arXiv:2603.15856v1 [math.CO] 16 Mar 2026

有限域上随机矩阵的积和

Zach Hunter、Matthew Kwan 和 Lisa Sauermann

摘要。固定一个有限域 $\mathbb{F}_q$，并令 $A \in \mathbb{F}_q^{n\times n}$ 为在 $\mathbb{F}_q$ 上均匀随机选取的 $n \times n$ 矩阵。行列式 $\det(A)$ 的渐近分布已为人熟知，但积和式 $\operatorname{per}(A)$ 的渐近分布仍然是个谜。本文在这一方向上迈出了第一步，证明 $\operatorname{per}(A)$ 比 $\det(A)$ 均匀得多。

1. 引言

两个重要的矩阵参数是行列式 和积和式：对于一个 $n \times n$ 矩阵 $A = (a_{i,\ j})$，它们定义为

$$\det(A) = \sum_{\pi\in S_n} \operatorname{sign}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)} \qquad \text{and} \qquad \operatorname{per}(A) = \sum_{\pi\in S_n} \prod_{i=1}^{n} a_{i,\pi(i)}. \tag{1.1}$$

如果我们固定一个有限域 $\mathbb{F}_q$并令 $A \in \mathbb{F}_q^{n\times n}$为均匀随机选取的 $n\times n$矩阵，其元素取自 $\mathbb{F}_q$，那么很容易计算 $\det(A)$ 的极限分布（这基本等价于计算 $\mathbb{F}_q$上的可逆矩阵数量，这个问题可追溯至伽罗瓦 [30, 第 p 页 280]）。

事实 1.1. 对于素数幂 q，令

$$\alpha_q = 1 - \prod_{i=1}^{\infty}(1 - q^{-i}).$$

那么，对于均匀随机的 $n \times n$ 矩阵 $A \in \mathbb{F}_q^{n\times n}$ 和任意 $x \in \mathbb{F}_q$，我们有

$$\lim_{n\to\infty} \Pr[\det(A) = x] = \begin{cases} \alpha_q & \text{if } x = 0 \\ (1-\alpha_q)/(q-1) & \text{otherwise.} \end{cases}$$

值得注意的是，这个极限分布在 $\mathbb{F}_q$ 上并非均匀分布：行列式取零值的概率显著高于取任何其他值的概率。例如，当 $q = 3$ 时，我们有 $\alpha_q \approx 0.44$，这显著大于 $1/q = 1/3$。粗略地说，这是因为事件 $\{\det(A) = 0\}$ 描述了 A 的各行线性相关：如果我们逐行揭示矩阵，并在某一步发现某一行落在前面各行的张成空间中，这就意味着无论后续各行如何，$\det(A) = 0$。另一方面，如果揭示倒数第二行后，我们仍未发现各行之间存在线性依赖关系，那么很容易看出，$\det(A)$ 的条件分布在 $\mathbb{F}_q$ 上是均匀分布的。

与行列式不同，积和式似乎没有任何线性代数意义（除非我们的域的特征为 2，此时行列式与积和式相等）。一个自然的猜想是，如果 $\mathbb{F}_q$ 的特征不为 2，那么$\mathbb{F}_q$ 上的均匀随机矩阵的积和式渐近服从均匀分布，具体如下。

猜想 1.2。设 $\mathbb{F}_q$ 是一个奇特征有限域。那么，对于均匀随机的 $n \times n$ 矩阵$A \in \mathbb{F}_q^{n\times n}$，以及任意 $x \in \mathbb{F}_q$，我们有

$$\lim_{n\to\infty} \Pr[\operatorname{per}(A) = x] = \frac{1}{q}.$$

Zach Hunter 获得了瑞士国家科学基金会（SNSF）项目 200021-228014 的资助。Matthew Kwan 获得了欧洲研究委员会启动基金“RAND-STRUCT”（编号 101076777）的资助。Lisa Sauermann 获得了德国研究联合会（DFG）——协同研究中心 1720（编号 539309657）的资助。

这个猜想似乎已在学界流传了一段时间，但我们不太确定它最初源自何处。计算机科学界对有限域上随机矩阵的积和式颇感兴趣（例如参见 [3,8–10,20]），这得益于一种称为 随机自归约性 的现象。但令人意外的是，我们未能在相关文献中找到关于 $\mathrm{per}(A)$ 渐近分布的任何研究。我们能找到的最早出处，是在 2017 年 Mathematisches Forschungsinstitut Oberwolfach 举办的组合数学研讨会上的公开问题环节 [16], ，Swastik Kopparty 在会上询问积和式在 $\mathbb{F}_3$ 上的极限分布。 $\mathbb{F}_3$ 猜想 1.2 的情形 也明确出现在 Scheinerman 最近的一篇论文中 [29] （并有相当有说服力的计算证据支持），而猜想 1.2的一般情形则出现在 Ghasemi、Gross 和 Kopparty 最近发表的一篇论文中 [11]。另请参阅 Esperet 提出的一个相关猜想 [7]（该猜想源于图论中的一些问题）。

注意，由对称性（通过对任意一行进行缩放），$\mathrm{per}(A)$ 取任意非零值的可能性都相同。因此，要了解$\mathrm{per}(A)$ 的分布，只需了解概率 $[\mathrm{per}(A) = 0]$。更具体地说，猜想 1.2 的断言等价于 $\lim_{n\to\infty}$ 概率 $[\mathrm{per}(A) = 0] = 1/q$。

尽管我们无法证明猜想 1.2，但至少能够证明积和式（渐近地）比行列式更加均匀分布，具体如下（回忆$\lim_{n\to\infty}$概率$[\det(A) = 0] = \alpha_q > 1/q$，并注意到 $\alpha_q - 1/q$ 的数量级为 $1/q^2$）。

定理 1.3。 固定一个特征为奇数的有限域 $\mathbb{F}_q$。对于均匀随机的 $n \times n$ 矩阵 $A \in \mathbb{F}_q^{n\times n}$，有

$$\Pr[\mathrm{per}(A) = 0] \geq \frac{1}{q} \tag{1.2}$$

对所有 n，并且我们有 严格的 不等式

$$\limsup_{n\to\infty} \Pr[\mathrm{per}(A) = 0] < \alpha_q. \tag{1.3}$$

此外，对所有 $n \geq 3$，我们有

$$\Pr[\mathrm{per}(A) = 0] \leq \frac{1}{q} + \frac{C}{q^3} \tag{1.4}$$

对于某个绝对常数 C。

对于 $n = 2$，有 概率$[\mathrm{per}(A) = 0] = 1/q + \Theta(1/q^2)$，因此假设 $n \geq 3$ 在 (1.4) 不可省略 .

我们指出，Budrevich 和 Guterman 此前证明了一个精神相近的定理 [2] （另见 [1], 中更简单的证明以及更早的工作 [5]）：用概率语言重述，他们的主要结果是，对于任意奇特征有限域 $\mathbb{F}_q$ 以及任意 $n \geq 3$，积和式为零的概率严格小于行列式为零的概率。然而，他们所证明的这两个概率之间的差距会随着 $n \to \infty$ 趋近而极快地趋于零。Budrevich 和 Guterman 受到 Pólya永久式问题（例如参见 [25,27,33]）的启发；该问题探讨能在多大程度上将矩阵的积和式改写为行列式。 [2] 中所证明的差距表明，不存在双射“转换器”f： $\mathbb{F}_q^{n\times n} \to \mathbb{F}_q^{n\times n}$，使得对所有 $A \in \mathbb{F}_q^{n\times n}$，$\mathrm{per}(A) = \det(f(A))$。注意，定理 1.3 推出了更强的结果：不存在对几乎所有 $A \in \mathbb{F}_q^{n\times n}$ 都适用的此类转换器。

1.1. **一般分布**。 事实证明， 事实 1.1 具有 普适性，即随机矩阵 $A \in \mathbb{F}_q^{n\times n}$的行列式分布并不强烈依赖于 A 的元素分布。例如，已知对于 任意 非常数分布 μ 在素数阶 $\mathbb{F}_p$ 有限域上，如果 $A \in \mathbb{F}_p^{n\times n}$是一个具有相互独立的 μ分布元素的随机矩阵，那么 极限$\lim_{n\to\infty}$概率$[\det(A) = 0] = \alpha_p$。 这似乎最早是由 Charlap、Rees 和 Robbins 于 1990 年证明的， [4], 尽管 Kozlov [18] 以及 Kovalenko 和 Levitskaja 早得多就证明了具有更严格限制条件的类似定理， [17],而关于任意有限域的一个非常一般的定理（其表述必然更具技术性）后来由 Kahn 和 Komlós 证明。 [15]另请参见 [6,21,23,24,26,36,37] 其中关于有限域上随机矩阵各种代数性质普适性的较新研究。

我们可以证明一个定理 沿用 定理 1.3 的思路，针对任意（非恒定）有限素数阶域上的分布如下所示。

定理 1.4。固定一个素数阶有限域 $\mathbb{F}_p$ $p \geq 3$。则存在 $\delta_p > 0$，使得以下结论成立。设 μ 是 $\mathbb{F}_p$ 上一个概率分布，其支撑集包含不止一个值。若 $A \in \mathbb{F}_p^{n\times n}$ 是一个随机

