arXiv:2601.01603v1 [math.NT] 4 Jan 2026

矩阵克罗内克和、随机矩阵统计与密码学

Tianshuo Yang

摘要

本文全面研究矩阵克罗内克和，包括其计算方面、分布行为以及在密码分析中的应用。在 [7], 的工作基础上，我们开发了通过格林多项式计算这些和的算法，并建立了分析其统计分布的一般框架。我们进一步考察相关的 L-函数，并阐明它们与对称函数和随机矩阵理论之间的关系。我们证明，与紧李群中随机矩阵的特征值统计类似，例如 $SU(n)$和 $Sp(2n)$，矩阵克罗内克和的归一化值呈现萨托–泰特等分布。最后，我们运用这一框架区分真正随机的序列与带有微妙代数偏差的序列，并基于矩阵克罗内克和的分布特征，提出一种用于评估密码安全性的新型谱检验。

1 引言

克洛斯特曼和是数论、代数几何和表示论中的基本对象。经典定义中，它们是如下形式的指数和

$$K(a,b;p)=\sum_{\substack{x\in\mathbb{F}_p^\times\\ xy=1}} e^{2\pi i(ax+by)/p},$$

并且它们与模形式、自守表示和 ℓ-进上同调 [4] 有着深刻的联系。它们在矩阵群上的自然推广——称为矩阵克罗内克和——在 Erd´elyi 和 T´oth [1], 最近的研究中得到探讨，Zelingher [7] 也独立进行了研究。这些进展为研究随机矩阵统计、等分布现象以及密码分析应用开辟了新途径。

矩阵克罗内克和定义在一般线性群 $\mathrm{GL}_n(\mathbb{F}_q)$ 中的矩阵上，同时涵盖乘法特征（通过行列式）和加法特征（通过迹）。其重要性体现在多个方面：

1. **代数结构**：矩阵克罗内克和通过格林多项式（[3, 5], 和 [7]）与 $\mathrm{GL}_n(\mathbb{F}_q)$ 的表示论和对称函数密切相关。2. **随机矩阵统计**：Deligne 等分布定理 [4] 表明，归一化的克洛斯特曼和应当类似于紧李群中随机矩阵的迹分布。这种数论与随机矩阵理论之间的联系，对于理解这些和的统计性质有着深远影响。3. **密码学应用**：矩阵克罗内克和的随机性使其适合用于测试密码算法。通过将根据密码输出计算出的矩阵克罗内克和的分布与理论随机矩阵分布进行比较，可以评估密码学随机性的质量。

本文在 Zelingher [7] 的奠基性工作基础上，利用格林多项式和经典克洛斯特曼和，开发了计算矩阵克罗内克和的算法。我们设计并实现了两种互补的算法：算法 I 用于计算 Jordan型矩阵的矩阵克罗内克和；算法 II 则通过 Jordan 分解将计算扩展到任意矩阵。

我们研究与矩阵克罗内克和相关的 L-函数，并确立它们与对称函数及随机矩阵统计之间的联系。通过大量数值实验，我们确认了归一化矩阵克罗内克和的 Sato–Tate 分布特征，并证明它们在紧李群中等分布。基于这些发现，我们提出一种以矩阵克罗内克和的分布为基础的密码学随机性新统计检验，并展示了该检验在检测偏离真正随机性的代数或结构偏差方面的有效性。

本文结构安排如下。第 2 节回顾有关 $\mathrm{GL}_n(\mathbb{F}_q)$ 的共轭类与表示、对称函数、经典克洛斯特曼和以及矩阵克罗内克和的必要背景。第 3 节介绍计算算法。第 4 节研究相关的 L-函数。第 5 节探讨与随机矩阵理论的联系。第 6 节介绍密码学应用和数值实验。第 7 节总结全文并指出未来研究方向。

2 预备知识

2.1 $\mathrm{GL}_n(\mathbb{F}_q)$的共轭类

设 $\mathbb{F}_q$ 是一个大小为 q的有限域，其中 q 是某个素数 p的幂。$\mathrm{GL}_n(\mathbb{F}_q)$ 中共轭类的分类是我们研究的基础。我们遵循 Green方法 [3]。

定义 2.1 (正则椭圆元素)。 若元素 $g \in \mathrm{GL}_n(\mathbb{F}_q)$ 的特征多项式在 $\mathbb{F}_q$上不可约，则称其为正则椭圆元素。这种元素在 $\mathbb{F}_{q^n}$中有 n 个不同的特征值： $\{\xi, \xi^q, \ldots, \xi^{q^{n-1}}\}$。

定理 2.2 (共轭分类)。 *[3]* 对于任意 $y \in \mathrm{GL}_n(\mathbb{F}_q)$，存在一个整数$s \geq 1$, $d_1, \ldots, d_s \geq 1$，以及正则椭圆元素 $y_j \in \mathrm{GL}_{d_j}(\mathbb{F}_q)$（它们在 $\mathbb{F}_q$上的特征值两两不相交）和非空分拆 $\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_s$，使得

$$y \sim \mathrm{diag}\left(J_{\boldsymbol{\mu}_1}(y_1), \ldots, J_{\boldsymbol{\mu}_s}(y_s)\right),$$

其中， $J_{\boldsymbol{\mu}_j}(y_j)$ 表示与分拆 $\boldsymbol{\mu}_j$ 及正则椭圆元素 y_j相关联的 *Jordan* 块矩阵。

单个部分 μ 和正则椭圆元素 $y \in$$\mathrm{GL}_d(\mathbb{F}_q)$对应的若尔当块 $J_{(\mu)}(y)$ 定义如下:

$$J_{(\mu)}(y) = \begin{pmatrix} y & I_d & & \\ & y & \ddots & \\ & & \ddots & I_d \\ & & & y \end{pmatrix} \in \mathrm{GL}_{d\mu}(\mathbb{F}_q),$$

其中， I_d 是单位矩阵 $d \times d$ 。

2.2 $\mathrm{GL}_n(\mathbb{F}_q)$的表示

$\mathrm{GL}_n(\mathbb{F}_q)$ 的表示论由 Green [3] 完整描述。令 $\mathrm{Irr}(\mathrm{GL}_n(\mathbb{F}_q))$ 表示不可约表示的集合，$\mathrm{Irr}^{\mathrm{cusp}}(\mathrm{GL}_d(\mathbb{F}_q))$ 表示其中尖点表示构成的子集。

