利期望值

$$\langle 0^n|C_n^\dagger(Z(s)\otimes I_{n-m})C_n|0^n\rangle$$

是经典可近似的。因此，根据定理 1，对于任意 SCP f_m， C_n 后接 f_m 是可经典模拟的。这恢复了 Van den Nest [23]的结果。

4.3 Clifford Magic 电路

我们考虑一个作用于 n 个量子比特、初始化为 $|0^n\rangle$ [24], 的 CliffordMagic 电路。该电路被提出作为另一种展现量子计算优势的模型:

1. 对所有量子比特施加哈达玛门。

2. 对所有量子比特施加 T 门。

3. 在 n 个量子比特上应用一个多项式规模的克利福德电路 E_n ，该电路由 H 个门、 S 个门和 CZ 个门组成。

[1]严格来说，Simon 算法中的基保持操作取决于给定的预言机，因此我们需要考虑相对于该预言机的论证，但这很容易做到 [15]。

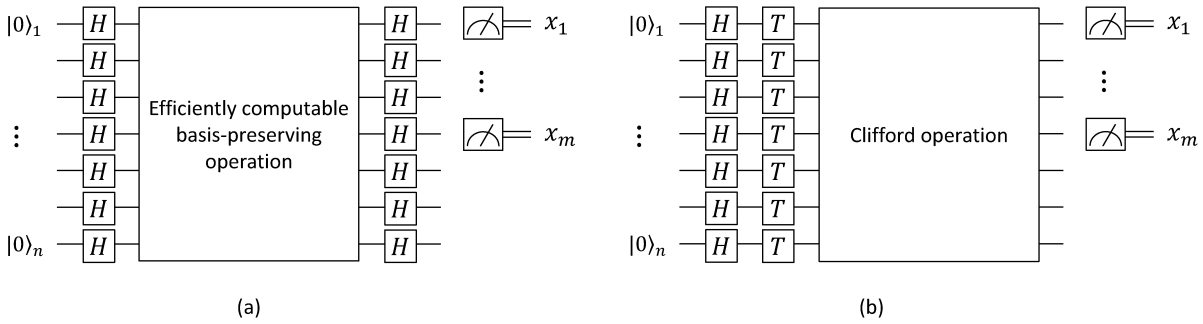


图 2：（a）夹在两个哈达玛层之间的高效可计算保基操作的量子电路。这类电路的例子包括 IQP 电路和 Simon 算法的量子部分。（b）Clifford Magic电路。

该量子电路如图2 (b) 所示，其中 m通常设为 n，讨论其输出概率分布采样的经典计算难度时即采用此设定。

设 $C_n = E_n T^{\otimes n} H^{\otimes n}$ 是任意一个多项式规模的 Clifford Magic电路。我们可以证明，对于任意 $s \in \{0,\ 1\}^m \setminus \{0^m\}$，

$$\langle 0^n | C_n^\dagger (Z(s) \otimes I_{n-m}) C_n | 0^n \rangle = \langle 0^n | H^{\otimes n} T^{\dagger \otimes n} E_n^\dagger (Z(s) \otimes I_{n-m}) E_n T^{\otimes n} H^{\otimes n} | 0^n \rangle$$

是经典可近似的。事实上，$T^{\otimes n} H^{\otimes n} |0^n\rangle$ 是一个乘积态，因此也是 CT 态。此外，由于 E_n 是一个 Clifford 电路，操作 $E_n^\dagger (Z(s) \otimes I_{n-m}) E_n$ 是一个 Pauli 操作，显然也是一种 ECS 操作。因此，根据定理 5，泡利期望值

$$\langle 0^n | C_n^\dagger (Z(s) \otimes I_{n-m}) C_n | 0^n \rangle$$

是经典可近似的。因此，根据定理 1，对于任意 SCP f_m，C_n 后接 f_m是可经典模拟的。值得注意的是，这一结果并不能直接从 Van den Nest [23], 的原始框架推出，这凸显了我们的定理 1 对涉及魔法态的量子电路具有更广泛的适用性。

5 常数深度量子电路后接 SCP

为了分析常数深度量子电路后接 SCP 的可模拟性，我们引入对易量子电路模型。作用于 n 个量子比特上的对易量子电路，是由两两对易的门构成的、作用于 n 个量子比特上的量子电路，其中每个对易门仅对常数个量子比特产生非平凡作用。若作用于 n 个量子比特上的对易量子电路中，每个对易门的支撑集至多包含 k 个量子比特，则称其为 k-局部的，其中 $k = O(1)$ [11]。