矩阵，其各个条目相互独立且服从 μ 分布，则对每个 $z \in \mathbb{F}_p$ 都有

$$\limsup_{n\to\infty} \Pr[\mathrm{per}(A) = z] \le \alpha_p - \delta_p \tag{1.5}$$

and

$$\frac{1}{p} - \frac{C}{p^3} \le \liminf_{n\to\infty} \Pr[\mathrm{per}(A) = z] \le \limsup_{n\to\infty} \Pr[\mathrm{per}(A) = z] \le \frac{1}{p} + \frac{C}{p^3}. \tag{1.6}$$

对于某个绝对常数 C。

注。 为简便起见，我们将 定理 1.4 仅针对素数域进行陈述，但在对各项分布施加某种非退化假设的条件下，我们的证明方法显然可以推广到任意有限域。不幸的是，我们的证明方法似乎无法适用于文献中最弱的非退化条件。例如，Kahn 和 Komlós [15] 证明，只要 μ 是有限域 $\mathbb{F}_q$ 上的一个分布，且其支撑不包含在 $\mathbb{F}_q$的某个子域的仿射平移中，那么对于一个 A 各项独立且服从 μ分布的随机矩阵，我们有 $\lim_{n\to\infty}$概率$[\det(A) = 0] = \alpha_q$。 在这种非常一般的情形下，我们甚至不知道如何证明不等式 $\limsup_{n\to\infty}$ 概率$[\mathrm{per}(A) = x] \le \alpha_q$。

注。在组合随机矩阵理论中，或许研究得最深入的一类随机矩阵就是随机符号矩阵。令 $A \in \{-1,1\}^{n\times n}$ 为一个均匀随机的、元素取值为 ± 1 的 $n \times n$ 矩阵；在近期一项卓越的工作中，Tikhomirov [32] 证明了，概率 $\Pr[\det(A) = 0] = (1/2 + o(1))^n$（另见综述 [12, 28, 34, 35]）。人们对随机符号矩阵的永久式颇感兴趣（例如参见 [13, 19, 22, 31]），但关于永久式的已知结果仍远少于行列式。$\mathrm{per}(A)$ 和 $\det(A)$ 的行为非常相似，这似乎颇为合理；但值得注意的是，(1.6) 给出了两者分布出现差异的首批例子之一：对于所有素数 $p \ge 3$，它们模 p 的统计性质截然不同。

1.2. **论文与证明概述**。 我们本可以给出一个统一的证明来证明 定理 1.3和 1.4，但我们发现将证明分别呈现会更加清晰。

在 第 2 节 中，我们给出 定理 1.3的简短证明。我们逐行揭示随机矩阵，并在此过程中研究子矩阵的积和式，通过归纳法证明“非零积和式出现的概率至少与非零行列式一样大”。接着，在最后几行中，我们采用稍有不同的方法，利用积和式的某种对称性。

在 第 3 节中，我们证明 定理 1.4。总体策略相同，但我们还需要利用这样一个事实：将大量相互独立的 μ-分布随机变量相加，所得结果近似服从均匀分布。因此，如果我们能够同时跟踪许多子矩阵的积和式，就可以在 μ-分布的情形下“模拟”均匀分布情形。这需要一些额外的思路。

2. 均匀分布情形的证明

本节我们证明定理 1.3。首先，很容易看出，积和式也满足行列式子式展开公式的类似形式，如下所述。这一事实使我们能够递归地研究积和式。

事实 2.1。对于任意矩阵 $A \in \mathbb{F}_q^{k\times k}$，有

$$\mathrm{per}(A) = \sum_{i=1}^{k} \mathrm{per}(A_i')x_i,$$

其中， A_i' 是从 A 中删除最后一行和第 i列后得到的子矩阵 $\times$ ，而x_i 是 A 中最后一行、第 i列的元素。

接下来，以下引理表明，每当我们揭示一行时，非零永久式子式的“增长速度至少不逊于”非零行列式子式（注意，对于均匀随机矩阵$A \in \mathbb{F}_q^{n\times n}$，在已知前 $n - s$ 行的结果线性无关的条件下，下一行属于它们张成空间的概率恰好是 q^{-s}）。

定义2.2。 在 定理 *1.3*的情形下，对于任意 $0 \le s \le n$，令 $A^{\uparrow s}$ 为 $(n-s)\times n$ 子矩阵，它由 A 删除最后 s 行得到。令 $\mathcal{E}(s)$ 表示这样的事件： $A^{\uparrow s}$ 包含一个 $(n-s)\times(n-s)$ 子矩阵，其积和式非零。

引理 2.3。 对于任意 $s \in \{1, \ldots, n\}$，以及满足 $\mathcal{E}(s)$的 $A^{\uparrow s}$ 的任意一种结果，我们有

$$\Pr[\mathcal{E}(s-1) \mid A^{\uparrow s}] \geq 1 - q^{-s}.$$

证明。 在整个证明过程中，我们隐式地以 $A^{\uparrow s}$ 的结果为条件（即将其视为非随机对象）。也就是说，我们只考虑$A^{\uparrow(s-1)}$的最后一行（即第（$n-s+1$）行）的随机性。将该行的各项记为 x_1、……、 x_n。

不失一般性，我们可以假设 $A^{\uparrow s}$ 中由最后 $n-s$ 列构成的（$n-s$）×（$n-s$）子矩阵的积和式非零。在此假设下，实际上我们只需利用 x_1、……、 x_s的随机性：固定 x_{s+1}、……、 x_n的任意结果，并且在证明的其余部分中也隐式地以这些结果为条件。

对于 $i \in \{1, \ldots, s\}$，记 t_i 为从 $A^{\uparrow(s-1)}$中删除前 s 列（第 i列除外）后得到的（$n-s+1$）×（$n-s+1$）矩阵的积和式。于是（回想一下，我们处于一个条件概率空间中，其中唯一相关的随机性来源是各项 x_1、……、 x_s；再回想事实 2.1），注意到 t_1、……、 t_s 彼此独立，且 t_i 是 x_i的双射仿射线性变换。这意味着t_1、……、 t_s 是相互独立且在 $\mathbb{F}_q$上均匀分布的随机变量。注意到$\mathcal{E}$（$s-1$）仅在 $t_1 = \cdots = t_s = 0$时才可能不成立，所需结论随即得证。□

迭代 引理 2.3 表明，积和式 至少 与行列式一样 服从均匀分布，具体如下。

推论 2.4。对于任意 $s \in \{1, \ldots, n\}$ 我们有

$$\Pr[\mathcal{E}(s-1)] \geq \prod_{i=s}^{n} (1 - q^{-i}),$$

特别地

$$\Pr[\operatorname{per}(A) = 0] = 1 - \Pr[\mathcal{E}(0)] \leq 1 - \prod_{i=1}^{n} (1 - q^{-i}) \leq \alpha_q.$$

证明。我们有

$$\Pr[\mathcal{E}(s-1)] \geq \prod_{i=s}^{n} \Pr[\mathcal{E}(i-1) \mid \mathcal{E}(i)] \geq \prod_{i=s}^{n} (1 - q^{-i}),$$

利用 引理 2.3 以及以下事实： 概率[$\mathcal{E}$（n）] = 1 （空矩阵的积和式为 1）。 □

我们还需要以下关于 3×3 矩阵的初等引理。

引理 2.5. 取一个奇特征有限域 $\mathbb{F}_q$，并设 $B \in \mathbb{F}_q^{3\times 3}$是一个对称 3×3 矩阵，其对角元全为零，非对角元全非零。那么秩$(B) = 3$。

证明. 写作 $B = (b_{i,j})$，并注意到 det(B)= $2b_{1,2}b_{1,3}b_{2,3} \neq 0$。 □

我们需要的最后一个要素是极值图论中的 Mantel 定理（例如，参见 [14, 定理 4.6]）。

定理 2.6. 如果一个有 n 个顶点的图包含超过 $n^2/4$ 条边，那么它就含有一个三角形。

现在我们已准备好证明定理 1.3。

定理 1.3 的证明。首先，(1.2) 中所需的下界几乎显而易见。事实上，根据事实 2.1， A 的积和式是 A 最后一行各元素的线性组合，其中系数是 $A^{\uparrow 1}$ 的 $(n-1) \times (n-1)$ 子矩阵的积和式。给定一个满足 $\mathcal{E}(1)$ 的 $A^{\uparrow 1}$ 取值，至少有一个线性组合的系数非零。 A 最后一行的元素是取值均匀分布于 $\mathbb{F}_q$ 的独立随机变量，因此该线性组合本身在 $\mathbb{F}_q$ 上均匀分布。因此，我们得到（注意，若事件 $\mathcal{E}(1)$ 不成立，则总有 per$(A) = 0$ ）

$$\Pr[\operatorname{per}(A) = 0] = (1/q) \Pr[\mathcal{E}(1)] + \Pr[\mathcal{E}(1)^c] \geq 1/q.$$

