Joint distribution of inverses in matrix groups over finite fields

Corentin Perret-Gentil

Abstract

We study the joint distribution of the solutions to the equation $gh = x$ in $G(F_p)$ as $p \to \infty$, for any fixed $x \in G(\mathbb{Z})$, where $G = \text{GL}_n, \text{SL}_n, \text{Sp}_{2n}$ or $\text{SO}^\pm_n$. In the special linear case, this answers in particular a question raised by Hu and Li, and improves their error terms. Similar results are derived in certain subgroups, and when the entries of $g, h$ lie in fixed intervals. The latter shows for example the existence of $g \in \text{GL}_n(F_p)$ such that $g, g^{-1}$ have all entries in $[0, c_n p^{1-1/(2n^2+2)+\epsilon}]$ for some absolute constant $c_n > 0$. The key for these results is to use Deligne's extension of the Weil conjectures on a sheaf on $G$, along with the stratification theorem of Fouvry, Katz and Laumon, instead of reducing to bounds on classical Kloosterman sums.

Mathematics Subject Classification: 11C20, 11K36, 11T24, 11L05

1 Introduction

Throughout, we let $n \geq 1$ be an integer, unless specified otherwise.

1.1 The cases of $(\mathbb{Z}/n)^\times$ and $\text{GL}_n(F_p)$

Following several similar results for the group $(\mathbb{Z}/n)^\times$ (see [16] for a survey), Hu and Li [13] have shown that for the matrix group $G = \text{GL}_n(F_p)$ and any fixed $x \in G$, the solutions to the equation $gh = x$ ($g, h \in G$) are uniformly distributed in $[0, 1]^{n^2} \times [0, 1]^{n^2}$ as $p \to \infty$, with respect to the embedding

$$
\eta : M_n(F_p) \to [0, 1]^{n^2}
$$

$$
g = (g_{ij})_{i,j} \mapsto \left(\{g_{ij}/p\}_{i,j}\right) \quad (1)
$$

where $\{\cdot\}$ denotes the fractional part. In particular, the entries of a nonsingular matrix and its inverse are jointly uniformly distributed. More precisely, they obtain a bound for the discrepancy.

Their main tools are bounds for matrix analogues of Kloosterman sums obtained in [8] by reducing to classical Kloosterman sums.

1.2 Special linear groups

At the end of their paper, Hu and Li note that this does not hold for $G = \text{SL}_2(F_p)$, but conjecture that there should be joint uniform distribution whenever $n \geq 3$. We positively answer this by showing:
Theorem 1.1 Let $G$ be
\[ GL_n \quad (\text{for } n \geq 2) \quad \text{or} \quad SL_n \quad (\text{for } n \geq 3), \]
and let $x \in G(\mathbb{Z})$. As $p \to \infty$, the elements
\[ A_x(g) = \begin{pmatrix} g & g^{-1}x \end{pmatrix} \in M_n(\mathbb{F}_p) \times M_n(\mathbb{F}_p) \quad (g \in G(\mathbb{F}_p)) \]
are uniformly distributed in $\Omega = [0, 1]^{n^2} \times [0, 1]^{n^2}$ with respect to the embedding $\eta$ in (1).
More precisely, for every product of intervals $R$ in $\Omega$, the number
\[ \left| \left\{ g \in G(\mathbb{F}_p) : \eta(A_x(g)) \in R \right\} \right| \]
\[ = \begin{cases} \frac{\text{meas}(R)}{|G(\mathbb{F}_p)|} & : G = GL_n, \\ \frac{O_n \left( \frac{(\log p)^{n^2+1}}{\sqrt{p}} \right)}{|G(\mathbb{F}_p)|} & : G = SL_n, \end{cases} \]
as $p \to \infty$, where $\text{meas}$ denotes the Lebesgue measure. The implied constants depend only on $n$. This also holds with $R \subset \Omega$ an arbitrary convex set if the errors are replaced by their $1/(2n^2)$th powers.

Remark 1.2 This improves the error terms of [13], which are for example $p^{-1/2(2n^2+1)}$ when $G = GL_n$. The bulk of the improvement comes from bounding nontrivially the $1/r(h)$ factors appearing in the Erdős–Turán–Koksma, which had been overlooked, as suggested by an anonymous referee.

Notation 1.3 We recall that for two complex-valued functions $f, g$, we write $f = O_n(g)$ or $f \ll_{n} g$ if there exists a constant $C_n > 0$, depending only on the variable $n$, such that $|f| \leq C_n g$.

1.2.1 Generalization to certain subgroups
The following variant shows that equidistribution of $A_x(g)$ still holds in certain subgroups of $GL_n$.

Theorem 1.4 Let us consider the setting of Theorem 1.1 for $G = GL_n$. For $f \in \mathbb{F}_p[G]^\times$ a nonvanishing nonconstant function and $U \leq \mathbb{F}_p^\times$ a subgroup, let
\[ H = f^{-1}(U) = \left\{ g \in G(\mathbb{F}_p) : f(g) \in U \right\}. \]
For every product of intervals $R \subset \Omega$, we have
\[ \left| \left\{ g \in H : \eta(A_x(g)) \in R \right\} \right| = \frac{\text{meas}(R)}{|H|} + O_n \left( \frac{\sqrt{p}}{|U|} \left( \log \frac{|U|}{\sqrt{p}} \right)^{n^2+1} \right) \]
as $p \to \infty$. The set $R$ can be replaced by an arbitrary convex set if the error term is replaced by its $1/(2n^2)$th power.

Example 1.5 One may take $H = \{ g \in GL_n(\mathbb{F}_p) : \det(g) \in \mathbb{F}_p^{\times r} \}$ with $r = o(\sqrt{p})$, where $\mathbb{F}_p^{\times r}$ denotes the set of $r$-powers in $\mathbb{F}_p^{\times}$.

Remarks 1.6 (1) It is a theorem of Rosenlicht (see e.g. [4]) that if $G$ is a connected affine algebraic group, then $f/f(1) \in \mathbb{F}_p[G]^\times$ must be a one-dimensional character (i.e. a character of the abelianization); in particular, the set $H$ in Theorem 1.4 is a normal subgroup.
In particular, we cannot get a nontrivial version of Theorem 1.4 for $\text{SL}_n(\mathbb{F}_p)$: since the latter is perfect for $p > 3$, $f$ must be constant. The classification of maximal subgroups of $\text{SL}_n(\mathbb{F}_p)$ [2] also shows that the restriction on the index is too stringent.

