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 $G(\mathbb{F}_p)$ as $p \to \infty$, for any fixed $x \in G(\mathbb{Z})$, where $G = \mathrm{GL}_n$, SL_n, Sp_{2n} or $\mathrm{SO}_n^{\pm}$. In the special linear case, this answers in particular a question raised by S. Hu and Y. 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 $g \in \mathrm{GL}_n(\mathbb{F}_p)$ such that g, g^{-1} have all entries in $[0, c_n p^{1-1/(2n^2+2)+\varepsilon}]$ 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.

1. Introduction

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

1.1. **The cases of $(\mathbb{Z}/n)^{\times}$ and $\mathrm{GL}_n(\mathbb{F}_p)$.** Following several similar results for the group $(\mathbb{Z}/n)^{\times}$ (see [Shp12] for a survey), Su Hu and Yan Li [HL13] have shown that for the matrix group $G = \mathrm{GL}_n(\mathbb{F}_p)$ and any fixed $x \in G$, the solutions to the equation

$$gh = x \qquad (g, h \in G)$$

are uniformly distributed in $[0,1]^{n^2} \times [0,1]^{n^2}$ as $p \to \infty$, with respect to the embedding

$$\begin{aligned} \eta : M_n(\mathbb{F}_p) &\to [0,1]^{n^2} \\ g = (g_{i,j})_{i,j} &\mapsto (\{g_{i,j}/p\})_{i,j}, \end{aligned} \qquad (1)$$

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 [FHL+10] 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 $G = \mathrm{SL}_2(\mathbb{F}_p)$, but conjecture that there should be joint uniform distribution whenever $n \geqslant 3$. We positively answer this by showing:

Date: October 2019.
2010 *Mathematics Subject Classification.* 11C20, 11K36, 11T24, 11L05.

Theorem 1.1. *Let G be*

$$\mathrm{GL}_n \quad (\textit{for } n \geqslant 2) \qquad \textit{or} \qquad \mathrm{SL}_n \quad (\textit{for } n \geqslant 3), \tag{2}$$

and let $x \in G(\mathbb{Z})$. As $p \to \infty$, the elements

$$A_x(g) = \left(g,\ g^{-1}x\right) \in M_n(\mathbb{F}_p) \times M_n(\mathbb{F}_p) \quad (g \in G(\mathbb{F}_p))$$

are uniformly distributed in $\Omega = [0,1]^{n^2} \times [0,1]^{n^2}$ with respect to the embedding η in (1). More precisely, for every product of intervals R in Ω,

$$\frac{|\{g \in G(\mathbb{F}_p) : \eta(A_x(g)) \in R\}|}{|G(\mathbb{F}_p)|} = \mathrm{meas}(R) + \begin{cases} O_n\left(\frac{(\log p)^{n^2+1}}{\sqrt{p}}\right) & : G = \mathrm{GL}_n \\ O_n\left(\frac{(\log p)^{n^2+2}}{\sqrt{p}}\right) & : G = \mathrm{SL}_n \end{cases}$$

as $p \to \infty$, where 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 [HL13], which are for example $p^{-1/(2(2n^2+1))}$ when $G = \mathrm{GL}_n$. The bulk of the improvement comes from bounding nontrivially the $1/r(\boldsymbol{h})$ 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 $|f| \leqslant C_n g$.

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 $G = \mathrm{GL}_n$. For $f \in \mathbb{F}_p[G]^\times$ a nonvanishing nonconstant function and $U \leqslant \mathbb{F}_p^\times$ a subgroup, let*

$$H = f^{-1}(U) = \{g \in G(\mathbb{F}_p) : f(g) \in U\}.$$

For every product of intervals $R \subset \Omega$, we have

$$\frac{|\{g \in H : \eta(A_x(g)) \in R\}|}{|H|} = \mathrm{meas}(R) + O_n\left(\frac{\sqrt{p}}{|U|}\left(\log \frac{|U|}{\sqrt{p}}\right)^{n^2+1}\right)$$

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 $H = \{g \in \mathrm{GL}_n(\mathbb{F}_p) : \det(g) \in \mathbb{F}_p^{\times r}\}$ 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. [Bro83]) that if G is a connected affine algebraic group, then $f/f(1) \in \overline{\mathbb{F}}_p[G]^\times$ 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.*