定理 2.3 (格林参数化)。 *[3]* 在 $\mathrm{Irr}(\mathrm{GL}_n(\mathbb{F}_q))$ 与满足 $|\varphi| = n$ 的参数 φ 之间存在双射，其中参数 φ 将每一对满足 $\sigma \in$ 的 (d, σ) $\mathrm{Irr}^{\mathrm{cusp}}(\mathrm{GL}_d(\mathbb{F}_q))$对应到一个分拆 $\varphi(d, \sigma)$，使得

$$|\varphi| = \sum_{(d,\sigma)} d \cdot |\varphi(d, \sigma)|.$$

尖点表示对应于正则特征的 Frobenius 轨道 $\theta : \mathbb{F}_{q^d}^{\times} \to \mathbb{C}^{\times}$。特征 θ 是正则的，当且仅当对于所有 $0 \le j \le d-1$ 都有 $\theta^{q^j} \neq \theta$，这意味着它的 Frobenius 轨道大小为 d。

2.3 对称函数与格林多项式

我们回顾对称函数和格林多项式的基本事实 [5]。

定义 2.4 (分拆)。 分拆 $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_\ell)$ 是一个弱递减的正整数序列。我们记作 $\boldsymbol{\lambda} \vdash r$，若 $|\boldsymbol{\lambda}| = \sum \lambda_i = r$。长度 $\ell(\boldsymbol{\lambda}) = \ell$，而 $m_i(\boldsymbol{\lambda})$ 统计等于 i 的部分数。

对于分拆 $\boldsymbol{\lambda}$，定义 $z_{\boldsymbol{\lambda}} = \prod_{i \ge 1} i^{m_i} m_i!$ 和 $n(\boldsymbol{\lambda}) = \sum_{i=1}^{\ell} (i-1)\lambda_i$。我们用 $p_{\boldsymbol{\lambda}}$ 表示与分拆 $\boldsymbol{\lambda}$ 相关联的幂和对称函数，并用 $P_{\boldsymbol{\mu}}(x; t)$ 表示与分拆 $\boldsymbol{\mu}$ 相关联的霍尔–利特尔伍德多项式。

定义 2.5 (格林多项式)。 格林多项式 $Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(q)$ 定义为 *by:*

$$Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(q) = q^{n(\boldsymbol{\mu})} X_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(q^{-1}),$$

其中 $X_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(t)$ 由以下展开式确定：

$$p_{\boldsymbol{\lambda}}(x) = \sum_{\boldsymbol{\mu}} X_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(t) P_{\boldsymbol{\mu}}(x; t).$$

格林多项式满足重要性质 [3]:

- $Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(t) \in \mathbb{Z}[t]$，且除非 $|\boldsymbol{\lambda}| = |\boldsymbol{\mu}|$，否则为零。
- $Q_{(r)\,\boldsymbol{\lambda}}(t) = 1$，对 r 的所有分拆 $\boldsymbol{\lambda}$ 均成立。
- $\sum_{|\boldsymbol{\lambda}|=r} z_{\boldsymbol{\lambda}}^{-1} Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(q) = 1$。
- 次 $(Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(t)) \le n(\boldsymbol{\mu}) = \sum_{i=1}^{\ell} (i-1)\,\mu_i$

格林多项式的表格见 Green [3] 关于 $n \le 5$ 的内容，以及 Morris [6] 关于 $n = 6$ 的内容和文献 7。

2.4 经典Kloosterman和与层

设 ψ： $\mathbb{F}_{q^d} \to \mathbb{C}^{\times}$ 是非平凡加性特征，且 $\boldsymbol{\alpha} =$（α_1，……，α_k）中有 α_i 个乘法特征。

定义 2.6（超Kloosterman和）。 秩为 k 的 *Kloosterman* 和为：

$$\mathrm{Kl}(\boldsymbol{\alpha}, \psi, \xi) = (-1)^{k-1} \sum_{\substack{t_1, \ldots, t_k \in \mathbb{F}_{q^d}^{\times} \\ t_1 \cdots t_k = \xi}} \alpha_1(t_1) \cdots \alpha_k(t_k) \psi(t_1 + \cdots + t_k).$$

Katz [4] 研究了克洛斯特曼层，它们是乘法群 $\mathbb{G}_m$上的 ℓ-进层，其 Frobenius迹给出了克洛斯特曼和。对于秩为 k 的克洛斯特曼层 $\mathrm{Kl}_k^{\mathbb{F}_{q^d}}(\boldsymbol{\alpha}, \psi)$，在 $\xi \in \mathbb{F}_{q^d}^{\times}$处的弗罗贝尼乌斯特征值记为 w_1，……，w_k，满足 $|w_j| = q^{d(k-1)/2}$。

2.5 矩阵 Kloosterman 和

我们记 矩阵克罗内克和的全部定义及其性质，来自 [1] 和 [7]。

2.5.1 定义

定义 2.7 (矩阵 Kloosterman 和**)**。 设 $y \in \mathrm{GL}_n(\mathbb{F}_q)$， $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ 为非平凡加性特征，且 $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k)$ 为 $\mathbb{F}_q^\times$ 的乘法特征。矩阵 *Kloosterman* 和定义如下：

$$\mathrm{Kl}_n(\boldsymbol{\alpha}, \psi, y) = \sum_{\substack{g_1,\ldots,g_k \in \mathrm{GL}_n(\mathbb{F}_q) \\ \prod_{j=1}^k g_j = y}} \left(\prod_{i=1}^k \alpha_i(\mathrm{Det}(g_i)) \right) \psi\left(\mathrm{Tr}\left(\sum_{i=1}^k g_i \right) \right).$$

这个定义从两个方面推广了经典克洛斯特曼和：从标量推广到矩阵，以及从乘积推广到乘积（通过条件 $\prod g_j = y$）和求和（通过加性特征中的迹）。

2.5.2 约化公式

矩阵克罗内克和在特征值互不相交的矩阵直和下具有乘法性质。

定理 2.8 (直和分解**)**。 *[1]* 设 $y_1 \in \mathrm{GL}_{n_1}(\mathbb{F}_q)$ 和 $y_2 \in \mathrm{GL}_{n_2}(\mathbb{F}_q)$ 在 $\mathbb{F}_q$ 上没有共同特征值。那么：

$$\mathrm{Kl}_{n_1+n_2}(\boldsymbol{\alpha}, \psi, \mathrm{diag}(y_1, y_2)) = q^{(k-1)n_1n_2} \mathrm{Kl}_{n_1}(\boldsymbol{\alpha}, \psi, y_1) \mathrm{Kl}_{n_2}(\boldsymbol{\alpha}, \psi, y_2).$$

对于正则椭圆元素，矩阵克罗内克和可化为经典克洛斯特曼和。

定理 2.9 (正则椭圆约化**)**。 *[7]* 设 $y \in \mathrm{GL}_n(\mathbb{F}_q)$ 是正则椭圆的，其特征值为 $\{\xi, \xi^q, \ldots, \xi^{q^{n-1}}\}$，$\xi \in \mathbb{F}_{q^n}^\times$。那么：

$$\mathrm{Kl}_n(\boldsymbol{\alpha}, \psi, y) = (-1)^{(k-1)(n+1)} q^{(k-1)\binom{d}{2}} \mathrm{Kl}_n(\boldsymbol{\alpha}, \psi, \xi),$$

