arXiv:2302.08083v1 [cs.CC] 16 Feb 2023

The 量子行列式的计算复杂性

Shih-Han Hung* En-Jui Kuo†

摘要

在本文中，我们研究量子行列式的计算复杂性。量子行列式是矩阵永久式的一种 q-形变：给定复平面单位圆上的一个复数 q，以及一个 $n \times n$ 矩阵 X， q-永久式 X 定义为

$$\mathrm{Per}_q(X) = \sum_{\sigma \in S_n} q^{\ell(\sigma)} X_{1,\sigma(1)} \dots X_{n,\sigma(n)},$$

其中， $\ell(\sigma)$ 是对称群 S_n 中作用于 n 个元素的置换 σ 的逆序数。该函数族推广了行列式和永久式，分别对应于情形 $q = -1$ 和 $q = 1$。

关于最坏情况困难性，借助刘维尔逼近定理和代数数论中的一些事实，我们证明：对于奇素数幂 $m = p^k$，若 q 是本原 m 次单位根，则精确计算 q-永久式是 Mod$_p$P-困难的。这意味着，若存在高效算法计算 q-永久式，则多项式层级将发生坍缩。接下来，我们证明，借助一个能够在多项式乘法误差范围内进行近似的预言机，以及一个针对有限代数整数集的成员资格预言机，可以实现 q-永久式的计算。因此，高效的近似算法也会意味着多项式层级发生坍缩。根据随机自归约性，对于满足所谓强自相关性质的广泛分布，计算 q-永久式仍然是困难的。具体而言，我们通过从 1-永久式到 q-永久式的归约，证明了这一点；该归约适用于单位圆上的 $O(1/n^2)$ 个点 z。由于永久式函数族具有共同的代数结构，为证明永久式困难性而开发的各种技术都可以推广到 q-永久式。

1 引言

矩阵永久式的研究在理论计算机科学和组合学中发挥了至关重要的作用。在一项开创性工作中，Valiant 证明了计算矩阵永久式是 #P-难的，即使矩阵的元素属于整数、非负整数或集合 $\{0, 1\}$ [Val79a]。这被认为是计算复杂性理论中最具影响力的成果之一。这些结果被用于论证图论中其他计算任务的困难性 [Bro86,CX21]以及矩阵分析中的计算任务的困难性 [HJ12]。相比之下，利用初等线性代数中的标准工具可知，矩阵行列式可在多项式时间内计算 [M+97]。

一个有趣的观察是，矩阵 X 的永久式和行列式都可以写成矩阵元素的多项式，其中相位系数是复平面单位圆上的元素。更具体地说，这两个函数都可以写成对 n 个元素的排列 σ 求和的形式，相位为 q。这里， $\ell(\sigma)$ 是<স্টyle id='14'>逆序数

*德克萨斯大学奥斯汀分校计算机科学系。电子邮箱：shung@cs.utexas.edu。

†量子信息与计算机科学联合中心，美国国家标准与技术研究院和马里兰大学，美国马里兰州大学公园市 20742。电子邮箱：kuoenjui@umd.edu

排列的数量 σ，定义为通过对相邻元素进行换位以恢复 $\sigma(1)\ldots,\sigma(n)$ 到其自然顺序1，2，…，n [Yan91]。对于永久式，$q=1$；而对于行列式，$q=-1$。然而，尽管这两个函数具有统一形式的表达式，它们的计算复杂度为何如此不同，仍然令人费解。

探索这个问题的一个自然思路，是研究矩阵多项式的 q-变形，从而连接 $q\in\{-1,1\}$这两种情形。在数学文献中，单位圆上或 $[-1,1]$ 中的 q-变形已有研究，并被赋予了不同的名称，包括 μ-永久式、q-永久式、q-行列式，或量子行列式 [Yan91、BL94、Lal98、dF18、DF10、dS18、TAG93]。然而，据我们所知，这些结果都未讨论计算其类似物的复杂度。本文聚焦于单位圆，并研究如下定义的函数的计算复杂性：

$$\mathrm{Per}_z(X):=\sum_{\sigma\in S_n} z^{\ell(\sigma)}\prod_i X_{i,\sigma(i)}. \tag{1}$$

对于对称群 S_n（其包含 n 个元素）以及满足 $|z|=1$ 的复数 z。在本文余下部分，对于矩阵 X，我们将称 $\mathrm{Per}_z(X)$ 为 X 的 z-永久式。

z-永久式并非矩阵永久式唯一的 q类比形式。特别是，*Immanant*[Har85、Bür00、MM11、dRA13、Spi20、Cur21] 和费米子行列式 [MM11、BKW19、RA13、dRA13]是两类得到广泛研究的函数。它们均由类函数定义，即对于对称群上在共轭作用下不变的某个函数 f，这些函数可以写成如下形式：

$$\sum_{\sigma\in S_n} f(\sigma)X_{1,\sigma(1)}\cdots X_{n,\sigma(n)}. \tag{2}$$

对于 Immanant，$f(\sigma)=\chi_\lambda(\sigma)$，其中 χ_λ 是群表示 λ 关于 S_n的特征标。永久式对应于 χ_λ 为平凡表示这一特殊情况，而行列式对应于符号表示。Curticapean 最近取得重大突破，对分拆族的 Immanant 计算复杂度进行了分类。通过证明，在合理的假设下，对于每个分拆族 Λ，矩阵 Immanant 可高效计算，当且仅当一个量 $b(\Lambda)$ 无界；该量统计了 $\lambda\in\Lambda$杨图中第一列右侧的方格数 [Curt21]。对于费米子行列式，$f(\sigma)=(-1)^n(-k)^{c(\sigma)}$，其中 $c(\sigma)$表示 σ中的循环数。在证明其困难性方面，Martins 和 Moore 表明，对于 $k>2$，费米子行列式在图灵归约下是 #P-困难的；对于 $k=2$，该问题是 $\oplus$P-困难的 [MM11]。另一方面，Björklund、Kaski 和 Williams 针对有限域 $\mathbb{F}_q$上含 q个元素的 $m\times m$矩阵，给出了一个时间复杂度为 $2^{m-\Omega(m/\log\log q)}\cdot O(\mathsf{M}(q))$ 的算法，其中 $\mathsf{M}(q)$ 是在 $\mathbb{F}_q$ [上进行乘法和除法的时间复杂度 19]BKW19]。这些结果表明，除特殊情况外，这些函数通常在计算上难以处理。

然而，据我们所知，对于任何 $z\notin\{-1,+1\}$，都尚无关于 z-永久式复杂度的分类；而且上述结果似乎都无法直接推出这一族问题的困难性，部分原因在于逆序数不是类函数。事实上，关于矩阵永久式的 q-变形，现有的复杂度结果甚至都未超出类函数的范围。

除了系数不是类函数这一点之外，人们或许还会想知道，为什么 z-永久式（也称为量子行列式）是一个值得研究的对象？首先，在表示论中，标准李代数可以推广为所谓的 q-变形代数（也称为量子群[Maj00]）。量子行列式会自然地出现在此类背景中。更具体地说，考虑 z-Grassmann 代数，它是由以下元素生成的结合代数：$K[z]$

$z=\zeta_{p^k},\in$ $\mathbb{T}\setminus\{\pm1\},\lvert\mathrm{Per}_z(X)\rvert^2$	精确	近似于 乘法误差 poly(n)
最坏情况	定理 3.10	定理 4.2
平均情况适用于 $X\sim\mathcal{H}$	常数比例 定理 5.3	定理 6.4

表 1：我们将困难性结果归纳为四个常见类别，并指出本文展示的四个主要定理。

$x_1,x_2,...,x_n$，满足对每个 $i\in[n]$ 都有 $x_i^2=0$，且当 $i<j$ 时有 $x_ix_j=zx_jx_i$。不难看出

$$\left(\sum_{j=1}^{n}a_{1j}x_j\right)\left(\sum_{j=1}^{n}a_{2j}x_j\right)\dots\left(\sum_{j=1}^{n}a_{nj}x_j\right)=\mathrm{Per}_z(A)x_1x_2\dots x_n. \tag{3}$$

其 A 为 n 由 n 矩阵使得 $A_{ij}=a_{ij}$。量子行列式也是此类 q-变形代数 [ER98], 中的重要对象，并且与不同特征下的表示论密切相关。其次，众所周知，量子行列式在物理学的诸多领域都有广泛应用，包括弦理论 [FK06] 和共形场论 [GRASRA96, PS90]。在量子信息论中，量子行列式在 q-变形交换关系 [BLW17] 或任意子关系 [GM04], 的 Fock 表示中也发挥着关键作用；这些关系推广了标准的玻色子／费米子交换关系 [BS91]。

受上述观察启发，我们着手研究z-永久式的计算复杂性，并给出复数 z 取值于单位圆上的一般困难性结果。在以下各节中，我们将概述我们的贡献。

1.1 我们的贡献

本文研究 z-永久式在 m阶本原单位根 z 下，对整数 $m>2$的计算复杂性。我们的贡献建立在代数数论工具之上。我们在表1中总结了结果。从第3节到第5节，我们在每一节中证明一个定理。

1.1.1 最坏情况困难性

首先，我们研究计算 ζ_m-永久式的困难性，其中输入为 $n\times n$ 二进制矩阵 X，取 m阶本原单位根 ζ_m。根据 (1)，我们可以将 z- 永久式写成关于 z 的多项式，其系数可以写成关于 X 中元素的多元多项式。对于 $z\notin\{+1,-1\}$，z-永久式通常是一个复数，可以写成关于z的整系数多项式。由于复数运算只能以有限精度进行计算，我们首先明确算法精确计算$\mathrm{Per}_z(X)$ 的含义。

虽然我们不知道如何为单位圆上的每个 z 给出合理的定义，但利用分圆域的性质，可以为本原单位根和二进制矩阵给出自然的定义。更具体地说，二进制矩阵的 ζ_m-永久式可以写成一个关于 ζ_m 的整系数多项式，其次数为 $d=\deg\Phi_m-1$，其中 Φ_m 是第 m 个圆分多项式。这意味着表示

将 $\mathrm{Per}_{\zeta_m}(X)$ 表示为次数为 d 的多项式时，其系数元组是唯一的。因此，我们将能够精确计算 $\mathrm{Per}_{\zeta_m}(X)$ 的算法定义为：输出一组系数 $a_0, \ldots, a_d$，使得 $\mathrm{Per}_{\zeta_m}(X) = \sum_{i=0}^{d} a_i \zeta_m^i$。

根据这个定义，我们证明，对于奇素数幂 $m = p^k$，任何能够计算ζ_m-永久式的预言机 $\mathcal{O}$ 都意味着 $\mathsf{BPP}^{\mathsf{Mod}_p\mathsf{P}} \subseteq \mathsf{BPP}^{\mathcal{O}}$。

定理 1.1 （永久式的困难性，非正式表述）。对于奇素数 p、素数幂 $m = p^k$ 以及一个本原 m 次单位根 ζ_m，计算 $\{0,1\}$ 矩阵的 ζ_m-永久式是 Mod$p$P-困难的。更明确地说，对于每个预言机 $\mathcal{O}$，若其输入一个二进制 $n \times n$ 矩阵 X，并输出 $\mathrm{Per}_{\zeta_m}(X)$ 的系数，则有

$$\mathsf{PH} \subseteq \mathsf{BPP}^{\mathsf{Mod}_p\mathsf{P}} \subseteq \mathsf{BPP}^{\mathcal{O}}. \tag{4}$$

（4）中的第一个不等式 由广义 Toda 定理推出 [TO92, Tod91]。要证明第二个不等式，我们依据这样一个事实：对于素数幂 $m = p^k$，分圆多项式在 1 处的取值为 p。这意味着系数之和模 $\mathrm{Per}(X)$ 与 p同余。接着，第二个不等式由以下事实推出：已知计算 $\mathrm{Per}(X)$ 模一个奇素数是 Mod$p$P-困难的，这一点由 Valiant 证明 [Val79a]。

虽然我们对精确计算的定义看起来很自然，但人们可能会疑惑，要求正确输出所有系数是否过于严格，以至于无法存在高效的经典算法。我们通过研究在 ℓ_2-范数下近似 $\mathrm{Per}_{\zeta_m}(X)$ 的困难性来回答这个问题。特别地，我们证明，只要找到一个足够接近 $\mathrm{Per}_{\zeta_m}(X)$ 的复数，就足以借助 NP 预言机提取所有系数。

1.1.2 近似困难性

接下来，我们证明，能够以多项式乘法误差近似 $\mathrm{Per}_{\zeta_m}(X)$ 的预言机也是 Mod$p$P-困难的。

定理 1.2 （近似困难性，非正式表述）。对于奇素数 p、素数幂 $m = p^k$以及本原的 m 次单位根 ζ_m，近似 $\{0,1\}$ 矩阵的 ζ_m-永久式是Mod$p$P-困难的。更明确地说，对于每个算法 $\mathcal{O}$，若其输入一个 $n \times n$ 二进制矩阵 X并输出一个乘法误差在 $g =$多项式(n)以内的近似值，则有

$$\mathsf{PH} \subseteq \mathsf{BPP}^{\mathsf{Mod}_p\mathsf{P}} \subseteq \mathsf{BPP}^{\mathsf{NP}^{\mathcal{O}}}. \tag{5}$$

定理 1.2 意味着，对 $\mathcal{O}$ 进行高效模拟会导致多项式层级坍缩。第一个不等式同样由广义 Toda 定理推出 [TO92, Tod91]。随后，我们通过以下两个步骤证明第二个不等式。首先，我们证明存在一种确定性算法，只需对 $\mathcal{O}$ 进行多项式次查询，就能将 $\delta = 2^{-\mathrm{poly}(n)}$中的误差降低到 ℓ_2-范数。我们的算法始终能成功输出一个与 δ相差不超过 $\mathrm{Per}_{\zeta_m}(X)$ 的复数。然而，仅凭这一步还无法得到符合我们精确计算定义的系数组。我们通过调用刘维尔逼近定理的一个变体来解决这一问题。根据该定理，我们证明，任意两个代数整数若表示为 ζ_m 上系数属于 $[-A, B]$ 且次数为 A的最小多项式，$B = 2^{\mathrm{poly}(n)}$ 则它们在 $2^{-\mathrm{poly}(n)}$-距离下相距至少 ℓ_2。利用一个能判定是否存在与目标相差不超过 δ的代数整数的预言机，我们可以通过二分搜索确定所有系数。最后，我们证明，判定是否存在一个与近似值足够接近、且其系数在 $[-A, B]$中有界的代数整数，可以由非确定性图灵机解决。

此外，在定理 3.11中，我们提供了证据，表明不存在能够计算大多数单位根的多项式算法。

1.1.3 精确计算 z-永久式的平均情形困难性

关于 1-永久式的平均情形困难性，Aaronson 和 Arkhipov [AA11] 证明，在合理的假设下，对大多数高斯矩阵精确计算$\mathrm{Per}(X)$ 是#P-困难的。Haferkamp、Hangleiter、Eisert 和 Gluza [HHEG20] 证明了对于大多数截断均匀分布情形，该问题是困难的。

在第5节中，我们调整了他们的技术，以证明对每个 z，如果在最坏情况下计算 z-永久式是困难的，那么通过随机自归约性，计算高斯矩阵的 z-永久式也是困难的。该证明利用了 Berlekamp-Welch 算法，以及 z-永久式是其矩阵元素的低次多项式这一事实。

此外，我们将困难性结果推广到一族满足某种性质的概率分布，这种性质称为强自相关性质。具体而言，如果原始分布经过平移或缩放后与原始分布之间的总变差距离很小，就称随机矩阵满足强自相关性质（详细定义见定义 5.2 ）。我们证明，对于从满足该性质的分布中抽取的矩阵，计算其 z-永久式仍然是#P-困难的。因此，这一困难性结果可应用于例如以零为中心、并在某个选定阈值处截断的均匀分布。

1.1.4 近似 z-永久式的平均情形困难性

在第6节中，我们证明，如果能在时间 $\Omega(n^2)$ 内计算 $\mathrm{Per}_z(X)$ 的特定$\mathrm{poly}(n, 1/\epsilon, 1/\delta)$个点，那么就能求出$\mathrm{Per}(X)$，其中 X 是从满足强自相关性质的分布 $\mathcal{H}$ 中采样得到的。这意味着，给定分布 $\mathcal{H}$ 和 $X \sim \mathcal{H}$，近似计算$\mathrm{Per}(X)$是困难的。我们的结果适用于乘法误差和加法误差。

此外，我们还证明，对于任意满足 X, X^* 同分布的分布 X ，近似计算 $\mathrm{Per}_z(X)$ 与近似计算 $\mathrm{Per}_{z^*}(X)$ 一样困难。该证明对 $|\mathrm{Per}_z(X)|^2$ 也成立。

1.2 相关工作

正如我们在引言中所述，永久式和行列式的计算复杂性截然不同。任何连接这两种情形的路径，从计算复杂性的角度来看都很有趣。更一般地，我们可以考虑此类

$$\sum_{\nu \in S_n} f(\nu) \prod_{i=1}^{n} A_{i,\nu(i)} \tag{6}$$

函数，并询问形如(6)的函数的复杂度。人们已经研究过一些函数族，包括 Immanant [MM11、Har85、Bür00、dRA13、Spi20、Bür00] 以及费米子行列式 [MM11、BKW19、RA13、dRA13]。然而，从以下角度来看，我们的工作与它们截然不同：