在证明的其余部分，我们着重于给 lim sup$_{n\to\infty}$ Pr[per$(A) = 0$] 作上界，以首先证明(1.3)，然后证明(1.4)。为此，我们将使用引理 2.3，但对最后两行稍作不同处理。为此，我们定义一个对称矩阵 $H = (h_{i,j}) \in \mathbb{F}_q^{n\times n}$，用于编码$(n-2) \times (n-2)$ 的积和式

在 $A^{\uparrow 2}$中的子矩阵：对于 $i \neq j$，令$h_{i,j}$ 为从 $A^{\uparrow 2}$ 中删除列 i 和 j后所得子矩阵的积和式；对于每个 i，令 $h_{i,i} = 0$。令 $\vec{x} \in \mathbb{F}_q^n$ 为 $A^{\uparrow 1}$ 的最后一行（即 A的倒数第二行）。那么，根据事实 2.1，不难看出， $H\vec{x}$ 的各项是 $A^{\uparrow 1}$中的$(n-1) \times (n-1)$子矩阵的积和式。因此， $\mathcal{E}(1)$成立当且仅当 $H\vec{x} = \vec{0}$。

若固定 $A^{\uparrow 2}$ 的一个取值，使得秩$(H) \geq 3$，那么在给定 $A^{\uparrow 2}$这一取值的条件下，随机向量 $H\vec{x}$ 在 $\mathbb{F}_q^n$ 的某个线性子空间上均匀分布，该子空间的维数至少为 3。因此，

$$\Pr[\mathcal{E}(1) \mid \operatorname{rank}(H) \geq 3] = \Pr[H\vec{x} = \vec{0} \mid \operatorname{rank}(H) \geq 3] \geq 1 - q^{-3}. \tag{2.1}$$

注意到 (2.1) 给出了比 $s = 2$ 情形下的 引理 2.3更强的界。证明余下部分的思路是证明 秩$(H) \geq 3$ 以非可忽略的概率成立，这样我们就可以利用 (2.1) 改进推论 2.4的证明。

考虑图 G，其顶点集为 $\{1, \ldots, n\}$，其中 ij是边，当且仅当 $h_{i,\ j} \neq 0$。给定一对 ij 不构成 G 中一条边的概率至多为 α_q，由 推论 2.4 可得（应用于一个 $(n-2) \times (n-2)$随机矩阵）。直接计算可得 $\alpha_q < 0.45$ （使用 $q \geq 3$）。因此，由马尔可夫不等式，我们的图 G 至少有 $\binom{n}{2} - n^2/4$ 条非边的概率至多为

$$\frac{\alpha_q \cdot \binom{n}{2}}{\binom{n}{2} - n^2/4} = 2\alpha_q + o(1) \leq 0.9$$

(假设 n 足够大，这样做是可行的）。若此情况不成立，则根据 Mantel 定理（定理 2.6）， G 包含一个三角形。这个三角形对应于 3×3 的一个主子矩阵 H，其对角元全为零，非对角元全非零，因此rank(H) ≥ 3，由引理 2.5可得。总之，令 $\mathcal{F}$ 表示rank$(H) \geq 3$这一事件，我们已经证明

$$\Pr[\mathcal{F}] \geq 1 - 2\alpha_q - o(1) \geq 0.1.$$

现在，我们有

$$\begin{aligned}
\Pr[\mathcal{E}(1)] &\geq \Pr[\mathcal{E}(1) \mid \mathcal{F}] \Pr[\mathcal{F}] + \Pr[\mathcal{E}(1) \mid \mathcal{E}(2) \setminus \mathcal{F}] \Pr[\mathcal{E}(2) \setminus \mathcal{F}] \\
&\geq (1 - q^{-3}) \Pr[\mathcal{F}] + (1 - q^{-2})(\Pr[\mathcal{E}(2)] - \Pr[\mathcal{F}]) \\
&\geq (1 - q^{-2}) \Pr[\mathcal{E}(2)] + \Pr[\mathcal{F}](q^{-2} - q^{-3}) \\
&\geq \prod_{i=2}^{n} (1 - q^{-i}) + \frac{q^{-2}}{20}.
\end{aligned}$$

在第二行中，我们使用(2.1) 对概率$[\mathcal{E}(1) \mid \mathcal{F}]$ 给出了下界，并使用引理 2.3 对概率$[\mathcal{E}(1) \mid \mathcal{E}(2) \setminus \mathcal{F}]$给出了下界。最后一行中，我们使用推论 2.4 对概率$[\mathcal{E}(2)]$给出了下界。

利用引理 2.3，可得

$$\Pr[\operatorname{per}(A) \neq 0] = \Pr[\mathcal{E}(0)] \geq \Pr[\mathcal{E}(0) \mid \mathcal{E}(1)] \Pr[\mathcal{E}(1)] \geq (1 - q^{-1}) \Pr[\mathcal{E}(1)] \geq \prod_{i=1}^{n} (1 - q^{-i}) + \frac{q^{-2}}{50} \geq 1 - \alpha_q + \frac{q^{-2}}{50}$$

因此，$\operatorname{limsup}_{n \to \infty}$ 概率$[\operatorname{per}(A) = 0] \leq \alpha_q - q^{-2}/50 < \alpha_q$，从而证明了(1.3)。

对于(1.4) 我们采用类似的方法。首先，注意到给定的一对 ij 不构成 G 的一条边的概率，也可以通过推论 2.4 由 $1 - \prod_{i=1}^{n-2} (1 - q^{-i}) \leq \sum_{i=1}^{n-2} q^{-i} \leq 2q^{-1}$来界定。因此，再次像之前一样应用马尔可夫不等式， G 至少有 $\binom{n}{2} - n^2/4$ 条非边的概率至多为

$$\frac{2q^{-1} \cdot \binom{n}{2}}{\binom{n}{2} - n^2/4} = 2q^{-1} \cdot \frac{2(n-1)}{n-2} \leq 8q^{-1},$$

回顾假设 $n \geq 3$。因此，我们得到概率$[\mathcal{F}] \geq 1 - 8q^{-1}$。

由推论 2.4 我们还可得概率$[\mathcal{E}(2)] \geq \prod_{i=3}^{n} (1 - q^{-i}) \geq 1 - \sum_{i=3}^{n} q^{-i} \geq 1 - 2q^{-3}$。然后，同上所述的论证表明

概率$[\mathcal{E}(1)] \geq (1 - q^{-2})$ 概率$[\mathcal{E}(2)] +$ 概率$[\mathcal{F}](q^{-2} - q^{-3}) \geq (1 - q^{-2})(1 - 2q^{-3}) + (1 - 8q^{-1})(q^{-2} - q^{-3}) \geq 1 - 11q^{-3}$

因此

$$\Pr[\operatorname{per}(A) \neq 0] \geq (1 - q^{-1}) \Pr[\mathcal{E}(1)] \geq (1 - q^{-1})(1 - 11q^{-3}) \geq 1 - q^{-1} - 11q^{-3}. \qquad \square$$

注。 这里，我们通过以特殊方式处理最后两行，得到了积和式与行列式之间的分离。对于 $s > 2$，以特殊方式处理最后 s 行，可以进一步改进我们的界。特别是，对于给定的 s，只需进行有限的分类讨论，似乎就能将误差项 $O(q^{-3})$ 改进为 $O(q^{-s-1})$。（我们已为 $s = 3$ 推导出详细结果，并打算在今后发表的本文配套短文中加以介绍；但随着 s 不断增大，分类讨论似乎会变得愈发复杂，复杂度呈指数增长。）

3. 一般分布的证明

现在，我们转而证明 定理 1.4。在本节中，我们固定一个素数 $p \geq 3$ 和一个概率分布 μ，它定义在 $\mathbb{F}_p$ 上且其支撑集包含多个值，并令 $A \in \mathbb{F}_p^{n\times n}$为一个随机矩阵，其各项相互独立且服从 μ分布。

为了证明 定理 1.4，我们需要调整 定理 1.3 的证明，以便同时考察多个具有非零积和式的子矩阵。我们将考察满足某种“补集不相交”性质的子矩阵，具体如下。

定义 3.1. 对于任意 $0 \leq s \leq n$，令 $A^{\uparrow s}$ 为从 A 中删除最后 s 行后得到的子矩阵。对于大小为 s的集合 $I \subseteq \{1, \ldots, n\}$，令 $\mathrm{per}(A;\ I)$ 表示从 $A^{\uparrow s}$中删除由 I索引的列后得到的$(n-s)\times(n-s)$ 子矩阵的积和式。对于正整数 ℓ，令 $\mathcal{E}(s,\ell)$ 表示存在ℓ 个两两不相交的集合 I_1、……、I_ℓ，且每个集合大小均为 s，使得对于每个 $i = 1$、……、ℓ，都有 $\mathrm{per}(A;\ I_i) \neq 0$ 的事件。

