arXiv:2601.03243v1 [cs.CC] 6 Jan 2026

QAC^0 包含 TC^0 （含有多个输入副本）

Daniel Grier* Jackson Morris† Kewen Wu‡

摘要

QAC^0 是由任意单量子比特门和广义托福利门构成的常数深度多项式规模量子电路类。可以说，它是尚未被证明能用于计算任何非平凡布尔函数的最小自然常数深度量子计算类。尽管如此，将经典 AC^0 下界移植到 QAC^0 的许多尝试都以失败告终。

我们对此给出一种可能的解释：QAC^0 电路比其经典对应物强大得多。我们证明，对于判定问题，$QAC^0 \not\subset$ 与 $AC^0[p]$ 之间存在无条件分离，这也首次解决了 AC^0 是否可能比 QAC^0更强这一问题。此外，我们证明，如果提供多个输入副本，QAC^0 电路就能计算范围广泛的布尔函数：$TC^0 \subseteq QAC^0 \circ NC^0$。在此过程中，我们引入了一种振幅放大技术，使若干近似常数深度构造变为精确构造。

目录

1 引言 3 1.1 技术概述 .5 1.2 未来方向 .7

2 预备知识 8

3 精确振幅放大 11 3.1 多对数权重阈值函数 .12 3.2 AC^0 中的对称函数.13

4 QAC 中的态-酉对偶性 14
4.1 $|W\rangle$ 态与汉明重量测试 .14 4.2 区分 QAC^0 与经典复杂度类 .16

A 第3节缺失的证明 21

B 索引需要较大的经典扇出 22

*加州大学圣迭戈分校。电子邮件：dgrier@ucsd.edu

†加州大学圣迭戈分校。电子邮件：jrm035@ucsd.edu

‡高等研究院。电子邮件：shlw kevin@hotmail.com.

C 朝着更优的副本复杂度迈进23C.1 截断并行重复.23C.2 概率计算.26

1 引言

常数深度量子电路长期以来一直在帮助我们理解量子计算机如何相较于经典计算机获得优势方面发挥着核心作用。事实上，即使是完全由单量子比特门和双量子比特门构成的常数深度电路，也已被证明能够在各种采样和搜索任务中胜过经典电路 [BGK18，WKST19，GS20，WP23，KOW24，GKM+25]。然而，一旦我们考虑判定问题（其目标是计算布尔函数的一个输出位），情况就会发生巨大变化。这类常数深度量子电路的光锥较小，显著限制了其行为，使其能力不超过常数深度经典电路。这一现象体现为复杂性类等式 $\mathsf{QNC}^0 = \mathsf{NC}^0$。

换言之，要展现常数深度量子电路在计算布尔函数方面的威力，量子电路必须能够使用可同时作用于多个量子比特的大型纠缠门。常数深度多项式规模量子电路中，一个尤为重要的类是 QAC^0, ，在该类中，电路可以施加任意单量子比特门以及广义托福利门（即可逆的 n 位与门函数）。QAC^0 作为一种可能适用于近期量子硬件的可行模型，近来备受关注 [WSM01], ；此外，作为著名经典电路类AC^0的自然对应类，它也有着悠久的研究历史。尽管人们早已知道AC^0的计算能力相当有限，但要证明QAC^0的能力存在局限，则要困难得多。

这种差异最著名、最能说明问题的例子，或许就是奇偶函数。尽管有多种方法可以证明奇偶函数无法由AC^0,QAC^0 在量子领域中，尽管研究者长期试图证明同样的结果，这一结论依然屹立不倒[FFG+06，PFGT25，Ros21，NPVY24，ADOY24，Ber11，JTVW25]计算。关键在于，那些在经典领域中证明下界的技术，例如随机限制 [Ajt83，FSS84，H˚as86]或傅里叶集中 [LMN93], ，都未能移植到量子领域（至少在不限制辅助量子比特使用的情况下如此）。当然，对这一现象的一种可能解释是，QAC^0 的能力确实远超先前的假设。

有鉴于此，自然会去寻找能够体现这种能力的QAC^0 电路。直到最近，这种研究思路受到的关注还相对较少。Rosenthal 给出了第一个非平凡的常数深度QAC 电路[1] 构造 [Ros21]：该构造利用指数规模的广义托福利门，在常数深度下近似计算奇偶性和量子扇出[2] 门。最近，研究者证明弱伪随机酉算子可以用QAC^0 电路 [FPVY25]实现。这一构造的一个组成部分，是将Ros21] 中的指数规模电路缩减为多项式规模的QAC^0电路，以便在对数多个量子比特上实现扇出。本文也将采用这一技术。尽管如此，我们尚不清楚如何将这一构造扩展到更多量子比特上的扇出。缺乏大规模扇出，可能会成为某些电路构造技术的障碍。例如，可以证明，经典AC^0 电路若要计算索引函数等相对简单的布尔函数，也必须具备大规模扇出（证明见第B节）。

鉴于此，寻找能够利用广义托福利门构造、以计算非平凡布尔函数的内在量子原语是很自然的。这一搜索正是

[1]我们将使用 QAC 指代由单量子比特门和广义托福利门组成的量子电路。也就是说，QAC^0 是由常数深度且具有多项式规模的 QAC 电路构成的类。[2]量子扇出在经典基态上的操作如下： $|b,\ x_1,\ \ldots\ldots,\ x_n\rangle \mapsto |b,\ x_1 \oplus b,\ \ldots\ldots,\ x_n \oplus b\rangle$。

我们工作的重点。具体而言，我们给出了一个判定问题，它可以由 QAC^0 电路求解，但需要规模呈指数增长的 $\mathsf{AC}^0[p]$ 电路。

定理 1 (另见定理 24)。 存在一种语言 L，它可以由具有完美完备性和可靠性 $2^{-\mathsf{poly}(n)}$、输入规模为 n的 QAC^0电路判定。然而， L 对于所有素数 $p > 1$，都需要规模为 $2^{\mathsf{poly}(n)}$ 的 $AC^0[p]$ 电路。因此，$\mathsf{BQAC}^0 \not\subset$与 $\mathsf{AC}^0[p]$是分离的。

我们注意到，$\mathsf{AC}^0[p]$ 严格包含AC^0 [Ajt83、FSS84、H°与86], ，因此定理 1 立即推出了新的分离结果：$\mathsf{QAC}^0 \not\subset$ 与 AC^0。换言之，在我们的结果出现之前，人们可以设想AC^0 在解决判定问题时，比QAC^0 更强大。我们推翻了这种可能性，证明常数深度量子电路即使没有大扇出，也能实现难以计算的布尔函数。

事实证明，定理 1 源于QAC^0 电路一个或许更令人惊讶的性质。具体而言，我们证明，向 QAC^0 电路提供多项式数量的输入字符串副本后，它们便能够模拟任意 TC^0 计算。[3]

定理 2 (另见定理 21)。 任何 TC^0可计算函数，都可以通过 QAC^0 在有界误差下，使用多项式数量的输入副本进行判定。等价地，$\mathsf{TC}^0 \subseteq \mathsf{BQAC}^0 \circ \mathsf{NC}^0$。

定理 1 给出了一个分离 QAC^0 电路与 $\mathsf{AC}^0[p]$电路的语言确实存在的结论，而定理 2 则表明，这种分离源于QAC^0 具有普遍的强大计算能力。例如，由于 TC^0 电路能够将 n位整数相乘， [HAB02], 那么 QAC^0 电路也能做到（至少在提供多个输入副本时）。这回答了多个经典副本是否能让 QAC^0 计算非平凡布尔函数这一问题；该问题由 Rosenthal 在其学位论文 [Ros23]中提出。

导出上述两个定理的电路构造依赖于两个关键的基本方法：“用于汉明重量检测的 W 检验”（见第 1.1 节）和“精确振幅放大”。后一种方法使我们能够立即消除此前若干个常数深度构造中存在的近似误差：

推论 3 (另见推论 8)。 奇偶性可以由常数深度、指数规模的 QAC 电路精确计算。

推论 4 (另见推论 9)。 奇偶性可以由常数深度、多项式规模的 QTC 电路精确计算。因此，$\mathsf{QTC}^0 = \mathsf{QNC}^0_{\mathrm{wf}} = \mathsf{QAC}^0_{\mathrm{wf}}$。

推论 3 和推论 4 分别解决了 [Ros23] 和 [GM24] 提出的未决问题。事实上，精确振幅放大还使我们能够改进 [ADOY24] 的一种构造，从而在QAC^0中制备具有长程纠缠的良态。特别地，令

$$|W\rangle = \frac{1}{\sqrt{n}} \sum_{|x|=1} |x\rangle$$

为汉明重量恰好为一的 n 位比特串的均匀叠加态 .

定理 5 （另见定理 17）。 存在一个 QAC^0 电路 U使得 $U|0^n\rangle|0^a\rangle = |W\rangle|0^a\rangle$其中 $a =$ 多项式(n)。

[3]回顾一下，TC^0 是指可由常数深度、多项式规模阈值电路计算的语言集合。 TC^0 严格包含$\mathsf{AC}^0[p]$ [Raz87，Smo87]。

1.1 技术概述

我们概述所采用的技术。

该 W 测试。 定理 1 和定理 2背后的主要技术工具是一种量子原语，我们称之为 W 测试。

用于检测汉明重量 $n/2$ 的 W 测试。	
所需：	用于制备 $\|W\rangle$ 态的酉算子 U： $U\|0^n\rangle = \|W\rangle$（省略辅助量子比特）
目标：	对于输入 $x \in \{0,1\}^n$，计算 $\mathsf{EX}^{n/2}(x)$，即检查 $\|x\| = n/2$ 是否成立。
误差：	如果 $\|x\| = n/2$，则必然接受。 如果 $\|x\| \neq n/2$，则以概率 $1/n^2$ 拒绝。

粗略地说，该 W 测试利用 W 态制备酉算子，以“弱”的方式计算精确函数$\mathsf{EX}^{n/2}$；当且仅当输入的汉明重量恰好为 $n/2$时，该函数的值为 1。具体而言，若U 是某个 n量子比特酉算子，用于制备 $|W\rangle$ 态（稍后我们会回到这一态制备任务），那么 W 测试会在常数深度内使用 U 及其逆算子，如下方图1 所示。

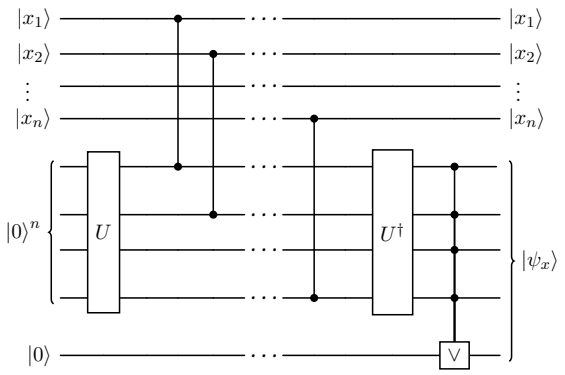


图 1： W 测试电路弱计算 $\mathsf{EX}^{n/2}$，其中上方第二层中的双量子比特门是受控 Z门。

图 1 中的电路实际上与 Moore 的构造相同 [Moo99] 不过在我们的情形中U 制备的是 $|W\rangle$ 态，而不是猫态。Moore 的电路表明，猫态与奇偶函数互为对偶：猫态可以用于以较低开销计算奇偶性，反之亦然。尽管只是近似的， W 测试表明，类似的对偶关系也存在于 $|W\rangle$ 与$\mathsf{EX}^{n/2}$ 函数之间。

对 该 W 测试的分析是一个直接的计算（形式化证明见引理 18 ）：

$$|\psi_x\rangle = \frac{n-2|x|}{n}|0^n\rangle|0\rangle + \sqrt{1-\left(\frac{n-2|x|}{n}\right)^2}|*_x\rangle|1\rangle,$$

