arXiv:2305.01085v1 [math.CO] 1 May 2023

随机基中的串行交换

Sean McGuinness 汤
普森河大学数学系 麦吉尔
路，坎卢普斯BC V2C5N3
加拿大 邮箱:
smcguinness@tru.ca

摘要

Kotlar 和 Ziv 猜想 [11] ，对于拟阵 M 中的任意两个基B_1 和 B_2 以及任意子集 $X \subset B_1$，都存在一个子集Y以及 X和 Y的排列 $x_1 \prec x_2 \prec \cdots \prec x_k$和 $y_1 \prec y_2 \prec \cdots \prec y_k$，使得对于 $i = 1, \ldots, k$，$B_1 - \{x_1, \ldots, x_i\} + \{y_1, \ldots, y_k\}$ 和 $B_2 - \{y_1, \ldots, y_i\} + \{x_1, \ldots, x_k\}$ 都是基；也就是说，X与 Y串行可交换。设 M 是一个可由 $\mathbb{F}_q$. 表示的秩为n 的拟阵。我们证明，对于 $q > 2$，若从 M的所有基中随机选取基 B_1 和 B_2 ，并在 B_1中随机选取一个大小为$k \leq \ln(n)$的子集 X ，则当 $n \to \infty$时，以趋近于 1 的概率，存在一个子集 $Y \subset B_2$ ，使得 X 与 Y.串行可交换

AMS 学科分类（2012年）：05D99,05B35。

1 引言

令 $\mathscr{B}(M)$ 表示拟阵 M. 中基的集合。为方便起见，如果从基 B 中删去 $X \subset B$ ，并加入 Y 中的元素来构造一个新基，则将所得的基记为 $B - X + Y$。当 $X = \{x_1, \ldots, x_k\}$ 且 $Y = \{y_1, \ldots, y_k\}$时，我们通常将新基写作 $B - x_1 - \cdots - x_k + y_1 + \cdots + y_k$.。例如，若 $X = \{e\}$ 且 $Y = \{f\}$，则新基就是 $B - e + f$。

对于所有正整数 k，令 $[k]$ 表示集合 $\{1, \ldots, k\}$.。对于满足 $a \leq b$ 的正整数 a、b，令 $[b \backslash a]$ 表示集合 $[b] - [a]$。

设 $B_i \in \mathscr{B}(M)$ $i = 1$，2。对于元素 $x \in B_1$和 $y \in B_2$，若$B_1' = B_1 - x + y$ 和 $B_2' = B_2 - y + x$ 是基，则称x 和 y 关于 B_i, $i = 1$，2 可对称交换。

我们有如下众所周知的对称交换性质：对于任意元素 $x \in B_1$，存在 $y \in B_2$，使得 x 和 y 可对称交换。对于基 $B_i,\ i = 1,\ 2$ 以及子集 $X_i \subseteq B_i,\ i = 1,\ 2$，若 $B_2 - X_2 + X_1$ 是基，我们记作$B_1, X_1 \to B_2, X_2$（若 $B_1 - X_1 + X_2$ 是基，则记作 $B_1, X_1 \leftarrow B_2, X_2$）。若$B_1, X_1 \to B_2, X_2$和 $B_1, X_1 \leftarrow B_2, X_2$同时成立，我们记作 $B_1, X_1 \leftrightarrow B_2, X_2$。Greene [7]和 Woodall [15] 证明，对称交换性质可以推广到集合：

1.1 定理（Greene、Woodall）
对于每个非空子集 $X_1 \subseteq B_1$，都存在一个子集 $X_2 \subseteq B_2$，使得 $B_1, X_1 \leftrightarrow B_2, X_2$。

对于 $i = 1,\ 2$，设 B_i 是拟阵 M 中的一个基，且 X_i 是 B_i. 的一个子集。若对 X_1 的某个排列 $x_{11} \prec x_{12} \prec \cdots \prec x_{1k}$ 和 X_2 的某个排列 $x_{21} \prec x_{22} \prec \cdots \prec x_{2k}$，$B_1 - \{x_{11}, \ldots, x_{1i}\} + \{x_{21}, \ldots, x_{2i}\}$ 和 $B_2 - \{x_{21}, \ldots, x_{2i}\} + \{x_{11}, \ldots, x_{1i}\}$ 是 $i = 1, \ldots, n$ 的基，则记作 $B_1, X_1 \leftrightarrows B_2, X_2$（若 M 可由上下文确定，则省略）。此时，我们称 $_MX_1$ 相对于 $B_i,\ i = 1$ 与 X_2 串行可交换，2。我们将 $X_i,\ i = 1, 2$ 的这类排列称为串行排列。对于拟阵 M 和正整数 k，若对于任意两个基 $B_1, B_2 \in \mathscr{B}$（M）以及任意满足 $|X_1| = k$ 的子集 $X_1 \subseteq B_1$，都存在满足 B_1 的子集 $X_2 \subseteq B_2$，使得 $X_1 \leftrightarrows B_2, X_2$，则称 M 具有 k-串行交换性质。

根据对称交换性质，所有拟阵都具有 1-串行交换性质。在 [11], Kotlar 和 Ziv 提出了以下有趣的猜想：

1.2 猜想（Kotlar，Ziv [11]）
对于所有拟阵 M 以及所有整数 $k \leq r$（M），M 具有 k-串行交换性质。

在 [11], 中证明了所有拟阵都具有 2-串行交换性质。此外，在 [10], 中证明了，对于秩至少为三的拟阵，对于任意两个基 B_1、B_2，存在 3-元子集 $A_i \subseteq B_i$、$i = 1$，使得 2 A_1 与 A_2. 串行可交换。在 [12], 中证明了，对于在 $\mathbb{F}_q$上可表示的拟阵集合 $\mathscr{M}_q$，只需对秩至多为 $(k + 2)q^{2k}$. 的拟阵 $M \in \mathscr{M}_q$ 证明猜想 1.2。此外，还证明了所有二元拟阵都具有 3-串行交换性质。猜想 1.2 蕴含 Gabow [6] 和 Cordovil、Moreira [3]的以下著名猜想：