在定理 1.3 的证明中（具体来说，在引理 2.3中），我们以 $A^{\uparrow s}$ 的一个结果为条件，该结果含有一个矩阵永久式非零的子矩阵，并研究 $A^{\uparrow(s-1)}$ 含有一个更大的矩阵永久式非零子矩阵的概率。引理 2.3 仅针对元素均匀分布的随机矩阵给出；虽然也可以考虑一般的元素分布，但这会改变概率界。下面的引理考虑了类似的情形：我们以 $A^{\uparrow s}$ 含有许多矩阵永久式非零的子矩阵为条件，并希望 $A^{\uparrow(s-1)}$ 含有许多更大的矩阵永久式非零子矩阵。遗憾的是，这里的“许多”有两种截然不同的含义，但在这个更“稳健”的情形下，我们能够得到基本上独立于元素分布的概率界（也就是说，无论元素分布如何，我们得到的 $1-p^{-s}$ 界都与引理 2.3 中的大致相同）。

引理 3.2。 对于任意 $s, \ell \in \mathbb{N}$和 $\varepsilon > 0$，存在 $L = L_\mu(s,\ell,\varepsilon) \in \mathbb{N}$，使得当 n 足够大时，以下结论成立。对于满足 $\mathcal{E}(s, L)$ 的 $A^{\uparrow s}$ 的任意取值，我们有

$$\Pr[\mathcal{E}(s-1,\ell)\,|\,A^{\uparrow s}] \geq 1 - p^{-s} - \varepsilon.$$

我们将 引理 3.2 的证明推迟到第 3.2 节。该引理的证明使用了针对“稳健高秩”线性映射的反集中不等式（该不等式将在本节后文作为引理 3.6 陈述，且可能具有更广泛的意义）。

我们希望递归地使用引理 3.2，从而推导出适用于一般分布的推论 2.4 的一个版本。遗憾的是，我们只能迭代引理 3.2 很少几次，因为每次迭代都需要越来越多具有非零矩阵永久式的子矩阵[1]。因此，我们还需要以下引理，作为应用引理 3.2的起点。

引理 3.3。 对于任意 $\varepsilon > 0$，存在 $S = S_\mu(\varepsilon) \in \mathbb{N}$ 使得

$$\Pr[\mathcal{E}(S, \lceil n^{0.99}\rceil)] \geq 1 - \varepsilon$$

当 n 足够大时（相对于 ε 和 μ）。

我们将引理 3.3 的证明推迟到第 3.1 节。证明是对陶哲轩和 Vu 的思路所作的直接改编 [31]。

现在我们可以证明 推论 2.4 的一个适用于一般分布的版本。

[1]我们对 引理 3.2 的表述没有给出定量界，因此按当前写法，它只能应用 $O(1)$ 次。更仔细一些，或许可以应用大约 $\log n$ 次，但肯定还需要其他想法。

推论 **3.4.** 对于任意 s、$\ell \in \mathbb{N}$ 和 $\varepsilon > 0$，如果 n 相对于 s、ℓ 和 ε 足够大，则 n

$$\Pr[\mathcal{E}(s-1,\ell)] \geq \prod_{i=s}^{\infty}(1-p^{-i}) - \varepsilon,$$

尤其是

$$\Pr[\mathrm{per}(A)=0] = 1 - \Pr[\mathcal{E}(0,1)] \leq \alpha_p + \varepsilon.$$

证明。我们在 $S_\mu(\cdot)$ 和 $L_\mu(\cdot,\cdot,\cdot)$ 的陈述中使用了这些量：引理 3.2 和 3.3。

设 $S = S_\mu(\varepsilon/2)$。设 $\ell_{s-1} = \ell$，对于 $i \in \{s,\dots,S\}$，设 $\ell_i = L_\mu(i,\ell_{i-1},\varepsilon/(2S))$。那么，根据引理 3.3，我们有 $\Pr[\mathcal{E}(S,\ell_S)] \geq \Pr[\mathcal{E}(S,\lceil n^{0.99}\rceil)] \geq 1-\varepsilon/2$，当 n 足够大时成立，因此

$$\Pr[\mathcal{E}(s-1),\ell] \geq \Pr[\mathcal{E}(S,\ell_S)] \prod_{i=s}^{S} \Pr[\mathcal{E}(i-1,\ell_{i-1}) \mid \mathcal{E}(i,\ell_i)] \geq \Big(1-\frac{\varepsilon}{2}\Big)\prod_{i=s}^{S}\Big(1-p^{-i}-\frac{\varepsilon}{2S}\Big) \geq \prod_{i=s}^{\infty}(1-p^{-i}) - \varepsilon,$$

使用引理 3.2。 □

现在，正如在 定理 1.3 的证明中一样，我们需要通过对最后两行作一些特殊考虑来改进 推论 3.4 。为了采用相同的证明策略，我们需要以下关于“鲁棒高秩”线性映射的反集中不等式，这一结果可能具有广泛的意义。为了陈述这个引理，我们还需要引入一些记号。

定义 3.5. 对于域 $\mathbb{F}$上的矩阵 $M \in \mathbb{F}^{m\times n}$、行集合 $I \subseteq \{1,\dots,m\}$和列集合$J \subseteq \{1,\dots,n\}$，令 $M[I\times J]$ 为通过删除索引不属于 I的所有行以及索引不属于 J的所有列而得到的 $|I|\times|J|$子矩阵。

引理 3.6. 对于任意 $r \in \mathbb{N}$ 和 $\varepsilon > 0$，存在 $K = K_\mu(r,\varepsilon) \in \mathbb{N}$ 使得以下结论成立。考虑矩阵 $M \in \mathbb{F}_p^{m\times n}$以及互不相交的子集 $I_1,\dots,I_K \subseteq \{1,\dots,n\}$，其中每个$i = 1,\dots,K$均满足秩 $M[\{1,\dots,m\}\times I_i] \geq r$。令 $\vec{x} \in \mathbb{F}_p^n$为一个随机向量，其各项相互独立且服从 μ分布。那么

$$\Pr[M\vec{x} = \vec{0}] \leq \frac{1}{p^r} + \varepsilon.$$

我们将引理 3.6 的证明推迟到第 3.2 节。证明采用分类讨论：要么 M 的秩很高，此时我们可以轻松地为 $M\vec{x}$ 得到良好的反集中界（见引理 3.10）；要么我们可以用 r 上的 $M\vec{x}$ 独立且服从均匀分布的随机变量来近似 $\mathbb{F}_p$。

引理引理 3.6证明中的第二种情况需要下面这个引理（我们推导定理 1.4时也会用到）：许多独立随机变量之和近似服从均匀分布。设随机变量 $X \in \mathbb{F}_p$ 是 ε-近似均匀的，如果 $|$概率$[X=z] - 1/p| \leq \varepsilon$ 对所有 $z \in \mathbb{F}_p$都成立。

引理 3.7。 对于任意 $\varepsilon > 0$，存在 $Q = Q_\mu(\varepsilon) \in \mathbb{N}$，使得下述结论成立。考虑 $h \in \mathbb{F}_p^n$，使得其中至少 Q 个元素非零，并考虑一个随机向量 $\vec{x} \in \mathbb{F}_p^n$，其元素相互独立且服从 μ 分布。则 $h\cdot\vec{x}$ 是 ε-近似均匀的。

证明。令 Q 相对于 ε 和 μ足够大，并令 $k = \lfloor Q/(p-1)\rfloor$。不失一般性，我们可以假设 h 的前 k 个元素 $h_1,\dots,h_k$ 都等于同一个非零值 $h \in \mathbb{F}_p$。记$\vec{x} = (x_1,\dots,x_n)$，部分和序列

$$x_1,\ x_1+x_2,\ \dots,\ x_1+\cdots+x_k$$

可以解释为一个马尔可夫链。通过一些直接的分析（例如参见 [15,引理 5.1]及其后的注释）可知，只要 k相对于ε和 μ 足够大，$x_1+\cdots+x_k$就是 ε-近似均匀分布的。现在，对于 $x_{k+1},\dots,x_n$的任意固定结果进行条件化，对任意 $z \in \mathbb{F}_p$，我们有

$$\Pr\big[\vec{h}\cdot\vec{x} = z \,\big|\, x_{k+1},\dots,x_n\big] = \Pr\big[x_1+\cdots+x_k = h^{-1}(z-h_{k+1}x_{k+1}-\cdots-h_nx_n) \,\big|\, x_{k+1},\dots,x_n\big] \in \left[\frac{1}{p}-\varepsilon,\frac{1}{p}+\varepsilon\right].$$

最后，对 $x_{k+1},\dots,x_n$的所有结果取平均，便得到对所有 $z \in \mathbb{F}_p$均有 $\Pr[h\cdot\vec{x} = z] \in [1/p-\varepsilon, 1/p+\varepsilon]$，证毕。 □

在定理 1.4的证明中，我们不能直接应用引理 3.6。相反，我们需要以下推论。

推论 3.8。对于任意的 r、$\ell \in \mathbb{N}$ 和 $\varepsilon > 0$，存在 $D = D_\mu(r, \ell, \varepsilon) \in \mathbb{N}$ 使得以下结论成立。考虑一个矩阵 $M \in \mathbb{F}_p^{n\times n}$，以及大小为 r 的两两不交子集 $I_1, \ldots, I_D \subseteq \{1, \ldots, n\}$，其中对每个 $i = 1, \ldots, D$，均有 秩 $M[I_i \times I_i] = r$。令 $\vec{x} \in \mathbb{F}_p^n$ 为一个随机向量，其各个条目相互独立且服从 μ 分布。则

$$\Pr[M\vec{x} \text{ has at most } \ell \text{ nonzero entries }] \le \frac{2}{p^r} + \varepsilon.$$