Using the same techniques, it should be possible to obtain Theorem 1.4 also when $H \leq \text{GL}_n(\mathbb{F}_p)$ is any normal subgroup of index $< \sqrt{p}$. However, this requires additional technicalities that we do not wish to pursue here (see Remark 2.8 for further comments).

1.3 Other classical groups

1.3.1 Symplectic groups

On the other hand, it is clear that Theorem 1.1 does not hold for $G = \text{Sp}_n$ ($n \geq 2$ even). Indeed, if

$$g = \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix} \in \text{Sp}_{2n}(\mathbb{F}_p), \text{ then } g^{-1} = \begin{pmatrix} g_4^t & -g_2^t \\ -g_3^t & g_1^t \end{pmatrix}$$

(with respect to the standard symplectic form, where $g_i \in M_{2n}(\mathbb{F}_p)$). Hence, the obstruction for $\text{SL}_2$ can be viewed as coming from the fact that $\text{SL}_2(\mathbb{F}_p) = \text{Sp}_2(\mathbb{F}_p)$.

1.3.2 Special orthogonal groups

Let $\Phi_1 \in \text{GL}_n(\mathbb{F}_p)$ be in one of the two equivalence classes of nonsingular symmetric bilinear forms on $\mathbb{F}_p^n$. Since $g^{-1} = \Phi g^f \Phi^{-1}$ for $g \in \text{GO}(\Phi)$, Theorem 1.1 does not hold either in this case. Actually, when $n = 2$, the elements of the special orthogonal group corresponding to the form $\text{diag}(a, 1)$ ($a \in \mathbb{F}_p^{\times}$) are themselves not uniformly distributed in $[0, 1]^4$ with respect to the embedding (1), since they are of the form $(a \alpha, a \alpha)$.

1.4 Distribution of elements

Nonetheless, the elements themselves are still uniformly distributed in all cases except $\text{SO}_2^\pm$, as in [13, Theorems 1.5–1.6] for $\text{GL}_n$ and $\text{SL}_n$.

**Theorem 1.7** For $n \geq 1$, let $G$ be\(^1\)

\[
\text{GL}_n, \text{ SL}_n, \text{ Sp}_n \text{ (n even), or } \text{ SO}_{n,1} \text{ (n \geq 3)}.
\]

As $p \to \infty$, the elements $g \in G(\mathbb{F}_p)$ are uniformly distributed in $\Omega = [0, 1]^{n^2}$ with respect to the embedding (1). More precisely, for every product of intervals $R$ in $\Omega$,

$$\frac{|\{g \in G(\mathbb{F}_p) : \eta(g) \in R\}|}{|G(\mathbb{F}_p)|} = \text{meas}(R) + O_n \left( \frac{(\log p)^{n^2 - \dim G + 1}}{\sqrt{p}} \right)$$

as $p \to \infty$. This also holds with $R \subset \Omega$ an arbitrary convex set if error term is replaced by its $1/(2n^2)$th power.

**Remark 1.8** Note that the exponent of the logarithms in the error term is 2, 3, $(n^2 + 1)/2$ if $G = \text{GL}_n$, $\text{SL}_n$ or $\text{Sp}_n$ respectively. Theorem 1.7 improves the errors terms:

- in [13], handling $\text{GL}_n$ and $\text{SL}_n$ using [12], which are $p^{-n/(n^2+1)}$.
- in Theorem 1.1 for the joint distribution.

\(^1\)In what follows, we let $\text{SO}_{n,1}$ be the special orthogonal group corresponding to the form given by the identity matrix $I_n$; in other words, $\text{SO}_{n,1}(\mathbb{F}_p)$ is the special orthogonal group with square determinant, i.e. $\text{SO}_n(\mathbb{F}_p)$ if $n$ is odd, and if $n$ is even, $\text{SO}_n^+(\mathbb{F}_p)$ if $p \equiv \pm 1 \pmod{4}$ respectively.
In the same vein as Theorem 1.4, we get the following generalization:

**Theorem 1.9** Under the assumptions of Theorem 1.7, let $H$ be as in Theorem 1.4. Then, for any product of intervals $R \subset \Omega$,

$$\frac{|\{g \in H : n(g) \in R\}|}{|H|} = \text{meas}(R) + O_p \left( \frac{\sqrt{p}}{|U|} \left( \log \frac{|U|}{\sqrt{p}} \right)^{n^2 - \dim G + 1} \right).$$

### 1.5 Distribution with entries in intervals

A related question in $G = (\mathbb{Z}/n)^\times$ is the distribution of the solutions to $gh = x$, for some fixed $x \in G$, when $1 \leq g, h \leq p - 1$ lie in fixed intervals. It is a conjecture (see [16, Section 3.1]) that for any $\varepsilon > 0$ and $p$ large enough, there exist integers $g, h$ such that $gh \equiv 1 \pmod{p}$ with $|g|, |h| \leq p^{1/2+\varepsilon}$. The best current result seems to be $|g|, |h| \ll p^{3/4}$, due to Garaev (note the absence of a logarithmic factor).

In matrix groups, we can similarly fix the entries of the matrices in intervals, yielding the following:

**Theorem 1.10** Let $G$ be as in Theorem 1.1. For a prime, let $E, F \subset [0, p - 1]^{n^2}$ be products of intervals. Then, for any $x \in G(\mathbb{Z})$, viewing $M_n(\mathbb{F}_p)$ embedded in $[0, p - 1]^{n^2}$, the density

$$\frac{|\{g \in G(\mathbb{F}_p) : g \in E \text{ and } g^{-1}x \in F\}|}{|G(\mathbb{F}_p)|} \tag{3}$$

is given by

$$\frac{\text{meas}(E \times F)}{p^{2n^2}} + O_p \left( \frac{(\log p)^{2n^2}}{p^{\dim G / 2}} \left( 1 + \left( \sum_{1 \leq k, l \leq n} \frac{\text{meas}(E_{kl})}{\sqrt{p}} \right)^{\dim G - 1} \right) \right),$$

if $E = \prod_{1 \leq k, l \leq n} E_{kl}$.

**Corollary 1.11** Let $G$ be as in Theorem 1.1 and let $p$ be a prime. For any $\varepsilon > 0$ and $x \in G(\mathbb{Z})$, there exist $g, h \in G(\mathbb{F}_p)$ such that $gh = x$ and whose entries, seen in $[0, p - 1]$, are all

$$\ll_{n, \varepsilon} \begin{cases} \frac{1}{p^{1 - \frac{1}{2(4n^2 + 1)}} + \varepsilon} : G = \text{GL}_n & \\ \frac{1}{p^{1 - \frac{1}{2(4n^2 + 2)}} + \varepsilon} : G = \text{SL}_n & \end{cases}.$$

We also refer the reader to [1] for related questions concerning matrices, and to [11], [9, Corollary 1.5] for general results about points on varieties in hypercubes.

