arXiv:2611.32163v1 [cs.CC] 24 Nov 2026

AND 函数的低次数环面近似与 ACC^0 电路

Shuhei Osaki Ryuhei Mori

摘要

环面多项式，即模一取值的实多项式，是 Bhrushundi、Hosseini、Lovett 和 Rao 提出的一条通向 ACC^0 下界的路径。我们证明了在每个输入上近似某个函数的环面多项式的次数上界。首先，对于每个 $\epsilon \in (0, 1/4)$，$\mathrm{AND}_n/2$ 都存在一个 ϵ-近似环面多项式，其次数为 $O(\log(n/\epsilon))$，改进了此前的 $O(\log^2(n/\epsilon))$。根据 Krishan 和 Vishwanathan 的下界，对于逆多项式误差而言，该结果在常数因子意义下是最优的，并且推翻了 Krishan 和 Sarma 提出的两个超对数次数猜想。其次，对于由深度为 d、大小为 s 的 $AC^0[m]$ 电路计算的任意布尔函数 g，$g/2$ 都存在一个 ϵ-近似环面多项式，其次数至多为 $C_m^d(\log s)^{\max\{1,\mu-1\}d}\log(1/\epsilon)$；其中，$\mu$ 是 m 的不同素因子个数，而 C_m 仅取决于 m。这改进了 Bhrushundi、Hosseini、Lovett 和 Rao 给出的界 $(\log s)^{O_m(d^2)}(\log(1/\epsilon))^{O_m(d)}$，使 $\log s$ 的指数关于深度呈线性关系，并且关于 $\log(1/\epsilon)$ 的依赖也呈线性关系。两个证明都会对傅里叶展开中的项进行抽样，并用低次数环面多项式对其进行近似。次数为 D 的环面近似可以写成至多 $(n+1)^D$ 个奇偶函数的线性组合，称为周期傅里叶表示；已知这种表示能够通过非自适应测量式量子计算实现线性侧处理，并且每个奇偶函数使用一个量子比特。因此，每个 ACC^0 函数都可以使用准多项式数量的量子比特，并以逆多项式错误概率在每个输入上完成计算。反过来，我们证明，具有 r 个奇偶函数且错误概率为 ϵ 的周期傅里叶表示，能够给出次数为 $O(\log(r/\epsilon))$的环面近似，因此这两个概念是等价的。

1 引言

低次数多项式近似为证明布尔电路的下界提供了一种方法。首先，需要证明给定类别中的每个小规模电路都有低次数近似。随后，利用相同的近似概念，函数的次数下界即可给出电路规模的下界。参见 Beigel [Bei93]和 Williams [Wil14]。

对于 AC^0, , Håstad 使用随机限制和切换引理证明：对于每个固定的 $d \geq 2$ [Hås86]，精确计算奇偶函数的深度-d电路都需要规模为 $\exp(\Omega_d(n^{1/(d-1)}))$。随后，Linial、Mansour 和 Nisan 使用切换引理证明了傅里叶谱在低次项上的集中性，从而得到

在L_2 [LMN93]中用实多项式进行近似。Håstad 和 Tal 对这一近似界的改进表明，与奇偶函数在至少三分之二的所有输入上一致的深度-d电路需要规模为 $\exp(\Omega_d(n^{1/(d-1)}))$[Hås01, Tal 17]。对于 $AC^0[p]$，其中 p 为素数，Razborov 和 Smolensky 使用基于 $\mathbb{F}_p$ 的概率多项式，获得了 MAJORITY 和 Mod_q 的电路规模指数下界，其中 $q \neq p$ 为素数 [Raz87, Smo87]。Kopparty 和 Srinivasan 改进了$p = 2$ [KS18]的次数上界。关于涵盖每个素数 p 的证明，参见 Oliveira 和 Santhanam [OS15]。

为了研究 ACC^0, , 需要一种能够处理模数具有不同素因子的模门的近似模型。Bhrushundi、Hosseini、Lovett 和 Rao 为此提出了环面多项式，并证明 ACC^0 电路具有低次数环面近似 [BHLR19]。环面多项式 P 是一个对模一求值的实多项式。

它通过满足以下条件来近似一个布尔函数 $f\colon \{0,1\}^n \to \{0,1\}$

$$\|P(x) - f(x)/2\|_{\mathbb{T}} \le \epsilon \qquad \forall x \in \{0,1\}^n,$$

其中 $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ 且 $\|a\|_{\mathbb{T}} = \min_{z\in\mathbb{Z}} |a - z|$。因子 $1/2$ 确保两个布尔值模 1 后仍然不同。对于布尔立方体上的实值函数 g，我们用 $\deg_{\mathbb{T},\epsilon}(g)$ 表示满足以下条件的多项式 P 的最低次数：对每个输入，$\|P(x) - g(x)\|_{\mathbb{T}} \le \epsilon$。

我们证明了两个环面逼近界。第一个界取决于傅里叶范数，并在逆多项式误差下，将 AND 函数的次数确定到常数因子范围内。第二个界取决于电路规模和深度，并显式体现模数的不同素因子个数。

傅里叶界与 AND 函数。我们将 $\{0,1\}$ 视为 $\mathbb{F}_2$。对于 $f\colon \mathbb{F}_2^n \to \mathbb{R}$，令 $\|f\|_1$ 为其归一化傅里叶系数绝对值之和。

定理 1。对于任意 $f\colon \mathbb{F}_2^n \to \mathbb{R}$ 和 $\epsilon \in (0, 1/2)$，

$$\deg_{\mathbb{T},\epsilon}(f) = O\left(\log \frac{n(1 + \|\widehat{f}\|_1)}{\epsilon}\right).$$

由于 $\|\mathrm{AND}_n\|_1 = 1$，推论16给出

$$\deg_{\mathbb{T},\epsilon}(\mathrm{AND}_n/2) = O(\log(n/\epsilon)).$$

对于 $\epsilon = n^{-c}$ 固定的 $c > 0$，这与 Krishan 和 Vishwanathan 的 $\Omega(\log(1/\epsilon))$ 下界在常数因子意义下相符 [KV26，定理 6]。特别地，误差为$1/(20n)$时的次数为 $\Theta(\log n)$，这反驳了 Krishan 和 Sarma 的猜想 5 [KS26]。将相同的下界应用于 $\alpha\mathrm{AND}_n$，对于任意固定的 $\alpha \in (0,1)$，同样反驳了他们的猜想 24 [KS26]。

模模电路。即使对于由线性规模、深度为二的 AC^0 电路计算的函数，傅里叶 ℓ_1 范数也可能关于 n 呈指数增长 [BS92]。因此，定理 1 本身无法为所有小型电路给出多对数次数上界。我们的第二个结果利用电路结构，根据电路规模和深度来界定环面近似次数。这里的 $\mathrm{AC}^0[m]$ 电路具有无界扇入的 AND 和 Mod_m 门，以及非门。Mod_m门当其输入之和可被 m整除时恰好输出 1。我们将输入顶点计入电路规模，并且不将非门计入规模或深度。

定理 2。对于每个 $m \ge 2$，存在一个仅取决于 m 的常数 $C_m \ge 1$，使得以下结论成立。设 μ 为 m 的不同素因子个数，并令 $\nu = \max\{1, \mu - 1\}$。对于每个 $n \ge 1$、每个 n-输入 $\mathrm{AC}^0[m]$ 电路 C（其深度至多为 d 且规模至多为 $s \ge 2$），以及每个 $\epsilon \in (0, 1/4)$，

$$\deg_{\mathbb{T},\epsilon}(C/2) \le C_m^d (\log s)^{\nu d} \log(1/\epsilon).$$

当 $\mu \ge 2$时，$\log s$的指数为 $(\mu - 1)\,d$；当 m为素数幂时，该指数为 d。[BHLR19] 中推论 20 的证明给出的次数上界为 $(\log s)^{O_m(d^2)}(\log(1/\epsilon))^{O_m(d)}$。我们的上界使规模对数的指数关于深度呈线性，并且关于 $\log(1/\epsilon)$ 的依赖也呈线性。

表 1 将这一结果与经典多项式逼近界及其改进进行了比较。这里 $s \ge \max\{n, 2\}$ 包含这些输入，$d \ge 2$ 是固定的，而 $\epsilon \in (0, 1/4)$。素数 $p \ne q$ 和模数 m 是固定的，μ 统计 m的不同素因子个数。

这三行采用了不同的逼近保证。对于 AC^0，，存在一个实多项式 P满足 $\|P - f\|_{L_2(U_n)} \le \epsilon$，其中 U_n 是均匀输入分布。对于 $\mathrm{AC}^0[p]$，随机多项式 P满足 $\Pr_P[P(x) \ne f(x)] \le \epsilon$，对每个固定输入 x均成立。对于环面多项式，存在一个多项式 P满足 $\max_x \|P(x) - f(x)/2\|_{\mathbb{T}} \le \epsilon$。

电路类	近似	次数上界	电路规模下界
AC^0	实多项式 $L_2(U_n)$ 错误	$O_d((L+E)^d)$ [LMN93] $O_d(LE(L+E)^{d-2})$ [Hås01] $O_d(L^{d-1}E)$ [Tal17]	奇偶函数$_n$: $\exp(\Omega_d(n^{1/d}))$ [LMN93] $\exp(\Omega_d(n^{1/(d-1)}))$ [Hås86、Hås01、Tal17]
$\mathsf{AC}^0[p]$	$\mathbb{F}_p$ 多项式逐点失败概率	$O_{p,\ d}((L+E)^d)$ [Raz87, Smo87] $O_{p,d}(L^{d-1}E)$ [KS18，OS15]	Mod_q，多数函数$_n$: $\exp(\Omega_{p,q,d}(n^{1/(2d)}))$ [Raz87，Smo87] $\exp(\Omega_{p,q,d}(n^{1/(2(d-1))}))$ [KS18、OS15]
$\mathsf{AC}^0[m]$ $(\mu \geq 2)$	环面多项式 L_∞ 环面误差	$L^{O_m(d^2)}E^{O_m(d)}$ [BHLR19] $O_{m,d}(L^{(\mu-1)d}E)$ 本文（定理 2）	多数函数$_n$: 一个无条件的超多项式下界是开放问题 [BHLR19]。

表 1：多项式逼近界和电路规模下界，其中 $L = \log s$ 和$E = \log(1/\epsilon)$。前两行中的下界涉及精确计算，并可通过取充分小的常数逼近误差得到。

多数函数的条件下界。对于 MAJORITY，足够强的环面次数下界将意味着一个超多项式级的 ACC^0 电路规模下界 [BHLR19]。[BHLR19] 的猜想 5 指出，每个以误差 $1/(20n)$ 逼近 $\mathrm{MAJORITY}_n/2$ 的环面多项式，其次数均为 $\Omega(\sqrt{n}/\log n)$。[BHLR19 的推论 23]证明了对称环面多项式满足这一界。

假设该猜想成立，并固定 $m \geq 2$ 和 $d \geq 1$。如果一个大小为 s 的深度-d $\mathsf{AC}^0[m]$ 电路计算 $\mathrm{MAJORITY}_n$，那么 $1/(20n)$ 误差下的早期次数上界 [BHLR19]给出

$$\sqrt{\frac{n}{\log n}} \leq O_{m,d}\Big((\log s)^{O_m(d^2)}(\log n)^{O_m(d)}\Big).$$

由于 $s \geq n$，我们可以将 $\log n$ 的所有幂吸收到 $\log s$的幂中。解出 s 可得$s \geq \exp(n^{c_m/d^2})$，其中 $c_m > 0$ 仅取决于 m，且对所有充分大的 n均成立。

在相同误差下，定理 2 给出的次数为 $O_{m,\ d}((\log s)^{\nu d}\log n)$。由此，该猜想推出

$$s \geq \exp\left(\Omega_{m,d}\left(\left(\frac{n}{(\log n)^3}\right)^{1/(2\nu d)}\right)\right).$$

这两个下界都表明，在该猜想成立时，多数函数 $\notin \mathsf{ACC}^0$。对于固定的 m，$\log s$ 的下界中 n 的幂次从 c_m/d^2 提升至 $1/(2\nu d)$。