1.3 猜想（Gabow、Cordovil 和 Moreira）
设 B_i 是拟阵 M 的不相交基，其秩为 $n.$。那么，存在 B_1 和 B_2 的元素排列 $b_1 \prec b_2 \prec \cdots \prec b_n$ 和 $b_{n+1} \prec b_{n+2} \prec \cdots \prec b_{2n}$，使得在循环排列 $b_1 \prec b_2 \prec \cdots \prec b_n \prec b_{n+1} \prec \cdots \prec b_{2n}$ 中任意 n 个连续元素都构成 $M.$ 中的一个基。

换言之，上述猜想断言，对于不相交的基 B_1 和B_2，基 B_1 与 $B_2.$ 串行可交换。已知该猜想对于横截拟阵（见 $[4, 6]$）和强基序可拟阵成立。在 $[5, 14],$ 中，该猜想已对图拟阵得到证明。在 $[2],$ 中，该猜想已在稀疏铺路拟阵中得到验证。

即使在 $k = 3$ 的情形下，猜想 1.2 仍未解决，而且目前看来也很难取得重大进展。不过，随机选取基时会引出一些有趣的问题。在一篇近期论文中，Sauermann $[13]$ 证明，Rota 基猜想（见 $[9]$）对于有限域上可表示的拟阵中几乎所有选取的基都成立。也就是说，如果从一个在有限域上可表示的秩为-n 的拟阵中随机选取 n 个基，那么以 $1 - o$ 的概率可以找到 n 个独立横截（1），其中 $n \to \infty.$。鉴于上述猜想，这一结果引出了以下自然问题：

1.4 问题
假设从一个拟阵中随机选取两个基 B_1 和 B_2，然后随机选取一个 k-子集 $X \subseteq B_1.$。存在一个 k-子集 $Y \subseteq B_2$，使得 X 与 Y串行可交换的概率是多少?

本文针对有限域上可表示的拟阵研究这一问题，但二元拟阵除外。下一个定理是本文的主要结果。

1.5 定理
设 B_1 和 B_2 是从 $\mathbb{F}_q^n$ 中随机选取的基，且 X 是从 B_1 中随机选取的 k-子集，其中 $k \leq \ln(n)$。若 $q > 2$，则存在一个 k-子集 $Y \subseteq B_2$，使得 X 与 Y串行可交换的概率趋于 1，当 $n \to \infty.$

2 记号

对于一个 $m \times n$ 矩阵 $A = [a_{ij}]$ 和子集 $S \subseteq [m]$、$T \subseteq [n]$，我们用$A_{S,T}$ 表示由元素 a_{ij} 诱导的 A 的子矩阵，其中 $i \in S$ 且 $j \in T.$

在我们所使用的模型中，每个基被选中的概率都相等。我们不只是选择基本身，而是随机选择有序基。由于每个基具有相同数量的排列，只需对有序基证明定理 1.5 即可。每个有序基 $B$of M都对应于一个 n-元组 $(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{F}_q^n$，使得 $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$的秩为 n.

令 B_1和 B_2为随机选取的（有序）基。令 $\mathbf{U}_1, \ldots, \mathbf{U}_n$为取值于 $\mathbb{F}_q^n$的随机变量，使得随机变量的 n元组 $(\mathbf{U}_1, \ldots, \mathbf{U}_n)$ 对应于 B_1。对于 $i = 1, \ldots, n$，令 $\mathbf{U}_i = (u_{1i}, u_{2i}, \ldots, u_{ni})$，其中$u_{ji}$也都是取值于 $\mathbb{F}_q$. 的随机变量。同理，令 $\mathbf{V}_i$，$i = 1, \ldots, n$ 为取值于 $\mathbb{F}_q^n$的随机变量，其中 n元组 $(\mathbf{V}_1, \ldots, \mathbf{V}_n)$ 对应于 B_2.。对于 $i = 1, \ldots, n$，令 $\mathbf{V}_i = (v_{1i}, v_{2i}, \ldots, v_{ni})$。

令 k 为一个正整数，我们假设 $k \leq \ln(n)$，并令 $\ell = \lfloor \frac{n}{k} \rfloor$.。对于 $i = 1, \ldots, \ell$，令 $\mathscr{V}_i = \{\mathbf{V}_{(i-1)k+1}, \ldots, \mathbf{V}_{ik}\}$；也就是说，$\mathscr{V}_i$对应于 B_2中位于位置 $(i-1)k+1, \ldots, ik$.的元素所构成的 k元子集。

选定 B_1 和 B_2后，我们将从 B_1中随机选取一组由 k 个元素组成的集合。根据对称性，不妨假设这些元素是（有序）基 B_1. 中最前面的 k 个元素。令 $\mathscr{U}_1 = \{\mathbf{U}_1, \ldots, \mathbf{U}_k\}$，它们对应于从 B_1. 中选出的随机 k 元素集合。要证明定理 1.5，只需证明当 $n \to \infty$. 时，对于某些 i,B_1, $\mathscr{U}_1 \leftrightarrows B_2, \mathscr{V}_i$ 的概率趋于 1。为此，我们定义随机变量 $_M$ $X_1, \ldots, X_\ell$ 和 $Y_1, \ldots, Y_\ell$，它们依赖于随机选出的 B_1 和 B_2，定义如下：对于 $j = 1, \ldots, \ell$,

$$X_j = \begin{cases} 1 & \text{if } B_1, \mathscr{U}_1 \to B_2, \mathscr{V}_j \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad Y_j = \begin{cases} 1 & \text{if } B_1, \mathscr{U}_1 \leftarrow B_2, \mathscr{V}_j \\ 0 & \text{otherwise} \end{cases}$$

需要注意的是，随机变量 $X_1, \ldots, X_n$ 不一定相互独立，$Y_1, \ldots, Y_n$. 也同样如此。

3 概率的下界

本节中，我们计算概率$\mathbb{P}(X_i = 1 \big| X_1, \ldots X_{i-1})$和 $\mathbb{P}(Y_i = 1 \big| Y_1, \ldots, Y_{i-1})$的下界。以下引理是一个众所周知的事实，为完整起见，我们给出其证明。