其中， $|*_x\rangle$ 是一个依赖于 x的归一化态。这立即意味着，对于 $|x| = n/2$， $|\psi_x\rangle$ 的最后一个量子比特始终为 $|1\rangle$；而如果 $|x| \neq n/2$，则测量 $|\psi_x\rangle$ 的最后一个量子比特得到 $|0\rangle$ 的概率至少为 $1/n^2$。

量子-经典分离。 为了证明定理1和定理2，我们注意到 W 测试的一个重要特性：单边错误。事实上，如果 $\mathsf{EX}^{n/2}(x) = 1$，那么 W 测试始终正确；否则 $\mathsf{EX}^{n/2}(x) = 0$，且其正确概率至少为 $1/n^2$。这意味着我们可以使用 与门 函数（值得注意的是，它属于 QAC^0），而不是使用多数函数（目前尚不清楚多数函数是否属于 QAC^0）。

更正式地说，取 与门 作用于 $c \approx n^2$ 个并行运行的 W 测试。如果 $\mathsf{EX}^{n/2}(x) = 1$，那么 与门 结果始终为 1；否则结果以概率 0.99 为 0。这几乎就是 定理 1 的证明，因为 $\mathsf{EX}^{n/2}$ 不属于 $\mathsf{AC}^0[p]$ [Raz87，而 Smo87]。

这里需要注意的是，c 个并行运行的 W 测试需要 c输入的不相交副本（关于如何通过部分进展绕过这一点，参见第 C 节），而且目前尚不清楚如何在 QAC^0中制作这么多输入副本。幸运的是，为了证明分离结果，我们不必拘泥于普通的$\mathsf{EX}^{n/2}$ 函数。我们可以使用一个变体。具体来说，我们将 c-copy 版本的 $\mathsf{EX}^{n/2}$ 定义为$\mathsf{CopyEX}^{n/2}$：$\{0,1\}^{n\times c} \to \{0,1\}$:

$$\mathsf{CopyEX}_{n/2}(X_1,\ldots,X_c) = \begin{cases} \mathsf{EX}_{n/2}(X_1) & X_1 = \cdots = X_c, \\ 0 & \text{otherwise}, \end{cases} \quad \text{for every } X_1,\ldots,X_c \in \{0,1\}^n.$$

使用 $\mathsf{CopyEX}^{n/2}$ 有两方面的好处。

- 关于经典下界，$\mathsf{AC}^0[p]$ 电路可以自由复制输入，因为允许使用无界扇出。因此，$\mathsf{CopyEX}_{n/2} \notin \mathsf{AC}^0[p]$由已知的下界 $\mathsf{EX}_{n/2} \notin \mathsf{AC}^0[p]$立即得到。

- 关于量子上界，QAC^0 电路现在可以使用所 c提供的输入副本并行执行 W 测试。此外，对于所有 n 坐标，均可使用广义托福利门并行检查输入副本之间的一致性。这意味着 $\mathsf{CopyEX}^{n/2} \in \mathsf{QAC}^0$。

定理 1 的证明至此完成。对于定理 2，只需说明如何在给定输入字符串的多个副本时，使用 QAC^0 电路计算所有阈值函数。这是一个标准的填充论证，将阈值函数归约为$\mathsf{EX}^{n/2}$，然后使用 $\mathsf{CopyEX}^{n/2}$的电路。详见第 4.2节。

精确制备 $|W\rangle$ 与 Nekomata。 现在我们回到 $|W\rangle$态的构造（定理 5），这是图 1 以及上述分离所要求的。为了使用 $|W\rangle$ 和 QAC^0 电路精确制备 $|W\rangle$，我们依赖于 精确振幅放大 [Gro98、BHMT02]。一般而言，振幅放大无法在常数深度下执行 [Zal99]。这里考虑的受限情形包括：(1) 一个非平凡地近似目标态的“热启动”态；(2) 一种“标记”目标态的方法。随后可以执行标准振幅放大，以获得精确的目标态（更多细节见定理 7）。尽管该技术此前已在量子态制备任务中得到研究 [GKW24、Ros24], ，但尚未应用于 QAC^0 电路的研究。

对于 $|W\rangle$ 态，“热启动”态最终是乘积态 $(\delta|1\rangle + \sqrt{1-\delta^2}|0\rangle)^{\otimes n}$其中 $\delta \approx 1/\sqrt{n}$。 此外，“标记”过程对应于计算精确阈值函数 EX_1，以筛除汉明重量恰好为一的字符串。需要指出的是，此时显然并不 容易看出如何计算 EX_1，我们稍后会对此进行讨论。

除了 $|W\rangle$ 态之外，上述协议还将 nekomata 态的若干近似构造精确化。*nekomata* 态是对常数深度电路具有重要意义的一族量子态[GHMP02、Ros21]。量子态 $|\psi\rangle$ 是 nekomata 态，当且仅当 $|\psi\rangle = \frac{1}{\sqrt{2}}|0^n\rangle|\phi_0\rangle + \frac{1}{\sqrt{2}}|1^n\rangle|\phi_1\rangle$ 存在某些归一化态 $|\phi_0\rangle$ 和 $|\phi_1\rangle$。要得到精确的 nekomata 态，“热启动”态颇为复杂，但幸运的是，[Ros23、GM24]提供了这些态；而“标记”过程最终只需通过简单的 QAC^0 筛选全零 $|0^n\rangle$ 和全一 $|1^n\rangle$ 字符串。详情请参见第 3 节。

在 QAC^0 中进行精确计算。 已知，计算奇偶函数和实现量子扇出等价于构造猫又态 [Ros23、GM24]。因此，上述猫又态的精确制备可以实现对奇偶函数的精确计算。在QAC^0, 的背景下，这证明了推论 3；而在 QTC^0,的背景下，这证明了推论 4。

通过缩小推论3 中的构造，并利用奇偶性与扇出的等价关系，可以用常数深度的多对数(n)-规模多项式(n)-规模的QAC电路合成规模为 QAC^0 可以据此精确模拟扇出为多对数的 AC^0 电路。事实上，我们证明了QAC^0能够计算更丰富的一类布尔函数。

定理 6 （另见推论 16）。每个 AC^0 中的对称函数都可以在QAC^0中精确计算。

回顾一下，精确制备 $|W\rangle$ 态要求在EX_1 中计算该函数QAC^0。由于EX_1 是AC^0, 中的对称函数，这由定理 6即可推出。我们强调，在我们的工作之前，甚至没人知道EX_1 能否在QAC^0中近似计算；定理 6肯定地回答了 Rosenthal 提出的一个开放问题 [Ros23] 。

定理 6 的证明依赖于 H˚astad、Wegner、Wurm 和 Yi [HWWY94]关于用极少线路计算对称 AC^0 函数的经典结果。我们注意到，他们的构造可以用多对数(n)-规模的扇出来实现（这可由推论3的缩减版本推出），并且可以用多对数(n)-位对称函数实现（这可由$\mathsf{QNC}^0_{\mathrm{wf}}$ 构造推出，参见 [H˘S05、TT16]）。详情请见第3.2节。

1.2 未来方向

我们证明，拥有多项式数量的输入经典副本，就能使QAC^0 计算超越$\mathsf{AC}^0[p]$的高度非平凡布尔函数。一个值得探讨的问题是，实际需要的副本数量能否得到更精确的刻画。事实上，如果这种“副本复杂度”能够降至多对数(n)，那么$\mathsf{QAC}^0 = \mathsf{QAC}^0_{\mathrm{wf}}$。围绕这一问题，我们在第C节取得了一些初步进展。具体而言，我们证明，QAC^0 电路可以用 $O(n^{3/2})$个输入副本计算奇偶性；更一般地，可以用 $O(n^2)$个副本计算任意对称函数。

关于我们在定理1中实现的分离，一个自然的问题是，能否将可靠性从指数倒数降至零。这将导致精确QAC^0 与$\mathsf{AC}^0[p]$之间的分离。此前，这类判定问题被称为EQAC^0 [GHMP02]。另一个自然的问题是，能否在QAC^0 中找到一个全函数，使其在平均情况下难以被$\mathsf{AC}^0[p]$ 电路计算。请注意，由于$\mathsf{CopyEX}^{n/2}$的分块性质，随机输入串以很高的概率是否定实例；因此，该函数与常零函数具有很高的相关性。

本文介绍的技术似乎没有直接回答$\mathsf{AC}^0 \subset \mathsf{QAC}^0$的问题。定理 6 或许可以视为取得了一些进展；然而，简单的 AC^0 函数

迄今开发的基本构件似乎仍无法实现需要大扇出的函数，例如索引函数。

另一个有趣的问题是，如何使用有限门集重现我们的结果。请注意， [GM24] 的近似 nekomata 构造只使用 Hadamard 门和布尔函数门，而我们的方法则严重依赖精确振幅放大；要实现这一点，似乎需要任意单量子比特门。

最后，我们回顾一下 Moore 在其开创性工作中留下的未解问题 [Moo99]:

(1) $\mathrm{QAC}^0 =$ 是否等于 $\mathrm{QAC}^0_{\mathrm{wf}}$? (2) 对任意素数 $p > 1$, $\mathrm{QAC}^0[p] =$ 是否等于 QACC^0？ (3) $\mathrm{QAC}^0_{\mathrm{wf}} =$ 是否等于 QTC^0?

对于上述问题，Moore 评论道:

> 我们猜想 所有这些问题的答案都是“否”，但量子电路可能会带来意想不到的结果

在 [GHMP02], 中，研究表明，问题 (2) 的答案实际上是“是”。我们的推论4基于 [GM24], 表明 (3) 也成立。尽管 (1) 仍未解决，但我们相信，我们的分离与模拟结果（定理1 和定理2）进一步展现了量子电路可能令人惊讶的其他方式，这也暗示 (1) 的答案或许也是“是”。

2 预备知识

对于每个整数 $n \geq 1$，我们用 $[n]$ 表示集合 $\{1, 2, \ldots, n\}$。对于每个二进制字符串 $x \in \{0,1\}^n$，我们用 $|x| = x_1 + \cdots + x_n$ 表示其汉明重量。对于长度相同的二进制字符串 x， y，我们用 $x \oplus y$ 表示它们逐位异或所得的二进制字符串。我们用 $1_{\mathcal{E}}$ 表示事件 $\mathcal{E}$的示性函数，即若 $\mathcal{E}$ 发生则为 $1_{\mathcal{E}} = 1$ ，否则为 $1_{\mathcal{E}} = 0$ 。我们用 $\mathbb{I}_n$ 表示作用于 n个量子比特上的单位矩阵。

对称布尔函数。 我们使用术语“布尔函数”时，仅指多对一函数。对于布尔函数 f: $\{0,1\}^n \to \{0,1\}$，如果 $f(x)$ 仅取决于 $|x|$，我们就称 f 为对称函数。

对于整数 $k \geq 0$，我们用 EX_k 表示汉明重量为 k 的精确阈值函数，定义为 $\mathrm{EX}_k(x) = 1_{|x|=k}$; 用 $\mathrm{Th}_{\geq k}$ 表示汉明重量为 k 的阈值函数，定义为 $\mathrm{Th}_{\geq k}(x) = 1_{|x|\geq k}$。

对于每个整数 $m \geq 2$，我们定义 MOD_m: $\{0,1\}^n \to \{0,1\}$ ，其定义为 $\mathrm{MOD}_m(x) = 1_{|x| \equiv 1 \,(\text{模}\ m)}$。我们还用 $\mathrm{Parity} = \mathrm{MOD}_2$ 专指奇偶函数，有时使用 Parity_n 来强调输入长度为 n。