- 与 Immanant 和费米子行列式不同， z-永久式不是类函数。据我们所知，这种矩阵函数的复杂度(6) 仅在 $f(\nu)$ 是类函数时才得到过研究。因此，不能使用标准的 Immanant 结果。

- 由于 z-永久式不是类函数，我们提出了涉及代数数论的全新方法。

- 据我们所知，关于最坏情况和平均情况的所有近似困难性结果均针对 1-永久式。对于 $f(\nu) \neq 1$，此前文献中尚未给出任何近似困难性结果。在 第4节、第5节和第6节中，我们提供了技术工具，从而得到关于一般函数 f的近似困难性结果。

1.3 组织结构

本文其余部分的结构安排如下。预备知识见第2节。在第3节中，关于最坏情况困难性，我们证明，对于奇素数幂 m 的本原 $m = p^k$ 次单位根，精确计算 z-永久式是 Mod$_p$P-困难的。在第4节中，我们证明，高效近似二元矩阵的 z-永久式意味着多项式层级坍缩。在第5节中，基于最坏情况困难性，我们证明，对于满足强自相关性质的分布族，精确计算z-永久式具有平均情形困难性。在第6节中，我们转而讨论平均情形困难性。最后，在第7节中，我们总结结果，并讨论若干与 z-永久式相关的开放问题。

2 预备知识

2.1 代数数论简介

这里我们介绍一些与我们的工作相关的域扩张 [Ben87] 和代数数论 [Lan13, Neu13, Wei98] 中的事实，不过本文只会用到关于分圆域的事实。

首先，我们回顾抽象代数和代数数论中的基本定义。阿贝尔群是一个在其群运算下封闭的元素集合，通常记作 $+$ （对于加法群）或 $\cdot$（对于乘法群），且每个元素都有逆元。交换环是一个加法群，同时还具有结合乘法运算和乘法单位元 1。域是一个环，其非零元素构成一个阿贝尔乘法群。例如，有理数集合 $\mathbb{Q}$ 是一个域，而整数集合 $\mathbb{Z}$ 构成一个环。

如果域 K 包含域 F 作为子域，则称 K 是域 F 的扩域（或简称扩张），记作 K/F。扩域 K 可以视为域 F 上的向量空间。域扩张 K/F 的次数记作 $[K\colon F]$，它是 K 作为 F 的向量空间时的维数。给定一个域 F 和某个值 α，令 $F(\alpha)$ 表示包含 F 和 α 的最小域，称为添入 α 所得到的域。向域中添入元素的运算构成域扩张。例如，$K = \mathbb{Q}(\zeta_3) = \{a + b\zeta_3\colon a, b \in \mathbb{Q}\}$ 是 $\mathbb{Q}$ 的一个二次扩域，因为 K 中的每个元素都可以表示为 $\mathbb{Q}$ 中的二维向量。对于不定元 x，我们还将 $\mathbb{Z}[x]$ 记作具有整数系数的多项式环。对于复数 α，集合 $\mathbb{Z}[\alpha] = \{f(\alpha)\colon f(x) \in \mathbb{Z}[x]\}$ 构成一个环。

数域是 $\mathbb{Q}$ 的有限次数扩域。我们回顾数域和代数数的定义。

定义 2.1. 代数数域（或简称数域）是有理数域 $\mathbb{Q}$ 的扩域 K，其中域扩张 $K/\mathbb{Q}$ 的次数有限（因此是代数扩张）。

定义 *2.2*。 *</style}*复数 $x \in \mathbb{C}$ 是代数数，当且仅当存在一个系数为有理数（等价地，系数为整数）的非零多项式f，使得 x 是 f的根。代数数集合 $\mathbb{Q}$ 构成 $\mathbb{C}$.的一个子域

定义 2.3。 </style>复数 $x \in \mathbb{C}$ 是代数整数，当且仅当存在一个系数为整数的首一多项式 f （其首项系数等于一），使得 x 是f的根。

¯代数整数的集合构成 $\mathbb{Q}$的一个子环。我们还有 $\alpha \in K$ 是一个代数整数，当且仅当 α 在 $\mathbb{Q}$ 上的最小首一多项式属于 $\mathbb{Z}[x]$ [Lan13]。利用高斯引理，我们可以得到一个关于有理数域和代数数的简单事实。

定理 2.4 ([Lan13]). 设 $\mathcal{O}$ 为代数整数的集合。代数整数与 $\mathbb{Q}$ 的交集是 $\mathbb{Z}$，即 $\mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$.

定义 2.5 (整数环). 代数数域 K 的整数环 $\mathcal{O}_K$ 是包含在 K中的所有代数整数构成的环，即 $\mathcal{O}_K = \mathcal{O} \cap K$。

圆分域是将本原单位根添入 $\mathbb{Q}$后得到的数域。在本文中，我们将 ζ_n 记作整数 $n > 1$对应的第 n 个本原单位根。请注意，本原单位根的选取并不唯一。事实上，对于 $n > 1$，若 $\gcd(a, n) = 1$，则 $e^{2\pi i a/n}$ 是一个本原单位根。

定义 2.6 (分圆域)。 n次分圆域是由 $\mathbb{Q}$ 生成的扩张 $\mathbb{Q}(\zeta_n)$ ζ_n。更明确地说：

$$\mathbb{Q}(\zeta_n) = \left\{ \sum_{i=0}^{n-1} a_i \zeta_n^i \middle| a_i \in \mathbb{Q} \right\}. \tag{7}$$

虽然 ζ_n可能有多种选择，但域 $\mathbb{Q}(\zeta_n)$ 是唯一的。这可由一个简单的观察得出：设 ζ、ξ是两个不同的 n次本原单位根。由于存在 $a \in \{0, 1, \ldots, n-1\}$，且 $\gcd(a, n) = 1$，使得 $\xi = \zeta^a$、$\mathbb{Q}(\xi) \subseteq \mathbb{Q}(\zeta)$，因此它们相等。类似地，我们考虑环

$$\mathbb{Z}[\zeta_n] = \left\{ \sum_{i=0}^{n-1} a_i \zeta_n^i \middle| a_i \in \mathbb{Z} \right\}. \tag{8}$$

对于分圆域 $\mathbb{Q}(\zeta_n)$，其整数环为 $\mathbb{Z}[\zeta_n]$。

定理 2.7 ([Lan13])。 对于整数 $n > 1$ 和 $K = \mathbb{Q}(\zeta_n)$， $\mathcal{O}_K = K \cap \mathcal{O} = \mathbb{Z}[\zeta_n]$。

我们将用到欧拉函数 [Lan13]的一些有用性质。

定义 2.8 （欧拉函数 [Lan13]）。 欧拉函数 ϕ 计算不超过给定整数的正整数个数 n这些正整数与 n互素。更明确地说，它可以通过以下公式计算：

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \tag{9}$$

其中，乘积遍历所有整除 n. 的互异素数

我们将需要以下关于 ϕ（n）[RS62]的下界。

定理 2.9 （[RS62]）。 对于 $n > 2$,

$$\phi(n) > \frac{n}{e^{\gamma} \log\log n + \frac{3}{\log\log n}}. \tag{10}$$

简而言之： $\phi(n)$ 的阶约为 n。因此，对于任意足够大的 $n.$，我们总有 $\phi(\Omega(n^c)) > n$，其中 γ 是欧拉–马歇罗尼常数。

对于一个 n 次本原单位根 ζ_n，第 n 个分圆多项式 Φ_n 是 ζ_n 在 $\mathbb{Q}$ 上的最小多项式。

定义 2.10 ([Lan12])。 对于整数 $n \geq 1$， n次分圆多项式定义为

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(x - e^{2i\pi \frac{k}{n}}\right). \tag{11}$$

多项式 $\Phi_n(x)$ 具有整数系数，即 $\Phi_n(x) \in \mathbb{Z}[x]$。

我们列出一些在本文工作中有用的分圆多项式的基本性质。由于 $\Phi_n(x)$ 在 $\mathbb{Q}$ 上不可约，因此它是 ζ_n 在 $\mathbb{Q}$ 上的最小多项式，次数 $[\mathbb{Q}(\zeta_n): \mathbb{Q}] = \deg \Phi_n = \phi(n)$。 $\mathbb{Q}(\zeta_n)$ 中每个元素在 $\mathbb{Q}$ 上的最小多项式次数至多为 $\phi(n)$。等价地，以下集合 $\{e^{2\pi aij/q}: 0 \leq j < \phi(q)\}$ 在 $\mathbb{Q}$ 上线性独立。对于 $n \geq 2$,

$$\begin{aligned} &\Phi_n(0) = 1, \\ &\Phi_n(1) = 1, \quad \text{if } n \text{ is not a prime power}, \\ &\Phi_n(1) = p, \quad \text{if } n = p^k \text{ is a prime power with } k \geq 1. \end{aligned} \tag{12}$$

定理 2.11 (分圆多项式系数的界 [Vau75])。 设 $\Phi_n(x) := \sum_{i=0}^{\phi(n)} a_i x^i$ 为 n次分圆多项式。系数 a_i 的 $\Phi_n(x)$的最大绝对值满足

$$\max_{i \in \mathbb{N}, 0 \leq i \leq \phi(n)} |a_i| \leq e^{\frac{1}{2} d(n) \log n}, \tag{13}$$

其中， $d(n)$ 是约数函数，用于计数整数 $n \geq 1$.[1]的因数个数（包括1 和 n）

对于 $n = p_1^{a_1} \ldots, p_k^{a_k}$, $d(n) = (a_1 + 1) \ldots (a_k + 1)$。由于 $p \geq 2$ 是素数，且 $a \geq 1$,$a + 1 \leq p^a$为整数，我们可以得到平凡界 $d(n) \leq n$。根据定理 2.11，我们最多只需用 $O(n \log n)$ 位来表示 $\Phi_n(x)$。

下面的定理将会很有用。

定理 2.12 (刘维尔逼近定理 [LW12])。 设 $\alpha \in \mathbb{C}$ 是一个代数数，其最小多项式为 $f(x) = a_0 x^d + a_1 x^{d-1} + .. + a_d$，次数为 d。那么对于任意 a， $b \in \mathbb{Z}$ 互素的

$$\left|\alpha - \frac{a}{b}\right| \geq \frac{1}{b^d a_0 (2|\bar{\alpha}| + 1)^{d-1}} \tag{14}$$

其中， $f(x) = a_0 \prod_\sigma (x - \sigma(\alpha))$，而 $|\bar{\alpha}|$ 是 α 在 $\mathbb{C}$中的代数共轭的最大复模，即 $|\bar{\alpha}| =$最大值 $|\sigma(\alpha)|$。

特别地，由于 0 和 1 互素，根据 定理 2.12，对于每个最小多项式为 $f(x) = a_0 x^d + \ldots + a_d$ 的代数数 α， $|\alpha| \geq \frac{1}{a_0 (|\bar{\alpha}|+1)^{d-1}}$。对于两个代数整数 α、 $\beta \in \mathbb{Z}[\zeta_n]$、 $\alpha - \beta \in \mathbb{Z}[\zeta_n]$, 以及 $|\alpha - \beta| \geq \frac{1}{(|\alpha-\beta|+1)^{\phi(n)-1}}$。

定理 2.13 (费马小定理[魏04])。 设 p 是一个素数。那么对于任意整数a，数 $a^p - a$ 是 p的整数倍。用模运算的记号表示为

$$a^p \equiv a \pmod{p}. \tag{15}$$

[1]例如，6 的因数是 1、2、3 和 6，因此 $d(6) = 4$。

定理 2.13推出

$$a^{p^k} \equiv a \pmod{p}. \tag{16}$$

因为 $k \geq 1$ 根据 定理 2.13， $a^{p^k} \equiv a^{p^{k-1}} \pmod{p}$。

定理 2.14. 设域 F的特征为 p，且 a， $b \in F$,

证明。 由二项式定理,

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \ldots + \binom{p}{p-1}ab^{p-1} + b^p. \tag{17}$$

我们只需证明以下引理：素数 p 整除每个二项式系数 $\binom{p}{r}$ ，其中 $1 \leq r \leq p-1.$。根据定义，引理的证明很简单:

$$\binom{p}{r} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-r+1)}{1 \cdot 2 \cdot \ldots \cdot r}. \tag{18}$$

结论由此得出，因为 p整除分子但不整除分母。 □

2.2 z-永久式的性质

令 $\mathbb{T} := \{z \in \mathbb{C} : |z| = 1\}$ 为复平面中的单位圆。对于矩阵 $X \in \mathbb{C}^{n\times n}$， X 的 z-永久式定义为

$$\mathrm{Per}_z(X) := \sum_{\sigma \in S_n} z^{\ell(\sigma)} \prod_i X_{i,\sigma(i)}, \tag{19}$$

其中， S_n 是由 n 个元素组成的对称群， $\ell(\sigma)$ 是 σ 的逆序数。逆序数定义为满足 $i < j$ 且 $\sigma(i) > \sigma(j)$ 的数对 (i, j) 的个数。显然， $\ell(\sigma) \leq \binom{n}{2} = \frac{1}{2}n(n-1)$。这意味着我们可以将 z-永久式写成关于 z 的多项式:

$$\mathrm{Per}_z(X) = \sum_{\ell=0}^{\binom{n}{2}} z^\ell \left(\sum_{\sigma:\ell(\sigma)=\ell} \prod_{i=1}^{n} X_{i,\sigma(i)} \right). \tag{20}$$

注意，根据 (20)， z-永久式是一个关于 z.的多项式，其次数为 $\binom{n}{2}$

这里列出 z-永久式 [Yan91、DS] 对于每个矩阵 $X \in \mathbb{C}^{n\times n}$ 的基本性质。其中大多数与永久式和行列式的性质完全相同。

1. $\mathrm{Per}_z(X)$ 是关于行和列的多重线性函数。
2. 对于分块三角形 X，$\mathrm{Per}_z(X)$ 等于其对角块的 z-永久式之积。
3. $\mathrm{Per}_z(X) = \mathrm{Per}_z(X^T)$，其中 X^T 是 X的转置。
4. （展开定理）令 X^{ij} 表示 X 的（i， j）子式，令 X_{ij} 表示 X.的元素。则

$$\mathrm{Per}_z(X) = \sum_{k=1}^{n} X_{1k} z^{k-1} \mathrm{Per}_z(X^{1k}) = \sum_{k=1}^{n} X_{jk} z^{k-1} \mathrm{Per}_z(X^{jk}) \tag{21}$$

对于 $j = 1$、2、.....、n。

5. 对于整数矩阵 X 和 n 次单位根 z，$\mathrm{Per}_z(X) \in \mathbb{Z}[\zeta_n]$。因此，$\mathrm{Per}_z(X)$ 在 $\mathbb{Q}$ 上的最小多项式首项系数为 1，次数至多为 $\phi(n)$。

我们给出最简单情形 $n=2$ 和 $n=3$ 的显式公式：对于 $n=2$,

$$\mathrm{Per}_z(X) = (X_{11}X_{22} + X_{21}X_{12}z).$$

对于 $n=3$,

$$\begin{aligned}\mathrm{Per}_z(X) = X_{13}X_{22}X_{31}z^3 + (X_{12}X_{23}X_{31} + X_{13}X_{21}X_{32})z^2 + \\ (X_{11}X_{23}X_{32} + X_{12}X_{21}X_{33})z + X_{11}X_{22}X_{33}.\end{aligned}$$

2.3 与永久式相关的常见任务

我们回顾 Aaronson 和 Arkhipov 定义的以下任务 [AA11]。我们将在本文中讨论其中一些任务的推广。

问题 1 ($\mathrm{GPE}_\times$)。给定输入 $X \sim \mathcal{N}_{\mathbb{C}}(0,1)^{n\times n}$ 个独立同分布的高斯变量（复正态分布）以及 ϵ, $\delta > 0$，估计 $\mathrm{Per}(X)$，误差不超过 $\pm\epsilon|\mathrm{Per}(X)|$，且概率至少为 $1-\delta$（以 X 为准）。

猜想 1。$\mathrm{GPE}_\times$ 是 #P-困难的。换言之，如果 $\mathcal{O}$ 是一个能够求解 $\mathrm{GPE}_\times$ 的预言机，那么$\mathsf{P}^{\#\mathsf{P}} \subseteq \mathsf{BPP}^{\mathcal{O}}$。

猜想 2。存在一个多项式 p，使得对于正整数 n、实数 $\delta > 0$,

$$\Pr_X\left[|\mathrm{Per}(X)|^2 \geq \frac{\sqrt{n!}}{p(n,1/\delta)}\right] \geq 1-\delta. \tag{22}$$