3.1 引理

在 $\mathbb{F}_q$ 上随机选取的 $k \times k$矩阵为非奇异矩阵的概率

is

$$\alpha_k = \prod_{i=1}^{k}(1 - \frac{1}{q^i}).$$

证明。我们首先计算在 $\mathbb{F}_q$. 上共有多少个 $k \times k$ 非奇异矩阵 A。为此，我们一次填写 A 的一行。填写第 1 行有 $q^k - 1$ 种方法。填写第二行时，有 q^k 种可能的选择，但不能选择第一行的倍数。因此，填写第二行有 $q^k - q$ 种方法。现在假设我们已经填写了第 1，...，i. 行。同样地，第 $i+1$ 行有 q^k 种选择，但不能选择第 1，...，i. 行的线性组合。因此，第 $i+1$ 行有 $q^k - q^i$ 种选择。继续进行下去，我们看到总共有 $\prod_{i=1}^{k}($ $q^k - q^{i-1}$) 个非奇异矩阵。由于 A 上总共有 q^{k^2} 个可能的矩阵， A 为奇异矩阵的概率是

$$\frac{\prod_{i=1}^{k}(q^k - q^{i-1})}{q^{k^2}} = \frac{q^{\frac{k^2-k}{2}}\prod_{i=1}^{k}(q^i - 1)}{q^{k^2}} = \prod_{i=1}^{k}\left(\frac{q^i - 1}{q^i}\right) = \prod_{i=1}^{k}(1 - \frac{1}{q^i}).$$

□

根据欧拉定理（见 [8, 定理 353]），我们有 $\prod_{i=1}^{\infty}(1 - x^n) =$ $1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} \cdots$。特别地，该定理意味着对于 $q > 1$, $\alpha = \prod_{i=1}^{\infty}(1 - \frac{1}{q^i}) > 1 - \frac{1}{q} - \frac{1}{q^2}$.

若一个 $k \times k$ 矩阵 A 满足：对于 $i = 1$、.....、 k，子矩阵 $A_{[i],[i]}$ 是满秩的，则称该矩阵具有顺序满秩。

3.2 观察

存在有 $(q-1)$ 上有 (q^{k^2-k}) 个 A 矩阵满足 A 具有顺序满秩。此外，随机选取的 $k \times k$ 矩阵具有顺序满秩的概率等于 $(1 - \frac{1}{q})^k$.

证明。设 $A = (a_{ij})$ 是 $\mathbb{F}_q$ 上任意一个 $k \times k$ 矩阵。我们将按 $i = 1, 2, \ldots, k$ 的顺序填入 $A_{[i],[i]}$ 的矩阵元素，从而得到一个顺序满秩矩阵。矩阵 $A_{[1],[1]}$ 只有一个矩阵元素，该元素可以是 $\mathbb{F}_q$. 中任意一个非零元素。因此有 $q - 1$ 种可能的取值。接下来，我们逐个填入 $A_{[2],[2]}$ 中剩余的 3 个矩阵元素。矩阵元素 a_{12} 和 a_{21} 可以是 $\mathbb{F}_q$ 中的任意元素，但为了确保 $det(A_{[2],[2]}) \neq 0$，剩余矩阵元素 a_{22}. 只有 $q - 1$ 种可能的取值。因此，矩阵 $A_{[2],[2]}$. 有 $(q-1)^2q^2$ 种可能的取值。继续归纳，假设

有 $(q-1)^j q^{j^2-j}$ 个矩阵 $A_{[j],[j]}$ 的可能取值，使其具有顺序满秩。现在，我们逐个填入 $A_{[j+1],[j+1]}$ 中剩余的 $2(j+1)$ 个矩阵元素。除 $a_{(j+1)(j+1)}$ 外的 $2j$ 个矩阵元素可以是 $\mathbb{F}_q$ 中的任意元素。为了确保 $det(A_{[j+1],j[+1]}) \neq 0$, 最后一个矩阵元素 $a_{(j+1)(j+1)}$· 只有 $q-1$ 种可能的取值。注意，这里我们使用了假设 $det(A_{[j],[j]}) \neq 0.$。因此有

$(q-1)^j q^{j^2-j} \cdot (q-1)q^{2j} = (q-1)^{j+1} q^{(j+1)^2-(j+1)}$ 个选法，对应于 $A_{[j+1],[j+1]}$·由归纳法可知，具有顺序满秩的矩阵 A 共有 $(q-1)^k q^{k^2-k}$ $k \times k$ 个。鉴于可能的矩阵 $k \times k$ 共有 q^{k^2} 个，随机选取的矩阵 $k \times k$ 具有顺序满秩的概率等于 $\frac{(q-1)^k q^{k^2-k}}{q^{k^2}} = (1-\frac{1}{q})^k.$

□

令 $\beta_k = (1-\frac{1}{q})^k.$ 令 $\overline{U} = (u_{ij})$ 为随机矩阵，其第 i 列对应于矩阵 U_i; 令 $\overline{V} = (v_{ij})$ 为随机矩阵，其第 i 列对应于矩阵 V_i.。这样的满秩矩阵 $\overline{U}$ 和 $\overline{V}$，分别与有序基 B_1 和 B_2. 一一对应

对于 $i = 0,\ldots,\ell$，令 $n_i = ik$，并令 $J_i = [n_i \backslash n_{i-1}] = \{n_{i-1}+1, \ldots, n_i\}.$

3.3 引理
对于 $i = 1、\ldots、\ell、\ \mathbb{P}\ (X_i = 1 \big|\ X_1、\ldots、X_{i-1})\ \geq \alpha_k.$

证明。只需在给定 B_2 时证明引理。由于存在一个将任意基映射到另一基的同构，我们可以假设 B_2 是$\mathbb{F}_q^n$的标准基；也就是说，我们可以假设对于 $i = 1,$ ....., $n,$ 矩阵 $\mathsf{V}_i = \mathsf{e}_i.$