(2) In particular, we cannot get a nontrivial version of Theorem 1.4 for $\mathrm{SL}_n(\mathbb{F}_p)$: since the latter is perfect for $p > 3$, f must be constant. The classification of maximal subgroups of $\mathrm{SL}_n(\mathbb{F}_p)$ [Asc84] also shows that the restriction on the index is too stringent.
(3) Using the same techniques, it should be possible to obtain Theorem 1.4 also when $H \leqslant \mathrm{GL}_n(\mathbb{F}_p)$ 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 $G = \mathrm{Sp}_n$ ($n \geqslant 2$ even). Indeed, if

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

(with respect to the standard symplectic form, where $g_i \in M_{2n}(\mathbb{F}_p)$). Hence, the obstruction for SL_2 can be viewed as coming from the fact that $\mathrm{SL}_2(\mathbb{F}_p) = \mathrm{Sp}_2(\mathbb{F}_p)$.

1.3.2. *Special orthogonal groups.* Let $\Phi \in \mathrm{GL}_n(\mathbb{F}_p)$ be in one of the two equivalence classes of nonsingular symmetric bilinear forms on $\mathbb{F}_p^n$. Since $g^{-1} = \Phi g^t \Phi^{-1}$ for $g \in \mathrm{GO}(\Phi)$, 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 $\mathrm{diag}(\alpha, 1)$ ($\alpha \in \mathbb{F}_p^\times$) are themselves not uniformly distributed in $[0,1]^4$ with respect to the embedding (1), since they are of the form $\left(\begin{smallmatrix} a & -\alpha c \\ c & a \end{smallmatrix}\right)$.

1.4. **Distribution of elements.** Nonetheless, the elements themselves are still uniformly distributed in all cases except $\mathrm{SO}_2^\pm$, as in [HL13, Theorems 1.5–1.6] for GL_n and SL_n.

Theorem 1.7. *For $n \geqslant 1$, let G be*[1]

$$\mathrm{GL}_n, \quad \mathrm{SL}_n, \quad \mathrm{Sp}_n \ (n \text{ even}), \quad \text{or} \quad \mathrm{SO}_{n,I_n} \ (n \geqslant 3).$$

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 Ω,

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

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.

[1] In what follows, we let SO_{n,I_n} be the special orthogonal group corresponding to the form given by the identity matrix I_n: in other words, $\mathrm{SO}_{n,I_n}(\mathbb{F}_p)$ is the special orthogonal group with square determinant, i.e. $\mathrm{SO}_n(\mathbb{F}_p)$ if n is odd, and if n is even, $\mathrm{SO}_n^\pm(\mathbb{F}_p)$ if $p \equiv \pm 1 \pmod 4$ respectively.

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

- in [HL13], handling GL_n and SL_n using [HL12], which are $p^{-n/(n^2+1)}$.
- in Theorem 1.1 for the joint distribution.

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 $R \subset \Omega$,*

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

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 $1 \leqslant g, h \leqslant p-1$ lie in fixed intervals. It is a conjecture (see [Shp12, Section 3.1]) that for any $\varepsilon > 0$ and p large enough, there exist integers g, h such that $gh = 1 \pmod p$ with $|g|, |h| \leqslant p^{1/2+\varepsilon}$. 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 p 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

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

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

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*

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

We also refer the reader to [AS07] for related questions concerning matrices, and to [Fou00], [FK01, 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

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

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

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

$$A_x(\boldsymbol{g}) = \big(g_1, \dots, g_{r-1}, (g_1 \dots g_{r-1})^{-1}x\big) \in M_n(\mathbb{F}_p)^r \qquad (\boldsymbol{g} \in G(\mathbb{F}_p)^{r-1})$$

are uniformly distributed in $\Omega = [0,1]^{rn^2}$ with respect to the embedding (1). More precisely, for every product of intervals R in Ω,

$$\frac{|\{\boldsymbol{g} \in G(\mathbb{F}_p)^{r-1} : \eta(A_x(\boldsymbol{g})) \in R\}|}{|G(\mathbb{F}_p)|^{r-1}} = \operatorname{meas}(R) + \begin{cases} O_{n,r}\left(\frac{(\log p)^{n^2+1}}{\sqrt{p}}\right) & : G = \mathrm{GL}_n \\ O_{n,r}\left(\frac{(\log p)^{n^2+2}}{\sqrt{p}}\right) & : G = \mathrm{SL}_n \end{cases}$$

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.

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 characteristic 2. 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.

2. Tools

2.1. **Equidistribution and discrepancy.** For the following results, we refer the reader to [DT97, Chapter 1]. Throughout, we let $\Omega = [0,1]^k$ for some integer $k \geqslant 1$.