### 1.6 Higher-dimensional variant

Using the same techniques, we can get an analogue of Theorem 1.1 for the uniform distribution of solutions to

$$g_1 \cdots g_r = x \quad (g_i \in G(\mathbb{F}_p))$$

for any $r \geq 2$ and $x$ fixed:

**Theorem 1.12** Let $G$ and $x$ be as in Theorem 1.1, and let $r \geq 2$ be an integer. As $p \to \infty$, the elements

$$A_x(g) = (g_1, \ldots, g_{r-1}, (g_1 \cdots g_{r-1})^{-1}x) \in M_n(\mathbb{F}_p)^r \quad (g \in G(\mathbb{F}_p)^{r-1})$$
are uniformly distributed in $\Omega = [0, 1]^{m^2}$ with respect to the embedding (1). More precisely, for every product of intervals $R$ in $\Omega$,

$$\left| \{ g \in G(F_p)^{r-1} : \eta(A_n(g)) \in R \} \right| = \text{meas}(R) + \begin{cases} O_n, r \left( \frac{(\log p)^{2^2+1}}{\sqrt p} \right) : G = \text{GL}_n \\ O_n, r \left( \frac{(\log p)^{2^2+2}}{\sqrt p} \right) : G = \text{SL}_n \end{cases}$$

as $p \to \infty$. This also holds with $R \subset \Omega$ an arbitrary convex set if the error terms are replaced by their $1/(2n^2)$th powers.

For the sake of clarity, we focus on proving the two-dimensional versions, and indicate the changes necessary for Theorem 1.12 at the end.

2 Tools

2.1 Equidistribution and discrepancy

For the following results, we refer the reader to [7, Chapter 1]. Throughout, we let $\Omega = [0, 1]^k$ for some integer $k \geq 1$.

**Definition 2.1** The discrepancy of a sequence $(x_n)_{n \geq 1}$ in $\Omega$ is

$$D_N(x_n) = \sup_{I \subset \Omega} \left| \left\{ n \leq N : x_n \in I \right\} \right| - \frac{\text{meas}(I)}{N},$$

where $I$ runs over all products of intervals in $\Omega$.

**Proposition 2.2** A sequence $(x_n)_{n \geq 1}$ in $\Omega$ is uniformly distributed if and only if $D_N(x_n) = o(1)$, and we have the Erdős–Turán–Koksma inequality: for any integer $T \geq 1$

$$D_N(x_n) \leq \left( \frac{3}{2} \right)^k \left( \frac{2}{T + 1} + \sum_{0 < |h| \leq k} \frac{1}{r(h)} \left| \frac{1}{N} \sum_{n \leq N} e(h \cdot x_n) \right| \right),$$

where $r(h) = \prod_{i=1}^k \max(1, |h_i|)$, $e(z) = \exp(2\pi iz)$.

**Proof** See [7, Theorem 1.6, Theorem 1.21] respectively. □

**Remark 2.3** If the sets $I$ in Definition 2.1 are replaced by arbitrary convex subsets, this yields the isotropic discrepancy $J_N(x_n)$, which satisfies $J_N(x_n) \ll_k D_N(x_n)^{1/k}$ (see [7, Theorem 1.12]).

By Weyl's criterion, $(x_n)_{n \geq 1}$ is equidistributed in $\Omega$ if and only if

$$\sum_{n \leq N} e(h \cdot x_n) = o(N)$$

for every nonzero $h \in \mathbb{Z}^k$, so the Erdős–Turán–Koksma inequality quantifies the equidistribution from the rate of decay of these exponential sums.

2.2 Exponential sums on matrix groups

The bounds of [8] used in [13] proceed by reducing to classical Kloosterman sums on $\mathbb{F}_p$, through averaging and interchanging summations. Instead, we use Deligne's extension of his proof of the Weil conjectures [6] to work directly with the sums over the matrix groups. This allows a precise control of when the sums exhibit cancellation.
Proposition 2.4 Let $G$ be as in Theorem 1.7, let $f \in \mathbb{F}_p(G)$ be a rational function on $G$, let $\psi : \mathbb{F}_p \to \mathbb{C}^\times$ be a nontrivial character, let $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ be a multiplicative character, and let $f_1 \in \mathbb{F}_p[G]^\times$ be a nonvanishing nonconstant function. Then
\[
\frac{1}{|G(\mathbb{F}_p)|} \sum_{\substack{g \in G(\mathbb{F}_p) \\ f(g) \neq \infty}} \psi(f(g)) \chi(f_1(g)) = \delta + O(p^{-1/2})
\]
with $\delta = 1$ if $f$ and $\chi \circ f_1$ are constant on $\{g \in G(\mathbb{F}_p) : f(g) \neq \infty\}$, $\delta = 0$ otherwise. The implied constant depends only on $n$, $\deg(f)$ and $\deg(f_1)$.

Proof The result is obvious if $f$ and $\chi \circ f_1$ are constant on $G(\mathbb{F}_p)$, so we may assume it is not the case and prove (4) with $\delta = 0$. Let $\ell \neq p$ be an auxiliary prime. Following [5, Exposé 6], let $L_0 := f^* \mathcal{L}_\psi = \mathcal{L}_{\psi(f)}$ (resp. $L_1 := f_1^* \mathcal{L}_\chi = \mathcal{L}_{\chi(f_1)}$) be the restriction to $G$ of the Artin–Schreier (resp. Kummer) sheaf on $\mathbb{A}_{G, p}^2$ corresponding to $\psi \circ f$ (resp. $\chi \circ f_1$), and let $L = L_0 \otimes L_1$ be the middle tensor product. These can be seen as representations $\rho_0, \rho_1, \rho = \rho_0 \otimes \rho_1 : \text{Gal}(\mathbb{F}_p(G)_{\text{sep}}/\mathbb{F}_p(G)) \to \overline{\mathbb{Q}}_\ell^\times$, such that at every point $g \in G(\mathbb{F}_p) \subseteq \mathbb{F}_p^n$ with $f_1(g) \neq \infty$, there is a Frobenius element $\text{Frob}_g$ with
\[
\iota \rho_0(\text{Frob}_g) = \psi(f(g)), \quad \iota \rho_1(\text{Frob}_g) = \chi(f_1(g)), \quad \iota \rho(\text{Frob}_g) = \psi(f(g)) \chi(f_1(g))
\]
for an embedding $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$. Hence, the left-hand side of (4) is
\[
\frac{1}{|G(\mathbb{F}_p)|} \sum_{\substack{g \in G(\mathbb{F}_p) \\ f(g) \neq \infty}} \iota \rho(\text{Frob}_g).
\]
By the Grothendieck–Lefschetz trace formula [5, Exposé 6, (1.1.1)], this is
\[
\frac{1}{|G(\mathbb{F}_p)|} \sum_{i=0}^{2 \dim G} (-1)^i \text{tr}(\text{Frob}_p | H^i_c(U \times \mathbb{F}_p, L)),
\]
for $U$ the open in $\mathbb{A}_{G, p}^2$ where $L_0$ is lisse (i.e. the complement of the zero set of $f$).