证明。令 $K = K_\mu(r, \varepsilon/2)$，其中 $K_\mu(\cdot,\cdot)$ 如引理 3.6 所述，并令 $D = 2\ell K$。考虑一个矩阵$M \in \mathbb{F}_p^{n\times n}$以及满足推论假设的子集 $I_1, \ldots, I_D \subseteq \{1, \ldots, n\}$。现在，对 $j = 1, \ldots, 2\ell$，令 $M_j = M[(I_{(j-1)K+1} \cup \cdots \cup I_{jK}) \times \{1, \ldots, n\}]$ 为 M 中由索引属于 $I_{(j-1)K+1} \cup \cdots \cup I_{jK}$ 的行组成的 $(rK) \times n$ 子矩阵。由于对所有 $i = 1, \ldots, K$，秩 $M_j[I_{(j-1)K+i} \times I_{(j-1)K+i}] =$秩 $M[I_{(j-1)K+i} \times I_{(j-1)K+i}] = r$，矩阵 M_j 连同集合 $I_{(j-1)K+1}, \ldots, I_{jK}$ 满足引理 3.6 的假设。因此，对所有 $j = 1, \ldots, 2\ell$，我们得到概率$[M_j\vec{x} = \vec{0}] \le p^{-r} + \varepsilon/2$。

现在，如果 $M\vec{x}$ 至多有 ℓ 个非零条目，那么至少有 $2\ell - \ell = \ell$ 个指标$j \in \{1, \ldots, 2\ell\}$满足 $M_j\vec{x} = \vec{0}$。由于满足 $M_j\vec{x} = \vec{0}$的指标 $j \in \{1, \ldots, 2\ell\}$ 的期望数量至多为 $(p^{-r}+\varepsilon/2)\cdot 2\ell = (2p^{-r} + \varepsilon)\ell$，由马尔可夫不等式可得

$$\text{概率}[M\vec{x} \text{ 至多有 } \ell \text{ 个非零条目 }] \le \text{概率}[M_j\vec{x} = \vec{0} \text{ 至少有 } \ell \text{ 个不同的 } j] \le \frac{(2p^{-r} + \varepsilon)\ell}{\ell} = \frac{2}{p^r} + \varepsilon. \quad \square$$

现在我们说明如何利用定理 1.4从引理 3.2和3.7以及推论 3.4和3.8推出。证明的结构与定理 1.3的证明非常相似，不过这里的记号稍显复杂，而且我们需要用本节迄今为止整理出的更精巧的引理，替换某些平凡的估计。

定理 *1.4* 的证明。任取 $\varepsilon > 0$ 和 $\ell \in \mathbb{N}$。我们将证明，当 n 相对于 ε充分大时，ℓ 且 μ时，有

$$\Pr[\mathcal{E}(1, \ell)] \ge \prod_{i=2}^{n}(1 - p^{-i}) + (1 - 2\alpha_p)(p^{-2} - 2p^{-3}) - \varepsilon. \tag{3.1}$$

为说明这已足够，考虑 $\ell = Q_\mu(\varepsilon)$ (其中 $Q_\mu(\cdot)$ 如引理 3.7所述)。对 $A^{\uparrow 1}$ 满足 $\mathcal{E}(1, \ell)$ 的一个结果进行条件化，由事实 2.1 可知，积和式$\mathrm{per}(A)$ 可解释为 A的最后一行各元素的线性组合，其中至少有 ℓ 个系数非零。因此，引理 3.7 给出

$$\Pr[\mathrm{per}(A) \ne z] \ge \Pr[\mathrm{per}(A) \ne z \,|\, \mathcal{E}(1, \ell)] \cdot \Pr[\mathcal{E}(1, \ell)] \ge \left(1 - \frac{1}{p} - \varepsilon\right)\Pr[\mathcal{E}(1, \ell)] \ge (1 - p^{-1})\Pr[\mathcal{E}(1, \ell)] - \varepsilon$$

并结合(3.1)，当 n 充分大时，我们得到

$$\Pr[\mathrm{per}(A) \ne z] \ge (1-p^{-1})\prod_{i=2}^{n}(1-p^{-i}) + (1-p^{-1})(1-2\alpha_p)(p^{-2}-2p^{-3}) - 2\varepsilon \ge 1 - \alpha_p + (1-2\alpha_p)p^{-2}/5 - 2\varepsilon.$$

取 $\varepsilon = (1 - 2\alpha_p)p^{-2}/20$，这意味着(1.5) (其中 $\delta_p = (1 - 2\alpha_p)p^{-2}/10$)。此外，取 $\varepsilon = p^{-3}$，引理 3.7 给出

$$\left|\Pr[\mathrm{per}(A) = z] - \frac{1}{p}\right| \le \left|\Pr[\mathrm{per}(A) = z \,|\, \mathcal{E}(1, \ell)] - \frac{1}{p}\right| + \Pr[\mathcal{E}(1, \ell)^{\mathrm{c}}] \le \varepsilon + \Pr[\mathcal{E}(1, \ell)^{\mathrm{c}}] = \Pr[\mathcal{E}(1, \ell)^{\mathrm{c}}] + p^{-3}$$

对于任意 $z \in \mathbb{F}_p$，利用 (3.1) 我们可以计算（同样要求 n 足够大）

$$\begin{aligned}
\Pr[\mathcal{E}(1, \ell)^{\mathrm{c}}] = 1 - \Pr[\mathcal{E}(1, \ell)] &\le 1 - \prod_{i=2}^{n}(1 - p^{-i}) - (1 - 2\alpha_p)(p^{-2} - 2p^{-3}) + \varepsilon \\
&\le \sum_{i=2}^{n} p^{-i} - (p^{-2} - 2p^{-3}) + 2\alpha_p p^{-2} + 2p^{-3} \\
&\le 2p^{-3} + 2p^{-3} + 2\alpha_p p^{-2} + 2p^{-3} \le 10p^{-3},
\end{aligned}$$

利用 $\alpha_p = 1 - \prod_{i=1}^{\infty}(1-p^{-i}) \le \sum_{i=1}^{\infty} p^{-i} \le 2p^{-1}$。因此，我们得到

$$\left|\Pr[\mathrm{per}(A) = z] - \frac{1}{p}\right| \le 10p^{-3} + p^{-3} = 11p^{-3}$$

对任意 $z \in \mathbb{F}_p$，证明 (1.6) 成立，其中 $C = 11$。

因此，我们只需证明 (3.1)。按照定理 1.3 证明中的定义，定义矩阵 $H \in \mathbb{F}_p^{n\times n}$和图 G （在 $A^{\uparrow 2}$ 中编码 $(n-2) \times (n-2)$ 子矩阵的积和式）。令 $D_\mu(\cdot,\cdot,\cdot)$ 如推论 3.8 中所述，并令 $D = D_\mu(3, \ell, \varepsilon/4)$。根据马尔可夫不等式和推论 3.4，我们的图 G 含有至少 $\binom{n}{2} - n^2/4 - 3Dn$ 条非边的概率至多为 $2\alpha_p + o(1)$。若此情况发生，我们便可以反复应用 Mantel 定理（定理 2.6），找到 D 个顶点不相交三角形。（每次应用 Mantel 定理找到一个三角形后，在下一次应用之前，删除所有与该三角形顶点关联的边。）

正如在 定理 1.3 的证明中一样，通过 引理 2.5， G 中的一个三角形给出一个大小为 3 的集合 $I \subseteq \{1,\dots,n\}$，使得 $\mathrm{rank}(H[I\times I]) = 3$。记 $\mathcal{F}^*$ 为如下事件：存在 D 个两两不交的大小为 3 的集合 $I_1, \dots, I_D \subseteq \{1,\dots,n\}$，使得对每个 $i = 1, \dots, D$；我们刚刚证明了

$$\Pr[\mathcal{F}^*] \ge 1 - 2\alpha_p + o(1).$$

对于 $A^{\uparrow 2}$ 的任意一个满足 $\mathcal{F}^*$ 的结果，我们可以将 推论 3.8 应用于矩阵 $H \in \mathbb{F}_p^{n\times n}$，并发现以至少 $1 - 2p^{-3} - \varepsilon/4$ 的概率，向量 $H\vec{x}$ 至少有 ℓ 个非零条目，其中 $\vec{x} \in F_p^n$ 表示由 A倒数第二行中的条目组成的随机向量。现在， $H\vec{x}$ 中的条目恰好是 $(n-1) \times (n-1)$ 的 $A^{\uparrow 1}$子矩阵的永久式，而至少有 ℓ 个这样的非零条目意味着事件 $\mathcal{E}(1, \ell)$ 成立。因此，我们得到

$$\Pr[\mathcal{E}(1,\ell) \mid \mathcal{F}^*] \ge 1 - 2p^{-3} - \varepsilon/4.$$

现在，令 $L_\mu(\cdot,\cdot,\cdot)$ 如 引理 3.2 中所述，并记 $\mathcal{E}^*(2) = \mathcal{E}(2, L_\mu(2, \ell, \varepsilon/4))$。那么由 推论 3.4 可得

