arXiv:2302.07239v2 [math.CO] 7 Jun 2023

有限域上的多斜矩阵与 Jacobi–Trudi 行列式

Omesh Dhar Dwivedi、Jonah Blasiak、Darij Grinberg

2023年6月5日

摘要。 从代数几何、拓扑学和组合学的角度，对计算代数簇上 $\mathbb{F}_q$ 值点数量的问题已有充分研究。我们探讨这一问题的一个带有组合色彩的版本，该版本由 Anzis 等人 [1]，研究，与 Kontsevich [7]，、 Elkies [4]，和 Haglund [5] 的工作相似。

Anzis 等人提出了这样一个问题：如果从有限域中均匀随机地选取变量，雅可比–特鲁迪矩阵的行列式为零的概率是多少？他们给出了若干类分拆的公式，例如钩形分拆、阶梯形分拆和矩形分拆。我们给出了各部分构成等差数列的分拆的公式，从而验证并推广了他们的一个猜想。更一般地，我们计算了一类由具有特定性质的托普利茨块构成的矩阵（“多斜矩阵”）的行列式为零的概率。

我们还证明，当斜分拆是带状分拆时，斜雅可比–特鲁迪矩阵的行列式在有限域上是均匀分布的。

关键词： Jacobi–Trudi 矩阵、Schur 函数、有限域、行列式、托普利兹矩阵。

MSC 类别（2020 年数学主题分类）： 05E05, 15B05, 11T06, 11C20。

1. 引言

设 $\mathbb{F}_q$ 为有限域。

一个*Jacobi–Trudi* 矩阵是如下形式的矩阵

$$J_{\lambda_1,\lambda_2,\ldots,\lambda_k}(z_1,z_2,z_3,\ldots) := \left(z_{\lambda_i-i+j}\right)_{1\leqslant i\leqslant k,\ 1\leqslant j\leqslant k} = \begin{pmatrix} z_{\lambda_1} & z_{\lambda_1+1} & \cdots & z_{\lambda_1+k-1} \\ z_{\lambda_2-1} & z_{\lambda_2} & \cdots & z_{\lambda_2+k-2} \\ \vdots & \vdots & \ddots & \vdots \\ z_{\lambda_k-k+1} & z_{\lambda_k-k+2} & \cdots & z_{\lambda_k} \end{pmatrix},$$

其中 $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k \geqslant 0$ 是整数。这里，$z_1,z_2,z_3,\ldots$ 是从$\mathbb{F}_q$ 中随机选取的元素（均匀且独立地），此外我们设$z_0 = 1$ 以及$z_i = 0$，其中$i < 0$。

我们研究该矩阵的行列式 $\det\left(J_{\lambda_1,\lambda_2,\ldots,\lambda_k}(z_1,z_2,z_3,\ldots)\right)$ 为零的概率。对于某些族的 λ_i，这一概率已在 [1] 中计算出。特别地，在以下情形中，该概率为 $1-q$：

- “矩形情形”：对于每个i，$\lambda_i = m$（参见 [1, 推论 6.4], ，或 [3] 中的推广）；
- “阶梯情形”：对于每个i，$\lambda_i = k+1-i$（参见 [1, 定理 6.5]）；
- “钩形情形”：λ_1 任意；$\lambda_i = 1$ 对于每个$i = 2$、3、.....、k（见 [1, 命题 1.2]）。

在更复杂的情形下，该概率的性质可能不太规则，尽管 Anzis 等人证明了 [1, 推论 5.2] 它总是大于或等于 $1-q$，并猜想 [1, 猜想 5.10]它总是小于或等于

$$1-\left|\mathrm{GL}_k\left(\mathbb{F}_q\right)\right|/q^{k^2} = 1-\prod_{i=1}^{k}\left(1-\frac{1}{q^i}\right).$$

本文的主要结果是在另一种情形下给出该概率的一个公式（见第 3 节中的证明）：

定理 1.1。设

$$(\lambda_1,\lambda_2,\ldots,\lambda_k) = (p+(k-1)n,\ p+(k-2)n,\ \ldots,\ p+n,\ p),$$

对于满足 $0 < p \leqslant n \leqslant k-1$ 的某些整数 p、n 和 k，则 $\det\left(J_{\lambda_1,\lambda_2,\ldots,\lambda_k}(z_1,z_2,z_3,\ldots)\right)$ 消失的概率为

$$1-\prod_{i=1}^{n}\left(1-\frac{1}{q^i}\right).$$

奇妙的是，这里的右侧也恰好是一个完全随机的一般$n \times n$-行列式消失的概率。

我们的证明以一个更一般的命题为基础，它适用于一类结构类似的更广泛的行列式（即所谓“多斜矩阵”的行列式）。

定理 1.1 证明并推广了 [1, 猜想 10。1] （同时也证实了该定理所涵盖的分拆类所满足的上界猜想 [1, 猜想 5。10]）。

定理 1.1 将作为下文定理 3.2 的**(ii)** 部分加以证明。同一定理的**(i)**部分将针对$k < n + 1$的情形给出类似的结论。对于$p >$ n </style}的情形，似乎也能得到类似的消失概率公式（猜想 3.3），但我们尚未能证明。

研究这些 Jacobi–Trudi 矩阵的行列式，一个重要动机来自*Schur* 函数理论：如果将z_i 替换为对称函数环的生成元h_i （定义见 § 2），那么 $\det\left(J_{\lambda_1,\lambda_2,\ldots,\lambda_k}(z_1, z_2, z_3, \ldots)\right)$ 就成为一个 Schur 函数。 [1]研究这些行列式时采用的正是这一观点。

我们的结果也可以从几何视角来理解：我们是在某些仿射概形上计数取值于 $\mathbb{F}_q$ 的点；Weil [12], Kontsevich [7], Stembridge [11], Stanley [10], Belkale-Brosnan [2], Elkies [4], Haglund [5], 等许多人都研究过类似问题。一个常见的问题是，取值于 $\mathbb{F}_q$ 的点的数量是否具有$f(q)$ 的形式，其中f是某个 Laurent 多项式；对于 $\det\left(J_{\lambda_1,\lambda_2,\ldots,\lambda_k}(z_1, z_2, z_3, \ldots)\right)$，这一点并非总是成立（见[1, 命题 5.7]），但在令人惊讶的许多情形下都成立，包括我们在此分析的情形。（Kontsevich 也曾针对某些图论多项式提出同样的问题，而答案是否定的 [2]。）

一般而言，$\det\left(J_{\lambda_1,\lambda_2,\ldots,\lambda_k}(z_1, z_2, z_3, \ldots)\right)$ 的取值在 $\mathbb{F}_q$ 中并非均匀分布，即使取值 0 的概率为 $1\ q$ 也是如此。例如，在钩形情形下，取值均匀分布（[1, 命题 1.2]），但在矩形情形下则不然（[1, 引理 9.3]）。我们将钩形情形推广，证明取值在带状分拆 （一类斜分拆）中均匀分布。我们还证明了一个关于这些行列式取某些值的概率的对称性性质（定理 4.1）。

致谢

我们感谢审稿人提出的有益意见，这些意见提升了本文的清晰度。

2. 记号与背景

固定一个有限域 $\mathbb{F}_q$。考虑多项式环

$$\mathcal{P} := \mathbb{Z}\left[h_1, h_2, h_3, \ldots\right]$$

在可数多个不定元 h_1,h_2,h_3,...。

定义 2.1. 对于任意的$f \in \mathcal{P}$ 和$a \in \mathbb{F}_q$，令$N \in \mathbb{N}$ 满足f 仅涉及不定元h_1, $h_2, \ldots, h_N$。定义f 取值为 a 的概率为有理数

$$P\left(f \mapsto a\right) := \frac{\left(\#\text{ of } \left(z_1, z_2, \ldots, z_N\right) \in \mathbb{F}_q^N \mid f\left(z_1, z_2, \ldots, z_N\right) = a\right)}{\left(\#\text{ of all } \left(z_1, z_2, \ldots, z_N\right) \in \mathbb{F}_q^N\right)}.$$

注意，右侧与N 的选取无关，因为N 增加 1 只会使分子和分母都乘以q。

顾名思义，$P\left(f \mapsto a\right)$ 表示将P 代入a 后得到该值的概率，其中h_1,h_2,h_3,... 被赋予从 $\mathbb{F}_q$ 中随机选取的元素（均匀且相互独立地选取）。由于f 只涉及有限个不定元，因此实际上不需要选取无限多个随机元素。

我们可以将多项式环 $\mathcal{P} = \mathbb{Z}\left[\mathrm{h}_1, \mathrm{h}_2, \mathrm{h}_3, \ldots\right]$ 与环Λ “对称函数”对应起来；事实上，对称函数是具有有界次数的、以可数多个不定元 $\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \ldots$ 为变量的对称形式幂级数（见[9, 第 7.1] 节或 [8, 第 I.2]节）。为此，我们将 $\mathcal{P}$ 中的每个生成元 h_i与完全齐次对称函数 $\mathrm{h}_i\left(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \ldots\right)$ =等同起来。

$\sum_{j_1 \leqslant j_2 \leqslant \ldots \leqslant j_i} x_{j_1} x_{j_2} \cdots x_{j_i} \in \Lambda$。本文实际上不会使用$x_i$。不过，我们会用到 Λ 的一些结构，特别是欧米伽对合ω: （例如参见 [9, 第 7.6] 节或 [8, (I.2.7)]）。