经典电路复杂性。 在布尔电路中，每个门都会对输入线上的信号计算某个布尔函数，并通过输出线传递计算结果。对于布尔电路，

- 深度是从输入位到输出的最大长度，规模是门的总数;
- 扇入 是每个门的输入线最大数量，扇出 是每个门的输出线最大数量，而门集 是不同门的集合。

我们用 $\neg$ 表示非门；用 AND（分别用 OR）表示与门（分别表示或门）/函数。有时我们用 AND_n、OR_n 来强调该函数接受 n 位输入；省略这一信息时，具体含义可从上下文中明确。

我们将用到以下标准经典电路类。这里给出非正式描述，并请读者参阅教科书 [AB09，J$^+$12]以了解形式化定义。

- NC^0 是指能够由门集为 $\{\neg$,与门、或$\}$的常深度常扇入布尔电路精确判定的语言集合。
- AC^0 是指能够由门集为 $\{\neg,$ 与门、或$\}$的常数深度多项式规模布尔电路精确判定的语言集合。
- $\mathsf{AC}^0[m]$ 是指能够由门集为 $\{\neg$,与门、 或、 $\mathsf{MOD}_m\}$的常数深度多项式规模布尔电路精确判定的语言集合。ACC^0 是所有 $m \geq 2$ 的 $\mathsf{AC}^0[m]$ 类的并集。
- TC^0 是指能够由门集为 $\{\neg,(\mathsf{Th}_{\geq k})_{k\geq 0}\}$的常数深度多项式规模布尔电路精确判定的语言集合。

我们强调，我们关注的是用于判定问题的电路类。已知对于每个常数素数 ^{0} $\subsetneq \mathsf{AC}^0 \subsetneq \mathsf{AC}^0[p] \subsetneq \mathsf{TC}^0$ 均 p [Ajt83、FSS84、H˚as86、Raz87、Smo87]。

（多量子比特）量子门。量子扇出门 F_n 是一个由下式定义的（$n+1$）量子比特酉算子：

$$\mathsf{F}_n\colon |b\rangle|x_1,\ldots,x_n\rangle \to |b\rangle|x_1\oplus b,\ldots,x_n\oplus b\rangle \quad \text{for every } x_1,\ldots,x_n,b\in\{0,1\}.$$

每个布尔函数 $f\colon \{0,1\}^n\to\{0,1\}$ 都会自然地诱导出一个（$n+1$）量子比特酉算子 U_f，其定义为

$$U_f\colon |x_1,\ldots,x_n\rangle|b\rangle \to |x_1,\ldots,x_n\rangle|b\oplus f(x_1,\ldots,x_n)\rangle \quad \text{for every } x_1,\ldots,x_n,b\in\{0,1\}.$$

对于所有 $n\geq 1$，广义托福利门对应于 U_{AND_n}。在含义明确时，我们有时使用 AND、OR 来表示 U_{AND}、U_{OR}。

量子电路。量子电路 C 是量子门的乘积。

- 我们称 C的深度为，如果 $C=M_dM_{d-1}\cdots M_1$，其中每个 M_i都是作用于不相交的量子比特集合上的门的乘积。 C 的规模是 C 中的门总数，以及 C所作用的量子比特数。
- 设 S 为酉算子的子集。如果 C 具有门集 S，则称其具有该门集；如果 C 中的每个门都属于 S。

令 $f\colon \{0,1\}^n\to\{0,1\}$。如果对于每个 $x\in\{0,1\}^n$， $C|x\rangle|0^a\rangle|0\rangle$ 的最后一个量子比特在计算基下测量为 $|f(x)\rangle$ 的概率至少为 $1-\varepsilon$，我们就说 C 使用 a 个辅助量子比特并具有 ε 的误差决定 f。此外，我们还说

- 如果对于每个 $x\in f^{-1}(1)$，最后一个量子比特测量为 $|1\rangle$ 的概率至少为 c，则它具有完备性 c；
- 如果对于每个 $x\in f^{-1}(0)$，最后一个量子比特测量为 $|1\rangle$ 的概率至多为 s，则它具有可靠性 s。

如果 C 以零错误判定 f，那么我们称 C 精确判定 f，并且不失一般性，可以假设 $C|x\rangle|0^a\rangle|0\rangle=|x\rangle|0^a\rangle|f(x)\rangle$，这是通过标准反计算实现的，只会使电路的深度和规模增加一个可忽略的常数倍。

QAC **与门** QAC^0。 我们主要研究 QAC电路及其对应的量子电路复杂度类 QAC^0。参见 [NC10，Ber10] 以了解更全面的介绍。

如果量子电路只使用单量子比特门和广义托福利门，它就是 QAC 电路。我们将 QAC^0 细分为以下几个更精细的类：EQAC^0 和 BQAC^0。

- EQAC^0 是能够由常数深度多项式规模 QAC 电路精确判定的语言集合。

- BQAC^0 是能够由常数深度多项式规模 QAC 电路判定，且误差[4] 至多为 $1/3$的语言集合。

我们强调，我们允许使用任意 单量子比特门，而非仅限于有限种单量子比特门。我们的量子电路允许使用辅助量子比特，其数量至多为电路规模。我们还指出，量子或门 U_{OR}: $|x\rangle|b\rangle \to |x\rangle|b \oplus \mathsf{OR}(x)\rangle$ 在 QAC 中具有常数深度和常数规模。

其他量子电路类。 我们有时会讨论 $\mathsf{QNC}^0, \mathsf{QNC}^0_{\mathrm{wf}}$， QTC^0，下面将简要介绍这些类。设 C 为一个量子电路。

- 我们称 C 为 QNC 电路，当且仅当它只使用单量子比特门和双量子比特门。EQNC^0 （相应地，BQNC^0）对应于能够由常数深度 QNC 电路以零错误（相应地，$1/3$ 错误）判定的语言。

- 我们称 C 为 $\mathsf{QNC}_{\mathrm{wf}}$ 电路，当且仅当它使用单量子比特门、双量子比特门以及扇出门（F_n）$_{n\geq 1}$。$\mathsf{EQNC}^0_{\mathrm{wf}}$ （相应地，$\mathsf{BQNC}^0_{\mathrm{wf}}$）对应于能够由常数深度多项式规模 $\mathsf{QNC}_{\mathrm{wf}}$ 电路以零错误（相应地，$1/3$错误）判定的语言。

- 我们称 C 为 QTC 电路，当且仅当它使用单量子比特门、双量子比特门以及量子阈值门（$U_{\mathsf{Th}\geq k}$）$_{k\geq 0}$。EQTC^0 （相应地，BQTC^0）对应于能够由常数深度多项式规模 QTC 电路以零错误（相应地，$1/3$ 错误）判定的语言。

量子态。 设 $|\psi\rangle$ 是一个 n量子比特量子态。如果 $C|0^n\rangle|0^a\rangle = |\psi\rangle|0^a\rangle$，我们称量子电路 C 使用 a 个辅助量子比特制备$|\psi\rangle$。此外，如果 $\||C|0^n\rangle|0^a\rangle - |\psi\rangle|0^a\rangle\|_2 \leq \varepsilon$，我们称 C制备了$|\psi\rangle$ 的一个 ε-近似。

设 $|\phi\rangle$ 为一个（$n+m$）量子比特的量子态。我们称 $|\phi\rangle$ 为一个 n量子比特的 nekomata，如果在改变量子比特排列顺序后，$|\phi\rangle$ 等于某些归一化的 m量子比特态 $|\phi_0\rangle \nsim |\phi_1\rangle$的 $\frac{1}{\sqrt{2}} \cdot |0^n\rangle|\phi_0\rangle + \frac{1}{\sqrt{2}}|1^n\rangle|\phi_1\rangle$。在 [GHMP02] 和 [Ros21], 中，研究者证明了：利用常数深度 QAC 电路计算奇偶函数 Parity_n 以及制备扇出酉算子 F_n ，等价于构造能够制备 n量子比特 nekomata 的常数深度 QAC 电路。

[4]这 $1/3$ 并非必要条件，而且可以通过黑盒方式将其提升到任意小的常数。如果有必要，我们有时也会根据完备性和可靠性给出更精确的误差界。

（非）一致性。 我们所有的电路上界（即构造）都是一致的 电路，可以从我们的证明和描述中高效地提取出来。我们所有的电路下界都针对非一致的 电路成立。（非）一致性并非我们的关注重点，因此不作详细讨论。

3 精确振幅放大

本节将说明，如何将在 [GM24]和 [Ros21]中已知的振幅放大技术调整到常数深度电路的环境中，以改进扇出构造，并完全消除先前已知构造中的任何近似误差。

这种振幅放大方法隐含于 Grover 的开创性工作 [Gro98] （另见[BHMT02，定理 2]），并且近期的量子态制备工作也以类似方式使用了该方法[Ros24、GKW24]。为完整起见，我们在附录A中给出证明。

定理 7 （[Gro98，BHMT02]）。 设 V 是一个深度为d s、规模为 QAC 电路，满足

$$V|0^n\rangle|0\rangle = \sin\theta|\psi_0\rangle|0\rangle + \cos\theta|\psi_1\rangle|1\rangle \quad for\ \theta = \frac{\pi}{4k+2}\ and\ k \in \mathbb{N}.$$

那么存在一个深度为$O(dk)$ $O(sk)$、规模为 QAC 的电路 C，使得 $C|0^n\rangle|0\rangle = |\psi_0\rangle|0\rangle$。

我们使用定理 7 来消除 [Ros21]和 [GM24]中的 nekomata 构造的近似误差。这些推论在以下推论中得到了精确表述，并由此立即推出推论3和推论4。

推论 8. 存在一个常数深度 $O(2^n)$规模的 QAC 电路，可以精确制备 *nekomata*。

推论 9. 存在一个常数深度多项式规模的 QTC 电路，可以精确制备 *nekomata*。因此，$\mathsf{BQTC}^0 = \mathsf{BQNC}^0_{\mathrm{wf}}$ 且 $\mathsf{EQTC}^0 = \mathsf{EQNC}^0_{\mathrm{wf}}$。

推论 *8* 和 *9* 的证明。假设我们的电路在前 ε个量子比特上生成一个 -近似 nekomata n，其中 $\varepsilon = O(1/\sqrt{n})$ 属于 [Ros21，GM24]。记 ¯

$$|\psi\rangle = a|0^n\rangle|\psi_0\rangle + b|1^n\rangle|\psi_1\rangle + c|\omega\rangle,$$

其中 $a^2+b^2+c^2=1$ 与 $|\omega\rangle$ 不包含形如 $|x\rangle|y\rangle$ （其中 $x \in \{0^n, 1^n\}$，且 y 任意）的基态。

如果现在在我们的状态中添加两个辅助量子比特，就可以对它们施加某个双量子比特酉算子 Q，从而得到一个状态，其 $|0^n\rangle$、$|1^n\rangle$ 分量的权重恰好满足定理 7的要求。具体而言，取一个满足以下条件的双量子比特酉算子 Q:

$$Q|00\rangle = p|00\rangle + q|11\rangle + \sqrt{1-p^2-q^2}|01\rangle,$$

其中 $p^2+q^2 \le 1$ 将在稍后设置。 Q 如何作用于另外两个双量子比特计算基态并不重要。将 Q 作用于新的辅助量子比特，结果为

$$|\phi'\rangle = ap|00\rangle|0^n\rangle|\psi_0\rangle + bq|11\rangle|1^n\rangle|\psi_1\rangle + c'|\omega'\rangle$$

其中，对于 $x \in \{0^{n+2}, 1^{n+2}\}$ 和任意的 y， $a^2p^2 + b^2q^2 + c'^2 = 1$ 和 $|\omega'\rangle$ 在 $|x\rangle|y\rangle$ 上不受支持。由于 $\varepsilon = O(1/\sqrt{n})$，当 n 足够大时，我们有 a^2， $b^2 \in (1/3,\ 2/3)$，因此可以选取p， $q \in (-1,\ 1)$，使得 $ap = bq = \frac{1}{\sqrt{2}} \sin\frac{\pi}{10} \approx .219$ 且 $p^2 + q^2 \leq 1$。