Definition 2.1. The discrepancy of a sequence $(\boldsymbol{x}_n)_{n \geqslant 1}$ in Ω is

$$D_N(\boldsymbol{x}_n) \quad = \quad \sup_{I \subset \Omega} \left| \frac{|\{n \leqslant N : \boldsymbol{x}_n \in I\}|}{N} - \operatorname{meas}(I) \right|,$$

where I runs over all products of intervals in Ω.

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

$$D_N(\boldsymbol{x}_n) \leqslant \left(\frac{3}{2}\right)^k \left(\frac{2}{T+1} + \sum_{\substack{\boldsymbol{h} \in \mathbb{Z}^k \\ 0 < ||\boldsymbol{h}||_\infty \leqslant T}} \frac{1}{r(\boldsymbol{h})} \left| \frac{1}{N} \sum_{n \leqslant N} e(\boldsymbol{h} \cdot \boldsymbol{x}_n) \right| \right),$$

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

Proof. See [DT97, 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 $J_N(\boldsymbol{x}_n)$, which satisfies $J_N(\boldsymbol{x}_n) \ll_k D_N(\boldsymbol{x}_n)^{1/k}$ (see [DT97, Theorem 1.12]).

By Weyl's criterion, $(\boldsymbol{x}_n)_{n\geqslant 1}$ is equidistributed in Ω if and only if

$$\sum_{n\leqslant N} e(\boldsymbol{h}\cdot\boldsymbol{x}_n) = o(N)$$

for every nonzero $\boldsymbol{h} \in \mathbb{Z}^k$, 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 [FHL⁺10] used in [HL13] 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 [Del80] 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*

$$\frac{1}{|G(\mathbb{F}_p)|} \sum_{\substack{g\in G(\mathbb{F}_p)\\ f(g)\neq\infty}} \psi(f(g))\chi(f_1(g)) = \delta + O\left(p^{-1/2}\right) \tag{4}$$

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 [Del77, Exposé 6], let $\mathcal{L}_0 := f^*\mathcal{L}_\psi = \mathcal{L}_{\psi(f)}$ (resp. $\mathcal{L}_1 := f_1^*\mathcal{L}_\chi = \mathcal{L}_{\chi(f_1)}$) be the restriction to G of the Artin–Schreier (resp. Kummer) sheaf on $\mathbb{A}^{n^2}_{\mathbb{F}_p}$ corresponding to $\psi\circ f$ (resp. $\chi\circ f_1$), and let $\mathcal{L} = \mathcal{L}_0 \otimes \mathcal{L}_1$ be the middle tensor product. These can be seen as representations

$$\rho_0,\ \rho_1,\ \rho = \rho_0\otimes\rho_1 : \mathrm{Gal}(\mathbb{F}_p(G)^{\mathrm{sep}}/\mathbb{F}_p(G)) \to \overline{\mathbb{Q}}_\ell^\times,$$

such that at every point $g \in G(\mathbb{F}_p) \subset \mathbb{F}_p^{n^2}$ with $f_1(g) \neq \infty$, there is a Frobenius element Frob_g with

$$\iota\rho_0(\mathrm{Frob}_g) = \psi(f(g)),\ \iota\rho_1(\mathrm{Frob}_g) = \chi(f_1(g)),\ \iota\rho(\mathrm{Frob}_g) = \psi(f(g))\chi(f_1(g))$$

for an embedding $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$. Hence, the left-hand side of (4) is

$$\frac{1}{|G(\mathbb{F}_p)|} \sum_{\substack{g\in G(\mathbb{F}_p)\\ f(g)\neq\infty}} \iota\rho(\mathrm{Frob}_g).$$

By the Grothendieck–Lefschetz trace formula [Del77, Exposé 6, (1.1.1)], this is

$$\frac{1}{|G(\mathbb{F}_p)|}\sum_{i=0}^{2\dim G}(-1)^i\iota\,\mathrm{tr}(\mathrm{Frob}_p \mid H_c^i(U\times\overline{\mathbb{F}}_p,\mathcal{L})),$$

for U the open in $\mathbb{A}_{\mathbb{F}_p}^{n^2}$ where $\mathcal{L}_0$ is lisse (i.e. the complement of the zero set of f).