定义 2.2. 分拆 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ 是一个弱递减的正整数有限序列，其中 $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k$。

与分拆相关的几个重要概念如下。

定义 2.3. 分拆 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ 的大小 是总和 $\lambda_1 + \lambda_2 + \cdots + \lambda_k$。记作 $|\lambda|$。

分拆 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ 的长度 是数值k。记作 $\ell(\lambda)$。

定义 2.4. 分拆 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ 的杨图 $Y(\lambda)$ 是一个表（形状不一定是矩形）。它的方格（也称为单元格）

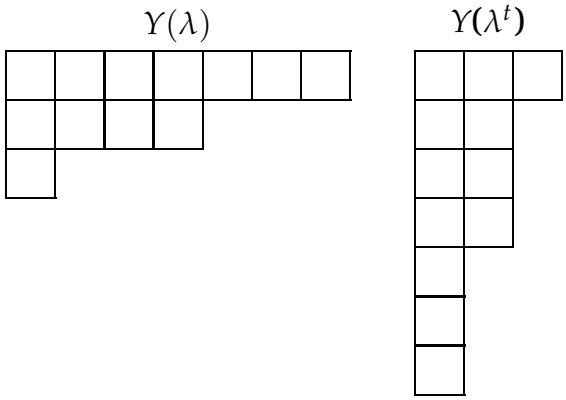
排列成k 行左对齐的行，其中第i行（从上往下数）有 λ_i 个方格。（因此，方格总数为 $|\lambda|$。）

形式上，$Y(\lambda)$ 定义为满足$i \leqslant k$ 和$j \leqslant \lambda_i$的所有正整数对(i, j) 构成的集合。数对(i,j) 对应图形中第i行从左数第j个方格。

定义 2.5. 分拆 λ 的共轭 λ^t 定义为这样一个分拆：其杨图由$Y(\lambda)$ 沿主对角线翻转得到（即，对于每个i，$Y\left(\lambda^t\right)$ 的第i行长度等于$Y(\lambda)$ 的第i列长度）。

下面的例 2.6 展示了如何为分拆 $\lambda = (7, 4, 1)$ 构造杨图及其共轭分拆。请注意，每行的方格数就是 λ中对应的部分。由于分拆是弱递减序列，图形中各行的方格数从上到下逐渐减少。

例 2.6. $\lambda = (7, 4, 1)$ 的共轭分拆为 $\lambda^t = (3, 2, 2, 2, 1, 1, 1)$。以下是这两个分拆的杨图：



定义 2.7. 若 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ 是一个分拆，则我们令 $\lambda_i := 0$，对每个$i > k$都成立。因此，分拆 λ 可视为无限弱递减序列$(\lambda_1, \lambda_2, \lambda_3, \ldots)$，其各项最终稳定为 0。

分拆的一种推广是斜分拆。

定义 2.8. (a) 斜分拆是满足$Y(\mu) \subseteq Y(\lambda)$ 的两个分拆组成的有序对(λ, μ)（或者等价地，对每个$i \geqslant 1$都有 $\mu_i \leqslant \lambda_i$）；记作 λ/μ。此处我们还将用 $\mu \subseteq \lambda$ 简写条件$Y(\mu) \subseteq Y(\lambda)$。

(b) 斜分拆 λ/μ 的斜图 $Y(\lambda/\mu)$ 定义为杨图的集合差：λ 和 μ 的杨图$Y(\lambda) \setminus Y(\mu)$ 之差，即属于 λ 的图形、但不属于 μ 的图形的方格集合。

(c) 任意分拆 λ 均可视为斜分拆 $\lambda/\varnothing$，其中 $\varnothing := (0, 0, 0, \ldots)$ 是空分拆。

现在我们将定义斜分拆的 Jacobi–Trudi 矩阵（推广[1,定义 2.3]）：

定义 2.9（Jacobi–Trudi 矩阵；斜舒尔函数）。**（a）**设 λ/μ 是一个斜分拆，且 $k = \ell(\lambda)$。定义 λ/μ 的 ***Jacobi–Trudi*** 矩阵为 $k \times k$ 阶矩阵

$$J(\lambda/\mu) := \left(h_{\lambda_i - \mu_j - i + j}\right)_{1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant k} \in \mathcal{P}^{k \times k}.$$

这里，对于所有的 $m < 0$，我们令 $h_0 := 1$ 和 $h_m := 0$。

（b） λ/μ 的斜舒尔函数定义为

$$s_{\lambda/\mu} := \det\left(J(\lambda/\mu)\right) \in \mathcal{P}. \tag{1}$$

(c) 当 $\mu = \varnothing$ 时，我们将矩阵 $J(\lambda/\mu)$ 和斜舒尔函数 $s^{\lambda/\mu}$ 分别记作 $J(\lambda)$ 和 s_λ。

注记 2.10. 若将 $\mathcal{P}$ 视为对称函数环，则斜舒尔函数 $s^{\lambda/\mu}$ 通常按如下组合方式定义：形状为 λ/μ 的半标准杨表 是对 λ/μ 的杨图进行填数所得的表，其中填入正整数，且各行从左到右弱递增，各列从上到下严格递增。于是，$s^{\lambda/\mu}$ 是单项式之和

$$\mathbf{x}_T = \prod_{i=1}^{\infty} x_i^{\#\text{ of } i\text{'s in } T}$$

对所有形状为 λ/μ 的半标准杨表 T 求和。根据这一表示法，(1) 是一个定理，称为第一 ***Jacobi–Trudi*** 恒等式（例如参见 [9, 定理 7.16.1]）。我们选择将 (1) 作为 $s^{\lambda/\mu}$ 的定义，因为在后续证明中，我们只会少量用到 $s^{\lambda/\mu}$ 的组合描述。

例如，如果 λ 是分拆 (7,4,1)，如例 2.6 所示，那么 Schur 函数 s_λ 为

$$s_{(7,4,1)} = \det\begin{pmatrix} h_7 & h_8 & h_9 \\ h_3 & h_4 & h_5 \\ 0 & 1 & h_1 \end{pmatrix},$$

等式右边的矩阵是$J(\lambda)$。

注 2.11. 设 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ 是一个分拆。那么，§ 1 中的矩阵 $J_{\lambda_1,\lambda_2,\ldots,\lambda_k}(z_1, z_2, z_3, \ldots)$ 恰好就是矩阵 $J(\lambda)$，其中每个 h_i 都已特化为 z_i。

3. 多斜矩阵与 p-平移 n 阶梯形分拆

3.1. p-平移 n-阶梯形分拆

我们将研究的第一类分拆是 p-平移 n 阶梯形分拆。这些分拆恰好是其各项构成非恒定等差数列的分拆。具体而言，它们定义如下：

定义 3.1。 设 $p > 0$、$n > 0$ 和 $k \geqslant 0$ 为整数。长度为 k 的 p-平移 n 阶梯分拆为

$$\lambda = (p + (k-1)n,\ p + (k-2)n,\ \ldots,\ p + n,\ p).$$

当 $p \leqslant n$ 时，我们称该分拆为内移 n 阶梯；当 $p > n$ 时，我们称其为外移 n 阶梯。

这个名称当然是指杨图的形状。

Anzis 等人 [1] 猜想，2-移位 2-阶梯 λ 满足 $P(s_\lambda \mapsto 0) = q^2 + q - 1\, q^3$。我们证明这一结果，并将其推广到任意的 n 和 p：

定理 3.2。 令 λ 为长度为 k 的 p-移位 n-阶梯（给定 $p > 0$、$n > 0$ 和 $k \geqslant 0$）。

(i) 假设 $k < n + 1$（p 任意）。则，

$$P(s_\lambda \mapsto 0) = 1 - \begin{cases} \prod_{i=1}^{k-1} \left(1 - \frac{1}{q^i}\right), & \text{if } p \leqslant k-1; \\ \prod_{i=1}^{k} \left(1 - \frac{1}{q^i}\right), & \text{if } p > k-1. \end{cases}$$

(ii) 假设 $p \leqslant n$ 且 $k \geqslant n + 1$。那么，

$$P(s_\lambda \mapsto 0) = 1 - \prod_{i=1}^{n} \left(1 - \frac{1}{q^i}\right).$$

猜想 3.3。 设 λ 为长度为 $k \geqslant n+1$、满足$p > n$的p-移位n-阶梯。那么，

$$P(s_\lambda \mapsto 0) = 1 - \prod_{i=1}^{n+1} \left(1 - \frac{1}{q^i}\right).$$

定理 3.2 与猜想 3.3 一同涵盖了整类p-移位n-阶梯形分拆。我们注意到，$P(s_\lambda \mapsto 0)$ 的四种表达式都不依赖于p。定理 3.2 **(ii)** 重述了引言中的定理 1.1。

定理 3.2 **(ii)** 右侧表示随机$n \times n$-矩阵在 $\mathbb{F}_q$ 上为奇异矩阵的概率。

我们将在第 3.3 小节证明定理 3.2 **(ii)** 。该证明将依托于一项关于某类结构化矩阵的更一般结果（这类矩阵由矩形 Toeplitz 块沿垂直边拼接而成），我们称之为多斜矩阵，并将在下文定义 3.9 中给出定义。这些矩阵具有良好的递归结构，因此可以显式计算其行列式为零的概率（定理 3.12）。完成这一步后，我们便可通过将适当的 Jacobi–Trudi 矩阵$J(\lambda)$ 的列重新排列，并识别出它是一个多斜矩阵，从而证明定理 3.2 **(ii)** （引理 3.18）。