最后将 f 定义为： $\{0,1\}^{n+2} \to \{0,1\}$

$$f(x) = \begin{cases} 0 & \text{if } x \in \{0^{n+2}, 1^{n+2}\}, \\ 1 & \text{otherwise,} \end{cases}$$

并注意到 U_f 属于 QAC^0，它将 $|u\rangle|v\rangle$ 映射为 $|u\rangle|v \oplus f(u)\rangle$，其中 $u \in \{0,1\}^{n+2}$ 和 $v \in \{0,1\}$。

将上述电路与 U_f 及一个标志量子比特相结合，我们得到一个常数深度电路 V，用于制备

$$|\phi''\rangle = \sin\frac{\pi}{10}\left(\frac{1}{\sqrt{2}}|0^{n+2}\rangle|\psi_0\rangle + \frac{1}{\sqrt{2}}|1^{n+2}\rangle|\psi_1\rangle\right)|0\rangle + \cos\frac{\pi}{10}|\omega''\rangle|1\rangle$$

对于某个任意态 $|\omega''\rangle$ 该态在 $|0^{n+2}\rangle$ 和 $|1^{n+2}\rangle$ 上仍不受支持。然后根据定理 7，我们得到一个精确的（$n+2$）量子比特 nekomata $\frac{1}{\sqrt{2}}|0^{n+2}\rangle|\psi_0\rangle + \frac{1}{\sqrt{2}}|1^{n+2}\rangle|\psi_1\rangle$。至此，两个推论的证明均告完成。 □

推论 8 的一个简单推论是，我们可以将规模缩减至一个 poly(n)-规模的 QAC电路，它能精确制备一个 log(n)-量子比特 nekomata，从而实现 F$_{\log(n)}$。通过反复应用这一方法，我们可以实现多对数规模的扇出。

推论 10. 对于任意常数 $d \geq 1$，存在一个常数深度、poly(n)规模的 QAC 电路，能够精确计算 F$_{\log^d(n)}$。

证明。 简记 $k = \log(n)$，并对 d进行归纳。基础情形 $d = 1$ 正是推论 8。对于 $d \geq 2$，注意到 F$_{k^d}$ 可以通过先进行规模为 $k^{d/2}$的扇出，再并行应用 $k^{d/2} - 1$ 个 F$_{k^{d/2}}$ 来实现。由于 d 是常数，因此该电路具有常数深度和多项式规模，证毕。 □

注 11. 在 *[FPVY25]*, 中，研究表明，近似伪随机酉算子和 *-design*（对于常数 t）可以在 QAC^0 中构造。他们依赖于 *Ros21*、*GM24]* 的近似 *nekomata* 构造，并指出，如果能够消除这些 *nekomata* 构造中的误差，就可以改进其随机酉矩阵构造的参数。我们预计，推论 *8*和推论 *9*将有助于实现他们的目标。

3.1 多对数权重阈值函数

现在我们证明，推论 10 使我们能够计算“较小”的阈值函数。对于每个 k，定义 Th$_{\geq k}$：$\{0,1\}^n \to \{0,1\}$ 为权重为 k 的阈值函数，当且仅当输入字符串的汉明重量至少为 k 时输出 1。在引理 12 中，我们将证明，对于所有满足 $k \leq$polylog(n) 的情形，Th$_{\geq k}$ 属于 QAC^0 。注意，或$_n$ 等价于 Th$_{\geq 1}$，因此可以直接在 QAC^0 中计算。我们指出，在我们的工作之前，人们甚至不清楚 Th$_{\geq 2}$ 是否属于 QAC^0。

引理 12. 如果 $k \leq$多对数(n)，那么 Th$_{\geq k}$ 属于 EQAC^0。

证明。 整体电路构造隐含于 [HWWY94、RW91], 中，其中某些经典组件被其（非平凡的）量子实现所替代 [HˇS05、TT16]。

我们将需要以下由 [HWWY94]提出的数论事实。其证明见第A 节，以保证完备性。

事实 13 ([HWWY94，引理 1])。 设 $S \subseteq [n]$。存在某个整数 $|S| \leq m \leq O\left(|S|^2 \log(n)\right)$，使得 $i \neq j \pmod m$ 对所有互不相同的 $i, j \in S$均成立。

对于每个 $m \geq k$与 $\ell = 0$，1、.....、$m-1$，定义

$$A_\ell^m = \{i \in [n] \mid i \equiv \ell \pmod m\}.$$

现在注意到 $\mathsf{Th}_{\geq k}(x) = 1$ 当且仅当存在 $S \subseteq [n]$，其规模为 k，使得 $x_i = 1$ 对所有 $i \in S$均成立。根据事实 13，存在某个 $k \leq m \leq L = O(k^2 \log(n))$，使得每个 $i \in S$ 都属于 A_ℓ^m，且对应不同的$\ell = 0$， 1、.....、$m-1$。这意味着

$$\mathsf{Th}_{\geq k}(x) \leq \bigvee_{m=k}^{L} \mathsf{Th}_{\geq k}\left(\mathsf{OR}(x \mid A_0^m), \mathsf{OR}(x \mid A_1^m), \ldots, \mathsf{OR}(x \mid A_{m-1}^m)\right), \tag{1}$$

其中，$\mathsf{OR}(x \mid S)$ 对 $S \subseteq [n]$ 中 x 的各位应用或函数。

另一方面，注意到 $\{A_\ell^m\}_\ell$ 将 $[n]$ 划分为 m 个不相交集合。因此，(1) 式右侧也是 (1) 式左侧的下界。因此

$$\mathsf{Th}_{\geq k}(x) = \bigvee_{m=k}^{L} \mathsf{Th}_{\geq k}\left(\mathsf{OR}(x \mid A_0^m), \mathsf{OR}(x \mid A_1^m), \ldots, \mathsf{OR}(x \mid A_{m-1}^m)\right). \tag{2}$$

现在我们将 (2) 转换为所需的以下 QAC电路。

- 我们首先为 $L =$ 个多对数(n副本，使用 x，针对 F_L 扇出并行处理 x的每一位。根据推论 10，这具有常数深度和多项式规模。
- 然后，对于每个 $k \leq m \leq L$ 和 $\ell = 0$，1，.....，$m-1$，我们分别并行地使用上一步中的副本计算 $y_\ell^m = \mathsf{OR}(x \mid A_\ell^m)$。这需要一层或门。
- 现在，对于每个 $k \leq m \leq L$，我们分别并行计算 $z_m = \mathsf{Th}_{\geq k}(y_0^m, y_1^m, \ldots..., y_{m-1}^m)$。这基于 [HˇS05，TT16]提出的以下事实。为保证完备性，我们还在第 A 节提供了一个自包含证明。

  事实 14 ([HˇS05, TT16])。 设 $f\colon \{0,1\}^m \to \{0,1\}$ 是对称的，且 $m \leq$多对数(n)。那么f可以由常数深度的 多项式(n)规模的 QAC电路精确计算。

- 最后，我们得到 $\mathsf{Th}_{\geq k}(x) =$或门$(z_k, z_{k+1}, \ldots, z_L)$，并使用一个或门。 □

3.2 AC中的对称函数^0

引理 12 中的小阈值函数实际上构成了 AC^0 [Mor87、BW87]中的对称函数的一组完备基。这使我们能够将 SymAC^0 包含于 QAC^0，，其中 SymAC^0 是可由 AC^0 计算的对称函数类。

以下对对称 AC^0 的已知刻画由 Moran 独立证明 [Mor87]，以及 Brustman 和 Wegner [BW87]。

定理 *15*（[*Mor87*，*BW87*]）。设 $f\colon \{0,1\}^n \to \{0,1\}$ 为对称函数，满足 $f(x) = v_k$ 对所有$k = 0, 1, \ldots, n$ 以及 $x \in \{0,1\}^n$ 汉明重量为 k的情况均成立。那么， $f \in AC^0$ 当且仅当 $v_k = v_{k+1} = \cdots = v_{n-k}$对于某个 $k =$多对数(n)成立。

现在我们将定理 6 证明为以下推论16。

推论 16. $\mathsf{SymAC}^0 \subseteq \mathsf{EQAC}^0$。

证明。 我们首先注意到 $\mathsf{Th}_{\geq n-k}(x) = \neg\mathsf{Th}_{\geq k+1}(\neg x)$，其中 $\neg x$ 是 x的逐位取反。因此，根据引理 12，EQAC^0 可计算$\mathsf{Th}_{\geq k}$，对所有 $k \leq$ 多对数(n) 和 $k \geq n -$ 多对数(n) 均成立。

对于每个 k，定义 $\mathsf{EX}_k\colon \{0,1\}^n \to \{0,1\}$ 为精确汉明重量函数，其权重为 k；当且仅当输入字符串的汉明重量恰好为 k 时，该函数输出 1。由于 $\mathsf{EX}_k(x) = \mathsf{Th}_{\geq k}(x) \wedge \neg\mathsf{Th}_{\geq k+1}(x)$，我们知道，对于所有 $k \leq$ 多对数(n) 和 $k \geq n -$ 多对数(n)，$\mathsf{EX}_k \in$ 属于 QAC^0。

根据定理 15， $f \in \mathsf{SymAC}^0$ 当且仅当它是多个 EX_k 的或（或 $\neg$或），其中个数为多对数(n)，且 $k \leq$多对数(n) 或 $k \geq n -$多对数(n)。因此，只需根据推论 10 将输入字符串复制多对数(n) 份，然后并行计算相应的 EX_k，最后用或或 $\neg$或汇总这些值。

□

4 QAC 中的态-酉对偶性^0

本节探讨某些量子态与酉算子之间的对偶性。Moore [Moo99] 曾观察到猫态与奇偶函数之间存在这种对偶性。具体而言，可以通过制备猫态的电路来实现奇偶函数对应的酉算子。

这里我们展示另一种对偶性，它使我们能够利用制备 $|W\rangle$ 态的电路来弱计算精确汉明重量函数：

$$|W\rangle = \frac{1}{\sqrt{n}} \sum_{i\in[n]} |e_i\rangle \quad \text{where } e_i = 0^{i-1}10^{n-i}.$$

接着，我们将这种弱计算提升为对 QAC^0 与经典电路类的区分。

4.1 |W 态与汉明重量测试

我们首先介绍一种 QAC^0 电路，用于构造 $|W\rangle$ 态。其思路是用简单的乘积态近似 $|W\rangle$，然后使用振幅放大来精确获得 $|W\rangle$。这一点可形式化为以下定理 17，它正是定理5。

定理 17。 存在一个常数深度多项式规模的QAC 电路 U 使得 $U|0^n\rangle|0^a\rangle \approx |W\rangle|0^a\rangle$ 其中 $a = \mathsf{poly}(n)$。

证明。 令 $\delta \in [0,1]$ 为稍后确定的参数。利用一层单量子比特门，我们制备出

$$\left(\sqrt{\delta}|0\rangle + \sqrt{1-\delta}|1\rangle\right)^{\otimes n} = \sqrt{n\delta^{n-1}(1-\delta)} \cdot |W\rangle + |W^{\perp}\rangle,$$

其中 $|W^{\perp}\rangle$ 是一个未归一化态，仅支撑在汉明重量不等于 1 的计算基态上。然后，根据推论 EQAC^0 实现的 EX_1 16，我们得到如下状态

$$\sqrt{n\delta^{n-1}(1-\delta)} \cdot |W\rangle|0\rangle + |W^{\perp}\rangle|1\rangle. \tag{3}$$

