arXiv:2603.01432v1 [math.PR] 2 Mar 2026

Cohen-Lenstra 普适类中的近对称矩阵

ELIA GOROKHOVSKY

Abstract. 本文研究了 $\mathbb{Z}$ 上满足由固定交替双线性型决定的对称条件的随机 $n \times n$ 矩阵的余核。这些矩阵包括对随机对称矩阵进行扰动的情形，扰动涉及的矩阵项数量非常少（但随 n 增长而无界）。我们证明，在矩阵项的分布满足相当弱的条件时，这些余核的分布弱收敛于 Cohen-Lenstra 分布；该分布是无对称性约束的随机矩阵的余核的极限分布。这一结果表明，对称矩阵的余核分布对对称条件的微小扰动相当敏感。

1. Introduction

我们研究具有整数矩阵项的大型随机矩阵的余核的极限分布。这个问题的动机来自算术统计。Cohen 和 Lenstra [CL84]基于数值证据，猜想了虚二次数域的类群中奇素数 p-Sylow 子群的一种分布。对于有限阿贝尔 p-群 p， GCohen-Lenstra 随机群 $\Gamma_{CL}^{(p)}$ 满足

$$\mathbb{P}[\Gamma_{CL}^{(p)} \cong G] \propto \frac{1}{|\operatorname{Aut}(G)|}.$$

后来，Friedman 和 Washington [FW89] 注意到，这一分布如今称为 Cohen-Lenstra 分布，是以下形式矩阵的余核的极限分布： $I - M$，其中 M 是 GL$_{2g}$($\mathbb{Z}_p$中的 Haar 随机元素；GL $2g \times 2g$ 是定义在 p-进整数上的可逆矩阵群，并且当 $g \to \infty$时成立。

Wood [Woo19] 以及 Nguyen 和 Wood [NW22] 发现，Cohen-Lenstra 分布具有普适性，即只要矩阵的矩阵项彼此独立，并满足一种称为 ε-平衡性（定义 3.4）的弱正则条件，就能从当 $n \to \infty$ 时整数矩阵的（p-部分）余核中得到相同的极限分布$n \times n$。后续研究又提供了许多方阵整数矩阵或 p-进随机矩阵系综的例子，即使矩阵项之间存在某些依赖关系，其余核也会以同样的意义收敛到 Cohen-Lenstra 分布，例如 Erd˝os-R´enyi 随机有向图的拉普拉斯矩阵 [M´es20], 具有足够宽带宽的随机带状矩阵 [M´es24], 在分块上满足弱正则条件的随机分块矩阵[Gor24],某些矩阵项固定为零的矩阵 [KLY24], 以及某些稀疏矩阵 [M´es25]。

与此同时，还有许多随机矩阵模型的余核并不收敛到 Cohen-Lenstra 分布，例如对称矩阵 [Woo17；NW25], 交替矩阵 [NW25], 独立随机矩阵的乘积 [NV24], Haar 随机 p-adic 矩阵中的二次多项式 [CK24], 以及固定为零的矩阵项过多的矩阵 [KLY24；M´es24]。自然会问，随机矩阵的矩阵项之间何种依赖关系会阻碍其余核收敛到 Cohen-Lenstra 分布。

日期：2026年3月3日。

有时，例如对称矩阵的情形，极限分布的差异可以用某些矩阵余核上存在额外结构（如完美配对）来解释。除了记录余核上的群结构之外，同时追踪这些结构，得到的分布会更接近 Cohen-Lenstra [Hod。

我们研究一种新的随机 矩阵模型，该模型由满足以下对称性约束的矩阵构成 :

定义 1.1。 设 C 是环 R上的交替 $n \times n$ 矩阵。若 $n \times n$ 矩阵 X在 R 上满足 $X - X^\intercal = C$，则称其为 C-对称 矩阵。特别地，矩阵是 0-对称的，当且仅当它是对称矩阵。

我们将在引言中介绍一些有趣的随机 C-对称矩阵的例子，并在第 7 节中作更详细的讨论。

我们的主要定理表明，对于“绝大多数” C 的选择，随机 C-对称整数矩阵系综的极限分布是 Cohen-Lenstra 分布，具体来说：

定理 1.2. 令 $\varepsilon > 0$。对于每个 n，令 C_n 为定义在 $\mathbb{Z}_p$ 上的确定性 $n \times n$ 交替矩阵。令 X_n 为定义在 $\mathbb{Z}_p$ 上的随机 C_n-对称矩阵，其对角线及其上方的矩阵项相互独立且平衡。假设我们有

$$\lim_{n\to\infty} \operatorname{rank}(C_n \mod p) = \infty.$$

那么对于任意有限阿贝尔 p-群 G，我们有

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{coker}(X_n) \cong G] = \frac{1}{|\operatorname{Aut}(G)|} \prod_{k=1}^{\infty} (1 - p^{-k})$$

换言之，$\operatorname{coker}(X_n)$ 的分布收敛到 ***Cohen-Lenstra*** 分布。

定理 1.2 是以下更强结果的推论（关于 $\operatorname{rank}(C_n \bmod p)$ 与 $n - g_n$之间的关系，参见注 6.6）：

定理 1.3. 令 $\varepsilon > 0$。对于每个 n，令 C_n 为定义在 $R = \mathbb{Z}$ 上的确定性 $n \times n$ 交替矩阵（对于 $a > 0$，分别为 $R = \mathbb{Z}/a\mathbb{Z}$；或为 $R = \mathbb{Z}_p$），并令 h 为一个整数，它整除每个 n 对应的 C_n 的所有矩阵项。假设 C_n/h 的余核可由 R 上的 g_n 个元素生成。令 X_n 为定义在 R 上的随机 C_n-对称矩阵，其对角线及其上方的矩阵项相互独立且平衡。假设我们有

$$\lim_{n\to\infty} n - g_n = \infty$$

对于任意有限阿贝尔群 G （分别地，指数整除 a 的有限阿贝尔群，或有限阿贝尔 p-群），我们有

$$\lim_{n\to\infty} \mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n), G)] = |\wedge^2 G[h]|.$$

其中 $G[h]$ 是 G 中由阶整除 h 的元素构成的子群 .

这里，$\operatorname{Sur}(\operatorname{coker}(X_n)\ G)$ 表示从 $\operatorname{coker}(X_n)$ 到G的满同态数量。对有限阿贝尔群 G 取该数量的平均值，称为余核分布的矩 （即 $\operatorname{coker}(X_n$的分布的矩），通常足以唯一确定该分布。定理 1.3中计算的矩，对应于从以下矩阵子群上的 Haar 测度中抽取的矩阵的余核分布：该子群由$\widehat{\ }$上的矩阵构成，其中 $\mathbb{Z}$ 是整数的 profinite 完备化，且这些矩阵模约化 h后为对称矩阵。这是例7.1中更一般的普适性结论的推论。

定理 1.3 的结果通过有限阿贝尔群的矩方法推出定理 1.2，我们将在第 3 节回顾该方法。该方法实际上比定理 1.3 的表述更强：它还证明，对任意有限个素数 p，coker(X_n) 的 p-Sylow 子群渐近独立，并且还可将定理 1.2 推广到 $\mathbb{Z}_p$ 和 $\mathbb{Z}/a\mathbb{Z}$ 等其他环上。这类结果与例如 [Woo17; Woo19]中的结果风格相同。矩由定理 1.3 所给出的分布，其 p-部分也有一个显式公式；由于多出参数 h，该公式复杂得多，可见于[SW24a，命题 7.1]（含 $R = \mathbb{Z}_p$ 和 $s = \varepsilon = 0$；另见 [SW24a，引理 7.2]）。

该 ε平衡条件要求每个矩阵项的分布在模任意素数时都不会过于集中（见定义3.4）。

关于 C_n 的秩的条件对 C_n的大多数选取都成立，这是因为 $\mathbb{F}_p$ 上的随机交错矩阵在矩阵规模增大时往往具有较大的秩。因此，若每个 C_n都随机选取，则 C_n/h模 p的秩序列所要求的条件以概率1成立。我们将在例7.1中更详细地说明这一点。

当 C_n 接近零矩阵时，我们并未确定极限余核分布，但我们在定理5.3 中观察到，在定理1.2的设定下，余核(X_n)的极限分布与对称矩阵余核的极限分布一致，当且仅当C_n 在 p进意义下收敛于0。这一结果表明，对称矩阵余核的分布对矩阵项对称性的小扰动高度敏感。我们还在定理5.4 中观察到，若 C_n/h的秩在定理1.3的设定下模任意素数时有界，则得不到该定理结论中的 $|\wedge^2 G[h]|$ 极限矩。这表明定理1.2中的假设$\lim_{n\to\infty}$秩$(C_n \bmod p) = \infty$ 是必要的，并且定理 1.3 中类似$\lim_{n\to\infty}(n - g_n) = \infty$ 的某个假设也是必要的。

在 $R = \mathbb{F}_2$ 上，当 C 是一个所有非对角线矩阵项均为 1 的矩阵时，C-对称矩阵会“自然地”以竞赛矩阵的形式出现，也就是竞赛图的邻接矩阵。

另一个关于 C上 $\mathbb{F}_2$ -对称矩阵的自然背景同样来自数论。R´edei[R´ed34] 指出，可以通过一个矩阵来研究二次数域的类群中的 4-挠子。该矩阵的矩阵项是对分歧素数对取值的二次剩余符号。根据二次互反律，这些$R\acute{}edei$ 矩阵是 C-对称的，其中 C 当对应的素数均模 4 同余于 3 时，矩阵项非零。后来，Gerth [Ger84]利用这一解释，研究了分歧素数个数固定的二次数域族中这种 4-挠子的分布。Gerth 的论证研究了添加一个新的随机行和列时，R´edei 矩阵的秩如何变化。使用这一策略并给出有效误差界的证明，见 [KP20] 。

作者和 Liu [GL26] 给出了 C 上有限域上的 -对称矩阵的极限余秩分布的另一种有效计算方法，其思路与本文的证明更为相似。

本文的结构安排如下。在第2节讨论记号与术语后，我们在第3 节介绍本文中出现的随机阿贝尔群的背景，并简要阐述我们将用于确定随机矩阵系综的极限余核分布的一般策略。该策略要求计算以下概率：对于每个有限阿贝尔群 $F \circ X_n = 0$以及映射 G F: $\mathbb{Z}^n \to G$，均满足4节中，我们介绍映射 F 上的一个称为各向同性的条件，它使我们能够将这一计算化归为 Wood 的结果 [Woo17]。在第5节中，我们描述矩阵项取自有限域时的各向同性条件，并据此研究当 C接近零矩阵时的 C -对称矩阵。在

第6节中，我们计算随机映射 $F\colon \mathbb{Z}^n \to G$ 为各向同性的概率，从而证明主要结果。最后，在第7节中，我们给出 C-对称矩阵系综的三个例子，以展示我们结果的强大之处。

2. Notation and Terminology

如果 G 是一个阿贝尔群，且 p 是素数，我们用 G_p 表示 p 的 Sylow 子群。如果 h 是一个正整数，我们用 $G[h]$ 表示 G 中阶整除 h 的元素集合。

如果 G, H 是群，我们用 $\mathrm{Hom}(G, H)$ 表示从 G 到 H 的同态集合，用 $\mathrm{Sur}(G, H)$ 表示从 G 到 H 的满同态集合，并用 $\mathrm{Aut}(G)$ 表示 G 的自同构集合。

所有环均 假定为交换环，且所有非零环均假定含有单位元 1 .

我们用 $\mathbb{P}$ 表示 事件的概率，用 $\mathbb{E}$表示随机变量的期望 .