3 $\{0,1\}$-矩阵的 z-永久式的困难性

在本节中，我们研究 z-永久式的困难性。我们只考虑 z 是单位根的情形，即存在正整数 m 使得 $z^m = 1$，原因有二。首先，集合 $\{z = e^{2\pi ia/b}:\ a、\ b \in \mathbb{N}\}$ 在单位圆上稠密，因此对于任意 $z \in \mathbb{T}$，该集合中都存在一个与之任意接近的元素。其次，从计算的角度来看，正如我们将看到的，给出关于 2π 的有理倍数的精确计算定义更为相关且方便。因此，在本文中，我们始终假设 z 是单位根，并将 $z = \zeta_m$ 写作对于整数 $m \geq 2$ 而言的本原 m 次单位根。

我们从三次单位根开始，证明计算满足$z^3 = 1$ 的 z z-永久式是 $\mathsf{Mod}_3\mathsf{P}$-困难的。因此，根据 Toda 定理，若存在计算 z-永久式的算法，则多项式层级将发生坍缩。

3.1 三次单位根

回顾代数数论中的结论，对于 $z = \zeta_p$ 和二进制矩阵 $X \in \{0,1\}^{n\times n}$，$\mathrm{Per}_z(X)$ 可以表示为关于 z 的多项式：

$$\mathrm{Per}_z(X) = \sum_k A_k z^k, \tag{23}$$

其中 $A_k := \sum_{\sigma:\ell(\sigma)\equiv k \pmod p} \prod_{i=1}^{n} X_{i,\,\sigma(i)}$。此外，对于 $z = \zeta_p$，$\mathrm{Per}_z(X) \in \mathbb{Z}[\zeta_p]$，因此它是数域 $\mathbb{Q}[\zeta_p]$ 中的代数整数。我们将把这一观察与计算 1-永久式的困难性及复杂度类 $\mathsf{Mod}_p\mathsf{P}$ 联系起来，定义如下。

定义 3.1 ($\mathsf{Mod}_k\mathsf{P}$)**：** 对于任意整数 $k \geq 2$，令 $\mathsf{Mod}_k\mathsf{P}$ 表示这样一类判定问题：可由多项式时间非确定性机器求解；当接受路径的数量可被 k 整除时，该机器拒绝，否则接受。当 $k = 2$ 时，$\mathsf{Mod}_k\mathsf{P}$ 也称为奇偶 P，记作 $\oplus\mathsf{P}$。

众所周知，Valiant 证明了计算 $\mathrm{Per}(X) \bmod p$ 是 $\mathsf{Mod}_p\mathsf{P}$-完全的，其中 $p > 2$[Val79a]。有趣的是，我们可以将计算 $\mathrm{Per}(X) \bmod p$ 的问题规约为计算 $\mathrm{Per}_{\zeta_p}(X)$ 的特殊情形 $p = 3$。

定理 3.2 (Valiant [Val79a])**：** 对于方阵M，计算 $\mathrm{Per}(M) \bmod p$ 的问题$M \in \mathbb{F}_p^{n\times n}$是 $\mathsf{Mod}_p\mathsf{P}$-完全的，其中 $p > 2$是任意素数。

现在我们陈述本节的定理。

定理 3.3。对于每个立方单位根 ζ，计算 $\mathrm{Per}_\zeta(X)$ 和 $|\mathrm{Per}_\zeta(X)|^2$ 都是 $\mathsf{Mod}_3\mathsf{P}$-困难问题。

证明。对于 $\zeta = 1$，由 Valiant [Val79a]，，定理成立，因此只需证明定理对于 $\zeta \in \{e^{i2\pi/3}, e^{i4\pi/3}\}$。对于 $\zeta = e^{i2\pi/3}$，我们可以将 $\mathrm{Per}_\zeta(X)$ 写成

$$\begin{aligned}\mathrm{Per}_\zeta(X) &= A_0 + \zeta A_1 + \zeta^2 A_2 \\ &= A_0 + \left(-\frac{1}{2} + \frac{\sqrt{3}i}{2}\right)A_1 + \left(-\frac{1}{2} - \frac{\sqrt{3}i}{2}\right)A_2 \\ &= \frac{2A_0 - A_1 - A_2}{2} + i\sqrt{3}\frac{A_1 - A_2}{2}\end{aligned} \tag{24}$$

如果能计算 $\mathrm{Per}_\zeta(X)$，那么取 $\mathrm{Per}_\zeta(X)$ 的实部，就能计算 $\mathrm{Per}(X) \bmod 3$，因为

$$2A_0 - A_1 - A_2 \equiv 2\mathrm{Per}(X) \pmod 3, \tag{25}$$

并且 2 在环 $\mathbb{Z}_3$ 中是一个单位。同样的推理也适用于 $\zeta = e^{i4\pi/3}$，只需交换 i 和 $-i$。

Valiant 的原始论文 [Val79b] 中证明了，模 $m = 2^k$ 的永久式可以在时间 $n^{O(k)}$内计算，但对于所有 $m \neq 2^k$，它都是NP-困难的（在随机归约下） [CX15，DJ21]。

对于 $|\mathrm{Per}_\zeta(X)|^2$，我们观察到

$$|\mathrm{Per}_\zeta(X)|^2 \equiv |\mathrm{Per}(X)|^2 \pmod 3.$$

因此，如果能够精确计算 $|\mathrm{Per}_\zeta(X)|^2$，我们就能得到 $|\mathrm{Per}(X)|^2$ 模 3。 □

广义 Toda 定理 [TO92] 指出，少数计数复杂性类与多项式层级一样难。

定理 3.4 (Todatheorem [Tod91，TO92])。对于素数 $k > 2$，令 A 为以下计数复杂性类之一：$\mathsf{Mod}_k\mathsf{P}$，#P、PP、或 GapP。则 $\mathsf{PH} \subseteq \mathsf{BPP}^A$。

根据 Toda 定理，我们立即得到以下定理。

定理 3.5。 对于 $\zeta \in \{1, e^{i2\pi/3}, e^{i4\pi/3}\}$，令 $\mathcal{O}$ 为任意预言机，该预言机以二进制矩阵 $X \in \{0,1\}^{n\times n}$为输入，输出 $\mathrm{Per}_\zeta(X)$。则

$$\mathsf{PH} \subseteq \mathsf{BPP}^{\mathsf{Mod}_3\mathsf{P}} \subseteq \mathsf{BPP}^{\mathcal{O}}. \tag{26}$$

换言之，如果能够对 $\mathcal{O}$ 进行高效的经典模拟，那么多项式层级就会坍缩到第二层。

如果多项式层级是无限的，定理 3.5 则排除了存在能够精确计算 ζ-永久式的高效经典算法。

3.2 素数幂 m 的本原 m 次单位根

接下来，我们将注意力转向任意素数 $p = n^{O(1)}$。由于一般而言，$\mathrm{Per}_{\zeta_p}(X)$ 在复平面上可能是无理数，因此有限精度下的任何截断都只能得到近似值。本节关注精确计算 $\mathrm{Per}_{\zeta_p}(X)$ 的难度，因此我们必须先明确的第一个问题是：对于二进制 X，如何定义“精确计算 $\mathrm{Per}_{\zeta_p}(X)$”。

对于二进制矩阵 X，$A_k \in \mathbb{Z}$ (见 (23))。因此，$\mathrm{Per}_{\zeta_p}(X)$ 可以写成关于 ζ_p的多项式，其次数至多为 $p-1$，且系数为整数。我们可以将 $\mathrm{Per}_{\zeta_p}(X)$的精确表示定义为一组系数。

定义 3.6 （代数整数的表示）。 代数整数 $\alpha \in \mathbb{Z}[\zeta_p]$ 的表示是一个满足以下条件的整数元组（b_0, b_1, ..., b_{p-1}）

$$\alpha = b_0 + b_1\zeta_p + \ldots b_{p-1}\zeta_p^{p-1}. \tag{27}$$

请注意，这种表示并不唯一，因为 ζ_p 是 f的一个根（x） $= 1 + x + \ldots + x^{p-1}$，因此对于任意整数 $c \in \mathbb{Z}$，都有$\alpha + cf$（ζ_p） $= \alpha$。

一般而言，可以在 $\alpha \in \mathbb{Z}[\zeta_n]$ 为一般的 n 的情况下，于定义 4.5中定义代数整数的表示。不过，在本节中，定义 3.6 足以说明其困难性。注意，也可以用满足以下条件的整数元组来定义这种表示：（b_0, b_1, ..., b_{p-2}），因为$\alpha = b_0 + b_1\zeta_p + \ldots b_{p-2}\zeta_p^{p-2}$有 $\zeta_p^{p-1} = -1 - \zeta_p - \zeta_p^2 - \ldots - \zeta_p^{p-2}$.

计算$\mathrm{Per}_{\zeta_p}(X)$ 的算法会精确输出一个系数元组 $(b_0, \ldots, b_{p-1}) \in \mathbb{Z}^p$，使得 (27) 成立。对于我们的目的而言，这一定义不失一般性。在 第4.2节中，我们将构造一种算法，利用 NP 预言机，将复平面中的一个近似值映射为精确表示。

定理 3.7。 设 p 为素数，ζ_p 是一个本原 p 次单位根，$\mathcal{O}$ 是任意一个预言机，其输入为一个二进制矩阵 $X \in \{0,1\}^{n\times n}$，输出为 $\mathrm{Per}_{\zeta_p}(X)$ 的一种表示。那么 $\mathsf{BPP}^{\mathsf{Mod}_p\mathsf{P}} \subseteq \mathsf{BPP}^{\mathcal{O}}$。

证明。 对于二进制矩阵 X，令 $\mathcal{O}(X)$ 的输出为 $(a_0, \ldots, a_{p-1})$。此外，令 A_i 按照(23)中的定义给出。根据 $\mathcal{O}$的正确性，

$$\mathrm{Per}_{\zeta_p}(X) = \sum_{i=0}^{p-1} A_i\zeta_p^i = \sum_{i=0}^{p-1} a_i\zeta_p^i. \tag{28}$$

注意，对于每个 $i, A_i = a_i$，该结论不一定成立，但这些多项式与 ζ_p 的最小多项式同余且相同。特别地，对于素数 p，由于 $0 = \sum_i (A_i - a_i)\zeta_p^i$，

$$\left(\sum_{i=0}^{p-1}(A_i - a_i)\zeta_p^i\right)^p = \sum_{i=0}^{p-1}(A_i - a_i)^p + ph = 0 \tag{29}$$

其中 $h \in \mathbb{Z}[\omega]$。由于等式左侧

$$\sum_{i=0}^{p-1}(A_i - a_i)^p = -ph \tag{30}$$

是一个整数，因此 $h \in \mathbb{Z}[\zeta_p] \cap \mathbb{Q} \subseteq \mathbb{Z}$。这意味着 p 整除 $\sum_i (A_i - a_i)^p$，并且

$$\begin{aligned} 0 &\equiv \sum_{i=0}^{p-1}(A_i - a_i)^p \\ &\equiv \sum_{i=0}^{p-1} A_i^p - \sum_{i=0}^{p-1} a_i^p \\ &\equiv \sum_{i=0}^{p-1} A_i - a_i \pmod{p}. \end{aligned} \tag{31}$$

最后一个等式由费马小定理（定理 2.13）得出。

总而言之，在可以访问预言机 $\mathcal{O}$ 、该预言机能够精确计算二进制 $X \in \{0,1\}^{n\times n}$ 的 $\mathrm{Per}_{\zeta_p}(X)$ 的情况下，以下算法计算 $\mathrm{Per}(X) \bmod p$:

- 运行 $(a_0, \ldots, a_{p-1}) \leftarrow \mathcal{O}(X)$。
- 输出 $\sum_{i=0}^{p-1} a_i \bmod p$。

□

根据 Toda 定理定理 3.4，我们得到以下推论。

推论 3.8. 对于素数 $p > 3$，设 $\mathcal{O}$ 表示任意一个预言机，它能对二进制矩阵 $X \in \{0,1\}^{n\times n}$精确计算 $\mathrm{Per}_{\zeta_p}(X)$ 。那么

$$\mathsf{PH} \subseteq \mathsf{BPP}^{\mathsf{Mod}_p\mathsf{P}} \subseteq \mathsf{BPP}^{\mathcal{O}}. \tag{32}$$

对于素数 p，我们可以轻松地将结果推广到素数幂 $q = p^k$ 。

定理 3.9. 对于素数 p 和素数幂 $q = p^k$，设 ζ_q 为一个本原的 q 次单位根，$\mathcal{O}$ 为任意一个预言机；该预言机在输入二进制矩阵 $X \in \{0,1\}^{n\times n}$时，输出$\mathrm{Per}_{\zeta_q}(X)$的精确表示。那么 $\mathsf{BPP}^{\mathsf{Mod}_p\mathsf{P}} \subseteq \mathsf{BPP}^{\mathcal{O}}$。

证明。 其基本思路源自 定理 3.9 的证明。对于 $\zeta_q = e^{2\pi i a/q}$ 以及 $\gcd(a,\ p) = 1$，我们有

$$\left(\sum_{i=0}^{q-1}(A_i - a_i)\zeta_q^i\right)^q = \sum_{i=0}^{q-1}(A_i - a_i)^q + ph = 0 \tag{33}$$

其中 $h \in \mathbb{Z}[\omega] \cap \mathbb{Q} \subseteq \mathbb{Z}$。接着我们使用费马小定理（定理 2.13），该定理意味着$a^q \equiv a$（模p），并且

$$\sum_{i=0}^{q-1}(A_i - a_i) + ph = 0. \tag{34}$$

因此，我们有（利用有限域性质 定理 2.14）

$$\mathrm{Per}(X) \equiv \sum_{i=0}^{q-1} A_i \equiv \sum_{i=0}^{q-1} a_i \pmod{p}, \tag{35}$$

由此完成证明。 □

我们在本节末总结针对这类特定 z 的 $\mathrm{Per}_z(X)$ 的经典困难性。

定理 3.10。对于奇素数 p 和素数幂 $q = p^k$，设 ζ_q 是一个本原 q 次单位根。精确计算二元矩阵的 ζ_q-永久式不属于 多项式层级；否则，多项式层级将会坍缩。更具体地说，对于任何能够计算二元矩阵的 ζ_q-永久式的预言机 $\mathcal{O}$，以下包含关系成立：

$$\mathsf{PH} \subseteq \mathsf{BPP}^{\mathsf{Mod}_p\mathsf{P}} \subseteq \mathsf{BPP}^{\mathcal{O}}.$$

遗憾的是，我们的方法无法推广到当 m 可被多个不同素数整除时的本原 m 次单位根。虽然我们的结果并未排除非素数幂情况下存在高效求解器的可能性，但探究这些点中是否存在任何一点可由多项式时间算法处理，仍然很有意思。由于这与我们的结果关系不大，我们将一般合数的计算复杂度留作未来工作。

对于 $p = 2$，我们注意到，使用能够计算 ζ_{2^k}-永久式的预言机，我们可以计算$\mathrm{Per}(X)$（模 2）。然而，由于$\mathrm{Per}(X) \equiv \det(X)$（模 2），我们并没有计算$\zeta_{2^k}$-永久式的困难性结果。事实上，已知模 2^k 的永久式存在高效算法 [DJ21，CX15]。关于 ζ_{2^k}-永久式的任何困难性结果，都不能由模 2^k的永久式的困难性推出。

遗憾的是，我们的方法无法用于证明分母为非素数幂的有理数的困难性。

3.3 有理相位的困难性

回顾一下，对于每个 $z \in \mathbb{T}$，二进制矩阵的 z-永久式始终是关于z 的次数至多为 $\binom{n}{2}$ 的整系数多项式。对于一个本原 m 次单位根 $z = \zeta_m$，当 $\phi(m) < \binom{n}{2}$ 时，我们还可以将同余取为 ζ_m 的最小多项式，从而进一步降低次数。在前面的章节中，我们应用这些事实，将计算模 m 的 1-永久式的问题约化为对于素数幂 m 的 ζ_m-永久式。

虽然我们没有关于所有非素数幂有理相位的一般性结果，但本节将考虑一种特殊情况，其中 $\phi(m) \geq \binom{n}{2}$。在这种情况下，由于单项式 $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\binom{n}{2}}$ 线性无关，因此可以直接从 ζ_m-永久式得到 1-永久式。

定理 3.11。令 $\mathcal{O}$ 表示任意一个预言机，其输入为二进制矩阵 X 和 m：$\mathbb{N} \to \mathbb{N}$，满足 $\phi(m(n)) \geq \binom{n}{2} + 1$，它会精确输出 $\mathrm{Per}_{\zeta_m}(X)$。那么 $\mathsf{P}^{\#\mathsf{P}} \subseteq \mathsf{P}^{\mathcal{O}}$。

证明。令 $d := \binom{n}{2}$。计算 $\mathcal{O}(m, X)$ 得到一个系数元组 $(a_0, \ldots, a_d)$，满足

$$\mathrm{Per}_{\zeta_m}(X) = \sum_{i=0}^{d} A_i \zeta_m^i = \sum_{i=0}^{d} a_i \zeta_m^i. \tag{36}$$

其中 $A_i = \sum_{\sigma \in \mathbb{S}_N,\ \ell(\sigma)=i} \left(\prod_{j=1}^{n} X_{j,\sigma(j)} \right)$。由于对于 $\phi(m) \geq d+1$，单项式 $1, \zeta_m, \ldots, \zeta_m^d$ 线性相关，因此对每个 $0 \leq i \leq d$，都有 $A_i = a_i$。这意味着 $\sum_{i=0}^{d} a_i = \mathrm{Per}_m(X)$。