By Deligne’s extension of the Riemann hypothesis over finite fields [6, Théorème 2] (see also [5, Théorème 1.17]), the eigenvalues of the Frobenius acting on $H^i_c(U \times \mathbb{F}_p, L)$ are $p$-Weil numbers of weight at most $i$. If the one-dimensional sheaf $L$ is not geometrically trivial, the coinvariant formula implies that $H^2 \dim G(U \times \mathbb{F}_p, L) = 0$, so that the left-hand side of (4)
\[
\ll p^{-1/2} \sum_{i=0}^{2 \dim G-1} \dim H^i_c(U \times \mathbb{F}_p, L).
\]
By [14, Theorem 12], the sum of Betti numbers in the error term is bounded by a quantity depending only on $n$, $\deg(f)$ and $\deg(f_1)$, for example
\[
3(2 + \max(\deg(f), n+2) + \deg(f_1))^3 p \right)
\]
Thus, it suffices to show that $L$ is not geometrically trivial to conclude. If it is not the case, since $L_1$ is tame everywhere and $L_0$ is not unless it is geometrically trivial, we then have that both $L_1$ and $L_0$ are geometrically trivial. Since $\pi_1(U, \overline{\eta})/\pi_1(U, \overline{\eta}) \cong \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, it follows as in [10, Proposition 8.5] that $\psi \circ f$ and $\chi \circ f_1$ are constant on $U(\mathbb{F}_p)$. The former implies that $f$ is of the form $f_2^p - f_2 + c$ for some $c \in \mathbb{F}_p^\times$ and $f_2 \in \mathbb{F}_p(G)$, whence $f$ is constant on $U(\mathbb{F}_p)$ as well. □
Remark 2.5 The function $f = \det^\rho - \det$ is not a counterexample to the theorem since, while not constant on $\text{GL}_n(\mathbb{F}_p)$, it is constant on $\text{GL}_n(\mathbb{F}_p)$. Alternatively, note that the implied constant in (4) depends on $\deg(f) = p$. In the following, we will always consider cases where $\deg(f)$, $\deg(f_1)$ are independent from $p$. Similarly, $f_1 = \det^{\text{ord}} \chi$ is not a counterexample since $\chi \circ f_1$ is constant on $\Gamma(\mathbb{F}_p)$.

2.2.1 Improved error terms via stratification

The anonymous referee of Hu and Li’s paper indicated (see [13, Section 4]) that the stratification results of Laumon, Katz and Fouvry may be employed to answer the conjecture for $\text{SL}_n$ ($n \geq 3$; see Sect. 1.2). This is not necessary to obtain uniform distribution (Proposition 2.4 suffices), but we can indeed use the powerful results of Fouvry–Katz [9] to improve the error terms.

Definition 2.6 We consider the inner product on $M_n(\mathbb{F}_p)$ given by

$$g_1 \cdot g_2 := \text{tr}(g_1^t g_2) = \sum_{1 \leq i,j \leq n} (g_1)_{ij} (g_2)_{ij} \quad (g_1,g_2 \in M_n(\mathbb{F}_p)).$$

The following provides a better bound on average over shifts. We will see in Sect. 3 that these types of sums precisely arise when bounding discrepancies of the sequences we consider.

Proposition 2.7 Under the hypotheses and notations of Proposition 2.4, assume that $f$ is obtained by reduction of a morphism of $\mathbb{Z}$-schemes $\hat{f} : G \to \mathbb{A}_\mathbb{Z}^{1}$. If $\delta = 0$, then, for every integer $2 \leq T < p$,

$$\sum_{h \in M_n(\mathbb{Z})} \frac{1}{|h|} \left| \frac{1}{|G(\mathbb{F}_p)|} \sum_{g \in G(\mathbb{F}_p)} \psi(f(g) + h \cdot g) \chi(f_1(g)) \right| \ll \frac{(\log T)^{n^2 - \dim G + 1}}{p^{1/2}},$$

where the implied constant depends only on $n$ and $\deg(\hat{f})$.

Proof By [9, Theorem 1.1, Section 3], there exist closed subschemes $X_j \subset \mathbb{A}_\mathbb{Z}^{n^2}$ ($0 \leq j \leq n^2$) of relative dimension $\leq n^2 - j$, depending on $G_\mathbb{Z}$ and $\hat{f}$, such that

$$X_{n^2} \subset X_{n^2-1} \subset \cdots \subset X_1 \subset X_0 \equiv \mathbb{A}_\mathbb{Z}^{n^2}$$

and

$$\frac{1}{|G(\mathbb{F}_p)|} \sum_{g \in G(\mathbb{F}_p)} \psi(f(g) + h \cdot g) \chi(f_1(g)) \ll \frac{p^{\frac{j-1}{2}}}{|G(\mathbb{F}_p)|^{1/2}},$$

(7)

if $h \in M_n(\mathbb{F}_p) \setminus X_j(\mathbb{F}_p)$, identifying $M_n(\mathbb{F}_p)$ with $\mathbb{F}_p^{n^2}$ (in the case of $G = \text{GL}_n$, the ambient space is $\mathbb{A}_\mathbb{Z}^{n^2+1}$, with an additional coordinate for $1/\det$, and one replaces the $X_j$, $0 \leq j \leq n^2 + 1$, given by ibid. with their projections to the first $n^2$ coordinates).