当 R 是一个环且 G 是一个 R-模时，我们用 $G^* = \mathrm{Hom}(G, R)$ 表示对偶 R-模。我们将自由 R-模 R^n 视为具有自然基，因此对于任意 n，都有一个自然同构$R^n \cong (R^n)^* \cong (R^*)^n$。若 $F\colon G \to H$是 R-模之间的映射，则将其对偶映射记作 $F^*\colon H^* \to G^*$。

我们将 R 上的一个 $n \times n$ 矩阵 M 视为映射 $M\colon (R^n)^* \to R^n$。我们用 $M^\intercal$ 表示转置映射 $M^*\colon (R^n)^* \to (R^n)^{**} = R^n$，并用 $\mathrm{coker}(M) = R^n/M((R^n)^*)$ 表示余核。

我们用 $[n]$ 表示集合 $\{1, \dots, n\}$。

3. Background on Cokernel Distributions and the Moment Method

本节将阐述 Wood 提出的通用策略（此后已成为标准方法），用以确定各种随机矩阵模型在有限多个素数处的余核极限分布。我们还将记录计算所需的文献结果。

使余核分布易于处理的主要工具是矩方法。设Γ 是一个随机群， G 是一个固定群。量 $\mathbb{E}[\#\,\mathrm{Sur}(\Gamma, G)],$，即从 Γ 到 G的满射数的期望，称为 Γ的 G阶矩。

若阿贝尔群 G 对正整数 a 满足 $G \otimes \mathbb{Z}/a\mathbb{Z}$ 是有限阿贝尔群，则称其模 a 有限。

定理 3.1 （推论，出自 [Woo19，定理 3.1], 另见 [SW24b]）。 设 $a > 0$ 为一个整数。设 Γ_1, Γ_2，.....为一列模 a 有限的随机阿贝尔群，且 Γ_∞ 为一个模 a有限的随机阿贝尔群。令 A 为指数整除 a的有限阿贝尔群同构类集合。若对每个 $G \in A$，都有

$$(*) \qquad \lim_{n\to\infty} \mathbb{E}[\#\,\mathrm{Sur}(\Gamma_n, G)] = \mathbb{E}[\#\,\mathrm{Sur}(\Gamma_\infty, G)] \le |\wedge^2 G|$$

那么对于每个 $H \in A$，我们都有

$$(**) \qquad \lim_{n\to\infty} \mathbb{P}[\Gamma_n \otimes \mathbb{Z}/a\mathbb{Z} \cong H] = \mathbb{P}[\Gamma_\infty \otimes \mathbb{Z}/a\mathbb{Z} \cong H]$$

在 [Woo19，定理 3。1], Wood 还证明了具有给定性态良好矩的随机群的存在性。在 [SW24b], 中，Sawin 与 Wood 针对菱形范畴中的随机对象证明了该定理的一个更为一般的版本，并给出了一个的分布公式

具有给定矩的随机对象。在本文中，我们将求得的矩已经与某个已知随机群的矩相吻合，因此我们不需要该存在性陈述。

注 3.2. 如果阿贝尔群 G 对每个正整数 a模 a 都是有限的，我们就称它是良态的。良态阿贝尔群包括所有有限生成阿贝尔群。通过指定一族形如以下形式的开集作为基，可以在良态阿贝尔群的同构类集合上定义一种拓扑

$$U_{a,H} = \{G \text{ well-behaved abelian} \mid G \otimes \mathbb{Z}/a\mathbb{Z} \cong H\}$$

其中 a为正整数， H 为指数整除 a 的有限阿贝尔群。 [LW20] 研究了定义在逆有限群同构类集合上的这种拓扑的一个版本。对 a 和 H 的所有取值，条件（$**$）等价于断言，在此拓扑下，（Γ_n 的分布）弱收敛到（Γ_∞ 的分布）。因此，有时我们会说一列随机群弱收敛到某个分布，以表示对所有 a、 H， （$**$）均成立。定理 3.1 指出，要证明弱收敛，只需验证对指数整除 a 的 a 和 G 的所有取值， （$*$）均成立。更多细节见 [Gor24，第 3 节。5]

现在我们定义两个与本文相关的随机群。

设 $u \geq 0$ 为一个整数。对于素数 p，定义随机群 $\Gamma_{CL}^{(p,u)}$ 为

$$\mathbb{P}[\Gamma_{CL}^{(p,u)} \cong G] = \frac{1}{|G|^u |\operatorname{Aut}(G)|} \prod_{k=1}^{\infty} (1 - p^{-k-u})$$

对于任意有限阿贝尔 p-群 G，并定义

$$\Gamma_{CL}^{(u)} \coloneqq \prod_{p \text{ prime}} \Gamma_{CL}^{(p,u)}$$

Cohen 和 Lenstra [CL84] 猜想，随机群 $\Gamma_{CL}^{(p,0)}$ 描述了p虚二次数域类群的 -部分的分布，而随机群 $\Gamma_{CL}^{(p,1)}$ 描述了实二次数域类群的分布。对所有素数p 取乘积来定义 $\Gamma_{CL}^{(u)}$ 对应于以下假设：这些类群的 p-部分对不同素数 p的表现“相互独立”。

对于素数 p，定义随机群 $\Gamma^{(p)}$ 沙堆 为

$$\begin{aligned}&\mathbb{P}[\Gamma_{\text{sandpile}}^{(p)} \cong G] \\ &\quad = \frac{\#\{\text{symmetric, bilinear, perfect } \phi\colon G \times G \to \mathbb{C}^*\}}{|G||\operatorname{Aut}(G)|} \prod_{k=1}^{\infty} (1 - p^{1-2k})\end{aligned}$$

对于有限阿贝尔 p-群 G，并定义

$$\Gamma_{\text{sandpile}} \coloneqq \prod_{p \text{ prime}} \Gamma_{\text{sandpile}}^{p}$$

Wood [Woo17] 证明了 $\Gamma^{(p)}$ 沙堆是相当一般的 Erd p-部分沙堆群（即这类图的约化拉普拉斯矩阵的余核）的极限分布。″os-R´enyi 随机图上沙堆群中完美配对的计数，这一术语 G 与对称矩阵余核的挠部分具有自然完美配对这一事实有关。Hodges [Hod24] 表明，Wood 的计算可以进一步细化：如果改为同时追踪沙堆群及其对偶配对，就会在带配对的群的同构类上得到类 Cohen-Lenstra 分布。

引理 3.3 ([Woo19，引理 3。2], [Woo17，定理 8.3，推论 9。2], 另见 [Cla+15，定理 2])。 对于有限阿贝尔群 G，我们有

$$\mathbb{E}[\#\operatorname{Sur}(\Gamma_{CL}^{(u)}, G)] = |G|^{-u}$$

and

$$\mathbb{E}[\#\operatorname{Sur}(\Gamma_{sandpile}, G)] = |\wedge^2 G|$$

Wood 等人已经证明，在对矩阵项施加相当宽松的条件时，这些矩可由矩阵模型产生。我们现在给出这些条件的定义。

定义 3.4。 设 N 是取值于环 R 中的随机变量，且 $\varepsilon > 0$。若对于 R 的任意极大理想 $\mathfrak{p}$ 以及任意剩余类 $r \in R/\mathfrak{p}$，都有以下性质，则称 N 为ε-平衡的：

$$\mathbb{P}[N \equiv r \pmod{\mathfrak{p}}] \leq 1 - \varepsilon$$

若一个随机矩阵的矩阵项取值于 R，且其矩阵项相互独立并且是ε-平衡的，则称该矩阵为 ε-平衡矩阵。若一个 ε-平衡（C-）对称矩阵的矩阵项取值于 R，且其对角线及对角线上方的矩阵项相互独立并且是 ε-平衡的，则称该矩阵为随机矩阵。请注意，按照记号滥用的惯例，ε-平衡（C-）对称矩阵绝不会是 ε-平衡的。本文仅讨论以下情形：$R = \mathbb{Z}$、$R = \mathbb{Z}_p$，其中 p为素数；以及 $R = \mathbb{Z}/a\mathbb{Z}$，其中 a 为正整数。

定理 *3.5*（[*Woo19*，定理 *2.9*]）。设 $\varepsilon > 0$ 和 G 是有限阿贝尔群，对于 $R = \mathbb{Z}$、$R = \mathbb{Z}_p$ 或 $R = \mathbb{Z}/a\mathbb{Z}$，具有 R-模结构。对每个自然数 n，设 X_n 是一个矩阵项取自 R 的 ε-平衡 $n \times (n+u)$ 矩阵。存在 c、$K > 0$，它们仅取决于 ε 和 G，使得

$$\left|\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n), G)] - |G|^{-u}\right| \leq Ke^{-cn}$$

余核(X_n)特别地，收敛于 $\Gamma_{CL}^{(u)}$（依弱收敛意义）。

定理 3.6 （[Woo17，定理 6.1]的推论）。设 $\varepsilon > 0$ 和 G 是有限阿贝尔群，对于 R，具有 $R = \mathbb{Z}$、$R = \mathbb{Z}_p$或 $R = \mathbb{Z}/a\mathbb{Z}$，具有 n模结构。对每个自然数 X_n，设 ε是一个平衡的对称 $n \times n$ 矩阵，矩阵项取自 R。存在 c、$K > 0$，仅取决于ε和 G，使得

$$\left|\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n), G)] - |\wedge^2 G|\right| \leq Ke^{-cn}$$

特别地，余核(X_n)弱收敛到 $\Gamma_{sandpile}$。

注 3.7. 如果 $R = \mathbb{Z}$ 或 $\mathbb{Z}_p$，当 G 的指数整除 a时，从余核(X_n)到 $\twoheadrightarrow G$ 的满射总是唯一地经由 $\mathbb{Z}/a\mathbb{Z}$ 分解。因此，在不失一般性的前提下，本文余下部分将仅考虑 $R = \mathbb{Z}/a\mathbb{Z}$。

事实上，Nguyen 和 Wood [NW22；NW25] 证明，在这两种情形下，余核实际上都按集合意义强收敛到极限分布，尽管他们对矩阵项施加了独立同分布假设。本文的结果仅限于弱收敛，但若能了解强收敛是否仍成立，将会很有意思。

我们简要概述定理 3.6 证明中的一些思路，这些思路对我们有所帮助。类似（但更简单）的方法也可用于证明定理 3.5。第一步是注意到，满射 coker(X_n) $\twoheadrightarrow G$ 对应于在 $R^n \twoheadrightarrow G$ 的像上取值为零的满射X_n。因此，我们得到以下众所周知的结果：

引理 3.8。 设 X_n 是一个取值于 R 上的随机 $n \times n$ 矩阵， G 是一个具有 R-模结构的有限阿贝尔群。那么

$$\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n), G)] = \sum_{F\colon R^n \twoheadrightarrow G} \mathbb{P}[F \circ X_n = 0]$$

理想情况下，我们可以针对每个 F 直接计算 $\mathbb{P}[F \circ X_n = 0]$，然后再求和。如果 F 足够一般，我们希望 $F \circ X_n$ 的分布容易理解，因为与 F 复合会混合构成 X_n 的许多独立随机性来源。我们将“足够一般”这一概念所需的条件精确表述如下：

定义 3.9。 对于 $\sigma \subset [n]$，记 R^n_σ 为由 R^n 中未 以 σ 为索引的标准基元素张成的子模。

我们称 $F \in \operatorname{Hom}(R^n, G)$ 是距离为 w 的码，如果对于每个满足 $\#\sigma < w$ 的 $\sigma \subset [n]$，映射 $F|_{R^n_\sigma}\colon R^n_\sigma \to G$ 都是满射。

于是我们有：

引理 3.10 ([Woo17，引理 4。1])。 设 ε， $w > 0$，设 a 为正整数，且 $R = \mathbb{Z}/a\mathbb{Z}$，并设 G 为指数整除 a的有限阿贝尔群。存在常数 $K > 0$ 使得以下结论成立。