□

然而，对于 $m = O(1)$ 为非素数幂的情况，这两种方法似乎都行不通。我们将固定非素数幂 m 时本原 m 次单位根的困难性留作一个开放问题。

4 近似 ζ_m-永久式的困难性

在第3节中，我们已经证明，对于奇素数 $m = p^k$ 的素数幂 p，精确计算$\mathrm{Per}_{\zeta_m}(X)$ 与计算 $\mathrm{Per}(X) \bmod p$ 一样困难。已知该问题是模 pP 困难的。本节将证明，对于整数 m 和二元矩阵，近似计算 $\mathrm{Per}_{\zeta_m}(X)$ 与精确计算一样困难。

在第4.1节中，我们证明，将 $|\mathrm{Per}_{\zeta_m}(X)|^2$近似到 $g = \mathrm{poly}(n)$ 以内的乘法误差，其难度不亚于将 $\mathrm{Per}_{\zeta_m}(X)$ 近似到 $2^{-\mathrm{poly}(n)}$ 的乘法误差，至多相差一个多项式乘法开销。在第4.2节中，我们证明，借助 NP 预言机，精确计算 $\mathrm{Per}_{\zeta_m}(X)$ 的难度不亚于将其近似到误差 $2^{-\mathrm{poly}(n)}$。结合这两节的结果，我们得出结论：一种高效的近似算法还将意味着多项式层级发生坍缩。

4.1 误差归约

在本节中，我们证明，对于素数 m 和 m 阶本原单位根 ζ_m，将 $|\mathrm{Per}_{\zeta_m}(X)|^2$ 近似到乘法误差 $g = n^{O(1)}$ 的难度，不亚于将 $\mathrm{Per}_{\zeta_m}(X)$ 近似到乘法误差 $1 + 2^{-n^{O(1)}}$。

首先，我们证明下面这个引理，稍后会用到。

引理 4.1. 对于整数 $n \geq 1$ 和 $\delta \leq \frac{1}{2n}$，设 $\alpha_1, \ldots, \alpha_n$ 为复数，且 $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n$ 满足 $i \in [n]$,

$$|\alpha_i - \tilde{\alpha}_i| \leq \delta |\alpha_i|. \tag{37}$$

则有

$$|\alpha_1 \ldots \alpha_n - \tilde{\alpha}_1 \ldots \tilde{\alpha}_n| \leq 2n\delta |\alpha_1 \ldots \alpha_n|. \tag{38}$$

证明。我们通过归纳法证明该引理。对于 $n = 1$，该引理显然成立。假设˜该引理对 $n = k$ 成立。那么对于 $n = k+1$，令 $A := \alpha_1 \ldots \alpha_k$ 且 $A := \tilde{\alpha}_1 \ldots \tilde{\alpha}_k$。根据归纳˜假设，$|A - A| \leq 2k\delta |A|$。于是

$$\begin{aligned}
\frac{|\alpha_{k+1} A - \tilde{\alpha}_{k+1} \tilde{A}|}{|\alpha_{k+1} A|} &\leq \frac{|\alpha_{k+1} - \tilde{\alpha}_{k+1}|}{|\alpha_{k+1}|} + \frac{|\tilde{\alpha}_{k+1}|}{|\alpha_k|} \frac{|A - \tilde{A}|}{|A|} \\
&\leq \delta + (1+\delta) 2k\delta \\
&\leq (2k+1)\delta + 2k\delta^2 \\
&\leq (2k+2)\delta.
\end{aligned} \tag{39}$$

第一个不等式由 (37) 和 $|\tilde{\alpha}_{k+1}| \le |\alpha_{k+1} - \tilde{\alpha}_{k+1}| + |\alpha_{k+1}| \le (1+\delta)|\alpha_{k+1}|$得到。最后一个不等式成立，因为 $2k\delta^2 \le 2n\delta^2 \le \delta$。 □

我们可以通过多项式开销，将近似算法的误差从乘法因子 $g = n^{O(1)}$ 降低到 $1 + 2^{-n^{O(1)}}$。

定理 4.2。对于 $g \in [1,$多项式$(n)]$，素数 m，以及一个原始的 m 次单位根 ζ_m，如果存在一个算法 $\mathcal{O}$，该算法在输入 $X \in \{0,1\}^{n\times n}$时，能够将 $|\mathrm{Per}_{\zeta_m}(X)|^2$ 近似到乘法因子 ˜以内，那么就存在一个算法，输出满足以下条件的 $\mathrm{Per}_{\zeta_m}(X)$估计值 P

$$\frac{|\mathrm{Per}_{\zeta_m}(X) - \tilde{P}|}{|\mathrm{Per}_{\zeta_m}(X)|} \le \epsilon \tag{40}$$

使用 $O(mn^2g^4 \log n + ng^4 \log g + ng^4 \log(1/\epsilon))$ 次查询来 $\mathcal{O}$。

证明。设 $z = \zeta_m$。我们将算法 $\mathcal{A}^{\mathcal{O}}$ 描述如下。首先，$\mathcal{A}^{\mathcal{O}}$ 判定 $|\mathrm{Per}_z(X)|^2 = 0$。如果 $|\mathrm{Per}_z(X)|^2 \ne 0$，则 $\mathcal{O}$ 返回一个值

$$p \in [g^{-1}|\mathrm{Per}_z(X)|^2, g|\mathrm{Per}_z(X)|^2] \tag{41}$$

对于 $g > 1$。这意味着 $p > 0$。否则，$\mathcal{O}(X) = 0$。这意味着存在一个算法，可以判定 $\mathrm{Per}_z(X) = 0$。此外，如果 $p = 0$，则 $\mathcal{A}$ 输出 0。

只需考虑的情形 $|\mathrm{Per}_z(X)|^2 \ne 0$。由于 X 取二进制值，我们可以写成

$$|\mathrm{Per}_z(X)|^2 = a_0 + a_1 z + \ldots + a_{m-1} z^{m-1}, \tag{42}$$

其中每个 a_i 都是非负整数，前提是 z 是一个本原 m 次单位根。

算法 $\mathcal{A}^{\mathcal{O}}$ 找出一列矩阵 $X_0 = X$、X_1、.....、X_{n-1}，使得每个 $X_i \in \mathbb{C}^{(n-i)\times(n-i)}$，并且 X_{i+1} 是通过删除第一列以及如下确定的行 k 之一而从 X_i 得到的子矩阵：从 $k = 1$开始，不断递增 k，直到删除第 k 行和第一列得到的子矩阵 W满足 $|\mathrm{Per}_z(W)|^2 \ne 0$。最后令 $X_{i+1} = W$。由于 $\mathrm{Per}_z(X) \ne 0$，可以保证存在 W使得 $|\mathrm{Per}_z(W)| \ne 0$。计算这一列矩阵需要 $O(n^2)$ 次查询。

该算法通过归纳，将 $\mathrm{Per}_z(X_{k-1})\ \mathrm{Per}_z(X_k)$ 近似到误差 $O(\epsilon/n)$，使用 $O(mng^4 \log n + g^4 \log g + g^4 \log(1/\epsilon))$ 次查询，从 $\mathcal{O}$ 到 0，并使用望远镜乘积

$$\mathrm{Per}_z(X) = \frac{\mathrm{Per}_z(X_0)}{\mathrm{Per}_z(X_1)} \cdot \frac{\mathrm{Per}_z(X_1)}{\mathrm{Per}_z(X_2)} \cdots \frac{\mathrm{Per}_z(X_{n-2})}{\mathrm{Per}_z(X_{n-1})} \cdot \mathrm{Per}_z(X_{n-1}). \tag{43}$$

计算基本情形 $\mathrm{Per}_z(X_{n-1})$ 是平凡的。应用 引理 4.1，可知将误差控制在 ϵ 所需的查询次数为 $O(mn^2g^4 \log n + g^4 n \log g)$ 次。

在下面的证明中，我们只考虑从 $Y := X_1$ 到 X_0的情形；同样的论证也适用于 $k = 2, \ldots, n-1$。为简单起见，我们只证明 Y是通过删除第一行和第一列从 X 得到的情形。其他情形（即，对于 $i > 1$，删除 X 的第 i行）也可以用同样的论证处理。

我们考虑量 $\mathrm{Per}_z(X) - \alpha \mathrm{Per}_z(Y)$。注意，对于本原单位根 z，$\mathrm{Per}_z(X)$ 和 $\mathrm{Per}_z(Y)$ 都是代数整数。这意味着比值 $\alpha = \mathrm{Per}_z(X)\ \mathrm{Per}_z(Y)$ 是代数数。为了证明两个代数数之间存在下界，我们应用刘维尔逼近定理的一个变体，该变体陈述于 定理 2.12。

由于 $\mathrm{Per}_z(X)$ 和 $\mathrm{Per}_z(Y)$ 都是代数整数，它们的最小多项式都是首一的。此外，对于 $\mathrm{Per}_z(X) = \mu$，$\max|\sigma(\mu)| \leq \mathrm{Per}(X) \leq n!$，并且对于 Y，同样的上界也成立。令 $a = 0$ 和 $b = 1$，$|\mathrm{Per}_z(Y)| \geq 1/M$ 和 $\mathrm{Per}_z(X) \geq 1/M$，其中 $M := (2n! + 1)^{m-2}$，并且

$$\frac{1}{n!M} \leq \frac{|\mathrm{Per}_z(X)|}{|\mathrm{Per}_z(Y)|} \leq n!M. \tag{44}$$

量值 $\mathrm{Per}_z(X) - t\mathrm{Per}_z(Y) = \mathrm{Per}_z(X^{[t]})$，其中 $X_{ij}^{[t]} = X_{ij} - t \cdot \mathbb{I}[i = 1]\mathbb{I}[j = 1]$，因此只需调用一次 $\mathcal{O}$，即可将其范数平方近似到乘法误差 g。为了估计 $\alpha = \mathrm{Per}_z(X)\,\mathrm{Per}_z(Y)$，我们递归地求出复数 α_0、……、α_ℓ，使得以下不变量成立：

$$\mathcal{O}(X^{[\alpha_{i+1}]}) \leq \frac{1}{2}\mathcal{O}(X^{[\alpha_i]}) \tag{45}$$

对每个 i。为了了解 α_i 与 α 有多接近，

$$\begin{aligned} |\alpha - \alpha_i| &= \frac{|\mathrm{Per}_z(X) - \alpha_i \mathrm{Per}_z(Y)|}{|\mathrm{Per}_z(Y)|} \\ &\leq \frac{\sqrt{g\mathcal{O}(X^{[\alpha_i]})}}{|\mathrm{Per}_z(Y)|} \\ &\leq g\sqrt{\frac{\mathcal{O}(X^{[\alpha_i]})}{\mathcal{O}(Y)}} \end{aligned} \tag{46}$$

另外，令

$$\beta_i := g\sqrt{\frac{\mathcal{O}(X^{[\alpha_i]})}{\mathcal{O}(Y)}}. \tag{47}$$

设初始猜测为 $\alpha_0 = 0$，

$$\begin{aligned} \mathcal{O}(X^{[\alpha_0]}) &\leq g|\mathrm{Per}_z(X)|^2 \\ &\leq g|\mathrm{Per}(X)|^2 \\ &= g(n!)^2. \end{aligned} \tag{48}$$

回顾一下，$\mathcal{O}(Y) \geq g^{-1}|\mathrm{Per}_z(Y)|^2 \geq \frac{1}{gM^2}$。那么我们有

$$\begin{aligned} |\alpha - \alpha_i| &\leq g\sqrt{\frac{\mathcal{O}(X^{[\alpha_i]})}{\mathcal{O}(Y)}} \\ &\leq g\sqrt{\frac{2^{-i}\mathcal{O}(X^{[\alpha_0]})}{\mathcal{O}(Y)}} \\ &\leq g\sqrt{2^{-i} \cdot g(n!)^2 \cdot gM^2} \\ &\leq g^2 \cdot n! \cdot M \cdot 2^{-i/2}. \end{aligned} \tag{49}$$

我们的目标是得到 $|\alpha - \alpha_\ell| \leq \frac{\epsilon}{2n \cdot n!}M$，因为这意味着 $|\alpha - \alpha_\ell| \leq \frac{\epsilon|\alpha|}{2n}$。因此，只需设置 $2^{\ell/2} > g^2 \cdot (n!)^2 \cdot n \cdot M^2 \cdot (1/\epsilon)$ 和 $\ell = O(mn\log n + \log g + \log(1/\epsilon))$。

现在我们给出一个算法，用于寻找满足 α_{i+1} 的 (45)，其来源为 α_i。根据定义，$|\alpha-\alpha_i| \leq \beta_i$。我们考虑圆盘

$$S_i := \{t : |t-\alpha_i| \leq \beta_i\}, \tag{50}$$

以及圆盘内由整数 L 确定的 $O(L^2)$ 个点构成的网格：

$$L_i := \left\{\alpha_i + (j-1)\frac{\beta_i}{L} + \sqrt{-1}(k-1)\frac{\beta_i}{L} \in S_i : |j|, |k| \in [L]\right\}. \tag{51}$$

该算法对每个 $t \in L_i \cap S_i$ 计算 $\mathcal{O}(X^{[t]})$，并输出使 $\mathcal{O}(X^{[t]})$ 最小的 t（若有多个，则任意选择）。

根据定义，$\alpha \in S_i$，因此存在 $t \in L_i$ 使得 $|t-\alpha| \leq \frac{\beta_i}{\sqrt{2}L}$。对于这样的 t，

$$\begin{aligned}
\mathcal{O}(X^{[t]}) &\leq g|\mathrm{Per}_z(X) - t\mathrm{Per}_z(Y)|^2 \\
&\leq g|\alpha - t|^2 |\mathrm{Per}_z(Y)|^2 \\
&\leq g \cdot \frac{\beta_i^2}{2L^2} \cdot |\mathrm{Per}_z(Y)|^2 \\
&\leq g \cdot \frac{\beta_i^2}{2L^2} \cdot g\mathcal{O}(Y) \\
&= \frac{g^4}{2L^2}\mathcal{O}(X^{[\alpha_i]}).
\end{aligned} \tag{52}$$

因此，对于 $L = g^2$，比值 $\frac{\mathcal{O}(X^{[t]})}{\mathcal{O}(X^{[\alpha_i]})}$ 至多为 $1/2$。 □

作为推论，我们通过定理 4.2重新得到 Aaronson 和 Arkhipov 关于 1-永久式的一个结果（查询复杂度略差），但同一定理也可应用于本原单位根 $z \in \mathbb{T}$。

推论 *4.3*（参见 [*AA11*，定理 28]）。对于 $g \in [1,\mathit{poly}(n)]$，，若存在一个算法 $\mathcal{O}$，它在输入 $X \in \{0,1\}^{n\times n}$ 时能以乘法因子 g 近似 $|\mathit{Per}(X)|^2$，那么就存在一个算法，使用 $O(mn^2g^4 \log n + ng^4 \log g)$ 次对 $\mathcal{O}$ 的查询，精确计算 $\mathit{Per}(X)$。

证明。由于 $\mathrm{Per}(X)$ 是整数，我们应用 定理4.2，其中 $\epsilon = 1/n!$。该算法需要$O(mn^2g^4 \log n + ng^4 \log g)$ 次查询。 □

此外，要获得加法误差在 2^{-n^2} 以内的近似，需要进行 poly(n) 次查询。

推论 4.4。对于 $g \in [1,\mathrm{poly}(n)]$，，如果存在一个算法 $\mathcal{O}$，其输入为 $X \in \{0,1\}^{n\times n}$时，能够将 $|\mathrm{Per}_{\zeta_m}(X)|^2$ 近似到乘法因子 g以内，那么存在一个算法，该算法~输出 $\mathrm{Per}_{\zeta_m}(X)$ 的估计值 P，满足

$$|\mathrm{Per}_{\zeta_m}(X) - \tilde{P}| \leq 2^{-n^2} \tag{53}$$

使用 $O(mn^2g^4 \log n + ng^4 \log n + g^4n^3)$ 次查询来 $\mathcal{O}$。

证明。要将加法误差近似到 2^{-n^2}以内，只需将其近似到乘法误差 $\epsilon = \frac{1}{n!\, 2^{n^2}}$，因为 $|\mathrm{Per}_{\zeta_m}(X)|$ 范数至多为 $n!$，然后根据 定理 4.2，需要$O(mn^2g^4 \log n + ng^4 \log n + ng^4 \log(\frac{1}{\epsilon})) = O(mn^2g^4 \log n + ng^4 \log n + g^4n^3)$ 次查询。 □

这里可以看到，近似困难性的证明依赖于这样一个事实：z给定矩阵的永久式 X 可以由其子矩阵的 z永久式计算得到（见方程(21)）。其他矩阵函数（如 Immanant）则不具备这一性质。

4.2 搜索到判定归约

在上一节中，我们展示了如何利用一个近似计算$\mathrm{Per}_{\zeta_m}(X)$ 的预言机，将其乘法误差控制在 $2^{-n^{O(1)}}$ 以内，从而近似计算 m次本原单位根 ζ_m 对应的 $|\mathrm{Per}_{\zeta_m}(X)|^2$ ，其乘法误差为 $g = n^{O(1)}$。本节将展示如何根据近似结果寻找$\mathrm{Per}_{\zeta_m}(X)$ 的表示（见定义 3.6）。