According to the second-to-last line of the proof of [9, Theorem 3.1] (from which Theorem 1.1 in ibid. follows), the implied constant in (7) is bounded by the sum of Betti numbers appearing in (5) above, bounded by (6), which only depends on $n$ and on the degree of $\hat{f}$ (alternatively, one may also see [15, (3.1.2), (3.4.2)], which controls the dependency on $\hat{f}$ of the implied constant in [9, Theorem 3.1, Theorem 2.1]).
If $\delta = 0$, we get by Proposition 2.4 and (7) that
\[
\sum_{h \in M_n(\mathbb{Z})} \frac{1}{|h|} \frac{1}{|G(\mathbb{F}_p)|} \sum_{g \in G(\mathbb{F}_p)} \psi(f(g + h \cdot g) \chi(f(g)) = 0 \quad (8)
\]

where $d = \dim G$. By induction as in [9, Lemma 9.5] and [19, Lemma 1.7], we get that
\[
\sum_{h \in M_n(\mathbb{Z})} \frac{1}{|h|} \frac{1}{|G(\mathbb{F}_p)|} \sum_{h \in M_n(\mathbb{Z})} \delta_{h \in X_d}(\mathbb{F}_p) \frac{1}{r(h)} \ll (\log T)^{\dim X_d}.
\]

Therefore, (8) is
\[
\ll \sum_{j=0}^{d-1} p^{j/2} (\log T)^{n^2-j} + \frac{1}{p^{1/2}} (\log T)^{n^2-d}
\]
\[
= (\log T)^{n^2} \left( \frac{1}{|G(\mathbb{F}_p)|^{1/2}} \sum_{j=0}^{d-1} \left( \frac{\sqrt{p}}{\log T} \right)^j + \frac{1}{p^{1/2}(\log T)^{d}} \right),
\]

where the implied constants depend only on $n$ and $\deg \hat{f}$. \qed

Remark 2.8 To handle normal subgroups $H \subseteq G(\mathbb{F}_p)$ as suggested in Remark 1.6, we would need to replace $\chi$ of $f_1$ by a character $\chi$ of $G(\mathbb{F}_p)$ (or of $G(\mathbb{F}_p)/H$). To do so, one would consider the Lang torsor $L_1$ corresponding to $\chi$ as in [5, 1.22–1.25]. Since all centralizers in $\text{GL}_n$ are connected, ibidem shows that the trace function associated to $L_1$ yields the character $\chi$. One could then proceed as in the proofs of [9, Corollary 3.2, Theorem 1.1].

Remark 2.9 Under the non-vanishing of an “A-number”, [9, Theorem 1.2] shows that the exponent in (7) can be improved to $\max(0, j/2 - 1)$, giving a nontrivial bound whenever $j < d+2$. This would be nontrivial for all $j$ with $G = \text{SL}_n$ as well. However, we cannot use [9, Theorem 8.1] to show the non-vanishing, since $|G(\mathbb{F}_p)| \equiv 0 \pmod{p}$ (see [18, Chapter 3]).

3 Proofs of Theorems 1.1, 1.4, 1.7 and 1.9
3.1 Setup of the exponential sums
To obtain the theorems from Proposition 2.2, we need to bound sums of the form
\[
\frac{1}{|H|} \sum_{g \in H} \psi(h_1 \cdot g + h_2 \cdot (g^{-1}x)) \quad (9)
\]
for $H \subseteq G(\mathbb{F}_p)$, $x \in G(\mathbb{Z})$ and $h_1, h_2 \in M_n(\mathbb{F}_p)$, where $\psi(x) = e(x/p)$. Note that in Theorems 1.1 and 1.7, we simply have $H = G(\mathbb{F}_p)$.

By the orthogonality relations, (9) can be written as
\[
\frac{1}{|G(\mathbb{F}_p)/H|} \sum_{\chi \in G(\mathbb{F}_p)/H} \chi(g) \left( \frac{1}{|H|} \sum_{g \in G(\mathbb{F}_p)} \psi(h_1 \cdot g + h_2 \cdot f(g)) \chi(f(g)) \right) \quad (10)
\]
\[
\ll \sum_{\chi \in G(\mathbb{F}_p)/H} \left| \frac{1}{|G(\mathbb{F}_p)|} \sum_{g \in G(\mathbb{F}_p)} \psi(h_1 \cdot g + h_2 \cdot f(g)) \chi(g) \right|,
\]

with $f(g) = g^{-1}x$. 

Under the assumptions of the theorems, $G(\mathbb{F}_p)/H$ is either trivial or isomorphic to a quotient $\mathbb{F}_p^x/U$ for a subgroup $U \subseteq \mathbb{F}_p^x$ (since $H = \ker(G \xrightarrow{f} \mathbb{F}_p^x \to \mathbb{F}_p^x/U)$), setting $U = \mathbb{F}_p^x$ if $H = G(\mathbb{F}_p)$. Hence, (10) is

$$
\sum_{\chi \in \mathbb{F}_p^x} \frac{1}{|G(\mathbb{F}_p)|} \sum_{g \in G(\mathbb{F}_p)} \psi(h_1 \cdot g + h_2 \cdot f(g)) \chi(f(g)).
$$

(11)

By Proposition 2.4, the inner sum is small whenever the rational function on $G$ appearing in $\psi$ is nonconstant. We determine when this is the case in the next section.

3.2 Constant functions on $G$

3.2.1 The case of $\text{GL}_n$ ($n \geq 2$) and $\text{SL}_n$ ($n \geq 3$)

Proposition 3.1 Let $G$ be as in (2), let $x \in G(\mathbb{F}_p)$, and let $h_1, h_2 \in M_n(\mathbb{F}_p)$. We assume that $p \geq 3$ if $n = 2$. If

$$(g \in G(\mathbb{F}_p)) \mapsto h_1 \cdot g + h_2 \cdot (g^{-1}x)$$

is constant, then $h_1 = h_2 = 0$.

Proof Since $h_2 \cdot (g^{-1}x) = (h_2x^t) \cdot g^{-1}$, it suffices to prove the result when $x = 1$.

With the identity matrix and the elementary matrices $g = I + e_{ij} \in \text{SL}_n(\mathbb{F}_p)$ for $1 \leq i, j \leq n$ distinct, we get that $(h_1)_{i,j} = (h_2)_{i,j}$.

When $G = \text{GL}_2$ and $p \neq 2$, the matrices $g = (\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix}) \in \text{GL}_2(\mathbb{F}_p)$ with $\lambda \in \mathbb{F}_p^x$ show that

$$(\lambda \in \mathbb{F}_p^x) \mapsto \lambda(h_1)_{1,1} + \lambda^{-1}(h_2)_{1,1},$$

is constant, so that $(h_1)_{1,1} = (h_2)_{1,1} = 0$ and the diagonals of $h_1$ and $h_2$ are zero by symmetry. Similarly, the matrices $g = \lambda (\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix})$ with $\lambda \in \mathbb{F}_p^x$ show that $(h_1)_{1,2} = \mp(h_1)_{2,1}$ and $(h_2)_{1,2} = \pm(h_2)_{2,1}$, whence $h_1 = h_2 = 0$. Thus, we may now suppose that $n \geq 3$.