令 X_n 为一个随机的 ε-平衡对称 $n \times n$ 矩阵，将其视为映射 $(R^n)^* \to R^n$。令 F 为一个距离为 w的码。令 $A \in \operatorname{Hom}((R^n)^*, G)$。对于所有 n， 我们有

$$\left|\mathbb{P}[F \circ X_n = 0] - |\wedge^2 G||G|^{-n}\right| \le \frac{K \exp\left(\frac{\varepsilon w}{4a^2}\right)}{|G|^n}$$

and

$$\mathbb{P}[F \circ X_n = A] \le K|G|^{-n}$$

引理 3.10 的第二部分并非引理 3.8 中由码 F产生的矩计算主项所必需。不过，当我们尝试处理 $F\colon R^n \to G$这类非码映射时，它就会派上用场。其思路是，任意映射 $F\colon R^n \to G$ 经过适当限制后，都是映到某个子群上的码。若 H 在 G 中的指数足够小，那么只需对映入 H 的限制映射的行为有所控制，就足以证明非码的贡献可以忽略不计。

为更严谨地说明这一点，Wood 按照非码 $F\colon R^n \to G$ 所能映到的最大子群 $H \le G$ 的指数，对它们进行分层：

定义 3.11. 对于素因数分解为 $D = \prod_i p_i^{e_i}$ 的整数 D，我们定义 $\ell(D) = \sum_i e_i$。

w-深度 映射 $F\colon R^n \to G$ 的深度，是满足存在一个子集 $\sigma \subset [n]$，使得 $\#\sigma < \ell(D)w$ 且 $D = [G : F(R^n_\sigma)]$, 的最大正整数 D；如果不存在这样的 D，则深度为 1。

我们注意到， w-深度为 1 的映射是距离为 w 的码。对于深度大于 1 的映射数量，我们有如下界：

引理 3.12 ([Woo17，引理 5。2])。 存在一个常数 K，其取决于 G，使得若 $D > 1$，则至多有

$$K\binom{n}{\lceil \ell(D)w \rceil - 1}|G|^n D^{-n+\ell(D)w}$$

从 w-深度 D 映射 $R^n \to G$。

于是，引理 3.10 可用于在 F 是一个码时界定 $\mathbb{P}[F \circ X_n = 0]$。如果对于任意子集 $\eta \subset [n]$ 以及满足$\mathcal{P}$的任意随机矩阵 X，随机矩阵 $X_{\eta\eta} = (X_{ij})_{i,\ j\in\eta}$ 都具有性质 $\mathcal{P}$，那么我们称方阵随机矩阵在 R 上的性质 $\mathcal{P}$ 是稳定的。稳定性质的例子包括：

- 所有矩阵都满足的平凡性质；
- 具有该性质，即 X 以概率 1 为对称矩阵；
- 具有该性质，即存在一个矩阵 C，使得 X 以概率 1 为 C-对称。

我们还称 X 具有许多独立元素，如果当$\{i,j\}$ 遍历 $[n]$的二元子集时，矩阵项 $(X_{ij}, X_{ji}) \in R^2$ 相互独立。特别地，除非$\{i,j\} = \{k,\ell\}$，否则 X_{ij} 与 $X_{k\ell}$ 相互独立。

以下引理在 [Woo17的引理 5 中针对对称矩阵得到证明。4], 但考察证明可知，该引理在此处给出的更一般情形下也成立。

引理 3.13。设 $\varepsilon > 0$，令 a 为正整数，且 $R = \mathbb{Z}/a\mathbb{Z}$，并令 G 为指数整除 a 的有限阿贝尔群。

设 X_n 是一个具有稳定性质 $\mathcal{P}$ 的随机 $n \times n$ 矩阵，其含有许多独立的 ε-平衡元素。

令 $F\colon\ R^n \to G$ 具有 w-深度 $D > 1$，且 $[G\colon\ F(R^n)] < D$。

假设以下条件成立：

（A）对于任意指数整除 a 的有限阿贝尔群 H、任意具有 $\mathcal{P}$ 且含有许多独立的 ε-平衡元素的 $m \times m$ 随机矩阵 Y_m、任意距离为 w 的码 $F'\colon\ R^m \to H$，以及任意映射 $A \in \mathrm{Hom}((R^m)^*, G)$，存在一个仅依赖于 a、H、w/m 的常数 K'，使得

$$\mathbb{P}[F' \circ Y_m = A] \le K'|H|^{-m}$$

那么存在一个仅依赖于 ε、a、G、w/n、D 的常数 $K > 0$，使得 t

$$\mathbb{P}[F \circ X_n = 0] \le K\left(e^{-\varepsilon}\frac{|G|}{D}\right)^{\ell(D)w-n}$$

最后，为了证明定理 3.6 (分别地，定理 3.5）、引理 3.10(分别地，关于非对称矩阵的类似结果）、引理 3.12和引理 3.13，我们将它们结合起来计算引理 3.8中求和式的右侧。我们将在引理4.2 中针对 C-对称矩阵的情形，更一般地推导这一结果。

4. Reduction to Symmetric Case

引理 4.1。设 $0 < \varepsilon, \delta < 1$。设 $a \in \mathbb{Z}_{>0}$ 和 G 为指数整除 a的有限阿贝尔群。则存在 $K, c > 0$，使得以下结论成立：

设 C 为一个矩阵项属于 $R := \mathbb{Z}/a\mathbb{Z}$的确定性交错矩阵。设 X 为一个随机的 C-对称矩阵，其对角线及以上的矩阵项相互独立且 ε-平衡。设 $F\colon\ R^n \to G$ 为一个距离为 δn的码。设 $A \in \mathrm{Hom}((R^n)^*, G)$。

如果不存在满足 $F \circ M = A$ 的 C-对称矩阵 M，那么 $\mathbb{P}[F \circ X = A] = 0$。

否则，我们有

$$\left|\mathbb{P}[F \circ X = A] - |\wedge^2 G||G|^{-n}\right| \le \frac{K\exp(-cn)}{|G|^n}$$

证明。 没有 C-对称矩阵 M 满足 $F \circ M = A$ 的情形显然。

现在假设 M 是一个 C-对称矩阵，且满足 $F \circ M = A$。那么 $X - M$ 是对称矩阵，并且由于 M 是确定性的， $X - M$ 仍然具有独立的、 ε在对角线上方平衡的矩阵项。此外， $F \circ X = A$ 当且仅当 $F \circ (X - M) = 0$。于是结论由 [Woo17，引理 41] 得出。 □

称映射 $F \in \mathrm{Hom}(R^n, G)$ 对交替 C 是各向同性的，若存在一个 C-对称矩阵 M 满足 $F \circ M = 0$。矩计算中的主项为

$$\sum_{F \text{ code}} \mathbb{P}[F \circ X = 0] \approx |\wedge^2 G| \frac{\#\{F \in \mathrm{Hom}(R^n, G) \mid F \text{ is a code of distance } \delta n \text{ isotropic for } C\}}{|G|^n}.$$

我们将把右侧的分数解释为均匀随机映射 $R^n \to G$ 对 C 各向同性（且是一个距离为 δn的码）的概率。以下引理处理所有误差项，使我们能够专注于计算这一概率。

引理 4.2. 设 $a \in \mathbb{Z}_{>0}$，且 G 是指数整除 a的有限阿贝尔群。设 $\varepsilon > 0$。那么存在 K、$c > 0$，使得以下结论成立：

设 C 是一个 $n \times n$ 交错矩阵，其矩阵项属于 $R := \mathbb{Z}/a\mathbb{Z}$。设 X 是一个随机C-对称矩阵，其对角线及对角线以上的矩阵项相互独立且 ε-平衡。设 F 是一个均匀随机同态 $R^n \to G$。那么

$$\left| \mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X), G)] - |\wedge^2 G| \mathbb{P}[\widetilde{F} \textit{ is isotropic for } C] \right| \leq K e^{-cn}$$

证明。 这一计算的大部分与例如 [Woo17，定理 6.1、定理 62] 以及 [Woo19，定理 29]的证明相同。详见该处。

令 $\delta > 0$ 足够小：我们稍后将选取它，以使误差呈指数衰减。将映射$F\colon\ R^n \to G$ 分为距离为 δn 的码与非码。根据引理 3.8 ，我们希望计算

$$\begin{aligned}
&|\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X), G)] - |\wedge^2 G|\mathbb{P}[\widetilde{F} \text{ is isotropic for } C]| \\
&= \left| \sum_{F\in \operatorname{Sur}(R^n,G)} \mathbb{P}[F\circ X = 0] - \sum_{\substack{F\in\operatorname{Hom}(R^n,G)\\ F \text{ isotropic}}} \frac{|\wedge^2 G|}{|G|^n} \right| \\
&\leq \left| \sum_{\substack{F\in \operatorname{Sur}(R^n,G)\\ F \text{ code}}} \mathbb{P}[F\circ X = 0] - \sum_{\substack{F\in\operatorname{Sur}(R^n,G)\\ F \text{ code}\\ F \text{ isotropic}}} \frac{|\wedge^2 G|}{|G|^n} \right| && (1)\\
&\quad + \sum_{\substack{D>1\\ D||G|}} \sum_{\substack{F\in\operatorname{Sur}(R^n,G)\\ F \text{ depth } D}} \mathbb{P}[F\circ X = 0] && (2)\\
&\quad + \sum_{\substack{D>1\\ D||G|}} \sum_{\substack{F\in\operatorname{Sur}(R^n,G)\\ F \text{ depth } D\\ F \text{ isotropic}}} \frac{|\wedge^2 G|}{|G|^n} && (3)\\
&\quad + \sum_{F\in\operatorname{Hom}(R^n,G)\setminus\operatorname{Sur}(R^n,G)} \frac{|\wedge^2 G|}{|G|^n} && (4)
\end{aligned}$$

我们分别对每一项进行估计。由引理 4.1，可得

$$(1)\qquad \left| \sum_{\substack{F\in \operatorname{Sur}(R^n,G)\\ F \text{ code}}} \mathbb{P}[F\circ X = 0] - \sum_{\substack{F\in\operatorname{Sur}(R^n,G)\\ F \text{ code}\\ F \text{ isotropic}}} \frac{|\wedge^2 G|}{|G|^n} \right| \leq |G|^n \frac{K_1 e^{-c_1 n}}{|G|^n} = K_1 e^{-c_1 n}$$

对于某个 $K_1,\ c_1 > 0$，它仅取决于 $a,\ G,\ \varepsilon,\ \delta$。

此外，由引理 4.1，引理 3.13 的条件 (A) 成立，因此若 F 具有 δn-深度 D，则$\mathbb{P}[F\circ X = 0] \leq K'_{2,D}\exp(-\varepsilon(1-\ell(D)\delta)n)|G|^{(\ell(D)\delta-1)n}D^{(1-\ell(D)\delta)n}$，其中某个常数为 $K'_{2,D} > 0$，且仅取决于 $a, G, \varepsilon, \delta, D$。然后由引理 3.12 可得

$$\sum_{\substack{F\in \operatorname{Sur}(R^n,G)\\ F \text{ depth } D}} \mathbb{P}[F\circ X = 0] \leq K_{2,D}\binom{n}{\lceil \ell(D)\delta n\rceil - 1} \exp(\varepsilon(1-\ell(D)\delta)n)|G|^{\ell(D)\delta n}$$

现在可以将 δ 取足够小，使得右侧被某个常数乘以 $\exp(-c_2 n)$ 所界，其中 $c_2 > 0$ 取决于 $a,\ G,\ \varepsilon,\ D$。由于 $|G|$ 只有有限个约数，我们得到

$$(2)\qquad \sum_{\substack{D>1\\ D||G|}} \sum_{\substack{F\in\operatorname{Sur}(R^n,G)\\ F \text{ depth } D}} \mathbb{P}[F\circ X = 0] \leq K_2 e^{-c_2 n}$$

其中 $K_2 > 0$ 仅取决于 a， G， ε。类似但更简单的计算可得

$$\sum_{\substack{D>1\\ D\|G|}} \sum_{\substack{F\in \mathrm{Sur}(R^n,G)\\ F \text{ depth } D\\ F \text{ isotropic}}} \frac{|\wedge^2 G|}{|G|^n} \le \sum_{\substack{D>1\\ D\|G|}} \sum_{\substack{F\in \mathrm{Sur}(R^n,G)\\ F \text{ depth } D}} \frac{|\wedge^2 G|}{|G|^n} \le K_3 e^{-c_3 n} \tag{3}$$