注意，$h(\delta) = \sqrt{n}\delta^{n-1}(1-\delta)$ 满足 $h(0) = 0$ 与

$$h\left(1-\frac{1}{n}\right) = \left(1-\frac{1}{n}\right)^{(n-1)/2} \geq \frac{1}{\sqrt{e}} \geq \frac{1}{2}.$$

因此根据连续性，我们可以选取 δ 使得 $h(\delta) = 1/2$ 并且（3）变为

$$\frac{1}{2}|W\rangle|0\rangle + |W^{\perp}\rangle|1\rangle = \sin\frac{\pi}{6}|W\rangle|0\rangle + |W^{\perp}\rangle|1\rangle.$$

根据定理7 ，利用上述态制备过程，我们得到用于精确制备 U 的所需电路 $|W\rangle$。

□

现在我们展示如何使用上面的 $|W\rangle$ 弱计算任意固定的汉明重量。我们从汉明重量恰好为 $n/2$开始。

引理 18。 存在一个常数深度多项式规模的QAC 电路 C ，使得对于每个 $x \in \{0,1\}^n$ 和 $b \in \{0,1\}$，都有 $C|x、\ 0^{n+a}、\ b\rangle = |x\rangle|\psi_{x,\ b}\rangle$ 以及

$$|\psi_{x,b}\rangle = \frac{n-2|x|}{n}\left|0^{n+a}\right\rangle|b\rangle + \sqrt{1-\left(\frac{n-2|x|}{n}\right)^2}|\phi_x\rangle|b\oplus 1\rangle,$$

其中 $a = \mathrm{poly}(n)$ ，且 $|\phi_x\rangle$ 是一个与 $|0^{n+a}\rangle$ 正交并取决于 x的归一化态。

证明。 令 U 为根据定理 $|W\rangle$ 5 使用 a 个辅助量子比特制备 $|W\rangle$ 的电路。考虑图1中的电路 C 。注意，在 C的前两层之后，态为

$$|x\rangle|0^a\rangle|W_x\rangle|b\rangle \quad \text{where } |W_x\rangle = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}(-1)^{x_i}|e_i\rangle.$$

注意到 $\langle W|W_x\rangle = \frac{n-2|x|}{n}$。因此我们表示为

$$|W_x\rangle = \frac{n-2|x|}{n}|W\rangle + \sqrt{1-\left(\frac{n-2|x|}{n}\right)^2}|W_x^{\perp}\rangle, \tag{4}$$

其中，$|W_x^{\perp}\rangle$ 是依赖于 x 的归一化态，并且与 $|W\rangle$正交。现在我们分别分析 $|x\rangle|0^a\rangle|W\rangle|b\rangle$ 和 $|x\rangle|0^a\rangle|W_x^{\perp}\rangle|b\rangle$ 的演化。

对于 $|x\rangle|0^a\rangle|W\rangle|b\rangle$，$C$后续各层的作用如下:

$$|x\rangle|0^a\rangle|W\rangle|b\rangle \xrightarrow{U^{\dagger}} |x\rangle|0^a\rangle|0^n\rangle|b\rangle \xrightarrow{\mathrm{OR}} |x\rangle|0^a\rangle|0^n\rangle|b\rangle.$$

对于 $|x\rangle|0^a\rangle|W_x^{\perp}\rangle|b\rangle$，由于 $|0^a\rangle|W\rangle$与 $|0^a\rangle|W^{\perp}\rangle$正交，$|\phi_x\rangle := U^{\dagger}|0^a\rangle|W_x^{\perp}\rangle$ 也与 $U^{\dagger}|0^a\rangle|W\rangle = |0^{n+a}\rangle$正交。因此，或操作总是翻转 $|b\rangle$，得到整体态 $|x\rangle|\phi_x\rangle|b\oplus 1\rangle$。

由线性性以及（4），我们将上述两种演化结合起来，得到

$$|\psi_{x,b}\rangle = \frac{n-2|x|}{n}\left|0^{n+a}\right\rangle|b\rangle + \sqrt{1-\left(\frac{n-2|x|}{n}\right)^2}|\phi_x\rangle|b\oplus 1\rangle$$

如前所述。

□

引理 18 说明了如何弱判定 $\mathsf{EX}^{n/2}$：测量最终寄存器（初始化为 $b=0$）后，若 $\mathsf{EX}^{n/2}(x)=1$，则我们总是输出 1；而若 $1/n^2$ 若$\mathsf{EX}^{n/2}(x)=0$，则以至少 $1/n^2$ 的概率输出 0。通过填充足够多的 1 或 0，我们可以修改这一构造，以类似的方式检测任何其他固定的汉明重量。

推论 19。对于每个整数 $0\le k\le n$，函数 EX_k 都可以在 QAC^0 中被弱判定。也就是说，存在一个常数深度多项式规模的 QAC 电路：当 $\mathsf{EX}_k(x)=1$ 时始终输出 1；当 $\mathsf{EX}_k(x)=0$ 时，以至少 $1/n^2$ 的概率输出 0。

证明。给定一个 n位输入 x，我们用一个 n位固定字符串 $1^{n-k}0^k$ 将其填充为 $y=x\circ 1^{n-k}0^k$。令$m=2n$。于是 $\mathsf{EX}_k(x)=\mathsf{EX}^{m/2}(y)$，对此我们可以使用引理 18。 □

推论 19 使得QAC^0 能够计算任意对称函数，前提是我们拥有输入字符串的经典副本。这一结果的影响将在下一节4.2中讨论。

4.2 将QAC^0 与经典类分离

推论 19 中的单边错误是一个非常重要的特性，它使我们能够使用与门而非多数函数来提高成功概率。这一点至关重要，因为尚不清楚多数函数是否属于QAC^0„ 但根据定义可以使用 与门 。

定理 20. 设 $f\colon\{0,1\}^n\to\{0,1\}$ 是任意对称函数。对于每个整数 $r\ge 1$，都存在一个常数深度多项式规模的 QAC 电路，使其在给定 $m=r\cdot(n+1)^3$ 个 n 位字符串 x 的相同副本时，计算 $f(x)$，其完备性为 1，可靠性为 $2^{-\Omega(r)}$。

也就是说，对于输入 $|x,x,\ldots,x\rangle$，该电路在 $f(x)=1$ 时总是输出 1；而在 $f(x)=0$ 时，以至少 $1-2^{-\Omega(r)}$ 的概率输出 0$\underbrace{x,x,\ldots,x}_{m\ copies}$。

证明。由于 f 是对称的，我们可以将其表示为 $f(x)=\bigvee_{k\in S}\mathsf{EX}_k(x)$，其中 $S\subseteq\{0,1,\ldots,n\}$ 是某个值。对于每个 $\mathsf{EX}_k(x)$，我们对推论 19 的 $r\cdot n^2$ 次独立试验取与门。这需要 $r\cdot n^2$ 个 x 的副本。此外，它以完备性 1 和可靠性 $(1-n^{-2})^{r\cdot n^2}=2^{-\Omega(r)}$ 计算 $\mathsf{EX}_k(x)$。然后，我们对上述结果取或门来计算 $f(x)$，从而得到完备性 1 和可靠性 $r\cdot 2^{-\Omega(r)}=2^{-\Omega(r)}$。所需 x 的副本总数为 $|S|\cdot r\cdot n^2\le r\cdot(n+1)^3$。

□

给定输入的经典副本，定理20 允许我们将经典电路中的任意对称门替换为一个QAC 多项式规模的电路。这个经典类恰好是TC^0 ，其论证与将电路转换为公式的标准方法类似。下面的定理 21 将其形式化，并证明定理 2。

定理 21。假设 $f\colon\{0,1\}^n\to\{0,1\}$ 可由一个对称门构成的常数深度多项式规模经典电路精确计算。那么存在一个常数深度多项式规模的QAC电路，使其在获得 $m=\mathsf{poly}(n)$ 个 n 位字符串 x 的相同副本后，以误差 $2^{-\mathsf{poly}(n)}$ 计算 $f(x)$ 。

也就是说，该电路以 $|\underbrace{x,x,\ldots,x}_{m\ copies}\text{作为输入}\rangle$，并以至少 $1-2^{-\mathsf{poly}(n)}$ 的概率输出 $f(x)$.

证明。 根据定理 20， f的每个对称门都可以用一个常数深度、多项式规模的 QAC 电路计算，误差为 $2^{-\mathsf{poly}(n)}$，前提是给定 $\mathsf{poly}(n)$ 个其扇入值的相同副本。因此，我们可以自顶向下地转换 f： 每次用一个小型 QAC 电路替换当前的对称

门，该电路的误差为 $2^{-\mathsf{poly}(n)}$，并且需要 $\mathsf{poly}(n)$ 个其扇入值的相同副本；然后以同样的方式递归展开其扇入门的副本。由于 f 具有常数深度和多项式规模，最终我们只需要输入字符串的 $\mathsf{poly}(n)$ 个副本。此外，根据并合界，误差为 $\mathsf{poly}(n) \cdot 2^{-\mathsf{poly}(n)} = 2^{-\mathsf{poly}(n)}$。

□

定理 21 已经使我们能够得到部分函数，从而分离QAC^0 与AC^0，甚至$\mathsf{AC}^0[p]$。具体做法是令 f 为多数函数，并定义一个提升版本，使其接收输入字符串的多项式个相同副本。幸运的是，使用广义托福利门可以轻松检查给定字符串是否具有这种“块状”形式。这一观察引出了一个全函数，可以用来证明分离。下面将其形式化。

令 $f\colon \{0,1\}^n \to \{0,1\}$。对每个整数 $m \geq 1$，定义 $f^{\uparrow m}\colon (\{0,1\}^n)^m \to \{0,1\}$ 为

$$f^{\uparrow k}(x^{(1)},\ldots,x^{(m)}) = \begin{cases} f(x^{(1)}) & x^{(1)} = \cdots = x^{(m)}, \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

注意，这与第 1.1 节中引入的提升装置 Copy 相同。我们在 $\uparrow k$ 中使用它，以突出输入副本的数量。

引理 22。 设 $f\colon \{0,1\}^n \to \{0,1\}$ 是一个布尔函数，可由一个常数深度多项式规模的QAC 电路计算，该电路具有 $m \leq \mathsf{poly}(n)$ 个相同输入副本，且误差为 ε。那么$f^{\uparrow m}\colon (\{0,1\}^n)^m \to \{0,1\}$ 在（5）中定义，可由一个常数深度多项式规模的 QAC电路计算，误差为 ε。

证明。 我们将 nm 位输入视为 $|x^{(1)}\rangle \cdots |x^{(m)}\rangle$，其中每个 $x^{(i)}$ 有 n 位。我们可以通过对每个坐标 $j \in [n]$ 检查 $x_j^{(1)} = \cdots = x_j^{(m)}$，来验证 $x^{(1)}$、…、$x^{(m)}$ 是否相等。这可以通过针对每个坐标并行计算 $\mathsf{EX}_0 \vee \mathsf{EX}_m$，再用与门合并各坐标的检查结果来实现；该电路具有常数深度，规模为 $\mathsf{poly}(m) = \mathsf{poly}(n)$。

与上述检查并行地，我们假设输入相等，并使用规模为 f 的 QAC 电路（给定m个相同的输入副本）计算其值。

最终结果是上述两项计算的与门。由于第一次相等性检查不会产生误差，误差仅来自第二部分，根据假设，这恰好是 ε。

□

于是我们得到如下推论。

推论 23. 假设 $f\colon \{0,1\}^n \to \{0,1\}$ 可由一个由对称门构成的常数深度多项式规模经典电路精确计算。那么存在某个 $m \leq$ 多项式(n)，使得 $f^{\uparrow m}$ 可由一个误差为 $2^{-\mathsf{poly}(n)}$ 的常数深度多项式规模QAC 电路计算。

证明。 我们只需结合定理21和引理22。

□

根据经典复杂性理论中已知的分离结果，我们得到如下定理，它将 QAC^0 与 $\mathsf{AC}^0[p] \supsetneq \mathsf{AC}^0$, 分离，从而证明定理 1。

