On some arithmetic statistics for matrices

Alina Ostafe

Joint work with

Igor Shparlinski

The University of New South Wales

Set-up and motivation

We look at some questions of arithmetic statistics for matrices from

$$\mathcal{M}_n(\mathbb{Z}) = \left\{ A = (a_{ij})_{i,j=1}^n : \ a_{ij} \in \mathbb{Z} \right\}.$$

For a real $H \geq 1$, let

$$\mathcal{M}_n(\mathbb{Z}; H) = \left\{ A = (a_{ij})_{i,j=1}^n : \ |a_{ij}| \leq H \right\}.$$

In particular, $\#\mathcal{M}_n(\mathbb{Z}; H) \sim (2H)^{n^2}$.

More precisely, we discuss various counting results with matrices/tuples of matrices from $\mathcal{M}_n(\mathbb{Z}; H)$ that

(I) have a given characteristic polynomial;
(II) are non-diagonalisable;
(III) are multiplicatively dependent;
(IV) multiplicatively generate a subgroup of $\mathrm{GL}_n(\mathbb{Q})$.

We will see that (I) plays an important role in (II), (III) and (IV).

This work was initially motivated by studying the multiplicative structure of matrices and was inspired by mathematical discussions between *Igor Shparlinski*, *Cam Stewart*, *Humpback* and myself:

AMS Meeting, Hawaii, March 2019

(I) Matrices with a given characteristic polynomial

For fixed $f \in \mathbb{Z}[X]$ of degree n and monic, let

$$\mathcal{R}_n(H; f) = \{A \in \mathcal{M}_n(\mathbb{Z}; H) : \ f \text{ is the characteristic polynomial of } A\}$$

and

$$R_n(H; f) = \#\mathcal{R}_n(H; f).$$

Goal: Motivated by applications to (II), (III) and (IV), we seek a good *uniform* upper bound for $R_n(H; f)$.

One of the coefficients of f is $\det(A)$ for $A \in \mathcal{R}_n(H; f)$, thus it is natural to know first the size

$$D_n(H; d) = \#\mathcal{D}_n(H; d)$$

of the set

$$\mathcal{D}_n(H; d) = \{A \in \mathcal{M}_n(\mathbb{Z}; H) : \ \det A = d\}.$$

Matrices with a given determinant

The size of the set

$$\widetilde{\mathcal{D}}_n(H;d) = \{A \in \mathcal{M}_n(\mathbb{Z}) : \ \|A\|_2 \le H \text{ and } \det A = d\}$$

has been studied by:

- *Duke, Rudnick & Sarnak* (**1993**) for $d \neq 0$,
- *Katznelson* (**1993**) for $d = 0$,

who, for a **fixed** d gave asymptotic formula with the main terms of orders

$$H^{n^2-n} \quad (d \neq 0) \qquad \text{and} \qquad H^{n^2-n}\log H \quad (d = 0).$$

However, these results are not sufficient for us as we need a *uniform* with respect to d upper bound:

Shparlinski (2010)

Uniformly over d, we have $D_n(H;d) \ll H^{n^2-n}\log H$.

As usual: $A \ll B \iff B \gg A \iff A = O(B)$.

Matrices with a given characteristic polynomial

Recall: For fixed $f \in \mathbb{Z}[X]$,

$\mathcal{R}_n(H; f) = \{A \in \mathcal{M}_n(\mathbb{Z}; H) : f$ is the characteristic polynomial of $A\}$,

and

$$R_n(H; f) = \#\mathcal{R}_n(H; f).$$

Eskin, Mozes & Shah (**1996**): asymptotic formula for a variant $\widetilde{R}_n(H; f)$ of $R_n(H; f)$, where the matrices are ordered by the L_2-norm rather than by the L_∞-norm,

$$\widetilde{R}_n(H; f) = (C(f) + o(1))H^{n(n-1)/2},$$

with $C(f) > 0$ depending on a *fixed* monic irreducible $f \in \mathbb{Z}[X]$.

Shah (**2000**), *Wei & Xu* (**2016**): some variants of the above.

Unfortunately this is not sufficient for the applications we have in mind for which we need an upper bound which:

- holds for arbitrary $f \in \mathbb{Z}[X]$, which is not necessary irreducible;
- is uniform with respect to the coefficients of f.

Conjecture (A.O. & Shparlinski)

Uniformly over polynomials f we have

$$R_n(H; f) \leq H^{n(n-1)/2+o(1)}, \qquad \text{as } H \to \infty.$$

Since we obviously have

$$R_n(H; f) \leq D_n(H; d) = \#\{A \in \mathcal{M}_n(\mathbb{Z}; H) : \det A = d\}$$

and

Shparlinski (2010)

Uniformly over d, we have $D_{n,s}(H; d) \ll H^{n^2-n} \log H$.

we call the bound

$$R_n(H; f) \leq H^{n^2-n+o(1)}$$

trivial.