其中常数 K_3， $c_3 > 0$ 仅取决于 a， G， ε。

对于（4），我们记

$$\begin{aligned}\sum_{F\in \mathrm{Hom}(R^n,G)\setminus \mathrm{Sur}(R^n,G)} \frac{|\wedge^2 G|}{|G|^n} &\le \sum_{H\lneq G} \sum_{F\in \mathrm{Hom}(R^n,H)} \frac{|\wedge^2 G|}{|G|^n} \\ &= \sum_{H\lneq G} |\wedge^2 G| \left(\frac{|H|}{|G|}\right)^n \\ &\le K_4 2^{-n}\end{aligned} \tag{4}$$

其中某个常数 K_4 仅取决于 G。结合这些界即可得到所需结果。□

~为便于在接下来的章节中计算矩 $|\wedge^2 G|\mathbb{P}[F$关于 $C]$ 的各向同性条件，我们~给出一个关于 F 的条件，该条件等价于其关于 C各向同性。在第 5 节中，我们将具体推导该条件在若干特殊情形下的含义，例如 R 为有限域的情形，这将说明定义中使用“各向同性”一词的合理性。

设 C 是一个双线性映射 $(R^n)^* \times (R^n)^* \to R$，其中 $R = \mathbb{Z}/a\mathbb{Z}$ 是一个有限循环群。设 $G = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$是一个有限阿贝尔群，且 $d_1 \mid d_2 \mid \cdots \mid d_n \mid a$。设 $F\colon R^n \to G$ 是一个同态。

对于 $1 \le k \le n$，令 $R_k := R \otimes_{\mathbb{Z}} \mathbb{Z}/d_k\mathbb{Z} \cong \mathbb{Z}/d_k\mathbb{Z}$ 且

$$G_k := G \otimes_R R_k = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{k-1}\mathbb{Z} \times (\mathbb{Z}/d_k\mathbb{Z})^{n-k+1}$$

令 $\pi_k\colon G \to G_k$ 为投影。将 G_k 视为一个 R_k-模，因此 $G_k^* = \mathrm{Hom}(G_k, R_k)$。

注意，若 V 是一个 R-模，则

$$\mathrm{Hom}(V,R) \otimes_{\mathbb{Z}} \mathbb{Z}/d_k\mathbb{Z} \cong \mathrm{Hom}(V,R) \otimes_R R_k \cong \mathrm{Hom}(V, R_k) \cong \mathrm{Hom}(V \otimes_R R_k, R_k),$$

其中所有同构都是典范的，最后一个同构源于任意映射 $V \to R_k$ 都可经由 V/d_kV分解这一事实。

我们将 C解释为映射 $(R^n)^* \to R^n$，对每个 k，将矩阵项模 d_k约化后，该映射诱导出映射 $C_k\colon (R_k^n)^* \to R_k^n$。此外，对每个 k， F 也诱导出映射 $F_k\colon R_k^n \to G_k$。

命题 4.3。令 C 为交替的。令 $F \in \mathrm{Sur}(R^n, G)$。

以下各项等价：

(1) F 关于 C是各向同性的。

(2) 我们有

$$F_k \circ C_k \circ F_k^* = 0 \qquad \textit{for all } k = 1, \dots, n$$

(3) G_k^* 上的交替双线性型由下式给出：

$$F_k \circ C_k \circ F_k^*$$

对所有 $k = 1, \dots, n$，在 G_k^* 的最后 $n - k + 1$ 个坐标上为零。

证明。 第一个条件蕴含第二个条件：

与 $\mathbb{Z}/d_k\mathbb{Z}$ 张量化后， R 上的 C-对称矩阵 M 变为 R_k 上的 C_k-对称矩阵 M_k，且 $F_k \circ M_k = 0$ 若 $F \circ M = 0$。于是 $M_k - M_k^\intercal = C_k$ 推出

$$F_k \circ C_k \circ F_k^* = F_k \circ M_k \circ F_k^* - F_k \circ M_k^\intercal \circ F_k^* = (F_k \circ M_k) \circ F_k^* - F_k \circ (F_k \circ M_k)^* = 0.$$

第二个条件立即推出第三个条件。

我们通过在坐标中进行推导，证明第三个条件推出第一个和第二个条件。注意，命题中的三个条件都不依赖于 R^n 的基的选取。

利用史密斯标准形，构造 R^n 的一组基 $e_1, \dots, e_n$，使映射 $F\colon R^n \to G$ 在每个坐标上都是投影 $R \to \mathbb{Z}/d_k\mathbb{Z}$。我们将明确确定条件 (1) 和 (3) 对于 C 在这组基下的矩阵所表达的含义。

令 $e_{k,i}$ 为将模 d_k 化简后得到的 R_k^n 的基。令 $\phi_{k,i}$ 为 $(R_k^n)^*$ 的对偶基，由 $\phi_{k,i}(e_{k,j}) = \delta_{ij}$ 给出。令 $g_{k,i} = f_k(e_{k,i})$ 为 G_k 的生成集，并令 $\chi_{k,i}$ 为由 $\chi_{k,i}(g_{k,j}) = \frac{d_k}{d_i}\delta_{ij}$ 定义的对偶生成集。令 $c_{k,ij}$ 为 C 的第 ij 个元素，模 d_k。

映射 $F_k \circ C_k \circ F_k^*$ 在每个生成元 $\chi_{k,j}$ 上的行为如下：

$$G_k^* \xrightarrow{F_k^*} (R_k^n)^* \xrightarrow{\quad C_k \quad} R_k^n \xrightarrow{\quad F_k \quad} G_k$$

$$\chi_{k,j} \longmapsto \tfrac{d_k}{\min\{d_j,d_k\}}\phi_{k,j} \longmapsto \tfrac{d_k}{\min\{d_j,d_k\}}\sum_{i=1}^n c_{k,ij}e_{k,i} \longmapsto \tfrac{d_k}{\min\{d_j,d_k\}}\sum_{i=1}^n c_{k,ij}g_{k,i}$$

该映射在 G_k^* 上为零的条件是

$$\frac{d_k}{\min\{d_j,d_k\}}c_{k,ij} \equiv \frac{d_k}{\min\{d_j,d_k\}}c_{ij} \equiv 0 \pmod{\min\{d_i,d_k\}}$$

对所有 i,j均成立。注意，由于 C的反对称性，我们可以在这些条件中交换 i 和 j。当$i,j \geq k$时，我们要求 $c_{ij} \equiv 0$ （模 d_k）。

这些条件之间存在一些冗余。当 $i < k$ 或 $j < k$时，关于 $c_{k,ij}$ 的条件已经由关于 $c_{i,ij}$的条件得到满足。（这表明条件 (3) 蕴含条件 (2)。）

现在在这个基下， $F \circ M = 0$ 的条件等价于要求 M 的第 k行可被 d_k整除。

假设条件 (3) 得到满足且 C 为交替的，我们通过任意选取对角线下方及对角线上的矩阵项（即满足 $i \geq j$的矩阵项）来构造一个 C-对称矩阵 M，但要求第 i行中位于 m_{ij} 的矩阵项可被 d_i整除。于是，对于这样选定的上三角矩阵项，存在唯一的 C-对称矩阵 M，当 $i \geq j$时由 $m_{ji} = m_{ij} - c_{ij}$ 给出。由于 $d_j \mid c_{ij}$ 和 $d_j \mid d_i \mid m_{ij}$，我们得到 $d_j \mid m_{ji}$，因此有 $F \circ M = 0$。□

注 4.4. 请注意，命题 4.3 中的等价关系是在 F 为满射$R^n \to G$时陈述的。将 F 视为逐坐标投影时，我们会用到这一假设。然而，在引理 4.2中，我们需要知道随机同态 $R^n \to G$ 对于C是各向同性的概率。无论条件 (3) 是否等价于各向同性，我们都会发现，求随机同态满足命题 4.3中条件 (3) 的概率要方便得多。

只需再做一些工作，命题 4.3 的条件就可以推广到非满射同态。不过，对于我们想要得到的结果，无需这样做，因为几乎所有

$\sim$（作为 $n \to \infty$）同态 $R^n \to G$ 都是满射。如果 F 是均匀随机同态$R^n \to G$，则有

$\sim\mathbb{P}[F$ 对 $C] = \mathbb{P}[F$ 是各向同性的 C 且是满射$]+\mathbb{P}[F$ 对 C 是各向同性的$]$且不是满射，同理，

$\sim\mathbb{P}[F$ 满足 (3)$] = \mathbb{P}[F$ 满足 (3) 且是满射$] + \mathbb{P}[F$ 满足 (3) 且不是满射$]$因此，应用命题 4.3后，我们得到

$$\sim|\mathbb{P}[F \text{ 对 } C] - \mathbb{P}[F \text{是各向同性的}]| \leq \mathbb{P}[F \text{满足 (3) } C \text{ 且不是满射}]$$

$$\sim+ \mathbb{P}[F \text{ 满足 (3) 且不是满射}].$$

我们有

$$\mathbb{P}[\widetilde{F} \text{ is not surjective}] \leq \frac{1}{|G|^n} \sum_{H \lneq G} \#\operatorname{Hom}(R^n, H) = \sum_{H \lneq G} \left(\frac{|H|}{|G|}\right)^n = K2^{-n}$$

对某个仅依赖于 G 的常数 K 。

$\sim$因此，项 $\mathbb{P}[F$ 对 $C]$ 在引理 4.2 中是各向同性的，可以安全地替换为 $\mathbb{P}[F$ 满足 (3)$]$，而不改变其他任何内容。这一改动只会额外引入一个指数误差项。

5. Isotropy over a Finite Field and Very Small Perturbations

在本节中，我们专门考虑 C 可被 a/p 整除的情形，其中 p 是整除 a 的素数。在此情形下，各向同性条件中唯一非平凡的部分处于“模 p”之中。作为推论，我们将看到，当 $a = p$ 为素数时，各向同性条件具有一种特别优美的形式，从而说明用“各向同性”一词来描述该条件是合理的。

引理 5.1. 设 $R = \mathbb{Z}/a\mathbb{Z}$，并设 $p \mid a$ 为素数。设 C 为 R^n 上可被 $b := a/p$ 整除的交替双线性型，并设C 为 $(R/pR)^n \cong \mathbb{F}_p^n$ 上由 C/b 诱导的型。固定 $r > 0$，并设 $F \in \operatorname{Sur}(R^n, R^r)$。设 $F \in \operatorname{Sur}(\mathbb{F}_p^n, \mathbb{F}_p^r)$ 为将 F 模 p 约化所得到的映射。设$V \subset \mathbb{F}_p^n$ 为 $F^*\colon \mathbb{F}_p^r \to \mathbb{F}_p^n$ 的像。则 F 对 C 是各向同性的，当且仅当 V 对C 在 $\mathbb{F}_p^n$ 的子空间意义下是各向同性的。

特别地，如果 $a = p$，那么 F对于 C是各向同性的，当且仅当 F^* 的像作为 $\mathbb{F}_p^n$的子空间对于 C是各向同性的。在本引理的表述以及本节的其余部分中，我们将自由地把 $\mathbb{F}_p^n$ 与 $(\mathbb{F}_p^n)^*$ 等同起来，并同样将其与 $\mathbb{F}_p^r$等同起来。

证明。 这里 $G = 1^{n-r} \times \mathbb{F}_p^r$，因此对于 $k = 1, \ldots, n-r$，我们有 $R_k = 0$。对于 $k = n-r+1, \ldots, n$，我们有 $R_k = R$ 和 $G_k = R^{n-k+1}$。

由命题 4.3，我们有 F对于 C是各向同性的，当且仅当复合 $F \circ C \circ F^*$为零。我们将其视为定义在 $(R^r)^*$ 上的双线性形式。由于 C 可被 b整除，所得双线性形式在 $p(R^r)^*$上为零，因此它下降为定义在 $\mathbb{F}_p^r$上的双线性形式，其定义为 $F \circ C \circ F^*$。该双线性形式为零，恰好等价于 V 对于 C是各向同性的条件。 □

