arXiv:2603.27128v1 [cs.CC] 28 Mar 2026

随机张　　正交与酉作用下的张量同构

Jeremy Chizewer* Samuel Everett† Deven Mithal‡ Youming Qiao§

2026年3月31日

摘要

我们研究如下问题：判断 $\mathbb{R}^\ell \otimes \mathbb{R}^m \otimes \mathbb{R}^n$ 中的两个张量在正交群的自然作用下是否同构：$\mathbf{O}(\ell,\mathbb{R}) \times \mathbf{O}(m,\mathbb{R}) \times \mathbf{O}(n,\mathbb{R})$；并研究相应的复数域 $\mathbb{C}$ 上的酉群问题。这些问题自然出现在多个领域，包括图同构与张量同构（Grochow–Qiao，*SIAM J. Comp.*'21）、轨道闭包交集的缩放算法（Allen-Zhu–Garg–Li–Oliveira–Wigderson，计算机科学理论研讨会'18）以及量子信息（Liu–Li–Li–Qiao，*Phys. Rev. Lett.*'12）。

我们研究正交与酉张量同构的平均情形算法，其中一个随机张量的每个元素均独立地从次高斯分布中均匀抽样，另一个张量则任意。对于算法设计，我们将高阶奇异值方法中的算法思想发展为多项式时间的精确（代数）算法和近似（数值）算法，并对其进行严格的平均情况分析。沿用（Allen-Zhu–Garg–Li–Oliveira–Wigderson，计算机科学理论研讨会'18）的思路，我们提出了一种用于带间隙版本的轨道距离近似问题的算法。在平均情况分析方面，我们基于随机矩阵理论近期关于次高斯Wishart矩阵特征值排斥的进展（Christoffersen–Luh–O'Rourke–Shearer 和 Han，*arXiv*'25），将他们的结果从Wishart矩阵边长呈线性关系的情形扩展到呈多项式关系的情形。

我们的算法与概率结果在若干研究方向上有着自然的推论和解读。首先，正交群和酉群作用下的张量轨道闭包交问题在平均情形下是容易的，这与其最坏情形难度的相关证据形成对照（B¨urgisser–Do˘gan–Makam–Walter–Wigderson，计算复杂性会议'21）；一般线性群作用下张量同构的平均情形难度也有类似证据（Grochow–Qiao，《*SIAM*计算杂志》'21）。其次，可以在多项式时间内检验一个 Haar随机三方量子态是否与任意给定的三方量子态局部酉等价。第三，我们为随机三方 3-均匀超图同构问题得到了一个谱算法。

*芝加哥大学。jchizew@uchicago.edu
†芝加哥大学。same@uchicago.edu
‡芝加哥大学。mithal@uchicago.edu§新南威尔士大学。
jimmyqiao86@gmail.com

目录

1 引言 **1**

1.1 正交与酉张量同构的动机.11.2 同构问题的平均情形复杂度.21.3 我们的结果.31.4 技术概述.71.4.1 算法技术.71.4.2 概率技术.81.5 开放问题.101.6 对先前工作的更广泛视角.10

2 张量同构算法 12

2.1 精确酉张量同构.132.2 近似酉张量同构.172.3 酉轨道近似.22

3 高瘦 Wishart 矩阵的特征值排斥 **27**

3.1 与 [CLOS25]在技术方面的比较.273.2 测度集中的预备知识.283.3 奇异向量并不稀疏.293.4 左奇异向量不具有强加性结构.353.5 高瘦 Wishart 矩阵具有定量特征值排斥 413.6 复数情形.43

关于代数数的有效且高效操作的背景介绍 45

B 推论证明概要1.2 45

1 引言

给定两个数学对象，判定它们是否等价的计算成本是多少？这类基本问题称为同构问题，在从量子信息到图论等众多领域中都至关重要。尽管人们为研究这些问题投入了大量精力，但许多基本问题仍未得到解决。

物理学中一个自然的问题（始于 [Kra10、LLLQ12]）是确定两个张量在正交（在 $\mathbb{R}$上）或酉（在 $\mathbb{C}$上）群作用下是否同构。针对这一问题，已有一些基于经典高阶奇异值理论方法的知名算法。然而，目前尚未对该方法进行复杂性分析，尤其是其平均情形效率仍不清楚。这种情况可以与 Spielman 和 Teng 的工作 [ST04]之前人们对单纯形算法的认识相比较。本文旨在将现有的算法思想发展为平均情形高效的算法。

更正式地说，酉张量同构问题 (U-TI)要判断两个张量A，$B \in \mathbb{C}^{\ell} \otimes \mathbb{C}^{m} \otimes \mathbb{C}^{n}$ 在酉群的直积 $\mathbf{U}(\ell, \mathbb{C}) \times \mathbf{U}(m, \mathbb{C}) \times \mathbf{U}(n, \mathbb{C})$的自然作用下是否等价。将 $\mathbb{C}$ 替换为 $\mathbb{R}$，并将 $\mathbf{U}$ 替换为 $\mathbf{O}$，即可得到正交张量同构 问题（O-TI）。将$\mathbf{U}$ 替换为$\mathbf{GL}$，即可得到一般线性张量同构 问题（GL-TI）。本文中的正交群均定义在 $\mathbb{R}$ 上，酉群均定义在 $\mathbb{C}$上。为便于阐述，我们主要讨论三阶张量。

1.1 正交张量同构与酉张量同构的动机

量子态的局部酉等价。 酉张量同构自然地出现在量子信息中。三方纯量子态是 $\mathbb{C}^{\ell} \otimes \mathbb{C}^{m} \otimes \mathbb{C}^{n}$ 中的单位张量。当且仅当两个量子态在酉群作用下同构时，它们才是局部酉（LU）等价的。量子态的局部酉等价是量子态的一种基本等价关系 [WGE16], ，并刻画了两个量子态在局部操作与经典通信（LOCC）下的等价性 [DVC00]。判断两个量子态是否局部酉等价的问题已有研究 [Kra10、LLLQ12]。

数据分析中的笛卡尔张量。 奇异值定理指出，$\mathbf{O}(n, \mathbb{R}) \times \mathbf{O}(m, \mathbb{R})$ 在 $\mathbb{R}^{n} \otimes \mathbb{R}^{m}$ 上的轨道由奇异值刻画。在数据分析研究中，一个核心问题是探索奇异值定理向多维数据统计分析的推广 [DSL08], ，因此正交张量同构受到关注 [DLDMV00、DSL08、HU17、Sei18]。带有正交等价的 $\mathbb{R}$上的张量有时被称为笛卡尔张量 [Tem04]。

轨道闭包相交问题。正交群和酉群是紧群，因此，正交群作用和酉群作用于张量所产生的轨道是闭的（在 Zariski 拓扑或欧几里得拓扑下）。因此，酉张量同构和正交张量同构也属于轨道闭包相交问题这一类。给定一个作用于拓扑空间 S 的群 G，相应的轨道闭包相交问题是询问 $s, s' \in S$ 的轨道闭包是否相交。

其渊源可追溯至希尔伯特和 Mumford 关于不变量理论的著名研究 [Hil93，MFK94], 对轨道闭包交问题开展复杂性理论研究，受到了广泛关注，其动机源于代数复杂性 [HW15，Mul12], 尽管其重要性

后来，人们认识到这类问题在组合学等多个领域都具有重要意义 [GGdOW20，IQS18], 张量网络 [AMN+23]、矩阵乘法 [BI13],统计学 [DM21], 和计数问题 [CY26]。

这一研究方向的一项重要成果，是解决矩阵元组在左右作用下的轨道闭包交问题 [GGdOW20、IQS18、HH21、AGL+18、IQ23]。此后，下一个自然的目标便是研究张量在特殊线性群作用下的轨道闭包问题[BFG+18、AGL+18]。文献 [GGdOW20、AGL+18]中的算法技术称为算子缩放，它推动了非交换优化理论的发展 [BFG+19]。简而言之，基于 Kempf–Ness 理论，算子缩放将一般或特殊线性群作用下的轨道闭包问题归约为酉群或正交群作用下的相应问题。因此，酉与正交矩阵元组或张量同构问题便自然产生。事实上，文献 [AGL+18] 中，矩阵元组在左右作用下的轨道闭包交算法的一个关键技术组成部分，就是酉矩阵元组等价算法。

图与张量同构问题。酉张量同构和正交张量同构与著名的图同构问题，以及一般线性张量同构问题（GL-TI）密切相关。 GL-TI一般线性张量同构问题因其与群、多项式和代数同构的联系而受到广泛关注 [GQ23，GQ24，CGQ+24，GQ25，GQSS25，JQSY19]。

简而言之，酉张量同构和正交张量同构处于图同构与 GL 张量同构之间，呈“夹心”关系。根据 [CGQ+24]，图同构可在多项式时间内归约到酉张量同构和正交张量同构，而正交张量同构可在多项式时间内归约到 GL 张量同构。Lysikov 和 Walter 回答了 [CGQ+24]中的一个开放问题，证明酉张量同构可在多项式时间内归约到 GL 张量同构 [LW25]。

关于图同构已有大量研究，近期的突破包括 Babai 提出的准多项式时间算法 [Bab16] 以及 Anastos、Kwan 和 Moore 对图同构的平滑分析 [AKM25]。Sun 在 p-群同构 [Sun23,IMQ+24]方面取得突破，推动了 GL 张量同构算法的显著进展。相比之下，酉张量同构和正交张量同构虽然与之密切相关，且本身也很有研究价值，但从算法角度来看仍未得到充分探索。

1.2 同构问题的平均情形复杂度

尤其是在应用场景中，理解同构问题的平均情形复杂度 至关重要。回顾一下，对于一个同构问题，输入由两个对象组成，我们要判断它们是否同构。平均情形设定是从某个随机模型中抽取一个对象，而另一个对象则不作限制。特别是，第二个对象可以根据随机抽样的结果来选择。目标是设计一种同构判定算法，使其在第一个对象的抽样过程中以高概率正确运行。

图同构的平均情形算法。 图同构是展示最坏情形复杂度与平均情形复杂度差异的经典例子。尽管图同构问题（GI）备受关注，但在 Babai 取得突破、提出 GI 的准多项式时间算法之前，完整 GI 的最坏情形复杂度仍为指数级 [BL83]。然而，长期以来，人们一直认为 GI 在实践中很容易求解 [Bab16]，软件 Nauty 和 Traces 便是明证 [MCK81],。 [MP14]。

最坏情形算法与实用算法之间的这种反差，理论上可以通过考察平均情形复杂度来调和。Babai、Erd˝os 和 Selkow 首次提出了一个用于图同构的平均情形线性

时间算法 [BES80]，适用于 Erd˝os–R´enyi 模型 $\mathcal{G}(n, p = 1/2)$。此后，Karp、Lipton 和 Bollob´as 等人开展了一系列研究 [Kar75, Lip78, BK79, Bol82, CP08, LM17],；最近，Anastos、Kwan 和 Moore [AKM25]，对图同构进行了平滑分析，并涵盖了 Erd˝os–R´enyi 模型 $\mathcal{G}(n, p)$ 中抽样得到的图的典范标记，适用于所有 p。

有限域上一般线性张量同构的平均情形算法。 有限域上的一般线性张量同构（GL-TI）被提出作为后量子密码学中的候选问题，见 [JQSY19]。基于 GL-TI 或其变体的数字签名已被设计并实现，见 [TDJ+22，CNP+23]。

平均情形算法对于理解这些密码方案的安全性发挥着重要作用。Li 和 Qiao 设计了第一个针对有限域上 GL-TI 的平均情形算法 [LQ17]，，并在 [BLQW20]中加以改进。对于 $n \times n \times n$ 上的张量，$\mathbb{F}_q$该平均情形算法的运行时间为 $q^{O(n)}$。相比之下，最好的最坏情形算法运行时间为 $q^{\tilde{O}(n^{1.5})}$[IMQ+24]，这是对 Sun 在 p-群同构方面的突破性成果的改进，见 [Sun23]。

随机图同构的谱算法。 Leighton 和 Miller [LM79][1]以及 Babai、Grigoryev 和 Mount [BGM82、Bab86]提出了用于检验具有无重数或有界特征值的图是否同构的算法。这些算法促使 Babai 在 20 世纪 80 年代提出这样一个问题：随机图的邻接矩阵是否以高概率具有单谱（参见 [TV17]）。三十年后，Tao 和 Vu 在逆 Littlewood–Offord 定理及随机矩阵理论普适性方面取得多项突破，并由此解决了这个问题，见 [TV17]，。因此，[TV09b、TV11]中的算法[LM79、BGM82、Bab86] 可以解释为用于随机图同构的高效算法。

1.3 我们的结果

我们的主要结果是针对正交和酉张量同构问题的平均情形高效算法。在深入细节之前，我们通过表格说明这些算法在密切相关的同构问题中的位置。1。

	轨道最坏情况	**轨道平均情况**	**轨道闭包交集**
图同构（GI）	准多项式时间 [Bab16]	多项式时间 [BES80，BK79，AKM25]	与轨道相同（在点集拓扑中）
酉 ($\mathbb{C}$) 和正交 ($\mathbb{R}$) 张量同构	图同构-困难 [CGQ+24]；PSPACE	**多项式时间** [本文]	与轨道相同（在扎里斯基或欧几里得拓扑中）
一般线性 $\mathbb{C}$上的张量同构	图同构-困难 [GQ23]；交互式证明系统 [Koi96] 或计数层级 [AGS26]	开放问题；与轨道闭包交	图同构-困难 [LW25]
一般线性张量同构 $\mathbb{F}_q$	GI-困难 [GQ23]；NP ∩ coAM；$q^{\tilde{O}(n^{1.5})}$时间算法 [Sun23，IMQ+24]	$q^{O(n)}$时间算法 [LQ17，BLQW20]	开放问题（在扎里斯基拓扑中）

表1：从不同角度对若干同构问题进行比较（参见第1.6节）。

[1]对 [LM79]的精彩阐述由 Spielman [Spi18]记录。

我们的张量随机模型。一种自然的张量随机模型 $\mathbb{C}^\ell \otimes \mathbb{C}^m \otimes \mathbb{C}^n$ 是对每个 ℓmn 元素进行采样，使其独立地服从一个固定的——均值为零、方差为单位值的——高斯分布。这与随机矩阵理论中的经典 Ginibre 系综类似。此外，这还有明确的量子信息论解释：归一化后，它对应于一个 Haar 随机纯态 [梅兹07]。

受随机矩阵理论中更广泛的应用和普适性结果的启发（参见第 1.6 节），我们实际上采用了 $\mathbb{R}^\ell \otimes \mathbb{R}^m \otimes \mathbb{R}^n$ 中的随机张量随机模型，其中每个元素均独立地从一个固定的——均值为零、单位方差的——次高斯分布中抽取ξ。在 $\mathbb{C}^\ell \otimes \mathbb{C}^m \otimes \mathbb{C}^n$ 的情况下，每个元素均独立地从一个定义在高斯有理数 ξ 上的固定的——均值为零、单位方差的——次高斯分布中抽取 $\mathbb{Q}(i) = \{s+it\colon\ \ s, t \in \mathbb{Q}\}$。回顾一下，实值随机变量 ξ 若满足高斯型尾界$\mathbb{P}[|\xi| > t] \le 2\exp(-t^2/K^2)$，其中某个 $K < \infty$ 成立，则称其为次高斯变量。

次高斯分布涵盖许多重要的分布。除了高斯分布外，它还包括*Rademacher* 分布，即在 ± 1 上等概率取值的分布。在这种情况下，$\mathbb{R}^\ell \otimes \mathbb{R}^m \otimes \mathbb{R}^n$ 中的随机张量可以看作是在记录一个随机的 3-均匀三部超图 $H = (L \cup M \cup N,\ E)$，其中 $|L| = \ell$、$|M| = m$、$|N| = n$、$E \subseteq L \times M \times N$，且每条超边 $(i,\ j,\ k)$ 以 H 中的概率 $1/2$ 出现。

我们的主要结果。为便于陈述我们的结果，我们将重点研究 $\mathbb{C}^{n\times n\times n} = \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$ 上的张量（在 $\mathbb{R}$ 上的情形类似）。形式上，我们首先研究以下问题。

问题 1。给定张量 $A, B \in \mathbb{C}^{n\times n\times n}$，是否存在 $n \times n$ 酉矩阵 L, R, T，使得$(L, R, T) \curvearrowright A = B$?

我们针对问题 1 的首个结果，是一种在随机模型下的平均情况、多项式时间算法，可求解精确的酉和正交张量同构问题：

定理 1.1 (酉张量同构问题的全局平均情况分析**)**。存在一种确定性算法，给定 $A = (a_{i,j,k}) \in \mathbb{Q}(i)^{n\times n\times n}$，其中元素 $a_{i,j,k} \sim \xi$独立同分布，服从固定的均值为零、单位方差的次高斯分布 ξ，且 $B \in \mathbb{Q}(i)^{n\times n\times n}$ 任意且确定，该算法对输入 A 和 B在多项式时间内运行，并且对于 A 的选取，以高概率判定

$$B \in \mathrm{Orb}_{\mathbb{C}}(A) \coloneqq \{(L, R, T) \curvearrowright A\colon\ L, R, T \in \boldsymbol{U}(n)\},$$

其中隐含常数仅取决于 ξ的分布。

另一方面，自然也会考虑这类问题的数值版本或近似类比问题。也就是说，我们还关注如何判定相关的轨道距离近似问题（也称为鲁棒轨道问题），如 [BDM+24] 中所讨论的。例如，设

$$\mathrm{dist}(X, Y) \coloneqq \inf_{x\in X, y\in Y} \|x - y\|_F$$

用弗罗贝尼乌斯范数 $\|\cdot\|_F$ 表示通常的集合距离。令

$$\mathrm{dist}_{\mathbb{C}}(A, B) \coloneqq \mathrm{dist}(\mathrm{Orb}_{\mathbb{C}}(A), \mathrm{Orb}_{\mathbb{C}}(B)) = \inf_{L,R,T\in \mathbf{U}(n)} \|(L, R, T) \curvearrowright A - B\|_F,$$

这里等号成立，是因为酉作用可逆，且弗罗贝尼乌斯范数在此类作用下保持不变。

我们还研究以下问题，沿用 [AGL+18, TheoremM3] 的方法。该文处理了一个相关问题（详见注 1.1 中的详细说明）。

问题 2. （带间隔的）酉张量轨道近似问题定义如下：给定$0 < \varepsilon < \eta$ 以及张量 A、$B \in \mathbb{C}^{n\times n\times n}$，区分以下两种情形：

$$\mathrm{dist}_{\mathbb{C}}(A, B) \le \varepsilon \quad and \quad \mathrm{dist}_{\mathbb{C}}(A, B) \ge \eta.$$

当然，对于有限精度问题，我们无法实际抽取 A的元素，甚至也未必能在将 B 视为 $\mathbb{C}^{n\times n\times n}$ 中的真实元素时读入它们。因此，我们考虑~ ~模型：算法获得 A，B，并将它们分别视为 A 和 B 的截断版本，根据给定的 ε，截断到我们选择的精度。

以下定 理给出了一个平均情形多项式时间算法，用于求解问题 2 .

定理 1.2 （酉轨道近似问题的全局平均情形分析）。 存在一种确定性算法，对于给定的 $\varepsilon > 0$，满足 $\varepsilon \le O(n^{-3})$、$A = (a_{i,j,k}) \in \mathbb{C}^{n\times n\times n}$，其元素为来自某个固定的均值为零、单位方差次高斯分布 ξ 的独立同分布元素，且$B \in \mathbb{C}^{n\times n\times n}$ 任意；所有对象的精度均指定为 $O(\log(n/\varepsilon))$ 位。该算法的运行时间关于n和$\log(1/\varepsilon)$ 为多项式时间，并且以高概率（相对于 A的选取）区分

$$\mathrm{dist}_{\mathbb{C}}(A, B) < \varepsilon \ from \ \mathrm{dist}_{\mathbb{C}}(A, B) > \gamma\varepsilon \ for \ \gamma = O(n^8).$$

在前一种情况下，算法还会输出一个见证（$\widetilde{L}$、$\widetilde{R}$、$\widetilde{T}$）$\in \boldsymbol{U}(n)^3$，使得

$$\|(\widetilde{L}, \widetilde{R}, \widetilde{T}) \curvearrowright A - B\|_F < \gamma\varepsilon.$$

Rema备注 1.1。将定理1.2 与 [AGL+18定理作比较很有启发性。 M3].

在 [AGL+18]中，受矩阵元组上左右作用的轨道闭包交问题启发，算子缩放技术将该问题归约为作用$\mathrm{U}(n,\mathbb{C}) \times \mathrm{U}(n,\mathbb{C})$在 $\mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^m$上的轨道问题。注意，在张量积中，$\mathbb{C}^m$ 分量~不受作用。对于 $A, B \in \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^m$，我们用$\mathrm{dist}_{\mathbb{C}}(A, B)$表示 A 和 B 在此作用下的轨道之间的距离。 [AGL+18中的定理 M3] 给出了一个多项式时间算法，用以区分

$$\widetilde{\mathrm{dist}}_{\mathbb{C}}(A, B) < \varepsilon \text{ from } \widetilde{\mathrm{dist}}_{\mathbb{C}}(A, B) > \gamma\varepsilon^{1/\mathrm{poly}(n,m)} \text{ for } \gamma = M^{\mathrm{poly}(n,m)},$$

其中 M 表示 A和 B中各元素的最大模。

与 [AGL+18的定理 M 相比，3], 我们注意到，定理1.2 的近似比更优。另一方面，需要注意的是，这些作用不同，而且我们的结果是一种平均情形算法，而 [AGL+18的定理 M3]处理的是最坏情形。

定理1.1 和1.2 的平均情形分析，关键在于深入理解随机矩阵的谱。具体而言，我们依赖于以下排斥结果，该结果在第3节中证明。

定理 1.3 (具有多项式间隙的特征值排斥)。 固定一个均值为零、方差为一的次高斯分布 ξ。令 M 为一个元素独立同分布且服从 $m_{ij} \sim \xi$ 的 $n \times p$ 矩阵，并满足 $p = \Theta(n^{\zeta})$

对于 $\zeta \in (0,1)$。然后，定义

$$\lambda_{\min}(M^\top M) \coloneqq \inf_{1\le i<p} (\lambda_i(M^\top M) - \lambda_{i+1}(M^\top M))$$

并且，对于 $\beta > \zeta$，我们有

$$\lambda_{\min}(M^\top M) \ge \Omega((n^{(1-\zeta)/2} - 1)n^{-\beta})$$

概率至少为 $1 - O(n^{\zeta-\beta})$。此外，设 M具有复数条目 $m_{ij} = a_{ij} + ib_{ij}$，其中 a_{ij}、b_{ij}为独立同分布实变量 $\sim \xi$，则 $M^\top M$的特征值也满足相同的界。

通过代换，很容易将这一结果从 $n \times n^{1/k}$ 范围转化为满足 $k \in \mathbb{R}_+$ 的 $n^k \times n$，从而得到间隙

$$\lambda_{\min}(M^\top M) \ge \Omega((n^{(k-1)/2} - 1)n^{-k\beta}) \tag{1.1}$$

概率 至少为 $1 - O(n^{1-k\beta})$，其中 $\beta > 1/k$，且 k 表示张量的阶数 s.