我们将通过在所有满秩的 $n \times n$ 矩阵中随机选择相应的秩为 n 的矩阵 $\overline{U}$，来选择 B_1。具体做法是，首先从所有秩为 k 的 $n \times k$ 矩阵中随机选择矩阵 $\overline{U}$ 的前 k 列（即 $\overline{U}_{[n],\ [k]}$）。我们按 $i = 1、2、\ldots\ldots、\ell$ 的顺序为 $\overline{U}_{J_i,\ [k]}$ 选择矩阵元素，从而选出 $U_{[n],\ [k]}$ 的矩阵元素；然后再为 $\overline{U}_{[n],\ [k]}$ 的其余部分选择剩下的矩阵元素。

由于 B_2 是标准基，因此当且仅当$\overline{U}_{J_i,\ [k]}$满秩时， $B_1、\mathscr{U}_1 \to B_2、\mathscr{V}_i$ 成立。因此，当且仅当$\overline{U}_{J_i,\ [k]}$满秩时， $X_i = 1$成立。由此，对于每个 i，概率 $\mathbb{P}(X_i = 1 \big|\ X_1, \ldots X_{i-1})$至少等于$\overline{U}_{J_i,\ [k]}$ 满秩的概率。根据引理 3.1，此概率等于 $\alpha_k = \prod_{i=1}^{k}(1-\frac{1}{q^i})$。因此 $\mathbb{P}(X_i = 1 \big|\ X_1, \ldots, X_{i-1})\ \geq \alpha_k.$

□

3.4 引理
对于 $i = 1、\ldots\ldots、\ell、\ \mathbb{P}\ (Y_i = 1 \big|\ Y_1、\ldots\ldots、Y_{i-1})\ \geq \alpha_k.$

证明。只需在给定 B_1 的情况下证明该引理。由于 $\mathbb{F}_q^n$ 中任意两个基之间都存在一个将其中一个映射到另一个的同构，我们不妨假设 B_1 是标准基；也就是说，$\mathbf{U}_i = \mathbf{e}_i,\ i = 1, \ldots, n.$。现在，我们通过在所有满秩矩阵中随机选取矩阵 $\overline{V}$ 来构造基 B_2。具体做法是依次选取 $\overline{V}_{[n],J_1}, \overline{V}_{[n],J_2}, \ldots, \overline{V}_{[n],J_\ell}$，然后为 $\overline{V}$. 选取其余矩阵元素。假设已给定 $\overline{V}_{[n],[n_{i-1}]}$；也就是说，$\overline{V}_{[n],J_1}, \ldots, \overline{V}_{[n],J_{i-1}}$ 已选定，其中$rank(\overline{V}_{[n],[n_{i-1}]}) = n_{i-1}.$。在所有秩为 k 的 $n \times k$ 矩阵中，我们按如下方式选择$\overline{V}_{[n],J_i}$：首先，随机为 $\overline{V}_{[k],J_i}$ 选取元素，但须满足其满秩。这样可以确保 $B_1, \mathscr{U}_1 \leftarrow B_2, \mathscr{V}_i$。接下来，我们填入 $\overline{V}_{[n],J_i}$ 的其余列，并要求矩阵 $\overline{V}_{[n],[n_i]}$ 的秩为 $n_i.$。正如引理 3.1 的证明中所见，有 $q^{\frac{k^2-k}{2}} \prod_{j=1}^{k}(q^i - 1)$ 个满秩 $k \times k$ 矩阵可供选择。因此，我们对 $\overline{V}_{[k],J_i}$ 也有同样多的选择。令 $r_0 = rank(\overline{V}_{[k],[n_{i-1}]})$，并且对于$j = 1, \ldots, k$，令 $r_j = rank(\overline{V}_{[k],[n_{i-1}+j]})$，注意到 $r_k = k.$

对于 $p = 1, \ldots, k$，令 $\mathbf{w}^p$ 为 $\overline{V}_{[n],J_i}$ 中的第 p 个列向量。此外，令 $\mathbf{w}_{[k],p} \in \mathbb{F}_q^k$ 为 $\overline{V}_{[k],J_i}$ 中的第 p 个列向量，并令 $\mathbf{w}_{[n\setminus k],p}$ 为 $\overline{V}_{[n\setminus k],J_i}$. 中的第 p 个列向量。也就是说，$\mathbf{w}_{[k],p}$ 是向量 $\mathbf{w}^p$ 截取其前 k 个分量所得的向量，而 $\mathbf{w}_{[n\setminus k],p}$ 是向量 $\mathbf{w}^p$ 截取其最后 $n-k$ 个分量所得的向量。我们假设 $\mathbf{w}_{[k],p},\ p = 1, \ldots, k$ 已经选定，使得 $rank(\overline{V}_{[k],[J_i]}) = k$。现在还需要选取 $\mathbf{w}_{[n\setminus k],p},\ p = 1, \ldots, k$，使得 $rank(\overline{V}_{[n],[n_i]}) = n_i.$

假设 $\mathbf{w}_{[k],1}$ 属于 $\overline{V}_{[k],[n_{i-1}]}$的列空间；也就是说，$r_1 = rank(\overline{V}_{[k],[n_{i-1}+1]}) = r_0.$。已知 $\overline{V}_{[k],[n_{i-1}]}$ 的秩为 r_0，因此 $\overline{V}_{[k],[n_{i-1}]}$ 的列恰好有 $q^{n_{i-1}-r_0}$ 个线性组合等于 $\mathbf{w}_{[k],1}$。因此，有 $q^{n-k} - q^{n_{i-1}-r_0}$ 种对 $\mathbf{w}_{[n\setminus k],1}$ 的选取方式，使矩阵 $\overline{V}_{[n],[n_{i-1}+1]}$ 的秩为 $n_{i-1}+1$。

假设相反，$\mathbf{w}_{[k],\ 1}$ 不属于$\overline{V}_{[k]}$的列空间$_{[n_{i-1}]\cdot}$。那么任取向量 $\mathbf{w}_{[n\setminus k],\ 1} \in \mathbb{F}_q^{n-k}$都会得到矩阵$\overline{V}_{[n],\ [n_{i-1}+1]}$，其秩为 $n_{i-1}+1.$。因此，在这种情况下，$\mathbf{w}_{[n\setminus k],\ 1}$有 q^{n-k} 种选取方式。