如果 C 非零，那么当 F 为均匀随机时，不难证明 $\mathbb{P}[F$ 对于远离 0 的 $C]$ 是各向同性的概率存在一致上界。令 c 为 C 的秩。

使用引理5.1中的记号。

令 $W := \mathbb{F}_p^n / \operatorname{rad}(\overline{C})$ 为 $\mathbb{F}_p^n$ 关于交错形式 C 的根基的商，并令 $V = \operatorname{im}(F^*)$。令 $\pi\colon \overline{\mathbb{F}_p^n} \twoheadrightarrow W$ 为投影。于是 C 诱导出 W 上的非退化交错形式 $\pi_* \overline{C}$。当且仅当 V 对 C 各向同性，当且仅当 $\pi(V)$ 对 $\pi_* C$ 各向同性时，F 对 C 各向同性。

设 $v_1, \dots, v_r$ 是 F^* 的列。若 $\overline{F} \in \operatorname{Hom}(R^n, R^r)$ 是均匀随机的，则 $v_1, \dots, v_r$ 是 $\mathbb{F}_p^n$ 中均匀随机且相互独立的向量。像 $\pi(v_1) \dots, \pi(v_r)$ 在 W 中均匀分布。$\pi(v_1)$ 与 $\pi(v_2)$ 配对为零的概率为

$$\mathbb{P}[\pi(v_1) = 0] + \mathbb{P}[\pi(v_1) \neq 0]\mathbb{P}[\pi_* \overline{C}(\pi(v_1), \pi(v_2)) = 0 \mid \pi(v_1) \neq 0] = p^{-c} + (1 - p^{-c})p^{-1}$$

So,

$$\mathbb{P}[F \text{ is isotropic for } C] \leq p^{-1} + p^{-c} - p^{-1-c} = p^{-1} + p^{-c}(1 - p^{-1})$$

等号成立当 $r = 2$ 时。只要 $c \geq 1$，该值就与 1 保持正距离。

注5.2。设 C 是一个定义在 $\mathbb{Z}/a\mathbb{Z}$ 上的 $n \times n$ 矩阵，其余核可由 g 个元素生成。那么对于素数 $p \mid a$，C 模 p 的秩至少为 $n - g$。如果 a 仅被一个素数 p 整除，那么 C 的余核所需的生成元的最大数量恰好等于 C 模 p 的余秩。

作为这些显式计算的推论，我们可以了解当 X 的余核在 X 是一个大的 ε-平衡 C-对称矩阵，且处于中间区域时，其余核的矩（此时C 具有非常大的余核，但不是零矩阵）。在这种情况下，如果极限矩存在，它们既不同于 $\Gamma_{sandpile}$ 的矩，也不同于 $\Gamma_{CL}^{(0)}$ 的矩。定理 5.3表明，只有当 $\Gamma_{sandpile}$ 以适当的意义趋于 0 时，C-对称矩阵才能达到这些极限矩；而定理 5.4 表明，只有当 $\Gamma_{CL}^{(0)}$ 的秩（更一般地说，$|\wedge^2 G[h]|$ 定理 1.3 中的极限矩）只能由 C-对称矩阵达到，前提是 C（更一般地说，C/h）模 p 的秩无界。

定理 5.3。设 $a \in \mathbb{Z}_{>0}$。对于每个自然数 n，设 C_n 是一个确定性的 $n \times n$交错矩阵，其矩阵项属于 $R := \mathbb{Z}/a\mathbb{Z}$。设 X_n 是一个随机的 C_n-对称矩阵，其对角线及其上方的矩阵项相互独立，且 ε-平衡。

那么，下列条件等价：

(1) 对于任意指数整除 a 的有限阿贝尔群 G，都有

$$\lim_{n \to \infty} \mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n), G)] = |\wedge^2 G|.$$

(2) 对所有足够大的 n，都有 $C_n = 0$。

这个定理表明，定理 3.6 （大型对称矩阵的余核普适性）的结论，在对称条件的小扰动下远非稳定。将定理应用于所有取值的 a 可知，若 X_n 是一个 C_n-对称矩阵序列，其余核依照备注 3.2的意义弱收敛到 $\Gamma_{sandpile}$，那么 C_n 最终会模任何整数为零。这并不意味着 C_n 最终本身就为零；我们也不能指望证明这样的结论，因为弱收敛只能反映“模 a”的信息。若在$\mathbb{Z}_p$上讨论，这个条件可以理解为：C_n 在 p-进意义下收敛到 0，也就是说，它最终能被 p的任意大的幂整除。

证明。蕴含关系 (2) $\implies$ (1) 是定理3.6。我们将证明 $\neg(2) \implies \neg$(1)。

假设 $C_n \neq 0$ 对无穷多个 n成立。由于 a 只有有限多个素因子，因此存在一个素数 $p \mid a$，使得 $C_n \neq 0$（模 p^f）对某个足够大的 f 成立，其中 $p^f \mid a$。令 f 为具有此性质的最小值，因此对所有足够大的 n，$p^{f-1} \mid C_n$ 都成立，但对无穷多个 n，$p^f \nmid C_n$ 成立。

不妨设 $a = p^f$，否则将 R 替换为 $R/p^f R$。由于对于无穷多个 n有 $p^f \nmid C_n$，因此 C_n/p^{f-1} 在 $(R/pR)^n$ 上无穷多次诱导出具有正秩的交错形式。上述论证表明，对于这样的 n，如果 F 是一个满足 $r \geq 2$的 $R^n \to R^r$ 上的均匀随机同态，那么 $\mathbb{P}[F$ 是各向同性的，而 $C_n]$ 以关于 p一致远离1的量为界。因此

$$\limsup_{n\to\infty} \mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n), (\mathbb{Z}/p^f\mathbb{Z})^r)] < |\wedge^2 (\mathbb{Z}/p^f\mathbb{Z})^r|$$

对于 $r \geq 2$，结论得证。 □

定理5.4。 设 $a \in \mathbb{Z}_{>0}$，并设 $h \mid a$。对于每个自然数 n，令 C_n 为一个确定性的$n \times n$ 交错矩阵，其矩阵项属于 $R := \mathbb{Z}/a\mathbb{Z}$ 均可被 h整除。令 X_n 为一个随机的 C_n-对称矩阵，其对角线及对角线以上的矩阵项相互独立且 ε-平衡。令 $p \mid a/h$为素数。若 C_n/h 模 p 的秩有界，则有

$$\liminf_{n\to\infty} \mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n), (\mathbb{Z}/hp\mathbb{Z})^2)] > |\wedge^2 (\mathbb{Z}/hp\mathbb{Z})^2[h]|.$$

特别地，当 $h = 1$时，这意味着，一个 ε-平衡的 C_n-对称矩阵序列只有在 C_n 模 p的秩对每个p都无限增长时，才表现出 Cohen-Lenstra余核普遍性。在 $\mathbb{Z}_p$上，根据备注 5.2，我们得到定理 1.2的逆命题。

证明。不妨设 $a = hp$，否则就将 R 替换为 R/hpR。令$F \in \operatorname{Hom}(R^n, R^2)$服从均匀随机分布。备注 5.2 之前的论证表明

$$\mathbb{P}[F \text{ is isotropic for } C_n] > p^{-1} = p^{-\binom{2}{2}} = \frac{|\wedge^2 (\mathbb{Z}/hp\mathbb{Z})^2[h]|}{|\wedge^2 (\mathbb{Z}/hp\mathbb{Z})^2|}.$$

事实上，对于 $C_n]$， $\mathbb{P}[F$ 是各向同性的，其概率以 C_n/h模 p的秩上界为条件而与 p^{-1} 保持有界距离。

结论由引理4.2得出。 □

6. Computing Isotropy Probabilities

在本小节中，假设 C 足够一般，我们计算均匀随机映射 $F\colon R^n \to G$ 是距离为 δn 的码且对于 C为各向同性的概率。

命题 4.3 将验证映射 $F \in \operatorname{Sur}(R^n, G)$ 对双线性形式 C 是各向同性的这一问题，化为在自由 R_k-模中进行一系列计算：我们只需验证双线性形式 $F_k \circ C_k \circ F_k^*$限制在 $R_k^{n-k+1} \subseteq G_k^*$上时为零。

令 h 为 C的矩阵项的一个最大公约数。

其思路是，$F_k \circ C_k \circ F_k^*|_{R_k^{n-k+1}}$在 R_k^{n-k+1} 上所有矩阵项均被 h整除的交错形式中，近似均匀分布。注意，这样的型可以视为$(R_k/R_k[h])^{n-k+1}$上的交错形式。在$F_{k-1} \circ C_{k-1} \circ F_{k-1}^*|_{R_{k-1}^{n-k+2}}$ 消失的条件下，我们得到一个关于 $d_{k-1}\mathbb{Z}/d_k\mathbb{Z}$ 的条件，我们预期该条件约有

$$\frac{|\wedge^2 ((R_{k-1}/R_{k-1}[h])^{n-k+1})|}{|\wedge^2 ((R_k/R_k[h])^{n-k+1})|} = \left(\frac{d_{k-1}\gcd(d_k, h)}{d_k \gcd(d_k, h)}\right)^{\binom{n-k+1}{2}}$$

的概率会成立。因此，所有这些条件都成立的概率约为

$$\begin{aligned}\prod_{k=1}^{n}\left(\frac{d_{k-1}\gcd(d_k,h)}{d_k\gcd(d_{k-1},h)}\right)^{\binom{n-k+1}{2}} &= \prod_{k=1}^{n}\left(\frac{\gcd(d_k,h)}{d_k}\right)^{\binom{n-k+1}{2}-\binom{n-k}{2}}\\ &= \prod_{k=1}^{n}\left(\frac{\gcd(d_k,h)}{d_k}\right)^{\binom{n-k+1}{2}-\binom{n-k}{2}}\\ &= \prod_{k=1}^{n}\left(\frac{\gcd(d_k,h)}{d_k}\right)^{n-k} = \frac{|\wedge^2 G[h]|}{|\wedge^2 G|}\end{aligned}$$

的时间。

现在， $F_k^*|_{R_k^{n-k+1}}$只是一个带有 R_k中矩阵项的 $(n-k+1)\times n$矩阵（记作 M_k）。类似地，将 F_k与 G_k到最后 $n-k+1$个坐标的投影复合，所得结果就是这个矩阵的转置。因此，$F_k\circ C_k\circ F_k^*|_{R_k^{n-k+1}} = M_k^\intercal C_k M_k$只是三个 R_k上矩阵的乘积。类似地， $F_{k-1}\circ C_{k-1}\circ F_{k-1}^*|_{R_{k-1}^{n-k+1}}$是将这三个矩阵中的矩阵项模 d_{k-1}化简后得到的。因此，我们真正关心的是：在 M_k均匀随机，且以$M_k^\intercal C_k M_k$的矩阵项都能被 d_k整除为条件时， $M_k^\intercal C_k M_k$为零的概率。

命题 6.1。设 R 是一个有限初等因子环。设 C 是一个矩阵项取自 R的交替 $n\times n$ 矩阵，且其余核可由 g 个 R 上的元素生成。设 M 是一个矩阵项取自 R的均匀随机 $n\times m$ 矩阵。设 S 是一个交替 $m\times m$ 矩阵。则

$$\left|\mathbb{P}[M^\intercal CM = S] - |R|^{-\binom{m}{2}}\right| \le 2^{m+g+1-n}$$

该命题将应用于 C_k/h ，其中 $R = R_k/R_k[h]$。

证明。设 $C = ADB$，其中 $A,\ B\in \mathbf{GL}_n(R)$，且 D 是对角线矩阵。由于 C 的余核可由 g 个元素生成，因此 D 至少有 $n-g$ 个对角线矩阵项是 R中的单位元。