回忆一下，根据 (27)，对于二进制矩阵 X，$\mathrm{Per}_{\zeta_m}(X)$ 是环 $\mathbb{Z}[\zeta_m]$ 中的一个元素，可以表示为 ζ_m 的多项式。由于 $\Phi_m(\zeta_m) = 0$ 且 $\deg \Phi_m = \phi(m)$，我们可以将 $\mathbb{Z}[\zeta_m]$中的任意代数整数表示为次数至多为 $\phi(m)-1$ 的多项式。事实上，这种表示是唯一的。更详细的背景见 定义 2.10。

定义 4.5 ($\mathbb{Z}[\zeta_m]$的表示)。对于整数 $m \geq 1$，代数整数 $\alpha \in \mathbb{Z}[\zeta_m]$ 的表示是一个元组 $(a_0,\ldots,a_{\phi(m)-1})$，满足

$$\alpha = \sum_{i=0}^{\phi(m)-1} a_i \zeta_m^i. \tag{54}$$

作为 ζ_m 的多项式，该表示是 α 除以分圆多项式Φ_m所得的余数。对于整数 A，若表示在 $[A,B]$ 中有界，则称其为有界表示；如果对每个 $0 \leq i \leq \phi(m)-1$，都有$A \leq a_i \leq B$。

为了从近似中提取表示，我们依赖以下引理，该引理指出，系数 a_i 可以用 $n^{O(1)}$ 位表示。

定理 4.6 (分圆多项式系数的界 [Vau75])。 对于整数 $m \geq 1$，令 $\Phi_m(x)$ 为第 m 个分圆多项式。$\Phi_m(x)$ 的系数的最大绝对值至多为 $e^{\frac{1}{2}d(m)\log(m)}$，其中 $d(n)$ 是约数函数，用于计算 m 的因数个数（包括1 和 m）。[2]

对于 $m = p_1^{a_1}\ldots,p_k^{a_k}$, $d(m) = (a_1+1)\ldots(a_k+1)$。因此我们可以得到平凡界 $d(m) \leq m$。根据定理 4.6，我们可以用至多 $O(m\log m)$ 位表示 $\phi_m(x)$。接下来的引理表明，$\mathrm{Per}_{\zeta_m}(X)$ 表示中的每个元素都可以用 poly(n) 位表示。

引理 *4.7* (*[BP86*，引理 2]) 。设 $s(x) = \sum_{i=0}^{m} s_i x^i, t(x) = \sum_{i=0}^{n} t_i x^i$ 是两个次数为 $m \geq n$ 的多项式。再设商 $q(x) = \sum_{i=0}^{m-n} q_i x^i$ 和余数 r 满足 $s(x) = q(x)t(x) + r(x)$。那么

$$\sum_{i=0}^{m-n} |q_i| \leq \left(1+\frac{N}{t_n}\right)^{m-n} \sum_{i=n}^{m} \frac{|s_i|}{t_n}, \tag{55}$$

其中 $N = \max(|t_n|, |t_{n-1}|, \ldots\ldots, |t_{2n-m}|)$，且当 $g < 0.$ 时 $t_g = 0$

就我们的目的而言，由于每个 A_i 都满足

$$A_\ell = \sum_{\sigma:\ell(\sigma)=\ell} \prod_{i=1}^{n} X_{i,\sigma(i)} \leq n!, \tag{56}$$

根据引理 4.7，我们得到以下推论。

[2]例如 $d(6) = 4$。

推论 4.8。 对于整数 $m \geq 1$ 和二进制 X，令 $(a_0,\ldots,a_{\phi(m)-1})$ 为$\mathrm{Per}_{\zeta_m}(X)$的表示。则

$$\max_{0\leq i\leq \phi(m)-1} \log|a_i| \leq O(m^2 \log m + n \log n). \tag{57}$$

证明。令

$$s(x) := \sum_{\ell=0}^{m-1} A_\ell \zeta_m^\ell. \tag{58}$$

根据定理 4.6，分圆多项式的系数至多为 $M = 2^{O(m \log m)}$。根据引理 4.7以及 Φ_m 是首一多项式这一事实，商的系数之和满足

$$\begin{aligned}\sum_{i=0}^{m-1-\phi(m)} |q_i| &\leq (1+M)^{m-\phi(m)-1} \cdot n! \cdot (m-\phi(m)-1) \\ &\leq 2^{O((m-\phi(m))\cdot m \log m + n\log n)}.\end{aligned} \tag{59}$$

该表示是 s 除以 Φ_m所得的余数。令 $r(x) = \sum_{i=0}^{\phi(m)-1} a_i x^i = s(x) - q(x)\Phi_m(x)$。我们有

$$\begin{aligned}|a_i| &\leq \left| s_i - \sum_{j=0}^{i} q_j t_{i-j} \right| \\ &\leq \max_i |s_i| + (\phi(m)-1)\cdot \max_i |q_i| \cdot \max_i |t_i| \\ &\leq n! + (\phi(m)-1)\cdot 2^{O((m-\phi(m))\cdot m\log m + n\log n)} \cdot M.\end{aligned} \tag{60}$$

Thus

$$\max_i \log|a_i| \leq O((m-\phi(m))\cdot m\log m + n\log n). \tag{61}$$

由于 $\phi(m) = \Omega(\frac{m}{\text{对数的对数}\, n})$，$m - \phi(m) = \Theta(m)$。 □

令 A 表示$\mathrm{Per}_{\zeta_m}(X)$的表示中系数的最大值。根据推论 4.8，对数 $A = O(m^2 \text{对数}\, m + n\text{对数}\, n)$，因此系数可用多项式$(n)$ 位表示，前提是 $m =$ 多项式(n)。

根据刘维尔逼近定理（定理 2.12），表示在 $[-A, A]$ 中有界的任意两个代数整数在复平面上的距离至少为 $\delta = 2^{-n^{O(1)}}$。

推论 4.9。 对于整数 A，设 α，β 是 $\mathbb{Z}[\zeta_m]$ 中的两个表示有界的代数整数。那么有 $|\alpha-\beta| \geq \frac{1}{(2A\cdot\phi(m)+1)^{\phi(m)-1}}$。

证明。 由于 $\mathbb{Z}[\zeta_m]$ 是一个加法群，$\alpha - \beta \in \mathbb{Z}[\zeta_m]$ 其最小多项式是首一的，且其表示在 $[-2A, 2A]$中有界。由 定理 2.12 可知，对于 $(a, b) = (0, 1)$，$d \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$，并且 $|\overline{\alpha-\beta}| \leq Ad$。这些事实给出

$$|\alpha-\beta| \geq \frac{1}{(2A\cdot\phi(m)+1)^{\phi(m)-1}}. \tag{62}$$

□

现在令 $M := (2A\phi(m)+1)^{\phi(m)-1}$。如果我们已经知道一个复数 $\tilde{\alpha}$，它与代数整数 α 的距离为 δ以内，且对于 $\delta \le \frac{1}{4M}$，那么对于每个表示同样在 $[-A, A]$中有界的其他代数整数 $\beta \neq \alpha$，$|\beta - \tilde{\alpha}| > \frac{3}{4M}$。基于这一观察，我们定义如下问题。

问题 2（近似代数整数问题（CAIP））。近似代数整数问题（CAIP）定义如下：给定（α、L_0、……、$L_{\phi(m)-1}$、T），其中 $\alpha \in \mathbb{C}$、L_0、……、$L_{\phi(m)-1}$、M 是非负整数（均使用 $n^{O(1)}$ 位表示），判断是否

- 存在一个代数整数 $\alpha' \in S$，使得 $|\alpha - \alpha'| \le 1/T$，或者
- 每个 $\alpha' \in S$ 都满足 $|\alpha - \alpha'| \ge 2/T$，

其中，集合 S 由 $\mathbb{Z}[\zeta_m]$ 中满足其表示（a_0、……、$a_{\phi(m)-1}$）满足 $0 \le a_i \le L_i$ 的代数整数组成，对于 $0 \le i \le \phi(m) - 1$。保证给定实例属于其中一种情况。

事实上，caip 可以使用非确定性图灵机（NTM）求解。

定理 4.10。CAIP $\in$NP。

证明。我们可以使用足够多的位（但仍然是多项式数量的位）来表示 ζ_m，将其表示为一个复数 ξ，使得

$$|\zeta_m - \xi| = o\left(\frac{1}{T \cdot \phi(m)^2 \cdot \max_i L_i}\right). \tag{63}$$

对于每个 $\beta = b_0 + b_1\zeta_m + \ldots + b_{\phi(m)-1}\zeta_m^{\phi(m)-1}$，由 $\tilde{\beta} = b_0 + b_1\xi + \ldots + b_{\phi(m)-1}\xi^{\phi(m)-1}$˜ 近似且满足 $|\beta - \beta| = o(1/T)$ 的情况，对每个 i 和整数 $b_i \in [L_i]$ 都成立。

˜如果非确定性图灵机非确定性地找到了满足 $|\alpha - \beta| \le 1.5/T$ 的 b_0、……、$b_{\phi(m)-1}$，那么 $|\alpha - \beta| \le 1/T$。否则，每个 β 都满足 $|\alpha - \beta| \ge 2/T$。 □

问题 caip 仅考虑每个系数 $b_i \in [0, L_i]$ 的情况。为了将其扩展到一般情况，即第 i 个元素位于 $[U_i, L_i]$ 中，我们可以将 α 平移到 $\beta = \alpha - U_i\zeta_m^i$，并使用 β 求解 caip，其中第 i 个参数为 $L_i - U_i$。因此，只需考虑前一种设定。

给定一个用于 caip 的预言机，我们可以搜索出一个满足条件的代数整数。

定理 4.11. 设 $\mathcal{O}$ 是一个求解 CAIP 的预言机。那么存在一种算法，只需向 $\mathcal{O}$ 发出 $O(\log(L_1 \ldots L_{\phi(m)-1}))$ 次查询，就能找到一个满足条件的代数整数；如果不存在，则返回 $\perp$。

证明。算法 $\mathcal{A}$ 基本上是针对每个系数进行二分搜索。

首先，$\mathcal{A}$ 运行 $b \leftarrow \mathcal{O}(\alpha, L_0, \ldots, L_{\phi(m)-1}, T)$；如果输出为 $b = 0$，那么 $\mathcal{A}$ 返回 $\perp$。否则，一定存在一个满足条件的代数整数 α'。然后 $\mathcal{A}$ 执行以下步骤：

1. 设 $\beta \leftarrow \alpha$。
2. 对于 $j = \phi(m) - 1, \ldots, 0$,
   （a）设定 $W \leftarrow 0$ 和 $R \leftarrow \lfloor L_j/2 \rfloor$。
   (b) 重复执行以下步骤，直到 $R = 0$:
      i. Compute $b_i \leftarrow \mathcal{O}(\beta, L_0, \ldots, L_{j-1}, R, 0, \ldots, 0, T)$.

ii. If $b = 0$, set $\beta \leftarrow \beta - (R+1)\xi^j$ and $W \leftarrow W + R + 1$.

iii. Set $R \leftarrow \lfloor R/2 \rfloor$.

(c) Set $a_j \leftarrow W$.

3. 输出 $(a_0, \ldots, a_{\phi(m)-1})$。

我们证明该算法对于 $j = \phi(m) - 1$ 是正确的；对于其他系数，正确性分析同样适用。首先，该算法必然终止，因为在每次迭代中 R 都会减少一半。关于正确性，我们注意到每次迭代后 $\beta + Wz^{\phi(m)-1} = \alpha$ 均成立。在每一步中，令一个满足条件的代数整数表示 β'，记作

$$\beta' = c_{\phi(m)-1} z^{\phi(m)-1} + a_{\phi(m)-2} z^{\phi(m)-2} + \ldots + a_0 \tag{64}$$

在运行 步骤 2(b)ii 之前。通过归纳法，只需证明在 步骤 2(b)ii之后，首项系数不超过 R。对于基例，由于 α' 的首项系数不超过 $L_{\phi(m)-1}$，该断言成立。若 $b = 0$，则 $R < c_{\phi(m)-1} \leq 2R+1$，且 $c_{\phi(m)-1} - (R+1) \geq 0$；否则，存在一个满足条件的 β'，使得 $c_{\phi(m)-1} \leq R$。因此，在 步骤 2(b)ii之后，存在一个满足条件的代数整数，其首项系数不超过 R。 □

5 平均情形困难性

在平均情形困难性的背景下，Aaronson 和 Arkhipov[AA11] 研究了1-永久式对于独立同分布高斯矩阵的计算困难性。近期，Haferkamp、Hangleiter、Eisert 和 Gluza[HHEG20] 研究了截断均匀分布的平均情形困难性。

在本节中，只要分布满足一种称为强自相关性质的性质，我们就将他们的结果扩展到 z-永久式以及范围广泛的分布。

我们的思路源自 Aaronson 和 Arkhipov [AA11]：如果能对足够多的点计算出低次多项式，那么就存在一种算法，能够以高概率恢复整个多项式。更准确地说，我们使用以下含噪多项式插值算法。

定理 *5.1*（*Berlekamp-Welch* 算法 [*BV*]）。设 q 是域 $\mathbb{F}$上的次数为 d的单变量多项式。假设给定 m 对 $\mathbb{F}$ 元素 $(x_1, y_1), \ldots, (x_m, y_m)$（其中 $x_i's$ 均互不相同），并且已知对于超过 $(m+d)/2$ 个 i 值，$y_i = q(x_i)$。那么存在一种确定性算法，可以用 $poly(n, d)$ 次域运算重构 q。

现在我们定义如下性质，在该性质成立时，可以应用基于 Berlekamp-Welch 算法的随机自归约性。

定义 *5.2*（强自相关性质）。考虑一个 X 具有实数 $\mathcal{F}$、均值为 *0* 且方差为 *1* 的随机变量。我们将其记为 $X \sim \mathcal{F}_{\mathbb{R}}(0, 1)$。通过平移和缩放随机变量 $X \to \mu + \sigma^2 X.$，我们定义均值为 μ、方差为 σ^2 的 $\mathcal{F}_{\mathbb{R}}(\mu, \sigma^2)$。我们取 $\epsilon < \frac{1}{2}$。我们可以定义复随机变量 $Z = X + iY$，$X \sim \mathcal{F}_{\mathbb{R}}(\mu_1, 1/2)$ $Y \sim \mathcal{F}_{\mathbb{R}}(\mu_2, 1/2)$，并且 X和Y相互独立。我们记为 $Z \sim \mathcal{F}_{\mathbb{C}}(\mu_1 + i\mu_2, 1)$。现在考虑以下三个分布

$$X = \mathcal{F}_{\mathbb{C}}(0, 1)^n \tag{65}$$

$$\mathcal{D}_1 = \mathcal{F}_{\mathbb{C}}\left(0, (1-\varepsilon)^2\right)^n, \tag{66}$$

$$\mathcal{D}_2 = \prod_{i=1}^{n} \mathcal{F}_{\mathbb{C}}(v_i, 1) \tag{67}$$

对于某个向量 $v \in \mathbb{C}^n$。如果存在常数定义 5.2，使得 M_1，M_2 且与 n无关，ϵ则称某个分布满足强自相关性质，

$$\|\mathcal{D}_1 - X\| \leq 2nM_1\varepsilon, \tag{68}$$

$$\|\mathcal{D}_2 - X\| \leq \sqrt{2n}M_2\|v\|_2 . \tag{69}$$

当 $\mathcal{F}$ 是复高斯分布或截断均匀分布时，通过直接计算可知二者都满足这一标准 [AA11，HHEG 20]。在附录 B中，我们给出一个充分条件，在此条件下，几乎所有行为良好的 $\mathcal{F}$ 都满足这一标准。

现在我们准备证明，和永久式一样，z-永久式也具有随机自归约性。

定理 5.3 (z-永久式的随机自归约性)。 假设不存在经典高效算法能够计算 z-永久式，且对所有 $\{0,1\}$-矩阵均如此。对所有 $\delta \geq 1/\mathrm{poly}(n)$，以下问题都是经典困难的：给定一个从 $\mathcal{F}_{\mathbb{C}}(0,\ 1)^{n\times n}$ 中抽取、且满足强自相关性质的 $n \times n$ 矩阵 X，以至少 $3/4 + \delta$ 的概率输出 $\mathrm{Per}_z(X)$，其中概率取自 $\mathcal{F}_{\mathbb{C}}(0,\ 1)^{n\times n}$。

证明。 令 $M = (x_{ij}) \in \{0,1\}^{n\times n}$ 为任意一个 $\{0,1\}$-矩阵。我们将说明，在能够访问满足以下条件的预言机 $\mathcal{O}$ 的情况下，如何用概率多项式时间计算 $\mathrm{Per}_z(M)$:

$$\Pr_{X\sim\mathcal{F}_{\mathbb{C}}(0,1)^{n\times n}}[\mathcal{O}(X) = \mathrm{Per}_z(X)] \geq \frac{3}{4} + \delta . \tag{70}$$