其中右侧是 $\mathbb{F}_{q^n}$ 中的经典克洛斯特曼和。

2.5.3 约当块公式

最复杂的情形涉及若尔当块。设 $n = dr$ 和 $y \in \mathrm{GL}_d(\mathbb{F}_q)$ 为正则椭圆，其特征值为 $\{\xi, \xi^q, \ldots, \xi^{q^{d-1}}\}$。

定理 2.10 （若尔当块公式）。 *[7]* 对于任意分拆 $\boldsymbol{\mu} \vdash r$：

$$\mathrm{Kl}_n(\boldsymbol{\alpha}, \psi, J_{\boldsymbol{\mu}}(y)) = (-1)^{(k-1)n} q^{(k-1)\binom{n}{2}} \sum_{\boldsymbol{\lambda} \vdash r} \frac{Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(q^d)}{z_{\boldsymbol{\lambda}}} (-1)^{(k-1)\ell(\boldsymbol{\lambda})} \prod_{j=1}^{\ell(\boldsymbol{\lambda})} \mathrm{Kl}_{d\lambda_j}(\boldsymbol{\alpha}, \psi, \xi).$$

设 $w_1, \ldots, w_k$ 为 $\mathrm{Kl}_k^{\mathbb{F}_{q^d}}(\boldsymbol{\alpha}, \psi)$ 在 ξ 处的弗罗贝尼乌斯特征值，并定义归一化特征值 $\widetilde{w}_j = q^{-d(k-1)/2} w_j$。利用恒等式

$$p_{\boldsymbol{\lambda}}(w_1, \ldots, w_k) = (-1)^{(k-1)\ell(\boldsymbol{\lambda})} \prod_{j=1}^{\ell(\boldsymbol{\lambda})} \mathrm{Kl}_{d\lambda_j}(\boldsymbol{\alpha}, \psi, \xi),$$

可得到一个对称函数表述：

推论 2.11。

$$\mathrm{Kl}_n(\boldsymbol{\alpha},\psi,J_{\boldsymbol{\mu}}(y))=(-1)^{(k-1)n}q^{(k-1)\binom{n}{2}}\sum_{\boldsymbol{\lambda}\vdash r}\frac{Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(q^d)}{z_{\boldsymbol{\lambda}}}p_{\boldsymbol{\lambda}}(w_1,\ldots,w_k).$$

这表明，矩阵克罗内克和本质上是将对称函数代入 Kloosterman 层的弗罗贝尼乌斯特征值所得到的值，并以 Green 多项式作为系数。

2.5.4 一般公式

组合 定理 2.8 和 2.10，从而得到任意矩阵的完整公式。

定理 2.12 (一般公式**)**。 *[7]*令 $y=\mathrm{diag}(J_{\boldsymbol{\mu}_1}(y_1)\ldots,J_{\boldsymbol{\mu}_s}(y_s))$，其中 $y_j\in\mathrm{GL}^{d_j}(\mathbb{F}_q)$是具有互不相交特征值的正则椭圆矩阵，并且 $\boldsymbol{\mu}_j\vdash r_j$ 与 $\sum_{j=1}^{s}d_jr_j=n$。令 $\eta_j\in\mathbb{F}_{q^{d_j}}^{\times}$对应于 y_j的特征值，且 w_{j1}、.....、w_{jk} 是 $\mathrm{Kl}_k^{q^{d_j}}(\boldsymbol{\alpha},\psi)$在 η_j处的弗罗贝尼乌斯特征值。则：

$$\mathrm{Kl}_n(\boldsymbol{\alpha},\psi,y)=(-1)^{(k-1)n}q^{(k-1)\binom{n}{2}}\times\prod_{j=1}^{s}\sum_{\boldsymbol{\lambda}\vdash r_j}\frac{Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}_j}(q^{d_j})}{z_{\boldsymbol{\lambda}}}p_{\boldsymbol{\lambda}}(w_{j1},\ldots,w_{jk}).$$

在特殊情形 $\boldsymbol{\mu}=(r)$ 下，也就是说， $J_{\boldsymbol{\mu}}(y)$ 是一个正则元素，我们有 $Q_{\boldsymbol{\lambda}}^{(r)}(t)=1$ 对所有 $\boldsymbol{\lambda}\vdash r$ 均成立，因此

$$\sum_{\boldsymbol{\lambda}=(\lambda_1,\ldots,\lambda_\ell)\vdash(r)}\frac{Q_{\boldsymbol{\lambda}}^{(r)}(t)}{z_{\boldsymbol{\lambda}}}p_{\boldsymbol{\lambda}}(x_1,\ldots,x_k)=h_r(x_1,\ldots,x_k)=\sum_{\boldsymbol{\lambda}\vdash r}m_{\boldsymbol{\lambda}}(x_1,\ldots,x_k)$$

是次数为 r的完全对称多项式。

3 计算算法

3.1 归一化

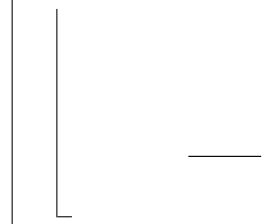
为了进行统计分析，我们使用归一化矩阵克罗伊斯特曼和：

$$\widetilde{\mathrm{Kl}}_n(\boldsymbol{\alpha},\psi,y)=q^{-(k-1)\frac{n^2}{2}}\mathrm{Kl}_n(\boldsymbol{\alpha},\psi,y).$$

根据 Green [3], $\deg\left(Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(t)\right)\leq n(\boldsymbol{\mu})=\sum_{i=1}^{\ell}(i-1)\mu_i$。对于所有分拆 $\boldsymbol{\mu}\vdash r$，最大值$n(\boldsymbol{\mu})$为$\binom{r}{2}$，在 $\boldsymbol{\mu}=(1,1,..,1)$ 处取得。我们有 $|\widetilde{\mathrm{Kl}_n(\boldsymbol{\alpha},\psi,y)}|\leq q^{\sum_{j=1}^{s}{}^{d_jr_j}_{(r_j-1)\,2}}$。特别地，对于 $\boldsymbol{\mu}=(r)$，所有 r 的分拆 $\boldsymbol{\lambda}$ 都有 $Q_{\boldsymbol{\lambda}}^{(r)}(t)=1$。因此，对于 Jordan block$J_{(r)}(y)$，其中 y 是正则椭圆元素，归一化和有界，且界与 q 无关。