定理 24. $\mathsf{BQAC}^0 \not\subset \mathsf{AC}^0[p]$。此外，若 $\mathsf{ACC}^0 \neq \mathsf{TC}^0$, ，则 $\mathsf{BQAC}^0 \not\subset \mathsf{ACC}^0$。

证明。 回忆一下，多数函数 Maj 不属于 $\mathsf{AC}^0[p]$ [Raz87、Smo87]。因此 $\mathsf{Maj}^{\uparrow \mathsf{poly}(n)} \notin \mathsf{AC}^0[p]$，因为 $\mathsf{AC}^0[p]$ 可以免费复制输入字符串。另一方面，根据推论 23，并且由于 $\mathsf{Maj} \in \mathsf{TC}^0$, ，我们知道 $\mathsf{Maj}^{\uparrow \mathsf{poly}(n)} \in \mathsf{BQAC}^0$。这表明 $\mathsf{BQAC}^0 \not\subset \mathsf{AC}^0[p]$。

第二个结果也可以由推论23 得出：取$\mathsf{TC}^0 \setminus \mathsf{ACC}^0$ 中的任意语言ACC^0，并注意到经典副本对它同样是免费的。

□

致谢

JM感谢Farzan Byramji、Sabee Grewal、Dale Jacobs、Kunal Marwaha和Gregory Rosenthal进行的启发性讨论。KW获得美国国家科学基金会DMS-2424441号资助，并得到IAS数学学院的支持。

参考资料

[AB09] Sanjeev Arora 和 Boaz Barak。《计算复杂性：一种现代方法》。剑桥大学出版社，2009年。[ADOY24] Anurag Anshu、Yangjing Dong、Fengning Ou 和 Penghui Yao。论 QAC^0 在仅有略超线性数量辅助量子比特时的计算能力。arXiv 预印本 arXiv:2410.06499，2024年。[Ajt83] Mikl´os Ajtai。有限结构上的Σ_1-公式。《纯粹与应用逻辑年鉴》，24(1):1–48，1983年。[Ber10] DEBAJYOTI Bera。《量子电路：能力与局限》。博士论文，波士顿大学，2010年。[Ber11] Debajyoti Bera。量子电路的一个下界方法。《信息处理快报》，111(15):723–726，2011年。[BGK18] Sergey Bravyi、David Gosset 和 Robert K¨onig。浅层电路带来的量子优势。《科学》，362(6412):308–311，2018年。[BHMT02] Gilles Brassard、Peter Høyer、Michele Mosca 和 Alain Tapp。量子振幅放大与估计。《当代数学》，305:53–74，2002年。[BW87] Bettina Brustmann 和 Ingo Wegener。有界深度电路中对称函数的复杂度。《信息处理快报》，25(4):217–219，1987年。[FFG+06] Maosen Fang、Stephen Fenner、Frederic Green、Steven Homer 和 Yong Zhang。扇出的量子下界。《量子信息与计算》，6(1):046–057，2006年。[FPVY25] Ben Foxman、Natalie Parham、Francisca Vasconcelos 和 Henry Yuen。常数（量子）时间内的随机酉矩阵。arXiv 预印本 arXiv:2508.11487，2025年。[FSS84] Merrick Furst、James B Saxe 和 Michael Sipser。奇偶性、电路与多项式时间层级。《数学系统理论》，17(1):13–27，1984年。[GHMP02] Frederic Green、Steven Homer、Cristopher Moore 和 Christopher Pollett。计数、扇出与量子 ACC 的复杂度。《量子信息与计算》，2(1):35–65，2002年。[GKM+25] Daniel Grier、Daniel M Kane、Jackson Morris、Anthony Ostuni 和 Kewen Wu。浅层电路采样带来的量子优势：超越边缘分布的困难性。arXiv 预印本 arXiv:2510.07808，2025年。

[GKW24] David Gosset、Robin Kothari 和 Kewen Wu。以最优 T-计数制备量子态。arXiv 预印本 arXiv:2411.04790，2024年。[GM24] Daniel Grier 和 Jackson Morris。量子阈值功能强大。arXiv 预印本 arXiv:2411.04953，2024年。[Gro98] Lov K Grover。量子计算机几乎可以利用任意变换快速搜索。Physical Review Letters，80(19):4329，1998年。[GS20] Daniel Grier 和 Luke Schaeffer。交互式浅层 Clifford 电路：相对于 NC^1 及更广范围的量子优势。载于第52届 ACM 计算理论研讨会论文集，第875–888页，2020年。[HAB02] William Hesse、Eric Allender 和 David A Mix Barrington。用于除法和迭代乘法的一致常数深度阈值电路。《计算机与系统科学杂志》，65(4):695–716，2002年。[H˚as86] Johan H˚astad。《小深度电路的计算局限》。博士论文，麻省理工学院，1986年。[HˇS05] Peter Høyer 和 Robert ˇSpalek。量子扇出功能强大。《计算理论》，1(1):81–103，2005年。[HWWY94] Johan Hastad、Ingo Wegener、Norbert Wurm 和 Sang-Zin Yi。对称函数的最优深度、极小规模电路。《信息与计算》，108(2):200–211，1994年。[0pt] Stasys Jukna 等。《布尔函数复杂度：进展与前沿》，第27卷。Springer，2012年。[+12] JTVW[Malvika Raj Joshi、Avishay Tal、Francisca Vasconcelos 和 John Wright。改进的 QAC0 下界，2025年。网址：https://arxiv.org/abs/2512.14643，arXiv: 2512.14643。25] KOW[Daniel M Kane、Anthony Ostuni 和 Kewen Wu。汉明切片采样的局部性界。载于第56届 ACM 计算理论研讨会论文集，第1279–1286页，2024年。24] LMN[Nathan Linial、Yishay Mansour 和 Noam Nisan。常数深度电路、傅里叶变换与可学习性。《ACM 杂志》，40(3):607–620，1993年。93] Moo[Cristopher Moore。量子电路：扇出、奇偶性与计数。arXiv 预印本 quant-ph/9903046，1999年。99] Mor[Shlomo Moran。由 Hastad 主引理导出的一般化下界。《信息处理快报》，25(6):383–388，1987年。87] NC[Michael A Nielsen 和 Isaac L Chuang。《量子计算与量子信息》。剑桥大学出版社，2010年。

[NPVY24] Shivam Nadimpalli、Natalie Parham、Francisca Vasconcelos 和 Henry Yuen。《关于 QAC^0 的泡利谱》。载于第 56 届 ACM 计算理论研讨会论文集，第 1498–1506 页，2024 年。[PFGT25] Daniel Pad´e、Stephen Fenner、Daniel Grier 和 Thomas Thierauf。《计算奇偶性的深度 2 QAC 电路的紧确界》。arXiv 预印本 arXiv:2504.06433，2025年。[Raz87] Alexander A Razborov。《基于逻辑加法的完备基上有界深度电路规模的下界》。《数学札记》，41(4):598–607，1987年。[Ros21] Gregory Rosenthal。《奇偶性近似的 QAC^0 复杂度界》。载于第 12 届理论计算机科学创新会议（ITCS 2021）。Schloss-Dagstuhl-Leibniz 信息学中心，2021年。[Ros23] Gregory Rosenthal。《量子态与酉复杂度》。博士论文，多伦多大学（加拿大），2023年。[Ros24] Gregory Rosenthal。《通过一次查询高效合成量子态》。载于 2024 年 ACM-SIAM 离散算法年度研讨会（SODA）论文集，第 2508–2534 页。SIAM，2024年。[RW91] Prabhakar Ragde 和 Avi Wigderson。《线性规模常数深度多对数阈值电路》。《信息处理快报》，39(3):143–146，1991年。[Smo87] Roman Smolensky。《布尔电路复杂度下界理论中的代数方法》。载于第十九届 ACM 计算理论研讨会论文集，第 77–82 页，1987年。[STV21] Srikanth Srinivasan、Utkarsh Tripathi 和 S Venkitesh。《对称布尔函数的概率次数》。《SIAM 离散数学杂志》，35(3):2070–2092，2021年。[TT16] Yasuhiro Takahashi 和 Seiichiro Tani。《常数深度精确量子电路层级的坍缩》。《计算复杂性》，25:849–881，2016年。[Wik25] 维基百科贡献者。《切比雪夫函数——维基百科，自由的百科全书》，2025年。 [在线；访问日期：7月22日，2025]。网址：https://en.wikipedia.org/w/index. php?title=切比雪夫_函数&oldid=1289843964.[WKST19] Adam Bene Watts、Robin Kothari、Luke Schaeffer 和 Avishay Tal。《浅层量子电路与无界扇入浅层经典电路之间的指数级分离》。载于第 51 届 ACM SIGACT 计算理论研讨会论文集，第 515–526 页，2019年。[WP23] Adam Bene Watts 和 Natalie Parham。《浅层电路采样的无条件量子优势》。arXiv 预印本 arXiv:2301.00995，2023年。[WSM01] X Wang、A Sørensen 和 K Mølmer。《用于量子计算的多比特门》。《物理评论快报》，86(17):3907–3910，2001年。[Zal99] Christof Zalka。《Grover 量子搜索算法是最优的》。《物理评论 A》，60(4):2746，1999年。

第3节中遗漏的证明

定理 7 ([Gro98,BHMT02])。 假设 V 是深度为d s、规模为 QAC 电路，满足 g

$$V|0^n\rangle|0\rangle = \sin\theta|\psi_0\rangle|0\rangle + \cos\theta|\psi_1\rangle|1\rangle \quad for\ \theta = \frac{\pi}{4k+2}\ and\ k \in \mathbb{N}.$$

那么存在一个深度为$O(dk)$ $O(sk)$、规模为 QAC 的电路 C，使得 $C|0^n\rangle|0\rangle = |\psi_0\rangle|0\rangle$。

证明。 设 $R_1 = \mathbb{I}_n \otimes Z$ 和 $R_2 = \mathbb{I}_{n+1} - 2|\alpha_1\rangle\langle\alpha_1|$ 是两个反射。注意， R_2 的深度为$O(d)$，规模为 $O(s)$，因为

$$R_2 = \mathbb{I}_{n+1} - 2|\alpha_1\rangle\langle\alpha_1| = V(\mathbb{I}_{n+1} - 2\left|0^{n+1}\right\rangle\left\langle 0^{n+1}\right|)V^\dagger.$$

对于 $t \in \mathbb{N}$，定义

$$|\alpha_t\rangle = \sin t\theta|\psi_0\rangle|0\rangle + \cos t\theta|\psi_1\rangle|1\rangle$$

并注意到

$$\begin{aligned} R_2R_1|\alpha_t\rangle &= (\mathbb{I}_{n+1} - 2|\alpha_1\rangle\langle\alpha_1|)(\sin t\theta|\psi_0\rangle|0\rangle - \cos t\theta|\psi_1\rangle|1\rangle) \\ &= (-2\sin^2\theta\sin t\theta + \sin 2\theta\cos t\theta + \sin t\theta)|\psi_0\rangle|0\rangle \\ &\qquad + (-\sin 2\theta\sin t\theta + 2\cos t\theta\cos^2\theta - \cos t\theta)|\psi_1\rangle|1\rangle \\ &= \sin((t+2)\theta)|\psi_0\rangle|0\rangle + \cos((t+2)\theta)|\psi_1\rangle|1\rangle \\ &= |\alpha_{t+2}\rangle. \end{aligned}$$

定义 $C = (R_2R_1)^kV$。由于 $\theta = \frac{\pi}{4k+2}$，我们得到 $C\left|0^{n+1}\right\rangle = |\alpha_{2k+1}\rangle = |\psi_0\rangle|0\rangle$ 如所需 d. □