By Deligne's extension of the Riemann hypothesis over finite fields [Del80, Théorème 2] (see also [Del77, Théorème 1.17]), the eigenvalues of the Frobenius acting on $H_c^i(U\times\overline{\mathbb{F}}_p,\mathcal{L})$ are p-Weil numbers of weight at most i. If the one-dimensional sheaf $\mathcal{L}$ is not geometrically trivial, the coinvariant formula implies that $H_c^{2\dim G}(U\times\overline{\mathbb{F}}_p,\mathcal{L})=0$, so that the left-hand side of (4)

$$\ll p^{-1/2}\sum_{i=0}^{2\dim G-1}\dim H_c^i(U\times\overline{\mathbb{F}}_p,\mathcal{L}). \tag{5}$$

By [Kat01, 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

$$3\left(2+\max(\deg(f),n+2)+\deg(f_1)\right)^{3n^2}. \tag{6}$$

Thus, it suffices to show that $\mathcal{L}$ is not geometrically trivial to conclude. If it is not the case, since $\mathcal{L}_1$ is tame everywhere and $\mathcal{L}_0$ is not unless it is geometrically trivial, we then have that both $\mathcal{L}_1$ and $\mathcal{L}_0$ are geometrically trivial. Since $\pi_1(U,\overline{\eta})/\pi_1(\overline{U},\overline{\eta})\cong\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, it follows as in [FKM15, 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 $f=\det^p-\det$ is not a counterexample to the theorem since, while not constant on $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$, it is constant on $\mathrm{GL}_n(\mathbb{F}_p)$. 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, $f_1=\det^{\mathrm{ord}\,\chi}$ is not a counterexample since $\chi\circ f_1$ is constant on $G(\mathbb{F}_p)$.

2.2.1. *Improved error terms via stratification.* The anonymous referee of Hu and Li's paper indicated (see [HL13, Section 4]) that the stratification results of Laumon, Katz and Fouvry may be employed to answer the conjecture for SL_n ($n\geqslant 3$; see Section 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 [FK01] to improve the error terms.

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

$$g_1\cdot g_2:=\mathrm{tr}(g_1^tg_2)=\sum_{1\leqslant i,j\leqslant n}(g_1)_{i,j}(g_2)_{i,j}\qquad(g_1,g_2\in M_n(\mathbb{F}_p)).$$

The following provides a better bound on average over shifts. We will see in Section 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 $\hat{f} : G \to \mathbb{A}^1_{\mathbb{Z}}$. If $\delta = 0$, then, for every integer $2 \leqslant T < p$,*

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

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

Proof. By [FK01, Theorem 1.1, Section 3], there exist closed subschemes $X_j \subset \mathbb{A}^{n^2}_{\mathbb{Z}}$ $(0 \leqslant j \leqslant n^2)$ of relative dimension $\leqslant n^2 - j$, depending on $G_{\mathbb{Z}}$ and $\hat{f}$, such that

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

and

$$\frac{1}{|G(\mathbb{F}_p)|} \sum_{g \in G(\mathbb{F}_p)} \psi(f(g) + h \cdot g)\chi(f_1(g)) \ll \frac{p^{\frac{j-1}{2}}}{|G(\mathbb{F}_p)|^{1/2}} \tag{7}$$

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

According to the second-to-last line of the proof of [FK01, 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 [KL85, (3.1.2), (3.4.2)], which controls the dependency on $\hat{f}$ of the implied constant in [FK01, Theorem 3.1, Theorem 2.1]).

If $\delta = 0$, we get by Proposition 2.4 and (7) that

$$\begin{aligned} &\sum_{\substack{h \in M_n(\mathbb{Z}) \\ ||h||_\infty \leqslant T}} \frac{1}{r(h)} \left| \frac{1}{|G(\mathbb{F}_p)|} \sum_{g \in G(\mathbb{F}_p)} \psi(f(g) + h \cdot g)\chi(f_1(g)) \right| \\ &\ll \sum_{j=0}^{d-1} \frac{p^{\frac{j}{2}}}{|G(\mathbb{F}_p)|^{1/2}} \sum_{\substack{h \in M_n(\mathbb{Z}) \\ ||h||_\infty \leqslant T}} \frac{\delta_{h \in X_j(\mathbb{F}_p) \backslash X_{j+1}(\mathbb{F}_p)}}{r(h)} + \frac{1}{p^{1/2}} \sum_{\substack{h \in M_n(\mathbb{Z}) \\ ||h||_\infty \leqslant T}} \frac{\delta_{h \in X_d(\mathbb{F}_p)}}{r(h)}, \end{aligned} \tag{8}$$

where $d = \dim G$. By induction as in [FK01, Lemma 9.5] and [Xu18, Lemma 1.7], we get that

$$\sum_{\substack{h \in M_n(\mathbb{Z}) \\ ||h||_\infty \leqslant T}} \frac{\delta_{h \pmod p \in X_j(\mathbb{F}_p)}}{r(h)} \ll (\log T)^{\dim X_j}.$$