一般而言，设 $p \in [k]$，并假设已选定向量 $\mathbf{w}_{[n\setminus k],1}, \ldots, \mathbf{w}_{[n\setminus k],p-1}$，使得 $rank(\overline{V}_{[n],[n_{i-1}+p-1]}) = n_{i-1}+p-1.$。现在我们来确定 $\mathbf{w}_{[n\setminus k],p\cdot}$ 的选取数量。若 $r_p = r_{p-1} = r$，则恰有 $q^{n_{i-1}+p-1-r}$ 个矩阵 $\overline{V}_{[k],[n_{i-1}+p-1]}$ 的列的线性组合等于 $\mathbf{w}_{[k],p}$。因此，对于使 $\overline{V}_{[n],[n_{i-1}+p]}$ 的秩为 $n_{i-1}+p.$ 的情况，$\mathbf{w}_{[n\setminus k],p}$ 有 $q^{n-k} - q^{n_{i-1}+p-1-r}$ 种选取方式。若 $r_p = r_{p-1}+1$，则 $\mathbf{w}_{[k],p}$ 不

在矩阵 $\overline{V}_{[k],[n_{i-1}+p-1]}$ 的列空间中，因此可以任意选取向量 $\mathbf{w}_{[n\backslash k],p} \in \mathbb{F}_q^{n-k}$，而 $\overline{V}_{[n],[n_{i-1}+p]}$ 的秩将为 $n_{i-1}+p.$。因此，在这种情况下，$\mathbf{w}_{[n\backslash k],p}$ 有 q^{n-k} 种选取方式。

鉴于 $rank(\overline{V}_{[k],J_i}) = k$，恰好存在 $k_0 = k - r_0$ 个整数$p \in [k]$，使得 $r_p = rank(\overline{V}_{[k],[n_{i-1}+p]}) > r_{p-1} = rank(\overline{V}_{[k],[n_{i-1}+p-1]})$，我们将这些整数记为 $p_1 < \cdots < p_{k_0}$。令 $p_0 = 0$。对于 $j = 1$、.....、k_0，令$\beta_j = p_j - p_{j-1} - 1$。令 $\beta_{k_0+1} = k - p_{k_0}.$。对于 $j = 0$、.....、k_0，令 $s_j = r_{p_j}.$。我们可以看到，$s_j = r_0 + j$、 $j = 1$、.....、$k_0.$。此外， $k_0 + \beta_1 + \beta_2 + \cdots + \beta_{k_0+1} = k$，因此 $\beta_1 + \ldots \beta_j + j - 1 + (k - s_{j-1}) + \beta_{j+1} + \cdots + \beta_{k_0+1} = k$。注意到 $\beta_1 + \cdots + \beta_{j-1} + j - 1 = p_{j-1}$，由前一个等式可得，

$$k - s_{j-1} + p_{j-1} = k - \beta_j - \cdots - \beta_{k_0+1}.$$

因此

$$s_{j-1} - p_{j-1} = \beta_j + \cdots + \beta_{k_0+1}.$$

假设 $\beta_j = p_j - p_{j-1} - 1 > 0$ 对某个 $j \in [k_0]$. 成立。那么向量 $\mathbf{w}_{[k],p_{j-1}+1}, \cdots, \mathbf{w}_{[k],p_{j-1}+\beta_i}$ 都属于 $\overline{V}_{[k],n_{i-1}+p_{j-1}}$ 的列空间。因此，向量 $\mathbf{w}_{[n\backslash k],p_{j-1}+1}, \cdots, \mathbf{w}_{[n\backslash k],p_{j-1}+\beta_i}$ 的选择数为

$$\begin{aligned}\prod_{u=1}^{\beta_j}(q^{n-k} - q^{n_{i-1}+p_{j-1}+u-1-s_{j-1}}) &= \prod_{u=1}^{\beta_j}(q^{n-k} - q^{(n_{i-1}-k)+k+p_{j-1}+u-1-s_{j-1}}) \\ &= \prod_{u=1}^{\beta_j}(q^{n-k} - q^{(n_{i-1}-k)+k-\beta_j-\cdots-\beta_{k_0+1}+(u-1)}).\end{aligned}$$

设 N为选择 $\overline{V}_{[n],J_i}$ 的方法数，使得 $\overline{V}_{[k],J_i}$ 满秩，且矩阵 $\overline{V}_{[n],[n_i]}$ 的秩为 n_i。由上文可得，

$$\begin{aligned}N &\geq \prod_{i=0}^{k-1}(q^k - q^i) \prod_{p\in[k]-\{p_1,\ldots,p_{k_0}\}}(q^{n-k} - q^{n_{i-1}+p-1-r_{p-1}}) \prod_{p\in\{p_1,\ldots,p_{k_0}\}} q^{n-k} \\ &= \prod_{i=0}^{k-1}(q^k - q^i)\left(\prod_{\beta_j>0}\prod_{u=1}^{\beta_j}(q^{n-k} - q^{n_{i-1}+p_{j-1}+u-1-s_{j-1}})\right) q^{k_0(n-k)} \\ &= \prod_{i=0}^{k-1}(q^k - q^i)\left(\prod_{\beta_j>0}\prod_{u=1}^{\beta_j}\left(q^{n-k} - q^{(n_{i-1}-k)+k-\beta_j-\cdots-\beta_{k_0+1}+(u-1)}\right)\right) q^{k_0(n-k)}\end{aligned}$$

已知 $k-\beta_1-\cdots-\beta_{k_0+1}=k_0$，可见

$$\prod_{\beta_j>0}\prod_{u=1}^{\beta_j}(q^{n-k}-q^{(n_{i-1}-k)+k-\beta_j-\cdots-\beta_{k_0+1}+(u-1)})=\prod_{j=k_0}^{k-1}(q^{n-k}-q^{(n_{i-1}-k)+j}).$$

Thus

$$N\geq\prod_{i=0}^{k-1}(q^k-q^i)\cdot\prod_{j=k_0}^{k-1}(q^{n-k}-q^{n_{i-1}-k+j})\cdot q^{k_0(n-k)}.$$