证明思路。对于任意模数 $q \geq 2$，令 $\delta_q(z)$ 在 $z \equiv 0 \pmod q$ 时取 1，否则取 0。两种证明都使用对加权零测试 $\alpha\delta_q(G(x))$ 的近似，其中 α 是实数，G 是整数多项式。当 $q = p^e$ 是素数幂时，有限差分论证可将 δ_q/p^k 模 1 表示为次数至多为 $(q-1)k$ 的有理多项式。对于 $0 < \eta < 1/2$，取 $k = \lceil \log_p(1/(2\eta)) \rceil$，并将 α 舍入到最近的 p^{-k} 整数倍。将所得多项式与 G 复合，误差至多为 η，次数为 $O_q(t\log(1/\eta))$，其中 $t = \deg G$。此界与 α 以及 G 的系数无关。

对于傅里叶界，恒等式

$$(-1)^{\sum_i \gamma_i x_i} = 2\delta_2\left(\sum_i \gamma_i x_i\right) - 1 \qquad \forall \gamma, x \in \{0,1\}^n$$

将奇偶特征与零测试联系起来。若 f 有 $r \geq 1$ 个非零傅里叶系数，将每个系数舍入到最近的 2^{-k} 整数倍，在每个输入上的实值误差至多为 $r2^{-k-1}$ 。取 $k = \lfloor \log(r/\epsilon) \rfloor$ 可将此误差界定为 ϵ，而上述表示随即给出环面次数 $O(\log(r/\epsilon))$。对于一般的 f，傅里叶采样给出 $O(1+n\|\widehat{f}\|_1^2/\epsilon^2)$ 个特征的加权和，该加权和以每个输入上至多为 $\epsilon/2$ 的实值误差近似 f [BS92，O'D14]。以环面误差 $\epsilon/2$ 近似此和，即可证明定理 1。

对于电路，记 $m = \prod_{i=1}^{\mu} p_i^{e_i}$和 $q_i = p_i^{e_i}$。中国剩余定理给出$\delta_m(G(x)) = \prod_{i=1}^{\mu} \delta_{q_i}(G(x))$。我们逐个引入因子。乘以布尔零测试不会改变先前的环面误差。接着，将当前多项式展开为单项式，并对每个系数乘以新的零测试，应用素数幂界。再将这些近似分别乘以相应的布尔单项式并求和，即完成这一步。对于整数仿射 G，所得的 $\alpha\delta_m(G(x))$近似的误差为 η ，次数为

$$O_m((\log(n+1))^{\mu-1}\log(1/\eta)).$$

第6节在电路深度归纳中使用这一界。将输入为原始输入文字或常量的门替换为独立变量，即可降低深度。将深度较小的电路近似为次数为D 的环面多项式后，我们把门函数代回其单项式中。每个单项式都变成仿射模零测试的乘积。特征正交性将这个乘积表示为

$$\prod_{j=1}^{u} \delta_m(G_j(x)) = \mathbb{E}_{\lambda \in \{0,\ldots,m-1\}^u}\left[\cos\left(\frac{2\pi}{m}\sum_{j=1}^{u}\lambda_j G_j(x)\right)\right].$$

我们联合采样单项式和特征。将多项式的系数模一约化，可将其绝对值之和限制在 $(s+1)^D$ 以内。利用集中性和并集界，可得到一个适用于所有输入的样本平均，其样本数的对数至多为$O((D+1)\log s + \log(1/\epsilon))$。每个采样得到的余弦都是 m 个仿射零测试的线性组合，每个剩余类对应一个测试。对每个加权测试应用上述界，并使误差总和至多为 $\epsilon/3$，可得次数

$$O_m((\log s)^{\mu-1}((D+1)\log s + \log(1/\epsilon))).$$

将另外三分之二的误差分配给归纳假设和采样，即可用指数 μd 完成归纳。所有输入共用同一组固定样本，从而得到一个单一的近似多项式。

对于 $\mu \geq 2$，借助附录 A 中描述的电路分解，可将界改进为 $(\mu-1)d$ 。在每个电路高度上，我们依次处理因子 q_1、……、q_μ。按照 Beigel 和 Tarui [BT91 第 5.2 节第 789]，页所述，在相邻高度交替反转这一顺序，使我们能够合并模数相同的相邻映射。复合映射至多包含 $(\mu-1)d+1$ 个布尔映射，每个映射都对应一个素数幂模数。最终映射具有关于该模数的常数次数多项式表示，因此除以二后，其环面近似次数为 $O_m(\log(1/\epsilon))$。其余至多 $(\mu-1)d$ 次代入各贡献一个 $O_m(\log s)$ 因子，由此得到定理 2。

在量子计算中的应用。 低环面次数为 NMQC⊕（采用线性侧处理的非自适应测量式量子计算）所需的量子比特数量提供了上界

通过周期傅里叶表示，我们的电路界为 ACC^0 在逆多项式误差下给出了准多项式量子比特上界。傅里叶采样还为布尔函数 f 提供了 $O(1+n\|\widehat{f}\|_1^2/\epsilon)$ 个量子比特，因此为 AND 函数提供了 $O(n/\epsilon)$ 个量子比特，并且在每个输入上的错误概率至多为 ϵ 。这些构造使用固定的输入奇偶校验以及 GHZ 态上的固定局部测量。

与周期傅里叶表示的联系源于 Werner 和 Wolf [WW01],Hoban、Campbell、Loukopoulos 以及 Browne [HCLB11], , 以及 Mori [Mor19]的工作。他们的结果刻画了每个固定输入分布下的最优值。结合极小极大定理，这给出了随机周期傅里叶表示所能达到的最坏情况误差，其中奇偶函数和系数都可以依赖于随机选择。对于 ACC^0, , 我们的环面近似给出了适用于每个输入的固定周期傅里叶表示。我们还将周期傅里叶表示转换为环面近似，其次数关于其稀疏度以及附加误差的倒数呈对数增长。

组织结构。 第2节回顾相关工作。第3节定义电路类和环面近似次数。第4节证明素幂表示和近似引理，并将近似界推广到合数模数。第5节证明傅里叶界以及关于 AND 函数的推论。第6节证明指数为 μd 的电路界。第7节讨论环面次数与周期傅里叶稀疏度之间的关系，并给出量子构造。第8节总结结果和方法。附录 A 证明 $\mu \geq 2$ 下的定理 2。附录 B 讨论函数度与多项式表示之间的关系，并记录素数幂零测试的精确次数。

2 相关工作

ACC 的多项式表示^0。Beigel 和 Tarui [BT94] 证明，每个 ACC^0函数都有一个准多项式规模的 SYM∘ AND 表示，其底层扇入为多对数级。等价地， $f(x) = h(P(x))$，其中 P是一个次数为多对数级、系数有准多项式上界的整数多项式，而 $h\colon \mathbb{Z} \to \{0, 1\}$ 是任意的。对于固定的 m，Chen 和 Papakonstantinou [CP19] 将深度为-d、规模为-s的 $\mathrm{AC}^0[m]$ 电路的规模上界从 $2^{(\log s)^{2^{O_m(d)}}}$ 改进到 $2^{(\log s)^{O_m(d)}}$。将这种表示转换为环面逼近，还需要控制解码函数 h。

Green、Köbler、Regan、Schwentick 和 Torán [GKR$^+$95]给出了一种表示，其中整数多项式的某个指定比特等于电路输出。 [BHLR19 的定理 19 和推论 20] 中的构造采用了一个加强形式，使该比特两侧均为零。将多项式除以适当的 2 的幂，即可得到环面逼近，其次数上界见引言。

我们在第6节中的直接归纳法使用了 Chen 和 Papakonstantinou 对模零测试的乘积 [CP19] 进行线性化时得到的特征展开。他们将该展开转化为关于辅助互素模数的整数同余。我们取其实部，并联合采样单项式和特征。对由此得到的加权零测试进行逼近，可得指数为 μd 且对 $\log(1/\epsilon)$ 呈线性依赖的界。对于 $\mu \geq 2$，利用附录 A 中的电路分解，可进一步将界改进至 $(\mu-1)d$ 。

AND 函数的环面次数。Krishan 和 Vishwanathan 曾提出疑问：对于 AND 函数，已知的 $O(\log^2(n/\epsilon))$上界是否可以改进到与其在逆多项式误差 [下的下界相匹配 4]KV26，引理17及开放问题。Krishan 和 Sarma 将其次数猜想表述为获得某些三层模电路规模下界的一种途径 [KS26]。

Krishan 和 Vishwanathan 还证明了：每个以误差 $1/(20n)$逼近 $\mathrm{AND}_n/2$ 的对称环面多项式，其次数均为 $\Omega(\sqrt{n}/\log\ n)$ [KV26，定理 7]。我们的构造使用次数为 $O(\log(n/\epsilon))$的环面多项式逼近 $\mathrm{AND}_n/2$，误差为 ϵ；该多项式不必是对称的。

傅里叶采样。 Bruck 和 Smolensky [BS92]使用傅里叶采样构造稀疏多项式阈值表示。另见 Siu 和 Bruck [SB91]。定理 1 中使用的实值一致近似界见 O'Donnell 的定理 5.12，历史注记见第 5 [O'D14]章。我们将其与定理 14 中从傅里叶稀疏度到环面次数的转换结合起来。[BHLR19 的引理 14] 也使用采样，将概率性的有限域近似转换为一个环面多项式，使其在每个输入上都能近似目标函数。

周期傅里叶表示。 周期傅里叶表示给出了 $\mathrm{NMQC}_{\oplus}$ [HCLB11、Mor19] 的 GHZ态实现。在无误差情形下，非恒定布尔函数的最小周期傅里叶稀疏度等于所需量子比特的最小数量。对于一个定义在 n 位上的非恒定布尔函数 f，Mori [Mor19 的构造 2 和定理 1]给出

$$2^d - 1 \le \mathsf{pfs}_0(f) \le n^d, \qquad d = \deg_{\mathbb{F}_2}(f),$$

其中，$\mathsf{pfs}_0(f)$ 表示精确周期傅里叶表示中非恒定奇偶特征的最小数量。因此，在无误差情形下，一个布尔函数族具有多对数 $\mathbb{F}_2$次数，当且仅当它具有准多项式周期傅里叶稀疏度。在有界误差情形下，同样的对应关系刻画了固定输入分布下的最优平均误差。相比之下，我们的逐点近似界给出了一个适用于每个输入的单一周期傅里叶多项式。

3 预备知识

3.1 符号

全文中，log 表示以 2 为底的对数，exp 表示自然指数函数。我们记作 $[n] = \{1, \ldots\ldots, n\}$。除非明确称为函数次数，否则所有多项式次数均指通常的总次数。在布尔立方体上，我们将多项式多重线性化，而不改变其函数值，也不增加其次数。

3.2 电路类

AC电路由无界扇入的 AND 门和非门组成。允许将常数作为门的输入。其深度 是电路中一条有向路径上非 NOT 门的最大数量。其规模 是非 NOT 门的数量与输入比特数量之和。根据德摩根定律，允许使用或门不会改变该模型。我们在对数表达式中使用规模上界 $s \ge 2$。对于规模为 1 的电路，令 $s = 2$。

定义 3（类 AC^0）。一族布尔函数 $(f_n\colon \{0,1\}^n \to \{0,1\})_{n\ge 1}$ 属于 AC^0，如果存在非负整数 c, d, k 以及 AC 电路 $(C_n)_{n\ge 1}$，使得 C_n 计算f_n，深度至多为 d，大小至多为 cn^k，对每个 $n \ge 1$均成立。

对于 $m \ge 2$，Mod_m 门定义如下

$$\mathsf{Mod}_m(x_1, \ldots, x_n) = \begin{cases} 1, & x_1 + \cdots + x_n \equiv 0 \pmod m, \\ 0, & \text{otherwise.} \end{cases}$$

$\mathsf{AC}[m]$ 电路还可以使用 Mod_m 门。其深度和大小的定义与上文相同，其中 Mod_m 门计作非 NOT 门。

定义 4（类 $\mathsf{AC}^0[m]$）。如果存在非负整数 c, d, k 以及 $\mathsf{AC}[m]$ 电路 $(C_n)_{n\geq 1}$，使得对于每个 $n \geq 1$，C_n 都计算 f_n，深度至多为 d，规模至多为 cn^k，那么布尔函数族 $(f_n)_{n\geq 1}$ 属于 $\mathsf{AC}^0[m]$。