设 v_1，.....， v_m是 M的各列。对于 $1\le \ell\le m$，令 M_ℓ为由 M的前 ℓ列构成的矩阵。令 S_ℓ为由S的第（$\ell+1$）列的前 ℓ 个矩阵项构成的 $\ell\times 1$ 矩阵。由于 C是交替的，当且仅当对 $1\le\ell\le m-1$有 $M^\intercal CM = SM_\ell^\intercal Cv_{\ell+1} = S_\ell$。由于 M是均匀随机的， v_ℓ 也是均匀随机的，因此 w_ℓ 也如此：对每个 ℓ，$= Bv_\ell$ 。我们的思路是对$M_\ell^\intercal$进行条件化，并计算 $M_\ell^\intercal ADw_{\ell+1} = S_\ell$的概率。注意， Dw_ℓ是一个矩阵项相互独立的向量，且每个矩阵项都在 R的某个理想中均匀分布。令 E_ℓ表示事件：对于 $1\le k\le \ell$， $M_k^\intercal ADw_{k+1} = S_k$；因此， E_{m-1}表示事件： $M^\intercal CM = S$且 $\mathbb{P}[E_0] = 1$。

我们有

$$\begin{aligned}\mathbb{P}[E_\ell] &= \sum_T \mathbb{P}[M_\ell^\intercal ADw_{\ell+1} = S_\ell \mid M_\ell^\intercal = TA^{-1}]\mathbb{P}[M_\ell^\intercal = TA^{-1}]\\ &= |R|^{-n\ell}\sum_T \mathbb{P}[M_\ell^\intercal ADw_{\ell+1} = S_\ell \mid M_\ell^\intercal = TA^{-1}]\\ &= |R|^{-n\ell}\sum_T \mathbb{P}[TDw_{\ell+1} = S_\ell]\end{aligned}$$

其中，$(TA^{-1})^\intercal$遍历满足如下条件的 $n\times\ell$矩阵 $\begin{bmatrix}t_1 & \cdots & t_\ell\end{bmatrix}$：若 $T_k = \begin{bmatrix}t_1 & \dots & t_k\end{bmatrix}$，则对 $1\le k<\ell$有$T_k^\intercal Ct_{k+1} = S_k$。注意，这类矩阵的数量 T为 $|R|^{n\ell}\mathbb{P}[E_{\ell-1}]$。

对于足够良好的 T，我们将能够证明

$$\mathbb{P}[TDw_{\ell+1} = S_\ell] = |R|^{-\ell}.$$

接下来，我们将估计不够理想、无法对 $\mathbb{P}[E_\ell]$ 得出估计的 T 的数量。

如果 T 的前 $n-g$ 列在 R 上张成 R^ℓ，我们就称 T 足够理想。下面的引理表明，如果 T 足够理想，则 $\mathbb{P}[TDw_{\ell+1} = S_\ell] = |R|^{-\ell}$:

引理 6.2。 假设 V 是一个有限的 R-模，且 U_1、...、U_k 是满足 $U_1 + \cdots + U_k = V$ 的子模。对于 $1 \le i \le k$，令 X_i 为 U_i 中的均匀随机元素，且这些 X_i 相互独立。那么， $X_1 + \cdots + X_k$ 是 V 中的均匀随机元素。

令 t_1、...、t_n 为 T 的列。令 α_1、...、α_n 为 D 的对角线矩阵项。令 X_1、...、X_n 为 $w_{\ell+1}$ 的矩阵项。我们有

$$TDw_{\ell+1} = \sum_{i=1}^{n} t_i\alpha_i X_i = \sum_{i=1}^{n-g} t_i\alpha_i X_i + \sum_{i=n-g+1}^{n} t_i\alpha_i X_i.$$

现在，对于 $1 \le i \le n-g$，我们有 $\alpha_i \in R^\times$，并且由于 X_i 在 R上服从均匀分布，因此 $t_i\alpha_i X_i$ 在 Rt_i 上也服从均匀分布。如果 t_1，$\ldots t_{n-g}$ 张成 R^ℓ，那么根据引理 6.2，和 $\sum_{i=1}^{n-g} t_i\alpha_i X_i$ 在 R^ℓ上服从均匀分布，因此 $TDw_{\ell+1}$ 也如此。

引理 *6.2* 的证明。对于每个 $1 \le i \le k$， X_i 在 U_i 上的分布是平移不变的。因此，对于任意满足以下条件的 $v = u_1 + \cdots + u_k \in V$： $u_i \in U_i$ 对每个 i均成立， X_i 的分布

$$X_1 + \cdots + X_k + v = (X_1 + u_1) + \cdots + (X_k + u_k)$$

与 $X_1 + \cdots + X_k$ 的分布相同。于是结论成立，因为均匀分布是 V 上唯一的平移不变分布。□

现在我们来界定那些不够好的 T 的数量。

引理 6.3。 假设 V 是一个由 ℓ 个元素生成的 R-模，且 $v_1, \ldots, v_k$ 是 V 中相互独立的均匀随机元素。我们有

$$\mathbb{P}[Rv_1 + \cdots + Rv_k \ne V] \le 2^{\ell-k}$$

那么， R^ℓ 中不能张成 R^ℓ 的 $(n-g)$ 元组数量至多为 $|R|^{\ell(n-g)} \cdot 2^{\ell-n+g}$；第一个 $n-g$ 个元素不能张成 R^ℓ 的 n 元组数量至多为 $|R|^{\ell n} \cdot 2^{\ell-n+g}$。不够好的、满足上述条件的 T 的数量不超过此数。

引理 *6.3* 的证明。 可以得到更精确的上界，但这对我们的目的而言并无必要。为证明此结论，我们可以假设 $\ell < k$，否则该命题为空。

令 $\mathfrak{m}$ 为 R 的一个极大理想，并令 $F = R/\mathfrak{m}$。令 $V = V/\mathfrak{m}V$，并令 v_i 为 v_i 模 $\mathfrak{m}$ 的约化，它们是 V 中相互独立的均匀随机元素。只有当 $Fv_1 + \cdots + Fv_k = V$ 时，我们才有 $Rv_1 + \cdots + Rv_k = V$。令 $d \le \ell$ 为 V 在 F 上的维数。

张成 V 的 k 元向量组的数量，与满射 $F^k \to F^d$ 的数量相同；根据对偶性，这也等于单射 $F^d \to F^k$ 的数量，即 $\prod_{i=0}^{d-1}(|F|^k - |F|^i)$。

因此， k 元向量组张成 V 的概率为

$$\prod_{i=0}^{d-1}(1-|F|^{i-k}) \geq \prod_{i=0}^{\ell-1}(1-2^{i-k}) \geq 1-\sum_{i=0}^{\ell-1}2^{i-k} = 1-2^{-k}(2^{\ell}-1).$$

□

现在我们有

$$\begin{aligned}
\left|\mathbb{P}[E_\ell] - |R|^{-\ell}\mathbb{P}[E_{\ell-1}]\right| &= \left||R|^{-n\ell}\sum_{T}\mathbb{P}[TDw_{\ell+1}=S_\ell] - |R|^{-\ell}\mathbb{P}[E_{\ell-1}]\right| \\
&= \left||R|^{-n\ell}\sum_{T \text{ nice}}\mathbb{P}[TDw_{\ell+1}=S_\ell] + |R|^{-n\ell}\sum_{T \text{ not nice}}\mathbb{P}[TDw_{\ell+1}=S_\ell] - |R|^{-\ell}\mathbb{P}[E_{\ell-1}]\right| \\
&\leq \left||R|^{-n\ell}\sum_{T \text{ nice}}|R|^{-\ell} - |R|^{-\ell}\mathbb{P}[E_{\ell-1}]\right| + 2^{\ell-n+g} \\
&= \left||R|^{-n\ell}\sum_{T \text{ not nice}}|R|^{-\ell}\right| + \ell\cdot 2^{\ell-n+g} \\
&\leq (1+|R|^{-\ell})2^{\ell-n+g} \\
&\leq 2^{\ell-n+g+1}
\end{aligned}$$

对 $1 \leq \ell \leq m-1$ 迭代这一过程，得到

$$\begin{aligned}
\left|\mathbb{P}[E_{m-1}] - |R|^{-\binom{m}{2}}\right| &= \left|\mathbb{P}[E_{m-1}] - |R|^{-(m-1)}\mathbb{P}[E_{m-2}]\right| + \left||R|^{-(m-1)}\mathbb{P}[E_\ell] - |R|^{-(m-1)-(m-2)}\mathbb{P}[E_{m-3}]\right| + \\
&\qquad \cdots + \left||R|^{-(m-1)-\cdots-2}\mathbb{P}[E_1] - |R|^{-\binom{m}{2}}\mathbb{P}[E_0]\right| \\
&\leq \sum_{\ell=1}^{m-1}|R|^{-\sum_{i=\ell+1}^{m-1}i}2^{\ell-n+g+1} \\
&= \sum_{\ell=1}^{m-1}|R|^{-\frac{(\ell+m)(m-\ell-1)}{2}}2^{\ell-n+g+1}.
\end{aligned}$$

现在我们有

$$2^{-m+n-g}\left|\mathbb{P}[E_{m-1}] - |R|^{-\binom{m}{2}}\right| \leq \sum_{\ell=1}^{m-1}|R|^{-\frac{(\ell+m)(m-\ell-1)}{2}}\cdot 2^{\ell-(m-1)}$$

在求和中将 ℓ 替换为 $m-1-\ell$，我们得到

$$2^{-m+n-g}\left|\mathbb{P}[E_{m-1}] - |R|^{-\binom{m}{2}}\right| \leq \sum_{\ell=0}^{m-2}|R|^{-\frac{\ell(2m-\ell+1)}{2}}2^{-\ell} \leq \sum_{\ell=0}^{m-2}2^{-\ell} \leq 2$$

从而

$$\left|\mathbb{P}[E_{m-1}] - |R|^{-\binom{m}{2}}\right| \leq 2^{m+g+1-n}$$

正如我们所希望的那样。 □

利用命题 6.1，我们可以计算 F 关于 C是各向同性的概率。

推论 6.4. 采用第 4 节的记号。设 $F\colon R^n \to G$ 为均匀随机映射。设C 为交替 $n \times n$ 矩阵，并设 h 为其矩阵项的一个最大公约数。假设 C/h 的余核由 g 个元素在 $R/R[h]$上生成。则存在常数 N、K，它们仅依赖于 G，使得只要 $n - g \geq N$，我们就有

$$\left|\mathbb{P}[F \text{ is isotropic for } C] - \frac{|\wedge^2 G[h]|}{|\wedge^2 G|}\right| \leq K \cdot 2^{g-n}$$

证明。设 E'_k表示交替双线性型在 G_k^*上由 $F_k \circ C_k \circ F_k^*$给出的型在 $n-k+1$ 的最后 G_k^*个坐标上消失的事件。设 $E_k = \bigcap_{1\leq \ell \leq k} E'_\ell$ 表示 E'_ℓ 对所有$1 \leq \ell \leq k$均发生的事件。那么， E_n 就是 F 满足命题 4.3 的条件（3）的事件。由注记 4.4 可知，证明以下结论即可得到原结论：将 $\mathbb{P}[F$ 对 $C]$ 是各向同性的 $\mathbb{P}[E_n]$ 替换为该结论。

假设 G 有 k_0 个非平凡直和项，因此对于 $1 \leq k \leq n - k_0$，我们有 d_k 是 R中的一个单位元。在这些情况下， R_k 是平凡的，并且 $\mathbb{P}[E_k] = 1$。因此，我们重点考虑 $k > n - k_0$的情形。

We want to compute $\mathbb{P}[E_k \mid E_{k-1}] = \mathbb{P}[E'_k \mid E_{k-1}]$.