For $1 \leq i, j, k \leq n$ distinct, the matrix $g = I - e_{ij} - e_{jk} + e_{ik} \in \text{SL}_n(\mathbb{F}_p)$, with inverse $g^{-1} = I + e_{ij} + e_{jk} + e_{ik}$, gives

$$
\text{tr}(h_1 + h_2) = h_1 \cdot g + h_2 \cdot g^{-1} = \text{tr}(h_1 + h_2) + (h_2)_{i,k},
$$

so that $(h_2)_{i,k} = 0$ and $h_2$ is diagonal. By symmetry, the same holds for $h_1$.

Using the matrices

$$
g = \begin{pmatrix}
1 & \lambda & \cdots & \lambda^{n-1} \\
1 & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots \\
0 & \cdots & 0 & 1
\end{pmatrix},
$$

$\lambda \in \mathbb{F}_p$ in $\text{SL}_n(\mathbb{F}_p)$, we get that $(\lambda \in \mathbb{F}_p) \mapsto (-1)^n \lambda (h_2)_{1,1}$ is constant, so that $(h_2)_{1,1} = 0$. By symmetry, $(h_1)_{1,1} = 0$ as well.

Finally, if $x \in \text{GL}_n(\mathbb{F}_p)$, we note that

$$
h_1 \cdot (x^{-1}gx) + h_2 \cdot (x^{-1}g^{-1}x) = (x^{-t}h_1x^t) \cdot g + (x^{-t}h_2x^t) \cdot g^{-1},$$

which shows that we may permute the diagonal elements of $h_1$ and $h_2$. By the previous steps, $h_1 = h_2 = 0$. $\Box$
Remark 3.2 By the affine linear sieve of Bourgain et al. [3] and the work of Salehi-Golsefidy–Varjú and others, this implies the following: Let $n \geq 3$, $S$ be a finite symmetric generating set for $\text{SL}_n(\mathbb{Z})$ and $(\gamma_N)_{N \geq 0}$ be a random walk on the Cayley graph of $\text{SL}_n(\mathbb{Z})$ with respect to $S$, starting at 1, i.e.

$$\gamma_{N+1} = \xi_{N+1} \gamma_N$$

for $N \geq 0$, with $\xi_{N+1}$ uniform in $S$.

Then, for any $h_1, h_2 \in M_n(\mathbb{Z})$ that are not both zero, there exists $M \geq 1$ such that

$$P\left(h_1 \cdot \gamma_N + h_2 \cdot \gamma_N^{-1} \text{ has } \leq M \text{ prime factors}\right) \approx \frac{1}{N}$$

as $N \to +\infty$.

3.2.2 Symplectic groups

Proposition 3.3 Let $n \geq 2$, $G = \text{Sp}_{2n}$, $x \in G(\mathbb{F}_p)$, and $h_1, h_2 \in M_{2n}(\mathbb{F}_p)$. Then

$$(g \in G(\mathbb{F}_p)) \mapsto h_1 \cdot g + h_2 \cdot g^{-1} \cdot x$$

is constant if and only if

$$h_1 = \begin{pmatrix} h_{11} & h_{12} \\ h_{13} & h_{14} \end{pmatrix}, \quad h_2 = \begin{pmatrix} -h_{14}^t & h_{12}^t \\ h_{13}^t & -h_{11}^t \end{pmatrix} x^{-t},$$

where $h_{1i} \in M_n(\mathbb{F}_p)$ ($1 \leq i \leq 4$).

Proof Again, it suffices to consider the case $x = 1$. With respect to the standard form,

$$g = \begin{pmatrix} A & 0 \\ 0 & A^{-t} \end{pmatrix}, \quad \begin{pmatrix} 0 & A \\ -A^t & 0 \end{pmatrix} \in \text{Sp}_{2n}(\mathbb{F}_p)$$

for any $A \in \text{GL}_n(\mathbb{F}_p)$. The result then follows from applying Proposition 3.1. \(\square\)

3.2.3 Special orthogonal groups

Proposition 3.4 For $n \geq 3$, let $G = \text{SO}_{n+1}$. Then, for $p \geq 3$ and $h \in M_n(\mathbb{F}_p)$,

$$(g \in G(\mathbb{F}_p)) \mapsto h \cdot g$$

is constant if and only if $h = 0$.

Proof Any permutation matrix $g_\sigma \in \text{SL}_n(\mathbb{F}_p)$ with $\sigma \in A_n$ belongs to $^2 G(\mathbb{F}_p)$. If $\sigma = (ijk) \in A_n$ is a cycle of length 3, the matrices $g_\sigma(I - 2e_j - 2e_k)$ and $g_\sigma$ show that $h$ is diagonal. For $1 \leq i, j \leq n$ distinct, the matrices $I - 2e_i - 2e_j$ show that the diagonal of $h$ is zero. \(\square\)

3.3 Proof of Theorems 1.1 and 1.4

By Proposition 2.2, for any integer $1 \leq T < p$, the discrepancy $D_N(A_x(g))$ is

$$\ll \frac{1}{T} + \sum_{h \in M_n(\mathbb{Z})^2} \frac{1}{r(h)} \left| \frac{1}{|H|} \sum_{g \in H} \psi(h_1 \cdot g + h_2 \cdot f(g)) \right|.$$
By (11), the second summand is

$$
\ll (\log T)^{n^2} \max_{h_2 \in M_n(\mathbb{Z})} \sum_{h_1 \in M_n(\mathbb{Z})} \frac{1}{r(h_1)} \sum_{g \in G(\mathbb{F}_p)} \psi(h_1 \cdot g + h_2 \cdot f(g)) \chi(f_1(g))
$$

By Propositions 2.7 and 3.1, we get

$$
D_N(A_N(g)) \ll \frac{1}{T} + \frac{|G(\mathbb{F}_p)|}{|H|} (\log T)^{2n^2 - \dim G + 1} \frac{\sqrt{p}}{|G(\mathbb{F}_p)/H|} \log \left( \frac{\sqrt{p}}{|G(\mathbb{F}_p)/H|} \right)^{2n^2 - \dim G + 1},
$$

taking $T = \lfloor \sqrt{p}/|G(\mathbb{F}_p)/H| \rfloor$.

The last statements in Theorems 1.1 and 1.4 follow from Remark 2.3.