定理 3.2（**i**）可以用类似的方法证明，但直接验证也相当容易，因为矩阵 J（λ）中的所有不定元都各不相同（并且该矩阵的所有元素都是不定元，除了最后一行中可能出现的一些 0 和 1）。

到目前为止，我们仍无法将这种推理方式应用于猜想 3.3；这似乎需要对“多斜矩阵”采用一种更宽松的定义，而这种定义不再适合轻松计算消失概率。

3.2. 多斜矩阵

我们用 $\mathbb{N}$ 表示集合 $\{0,1,2,\circ\}$。我们对每个 $n \in \mathbb{N}$令 $[n] = \{1,2,\circ\}$。

以下出现的所有矩阵都定义在 $\mathbb{F}_q$ 上，或定义在 $\mathbb{F}_q$ 上的多项式环上。

定义 3.4。 设 $A_1, A_2, \circ_k$ 是有限个行数相同的矩阵。那么，（$A_1 \mid A_2 \mid \cdots \mid A_k$）表示这样的分块矩阵：其各个块为 $A_1, A_2, \circ_k$，并从左到右水平排列。

例如，若 $A_1 = \begin{pmatrix} a & b & c & d \end{pmatrix}$ 且 $A_2 = \begin{pmatrix} e & f \end{pmatrix}$ 且 $A_3 = \begin{pmatrix} g & h & i & j \end{pmatrix}$，则 $(A_1 \mid A_2 \mid A_3) = \begin{pmatrix} a & b & e & g & h & c & d & f & i & j \end{pmatrix}$。

下文中，矩阵里的空格均视为填入零。例如，$\begin{pmatrix} 1 & & \\ 2 & 3 & \\ & 4 & 5 \end{pmatrix}$ 表示 3×3矩阵 $\begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 0 & 4 & 5 \end{pmatrix}$。

定义 3.5。若$u \times v$-矩阵满足高矩阵 条件$u \geqslant v$，则称其为高矩阵。

现在我们将定义一种符合我们需求的“托普利兹矩阵”概念。（在文献中，托普利兹矩阵通常是方阵，有时还是无限矩阵，而我们的矩阵是有限的，但通常不是方阵。除这些差异外，我们的概念与标准概念一致。）

定义 3.6。设$A = \left(a_{i,j}\right)_{1 \leqslant i \leqslant u,\, 1 \leqslant j \leqslant v}$为一个$u \times v$-矩阵。

(a) 对每个$k \in \mathbb{Z}$，A 的第 k 条副对角线 指A 中所有满足$i - j = k$的元素$a_{i,j}$所组成的列表。（这些元素按i递增的顺序排列，等价地说，也按j递增的顺序排列。）

例如，矩阵 $\begin{pmatrix} a & b & c & d & e & f \end{pmatrix}$ 的非空副对角线为

$$\underbrace{(b)}_{(-1)\text{-st paradiagonal}}, \quad \underbrace{(a,d)}_{0\text{-th paradiagonal}}, \quad \underbrace{(c,f)}_{1\text{-st paradiagonal}}, \quad \underbrace{(e)}_{2\text{-nd paradiagonal}}.$$

(b) 如果A 的一条副对角线含有v个元素，则称其为完整的。
例如，矩阵 $\begin{pmatrix} a & b & c & d & e & f \end{pmatrix}$ 的完整副对角线为(a,d)和(c,f)。注意，非高矩阵没有任何完整副对角线。

(c) 如果$u \geqslant v$，那么$(u-v)$阶副对角线也称为A 的最底部完整副对角线，其中$u \times v$-矩阵A。（它确实是完整的，也是A的完整副对角线中最底部的一条。）

(d) 如果矩阵 A 的每条副对角线上的元素都相等（即同一副对角线上的任意两个元素都相等），则称 A 为托普利兹矩阵。

例如，4×3-矩阵是托普利兹矩阵，当且仅当它具有以下形式
$\begin{pmatrix} c & b & a \\ d & c & b \\ e & d & c \\ f & e & d \end{pmatrix}$ for some a, b, c, d, e, f.

(e) 矩阵 A 中满足$i < j$ 的元素$a_{i,j}$ 称为阁楼项 。例如，矩阵 $\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix}$ 中唯一的阁楼项是b。**(f)** 矩阵 A 中满足$i > j + u - v$ 的元素$a_{i,j}$ 称为地下室项。例如，矩阵 $\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix}$ 中唯一的地下室项是e。

在高矩阵中，阁楼项是最顶部完整副对角线以上的项，而地下室项是最底部完整副对角线以下的项。

定义 3.7。 斜矩阵 是指形如

$$\begin{pmatrix} u_m & * & * & * \\ \vdots & \ddots & \vdots & \vdots \\ u_2 & \ddots & u_m & * \\ u_1 & \ddots & \vdots & u_m \\ u_0 & \ddots & u_2 & \vdots \\ & \ddots & u_1 & u_2 \\ & & u_0 & u_1 \\ & & & u_0 \end{pmatrix},$$

其中

- 每个星号（“$*$”）是不定元或 $\mathbb{F}_q$ 的一个元素；
- $u1$、$u2$、.....、u_m 是两两不同的m 个不定元；并且
- $u0$ 要么是不定元，且与$u1$、$u2$、.....、u_m 各不相同；要么是 $\mathbb{F}_q$ 中的一个元素；
- 阁楼项中的不定元均不会出现在任何完整副对角线上。

我们要求$m \geqslant 0$，并要求矩阵至少有一列。若u_0 是一个不定元，则称上面所示的斜矩阵为X 型；若$u_0 = 0$，则称其为0 型；若$u_0 \in \mathbb{F}_q \setminus \{0\}$，则称其为$1$ 型。

因此，在斜矩阵中，

- 所有阁楼项都是不定元或 $\mathbb{F}_q$ 的元素，并且在每条副对角线上相等（但不同副对角线上的值可以不同）；
- 所有地下室项均为 0；
- 每条副对角线上的元素都相等（即，位于同一副对角线上的任意两个元素相等）；
- 每条完整副对角线上的（相等）元素都是不定元，但最底部的完整副对角线除外，其元素也可以是 $\mathbb{F}_q$ 的一个元素；
- 任意两条不同副对角线上的不定元彼此不同，但如果两条副对角线都位于阁楼区域（即非完整副对角线上），则可能例外。

例如，矩阵

$$\begin{pmatrix} z & 2 & w \\ y & z & 2 \\ x & y & z \\ & x & y \\ & & x \end{pmatrix}, \quad \begin{pmatrix} z & 4 \\ y & z \\ 0 & y \\ & 0 \end{pmatrix}, \quad \begin{pmatrix} z & 3 & 1 & w \\ y & z & 3 & 1 \\ 4 & y & z & 3 \\ & 4 & y & z \\ & & 4 & y \\ & & & 4 \end{pmatrix}$$

（其中x、y、z、w 是四个不同的不定元）分别是 $\mathbf{X}$ 型、$\mathbf{0}$ 型和 $\mathbf{1}$ 型斜矩阵（假设 $4 \neq 0$ 属于 $\mathbb{F}_q$）。

定义3.8。 如果两个斜矩阵中没有共同出现的不定元，则称它们不相交 。

例如，斜矩阵 $\begin{pmatrix} & 3 & \\ z & & \\ & & \\ & 0 & \end{pmatrix} y\, z\, \mathbf{0}\, y$ 和 $\begin{pmatrix} & 3 & \\ w & & \\ & & \\ & 0 & \end{pmatrix} x\, w\, \mathbf{0}\, x$ 互不相交（其中 x、y、z、w 是四个不同的不定元），而斜矩阵 $\begin{pmatrix} & 0 & \\ z & & \\ & & \\ & 0 & \end{pmatrix} y\, z\, \mathbf{0}\, y$

and $\begin{pmatrix} z & 2 \\ x & z \\ 0 & x \\ & 0 \end{pmatrix}$ are not.