Therefore, (8) is

$$\begin{aligned}
&\ll \sum_{j=0}^{d-1} \frac{p^{\frac{j}{2}}}{|G(\mathbb{F}_p)|^{1/2}} (\log T)^{n^2-j} + \frac{1}{p^{1/2}} (\log T)^{n^2-d} \\
&= (\log T)^{n^2} \left(\frac{1}{|G(\mathbb{F}_p)|^{1/2}} \sum_{j=0}^{d-1} \left(\frac{\sqrt{p}}{\log T} \right)^j + \frac{1}{p^{1/2} (\log T)^d} \right),
\end{aligned}$$

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

Remark 2.8. To handle normal subgroups $H \leqslant G(\mathbb{F}_p)$ as suggested in Remark 1.6, we would need to replace $\chi \circ f_1$ by a character χ of $G(\mathbb{F}_p)$ (or of $G(\mathbb{F}_p)/H$). To do so, one would consider the Lang torsor $\mathcal{L}_1$ corresponding to χ as in [Del77, 1.22-25]. Since all centralizers in GL_n are connected, ibidem shows that the trace function associated to $\mathcal{L}_1$ yields the character χ. One could then proceed as in the proofs of [FK01, Corollary 3.2, Theorem 1.1].

Remark 2.9. Under the non-vanishing of an "A-number", [FK01, 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 $G = \mathrm{SL}_n$ as well. However, we cannot use [FK01, Theorem 8.1] to show the non-vanishing, since $|G(\mathbb{F}_p)| \equiv 0 \pmod{p}$ (see [Wil09, 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

$$\frac{1}{|H|} \sum_{g \in H} \psi\left(h_1 \cdot g + h_2 \cdot (g^{-1} x)\right) \tag{9}$$

for $H \trianglelefteq G(\mathbb{F}_p)$, $x \in G(\mathbb{Z})$ 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

$$\begin{aligned}
&\frac{1}{|G(\mathbb{F}_p)/H|} \sum_{\chi \in \widehat{G(\mathbb{F}_p)/H}} \overline{\chi}(g) \left(\frac{1}{|H|} \sum_{g \in G(\mathbb{F}_p)} \psi\left(h_1 \cdot g + h_2 \cdot f(g)\right) \chi(g) \right) \\
\ll &\sum_{\chi \in \widehat{G(\mathbb{F}_p)/H}} \left| \frac{1}{|G(\mathbb{F}_p)|} \sum_{g \in G(\mathbb{F}_p)} \psi\left(h_1 \cdot g + h_2 \cdot f(g)\right) \chi(g) \right|, \qquad (10)
\end{aligned}$$

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 $\mathbb{F}_p^\times / U$ for a subgroup $U \leqslant \mathbb{F}_p^\times$ (since $H = \ker(G \xrightarrow{f_1}$

$\mathbb{F}_p^\times \to \mathbb{F}_p^\times/U)$), setting $U = \mathbb{F}_p^\times$ if $H = G(\mathbb{F}_p)$. Hence, (10) is

$$\sum_{\substack{\chi \in \widehat{\mathbb{F}_p^\times} \\ \chi|_U = 1}} \left| \frac{1}{|G(\mathbb{F}_p)|} \sum_{g \in G(\mathbb{F}_p)} \psi\left(h_1 \cdot g + h_2 \cdot f(g)\right) \chi(f_1(g)) \right|. \tag{11}$$

By Proposition 2.4, the inner sum is small whenever the rational function on G appearing in ψ 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* GL_n $(n \geqslant 2)$ *and* SL_n $(n \geqslant 3)$.

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 $p \geqslant 3$ if $n = 2$. If*

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

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

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

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

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

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

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 $g = \lambda \left(\begin{smallmatrix} 0 & 1 \\ \pm 1 & 0 \end{smallmatrix}\right)$ with $\lambda \in \mathbb{F}_p^\times$ 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 $n \geqslant 3$.