**Remark 3.5** Using Proposition 2.4 only instead of Proposition 2.7 would have given an exponent of the logarithm equal to $2n^2$.

### 3.4 Proof of Theorems 1.7 and 1.9

Similarly, by Propositions 2.2, 2.7 and (11), for $1 \leq T < p$, the discrepancy $D_N(\eta(g))$ is

$$
\ll \frac{1}{T} + \sum_{0 < |h|_\infty \leq T} \frac{1}{r(h)} \sum_{g \in H} \frac{1}{|H|} \psi(h \cdot g)
$$

$$
\ll \frac{1}{T} + \sum_{\chi \in G(\mathbb{F}_p)/H} \sum_{h_2 \in M_n(\mathbb{Z})} \sum_{0 < |h|_\infty \leq T} \frac{1}{r(h)} \sum_{g \in G(\mathbb{F}_p)} \frac{1}{|G(\mathbb{F}_p)|} \psi(h \cdot g) \chi(g)
$$

$$
\ll \frac{1}{T} + \frac{|G(\mathbb{F}_p)|}{|H|} (\log T)^{n^2 - \dim G + 1} \frac{\sqrt{p}}{p^{1/2}} \ll \frac{|G(\mathbb{F}_p)/H|}{\sqrt{p}} \log \left( \frac{\sqrt{p}}{|G(\mathbb{F}_p)/H|} \right)^{n^2 - \dim G + 1}
$$

**Remark 3.6** As above, using Proposition 2.4 instead of Proposition 2.7 would have given an exponent of the logarithm equal to $n^2$. Note that these exponents in the case of $GL_n$ or $SL_n$ do not depend on $n$.

### 3.5 Higher-dimensional variant

To obtain Theorem 1.12, we need to control sums of the form

$$
\sum_{g \in G_n^{-1}(\mathbb{F}_p)} \psi \left( \sum_{i=1}^{r-1} h_i \cdot g_i + h_r (g_1 \ldots g_{r-1})^{-1} x \right)
$$

(13)

for $h = (h_1, \ldots, h_r) \in M_n(\mathbb{F}_p)^r$. To do so, it suffices to replace $G$ by $G^{-1}$ and $M_n(\mathbb{F}_p)^2$ by $M_n(\mathbb{F}_p)^r$ in the arguments above. In the first bound, there is no dependency with $r$ in the exponent since we average over all but one $h_i$, and we can use Proposition 2.7. From Proposition 3.1, we see that the rational function in (13) is constant if and only if $h = 0$. 
4 Proof of Theorem 1.10 and Corollary 1.11

4.1 Proof of Theorem 1.10

By orthogonality, we can write the density (3) as

\[
\frac{1}{|G(F_p)|} \sum_{g \in G(F_p)} \sum_{e \in E_p} \sum_{f \in F_p} \frac{1}{p^{2n^2}} \psi \left( u \cdot (g - e) + v \cdot (g^{-1}x - f) \right)
\]

\[
= \frac{1}{p^{2n^2}} \sum_{u, v \in M_n(F_p)} \sum_{e \in E_p} \sum_{f \in F_p} \psi(u \cdot e) \sum_{f \in F_p} \psi(v \cdot f) S(u, v)
\]

\[
= \frac{|E_p| |F_p|}{p^{2n^2}} + O \left( \frac{1}{p^{2n^2}} \sum_{u, v \in M_n(F_p) \atop (u, v) \neq 0} \left| \sum_{e \in E_p} \psi(u \cdot e) \right| \left| \sum_{f \in F_p} \psi(v \cdot f) \right| |S(u, v)| \right), \tag{14}
\]

where \(E_p = E \pmod p\), \(F_p = F \pmod p \subset F_p\) and

\[
S(u, v) = \frac{1}{|G(F_p)|} \sum_{g \in G(F_p)} \psi \left( u \cdot g + v \cdot (g^{-1}x) \right).
\]

Since \(E = \prod_{1 \leq k, l \leq n} E_{kl}\) is a product of intervals, Weyl's bound gives

\[
\sum_{e \in E_p} \psi(u \cdot e) = \prod_{1 \leq k, l \leq n} \sum_{e \in E_{kl}} \psi(u_{kl} e_{kl}) \ll \prod_{1 \leq k, l \leq n} \min \left( |E_{kl}|, |u_{kl}/p|^{-1} \right),
\]

and similarly for \(F\), with \(| \cdot |\) denoting the distance to the nearest integer and \(|E_{kl}| := \text{meas}(E_{kl})\). Hence, the error term in (14) is

\[
\ll \frac{1}{p^{n^2}} \sum_{v \in M_n(F_p)} \prod_{1 \leq k, l \leq n} \min \left( |F_{kl}|, |v_{kl}/p|^{-1} \right)
\]

\[
\times \frac{1}{p^{n^2}} \sum_{u \in M_n(F_p) \atop (u, v) \neq 0} |S(u, v)| \prod_{1 \leq k, l \leq n} \min \left( |E_{kl}|, |u_{kl}/p|^{-1} \right).
\]

To bound the sum over \(u\), we proceed as in Proposition 2.7, using [9]. With \(d = \dim G\),

\[
\frac{1}{p^{n^2}} \sum_{u \in M_n(F_p) \atop (u, v) \neq 0} |S(u, v)| \prod_{1 \leq k, l \leq n} \min \left( |E_{kl}|, |u_{kl}/p|^{-1} \right)
\]

\[
\ll \left( \frac{1}{p^{n/2}} \sum_{j=0}^{d-1} p^{j/2} + \sum_{j=d}^{n^2} p^{-j/2} \right) \frac{1}{p^{n^2}} \sum_{u \in X_j(F_p)} \prod_{1 \leq k, l \leq n} \min \left( |E_{kl}|, |u_{kl}/p|^{-1} \right). \tag{15}
\]