定义 3.9。多斜矩阵是指形如$(A_1 \mid A_2 \mid \cdots \mid A_k)$的矩阵$M$ ，其中$A_1, A_2, \ldots,$ A_k 是行数相同且两两不相交的斜矩阵。在这种情况下，斜矩阵$A_1, A_2, \ldots,$ A_k称为M的块。此外，M 的签名定义为三元组$(i,\ j,\ \ell)$，其中

- i 是M 中类型为 X 型的块的数量，
- j 表示M 中 0 型块的数量，而
- ℓ 表示M 中 1 型块的数量。

（当然，在这种情况下，$i+j+\ell=k$。）

例如，矩阵

$$\begin{pmatrix} z & 1 & 0 & p & w & 3 & 3 & e & 0 & t & 3 & 4 & 9 \\ y & z & 1 & 0 & v & w & 3 & d & e & s & t & 3 & 4 \\ 0 & y & z & 1 & u & v & w & c & d & 3 & s & t & 3 \\ & 0 & y & z & 1 & u & v & b & c & & 3 & s & t \\ & & 0 & y & & 1 & u & a & b & & & 3 & s \\ & & & 0 & & & 1 & & a & & & & 3 \end{pmatrix}$$

（其中所有字母都是互不相同的不定元）是一个含有四个块的多斜矩阵。该多斜矩阵的签名为 $(1,1,2)$，如果 $3\neq 0$ 属于 $\mathbb{F}_q$（因为它有 1 个 X 型块、1 个 0 型块和 2 个 1 型块）；如果 $3=0$ 属于 $\mathbb{F}_q$，则签名为 $(1,2,1)$。

注意，空的 0×0-矩阵是一个多斜矩阵（含有 0 个块，签名为 $(0,0,0)$），但不是斜矩阵。我们回顾一下，这个 0×0-矩阵的行列式为 1（根据定义）。

定义 3.10。设 M 是一个方阵多斜矩阵。M 的奇异概率定义为：对每个出现在 M 中的不定元，以 $\mathbb{F}_q$ 中的随机元素替代后，$\det M$ 变为 0 的概率。（这里，$\mathbb{F}_q$ 中的随机元素指的是均匀且独立地选取的元素。）M 的奇异概率记为 $\mathrm{SiPr}\, M$。

例如，若M 是多斜矩阵 $\begin{pmatrix} b & 3 & y & a & b & x & a & 1 \end{pmatrix}$（对应四个互不相同的不定元$a$、$b$、$x$、$y$），那么$M$ 的奇异概率 $\mathrm{SiPr}\, M$ 就是四个从$\mathbb{F}_q$ 中（均匀且独立地）选取的随机元素 α、β、ξ、θ 满足 $\det\begin{pmatrix} \beta & \beta & \theta \\ \alpha & \beta & \xi \\ & \alpha & 1 \end{pmatrix}=0$的概率。结果表明，

该概率恰为 $1-q$。更一般地，我们将给出任意多斜矩阵的奇异概率公式。

–

首先，我们需要介绍一种记号：

定义 3.11。 对于每个正整数 k，我们记

$$\gamma_k := \left(1-\frac{1}{q^{k-1}}\right)\left(1-\frac{1}{q^{k-2}}\right)\cdots\left(1-\frac{1}{q^1}\right).$$

因此，特别地， $\gamma_1 = 1$ 和 $\gamma_2 = 1-\frac{1}{}q$。我们还设 $\gamma_0 = 1$。

众所周知，对于任意正整数 k， $\gamma_k = \left|\mathrm{GL}_{k-1}\left(\mathbb{F}_q\right)\right| / \left|\mathbb{M}_{k-1}\left(\mathbb{F}_q\right)\right|$。（但这实际上是下文定理 3.12 的一个特例。）

注意，使用q演算的记号（具体而言，使用$(a;q)_n$ 中定义的q-Pochhammer 符号，例如见 [6, §1.2]），我们可以将 γ_k 的定义改写为$\gamma_k = (1/q;1/q)_{k-1}$。

现在，我们提出如下结论：

定理 3.12. 设M 是一个非平凡的方阵多斜矩阵。设M的签名为(i,j,ℓ)，并设M的块数为$k = i+j+\ell$。那么，

$$\mathrm{SiPr}\, M = 1-\gamma_k\left(1-\frac{0^\ell}{q^i}\right). \tag{2}$$

当然，

$$0^\ell = \begin{cases} 0, & \text{if } \ell > 0; \\ 1, & \text{if } \ell = 0. \end{cases}$$

因此，(2) 可改述如下：

- 如果 $\ell > 0$（即M 至少有一个 1 型块），那么 $\mathrm{SiPr}\, M = 1-\gamma_k$。
- 如果 $\ell = 0$（即M 没有 1 型块），那么 $\mathrm{SiPr} M = 1-\gamma_k\left(1-\frac{1}{q^i}\right)$。

定理 3.12 通过归纳法证明，证明基于几个引理。首先，我们需要引入一些记号：

定义 3.13。 设A 为一个斜矩阵。设u_0 为A最后一列中的最底部元素。因此，u_0 或者是不定元（若A 为 X 型），或者为 0（若A 为 0 型），或者为 $\mathbb{F}_q$ 中的非零元素（若A 为 1 型）。此外，A 的最底部完整副对角线为$(u_0,u_0,\ldots,u_0)$。

(a) 我们称u_0 为A的底部元素。

(b) 对于任意$v \in \mathbb{F}_q$，我们用$A^{\to v}$ 表示将A 最底部完整副对角线上的所有元素替换为v后所得的矩阵。因此，当$v = 0$时，$A^{\to v}$ 是一个 0 型斜矩阵；否则，它是一个 1 型斜矩阵。

例如，若$A = \begin{pmatrix} z & 3 & 2 \\ y & z & 3 \\ x & y & z \\ & x & y \\ & & x \end{pmatrix}$，则$A$ 的底部元素是

不定元 x，并且我们有

$$A^{\to 0} = \begin{pmatrix} z & 3 & 2 \\ y & z & 3 \\ 0 & y & z \\ & 0 & y \\ & & 0 \end{pmatrix} \qquad \text{and} \qquad A^{\to 5} = \begin{pmatrix} z & 3 & 2 \\ y & z & 3 \\ 5 & y & z \\ & 5 & y \\ & & 5 \end{pmatrix}.$$

定义 3.14. (a) 如果斜矩阵的所有阁楼项都是 $\mathbb{F}_q$ 中的元素（而非不定元），则称该斜矩阵为严格的 。

(b) 如果多斜矩阵的所有块都是严格的，则称该多斜矩阵为严格的。

For example, the multislant matrix $\begin{pmatrix} z & t & 2 & v & 1 & s \\ y & z & t & u & v & r \\ x & y & z & w & u & q \\ & x & y & 1 & w & p \\ & & x & & 1 & 0 \end{pmatrix}$ is not strict, since 其第一个块的阁楼中有不定元 t ；将该不定元t替换为 $\mathbb{F}_q$ 中的任意常数元素，就能使此矩阵成为严格矩阵。

现在，我们可以陈述一些引理，通过归纳法帮助我们证明定理 3.12：

引理 3.15. 设M 是一个方阵严格多斜矩阵。假设M 至少有两个 1 型块。设A_i 和A_j 是M 中两个 1 型块，且$i \neq j$。假设块A_i 的列数不少于块A_j。那么，存在一个严格多斜矩阵M'，具有以下性质：

- 矩阵M' 是方阵，且与M大小相同。
- 它满足 $\mathrm{SiPr}\, M = \mathrm{SiPr}(M')$。
- 矩阵M' 与M 的唯一区别是：块A_j 被一个新的块替换，该块为 0 型。

*Pro*证明。 首先，我们概述论证；然后通过一个例子加以说明。

块 A_i 的列数至少与块 A_j一样多，因此其完整副对角线的数量至多与块 A_j 一样多（因为这两个块的高度相同）。因此，块 A_i 的不定元数量至多与

块 A^j 一样多（因为这两个块都是 1 型且为严格的，因此它们的不定元数量等于完整副对角线的数量减 1）。

现在，我们从A^j的每一列中减去A_i [1] 对应列的一个标量倍数（选择标量因子，使相减后A^j最底部完整副对角线变为$(0, 0, \ldots, 0)$）。相减后，A^j 中的不定元被替换为“准不定元”（即“一个不定元减去一个标量”或“一个不定元减去另一个不定元的标量倍数”这类差）。然而，在计算概率时，这些“准不定元”在$\mathbb{F}_q$上仍然是均匀独立分布的，因此我们可以通过变量替换将它们变回彼此不同的不定元；结果，块A^j再次成为一个斜矩阵，不过现在是 0 型（因为它的最底部完整副对角线为$(0, 0, \ldots, 0)$）。

因此，我们将块 A^j 变换成了一个新块，它是一个 0 型斜矩阵。M 的所有其他块保持不变。通过这些变换得到的整个矩阵称为 M'。

例如，假设

$$M = \begin{pmatrix} b & 2 & 3 & z & 5 \\ a & b & 2 & y & z \\ 1 & a & b & x & y \\ & 1 & a & 1 & x \\ & & 1 & & 1 \end{pmatrix}.$$

这个多斜矩阵只有两个块：

$$A_i = \begin{pmatrix} b & 2 & 3 \\ a & b & 2 \\ 1 & a & b \\ & 1 & a \\ & & 1 \end{pmatrix}, \qquad A_j = \begin{pmatrix} z & 5 \\ y & z \\ x & y \\ 1 & x \\ & 1 \end{pmatrix},$$

二者均为 1 型。现在，我们来做之前所说的事：从 A^j 的每一列中减去A_i 对应列的一个标量倍数。在这种情况下，所需的标量因子为 1（因为 A_i 和 A^j 的底部元素均为 1），因此我们只需从 A^j 的每一列中减去 A_i 的对应列。所得矩阵为

$$\widetilde{M} = \begin{pmatrix} b & 2 & 3 & z-2 & 5-3 \\ a & b & 2 & y-b & z-2 \\ 1 & a & b & x-a & y-b \\ & 1 & a & 0 & x-a \\ & & 1 & & 0 \end{pmatrix}.$$

[1]这里，我们从右向左对块的列进行计数。也就是说，A^j 中从右数第 3 列的“对应列”，就是A_i中从右数第 3 列。这一“对应列”总是存在，是因为块A_i 的列数至少与块A^j一样多。