$$\Pr[\mathcal{E}^*(2)] \ge \prod_{i=3}^{\infty}(1-p^{-i}) - \varepsilon/4$$

当 n 充分大时。

综合以上结果，并应用 引理 3.2，可得

$$\begin{aligned}
\Pr[\mathcal{E}(1,\ell)] &\ge \Pr[\mathcal{E}(1,\ell) \mid \mathcal{F}^*]\Pr[\mathcal{F}^*] + \Pr[\mathcal{E}(1,\ell) \mid \mathcal{E}^*(2)\setminus\mathcal{F}^*]\Pr[\mathcal{E}^*(2)\setminus\mathcal{F}^*] \\
&\ge (1 - 2p^{-3} - \varepsilon/4)\Pr[\mathcal{F}^*] + (1 - p^{-2} - \varepsilon/4)\Pr[\mathcal{E}^*(2)\setminus\mathcal{F}^*] \\
&\ge (1 - 2p^{-3})\Pr[\mathcal{F}^*] + (1 - p^{-2})\Pr[\mathcal{E}^*(2)\setminus\mathcal{F}^*] - \varepsilon/2 \\
&\ge (1 - 2p^{-3})\Pr[\mathcal{F}^*] + (1 - p^{-2})\left(\prod_{i=3}^{\infty}(1-p^{-i}) - \varepsilon/4 - \Pr[\mathcal{F}^*]\right) - \varepsilon/2 \\
&\ge \prod_{i=2}^{\infty}(1-p^{-i}) + (p^{-2} - 2p^{-3})\Pr[\mathcal{F}^*] - 3\varepsilon/4 \\
&\ge \prod_{i=2}^{\infty}(1-p^{-i}) + (p^{-2} - 2p^{-3})(1 - 2\alpha_p + o(1)) - 3\varepsilon/4,
\end{aligned}$$

并且当 (3.1) 充分大时，式 n成立。 □

3.1. **生成许多具有非零矩阵永久式的矩阵**。 本节我们证明 引理 3.3，并改编 Tao 和 Vu [31] 的一种策略。回顾 定义 3.1中的定义。首先，下面的引理适用于找出一个具有单个 非零矩阵永久式的子矩阵。

引理 3.9。 对于任意 $\varepsilon > 0$，存在 $T = T_\mu(\varepsilon) \in \mathbb{N}$，使得以下结论成立。考虑任意大小为 $|J| = 2T$ 的子集合 $J \subseteq \{1,\dots,n\}$。则，

$$\Pr[\textit{there is a subset } I \subseteq J \textit{ of size } |I| = T \textit{ with } \mathrm{per}(A;I) \ne 0] \ge 1 - \varepsilon.$$

证明。令 $\rho = \max_{z\in\mathbb{F}_p} \mu(z) < 1$（注意到 μ 至少支撑于两个取值），并选取充分小的 $0 < \delta < 1$，使得 $1-\rho(1+\delta) > \delta$。此外，选取充分大的 $T > 2(1+\delta)/(\varepsilon\delta^2)$，使得 $\rho^{\delta T}/(1-\rho) < \varepsilon/4$。

我们考虑一个随机过程，尝试构造一个嵌套集合序列 $I_0 \supseteq \cdots \supseteq I_{n-T}$（从 $I_0 = \{1,\dots,n\}$ 开始，并在每一步移除一个元素），使得对于所有 $t = 0,\dots,n-T$，以及 $I_{n-T} \subseteq J$，都有 $\mathsf{per}(A;\, I_t) \neq 0$。如果该过程成功，我们就可以将 I_{n-T} 作为所需的集合 I。

具体而言，该过程定义如下。令 $T' = 2T + \lfloor \delta T \rfloor$。对于每一步 $t = 1,\dots,n-T'$，我们如下定义 I_t：

- 如果存在满足 $\mathsf{per}(A;\, I_{t-1}\setminus\{i\}) \neq 0$ 的 $i \in I_{t-1}\setminus J$，则取最小的此类 i 并令 $I_t = I_{t-1}\setminus\{i\}$。
- 否则，终止该过程。

对于每一步 $t = n-T'+1$、.....、$n-T$，我们定义 I_t 如下：

- 若存在满足 $\mathsf{per}(A;\, I_{t-1}\setminus\{i\}) \neq 0$ 的 $i \in I_{t-1}\setminus J$，则取其中最小的 i，并令 $I_t = I_{t-1}\setminus\{i\}$。
- 否则，若存在满足 $\mathsf{per}(A; I_{t-1}\setminus\{i\}) \neq 0$ 的任何 $i \in I_{t-1}$，则取其中最小的 i，并令$I_t = I_{t-1}\setminus\{i\}$。
- 否则，终止该过程。

也就是说：在前 $n-T'$ 步中的每一步，我们都确保移除一个 J 之外的元素。在随后的每一步中，如果可能，我们仍然尝试移除一个 J 之外的元素；若不可能，则允许移除其他元素。注意，只要集合 I_t 有定义，我们总有 $|I_t| = n-t$ 且 $\mathsf{per}(A; I_t) \neq 0$；还要注意，$I_t$ 仅取决于 $A^{\uparrow(n-t)}$ 的结果（也就是说，仅取决于矩阵 A 的前 t 行）。

只需证明，以至少 $1-\varepsilon/2$ 的概率，该过程在定义 I_{n-T} 之前的任何步骤都不会终止，并证明其[2] $I_{n-T} \not\subseteq J$ 以至多 $\varepsilon/2$ 的概率成立。

首先注意，对于 $A^{\uparrow(n-t)}$ 的任意结果，只要 $\mathsf{per}(A; I_t) \neq 0$，就有

$$\Pr[\text{the process terminates at step } t+1 \mid A^{\uparrow(n-t)}] \le \begin{cases} \rho^{|I_t\setminus J|} \le \rho^{n-t-2T} & \text{if } t < n-T' \\ \rho^{|I_t|} = \rho^{n-t} & \text{if } n-T' \le t < n-T \end{cases}$$

其推理基本上与引理 2.3 的证明相同。事实上，写作 $A = (a_{i,\,j})$，在给定 $A^{\uparrow(n-t)}$ 的一个结果的条件下，再对所有 $i \notin I_t$ 给定 $a_{t+1,\,i}$ 的条件。于是，对于 $i \in I_t$，量 $\mathsf{per}(A; I_t\setminus\{i\})$ 变为独立随机变量（每个变量仅取决于 $a_{t+1,\,i}$ 的结果），并且每个变量取任意特定值的概率至多为 ρ，尤其是取零值的概率也至多为该值。

由并集界可知，该过程在某一步终止（即 I_{n-T} 未被定义）的概率至多为

$$\sum_{t=0}^{n-T'-1} \rho^{n-t-2T} + \sum_{t=n-T'}^{n-T-1} \rho^{n-t} = \sum_{j=T'+1-2T}^{n-2T} \rho^j + \sum_{j=T+1}^{T'} \rho^j \le \frac{\rho^{\lfloor\delta T\rfloor+1} + \rho^{T+1}}{1-\rho} \le \frac{2\rho^{\delta T}}{1-\rho} \le \frac{\varepsilon}{2}.$$

现在我们研究 $I_{n-T} \not\subseteq J$ 的概率。对于 $t = n-T'+1,\dots,n-T$，若步骤 t 满足$I_t \setminus J = I_{t-1} \setminus J \neq \emptyset$（即，若 $I_{t-1} \not\subseteq J$，且步骤 t 中从 I_{t-1} 移除的元素属于 J），则称该步骤为坏步骤。那么，对于满足 $I_{t-1} \not\subseteq J$ 的 $A^{\uparrow t}$ 的任意结果，我们有

$$\Pr[t \text{ is bad} \mid A^{\uparrow t}] \le \rho^{|I_{n-t}\setminus J|} \le \rho,$$

并且，对于满足 $I_{t-1} \subseteq J$ 的 $A^{\uparrow t}$ 的任意结果，我们有：步骤 $[t$ 为坏步骤的概率为 $\mid A^{\uparrow t}] = 0 \le \rho$。因此，坏步骤的数量在随机意义上被一个服从二项分布$(T'-T, \rho)$的随机变量所支配。

现在，若 $I_{n-T} \not\subseteq J$，则必定存在一个元素 $h \in I_{n-T} \not\subseteq J$。这意味着，对于所有 $t = n-T'+1,\dots,n-T$，都有 $I_t \not\subseteq J$。此外，在步骤 $n-T'+1,\dots,n-T$ 这 $T'-T$ 步中，最多有 $|I_{n-T'} \setminus J| \le |I_{n-T'}| - |J| = T' - 2T = \lfloor \delta T \rfloor$ 个外部于 J 的元素被移除。这意味着这些步骤中至少有 $T' - T - \lfloor \delta T \rfloor = T$ 步必须是坏步骤。

因此，记为 $B \sim$二项分布$(T'-T,\ \rho)$（其期望为 $\rho(T'-T)$，标准差至多为$\sqrt{T'-T} \le \sqrt{(1+\delta)T}$），我们有

$$\Pr[I_{n-T} \not\subseteq J] \le \Pr[\text{at least } T \text{ of the steps } n-T'+1,\dots,n-T \text{ are bad}]$$