We define γ_n as the largest real number such that uniformly over polynomials f we have

$$R_n(H; f) \le H^{n^2-n-\gamma_n+o(1)}, \qquad \text{as } H \to \infty.$$

Remark: $\gamma_n = n(n-1)/2$ corresponds to the above *Conjecture*, while by *Shparlinski* (**2010**) it always holds with $\gamma_n = 0$.

What we can prove is somewhere *in-between* ... but unfortunately it is not in the middle, it is closer to the bottom end.

The above holds with

$$\gamma_2 = \gamma_3 = 1 \qquad \text{and} \qquad \gamma_n \ge \frac{1}{(n-3)^2}, \quad \text{for } n \ge 4.$$

Remark: Only $\gamma_2 = 1$ corresponds the above *Conjecture*: $\gamma_n = n(n-1)/2$.

We get $\gamma_n \approx 1/n^2$ while we expect $\gamma_n \approx n^2/2$.

Bounds

For $n = 2, 3$ we estimate $R_n(H; f)$ directly:

A.O. & Shparlinski (2022)

For $n = 2, 3$, uniformly over $f \in \mathbb{Z}[X]$ with $\deg f = n$ we have

$$R_2(H; f) \le H^{1+o(1)} \quad \textit{and} \quad R_3(H; f) \le H^{5+o(1)}.$$

For $n \ge 4$ we count matrices with fixed determinant and trace, i.e.,

$$S_n(H; d, t) = \#\mathcal{S}_n(H; d, t)$$

where $\mathcal{S}_n(H; d, t) = \{A \in \mathcal{M}_n(\mathbb{Z}; H) : \ \det A = d \text{ and } \mathrm{Tr}(A) = t\}$.

A.O. & Shparlinski (2022)

For $n \ge 4$, uniformly over d and t we have

$$S_n(H; d, t) \ll H^{n^2 - n - \sigma_n}, \qquad n \ge 4,$$

where $\sigma_n = 1/(n-3)^2$.

Ideas behind the proof

★ For $n = 2, 3$ we write the equations for $\mathrm{Tr}(A)$, $\mathrm{Tr}(A^2)$ and $\det A$, eliminate variables, use a bound on the divisor function, etc.

★ For $n \geq 4$ we use very different approach, which we sketch below.

For a vector $\mathbf{u}$ (of any dimension), we use $|\mathbf{u}|$ for its L_∞-norm.

We write $A \in \mathcal{M}_n(\mathbb{Z}; H)$ in the form

$$A = \begin{pmatrix} R^* & \mathbf{a}^* \\ (\mathbf{b}^*)^T & a_{nn} \end{pmatrix}$$

for some

$$R^* \in \mathcal{M}_{n-1}(\mathbb{Z}; H), \qquad \mathbf{a}^*, \mathbf{b}^* \in \mathbb{Z}^{n-1}, \qquad a_{nn} \in \mathbb{Z},$$

with

$$|\mathbf{a}^*|, |\mathbf{b}^*| \leq H \quad \text{and} \quad |a_{nn}| \leq H.$$

Reduction

Recall

$$A = \begin{pmatrix} R^* & \mathbf{a}^* \\ (\mathbf{b}^*)^T & a_{nn} \end{pmatrix} \in \mathcal{S}_n(H; d, t), \qquad \det A = d, \qquad \mathrm{Tr}(A) = t.$$

- We first count matrices $\in \mathcal{S}_n(H; d, t)$ with $\mathbf{a}^* = 0$ or $\mathbf{b}^* = \mathbf{0}$, $\Longrightarrow$ $H^{n^2-n-1+o(1)}$ matrices.
- Next, we count matrices $R^* \in \mathcal{M}_{n-1}(\mathbb{Z}; H)$ for which there are unique $\mathbf{a}^*$, $\mathbf{b}^*$ with $A \in \mathcal{S}_n(H; d, t) \Longrightarrow H^{(n-1)^2} \le H^{n^2-n-1+o(1)}$ matrices.
- Hence, it remains to count triples $(R^*, \mathbf{a}^*, \mathbf{b}^*)$ with $A \in \mathcal{S}_n(H; d, t)$ such that $R^* \in \mathcal{M}_{n-1}(\mathbb{Z}; H)$ appears for at least two distinct triples $(R^*, \mathbf{a}_1^*, \mathbf{b}_1^*)$ and $(R^*, \mathbf{a}_2^*, \mathbf{b}_2^*)$.

$$\Downarrow$$

Algebraic manipulations reduce this to bounding $\#\mathcal{U}_n(2H)$, where

$$\mathcal{U}_n(K) = \{A \in \mathcal{M}_n(\mathbb{Z}; K) : \ \det A = 0, \ \mathbf{a}^*, \mathbf{b}^* \neq \mathbf{0}, \ a_{nn} = 0\}.$$