注 1.2（概率与精度的权衡）。 在定理 1.3 中，目标间隙同时出现在排斥事件和概率上界中。这是基于逆 Littlewood–Offord 的排斥结果的常见特点（参见 [NTV17、CLOS25、Han25]），并且在我们的设定中，这使成功概率与数值算法所需精度之间能够实现清晰的权衡。

定理 1.1 至 1.3的分析结果，以及 Weyl 不等式的谱稳定性推论表明，我们可以得出以下平滑分析/局部平均情形复杂度结论。其证明显然，因此略去。

定理 1.4（酉张量同构问题的局部分析）。 存在一种确定性算法：给定具有独立同分布元素 $E = (e_{ijk}) \in \mathbb{Q}(i)^{n\times n\times n}$ 的固定的——均值为零、单位方差——次高斯分布 ξ，常数 $\beta \in (1/3, 1/2)$，扰动幅度 $\eta \ge 2\cdot\|A\|(\|A\| + \sqrt{n} + K\sqrt{p})\cdot n^{3\beta}/(n+1)$，以及任意且确定的 $A, B \in \mathbb{Q}(i)^{n\times n\times n}$，在输入 $A + \eta E$ 和 B 上以多项式时间运行，并以高概率判定是否

$$B \in \mathrm{Orb}(A) \coloneqq \{(L,R,T) \curvearrowright A : \ L,R,T \in \boldsymbol{U}(n)\},$$

其中隐含常数仅取决于 ξ的分布。

定理 *1.5*（酉轨道逼近问题的局部分析）。存在一种确定性算法，给定满足 $\varepsilon = O(n^{-3})$的 $\varepsilon > 0$、满足$e_{ijk}(\in \mathbb{R}^{n\times n\times n})$且具有 $e_{ijk} \sim \xi$ 的 $E =$，其中元素独立同分布，服从固定的均值为零、单位方差次高斯分布 ξ；一个常数 $\beta \in (1/3, 1/2)$；一个扰动幅度 $\eta \ge 2\cdot\|A\|(\|A\| + \sqrt{n} + K\sqrt{p})\cdot n^{3\beta}/(n+1)$；以及任意的确定性$A$、$B \in \mathbb{C}^{n\times n\times n}$，且每项均以 $O(\log(n/\varepsilon))$位精度给定。该算法的运行时间关于 n和$\log(1/\varepsilon)$为多项式时间，并以高概率区分 $\mathrm{dist}_{\mathbb{C}}(A+\eta E, B) < \varepsilon$与 $\mathrm{dist}_{\mathbb{C}}(A+\eta E, B) > \gamma\varepsilon$，其中 $\gamma = O(n^8)$；在前一种情形下，算法会输出一个见证$(\widetilde{L}, \widetilde{R}, \widetilde{T}) \in U(n)^3$，使得

$$\|(\widetilde{L}, \widetilde{R}, \widetilde{T}) \curvearrowright (A + \eta E) - B\|_F < \gamma\varepsilon.$$

扰动大小 η 的选取使得我们可以通过谱稳定性推导出，在来自 A的加性扰动下，$(A+\eta E)^T(A+\eta E)$的谱的简单性得以保留。这些简单的定理旨在为更复杂的光滑分析提供基准（见第1.5节）。

事实上，请注意，对于 k 足够大的值（其中 k 仍表示张量的阶数），并且目标成功概率足够小时，根据定理1.3 ，谱隙可能增大，此时定理 η 1.4 和1.5 中的扰动大小可以相应减小。另一方面，当 k 较小时，扰动 η 则相当大。这表明，随着 k变化，-TI 的平滑分析设置存在定性差异，也表明了我们平滑分析的一项局限。

我们结果的应用。我们的主要结果有以下几种解释。

首先，我们在定理 1.1 中采用高斯分布作为次高斯分布，并将 $\mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$ 中的单位张量视为纯量子态。假设给定一个以 $n \times n \times n$ 张量表示的量子态。那么：

推论 1.1。存在一个多项式时间算法，可以判定 *Haar* 随机量子态与 $\mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$ 中的任意量子态是否局部酉等价。

其次，我们采用 Rademacher 分布作为次高斯分布，并将 ± 1 中的张量 $\mathbb{R}^n \otimes \mathbb{R}^n \otimes \mathbb{R}^n$ 视为 3- 均匀三部超图的邻接张量。结合定理 1.3 与 Leighton 和 Miller 的图同构谱算法 [LM79] (参见 [Spi18]) ，得到以下结果，其证明概要见附录B。

推论 1.2。 存在一个多项式时间算法，可以判定一个随机 *3*-均匀三部超图与一个任意的 *3*-均匀三部超图是否同构。

注意，推论 1.2 可视为超图类比，对应于第1.2节末尾讨论的随机图同构谱算法。无法从这些算法推导出该结论，因为将超图同构归约为图同构的 [KST93]并不能保持平均情形分析所依据的分布。

1.4 技术概述

在此，我们介绍 用于证明本文主要结果的核心工具和技术 .

1.4.1 算法技术

一个同构不变量。设 $A = (a_{i,j,k}) \in \mathbb{C}^{n\times n\times n}$。在 $\mathrm{U}(n)^3$ 的作用下，A 的一个经典同构不变量如下。首先，沿第三个指标切片，得到一个矩阵组 $(A_1, \ldots, A_n)$，其中 $A_k(i,j) = a_{i,j,k}$；将其视为一个 $n \times n^2$ 矩阵 $\hat{}A$。构造格拉姆矩阵 $G_3(A) = AA^*$ ，其中 A^* 是 A 的共轭转置，下标中的 3 表示该格拉姆矩阵由沿第三个方向切片得到。显然， $G_3(A)$ 在 $\mathrm{U}(n)^3$ 的前两个分量的作用下保持不变（即在 $(L,R,T) \curvearrowright A$ 中）。第三个分量 $T \in \mathrm{U}(n)$ 将 $G_3(A)$ 映射为 $TG_3(A)T^*$。因此， $G_3(A)$ 的谱是 $\mathrm{U}(n)^3$ 在 $A = (a_{i,j,k}) \in \mathbb{C}^{n\times n\times n}$ 上作用的一个同构不变量。

如果 $G_3(A)$ 的谱是简单的，也就是说每个特征值的重数都是 1，那么在从 A 到一个同构的 B 的同构中，这些一维特征空间需要相应地匹配。请注意， $G_3(A)$ 的特征值对应于矩阵 A 的奇异值。假设 $G_1(A)$ 和 $G_2(A)$（沿另外两个方向切片得到的格拉姆矩阵）也满足这一条件。那么不难看出，以类似方式可以检验 A 与另一个 $B \in \mathbb{C}^{n\times n\times n}$ 是否同构；格拉姆矩阵 $G_i(A)$ 和 $G_i(B)$ 的谱对齐是 A 与 B 酉同构的必要条件，尽管并非充分条件。

精确酉张量同构。 现在我们概述用于证明定理 1.1 的算法。首先，计算以下对象的特征值及其特征子空间： $G_d(A)$、 $d = 1$、2、3（如上所定义）。要使 A 和 B 同构， $G_d(B)$ 对每个 $G_d(A)$ 都必须具有相同的特征值及其重数，其中 $d = 1$、2、3。然后，问题便归结为判断 A 和 B 是否在可逆对角矩阵作用下同构。最后，我们求解相应的张量对角同构问题。

要实现上述算法概要，需要谨慎处理。例如，尽管计算特征值和特征子空间是计算线性代数中的基本任务，但要进行具有可证明保证的严格分析可能颇为棘手。在代数模型中，Cai [Cai94]，给出了一个精确算法，而 Dey、Kannan、Ryder 和 Srivastava [DKRS23]直到最近才给出了一个具有严格分析的数值算法。根据计算模型（代数模型或数值模型），我们可以使用 [Cai94] 或 [DKRS23]。另一个例子是，为了解决张量对角同构问题，我们借助了近期关于环面作用的工作 [BDM+21]。将这些结果结合起来即可得到定理1.1。

酉轨道近似。 证明的一个核心部分是应用高阶奇异值分解（HOSVD），这与精确酉同构的情形相同。然而，我们必须发展额外的技术，以便针对“鲁棒”设置修改该算法。现有的 HOSVD 算法可以判定两个张量是否精确同构。要回答鲁棒版本的问题，则需要对该算法进行非平凡的修改。

本质上，HOSVD 算法会针对每个模式 d，计算每个张量的展平$d = 1, 2、3$，然后将每个展平后的张量与其共轭转置相乘，从而计算模式 d 格拉姆矩阵。接着，算法计算这些格拉姆矩阵的谱并进行比较。在问题的精确版本中，我们还要求这些谱是简单谱；只有当两个张量对应的格拉姆矩阵具有匹配的简单谱时，它们才是同构的。如果谱确实匹配，我们就建立一个线性等式系统；该系统存在一个解对应于一组“相位矩阵”，当且仅当这些张量同构时成立。

在算法的鲁棒版本中，我们再次计算格拉姆矩阵，并要求谱具有足够大的特征值间隙（类似于精确情形中的简单谱条件）。现在，我们不再检查谱是否完全相等，而是检查它们是否足够接近。然后，我们不再建立等式系统，而是建立一个不等式 系统，对应于一组近似相位矩阵。虽然这些修改合乎直觉，但证明新算法的正确性仍是主要难点。

为了证明正确性，我们必须说明近似解与真实轨道距离相差不大。我们首先利用 Weyl不等式，将张量上的距离界与格拉姆矩阵上的距离界联系起来。然后，我们使用一种概率技巧，将 Gram矩阵的对角元素视为随机变量的取值，并将酉矩阵的一行视为这些取值对应的概率。通过这种视角，我们可以利用这个假想随机变量的方差来界定与最优解的距离。请注意，对于酉轨道近似，我们并不依赖 [BDM+21] 的结果。

1.4.2 概率技术

平均情况分析。 我们的算法的关键在于假设 $G_d(A)$ 具有单谱且存在一定的定量排斥。我们采用的证明策略最初由 [NTV17]在厄米随机矩阵的背景下提出，随后被应用于次高斯Wishart矩阵，见

[CLOS25], 的整体结构与 [CLOS25]大体相同。这两篇论文都通过将最小特征值间隙问题归结为为随机矩阵 M所关联的某个小球概率给出下界来处理该问题。在 [NTV17] 中，这意味着要控制子矩阵 M' （它是 M 的子矩阵）的一个特征值 v 与一个独立的次高斯向量之间内积的集中性质；而在 [CLOS25] 中， $M = A^\top A$ 与由独立同分布元素构成的 A 之间的依赖结构更加复杂，因此作者控制了与 M相关的左、右奇异向量的性质。两种情况下，用于控制内积的工具都来自一个称为“逆 Littlewood–Offord 理论”的领域。我们的范围$p = o(n)$面临的主要技术障碍是，在处理左、右奇异向量时， [CLOS25] 中的论证有相当一部分对称性不复存在。我们在第 3.1 节讨论 [CLOS25], 的结果以及我们如何在此基础上推进。

量 $|v'X|$ 可能因两种情况而变小：1）奇异向量中有相当多的零元素（或接近零的元素），这由可压缩性这一概念刻画；或 2）奇异向量具有显著的加性结构，因此内积中可能发生抵消，这由低最小公分母这一概念刻画，其中 LCD 在此表示最小公分母。上述论文通过依次排除条件 1）和 2）来开展研究。我们排除了左奇异向量的这两种性质，但对于右奇异向量，只需证明条件 1）不成立。

关于排斥的启发式解释。我们简要讨论两种启发式解释，说明为何应当预期定理 1.3 中所呈现的这种定量排斥。特别是，我们可以注意到，在定理 1.3 中，如果 $p = n^\zeta$ 对于 $\zeta > 0$ 足够小，那么存在一些目标间隙的取值（由足够小的 β 配置），使得 $M^\top M$ 的极端特征值间隙实际上会 增大。乍看之下，这或许有些令人意外，因此我们在此作简要说明。

首先，对于具有 $n > p$ 的 $n \times p$ 次高斯矩阵 M，以压倒性概率， M 的奇异值落在窗口 $[\sqrt{n} - \Theta(\sqrt{p})\ \sqrt{n} + \Theta(\sqrt{p})]$ 内（见第 3.2 节）。由于共有 p 个奇异值，单个奇异值间隙的量级约为 $1/\sqrt{p}$。由于极端奇异值间隙更小，我们假设奇异值间隙具有如下形式： $1/p^\Delta$ ，其中$\Delta > 1/2$，且与 ζ 独立。现在，奇异值平方之间的第 i 个间隙可以写成平方之差 $\sigma_i^2(M) - \sigma_{i+1}^2(M) = (\sigma_i(M) - \sigma_{i+1}(M))(\sigma_i(M) + \sigma_{i+1}(M))$。根据上述假设以及关于最小奇异值的压倒性概率界，可得

$$\sigma_i^2(M) - \sigma_{i+1}^2(M) \geq 2\sqrt{n} - \Theta(\sqrt{p}) / p^\Delta = 2n^{1/2} - \Theta(n^{\zeta/2}) / n^{\zeta\cdot\Delta} \qquad 1 \leq i \leq p$$

对所有 ζ 都成立。显然，当 ζ 足够小时，分子中的$\sqrt{n}$ 项占主导，因此极端间隙会随着 $n \to \infty$ 发散。不过请注意，为了在定理 1.3 中获得最强的排斥概率，需要令 β 任意大，因此自然会研究一个收缩的间隙。

其次，我们描述一种有限情形，在该情形下，我们关于高维情形右奇异向量结构的结果（定理 3.8）可以由 [Han25、CLOS25] 中线性相关的结果推导出来。如果矩阵 M具有服从 $\sim \mathcal{N}(0, 1)$的独立同分布元素，即经典 Wishart 系综（记为 $W(p, n)$），那么矩阵系综 $W(p, n)$ 是正交不变的，因此其特征向量在 $O(p)$ 上服从 Haar 分布，并且无论 n 如何都与特征值独立（见 [AGZ10]）；系综 $W(p, p)$ 和 $W(p, n)$ 的特征向量结构性结论在 $n > p$下是相同的。这也为间距启发式中假设 Δ 和 ζ 相互独立提供了动机。

1.5 开放问题

我们的主要结果以及用于证明这些结果的技术，使我们确定了以下几个重要的开放问题。这些问题最直接地影响着我们对张量同构问题的更完整理解，尤其涉及其平均情形复杂度。

开放问题 1 (一般线性群张量同构。)。 我们的工作留下的、值得进一步研究的首要问题，或许是：一般线性群作用下的三阶张量同构是否在平均情形下容易求解。尽管 3-张量同构在有限域上仍然是指数级困难的 *[LQ17, BLQW20]*, 但或许可以为 $\mathbb{R}$ 或 $\mathbb{C}$开发更多工具和技术。

开放问题 2 (张量正交与酉同构的平滑分析。)。 在高阶奇异值分解的研究中，通常假设边缘谱是简单的。这引出了对这一现象进行平滑分析的研究 *[ST04]* ：对固定张量的元素施加微小扰动，会使边缘谱变为简单谱。定理 *1.4* 正是受这一考虑启发，是朝这一方向迈出的第一步。

开放问题 3 (张量轨道闭包交的平均情形算法。)。 如第 *1.1* 节所述，张量轨道闭包交（*TOCI*）一直是非交换优化中的一个重要问题，但有些研究指出了现有技术面临的某些障碍。然而，据我们所知，目前尚无针对这类问题的正式平均情形算法研究。鉴于张量酉同构在其中若干算法中发挥着关键作用，我们预计，针对张量酉同构的平均情形算法将推动这一方向的研究。

开放问题 4 (有限域上的张量正交与酉同构。)。 张量正交同构也可以在有限域上研究。尽管随机矩阵的谱已有相关研究 *[NP98, LMN21]*, 但有限域上 *Wishart* 矩阵的奇异值似乎尚未得到研究，而且尚不清楚原有限域上是否存在奇异值。

开放问题 5 (从简单谱到有界重数。)。 另一个引人关注的问题是，将简单谱（每个特征值的重数为 1）放宽为有界重数（每个特征值的重数至多为 c ，其中 c为某个常数）。在这种情形下，基于不变量理论的高效算法（沿用 *[BDM+21]*）或许可行，因为“非交换部分”受到较大限制，因此可以在此处使用生成次数的指数上界 *[Der01]* 。

1.6 对先前工作的更广阔视角

三阶-**张量与** k**-张量**。张量同构问题自然地从三阶张量推广到任意阶张量。有趣的是，对于任意 $k > 3$，一般线性 k-张量同构都可以在多项式时间内归约为一般线性三阶张量同构 [GQ23] ，相应的酉版本和正交版本也同样如此 [CGQ+24]。因此，我们将限于研究三阶张量同构问题，并滥用记号 TI，使其既表示张量同构问题，也表示相应的复杂度类（对于 GI 类，我们也将采用类似的记号滥用）。

图同构的平均情形算法。在 Babai、Erd˝os 和 Selkow [BES80], 提出第一个图同构平均情形算法之后，多项工作改进了平均情形算法的失败概率，包括 Karp [Kar75], 、Lipton [Lip78], 以及 Babai 和 Kuˇcera[BK79]的工作。一般 Erd˝os–R´enyi 模型 $\mathcal{G}(n,p)$ 中的随机图同构（ p 不一定 $1/2$）已由 Bollob´as [Bol82], 、Czajka 和 Pandurangan [CP08], 以及 Linial 和 Mosheiff[LM17] 进行研究。随机超图同构在 [CFHH21]中进行了讨论。

随机矩阵理论。 在随机矩阵理论中，现代研究中一条富有成果的路线，是理解给定随机矩阵系综的全局和局部谱统计。特别值得关注的量包括随机矩阵的可逆性、相邻特征值间隔的渐近行为，以及所有此类间隔中最小间隔的行为。随着随机矩阵系综的性质发生变化，例如元素的边缘分布、元素之间的依赖关系以及矩阵的维度，这些谱性质可能会有很大变化。

关于随机矩阵可逆概率的问题，随着以下一系列研究取得了重大进展 [RV08,TV09b, TV09a,RV09, Ver14] ，这些研究全面解决了次高斯随机矩阵的相关问题，并为随机矩阵理论文献提供了 Littlewood–Offord 理论及其逆理论等工具。

粗略地说，给定一个确定性向量 $x \in \mathbb{R}^n$ 和一个随机向量 $X \in \mathbb{R}^n$，Littlewood–Offord问题探讨 x 的结构会如何影响以下事件的概率： $\langle x, X\rangle$ 很大。反过来，逆 Littlewood–Offord 问题则探讨：如果 x 在 $\langle x, X\rangle$ 以很小的概率才会很大，那么这对 [TV09b]的结构有何启示。正如[NTV17、Han25、CLOS25], 以及我们自己的工作所体现的那样，逆 Littlewood–Offord 理论的洞见能清晰地列举出必须排除的特征向量性质，从而推导出特征值排斥。

研究特征值间隙通常以谱的“主体”部分（即远离最大和最小特征值的区域）较为容易。关于 Wigner 矩阵和 Wishart 矩阵主体部分的局部特征值统计结果分别由 [TV11]和 [TV12]得出，随后又分别由 [TV10] 和 [Wan12] 推广至谱边缘。值得注意的是，这些结果具有普适性，即对于坐标分布满足温和正则性条件（通常与测度集中有关）的矩阵系综，它们通常都成立。

极端间隙的控制自然更加难以捉摸，但在最初采用较强的分布假设时，已有一些进展，例如 [BAB13]的论文研究了高斯酉系综。尽管酉不变和正交不变高斯系综在解析处理上具有显著优势，但人们预期极端间隙的定性性质具有普适性。对于 Wigner 情形， [NTV17]在普适框架下控制了极端间隙的尾界，进而控制了谱简单概率。此前的结果采用了上述逆 Littlewood–Offord 理论；而最近，[CLOS25]和 [Han25] 分别利用类似的逆 Littlewood–Offord 技术，在普适框架下同时证明了 Wishart 矩阵具有类似性质，使其达到与 Wigner 情形相当的水平。

应当注意的是，尽管采用逆 Littlewood–Offord 理论的技术，以及总体上源自组合随机矩阵理论的方法 [Vu14、Vu21], 为研究局部特征值统计提供了广泛使用且有效的工具，但要在极端间隙方面取得进展，同样还需要新的思想和工具，这一点已在诸如 [ESY10、EY15]等论文中体现出来。

表1中一些元素的注释。表1中的一些元素需要进一步说明。

- 酉和正交张量同构属于PSPACE，因为我们可以将这些问题表述为在 $\mathbb{R}$上求解多项式方程。这可以通过先为变换矩阵设定变量矩阵来实现；对于$\mathbf{U}(n,\mathbb{C})$的情形，我们需要分别记录实部和虚部。然后，我们可以将两个张量同构表述为一组在 $\mathbb{R}$上的多项式方程。在 $\mathbb{R}$上求解多项式方程已知属于PSPACE，见 [Can88]。

- 在 $\mathbb{C}$ 上的一般线性张量同构也可以表述为求解一个多项式方程组。由于不需要共轭转置，我们无需（将实部和虚部作为实数变量）分别记录实部和虚部。文献 [Koi96]和 [AGS26]中的结果代表了关于希尔伯特零点定理目前已知的最佳复杂性理论结果。请注意， [Koi96] 假设广义黎曼猜想，且张量的元素为整数。

- 在 $\mathbb{C}$ 上的平均情形一般线性张量同构与其轨道闭包相交问题相关，因为轨道为闭轨道的张量构成一个扎里斯基开集。因此，对于自然的随机张量模型，随机张量会具有闭轨道；对于这类张量，轨道相交问题与轨道闭包相交问题是相同的。

- 在 $\mathbb{F}_q$ 上的一般线性张量同构属于coAM，可通过沿用图非同构的相同交互式证明协议 [GS86]。

2 张量同构算法

我们首先确立本文中通篇使用的记号。

我们用 A和 B表示 $n\times n\times n$张量，并用 L， R， T表示酉矩阵和正交矩阵，除非另有说明。对于 L， R， $T\in\mathbf{U}(n)$，记

$$((L,R,T)\curvearrowright A)_{ijk}=\sum_{p,q,r}L_{ip}R_{jq}T_{kr}A_{pqr}.$$

为避免记号歧义，我们用 $\mathsf{Orb}(A)$ 表示张量 A的轨道，用$\mathbf{U}(n)$表示 n维酉群，用$\mathbf{O}(n)$表示 n维正交群，并用 $O(\cdot)$表示大“O”函数。因此，$\mathsf{Orb}_{\mathbb{C}}(A):=\mathsf{Orb}^{\mathbf{U}(n)^3}(A)$表示 A 在$\mathbf{U}(n)^3$作用下的轨道。类似地，$\mathsf{Orb}_{\mathbb{R}}(A):=\mathsf{Orb}^{\mathbf{O}(n)^3}(A)$。

令 $\mathbb{Q}(i)=\{s+it:\ s,\ t\in\mathbb{Q}\}$ 表示高斯有理数域，并假设它采用通常方式编码——对于通常的浮点表示，它们的形式为 $(s+it)2^p$，其中 s， $t\in\mathbb{Q}$，且$p\in\mathbb{Z}$ 按标准方式以二进制编码。令 $S^1=\{z\in\mathbb{C}^\times:\ |z|=1\}$。对于向量空间$V$中的 v，记

$$\mathrm{supp}(v):=\{j\in[n]:v_j\neq 0\}.$$

当 $A\in\mathbb{C}^{n_1\times n_2\times\cdots\times n_k}$ 时， A 的模式-d 展平为一个矩阵

$$A_d\in\mathbb{C}^{n_d\times(n_1\cdots n_{d-1}n_{d+1}\cdots n_k)}.$$

令 $G_d(A)$ 表示格拉姆矩阵 $A_dA_d^*$；注意，这些矩阵都是厄米半正定的，因此具有

非负实特征值。本文中，$A \in \mathbb{C}^{n\times n\times n}$ 的模式-d 展平为 $A \in \mathbb{C}^{n\times n^2}$，而 $G_d(A)$ 为 $n \times n$。

我们用 $\mathbb{A}$ 表示代数数。关于如何有效且高效地处理代数数，已有相当成熟的理论，详见第 A 节。值得注意的是，对于矩阵 $M \in \mathbb{A}^{n\times n}$，我们可以在代数数域上精确计算 M 的约当标准形，例如可使用 Cai [Cai94]的多项式时间算法。

令 $\|\cdot\|$ 表示矩阵的谱范数，$\|\cdot\|_F$ 表示弗罗贝尼乌斯范数。

2.1 精确酉张量同构

本节旨在证明以下定理，该定理蕴含定理1.1。

定理 2.1。令 $A \in \mathbb{Q}(i)^{n\times n\times n}$ 的元素独立地取自某个固定的次高斯分布，并令 $B \in \mathbb{Q}(i)^{n\times n\times n}$ 为任意对象。存在一个确定性算法，其输入为A、B，并以高概率（概率为 $1 - \frac{1}{\mathrm{poly}(n)}$）判定以下命题是否成立

$$B \in \mathrm{Orb}_{\mathbb{C}}(A) \coloneqq \{(L,R,T) \curvearrowright A : \ L,R,T \in \boldsymbol{U}(n)\}$$

在多项式时间内，并在肯定的情况下输出这样的（L, R, T）。

用于证明定理2.1 的算法中一个关键步骤，是将问题归约为判定紧环面作用下的轨道相等问题；因此，我们采用 B¨urgisser、Do˘gan、Makam、Walter 和 Wigderson 在 [BDM+21]中的结果。

[BDM+21] 的主要目的是在交换群（特别是环面）的作用这一背景下，运用不变量理论中的技术，研究轨道相等、轨道闭包交以及轨道闭包包含问题。他们的主要成果是开发出用于判定环面作用下这些轨道问题的多项式时间算法。作者在 [BDM+21] 中的一个关键洞见是注意到，对于环面作用，存在一种情形，使这些问题容易受到一种基于 Mumford 结果的技术的攻击（见 [MFK94]）。具体而言，如果向量 v、w 在向量空间 V 中的轨道闭包不相交，那么总能用一个不变多项式将它们区分开。[2] 尤其重要的是，对于环面作用，作者设计了一种方法，构造一个带除法的算术电路，其输出门计算一组生成 Laurent 单项式（有理不变量），可用于高效检验轨道闭包是否能够分离。这构成了他们算法的核心，并给出了一个显式的分离不变量。

下面我们要用到的主要结果来自 [BDM+21]