定义 5（类 ACC^0）。类 ACC^0 是以下各类的并集

$$\mathsf{ACC}^0 = \bigcup_{m\geq 2} \mathsf{AC}^0[m].$$

特别地，在每个电路族中，模数都是固定的。

3.3 环面多项式

设 $\mathbb{T} = \mathbb{R}/\mathbb{Z}$。

定义 6（环面多项式 [BHLR19]）。函数 $P\colon \{0,1\}^n \to \mathbb{T}$ 是次数至多为 d 的环面多项式，当且仅当存在实系数 α_S 使得

$$P(x) = \sum_{\substack{S\subseteq[n]\\ |S|\leq d}} \alpha_S \prod_{i\in S} x_i \pmod 1.$$

定义 7（环面上到零的距离）。对于 $\alpha \in \mathbb{R}$，令

$$\|\alpha\|_{\mathbb{T}} = \min_{z\in\mathbb{Z}} |\alpha - z|.$$

这定义了 $\mathbb{T}$中到零的距离。

$\alpha, \beta \in \mathbb{T}$ 之间的距离为 $\|\alpha - \beta\|_{\mathbb{T}}$。它满足三角不等式

$$\|\alpha - \gamma\|_{\mathbb{T}} \leq \|\alpha - \beta\|_{\mathbb{T}} + \|\beta - \gamma\|_{\mathbb{T}} \qquad \forall \alpha, \beta, \gamma \in \mathbb{T},$$

这可由 $\mathbb{R}$ 中的三角不等式通过对整数移位取最小值推出。

定义 8（环面近似次数）。设 $f\colon \{0,1\}^n \to \mathbb{R}$ 且 $\epsilon > 0$。若环面多项式P ϵ-近似 f，则

$$\|P(x) - f(x)\|_{\mathbb{T}} \leq \epsilon \qquad \forall x \in \{0,1\}^n.$$

此类多项式的最小次数记为 $\deg_{\mathbb{T},\epsilon}(f)$。对于常数近似多项式（包括零多项式），我们将次数记为零。

该定义允许任意实值目标。对于布尔函数 f，[BHLR19] 的约定对应于 $\deg_{\mathbb{T},\,\epsilon}(f/2)$。对于这一目标，我们将范围限制为 $\epsilon \in (0,\ 1/4)$：常数多项式 $P = 1/4$ 对每个布尔函数都已经给出误差 $1/4$。

4 模零测试的逼近

对于 $m \geq 2$ 和 $z \in \mathbb{Z}$，令 $\delta_m(z)$ 在 $z \equiv 0 \pmod m$ 时取 1，否则取 0。对于 $q = p^e$，我们首先用次数至多为 $(q-1)k$ 的多项式表示 δ_q/p^k modulo 1，然后通过系数舍入来近似 $\alpha\delta_q(G(x))$。接着，我们将近似界推广到任意模数。

引理 9 (素幂表示). 设 $q = p^e$，其中 p 是素数且 $e \geq 1$。对于每个整数 $k \geq 1$，存在一个多项式 $Q_{q,k} \in \mathbb{Q}[z]$，其次数至多为 $(q-1)k$，使得

$$Q_{q,k}(z) = \frac{\delta_q(z)}{p^k} \pmod 1 \qquad \forall z \in \mathbb{Z}.$$

证明。对于取整数值的 q-周期函数，令 $Tf(z) = f(z+1)$ 且 $\Delta = T - I$。由于$q = p^e$，对 $\mathbb{F}_p$ 求和的恒等式 $(1+X)^q = 1 + X^q$ 表明，对于 $1 \leq j < q$，p 整除 $\binom{q}{j}$。由于$T^q = I$，我们得到

$$\Delta^q = -\sum_{j=1}^{q-1} \binom{q}{j} \Delta^j = p\Delta A(\Delta)$$

对于某个 $A \in \mathbb{Z}[X]$。由归纳法可得

$$\Delta^{k(q-1)+1} = p^k \Delta A(\Delta)^k \equiv 0 \pmod{p^k}.$$

令 $d = (q-1)k$。对于 $0 \leq j \leq d$，选取 $a_j \in \{0, \ldots, p^k - 1\}$ 使得 $a_j \equiv (\Delta^j \delta_q)(0)$（模 p^k）。对于 $z \geq 0$，利用二项式定理展开 $T^z = (I + \Delta)^z$。由于 Δ^{d+1} 模 p^k会消去每个取整数值的 q-周期函数，因此，Δ 的幂次大于 d的所有项都模 p^k消失。因此

$$\begin{aligned}
\delta_q(z) &= (T^z \delta_q)(0) \\
&= \big((I+\Delta)^z \delta_q\big)(0) \\
&\equiv \sum_{j=0}^{d} \binom{z}{j} (\Delta^j \delta_q)(0) \\
&\equiv \sum_{j=0}^{d} a_j \binom{z}{j} \pmod{p^k}.
\end{aligned}$$

对于负的 z，同样的展开也成立，其中 $\binom{z}{j} = z(z-1)\cdots(z-j+1)/j!$ 且 $\binom{z}{0} = 1$。事实上，幂零性给出

$$T^{-1} = (I+\Delta)^{-1} \equiv \sum_{j=0}^{d} (-1)^j \Delta^j \pmod{p^k}.$$

将这个有限展开提升到 $-z$ 次幂，即得到 T^z 的广义二项式展开，其中所有高于 d 次的幂再次都模 p^k 消失。

定义

$$Q_{q,k}(z) = \frac{1}{p^k} \sum_{j=0}^{d} a_j \binom{z}{j}.$$

上述同余意味着

$$Q_{q,k}(z) - \frac{\delta_q(z)}{p^k} = \frac{\sum_{j=0}^{d} a_j \binom{z}{j} - \delta_q(z)}{p^k} \in \mathbb{Z} \qquad \forall z \in \mathbb{Z}.$$

因此，对于每个整数 z，$Q_{q,k}(z) = \delta_q(z)/p^k$ 模 1。由于 $\binom{z}{j}$ 是次数为 j 的有理多项式，我们还有 $\deg Q_{q,k} \leq d = (q-1)k$。 □

$Q_{q,k}$ 的精确次数为

$$(p-1)p^{e-1}k + p^{e-1} - 1 = (q-1)k - (p^{e-1} - 1)(k-1).$$

附录 B 证明了这个公式及其最优性。较简单的界 $(q-1)k$ 足以用于下文的逼近论证。

备注 （通过模数放大的另一种表示）。 引理 9 中表示的一种替代构造使用了 Beigel–Tarui 的模数放大多项式 [BT94]。令 $q = p^e$。对于 $z \geq 0$，Lucas 定理表明，$\binom{z}{p^j} \bmod p$ 是 z 在 $0 \leq j < e$时的第 j 个 p 进制数字。因此，由费马小定理可得

$$H_q(z) = \prod_{j=0}^{e-1} \left(1 - \binom{z}{p^j}^{p-1}\right) \equiv \delta_q(z) \pmod{p}.$$

这里， H_q 是一个次数为 $q-1$ 的整数值有理多项式。由于乘积中的二项式系数模 p 具有 q 周期性，该同余对每个 $z \in \mathbb{Z}$ 都成立。对于 $e = 1$，这就是通常的测试 $H_p(z) = 1 - z^{p-1}$。

令 $A_k \in \mathbb{Z}[X]$ 为次数为 $2k-1$ 的模数放大多项式，满足

$$A_k(u) \equiv b \pmod{p^k} \quad \text{whenever } u \equiv b \pmod{p}, \quad b \in \{0, 1\}$$

如 BHLR19 中的引理 10]所述， [。于是

$$\widetilde{Q}_{q,k}(z) = \frac{A_k(H_q(z))}{p^k} \equiv \frac{\delta_q(z)}{p^k} \pmod{1}, \qquad \deg \widetilde{Q}_{q,k} \leq (q-1)(2k-1).$$

引理 9 给出了次数上界 $(q-1)k$。由于 $(q-1)(2k-1) < 2(q-1)k$，上述构造也足以满足后续各节中的渐近上界。

将权重舍入到最接近的 p^{-k} 整数倍，即得到下文使用的近似。

引理 10 (素数幂近似**)。** 设 $q = p^e$，其中 p 是素数且 $e \geq 1$。对于每个 $\alpha \in \mathbb{R}$， $\epsilon \in (0,\ 1/2)$，以及次数至多为 t 的整数多项式 $G \in \mathbb{Z}[x_1, \ldots, x_n]$，

$$\mathsf{deg}_{\mathbb{T},\epsilon}(\alpha \delta_q(G(x))) \leq t(q-1)\log(1/\epsilon).$$

证明。 设 $k = \lceil \log_p(1/(2\epsilon)) \rceil \geq 1$，并选取满足 $|\alpha - c/p^k| \leq 1/(2p^k) \leq \epsilon$ 的 $c \in \mathbb{Z}$。根据引理 9， $cQ_{q,\ k}(G(x))$ 对每个布尔 x模一等于 $(c/p^k)\delta_q(G(x))$。由于 δ_q 是布尔值，这以至多 ϵ 的环面误差近似了 $\alpha\delta_q(G(x))$。其次数至多为 $t(q-1)k$，并且

$$k \leq 1 + \frac{\log(1/\epsilon) - 1}{\log p} \leq \log(1/\epsilon).$$

多线性化不会增加次数。 □

下一个引理将引理 10 推广到任意模数。我们通过对不同素因子的数量进行归纳来证明它。

引理 11 (合数模数近似**)。** 设 $m = \prod_{i=1}^{\mu} p_i^{e_i}$，其中 p_i 是不同的素数，并设 $n, t \geq 1$。对于任意 $\alpha \in \mathbb{R}$, $\epsilon \in (0, 1/2)$，以及次数至多为 t 的整数多项式 $G \in \mathbb{Z}[x_1, \ldots, x_n]$，

$$\mathsf{deg}_{\mathbb{T},\epsilon}(\alpha \delta_m(G(x))) \leq (m-1)t^{\mu}(\log(n+1))^{\mu-1}\log(\mu/\epsilon).$$

证明。 我们对 μ 进行归纳。 $\mu = 1$ 的情形即为引理 10。对于 $\mu \geq 2$，令

$$q_i = p_i^{e_i}, \qquad m' = \prod_{i=1}^{\mu-1} q_i, \qquad L = \log(n+1), \qquad \lambda = \log(\mu/\epsilon).$$

中国剩余定理给出

$$\delta_m(G(x)) = \delta_{q_\mu}(G(x))\delta_{m'}(G(x)).$$

将误差为 $(\mu-1)\epsilon/\mu$ 的归纳假设应用于此。我们得到一个次数至多为

$$d=(m'-1)t^{\mu-1}L^{\mu-2}\lambda$$

使得

$$\|P(x)-\alpha\delta_{m'}(G(x))\|_{\mathbb{T}}\le\frac{(\mu-1)\epsilon}{\mu}\qquad\forall x\in\{0,1\}^n.$$

乘以布尔值 $\delta_{q_\mu}(G(x))$不会增大此误差界。因此

$$\|\delta_{q_\mu}(G(x))P(x)-\alpha\delta_m(G(x))\|_{\mathbb{T}}\le\frac{(\mu-1)\epsilon}{\mu}.$$

记 $x_S=\prod_{i\in S}x_i$，并选取一个实数表示 $P(x)=\sum_{|S|\le d}\alpha_S x_S$。此和中至多有 $(n+1)^d$ 项。由引理 10，对于每个 S，都存在一个次数至多为

$$t(q_\mu-1)\log\frac{\mu(n+1)^d}{\epsilon}=t(q_\mu-1)(\lambda+dL)$$

的环面多项式 $\alpha_S\delta_{q_\mu}$，其对 $G(x)$ 的近似误差至多为 $\epsilon/(\mu(n+1)^d)$。由于 $x_S\in\{0,1\}$，多项式

$$R(x)=\sum_{|S|\le d}P'_S(x)x_S$$

以至多 ϵ/μ 的误差近似 $\delta_{q_\mu}(G(x))P(x)$。因此，R 以至多 ϵ的误差近似 $\alpha\delta_m(G(x))$。其次数至多为

$$\begin{aligned}d+t(q_\mu-1)(\lambda+dL)&=d(1+t(q_\mu-1)L)+t(q_\mu-1)\lambda\\&\le dtq_\mu L+t(q_\mu-1)\lambda\\&\le\big((m'-1)q_\mu+(q_\mu-1)\big)t^\mu L^{\mu-1}\lambda\\&=(m-1)t^\mu L^{\mu-1}\lambda,\end{aligned}$$