现在 F_{k-1} 是 F_k 在商下的像

$$\mathrm{Hom}_{R_k}(V_k, G_k) \twoheadrightarrow \mathrm{Hom}_{R_k}(V_k, G_k) \otimes_{R_k} R_{k-1} \cong \mathrm{Hom}_{R_{k-1}}(V_{k-1}, G_{k-1}),$$

它也是通过后复合投影 $G_k \twoheadrightarrow G_{k-1}$得到的映射 $\mathrm{Hom}^{R_k}(V_k, G_k) \twoheadrightarrow \mathrm{Hom}^{R_k}(V_k, G_{k-1}) \cong \mathrm{Hom}^{R_{k-1}}(V_{k-1}, G_{k-1})$。给定 F_{k-1} 意味着固定 F_k 模 d_{k-1}的剩余类。给定 F_{k-1} 时， F_k 的条件分布是在具有该剩余类的映射中均匀分布。

令 $\pi_k^{(m)}$ 为从 G_k 到其第 m个坐标的投影 $G_k \twoheadrightarrow \mathbb{Z}/\min\{d_m, d_k\}\mathbb{Z}$。令 $\pi_k^{(\geq m)} = (\pi_k^{(m)}, \pi_k^{(m+1)}, \ldots, \pi_k^{(n)})$为从 G_k 到其最后 $n-m+1$ 个坐标的投影。我们注意到，若 F_k 是均匀随机的，则函数 $\pi_k^{(m)} \circ F_k$ 是相互独立的均匀随机函数 $V_k \to \mathbb{Z}/\min\{d_m, d_k\}\mathbb{Z}$，它们共同确定 F_k。事件 E'_k 表示$(\pi_k^{(\geq k)} \circ F_k) \circ C_k \circ (\pi_k^{(\geq k)} \circ F_k)^*$为零；当 $m < k$时，这与 $\pi_k^{(m)} \circ F_k$ 独立。因此，给定 F_{k-1} 时 $\pi_k^{(\geq k)} \circ F_k$ 的条件分布，与给定$\pi_{k-1}^{(\geq k)} \circ F_{k-1}$时 $\pi_k^{(\geq k)} \circ F_k$ 的条件分布相同。

映射 $\pi_k^{(\geq k)} \circ F_k$ 是一个均匀随机映射 $R_k^n \to R_k^{n-k+1}$，而 $\pi_{k-1}^{(\geq k)} \circ F_{k-1}\colon R_{k-1}^n \to R_{k-1}^{n-k+1}$ 是其模约化 d_{k-1}。

设 $R'_k = R_k/R_k[h]$。将型 $F_k \circ C_k \circ F_k^*$限制在 G_k^* 的最后 $n-k+1$ 个坐标上，等价于在 $(R'_k)^{n-k+1}$ 上的一个型，而 E'_k 是该型消失的事件。

的无条件概率 E'_k 由命题 6.1给出，将其应用于 C/h在 R'_k上：

$$\left|\mathbb{P}[E'_k] - |R'_k|^{-\binom{n-k+1}{2}}\right| \leq 2^{g-k+2} < 2^{g+k_0+2-n}$$

类似地，设 $E''_k \supseteq E'_k$ 是事件，即 $(\pi_{k-1}^{(\geq k)} \circ F_{k-1}) \circ C_{k-1} \circ (\pi_{k-1}^{(\geq k)} \circ F_{k-1})^* = 0$。我们有

$$\left|\mathbb{P}[E''_k] - |R'_{k-1}|^{-\binom{n-k+1}{2}}\right| < 2^{g+k_0+2-n}$$

此外，

$$\mathbb{P}[E'_k \mid E''_k] = \mathbb{P}[E'_k \mid E_{k-1}]$$

因为随机变量 $\mathbb{P}[E'_k \mid \pi_{k-1}^{(\geq k)} \circ F_{k-1}]$ 和 $\mathbb{P}[E'_k \mid F_{k-1}]$ 具有相同的分布。因此

$$\left|\mathbb{P}[E'_k \mid E_{k-1}] - \left(\frac{|R'_{k-1}|}{|R'_k|}\right)^{\binom{n-k+1}{2}}\right| = \left|\frac{\mathbb{P}[E'_k]}{\mathbb{P}[E''_k]} - \left(\frac{|R'_{k-1}|}{|R'_k|}\right)^{\binom{n-k+1}{2}}\right|$$

为了界定这个误差，我们使用以下简单结果。证明很直接，但也可见于例如 [Gor24，引理 4。12]。

引理 6.5。 设 x_1、. . . 、 x_m 为实数，使得 $\sum_{i=1}^m |x_i| \leq \log 2$。则

$$\left|\prod_{i=1}^m (1+x_i) - 1\right| \leq 2\sum_{i=1}^m |x_i|$$

应用引理 6.5，取 $x_1 = \mathbb{P}[E'_k]|R'_k|^{\binom{n-k+1}{2}} - 1$ 和 $x_2 = \mathbb{P}[E''_k]^{-1}|R'_{k-1}|^{-\binom{n-k+1}{2}} - 1$。我们有

$$|x_1| < |R'_k|^{\binom{n-k+1}{2}} \cdot 2^{g+k_0+2-n} \leq |R'_k|^{\binom{k_0}{2}} \cdot 2^{g+k_0+2-n}$$

and

$$|x_2| < \mathbb{P}[E''_k]^{-1} \cdot 2^{g+k_0+2-n}.$$

我们有

$$\mathbb{P}[E''_k] \geq |R'_{k-1}|^{-\binom{n-k+1}{2}} - 2^{g+k_0+2-n} \geq |R'_{k-1}|^{-\binom{k_0}{2}} - 2^{g+k_0+2-n}.$$

设 N满足：当 $n-g \geq N$时，我们有 $|R'_{k-1}|^{-\binom{k_0}{2}} - 2^{g+k_0+2-n} \geq \frac{1}{2}|R'_{k-1}|^{-\binom{k_0}{2}}$，因此

$$|x_2| < |R'_{k-1}|^{\binom{k_0}{2}} \cdot 2^{g+k_0+3-n}$$

现在我们可以适当增大 N，使得当 $n-g \geq N$ 时，有 $|x_1| + |x_2| \leq \log 2$。于是得到

$$\left|\mathbb{P}[E'_k|E_{k-1}]\left(\frac{|R'_k|}{|R'_{k-1}|}\right)^{\binom{n-k+1}{2}} - 1\right| < 2\left(|R'_{k-1}|^{\binom{k_0}{2}} \cdot^{g+k_0+3-n} + |R'_k|^{\binom{k_0}{2}} \cdot 2^{g+k_0+2-n}\right)$$
$$\leq 3d_k^{\binom{k_0}{2}} 2^{g+k_0+3-n}$$

现在我们再次应用引理 6.5，取 $x_k = \mathbb{P}[E'_k|E_{k-1}]\left(\frac{|R'_k|}{|R'_{k-1}|}\right)^{\binom{n-k+1}{2}} - 1$。我们有

$$\sum_{k=n-k_0+1}^{n} 3d_k^{\binom{k_0}{2}} 2^{g+k_0+3-n} \leq 3k_0 d_n^{\binom{k_0}{2}} 2^{g+k_0+3-n}$$

并且我们还可以进一步增大 N，使得右侧不超过 $\log 2$。于是当$n-g \geq N$时，引理 6.5 表明

$$\left|\prod_{k=n-k_0+1}^{n} \mathbb{P}[E'_k|E_{k-1}]\left(\frac{|R'_k|}{|R'_{k-1}|}\right)^{\binom{n-k+1}{2}} - 1\right| \leq 3k_0 d_n^{\binom{k_0}{2}} 2^{g+k_0+3-n}$$

现在我们有

$$\prod_{k=n-k_0+1}^{n} \mathbb{P}[E'_k|E_{k-1}] = \prod_{k=n-k_0+1}^{n} \mathbb{P}[E_k|E_{k-1}] = \mathbb{P}[E_n]$$

and

$$\prod_{k=n-k_0+1}^{n}\left(\frac{|R'_k|}{|R'_{k-1}|}\right)^{\binom{n-k+1}{2}}=\prod_{k=1}^{n}\left(\frac{d_k\gcd(d_{k-1},h)}{d_{k-1}\gcd(d_k,h)}\right)^{\binom{n-k+1}{2}}=\frac{\prod_{k=1}^{n}d_k^{n-k}}{\prod_{k=1}^{n}\gcd(d_k,h)^{n-k}}=\frac{|\wedge^2 G|}{|\wedge^2 G[h]|}$$

从而

$$\left|\mathbb{P}[E_n]-\frac{|\wedge^2 G[h]|}{|\wedge^2 G|}\right|\leq 3k_0d_n^{\binom{k_0}{2}}\frac{|\wedge^2 G[h]|}{|\wedge^2 G|}2^{g+k_0+3-n}.$$

□

结合推论 6.4和引理 4.2 可得:

定理 6.6。 设 $a\in\mathbb{Z}_{>0}$ 为指数整除 a的有限阿贝尔群。设 $\varepsilon>0$。则存在 K、$c>0$，使得以下结论成立:

设 C 为关于 $\mathbb{Z}/a\mathbb{Z}$ 的交替 $n\times n$ 矩阵，令 h 为其矩阵项的最大公约数。假设 C/h 的余核由关于 $\mathbb{Z}/\gcd(a、h)\mathbb{Z}$的 g 个元素生成。令 X 为随机的 ε-平衡 C-对称矩阵。则有

$$\left|\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X),G)]-|\wedge^2 G[h]|\right|\leq K(e^{-cn}+2^{g-n})$$

最后，结合定理 3.1 和引理 3.3，在 $h=1$ 的特殊情形下，我们得到:

推论 6.7。 设 $\varepsilon>0$。对于每个 n，令 C_n 为一个确定性的 $n\times n$ 交替矩阵，其矩阵项属于 $R=\mathbb{Z}_p$（分别属于 $R=\mathbb{Z}$ 或 $R=\mathbb{Z}$），且 C_n 的余核由 g_n个元素生成。令 X_n 为一个随机的 ε-平衡 C_n-对称矩阵，其矩阵项属于 R。假设

$$\lim_{n\to\infty}n-g_n=\infty$$

那么，余核(X_n) 的分布弱收敛于 $\Gamma_{CL}^{(p,0)}$ *(*分别为， $\Gamma_{CL}^{(0)}$*)*，其含义见备注 *3.2*。

7. Examples

其 C-对称条件本身相当严格。不过，我们强调，定理 6.6 的优势之一在于，它对 C 具体形式的依赖很弱。这一普适性结果使我们能够通过对 C进行随机化，确定其他各种随机矩阵系综的余核分布，以下三个例子将对此加以说明。

例 7.1（矩阵模 f 对称时的普适性）。 这一结果早已为专家所知，但据我们所知，尚未有人将其明确写下。

设 $R=\mathbb{Z}/a\mathbb{Z}$。设 $\varepsilon>0$ 和 $h\mid a$。对于每个 n，令 X_n 为一个 R 上的随机矩阵:先取一个随机的 ε-平衡对称矩阵，再对每个 $i<j$，将一个随机变量 hy_{ij} 加到第 ij 个元素上，其中 y_{ij} 相互独立，且为 ε-平衡的 R 值随机变量。所得矩阵可称为“模 h 对称的 ε-平衡矩阵”。

由定理 6.6 及一些进一步的工作可知，对于任意有限阿贝尔群 G 其指数整除 a 我们有

$$\lim_{n\to\infty}\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n),G)]=|\wedge^2 G[h]|.$$

我们简要说明如何验证这一点。

我们可以将 X_n 描述为一个 ε-平衡 C_n-对称矩阵，其中 C_n 是一个随机交错矩阵，其对于 $i<j$ 的第 ij 个元素为 hy_{ij}。假设 C_n/h 的余核由 g_n 个元素生成。对于有限阿贝尔群 G，我们有

$$\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n),G)]=\left(\frac{a}{h}\right)^{-\binom{n}{2}}\sum_{\substack{C\text{ alternating}\\ h|C}}\mathbb{E}\left[\#\operatorname{Sur}(\operatorname{coker}(X_n),G)\mid C_n=C\right]$$

Nguyen 和 Wood [NW25] 研究了随机交错整数矩阵的余核分布。特别是，他们证明了随机 ε-平衡交错矩阵在$R/R[h]\cong h\mathbb{Z}/a\mathbb{Z}$ 上的余核具有极限分布，该分布取决于矩阵尺寸的奇偶性。特别是，在极限情形下，$\operatorname{coker}(C_n/h)$ 的挠部分几乎总是有限的，且 C_n/h的秩几乎总是至少为 $n-1$ [NW25，定理 1。13]因此，存在一个常数 r 使得 $\lim_{n\to\infty}\mathbb{P}[g_n>r]=0$。