另一方面，给定 $\overline{V}_{[n],n_{i-1}}$，满足 $rank(\overline{V}_{[n],n_i})=n_i$ 为 $\prod_{j=0}^{k-1}(q^n-q^{n_{i-1}+j})$ 的 $\overline{V}_{[n],J_i}$ 的选取方式总数为此。因此我们有

$$\begin{aligned}\mathbb{P}(Y_i=1\big|\ Y_1,\ldots,Y_{i-1})&\geq\frac{N}{\prod_{j=0}^{k-1}(q^n-q^{n_{i-1}+j})}=\frac{N}{q^{k^2}\prod_{j=0}^{k-1}(q^{n-k}-q^{n_{i-1}-k+j})}\\&\geq\frac{\prod_{i=0}^{k-1}(q^k-q^i)\cdot\prod_{j=k_0}^{k-1}(q^{n-k}-q^{n_{i-1}-k+j})\cdot q^{k_0(n-k)}}{q^{k^2}\prod_{j=0}^{k-1}(q^{n-k}-q^{n_{i-1}-k+j})}\\&=\frac{q^{k_0(n-k)}\prod_{i=0}^{k-1}(q^k-q^i)}{q^{k^2}\prod_{j=0}^{k_0-1}(q^{n-k}-q^{n_{i-1}-k+j})}\\&\geq\prod_{i=0}^{k-1}\left(\frac{q^k-q^i}{q^k}\right)=\prod_{i=1}^{k}\left(1-\frac{1}{q^i}\right)=\alpha_k.\end{aligned}$$

□

3.1 Chernoff 界

设 $Z_1,\ldots,Z_n$ 是 n 个相互独立的 0-1 随机变量，其中对所有 i,$\mathbb{P}(Z_i=1)=p.$。那么总和 $Z=\sum_{i=1}^n Z_i$ 服从二项分布 $B(n,p)$，并且我们有以下由 Chernoff 提出的著名集中不等式（参见 [1]）：

3.5 定理（Chernoff 界）

对于所有 $0\leq t\leq np$，我们有

$$\mathbb{P}(|Z-np|>t)<2e^{-\frac{t^2}{3np}}.$$

由此界可直接得出

3.6 引理
对于 $Z \sim Bin(n,p)$ $\mathbb{P}(Z > (1-\epsilon)np) > 1 - 2e^{-\frac{\epsilon^2 np}{3}}$.

设 $X = \sum_{i=1}^{\ell} X_i$ 和 $Y = \sum_{i=1}^{\ell} Y_i$。由引理 3.3 和 3.4 可知， X 和 Y 的概率分布支配随机变量 $Z \sim Bin(\ell, \alpha_k)$ 的概率分布。也就是说，对所有 $a > 0$, $\mathbb{P}(X \geq a) \geq \mathbb{P}(Z \geq a)$ 且 $\mathbb{P}(Y \geq a) \geq \mathbb{P}(Z \geq a)$。因此，由引理 3.6 可得:

3.7 引理
$\mathbb{P}(X \geq (1-\epsilon)\ell\alpha_k) > 1 - 2e^{-\frac{\epsilon^2 \ell \alpha_k}{3}}$ *and* $\mathbb{P}(Y \geq (1-\epsilon)\ell\alpha_k) > 1 - 2e^{-\frac{\epsilon^2 \ell \alpha_k}{3}}$.

在上述引理中固定 ϵ，并给定 $k \leq \ln(n)$，我们有 $\ell = \lfloor \frac{n}{k} \rfloor \to \infty$，当 $n \to \infty$. 时。因此 $\mathbb{P}(X \geq (1-\epsilon)\ell\alpha_k) \to 1$，且 $\mathbb{P}(Y \geq (1-\epsilon)\ell\alpha_k) \to 1$，当 $n \to \infty$. 时

我们定义随机变量 Z_i、 Z_i'、 $i \in [\ell]$，其中

$$Z_i = \begin{cases} 1 & \text{if } B_1, \mathscr{U}_1 \leftrightarrow B_2, \mathscr{V}_i \\ 0 & \text{otherwise} \end{cases} \qquad Z_i' = \begin{cases} 1 & \text{if } B_1, \mathscr{U}_1 \leftrightarrows B_2, \mathscr{V}_i \\ 0 & \text{otherwise} \end{cases}$$

Let $Z = Z_1 + \cdots + Z_\ell$ and $Z' = Z_1' + \cdots + Z_\ell'$. Recall that $\alpha = \prod_{i=1}^{\infty}(1 - \frac{1}{q^i})$.

3.8 观察
对于 $\epsilon > 0$, $\mathbb{P}(Z \geq (2(1-\epsilon)\alpha - 1)\ell) > 1 - 4e^{-\frac{\epsilon^2 \ell \alpha}{3}}$. 此外，若 $q > 2$，则存在常数 $c > 0$，使得 $\mathbb{P}(Z \geq c\ell) \to 1$，因为 $n \to \infty$.

证明。由引理 3.7，我们有，对于 $\epsilon > 0$, $\mathbb{P}(X \geq (1-\epsilon)\ell\alpha_k) > 1 - 2e^{-\frac{\epsilon^2 \ell \alpha_k}{3}}$. 由于 $\alpha = \prod_{i=1}^{\infty}(1 - \frac{1}{q^i}) < \alpha_k$，因此可得 $\mathbb{P}(X \geq (1-\epsilon)\ell\alpha) > 1 - 2e^{-\frac{\epsilon^2 \ell \alpha}{3}}$.