其中我们用到了 $t,L\ge1$。 □

5 基于傅里叶界的环面逼近

我们将$\{0,1\}$ 视为 $\mathbb{F}_2$，并使用归一化傅里叶变换。背景介绍请参见 [O'D14]。对于 $\gamma,x\in\mathbb{F}_2^n$，令 $\langle\gamma,x\rangle=\sum_{i=1}^n\gamma_i x_i$属于 $\mathbb{F}_2$。我们也用子集为特征编索引$S\subseteq[n]$，将 S 视为其指示向量。

定义 12（傅里叶系数）。对于 $f\colon\ \mathbb{F}_2^n\to\mathbb{R}$，定义

$$\widehat{f}(\gamma)=\mathbb{E}_{x\in\mathbb{F}_2^n}[f(x)(-1)^{\langle\gamma,x\rangle}],\qquad\forall\gamma\in\mathbb{F}_2^n,$$

其中 x 服从均匀分布。

傅里叶反演给出

$$f(x)=\sum_{\gamma\in\mathbb{F}_2^n}\widehat{f}(\gamma)(-1)^{\langle\gamma,x\rangle}.$$

定义 13（傅里叶稀疏度）。$f\colon\ \mathbb{F}_2^n\to\mathbb{R}$ 的傅里叶稀疏度为

$$\mathrm{sparsity}(\widehat{f})=\big|\{\gamma\in\mathbb{F}_2^n:\widehat{f}(\gamma)\ne0\}\big|.$$

我们首先通过傅里叶稀疏度界定环面次数。将非零傅里叶系数舍入为具有公共分母 2^k的有理数。由于特征取值于 $\{\pm1\}$ 中，系数误差之和界定了每个输入上的误差。随后，引理 9 将每个加权特征模一表示为次数至多为 $k-1$ 的形式。

定理 m 14（（基于傅里叶稀疏度的近似）。 对于每个 $f\colon \mathbb{F}_2^n \to \mathbb{R}$ 以及 $\epsilon \in (0,\ 1/2)$ ，

$$\deg_{\mathbb{T},\epsilon}(f) \le \log \frac{\max\{1, \mathrm{sparsity}(\widehat{f})\}}{2\epsilon}.$$

证明。 设 $r = \mathrm{sparsity}(f)$。若 $r = 0$，则 $f = 0$ ，结论显然成立。否则，令$k = \lfloor \log(r/\epsilon)\rfloor \ge 1$。对每个 γ，选取 $c_\gamma \in \mathbb{Z}$ 使得

$$\left|\widehat{f}(\gamma) - \frac{c_\gamma}{2^k}\right| \le 2^{-k-1},$$

在 $f(\gamma) = 0$时取 $c_\gamma = 0$ 。定义

$$\widetilde{f}(x) = \sum_\gamma \frac{c_\gamma}{2^k}(-1)^{\langle \gamma, x\rangle}.$$

傅里叶反演给出

$$|f(x) - \widetilde{f}(x)| \le r2^{-k-1} \le \epsilon \qquad \forall x \in \mathbb{F}_2^n.$$

此外,

$$\widetilde{f}(x) = \sum_\gamma \frac{c_\gamma}{2^{k-1}} \delta_2\left(\sum_{i=1}^n \gamma_i x_i\right) - \sum_\gamma \frac{c_\gamma}{2^k}.$$

若 $k \ge 2$，引理 9 给出一个 f 的环面多项式表示，其次数至多为 $k-1$。若$k = 1$，则狄拉克函数项具有整数系数，因此 f 模一为常数，且同样的界仍然成立。无论哪种情况,

$$\deg_{\mathbb{T},\epsilon}(f) \le k - 1 \le \log \frac{r}{2\epsilon}.$$

□

定义 15（傅里叶 ℓ_1 范数）。 函数 f 的傅里叶 ℓ_1 范数为: $\mathbb{F}_2^n \to \mathbb{R}$ 是

$$\|\widehat{f}\|_1 = \sum_{\gamma \in \mathbb{F}_2^n} |\widehat{f}(\gamma)|.$$

一个函数可能有许多非零傅里叶系数，但傅里叶 ℓ_1 范数却很小。在应用定理 14 之前，采样会缩小支集。Bruck 和 Smolensky [BS92]，在 O'Donnell [O'D14, 定理 5.12]，中提出的论证，以通常的实值距离对这类函数进行一致逼近。我们纳入这一论证，以便跟踪误差和样本数量。

定理 1（重述）。 对于每个 $f\colon \mathbb{F}_2^n \to \mathbb{R}$ 以及 $\epsilon \in (0,\ 1/2)$ ，

$$\deg_{\mathbb{T},\epsilon}(f) = O\left(\log \frac{n(1 + \|\widehat{f}\|_1)}{\epsilon}\right).$$

证明。 当 $f = 0$ 时结论显然成立。否则，以概率 $|f(\gamma)|/\|f\|_1$ 选择 γ，并定义

$$X_\gamma(x) = \|\widehat{f}\|_1 \ \mathrm{sgn}(\widehat{f}(\gamma))(-1)^{\langle \gamma, x\rangle}.$$

然后 $|X_\gamma(x)| = \|f\|_1$和 $\mathbb{E}_\gamma[X_\gamma(x)] = f(x)$。令

$$M = \left\lceil \frac{8(n+2)\|\widehat{f}\|_1^2}{\epsilon^2} \right\rceil$$

并从该分布中独立地选择 $\gamma^{(1)}, \ldots, \gamma^{(M)}$。对于每个固定的 x，霍夫丁不等式 [Hoe63] 给出

$$\Pr\left[\left|\frac{1}{M}\sum_{j=1}^{M} X_{\gamma^{(j)}}(x) - f(x)\right| > \frac{\epsilon}{2}\right] \le 2\exp\left(-\frac{\epsilon^2 M}{8\|\widehat{f}\|_1^2}\right) \le 2^{-(n+1)}.$$

A 因此，对所有 2^n 输入应用并集界可知，存在某种样本选择满足

$$\left|\frac{1}{M}\sum_{j=1}^{M} X_{\gamma^{(j)}}(x) - f(x)\right| \le \frac{\epsilon}{2} \qquad \forall x \in \{0,1\}^n.$$

固定这样一种选择，并令 $g(x) = M^{-1}\sum_{j=1}^{M} X_{\gamma^{(j)}}(x)$。其傅里叶稀疏度至多为 M。定理 14 给出了一个对 g 进行 $\epsilon/2$-逼近的环面多项式，其次数至多为 $\log(M/\epsilon)$。该多项式对 f 的逼近误差至多为 ϵ。最后，

$$M \le 1 + \frac{8(n+2)\|\widehat{f}\|_1^2}{\epsilon^2}$$

^意味着 $\log(M/\epsilon) = O(\log(n(1+\|f\|_1)/\epsilon))$。 □

^由于 $\|\mathsf{AND}_n\|_1 = 1$，我们立即得到以下界。

推论16。 对于每个 $n \ge 1$ 和 $\epsilon \in (0, 1/4)$，

$$\deg_{\mathbb{T},\epsilon}(\mathsf{AND}_n/2) = O(\log(n/\epsilon)).$$

^备注。更一般地，对于每个固定的 $\alpha \in (0,1)$，$\|\alpha\mathsf{AND}_n\|_1 = \alpha$，因此定理 1 给出

$$\deg_{\mathbb{T},\epsilon}(\alpha\mathsf{AND}_n) = O(\log(n/\epsilon)).$$

对于固定的 $c > 0$，目标 $\mathsf{AND}_n/2$ 和 $\epsilon = n^{-c}$，推论16与已知下界 [KV26] 相差一个常数因子以内。该下界无法确定常数误差下的最优次数。

备注 （AND 函数的显式构造）。对于 AND 函数，小偏差空间为傅里叶采样提供了一种确定性替代方案。设 S 是 $\mathbb{F}_2^n$ 中的一个 η-偏差多重集，即对每个非零 $y \in \mathbb{F}_2^n$，都有 $|\mathbb{E}_{a\in S}[(-1)^{\langle a,\ y\rangle}]| \le \eta$。显式构造给出 $|S| = \mathrm{poly}(n/\eta)$ [NN93, AGHP92]。于是

$$P_S(x) = \frac{1}{2|S|}\sum_{a\in S}(-1)^{\langle a, \mathbf{1}-x\rangle} \qquad \text{satisfies} \qquad \|P_S - \mathsf{AND}_n/2\|_\infty \le \eta/2.$$

事实上，$P_S(\mathbf{1}) = 1/2$，并且小偏差条件适用于其他每个输入。对于 $0 < \epsilon < 1/4$，取 $\eta = \epsilon$，并在误差为 $\epsilon/2$ 的情况下应用定理 14 中的系数舍入构造。由于 P_S 的傅里叶稀疏度至多为 $|S|$，这给出了一个对 $\mathsf{AND}_n/2$ 进行 ϵ-逼近的环面多项式，其次数为 $O(\log(n/\epsilon))$。

即使对于小型二层电路，傅里叶 ℓ_1 范数也可能随输入数量呈指数增长 [BS92]。例如，

$$f(x,y) = \prod_{j=1}^{r}(1 - x_j y_j) \qquad \text{has} \qquad \|\widehat{f}\|_1 = (3/2)^r.$$

该函数有一个深度为二、规模为 $O(r)$ 的 AC^0 电路。每个因子的傅里叶 ℓ_1 范数为 $3/2$，且由于各因子分别依赖于互不相交的变量对，这些范数会相乘。因此，仅凭定理 1 并不能为所有小型电路给出多对数界。下一节将利用门结构来获得这样的界。

6 从模电路到环面多项式

我们利用引理 11，通过深度归纳直接证明指数为 μd 的电路近似界。在每一步中，我们都将门替换为其输入为原始输入文字或常量的门。对于 $\mu = 1$，这就证明了定理 2。对于 $\mu \geq 2$，附录 A 给出了分解论证，可将指数改进为 $(\mu - 1)d$。

命题 17. 对于每个 $m \geq 2$，都存在一个仅依赖于 m 的常数 $A_m \geq 1$，使得下述结论成立。设 μ 为 m 的不同素因子个数。对于每个 n输入$\mathsf{AC}^0[m]$ 深度至多为 d、电路规模至多为 $s \geq 2$的电路 C，以及每个 $\epsilon \in (0,\ 1/4)$，

$$\mathsf{deg}_{\mathbb{T},\epsilon}(C/2) \leq A_m^d (\log s)^{\mu d} \log(1/\epsilon).$$

证明。 我们将证明如下界

$$\mathsf{deg}_{\mathbb{T},\epsilon}(C/2) \leq B_m^d (\log(s+1))^{\mu d} \log(1/\epsilon),$$

其中 $B_m \geq 1$是一个仅依赖于 m的常数，具体取值将在下文确定。由于对于 $s \geq 2$，有 $\log(s+1) \leq 2 \log s$，因此取 $A_m = 2^{\mu} B_m$即可得到所述界。令 $L = \log(s+1)$，且 $E = \log(1/\epsilon)$，于是 $L,\ E \geq 1$。将每个与门替换为一个所有输入均取反的或非门。这样不会改变电路规模或深度。我们对 d进行归纳。若 $d = 0$，则输出为常数或输入文字，因此 $C/2$ 可由次数至多为一的环面多项式精确表示。

假设 $d \geq 1$ 并且该界对深度至多为 $d-1$时成立。我们将归纳步骤分为三个部分。

应用归纳假设。令 k 表示其所有输入均为原始输入文字或常数的门的数量，并令它们的输出为 $h_{n+1}(x)$,..... $h_{n+k}(x)$。令$r = n + k$，并令 $h_a(x) = x_a$ 对 $1 \leq a \leq n$成立。将这些 k 门替换为新的相互独立的输入变量，同时保留原始输入，从而得到一个电路 C'，满足

$$C(x) = C'(h_1(x), \ldots, h_r(x)).$$

考虑经过剩余门的任意路径。其第一个门未被移除，因此在 C 其某个输入（除相应的取反外）是另一个门的输出；沿着这样的输入向下追踪，最终会到达一个被移除的门。将这条链添加到该路径的前端，便至少在原电路中增加了一个门。因此，C' 的深度至多为 $d-1$。它有 r 个输入，以及至多 $s - n - k$ 个非 NOT 门。因此，其规模至多为

$$r + (s - n - k) = s.$$

因此，在归纳假设中可以使用相同的大小界 s。

根据该假设，存在一个环面多项式 P，满足

$$\|C'(y)/2 - P(y)\|_{\mathbb{T}} \leq \epsilon/3 \qquad \forall y \in \{0,1\}^r,$$