3.2 算法 I：若尔当块计算

算法 1：计算 $\widetilde{\mathrm{Kl}}_n(\boldsymbol{\alpha}, \psi, J_{\boldsymbol{\mu}}(y))$ **输入**：$q = p^m$，n，正则椭圆 $y \in \mathrm{GL}_d(\mathbb{F}_q)$，分拆 $\boldsymbol{\mu} \vdash r$，满足 $n = dr$ **输出**：$\widetilde{\mathrm{Kl}}_n(\boldsymbol{\alpha}, \psi, J_{\boldsymbol{\mu}}(y))$ **开始** 计算 $P(T) = \det(TI_d - y)$，在 $\mathbb{F}_q[T]$ 中；查找满足 $P(\xi) = 0$ 且 $\mathbb{F}_{q^d} = \mathbb{F}_q[\xi]$ 的 $\xi \in \mathbb{F}_{q^d}^{\times}$；初始化总和 $= 0$；对于每个分拆 $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_\ell) \vdash r$，执行：加载 $Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(t)$（预计算表）；计算 $z_{\boldsymbol{\lambda}} = \prod_{i \geq 1} i^{m_i} m_i!$；计算 $j = 1, \ldots, \ell$ 对应的 $\widetilde{\mathrm{Kl}}_{d\lambda_j}(\boldsymbol{\alpha}, \psi, \xi)$；项 $= Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(q^d)\, z_{\boldsymbol{\lambda}}^{-1} (-1)^{(k-1)\ell} \prod_{j=1}^{\ell} \widetilde{\mathrm{Kl}}_{d\lambda_j}(\boldsymbol{\alpha}, \psi, \xi)$；sum $=$ sum $+$term；返回 $(-1)^{(k-1)n} \cdot$sum



该算法需要预先计算分拆大小为 $\widetilde{\mathrm{Kl}}$、不超过 r的格林多项式 $Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(t)$表。经典克洛斯特曼和 $\mathrm{Kl}_{d\lambda_j}(\boldsymbol{\alpha}, \psi, \xi)$ 可通过成熟的方法高效计算。具体而言，GL_n 的布鲁哈特分解提供了显式求和公式，而基于高斯和与乘法特征展开的特征和技巧则进一步简化了求值过程。这些工具共同构成了现代克洛斯特曼型和计算算法的基础。

3.3 算法 II：一般矩阵计算

算法 2： 计算 $\widetilde{\mathrm{Kl}}_n(\boldsymbol{\alpha}, \psi, y)$ 对一般 y计算 $\mathrm{Kl}_n(\boldsymbol{\alpha}, \psi, y)$

输入： $q = p^m$，n，$y \in \mathrm{GL}_n(\mathbb{F}_q)$

输出： $\widetilde{\mathrm{Kl}}_n(\boldsymbol{\alpha}, \psi, y)$

开始

- 计算约当标准形：$y = \mathrm{diag}(J_{\boldsymbol{\mu}_1}(y_1), \ldots, J_{\boldsymbol{\mu}_s}(y_s))$；
- 初始化结果 $= 1$；
- **对于** $j = 1$ **至** s，**执行**
  - 令 $d_j =$维数为y_j，$r_j = |\boldsymbol{\mu}_j|$；
  - 计算 $\eta_j \in \mathbb{F}_{q^{d_j}}^{\times}$ 根据算法 1 中的 y_j；
  - 块值 $=$ 使用算法 1 计算 $\widetilde{\mathrm{Kl}}_{d_j r_j}(\boldsymbol{\alpha}, \psi, J_{\boldsymbol{\mu}_j}(y_j))$；
  - 结果 $=$结果 $\times$blockVal；
- **返回** 结果

3.4 复杂度分析

计算复杂度取决于若干因素：

- **Jordan 分解**：在有限域 $\mathbb{F}_q$ 上，可以在多项式时间内计算矩阵 $n \times n$ 的有理标准形和 Jordan 标准形。特别是，标准算法（例如先求 Frobenius 形式，再进行主分解）需要 $O(n^3)$ 次域运算。

- **格林多项式**：$\mathrm{GL}_n(\mathbb{F}_q)$ 的格林多项式 $Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(t)$ 可通过将其解释为 Hall–Littlewood

基与对称函数环 [5] 中幂和基之间的变换系数，从而有效地计算。递归公式、顶点算子构造以及计算机代数实现，使得在固定 n 的情况下，可以在关于分拆数据大小的多项式时间内计算单个 $Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(t)$。

然而，在矩阵克罗内克和的应用中，通常需要给定大小的所有格林多项式。对于 $y \sim \mathrm{diag}(J_{\boldsymbol{\mu}_1}(y_1)\dots,J_{\boldsymbol{\mu}_s}(y_s))$，计算 $\mathrm{Kl}_n(\boldsymbol{\alpha},\psi,y)$ 需要所有分拆 $\boldsymbol{\lambda}\vdash|\boldsymbol{\mu}_j|$ 和 $1\le j\le s$对应的 $Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}_j}(t)$ 值。由于分拆数 $p(n)$ 根据哈代–拉马努金渐近公式呈指数增长，获取完整的 $\{Q_{\boldsymbol{\lambda}}^{\boldsymbol{\mu}}(t):|\boldsymbol{\lambda}|=|\boldsymbol{\mu}|\le n\}$ 集合会带来重大的计算挑战。因此，开发更高效的算法来计算所有有界大小的格林多项式是十分必要的。

- **经典克洛斯特曼和**：直接计算 $\mathrm{Kl}_d(\boldsymbol{\alpha},\psi,\xi)$ 需要 $O(q^{d/2})$ 次运算，但可以利用特征和技巧以及结构分解来加速，从而在实践中取得显著改进。

对于取值适中的 n和 q，这些算法是可行的。

4 L函数与对称函数

4.1 L函数的经典克洛斯特曼和

对于固定的 $\xi\in\mathbb{F}_{q^d}^{\times}$，考虑归一化经典克洛斯特曼和的生成级数：

$$L(T)=\exp\left(\sum_{n=1}^{\infty}\widetilde{\mathrm{Kl}}_{dn}(\boldsymbol{\alpha},\psi,\xi)\frac{T^n}{n}\right).$$

定理 4.1。（例如参见 *[2]*） $L(T)^{(-1)^k}$ 是一个次数为 k的多项式：

$$L(T)^{(-1)^k}=\prod_{i=1}^{k}(1-\widetilde{w}_iT),$$

其中，$\widetilde{w}_i=q^{-d(k-1)/2}w_i$ 是归一化的弗罗贝尼乌斯特征值。

4.2 系数公式

展开该乘积可得到用初等对称函数表示的表达式：

$$L(T)^{(-1)^k}=\sum_{r=0}^{k}(-1)^r e_r(\widetilde{w}_1,\dots,\widetilde{w}_k)T^r.$$