[2]如果我们在某一步终止（因此未定义 I_{n-T}），就说事件 $\{I_{n-T} \not\subseteq J\}$ 未发生。

$$\le \Pr[B \ge T]$$
$$\le \Pr[B \ge \rho(T'-T)+\delta T] \le \frac{(1+\delta)T}{\delta^2 T^2} = \frac{(1+\delta)}{\delta^2 T} \le \frac{\varepsilon}{2},$$

注意到，根据 T' 和 δ 的定义， $\rho(T'-T)+\delta T \le \rho(1+\delta)T+\delta T \le T$，并使用切比雪夫不等式。□

现在我们说明如何推出 引理 3.3。

引理 3.3 的证明。令 $T_\mu(\cdot)$ 如引理 3.9 中所述，并令 $S = T_\mu(\varepsilon/2)$。令 $\ell = 2\lceil n^{0.99}\rceil$，并固定互不相交的子集 $J_1, \ldots, J_\ell \subseteq \{1,\ldots,n\}$，其大小均为 $2S$。若存在一个大小为 $|I_i| = S$ 的子集 $I_i \subseteq J_i$，使得 $\mathrm{per}(A; I_i) \neq 0$，则称 J_i 是好的；否则称 J_i 是坏的。于是，根据引理 3.9，每个 J_i 为坏的概率至多为 $\varepsilon/2$。根据马尔可夫不等式， $J_1, \ldots, J_\ell$ 中超过一半为坏的概率至多为 $2(\varepsilon/2) = \varepsilon$。如果这种情况没有发生，即至少有 $\ell/2 = \lceil n^{0.99}\rceil$ 个集合 $J_1, \ldots, J_\ell$ 是好的，那么 $\mathcal{E}(S, \lceil n^{0.99}\rceil)$ 就会发生。□

3.2. **线性映射的近似均匀性**。 本节将证明 引理 3.6 并用它推导出引理 3.2。首先，我们需要下面这个简单引理，它根据 $M\vec{x}$ 的秩以及 M 的元素分布，给出了 $\vec{x}$的反集中界。

引理 3.10。 设 $\rho = \max_{z\in\mathbb{F}_p} \mu(z) < 1$，并设 $\vec{x} \in F_p^n$ 是一个各元素相互独立且服从 μ 分布的向量。那么对于任意矩阵 $M \in \mathbb{F}_p^{m\times n}$ 和任意 $\vec{z} \in \mathbb{F}_p^m$，我们有

$$\Pr[M\vec{x} = \vec{z}] \le \rho^{\operatorname{rank} M}.$$

证明。 我们可以将 $M\vec{x} = \vec{z}$ 视为一个线性方程组。令 $r =$ 为秩 M，则该方程组恰有 $n-r$ 个自由变量。将 $\vec{x}$ 中对应于这些自由变量的元素取值固定后，对于其余的 r 个元素，至多有一种取值使得 $M\vec{x} = \vec{z}$。对于这些元素中的每一个，取到相应值的概率至多为 ρ，因此总体而言，概率 $[M\vec{x} = \vec{z}]$ 至多为 $\rho^r = \rho^{\operatorname{rank} M}$。□

现在，我们可以证明引理 3.6。

引理 *3.6* 的证明。 不失一般性，我们可以假设 $\varepsilon < 1/2$。令 $\rho =$ 的最大值$_{z\in\mathbb{F}_p} \mu(z) < 1$ 为 μ的最大点概率，并令 $R \in \mathbb{N}$ 满足 $\rho^R \le p^{-r}$。此外，令 $Q_\mu(\cdot)$ 如引理 3.7所述，令 $Q = Q_\mu(\varepsilon/r)$ 并令 $K = 2p^R Q$。

首先，考虑秩 $M > R$的情形。由引理 3.10 可得

$$\Pr[M\vec{x} = \vec{0}] \le \rho^{\operatorname{rank} M} \le \rho^R \le p^{-r} + \varepsilon,$$

正如所需。

因此，以下我们假设 $\mathrm{rank}(M) \le R$。那么存在一个大小为 $|I| \le R$ 的集合 $I \subseteq \{1,\ldots,m\}$，使得由 I 索引的行张成矩阵 M 的行空间。特别地，对任意 $i = 1,$ ....., K，矩阵 $M[\{1,\ldots,m\} \times I_i]$ 的行空间由 I 索引的行张成，因此我们的假设 rank $M[\{1,\ldots,m\} \times I_i] \ge r$ 蕴含 rank $M[I \times I_i] \ge r$。于是，对每个 $i = 1,$ ....., K，子矩阵 $M[I \times I_i]$ 有 r 个线性无关列。

令 $S \subseteq \mathbb{F}_p^I$ 为至少作为 $M[I \times \{1,\ldots,n\}]$ 的列出现 $K/(2p^R) = Q$ 次的“流行”向量集合。$M[I \times \{1,\ldots,n\}]$ 中至多有 $p^{|I|} \cdot K/(2p^R) \le p^R \cdot K/(2p^R) = K/2$ 列不是流行向量，因此存在一个索引 $i \in \{1,\ldots,K\}$，使得 $M[I \times I_i]$ 的所有列都是流行向量。这尤其意味着存在 r 个线性无关的流行向量 $\vec{v}_1,$ ..., $\vec{v}_r \in S \subseteq \mathbb{F}_p^I$。将 M 的列重新排列后，不妨假设 $M[I \times \{1,\ldots,n\}]$的前 Q 列都等于 $\vec{v}_1$，接下来的 Q 列都等于 $\vec{v}_2$，依此类推。那么，每当有 $M\vec{x} = \vec{0}$ 时，就可得出 $M[I \times \{1,\ldots,n\}]\vec{x} = \vec{0}$，因此

$$(x_1 + \cdots + x_Q)\vec{v}_1 + \cdots + (x_{(r-1)Q+1} + \cdots + x_{rQ})\vec{v}_r + M[I \times \{rQ+1,\ldots,n\}](x_{rQ+1},\ \ldots,\ x_n)^T = M\vec{x} = \vec{0}.$$

因此，记 $\vec{z} = -M[I \times \{rQ+1,\ldots,n\}](x_{rQ+1},\ \ldots,\ x_n)^T$和 $y_j = x_{(j-1)Q+1} + \cdots + x_{jQ}$ 为 $j = 1,\ \ldots,\ r$，我们得到

$$\Pr[M\vec{x} = \vec{0}] \le \Pr\big[M[I \times \{1,\ldots,n\}]\vec{x} = \vec{0}\big] \le \Pr[y_1\vec{v}_1 + \cdots + y_r\vec{v}_r = \vec{z}].$$

现在，由于 $\vec{v}_1, \ldots, \vec{v}_r \in F_p^I$线性无关，对于 $\vec{z}$的任意结果， $y_1, \ldots, y_r \in \mathbb{F}_p$至多只有一个可能的结果，使得 $y_1\vec{v}_1 + \cdots + y_r\vec{v}_r = \vec{z}$。注意， $y_1, \ldots, y_r$相互独立，并且根据引理 3.7 每个 y_i 都是 (ε/r)-近似均匀分布，因此我们可以得出

$$\Pr[M\vec{x} = \vec{0}] \le \Pr[y_1\vec{v}_1 + \cdots + y_r\vec{v}_r = \vec{z}] \le \left(\frac{1}{p} + \frac{\varepsilon}{r}\right)^r \le \frac{1}{p^r} + \varepsilon. \qquad \square$$

现在我们说明如何推导出 引理 3.2。

引理 3.2 的证明。对于较大的 L，固定 $A^{\uparrow s}$ 的一个满足 $\mathcal{E}(s, L)$ 的取值，因此存在互不相交的、大小为 s 的集合 I_1、……、I_L，每个都满足 $\mathrm{per}(A; I_i) \neq 0$。对于每个 $j \in \{1, \ldots, L\}$，令 $\mathcal{F}_j$ 表示事件：对于所有 $i \in I_j$，$\mathrm{per}(A; I_j \setminus \{i\}) = 0$；并令 X 表示使 $\mathcal{F}_j$ 成立的 $j \in \{1, \ldots, L\}$ 的数量。我们的目标是证明，对于充分大的 L，有

$$\Pr[X > L - \ell] \le \frac{1}{p^s} + \varepsilon.$$

我们将通过研究 的一个足够高阶的矩来实现这一点， X并使用引理 3.6。

记 $\vec{x}$ 为 A 的第 $(n-s+1)$ 行。首先注意到（给定 $A^{\uparrow s}$ 的取值），对于每个 $j \in \{1, \ldots, L\}$，当 $i \in I_j$ 时，$\mathrm{per}(A; I_j \setminus \{i\})$ 的值关于 $\vec{x}$ 呈线性关系。我们定义一个 $s \times n$ 矩阵 M_j 来记录这种线性依赖（行由 I_j 索引，列由 $\{1, \ldots, n\}$ 索引），具体如下。对于 $i \in I_j$ 和 $h \notin I_j$，记 $I_j - i + h$ 表示大小为 s 的集合 $(I_j \setminus \{i\}) \cup \{h\}$。那么，对于 $i \in I_j$ 和 $h \in \{1, \ldots, n\}$，将 M_j 的 $(i,\ h)$ 项定义为

$$\begin{cases} \mathrm{per}(A; I_j - i + h) & \text{if } h \notin I_j, \\ \mathrm{per}(A; I_i) & \text{if } i = h, \\ 0 & \text{if } h \in I_j \setminus \{i\}. \end{cases}$$