请注意，这个矩阵中的元素 $x-a$、$y-b$和$z-2$是“准不定元”，而 $5-3$ 只是一个常数。如果现在对这个矩阵进行变量替换，将x、y 和z 分别代入$x-a$、$y-b$ 和$z-2$（由于这些是不定元且彼此独立，因此这样做不会改变奇异概率），那么我们得到

$$\begin{pmatrix} b & 2 & 3 & z & 5-3 \\ a & b & 2 & y & z \\ 1 & a & b & x & y \\ & 1 & a & 0 & x \\ & & 1 & & 0 \end{pmatrix};$$

这就是我们的矩阵 M'。它仍然是一个严格多斜矩阵，与M 的唯一区别在于，块 A_j 被一个 $\mathbf{0}$ 型块替换了。由于列运算没有改变行列式（而代换没有改变奇异概率），我们有 $\operatorname{SiPr} M = \operatorname{SiPr}(M')$。

请注意，我们用到了块 A_i 的列数至少与块 A_j 一样多这一点（事实上，这确保了A_j 的每一列都有A_i 中对应的一列可供相减），还用到了块 A_i 的不定元数至多与块 A_j 一样多这一点（事实上，这确保了列相减后，A_i 中的不定元只会与A_j中的不定元相减，而不会与阁楼项相减）。此外，M 的严格性确保我们没有从任何常数中减去不定元。

刚才分析的例子具有一般情形的代表性。如果M 除了A_i 和A_j之外还有其他块，那么这些额外的块不会受到减法操作的影响，也不会妨碍论证。如果A_i 和 A_j 的底部元素不是 $\mathbf{1}$，而是 $\mathbb{F}_q$中的其他非零元素，那么我们就必须从A_j 的列中减去非平凡的标量倍数，而不是直接减去这些列，但论证的实质不会改变。

□

引理 3.16. 设M 是一个方阵多斜矩阵。设A_j 是M 中一个 $\mathbf{X}$ 型块。对于任意$v \in \mathbb{F}_q$，令$M^{j\to v}$ 为将M 中的块A_j 替换为$A_j^{\to v}$后得到的多斜矩阵。那么，

$$\operatorname{SiPr} M = \frac{1}{q} \sum_{v\in\mathbb{F}_q} \operatorname{SiPr}\left(M^{j\to v}\right).$$

证明。 考虑A_j的底部元素；它是一个不定元（因为A_j 是 $\mathbf{X}$ 型）。当我们为M中出现的每个不定元都代入 $\mathbb{F}_q$ 中的一个随机元素时，这个不定元就变成了 $\mathbb{F}_q$中的一个元素。更具体来说，对于每个$v \in \mathbb{F}_q$，该不定元以概率 $1q$变为v 。因此，由全概率公式可得结论。

□

引理 3.17. 设M 是一个方形多斜矩阵，它有k 个块，且签名为$(0, k-1, 1)$。

因此，M 的所有块中，除一个之外均为 0 型，而剩下的块为 1 型。我们将后者称为“奇异块”。令M' 为从M 中删去M 的最底行以及奇异块的最右列后得到的矩阵。（注意，如果奇异块只有一列，这样做会使其完全消失。）于是：

(a) 矩阵M' 仍是一个签名为$(k-1, 0, 1)$ 或$(k-1, 0, 0)$ 的多斜矩阵（取决于奇异块是否有多于一列）。

(b) 我们有 $\mathrm{SiPr}M = \mathrm{SiPr}(M')$。

证明。 **(a)** 从M 变为M'时，每个 0 型块都会变为 X 型块（因为它少了一行，因此失去了最底部完整副对角线，而该副对角线由零组成[2]）。奇异块则要么仍为 1 型块（如果它有多于一列），要么完全消失（如果不是）。这涵盖了M'的所有块。因此，矩阵M' 是一个签名为$(k-1, 0, 1)$ 或$(k-1, 0, 0)$ 的多斜矩阵（取决于奇异块是否有多于一列）。

（**b**）M 的底行只有一个非零项，它是奇异块的底部元素。由于奇异块是 1 型，这个底部元素必定是某个非零元素$v \in \mathbb{F}_q$。因此，沿M 的底行展开行列式可得 $\det M = \pm v \det(M')$（因为v是M底行中唯一的非零项）。由于v 非零，这说明 $\det M$ 恰在 $\det(M')$ 为零时才为零。因此，$\mathrm{SiPr}\, M = \mathrm{SiPr}\,(M')$。

□

定理 *3.12* 的证明。对矩阵M的大小作归纳。在该归纳步骤中，对 $2i+\ell$ 使用强归纳法。因此，考虑一个非空方阵多斜矩阵M，其签名为$(i、j、\ell)$。设$k = i + j + \ell$ 为其块数。我们必须证明等式（2）。

不失一般性，我们假设多斜矩阵 M 是严格的。[3]我们属于以下四种情形之一：

[2]由于它的行数多于列数，因此它至少有两条完整副对角线[3]事实上，假设$\ell(2)$ 已在M 为严格的情况下得到证明。换言之，只要M 是严格的，$\mathrm{SiPr}M = \prod^{1-\gamma_k}\left(1-\frac{}{q^i}\right)$。现在，令$M$ 为

任意矩阵（不一定严格）。我们将M 各块中作为阁楼项出现的不定元称为阁楼变量。若为每个阁楼变量代入 $\mathbb{F}_q$ 中的一个随机元素，则矩阵M 就变为严格矩阵，因此（根据我们的假设），$\mathrm{SiPr}M$ 变为 $1-\gamma_k\left(1-\frac{0^\ell}{}q^i\right)$。

情形 *1*：矩阵 M 至少有一个 X 型块。

情形 *2*：矩阵 M 没有 X 型块，但有超过 1 个 1 型块。

情形 *3*：矩阵 M 没有 X 型块，且恰好有一个 1 型块。

情形 *4*：矩阵 M 没有 X 型块，也没有 1 型块。

我们先考虑情形 1。在这种情况下，矩阵 M 至少有一个 X 型块。令 Ai 为该块。因此，由引理 3.16 可得

$$\operatorname{SiPr} M = \frac{1}{q} \sum_{v \in \mathbb{F}_q} \operatorname{SiPr}\left(M^{j \to v}\right), \tag{3}$$

其中$M^{j\to v}$ 的定义与引理 3.16 中相同。现在，对任意非零$v \in \mathbb{F}_q$，矩阵$M^{j\to v}$ 的签名为$(i-1, j, \ell+1)$（因为它是将M 中的 X 型块Ai 替换为 1 型块得到的），且仍有k 个块，因此满足

$$\operatorname{SiPr}\left(M^{j \to v}\right) = 1 - \gamma_k \left(1 - \frac{0^{\ell+1}}{q^{i-1}}\right)$$

（根据强归纳法的归纳假设，因为 $2 -1 + \ell+1 < (i)()i)$。由于，这可化简为 $2 + \ell \qquad 0^{\ell+1} = 0$

$$\operatorname{SiPr}\left(M^{j \to v}\right) = 1 - \gamma_k. \tag{4}$$

另一方面，矩阵$M^{j\to 0}$ 的签名为$(i-1, j+1, \ell)$（因为它是将M 中的 X 型块Ai 替换为 0 型块得到的），且仍有k 个块，因此满足

$$\operatorname{SiPr}\left(M^{j \to 0}\right) = 1 - \gamma_k \left(1 - \frac{0^{\ell}}{q^{i-1}}\right) \tag{5}$$

（根据强归纳法的归纳假设，因为 $2(i-1) + \ell < 2i +$

~~因此，在进行这些代换之前，SiPr~~ M 也等于 $1 - \gamma_k \left(1 - \frac{0^{\ell}}{} q^{i}\right)$。换言之，(2) 对任意的 M都成立。这表明，确实可以不失一般性地假设“M 是严格的”。

ℓ)。现在，(3) 变为

$$\begin{aligned}
\operatorname{SiPr} M &= \frac{1}{q}\sum_{v\in\mathbb{F}_q}\operatorname{SiPr}\left(M^{j\to v}\right) = \frac{1}{q}\left(\operatorname{SiPr}\left(M^{j\to 0}\right) + \sum_{\substack{v\in\mathbb{F}_q;\\ v\neq 0}}\operatorname{SiPr}\left(M^{j\to v}\right)\right) \\
&= \frac{1}{q}\left(\left(1-\gamma_k\left(1-\frac{0^\ell}{q^{i-1}}\right)\right) + \sum_{\substack{v\in\mathbb{F}_q;\\ v\neq 0}}\left(1-\gamma_k\right)\right) \\
&\qquad \left(\text{by (5) and (4)}\right) \\
&= \frac{1}{q}\left(\left(1-\gamma_k\left(1-\frac{0^\ell}{q^{i-1}}\right)\right) + (q-1)\left(1-\gamma_k\right)\right) \\
&\qquad \left(\text{since the } \sum \text{ sum has precisely } q-1 \text{ addends}\right) \\
&= 1-\gamma_k\left(1-\frac{0^\ell}{q^i}\right) \qquad \left(\text{by a straightforward computation}\right).
\end{aligned}$$

因此，情形 1 中的（2）已得到证明。

接下来考虑情形 2。在此情形下，矩阵 M 没有 X 型块，但有多于 1 个 1 型块。因此，(i,j,ℓ) M 的签名满足 $\ell > 1$，所以 $0^\ell = 0$ 且 $0^{\ell-1} = 0$。