其次数 D 满足

$$D \leq B_m^{d-1} L^{\mu(d-1)} \log(3/\epsilon). \tag{1}$$

每个布尔单项式的取值都属于{0,1}，因此将系数改变一个整数不会改变这个取值为环面值的函数。因此我们可以写成

$$P(y) = \sum_{S \in \mathcal{U}} \alpha_S \prod_{a \in S} y_a \pmod 1, \qquad \mathcal{U} = \{S \subseteq [r] : |S| \leq D\},$$

其中 $\alpha_S \in [-1/2, 1/2)$。令

$$K = |\mathcal{U}|, \qquad A = \sum_{S \in \mathcal{U}} |\alpha_S|.$$

于是 $K \le (r+1)^D \le 2^{DL}$ 且 $A \le K/2$。如果 $A = 0$，那么零多项式已经给出了所需的近似，因此假设 $A > 0$。定义实值函数

$$b_S(x) = \prod_{a \in S} h_a(x), \qquad Q(x) = \sum_{S \in \mathcal{U}} \alpha_S b_S(x).$$

代入 P 可得

$$\|C(x)/2 - Q(x)\|_{\mathbb{T}} \le \epsilon/3 \qquad \forall x \in \{0,1\}^n. \tag{2}$$

将零测试的乘积替换为一个短和。 每个 b_S 都是整数仿射多项式的模零测试之积。为说明这一点，将被移除门的输入文字写成 $\ell_j(x) \in \{x_i, 1 - x_i, 0, 1\}$ 并使用

$$\begin{aligned}
\mathsf{NOR}(\ell_1(x), \ldots, \ell_u(x)) &= \prod_{j=1}^{u} \delta_m(\ell_j(x)), \\
\mathsf{Mod}_m(\ell_1(x), \ldots, \ell_u(x)) &= \delta_m\left(\sum_{j=1}^{u} \ell_j(x)\right), \\
x_i &= \delta_m(x_i - 1).
\end{aligned}$$

因此，对于某些整数仿射多项式 $G_{S,1}, \ldots, G_{S,u_S}$，

$$b_S(x) = \prod_{j=1}^{u_S} \delta_m(G_{S,j}(x)).$$

根据特征正交性，如同展开 [CP19], 时一样

$$\begin{aligned}
b_S(x) &= \mathbb{E}_{\lambda \in \{0,\ldots,m-1\}^{u_S}} \left[\exp\left(\frac{2\pi i}{m} \sum_{j=1}^{u_S} \lambda_j G_{S,j}(x)\right)\right] \\
&= \mathbb{E}_{\lambda} \left[\cos\left(\frac{2\pi}{m} G_{S,\lambda}(x)\right)\right],
\end{aligned}$$

其中 $G_{S,\lambda}(x) = \sum_{j=1}^{u_S} \lambda_j G_{S,j}(x)$.

为用一个短和近似 Q ，我们将这些期望合并为一个，然后用样本平均来近似它。以概率 $|\alpha_S|/A$ 抽取一个索引 $S \in \mathcal{U}$ ，并在给定 S的条件下，从 $\{0, \ldots, m-1\}^{u_S}$ 中均匀抽取 λ。定义随机函数

$$Z(x) = \operatorname{sgn}(\alpha_S) \cos\left(\frac{2\pi}{m} G_{S,\lambda}(x)\right).$$

然后 $|Z(x)| \le 1$ 和

$$A\mathbb{E}[Z(x)] = A \sum_{S \in \mathcal{U}} \frac{|\alpha_S|}{A} \operatorname{sgn}(\alpha_S) b_S(x) = Q(x).$$

Take

$$M = \left\lceil \frac{18(s+1)A^2}{\epsilon^2} \right\rceil$$

独立样本 Z_1、.....、Z_M。对于每个固定输入 x，由霍夫丁不等式 [Hoe63] 可得

$$\Pr\left[\left|\frac{A}{M} \sum_{j=1}^{M} Z_j(x) - Q(x)\right| > \epsilon/3\right] \le 2\exp\left(-\frac{\epsilon^2 M}{18A^2}\right) < 2^{-s}.$$

由于 $n \le s$，对所有 2^n 输入应用并集界，失败概率严格小于一。因此，我们可以固定这些样本并定义

$$\widetilde{Q}(x) = \frac{A}{M} \sum_{j=1}^{M} Z_j(x)$$

因此

$$|\widetilde{Q}(x) - Q(x)| \le \epsilon/3 \qquad \forall x \in \{0,1\}^n. \tag{3}$$

近似采样项。对于每个整数仿射多项式 $G_{S,\ \lambda}$，

$$\cos\left(\frac{2\pi}{m} G_{S,\lambda}(x)\right) = \sum_{a=0}^{m-1} \cos\left(\frac{2\pi a}{m}\right) \delta_m(G_{S,\lambda}(x) - a).$$

因此，$\widetilde{Q}$ 是至多 Mm 个模零测试的线性组合。对每个带权测试应用引理 11，取 $t = 1$ 和误差 $\epsilon/(3Mm)$，并将所得多项式相加。由此得到一个环面多项式 P_{new}，满足

$$\|\widetilde{Q}(x) - P_{\mathrm{new}}(x)\|_{\mathbb{T}} \le \epsilon/3 \qquad \forall x \in \{0,1\}^n \tag{4}$$

and

$$\deg P_{\mathrm{new}} \le (m-1)(\log(n+1))^{\mu-1} \log \frac{3\mu M m}{\epsilon}.$$

合并 通过三角不等式将 (2)、(3) 和 (4) 合并，可证明 P_{new} ϵ 近似 $C/2$.

剩下的任务是界定其次数。由于 $A \le K/2$，我们有 $M \le 5(s+1)K^2/\epsilon^2$。结合 $K \le 2^{DL}$，可得

$$\deg P_{\mathrm{new}} = O_m\big(L^{\mu-1}((D+1)L + E)\big).$$

利用 (1)、$\log(3/\epsilon) \le 3E$ 和 $B_m,\ L,\ E \ge 1$，我们得到

$$\deg P_{\mathrm{new}} \le c_m B_m^{d-1} L^{\mu d} E$$

其中常数 c_m 仅取决于 m。取 $B_m \ge \max\{1,\ c_m\}$ 即可完成归纳法。 □

7 量子计算的应用

7.1 周期傅里叶多项式与平均误差

现在，我们利用环面近似次数和傅里叶采样，来界定非自适应测量式量子计算（带线性侧处理，记作 NMQC⊕）所需的量子比特数。在 NMQC⊕ 中，资源态、每个量子比特可用的两种二元测量，以及输入奇偶校验都在给定输入之前固定。每个输入奇偶校验会选定两种局部测量中的一种。测量选择不依赖测量结果，输出则是这些结果的奇偶函数。我们首先陈述平均误差情形下与周期傅里叶多项式的对应关系。应用极小极大定理可得共享经典随机性能够选择协议时的最优最坏情况误差。我们的上界将使用固定表示。

将从 $\mathbb{T}$ 到单位圆 S^1 的映射写作 $\mathrm{e}(a) = \exp(2\pi i a)$。

定义 18（环面上的误差与距离）. 对于 $a, b \in \mathbb{T}$，定义

$$\mathrm{Err}(a,b) = \frac{1 - \cos(2\pi(a-b))}{2} = \sin^2(\pi(a-b)),$$
$$\mathsf{D}(a,b) = \frac{|\mathrm{e}(a) - \mathrm{e}(b)|}{2} = |\sin(\pi(a-b))|.$$

因此，Err $=\mathsf{D}^2$, 和 D 是 $\mathbb{T}$ 上的平移不变度量。

事实 19. 对于所有 $a, b \in \mathbb{R}$,

$$2\|a-b\|_{\mathbb{T}} \le \mathsf{D}(a,b) \le \pi\|a-b\|_{\mathbb{T}}.$$

这由 $2t \le \sin(\pi t) \le \pi t$ 对于 $0 \le t \le 1/2$ 得出。

设 $\phi\colon \{0,1\} \to \{\pm 1\}$ 由 $\phi(x) = 1-2x$ 给出，并令 $\phi^{\otimes n}$ 表示其逐坐标作用。

定义 20（周期傅里叶多项式与稀疏度）。我们称一个实多线性多项式 1

$$P(u) = \sum_{S \subseteq [n]} \alpha_S \prod_{i \in S} u_i, \qquad \alpha_S \in \mathbb{R},$$

当我们将其在$\{\pm 1\}^n$ 上的取值按模一解释时，它是一个周期傅里叶多项式。根据 [Mor19], , 其周期傅里叶稀疏度 是非零非恒定单项式的数量,

$$\mathsf{pfs}(P) = \big|\{S \subseteq [n] : S \neq \varnothing,\ \alpha_S \neq 0\}\big|.$$

Werner 和 Wolf 对全关联贝尔表达式的优化、 [HCLB11 中的对应关系、定理 2], 以及 [Mor19 第 (4) 式和第 1 节中的周期傅里叶表述，为每个固定的输入分布给出了如下刻画。

定理 21（平均误差与周期傅里叶稀疏度 [WW01, HCLB11, Mor19]）。设$f\colon \{0,1\}^n \to \{0,1\}$ 为一个布尔函数，设 D 是定义在 $\{0,1\}^n$ 上的概率分布，并设 $r \ge 1$ 为一个整数且为 $\epsilon \in [0,1]$。当且仅当存在一个周期傅里叶多项式 P，其 pfs（P） $\le r$ 满足以下条件时，存在一个使用至多r 量子比特、在 D 下平均误差至多为 ϵ 的 NMQC$\oplus$ 计算:

$$\mathbb{E}_{x \sim \mathcal{D}} \left[\mathrm{Err}\big(f(x)/2, P(\phi^{\otimes n}(x))\big)\right] \le \epsilon.$$

对于固定的输入奇偶校验，该等价关系同样成立，但 P 仅限于相应的非恒定单项式。

最坏情况误差。固定 $r \ge 1$，令 $\mathcal{P}_r$ 为稀疏度至多为 r 的周期傅里叶多项式集合。对于每个输入分布$\mathcal{D}$，定理 21 将使用至多 r 个量子比特的 NMQC$\oplus$ 计算的最小平均误差，等同于在 $P \in \mathcal{P}_r$ 上取最小值。输入奇偶校验的选择可以依赖于$\mathcal{D}$。极小极大定理给出

$$\begin{aligned}\max_{\mathcal{D}} \min_{P \in \mathcal{P}_r} \mathbb{E}_{x \sim \mathcal{D}} \left[\mathrm{Err}\big(f(x)/2, P(\phi^{\otimes n}(x))\big)\right] \\ = \min_{\Lambda} \max_{x \in \{0,1\}^n} \mathbb{E}_{P \sim \Lambda} \left[\mathrm{Err}\big(f(x)/2, P(\phi^{\otimes n}(x))\big)\right],\end{aligned}$$

其中 Λ 遍历$\mathcal{P}_r$ 上的概率分布。因此，对每个输入分布都成立的平均误差保证，等价于在每个输入上具有相同误差界的随机周期傅里叶表示。每个抽样得到的多项式至多有 r 个非恒定单项式，但它们的支撑集不必相同。奇偶函数和系数都可以是随机的。从操作层面看，这使得共享经典随机性可以在输入给出之前选择一个 NMQC$\oplus$ 协议。

对于 ACC，下面的构造给出了一个固定多项式，其在每个输入上的误差界均满足要求。

定义 22（带误差的周期傅里叶表示）。设 $f\colon \{0,1\}^n \to \{0,1\}$ 是一个布尔函数，且 $0 \le \epsilon < 1/2$。若周期傅里叶多项式 P 是 f 的一个周期傅里叶表示，其误差至多为 ϵ，则

$$\mathrm{Err}(f(x)/2, P(\phi^{\otimes n}(x))) \le \epsilon \qquad \forall x \in \{0,1\}^n.$$