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

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

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

Using the matrices

$$g = \begin{pmatrix} & & & & (-1)^{n+1} \\ 1 & & & & \lambda \\ & 1 & & & 0 \\ & & \ddots & & \vdots \\ & & & 1 & 0 \end{pmatrix}, \quad g^{-1} = \begin{pmatrix} (-1)^n \lambda & 1 & & & \\ 0 & & 1 & & \\ \vdots & & & \ddots & \\ 0 & & & & 1 \\ (-1)^{n+1} & & & & \end{pmatrix}$$

in $\mathrm{SL}_n(\mathbb{F}_p)$, for $\lambda \in \mathbb{F}_p$, 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 $x \in \mathrm{GL}_n(\mathbb{F}_p)$, we note that

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

which shows that we may permute the diagonal elements of h_1 and h_2. By the previous steps, $h_1 = h_2 = 0$. ∎

Remark 3.2. By the affine linear sieve of Bourgain, Gamburd and Sarnak [BGS10] and the work of Salehi-Golsefidy–Varjú and others, this implies the following: Let $n \geqslant 3$, S be a finite symmetric generating set for $\mathrm{SL}_n(\mathbb{Z})$ and $(\gamma_N)_{N\geqslant 0}$ be a random walk on the Cayley graph of $\mathrm{SL}_n(\mathbb{Z})$ with respect to S, starting at 1, i.e.

$$\gamma_{N+1} = \xi_{N+1}\gamma_N \text{ for } N \geqslant 0, \text{ with } \xi_{N+1} \text{ uniform in } S.$$

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

$$P\Big(h_1 \cdot \gamma_N + h_2 \cdot \gamma_N^{-1} \text{ has } \leqslant M \text{ prime factors}\Big) \asymp 1/N$$

as $N \to +\infty$.

3.2.2. *Symplectic groups.*

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

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

is constant if and only if

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

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

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

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

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

3.2.3. *Special orthogonal groups.*

Proposition 3.4. *For $n \geqslant 3$, let $G = \mathrm{SO}_{n,I_n}$. Then, for $p \geqslant 3$ and $h \in M_n(\mathbb{F}_p)$,*

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

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

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

[2]If G corresponded instead to the form $\mathrm{diag}(\alpha, 1, \ldots, 1)$, $\alpha \neq 1$, this would be true only for the permutations fixing 1.

3.3. **Proof of Theorems 1.1 and 1.4.** By Proposition 2.2, for any integer $1 \leqslant T < p$, the discrepancy $D_N(A_x(g))$ is

$$\ll \frac{1}{T} + \sum_{\substack{\boldsymbol{h} \in M_n(\mathbb{Z})^2 \\ 0 < ||h||_\infty \leqslant T}} \frac{1}{r(\boldsymbol{h})} \left| \frac{1}{|H|} \sum_{g \in H} \psi\left(h_1 \cdot g + h_2 \cdot f(g)\right) \right|.$$

By (11), the second summand is

$$\ll (\log T)^{n^2} \max_{\substack{h_2 \in M_n(\mathbb{Z}) \\ ||h_2||_\infty \leqslant T}} \sum_{\substack{h_1 \in M_n(\mathbb{Z}) \\ ||(h_1,h_2)||_\infty \leqslant T \\ (h_1,h_2) \neq 0}} \frac{1}{r(h_1)} \sum_{\substack{\chi \in \widehat{\mathbb{F}_p^\times} \\ \chi|_U = 1}} \left| \frac{1}{|G(\mathbb{F}_p)|} \sum_{g \in G(\mathbb{F}_p)} \psi\left(h_1 \cdot g + h_2 \cdot f(g)\right) \chi(f_1(g)) \right|.$$

By Proposition 2.7 and Proposition 3.1, we get

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

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

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 $1 \leqslant T < p$, the discrepancy $D_N(\eta(g))$ is

$$\begin{aligned} &\ll \frac{1}{T} + \sum_{\substack{h \in \mathbb{Z}^{n^2} \\ 0 < ||h||_\infty \leqslant T}} \frac{1}{r(h)} \left| \sum_{g \in H} \frac{1}{|H|} \psi(h \cdot g) \right| \\ &\ll \frac{1}{T} + \sum_{\chi \in \widehat{G(\mathbb{F}_p)/H}} \sum_{\substack{h \in M_n(\mathbb{Z}) \\ 0 < ||h||_\infty \leqslant T}} \frac{1}{r(h)} \left| \frac{1}{|G(\mathbb{F}_p)|} \sum_{g \in G(\mathbb{F}_p)} \psi\left(h \cdot g\right) \chi(g) \right| \\ &\ll \frac{1}{T} + \frac{|G(\mathbb{F}_p)|}{|H|} \frac{(\log T)^{n^2 - \dim G + 1}}{p^{1/2}} \ll \frac{|G(\mathbb{F}_p)/H|}{\sqrt{p}} \log\left(\frac{\sqrt{p}}{|G(\mathbb{F}_p)/H|}\right)^{n^2 - \dim G + 1} \end{aligned}$$