事实 13 ([HWWY94，引理 1])。 令 $S \subseteq [n]$。存在某个整数 $|S| \le m \le O\left(|S|^2\log(n)\right)$，使得 $i \neq j$ (模 m) 对所有互不相同的 i， $j \in S$。

证明。 令 $m \ge 2$ 为满足对所有 $i \neq j \in S$都有 $i \neq j$ (模 m) 的最小整数。注意到 m存在，特别是 $m \le n+1$。此外， $m \ge |S|$，因为不同的 $i \in S$ 需要占据模 m下不同的余数。

根据 m 的选取，任意整数 $m' < m$ 都对某个 $i \neq j \in S$ 整除 $|i-j|$。这意味着 1、2、...、$m-1$ 的最小公倍数，记为 lcm(1、2、.....、$m-1$)，整除 $\prod_{i\neq j\in S}|i-j|$。特别地，

$$\mathsf{lcm}(1,2,\ldots,m-1) \le \prod_{i\neq j\in S}|i-j| \le n^{|S|^2}$$

由于 i， $j \in S \subseteq [n]$。另一方面，已知第二切比雪夫函数 $\psi(m-1)$：=ln lcm(1、2、.....、$m-1$具有渐近行为 $\psi(x) = \Theta(x)$（例如参见 [Wik25]）。因此

$$m \le 2(m-1) = \Theta(\psi(m-1)) \le O\left(|S|^2\log(n)\right)$$

如所要求的。 □

事实 14 ([H˙S05， TT16])。 设 f： $\{0,1\}^m \to \{0,1\}$ 是对称的，且 $m \le$为多对数(n)。那么 f 可以由一个常数深度、规模为 多项式(n) 的 QAC 电路精确计算。

证明。回忆一下，EX_k 是权重为 k的精确汉明重量函数。我们首先为每个EX_k构造QAC电路。对于一般的 f，注意到 $f(x) = \bigvee_{k\in S}\mathrm{EX}_k(x)$，其中$S \subseteq \{0,1,\ldots,m\}$。因此，为了计算 $f(x)$，我们首先利用推论 10 中的$\mathsf{F}^{|S|}$，生成 $|S| \le \mathrm{polylog}(n)$个 x 副本。然后分别使用这些副本并行计算$\mathrm{EX}_k(x)$，最后对结果取或，得到 $f(x)$。

Now 我们关注 EX_k。定义 $r = \lfloor \log(m) \rfloor$ 和 $|x|$ 为 x an 的汉明重量 d

$$|\phi_t\rangle = \frac{|0\rangle + e^{i\pi(|x|-k)/2^t}|1\rangle}{\sqrt{2}} \quad \text{for each } t = 0,1,\ldots,r.$$

注意，$|\phi_0\rangle|\phi_1\rangle\cdots|\phi_r\rangle$ 可以按如下方式以常数深度和多项式规模构造。

- 我们首先构造 $r+1 \le$ 多对数(n) 个 x 的副本，使用 F^{r+1} （推论 10）。
- 对每个 t 并行地，我们使用 x 的第 t 个副本来构造 $|\phi_t\rangle$:

$$\begin{aligned}
|x\rangle|0^m\rangle &\to |x\rangle\frac{|0\rangle + e^{-i\pi k/2^t}|1\rangle}{\sqrt{2}}\left|0^{m-1}\right\rangle && \text{(a single-qubit rotation gate)}\\
&\to |x\rangle\frac{|0^m\rangle + e^{-i\pi k/2^t}|1^m\rangle}{\sqrt{2}} && \text{(a } \mathsf{F}_{m-1} \text{ gate using Corollary 10)}\\
&\to |x\rangle\frac{|0^m\rangle + e^{-i\pi k/2^t}\cdot\prod_{j\in[m]} e^{i\pi x_j/2^t}|1^m\rangle}{\sqrt{2}} \\
& && \text{(a layer of controlled } (\pi/2^t)\text{-phase gate)}\\
&\to |x\rangle\frac{|0\rangle + e^{-i\pi k/2^t}\cdot\prod_{j\in[m]} e^{i\pi x_j/2^t}|1\rangle}{\sqrt{2}}\left|0^{n-1}\right\rangle && \text{(a } \mathsf{F}_{m-1} \text{ gate using Corollary 10)}\\
&= |x\rangle|\phi_t\rangle\left|0^{m-1}\right\rangle.
\end{aligned}$$

注意，m =为多对数(n)，因此上述操作具有常数深度和 $\mathrm{poly}(n)$ 规模 .

通过一层 Hadamard 门和 X门，我们得到 $|\psi_0\rangle|\psi_1\rangle\cdots|\psi_r\rangle$，其中 $|\psi_t\rangle = XH|\phi_t\rangle$。接着，我们在 $|\psi_0\rangle|\psi_1\rangle\cdots|\psi_r\rangle$ 上应用广义托福利门与门，并将该值存储在另一个量子寄存器中。现在我们证明该值等于 $\mathrm{EX}_k(x)$。

- 如果 $\mathrm{EX}_k(x) = 1$，那么 $|x| = 1$，并且对于所有 $t = 0,\ 1,\ \ldots,\ r$，都有 $|\phi_t\rangle = |+\rangle$。因此，对于所有 t，$|\psi_t\rangle = XH|+\rangle = |1\rangle$，最终的与门值也等于 1。
- 如果 $\mathrm{EX}_k(x) = 0$，那么对于某个 $t^* = 0,\ 1,\ \ldots,\ r$和奇整数 v，有 $|x| - k = 2^{t^*}v$。因此$|\phi_{t^*}\rangle = \frac{|0\rangle+e^{i\pi v}|1\rangle}{\sqrt{2}} = |-\rangle$。由此，$|\psi_{t^*}\rangle = XH|-\rangle = |0\rangle$，最终的与门值等于 0。

最后，我们撤销上述门（最后一个与门除外），以清理工作区。这样便得到了所需的 EX_k 电路，也得到了适用于一般 f 的电路。 □

B 索引需要较大的经典扇出

本节将证明，即使在 TC^0 中，合取函数和索引函数也需要较大的扇出。这是一个简单的计数论证，我们在此给出以确保完备性。

我们从对数规模的合取函数开始。

定理 25. 存在一个函数 $f\colon \{0,1\}^{\log(n)} \to \{0,1\}$，使得如果 f 可以由门集为 $\{\neg,(\mathsf{Th}^{\geq k})_{k\geq 0})\}$的常数深度电路计算，那么该电路的扇出为 $n^{\Omega(1)}$。

证明。任意深度为 d 且扇出为 r 的电路最多有 $O(r^d)$ 个门。由于每个门有 $O(r^d)+\log(n)$ 种可能，因此此类电路最多有 $(r^d+\log(n))^{O(r^d)}$ 个。另一方面，在 $\log(n)$ 位上有 2^n 个不同的布尔函数，因此需要不同的电路。这意味着 $r = n^{\Omega(1)}$ 如 $d = O(1)$。

□

回顾索引函数 Ind 的定义：$\{0,1\}^n \times \{0,1\}^{\log(n)} \to \{0,1\}$ 即

$$\mathsf{Ind}(x_1,\dots x_n, i_1,\dots,i_{\log(n)}) = x_{i_1\cdots i_{\log(n)}}.$$

推论 26。 如果 Ind 可以由门集为 $\{\neg,(\mathsf{Th}^{\geq k})_{k\geq 0}\}$ 的常数深度电路计算，那么该电路的扇出为 $n^{\Omega(1)}$。

证明。对于每个 $x\in\{0,1\}^n$，我们定义 $\mathsf{Ind}_x\colon \{0,1\}^{\log(n)} \to \{0,1\}$ 为

$$\mathsf{Ind}_x(i_1,\dots,i_{\log(n)}) = \mathsf{Ind}(x,i_1,\dots,i_{\log(n)}).$$

于是，Ind_x 枚举了 $\log(n)$ 位上的所有布尔函数，包括定理 25中的那个函数。由此完成证明。

□

C 提升副本复杂度

本节介绍一些额外的技术，以降低各种对称函数的副本复杂度。

C.1 截断式并行重复

第 $\mathsf{EX}^{n/2}(x)$ 的计算在第 4.1 节中相当弱，因为其正确概率可能仅为 $1/n^2$，当 $|x|\neq n/2$ (见推论 19)。在这一部分，我们展示如何将其适度提升至 多对数$(n)/n$。

一般而言，这种误差缩减通过并行重复测试来实现，这是第 4.2 节的关键思路；也就是说，我们只需消耗更多输入字符串的副本，以便对 W 测试进行更多轮次。

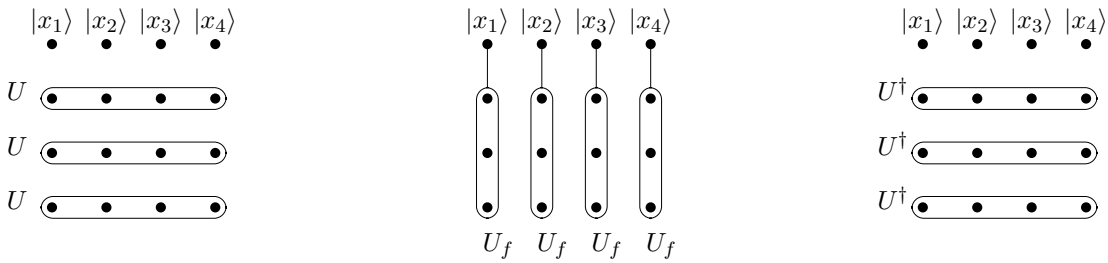
然而，在 QAC^0，中，我们只知道如何通过推论 多对数(n) 次复制10，这相当于进行 多对数(n) 次并行运行，成功率为 多对数$(n)/n^2$。

我们将在下文的定理 27 中证明，如何达到 多对数$(n)/n$的成功率，这与每 n ·多对数(n) 次并行运行相当。

定理 27。 对于每个 n，都存在一个常数深度多项式规模的 QAC 电路，使得 t

- 当 $\mathsf{EX}^{n/2}(x) = 1$时，它以至少 $1-2^{-\text{多对数}(n)}$ 的概率输出 1；
- 当 $\mathsf{EX}^{n/2}(x) = 0$时，它以至少 多对数$(n)/n$ 的概率输出 0 。

证明。不失一般性，我们假设 n是偶数，整体电路如图2所示。



阶段 1： $|W\rangle$ 准备　　阶段 2：受控 U_f　　阶段 3：反计算 $|W\rangle$

图 2： $n = 4$的截断并行重复电路。

令 $m = n \cdot \text{polylog}(n)$。我们将证明，存在一个常数深度多项式规模 QAC 电路，它在 $|x\rangle$ 上制备的状态与.....极其接近

$$|\phi_x\rangle = |x\rangle \otimes \Bigg(\underbrace{\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |e_i\rangle}_{|W_x\rangle} \Bigg)^{\otimes m}, \tag{6}$$

由此，我们可以通过以下断言完成证明28。

断言 28. 存在一个常数深度多项式规模QAC</style电路，使得对于，当EX$^{n/2}(x) = 1$时，它总是输出 1；而当EX$^{n/2}(x) = 0$时，它以至少 $1 - (1 - 1/n^2)^m =$ 多对数$(n)/n$ 的概率输出0 。

证明。令 U 为定理5 中制备 $|W\rangle$的电路。引理18 的证明或$_n \circ (U^\dagger \otimes \mathbb{I}_1)(|W_x\rangle |0\rangle)$
$= \binom{n-2|x|}{n} |0^n\rangle |0\rangle + \sqrt{1 - \binom{n-2|x|}{n}^2} |\tau_x\rangle |1\rangle$，其中 $|\tau_x\rangle$与 $|0^n\rangle$ 正交，并且或$_n$ 将前或个 n 量子比特的结果放在第（$n + 1$）个量子比特中。这意味着

$$(\text{OR}_n \circ (U^\dagger \otimes \mathbb{I}_1))^{\otimes m} (|W_x\rangle |0\rangle)^{\otimes m} = \left(1 - \left(\frac{n - 2|x|}{n}\right)^2\right)^{m/2} |\tau_x\rangle^{\otimes m} |1^m\rangle + \sum_{b \in \{0,1\}^m \setminus \{1^m\}} |\star_b\rangle |b\rangle, \tag{7}$$