我们用 $\mathsf{pfs}_\epsilon(f)$ 表示所有此类多项式的 $\mathsf{pfs}(P)$ 的最小值。

下面的上界构造了固定的周期傅里叶表示，因此给出了具有固定输入奇偶校验和固定局部测量对的 NMQC$^\oplus$ 计算。

7.2 量子比特上界与环面次数

GHZ 构造给出了一个逐点上界，该上界由固定周期傅里叶表示的最小稀疏度决定。

命题 23 ([HCLB11, Mor19])。对于每个布尔函数 f 和 $0 < \epsilon < 1/2$，都存在一个NMQC$^\oplus$ 计算来计算 f，所用量子比特不超过 $\max\{1, \mathsf{pfs}_\epsilon(f)\}$，且其在每个输入上的错误概率至多为 ϵ。

事实 19 根据环面距离给出了周期傅里叶表示的错误上界：

$$\mathrm{Err}(a,b) \le \pi^2 \|a-b\|_{\mathbb{T}}^2.$$

对于 $0 < \epsilon < 1/2$，环面误差 $\sqrt{\epsilon}/\pi$ 小于 $1/4$。令 $D = \deg_{\mathbb{T},\sqrt{\epsilon}/\pi}(f/2)$。仿射变量变换 $\phi^{-1}(u) = (1-u)/2$ 不会增加次数，因此，次数为 D 的环面逼近可得到一个周期傅里叶表示，其中至多含有 $(n+1)^D$ 个非恒定单项式。因此

$$\mathsf{pfs}_\epsilon(f) \le (n+1)^D.$$

结合定理 2，即可证明以下推论。

推论24。固定 $m \ge 2$。如果 $f\colon \{0,1\}^n \to \{0,1\}$ 可由深度至多为 d、规模至多为 $s \ge 2$ 的 $\mathsf{AC}^0[m]$ 电路计算，那么对于每个 $0 < \epsilon < 1/2$，都可以使用至多 ϵ 个量子比特，通过 NMQC$^\oplus$ 在每个输入上的错误概率至多为 ϵ 来计算

$$2^{(\log s)^{O_m(d)} \log(1/\epsilon)}$$

量子比特。

证明定理 1 所用的傅里叶采样论证也直接给出了周期傅里叶稀疏度的上界 [BS92,O'D14]。

命题25。对于任意 $n \ge 1$、任意布尔函数 $f\colon \{0,1\}^n \to \{0,1\}$，以及任意$0 < \epsilon < 1/2$，

$$\mathsf{pfs}_\epsilon(f) = O\left(\frac{n\|\widehat{f}\|_1^2}{\epsilon}\right).$$

因此，f可以通过 NMQC$^\oplus$ 使用 $O(1+n\|\widehat{f}\|_1^2/\epsilon)$ 个量子比特来计算，且对每个输入的错误概率至多为 ϵ。

证明。对于 $f = 0$，我们有 $\mathsf{pfs}_\epsilon(f) = 0$，且一个量子比特就足够了。假设 $f \ne 0$，则 $\|f\|_1 \ge \max_x |f(x)| = 1$。在定理 1 的证明中，将抽样论证应用于 $f/2$，偏差为 $\sqrt{\epsilon}/\pi$，并使用 $M = \lceil \pi^2(n+2)\|\widehat{f}\|_1^2/(2\epsilon) \rceil$ 个样本，可得到一个函数 $g\colon \{0,1\}^n \to \mathbb{R}$，使得

$$\|g - f/2\|_\infty \le \frac{\sqrt{\epsilon}}{\pi}, \qquad \mathrm{sparsity}(\widehat{g}) \le M = O\left(\frac{n\|\widehat{f}\|_1^2}{\epsilon}\right).$$

Set

$$P(u) = \sum_{S \subseteq [n]} \widehat{g}(S) \prod_{i \in S} u_i.$$

于是 $P(\phi^{\otimes n}(x)) = g(x)$，并且对于每个输入，

$$\mathrm{Err}\big(f(x)/2, P(\phi^{\otimes n}(x))\big) = \sin^2\big(\pi(f(x)/2 - g(x))\big) \le \pi^2 |f(x)/2 - g(x)|^2 \le \epsilon.$$

因此， P 是一个具有所述稀疏度的周期傅里叶表示。量子比特上界由命题 23 得出。

□

由于 $\|\mathrm{AND}_n\|_1 = 1$，命题25给出 $\mathsf{pfs}_\epsilon(\mathrm{AND}_n) = O(n/\epsilon)$，以及一个使用 $O(n/\epsilon)$个量子比特的 $\mathrm{NMQC}^\oplus$ 计算来计算 AND_n。在这一构造中，奇偶校验族和系数都是固定的。如果允许随机选择输入奇偶校验，那么如 Mori [Mor19 第 1 节所述，Smolensky 构造给出一种使用 $O(1/\epsilon)$个量子比特的 $\mathrm{NMQC}^\oplus$ 计算来计算 AND 函数，且对每个输入的错误概率至多为 ϵ。事实上，在取反输入上进行 $k = \lceil \log(1/\epsilon) \rceil$ 次随机奇偶校验，可将问题化简为对 k位输入计算 AND 函数，错误不超过 2^{-k}；而这个规模较小的 AND 函数可用$2^k - 1 = O(1/\epsilon)$个量子比特精确计算。

反过来，含有 r 个非恒定项的周期傅里叶表示，可以给出一个环面逼近，其次数关于 r 以及额外误差的倒数呈对数级。这里的表示具有固定系数。

命题 26. 对于每个布尔函数 $f : \{0,1\}^n \to \{0,1\}$ 以及 $\epsilon, \eta > 0$，若满足 $\sqrt{\epsilon}/2 + \eta < 1/4$，

$$\mathsf{deg}_{\mathbb{T}, \sqrt{\epsilon}/2+\eta}(f/2) \le \log \frac{\max\{1, \mathsf{pfs}_\epsilon(f)\}}{2\eta}.$$

证明. 令 $r = \mathsf{pfs}_\epsilon(f)$。若 $r = 0$，则常数相位的误差至多为 ϵ，而事实 19 给出了误差至多为 $\sqrt{\epsilon}/2$ 的常数环面逼近。因此，假设 $r > 0$。选取稀疏度最小的周期傅里叶表示，并写作

$$P(u) = \alpha + \sum_{S \in \mathcal{S}} \beta_S \prod_{i \in S} u_i, \qquad \mathcal{S} \subseteq 2^{[n]} \setminus \{\varnothing\}, \qquad |\mathcal{S}| = r.$$

那么， $Q(x) = P(\phi^{\otimes n}(x))$ 满足对每个输入均有 $\mathrm{Err}(f(x)/2,\ Q(x)) \le \epsilon$，并且

$$Q(x) - \alpha = \sum_{S \in \mathcal{S}} \beta_S (-1)^{\sum_{i \in S} x_i}.$$

因此， $Q - \alpha$ 的傅里叶稀疏度至多为 r。根据定理 14，存在一个次数至多为 $\log(r/(2\eta))$ 的环面多项式 R，使得

$$\|Q(x) - \alpha - R(x)\|_{\mathbb{T}} \le \eta \qquad \forall x \in \{0,1\}^n.$$

集合 $\widetilde{Q} = \alpha + R$。添加常数不会增加次数，并且对于每个 $x \in \{0,1\}^n$，

$$\begin{aligned} \|f(x)/2 - \widetilde{Q}(x)\|_{\mathbb{T}} &\le \|f(x)/2 - Q(x)\|_{\mathbb{T}} + \|Q(x) - \widetilde{Q}(x)\|_{\mathbb{T}} \\ &\le \frac{1}{2}\sqrt{\mathrm{Err}(f(x)/2, Q(x))} + \eta \\ &\le \sqrt{\epsilon}/2 + \eta. \end{aligned}$$

□

8 结论

我们基于傅里叶 ℓ_1 范数，以及模模电路的规模和深度，证明了环面近似次数的上界。傅里叶界给出了 AND$_n$/2 的次数 O(log(n/ϵ))，在逆多项式误差下，这与已知下界仅相差常数因子，并推翻了 Krishan 和 Sarma 提出的超对数次数猜想。对于规模为 s、深度为 d 的 AC$^0[m]$ 电路，log s 的指数为 max$\{1, \mu - 1\}d$，其中 μ 是 m 的不同素因子个数，且该上界与 log$(1/\epsilon)$ 成线性关系。

这两种论证都将采样与加权模零测试的低次数环面近似结合起来。在傅里叶论证中，采样减少了特征的数量，而系数舍入使每个加权特征都能用模一的低次数表示。对于电路，模近似引理支撑了深度归纳。通过交替排列素数幂因子的顺序进行分解，可以得到更精细的电路指数。

周期傅里叶表示将这些近似界转化为量子构造。ACC^0 中的函数可以通过 NMQC$_\oplus$ 计算来计算，所需量子比特数为准多项式级，错误概率为逆多项式；而傅里叶采样给出了一个用于 AND 函数的 $O(n/\epsilon)$量子比特构造。这些计算采用固定的输入奇偶校验和固定的测量，且对每个输入的错误概率至多为 ϵ。反过来，稀疏度为 $r \geq 1$、误差至多为 $\epsilon < 1/16$ 的周期傅里叶表示，可以转化为次数至多为 log$(r/\sqrt{\epsilon})$、误差为 $\sqrt{\epsilon}$的环面近似。因此，在逆多项式误差下，对数多项式环面次数等价于准多项式周期傅里叶稀疏度。

致谢

RM 的研究工作得到了 JST FOREST 计划资助，资助编号为 JPMJFR216V；还得到了日本学术振兴会科研费资助，资助编号为 JP22H00522 和 JP26H02504。

人工智能使用声明

本文在整个写作过程中均使用 ChatGPT (OpenAI) 辅助推导和检查数学论证、查找相关文献，以及起草和修改阐述内容，包括正文和附录中的证明。作者对本文的正确性、原创性和完整性负全部责任，包括其中的证明和参考文献。

参考文献

[AGHP92] Noga Alon、Oded Goldreich、Johan Håstad 和 René Peralta。几乎 k独立随机变量的简单构造。*Random Structures & Algorithms*，3(3):289–304，1992。 https://doi.org/10.1002/rsa.3240030308.[AM21] Erhard Aichinger 和 Jakob Moosbauer。阿贝尔群上的 Chevalley–Warning 类型结果。*Journal of Algebra*，569:30–66，2021。 https://doi.org/10.1016/j.jalgebra.2020.10.033.[Bei93] Richard Beigel。电路复杂性中的多项式方法。载于复杂性理论结构会议第八届年会论文集，第 82–95 页。IEEE 计算机学会，1993。 https://doi.org/10.1109/SCT.1993.336538.[BHLR19] Abhishek Bhrushundi、Kaave Hosseini、Shachar Lovett 和 Sankeerth Rao。环面多项式：一种用于 ACC 下界的代数方法。载于第 *10* 届创新

载于理论计算机科学会议（ITCS 2019），莱布尼茨国际信息学论文集第124卷，第13:1–13:16页。Schloss Dagstuhl – Leibniz-Zentrum für Informatik，2019年。 https://doi.org/10.4230/LIPIcs.ITCS.2019.13.[BS92] Jehoshua Bruck 和 Roman Smolensky。多项式阈值函数、 AC^0函数和谱范数。SIAM计算学杂志，21(1):33–42，1992年。https://doi.org/10.1137/0221003.[BT91] Richard Beigel 和 Jun Tarui。关于 ACC。载于第32届计算机科学基础年会（FOCS 1991），第783–792页。IEEE 计算机学会，1991年。https://doi.org/10.1109/SFCS.1991.185449.[BT94] Richard Beigel 和 Jun Tarui。关于 ACC。计算复杂性，4(4):350–366，1994年。 https://doi.org/10.1007/BF01263423.[CP19] Shiteng Chen 和 Periklis A. Papakonstantinou。复合函数的深度约简。SIAM计算学杂志，48(2):668–686，2019年。 https://doi.org/10.1137/17M1129672.[CS22] Pete L. Clark 和 Uwe Schauz。函数次数与算术应用 I：函数次数集合。Journal of Algebra，608:691–718，2022年。 https://doi.org/10.1016/j.jalgebra.2022.05.035.[GKR+95] Frederic Green、Johannes Köbler、Kenneth W. Regan、Thomas Schwentick 和 Jacobo Torán。#P函数中间位的威力。Journal of Computer and System Sciences，50(3):456–467，1995年。 https://doi.org/10.1006/jcss.1995.1036.[Hås86] Johan Håstad。小深度电路的近乎最优下界。载于第十八届 ACM 计算理论研讨会论文集（STOC 1986），第6–20页。ACM，1986年。 https://doi.org/10.1145/12130.12132.[Hås01] Johan Håstad。对 LMN 的略微改进。Journal of Computer and System Sciences，63(3):498–508，2001年。 https://doi.org/10.1006/jcss.2001.1803.[HCLB11] Matty J. Hoban、Earl T. Campbell、Klearchos Loukopoulos 和 Dan E. Browne。非自适应测量式量子计算与多方贝尔不等式。新物理学杂志，13(2):023014，2011年。 https://doi.org/10.1088/1367-2630/13/2/023014.[Hoe63] Wassily Hoeffding。有界随机变量之和的概率不等式。Journal of the American Statistical Association，58(301):13–30，1963年。 https://doi.org/10.1080/01621459.1963.10500830.[KS18] Swastik Kopparty 和 Srikanth Srinivasan。用于 $AC^0[\oplus]$电路的认证多项式及其在下界和电路压缩中的应用。Theory of Computing，14(12):1–24，2018年。 https://doi.org/10.4086/toc.2018.v014a012.[KS26] Vaibhav Krishan 和 Jayalal Sarma。通过环面多项式研究 AND 的 CC^0 下界。载于第51届国际计算机科学数学基础研讨会（MFCS 2026），莱布尼茨国际信息学论文集第386卷，第62:1–62:16页。Schloss Dagstuhl – Leibniz-Zentrum für Informatik，2026年。 https://doi.org/10.4230/LIPIcs.MFCS.2026.62.