同理，我们有 $\mathbb{P}(Y \geq (1-\epsilon)\ell\alpha) > 1 - 2e^{-\frac{\epsilon^2 \ell \alpha}{3}}$。因此

$$\begin{aligned} \mathbb{P}(X \geq (1-\epsilon)\ell\alpha \text{ and } Y \geq (1-\epsilon)\ell\alpha) &= 1 - \mathbb{P}(X < (1-\epsilon)\ell\alpha \text{ or } Y < (1-\epsilon)\ell\alpha) \\ &\geq 1 - \mathbb{P}(X < (1-\epsilon)\ell\alpha) - \mathbb{P}(X < (1-\epsilon)\ell\alpha) \\ &\geq 1 - 4e^{-\frac{\epsilon^2 \ell \alpha}{3}} \end{aligned}$$

由此可得 $\mathbb{P}(X + Y \geq 2(1-\epsilon)\ell\alpha) \geq 1 - 4e^{-\frac{\epsilon^2 \ell \alpha}{3}}$. 注意到$Z \geq X + Y - \ell$, 可得 $\mathbb{P}(Z + \ell \geq (1-\epsilon)2\ell\alpha) \geq 1 - 4e^{-\frac{\epsilon^2 \ell \alpha}{3}}$ 从而 $\mathbb{P}(Z \geq (2(1-\epsilon)\alpha - 1)\ell)$ $\geq 1 - 4e^{-\frac{\epsilon^2 \ell \alpha}{3}}$. 根据欧拉定理，我们有$\alpha > 1 - \frac{1}{q} - \frac{1}{q^2}$. 因此，当 $q > 2$时, 我们有 $\alpha > \frac{5}{9}$以及 $\mathbb{P}(Z \geq (\frac{1}{9} - \frac{10}{9}\epsilon)\ell) > 1 - 4e^{-\frac{\epsilon^2 \ell \alpha}{3}}$.特别地，取$\epsilon < \frac{1}{10}$, 存在常数 $c > 0$使得 $\mathbb{P}(Z \geq c\ell) \to 1$，因为 $n \to \infty$.

□

我们将利用以下观察。

3.9 观察
设 D_i、 $i=1$、2 是拟阵中的基，且 $X_i \subseteq D_i$、 $i=1$、2 是子集，其中 D_1、$X_1 \to D_2$、X_2.。那么，对于 X_2 中元素的任意排列 $x_{21} \prec x_{21} \prec \cdots \prec x_{2k}$，存在 X_1 中元素的一个排列 $x_{11} \prec x_{11} \prec \cdots \prec x_{1k}$，使得对于 $i=1$、.....、 k, $D_2 - \{x_{21}, \ldots, x_{2i}\} + \{x_{11}, \ldots, x_{1i}\}$ 是一个基。

证明。设 $D_2' = D_2 - X_2 + X_1$，根据假设它是一个基。假设 X_2 的元素按 $x_{21} \prec x_{22} \prec \cdots \prec x_{2k}$ 排列。由于 $|D_2 - x_{21}| \lhd D_2'|$，存在一个元素 $x_{11} \in D_2'$，使得 $D_2^1 = D_2 - x_{21} + x_{11}$ 是一个基。我们注意到 $x_{11} \in X_1$. 。接下来，由于 $|D_2^1 - x_{22}| < |D_2'|$，存在 $x_{12} \in D_2'$，使得 $D_2^2 = D_2^1 - x_{22} + x_{12}$ 是一个基。同样，我们注意到 $x_{12} \in X_1$。现在假设对于某个 $1 \le i < k$，我们有 $D_2^i = D_2 - \{x_{21}, \ldots, x_{2i}\} + \{x_{11}, \ldots, x_{1i}\}$ 是一个基，其中 $\{x_{11}, \ldots, x_{1i}\} \subseteq X_1$。由于 $|D_2^i - x_{2(i+1)}| < |D_2'|$ $x_{1(i+1)} \in D_2'$ $D_2^{i+1} =$，存在 $D_2^i - x_{2j} + x_{1(j+1)}$ $x_{1(i+1)} \in X_1$. 这样的，使得其为一个基；此外，我们必须有 继续下去，我们生成元素 x_{11}、 x_{12}、.....、 x_{1k}，这将成为 X_1. 的元素所需的排列。 □

Recall that $\beta_k = \left(1 - \frac{1}{q}\right)^k$. We have the following lemma:

3.10 引理
设 $S \subseteq [\ell]$ 其中 $s = |S|$. 则

$$\mathbb{P}(Z_i' = 0,\ \forall i \in S \ \big|\ Z_i = 1, \forall i \in S) \le\ (1 - \beta_k)^s.$$

此外， $\mathbb{P}(Z' = 0 \ \big|\ Z = s) \le (1 - \beta_k)^s$.

证明。假设 $Z_i = 1, \forall i \in S$. 那么 $B_1, \mathscr{U}_1 \to B_2, \mathscr{V}_i$ 且 $B_1, \mathscr{U}_1 \leftarrow B_2, \mathscr{V}_i$，对所有 $i \in S$. 令 $i \in S$. 由观察 3.9 可知，对于某种 $\mathscr{V}_i$ 的排列 $V_{i_1} \prec V_{i_2} \prec \cdots \prec V_{i_k}$，有：对于 $j = 1, \ldots, k$， $B_1 - \{U_1, \ldots, U_j\} + \{V_{i_1}, \ldots, V_{i_j}\}$ 是一个基。鉴于此，我们可以假设，对于每个 $i \in S$，我们都已重新排列 $\mathscr{V}_i$ 中的向量，使得对于 $j = 1, \ldots, k$, $B_1 - \{U_1, \ldots, U_j\} + \{V_{n_{i-1}+1}, \ldots, V_{n_{i-1}+j}\}$ 是一个基。令 $\overline{W}$ 为将 $\overline{U}$ 与 $\overline{V}$ 拼接得到的矩阵，并令 $\overline{W}'$ 为对 $\overline{W}$ 进行行变换后得到的矩阵，使得 $\overline{V}$ 化为单位矩阵 I_n，而 $\overline{U}$ 化为矩阵 $\overline{U}' = (u'_{ij})$。注意，这些行变换不会改变 $\overline{W}$ 列空间中列子集的独立性；也就是说， $\overline{W}$ 中的一组列线性