命题（[*BDM+21*，推论 *1.6*]）。设权矩阵 $M \in \mathit{Mat}_{d,n}(\mathbb{Z})$ 定义了 n 维的 $\mathcal{T} = (\mathbb{C}^\times)^d$ 表示，并令 $\mathcal{K} = (S^1)^d$。进一步，设 $v, w \in \mathbb{Q}(i)^n$，并假设 v, w 和 M 的元素的位长度均不超过 b。那么，我们可以在 $\mathit{poly}(d, n, b)$ 时间内判定 $\mathit{Orb}_{\mathcal{K}}(v) = \mathit{Orb}_{\mathcal{K}}(w)$ 是否成立。

我们还将隐式地使用

[2]如果多项式函数 f 在 V 上沿轨道为常数，则称其为 *invariant*，因此对所有 $g \in G$ 和 $v \in V$，都有 $f(gv) = f(v)$。此外，回顾一下，我们考虑的是 G 在 V 上的（线性）作用，使用表示 $\rho\colon G \to \mathrm{GL}(V)$，并将轨道（记 $\rho(g)v$ 为 gv）记作 $\mathrm{Orb}(v) = \{gv\colon g \in G\}$。那么 Mumford 的结果表明，若 $\mathrm{Orb}(v) \cap \mathrm{Orb}(w) = \emptyset$，则存在一个不变多项式 f，使得 $f(v) \neq f(w)$。

命题（[BDM+21，命题 8.1]）。设 $M \in Mat_{d,n}(\mathbb{Z})$ 定义了 $\mathcal{T} = (\mathbb{C}^\times)^d$ 和 $\mathcal{K} = (S^1)^d$ 的一个 n 维表示。设 $v, w \in \mathbb{C}^n$。那么，$Orb_{\mathcal{K}}(v) = Orb_{\mathcal{K}}(w)$ 当且仅当 $Orb_{\mathcal{T}}(v) = Orb_{\mathcal{T}}(w)$，且对所有 j，$|v_j| = |w_j|$。

现在，我们介绍本文的主要算法，用于证明定理 2.1。首先给出一些额外的记号和约定。令 $\mathcal{K} = (S^1)^{3n}$。那么，对于 $(a, b, c) \in \mathcal{K}$，我们得到对角酉矩阵

$$D_1 = \mathrm{diag}(a_1, \ldots, a_n),\ D_2 = \mathrm{diag}(b_1, \ldots, b_n),\ D_3 = \mathrm{diag}(c_1, \ldots, c_n),$$

因此，$\mathcal{K}$ 通过以下方式作用于张量 A 和 B 的向量化 v_A 和 v_B

$$(D_3 \otimes D_2 \otimes D_1)v_A \text{ and } (D_3 \otimes D_2 \otimes D_1)v_B.$$

具体而言，逐坐标来看，(i, j, k) 项会乘以 $a_i b_j c_k$。

算法 1 判定具有单谱的三阶张量的酉等价性。

输入 给定输入 A, B 以及 $\Lambda_d^A, U_d, \Lambda_d^B, V_d$, $d = 1, 2, 3$，我们旨在用关于输入规模（以输入的位长度衡量）的多项式时间，判定是否存在 L, R, T 属于 $\mathbf{U}(n)$，使得 $(L, R, T) \curvearrowright A = B$。不失一般性，假设组成 Λ_d^A 和 Λ_d^B 的特征值均按非递增顺序给出。

步骤 1 对每个 $d = 1$，2、3，通过考察元素矩阵 Λ_d^A，Λ_d^B，检查是否存在某个 d，使得 $G_d(A)$ 或 $G_d(B)$ 的谱是单谱。若谱不是单谱，则输出无法判定该实例并停止。若谱是单谱，则检查 $\Lambda_d^A = \Lambda_d^B$，$d = 1$，2、3。若谱不相等，则输出否。若相等，则令 $\Lambda = \Lambda_d^A = \Lambda_d^B$。

步骤 2 令

$$S_A \coloneqq (U_1^*, U_2^*, U_3^*) \curvearrowright A, \text{ and } S_B \coloneqq (V_1^*, V_2^*, V_3^*) \curvearrowright B.$$

令 $v_A = \mathrm{vec}(S_A)$ $v_B = \mathrm{vec}(S_B) \in \mathbb{C}^N$，其中 $N = n^3$，为 S_A 和 S_B 的向量化，并按字典序 $l = (k-1) + n(j-1) + n^2(i-1)$ 使 $(v_A)_l = (S_A)_{ijk}$（v_B 亦同）。

步骤 3 验证 $\mathrm{supp}(v_A) = \mathrm{supp}(v_B)$，并验证对所有 $l \in [n^3]$，都有 $|(v_A)_l| = |(v_B)_l|$。若任何条件不成立，则输出否。

步骤 4 如 [BDM+21] 中所述，根据 Ge [Ge93] 的一项结果，他们的主要结果可扩展到以下情形：被作用元素 $v \in \mathbb{C}$ 的元素取自某个代数数域。我们利用这一事实，将他们的算法应用于向量 v_A 和 v_B 取自域 $\mathbb{Q}(i, \{\lambda_p\}, \{u_{pq}\}, \{v_{pq}\})$ 的情形，其中 λ_p 格拉姆矩阵 $G_d(A)$ 和 $G_d(B)$ 的特征值，以及 u_{pq}, v_{pq} U_d, V_d, $d = 1$ 的元素为 2、3。

步骤5 使用 [BDM+21] 中的推论 1.6（具体而言，算法 2），检查 $\mathrm{Orb}_{\mathcal{K}}(v_A) = \mathrm{Orb}_{\mathcal{K}}(v_B)$ 是否成立。如果成立，则输出 是，并可选择输出见证 $L = V_1 D_1 U_1^*$、$R = V_2 D_2 U_2^*$、$T = V_3 D_3 U_3^*$，其中

$$D_1 = \mathrm{diag}(a_1, \ldots, a_n),\ D_2 = \mathrm{diag}(b_1, \ldots, b_n),\ D_3 = \mathrm{diag}(c_1, \ldots, c_n)$$

对于算法找到的适当元素（a、b、c）$\in \mathcal{K}$。否则输出否。

在陈述定理2.1 的证明之前，我们需要一些引理。

引理 2.2. 设 $A, B \in \mathbb{C}^{n\times n\times n}$。假设对于每个 $d = 1$，2、3， $G_d(A)$ 和 $G_d(B)$ 的单谱在排列意义下相同。将酉对角化写作 $G_d(A) = U_d\Lambda_d^A U_d^*$和$G_d(B) = V_d\Lambda_d^B V_d{}^*$，其中特征值按非递增顺序排列，并固定相位约定。定义

$$S_A \coloneqq (U_1^*, U_2^*, U_3^*) \curvearrowright A, \quad S_B \coloneqq (V_1^*, V_2^*, V_3^*) \curvearrowright B.$$

那么，存在酉矩阵 $L, R, T \in \boldsymbol{U}(n)$ 使得 $(L, R, T) \curvearrowright A = B$，当且仅当存在对角 $D_1, D_2, D_3 \in \boldsymbol{U}(1)^n$ 使得 $(D_1, D_2, D_3) \curvearrowright S_A = S_B$。

证明。 我们首先回顾，若 $B = (L, R, T) \curvearrowright A$，则

$$G_1(B) = LG_1(A)L^*,\ G_2(B) = RG_2(A)R^*,\ G_3(B) = TG_3(A)T^*;$$

例如，对于 $d = 1$, $B_1 = LA_1(T \otimes R)^*$，因此 $G_1(B) = B_1B_1{}^* = LA_1A_1{}^*L^* = LG_1(A)L^*$。

现在我们继续证明。

($\Longrightarrow$) 令 $L_1 = L$、 $L_2 = R$、 $L_3 = T$ 取自 $\mathbf{U}(n)$。回顾 $G_d(A) = U_d\Lambda_d^A U_d^*$和$G_d(B) = V_d\Lambda_d^B V_d{}^*$。假设 $B = (L_1, L_2, L_3) \curvearrowright A$。于是 $\Lambda_d^A = \Lambda_d^B = \Lambda_d$，因此我们有

$$G_d(B) = V_d\Lambda_d V_d{}^* = L_dG_d(A)L_d^* = L_dU_d\Lambda_dU_d^*L_d^*.$$

Λ_d 是简单且有序的，因此 $G_d(B)$ 的有序特征基在相位意义下唯一。因此存在一个 $D_d \in U(1)^n$ 使得

$$V_d = L_dU_dD_d \text{ for } d = 1, 2, 3.$$

因此,

$$\begin{aligned} S_B &= (V_1^*, V_2^*, V_3^*) \curvearrowright B \\ &= (V_1^*L_1, V_2^*L_2, V_3^*L_3) \curvearrowright A \\ &= (D_1^*U_1^*, D_2^*U_2^*, D_3^*U_3^*) \curvearrowright A \\ &= (D_1^*, D_2^*, D_3^*) \curvearrowright S_A. \end{aligned}$$

代入 $D_d \leftarrow D_d^*$，我们得到第一个方向。

($\Longleftarrow$) 另一方面，假设 $(D_1, D_2, D_3) \curvearrowright S_A = S_B$，其中 $D_d \in U(1)^n$ 与前面相同。令

$$L \coloneqq V_1D_1U_1^*, \quad R \coloneqq V_2D_2U_2^*, \quad T \coloneqq V_3D_3U_3^* \in \mathbf{U}(n).$$

然后，利用假设,

$$\begin{aligned} (L, R, T) \curvearrowright A = (V_1D_1, V_2D_2, V_3D_3) \curvearrowright (U_1^*, U_2^*, U_3^*) \curvearrowright A \\ = (V_1, V_2, V_3) \curvearrowright \big((D_1, D_2, D_3) \curvearrowright S_A\big) \\ = (V_1, V_2, V_3) \curvearrowright S_B \\ = B. \end{aligned}$$

此外， $S_B = (V_1^*,\ V_2^*,\ V_3^*) \curvearrowright B$ 意味着 $B = (V_1,\ V_2,\ V_3) \curvearrowright S_B$，因此我们得出结论： A 和 B 是酉等价的。 □

现在我们证明算法 1 的正确性和高效运行时间。

引理 2.3. 算法*1*是正确的。

证明。 我们证明，算法 1 输出 是 当且仅当存在 L、 R、 $T \in \mathbf{U}(n)$，使得 $(L,\ R,\ T) \curvearrowright A = B$。

首先注意，格拉姆矩阵的元素属于 $\mathbb{Q}(i)$，因此通过扩展到代数数域即可将其对角化。可采用许多已知方法中的任意一种（例如 Cai 方法[Cai94]），精确得到分解 $G_d(A) = U_d \Lambda_d U_d^*$ 和 $G_d(B) = V_d \Lambda_d V_d^*$，同时使用有效处理代数数的方法。 $G_d(A)$ 和$G_d(B)$ 的谱是简单谱，这一点是算法第四步所要求的。显然，如果 $G_d(A)$ 和 $G_d(B)$ 的特征值（在排列意义下）不相等，那么就不存在 $L, R, T \in \mathrm{U}(n)$ 使得 $(L, R, T) \curvearrowright A = B$。

检查格拉姆矩阵 $G_d(A)$ 和 $G_d(B)$ 的谱后，定理 2.2 告诉我们，只需确定所构造的 S_A 和 S_B 是否处于同一轨道（在紧致环面作用下）： A 和 B 是 $\mathrm{U}(n)^3$-同构的，当且仅当存在对角矩阵D_1, $D_2, D_3 \in \mathrm{U}(1)^n$，使得 $(D_1, D_2, D_3) \curvearrowright S_A = S_B$。按照步骤 2 中提到的标准方式将 S_A和 S_B向量化不会对此产生影响，这样做仅仅是为了更便于应用 [BDM+21]的算法。步骤 3 中对 v_A 和 v_B 的支撑及模是否匹配所做的检查，依据的是 [BDM+21]中的命题 8.1 和引理 3.2 的逆否命题。最后， [BDM+21] 的算法会告知我们 $\mathrm{Orb}_{\mathcal{K}}(v_A)$ =$\mathrm{Orb}_{\mathcal{K}}(v_B)$ 是否成立。

此外，如果算法输出“是”，还可以输出 $L = V_1 D_1 U_1^*$、 $R = V_2 D_2 U_2^*$ 和 $T = V_3 D_3 U_3^*$。首先注意，根据构造，每个 U_d 和 V_d 都是酉矩阵；每个 D_d 都是对角矩阵，其元素位于复单位圆上，因此也是酉矩阵。最后，我们有

$$\begin{aligned}(L,R,T) \curvearrowright A &= (V_1 D_1 U_1^*, V_2 D_2 U_2^*, V_3 D_3 U_3^*) \curvearrowright A \\ &= (V_1, V_2, V_3) \curvearrowright \big((D_1, D_2, D_3) \curvearrowright (U_1^*, U_2^*, U_3^*) \curvearrowright A\big) \\ &= (V_1, V_2, V_3) \curvearrowright \big((D_1, D_2, D_3) \curvearrowright S_A\big) \\ &= (V_1, V_2, V_3) \curvearrowright S_B \\ &= B\end{aligned}$$

如所需。 □

引理 2.4. 算法 在 *1* 多项式时间内终止，其中时间取决于 A， B 的二进制编码长度 .

证明。 构造 $G_d(A)$ 和 $G_d(B)$ 需要 $O(n^4)$ 次算术运算。此外，通过扩展到代数数来计算特征多项式并检验谱的简单性，都可以在多项式时间内完成；具体而言，精确计算 Jordan 标准形，从而精确求出代数数域上 $G_d(A)$ 和 $G_d(B)$ 的分解，可在多项式时间内完成 [Cai94]。因此，可以高效构造 S_A 和 S_B，其向量化也可以高效构造。在 步骤 3中检验支撑和模长是否相等，至多需要 n^3次检查；每次检查都是对代数数进行比较，其所需时间关于这些数的表示长度为多项式时间（见第 A 节）。

对于步骤5，我们可以构造一个整数权重矩阵 $M \in \mathbb{Z}^{3n \times N}$，其对应于（$i$、 j、 k）的列为 $e_i \oplus e_{n+j} \oplus e_{2n+k}$；根据 [BDM+21]的推论 1.6，检查轨道相等的算法随后可在多项式时间内运行；当扩展到不同的代数数域 [BDM+21、Ge93]时，仍可在多项式时间内运行。

由此可得，该算法会在输入长度的多项式时间内终止。 □

有了这些引理，我们就可以证明定理 2.1。

定理*2.1*的证明。定理2.3 和2.4 证明了算法1的正确性及多项式运行时间。根据定理1.3 ，格拉姆矩阵 $G_d(A)$ 和 $G_d(B)$ 以高概率具有单谱；由此可知，该算法以高概率判定 A和 B 是否酉同构。

□

注 2.1。也许算法1 要求格拉姆矩阵 $G_d(A)$ $G_d(B)$ 具有单谱，这一点并非显而易见。要在验证特征基对齐后调用 [BDM+21]，单谱是必要的：任何额外的自由度都只是逐坐标相位（环面作用）。如果谱不单纯，那么在每个重数为 m的特征子空间内，剩余自由度是整个酉群$\mathbf{U}(n)$，而不仅仅是相位。在这种情况下，需要使用不同的算法。

注 2.2。步骤5的算法1 调用了 [BDM+21] 中相当繁重的工具来判定 A 和 B 是否同构。另一方面，在第2.3 节中，我们将介绍一种相关算法（适用于固定精度情形，并且可以很容易地调整到完美精度情形），它不需要 [BDM+21]的环面作用工具，而是使用简单的线性规划来解决一个与算法步骤5所实现目标相关的问题。看起来，一种类似但更微妙的方法可以用来替代第 [BDM+21] 节步骤5中对环面作用结果的调用。

2.2 近似酉张量同构

本节将转向数值环境下的近似情形，研究轨道距离问题，而非像上一节那样研究精确的轨道相等问题。我们首先陈述一些关于矩阵和张量扰动的结果。

回顾一下，矩阵 $A \in \mathbb{C}^{n\times n}$ 的迹范数定义为

$$\|A\|^2 = \mathrm{Tr}(AA^*) = \mathrm{Tr}(A^*A) = \sum_{1\le i,j\le n} |A_{i,j}|^2.$$

我们用 $\|A\|_F = \sqrt{\|A\|^2}$ 表示弗罗贝尼乌斯范数。显然，弗罗贝尼乌斯范数满足以下上界：

$$\|A\|_F \le n \max_{i,j} |a_{i,j}|$$

对于 $A \in \mathbb{C}^{n\times n}$。

现在回顾一个霍夫曼和维兰特提出的有用不等式 [HW+53]。霍夫曼-维兰特不等式指出，若 A, $B \in \mathbb{C}^{n\times n}$ 是正规矩阵，其对应的特征值分别为 $\lambda_1(A)\ldots,\lambda_n(A)$ 和 $\lambda_1(B)\ldots,\lambda_n(B)$，那么，令 $\mathcal{S}_n$ 表示 $\{1,\ldots,n\}$ 的置换群，可得

$$\min_{\sigma\in\mathcal{S}_n} \sqrt{\sum_{i=1}^{n} |\lambda_i(A) - \lambda_{\sigma(i)}(B)|^2} \le \|A-B\|_F.$$

韦尔和 Mirsky 还给出了关于奇异值的一些相关且有用的不等式（参见 [Ste98]）。我们需要以下内容

引理 2.5。 设 $A, A \in \mathbb{R}^{n\times n}$ 为对称矩阵，且令 $\varepsilon = \max_{i,\ j} |A_{i,\ j} - A_{i,\ j}|$。则

$$\min_{\sigma\in\mathcal{S}_n} \sqrt{\sum_{i=1}^{n} |\lambda_i(A) - \lambda_{\sigma(i)}(\tilde{A})|^2} \leq n\varepsilon.$$

证明。 如果 A， $A \in \mathbb{R}^{n\times n}$ 是实对称矩阵，那么它们就是正规矩阵；霍夫曼和维兰特不等式适用。因此，利用 $\|A\|_F \leq n\max_{i,\ j} |a_{i,\ j}|$ 对于 $A \in \mathbb{R}^{n\times n}$这一事实，即可得出结论。 □

注 2.3。 根据 Mirsky 的一个定理 [Mir60], 我们有如下结论：如果 $A = A + E$ 是任意矩阵 A 的扰动，那么

$$\min_{\sigma\in\mathcal{S}_n} \sqrt{\sum_{i=1}^{n} |\mu_i - \tilde{\mu}_{\sigma(i)}|^2} \leq \|E\|_F,$$

其中 μ_i， $\tilde{\mu}_i$ 分别是 A 和 A的奇异值。不过，由于实对称矩阵的特征值与奇异值一致，这意味着前面的引理在更一般的情形下也成立：我们实际上无需假设受扰动的矩阵 A 是对称的。

这些结果的用途在于：在数值环境中，当矩阵的元素被截断到固定精度时，我们可以得出结论，矩阵的特征值和奇异值不会因截断操作而发生太大变化。因此，特征值间隙的下界也适用于固定精度设置。

我们给出一个有用的推论。

推论 2.1。 设 A 和 $B \in \mathbb{C}^{n\times n}$ 是具有单谱的实对称矩阵。令

$$\delta_{max} = \max_{1\leq i\leq n} \min_{\sigma\in\mathcal{S}_n} |\lambda_i(A) - \lambda_{\sigma(i)}(B)|.$$

则存在一个酉 $L \in \mathbb{C}^{n\times n}$ 使得

$$\|A - LBL^*\|_F \leq n\delta_{max}.$$

证明。 矩阵 A、B 是具有单谱的实对称矩阵，因此我们可以将 $A = U\Lambda U^*$ 和 $B = V\Sigma V^*$ 分别写作 U、V 酉矩阵。令 $L = UV^*$，并令 $\delta_i = \min_{\sigma\in\mathcal{S}_n} |\lambda_i(A) - \lambda_{\sigma(i)}(B)|$。于是 $A - LBL^* = U(\Lambda - \Sigma)U^*$。由于弗罗贝尼乌斯范数 $\|\cdot\|_F$ 具有酉不变性，

$$\|A - LBL^*\|_F = \|U(\Lambda - \Sigma)U^*\|_F = \|\Lambda - \Sigma\|_F = \sqrt{\sum_{i=1}^{n} \delta_i^2} \leq n\delta_{max}.$$ □

以下引理对于将涉及张量的精确轨道相等或闭包交集的问题转化为其近似（或数值）对应问题很有用。对于 $X \in \mathbb{C}^{n\times n\times n}$，令$\|X\|_\infty$ 表示逐项 ℓ_∞ 范数，即 $\max_{1\leq i,\ j,\ k\leq n} |X_{ijk}|$。

引理 2.6. 设 A， $B \in \mathbb{C}^{n\times n\times n}$，并假设存在酉 L、R、T，使得（L、R、T） $\curvearrowright$

~ ~$A = B$。固定 $\varepsilon_0 > 0$。那么对于所有满足 $\|A - A\|_\infty \le \varepsilon_0$的 $A \in \mathbb{C}^{n\times n\times n}$，

$$\|(L, R, T) \curvearrowright \tilde{A} - B\|_F \le n^{3/2}\varepsilon_0.$$

~证明。令 $\Delta = A - A$。注意到

$$\begin{aligned}(L, R, T) \curvearrowright \tilde{A} - B &= (L, R, T) \curvearrowright (A + \Delta) - (L, R, T) \curvearrowright A \\ &= (L, R, T) \curvearrowright \Delta.\end{aligned}$$

该作用关于弗罗贝尼乌斯内积在 $\mathbb{C}^{n\times n\times n}$ 上是酉的，因此保持范数不变。于是

$$\|(L, R, T) \curvearrowright \Delta\|_F = \|\Delta\|_F.$$

根据假设 ~，即 $\|A - A\|_\infty \le \varepsilon_0$，我们有 $\|\Delta\|_\infty < \varepsilon_0$ 且 $|\Delta_{ijk}| \le \varepsilon_0$，对所有 i，j，k 均成立。但

$$\|\Delta\|_F^2 = \sum_{i,j,k} |\Delta_{ijk}|^2 \le \sum_{i,j,k} \varepsilon_0^2 = n^3\varepsilon^2$$

由此可得 $\|\Delta\|_F \le n^{3/2}\varepsilon$。结合以上观察，我们得到

$$\|(L, R, T) \curvearrowright \tilde{A} - B\|_F \le n^{3/2}\varepsilon_0. \qquad \square$$

利用这些观察和定理 2.1，我们得出：若存在酉矩阵 L，R，T~ ~使得 $B = (L,\ R,\ T) \curvearrowright A$，其中 A 表示对一个具有复数条目的张量进行截断 A，那么

$$\|(L, R, T) \curvearrowright A - B\|_F \le \frac{n^{3/2}}{2^\ell}.$$

~这是定理 2.6 的推论，因为如果 $(L, R, T) \curvearrowright A = B$，那么对于所有满足 $A \in \mathbb{C}^{n\times n\times n}$ 的 $\|A - \tilde{A}\|_\infty \le \varepsilon_0$，$\|(L, R, T) \curvearrowright A - B\|_F \le n^{3/2}\varepsilon_0$。在我们的设定中 $\varepsilon_0 = 1/2^\ell$，因此断言成立。这一观察自然地引出了后续内容。

近似酉张量同构。 与算法1 中采用完美精度技术不同，使用数值算法会引入误差，使得（紧致）轨道相等问题难以判定。另一种思路是，判断两个三阶张量在酉作用下的轨道彼此是“接近”还是“相距甚远”。下述定理的内容是证明，在固定精度设置下，存在一种用于酉三阶张量同构的数值算法，具有这样的性质：“是”实例蕴含距离的一个上界

$$\operatorname{dist}_{\mathbb{C}}(A, B) \coloneqq \inf_{L,R,T\in\mathbf{U}(n)} \|(L, R, T) \curvearrowright A - B\|_F$$

当 A 和 $B \in \mathbb{Q}(i)^{n\times n\times n}$。

更具体地说，以下定理证明了存在一种算法，可以解决我们称为近似酉张量同构问题。

问题 3. 近似酉张量同构问题如下：给定运算精度为 ℓ 的输入，以及 $\mathbb{Q}(i)^{n\times n\times n}$ 中的张量 A 和 B，其元素以 ℓ 位精度表示，判断以下情形中的哪一种成立。

1. 若不存在正交矩阵 L、R、T 使得

$$(L, R, T) \curvearrowright A = B.$$

2. 否则，尝试构造一个固定精度见证 $(\widetilde{L}, \widetilde{R}, \widetilde{T}) \in \boldsymbol{U}(n)^3$，使得

$$\|(\widetilde{L}, \widetilde{R}, \widetilde{T}) \curvearrowright A - B\|_F \leq O\left(\frac{n}{2^\ell}\right),$$

如果能找到这样的见证，则输出“是”。

定理 2.7。 存在一种确定性多项式时间算法，对于给定的 $A \in \mathbb{Q}(i)^{n\times n\times n}$，其元素来自某个固定的——均值为零、单位方差——次高斯分布 ξ，且相互独立同分布；以及任意确定性的 $B \in \mathbb{Q}(i)^{n\times n\times n}$，该算法以高概率判定 A 和 B 的近似酉张量同构问题，其中隐含常数仅依赖于 ξ 的分布。

我们通过直接改编算法 2.7 来证明定理 1。算法 1 与下文给出的算法2 之间的关键区别在于格拉姆矩阵的分解数值计算 $G_d(A),\ G_d(B),\ d = 1,2,3$，而非使用代数数完美地计算分解。这一步会在该过程中引入误差，使我们无法判定 $\mathsf{Orb}_{\mathbb{C}}(A) = \mathrm{Orb}_{\mathbb{C}}(B)$ 是否相等，因此只能得出轨道接近的结论。

修改后的数值算法如下，见算法2。

算法 2 酉作用下的紧致轨道距离判定过程 .