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

$$\sum_{\boldsymbol{g}\in G^{r-1}(\mathbb{F}_p)} \psi\left(\sum_{i=1}^{r-1} h_i \cdot g_i + h_r (g_1 \dots g_{r-1})^{-1} x\right) \tag{13}$$

for $\boldsymbol{h} = (h_1, \dots, h_r) \in M_n(\mathbb{F}_p)^r$. To do so, it suffices to replace G by G^{r-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 $\boldsymbol{h} = 0$.

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

$$\begin{aligned}
&\frac{1}{|G(\mathbb{F}_p)|} \sum_{g\in G(\mathbb{F}_p)} \sum_{\substack{e\in E_p \\ f\in F_p}} \frac{1}{p^{2n^2}} \sum_{u,v\in M_n(\mathbb{F}_p)} \psi\left(u\cdot(g-e) + v\cdot(g^{-1}x - f)\right) \\
=\ & \frac{1}{p^{2n^2}} \sum_{u,v\in M_n(\mathbb{F}_p)} \sum_{e\in E_p} \overline{\psi}(u\cdot e) \sum_{f\in F_p} \overline{\psi}(v\cdot f) S(u,v) \qquad (14) \\
=\ & \frac{|E_p||F_p|}{p^{2n^2}} + O\left(\frac{1}{p^{2n^2}} \sum_{\substack{u,v\in M_n(\mathbb{F}_p) \\ (u,v)\neq 0}} \left|\sum_{e\in E_p} \overline{\psi}(u\cdot e)\right| \left|\sum_{f\in F_p} \overline{\psi}(v\cdot f)\right| |S(u,v)|\right),
\end{aligned}$$

where $E_p = E \pmod p$, $F_p = F \pmod p \subset \mathbb{F}_p$ and

$$S(u,v) = \frac{1}{|G(\mathbb{F}_p)|} \sum_{g\in G(\mathbb{F}_p)} \psi\left(u\cdot g + v\cdot(g^{-1}x)\right).$$

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

$$\begin{aligned}
\sum_{e\in E_p} \overline{\psi}(u\cdot e) &= \prod_{1\leqslant k,l\leqslant n} \sum_{e_{kl}\in E_{kl}} \overline{\psi}(u_{kl}e_{kl}) \\
&\ll \prod_{1\leqslant k,l\leqslant n} \min\left(|E_{kl}|, ||u_{kl}/p||^{-1}\right),
\end{aligned}$$

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

$$\begin{aligned}
\ll\ & \frac{1}{p^{n^2}} \sum_{v\in M_n(\mathbb{F}_p)} \prod_{1\leqslant k,l\leqslant n} \min\left(|F_{kl}|, ||v_{kl}/p||^{-1}\right) \\
&\times \frac{1}{p^{n^2}} \sum_{\substack{u\in M_n(\mathbb{F}_p) \\ (u,v)\neq 0}} |S(u,v)| \prod_{1\leqslant k,l\leqslant n} \min\left(|E_{kl}|, ||u_{kl}/p||^{-1}\right).
\end{aligned}$$

To bound the sum over u, we proceed as in Proposition 2.7, using [FK01]. With $d = \dim G$,

$$\frac{1}{p^{n^2}} \sum_{\substack{u \in M_n(\mathbb{F}_p) \\ (u,v) \neq 0}} |S(u,v)| \prod_{1 \leqslant k,l \leqslant n} \min\left(|E_{kl}|, ||u_{kl}/p||^{-1}\right) \tag{15}$$

$$\ll \left(\frac{1}{p^{d/2}} \sum_{j=0}^{d-1} p^{j/2} + \sum_{j=d}^{n^2} p^{-1/2} \right) \frac{1}{p^{n^2}} \sum_{u \in X_j(\mathbb{F}_p)} \prod_{1 \leqslant k,l \leqslant n} \min\left(|E_{kl}|, ||u_{kl}/p||^{-1}\right).$$

By [FK01, Lemma 9.5] (or [Fou00, (2.6)]), if $X \subset \mathbb{A}^{n^2}$ has dimension $\leqslant n^2 - j$,

$$\sum_{u \in X(\mathbb{F}_p)} \prod_{1 \leqslant k,l \leqslant n} \min\left(|E_{kl}|, ||u_{kl}/p||^{-1}\right) \ll (p \log p)^{n^2 - j} M_E^j,$$

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

$$\sum_{u \in X(\mathbb{F}_p)} \prod_{1 \leqslant k,l \leqslant n} \min\left(|E_{kl}|, ||u_{kl}/p||^{-1}\right) \ll (p \log p)^{n^2 - j} e_j(|E_{kl}|) \tag{16}$$

when the $|E_{kl}|$ may not be all equal, where e_j is the jth elementary symmetric polynomial in n^2 variables.