无关，当且仅当 $\overline{W}'$ 中对应的列子集线性无关。令 $i \in S$. 由于 B_1, $\mathscr{U}_1 \underset{M}{\to} B_2, \mathscr{V}_i$，可知 $\overline{U}'_{J_i,[k]}$满秩。此外，若 $\overline{U}'_{J_i,[k]}$ 顺序满秩，则可见，对于 $j = 1, \ldots, k$，用 I_n 的前 j 列替换 j 的前 j 列，将得到一个满秩矩阵。因此，若 $\overline{U}'_{J_i,[k]}$顺序满秩，则对于 $j = 1, \ldots, k$, $B_2 - \{V_{n_{i-1}+1}, \ldots, V_{n_{i-1}+j}\} + \{U_1, \ldots, U_j\}$是一个基。在这种情况下，我们看到 $Z'_i = 1$. 根据观察 3.2, $\overline{U}'_{J_i,[k]}$顺序满秩的概率为 $\beta_k = (1-\frac{1}{q})^k$。因此 $\mathbb{P}(Z'_i = 1 \big| Z_i = 1) \geq \beta_k$，且此界与其他随机变量无关。现在可知 $\mathbb{P}(Z'_i = 0, \forall i \in S \mid Z_i = 1, \forall i \in S) \leq (1-\beta_k)^s$。

第二个断言由第一个陈述推出。 □

3.2 定理 1.5 的证明

假设 $q > 2$. 根据引理 3.8，存在常数 $c > 0$ 使得$\mathbb{P}(Z \geq c\ell) \to 1$，因为 $\ell \to \infty$. 要完成定理 1.5 的证明，只需证明当 $n \to \infty$ 时， $\mathbb{P}(Z' > 0) \to 1$. 根据引理 3.10，我们有

$$\begin{aligned}
\mathbb{P}(Z' = 0) &= \sum_{s=0}^{\ell} \mathbb{P}(Z' = 0, Z = s) = \sum_{s=0}^{\ell} \mathbb{P}(Z' = 0 \mid Z = s)\mathbb{P}(Z = s) \\
&\leq \sum_{s=0}^{\ell} (1-\beta_k)^s \mathbb{P}(Z = s) = \sum_{s<c\ell} (1-\beta_k)^s \mathbb{P}(Z = s) + \sum_{s \geq c\ell} (1-\beta_k)^s \mathbb{P}(Z = s) \\
&\leq \mathbb{P}(Z < c\ell) + (1-\beta_k)^{c\ell} \mathbb{P}(Z \geq c\ell).
\end{aligned}$$

我们有 $\lim_{n\to\infty} \mathbb{P}(Z < c\ell) = 0.$。我们断言 $\lim_{n\to\infty}(1-\beta_k)^{c\ell} = 0$。只需在 $k = \ln(n)$ 时证明这一点（因为 $\beta_{k'} > \beta_k$ 且当 $k' < k$ 时 $\frac{n}{k'} > \frac{n}{k}$）。令 $\delta = \ln(1 - \frac{1}{q})$。注意到 $-1 < \delta < 0$，我们有

$$\begin{aligned}
(1-\beta_k)^{c\ell} &= (1 - (1 - \frac{1}{q})^k)^{c\ell} = (1 - e^{\delta k})^{c\ell} \\
&= (1 - e^{\delta \ln(n)})^{c\ell} = (1 - n^{\delta})^{c\ell} = \left((1 - \frac{1}{n^{-\delta}})^{n^{-\delta}}\right)^{\frac{cn^{1+\delta}}{\ln(n)}}
\end{aligned}$$

由于 $\lim_{n\to\infty}(1-\frac{1}{n^{-\delta}})^{n^{-\delta}} = e^{-1}$，可知 $\lim_{n\to\infty} \left((1 - \frac{1}{n^{-\delta}})^{n^{-\delta}}\right)^{\frac{cn^{1+\delta}}{n}\ln()} = 0$。因此 $\lim_{n\to\infty}(1-\beta_k)^{c\ell} = 0$. 由上述内容可知，当 $n \to \infty$,$\mathbb{P}(Z' > 0) \to 1$. 这就完成了证明。

4 讨论

鉴于定理 1.5 不适用于二元拟阵，以下问题便顺理成章：

4.1 问题

设 M 是一个秩为n 的二元拟阵，且 k 是一个固定整数。假设随机选取两个基 B_1 和 B_2，然后随机选取一个k-子集 $X \subseteq B_1$. 。找到一个与 X 串行可交换的 k-子集 $Y \subseteq B_2$ 的概率是否会随着 $n \to \infty$ 趋近于 1?

参考文献

[1] N. Alon、J. Spencer，《概率方法》，Wiley，纽约，1992 年，[2] J. Bonin，《稀疏铺路拟阵的基交换性质》，《应用数学进展》，50（2013）第 1 期，6–15。[3] R. Cordovil、R. Moreira，《拟阵的基-余基图与多面体》，《组合数学》13（1993），157–165。[4] M. Farber，《横截拟阵的基本对图》，《离散数学》，73（1989），245–248。[5] M. Farber、B. Richter、H. Shank，《边不相交生成树：一项连通性定理》，《图论杂志》，9（1985）第 3 期，319–324。[6]G. Gabow，《拟阵基中对称交换的分解》，《数学规划》，10（1976），271–276。[7]C. Greene，《基的多重交换性质》，《美国数学会会刊》，39（1973），45–50。[8] G.H. Hardy、E.M. Wright，《数论导论》，牛津大学出版社，第五版，1979 年。[9] R. Huang 和 G.-C. Rota，《关于拉丁方的各种猜想与标准化系数之间的关系》，《离散数学》128（1994），225–236。[10] D. Kotlar，《拟阵中的回路与串行对称基交换》，《SIAM 离散数学杂志》，27（2013）第 3 期，1274–1286。

[11] D.Kotlar、R. Ziv，《基的串行对称交换》，J. Graph Theory，73 3（2012年），296-304。[12] S. McGuinness，《拟阵中的串行交换》，Discrete Mathematics，345 2（2022年）。[13] L. Sauermann，《Rota 的基猜想对向量空间的随机基成立》，arXiv:2203.17121，2022年。[14] D.Wiedemann，《拟阵的循环基序》，手稿，2006年[15] D.R. Woodall，《拟阵的基交换定理》，J. Combinatorial Theory Series B，16（1974），227-228。