输入 令正整数 ℓ 表示运算精度。输入为 $A,\ B \in \mathbb{Q}(i)^{n\times n\times n}$（其中 ℓ是 A 和 B 中元素在标准二进制编码下的最大位长）。

步骤 1 令 $G_d(A)$ 和 $G_d(B),\ d = 1,2,3$ 表示由d的第 A模式展平以及 B分别得到的格拉姆矩阵；并使用具有良好前向误差界的数值算法（例如 [DKRS23]中提出的算法），计算 $\widetilde{U_d}\widetilde{\Lambda_d^A}\widetilde{U_d}^*$ 的$G_d(A)$以及 $\widetilde{V_d}\widetilde{\Lambda_d^B}\widetilde{V_d}^*$ 的 $G_d(B)$的酉对角化（若尔当标准形），使矩阵中每个元素的精度达到 ℓ 位。

具体而言，若 $\|\cdot\|$ 表示矩阵的算子范数，而 $\|\cdot\|_\infty$ 表示逐项无穷范数，回顾 $\|M\|_\infty \le \|M\| \le n\|M\|_\infty$；则 [DKRS23]的算法 1 给出一个多项式时间过程，产生 $\widetilde{U_d}\widetilde{\Lambda_d^A}\widetilde{U_d}^*$ 和 $\widetilde{V_d}\widetilde{\Lambda_d^B}\widetilde{V_d}^*$，使得

$$\|U_d - \widetilde{U_d}\| \le \frac{n\|U_d\|_\infty}{2^\ell} \text{ and } \|\Lambda_d^A - \widetilde{\Lambda_d^A}\| \le \frac{n\|\Lambda_d^A\|_\infty}{2^\ell}$$

for 精确的 $G_d(A) = U_d\Lambda_d^A U_d^*$。对于 $G_d(B)$ 的分解，同样成立。

$\sim$ $\sim$不失一般性地假设，构成 Λ_d^A和 Λ_d^B的特征值按非递增顺序给出。对于每个 $d = 1$, 2，3，通过研究元素矩阵 Λ_d^A，Λ_d^B，检查是否存在某个 d，使得 $\sim$ $\sim$ $\sim$ $\sim$的谱（无论是 $G_d(A)$ 还是 $G_d(B)$）为单谱。如果 Λ_d^A或 Λ_d^B的谱不是单谱，则输出“无法判定该实例”并停止。如果这些谱均为$\sim$ $\sim$ $\sim$ $\sim$单谱，则检查对于每个 $d = 1$，2，3，是否满足 $\Lambda_d^A = \Lambda_d^B$。如果某个 d使得 $\Lambda_d^A \ne \Lambda_d^B$，则输出“否”。

步骤 2 设置

$$\widetilde{S_A} \coloneqq (\widetilde{U_1}^*, \widetilde{U_2}^*, \widetilde{U_3}^*) \curvearrowright A, \text{ and } \widetilde{S_B} \coloneqq (\widetilde{V_1}^*, \widetilde{V_2}^*, \widetilde{V_3}^*) \curvearrowright B.$$

令 $v_A = \mathrm{vec}(\widetilde{S_A})$ $v_B = \mathrm{vec}(\widetilde{S_B}) \in \mathbb{C}^N$ with $N = n^3$ 分别为 S_A 和 S_B 的向量化。特别地，使用字典序 $l = (k-1) + n\,j - 1 + n^2\,i - 1$（$v_B$ 同样如此）设置 $(v_A)_l = (\widetilde{S_A})_{ijk}$。

步骤 3 验证：(i) $\mathrm{supp}(v_A) = \mathrm{supp}(v_B)$，以及 (ii) 对所有 $l \in [n^3]$，均有 $|(v_A)_l| = |(v_B)_l|$。如果任一条件不满足，则输出否。

步骤 4 现在我们应用 [BDM+21] 的紧致环面作用结果：使用 [BDM+21] 中的推论 1.6（具体来说是算法 2），检查 $\mathrm{Orb}_{\mathcal{K}}(v_A) = \mathrm{Orb}_{\mathcal{K}}(v_B)$ 是否成立。如果成立，则输出 是$\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$，并可选择输出见证 $L = V_1 D_1 U_1$, $R = V_2 D_2 U_2$, $T = V_3 D_3 U_3$ ，其中

$$\widetilde{D_1} = \mathrm{diag}(a_1, \ldots, a_n),\ \widetilde{D_2} = \mathrm{diag}(b_1, \ldots, b_n),\ \widetilde{D_3} = \mathrm{diag}(c_1, \ldots, c_n)$$

对于算法找到的适当元素 $(a,\ b,\ c) \in \mathcal{K}$（回想 $\mathcal{K} = (S^1)^{3n}$）。否则输出 否。

算法2 正确性和高效运行时间的证明与算法1的正确性和高效运行时间证明完全相同。现在我们可以证明定理2.7。

定理*2.7*的证明。算法2 的正确性及运行效率证明

定理2.3 和2.4，作相应修改。根据定理1.3，格拉姆矩阵以高概率具有$G_d(A)$ 有单谱，且关键的是，其特征值之间的最小距离大于 $O(1/2^\ell)$ ；这使得算法能够以 ℓ的精度区分这些特征值，从而以高概率输出是或否。

$\widetilde{\ }\ \widetilde{\ }\ \widetilde{\ }$最后，假设算法输出 是，并给出见证（$L$， R， T）。步骤 1 中给出的前向误差界 步骤 1 保证 $\|\widetilde{U}_d - U_d\| \le O$（$n2^{-\ell}$），同理 $\widetilde{V}_d$。将此误差沿着$\widetilde{\ }\ \widetilde{\ }\ \widetilde{\ }$作用传播，可知所得到的见证（$L$， R， T）满足

$$\|(\widetilde{L},\widetilde{R},\widetilde{T}) \curvearrowright A - B\|_F \le \left(\|\widetilde{L} - L\| + \|\widetilde{R} - R\| + \|\widetilde{T} - T\|\right)\|A\|_F + O(2^{-2\ell})\|A\|_F$$

其中（L， R， T）是一个精确见证。但 $\|\widetilde{L} - L\| \le O(n2^{-\ell})$（与 R， T 一样）给出了具体界

$$\|(\widetilde{L},\widetilde{R},\widetilde{T}) \curvearrowright A - B\|_F \le O\left(\frac{n}{2^\ell}\right). \qquad \square$$

2.3 酉轨道近似

现在，我们进一步从宏观角度来看张量同构问题的鲁棒变体。回顾引言中提到的（带间隙）酉张量轨道近似问题（问题2）：

问题 （问题2，重述）。 （带间隙）酉张量轨道近似问题定义如下：给定 $0 < \varepsilon < \eta$ 以及张量 A, $B \in \mathbb{C}^{n\times n\times n}$，判断以下两种情况中哪一种成立：

$$\mathrm{dist}(\mathrm{Orb}_{\mathbb{C}}(A), \mathrm{Orb}_{\mathbb{C}}(B)) \le \varepsilon \quad \textit{and} \quad \mathrm{dist}(\mathrm{Orb}_{\mathbb{C}}(B), \mathrm{Orb}_{\mathbb{C}}(B)) \ge \eta.$$

注意，问题 2 与问题3不同：前者判定距离是否足够近（轨道距离 $\le \epsilon$）或相当远（轨道距离 $\ge \eta$）。另一方面，问题 3 判定是否同构（轨道距离 $= 0$）或不同构（轨道距离 > 0）。

我们给出一种算法（定理 2.8 及下文的算法 3 ），用于解决酉张量轨道近似问题中的问题 2，适用于 A、 $G_d(A)$ 的格拉姆矩阵对 $d \in [3]$均具有单谱，且最小特征值间隙至少为 $\delta > 0$ 的情形。定理 1.3 保证定理 A 1.2 中给出的随机量满足上述条件；结合下述定理即可证明定理1.2。

定理 *2.8*（判定酉轨道近似问题）。设 $A, B \in \mathbb{C}^{n\times n\times n}$，使得对于每个 $d \in [3]$，$G_d(A)$ 都具有单谱，且最小特征值间隙至少为 $\delta > 0$。那么，对于每个满足 $\delta/4(\|A\|_F + \|B\|_F) > \varepsilon > 0$ 的 ε，存在一种算法，其运行时间为 $O(poly(n, log(1/\varepsilon))$，能够区分 $dist_{\mathbb{C}}(A, B) < \varepsilon$ 与 $dist_{\mathbb{C}}(A, B) > \gamma\varepsilon$（针对 $\gamma = O(n^{7/2}\|A\|_F^2/\delta)$）；在前一种情况下，算法会输出一个见证 $(\widetilde{L}, \widetilde{R}, \widetilde{T}) \in U(n)^3$，使得 $\|(\widetilde{L}, \widetilde{R}, \widetilde{T}) \curvearrowright A - B\|_F < \gamma\varepsilon$。

注 2.4。 我们不对常数进行优化，包括 poly(n) 项中的常数指数。

算法 3 正交作用下的轨道距离判定过程。

输入取 $A, B \in \mathbb{C}^{n\times n\times n}$，并令 A, B 表示张量 A, B 的截断，我们将其取为 $\ell = \lceil \log(1000n^7/\varepsilon) \rceil$ 位精度。令 $\gamma = O(n^{7/2}\|A\|_F^2/\delta)$。回顾一下，3-张量 W *mode-d* 展平记为 $W_d \in \mathbb{C}^{n\times(n^2)}$。回顾一下，格拉姆矩阵 $G_d(A)$ 定义为 $A_d A_d^*$，$G_d(B)$ 也类似。

步骤 1 检查 $\left|\|\widetilde{A}\|_F - \|\widetilde{B}\|_F\right| < 2\varepsilon$，若不满足则输出否（即 $\mathrm{dist}_{\mathbb{C}}(A, B) > \gamma\varepsilon$）。

步骤 2 写出格拉姆矩阵 $G_d(A) = U_d \Lambda_d^A U_d^*$ 和 $G_d(B) = V_d \Lambda_d^B V_d^*$，其特征值按非-递增顺序排列。令 $K := 2\|A\|_F$。我们近似计算 $\widetilde{A}, \widetilde{B}$ 的格拉姆矩阵的酉对角化，得到 $\widetilde{G_d\ A}() = \widetilde{U_d}\widetilde{\Lambda_d^A}\widetilde{U_d^*}$，以及 $\widetilde{G_d\ B}() = \widetilde{V_d}\widetilde{\Lambda_d^B}\widetilde{V_d^*}$，使得

$$\|\widetilde{U_d} - U_d\|_F, \|\widetilde{V_d} - V_d\|_F, \|\widetilde{\Lambda_d^A} - \Lambda_d^A\|_F, \|\widetilde{\Lambda_d^B} - \Lambda_d\|_F < \frac{\varepsilon}{1000n^7\|A\|_F} \tag{2.1}$$

使用 [DKRS23][3] 中的算法 1，并通过用适当的置换矩阵共轭格拉姆矩阵，将特征值按非递增顺序排列。Λ_d^B 的最小特征值间隙小于 $\delta/2$，**输出** 否 $(\mathrm{dist}_{\mathbb{C}}(A, B) > \gamma\varepsilon)$ 并停止。

步骤 3 定义

$$\widetilde{S_A} := \left(\widetilde{U_1^*}, \widetilde{U_2^*}, \widetilde{U_3^*}\right) \curvearrowright \widetilde{A}, \qquad \widetilde{S_B} := \left(\widetilde{V_1^*}, \widetilde{V_2^*}, \widetilde{V_3^*}\right) \curvearrowright \widetilde{B}.$$

如果存在 (i, j, k)，使得 $\left||\widetilde{S_A}(i, j, k)| - |\widetilde{S_B}(i, j, k)|\right| > 2\varepsilon n^2\delta^{-1}(\|\widetilde{A}\|_F + \|\widetilde{B}\|_F)$，**输出**~ ~ **否** $(\mathrm{dist}_{\mathbb{C}}(A, B) > \gamma\varepsilon$ $|S_A(i,j,k)| + |S_B(i,j,k)| > 2\varepsilon n^2\delta^{-1}(\|\widetilde{A}\|_F + \|\widetilde{B}\|_F)$。否则，对于每个满足 (i, j, k) 的 (i, j, k) (i, j, k)，定义

$$\Phi_{ijk} := \arg\left(\frac{\widetilde{S_B}(i, j, k)}{\widetilde{S_A}(i, j, k)}\right)$$

步骤 4 引入未知数 $\alpha_i, \beta_j, \gamma_k \in [0, 2\pi)$（编码相位 $s_1(i) = e^{i\alpha_i}$, $s_2(j) = e^{i\beta_j}$, $s_3(k) = e^{i\gamma_k}$）以及线性不等式

$$|\Phi_{ijk} - (\alpha_i + \beta_j + \gamma_k)| \pmod{2\pi} < \arccos\left(\frac{|\widetilde{S_A}(i, j, k)|^2 + |\widetilde{S_B}(i, j, k)|^2 - 2\varepsilon^2 n^4\delta^{-2}(\|\widetilde{A}\|_F + \|\widetilde{B}\|_F)^2}{2\,|\widetilde{S_A}(i, j, k)|\,|\widetilde{S_B}(i, j, k)|}\right)$$

对所有满足上述定义的 (i, j, k)。

- 如果不可行，则输出 NO（$\mathrm{dist}_{\mathbb{C}}(A, B) > \gamma\varepsilon$）。
- 如果可行，构造 $D_1 = \mathrm{diag}(e^{-i\alpha_i})$、$D_2 = \mathrm{diag}(e^{i\beta_j})$、$D_3 = \mathrm{diag}(e^{i\gamma_k})$，并设

$$\widetilde{L} := \widetilde{V_1} D_1 \widetilde{U_1^*}, \quad \widetilde{R} := \widetilde{V_2} D_2 \widetilde{U_2^*}, \quad \widetilde{T} := \widetilde{V_3} D_3 \widetilde{U_3^*}.$$

~ ~ ~输出 是（$\mathrm{dist}_{\mathbb{C}}(A, B) < \varepsilon$），并且（可选）输出见证（$L, R, T$）（注意，这些见证仅能证明 $\mathrm{dist}_{\mathbb{C}}(A, B) < \gamma\varepsilon$ 这一事实）。

在证明我们的算法正确且运行高效之前，我们先给出一些引理。

引理 2.9. 设 $A, B \in \mathbb{C}^{n\times n\times n}$ 满足 $G_d(A) = U_d\Lambda_d^A U_d^*$ 且 $G_d(B) = V_d\Lambda_d^B V_d^*$，其中 $d \in [3]$，且 Λ_d^A, Λ_d^B 的对角线元素按非递增顺序排列。令 $\varepsilon > 0$，并令 $\delta > 0$ 表示对所有 $d \in [3]$ 取值时 $G_d(A)$ 的最小特征值间隙。

若 $G_d(B)$ 在某个 d 和 i 处具有特征值间隙 $\lambda_i - \lambda_j < \delta - 2\varepsilon$，且 j，则

$$\mathrm{dist}_{\mathbb{C}}(A, B) > \frac{\varepsilon}{(\|A\|_F + \|B\|_F)}.$$

证明。令

$$S_A \coloneqq (U_1^*, U_2^*, U_3^*) \curvearrowright A, \qquad S_B \coloneqq (V_1^*, V_2^*, V_3^*) \curvearrowright B.$$

由于 S_A, S_B 分别属于 A, B 的酉轨道，故 $\mathrm{dist}_{\mathbb{C}}(A, B) = \mathrm{dist}_{\mathbb{C}}(S_A, S_B)$。不失一般性，可假设 $G_1(B)$ 具有 $\lambda_i - \lambda_j < \delta - 2\varepsilon$。于是

$$\begin{aligned}
\|(L, R, T) \curvearrowright S_A - S_B\|_F &= \|LS_{A[1]}(R \otimes T)^* - S_{B[1]}\|_F \\
&\geq \frac{\|LS_{A[1]}S_{A[1]}^*L^* - S_{B[1]}S_{B[1]}^*\|_F}{\|S_A\|_F + \|S_B\|_F} \\
&\geq \frac{\|LG_1(S_A)L^* - G_1(S_B)\|_F}{\|S_A\|_F + \|S_B\|_F} \\
&> \frac{\varepsilon}{\|A\|_F + \|B\|_F}
\end{aligned}$$

最后一行由 Weyl不等式以及弗罗贝尼乌斯范数在酉作用下的不变性得出。

□

在下一个引理中，我们将证明：如果酉矩阵 U 的某一列有两个足够大的元素，且 D 是特征值间隙至少为 δ 的实对角矩阵，那么 UDU^* 将有一个比例上较大的非对角元。

引理 2.10。设 $v_1, \ldots, v_n$ 是 $\mathbb{C}^n$ 中的标准正交向量，D 是对角元素严格递减且为正的对角矩阵 $d_1 > d_2 > \cdots > d_n > 0$，并且 $d_i - d_{i+1} > \delta > 0$ 对于 $i \in [n-1]$ 成立。对于$\varepsilon > 0$，若存在某个 $i \neq j$ 使得 $|v_{ni}| > \varepsilon$ 且 $|u_{nj}| > \varepsilon$，则存在 $k \in [n-1]$ 使得$\langle v_n, Dv_k\rangle > \frac{\varepsilon\delta}{\sqrt{2(n-1)}}$。

证明。注意，由于 D 是对称的，$\langle v_n, Dv_k\rangle = \langle Dv_n, v_k\rangle$。令 $w \coloneqq Dv_n - \langle Dv_n, v_n\rangle v_n$，并注意 $w \in$ 张成 $\{v_1, \ldots, v_{n-1}\}$。由帕塞瓦尔恒等式，

$$\sum_{k=1}^{n-1} |\langle Dv_n, v_k\rangle|^2 = \sum_{k=1}^{n-1} |\langle w, v_k\rangle|^2 = \|w\|^2. \tag{2.2}$$

因此，$\max_{k\in[n-1]} |\langle Dv_n, v_k\rangle|^2 \geq \|w\|^2/(n-1)$。还需证明 $\|w\|^2 \geq \varepsilon^2\delta^2/\sqrt{2}$。我们有

$$\|w\|^2 = \|Dv_n\|^2 - |\langle Dv_n, v_n\rangle|^2 = \sum_{k=1}^{n} d_k^2|v_{nk}|^2 - \left(\sum_{k=1}^{n} d_k|v_{nk}|^2\right)^2.$$

[3]请注意，我们并未充分利用该算法的全部能力

令 X 为取值为 d_k 的随机变量，其概率为 $|v_{nk}|^2$ （这是定义良好的，因为 $\|v_n\| = 1$）。那么方程（2.2）给出 $\|w\|^2 = \mathrm{Var}(X)$。令 Y 为指示随机变量，

$$Y = \begin{cases} 1 & \text{if } X = d_i \text{ or } X = d_j, \\ 0 & \text{otherwise.} \end{cases}$$

根据全方差定律，

$$\begin{aligned} \mathrm{Var}(X) &= \mathbb{E}[\mathrm{Var}(X|Y)] + \mathrm{Var}(\mathbb{E}[X|Y]) \\ &\geq \mathbb{P}(Y=1) \cdot \mathrm{Var}(X|Y) \\ &= (|v_{ni}|^2 + |v_{nj}|^2) \cdot \frac{|v_{ni}|^2 |v_{nj}|^2}{(|v_{ni}|^2 + |v_{nj}|^2)^2} (d_i - d_j)^2 \\ &> \frac{\varepsilon^2 \delta^2}{2} \end{aligned}$$

其中，最后一个不等式由 $|d_i - d_j| > \delta$ 这一事实以及 $|u_i|^2$，$|u_j|^2 > \varepsilon^2$ 这一事实得出。因此 $\|w\| > \frac{\varepsilon\delta}{\sqrt{2}}$，结论成立。 □

引理 2.11. 设 $A, B \in \mathbb{C}^{n\times n\times n}$ 满足条件，使得 $G_d(A)$ $G_d(B)$ 是元素为正实数、按降序排列且最小间隔为 δ 的对角矩阵，其中对所有 $d \in [3]$ 均成立。进一步假设存在 L, R, T 酉矩阵，使得对于某个 $0 < \varepsilon < \delta/(\|A\|_F + \|B\|_F)$，有 $\|(L, R, T) \curvearrowright A - B\|_F < \varepsilon$。那么存在对角相位矩阵 D_1, D_2, D_3，使得对于 $\gamma = O(n^2(\|A\|_F + \|B\|_F)^2/\delta)$，有 $\|(D_1, D_2, D_3) \curvearrowright A - B\|_F < \gamma\varepsilon$。

证明。我们有

$$\|(L,R,T) \curvearrowright A - B\|_F \geq \frac{\|(LA_{[1]}(R\otimes T)^*)(LA_{[1]}(R\otimes T)^*)^* - B_{[1]}B_{[1]}^*\|_F}{\|A\|_F + \|B\|_F} = \frac{\|LG_1(A)L^* - G_1(B)\|_F}{\|A\|_F + \|B\|_F}.$$

根据引理 2.10，如果存在一行 i属于 L，满足

$$|L_{ij}| > \varepsilon\delta^{-1}\sqrt{2(n-1)}(\|A\|_F + \|B\|_F) \text{ and } |L_{ik}| > \varepsilon\delta^{-1}\sqrt{2(n-1)}(\|A\|_F + \|B\|_F), \text{ for } j \neq k,$$

那么存在 ℓ，$m \in [n], \ell \neq m$ 使得

$$\|LG_1(A)L^* - G_1(B)\| \geq |(LG_1(A)L^*)_{\ell m}| > \varepsilon(\|A\|_F + \|B\|_F),$$

这就产生了矛盾。由于 L 的各行均为单位范数，因此我们可以将注意范围限制为满足以下条件的 L

$$\|L - \Pi\|_F < 2n^{3/2}\varepsilon\delta^{-1}\sqrt{2(n-1)}(\|A\|_F + \|B\|_F)$$

对于带相位置换矩阵 Π。然而，根据 $G_d(A)$ $G_d(B)$的元素顺序以及特征值分离，我们必须有 Π 为对角矩阵。由对称性，R，T 也同样如此。因此，我们可以找到对角相位矩阵 D_1，D_2，D_3，使得

$$\|(D_1, D_2, D_3) \curvearrowright A - B\|_F < \varepsilon + 6n^{3/2}\varepsilon\delta^{-1}\sqrt{2(n-1)}\|B\|_F(\|A\|_F + \|B\|_F) < \gamma\varepsilon. \qquad \square$$

现在我们证明定理 2.8。

引理 2.12. 算法 *3*是正确的。

证明。令 $K := \|A\|_F + \|B\|_F$，并假设 $G_d(A)$ 具有单谱且 $\varepsilon < \delta/4K$。我们需要证明，当且仅当 $(\widetilde{L}, \widetilde{R}, \widetilde{T}) \in \mathbf{U}(n)^3$，且 $\|(\widetilde{L}, \widetilde{R}, \widetilde{T}) \curvearrowright \widetilde{A} - \widetilde{B}\|_F < \gamma\varepsilon$ 时，算法输出是（即 $\mathrm{dist}_{\mathbb{C}}(A, B) < \varepsilon$）以及 (L, R, T)。我们按步骤进行证明。

若算法在步骤 1处终止，则显然 $\mathrm{dist}_{\mathbb{C}}(A, B) > \varepsilon$，因为 $\mathrm{dist}_{\mathbb{C}}(A, B) \geq |\|A\|_F - \|B\|_F| > \left|\|\widetilde{A}\|_F - \|\widetilde{B}\|_F\right| - \varepsilon/2$，且算法输出了正确答案。

若算法在步骤 2处终止，则我们再次输出了否（即 $\mathrm{dist}_{\mathbb{C}}(A, B) > \gamma\varepsilon$）。此输出正确，因为根据引理 2.9 和方程（2.1）中的精度界，$\mathrm{dist}_{\mathbb{C}}(A, B) > \delta/4K > \varepsilon$。

若算法在步骤 3处终止，则根据定理 2.11，$\mathrm{dist}_{\mathbb{C}}(A, B) > \gamma\varepsilon$.