利用牛顿恒等式，系数可以用克洛斯特曼和 $\sim K_j=\mathrm{Kl}_{dj}(\boldsymbol{\alpha},\ \psi,\ \xi)$ 表示。

命题 4.2. T^r 在 $L(T)^{(-1)^k}$ 中的系数 C_r 为：

$$C_r=\sum_{\substack{s_1,\dots,s_r\ge0\\ 1s_1+\cdots+rs_r=r}}\frac{K_1^{s_1}\cdots K_r^{s_r}(-1)^{k(s_1+\cdots+s_r)}}{s_1!\cdots s_r!1^{s_1}\cdots r^{s_r}}.$$

这可以通过分拆枚举高效计算。

4.3 矩阵 Kloosterman 和与生成函数

关于分拆（n）的矩阵克罗内克和生成函数，我们有如下结果：

定理 4.3。 对于正则椭圆 $y \in \mathrm{GL}_d(\mathbb{F}_q)$，有

$$\sum_{n=0}^{\infty}(-1)^{(k-1)dn}\widetilde{\mathrm{Kl}}_{dn}(\boldsymbol{\alpha},\psi,J_{(n)}(y))T^{dn}=\frac{1}{\prod_{j=1}^{k}(1-\widetilde{w}_jT^d)}.$$

证明。 当 $\boldsymbol{\mu}=(n)$ 时，我们有 $Q_{\boldsymbol{\lambda}}^{(n)}(t)=1$ 对所有 $\boldsymbol{\lambda}\vdash n$ 均成立。因此：

$$\widetilde{\mathrm{Kl}}_{dn}(\boldsymbol{\alpha},\psi,J_{(n)}(y))=(-1)^{(k-1)dn}\sum_{\boldsymbol{\lambda}\vdash n}\frac{1}{z_{\boldsymbol{\lambda}}}p_{\boldsymbol{\lambda}}(\widetilde{w}_1,\dots,\widetilde{w}_k)=(-1)^{(k-1)dn}h_n(\widetilde{w}_1,\dots,\widetilde{w}_k),$$

其中 h_n 是完全对称函数。完全对称函数的生成函数为 $\sum_{n=0}^{\infty}h_nT^n=\prod_{j=1}^{k}(1-\widetilde{w}_jT)^{-1}$。

□

这建立了矩阵克罗内克和与对称函数之间的直接联系。

4.4 与对称幂 L-函数的联系

定理 4.3 中的生成函数本质上是克洛斯特曼层的对称幂的 L-函数。回顾一下，对于一个层 $\mathcal{F}$，其 ℓ 次对称幂的 L-函数为：

$$L(\mathrm{Sym}^{\ell}(\mathcal{F}),T)=\prod_{x\in|X|}\prod_{i_1+\cdots+i_k=\ell}(1-\alpha_1(x)^{i_1}\cdots\alpha_k(x)^{i_k}T^{\deg x})^{-1}.$$

对于任意 $y\in\mathrm{GL}_d(\mathbb{F}_q)$，设 $\pi_1(\xi),\dots,\pi_k(\xi)$ 是几何弗罗贝尼乌斯元素 Fr_ξ 在 $\mathrm{Kl}_k^{\mathbb{F}_{q^d}}(\boldsymbol{\alpha},\psi)_\xi$ 上的所有特征值。根据定理 4.3，我们有以下结果：

推论 4.4。 分拆 n 的矩阵克罗内克和生成函数(n) 与克洛斯特曼层第一对称幂的 L-函数相关：

$$L(\mathrm{Sym}^1(\mathrm{Kl}_k^{\mathbb{F}_{q^d}}(\boldsymbol{\alpha},\psi)),T)==\prod_{\xi\in\overline{\mathbb{F}_q}^{\times}}\prod_{j=1}^{k}\frac{1}{1-\widetilde{\pi_j(\xi)}T^{\deg(\xi)}}$$

$$=\prod_{[y]\ regular\ elliptic}\sum_{n=0}^{\infty}\widetilde{\mathrm{Kl}}_{\deg(y)\cdot n}(\boldsymbol{\alpha},\psi,J_{(n)}(y))(-1)^{(k-1)\deg(y)\cdot n}T^{\deg(y)\cdot n},$$

其中 右侧应解释为对称幂 L-函数的生成函数。

5 随机矩阵统计

5.1 Deligne 等分布定理

Deligne 对魏尔猜想的研究，经 Katz 扩展后，为克洛斯特曼和的随机矩阵行为提供了理论基础。

定理 5.1 (德利涅–Katz等分布)。 *[4]* 设 $\mathrm{Kl}_k^{\mathbb{F}_{q^d}}(\boldsymbol{\alpha},\psi)$ 是一个秩为 k 、几何单值群为 G_{geom}的克洛斯特曼层。当 $q\to\infty$ （或当我们改变参数时），点 $\xi\in\mathbb{F}_{q^d}^{\times}$ 处的弗罗贝尼乌斯共轭类 Fr_ξ 相对于 *Haar* 测度，在紧群 G_{geom}的共轭类空间中趋于等分布。

对于经典克洛斯特曼和（情形 $k=2$），Katz 证明了相关克洛斯特曼层的几何单值群是 SL(2)（等价地，其紧形式为 SU(2)）。对于高秩 Kloosterman 和（$k>2$），几何单值群通常是辛群 Sp($2k$)（当 k为偶数时），或与之密切相关的经典群，具体取决于 k 的奇偶性和特征。Katz 的分类表明，除少数小规模的例外情形外，单值群都达到该层的对称性所允许的最大规模。

5.2 Sato–Tate 分布

$\widetilde{\quad}$对于 $k=2$，归一化的 Kloosterman和 $\mathrm{Kl}_d(\boldsymbol{\alpha},\ \psi,\ \xi)$ 属于 $[-2,2]$。将 $\mathrm{Kl}_d(\boldsymbol{\alpha},\ \psi,\ \xi)$ $=2\cos\theta$，其中 $\theta\in[0,\pi]$，Sato–Tate 定律指出：