Thus, (15) is

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

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

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

By Maclaurin's inequality [Ste04, (12.3)], letting $L_E = e_1(|E_{kl}|)$, this is

$$\ll (\log p)^{n^2} \left(\frac{1}{p^{d/2}} \sum_{j=0}^{d-1} (L_E/\sqrt{p})^j + \frac{(L_E/p)^d}{\sqrt{p}} \right)$$

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

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

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

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

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

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

The main term dominates if and only if

$$x \gg_{n,\varepsilon} p^{1-\frac{1}{2(2n^2-\dim G+1)}+\varepsilon}$$

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

References

[AS07] Omran Ahmadi and Igor E. Shparlinski. Distribution of matrices with restricted entries over finite fields. *Indag. Math. (N.S.)*, 18(3):327–337, 2007.

[Asc84] Michael Aschbacher. On the maximal subgroups of the finite classical groups. *Inventiones mathematicae*, 76(3):469–514, 1984.

[BGS10] Jean Bourgain, Alex Gamburd, and Peter Sarnak. Affine linear sieve, expanders, and sum-product. *Inventiones mathematicae*, 179(3):559–644, March 2010.

[Bro83] Sean Allen Broughton. A note on characters of algebraic groups. *Proceedings of the American Mathematical Society*, 89(1):39–40, 1983.

[Del77] Pierre Deligne. *Cohomologie étale, séminaire de géométrie algébrique du Bois-Marie SGA $4\frac{1}{2}$*, volume 569 of *Lecture notes in Mathematics*. Springer, 1977.

[Del80] Pierre Deligne. La conjecture de Weil. II. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 52(1):137–252, 1980.

[DT97] Michael Drmota and Robert F. Tichy. *Sequences, discrepancies, and applications*. Number 1651 in Lecture notes in mathematics. Springer, 1997.

[FHL$^+$10] Ron Ferguson, Corneliu Hoffman, Florian Luca, Alina Ostafe, and Igor E. Shparlinski. Some additive combinatorics problems in matrix rings. *Revista Matemática Complutense*, 23(2):501–513, July 2010.

[FK01] Etienne Fouvry and Nicholas M. Katz. A general stratification theorem for exponential sums, and applications. *Journal für die reine und angewandte Mathematik*, 2001(504):115–166, 2001.

[FKM15] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. Algebraic twists of modular forms and Hecke orbits. *Geom. Funct. Anal.*, 25(2):580–657, 2015.

[Fou00] Étienne Fouvry. Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums. *Israel Journal of Mathematics*, 120(1):81–96, 2000.

[HL12] Su Hu and Yan Li. Gauss sums over some matrix groups. *Journal of Number Theory*, 132(12):2967 – 2976, dec 2012.

[HL13] Su Hu and Yan Li. On a uniformly distributed phenomenon in matrix groups. *Journal of Number Theory*, 133(11):3578–3588, November 2013.

[Kat01] Nicholas M. Katz. Sums of Betti numbers in arbitrary characteristic. *Finite fields and their Applications*, 7(1):29–44, 2001.

[KL85] Nicholas M. Katz and Gérard Laumon. Transformation de Fourier et majoration de sommes exponentielles. *Inst. Hautes Études Sci. Publ. Math.*, (62):361–418, 1985.

[Shp12] Igor E. Shparlinski. Modular hyperbolas. *Japanese Journal of Mathematics*, 7(2):235–294, November 2012.

[Ste04] J. Michael Steele. *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.

[Wil09] Robert A. Wilson. *The Finite Simple Groups*, volume 251 of *Graduate Texts in Mathematics*. Springer, 2009.

[Xu18] Junyan Xu. Stratification for Multiplicative Character Sums. *International Mathematics Research Notices*, May 2018. rny096.

Centre de Recherches Mathématiques, Université de Montréal, Canada
Current address: Zürich, Switzerland
Email address: `corentin.perretgentil@gmail.com`