若在步骤 4处，线性方程组不可行，那么对于任意对角相位矩阵 D_1, D_2, D_3，必定存在某个 (i, j, k)，

$$|\widetilde{S_A}(i,j,k)| + |\widetilde{S_B}(i,j,k)| > 2\varepsilon n^2 \delta^{-1} K$$

and

$$\arg\left(\frac{\widetilde{S_B}(i,j,k)}{(D_1,D_2,D_3) \curvearrowright \widetilde{S_A}(i,j,k)}\right) > \arccos\left(\frac{|\widetilde{S_A}(i,j,k)|^2 + |\widetilde{S_B}(i,j,k)|^2 - 2\varepsilon^2 n^4 \delta^{-2} K^2}{2\,|\widetilde{S_A}(i,j,k)|\,|\widetilde{S_B}(i,j,k)|}\right),$$

因此，对两边分别取余弦并重新排列各项，

$$\|(D_1, D_2, D_3) \curvearrowright \widetilde{S_A} - \widetilde{S_B}\|_F > 2\varepsilon n^2 \delta^{-1} K$$

因此，根据引理 2.11，$\mathrm{dist}_{\mathbb{C}}(A, B) > \varepsilon$。否则，步骤 4 中的线性方程组可行，对于构造出的对角符号矩阵 D_1，D_2，D_3，我们有

$$\|(D_1, D_2, D_3) \curvearrowright \widetilde{S_A} - \widetilde{S_B}\|_F < 2\varepsilon n^{5/2} \delta^{-1} K,$$

因为对于每个 $(i, j, k) \in [n]^3$，我们有 $|((D_1, D_2, D_3) \curvearrowright \widetilde{S_A})(i, j, k) - \widetilde{S_B}(i, j, k)| < 2\varepsilon n^2 \delta^{-1} K$。加回有限精度计算所对应的误差后，我们仍有 $\mathrm{dist}_{\mathbb{C}}(S_A, S_B) < \gamma\varepsilon$，因此 $\mathrm{dist}_{\mathbb{C}}(A, B) < \gamma\varepsilon$。最后，很容易验证

$$\|(\widetilde{L}, \widetilde{R}, \widetilde{T}) \curvearrowright \widetilde{A} - \widetilde{B}\|_F = \|(D_1, D_2, D_3) \curvearrowright \widetilde{S_A} - \widetilde{S_B}\|_F$$

由构造可知，因为弗罗贝尼乌斯范数在正交作用下保持不变。因此，L，R，T见证了 $\mathrm{dist}_{\mathbb{C}}(A, B) < \gamma\varepsilon$ 这一事实。 □

引理 2.13. 算法 *3* 的运行时间为 $O(\mathrm{poly}(n, \log(1/\varepsilon)))$。

证明。只需注意到每一步的运行时间均为 $O(\mathrm{poly}(n, \log(1/\varepsilon)))$。事实上，根据 [DKRS23], , 步骤 2 的运行时间为 $O(\mathrm{poly}(n, \log(1/\varepsilon)))$；而步骤 4 的运行时间为 $O(\mathrm{poly}(n, \log(1/\varepsilon)))$，这是通过使用内点法求解线性方程组得到的（参见例如 [Kar84]）。请注意，尽管直接应用线性规划无法处理模 2π 的循环问题，但问题中对常数的先决条件保证了每个线性不等式中可能的循环移位唯一，并且可以轻松计算出来。算法的其余部分显然都在 $O(\mathrm{poly}(n, \log(1/\varepsilon)))$ 时间内运行。 □

定理 *2.8*的证明。 该结论直接由定理 2.12 和定理 2.13得出。 □

定理 *1.2* 的证明。 根据定理 1.3，张量 A 以高概率满足定理 2.8 的假设条件，并且 步骤 1 解决了 $\|B\|_F$ 过大的潜在问题。 □

3 高大 Wishart 矩阵的特征值排斥

如定理 1.1 所述，本文考虑的随机模型（展平后）是一个具有独立同分布的次高斯元素的随机 $n \times p$ 矩阵，其中 $p = o(n)$。我们称 p 对 n 的这种依赖关系为“高瘦”范围。本节证明此类矩阵的一般定量特征值排斥结果，扩展了文献 [CLOS25] 中针对 $p = \Theta(n)$ 情形的近期结果。

回想一下，与 [NTV17、CLOS25], 一样，我们的方法归结为证明左奇异向量 v 与一个独立同分布的次高斯向量 X 之间的内积通常较大。这样的结果称为“小球概率”。 v 基本上，

1. v 是稀疏的，因此会直接使 X 中的许多系数失效。
2. v 具有加性结构，会与 X 元素的对称性和独立性相互作用，从而以不可忽略的概率产生抵消。

我们将在第 3.3 节和3.4节中，沿用逆 Littlewood–Offord 理论中的成熟技巧，以高概率排除这两种障碍。在此之前，我们将在第3.1节讨论论文 [CLOS25], ，它是我们证明策略的基础；随后在第 3.2 节介绍一些概率预备知识。

3.1 与 [CLOS25] 在技术层面上的比较

本节简要讨论 [CLOS25], 中排斥结果的证明，因为我们的策略是沿用其证明框架，并在必要之处针对高矩阵情形作出调整。 [CLOS25] 本身采用了早期工作中确立的典型逆 Littlewood–Offord 理论技巧，因此我们先概述 [CLOS25] 中的新颖技巧，然后讨论相较于 [CLOS25], 我们证明的新意所在。我们将指出自己的证明在哪些方面忠实遵循了 [CLOS25], 又在哪些方面有所不同。

关于 [CLOS25]技术贡献的注。 在 [CLOS25] 中，核心难点在于 Wishart 矩阵元素之间复杂的依赖结构。在 Wigner 矩阵的情形中，矩阵元素要么相互独立，要么彼此确定；由于这种结构简单，直接控制特征值方程 $Ax = \lambda x$ 即可。Wishart 矩阵则并非如此， [CLOS25] 通过观察特征值方程 $M^T M x = \lambda x$ 可分解为一对奇异值方程$Mx = \sqrt{\lambda} y$和 $M^T y = \sqrt{\lambda} x$，从而处理了更复杂的结构。这一转换将关于元素依赖关系复杂的矩阵的问题，转化为关于依赖结构简单的矩阵的两个问题。完成这一分解后， [CLOS25]再将已有的逆 Littlewood–Offord 技巧应用于 M的右奇异向量和左奇异向量，最后通过论证，证明分别针对每个奇异值方程得出的所需性质能够同时成立。

总而言之， [CLOS25] 其主要创新在于通过奇异值方程，提供了研究 Wishart 矩阵谱事件的技术，使之适用于成熟的逆 Littlewood–Offord 理论。

关于我们技术贡献的几点说明。遵循 [CLOS25], 我们将 Wishart 矩阵的特征值事件分解为右、左奇异向量相关事件的交集。

我们所研究的高矩阵情形的核心难点，在于右、左奇异向量相关情形之间存在显著的对称性损失，而这种对称性在 [CLOS25]中得以保留。因此，尽管我们希望针对 Wishart 矩阵的右、左奇异向量得出类似的结论，但 [CLOS25]中使用的一些分解和论证在我们的情形下并不适用。然而，在高矩阵情形中，我们虽失去了对称性，却获得了相对较强的 M奇异值集中性质，因为此时该矩阵是一个高矩形矩阵。这也使我们能够讨论复数情形（见第3.6节），而 [CLOS25] [4]并未涉及这一情形。我们将在本节中介绍具体的调整（见注3.2、3.4和3.5）。

我们对排斥文献的主要贡献，是在必要时调整或替换 [CLOS25] 中的论证，以处理这种新的不对称性。对于定理3.8 和3.9 ，我们采用了不同的证明策略，但认为 [CLOS25]中的方法应该可行。关于这一选择背后的理由，请参见注3.2。在定理3.16 中，我们采用了与 [CLOS25],类似的策略，但我们所处范围内的不对称性带来了尤为棘手的问题，因此需要进行重大调整。定理3.10 和3.17 至3.19利用主要引理排除排斥障碍，并最终得出排斥结论；其论证与 [CLOS25], 中的对应论证相似，但更普遍地说，这类论证是逆Littlewood-Offord结果中的典型做法。例如，参见 [NTV17] ，它是[CLOS25]的代表性先驱文献。

3.2 测度集中的预备知识

接下来，我们将处理大量常数，其中一些是普适常数，另一些则取决于 ξ 的分布律。我们将重复使用符号 c、$\hat{c}$、C、K 表示可能随结果而变化的量，但会说明哪些常数依赖于 ξ、哪些不依赖于它，以及常数的取值何时发生变化。

本文通常考虑元素为 $M \in \mathbb{C}^{n\times p}$ 的复随机矩阵 $\zeta_{ij} = \xi_{ij} + i\xi'_{ij}$，其中 ξ_{ij} 和 ξ'_{ij} 都是独立同分布实值随机变量。大多数相关结果都可以直接从实数情形推广到复数情形，因此我们主要给出实数情形的结果，并在第 3.6 节讨论所需的复数推广中不显然的部分。

在 [CLOS25] 中，作者研究了 Wishart 矩阵，其坐标分布所需的集中性假设显著较弱，即只要求有限四阶矩。他们通过将关注事件与诸如 $\{\|M\| \geq C\sqrt{n}\}$ 这样的辅助结构事件取交，来确保次高斯矩阵以高概率通常具备的那些性质。本文选择研究较为简洁的次高斯情形（见定理 3.1），因此仅以次高斯形式呈现 [CLOS25] 中所需的结果。我们建议感兴趣的读者查阅该文中的相应结果，以了解其最一般的形式。我们预计，通过选择适当的辅助事件，我们在高矩阵情形下的排斥结果可以推广到四阶矩假设。

此外，我们研究均值为零、单位方差的随机变量 ξ，并在需要时通过缩放推广主要结果。现在回顾以下内容：

定义 3.1（次高斯随机变量和向量）。 如果实值随机变量 ξ 满足尾部集中上界，则称其为次高斯随机变量

$$\mathbb{P}[|\xi| > t] \leq 2\exp(-t^2/K^2)$$

[4]复数情形已由 [Han25]的工作涵盖。我们将在第[CLOS25] 节3.6讨论省略复数情形一事。

对所有 $t > 0$ 以及某个 $K > 0$均成立。我们将使集中性不等式成立的最小 K 称为 ξ的次高斯常数。

若随机向量 $X \in \mathbb{R}^n$ 具有次高斯边缘分布，则称其为次高斯随机向量。此外，若 $\mathbb{E}[X] = 0$，则称其为零均值；若 $\mathbb{E}[XX^\top] = I$，则称其为各向同性。

下文中的隐含常数通常依赖于 K，且往往只依赖于 K。对于一个$n \times p$ 矩阵 M，记 $s_k(M)$（ $1 \le k \le p$ ）为第 k 大奇异值。此外，令$s_{\min}(M) := s_p(M)$，且 $s_{\max}(M) := s_1(M)$。

由独立同分布的次高斯随机变量构成的矩阵，其奇异值具有良好的集中性，正如下一个结果所示。

命题 3.2 (次高斯矩阵的奇异值 ([Ver18, 定理 4.6。1]))。 对于 $n \ge p$，令 $M \in \mathbb{R}^{n\times p}$ 为一个行向量独立同分布、零均值、各向同性且服从次高斯分布的随机矩阵。那么对于任意 $u > 0$，包含关系

$$[s_{\min}(M), s_{\max}(M)] \subseteq [\sqrt{n} - CK^2(\sqrt{p} + t), \sqrt{n} + CK^2(\sqrt{p} + t)]$$

成立的概率至少为 $1 - 2\exp(t^2)$，其中 C 是一个普适常数。

如第 3 节开头所述，高矩阵情形所引入的左、右奇异向量的不对称性是本文面临的主要障碍。命题 3.2 部分抵消了这一影响，该命题表明，以压倒性概率，奇异值集中在以 $\Theta(\sqrt{p}$ 为中心、宽度为 $\sqrt{n}$ 的带状区域内。具体而言，当 $p = o(n$ 时，我们可以取 $t = \sqrt{p}$，此时由命题 3.2 可得

$$[s_{\min}(M), s_{\max}(M)] \subseteq [\sqrt{n} - 2CK^2\sqrt{p}, \sqrt{n} + 2CK^2\sqrt{p}] \tag{3.1}$$

成立的概率至少为 $1 - 2\exp(-p)$。这使我们能够将范围限制在较小的一组候选奇异值内。

3.3 奇异向量并不稀疏

现在，我们定义并排除本节开头所述的关于 $|v^T X|$ 的小球概率的第一个障碍。我们需要先给出几个定义。

定义 3.3 (L´évy 集中函数)。 *L´évy* 集中函数定义为

$$\mathcal{L}(X, \varepsilon) := \sup_{a\in\mathbb{R}^n} \mathbb{P}[\|X - a\| \le \varepsilon]$$

其中， $X \in \mathbb{R}^n$ 是随机向量， ε 是<样式 id='3'>(0,1) 中的邻近参数，而 $\|\cdot\|$ 是欧几里得范数。

函数 $\mathcal{L}$ 给出了随机向量集中性的上界，同时隐藏了具体的集中点。在对 $\mathcal{L}$ 作温和假设时， X 是有限的。下面的两个结果是标准结论，但我们遵循 [CLOS25]中的表述。

引理 3.4 ([CLOS25，引理 2。1])。 设 X 是一个均值为零、方差为一的次高斯随机变量。那么，对于所有 $\varepsilon \in (0, 1)$，存在一个概率 $p = p(K, \varepsilon) < 1$ 使得

$$\mathcal{L}(X, \varepsilon) \le p$$

当然，次高斯随机变量 ξ 满足矩界 $\mathbb{E}[|\xi|^q]^{1/q} \le CK\sqrt{q}$，对于所有 $q \ge 1$，其中普适常数为 C (⊢参见 [Ver18] 中的命题 2.5.2)，因此[CLOS25] 中声明依赖于 $\mathbb{E}[|\xi|^4]$ 的常数，也可以改为依赖于 K 。

下面这个引理称为张量化引理，它允许我们根据$\mathcal{L}$ 对于一个具有独立坐标的随机向量 X 的有限性，推导出 $\mathcal{L}$ 对各个坐标本身的有限性。该结果最初见于 [Ver14，引理 3。4],我们采用 [CLOS25，引理 2。2]中的版本。

引理 3.5 (张量化（[CLOS25，引理 2。2]）)。 设 X 是一个取值于 $\mathbb{R}^n$ 且具有独立坐标的随机变量。若存在一个 $\varepsilon > 0$ 和一个概率 $p \in (0,1)$ 使得

$$\mathcal{L}(X_i, \varepsilon) \le p \tag{3.2}$$

对所有 $i \in [n]$，则存在一个 $\varepsilon' = \varepsilon'(\varepsilon, p) > 0$ 以及一个概率 $p' = p'(\varepsilon, p) \in (0,\ 1)$ 使得

$$\mathcal{L}(X, \varepsilon'\sqrt{n}) \le (p')^n$$

另一个相关工具如下，它允许我们对 $\mathcal{L}$ 在 $\langle x,\ X\rangle$ 满足 $x \in S^n$ 且 X 为引理 3.5中所述的随机向量时进行界定。

引理 3.6 ([CLOS25，引理 2.3])。 设 X 是一个随机向量，其各元素相互独立、均值为零、方差为单位方差，且次高斯常数均由某个 $K < \infty$一致有界。则对所有 $\varepsilon \in (0,\ 1)$，存在一个概率 $p = p(K,\ \varepsilon) \in (0,\ 1)$，使得对所有$x \in S^{n-1}$ 都有

$$\mathcal{L}(\langle x, X\rangle, \varepsilon) \le p$$

控制小球概率的第一个障碍在于考察向量中零／近零项所占的比例。

定义 3.7 (稀疏向量与可压缩向量)。 给定 $c_0 \in (0,\ 1)$，如果向量 $x \in \mathbb{R}^n$ 的支撑至多包含 $\lfloor c_0 n \rfloor$ 个坐标，则称其为 c_0-稀疏向量，其中 x的支撑是取值为 $\ne 0$的坐标所组成的集合。

此外，给定 $c_1 > 0$，如果存在 c_0-稀疏向量 $x \in \mathbb{R}^n$ 使得 $\|y - x\| \le c_1$，则称向量 $y \in S^{n-1}$ 为 $(c_0,\ c_1)$-可压缩向量（或者在参数明确时简称为可压缩向量）。这类 y 的集合记为 $\mathrm{Comp}_n(c_0,\ c_1)$，并定义其补集$\mathrm{Incomp}_n(c_0,\ c_1) := S^{n-1} \setminus \mathrm{Comp}(c_0,\ c_1)$。

因此，如果一个向量至多只有固定比例的元素非零，它就是稀疏的；如果它在欧几里得距离意义下接近稀疏向量，它就是可压缩的。上述定义将球面划分为$S^{n-1} = \mathrm{Comp}(c_0,\ c_1) \cup \mathrm{Incomp}(c_0,\ c_1)$，而 $\mathrm{Comp}(c_0,\ c_1)$ 恰好是表示小球概率第一种障碍的向量集合。

现在我们证明，可压缩向量以高概率不是近似奇异向量。按照 [CLOS25], 中的策略，我们首先证明，对于范围如方程 (3.1) 所示的任意固定奇异值，可压缩向量都不可能是近似奇异向量。然后，我们对候选奇异值范围应用并集界，从而完成所需的论证。

根据方程 3.1 ，我们假设 $\sigma \in [\sqrt{n} - K\sqrt{p}, \sqrt{n} \mp K\sqrt{p}]$ 对某个常数成立，该常数 $K > 0$ 取决于 ξ的分布律。

引理 3.8 (右奇异向量的反集中)。 固定一个零均值、单位方差的次高斯分布 ξ。令 M 为一个元素独立同分布于 $m_{ij} \sim \xi$ 的 $n \times p$ 矩阵，并且 $p = \Theta(n^{\zeta})$

对于 $\zeta \in (0, 1)$。此外，令 $\sigma \in [\sqrt{n} - K\sqrt{p}, \sqrt{n} + K\sqrt{p}]$、 c_0、 c_1、 $c > 0$，并定义事件

$$\mathcal{C}_R := \left\{ \inf_{u \in \mathrm{Comp}_p(c_0, c_1)} \|M^\top M u - \sigma^2 u\| \le c\sqrt{np} \right\}. \tag{3.3}$$

那么存在 c_0、 c_1、 c 的正值，使得

$$\mathbb{P}[\mathcal{C}_R] \le \exp(-\Theta(p)), \tag{3.4}$$

其中 c_0、 c_1、 c 以及隐含常数仅依赖于 ξ 的分布律。

证明。 我们对 $\mathcal{C}_R$ 使用并集界。具体而言，由于可压缩向量必定接近某个稀疏向量，而每个稀疏向量的支撑由坐标的某个子集给出，因此我们对每个允许的支撑坐标子集使用并集界。

令 $\mathrm{Comp}_{p,T}(c_0, c_1)$ 表示 $\mathrm{Comp}_p(c_0, c_1)$ 中与某个支撑包含于满足 $|T| = \lfloor c_0 p \rfloor$ 的指标 $T \subseteq [p]$ 的 c_0-稀疏单位向量的距离不超过 c_1 的子集。令 T 变化，可得

$$\mathrm{Comp}_p(c_0, c_1) \subseteq \bigcup_{T \subseteq I:\, |T| = \lfloor c_0 p \rfloor} \mathrm{Comp}_{p,T}(c_0, c_1)$$

因此，定义事件

$$\mathcal{C}_{R,T} := \left\{ \inf_{u \in \mathrm{Comp}_{p,T}(c_0, c_1)} \|M^\top M u - \sigma^2 u\| \le c\sqrt{np} \right\}$$

我们有

$$\mathcal{C}_R \subseteq \bigcup_{T \subseteq I:\, |T| = \lfloor c_0 p \rfloor} \mathcal{C}_{R,T}$$

并继续对每个 $\mathcal{C}_{R,\,T}$ 进行界定。通过重新排列，我们可以假设 $T = \{1, ..., \lfloor c_0 p \rfloor\}$，并将其分解写为

$$M = (X|Y)$$

其中 X 是一个 $n \times \lfloor c_0 p \rfloor$ 矩阵，而 Y 是一个 $n \times \lceil (1 - c_0) p \rceil$ 矩阵。考察特征值项 $M^\top M u_0 - \sigma^2 u_0$ 的底部 $p - \lfloor c_0 p \rfloor$ 个坐标，我们得到

$$\|M^\top M u_0 - \sigma^2 u_0\| \ge \|Y^\top X u_0'\|$$

其中 u_0 是 $\mathrm{Comp}_{p,\,T}(c_0,\ c_1)$ 中的一个 c_0-稀疏向量，其支撑为 $\subseteq T$；而 u_0' 是由 u_0 的前 $\lfloor c_0 p \rfloor$ 个坐标构成的向量。注意，我们可以写成

$$\|Y^\top X u_0'\| = \|X u_0'\| \cdot \|Y^\top (X u_0' / \|X u_0'\|)\| \ge s_{\min}(X) \cdot \|Y^\top (X u_0' / \|X u_0'\|)\| \tag{3.5}$$

因为 u_0' 是一个单位向量。现在， X 是一个维度为 $n \times \lfloor c_0 p \rfloor$ 的次高斯矩形矩阵，因此根据命题 3.2 我们有

$$s_{\min}(X) \ge \sqrt{n} - K\sqrt{\lfloor c_0 p \rfloor} \tag{3.6}$$

以至少为 $1 - e^{-Cn}$ 的概率，对于仅取决于 ξ 的分布律的常数 K， C。现在，在控制了 $s_{\min}(X)$ 后，我们需要处理 $\|Y^\top (X u_0' / \|X u_0'\|)\|$。注意，在以

X 为条件后，

$$\|Y^\top (Xu_0'/\|Xu_0'\|)\| \geq \inf_{x\in \mathrm{span}(X):\, \|x\|=1} \|Y^\top x\|$$

这对应于 $s_{\min}(Y^\top U)$，其中 U 是一个 $n\times \lfloor c_0 p\rfloor$ 矩阵，其列构成 X 的标准正交基。注意，给定 X 时， U 是确定的。因此，给定 X 后， $Y^\top U$ 的各行是独立同分布的次高斯向量，因此

$$\|Y^\top (Xu_0'/\|Xu_0'\|)\| \geq \inf_{x\in \mathrm{span}(X):\, \|x\|=1} \|Y^\top x\| = s_{\min}(Y^\top U) \geq \sqrt{\lceil (1-c_0)p\rceil} - K\sqrt{\lfloor c_0 p\rfloor}) \quad (3.7)$$

以至少 $1-e^{-C'p}$ 的（条件）概率。将方程 3.6和 3.7代入方程 3.5，并选择 $\hat{c}>0$ 使得 $\hat{c}\sqrt{np} \leq (\sqrt{n} - K\sqrt{\lfloor c_0 p\rfloor})(\sqrt{\lceil (1-c_0)p\rceil} - \overline{K}\sqrt{\lfloor c_0 p\rfloor})$ 对充分大的 n，我们有

$$\|Y^\top (Xu_0')\| \geq \hat{c}(\sqrt{np})$$

由于 X 和 Y 相互独立，以至少 $(1-e^{-Cn})(1-e^{-Cp})$ 的概率成立。这就得到了如下结论

$$\inf_{u\in \mathrm{Comp}_{p,T}(c_0,c_1)\cap c_0-\mathrm{sparse}} \|M^\top Mu - \sigma^2 u\| \geq \hat{c}\sqrt{np} \quad (3.8)$$

以至少 $(1-e^{-Cn})(1-e^{-Cp})$ 的概率。根据反三角不等式，对于$u\in \mathsf{Comp}_{p,\ T}(c_0,\ c_1)$，我们有

$$\|M^\top Mu - \sigma^2 u\| \geq \|M^\top Mu_0 - \sigma^2 u_0\| - \|M^\top M(u-u_0) - \sigma^2(u-u_0)\|$$

现在注意到

$$\|M^\top M(u-u_0) - \sigma^2(u-u_0)\| \leq c_1 \|M^\top M - \sigma^2 I\| = c_1 \max_{1\leq i\leq p} |s_i(M)^2 - \sigma^2| \leq c_1 \Theta(\sqrt{np})$$