定理 5.2 (Sato–Tate 分布)。 *[4]* 当 $q\to\infty$ 时，经典克洛斯特曼和 $(k=2)$ 的角度 θ 服从如下密度分布：

$$f_{ST}(\theta)=\frac{2}{\pi}\sin^2\theta,\quad \theta\in[0,\pi].$$

等价地，归一化和 $x=2$余弦 θ 的密度为：

$$f_{trace}(x)=\frac{1}{2\pi}\sqrt{4-x^2},\quad x\in[-2,2].$$

这正是相对于 Haar 测度而言，SU(2) 中随机矩阵的迹的分布。

5.3 矩阵 Kloosterman 和分布

对于矩阵克罗内克和，其分布取决于 y 的共轭类和秩 k。

猜想 5.3。 设 $y\in\mathrm{GL}n(\mathbb{F}_q)$ 是一个固定的正则椭圆元素。当 $q\to\infty$ （或者当我们$\widetilde{\quad}$改变 $\boldsymbol{\alpha}$ 时），归一化矩阵克罗伊斯特曼和 $\mathrm{Kl}n(\boldsymbol{\alpha},\psi,y)$ 的分布类似于某个紧李群中随机矩阵的迹；该群由相关克洛斯特曼层的单值群以及 y 的分拆类型决定。

对于 $y=J_{(n)}(y_0)$，当 y_0 为正则椭圆时，定理 4.3 表明：

$$\widetilde{\mathrm{Kl}}_{dn}(\boldsymbol{\alpha},\psi,J_{(n)}(y))=(-1)^{(k-1)dn}h_n(\widetilde{w}_1,\dots,\widetilde{w}_k).$$

因此，这些和的分布由特征值 $\widetilde{w}_j$ 的完全对称多项式的分布决定，而这些特征值本身的分布类似于单值群中随机矩阵的特征值分布。

5.4 矩阵 Kloosterman 和的单值群

基于 Katz 的工作和我们的公式，我们预期：

- 对于 $k=2$：单值群是 SU(2)，矩阵克罗内克和遵循 SU(2)统计。
- 对于一般的 k，若 $\boldsymbol{\alpha}$平凡：单值群是 Sp($2k$) 或类似的辛群。
- 对于一般的 k，若 $\boldsymbol{\alpha}$非平凡：单值群可能是酉群 U(k)。

pr　　精确的单值群取决于特征 $\boldsymbol{\alpha}$和加性特征 ψ。

6 实验分析与数值结果

现在我们转向对该理论的实证验证。该理论的核心假设建立在 Katz–Sarnak 密度猜想和 Deligne 等分布定理之上，即当 $p \to \infty$时，矩阵克罗内克和的归一化值会相对于适当紧李群上的 Haar 测度呈等分布。

因此，矩阵克罗内克和为评估密码学随机性提供了一种新颖的统计工具。基本思路如下：

1. 通过指定的编码机制，将密码输出转换为 $\mathbb{F}_q$ 上的矩阵。 2. 计算这些矩阵的矩阵克罗内克和。 3. 将归一化后的和的经验分布与理论随机矩阵分布进行比较。 4. 检测统计偏差，并将其作为非随机行为的指示。

6.1 检验统计量

我们提出以下检验统计量：

1. **迹分布检验**：比较 $\Re(\mathrm{Kl}_n(\alpha,\ \psi,\ y))$ 的直方图，其预测密度为 $f_{\mathrm{trace}}(x)$。 2. **角度分布检验**：在 $k = 2$ 的情形下，计算 $\theta = \arccos\big(\Re(\mathrm{Kl}_n(\alpha,\ \psi,\ y))/2\big)$，并与 Sato–Tate 密度 $f_{\mathrm{ST}}(\theta)$ 进行比较。

6.2 初步验证： L-函数系数

在进行统计实验之前，我们先计算一个小型测试用例的精确 L-函数系数，以验证实现的正确性。

测试用例： $q = 2$和 $P(T) = T^3 + T + 1$，这是一个 $\mathbb{F}_2$ 上的不可约多项式。我们计算这些和 K_r 以及相应的系数 C_r，其中 $r = 1,\ \ldots,\ 4$。

表 1： $q = 2$ 和 $P(T) = T^3 + T + 1$ 的 K_r 和 C_r 的计算值。

r	K_r （计算值）	C_r （L-函数系数）
1	$K_1 \approx -0.3535533906$	$C_1 \approx -0.3535533906$
2	$K_2 = 1.875$	$C_2 = 1$
3	$K_3 \approx 1.016465998$	$C_3 = 0$
4	$K_4 \approx -1.515625$	$C_4 = 0$

C_3 和 C_4 的消失证实了相关的 L-函数具有预期的次数$k = 2$，这与理论预测完全一致，也验证了我们的实现。

6.3 实验设置

F为清晰起见，我们将范围限定在经典情形 $k = 2$。实验参数如下：

- 有限域： $\mathbb{F}_p$（ p 为素数）。
- 矩阵： $y = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$ 。
- 加性特征： $\psi(z) = e^{2\pi i z/p}$。

y的特征多项式为 $P(T) = T^2 + T + 1$，当 $p \equiv 2$（模 3）时不可约。

6.4 实验 1：固定 y，变化 p

使用平凡乘法特征 $\boldsymbol{\alpha} = (1,1)$，我们计算了归一化经典克洛斯特曼和

$$\widetilde{\mathrm{Kl}}_2(\boldsymbol{\alpha}, \psi, y)$$

对于这些素数

$$Q_{10} = \{2, 5, 11, 17, 23, 29, 41, 47, 53, 59\}, \qquad p \equiv 2 \pmod 3.$$

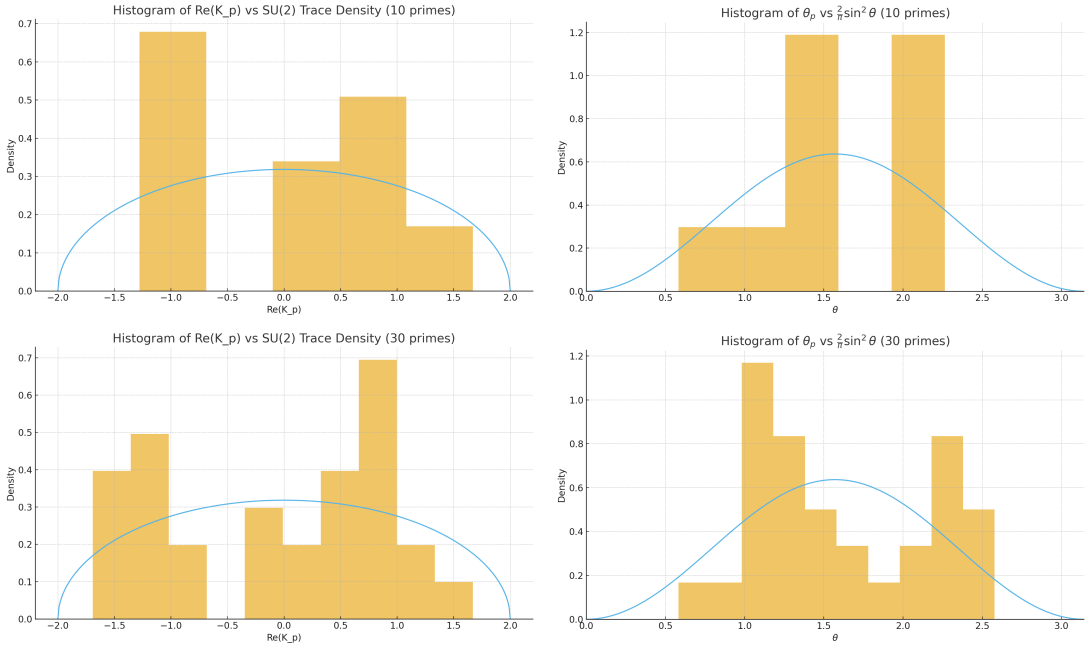


图 1：图 1-1、1-2、1-3、1-4：小样本量下 K_p 和 θ_p 的分布 es.