于是我们有

$$\begin{aligned}\left|\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n),G)]-|\wedge^2 G[h]|\right|&\le\left(\frac{a}{h}\right)^{-\binom{n}{2}}\sum_{\substack{C\text{ alternating}\\ h|C}}\left|\mathbb{E}\left[\#\operatorname{Sur}(\operatorname{coker}(X_n),G)\mid C_n=C\right]-|\wedge^2 G[h]|\right|\\&\le\left(\frac{a}{h}\right)^{-\binom{n}{2}}\sum_{\substack{C\text{ alternating}\\ h|C\\ g_n(C/h)\le r}}\left|\mathbb{E}\left[\#\operatorname{Sur}(\operatorname{coker}(X_n),G)\mid C_n=C\right]-|\wedge^2 G[h]|\right|\\&\quad+\left(\frac{a}{h}\right)^{-\binom{n}{2}}\sum_{\substack{C\text{ alternating}\\ h|C\\ g_n(C/h)>r}}\left|\mathbb{E}\left[\#\operatorname{Sur}(\operatorname{coker}(X_n),G)\mid C_n=C\right]-|\wedge^2 G[h]|\right|\end{aligned}$$

其中，我们用 $g_n(C/h)$ 表示 $\operatorname{coker}(C/h)$ 的极小生成集的大小。

为了处理右侧求和的第二部分，我们注意到，若 Y_n 是任意一个由 ε-平衡 C_n-对称矩阵构成的序列，则有 $\operatorname{limsup}_{n\to\infty}\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(Y_n)\ G)]\le|\wedge^2 G|$ 根据引理4.1。于是

$$\begin{aligned}\limsup_{n\to\infty}\left(\frac{a}{h}\right)^{-\binom{n}{2}}\sum_{\substack{C\text{ alternating}\\ h|C\\ g_n(C/h)>r}}\left|\mathbb{E}\left[\#\operatorname{Sur}(\operatorname{coker}(X_n),G)\mid C_n=C\right]-|\wedge^2 G[h]|\right|&\\\le\lim_{n\to\infty}\mathbb{P}[g_n^0>r](|\wedge^2 G|-|\wedge^2 G[h]|)=0.&\end{aligned}$$

在第一个求和中，我们只考虑矩阵 C，使得 C/h 的余核至多由 $n+r-1$ 个元素生成。对于这些矩阵，定理 6.6 给出的各项上界仅取决于 a、G、ε、r。因此，第一个求和也收敛于 0，于是得到

$$\lim_{n\to\infty}\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n),G)]=1$$

正如我们所希望的
那样。

例 7.2（在一组“普遍”的小型矩阵项集合上进行扰动）。设 $R=\mathbb{Z}_p$、$R=\mathbb{Z}$ 或 $R=\mathbb{Z}/a\mathbb{Z}$。设 $\varepsilon>0$。对于每个 n，令 Y_n 为一个随机 ε-平衡对称矩阵。

设 k_n 满足 $\lim_{n\to\infty} k_n = \infty$。对于每个 n，固定 Y_n 中 k_n 个彼此不同行、不同列的矩阵项，并令 X_n 为从 Y_n 得到的随机矩阵，即在这些 k_n 个矩阵项上分别加上若干固定单位元。

设 $C_n = X_n - X_n^{\intercal}$。这是一个确定性交错矩阵，其 $2k_n$ 矩阵项为单位元，其余位置为零，并且 X_n 是 C_n-对称的。C_n 的余核由 $g_n = n - 2k_n$ 个元素生成，且 $n - g_n = 2k_n \to \infty$。因此，$\operatorname{coker}(X_n)$ 的矩在极限下与定义在 R 上的 ε-平衡 $n \times n$ 矩阵的余核的矩一致。

例 7.3（具有非对称角块的对称矩阵）。设 $R = \mathbb{Z}/a\mathbb{Z}$。令 C_n 从定义在 R 上的严格上三角 $n \times n$ 矩阵群的均匀分布中抽取，其中左上角 $k_n \times k_n$ 区块以外的矩阵项均为零。令 $C_n = C_n + C_n^{\intercal}$。

设 X_n 取自 R 上对称 $n \times n$ 矩阵的均匀分布，并令 $X_n = X_n + C_n$。

则 X_n 是在“左上 $k_n \times k_n$ 角之外”对称的那些矩阵中均匀随机的一个矩阵，即仅对这一角之外的矩阵项施加对称条件的矩阵中的均匀随机矩阵。此外，X_n 是 C_n-对称的。我们将证明，只要

$$\lim_{n\to\infty} k_n = \infty,$$

我们有

$$\lim_{n\to\infty} \mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n), G)] = 1$$

对所有指数整除 a 的有限阿贝尔群 G。

作为推论，若改为从 $\mathbb{Z}_p$ 上在左上 $k_n \times k_n$ 角之外对称的矩阵的加法 Haar 测度中抽取 X_n，则这一计算将表明：只要 k_n 增长得足够快，余核(X_n) 便弱收敛于 $\Gamma_{CL}^{(p,0)}$。

对指数整除 a 的有限阿贝尔群 G，我们有

$$\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n), G)] = a^{-\binom{n}{2}} \sum_{\widetilde{C} \text{ strictly upper triangular}} \mathbb{E}\left[\#\operatorname{Sur}(\operatorname{coker}(X_n), G) \;\middle|\; \widetilde{C}_n = \widetilde{C}\right]$$

矩阵 C_n 大部分由零组成，其左上角的 $k_n \times k_n$ 子矩阵是取自 R 上的均匀随机交错 $k_n \times k_n$ 矩阵 C_n^0。那么，如果 C_n^0 的余核作为 R 上的模由 g_n^0 个元素生成，则 C_n 的余核由 $g_n = n - k_n + g_n^0$ 个元素生成，并且

$$n - g_n = k_n - g_n^0$$

与例子 7.1 中的论证几乎完全相同的论证表明，由于随机交错矩阵的余核以极高概率具有较小的秩，因此 $\mathbb{E}[\#\operatorname{Sur}(\operatorname{coker}(X_n)\ G)]$ 的主要贡献来自以下情形：$\mathbb{E}\left[\#\operatorname{Sur}(\operatorname{coker}(X_n)\ G) \;\middle|\; \widetilde{C}_n = \widetilde{C}\right]$ 由定理 6.6控制。

类似的方法可用于确定 C-对称矩阵余核的极限分布，其中 C 可以来自更一般得多的随机交错矩阵模型。

致谢。作者获得美国国家科学基金会研究生研究奖学金的资助。作者感谢Mengzhen (August) Liu、Carlo Pagano和Melanie Matchett Wood的宝贵讨论。作者还感谢Yifeng Huang和Roger van Peski对本文早期版本提出的有益意见。

References

[CK24] Gilyoung Cheong和Nathan Kaplan. “Friedman和Washington关于随机p进矩阵余核之结果的推广”. 载于：代数杂志 604.C (2024). DOI: 10.1016/j.jalgebra.2022.03.035.[CL84] H. Cohen和H. W. Lenstra, Jr. “数域类群的启发式”. 载于：数论. 第1068卷. 数学讲义. 诺德韦克豪特, 1984, 第 33–62 页 .[Cla+15] Julien Clancy 等 . “ 关于随机图雅可比簇的科恩 – 伦斯特拉启发式 ”. 载于：代数组合学杂志 42.3 (2015年11月), 第701–723页. ISSN: 1572-9192.DOI: 10.1007/s10801-015-0598-x.[FW89] Eduardo Friedman和Lawrence C. Washington. “有限域上曲线除子类群的分布”. 载于：1987年7月5–18日在Universit ´e Laval举行的国际数论会议论文集. Jean M. de Koninck和Claude Levesque编. 柏林, 纽约: 德古意特, 1989, 第227–239页. ISBN: 9783110852790. DOI: 10.1515/9783110852790.227.[Ger84] Frank Gerth. “二次域的4-类秩”. 载于：数学发明 77.3 (1984年10月), 第489–515页. ISSN: 1432-1297. DOI: 10.1007/BF01388835.[GL26] Elia Gorokhovsky和Mengzhen Liu. 经由C-对称矩阵的超椭圆曲线皮卡群的4-秩分布. 2026年2月. arXiv: 2602.23707 [math].[Gor24] Elia Gorokhovsky. 有限群上的时间非齐次随机游走与随机整数分块矩阵的余核. 2024. arXiv: 2405.11435 [math.PR].[Hod24] Eliot Hodges. “随机图沙堆群及其配对的分布”. 载于：美国数学会汇刊 377.12 (2024年12月), 第8769–8815页. ISSN: 0002-9947, 1088-6850. DOI: 10.1090/tran/9244.[KLY24] Dong Yeap Kang、Jungin Lee和Myungjun Yu. 具有固定零矩阵项的随机 p进矩阵与科恩–伦斯特拉分布. 2024. arXiv: 2409.01226 [math.NT].[KP20] Peter Koymans和Carlo Pagano. “随机R´edei矩阵余秩的有效收敛”. 载于：算术学报 (2020).[LW20] Yuan Liu和Melanie Matchett Wood. “当n趋于无穷时，n个生成元上的自由群模n + u个随机关系”. 载于：纯粹与应用数学杂志f ¨（克雷尔杂志）2020.762 (2020), 第123–166页. DOI: doi:10.1515/crelle-2018-0025.[M´es20] Andr´as M´esz´aros. “随机正则图沙堆群的分布”. 载于：美国数学会汇刊 373.9 (2020年9月), 第6529–6594页.ISSN: 0002-9947, 1088-6850. DOI: 10.1090/tran/8127.[M´es24] Andr´as M´esz´aros. p 进整数上随机带状矩阵余核的相变. 2024. arXiv: 2408.13037 [math.PR].[M´es25] Andr´as M´esz´aros. “具有行列式偏置的稀疏矩阵的科恩–伦斯特拉分布”. 载于：国际数学研究通告 2025.3 (2025年2月), rnae292.ISSN: 1073-7928. DOI: 10.1093/imrn/rnae292.[NV24] Hoi H. Nguyen和Roger Van Peski. “随机矩阵乘积余核的普适性”. 载于：数学进展 438 (2024), 第109451页. ISSN: 0001-8708. DOI:10.1016/j.aim.2023.109451.[NW22] Hoi H. Nguyen和Melanie Matchett Wood. “随机整数矩阵：满射性与余核的普适性”. 载于：数学发明 228.1 (2022年4月), 第1–76页. ISSN: 1432-1297. DOI: 10.1007/s00222-021-01082-w.[NW25] Hoi H. Nguyen和Melanie Matchett Wood. “随机矩阵余核的局部与整体普适性”. 载于：数学年刊 391.4 (2025年4月), 第5117–5210页. ISSN: 1432-1807. DOI: 10.1007/s00208-024-03050-0.

[R´ed34] L. R´edei.《关于二次数域中绝对类群可被四整除的不变量个数定理的算术证明》。载于：Journal für die reine und angewandte Mathematik 171（1934），第 55–60 页。URL: http://eudml.org/doc/149883.[SW24a] Will Sawin 和 Melanie Matchett Wood。《包含单位根的数域扩张的类群分布猜想》。2024 年 2 月。arXiv：2301.00791[math].[SW24b] Will Sawin 和 Melanie Matchett Wood。《范畴中随机对象的矩问题》。2024 年。arXiv: 2210.06279 [math.PR].[Woo17] Melanie Matchett Wood。《随机图沙堆群的分布》。载于：美国数学会杂志 30.4（2017），第 915–958 页。[Woo19] Melanie Matchett Wood。《随机整矩阵与 Cohen-Lenstra 启发式》。载于：美国数学杂志 141.2（2019），第 383–398 页。

Harvard University, Cambridge, USA