我们假设 M 有多于 1 个 1 型块。因此，M 至少有两个不同的 1 型块。设这两个块分别为 A_i 和 Aj，并按如下方式标记：块 A_i 的列数不少于块 Ai的列数。因此，由引理 3.15 可得，存在一个严格多斜矩阵 M'，具有以下性质：

- 矩阵 M' 是方阵，且与 M大小相同。
- 它满足 $\operatorname{SiPr} M = \operatorname{SiPr}(M')$。
- 矩阵 M' 与 M 的区别仅在于，块 A_j 被一个新块取代，而该新块为 0 型。

考虑这个矩阵 M'。根据它的第三个性质，该矩阵 M' 的签名为$(i, j+1,\ell-1)$，因此仍有 k 个块。因此，

$$\operatorname{SiPr}\left(M'\right) = 1-\gamma_k\left(1-\frac{0^{\ell-1}}{q^i}\right)$$

（根据强归纳法的归纳假设，因为 $2 + \ell - 1 < 2 + i()\,i)$。
鉴于 $\operatorname{SiPr} M \operatorname{SiPr}(M)$ 以及 ，可改写为 $= \quad ' \quad 0^{\ell-1} = 0 = 0^\ell$

$$\operatorname{SiPr} M = 1-\gamma_k\left(1-\frac{0^\ell}{q^i}\right).$$

因此，（2）已在情形 2 中得到证明。

接下来考虑情形 3。在这种情况下，矩阵 M 没有 X 型块，且恰有一个 1 型块。因此，M 的签名 (i, j,ℓ) 满足 $\mathrm{i} = 0$ and $\ell \neq 1$。于是，由 $\mathrm{k} = \underbrace{\mathrm{i}}_{=0} + \mathrm{j} + \underbrace{\ell}_{=1} = \mathrm{j} + 1$，可得 $\mathrm{j} = \mathrm{k} - 1$，从而 $\left(\underbrace{\mathrm{i}}_{=0}, \underbrace{\mathrm{j}}_{=\mathrm{k}-1}, \underbrace{\ell}_{=1}\right) = (0, \mathrm{k} - 1, 1)$。

因此，矩阵 M 的签名为 $(0, \mathrm{k} - 1, 1)$。所以，M 中除一个块外，其余块均为 0 型，而剩下的块为 1 型。我们将后者称为“奇异块”。令 M′ 为从 M 中删去最底行和奇异块的最右列后得到的矩阵。（注意，如果奇异块只有一列，这样做会使其整个消失。）于是，引理 3.17 (a) 表明，矩阵 M′ 仍是一个签名为 $(\mathrm{k} - 1, 0, 1)$ 或 $(\mathrm{k} - 1, 0, 0)$ 的多斜矩阵（分别对应奇异块有多于一列或没有多于一列的情况）。此外，引理 3.17 (b) 表明，$\operatorname{SiPr} \mathrm{M} = \operatorname{SiPr}(\mathrm{M}')$。

不失一般性，我们假设M 不是 1×1-矩阵（因为如果M 是 1×1-矩阵，那么很容易看出$k = 1$ 且$M = \begin{pmatrix} 1 \end{pmatrix}$，因此 $\operatorname{SiPr} M = 0 = 1 - \gamma_k \left(1 - \frac{0^\ell}{} q^i\right)$）。

因此，如果M 的奇异块至多有一列，那么必有$k > 1$（否则，奇异块将是M的唯一块，从而M 将是 1×1-矩阵），于是我们有

$$\gamma_{k-1}\left(1 - \frac{1}{q^{k-1}}\right) = \gamma_k \tag{6}$$

在这种情况下（根据 γ_{k-1} 和 γ_k的定义）。（注意，当$k = 1$时，等式（6）不成立；这就是我们必须单独处理 1×1-矩阵情形的原因。）

现在，我们已经证明M' 是一个签名为$(k - 1, 0, 1)$ 或$(k - 1, 0, 0)$ 的多斜矩阵（这取决于奇异块是否多于一列）。由于该矩阵M' 的大小小于M，我们可以

因此使用（第一次归纳中的）归纳假设，得到

$$\begin{aligned}
&\operatorname{SiPr}\left(M'\right) \\
&= \begin{cases} 1-\gamma_k\left(1-\dfrac{0^1}{q^{k-1}}\right), & \text{if the strange block had more than one column;} \\ 1-\gamma_{k-1}\left(1-\dfrac{0^0}{q^{k-1}}\right), & \text{otherwise} \end{cases} \\
&= \begin{cases} 1-\gamma_k, & \text{if the strange block had more than one column;} \\ 1-\gamma_{k-1}\left(1-\dfrac{1}{q^{k-1}}\right), & \text{otherwise} \end{cases} \\
&= 1-\gamma_k \qquad (\text{by (6)}).
\end{aligned}$$

因此，

$$\begin{aligned}
\operatorname{SiPr} M &= \operatorname{SiPr}\left(M'\right) = 1-\gamma_k \\
&= 1-\gamma_k\left(1-\frac{0^\ell}{q^i}\right) \qquad \left(\text{since } \ell = 1 \text{ and thus } 0^\ell = 0\right).
\end{aligned}$$

由此，情形 3 中的 (2) 得证。

最后考虑情形 4。在这种情形下，矩阵 M 没有 X 型块，也没有 1 型块。换言之，$i = 0$ 且 $\ell = 0$。M 的所有块都是 0 型（因为 M 没有 X 型块，也没有 1 型块）。因此，M 的底行为 $(0, 0, \ldots, 0)$。由此可得 $\det M = 0$，因此 $\operatorname{SiPr} M = 1$。将此与

$$1-\gamma_k\left(1-\frac{0^\ell}{q^i}\right) = 1-\gamma_k\underbrace{\left(1-\frac{0^0}{q^0}\right)}_{=0} \qquad (\text{since } \ell = 0 \text{ and } i = 0)$$

$$= 1,$$

比较可得 $\operatorname{SiPr} M = 1-\gamma_k\left(1-0^\ell q^i\right)$。由此，情形 4 中的 (2) 得证。

因此，我们已经证明了上述四种情形下的 (2)。至此归纳步骤完成，定理 3.12 得证。

□

3.3. 定理 3.2 (ii) 的证明

现在我们将定理 3.12 应用于 p-移位的 n-阶梯形分拆的 Jacobi–Trudi 矩阵。

引理 3.18. 设$p \leqslant n \leqslant k-1$。令 λ 为长度k的p-移位n-阶梯形分拆。那么，存在一个矩阵J'，它由对$J(\lambda)$的列进行置换得到，并且是签名为$(p,\ n-p,\ 1)$的多斜矩阵。（签名的定义见定义 3.9。）

证明。根据定义，$\lambda = (p+(k-1)n, p+(k-2)n, \ldots, p+n, p)$。因此，对于每个$i \in [k]$，$\lambda_i = p+(k-i)n$。

定义一个$k \times k$-矩阵$M = \left(M_{i,j}\right)_{i,j\in[k]}$，其定义如下

$$M_{i,j} = \lambda_i - i + j = p + kn - i(n+1) + j \qquad \text{for all } i,j \in [k].$$

因此，$J(\lambda) = \left(h_{M_{i,j}}\right)_{i,j\in[k]}$.

我们注意到，M 的同一列中的任意两个元素模 n +1同余。对于每个满足 q 6 n +1的指标，M 的第 q、q +(n +1)、q +2(n +1)、.....列恰好包含 M 中与 $M_{q,q} = \lambda_q$模 n +1同余的元素。因此，J(λ)中由相应列构成的子矩阵是一个斜矩阵[4]，而不同指标 q 6 n +1 对应的斜矩阵彼此不相交。这些斜矩阵的底部元素是 J(λ) 最后一行的最后 n +1 个元素；它们是 $h_p, h_{p-1}, \ldots, h_1, 1, 0, 0, \ldots, 0$。

对$J(\lambda)$ 的列进行置换，使得这些斜矩阵中的每一个都呈现为一个连续的块，由此我们得到一个签名为$(p, n-p, 1)$的多斜矩阵。

□

定理 *3.2 (ii)*的证明。引理 3.18 表明，对列进行置换后，$J(\lambda)$ 是一个签名为$(p, n-p, 1)$ 的多斜矩阵（因此具有$n+1$ 个块）。于是，定理 3.12 给出

$$\mathrm{SiPr}\left(J(\lambda)\right) = 1 - \gamma_{n+1}\underbrace{\left(1 - \frac{0^1}{q^p}\right)}_{=1} = 1 - \gamma_{n+1} = 1 - \prod_{i=1}^{n}\left(1 - \frac{1}{q^i}\right)$$

（根据 γ_{n+1} 的定义）。由于$P(s_\lambda \mapsto 0) = \mathrm{SiPr}\left(J(\lambda)\right)$，这正是定理 3.2 **(ii)**的断言。

□

定理 3.2 **(i)** 也可以用类似的方法证明（不过，如上所述，由于矩阵[5]中的所有不定元彼此不同，也可以通过初等的张成与线性无关性推理得出）。

[4]假设$n \leqslant k-1$ 确保该子矩阵非空。假设$p \leqslant n$确保其所有地下室项均为 0。M 的定义以及$J(\lambda) = \left(h_{M_{i,j}}\right)_{i,j\in[k]}$ 这一事实确保每条副对角线上的元素均为常数。斜矩阵定义中的其余要求很容易验证。[5]参见 [5, 定理 1]，其中给出了一个密切相关且证明非常相似的结果。事实上，如果不是$J(\lambda/\mu)$ 中的某个项为$h_0 = 1$，定理 3.2 **(i)** 将是 [5, 定理 1]的一个特例。