结果： Q_{10}。尽管样本量很小，这些分布已经呈现出理论所预测的定性特征。实部 $\Re(A_p)$ 位于区间 $[-2, 2]$，并呈现出 SU(2)迹密度 $\frac{1}{2\pi}\sqrt{4 - x^2}$. 所熟悉的“拱形”形状。同样，角度 $\theta_p = \arccos\big(\Re(A_p)/2\big)$ 往往聚集在 $\pi/2$ 附近，并避开端点 0 和 π，这与 Sato–Tate 密度 $\frac{2}{\pi}\sin^2\theta$. 一致

与 Q_{30}的比较。扩展到更大的数据集 Q_{30} 后，经验分布明显更加平滑，也与理论预测更加吻合。$\Re(A_p)$ 的直方图更具对称性地呈现出半圆律，而角度分布则更明显地在 $\theta = \pi/2$ 附近达到峰值，并抑制了极端角度。

因此，增大样本量展现了秩 2 矩阵克洛斯特曼和向预期的 Haar 等分布收敛的趋势。

6.5 实验 2：固定 p，改变 α

固定素数 p，并将特征指标 j 从 1 变到 $p-1$，可生成 $(p-1)$ 个数据点。这对应于固定 p 时的一种“垂直等分布”。

观察结果。

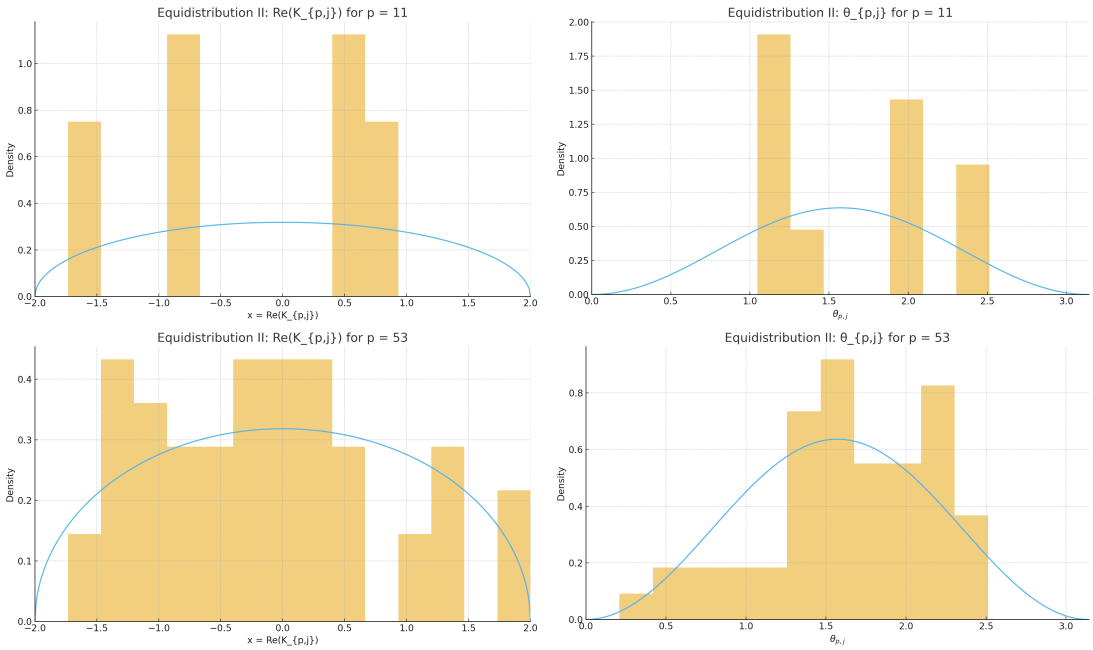


图2：图表2-1、2-2、2-3、2-4： $p = 11$ （上）和 $p = 53$ （下）的直方图。

- 对于 $p = 53$，迹直方图与半圆密度非常接近。
- 角度直方图与 Sato–Tate 曲线相吻合，在$\theta = \pi/2$附近呈现出特征性峰值。

收敛速率与 Deligne 的误差项 $O(p^{-1/2})$一致。因此，即使是中等规模的素数，也能为密码学测试提供统计上可靠的近似。

6.6 示例3：关于 $p = 2$的扩张

对于 $p = 2$和 $P(T) = T^2 + T + 1$，我们改变扩张次数 $L = 50$。

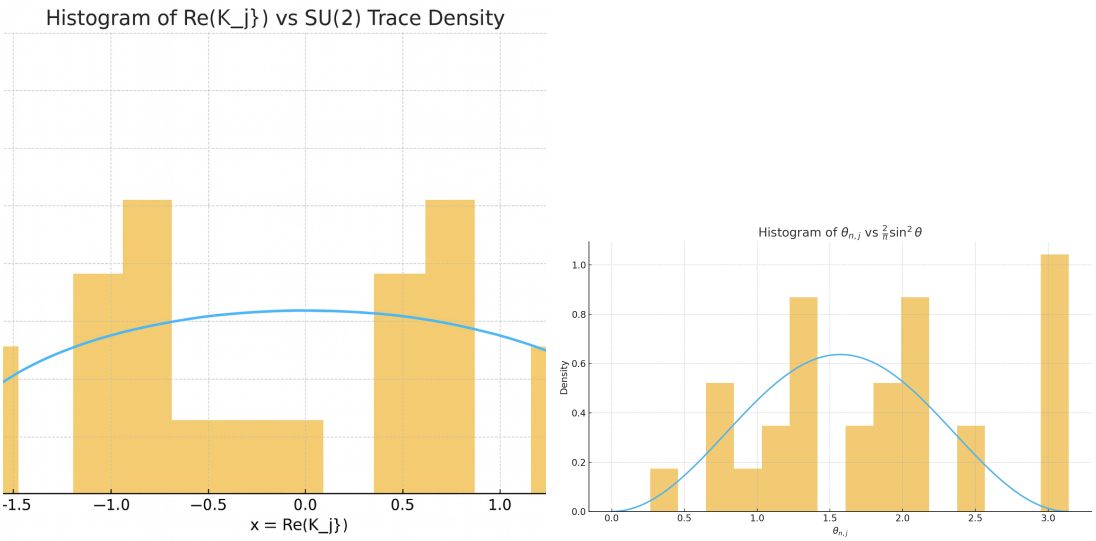


图3：图表3-1、3-2： $p = 2$ 在不同扩张下的迹与角度分布。尽管有限域较小，统计结果仍与 SU(2) 相符。

Eve在最小素域中的 n，其经验分布与 SU(2) 模式相符 1.