设 C_n 是一个任意的常数深度多项式规模量子电路 d，作用于 n 个初始化为 $|0^n\rangle$ 的量子比特上，并且 m 是任意一个满足 $m \le n \le \mathrm{poly}(m)$ 的整数。此外，我们固定一个任意的 SCP f_m，并考虑 $g_m(x) = (-1)^{f_m(x)}$。为证明定理 2，我们应用引理 3证明前紧接着描述的算法。更具体地说，只需~证明，对于每个 $s \in L$，泡利期望值

$$\langle 0^n | C_n^\dagger (Z(s) \otimes I_{n-m}) C_n | 0^n \rangle$$

可由一种多项式时间概率算法近似，该算法可访问满足定理2条件的对易量子电路，且具有多项式小加性误差和指数小的错误概率。由于当 $s = 0^m$时，泡利期望值为 1，因此我们将其估计值设为 1，并在下文中着重讨论 $s \neq 0^m$ 的情况。我们采用哈达玛测试来估计所需的泡利期望值。具体来说，对于任意固定的 $s \in \widetilde{L}$，我们在 $n+1$ 个初始化为 $|0^{n+1}\rangle$的量子比特上使用以下量子电路：

1. 对顶端的量子比特施加哈达玛门，并对其余 n 个量子比特施加 C_n 。

2. 对于每个带有 $1 \le j \le m$ 的 $s_j = 1$，对顶层量子比特和量子比特 j 这一对应用受控-Z 门。

3. 对顶层量子比特应用哈达玛门，并对其他 n 个量子比特应用 $C_n^\dagger$ 。

包含 $m = n$ 和 $s = 1^n$ 的量子电路如图 3左侧所示。哈达玛测试的量子电路与泡利期望值的关系如下：

引理 6。 在步骤 *3* 之后，对哈达玛测试量子电路的顶层量子比特在 Z 基下进行测量，得到 0 的概率为

$$\mathrm{Prob}(0) = \frac{1 + \langle 0^n | C_n^\dagger (Z(s) \otimes I_{n-m}) C_n | 0^n \rangle}{2}.$$

证明。B 由上述描述的作用于 $n+1$ 个量子比特的量子电路，我们得到如下状态 e:

$$\begin{aligned}
|0^{n+1}\rangle &\mapsto \frac{1}{\sqrt{2}}|0\rangle \otimes C_n|0^n\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes C_n|0^n\rangle \\
&\mapsto \frac{1}{\sqrt{2}}|0\rangle \otimes C_n|0^n\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes (Z(s) \otimes I_{n-m}) C_n|0^n\rangle \\
&\mapsto \frac{1}{\sqrt{2}}|0\rangle \otimes \frac{I + C_n^\dagger (Z(s) \otimes I_{n-m}) C_n}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes \frac{I - C_n^\dagger (Z(s) \otimes I_{n-m}) C_n}{\sqrt{2}}|0^n\rangle,
\end{aligned}$$

其中每个箭头对应一个步骤。因此，

$$\begin{aligned}
\mathrm{Prob}(0) &= \frac{1}{4}\langle 0^n | (I + C_n^\dagger (Z(s) \otimes I_{n-m}) C_n)(I + C_n^\dagger (Z(s) \otimes I_{n-m}) C_n) | 0^n \rangle \\
&= \frac{1 + \langle 0^n | C_n^\dagger (Z(s) \otimes I_{n-m}) C_n | 0^n \rangle}{2},
\end{aligned}$$

这就是所需的关系。 □

利用该引理，我们可以如下证明定理 2：

定理 *2*的证明。 令 X 为引理6中定义的、作为测量经典测量结果的实值随机变量。于是，

$$\mathbb{E}[X] = \frac{1 - \langle 0^n | C_n^\dagger (Z(s) \otimes I_{n-m}) C_n | 0^n \rangle}{2},$$

这就是获得 1 的概率。因此，根据第3.3节所述的切尔诺夫–霍夫丁界，存在一种可访问上述量子电路的多项式时间概率算法，能够近似所需的值

$$\langle 0^n | C_n^\dagger (Z(s) \otimes I_{n-m}) C_n | 0^n \rangle$$

并具有多项式小加性误差，且错误概率为指数小的错误概率 .

现在，我们将上述作用于 $n+1$ 个量子比特的哈达玛测试量子电路转化为作用于 $n+1$ 个量子比特的对易量子电路，同时不影响输出概率分布。按照 [11]，的方法，这可以通过利用以下关系来实现

$$C_n^\dagger (Z(s) \otimes I_{n-m}) C_n = \prod_{1 \le j \le m : s_j = 1} (C_n^\dagger (Z_j \otimes I_{n-m}) C_n).$$