By [9, Lemma 9.5] (or [11, (2.6)]), if \(X \subset A^{n^2}\) has dimension \(\leq n^2 - j\),

\[
\sum_{u \in X(F_p) \atop 1 \leq k, l \leq n} \min \left( |E_{kl}|, |u_{kl}/p|^{-1} \right) \ll (p \log p)^{n^2 - j} M_E^j
\]

where \(M_E = \max_{k, l} |E_{kl}|\). Proceeding by induction as in op. cit., we get the more precise bound

\[
\sum_{u \in X(F_p) \atop 1 \leq k, l \leq n} \min \left( |E_{kl}|, |u_{kl}/p|^{-1} \right) \ll (p \log p)^{n^2 - j} e_j(|E_{kl}|) \tag{16}
\]

when the \(|E_{kl}|\) may not be all equal, where \(e_j\) is the \(j\)th elementary symmetric polynomial in \(n^2\) variables.
Thus, (15) is

\[
\ll \left( \frac{1}{p^{d/2}} \sum_{j=0}^{d-1} p^{j/2} + \sum_{j=d}^{n^2} p^{-1/2} \right) (\log p)^2 e_j(|E_{kl}|) p^{-j} \\
\ll (\log p)^2 \left( \frac{1}{p^{d/2}} \sum_{j=0}^{d-1} e_j \left( \frac{|E_{kl}|}{\sqrt{p}} \right) + \frac{1}{\sqrt{p}} \sum_{j=d}^{n^2} e_j \left( \frac{|E_{kl}|}{p} \right) \right) \\
\ll (\log p)^2 \left( \frac{1}{p^{d/2}} \sum_{j=0}^{d-1} e_j \left( \frac{|E_{kl}|}{\sqrt{p}} \right) + \frac{1}{\sqrt{p}} e_d \left( \frac{|E_{kl}|}{p} \right) \right). 
\]

By Maclaurin’s inequality [17, (12.3)], letting \( L_E = e_1(|E_{kl}|) \), this is

\[
\ll (\log p)^2 \left( \frac{1}{p^{d/2}} \sum_{j=0}^{d-1} \left( L_E / \sqrt{p} \right)^j + \frac{(L_E / p)^d}{\sqrt{p}} \right) \\
\ll (\log p)^2 \left( \frac{1}{p^{d/2}} \max \left( 1, \left( L_E / \sqrt{p} \right)^{d-1} \right) + \frac{(L_E / p)^d}{\sqrt{p}} \right) \\
\ll \frac{(\log p)^2}{p^{d/2}} \max \left( 1, \left( L_E / \sqrt{p} \right)^{d-1} \right). 
\]

Using (16) again, we find that the total error in (14) is

\[
\ll \frac{(\log p)^2 n^2}{p^{d/2}} \max \left( 1, \left( L_E / \sqrt{p} \right)^{d-1} \right) 
\]

4.1.1 Proof of Corollary 1.11

Finally, if \( E \) and \( F \) are the products of intervals of the same integral length \( x \), then the density (3) is

\[
\left( \frac{x}{p} \right)^{2n^2} + O_p \left( \frac{(\log p)^2 n^2}{p^{d/2}} \max \left( 1, \left( \frac{x}{\sqrt{p}} \right)^{d-1} \right) \right). 
\]

The main term dominates if and only if

\[
x \gg_{n,\varepsilon} p^{-\frac{1}{2n^2} - \frac{1}{\dim G + 1}} \varepsilon 
\]

for any \( \varepsilon > 0 \), which yields the corollary.

Author details

1 Centre de Recherches Mathématiques, Université de Montréal, Montreal, Canada; 2 Present address: Zurich, Switzerland.

Acknowledgements

The author thanks Lucile Devin, his colleagues in Montréal, and anonymous referees for useful feedback on this work, as well as Yan Li for suggesting a modification of the proof of Proposition 3.1 that makes it shorter and able to handle the characteristic 2 case. This work was partially supported by Koukoulopoulos’ Discovery Grant 435272-2013 of the Natural Sciences and Engineering Research Council of Canada, and by Radziwiłł’s NSERC DG grant and the CRC program.

Received: 25 April 2019  Accepted: 25 October 2019  Published online: 7 November 2019

References

1. Ahmadi, O., Shparlinski, I.E.: Distribution of matrices with restricted entries over finite fields. Indag. Math. (N.S.) 18(3), 327–337 (2007)
2. Aschbacher, M.: On the maximal subgroups of the finite classical groups. Invent. Math. 76(3), 469–514 (1984)
3. Bourgain, J., Gamburd, A., Sarnak, P.: Affine linear sieve, expanders, and sum-product. Invent. Math. 179(3), 559–644 (2010)
4. Sean Allen Broughton: A note on characters of algebraic groups. Proc. Am. Math. Soc. 89(1), 39–40 (1983)
5. Deligne, P.: Cohomologie étale, séminaire de géométrie algébrique du Bois-Marie SGA 4 1/2. Lecture Notes in Mathematics, vol. 569. Springer (1977)
6. Deligne, P.: La conjecture de Weil. II. Publications Mathématiques de l’Institut des Hautes Études Scientifiques 52(1), 137–252 (1980)
7. Drmota, M., Tichy, R.F.: Sequences, Discrepancies, and Applications. Lecture Notes in Mathematics, vol. 1651. Springer (1997)
8. Ferguson, R., Hoffman, C., Luca, F., Ostafe, A., Shparlinski, I.E.: Some additive combinatorics problems in matrix rings. Rev. Mat. Complut. 23(2), 501–513 (2010)
9. Fouvry, E., Katz, N.M.: A general stratification theorem for exponential sums, and applications. J. für die reine Angew. Math. 2001(504), 115–166 (2001)
10. Fouvry, E., Kowalski, E., Michel, P.: Algebraic twists of modular forms and Hecke orbits. Geom. Funct. Anal. 25(2), 580–657 (2015)
11. Fouvry, E.: Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums. Israel J. Math. 120(1), 81–96 (2000)
12. Su, H., Li, Y.: Gauss sums over some matrix groups. J. Number Theory 132(12), 2967–2976 (2012)
13. Su, H., Li, Y.: On a uniformly distributed phenomenon in matrix groups. J. Number Theory 133(11), 3578–3588 (2013)
14. Katz, N.M.: Sums of Betti numbers in arbitrary characteristic. Finite Fields Appl. 7(1), 29–44 (2001)
15. Katz, N.M., Laumon, G.: Transformation de Fourier et majoration de sommes exponentielles. Inst. Hautes Études Sci. Publ. Math. 62, 361–418 (1985)
16. Shparlinski, I.E.: Modular hyperbolas. Jpn. J. Math. 7(2), 235–294 (2012)
17. Michael Steele, J.: The Cauchy-Schwarz Master Class. MAA Problem Books Series. Mathematical Association of America, Washington, DC; Cambridge University Press, Cambridge (2004). (An introduction to the art of mathematical inequalities)
18. Wilson, R.A.: The Finite Simple Groups, vol. 251 of Graduate Texts in Mathematics. Springer (2009)
19. Xu, J.: Stratification for Multiplicative Character Sums. International Mathematics Research Notices (2018). my096

**Publisher’s Note**

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.