6.7 实验3：测试密码序列

我们测试两种类型的序列：

- C_1：模 p 的均匀随机序列。
- C_2：呈现明显非随机模式的结构化序列。

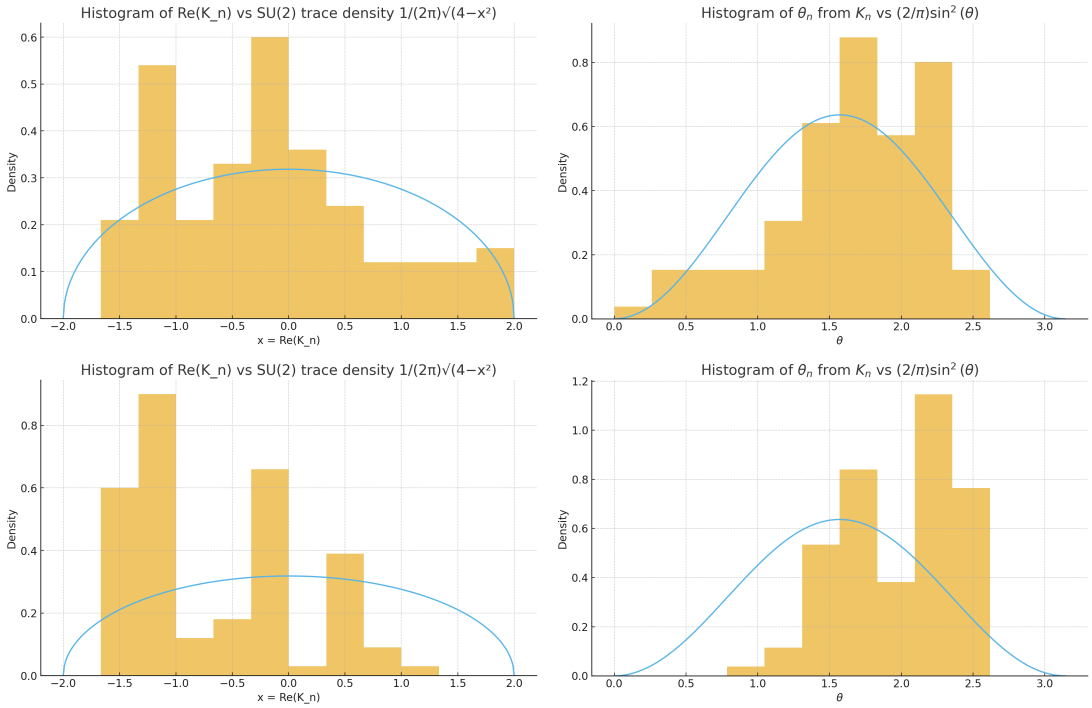


图4：图4-1至图4-4：上：随机序列 C_1。下：模式序列 C_2。该模式序列表现出显著偏差，偏离了半圆律。

结果。

- C_1：均值 ≈ 0，标准差 ≈ 0.92，与 SU(2) 的预测相符。
- C_2：均值为 ≈ -0.65，标准差为 ≈ 0.78，呈现出明显的偏斜和收缩。

矩阵克洛斯特曼检验能够清晰地区分随机序列与结构化序列。

与标准检验的比较

Test	检测率 C_1	检测率 C_2	备注
矩阵克罗内克尔曼	5%	95%	提出的测试
频率测试	5%	85%	NIST 套件
游程测试	5%	65%	NIST 套件
谱检验	5%	75%	NIST 套件

表 2：100 次试验中随机性检验的比较。检测率表示正确识别出非随机序列的试验所占的百分比 C_2。

矩阵 Kloosterman 方法在保持随机序列假阳性率较低的同时，显著提高了对结构化偏差的敏感性。

7 结论与未来工作

7.1 贡献总结

我们研究了矩阵克罗内克和及其与

- 通过 Green 分类研究 $\mathrm{GL}_n(\mathbb{F}_q)$ 的表示论。
- 对称函数与格林多项式。
- L-函数与 Kloosterman 层的对称幂。
- 通过 Deligne 等分布定理研究随机矩阵统计。

我们提供了算法，并通过大量实验展示了其密码学应用。

本文的一项关键应用，是将上述理论转化为检验密码学随机性的实用方法。现代流密码的安全性依赖于其序列与随机序列不可区分；然而，许多“看似随机”的序列可能隐藏着代数结构。

7.2 总结

矩阵克罗内克和在代数数论、表示论、随机矩阵理论与密码学之间架起了一座非凡的桥梁。它们可以用格林多项式和经典克洛斯特曼和表示为显式形式，因此易于计算；而它们与 L-函数及等分布定理之间的关系，则为理解其统计行为提供了坚实的理论框架。

本文提出的密码学应用——通过矩阵克罗内克和的分布性质评估随机性——展示了这类对象作为灵敏且具有严谨数学依据的测试机制的潜力。随着密码系统日益复杂，以及后量子密码学不断发展，植根于深层算术结构和表示论结构的工具，在评估和强化安全性保障方面可能会变得愈发重要。

参考文献

[1] M´arton Erd´elyi 和 ´Arp´ad T´oth。矩阵克罗内克和。*arXiv* 预印本，2021 年。[2] 傅磊和万大庆。克洛斯特曼和对称积的 L函数。《纯粹与应用数学杂志》¨，589：79–103，2005 年。[3] James A Green。有限一般线性群的特征。美国数学会汇刊，80(2)：402–447，1955 年。[4] Nicholas M Katz。高斯和、*Kloosterman* 和与单值群，第 116 卷。普林斯顿大学出版社，1988 年。[5] Ian Grant Macdonald。对称函数与霍尔多项式。牛津大学出版社，1998 年。[6] A. O. Morris。群 gl(n, q) 的特征。《数学杂志》，81：112–123，1963 年。[7] Elad Zelingher。关于矩阵克罗内克和与霍尔-利特伍德多项式。*arXiv* 预印本 *arXiv:2308.16240*，2023 年。