不难看出（利用事实 2.1），对于任意 $i \in I_j$，i在 $M_j\vec{x}$ 中的元素恰好是$\mathrm{per}(A; I_j \setminus \{i\})$。特别地，当且仅当 $M_j\vec{x} = \vec{0}$时， $\mathcal{F}_j$ 出现。还需注意， $s \times s$ 子矩阵 $M_j[I_j \times I_j]$ 是一个对角矩阵，其对角线上的所有元素均为$\mathrm{per}(A; I_i) \neq 0$，因此有秩 $M_j[I_j \times I_j] = s$。

现在，设 $K_\mu(\cdot,\cdot)$ 如引理 3.6 中所述，并设 $K = K_\mu(s, \varepsilon/2)$。对于每个满足 $|J| = K$ 的子集 $J \subseteq \{1, \ldots, L\}$，令 $M_J \in \mathbb{F}_p^{(Ks)\times n}$ 为将矩阵 M_j （$j \in J$）依次上下拼接得到的矩阵（即其行由所有矩阵 M_j （$j \in J$）的行组成）。那么， M_J 满足引理 3.6 的条件，其中 $r = s$（因为对于所有 $j = 1$, ……， K，秩 $M_J[\{1, \ldots, Ks\} \times I_j] \ge$ 秩 $M_j[I_j \times I_j] = s$），因此

$$\Pr\left[\bigcap_{j \in J} \mathcal{F}_j\right] = \Pr[M_J\vec{x} = \vec{0}] \le \frac{1}{p^s} + \frac{\varepsilon}{2}.$$

这意味着

$$\mathbb{E}\left[\binom{X}{K}\right] \le \left(\frac{1}{p^s} + \frac{\varepsilon}{2}\right)\binom{L}{K},$$

因此，根据马尔可夫不等式，

$$\Pr[X > L - \ell] \le \Pr\left[\binom{X}{K} \ge \binom{L-\ell}{K}\right] \le \left(\frac{1}{p^s} + \frac{\varepsilon}{2}\right)\binom{L}{K}\binom{L-\ell}{K}^{-1} \le \frac{1}{p^s} + \varepsilon$$

当 L 足够大时。 $\square$

参考文献

[1] L. A. Bassalygo，奇特征有限域上非零积和式的数量，《信息传输问题》**49**（2013），第4期，382–383；Problemy Peredachi Informatsii 49（2013），第4期，95–97的译文。[2] M. V. Budrevich 和 A. E. Guterman，在有限域上，积和式的零点少于行列式，《有限域理论与应用》，《当代数学》，第579卷，美国数学会，普罗维登斯，罗得岛州，2012年，第33–42页。[3] J.-Y. Cai、A. Pavan 和 D. Sivakumar，关于永久式的计算困难性，STACS 99（特里尔），《计算机科学讲义》，第1563卷，施普林格，柏林，1999年，第90–99页。[4] L. S. Charlap、H. D. Rees 和 D. P. Robbins，随机偏置矩阵可逆的渐近概率，《离散数学》**82**（1990 年），第2期，153–163。[5] G. Dolinar、A. E. Guterman、B. Kuzma 和 M. Orel，有限域上的波利亚永久式问题，《欧洲组合数学杂志》**32**（2011），第1期，116–132。

[6] S. Eberhard，随机矩阵的特征多项式，《Combinatorica》42（2022），第4期，491–527。[7] L. Esperet，二部多重图中的反因子，arXiv预印本 arXiv:2205.14904。[8] U. Feige 和 C. Lund，关于计算随机矩阵永久式的计算困难性，《Comput. Complexity》6（1996），第2期，101–132。[9] P. Gemmell、R. Lipton、R. Rubinfeld、M. Sudan 和 A. Wigderson，多项式及近似函数的自测试/纠错，《第二十三届ACM计算理论研讨会论文集》——STOC '91，STOC '91，ACM出版社，1991年，第33–42页。[10] P. Gemmell 和 M. Sudan，多项式的高韧性纠错器，《Inform. Process. Lett.》43（1992），第4期，169–174。[11] F. Ghasemi、G. Gross 和 S. Kopparty，有限域上随机矩阵的积和式秩与行列式秩，arXiv预印本 arXiv:2512.03221（2025）。[12] A. Guionnet，伯努利随机矩阵，《欧洲数学大会》，EMS Press，柏林，2023年，第45–71页。[13] Z. Hunter、M. Kwan 和 L. Sauermann，积和式的指数级反集中，arXiv预印本 arXiv:2509.22577。[14] S. Jukna，极值组合学，《理论计算机科学丛书：EATCS系列》，施普林格出版社，柏林，2001年，附计算机科学应用。[15] J. Kahn 和 J. Komlós，有限域上随机矩阵的奇异概率，《Combin. Probab. Comput.》10（2001），第2期，137–157。[16] S. Kopparty，问题讨论（问题9），《组合学》，《Oberwolfach报告》14（2017），第1期，5–81；选自2017年1月1日至7日举行的研讨会摘要，由Jeff Kahn、Angelika Steger和Benny Sudakov组织。[17] I. N. Kovalenko 和 A. A. Levitskaja，有限域和有限环上随机线性方程组解的数量的极限行为，《苏联科学院学报》221（1975），第4期，778–781。[18] M. V. Kozlov，具有随机布尔元素的矩阵的秩，《苏联科学院学报》169（1966），1013–1016。[19] M. Kwan 和 L. Sauermann，关于随机对称矩阵的积和式，《Selecta Math.》（新系列）28（2022），第1期，论文编号15，29页。[20] R. J. Lipton，测试的新方向，《分布式计算与密码学》（普林斯顿，新泽西州，1989），DIMACS系列《离散数学、理论计算机科学与计算机科学》，第2卷，美国数学会，普罗维登斯，罗得岛州，1991年，第191–202页。[21] K. Luh、S. Meehan 和 H. H. Nguyen，有限域上随机矩阵的一些新结果，《伦敦数学学会杂志》（第2辑）103（2021），第4期，1209–1252。[22] P. H. Lundow 和 K. Markström，积和式的高效计算及其在玻色子采样和随机矩阵中的应用，arXiv预印本 arXiv:1904.06229。[23] K. Maples，随机矩阵的余核满足Cohen-Lenstra启发式，arXiv预印本 arXiv:1301.1239。[24] K. Maples，有限域上随机矩阵的奇异性，arXiv预印本 arXiv:1012.2372。[25] M. Marcus 和 H. Minc，关于行列式与积和式之间的关系，《伊利诺伊数学杂志》5（1961），376–381。[26] H. H. Nguyen 和 M. M. Wood，随机整矩阵：满射性的普适性与余核，《Invent. Math.》228（2022），第1期，1–76。[27] N. Robertson、P. D. Seymour 和 R. Thomas，永久式、Pfaffian定向与偶有向回路，《数学年刊》（第2辑）150（1999），第3期，929–975。[28] J. Sahasrabudhe，指数级小尺度下的概率组合学，arXiv预印本 arXiv:2512.15077。[29] D. Scheinerman，通过 $\mathbb{F}_3$ 进行积和式的快速计算，借助 $\mathbb{F}_2$ 算术，arXiv预印本 arXiv:2407.20205。[30] D. E. Smith，《数学资料汇编》，多佛出版社，纽约，1959年。[31] T. Tao 和 V. Vu，关于随机伯努利矩阵的积和式，《Adv. Math.》220（2009），第3期，657–669。[32] K. Tikhomirov，随机伯努利矩阵的奇异性，《数学年刊》（第2辑）191（2020），第2期，593–634。[33] V. V. Vazirani 和 M. Yannakakis，Pfaffian定向、0 25、1989、1 1987 179 190-永久式以及有向图中的偶圈，《组合学与复杂性》（芝加哥，伊利诺伊州，），第2卷，第–页。[34] V. H. Vu，随机矩阵理论中的组合问题，《国际数学家大会论文集——首尔2014》，第IV卷，Kyung Moon Sa，首尔，2014年，第489–508页。[35] V. H. Vu，组合随机矩阵理论的最新进展，《概率调查》18（2021），179–200。[36] M. M. Wood，随机图的沙堆群分布，《美国数学会杂志》30（2017），第4期，915–958。[37] M. M. Wood，随机整矩阵与Cohen-Lenstra启发式，《美国数学杂志》141（2019），第2期，383–398。数学系

，苏黎世联邦理工学院，苏黎世，瑞士。
电子邮件地址：zach.hunter@math.ethz.ch

奥地利科学技术研究所（ISTA）。奥地利克洛斯特新堡3400，Am Campus 1电子邮件地址：matthew.kwan@ist.ac.at

应用数学研究所，波恩大学，德国
电子邮件地址: sauermann@iam.uni-bonn.de