[KV26] Vaibhav Krishan 和 Sundar Vishwanathan。环面多项式的下界与分离。在第17届理论计算机科学创新会议（ITCS 2026）上，收录于《莱布尼茨国际信息学论文集》第362卷，页码88:1–88:20。Schloss Dagstuhl – Leibniz-Zentrum für Informatik，2026年。 https://doi.org/10.4230/LIPIcs.ITCS.2026.88。[LMN93] Nathan Linial、Yishay Mansour 和 Noam Nisan。常深度电路、傅里叶变换与可学习性。《ACM学报》，40(3):607–620，1993年。 https://doi.org/10.1145/174130.174138。[Mor19] Ryuhei Mori。布尔函数的周期傅里叶表示。《Quantum Information and Computation》，19(5–6):392–412，2019年。 https://doi.org/10.26421/QIC19.5-6-2。[NN93] Joseph Naor 和 Moni Naor。小偏差概率空间：高效构造与应用。《SIAM计算学杂志》，22(4):838–856，1993年。 https://doi.org/10.1137/0222053。[O'D14] Ryan O'Donnell。《布尔函数分析》。剑桥大学出版社，2014年。https://doi.org/10.1017/CBO9781139814782。[OS15] Igor Carboni Oliveira 和 Rahul Santhanam。多数函数无法被 $\mathrm{AC}^0[p]$电路压缩。在第30届计算复杂性会议（CCC 2015）上，收录于《莱布尼茨国际信息学论文集》第33卷，页码124–157。Schloss Dagstuhl – Leibniz-Zentrum für Informatik，2015年。 https://doi.org/10.4230/LIPIcs.CCC.2015.124。[Raz87] Alexander A. Razborov。在带逻辑加法的完备基上，有界深度电路大小的下界。《数学札记》，41(4):333–338，1987年。https://doi.org/10.1007/BF01137685。[SB91] Kai-Yeung Siu 和 Jehoshua Bruck。论小权重阈值电路的能力。《SIAM离散数学杂志》，4(3):423–435，1991年。 https://doi.org/10.1137/0404038。[Smo87] Roman Smolensky。布尔电路复杂性下界理论中的代数方法。在第19届ACM计算理论年度研讨会（STOC 1987）论文集上，页码77–82。ACM，1987年。 https://doi.org/10.1145/28395.28404。[Tal17] Avishay Tal。AC^0的傅里叶谱的紧致界。在第32届计算复杂性会议（CCC 2017）上，收录于《莱布尼茨国际信息学论文集》第79卷，页码15:1–15:31。Schloss Dagstuhl – Leibniz-Zentrum für Informatik，2017年。 https://doi.org/10.4230/LIPIcs.CCC.2017.15。[TZ12] Terence Tao 和 Tamar Ziegler。低特征有限域上 Gowers范数的逆猜想。《组合年刊》，16:121–188，2012年。https://doi.org/10.1007/s00026-011-0124-3。[Wil06] Richard M. Wilson。关于模 p^m 多项式的一个引理及其在编码理论中的应用。《离散数学》，306(23):3154–3165，2006年。 https://doi.org/10.1016/j.disc.2004.10.030。[Wil14] Richard Ryan Williams。电路复杂性中的多项式方法及其在算法设计中的应用。在第34届软件基础国际会议

技术与理论计算机科学（*FSTTCS 2014*），第29卷，收录于《莱布尼茨国际信息学论文集》，页码47–60。Schloss Dagstuhl – Leibniz-Zentrum für Informatik，2014年。 https://doi.org/10.4230/LIPIcs.FSTTCS.2014.47。

[WW01] Reinhard F. Werner 和 Michael M. Wolf。每个位置有两个二分观测量的全多方贝尔相关不等式。《物理评论*A*》，64(3):032112，2001 年。
https://doi.org/10.1103/PhysRevA.64.032112。

A 改进电路指数

A.1 使用更少映射的分解

对于 $\mu = 1$，定理 2 可由命题 17 推出。我们通过将电路分解为与素数幂模数相关联的布尔映射，并近似它们的复合，来证明剩余情形 $\mu \geq 2$。证明分两步：先将其分解为至多 $(\mu-1)d+1$ 个映射，再给出一个映射代换时的次数上界。最终的映射具有模其模数的直接多项式表示，因此只有其他映射会带来 $\log s$ 因子。设

$$m = \prod_{i=1}^{\mu} p_i^{e_i}, \qquad q_i = p_i^{e_i}.$$

该分解调整了 Beigel 和 Tarui 的转换中交替素数顺序的形式，使其更加简洁 [BT91，第 5.2 节，第 789] 页。我们将中间门值保留为布尔坐标，因此坐标数量仍受原始电路规模的限制。

引理 27（具有交替素数幂顺序的电路分解）。设 m 具有 $\mu \geq 2$个不同素因子。存在一个仅依赖于 m 的常数 $t_m \geq 1$，使得每个具有 n个输入、深度至多为 $d \geq 1$ 且规模至多为 s 的 $\mathsf{AC}^0[m]$ 电路 C 都允许进行因式分解

$$C = B_H \circ \cdots \circ B_1, \qquad H \leq (\mu-1)d+1,$$

其中 $B_j\colon \{0,1\}^{r_{j-1}} \to \{0,1\}^{r_j}$、$r_0 = n$、$r_H = 1$和 $r_j \leq s$。存在一个映射 $\sigma\colon [H] \to [\mu]$，使得 B_j 的每个坐标都具有如下形式

$$(B_j)_a(y) = \prod_{\ell} \delta_{q_{\sigma(j)}}(G_{j,a,\ell}(y)),$$

其中 $G_{j,\,a,\,\ell} \in \mathbb{Z}[y]$ 且 $\deg G_{j,\,a,\,\ell} \leq t_m$。此外，存在一个次数至多为 t_m 的整数多项式 Q，使得在布尔立方体上 $B_H(y) \equiv Q(y)$（模 $q_{\sigma(H)}$）。

证明。如果 C 没有非 NOT 门，则其输出为常量或输入文字，一个带有 $\sigma(1) = 1$ 的映射就足够了。否则，删除不向输出馈送的门，并按层对剩余的门进行分组，其中门的层是以该门为终点的有向路径上非 NOT 门的最大数量，且包括该门本身。设 $h \leq d$ 为非空层的数量。否定被并入输入文字中，并在必要时并入最终输出。

Put

$$u_m = 1 + \max_{i \in [\mu]} e_i(q_i - 1).$$

对于每个 $i \in [\mu]$ 以及任意一列布尔文字 $\ell_1(y), \ldots, \ell_u(y)$，引理 9 结合 $k = e_i$给出，在布尔输入下

$$q_i Q_{q_i,e_i}\left(\sum_{a=1}^{u} \ell_a(y)\right) \equiv \delta_{q_i}\left(\sum_{a=1}^{u} \ell_a(y)\right) \pmod{q_i}.$$

左侧的多项式次数至多为 $e_i(q_i-1)$，并且在布尔输入上取整数值。因此，其多线性化具有整数系数：每个系数都是布尔顶点处取值的交错整数和。将这个整数多项式记为 R_i。因此，R_i 的次数至多为 $u_m - 1$，并且模 q_i精确表示 Mod_{q_i} 门。特别地，它在布尔输入上的剩余为零或一。由中国剩余定理可得

$$\mathsf{Mod}_m(\ell_1(y), \ldots, \ell_u(y)) = \prod_{i=1}^{\mu} \delta_{q_i}\left(\sum_{a=1}^{u} \ell_a(y)\right).$$

每次处理一层，并将所有输入比特和先前计算出的门值作为坐标保留。将一层替换为 μ 个映射，按照选定顺序，每个素数幂因子对应一个映射。对于每个新的 Mod_m 门，维护一个布尔坐标 b，表示到目前为止已处理的测试之积。在模数为 q_i 的阶段，若这是第一个阶段，则设 $b = R_i(y) \bmod q_i$；否则更新

$$b \longmapsto bR_i(y) \bmod q_i.$$

这里，模 q_i 约简后，对于映射的每个布尔输入，都会得到布尔剩余 0 或 1。更新具有模 q_i 的整数多项式表示，次数至多为 u_m。使用

$$\mathsf{AND}(\ell_1(y), \ldots, \ell_u(y)) = \prod_{a=1}^{u} \delta_{q_i}(\ell_a(y) - 1),$$

计算第一张映射中该层的每个 AND 门，并通过其余映射传递其值。部分积使用为其原始门预留的坐标。因此，在任何阶段至多需要 s 个坐标。

每个映射的坐标都是次数至多为 u_m 的整数多项式零测试的乘积。事实上，模 q 下由 R 表示的布尔坐标等于 $\delta_q(R-1)$。取 $R = y_a$ 即可包含复制操作。除每个层级的第一个映射外，其余映射的坐标也都是模其模数的整数多项式，次数至多为 u_m，因为它们只更新部分积并复制其他坐标。

在奇数层使用顺序 $(q_1, \ldots\ldots, q_\mu)$，在偶数层使用相反顺序。一层的最后一个映射与下一层的第一个映射使用相同的模数 q。前者的坐标是模 q 的整数多项式。将这些多项式代入后者的零测试，即可得到它们的精确复合，因为多项式代入保持模 q 同余。每个所得测试的次数至多为 u_m^2。被合并的 $h-1$ 对彼此不相交：每个层级至少有两个映射。因此，这些代入不会累积，映射总数为

$$H = \mu h - (h-1) = (\mu - 1)h + 1 \le (\mu - 1)d + 1.$$

最终映射未合并，其坐标是在模数下的多项式。选取其中的电路输出坐标；如果输出取反，则应用 $1 - y_a$。这就得到了所需的标量多项式 Q。

对于每个所得的映射 B_j，当其模数为 q_i 时，定义 $\sigma(j) = i$。取 $t_m = u_m^2$ 即完成证明。

□

A.2 代入布尔映射

我们使用模零测试的乘积 [CP19] 的特征展开来近似 $P \circ B$。与第6节一样，我们联合采样单项式和特征。所得次数仅对单项式的数量呈对数依赖，而不会因每个坐标中的零测试数量而增加一个因子。

引理 28（布尔映射的代入）。设 $q = p^e$ 为素数幂，设 n、r、$t \ge 1$，并设 $B\colon \{0,1\}^n \to \{0,1\}^r$ 具有坐标

$$B_a(x) = \prod_j \delta_q(G_{a,j}(x)), \qquad G_{a,j} \in \mathbb{Z}[x], \quad \deg G_{a,j} \le t.$$