因为 σ 位于 $\sqrt{n}$ 周围一个宽度为 $\Theta(\sqrt{p})$ 的区间内，并且以至少 $1-e^{-c'p}$ 的概率， M 的所有奇异值也都如此。充分小地选取 c_0， $c_1>0$，我们有

$$\mathbb{P}[\mathcal{C}_{R,T}] \leq O(e^{-Cn}) + O(e^{-Cp}) \leq O(e^{-Cp})$$

上述表达式中的隐含常数均为普适常数。现在，根据斯特林近似，我们有

$$\binom{p}{c_0 p} \leq e^{H(c_0)p}$$

其中

$$H(x) := -x\log x - (1-x)\log(1-x)$$

是二元熵函数（见 [Gal14]中的定理 3.1）。利用并集界可得

$$\mathbb{P}[\mathcal{C}_R] \leq \sum_{T\subseteq[p]:\, |T|=c_0 p} \mathbb{P}[\mathcal{C}_{R,T}] \leq 2e^{H(c_0)p - Cp}$$

其中有 $c=\hat{c}-c_1$。注意，由于 $\hat{c}$ 不依赖于 c_1，且减小 c_1 只会改善我们的集中性，因此我们可以选择足够小的 c_1，使得 $c>0$。至此，论证完成。 □

现在我们来证明左奇异向量的一个类似结论。与右奇异向量不同，

在右奇异向量的情形中，奇异向量作用到的第一个矩阵具有有利的维数；而在这里，第二个矩阵具有有利的性质，因此我们需要更仔细地给出下界。

引理 3.9 (左奇异向量反集中)。 固定一个零均值、单位方差的次高斯分布 ξ。设 M 是一个元素独立同分布且服从 $m_{ij} \sim \xi$ 的 $n \times p$ 矩阵，并且满足 $p = \Theta(n^{\zeta})$，其中$\zeta \in (0,\ 1)$。此外，设 $\sigma \in [\sqrt{n} - K\sqrt{p}, \sqrt{n} + K\sqrt{p}]$ 和 c_0、c_1、$c > 0$，并定义事件

$$\mathcal{C}_L := \left\{ \inf_{u \in \mathrm{Comp}_n(c_0,c_1)} \|MM^\top u - \sigma^2 u\| \le cn \right\}. \tag{3.9}$$

那么存在正数 c_0、c_1、c，使得

$$\mathbb{P}[\mathcal{C}_L] \le \exp(-\Theta(n)), \tag{3.10}$$

其中 c_0、c_1、c 以及隐含常数仅取决于 ξ 的分布律。

证明。 与处理右奇异向量的方法类似，令 $\mathrm{Comp}_{n,T}(c_0, c_1)$ 表示 $\mathrm{Comp}_n(c_0, c_1)$ 的子集，其中的向量与某个 c_0-稀疏单位向量的距离不超过 c_1，且该单位向量的支撑包含于满足 $|T| = \lfloor c_0 n \rfloor$ 的指标$T \subseteq [n]$ 中。令 T 变化，可得

$$\mathrm{Comp}_n(c_0, c_1) \subseteq \bigcup_{T \subseteq I:\, |T| = \lfloor c_0 n \rfloor} \mathrm{Comp}_{n,T}(c_0, c_1)$$

因此定义这些事件

$$\mathcal{C}_{L,T} := \left\{ \inf_{v \in \mathrm{Comp}_{n,T}(c_0,c_1)} \|MM^\top v - \sigma^2 v\| \le cn \right\}$$

我们有

$$\mathcal{C}_L \subseteq \bigcup_{T \subseteq I:\, |T| = \lfloor c_0 n \rfloor} \mathcal{C}_{L,T}$$

并可以继续对每个$\mathcal{C}_{L,\ T}$进行界定。通过重新排列，我们可以假设 $T = \{1, ..., \lfloor c_0 n \rfloor\}$，并写出分解

$$M = \begin{pmatrix} X \\ \hline Y \end{pmatrix}$$

其中 X 是一个 $\lfloor c_0 n \rfloor \times p$ 矩阵，而 Y是一个 $\lceil (1 - c_0) n \rceil \times p$ 矩阵。我们有

$$\|MM^\top v_0 - \sigma^2 v_0\| = \|YX^\top v_0' + XX^\top v_0' - \sigma^2 v_0'\| = \|YX^\top v_0'\| + \|XX^\top v_0' - \sigma^2 v_0'\| \tag{3.11}$$

其中 v_0是 $\mathrm{Comp}_{n,\ T}(c_0,\ c_1)$ 中的一个 c_0-稀疏向量，支撑为 $\subseteq T$；而 v_0'是由 v_0的前 $\lfloor c_0 n \rfloor$个坐标构成的向量。

在 X的条件下，令 $v_\perp$为 v_0'在 $X^\top$的核上的投影，并定义$v_\parallel := v_0' - v_\perp$。方程3.11两边平方后可得下界

$$\begin{aligned} \|MM^\top v_0 - \sigma^2 v_0\|^2 &\ge \|YX^\top v_\parallel\|^2 + \|XX^\top (v_\perp + v_\parallel) - \sigma^2 (v_\perp + v_\parallel)\|^2 \\ &= \|YX^\top v_\parallel\|^2 + \|(XX^\top v_\parallel - \sigma^2 v_\parallel) - \sigma^2 v_\perp\|^2 \\ &= \|YX^\top v_\parallel\|^2 + \|(XX^\top v_\parallel - \sigma^2 v_\parallel)\|^2 + \|\sigma^2 v_\perp\|^2 \\ &\ge \|YX^\top v_\parallel\|^2 + \|\sigma^2 v_\perp\|^2 \end{aligned}$$

根据第二个等号处应用正交性可得。该 $v_\perp$ 项使我们能够兼顾$v_\parallel$ 可能较小的情况。现在，由于 $X^\top$ 的行空间由 $X^\top$ 中仅对应于非零奇异值的奇异向量张成，按照引理3.8中的技巧，可得

$$\|YX^\top v_\parallel\| \geq \|v_\parallel\| \cdot s_{\min}(X) \cdot s_{\min}(Y)$$

因此，合并可得

$$\|MM^\top v_0 - \sigma^2 v_0\|^2 \geq \|v_\parallel\|^2 \cdot (s_{\min}(X)^2 \cdot s_{\min}(Y)^2) + \sigma^4 \|v_\perp\|^2$$

由于 v_0' 是单位向量，该下界以至少 $(1-e^{-Cn})^2$ 的概率成立，并且是一些 $\Theta(n^2)$ 项的凸组合。因此，存在某个 $\hat{c} > 0$ （与 c_1无关），使得以至少 $(1-e^{-Cn})^2$的概率有 $\hat{c}^2 n^2 \leq \min(s_{\min}(X)^2 \cdot s_{\min}(Y)^2)$。

。由于 v_0'在 $\mathsf{Comp}_{n,T}(c_0, c_1) \cap c_0$–稀疏范围内是任意的，我们通过观察到在整个簇上都一致地以至少 $(1-e^{-Cn})^2$ 的概率有以下结论，将结果推广到 $\mathsf{Comp}_{n,T}(c_0, c_1)$的全部范围：

$$\|MM^\top u - \sigma^2 u\| \geq \|MM^\top u_0 - \sigma^2 u_0\| - \|MM^\top (u-u_0) - \sigma^2 (u-u_0)\| \geq \hat{c}n - c_1\Theta(n)$$

同样由 σ^2和 $\|M\|$的上界可得。对簇 $\mathsf{Comp}_{n,T}(c_0, c_1)$应用并集界，并使用斯特林近似，可得

$$\mathbb{P}[\mathcal{C}_L] \leq 2e^{H(c_0)n - Cn}$$

这里我们再次选择足够小的 c_0, c_1，并令 $c = \hat{c} - c_1$；注意到 $c > 0$，因为 $\hat{c}$ 与 c_1 独立，而且 c_1 可以任意小。 □

引理 3.8 和 3.9 之间一个重要的区别是，前者需要对 M 的奇异值集中性进行更精细的控制，而后者不需要。

注意，在引理 3.8 和 3.9 中，减小 c_0, c_1, c 这些量只会提高集中概率，因此我们可以为右奇异向量和左奇异向量选取相同的相关常数。事实上，定理 3.8 和 3.9的证明通过选取 c （它依赖于 c_1）来证明适当常数的存在；随后可以利用测度的单调性减小 c，并利用集合包含关系的单调性减小 c_0, c_1 。

现在，我们可以以压倒性概率排除第一个小球障碍。

命题 3.10 （可压缩奇异向量不太可能出现）。 令 $\mathcal{G}$ 表示如下事件：存在向量 $u \in \mathrm{Comp}^p(c_0, c_1)$ 和数值 $\sigma^2 > 0$，使得 $M^\top M u = \sigma^2 u$，并且$u \in \mathrm{Comp}^p(c_0, c_1)$ 或 $Mu = v \in \mathrm{Comp}^p(c_0, c_1)$。那么

$$\mathbb{P}[\mathcal{G}] \leq \exp(-\Theta(p))$$

当 n 充分大时，且隐含常数仅依赖于 ξ 的分布律。

证明。 策略是对候选奇异值集合进行某种离散化，通过定理 3.8 和3.9处理该离散化中的每个固定点，最后通过并集界得出结论。因此，这是针对奇异值的网论证。

令 $\mathcal{G}_R$ 表示存在命题陈述中所述的可压缩右奇异向量，令 $\mathcal{G}_L$ 表示左奇异向量事件，使得 $\mathcal{G} = \mathcal{G}_R \cup \mathcal{G}_L$。我们处理

右奇异向量，因为左侧情形可用完全相同的方法证明。

假设存在这样的 $u \in \mathrm{Comp}^p(c_0, c_1)$ 和 σ^2，并令 σ_0^2 为$c\sqrt{np}$（其中 c 如引理 3.8所示）范围内的一个整数倍 $[(\sqrt{n}-K\sqrt{p})^2,(\sqrt{n}+K\sqrt{p})^2]$。那么，这样的值有$O(2K\sqrt{np})/c\sqrt{np}$ 个，并且 $|\sigma^2-\sigma_0^2| \le c\sqrt{np}$，因此我们有

$$\|M^\top Mu - \sigma_0^2 u\| = |\sigma^2 - \sigma_0^2| \le c\sqrt{np}$$

根据引理 $-\Theta(p)$)，该事件发生的概率至多为 exp(3.8。对 σ_0^2 的多项式多个取值应用并集界，可得

$$\mathbb{P}[\mathcal{G}_R] \le \exp(-\Theta(p))$$

当 n 充分大时成立，其中隐含常数仅取决于 ξ的分布律。通过类似的论证并运用引理3.9 ，我们得到

$$\mathbb{P}[\mathcal{G}_L] \le \exp(-\Theta(n))$$

同样，隐含常数仅取决于 ξ 的分布律。最后应用并集界即可得到所述结论。

□

本节最后给出几点注释。

注 3.1 (上界的表面性与网格粒度)。 请注意，引理 3.8 和 3.9 中关于下确界的特定上界大多只是表面上的。一旦能够证明相关下确界以至少 $\le n^\alpha$ 的概率满足 $\alpha \in \mathbb{R}$，其中 $1-\exp(-\Theta(p))$，那么 α 的影响就仅体现在奇异值网格的大小上；通过并集界引入的一个 $n^{-\xi'}$ 乘法因子，最终会被固定 σ 事件的指数级小概率所压倒。具体阈值仅仅是技术局限所致。

注 3.2 （网技术）。 注意，在 [CLOS25] 中，作者利用可压缩向量上的一个网证明了其引理3.8 和 3.9的对应版本。我们推测，若在这一论证中补充方程 3.1 提供的额外奇异值信息，以及引理3.8中更精细的下界，就足以得到命题3.10。

本文选择采用支撑集并合论证，而非网并合论证，因为前者略为简单，能得到稍精细一些的结果和更强的中间结论，对指数收敛速率关于 c_0 的依赖关系更优，且该速率不依赖于 c_1。尤其是，支撑集并合界使我们能够考虑c_0 和 c_1 变化的情形，而这会受到网并合乘法项（$9/c_0c_1$）^{c_0n}的限制。

3.4 左奇异向量不具有强加性结构

小球概率的第二个障碍，即加性结构的存在，可以用一个称为最小公分母（LCD）的概念来量化，该概念由 [RV08]提出。继 [CLOS25], 之后，我们使用一种称为正则化LCD 的变体。

定义 3.11 （LCD 和正则化 LCD）。 设 $\kappa > 0$ 和 $\gamma \in (0,\ 1)$。对于单位向量 $x \in S^{n-1}$，我们将 $\mathrm{LCD}_{\kappa,\ \gamma}(x)$ 定义为

$$\mathrm{LCD}_{\kappa,\gamma}(x) := \inf\{\theta > 0 :\ \mathrm{dist}(\theta x, \mathbb{Z}^n) < \min(\gamma\|\theta x\|, \kappa)\}$$

此外，对于 $\alpha \in (0,\ c')$，给定 $c' = c_0 c_1^2/4$、$0 < \alpha < c'/4$ 和 $\frown x \in$ 不可压缩集$_n(c_0,\ c_1)$，我们定义正则化 ***LCD***，记作 $\mathrm{LCD}_{\kappa,\ \gamma}(x,\ \alpha)$，其定义为

$$\widehat{\mathrm{LCD}}_{\kappa,\gamma}(x,\alpha) \coloneqq \sup\{\mathrm{LCD}_{\kappa,\gamma}(x_I/\|x_I\|) : I \subseteq \mathrm{spread}(x),\ |I| = \lceil \alpha n \rceil\}$$

其中

$$\mathrm{spread}(x) \coloneqq \{i \in [n] :\ \frac{c_1}{\sqrt{2n}} \le |x_i| \le \frac{1}{\sqrt{c_0 n}}\}$$

$\mathrm{LCD}_{\kappa,\gamma}(x)$ 找到满足以下条件的最小 $\theta > 0$：θx近似取整数值。这描述了 x 的元素在多大程度上近似嵌入某个等差数列中。κ 用于设定“近似”的概念，而 $\gamma\|\theta x\|$ 则防止用偏离 x 很多的 $\widehat{\ }$ 整数向量方向来近似 θx。$\mathrm{LCD}_{\kappa,\gamma}(x,\alpha)$ 是 $\mathrm{LCD}_{\kappa,\gamma}(x)$ 的一个更稳健版本；由于 $x \in S^{n-1}$，$\mathrm{LCD}_{\kappa,\gamma}(x)$ 可能仅仅因为 x 的元素“分散开来”，而非具有真正的算术结构，就取较大值。因此，$\mathrm{LCD}_{\kappa,\gamma}(x,\alpha)$ 会考察 x 所有这类充分分散的子集上的算术结构。更详尽的讨论见 [Rud10]。

以　　下内容描述了正则化 LCD 对集中性的定量影响。

引理 3.12 ([CLOS25, 引理 4.1])**.** 设 X 是一个取值于 $\mathbb{R}^n$ 的随机向量，其坐标独立同分布，并假设存在 $\varepsilon_0, p_0 > 0$ 使得 $\mathcal{L}(X_i, \varepsilon_0) \le 1 - p_0$ 对所有 $i \in [n]$ 均成立。若 $x \in$ 不可压缩集 $_n(c_0, c_1)$ 且 $\kappa > 0$，若 ε 满足

$$\varepsilon \ge \frac{\sqrt{\alpha}}{c_0 \widehat{\mathrm{LCD}}_{\kappa,\gamma}(x,\alpha)}$$

then

$$\mathcal{L}(\langle X, x\rangle, \varepsilon) \le C\left(\frac{\varepsilon}{\gamma c_1 \sqrt{\alpha}} + e^{-\Theta(\kappa^2)}\right) \tag{3.12}$$

其中隐含常数仅取决于 X_1的分布律。

请注意，在我们的设定中，上述常数仅与用于构造矩阵 M 的各个随机变量有关，因此是固定的。

由于较小的 $\widehat{\ }$ LCD 表示强加性结构，因此我们旨在证明左奇异向量的 LCD 以高概率具有下界。回顾一下，对于度量空间 (X, d)，子集 $S \subseteq X$ 的 ε-网是一个子集 $\mathcal{N} \subseteq S$，满足对于所有 $s \in S$，若 $d(\mathcal{N}, s)$，则 $< \varepsilon$。网是构造并集界论证的有用结构，以下结果给出了关于正则化 LCD 的次水平集的 ε-网大小的上界。

引理 3.13 ([NTV17，引理 B.1])。考虑 $D \ge 1$ 和 $n^{-c} \le \alpha \le c'/4$。我们用 S_D表示次水平集

$$S_D \coloneqq \left\{x \in \mathrm{Incomp}_n(c_0, c_1) :\ \widehat{\mathrm{LCD}}_{\kappa,\gamma}(x,\alpha) \le D\right\}$$

S_D 有一个$\frac{\kappa}{D\sqrt{\alpha}}$-网 $\mathcal{N}$，满足

$$|\mathcal{N}| \le \frac{C^n D^{n+2/\alpha}}{(\alpha n)^{c'n/4}}$$

其中，C 是一个普适常数。

上述结果的一个更精细版本考虑了子水平集的一个切片，从而能够更严格地控制并集界。

引理 3.14 ([CLOS25，定义 4。6])。 类比引理 *3.13*，我们定义水平集切片

$$S_{D,k} \coloneqq \left\{ x \in \mathrm{Incomp}_n(c_0, c_1) : 2^{-(k+1)} D \le \widehat{\mathrm{LCD}}_{\kappa,\gamma}(x, \alpha) \le 2^{-k} D \right\}$$

其中 $k \in [0, \text{对数}_2\, D]$，它有一个 $\frac{2^k \kappa}{D\sqrt{\alpha}}$-网 $\mathcal{N}$，满足

$$|\mathcal{N}| \le \frac{C^n D^{n+2/\alpha}}{(\alpha n)^{c'n/4}} 2^{-kn-(2k/\alpha)}$$

其中 C 是一个普适常数。

现在，我们排除具有低 LCD 的左奇异向量。在 [CLOS25], 中，作者主要关注一般矩阵族 $\Sigma^{1/2}M$ （其中 Σ 为正定矩阵）的奇异值，并通过左奇异向量的高 LCD 界以及右奇异向量的不可压缩性来实现排斥。然而，由于 $p = \Theta（n）$ 范围内的对称性，作者也能够并且确实证明了右奇异向量的高 LCD 界，从而得到了关于矩阵 $M\Sigma^{1/2}$的类似排斥结论。在我们的设定中，既没有必要，也无法凭借当前技术建立 M的右奇异向量的高 LCD 界；我们将在引理 3.16之后讨论这一障碍。

首先，我们需要 [CLOS25]中的一个结果；以下结论可从引理 4.4 的证明中提取。

引理 *3.15*（[*CLOS25*，引理 *4.*4] 的一半）。设 ξ 是一个零均值、单位方差的次高斯分布。令 M 为一个元素独立同分布且服从 $m_{ij} \sim \xi$ 的 $n \times p$ 矩阵，并且对于 $\zeta \in \in (0, 1)$，满足 $p = \Theta(n^{\zeta})$。回顾 $c' = c_0 c_1^2/4$。那么存在常数 $C > 0$，其仅依赖于 ξ 的分布律，使得对于任意 $x \in \in$不可压缩集$_p(c_0, c_1)$ 和 $y \in \in$不可压缩集$_n(c_0, c_1)$，$0 < \alpha < c'/4$，以及满足下述条件的 $\varepsilon > 0$

$$\varepsilon \ge \frac{\sqrt{\alpha}}{c_0 \widehat{\mathrm{LCD}}_{\kappa,\gamma}(x, \alpha)}$$

那么我们有

$$\sup_{a \in \mathbb{R}^n} \mathbb{P}[\{\|Mx - a\| < \varepsilon\sqrt{n}\}] \le C\left(\frac{\varepsilon\sqrt{2}}{\gamma c_1 \sqrt{\alpha}} + e^{-\Theta(\kappa^2)} \right)^{n - \lfloor \alpha n \rfloor}$$

现在，我们可以排除近似左奇异向量具有低最小公分母的情形，其目标奇异值固定，且参数范围类似于 [CLOS25]。

引理 3.16。设 M 满足定理 *3.15* 的假设。存在某个 $c > 0$，其仅依赖于 c_0 和 c_1，使得对于任意固定的 $\sigma_0^2 \in [(\sqrt{n} - K\sqrt{p})^2, (\sqrt{n} + K\sqrt{p})^2]$ 以及任意固定的 $a \in \mathbb{R}^n$，在以下限制条件下

$$\kappa = n^c,\ D \le (\kappa)^{1/\alpha},\ \alpha \ge 1/\sqrt{\kappa}$$

我们有，且

$$\beta = \frac{\kappa}{\sqrt{\alpha} D}$$

该事件

$$\mathcal{E} \coloneqq \{\exists (u, v) \in \mathrm{Incomp}(c_0, c_1) \times S_D : \|Mu - \sigma_0 v - a\| \le \beta\sqrt{n}\}$$

的概率至多为$\exp(-O(n\log\ n))$，其中隐含常数仅取决于 ξ的分布律，

，且 S_D 表示LCD 子水平集。

证明。我们可以将 $\mathcal{E}$ 分解为事件 $\mathcal{E}_k$，表示 $\mathcal{E}$ 在 $v \in S_D$ 时发生，k 如引理 3.14 中所述。我们进一步将 $\mathcal{E}_k$ 分解为事件 $\mathcal{E}_{k,-}$ 和 $\mathcal{E}_{k,+}$，分别表示 $\mathcal{E}$ 成立，且 $\mathrm{LCD}_{\kappa,\gamma}(v,\alpha) \le \mathrm{LCD}_{\kappa,\gamma}(u,\alpha)$，以及 $\mathrm{LCD}_{\kappa,\gamma}(v,\alpha) \ge \mathrm{LCD}_{\kappa,\gamma}(u,\alpha)$。最后，我们将 $\mathcal{E}_{k,+}$ 分解为事件 $\mathcal{E}_{k,+,l}$，其中 $1 \le l \le k$ 表示 $u \in S_{D,l}$。该分解可概括为

$$\mathcal{E} \subseteq \bigcup_{1\le k\le \log D}\left(\mathcal{E}_{k,-} \cup \left(\bigcup_{1\le l\le k}\mathcal{E}_{k,+,l}\right)\right)$$

并对每个单独的事件分别进行界定。首先，考虑 $\mathcal{E}_{k,-}$。那么 $\widehat{\mathrm{LCD}}_{\kappa,\gamma}(x,\alpha) \ge D2^{-(k+1)}$，我们选取一个左侧水平集切片的 (β_k)-网，记为 $\mathcal{L}_k$，以及一个超水平集的 (β_k)-网，记为 $\mathcal{R}_k$，使其基数满足以下界

$$|\mathcal{L}_k| \le \frac{(CD)^n}{(2^k)^n(\sqrt{\alpha n})^{c'n/2}}(2^{-k}D)^{2/\alpha},\ |\mathcal{R}_k| \le \left(\frac{C}{\beta_k}\right)^p$$

根据标准球面界和引理3.14。此外，定义

$$\beta_k = \frac{2^k\kappa}{\sqrt{\alpha}D}$$

不失一般性，我们可以假设左侧网和右侧网中的元素分别属于子水平切片集和子水平集。现在，注意在事件 $\mathcal{E}_{R,k}$ 即存在某个u_0，$v_0 \in \mathcal{R}_k \times \mathcal{L}_k$ 使得

$$\begin{aligned}\|Mu_0 - \sigma_0 v_0 - a\| &\le \|M(u-u_0)\| + \sigma_0\|v-v_0\| + \|Mu - \sigma_0 v - a\| &(3.13)\\ &\le \|M\|\beta_k + \sqrt{n}\beta_k + \beta_R\sqrt{n} = O(\beta_k\sqrt{n}) &(3.14)\end{aligned}$$

并且

$$\varepsilon = \beta_k = \frac{2^k\kappa}{\sqrt{\alpha}D} \ge \frac{\sqrt{\alpha}}{\widehat{\mathrm{LCD}}_{\kappa,\gamma}(u_0,\alpha)}$$

结合起来，t 这些事实使并集界变得可行。应用引理 3.15可得

$$\begin{aligned}\mathbb{P}[\mathcal{E}_{L,k,-}] \le C_5&\left(\frac{C}{\beta_k}\right)^p\\ &\times\left(\frac{(CD)^n}{(2^k)^n(\sqrt{\alpha n})^{c'n/2}}(2^{-k}D)^{2/\alpha}\right)\\ &\times\left(\frac{\varepsilon\sqrt{2}}{\gamma c_1\sqrt{\alpha}} + e^{-\Theta(\kappa^2)}\right)^{n-\lfloor\alpha n\rfloor}\end{aligned}$$

现在，注意到

$$\begin{aligned}
\Big(①\Big) &= \left(\frac{C}{\beta_k}\right)^p = \exp(\pm O(p\log n))\\
\Big(②\Big) &= \left(\frac{(CD)^n}{(2^k)^n(\sqrt{\alpha n})^{c'n/2}}(2^{-k}D)^{2/\alpha}\right) = \exp(\pm O(n\log n))\\
\Big(③\Big) &= \left(\frac{\varepsilon\sqrt{2}}{\gamma c_1\sqrt{\alpha}} + e^{-\Theta(\kappa^2)}\right)^{n-\lfloor\alpha n\rfloor} = \exp(\pm O(n\log n))
\end{aligned}$$