我们从分布 $\mathcal{F}_{\mathbb{C}}(0,\ 1)^{n\times n}$ 中选择一个矩阵 $Y \in \mathbb{C}^{n\times n}$，并定义

$$X(t) := (1-t)Y + tM, q(t) := \mathrm{Per}_z(X(t)) \tag{71}$$

使得 $X(0) = Y$ 且 $X(1) = M$，并且 $q(t)$ 是关于 t 的次数至多为 n 的单变量多项式，且$q(1) = \mathrm{Per}_z(X(1)) = \mathrm{Per}_z(M)$。现在令

$$L := \left\lceil \frac{n}{\delta} \right\rceil \quad \text{and} \quad \varepsilon := \frac{\delta}{(4n^2M_1 + 4n^2M_2)L} .$$

对于每个 $\ell \in [L]$，在输入矩阵 $X(\varepsilon\ell)$ 上调用预言机 $\mathcal{O}$。然后，使用 Berlekamp-Welch 算法（定理 5.1），尝试找到一个次数为 n 的多项式 q'： $\mathbb{C} \to \mathbb{C}$，使得

$$q'(\varepsilon\ell) = \mathcal{O}(X(\varepsilon\ell)) \tag{72}$$

对于至少 $3/4 + \delta$ $\ell \in [L]$ 的一个比例。如果没有找到这样的 q'，则失败；否则，输出 $q'(1)$ 作为 $\mathrm{Per}_z(M)$ 的猜测值。现在我们证明上述算法成功（即输出 $q'(1) = \mathrm{Per}_z(M)$）的概率至少为 $1/2+\delta/2$，其中 Y。假设这一点成立，很明显，只需针对 Y 采用不同的选择重复运行算法 $O\left(1/\delta^2\right)$ 次，然后输出多数结果，就可以将成功概率提高到（例如） $2/3$。为了证明这一结论，请注意，对每个 $\ell \in [L]$，都可以将矩阵 $X(\varepsilon\ell)$ 视为从分布中抽取

$$\mathcal{D}_\ell := \prod_{i,j=1}^{n} \mathcal{F}_{\mathbb{C}}\left(\varepsilon\ell a_{ij}, (1-\varepsilon\ell)^2\right) . \tag{73}$$

Let

$$\mathcal{D}'_\ell := \prod_{i,j=1}^{n} \mathcal{F}_{\mathbb{C}}(\varepsilon\ell a_{ij}, 1). \tag{74}$$

根据三角不等式以及 定义 5.2 ($X \sim \mathcal{F}_{\mathbb{C}}(0,\ 1)^{n\times n}$)，

$$\begin{aligned}\|\mathcal{D}_\ell - X\| &\le \left\|\mathcal{D}_\ell - \mathcal{D}'_\ell\right\| + \left\|\mathcal{D}'_\ell - X\right\| \\ &\le 2n^2 M_1 \varepsilon\ell + \sqrt{2n^2}M_2\sqrt{n^2(\varepsilon\ell)^2} \\ &\le \left(2n^2M_1 + 2n^2M_2\right)\varepsilon l \le (2n^2M_1 + 2n^2M_2)\varepsilon L \\ &\le \frac{\delta}{2}\,. \end{aligned} \tag{75}$$

我们有

$$\begin{aligned}\Pr[\mathcal{O}(X(\varepsilon\ell)) = q(\varepsilon\ell)] &\ge \frac{3}{4} + \delta - \|\mathcal{D}_\ell - X\| \\ &\ge \frac{3}{4} + \frac{\delta}{2}\,. \end{aligned} \tag{76}$$

现在令 S 表示所有满足 $\ell \in [L]$ 的 $\mathcal{O}$（X（$\varepsilon\ell$））$= q$（$\varepsilon\ell$）。根据反向马尔可夫不等式[EG01],

$$\Pr\left[|S| \ge \left(\frac{1}{2} + \frac{\delta}{2}\right)L\right] \ge 1 - \frac{\frac{1}{4} - \frac{\delta}{2}}{\frac{1}{2} - \frac{\delta}{2}} \ge \frac{1}{2} + \frac{\delta}{2}\,. \tag{77}$$

因此，我们只需运行上述算法 $O(\frac{1}{\delta^2})$ 次，以放大成功概率。之后，以高概率，我们有

$$|S| \ge \left(\frac{1}{2} + \frac{\delta}{2}\right)L\,.$$

根据定理 5.1，Berlekamp-Welch 算法成功；其输出的多项式 q' 将等于 q。这证明了该结论。

□

6 平均情形困难性与近似

自 Aaronson 和 Arkhipov 关于玻色子采样的开创性工作 [AA11] 发表以来，针对特定分布 [AA11, HHEG20]，平均情况下对 1-永久式进行近似的问题一直受到研究。特别地，Aaronson 和 Arkhipov [AA11] 猜想，一个称为高斯永久式估计（也记作 GPE$_\times$）的问题是 #P-困难的。GPE$_\times$ 问题要求计算 Per(X)，其乘法误差为 ϵ，并且对于矩阵 X，以至少 $1-\delta$ 的概率成立；该矩阵的每个元素都独立地从归一化高斯分布中采样。对于玻色子采样所体现的量子优越性，最终目标是证明 GPE$_\times$ 的加法版本（记作 GPE$_\pm$）同样困难。基于另一个称为永久函数反集中猜想（PACC）的猜想，可以推导出 GPE$_\pm$ 与 GPE$_\times$ 一样困难。下文中，我们将 $\mathcal{G} = \mathcal{N}_{\mathbb{C}}(0,1)^{n\times n}$ 表示为均值为零、方差为单位方差的 $n \times n$ 独立同分布高斯矩阵的分布。

问题 3 (GPE$_\times$)。给定输入 $X \sim \mathcal{N}_{\mathbb{C}}(0,1)^{n\times n}$ 个独立同分布高斯变量（复正态分布）以及 $\epsilon, \delta > 0$，估计 $\mathrm{Per}(X)$，误差不超过 $\pm\epsilon|\mathrm{Per}(X)|$，其概率至少为 $1-\delta$，其中 X。

问题 4 (GPE$_\pm$)。给定输入 $X \sim \mathcal{N}_{\mathbb{C}}(0,\ 1)^{n\times n}$ 个独立同分布高斯变量（复正态分布）以及 ϵ，$\delta > 0$，以加法方式估计 $\mathrm{Per}(X)$（即误差在 $\pm\epsilon\sqrt{n!}$ 以内），其概率至少为 $1-\delta$，其中 X

本节将讨论从一般分布 $\mathcal{H}$ 中采样的矩阵的 z-永久式计算难度，其中每个元素均为独立同分布采样。我们首先为分布 $\mathcal{H}$定义永久式估计（PE）的乘法版本和加法版本。

问题 5 ($\mathrm{PE}_{\mathcal{H},\ z,\ \times}$)。 给定输入 $X \sim \mathcal{H}$ 和 $\epsilon,\ \delta > 0$，估计 $\mathrm{Per}(X)$ ，使误差不超过$\pm\epsilon|\mathrm{Per}(X)|$，且在 X 上的概率至少为 $1-\delta$。

为方便起见，$\mathrm{PE}_{\mathcal{H},\ 1,\ \times}$ 也记作 $\mathrm{PE}_{\mathcal{H},\ \times}$。类似地，我们可以定义上述问题的加法版本。

问题 6 ($\mathrm{PE}_{\mathcal{H},\ z,\ \pm}$)。 给定输入 $X \sim \mathcal{H}$ 和 $\epsilon,\ \delta > 0$，估计 $\mathrm{Per}_z(X)$ ，使误差不超过$\pm\epsilon g(n)$，且在 X 上的概率至少为 $1-\delta$。为方便起见，$\mathrm{PE}_{\mathcal{H},\ 1,\ \pm}$ 也记作 $\mathrm{PE}_{\mathcal{H},\ \pm}$。

根据定义，我们有 $\mathrm{GPE}_{\times} = \mathrm{PE}_{\mathcal{G},\ \times}$ 和 $\mathrm{GPE}_{\pm} = \mathrm{PE}_{\mathcal{G},\ \pm}$，其中 $g = \sqrt{n!}$ 设 $d = \binom{n}{2}$。对于 $r \in (0, \frac{1}{d+1})$，设 $S_r := \{z = e^{i2\pi r}\zeta_{d+1}^{i-1} :\ i \in [d+1]\}$，其中 $\zeta_k := e^{i2\pi/k}$ 是一个本原 k 次单位根。设 $\mathcal{O}$ 为一个预言机，给定 $X \sim \mathcal{H}$，输出 z 个点的永久式近似值，即 $\mathrm{Per}_{z_1}(X) \ldots, \mathrm{Per}_{z_{d+1}}(X)$，其中 $z_1, \ldots, z_{d+1} \in S_r$。更正式地说，我们定义 $\mathcal{O}_{\times}$和 $\mathcal{O}_{\pm}$为预言机，分别给出乘法误差和加法误差近似：

定义 6.1 ($\mathcal{O}_{\times}$，$\mathcal{O}_{\pm}$)。 预言机 $\mathcal{O}_{\times}$ 和 $\mathcal{O}_{\pm}$ 定义如下：

- 给定 $X \sim \mathcal{H}$，$\mathcal{O}_{\times}(X,\ \epsilon,\ \delta)$ 是一个预言机，它输出向量 $y = (y_1,\ \ldots\ldots,\ y_{d+1})^{\top}$，使得对于每个 $i \in [d+1]$，$|y_i - 永久式_{z_i}(X)| \le \epsilon|永久式_{z_i}(X)|$ 的概率至少为 $1-\delta$，其中概率取自对 X的选择。

- 给定 $X \sim \mathcal{H}$和一个可高效计算的函数 g，$\mathcal{O}_{\pm}(X,\ \epsilon,\ \delta)$ 是一个预言机，它输出向量 $y = (y_1,\ \ldots\ldots,\ y_{d+1})^{\top}$，使得对于每个 $i \in [d+1]$，都有：$|y_i - 永久式_{z_i}(X)| \le \epsilon g(n)$的概率至少为 $1-\delta$，其中概率取自对 X的选择。

本节余下部分将致力于证明：如果 $\mathcal{O}_{\times}$ 可以被经典模拟，那么$\mathrm{PE}_{\mathcal{H},\ \times}$ 就可以高效求解；对于 $\mathcal{O}_{\pm}$ 和 $\mathrm{PE}_{\mathcal{H},\ \pm}$ 以 $\mathcal{O}_{\times}$ 和 $\mathrm{PE}_{\mathcal{H},\ \pm}$代替时，结论同样成立。证明与 Lipton 的证明 [Lip91] 类似，后者证明了在有限域 $\mathbb{F}_p$ 上 $p > n$的永久式具有平均情形困难性。在我们的情形中，给定单位圆上 $\mathrm{Per}(X)$ 个点处的近似值，我们可以近似 $\Omega(n^2)$ 。

首先，我们给出以下两个关于多项式插值的引理。一个针对乘法误差，另一个针对加法误差。

引理 6.2. 对于整数 $d \ge 1$，设 f 是一个次数为 d 的复值多项式，$\mathcal{A}$ 是一个算法，可在点 $x_1,\ldots,x_{d+1}$ 上将 f 近似到加法误差 ϵ。存在一个算法，在输入 $x \in \mathbb{T}$ 时，调用 $\mathcal{A}$ 共 $d+1$ 次，并输出 $f(x)$ 的估计值，其加法误差为 $(d+1)\|V^{-1}\|\epsilon$，其中 $V = V(x_1,\ldots,x_{d+1})$ 是节点为 $x_1,\ldots,x_{d+1}$ 的范德蒙德矩阵。

证明. 令 $\tilde{y}_1,\ldots,\tilde{y}_{d+1}$ 分别为 $\mathcal{A}$ 在 $x_1,\ldots,x_{d+1}$ 上的估计值。令 $\tilde{y} = (\tilde{y}_1,\ldots,\tilde{y}_{d+1})^{\top}$ 和 $x = (x_1,\ldots,x_{d+1})^{\top}$ 为相应的列向量。由于对于每个 $i \in [d+1]$，$|\tilde{y}_i - y_i| \le \epsilon$，$\|\tilde{y} - y\| \le \epsilon\sqrt{d+1}$。

令 $c = (c_0,\ldots,c_d)^{\top}$ 为 $f(x) = \sum_{i=0}^{d} c_i x^i$ 的系数向量。求解线性方程 $V\tilde{c} = \tilde{y}$，即可得到系数的估计值。对于 $x \in \mathbb{T}$，令 $v = (1, x, x^2, \ldots, x^d)$ 为在 x 上求值所得的单项式向量。我们的目标是界定距离

$$|v \cdot (\tilde{c} - c)| \le \|(V^{-1})^{\top}v\|\|V(c - c')\| \le \|v\|\|V^{-1}\|\|\tilde{y} - y\| \le (d+1)\|V^{-1}\|\epsilon. \tag{78}$$

第一个不等式由柯西-施瓦茨不等式得出。第二个不等式由矩阵范数的定义得出。最后一个不等式成立是因为 $\|\tilde{y} - y\| \le \epsilon$ 和 $\|v\| = \sqrt{d+1}$。 □

如果我们将问题限制为近似具有非负系数多项式的 $f(1)$，就能做得更好。具体而言，我们证明：如果 $\mathcal{A}$ 以乘法误差 ϵ近似 x_1，……，x_{d+1}，其中多项式 f具有非负系数，那么存在一种算法，能够以如上所述的乘法误差近似 $f(1)$。

引理 6.3. 对于整数 $d \geq 1$，设 f 是一个次数为 d 、系数非负的多项式， $\mathcal{A}$ 是一个算法，它在 $x_1,\ldots,x_{d+1} \in \mathbb{T}$ 上以乘法误差 ϵ 近似 f。那么存在一个算法，以乘法误差 $(d+1)\|V^{-1}\|\epsilon$ 近似 $f(1)$，其中$V = V(x_1,\ldots,x_{d+1})$ 是节点为 $x_1,\ldots,x_{d+1}$ 的范德蒙德矩阵。

证明。令 $\tilde{y}_1,\ldots,\tilde{y}_{d+1}$ 为 $\mathcal{A}$ 在 $x_1,\ldots,x_{d+1}$ 上的估计值，以及 $y = (\tilde{y}_1,\ldots,\tilde{y}_{d+1})^\top$。求解线性方程 $V\tilde{c} = \tilde{y}$ 得到 $\tilde{c} = V^{-1}\tilde{y}$。另外，令 $\tilde{f}(z) := \sum_{i=0}^{d} \tilde{c}_i z^i$ 为通过求解线性方程组得到的近似多项式。

由于 f具有非负系数，因此对于每个 $x \in \mathbb{T}$， $|f(x)| \leq f(1) = \langle 1^{d+1}, c\rangle$。由于 $\|\tilde{y} - y\| \leq \epsilon\|y\| \leq \epsilon\sqrt{d+1}\cdot f(1)$,

$$|\tilde{f}(1) - f(1)| = |\langle 1^{d+1}, \tilde{c} - c\rangle| \leq \sqrt{d+1}\|\tilde{c} - c\| \leq (d+1)\|V^{-1}\|\cdot\epsilon\cdot|f(1)|. \tag{79}$$

第一个不等式由柯西-施瓦茨不等式得出。因此，一个算法输出的近似值为 $|\tilde{c}|_1$，乘法误差为 $(d+1)$ $\epsilon\|V^{-1}\|$。 □

现在我们准备证明定理 6.4。根据引理 6.2 和引理 6.3，我们将其分为两种情况。

定理 6.4。以下陈述成立：

1. 假设$\mathrm{PE}_{\mathcal{H},\times}$ 是#P-困难问题，且 $\mathcal{H}$ 是非负分布，并且多项式层级是无限的，那么 $\mathcal{O}_\times$ 不具有经典高效算法，即不存在一个运行时间为$\mathrm{poly}(n, \frac{1}{\epsilon}, \frac{1}{\delta})$的 $\mathcal{O}_\times$ 模拟。 *2.* 假设$(\mathrm{PE}_{\mathcal{H},\pm}, g)$ 是 #P- 困难问题，且多项式层级是无限的，那么 $\mathcal{O}_\pm$ 不具有经典高效算法，即不存在一个运行时间为$\mathrm{poly}(n, \frac{1}{\epsilon}, \frac{1}{\delta})$)的 $\mathcal{O}_\pm$ 经典模拟。

证明。对于 (1)，我们给出非构造性证明。令 $d = \binom{n}{2}$。对于 $r \in (0, \frac{1}{d+1})$，令 $S_r := \{z = e^{i2\pi r}\zeta_{d+1}^{i-1} : i \in [d+1]\}$，其中 $\zeta_k := e^{i2\pi/k}$ 是一个本原 k 次单位根。我们证明，使 $\mathrm{Per}_z(X)$ 可高效计算的点 $z \in S_r$ 的数量不可能超过 d。反设并非如此。于是令 $\mathcal{O}_\times$ 为运行时间为 $\mathrm{poly}(n, 1/\epsilon, 1/\delta)$ 的算法，以概率 $1-\delta$ 将 $\mathrm{Per}_{z_1}(X)\ldots,\mathrm{Per}_{z_{d+1}}(X)$ 近似到精度 ϵ，其中 $S_r = \{z_1,\ldots,z_{d+1}\}$。应用引理 6.3 证明中的算法，我们通过以下算法调用用于 $\mathcal{H}_\times$ 的预言机$\mathcal{O}_\times(X,\epsilon,\delta)$:

1. 获取 $y = (y_1,\ldots,y_{d+1})^\top \leftarrow \mathcal{O}_\times(X, \epsilon(d+1)^{-1/2}, \delta/(d+1))$;

2. 求解线性方程组 $Vc = y$，其中 $V = V(z_1,\ldots,z_{d+1})$。

3. 输出 c 的元素求和，作为 $\mathrm{Per}(X)$ 的近似。

根据假设，对于每个 $i \in [d+1]$，以至少 $1 - \frac{\delta}{d+1}$ 的概率， $|y_i - \mathrm{Per}_{z_i}(X)| \leq \frac{\epsilon}{\sqrt{d+1}}|\mathrm{Per}_{z_i}(X)|$。由于 S_r中的点等间距分布， $\frac{1}{\sqrt{d+1}}V$是一个酉矩阵，且$\sqrt{d+1}V^{-1}$也是如此。这意味着矩阵范数 $\|V^{-1}\| = (d+1)^{-1/2}$。根据 引理 6.3 以及并集

界，该算法以乘法误差 ϵ 近似 $\mathrm{Per}(X)$，成功概率至少为 $1-\delta$。根据假设 $\mathrm{PE}_{\mathcal{H},\times}$ 是困难的，我们可以得出 $\mathrm{P}^{\#\mathrm{P}} \subseteq \mathrm{BPP}^{\mathcal{O}_\times} \subseteq \mathrm{BPP}$，并且多项式层级坍缩。

对于 (2)，我们使用相同的 S_r，然后令 $\mathcal{O}_\pm$ 为算法，它们的运行时间为 $\mathrm{poly}(n, 1/\epsilon, 1/\delta)$，并分别以概率 $1-\delta$ 将 $\mathrm{Per}_{z_1}(X) \ldots, \mathrm{Per}_{z_{d+1}}(X)$ 近似到精度 ϵ，其中$S_r = \{z_1, \ldots, z_{d+1}\}$。应用引理 6.2 证明中的算法，我们通过以下算法调用预言机$\mathcal{O}_\pm(X, \epsilon, \delta)$ 来处理 $\mathcal{H}_\pm$：

1. 获取 $y = (y_1, \ldots, y_{d+1})^\top \leftarrow \mathcal{O}_\pm(X, \epsilon(d+1)^{-1/2}, \delta/(d+1))$】【。
2. 求解线性方程组 $Vc = y$，其中 $V = V(z_1, \ldots, z_{d+1})$。
3. 输出 c 中各元素的求和，作为 $\mathrm{Per}(X)$ 的近似值。

根据假设，对于每个 $i \in [d+1]$，以至少 $1 - \frac{\delta}{d+1}$ 的概率，$|y_i - \mathrm{Per}_{z_i}(X)| \leq \frac{\epsilon}{\sqrt{d+1}} g(n)$。由于 S_r 中的点等间距排列，$\frac{1}{\sqrt{d+1}} V$ 是酉矩阵，$\sqrt{d+1} V^{-1}$ 也是酉矩阵。这意味着矩阵范数 $\|V^{-1}\| = (d+1)^{-1/2}$。根据 引理 6.2 和并合界，该算法以至少 $1-\delta$ 的概率输出 $\mathrm{Per}(X)$ 的一个近似，其加法误差为 $\epsilon g(n)$。根据我们的假设 $(\mathrm{PE}_{\mathcal{H},\times}, g)$ 是 #P-困难的，我们得出 $\mathrm{P}^{\#\mathrm{P}} \subseteq \mathrm{BPP}^{\mathcal{O}_\pm} \subseteq \mathrm{BPP}$，且多项式层级坍缩。

□

乍看之下，我们的结果似乎不适用于独立同分布高斯矩阵，因为它只有在概率指数级小的情况下才是正定的。然而，类似于 [AA11], ，我们证明了 $\mathrm{PE}_{\mathcal{G},z,\pm}$ 可以在 $g(n) = \sqrt{n!}$ 下归约到 $\mathrm{PE}_{\mathcal{G},z,\times}$。

引理 6.5. $(\mathrm{PE}_{\mathcal{G},z,\pm})$ 在 $g = \sqrt{n!}$ 可在多项式时间内归约到 $\mathrm{PE}_{\mathcal{G},z,\times}$.

证明。 假设我们有一个多项式时间算法 M，它能输出 $\mathrm{Per}_z(X)$ 的一个良好乘法近似——也就是说，一个 w，使得：

$$|w - \mathrm{Per}_z(X)| \leq \epsilon |\mathrm{Per}_z(X)|. \tag{80}$$

以至少 $1-\delta$ 在 X 上的马尔可夫不等式（$\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^2] = n!$，参见 引理 A.1 ）：

$$\Pr_{X\sim\mathcal{G}}\left[|w - \mathrm{Per}_z(X)| > k\sqrt{n!}\right] < \frac{1}{k^2} \tag{81}$$

根据并合界，

$$\begin{aligned}\Pr_{X\sim\mathcal{G}}\left[|w - \mathrm{Per}_z(X)| > \epsilon k\sqrt{n!}\right] &\leq \Pr_{X\sim\mathcal{G}}\left[|w - \mathrm{Per}_z(X)| > \epsilon|\mathrm{Per}_z(X)|\right] + \Pr_{X\sim\mathcal{G}}\left[\epsilon|\mathrm{Per}_z(X)| > \epsilon k\sqrt{n!}\right] \\ &\leq \delta + \frac{1}{k^2}.\end{aligned}$$

令 $\delta = \frac{\delta'}{2}, k = \sqrt{\frac{2}{\delta}}$ 和 $\epsilon = \frac{\epsilon'}{k}$，我们有 $\delta + \frac{1}{k^2} = \delta'$，由此完成证明。

□

现在我们引入一个推广原始永久式反集中性猜想的猜想。

猜想3 (z-永久函数反集中猜想 (z-PACC))。 存在一个多项式p，使得对于正整数 n、实数 $\delta > 0$ 和 $z \in \mathbb{T}$,

$$\Pr_{X\sim\mathcal{G}}\left[|\mathrm{Per}_z(X)|^2 \geq \frac{\sqrt{n!}}{p(n, 1/\delta)}\right] \geq 1 - \delta. \tag{82}$$

特别是，$z=-1$ 由 Aaronson 证明 [AA11] 并且 $z=1$ 是一个被广泛认为成立的标准猜想。

推论 6.6. 假设1-*PACC*成立。设$\mathrm{GPE}_{\times}$ 是#P-困难问题，且多项式层级是无限的，那么 $\mathcal{O}_{\times}$ 不具有经典高效算法，也就是说，不存在一个在$\mathrm{poly}(n,\frac{1}{\epsilon},\frac{1}{\delta})$时间内运行的 $\mathcal{O}_{\times}$ 模拟算法。

证明。假设 $\mathrm{PE}_{\mathcal{G},z,\times}$ 存在一个运行时间为 $\mathrm{poly}(n,\frac{1}{\epsilon},\frac{1}{\delta})$ 的经典高效算法。那么，我们可以求解 $\mathrm{PE}_{\mathcal{G},z,\times}$，进而求解 $d+1$ 个点上的 $\mathrm{GPE}_{z,\times}$。根据引理 6.5，该算法可以求解 $d+1$ 个点上的$\overline{(\mathrm{PE}_{\mathcal{G},z,\pm})}$，其时间为 $\sqrt{n!}$，进而求解 $\mathrm{GPE}_{\pm}$。假设 1-PACC [AA11], $\mathrm{GPE}_{\pm}$ 与 $\mathrm{GPE}_{\times\cdot}$ 多项式等价，那么就存在一个经典多项式算法求解 $\mathrm{GPE}_{\times}$，这与多项式层级无限的假设矛盾。

□

最后，我们证明，对于任意满足 X, X^* 同分布的分布 X，近似 $\mathrm{Per}_z(X)$ 与近似 $\mathrm{Per}_{z^*}(X)$ 一样困难。类似的证明思路也适用于 $|\mathrm{Per}_z(X)|^2$。

引理 6.7。 对于任意分布 X，若 X, X^* 同分布，且存在一个运行时间为 $\mathrm{poly}(n,1/\delta,1/\epsilon)$ 的算法，能以概率 $1-\delta$将$\mathrm{Per}_z(X)$ 近似到乘法（分别为加法）误差 ϵ 以内，则存在一个算法，能以概率 $1-\delta$将$\mathrm{Per}_{z^*}(X)$ 近似到乘法（分别为加法）误差 ϵ 以内。

证明。根据假设，设 $\mathcal{A}(X,0^{1/\epsilon},0^{1/\delta})$ 是一个算法，它能以概率 $1-\delta$ 将 $\mathrm{Per}_z(X)$ 近似到误差 ϵ 以内。

由于 $\mathrm{Per}_{z^*}(X)^*=\mathrm{Per}_z(X^*)$，且 X, X^* 同分布，为了计算 $\mathrm{Per}_{z^*}(X)$，算法 $\mathcal{B}$ 运行 $\mathcal{A}(X^*, 0^{1/\epsilon},0^{1/\delta})$，以概率 $1-\delta$ 得到 $\mathrm{Per}_z(X^*)$ 的一个近似值 $\tilde{P}$，其中概率取自 X^*。由于复数取复共轭后绝对值不变，

$$\begin{aligned}\Pr_X[|\tilde{P}-\mathrm{Per}_z(X^*)|\le\alpha(z,X^*)]&=\Pr_X[|\tilde{P}^*-\mathrm{Per}_{z^*}(X)|\le\alpha(z^*,X)]\\&\ge 1-\delta.\end{aligned}\tag{83}$$

这里针对乘法误差

$$\alpha(z,X^*)=\epsilon|\mathrm{Per}_z(X^*)|=\epsilon|\mathrm{Per}_{z^*}(X)|=\alpha(z^*,X).\tag{84}$$

对于加法误差，

$$\alpha(z,X^*)=\epsilon\sqrt{n!}=\alpha(z^*,X).\tag{85}$$

□

7 开放问题与讨论

本文研究了量子行列式的计算复杂性。量子行列式是矩阵永久式的一种 q 变形。矩阵 X 的 q-永久式定义如下，它同时推广了行列式和永久式。研究表明，当 $m=p^k$ 为奇素数幂，且 q 是一个本原 m 次单位根时，计算 q-永久式是 $\mathrm{Mod}_p\mathrm{P}$-困难的。这一结果意味着，若存在一种高效算法来计算 q-永久式，多项式层级就会坍塌。我们还证明，高效的

近似算法若用于计算 q-永久式，也会导致多项式层级坍塌。由于随机自归约性，对于广泛的一类分布，计算 q-永久式仍然是困难的。针对永久式困难性所发展的技术，可以推广到 z-永久式的最坏情形和平均情况。

这里列出几个本文尚未解决的有趣问题。

- 众所周知，可以通过判断一个二分图中是否存在完美匹配，来确定对于 $\{0,1\}$-矩阵 X，$\mathrm{Per}(X) \neq 0$ 是否成立；该二分图的邻接矩阵为 X。对于 $z \neq 1$，关于 z-永久式的这一性质能否高效计算？也就是说，是否存在一个多项式时间算法来确定 $\mathrm{Per}_z(X) \neq 0$ 是否成立？

- 我们已经证明 问题 2 属于 NP。 问题 2 是否存在多项式时间算法？

- 本文讨论了 $z \in \mathbb{T}$ 上 z-永久式的计算复杂性。自然会想到考虑复数的其他子集。例如，实数 z 上 z-永久式的计算复杂性是什么？

- 如 第 3.2 节所述，我们用于证明 ζ_m-永久式困难性的技术，只适用于 m 为素数幂的特殊情形。因此，我们的结果并未排除存在针对非素数幂 m的高效算法。是否存在一个多项式时间算法，能够计算 ζ_m-永久式，其中 m 不是素数幂？

- 永久函数反集中猜想最初由 Aaronson 和 Arkhipov 提出，对于证明高斯矩阵的1-永久式的加法近似与乘性近似等价至关重要。永久函数反集中猜想与 z-永久式反集中猜想3之间有何关系？能否由一个证明另一个，或者利用多项式插值给出多对一归约？

- $|\mathrm{Per}_z(X)|^2$ 的高阶矩，其中 X 取自复高斯分布 $\mathcal{G}$。

致谢

感谢 Scott Aaronson、Mohammad Hafezi 和 Dominik Hangleiter 提供的有益讨论。EJ 的研究由 ARO W911NF-15-1-0397、美国国家科学基金会 QLCI 项目资助（OMA-2120757）、AFOSR MURI FA9550-19-1-0399、美国能源部 QSA 计划以及西蒙斯基金会资助。SHH 感谢西蒙斯计算机科学研究员奖（奖项编号 510817）的支持。

参考文献

[AA11] Scott Aaronson 和 Alex Arkhipov。线性光学的计算复杂性。载于第四十三届 *ACM* 计算理论年度研讨会论文集，第 333–342 页，2011 年。[Ben87] Georgia Benkart。In herstein 的《抽象代数》。《美国数学月刊》，94(8)：804–806，1987 年。

[BKW19] Andreas Björklund、Petteri Kaski 和 Ryan Williams。用于多项式求值的广义 Kakeya 集与更快的费米子行列式计算。Algorithmica，81(10)：4010–4028，2019 年。[BL94] RB Bapat 和 AK Lal。关于 q-永久式的不等式。《线性代数及其应用》，197：397–409，1994 年。[BLW17] Marek Bożejko、Eugene Lytvynov 和 Janusz Wysoczański。q 变形交换关系的 Fock 表示。《数学物理学杂志》，58(7)：073501，2017 年。[BP86] Dario Bini 和 Victor Pan。多项式除法及其计算复杂度。《复杂性杂志》，2(3)：179–203，1986 年。[Bro86] Andrei Z Broder。随机匹配有多难？（关于永久式的近似）。载于《第十八届 ACM 计算理论年度研讨会论文集》，第 50–58 页，1986 年。[BS91] Marek Bożejko 和 Roland Speicher。广义布朗运动的一个例子。《数学物理通讯》，137(3)：519–531，1991 年。[Bür00] Peter Bürgisser。不变量式的计算复杂性。《SIAM 计算杂志》，30(3)：1023–1040，2000 年。[BV] ODYSSEAS BAKAS 和 MARCO VITTURI。多项式方法讲座 4：技术中的应用。[Cur21] Radu Curticapean。不变量式族的完整复杂度二分。载于《第 53 届 ACM SIGACT 计算理论年度研讨会论文集》，第 1770–1783 页，2021 年。[CX15] Radu Curticapean 和 Mingji Xia。永久式参数化：亏格、顶点、子图、模 2k 求值。载于《2015 年 IEEE 第 56 届计算机科学基础年度研讨会》，第 994–1009 页。IEEE，2015 年。[CX21] Radu Curticapean 和 Mingji Xia。永久式参数化：对于k_8-子图自由图的困难性。arXiv 预印本 arXiv:2108.12879，2021 年。[DF10] CM Da Fonseca。三对角矩阵的 μ-永久式、正交多项式与链序列。《线性代数及其应用》，432(5)：1258–1266，2010 年。[dF18] Carlos M da Fonseca。重新审视 μ -永久式。arXiv 预印本 arXiv:1804.02231，2018 年。[DJ21] Samir Datta 和 Kishlaya Jaiswal。模 2 的幂的并行多项式永久式与最短不相交环。arXiv 预印本 arXiv:2106.00714，2021 年。[dRA13] Nicolas de Rugy-Altherre。行列式与永久式：通过推广获得拯救？费米子行列式与不变量式的代数复杂性。arXiv 预印本 arXiv:1309.2156，2013 年。[DS] EDUARDO MARQUES DE SA。关于 q-永久式展开及环手术定理。

[dS18] Eduardo Marques de Sá. 非交叉划分、非交叉图与 q-永久式方程。《线性代数及其应用》, 541:36–53, 2018.[EG01] Bennett Eisenberg and BK Ghosh. 马尔可夫不等式的一种推广。《统计与概率快报》, 53(1):59–65, 2001.[EM18] Lior Eldar and Saeed Mehraban. 近似计算均值趋于零的随机矩阵的永久式, 2018.[ER98] Pavel Etingof and Vladimir Retakh. 量子行列式与拟行列式。arXiv 预印本 math/9808065, 1998.[FK06] Jürg Fröhlich and Thomas Kerler. 量子群、量子范畴与量子场论。施普林格, 2006.[GM04] Gerald A Goldin and Shahn Majid. 关于非相对论任意子场的福克空间与编织张量积。《数学物理学杂志》, 45(10):3770–3787, 2004.[GRASRA96] César Gómez, Martí Ruiz-Altaba, Germán Sierra, and Marti Ruiz-Altaba. 二维物理中的量子群, 第139卷。剑桥大学出版社 Cambridge, 1996.[Har85] Werner Hartmann. 关于 Immanant 的复杂度。《线性与多重线性代数》, 18(2):127–140, 1985.[HHEG20] Jonas Haferkamp, Dominik Hangleiter, Jens Eisert, and Marek Gluza. 收缩投影纠缠对态在平均情形下是困难的。《物理评论研究》, 2(1):013010, 2020.[HJ12] Roger A Horn and Charles R Johnson. 矩阵分析。剑桥大学出版社, 2012.[Lal98] AK Lal. q-永久式的不等式。II。《线性代数及其应用》, 274(1-3):1–16, 1998.[Lan12] Serge Lang. 圆分域 I 与 II, 第121卷。Springer Science & Business Media, 2012.[Lan13] Serge Lang. 代数数论, 第110卷。Springer Science & Business Media, 2013.[Lip91] Richard Lipton. 测试的新方向。《分布式计算与密码学》, 2:191–202, 1991.[LW12] Claude Levesque and Michel Waldschmidt. 用有理数与单位的乘积近似代数数。《澳大利亚数学学会杂志》, 93(1-2):121–131, 2012.[M+97] Meena Mahajan et al. 行列式：组合学、算法与复杂度。《芝加哥理论计算机科学杂志》, 1997(5), 1997.[Maj00] Shahn Majid. 量子群理论基础。剑桥大学出版社, 2000.