对于每个在 r 个变量中次数至多为 $D \ge 1$ 的环面多项式 P，以及每个 $\eta \in (0, 1/2)$，都存在一个环面多项式 R，使得

$$\|R(x) - P(B(x))\|_{\mathbb{T}} \le \eta \qquad \forall x \in \{0,1\}^n$$

and

$$\deg R \le c_q t\big(D\log(r+1)+\log(n+1)+\log(1/\eta)\big),$$

其中 c_q 仅取决于 q。

*Pr*哎。 将 P 的多线性表示的系数模一化，并写 te

$$P(y)=\sum_{S\in\mathcal{U}}\alpha_S y_S \pmod 1, \qquad y_S=\prod_{a\in S} y_a, \qquad 0<|\alpha_S|\le 1/2.$$

这里，对于每个 $S\in\mathcal{U}$，都有 $|S|\le D$。令 $K=|\mathcal{U}|$，并令 $A=\sum_S|\alpha_S|$。于是 $K\le(r+1)^D$且$A\le K/2$。如果 $A=0$，则取 $R=0$。否则，定义实值函数

$$F(x)=\sum_{S\in\mathcal{U}}\alpha_S b_S(x), \qquad b_S(x)=\prod_{a\in S}B_a(x).$$

它表示 $P(B(x))$ 模一。每个 b_S都是零测试 $\delta_q(G_{S,j})$ 的乘积，其中 $\deg G_{S,j}\le t$。特征正交性给出

$$b_S(x)=\mathbb{E}_{\lambda\in\{0,\dots,q-1\}^{u_S}}\left[\cos\left(\frac{2\pi}{q}\sum_{j=1}^{u_S}\lambda_j G_{S,j}(x)\right)\right].$$

为了用短和近似 F，我们将这些期望合并为一个，然后用样本平均对其进行近似。以概率 $|\alpha_S|/A$ 采样一个索引 $S\in\mathcal{U}$，并在给定 S的条件下，从$\{0,\dots,q-1\}^{u_S}$中均匀采样 λ。定义随机函数

$$Z_{S,\lambda}(x)=\operatorname{sgn}(\alpha_S)\cos\left(\frac{2\pi}{q}\sum_j\lambda_j G_{S,j}(x)\right).$$

于是$|Z_{S,\lambda}(x)|\le 1$ 并且

$$A\mathbb{E}[Z_{S,\lambda}(x)]=A\sum_{S\in\mathcal{U}}\frac{|\alpha_S|}{A}\operatorname{sgn}(\alpha_S)b_S(x)=F(x).$$

取 $M=\lceil 8(n+1)A^2/\eta^2\rceil$ 个独立样本。对于每个固定输入，Hoeffding 不等式 [Hoe63] 给出

$$\Pr\left[\left|\frac{A}{M}\sum_{j=1}^{M}Z_j(x)-F(x)\right|>\eta/2\right]\le 2\exp\left(-\frac{M\eta^2}{8A^2}\right)\le 2\exp(-(n+1))<2^{-n}.$$

因此，对所有 2^n 输入应用并集界，我们可以固定一组样本，使其加权平均值~ ~F处处满足 $|F(x)-F(x)|\le\eta/2$。

每个样本都是一个整数多项式 G的带符号余弦，其次数至多为 t。利用

$$\cos(2\pi G(x)/q)=\sum_{a=0}^{q-1}\cos(2\pi a/q)\delta_q(G(x)-a),$$

~将 F 写成至多 Mq 个加权零测试之和。对每个零测试应用引理 10，误差为~$\eta/(2Mq)$，并将所得多项式相加。它们的和 R 以至多 $\eta/2$的环面误差逼近 F，因此以至多 η的误差逼近 $P\circ B$。其次数至多为

$$t(q-1)\log(2Mq/\eta).$$

由于 $M\le 3(n+1)K^2/\eta^2$，这至多为

$$t(q-1)\big(2D\log(r+1)+\log(n+1)+3\log(1/\eta)+\log(6q)\big).$$

将常数吸收到 c_q 中即可证明该断言。 □

A.3 定理 2 的证明

定理 2（重述）。对于每个 $m \geq 2$，存在一个仅依赖于 m 的常数 $C_m \geq 1$，使得以下结论成立。设 μ 为 m 的不同素因子个数，并令 $\nu = \max\{1, \mu - 1\}$。对于每个 $n \geq 1$、每个具有 n 个输入的 $\mathsf{AC}^0[m]$ 电路 C（其深度至多为 d、大小至多为 $s \geq 2$），以及每个 $\epsilon \in (0, 1/4)$，

$$\mathsf{deg}_{\mathbb{T},\epsilon}(C/2) \leq C_m^d (\log s)^{\nu d} \log(1/\epsilon).$$

证明。若 $\mu = 1$，则应用命题 17，并取 $C_m = A_m$。以下假设 $\mu \geq 2$，因此 $\nu = \mu - 1$。令 $L = \log s \geq 1$。若 C 没有非 NOT 门，则 $C/2$ 有精确的仿射表示，所需界即得。这包括 $d = 0$。否则，应用引理 27，将 $C = B_H \circ \cdots \circ B_1$ 写成满足 $H \leq (\mu - 1)d + 1$ 的形式。对于 $1 \leq j \leq H$，令

$$F_j = B_H \circ \cdots \circ B_{H-j+1}.$$

我们证明存在常数 $a_m \geq 1$，使得对每个 $\eta \in (0, 1/4)$，$F_j/2$ 都有一个次数至多为以下值的 η-逼近环面多项式

$$a_m^j L^{j-1} \log(1/\eta). \tag{5}$$

对于 $j = 1$，最终映射有一个模 $q_{\sigma(H)}$ 的多项式表示 Q，其次数至多为 t_m。由于 F_1 是布尔值且 $Q \equiv F_1$（模 $q_{\sigma(H)}$），

$$F_1 = \delta_{q_{\sigma(H)}}(Q - 1).$$

引理 10 使用权重 $1/2$，给出至多为 $t_m(q_{\sigma(H)} - 1) \log(1/\eta)$ 的次数，从而在 a_m 足够大时证明基例。

假设该结论对 $j < H$ 成立，并令 $E_\eta = \log(1/\eta)$。根据归纳假设，选取一个对 $F_j/2$ 的 $(\eta/2)$-近似 P，并令 $D = \max\{1, \deg P\}$。于是

$$D \leq a_m^j L^{j-1} \log(2/\eta) \leq 2 a_m^j L^{j-1} E_\eta.$$

对 $P \circ B_{H-j}$ 应用引理 28，模数为 $q_{\sigma(H-j)}$，误差为 $\eta/2$。所有输入和输出维度均至多为 s，所有测试次数均至多为 t_m，且所有模数均整除 m。由于 $\log(s + 1) \leq 2L$，所得多项式的次数至多为

$$b_m\big((D + 1)L + \log(2/\eta)\big) \leq 5 b_m a_m^j L^j E_\eta$$

其中常数 b_m 仅取决于 m。根据三角不等式，它相对于 $F_{j+1}/2$ 的误差至多为 η。取 $a_m \geq 5b_m$，即可对 $j + 1$ 证明 (5)。

最后，$H - 1 \leq (\mu - 1)d$ 和 $H \leq \mu d$，因为 $d \geq 1$。将 $j = H$ 和 $\eta = \epsilon$ 代入 (5)，得到

$$\mathsf{deg}_{\mathbb{T},\epsilon}(C/2) \leq a_m^H L^{H-1} \log(1/\epsilon) \leq C_m^d L^{(\mu-1)d} \log(1/\epsilon),$$

其中 $C_m = a_m^\mu$。 □

B 函数度与多项式表示

引理 9 中的上界 $(q - 1)\,k$ 足以用于主要证明。这里我们将函数度与多项式表示联系起来，并记录素数幂零测试的精确次数。

Aichinger 和 Moosbauer [AM21] 为阿贝尔群之间的映射发展了有限差分演算。Clark 和 Schauz [CS22] 确定了这类

映射可能具有的函数次数，包括下文所使用的精确次数。关于模素数幂的多项式表示的相关结果，参见 Wilson [Wil06]。

对于阿贝尔群 A，B和映射 $f\colon A \to B$，记 $\Delta_h f(z) = f(z+h) - f(z)$。对于非零的 f，其函数度 $\mathrm{fdeg}(f)$ 是满足以下条件的最小 $d \geq 0$：$\Delta_{h_1} \cdots \Delta_{h_{d+1}} f = 0$ 对每个 $h_1, \ldots, h_{d+1} \in A$ 都成立；若不存在这样的 d，则为 $+\infty$。令 $\mathrm{fdeg}(0) = -\infty$。

当 $A = \mathbb{F}_p^r$、$B = \mathbb{T}$ 且 $\mathrm{fdeg}(f) < +\infty$ 时，f 的函数度与其作为非经典多项式的次数一致 [TZ12，定义 1.2]。经典的 $\mathbb{F}_p$ 值多项式可通过嵌入 $a \mapsto a/p \pmod 1$ 纳入其中。下文将同一有限差分定义应用于循环群 $\mathbb{Z}/q\mathbb{Z}$，并将其与通常的一元多项式次数联系起来。

命题 29 (多项式表示)。设 $q \geq 1$ 和 $d \geq 0$ 为整数，且令$f\colon \mathbb{Z}/q\mathbb{Z} \to \mathbb{T}$。那么 $\mathrm{fdeg}(f) \leq d$ 当且仅当存在一个次数至多为 d 的实多项式 $P \in \mathbb{R}[z]$，使得

$$P(z) = f(z \bmod q) \pmod 1 \qquad \forall z \in \mathbb{Z}.$$

证明。设 $F(z) = f(z \bmod q)$，且 $\Delta F(z) = F(z+1) - F(z)$。若 $\mathrm{fdeg}(f) \leq d$，则 $\Delta^{d+1} F = 0$。有限牛顿展开对负整数也成立，因此有

$$F(z) = \sum_{j=0}^{d} \binom{z}{j} (\Delta^j F)(0) \qquad \forall z \in \mathbb{Z}.$$

事实上，在由 F 的平移生成的子群上，移位算子 $T = I + \Delta$ 对每个整数 z 都满足 $T^z = \sum_{j=0}^{d} \binom{z}{j} \Delta^j$。因此，取 $(\Delta^j F)(0)$ 的实数表示 c_j，便得到 $P(z) = \sum_{j=0}^{d} c_j \binom{z}{j}$，正如所需。反过来，每个加性导数都会使实多项式的次数至少降低一，因此，若存在这样的 P，则 f 的任意 $d+1$ 个加性导数都为零。

□

命题30 ([CS22，命题4.4和定理4.7])。对于每个素数 p 和整数e，$k \geq 1$，

$$\mathrm{fdeg}\left(\frac{\delta_{p^e}}{p^k}\right) = (p-1)p^{e-1}k + p^{e-1} - 1.$$

这里，定义域是 $\mathbb{Z}/p^e\mathbb{Z}$，陪域是 $\mathbb{T}$。

证明。Clark 和 Schauz 给出了 δ函数 $\mathbb{Z}/p^e\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ 的这个次数。从 $\mathbb{Z}/p^k\mathbb{Z}$ 到 $\mathbb{T}$ 的单射同态 $a \mapsto a/p^k \pmod 1$ 与加性导数可交换，因此保持函数度。

□

令 $q = p^e$。根据命题 29，这个函数度也是在整数上模 1 表示 δ_q/p^k 的实多项式的最小次数。如果这个函数度是 D，那么对每个 $j > D$，$\Delta^j(\delta_q/p^k) = 0$ 属于 $\mathbb{T}$。特别地，对每个 $j > D$，$(\Delta^j \delta_q)(0) \equiv 0 \pmod{p^k}$。因此，引理 9 中选取的系数 a_j 均为零，所以在那里构造的多项式$Q_{q,\,k}$ 的次数至多为这个值。由最小性可得反向不等式。因此，该多项式达到最优次数

$$\deg Q_{q,k} = (p-1)p^{e-1}k + p^{e-1} - 1 = (q-1)k - (p^{e-1}-1)(k-1) \leq (q-1)k,$$

当 $e, k > 1$ 时为严格不等式。对于 $e = 1$，精确次数为 $k(p-1)$，这也是 δ_p/p^k 在 $\mathbb{F}_p$ 上的非经典次数。正文中的逼近论证使用了更简单的界 $(q-1)k$。