因此，我们可以放心地忽略项 1○，并处理项 2○ 和 3○。对于充分大的 n，我们有

$$\begin{aligned}
\Big(②\Big)\cdot\Big(③\Big) &\le \left(\frac{(CD)^n}{(2^k)^n(\sqrt{\alpha n})^{c'n/2}}(2^{-k}D)^{2/\alpha}\right)\cdot\left(\frac{2^k\kappa\sqrt{2}}{\gamma c_1\alpha D} + e^{-\Theta(\kappa^2)}\right)^{n-\lfloor\alpha n\rfloor}\\
&= \frac{2^{(n-\lfloor\alpha n\rfloor)/2}C^n D^{\lfloor\alpha n\rfloor+2/\alpha}\kappa^{n-\lfloor\alpha n\rfloor}}{(2^k)^{\lfloor\alpha n\rfloor+2/\alpha}\alpha^{c'n/4+n-\lfloor\alpha\rfloor}n^{c'n/4}(c_1\gamma)^{n-\lfloor\alpha n\rfloor}}\\
&= \frac{2^{(n-\lfloor\alpha n\rfloor)/2}C^n}{(2^k)^{\lfloor\alpha n\rfloor+2/\alpha}\alpha^{c'n/4+n-\lfloor\alpha n\rfloor}(c_1\gamma)^{n-\lfloor\alpha n\rfloor}}\cdot\frac{D^{\lfloor\alpha n\rfloor+2/\alpha}\kappa^{n-\lfloor\alpha n\rfloor}}{n^{c'n/4}}\\
&\le \frac{2^{(n-\lfloor\alpha n\rfloor)/2}C^n}{(2^k)^{\lfloor\alpha n\rfloor+2/\alpha}(c_1\gamma)^{n-\lfloor\alpha n\rfloor}}\cdot\frac{D^{\lfloor\alpha n\rfloor+2/\alpha}\kappa^{n-\lfloor\alpha n\rfloor+(c'n/4+n-\lfloor\alpha n\rfloor)/2}}{n^{c'n/4}}\\
&\le \frac{2^{(n-\lfloor\alpha n\rfloor)/2}C^n}{(2^k)^{\lfloor\alpha n\rfloor+2/\alpha}(c_1\gamma)^{n-\lfloor\alpha n\rfloor}}\cdot\frac{n^{c(n+n^c+n-\lfloor\alpha n\rfloor+(c'n/4+n-\lfloor\alpha n\rfloor)/2)}}{n^{c'n/4}}\\
&= \Big(ⓐ\Big)\cdot\Big(ⓑ\Big)
\end{aligned}$$

考察 b○，我们发现，选择足够小的 cs 后，(2○) ·(3○) = exp(−O(nlog n))，因为 a○ 有一个上界 exp(O(n))，其中隐含常数与 k 独立。特别地，我们要求 $c < 1$，以确保分子为 exp(O(nlog n))。

上述论证证明了 $\mathbb{P}[\mathcal{E}_{L,k,+}] \le$ exp(−O(nlog n))，其中隐含常数仅依赖于 ξ，特别是与 k 独立。为处理事件 $\mathcal{E}_{L,\ k,\ +,\ l}$，我们用网参数 ($\beta_l$)，并在两侧使用精细化的 LCD 切片网，重复上述论证。这只会使上界更强，因此我们得到一个 exp(−O(nlog n)) 上界，其隐含常数与 l 和 k 独立。

现在，事件 $\mathcal{E}_{L,k,-}$有 log D 个，事件 $\mathcal{E}_{L,k,+}$有 log D(log $D+1$)/2 个，因此通过并集界，可得到 $\mathcal{E}_L$ 的上界，其量级为 exp(−O(nlog n))，从而完成证明。

□

关于定理 3.15 的证明，有几点值得说明。首先，若将定理 3.15 与 [CLOS25]，中的命题 4.8 相比较，就会发现我们的证明对于左、右奇异值并不对称，但也没有完全解耦。注 3.3 讨论了为何我们仍需在一定程度上处理右奇异向量；注 3.4 则说明为何此处也不需要 [CLOS25] 中命题 4.8 所具有的完全对称性。其次，注3.5说明了为何我们目前的方法无法证明右奇异向量的强 LCD 下界。

注记 3.3 (右 定理中涉及的向量3.16）。鉴于根据假设，候选 e

定理陈述中涉及的向量3.16 均为不可压缩向量，因此不难看出，无法找到一种统一结构来划分不可压缩集并应用并集界n ，故我们采用网论证。现在，对于左奇异向量的陈述，任何单侧网自然都应包含一个指数为 $\Theta(n)$ 的网，但结合定理3.12 与定理3.5 ，预计得到的概率指数为 $\Theta(p)$ 。这样的论证似乎不够充分，而引入右奇异向量是为了得到一个阶数合适的概率项。

注 3.4 (引理 3.16 的不对称性)。 请注意，在定理3.16中，上界由三项组成：一个左侧网、一个右侧网，以及一个概率项。这个证明完全可以仿照 [CLOS25] 中命题 4.8 的做法，采用定理3.15 的双管齐下版本，并推导出方程 (3.13的左侧对应式。不过，第二个概率项的指数为 $\Theta(p)$，因此整个项渐近地被项（ 2◯）·(3◯) 所支配，因而变得无关紧要。此外，可以验证，方程 (3.13的左侧对应式会使左侧概率中出现一个 $\varepsilon = \Theta(n/p)$，因此概率界会随着 $n \to \infty$而发散，尽管渐近上无害，却会实际削弱上界。在 [CLOS25]中，界中的四项阶数相同，且两个概率项都有帮助，这也解释了他们为何采用双管齐下方法。

注 3.5 （关于右奇异向量的信息）。 请注意，精细网项对于证明概率收敛至关重要，而且 仅 在左奇异向量情形中，才会按适当的指数放大。若在右侧情形中重复定理 3.16，或者采用注3.4 中所述的双管齐下方法，精细网就无法拥有适当的指数。

此外，此时只有来自右奇异向量的概率项有助于证明，因此我们必须始终确保右侧有 LCD 下界。为此，我们对右侧子水平集进行切片。这并不等同于 [CLOS25]中命题 4 8 的右侧事件证明。该证明处理的是这样一种情形：对于 $\mathrm{LCD}_{\gamma,\kappa}(u, \widehat{\alpha}) < \mathrm{LCD}_{\gamma,\kappa}(v, \widehat{\alpha})$ 的右左配对 (u, v)， v 的 LCD 可以任意大；但定理 3.16 仅在 v的 LCD 有多项式上界时才能确立这一事实，这不足以得出结论：以压倒性概率，任何右奇异向量的 LCD 都是多项式级别的大。

现在，w e 可以在右奇异向量上建立多项式级别的 LCD 下界 .

命题3.17。 令 M 满足定理*1.3*的假设，并令 α、 κ 和 c 满足定理*3.16*的假设。则以至多$\exp(-O(p))$ 的概率，任意 M 的左奇异向量 w 都满足 $\widehat{\mathrm{LCD}_{\kappa,\gamma}(w、\ \alpha)} \geq n^{c/\alpha}$。

证明。 根据定理3.10 ，左奇异向量或右奇异向量是可压缩的概率至多为 $\exp(-O(p))$。

假设 w 是与不可压缩右奇异向量 v 及奇异值 σ相关联的不可压缩左奇异向量。选取区间 $[\sqrt{n} - K\sqrt{p}, \sqrt{n} + K\sqrt{p}]$上间距为 $\beta\sqrt{n}$ 的网格，则存在一个网格值 σ_0，使得 $|\sigma - \sigma_0| < \beta\sqrt{n}$ 的概率至少为 $1 - \exp(-O(p))$，因此

$$\|Mv - \sigma_0 u\| \leq \beta\sqrt{n}$$

通过对 σ_0 取并集界，并应用定理3.16 即可得出该结论。 □

定理 3.10和定理 3.17 推出了以下定理，该定理排除了大额小球概率的主要障碍，从而确保特征值排斥。

定理 3.18. 设 M 满足定理 *1.3*的假设，并设 α, κ 和 c 满足定理 *3.16*的假设。那么，以至少 $1-\exp(-O(p))$ 的概率，有

1. 左、右奇异向量均不可压缩（其中 c_0 和 c_1 与定理 *3.10*中相同）。
2. 左奇异向量满足 $\widehat{\text{LCD}}$ 下界 $n^{c/\alpha}$。

注意，与 [CLOS25], 类似，在多项式下界的指数中加入乘法项 $1/\alpha$，当 α 随 n衰减时，可以证明极强的下界。不过，对于最终的特征值排斥结果，我们只要求 α 是某个较小的常数。事实上，如果愿意将3.16 限制为不超过 D 的上界，则可以稍微简化定理 $n^{O(1)}$的证明。

3.5 高矩形 Wishart 矩阵具有定量特征值排斥

现在我们将 运用 [NTV17] 和 [CLOS25]的技术，总结主要的特征值排斥结果。

定理 3.19 (高实 Wishart 矩阵的平方奇异值排斥)。 设 M 满足定理 *1.3*的假设。存在一个 $c \in (0,1)$，使得对于 α 和 κ 满足定理 *3.18*的假设，且 $\delta \geq n^{-c/\alpha}$时，事件

$$\mathcal{E}_i := \{\sigma_i^2(M) - \sigma_{i+1}^2(M) \leq \sigma_{i+1}(M) \cdot \delta \cdot p^{-1/2}\}$$

满足

$$\sup_{1\leq i\leq p} \mathbb{P}[\mathcal{E}_i] \leq O(\frac{\delta}{\sqrt{\alpha}}) \tag{3.15}$$

其隐含常数仅依赖于 c_0、 c_1 和 ξ 的分布律。此外，事件

$$\mathcal{F}_i := \{\sigma_i^2(M) - \sigma_{i+1}^2(M) \leq (\sqrt{n} - K\sqrt{p}) \cdot \delta \cdot p^{-1/2}\}$$

满足

$$\sup_{1\leq i\leq p} \mathbb{P}[\mathcal{F}_i'] \leq \sup_{1\leq i\leq p} \mathbb{P}[\mathcal{F}_i] \leq O(\frac{\delta}{\sqrt{\alpha}}) + \exp(-\Theta(p)) \tag{3.16}$$

证明。 固定某个 $1 \leq i \leq p$。将矩阵 M 分解为

$$M = (M'|X)$$

其中 X 是第 p 列，而对应于 M 的第 i 个奇异值的右奇异向量为

$$u = \begin{pmatrix} u' \\ b \end{pmatrix}$$

此外，定义事件

$$\mathcal{E}_i' := \{\sigma_i^2(M) - \sigma_{i+1}^2(M') \leq \sigma_{i+1}(M') \cdot \delta \cdot p^{-1/2}\}$$
$$\mathcal{F}_i' := \{\sigma_i^2(M) - \sigma_{i+1}^2(M') \leq (\sqrt{n} - K\sqrt{p}) \cdot \delta \cdot p^{-1/2}\}$$

于是，奇异值方程可以写为

$$\begin{pmatrix} M'^\top M' & M'^\top X \\ X^\top M' & X^\top X \end{pmatrix} \begin{pmatrix} u' \\ b \end{pmatrix} = \sigma_i^2(M) \begin{pmatrix} u' \\ b \end{pmatrix}$$

上述方程的前 $p-1$ 行等价于

$$M'^\top M' u' - \sigma_i^2(M) u' = -M'^\top X b$$

令 $\hat{u}$ 为 M' 的第 i 个奇异值对应的右奇异向量，在左侧乘以 $\hat{u}$ 的转置，可得

$$(\sigma_i^2(M') - \sigma_i^2(M)) \hat{u}^\top u' = -b\sigma_i(M') \hat{w}^\top X$$

其中，$\hat{w}$ 是 M' 对应于 $\sigma_i(M')$ 的左奇异向量。取绝对值，并对左侧应用柯西-施瓦茨不等式，可得不等式

$$|\hat{w}^\top X| \le \left| \frac{\sigma_i^2(M') - \sigma_i^2(M)}{b\sigma_i(M')} \right|$$

因此，在事件 $\mathcal{E}_i'$ 上，我们有

$$|\hat{w}^\top X| \le \left| \frac{\delta p^{-1/2}}{b} \right|$$

其中 X 与 w 的左奇异向量独立，而 M'，b 是 M 的右奇异向量的一个坐标。由于 $u \in$ 不可压缩集$_p(c_0,\ c_1)$ 良好分散（按照定理 3.11 的意义），因此，以至少 $1-\exp(-O(p))$ 的概率，我们有至少 $c_0 c_1^2 p/2$ 个坐标的 u 的绝对值不小于 $c_1 p^{-1/2}/\sqrt{2}$。参照 [CLOS25]，我们定义阈值和事件:

$$B \coloneqq c_1 p^{-1/2}/\sqrt{2}\,, \mathcal{G}_{ij} \coloneqq \mathcal{E}_i \wedge \{u_j \ge B\}\,, p_B \coloneqq |\{j : u_j \ge B\}|$$

其中 p_B 可写为 $\sum_{j=1}^p l_j$，其中 l_j 是事件 $\{u_j \ge B\}$的指示函数。将事件 $\mathcal{E}_i'$分解后，利用单调性并应用马尔可夫不等式可得，对任意 $N \ge 1$，有

$$\mathbb{P}[\mathcal{E}_i'] \le \frac{p}{N} \mathbb{P}[\mathcal{G}_{ip}] + \mathbb{P}[p_B < N]$$

因为对所有 $1 \le i,\ j \le p$，都有 $\mathbb{P}[\mathcal{G}_{ij}] = \mathbb{P}[\mathcal{G}_{ip}]$。令 $N = c_0 c_1^2 p/2$，可得

$$\mathbb{P}[\mathcal{E}_i'] \le \frac{p}{N} \mathbb{P}[|\hat{w}^\top X| \le \frac{\delta p^{-1/2}}{B}] + \mathbb{P}[p_B < N] = \frac{2}{c_0 c_1^2} \mathbb{P}[|\hat{w}^\top X| \le \delta \frac{\sqrt{2}}{c_1}] + Ce^{-\Theta(p)}$$

现在，通过选取一个足够大的常数 K，该常数仅依赖于 c_0 和 c_1，可得

$$\mathbb{P}[|\hat{w}^\top X| \le \delta \frac{\sqrt{2}}{c_1}] \le Ce^{-\Theta(n)} + \mathcal{L}(\hat{w}^\top X, K\sqrt{2}\delta/c_1) \le O(\frac{\delta}{\sqrt{\alpha}}) + C' \exp(-\Theta(n))$$

因为 α 有一个常数上界。根据柯西交错定理，$\mathcal{E}_i$ 也有类似的界。对于事件 $\mathcal{F}_i$ 和 $\mathcal{F}_i'$ 的最后一项观察，则由 M 的奇异值具有高概率下界这一事实得出。

□

推论 3.1 (高瘦实 Wishart 矩阵的极端特征值间隙)。 对于 M，如定理 *3.19*所述，我们有

$$\inf_{1\le i\le p}(\lambda_i(M^\top M)-\lambda_{i+1}(M^\top M))\ge(\sqrt{n}-K\sqrt{p})p^{-3/2-o(1/\log(n))}$$

以高概率。

3.6 复数情形

本节简要介绍为在复 Wishart 矩阵中获得类似的特征值排斥结果所需进行的修改。总体策略是将复对象分别嵌入到 $M\in\mathbb{C}^{n\times p}$ 和 $u\in C^p$ 中 $\mathbb{R}^{2n\times 2p}$ 和 $\mathbb{R}^{2p}$，这与[NTV17]第 6.3 节中的做法类似。我们使用的复对象的实表示及其大部分性质，似乎都是随机矩阵理论领域的公认知识。

事实上，在随机矩阵理论中，实数结果的复数类比通常被视为显而易见的推论。然而，在 Wishart 矩阵的情形下，实矩阵表示中出现的新依赖关系带来了复杂性。[CLOS25] 的作者没有讨论复数情形，我们认为这主要是因为他们的引理 4.4 的依赖结构较为脆弱。

对于一个元素 $M\in\mathbb{C}^{n\times p}$，用 $\Re(M)$ $\Im(M)$ $\in\mathbb{R}^{m\times n}$表示 M的实部和虚部，并将 $M\in C^{m\times n}$ 的分块实表示定义为矩阵

$$\rho(M):=\begin{pmatrix}\Re(M) & -\Im(M)\\ \Im(M) & \Re(M)\end{pmatrix}$$

对于向量 $x\in\mathbb{C}^n$，我们使用平坦实表示

$$r(x):=(\Re(x),\Im(x))$$

利用这些表示的性质，我们发现近似特征值方程等价于

$$\|M^*Mu-\sigma^2u\|=\|\rho(M)^\top\rho(M)r(u)-\sigma^2r(u)\| \tag{3.17}$$

右奇异向量方程也同理

$$\|Mx-a\|=\|\rho(M)r(x)-r(a)\| \tag{3.18}$$

虽然由于 $\rho(M)$ 存在逐坐标依赖，我们无法直接应用实数情形中的内容，但 $\rho(M)$ 的依赖结构相当简单，只需对关键引理做少许修改，我们现在就来说明。

在定理 3.8 中，分解 $M=(X|Y)$ 并不完全充分，因为无论 c_0 如何， X 和 Y 都存在某种非平凡的依赖关系。不过，利用 $c_0<1/2$，我们可以进一步将 $Y=(Y_1|Y_2)$ 分解，其中 Y_1 是一个 $n\times(1/2-c_0)$ 矩阵，因此 X 与 Y 的拼接等于 $(\Re(M)|-\Im(M))$，从而 X 与 Y_1 相互独立。随后，我们可以用 $\|Y_1^\top Xu_0'\|$ 替换下界 $\|Y^\top Xu_0'\|$，证明过程与之前完全相同。

可以用类似的方法得到定理 3.8 的一个类似结果。取水平分解$M=\binom{X}{Y}$，并进一步分解 $Y=\binom{Y_1}{Y_2}$，使得 Y_1 是一个 $(1/2-c_0)\ n\times p$ 矩阵，且与 X独立，然后像之前一样继续证明。注意，与上面的右奇异向量情形不同，

其中 X 和 Y_1 的元素独立同分布；左奇异向量情形中涉及的 X 和 Y_1 则只有次高斯行，且行内元素独立同分布，这仍足以得到奇异值界（见定理 3.2）。

最后，定理3.15 可以通过采用新的依赖结构来实现，方法是省去 [CLOS25] 中引理 4.4 证明中的左分支，并使用略有不同的分解。注意，引理 4.4 的证明涉及如下分解：

$$M \coloneqq \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

其中 A 是一个 $(n - \lfloor \alpha n \rfloor) \times (p - \lfloor \alpha p \rfloor)$ 矩阵。我们改为考虑相同的分解，其中 A 是一个 $(n/2) \times (p - \lfloor \alpha p \rfloor)$ 矩阵，此时下界

$$\|Mx - a\| \geq \|Ax' + Bx'' - a'\|$$

具有 A ，且 B 相互独立，因此应用定理3.5 可得上界

$$\sup_{a \in \mathbb{R}^n} \mathbb{P}[\{\|Mx - a\| < \varepsilon\sqrt{n}\}] \leq C\left(\frac{\varepsilon\sqrt{2}}{\gamma c_1 \sqrt{\alpha}} + e^{-\Theta(\kappa^2)}\right)^{n/2}$$

这对定理 3.16没有实质影响。 [CLOS25] 中类似分解的维数至关重要，因为必须确保构成上界的两个概率所对应的两个事件相互独立。我们认为，这正是 [CLOS25] 处理复数情形的主要障碍；但由于我们只关注论证的一半，因此无需维持同样脆弱的分解结构。

最后，我们以与定理 3.19类似的方式完成排斥论证。通过相同的论证，我们推出不等式

$$|\hat{w}^\top X| \leq \left|\frac{\sigma_i^2(M') - \sigma_i^2(M)}{b\sigma_i(M')}\right|$$

其中 $|\cdot|$ 是 复数模。在类似的事件 $\mathcal{E}_i$ 上，这可化为不等式

$$|\hat{w}^\top X| \leq \frac{\delta p^{-1/2}}{|b|}$$

现在，按照 [NTV17，注 6。3] 并令 $w = (\Re(\hat{w})\ \Im(\hat{w}))$，$w' = (\Im(\hat{w})\ -\Re(\hat{w}))$ 和$Y = (\Re(X)\ \Im(X))$，上述事件可化为

$$\{|w^\top Y| \leq \frac{\delta p^{-1/2}}{|b|} \wedge |w'^\top Y| \leq \frac{\delta p^{-1/2}}{|b|}\} \subseteq \{|w^\top Y| \leq \frac{\delta p^{-1/2}}{|b|}\}$$

最后，项 b 是 $\hat{w}$的一个（复数）坐标，因此 $|b|$是不可压缩实向量 $r(\hat{w}) = w$的两个坐标的绝对值之和，因此定理 3.19 中的同一论证适用，由此可推得 $\mathcal{E}_i$ 出现的概率至多为 $O(\underline{\delta}/\sqrt{\alpha})$。综上可得定理 3.19的复数类比。

关于代数数的有效且高效操作的背景

我们的酉张量同构精确判定算法，关键在于能够以完美精度有效且高效地处理代数数（即 $\alpha \in \mathbb{A}$ 满足单变量整数系数多项式的根的数值）。关于以完美精度高效处理代数数，已有相当成熟的研究文献（参见 [BPR05、Coh13]）。我们将陈述这一理论中的一些基本且重要的事实。

首先，对于任意代数数 $\alpha \in \mathbb{A}$，都与一个定义多项式 p_α 相关联，该多项式是使 α为根的最低次数唯一多项式（其系数没有公因子）。因此，任何代数数，即使是无理数，也都具有标准的有限编码，由其定义多项式以及实部和虚部的有理数近似组成；这些近似的精度足以将 α 与 p_α 的其他根区分开来：其表示是一个元组 $(p_\alpha,\ a,\ b,\ r) \in \mathbb{Z}[x] \times \mathbb{Q}^3$，其中 r 是指定以点 $a+bi$为中心、包含该根的圆盘半径。Mignotte 的分离界 [Mig82] 使得这种表示可以快速计算：对于多项式 $p \in \mathbb{Z}[x]$的不同根 $\alpha,\ \beta$

$$|\alpha - \beta| > \frac{\sqrt{6}}{d^{(d+1)/2} H^{d-1}},$$

其中 d 是次数，H 是 p的高度。特别是，当 r 足够小时，可以检验代数数是否相等。此外，计算 $\alpha+\beta$、$\alpha\beta$、$1/\alpha$、α、$|\alpha|$、$\sqrt{\alpha}$，以及判定不同代数数 α 和 β是否满足 $\alpha > \beta$，都可以在多项式时间内完成（以表示长度计）。

B 推论证明概要 1.2

设 $L = M = N = [n] := \{1, 2, \ldots, n\}$，且令 $G,\ H \subseteq L \times M \times N$ 为定义在顶点集 $L \cup M \cup N$ 上的两个 3-均匀三部超图的边集。令 $A_G \in \mathbb{R}^n \otimes \mathbb{R}^n \otimes \mathbb{R}^n$ 为 G 的邻接张量，使得当 $(i,\ j,\ k) \in G$ 时，$A_G(i,\ j,\ k) = 1$，否则为 -1。那么，检验 G 与 H 是否同构，等价于检验在 $\mathrm{Sym}_n \times \mathrm{Sym}_n \times \mathrm{Sym}_n$ 对 $\mathbb{R}^n \otimes \mathbb{R}^n \otimes \mathbb{R}^n$ 的自然作用下，A_G 与 A_H 是否同构，其中 Sym_n 是 $[n]$ 上的对称群。

假设 G 是一个随机超图，也就是说，每条边 (i,j,k) 以概率 $1/2$ 被包含在 G 中。令 F_G 为沿顶点集 N 方向对 A_G 展平所得的张量，因此 $F_G \in \mathrm{M}(n^2 \times n, \mathbb{R})$。根据定理 1.3，对于 F_G（其元素取自 Rademacher 分布），以高概率，$F_G^\top F_G$ 的特征值重数均为 1，且彼此间隔明显。令 F_H 为沿顶点集 N 方向对 A_H 展平所得的张量。若 G 与 H 同构，则一个必要条件是 F_G 的奇异值与 F_H 的奇异值相同。

令 $C_N = \{\pi \in \mathrm{Sym}_n \mid \pi^\top F_G^\top F_G \pi = F_H^\top F_H\}$。注意，$C_N$是群 B_N的一个陪集：$= \{\pi \in \mathrm{Sym}_n \mid \pi^\top F_G^\top F_G \pi = F_G^\top F_G\}$。根据 [LM79]（另见 [Spi18]），我们可以计算 C_N，它由陪集代表元 $\sigma \in \mathrm{Sym}_n$ 以及 B_N的一个生成集表示。此外，B_N 是一个 2-群，也就是说，$|B_N|$ 是 2 的幂。