所得的对易量子电路，其组成包括 $m = n$ 和 $s = 1^n$ ，如图3右侧所示。事实上，对于任意 $1 \le j \le m$ 满足 $s_j = 1$的

$$(H \otimes C_n^\dagger)(CZ_j \otimes I_{n-m})(H \otimes C_n)$$

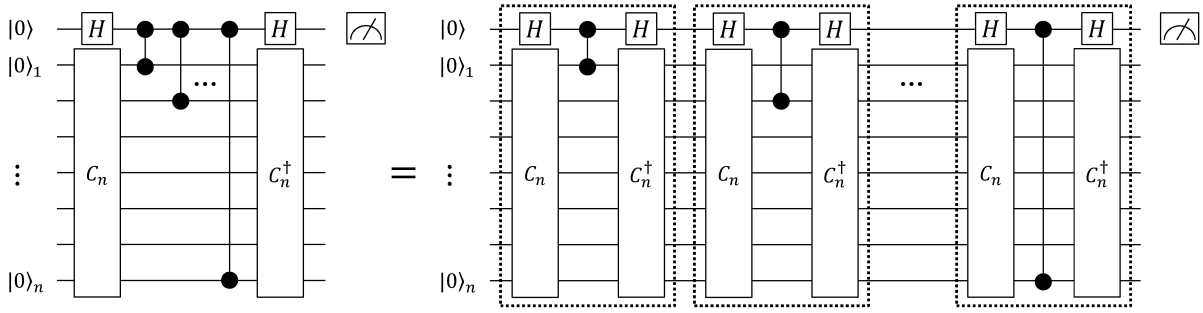


图 3：用于近似$\langle 0^n|C_n^\dagger Z(1^n)C_n|0^n\rangle$的量子电路。等式右侧是一个对易量子电路，其输出概率分布与左侧相同。

将其视为一个门，其中 CZ_j 表示作用于顶端量子比特和量子比特 j上的受控-Z_j 门。该对易量子电路中的对易门数量为 $|s|$，其上界为deg(g_m)。由于 $g_m(x) = 1 - 2f_m(x)$且 f_m 是一个非零函数，因此deg(g_m) = deg(f_m)。此外，每个对易门作用的量子比特数量至多为

$$1 + \max\{|\mathrm{supp}(C_n^\dagger(Z_j \otimes I_{n-m})C_n)| \mid 1 \le j \le m\}.$$

定理2的证明至此完成。 □

6 结论与未来工作

我们研究了多项式规模量子电路 C_n 后接 SCPf_m 的经典可模拟性，其中 $m \le n \le$ poly(m)。我们的首要贡献是给出了关于 C_n 的一个充要条件，确保对于任意 SCP f_m，C_n 后接 f_m 都可经典模拟。该刻画重现了 Van den Nest 的结果，并同样适用于 IQP 电路和 Clifford Magic 电路，而后者此前尚未得到研究。

随后，我们考虑了 C_n 具有常数深度的情形。尽管对于任意 SCP f_m，C_n 后接 f_m 都可经典模拟的可能性不大，但我们证明，只要能够使用作用于 $n+1$ 个量子比特的对易量子电路，就可以通过多项式时间概率算法实现模拟。我们还通过将所需对易门的数量及其局部性分别界定为 deg(f_m) 和 $|\mathrm{supp}(C_n^\dagger(Z_j \otimes I_{n-m})C_n)|$ 的函数，进一步量化了所需的量子资源。这有助于更精细地理解对常数深度量子电路后接 SCP 进行模拟的难度。

我们的结果表明，未来研究有几个值得探索的方向。

- **超越傅里叶稀疏度**。SCP 是通过傅里叶稀疏度定义的，但进一步探究我们的技术能否推广到更广泛的后处理函数类别，将是很自然的方向，例如具有准多项式傅里叶稀疏性或近似稀疏性的函数。要理解能够保持经典可模拟性的后处理的确切边界，仍是一项尚待解决的挑战。

- **常数深度量子电路的更精确界**。对于常数深度量子电路，值得探究定理 2中使用的对易量子电路是否已达到最优，或者能否为所需的量子资源建立更紧的上界或下界。具体而言，理解此类对易量子电路所需的最小局部性或深度，或许能为可模拟性层级带来更细致的划分。

- **对易量子电路的计算能力**。 我们的分析凸显了对易量子电路作为模拟原语的用途。进一步探索

其计算能力——尤其是与非对易扩展、Clifford对易电路或受限门集的关系——或可为理解量子优势的结构带来新的见解 [11, 21]。

- **函数稀疏性与分布稀疏性**。 我们的工作关注傅里叶稀疏意义上的函数稀疏性，而 Schwarz 等人 [15] 研究了分布稀疏性，即输出分布中只有多项式数量的结果具有非可忽略的概率。阐明这两种概念之间的关系，或许有助于统一理解量子电路何时能够进行高效经典模拟。

- **其他量子电路族**。 研究其他被认为能够执行经典难题的量子电路族的经典可模拟性也很有价值，例如共轭Clifford电路 [2]。将我们的框架应用于这些模型，或许能揭示新的结构性质或出乎意料的可模拟区域。

总而言之，我们的研究成果有助于推进更广泛的研究计划，即理解量子计算与经典计算之间的边界。我们希望这些成果能够推动人们进一步探究量子电路结构、经典后处理与经典可模拟性之间的相互作用。

致谢

本研究得到日本 JST K计划资助，资助编号为 JPMJKP24U2，Japa n.