其中每个 $|\star_b\rangle$ 都是一个未归一化的 nm量子比特态。现在，我们对最后 m个量子比特施加一个与门，并将结果存储在一个额外的辅助量子比特中。

- 如果EX$^{n/2}(x) = 1$，那么（7）就只是 $|\tau_x\rangle^{\otimes m} |1^m\rangle$ ，而与门的结果是确定性的 1；
- 否则 EX$^{n/2}(x) = 0$，那么 $|x| \neq n/2$ 并且 $|\tau_x\rangle^{\otimes m} |1^m\rangle$ 在 (7) 中的振幅至多为 $(1 - 1/n^2)^{m/2}$。因此，与门 结果为 0 的概率至少为 $1 - (1 - 1/n^2)^m$。

通过将电路设为 (或 28 OR$_n \circ (U^\dagger \otimes \mathbb{I}_1))^{\otimes m}$，然后接一个与门$_m$ 门。

□

现在我们转而近似（6）。为方便起见，我们用 $A \in \{0,1\}^{n \times m}$ 表示一个具有 n 行和 m 列的二进制矩阵。对于每个 $i \in [n]$，我们用 $A[i]$ 表示 i的第 A 行，并且

用 $|A[i]|$ 表示 $A[i]$的汉明重量。对于 $a \in [n]^m$，我们通过将第 j列设为示性向量 e_{a_j}，将其与矩阵$A_a \in \{0,1\}^{n\times m}$关联起来。于是

$$|W_x\rangle^{\otimes m} = \left(\frac{1}{\sqrt{n}}\sum_i (-1)^{x_i}|e_i\rangle\right)^{\otimes m} = \frac{1}{\sqrt{n^m}}\sum_{a\in[n]^m}(-1)^{x_1 s_1(a)+\cdots+x_n s_n(a)}|A_a\rangle$$

($s_i(a)$ is the number of i's appearance 属于 a)

$$= \frac{1}{\sqrt{n^m}}\sum_{a\in[n]^m}(-1)^{x_1|A_a[1]|+\cdots+x_n|A_a[n]|}|A_a\rangle \qquad (\text{since } s_i(a) = |A_a[i]|)$$

$$= \frac{1}{\sqrt{n^m}}\sum_{a\in[n]^m}(-1)^{x_1\cdot\mathsf{Parity}(A_a[1])+\cdots+x_n\cdot\mathsf{Parity}(A_a[n])}|A_a\rangle\,. \tag{8}$$

令 $h = \mathsf{polylog}(n)$，并定义 $t = h\cdot m/n = \mathsf{polylog}(n)$。现在我们定义对称函数$f$：$\{0,1\}^m \to \{0,1\}$ 如下

$$f(x) = \begin{cases}\mathsf{Parity}(x) & |x|\le t,\\ 0 & \text{otherwise,}\end{cases}$$

并定义

$$|\rho_x\rangle = \frac{1}{\sqrt{n^m}}\sum_{a\in[n]^m}(-1)^{x_1\cdot f(A_a[1])+\cdots+x_n\cdot f(A_a[n])}|A_a\rangle\,. \tag{9}$$

根据简单的球入箱计算，它近似于 $|W_x\rangle^{\otimes m}$。

断言 29. *ℓ_2 与 $|\rho_x\rangle$ 之间的距离为 $2^{-\mathsf{polylog}(n)}$。*

证明。 比较（8）和（9，可得

$$\begin{aligned}\left\||\rho_x\rangle - |W_x\rangle^{\otimes m}\right\|_2^2 &\le 4\cdot\Pr_{a\sim[n]^m}[|A_a[i]|>t \text{ for some } i\in[n]]\\ &\le 4n\cdot\Pr_{a\sim[n]^m}[|A_a[1]|>t] \qquad (\text{by union bound and symmetry})\\ &= 4n\cdot\Pr[\mathsf{binom}(m,1/n)>t]\,,\end{aligned}$$

其中，$\mathsf{binom}(m,1/n)$是偏置为 $1/n$的 m 枚硬币的二项分布。由于 $t = h\cdot m/n$ 与h =多对数(n)，根据标准的集中性，可知上述概率为 $2^{-\mathsf{polylog}(n)}$。 □

我们还可由定理15 和推论16 得知， f 可以通过一个常数深度多项式规模的QAC 电路精确计算。此时，只需按如下方式构造 $|x\rangle|\rho_x\rangle$：

$$\begin{aligned}|x\rangle &\xrightarrow{U^{\otimes m}} |x\rangle|W\rangle^{\otimes m} \qquad (U \text{ is the circuit in Theorem 5 preparing } |W\rangle)\\ &= \frac{1}{\sqrt{n^m}}\sum_{a\in[n]^m}|x\rangle|A_a\rangle \qquad (\text{by the definition of } |W\rangle \text{ and } A_a)\\ &= \frac{1}{\sqrt{n^m}}\sum_{a\in[n]^m}\bigotimes_{i\in[n]}(|x_i\rangle|A_a[i]\rangle) \qquad (\text{separating rows of } A_a)\\ &\xrightarrow{U_f^{\otimes n}} \frac{1}{\sqrt{n^m}}\sum_{a\in[n]^m}\bigotimes_{i\in[n]}(|x_i\rangle|A_a[i]\rangle|f(A_a[i])\rangle)\\ &\qquad (\text{each } U_f \text{ evaluates } f(A_a(i)) \text{ and by Corollary 16})\end{aligned}$$

$$\xrightarrow{R^{\otimes n}} \frac{1}{\sqrt{n^m}} \sum_{a\in[n]^m} \bigotimes_{i\in[n]} \left((-1)^{x_i\cdot f(A_a[i])} |x_i\rangle |A_a[i]\rangle |f(A_a[i])\rangle\right)$$

$$(R\colon |u,v\rangle \to (-1)^{u\cdot v} |u,v\rangle \text{ is a two-qubit unitary})$$

$$\xrightarrow{U_f^{\otimes n}} \frac{1}{\sqrt{n^m}} \sum_{a\in[n]^m} \bigotimes_{i\in[n]} \left((-1)^{x_i\cdot f(A_a[i])} |x_i\rangle |A_a[i]\rangle\right) \qquad (\text{uncompute } U_f^{\otimes n})$$

$$= \frac{1}{\sqrt{n^m}} \sum_{a\in[n]^m} (-1)^{x_1\cdot f(A_a[1])+\cdots+x_n\cdot f(A_a[n])} |x\rangle |A_a\rangle = |x\rangle |\rho_x\rangle .$$

结合断言29 和断言28，即可完成定理27的证明。 □

在此我们指出，如果能够将定理 27 中的可靠性界改进n为$/n$ 多对数（或者直观地说，实现 $\sim n^2$ 次并行运行的QAC^0），那么我们就有奇偶性 $\in\mathsf{QAC}^0$。定理 27 的一个直接推论是，在完备性仅有可忽略的牺牲下，推论 19得到了改进。

推论 30。对于每个 n 和 $0 \le k \le n$，都存在一个常数深度多项式规模的 QAC 电路：若 $\mathsf{EX}_k(x) = 1$，则以至少 $1 - 2^{-\mathsf{polylog}(n)}$ 的概率输出 1；若 $\mathsf{EX}_k(x) = 0$，则以至少 多对数$(n)/n$ 的概率输出 0。

因此，$m = n/$多对数(n) 个输入副本就足以让常数深度多项式规模的QAC 电路以完备性 $1 - 2^{-\mathsf{polylog}(n)}$ 和可靠性 $2^{-\mathsf{polylog}(n)}$ 判定 EX_k。

推论 30表明，每个 n位对称函数的副本复杂度至多为$n^2/$多对数(n).

C.2 概率计算

为了进一步降低副本复杂度，我们考虑概率计算，即一个随机的 QAC^0电路，能够以高概率正确计算目标函数。

我们以奇偶函数说明这一思想。我们用 $\mathsf{Parity}^{\uparrow m}\colon (\{0,1\}^n)^m \to \{0,1\}$ 表示奇偶函数的 m副本版本，其定义为

$$\mathsf{Parity}^{\uparrow m}(y_1,\ldots,y_m) = \mathsf{Parity}(y_1)\cdot 1_{y_1=\cdots=y_m} \quad \text{for all } y_1,\ldots,y_c \in (\{0,1\}^n)^m.$$

回顾一下，推论30 表明，$\mathsf{Parity}^{\uparrow n^2/\text{多对数}(n)} \in \mathsf{QAC}^0$。下面我们将展示，概率计算还能带来另一个平方根级别的节省。

定理 31。令 $m = n^{1.5}/$多对数(n)。存在一个常数深度多项式规模QAC 电路的系综 $\{C_r\}_r$，使得

$$\Pr_r\left[C_r(y_1,\ldots,y_m) = \mathsf{Parity}^{\uparrow m}(y_1,\ldots,y_m)\right] \ge 1 - 2^{-\mathsf{polylog}(n)} \quad \textit{holds for every } y_1,\ldots,y_m \in \{0,1\}^n.$$

证明。定义 $f\colon \{0,1\}^n \to \{0,1\}$ 如下

$$f(y) = \begin{cases} \mathsf{Parity}(y) & |y| \in \frac{n}{2} \pm \sqrt{n\cdot\mathsf{polylog}(n)}, \\ 0 & \text{otherwise.} \end{cases}$$

那么 f 是由 $\sqrt{n}\cdot$多对数(n) 个精确阈值函数构成的析取。根据推论 30，使用 $m = n^{1.5}/$多对数(n) 个副本，常数深度多项式规模 QAC 电路可以计算 f，误差为$2^{-\mathsf{polylog}(n)}$。

现在，对于每个具有偶数汉明重量的 $r \in \{0,1\}^n$，我们用 C'_r 表示在 $n^{1.5}/$个n的多对数副本上、以误差 $2^{-\mathsf{polylog}(n)}$计算 $f(y \oplus r)$的 QAC 电路。我们注意到，由于 r 被硬连线到 C'_r中，可以通过一层单量子比特门将 y 的副本转换为 $y \oplus r$ 的副本。此外，由于 r 是偶字符串，Parity(y) = Parity$(y \oplus r)$；当$|y \oplus r| \in \frac{n}{2} \pm \sqrt{n} \cdot$为$n$的多对数时，该结果等于 $f(y \oplus r)$。

将 QAC 电路 C_r 定义为 C'_r，并额外增加一层常数深度的门，用于检查输入副本是否相同。固定任意的 $y_1, \ldots, y_m \in \{0,1\}^n$，并令 $y = y_1$。如果 $C_r(y_1, \ldots, y_m) \neq \mathrm{Parity}^{\uparrow m}(y_1, \ldots, y_m)$，那么有以下两种情况。

- $|y \oplus r| \notin \frac{n}{2} \pm \sqrt{n \cdot \mathrm{polylog}(n)}$。这种情况发生的概率为 $2^{-\text{多对数}(n)}$，因为 r 是一个均匀随机的偶字符串。
- $|y \oplus r| \in \frac{n}{2} \pm \sqrt{n \cdot \text{多对数}(n)}$，但 C'_r 无法计算 $f(y \oplus r) =$ 奇偶性(y)。根据推论 $2^{-\text{多对数}(n)}$，这种情况发生的概率为 30。

利用并合界即可完成证明。 □

上述构造可以推广到其他对称函数（例如，[STV21]）。