证明定理 3.2 后，我们可以看到，对于$n = 1$，有$P(s_\lambda \mapsto 0) = 1\,q$；对于$n = 2$，有$P(s_\lambda \mapsto 0) = q^2 + q - 1\,q^3$，从而重新得到定理 6.5，并证明了 Anzis 等人提出的猜想 10.1 [1]。

4. 共轭斜分拆

接下来，我们将证明一个一般性结果，将 [1, 推论 3.3] 从分拆推广到斜分拆。回顾一下，λ^t 表示分拆λ的共轭分拆。

定理 4.1。设 λ/μ 是一个斜分拆。设 $a \in \mathbb{F}_q$。则，

$$P\left(s_{\lambda/\mu} \mapsto a\right) = P\left(s_{\lambda^t/\mu^t} \mapsto a\right).$$

下面的观察将有助于证明。

命题 4.2. 设$f \in \Lambda_{\leq N} := \mathbb{Z}[h_1, h_2, \ldots, h_N]$和$a \in \mathbb{F}_q$。则

$$P(f \mapsto a) = \frac{\left(\#\text{ of ring homomorphisms } \Lambda_{\leq N} \to \mathbb{F}_q \text{ that send } f \text{ to } a\right)}{q^N}. \quad (7)$$

证明。由多项式环的泛性质可知，对于每个N元组$(z_1, z_2, \ldots, z_N) \in \mathbb{F}_q^N$，存在唯一的环同态$\varphi: \Lambda_{\leqslant N} \to \mathbb{F}_q$使得$h_1 \mapsto z_1, h_2 \mapsto z_2, \ldots, h_N \mapsto z_N$。因此，$\mathbb{F}_q^N$中的$N$元组与环同态$\Lambda_{\leq N} \to \mathbb{F}_q$一一对应。因此，(7)式右侧与$P(f \mapsto a)$的定义一致。 □

定理 *4.1* 的证明。按照§ 2中的方式，将 $\mathcal{P}$ 与 Λ 视为相同。对于每个正整数n，令$e_n = s_{(1^n)} \in \Lambda = \mathcal{P}$为第$n$个初等对称函数。

根据对称函数理论（[9, §7.6] 或 [8, (2.7)]），已知存在一个对合环自同构[6] $\omega: \Lambda \to \Lambda$（称为欧米伽对合或基本对合），其定义为

$$\omega(h_n) = e_n \qquad \text{for all } n \geqslant 1.$$

现在，初等对称函数 e_n 可以写成关于 $h_1, h_2, \ldots\ldots$、h_n的多项式，这例如可由 Jacobi–Trudi 恒等式推出：

[6]如果一个映射是自身的逆映射，则称其为对合的。

$e_n = s_{(1^n)} = \det\left(h_{1+i-j}\right)_{1\leqslant i\leqslant n}$, $1\leqslant j\leqslant n$。将 ω 应用于此，我们看到 h_n 同样可以写成关于 $e_1, e_2, \ldots\ldots$、e_n的多项式。因此

$$\begin{aligned}\Lambda_{\leq N} &= (\text{subring of } \Lambda \text{ generated by } h_1, \ldots, h_N)\\ &= (\text{subring of } \Lambda \text{ generated by } e_1, \ldots, e_N),\end{aligned}$$

且 ω 限制为自反环自同态 $\omega_N\colon\ \Lambda_{\leq N} \to \Lambda_{\leq N}$。

现在，给定一个斜舒尔函数 $s^{\lambda/\mu}$，选取 N 使得 $s_{\lambda/\mu} \in \Lambda_{\leq N}$。于是，$\omega_N\left(s_{\lambda/\mu}\right) = \omega\left(s_{\lambda/\mu}\right) = s_{\lambda^t/\mu^t}$（参见，例如，[9, 定理 7.15。6] 或 [8, (5.6)]）。因此，存在一个映射

$$\begin{aligned}&\left(\text{ring homomorphisms } \Lambda_{\leq N} \to \mathbb{F}_q \text{ that send } s_{\lambda^t/\mu^t} \text{ to } a\right)\\ &\to \left(\text{ring homomorphisms } \Lambda_{\leq N} \to \mathbb{F}_q \text{ that send } s_{\lambda/\mu} \text{ to } a\right)\end{aligned}$$

将每个 φ 映射到 $\varphi\circ\omega_N$。此外，由于 ω_N 是一个自同构，该映射还是一个双射。因此，将 $s^{\lambda/\mu}$ 映射到 a 的环同态 $\Lambda_{\leq N} \to \mathbb{F}_q$ 的数量，在我们将 λ/μ 替换为 λ^t/μ^t时不会改变。根据命题 4.2，这意味着 $P\left(s^{\lambda/\mu} \mapsto a\right) = P\left(s_{\lambda^t/\mu^t} \mapsto a\right)$。 □

5. 块阶梯

利用定理 4.1，我们可以将关于p-移位n-阶梯形分拆的结果推广到其共轭分拆。这些共轭分拆可以独立描述。我们将使用分拆的指数记法，即将 $\lambda = ((c_1)^{a_1}, (c_2)^{a_2}, \ldots, (c_k)^{a_k})$简写为 $\lambda = (\underbrace{c_1, \ldots, c_1}_{a_1\text{次}}, \underbrace{c_2, \ldots, c_2}_{a_2\text{次}}, \ldots, \underbrace{c_k, \ldots, c_k}_{a_k\text{次}})$.

定义 5.1. 设 $p > 0$、$n > 0$ 和 $k \geqslant 0$ 为整数。我们将相应的块阶梯 定义为分拆

$$\lambda = (k^p, (k-1)^n, (k-2)^n, \ldots, 2^n, 1^n)$$

(长度为 $\ell(\lambda) = p + (k-1)n$)。

容易看出，块阶梯是p-移位n-阶梯分拆的共轭分拆。因此，我们可以将定理 4.1 应用于定理 3.2 和猜想 3.3，从而得到以下推论和猜想：

推论 5.2. 设 λ 为一个块阶梯。

(i) 设$k < n+1$（其中p 任意）。那么，

$$P(s_\lambda \mapsto 0) = 1 - \begin{cases}\prod_{i=1}^{k-1}\left(1-\frac{1}{q^i}\right), & \text{if } p \leqslant k-1;\\ \prod_{i=1}^{k}\left(1-\frac{1}{q^i}\right), & \text{if } p > k-1.\end{cases}$$

(ii) 设$p \leqslant n$ 且$k \geqslant n+1$。那么，

$$P(s_\lambda \mapsto 0) = 1 - \prod_{i=1}^{n} \left(1 - \frac{1}{q^i}\right).$$

猜想 5.3。设 λ 是一个块阶梯，其中含有 $k \geqslant n+1$，且满足 $p > n$。那么，

$$P(s_\lambda \mapsto 0) = 1 - \prod_{i=1}^{n+1} \left(1 - \frac{1}{q^i}\right).$$

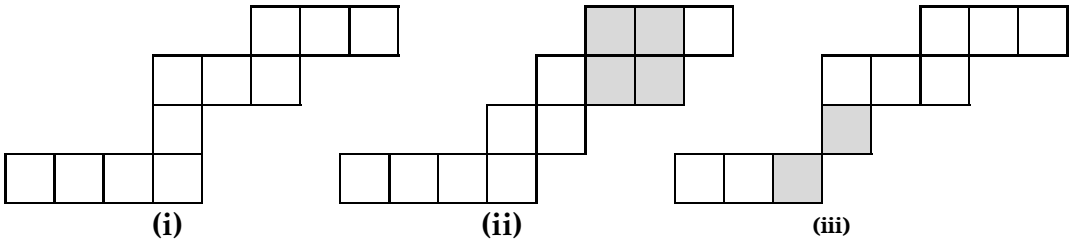
6. 带状图形等分布

在本节中，我们将注意力转向一类特殊的斜分拆，称为带状分拆。我们从其定义开始（例如参见 [9, §7.17]）：

定义 6.1。若斜分拆 λ/μ 的杨图内部（将其视为其方格的并集）是连通的，则称其为连通的。

带状分拆是一种连通的斜分拆 λ/μ，其杨图不包含任何由 2×2 个方格组成的块。

例 6.2。下面的三个斜分拆中，只有第一个是带状分拆，因为**(ii)** 包含一个由 2×2 个方格组成的块（阴影部分），而**(iii)** 是不连通的。



让我们重新考察 Jacobi–Trudi 矩阵。对于例 6.2 (i) 中的带状分拆 $\lambda/\mu = (8, 6, 4, 4)/(5, 3, 3)$，我们可以写出$J(\lambda/\mu)$ 如下：

$$J(\lambda/\mu) = \begin{pmatrix} h_3 & h_6 & h_7 & h_{11} \\ 1 & h_3 & h_4 & h_8 \\ 0 & 1 & h_1 & h_5 \\ 0 & 0 & 1 & h_4 \end{pmatrix}.$$

引理 6.3。设 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ 和 $\mu = (\mu_1, \mu_2, \ldots, \mu_\ell) \subseteq \lambda$ 是两个分拆，且 λ/μ 是一个带状分拆。假设 $\lambda_1 > \mu_1$ 和 $\lambda_\ell > \mu_\ell = 0$。

带状分拆 λ/μ 的 Jacobi–Trudi 矩阵 $J(\lambda/\mu)$ 具有以下性质（其中记号 $(J(\lambda/\mu))_{i,j}$ 表示该矩阵的第(i,j)个元素）：

(i) We have $J(\lambda/\mu)_{j+1,j} = 1$ for each $j \in [\ell - 1]$.