参考文献

[1] A. Anshu、Y. Dong、F. Ou 和 P. Yao。论仅使用略超线性辅助量子比特的 QAC^0 计算能力。载于第*57*届 *ACM* 理论计算机研讨会（*STOC*）论文集，第 1476–1487 页，2025年。[2] A. Bouland、J. F. Fitzsimons 和 D. E. Koh。共轭Clifford电路的复杂性分类。载于第*33*届计算复杂性会议（*CCC*）论文集，第 102 卷，莱布尼茨国际信息学会议论文集，第 21:1–21:25 页，2018年。[3] S. Bravyi、D. Gosset 和 Y. Liu。尖峰浅层量子电路的经典模拟。载于第*56*届 *ACM* 理论计算机研讨会（*STOC*）论文集，第 561–573 页，2024年。[4] S. Bravyi、D. Gosset 和 R. Movassagh。量子均值的经典算法。自然物理，17(3):337–341，2021年。[5] S. Bravyi、G. Smith 和 J. A. Smolin。经典与量子计算资源的权衡。物理评论 *X*，6(2):021043，2016年。[6] S. Fenner、F. Green、S. Homer 和 Y. Zhang。常数深度量子电路能力的界限。载于计算理论基础会议（*FCT*）论文集，第 3623 卷，计算机科学讲义，第 44–55 页，2005年。[7] S. Ghosh、S. Subramanian 和 W. Zhan。针对浅层量子电路的无条件伪随机性。载于第*17*届理论计算机科学创新会议（*ITCS*）论文集，第 362 卷，莱布尼茨国际信息学会议论文集，第 70:1–70:25 页，2026年。[8] A. W. Harrow 和 A. Montanaro。量子计算优越性。自然，549:203–209，2017年。

[9] E. Kushilevitz 和 Y. Mansour。利用傅里叶谱学习决策树。*SIAM*计算杂志，22(6):1331–1348，1993年。[10] A. Montanaro。量子算法：概述。*npj*量子信息，2(15023):1–8，2016年。[11] X. Ni 和 M. van den Nest。对易量子电路：高效经典模拟与困难性结果。量子信息与计算，13(1&2):54–72，2013年。[12] M. A. Nielsen 和 I. L. Chuang。量子计算与量子信息。剑桥大学出版社，2000年。[13] H. Nishimura 和 M. Ozawa。一致量子电路族与量子图灵机的计算复杂性。理论计算机科学，276(1–2):147–181，2002年。[14] R. O'Donnell。布尔函数分析。剑桥大学出版社，2014年。[15] M. Schwarz 和 M. van den Nest。模拟具有稀疏输出分布的量子电路，2013年。arXiv:1310.6749。[16] D. J. Shepherd 和 M. J. Bremner。时间无序量子计算。英国皇家学会会刊 *A* 辑，465(2105):1413–1439，2009年。[17] P. W. Shor。量子计算机上的素数分解与离散对数多项式时间算法。*SIAM*计算杂志，26(5):1484–1509，1997年。[18] D. R. Simon。论量子计算的能力。*SIAM*计算杂志，26(5):1474–1483，1997年。[19] J. Slote。奇偶性与 AC^0 ：简单量子预处理。载于第*15*届理论计算机科学创新会议（*ITCS*）论文集，第 287 卷，莱布尼茨国际信息学会议论文集，第 92:1–92:21 页，2024年。[20] Y. Takahashi、Y. Takeuchi 和 S. Tani。局部退极化噪声下量子电路的经典模拟。理论计算机科学，893:117–132，2021年。[21] Y. Takahashi、S. Tani、T. Yamazaki 和 K. Tanaka。少量输出的对易量子电路不太可能可经典模拟。量子信息与计算，16(3&4):251–270，2016年。[22] Y. Takahashi、T. Yamazaki 和 K. Tanaka。具有无界 Toffoli 门和扇出门的量子电路经典模拟的困难性。量子信息与计算，14(13&14):1149–1164，2014年。[23] M. van den Nest。用概率方法模拟量子计算机。量子信息与计算，11(9&10):784–812，2011年。[24] M. Yoganathan、R. Jozsa 和 S. Strelchuk。带魔态输入的酉克利福德电路的量子优势。英国皇家学会会刊 *A* 辑，475(2225):1–19，2019年。