[MM11] Stephan Mertens and Cristopher Moore. 费米子行列式的复杂度及常宽 Immanant。arXiv 预印本 arXiv:1110.1821, 2011.[Neu13] Jürgen Neukirch. 代数数论, 第322卷。Springer Science & Business Media, 2013.[Nez21] Sepehr Nezami. 表示论中的随机矩阵永久式：矩、数值计算、集中性及关于玻色子采样困难性的评论。arXiv 预印本 arXiv:2104.06423, 2021.[PS90] V Pasquier and H Saleur. 量子群视角下有限系统与共形场论的共同结构。《核物理B》, 330(2-3):523–556, 1990.[R+76] Walter Rudin et al. 《数学分析原理》, 第3卷。McGraw-Hill New York, 1976.[RA13] Nicolas de Rugy-Altherre. 行列式与永久式：通过推广找到出路？载于《欧洲可计算性会议》, 页码 87–96。施普林格, 2013.[RS62] J Barkley Rosser and Lowell Schoenfeld. 素数某些函数的近似公式。《伊利诺伊数学杂志》, 6(1):64–94, 1962.[Spi20] Dylan Spivak. Immanant 及其在量子光学中的应用。博士论文, 2020.[TAG93] Hiroyuki TAGAWA. 行列式的 q-类比与对称链分解。《东京数学杂志》, 16(2):311–320, 1993.[TO92] Seinosuke Toda and Mitsunori Ogiwara. 计数复杂性类至少与多项式时间层次一样难。《SIAM 计算杂志》, 21(2):316–328, 1992.[Tod91] Seinosuke Toda. PP 与多项式时间层次一样难。《SIAM 计算杂志》, 20(5):865–877, 1991.[Val79a] Leslie G Valiant. 代数中的完备性类。载于第十一届 ACM 计算理论年度研讨会论文集, 页码 249–261, 1979.[Val79b] Leslie G Valiant. 计算永久式的复杂度。《理论计算机科学》, 8(2):189–201, 1979.[Vau75] RC Vaughan. 分圆多项式系数的界。《密歇根数学杂志》, 21(4):289–295, 1975.[Wei98] Edwin Weiss. 代数数论。Courier Corporation, 1998.[Wei04] Eric W Weisstein. 费马小定理。https://mathworld. wolfram. com/, 2004.[Yan91] Kung-Wei Yang. q-行列式与排列。《斐波那契季刊》, 29:160–163, 1991.

z-永久式的矩与反集中猜想

反集中不仅在玻色子采样中发挥着重要作用[AA11] 而且在随机矩阵理论中也有其自身的研究价值 [EM18, Nez21]。本节讨论由独立同分布复高斯分布抽取得到的z-永久式的矩，以及关于 z-永久式的反集中猜想。

首先，我们明确计算 $|\mathrm{Per}_z(X)|^2$ 的一阶矩。有趣的是，结果不依赖于 z。

引理 A.1. 对于 $z \in \mathbb{T}$， $\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^2] = n!$

证明。通过直接计算，

$$\begin{aligned}\mathop{\mathbb{E}}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^2] &= \sum_{\sigma,\alpha} z^{\ell(\sigma)-\ell(\alpha)} \mathop{\mathbb{E}}_{X\sim\mathcal{G}}\left[\prod_i X_{i,\sigma(i)}X^*_{i,\alpha(i)}\right] \\ &= \sum_{\sigma,\alpha} z^{\ell(\sigma)-\ell(\alpha)} \prod_i \mathbb{I}[\sigma(i)=\alpha(i)] \\ &= \sum_{\sigma,\alpha} z^{\ell(\sigma)-\ell(\alpha)} \cdot \mathbb{I}[\sigma=\alpha] \\ &= \sum_{\sigma} 1 = n!. \end{aligned} \tag{86}$$

□

事实上，如果我们将 $\mathcal{G}$ 替换为一个随机矩阵，其每个元素都独立地从任意零均值、单位方差的分布中抽取，则二阶矩为 $n!$ 。现在我们要计算$\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^4]$。我们先回顾 $\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}(X)|^4]$的计算，见 [AA11]。

引理 A.2. 对于 $z=1$， $\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^4] = (n!)^2(n+1)$。

证明。 通过直接计算，

$$\mathop{\mathbb{E}}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^4] = \sum_{\sigma,\tau,\alpha,\beta} z^{\ell(\sigma)+\ell(\tau)-\ell(\alpha)-\ell(\beta)} \cdot M(\sigma,\tau,\alpha,\beta), \tag{87}$$

其中

$$M(\sigma,\tau,\alpha,\beta) := \prod_i \mathop{\mathbb{E}}_{X\sim\mathcal{G}}[X_{i,\sigma(i)}X_{i,\tau(i)}X^*_{i,\alpha(i)}X^*_{i,\beta(i)}]. \tag{88}$$

如果 $\sigma\cup\tau \neq \alpha\cup\beta$, $M(\sigma,\tau,\alpha,\beta) = 0$。

为计算 $M(\sigma,\tau,\alpha,\beta)$，我们先给出一些直观解释：若 $\tau = 1$ 且 $\sigma = \gamma_1\ldots\gamma_m$，其中每个 γ_i 都是长度大于 1 的循环。那么，要么 α 具有 γ_i 而 β 是恒等置换，要么 α 是恒等置换而 β 具有 γ_i。这意味着 $\beta\alpha = \sigma$ ，并且 2^m 有种 α的选择。对于任意 τ，我们可以通过将 τ^{-1} 右乘来“平移”每个置换，从而化简为上述较简单的情形。由于 $\sigma\tau^{-1}$和 $\tau\sigma^{-1}$具有相同的循环类型，上述论证对于交换 σ 和 τ 的角色是对称的（即，我们可以从 $\sigma = 1$ 开始，并得到相同的结果）。

更正式地说，如果 $\sigma\tau^{-1}$ 的循环类型为 $\lambda = (\lambda_1, \ldots\ldots, \lambda_k)$，且 $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_m > \lambda_{m+1} = \ldots = \lambda_k = 1$，我们可以将其写成如下形式

$$\sigma\tau^{-1} = \gamma_1\gamma_2\ldots\gamma_m. \tag{89}$$

那么，如果 $\sigma \cup \tau = \alpha \cup \beta$，则有

$$(\alpha, \beta) \in A(\sigma, \tau) \tag{90}$$

其中

$$A(\sigma, \tau) = \left\{(\alpha, \beta) : \alpha = \gamma_1^{b_1} \dots \gamma_m^{b_m} \tau, \beta = \tau \alpha^{-1} \sigma, b_1, \dots, b_m \in \{0, 1\}\right\}. \tag{91}$$

显然，对于每个 (σ, τ)，只要 $\sigma\tau^{-1}$ 是 λ 类型，$|A(\sigma, \tau)| = 2^m$，因为 2^m 个 α 可供选择，而一旦固定 α，β 就唯一确定。

此外，对于每个不动点 i，$\sigma(i) = \tau(i) = \alpha(i) = \beta(i)$，因此 $\prod_{i:\ \sigma(i)=\tau(i)} \mathbb{E}_{X\sim\mathcal{G}}[|X_{i,\sigma(i)}|^4] = 2^{k-m}$。因此，我们证明了

$$M(\sigma, \tau, \alpha, \beta) = 2^{F(\sigma\tau^{-1})} \cdot \mathbb{I}[(\alpha, \beta) \in A(\sigma, \tau)] \tag{92}$$

and

$$\sum_{\alpha,\beta} M(\sigma, \tau, \alpha, \beta) = 2^{C(\sigma\tau^{-1})}, \tag{93}$$

其中 $F(\xi)$ 是不动点的数目，而 $C(\xi)$ 是 $\xi \in S_n$ 中循环的数目。对于 $z = 1$，

$$\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}(X)|^4] = \sum_{\sigma,\tau,\alpha,\beta} M(\sigma, \tau, \alpha, \beta) = \sum_{\sigma,\tau} 2^{C(\sigma\tau^{-1})} = (n!)^2(n + 1). \tag{94}$$

这里我们应用了如下事实：$\sum_{\xi\in S_n} 2^{C(\xi)} = (n + 1)!$。

□

然而，我们无法得到 $\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^4]$ 的显式公式，因为当 $\sigma\cup\tau = \alpha\cup\beta$ 时，逆序数可能非零：即 $\ell(\sigma) + \ell(\tau) - \ell(\alpha) - \ell(\beta) \neq 0$。不过，我们仍然可以得到以下结果：

引理 A.3. 对于 $z \in \mathbb{T}$，$\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^4] \le \mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}(X)|^4]$.

证明很简单，因为 $M(\sigma, \tau, \alpha, \beta) \ge 0$ 且 $\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^4]$ 必须是一个正数。因此我们有

$$\begin{aligned}
\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^4] &= \sum_{\sigma,\tau,\alpha,\beta} z^{\ell(\sigma)+\ell(\tau)-\ell(\alpha)-\ell(\beta)} \cdot M(\sigma, \tau, \alpha, \beta) \\
&\le \sum_{\sigma,\tau,\alpha,\beta} M(\sigma, \tau, \alpha, \beta) \\
&= \mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}(X)|^4].
\end{aligned} \tag{95}$$

更一般地，我们有以下不等式。

引理 A.4. 对于 $z \in \mathbb{T}$ 且 $k \ge 2$，$\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^{2k}] \le \mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}(X)|^{2k}]$.

由于缺乏高效计算永久式的公式，证明永久式的反集中猜想很困难。正如我们在论文中所展示的，不存在适用于一般z-永久式的高效公式。因此，我们认为，证明 z-永久式的反集中猜想同样是一个难题。然而，z-永久式的高阶矩小于永久式的高阶矩（但一阶矩相同）。这提示我们，z-永久式的反集中性猜想也成立。我们有如下与 $z = 1$类似的结果。

定理 A.5 （ z-永久式的弱反集中性）。 对于 $\alpha < 1$,

$$\Pr_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^2 > \alpha \cdot n!] > \frac{(1-\alpha)^2}{n+1}. \tag{96}$$

证明。 根据切比雪夫不等式，利用 $\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^2] = n!$ 和 $\mathbb{E}_{X\sim\mathcal{G}}[|\mathrm{Per}_z(X)|^4] \le n!^2(n+1)$，即可立即得到该界。 □

B 强自相关性质

考虑一个随机变量 X，其具有均值为 0、方差为 1 的实分布 $\mathcal{F}$。我们将其记为 $X \sim \mathcal{F}_{\mathbb{R}}(0,1)$。通过平移和缩放随机变量 $X \to \mu + \sigma^2 X.$，我们定义均值为 μ、方差为 σ^2 的 $\mathcal{F}_{\mathbb{R}}(\mu,\sigma^2)$。我们将这种分布记为 $\mathcal{F}_{\mathbb{R}}(\mu,\sigma^2)$。我们选取 ϵ，使得 $\epsilon < \frac{1}{2}$.

$$X = \mathcal{F}_{\mathbb{R}}(0,1)^n \tag{97}$$

$$\mathcal{D}_1 = \mathcal{F}_{\mathbb{R}}\Big(0,(1-\varepsilon)^2\Big)^n, \tag{98}$$

$$\mathcal{D}_2 = \prod_{i=1}^{n} \mathcal{F}_{\mathbb{R}}(v_i,1) \tag{99}$$

我们定义

$$G(\epsilon) = \big\|\mathcal{F}_{\mathbb{R}}(0,1) - \mathcal{F}_{\mathbb{R}}(0,(1-\epsilon)^2)\big\|, H(v_i) = \|\mathcal{F}_{\mathbb{R}}(0,1) - \mathcal{F}_{\mathbb{R}}(v_i,1)\|. \tag{100}$$

引理 B.1. 如果 $G(\epsilon)$ $^{dG}\!/_{(\epsilon)\,d\epsilon}$ 在 $\epsilon \in [0,\frac{1}{2}]$ 时均连续，并且 $H(x)$ $^{dH}\!/_{(x)\,dx}$ 在 $x \in [0,1]$ 时均连续。那么，

$$\|\mathcal{D}_1 - X\| \le nM_1\epsilon, \forall\epsilon \in [0,1/2]$$
$$\|\mathcal{D}_2 - X\| \le M_2\|v\|_1,$$

其中，对于每个 i， M_1, M_2 均与 ϵ, v_i 相互独立。

证明。 我们先证明第一个不等式:

$$\|\mathcal{D}_1 - X\| \le n\big\|\mathcal{F}_{\mathbb{R}}(0,1) - \mathcal{F}_{\mathbb{R}}(0,(1-\epsilon)^2)\big\| = n|G(\epsilon)| \le n\epsilon M_1.$$

为了界定差值，我们对变量 ϵ 使用中值定理。注意， $G(0) = 0$。对于所有 $\epsilon \in [0,\frac{1}{2}]$，我们有:

$$|G(\epsilon) - G(0)| \le \epsilon \max_{\epsilon\in[0,\frac{1}{2}]}\left|\frac{dG(\epsilon)}{d\epsilon}\right| \le \epsilon M_1. \tag{101}$$

这里， M_1 定义为 $\left|^{dG}\!/_{d\epsilon}(\epsilon)\right|$。由于 $\left|\frac{dG(\epsilon)}{d\epsilon}\right|$ 的连续性以及以下引理，该对象必然存在。

引理 B.2 (极值定理[R+76])。 从非空紧空间到实数子集的连续函数能够取到最大值和最小值。

至此，第一条不等式的证明完成。
第二个不等式再次利用三角不等式得出:

$$\|\mathcal{D}_2 - X\| \le \sum_{i=1}^{n}\|\mathcal{F}_{\mathbb{R}}(0,1) - \mathcal{F}_{\mathbb{R}}(v_i,1)\| \le \sum_{i=1}^{n}|v_i|M_2 \le M_2\|v\|_1$$

这里我们使用相同的技巧（注意 $H(0) = 0$，不失一般性，我们可以假设 $v_i \geq 0$.）

$$|H(v_i) - H(0)| \leq |v_i| \max_{x\in[0,1]} \left|\frac{dH(x)}{dx}\right| \leq |v_i| M_2. \tag{102}$$

此处 M_2 定义为 $\left|\frac{dH(x)}{dx}\right|$。 □

我们可以定义复随机变量 $Z = X + iY, X \sim \mathcal{F}_{\mathbb{R}}(\mu_1, 1/2)$ $Y \sim \mathcal{F}_{\mathbb{R}}(\mu_2, 1/2)$，且 X, Y 相互独立。因此，$Z \sim \mathcal{F}_{\mathbb{C}}(\mu_1 + i\mu_2, 1)$。将每个复坐标视为两个实坐标会很有帮助，而 v 是 $\mathbb{R}^{2N}$ 中的一个向量。

推论 B.3。 如果我们考虑由实数组成且具有相同条件的复数版本：

$$X = \mathcal{F}_{\mathbb{C}}(0,1)^n = \mathcal{F}_{\mathbb{R}}(0, 1/2)^{2n} \tag{103}$$

$$\mathcal{D}_1 = \mathcal{F}_{\mathbb{C}}\left(0, (1-\varepsilon)^2\right)^n = \mathcal{F}_{\mathbb{R}}(0, (1-\epsilon)^2/2)^{2n}, \tag{104}$$

$$\mathcal{D}_2 = \prod_{i=1}^{n} \mathcal{F}_{\mathbb{C}}(v_i, 1) \tag{105}$$

我们有：

$$\|\mathcal{D}_1 - X\| \leq 2nM_1\epsilon, \forall \epsilon \in [0, \frac{1}{2}]$$
$$\|\mathcal{D}_2 - X\| \leq M_2\|v\|_1 \leq \sqrt{2n} M_2 \|v\|_2.$$

在最后一行中，我们使用 1-范数和 2-范数不等式。注意，对于 1-范数，我们将 ν 视为一个 $\mathbb{R}^{2n}$ 向量；但对于 2-范数，我们将它们打包到 $\mathbb{C}^n$ 中。

注意，在 [AA11], 这里可以利用旋转不变性，为高斯矩阵得到更紧的界。但这对我们的目的来说已经足够。