然后，我们沿着 M 和 L 方向执行上述过程，得到 C_M 和 B_M，以及 C_L 和 B_L。应用陪集代表元将 A_G 变换为 A'_G后，问题就变成了检验是否存在一个来自 $B_L \times B_M \times B_N$ 的元素，将 A'_G 变换为 A_H。注意，$B_L \times B_M \times B_N$ 是一个 2-群。Luks 在其关于有界度图同构的著名结果中解决了这个问题，即 2-群作用下的集合传输问题 [Luk82]。

致谢。作者感谢 Peter B¨urgisser 对本文的关注以及与作者的讨论。Y.Q. 感谢 Robert Andrews 分享其在 $\mathbb{R}$ 上进行 Gr¨obner 基计算的见解。S.E. 获得了美国国家科学基金会研究生研究奖学金计划的资助，项目编号为 2140001。

参考文献

[AGL+18] Zeyuan Allen-Zhu、Ankit Garg、Yuanzhi Li、Rafael Mendes de Oliveira 和 Avi Wigderson。通过测地凸优化、不变量理论和多项式恒等式检验进行算子缩放。载于 Ilias Diakonikolas、David Kempe 和 Monika Henzinger（编），第50届ACM SIGACT计算理论研讨会论文集，STOC 2018，美国加利福尼亚州洛杉矶，2018年6月25日至29日，第172–181页。ACM，2018年。doi:10.1145/3188745.3188942。[AGS26] Robert Andrews、Abhibhav Garg 和 ´Eric Schost。希尔伯特零点定理属于计数层级，2026年。URL：https://arxiv.org/abs/2602.17904，arXiv：2602.17904。[AGZ10] Greg W Anderson、Alice Guionnet 和 Ofer Zeitouni。随机矩阵导论。第118卷。剑桥大学出版社，2010年。[AKM25] Michael Anastos、Matthew Kwan 和 Benjamin Moore。图同构的平滑分析。载于第57届ACM计算理论年会论文集，第2098–2106页，2025年。[AMN+23] Arturo Acuaviva、Visu Makam、Harold Nieuwboer、David P´erez-Garc´ıa、Friedrich Sittner、Michael Walter 和 Freek Witteveen。张量网络的最小规范形式。载于 2023 年 IEEE 第 64 届计算机科学基础年会（FOCS），第328–362页。IEEE，2023年。[Bab86] L´aszl´o Babai。具有有界特征值重数的图同构的拉斯维加斯-NC算法。载于第27届计算机科学基础年会，加拿大多伦多，1986年10月27日至29日，第303–312页。IEEE计算机学会，1986年。doi:10.1109/SFCS.1986.1。[BAB13] Gerard Ben Arous 和 Paul Bourgade。随机矩阵特征值之间的极端间距。2013年。[Bab16] L´aszl´o Babai。准多项式时间内的图同构 [扩展摘要]。载于 Daniel Wichs 和 Yishay Mansour（编），第48届ACM SIGACT计算理论研讨会论文集，STOC 2016，剑桥，美国马萨诸塞州，2016年6月18日至21日，第684–697页。ACM，2016年。doi:10.1145/2897518.2897542。[BDM+21] Peter B¨urgisser、M. Levent Do˘gan、Visu Makam、Michael Walter 和 Avi Wigderson。环面作用不变量理论中的多项式时间算法。载于 Valentine Kabanets（编），第36届计算复杂性会议（CCC 2021），莱布尼茨国际信息学会议录（LIPIcs）第200卷，第32:1–32:30页，德国达格施图尔，2021年。Schloss Dagstuhl – Leibniz-Zentrum f¨ur Informatik。

[BDM+24] Peter B¨urgisser、Mahmut Levent Do˘gan、Visu Makam、Michael Walter 和 Avi Wigderson。环面作用下鲁棒轨道问题的复杂性与 abc 猜想。载于 Rahul Santhanam（编），第39届计算复杂性会议（CCC 2024），莱布尼茨国际信息学会议录（LIPIcs）第300卷，第14:1–14:48页，德国达格施图尔，2024年。Schloss Dagstuhl – Leibniz-Zentrum f¨ur Informatik。[BES80] L´aszl´o Babai、Paul Erd¨os 和 Stanley M. Selkow。随机图同构。《SIAM计算杂志》，9(3)：628–635，1980年。doi:10.1137/0209047。[BFG+18] Peter B¨urgisser、Cole Franks、Ankit Garg、Rafael Oliveira、Michael Walter 和 Avi Wigderson。张量缩放、量子边缘分布和矩多面体的高效算法。载于2018年IEEE第59届计算机科学基础年会（FOCS），第883–897页。IEEE，2018年。[BFG+19] Peter B¨urgisser、Cole Franks、Ankit Garg、Rafael Mendes de Oliveira、Michael Walter 和 Avi Wigderson。迈向非交换优化理论：矩映射和矩多面体的测地一阶与二阶方法。载于 David Zuckerman（编），第60届IEEE计算机科学基础年会，FOCS 2019，美国马里兰州巴尔的摩，2019年11月9日至12日，第845–861页。IEEE计算机学会，2019年。doi:10.1109/FOCS.2019.00055。[BGM82] L´aszl´o Babai、D Yu Grigoryev 和 David M Mount。具有有界特征值重数的图同构。载于第14届ACM计算理论研讨会论文集，第310–324页，1982年。[BI13] Peter B¨urgisser 和 Christian Ikenmeyer。通过几何复杂性理论给出的显式下界。载于 Dan Boneh、Tim Roughgarden 和 Joan Feigenbaum（编），计算理论研讨会会议，STOC'13，美国加利福尼亚州帕洛阿尔托，2013年6月1日至4日，第141–150页。ACM，2013年。doi:10.1145/2488608.2488627。[BK79] L´aszl´o Babai 和 Ludek Kucera。线性平均时间内的图的典范标记。载于第20届计算机科学基础年会，波多黎各圣胡安，1979年10月29日至31日，第39–46页。IEEE计算机学会，1979年。doi: 10.1109/SFCS.1979.8。[BL83] L´aszl´o Babai 和 Eugene M. Luks。图的规范标记。载于 David S. Johnson、Ronald Fagin、Michael L. Fredman、David Harel、Richard M. Karp、Nancy A. Lynch、Christos H. Papadimitriou、Ronald L. Rivest、Walter L. Ruzzo 和 Joel I. Seiferas（编），第15届ACM计算理论研讨会论文集，1983年4月25日至27日，美国马萨诸塞州波士顿，第171–183页。ACM，1983年。doi: 10.1145/800061.808746。[BLQW20] Peter A. Brooksbank、Yinan Li、Youming Qiao 和 James B. Wilson。交替矩阵空间等距的改进算法：从理论到实践。载于 Fabrizio Grandoni、Grzegorz Herman 和 Peter Sanders（编），第28届欧洲算法研讨会，ESA 2020，2020年9月7日至9日，意大利比萨（线上会议），LIPIcs第173卷，第26:1–26:15页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2020年。doi:10.4230/LIPIcs.ESA.2020.26。

[Bol82] B´ela Bollob´as. 随机图的可区分顶点。载于《北荷兰数学研究》，第62卷，第33–49页。爱思唯尔，1982年。[BPR05] S. Basu、R. Pollack 和 M-F. Roy。实代数几何算法。施普林格，2005年。[Cai94] 蔡金义。多项式时间内精确计算可交换矩阵的约当标准形。《国际计算机科学基础杂志》，5(03n04):293–302，1994年。[Can88] John F. Canny。在 PSPACE 中的一些代数与几何计算。载于第20届 ACM计算理论研讨会论文集，第460–467页，1988年。[CFHH21] Debsoumya Chakraborti、Alan Frieze、Simi Haber 和 Mihir Hasabnis。随机k均匀超图的同构。《信息处理快报》，166:106039，2021年。[CGQ+24] Zhili Chen、Joshua A. Grochow、Youming Qiao、Gang Tang 和 Chuanqi Zhang。张量、群和多项式同构问题的复杂性 III：经典群作用。载于 Venkatesan Guruswami（编），第15届理论计算机科学创新会议（ITCS 2024），2024年1月30日至2月2日，美国加利福尼亚州伯克利，第287卷 LIPIcs，第31:1–31:23页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2024年。网址：https://doi.org/10.4230/LIPIcs. ITCS.2024.31，doi:10.4230/LIPICS.ITCS.2024.31。[CLOS25] Nicholas Christoffersen、Kyle Luh、Sean O'Rourke 和 Calum Shearer。样本协方差矩阵奇异值之间的间隙。arXiv 预印本 arXiv:2502.15002，2025年。[CNP+23] Tung Chou、Ruben Niederhagen、Edoardo Persichetti、Tovohery Hajatiana Randri-anarisoa、Krijn Reijnders、Simona Samardjiska 和 Monika Trimoska。尽情享用 MEDS：基于矩阵码等价的数字签名。载于《密码学进展——非洲密码学 2023——第14届非洲密码学国际会议》，突尼斯苏塞，2023年7月19日至21日，论文集，第14064卷《计算机科学讲义》，第28–52页。施普林格，2023年。doi:10.1007/978-3-031-37679-5_2.[Coh13] Henri Cohen。《计算代数数论教程》，第138卷。Springer Science & Business Media，2013年。[CP08] Tomek Czajka 和 Gopal Pandurangan。改进的随机图同构。《离散算法杂志》，6(1):85–92，2008年。[CY26] 蔡金义和 Ben Young。消失签名、轨道闭包与 Holant定理的逆定理。载于第17届理论计算机科学创新会议（ITCS 2026），第32–1页。Schloss Dagstuhl–Leibniz-Zentrum f¨ur Informatik，2026年。[Der01] Harm Derksen。不变量环的多项式界。《美国数学会会刊》，129(4):955–963，2001年。

[DKRS23] Papri Dey、Ravi Kannan、Nick Ryder 和 Nikhil Srivastava。约当标准形与多项式谱因式分解的位复杂度。载于第14届理论计算机科学创新会议（ITCS 2023），第42–1页。Schloss Dagstuhl–Leibniz-Zentrum f¨ur Informatik，2023年。[DLDMV00] Lieven De Lathauwer、Bart De Moor 和 Joos Vandewalle。多线性奇异值分解。《SIAM矩阵分析与应用杂志》，21(4):1253–1278，2000年。[DM21] Harm Derksen 和 Visu Makam。通过箭图表示对矩阵正态模型进行最大似然估计。《SIAM应用代数与几何期刊》，5(2):338–365，2021年。[DSL08] Vin De Silva 和 Lek-Heng Lim。张量秩与最佳低秩近似问题的不适定性。《SIAM矩阵分析与应用杂志》，30(3):1084–1127，2008年。doi:10.1137/06066518X。[DVC00] Wolfgang D¨ur、Guifre Vidal 和 J Ignacio Cirac。三个量子比特可以以两种不等价的方式纠缠。《物理评论A》，62(6):062314，2000年。[ESY10] L´aszl´o Erd˝os、Benjamin Schlein 和 Horng-Tzer Yau。Wegner估计与 Wigner随机矩阵的能级排斥。《国际数学研究通知》，2010(3):436–479，2010年。[EY15] L´aszl´o Erd˝os 和 Horng-Tzer Yau。广义 Wigner 系综与 beta 系综的间隙普适性。《欧洲数学学会杂志》，17(8):1927–2036，2015年。[Gal14] David Galvin。关于熵与计数的三讲。arXiv 预印本 arXiv:1406.7872，2014年。[Ge93] Guoqiang Ge。在多项式时间内检验乘法表示是否相等。载于1993年 IEEE 第34届计算机科学基础年会论文集，第422–426页。IEEE，1993年。[GGdOW20]Ankit Garg、Leonid Gurvits、Rafael Mendes de Oliveira 和 Avi Wigderson。算子缩放：理论与应用。《计算数学基础》，20(2):223–290，2020年。网址：https://doi.org/10.1007/s10208-019-09417-z，doi:10.1007/S10208-019-09417-Z。[GQ23] Joshua A. Grochow 和 Youming Qiao。张量、群和多项式同构问题的复杂性 I：张量同构完备性。《SIAM计算杂志》，52(2):568–617，2023年。网址：https://doi.org/10.1137/21m1441110，doi: 10.1137/21M1441110。[GQ24] Joshua A. Grochow 和 Youming Qiao。关于 p 群同构：通过张量实现搜索到判定、计数到判定以及幂零类归约。《ACM计算理论汇刊》，16(1):2:1–2:39，2024年。doi:10.1145/3625308。[GQ25] Joshua A. Grochow 和 Youming Qiao。张量、群和多项式同构问题的复杂性 IV：线性长度归约及其应用。载于 Michal Kouck´y 和 Nikhil Bansal（编），第57届年度

ACM计算理论研讨会，STOC 2025，布拉格，捷克，2025年6月23日至27日，第766–776页。ACM，2025年。doi:10.1145/3717823.3718282.[GQSS25] Joshua A. Grochow、Youming Qiao、Katherine E. Stange 和 Xiaorui Sun。《张量、群和多项式同构问题的复杂性 V：交换环上的情形》。载于 Michal Kouck´y 和 Nikhil Bansal 编，2025年6月23日至27日在捷克布拉格举行的第57届ACM计算理论年会论文集（STOC 2025），第777–784页。ACM，2025年。doi:10.1145/3717823. 3718286.[GS86] Shafi Goldwasser 和 Michael Sipser。交互式证明系统中的私有随机币与公开随机币。载于第18届ACM计算理论研讨会论文集，第59–68页，1986年。[Han25] Yi Han。随机矩阵奇异值谱的单纯性与两点定量可逆性。arXiv预印本，arXiv:2502.13819，2025年。[HH21] Masaki Hamada 和 Hiroshi Hirai。通过 CAT(0)空间上的离散凸优化计算非交换秩。《SIAM应用代数与几何杂志》，5(3):455–478，2021年。doi:10.1137/20M138836X。[Hil93] D. Hilbert。关于完备不变量系。Math. Ann., (42):313–370, 1893年。[HU17] Wolfgang Hackbusch 和 Andr´e Uschmajew。实张量高阶奇异值之间的相互关系。《数值数学》，135:875–894，2017年。doi:10.1007/s00211-016-0819-9。[HW+53] Alan J Hoffman、Helmut W Wielandt 等。正规矩阵的谱变化。Duke Math. J, 20(1):37–39, 1953年。[HW15] Pavel Hrubeˇs 和 Avi Wigderson。带除法的非交换算术电路。《计算理论》，11(14):357–393，2015年。网址：https://theoryofcomputing. org/articles/v011a014, doi:10.4086/toc.2015.v011a014。[IMQ+24] G´abor Ivanyos、Euan J. Mendoza、Youming Qiao、Xiaorui Sun 和 Chuanqi Zhang。更快地判定 Frattini类2 p-群的同构。载于第65届IEEE计算机科学基础年会（FOCS 2024），2024年10月27日至30日在美国伊利诺伊州芝加哥举行，第1408–1424页。IEEE，2024年。doi:10.1109/FOCS61266.2024. 00090。[IQ23] G´abor Ivanyos 和 Youming Qiao。矩阵元组在共轭作用与左右作用下的轨道闭包相交问题。载于 Nikhil Bansal 和 Viswanath Nagarajan 编，2023年1月22日至25日在意大利佛罗伦萨举行的2023年ACM-SIAM离散算法研讨会论文集（SODA 2023），第4115–4126页。SIAM，2023年。网址：https://doi.org/10.1137/1.9781611977554.ch158, doi:10.1137/1.9781611977554.CH158。[IQS18] G´abor Ivanyos、Youming Qiao 和 K. V. Subrahmanyam。构造性非交换秩计算属于确定性多项式时间。《计算复杂性》，27(4):561–593，2018年。网址：https://doi.org/10.1007/s00037-018-0165-7, doi:10.1007/S00037-018-0165-7。

[JQSY19] Zhengfeng Ji、Youming Qiao、Fang Song 和 Aaram Yun。张量上的一般线性群作用：后量子密码学的一个候选方案。载于 Dennis Hofheinz 和 Alon Rosen 编，《密码学理论——第17届国际会议》（TCC 2019），2019年12月1日至5日在德国纽伦堡举行，论文集第一部分，计算机科学讲义第11891卷，第251–281页。施普林格，2019年。doi: 10.1007/978-3-030-36030-6_11.[Kar75] Richard M Karp。困难组合问题的快速近似解。载于第六届东南部组合学、图论与计算会议论文集（佛罗里达大西洋大学，1975年），第15–31页，1975年。[Kar84] N. Karmarkar。线性规划的一种新的多项式时间算法。载于第16届ACM计算理论研讨会论文集（STOC '84），第302–311页，美国纽约州纽约，1984年。计算机协会。doi:10.1145/800057.808695。[Koi96] Pascal Koiran。希尔伯特零点定理属于多项式层次。《复杂性杂志》，12(4):273–286，1996年。[Kra10] B Kraus。多体纯态的局部酉等价。《物理评论快报》，104(2):020504，2010年。[KST93] Johannes K¨obler、Uwe Sch¨oning 和 Jacobo Tor´an。《判定问题、搜索问题与计数问题》。载于 Johannes K¨obler、Uwe Sch¨oning 和 Jacobo Tor´an 编，《图同构问题：其结构复杂性》，理论计算机科学进展，第11–50页。Birkh¨auser，波士顿，马萨诸塞州，1993年。doi:10.1007/978-1-4612-0333-9_3.[Lip78] Richard J Lipton。图同构的信标集方法。耶鲁大学计算机科学系，1978年。[LLLQ12] Bin Liu、Jun-Li Li、Xikun Li 和 Cong-Feng Qiao。任意维多体纯态的局部幺正分类。《物理评论快报》，108(5):050501，2012年。[LM79] F. Thomson Leighton 和 Gary L. Miller。具有不同特征值的图的证书，1979年。[LM17] Nati Linial 和 Jonathan Mosheiff。稀疏随机图的刚性。《图论杂志》，85(2):466–480，2017年。[LMN21] Kyle Luh、Sean Meehan 和 Hoi H Nguyen。有限域上随机矩阵的一些新结果。《伦敦数学学会杂志》，103(4):1209–1252，2021年。[LQ17] Yinan Li 和 Youming Qiao。图同构问题和 Erd˝os-R´enyi 模型的线性代数类比问题。载于 Chris Umans 编，第58届IEEE计算机科学基础年会（FOCS 2017），2017年10月15日至17日在美国加利福尼亚州伯克利举行，第463–474页。IEEE计算机学会，2017年。doi:10.1109/ FOCS.2017.49。

[Luk82] Eugene M. Luks. 有界度图同构可在多项式时间内判定。计算机与系统科学杂志，25(1):42–65，1982。doi:10.1016/0022-0000(82) 90009-5.[LW25] Vladimir Lysikov 和 Michael Walter. 张量轨道闭包交问题的复杂性理论：归约、完备性与图同构困难性。载于第66届IEEE计算机科学基础年会，FOCS 2025，悉尼，澳大利亚，2025年12月14日至17日，第486–511页。IEEE，2025。doi: 10.1109/FOCS63196.2025.00027.[MCK81] BD MCKAY. 实用图同构。Congressus Numeranitum，30:45–87，1981.[Mez07] Francesco Mezzadri. 如何从经典紧群生成随机矩阵。《美国数学学会通报》，54(5):592–604，2007.[MFK94] David Mumford、John Fogarty 和 Frances Kirwan. 几何不变理论，第34卷。Springer Science & Business Media，1994.[Mig82] Maurice Mignotte. 一些有用的界。载于《计算机代数：符号与代数计算》，第259–263页。施普林格，1982.[Mir60] Leon Mirsky. 对称规范函数与酉不变范数。《数学季刊》，11(1):50–59，1960.[MP14] Brendan D McKay 和 Adolfo Piperno. 实用图同构，II。《符号计算杂志》，60:94–112，2014.[Mul12] Ketan Mulmuley. 几何复杂性理论 V：黑盒多项式恒等式检验去随机化与诺特正规化引理去随机化之间的等价性。载于第53届IEEE计算机科学基础年会，FOCS 2012，新不伦瑞克州，新泽西州，美国，2012年10月20日至23日，第629–638页，2012。URL: http://dx.doi.org/10.1109/FOCS.2012.15, doi:10.1109/FOCS. 2012.15.[NP98] Peter M. Neumann 和 Cheryl E. Praeger. 有限经典群中的错排与无特征值元素。《伦敦数学学会杂志》，58(3):564–586，1998。doi:10.1112/S0024610798006772.[NTV17] Hoi Nguyen、Terence Tao 和 Van Vu. 随机矩阵：特征值间隙的尾界。《概率论及相关领域》，167(3):777–816，2017。[Rud10] M Rudelson. 随机矩阵非渐近理论讲义，2007，2010。[RV08] Mark Rudelson 和 Roman Vershynin. Littlewood–Offord问题与随机矩阵的可逆性。《数学进展》，218(2):600–633，2008。[RV09] Mark Rudelson 和 Roman Vershynin. 随机矩形矩阵的最小奇异值。《纯粹与应用数学通讯：库朗数学科学研究所发行的期刊》，62(12):1707–1739，2009。

[Sei18] Anna Seigal. 实二元张量的格拉姆行列式。《线性代数及其应用》，544:350–369，2018。doi:10.1016/j.laa.2018.01.019.[Spi18] Daniel A. Spielman. 测试具有互异特征值的图的同构性。https: //www.cs.yale.edu/homes/spielman/561/lect08-18.pdf，2018年9月。谱图论第8讲。[ST04] Daniel A Spielman 和 Shang-Hua Teng. 算法的平滑分析：为什么单纯形算法通常能在多项式时间内运行。《ACM杂志》(JACM)，51(3):385–463，2004。[Ste98] Gilbert W Stewart. 奇异值分解的摄动理论。1998。[Sun23] Xiaorui Sun. 二阶且指数为 p 的 p-群的更快同构算法。载于 Barna Saha 和 Rocco A. Servedio（编），第55届ACM计算理论研讨会年会论文集，STOC 2023，美国佛罗里达州奥兰多，2023年6月20日至23日，第433–440页。ACM，2023。doi:10.1145/3564246.3585250.[TDJ+22] Gang Tang、Dung Hoang Duong、Antoine Joux、Thomas Plantard、Youming Qiao 和 Willy Susilo. 基于三线性形式同构问题的实用后量子签名方案。载于 Orr Dunkelman 和 Stefan Dziembowski（编），密码学进展——EUROCRYPT 2022——第41届密码学技术理论与应用国际年会，挪威特隆赫姆，2022年5月30日至6月3日，论文集，第III部分，计算机科学讲义第13277卷，第582–612页。施普林格，2022。doi:10.1007/978-3-031-07082-2_21.[Tem04] George Frederick James Temple. 笛卡尔张量：导论。Courier Corporation，2004。[TV09a] Terence Tao 和 Van Vu. 从Littlewood-Offord问题到圆律：随机矩阵谱分布的普适性。《美国数学会通报》，46(3):377–396，2009。[TV09b] Terence Tao 和 Van H Vu. 逆Littlewood-Offord定理与随机离散矩阵的条件数。《数学年刊》，第595–632页，2009。[TV10] Terence Tao 和 Van Vu. 随机矩阵：直至边缘的局部特征值统计普适性。《数学物理通讯》，298(2):549–572，2010年4月。URL: http://dx.doi.org/10.1007/s00220-010-1044-5, doi: 10.1007/s00220-010-1044-5.[TV11] Terence Tao 和 Van Vu. 随机矩阵：局部特征值统计的普适性。《数学学报》，206:127–204，2011。[TV12] Terence Tao 和 Van Vu. 随机协方差矩阵：特征值局部统计量的普适性。《概率年刊》，40(3)，2012年5月。URL: http://dx.doi.org/10.1214/11-AOP648, doi:10.1214/11-aop648.[TV17] Terence Tao 和 Van Vu. 随机矩阵具有单谱。《组合数学》，37(3):539–553，2017。

[Ver14] Roman Vershynin. 对称随机矩阵的可逆性. 随机结构与算法, 44(2):135–182, 2014.[Ver18] Roman Vershynin. 高维概率：数据科学中的导论与应用, 第 47 卷. 剑桥大学出版社, 2018.[Vu14] V Vu. 随机矩阵理论中的组合问题. 载于 国际数学家大会论文集, 第 4 卷, 第 489–508 页, 2014.[Vu21] Van H Vu. 组合随机矩阵理论的最新进展. 概率调查, 18:179–200, 2021.[Wan12] Ke Wang. 随机协方差矩阵：特征值局部统计量直至边缘的普适性. 随机矩阵：理论与应用, 1(01):1150005, 2012.[WGE16] Michael Walter, David Gross, and Jens Eisert. 多体纠缠. 量子信息：从基础到量子技术应用, 第 293–330 页, 2016.