(ii) 当 i、$j \in [\ell]$ 满足 $i > j + 1$ 时，我们有 $J(\lambda/\mu)_{i,j} = 0$。

(iii) 设 $N = \lambda_\ell - \mu_l - 1 + \ell$。$J(\lambda/\mu)$ 的右上角元素为 h_N，而 $J(\lambda/\mu)$ 的其余元素都属于 $\mathbb{Z}[h_1, h_2, h_3, ..., h_{N-1}]$。

注 6.4。引理 6.3 实质上断言，矩阵 $J(\lambda/\mu)$ 具有以下结构（此处展示 $\ell = 5$）：

$$J(\lambda/\mu) = \left(h_{\lambda_i - \mu_j - i + j}\right)_{i,j \in [\ell]} = \begin{pmatrix} * & * & * & * & h_N \\ 1 & * & * & * & * \\ 0 & 1 & * & * & * \\ 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 1 & * \end{pmatrix},$$

其中每个星号都是 $\mathbb{Z}[h_1, h_2, h_3, ..., h_{N-1}]$ 中的一个元素。

引理 *6.3* 的证明。由 $\lambda_\ell > \mu_\ell = 0$，可得 $\ell = \ell(\lambda)$。

(i) 固定 j $\in [\ell - 1]$。斜图 Y(λ/μ) 中的方格，若位于第 1、2、...、j 行之一，则称为高方格；若位于第 j $+1$、j $+2$、...、ℓ 行之一，则称为低方格。注意，图形 λ/μ 同时包含高方格和低方格（因为 $\lambda_1 > \mu_1$ 和 $\lambda_\ell > \mu_\ell = 0$）。由于它是连通的，因此必定包含一个彼此相邻的高方格和低方格。这两个方格因此具有 (j, p) 和 (j $+1$, p) 的形式，其中某个 p > 0。于是这个 p 满足 $\mu_j <$ p （因为 (j, p) $\in$ Y(λ/μ)），且 p $\leqslant \lambda_{j+1}$ （因为 (j $+1$, p) $\in$ Y(λ/μ)）。因此，$\mu_j <$ p $\leqslant \lambda_{j+1}$。

另一方面，如果我们有 $\lambda_{j+1} > \mu_j + 1$，那么图形 $Y(\lambda/\mu)$ 将包含一个由方格组成的 2×2 块，即这四个方格 $(j, \mu_j + 1)$、$(j, \mu_j + 2)$、$(j + 1, \mu_j + 1)$ 和 $(j + 1, \mu_j + 2)$（因为 $\lambda_j \geqslant \lambda_{j+1} \geqslant \mu_j + 2 \geqslant \mu_j + 1 > \mu_j \geqslant \mu_{j+1}$）。但这与 λ/μ 是带状分拆这一事实矛盾，因此它不含这样的块。

因此，我们不可能有 $\lambda_{j+1} > \mu_j + 1$。所以，$\lambda_{j+1} \leqslant \mu_j + 1$。结合 $\mu_j < \lambda_{j+1}$，可得 $\lambda_{j+1} = \mu_j + 1$，正如所需。

(ii) 命题 **(ii)** 等价于证明：当$i > j + 1$时，$\lambda_i - \mu_j - i + j < 0$。这由 **(i)** 得出，因为 Jacobi–Trudi 矩阵 $J(\lambda/\mu)$ 中的指标 $\lambda_i - \mu_j - i + j$ 在每一行中都从左到右严格递增。

(iii) 命题 **(iii)** 同理可得，因为这些指标沿行严格递增，沿列严格递减（从而使右上角入口的指标唯一最大）。

try 的指标唯一地是最大的一个）。 □

定理 6.5。 设 λ/μ 是一个带状分拆，并回顾一下，$s^{\lambda/\mu}$ 是相应的 Schur 函数。设$a \in \mathbb{F}_q$。那么，

$$P(s_{\lambda/\mu} \mapsto a) = 1/q.$$

证明。 根据注记 2.10，斜舒尔函数 $s^{\lambda/\mu}$ 在平移 λ/μ 的图形时保持不变。因此，我们不妨假设 λ/μ 的图形已尽可能向西北方向平移——也就是说，我们有 $\lambda_1 > \mu_1$ 和 $\lambda_\ell > \mu_\ell = 0$，其中 ℓ 是 λ的长度。

从矩阵 $J(\lambda/\mu)$ 中删去第一行和最后一列后得到的子矩阵。根据引理 6.3 **(i)** 和**(ii)**，该子矩阵是对角线元素为 1,1, . . . , 1 的上三角矩阵，因此其行列式为 1。因此，沿第一行对$J(\lambda/\mu)$ 的行列式进行余子式展开，形式如下

$$s_{\lambda/\mu} = \det(J(\lambda/\mu)) = (-1)^{\ell+1} h_N + g(h_1, h_2, \ldots, h_{N-1})$$

对于某个多项式 $g(h_1, h_2, \ldots, h_{N-1}) \in \mathbb{Z}[h_1, h_2, h_3, \ldots, h_{N-1}]$，根据引理 6.3**(iii)**。

因此，一个 N 元组 $(z_1, z_2, \ldots, z_N) \in \mathbb{F}_q^N$满足 $s^{\lambda/\mu}(z_1, z_2, \ldots, z_N) = a$，当且仅当 $(-1)^{\ell+1} z_N + g(z_1, z_2, \ldots, z_{N-1}) = a$。显然，若 $z_1, z_2, \ldots, z_{N-1}$ 已给定，后一等式关于 z_N 有唯一解。

因此，对于任意 $(z_1, z_2, \ldots, z_{N-1}) \in \mathbb{F}_q^{N-1}$，恰有一个 $z_N \in \mathbb{F}_q$的值满足 $s^{\lambda/\mu}(z_1, z_2, \ldots, z_N) = a$。换言之，我们有

$$\left(\#\text{ of } (z_1, z_2, \ldots, z_N) \in \mathbb{F}_q^N \mid (-1)^{n+1} z_N + g(z_1, z_2, \ldots, z_{N-1}) = a\right) = q^{N-1}.$$

由定义 2.1 可得

$$P\left(s_{\lambda/\mu} \mapsto a\right) = \frac{\left(\#\text{ of } (z_1, z_2, \ldots, z_N) \in \mathbb{F}_q^N \text{ such that } s_{\lambda/\mu}(z_1, z_2, \ldots, z_N) = a\right)}{\left(\#\text{ of all } (z_1, z_2, \ldots, z_N) \in \mathbb{F}_q^N\right)}$$

$$= \frac{q^{N-1}}{q^N} = \frac{1}{q}.$$

□

参考文献

[1] Ben Anzis、Shuli Chen、Yibo Gao、Jesse Kim、Zhaoqi Li 和 Rebecca Patrias。《有限域上的 Jacobi-Trudi 行列式》。载于：《组合年刊》22.1（2018），第 447–489 页。

[2] Prakash Belkale 和 Patrick Brosnan。《拟阵、动机与 Kontsevich 的一个猜想》。载于：《杜克数学杂志》116.1（2003 年 1 月）。doi: 10.1215/s0012-7094-03-11615-4。url:https://doi.org/10.1215/s0012-70 94-03-11615-4.

[3] Omesh Dhar Dwivedi 和 Darij Grinberg。《有限域上 Hankel 矩阵的秩》。载于：线性代数及其应用641（2022 年 5 月），第 156–181 页。[4] Noam D. Elkies。《满足线性递推的有限序列》。载于：《纽约数学杂志》8（2002 年）。[5] James Haglund。《q-车多项式与有限域上的矩阵》。载于：《应用数学进展》20.4（1998 年 5 月），第 450–487 页。doi：10.1006/aama.1998.0582。url：https://doi.org/10.1006/aama.1998.0582。[6] Warren P. Johnson。《q-分析导论》。美国数学学会，2020 年。[7] Maxim Kontsevich。《*Gelfand* 研讨会演讲，罗格斯大学》1997 年。[8] Ian G. Macdonald。《对称函数与 *Hall* 多项式》。第 2 版。牛津科学出版社，1998 年。[9] Richard P. Stanley。《计数组合学：第 *2* 卷》。剑桥大学出版社，2001 年。[10] Richard P. Stanley。《生成树与 Kontsevich 猜想》。载于：《组合学年刊》2.4（1998 年 12 月），第 351–363 页。doi：10.1007/bf01608530。arXiv：math/9806055 [math.CO]。url：https://doi.org/10.1007/bf01608530

[11] John R. Stembridge.《与 Kontsevich 猜想相关的有限域上的簇的点计数》。载于：《组合学年刊》2（1998），第 365–385 页。doi：10.1007/BF01608531。[12] Andre Weil.《有限域中方程的解的数量》。载于：《美国数学学会通报》55（5，1949），第 497–508 页。doi：10.1090/S0002-9904-1949-09219-4。