Adapting Katznelson's idea

- Since $\det A = 0$, there is non-zero vector $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$ such that $A\boldsymbol{\lambda} = \mathbf{0}$. Since $\mathbf{a}^*, \mathbf{b}^* \neq \mathbf{0}$ we have $\boldsymbol{\lambda} \neq (0, \ldots, 0, 1)$.
- *Katznelson* (**1993**) has refined this as following: there is a primitive (i.e. with $\gcd(\lambda_1, \ldots, \lambda_n) = 1$) vector $\boldsymbol{\lambda} \in \mathbb{Z}^n$ such that

$$A\boldsymbol{\lambda} = \mathbf{0} \quad \text{and} \quad |\boldsymbol{\lambda}| \ll H^{n-1},$$

and such that the lattice

$$\mathcal{L}_\lambda = \{\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n : \; u_1\lambda_1 + \ldots + u_n\lambda_n = 0\}$$

has a basis of size $O(H)$, i.e., an almost *orthogonal* basis.
- We call such primitive $\boldsymbol{\lambda} \in \mathbb{Z}^n$ for which $\mathcal{L}_\lambda$ has a short basis *H-good*.
- Next, we split $\#\mathcal{U}_n(H)$ into contributions $U_n(H; \boldsymbol{\lambda})$ from each *primitive H-good vector $\boldsymbol{\lambda}$*:

$$\#\mathcal{U}_n(H) \leq \sum_{|\boldsymbol{\lambda}| \leq c_0 H^{n-1}}^{\sharp} U_n(H; \boldsymbol{\lambda}),$$

where $\Sigma^\sharp$ means that the sum runs over primitive H-good $\boldsymbol{\lambda} \neq (0, \ldots, 0, 1)$, and $U_n(H; \boldsymbol{\lambda}) = \#\{A \in \mathcal{U}_n(H) : \; A\boldsymbol{\lambda} = 0\}$.

- The top $n-1$ rows of A come from the lattice
$$\mathcal{L}_\lambda = \{\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n : \ u_1\lambda_1 + \ldots + u_n\lambda_n = 0\}.$$
- The bottom row belongs to the lattice
$$\mathcal{L}_\lambda^* = \{\mathbf{v} = (v_1, \ldots, v_{n-1}) \in \mathbb{Z}^{n-1} : \ v_1\lambda_1 + \ldots + v_{n-1}\lambda_{n-1} = 0\}.$$
- To count the number of possibilities for the top $n-1$ rows, as in *Katznelson* (**1993**), we use a result of *Schmidt* (**1968**) on counting integer lattice points in a box.
- For the bottom row, unfortunately, we control neither *primitiveness* nor *H-goodness* of $(\lambda_1, \ldots, \lambda_{n-1})$, so now our argument deviates from that of *Katznelson* (**1993**).
  We need to count lattice points in "bad" (="skewed") lattices $\mathcal{L}_\lambda^*$. To do this, we introduce a measure of quality of $\boldsymbol{\lambda}$ and count the number of $\boldsymbol{\lambda}$ with this parameter in a dyadic interval. This is the most involved part of the argument.

Question

Can we get a better bound if we also fix $\mathrm{Tr}A^2$ *(besides* $\det A$ *and* $\mathrm{Tr}A$*)?*

(II) Non-diagonalisable matrices

Let $K_n(H) =$ the number of of matrices from $\mathcal{M}_n(\mathbb{Z}; H)$ which are not diagonalisable.

Hetzel, Liew & Morrison (**2007**): counting matrices with a repeated eigenvalue, they show that

$$K_n(H) = O\left(H^{n^2-1}\right).$$

Using again that the characteristic polynomial of a non-diagonalisable matrix has a multiple root, under the **Conjecture** above on $R_n(H; f)$, one has

$$K_n(H) \le H^{\frac{(n-1)(n+2)}{2}+o(1)}.$$

For $n = 2$, the conjecture holds and we get:

$$H^2 \ll K_2(H) \le H^{2+o(1)}.$$

Unconditionally we can prove the following, improving *Hetzel, Liew & Morrison* (**2007**).

A.O. & Shparlinski (In progress)

For $n \geq 3$, we have

$$H^{\frac{n^2-(n-2)}{2}} \ll K_n(H) \ll H^{n^2-\Delta_n} \log H,$$

where

$$\Delta_n = \max_{r=1,\ldots,n} \min\left\{n - \frac{r(r+1)}{2}, r+1\right\}.$$

One has

$$\Delta_3 = \Delta_4 = 2, \qquad \Delta_5 = \ldots = \Delta_8 = 3,$$

and

$$\lim_{n\to\infty} \Delta_n/\sqrt{2n} = 1.$$

For some small values of n, a tweak of the argument gives better bounds:

$$K_5(H), K_7(H) \leq H^{5^2-4+o(1)}, \qquad K_8(H) \leq H^{8^2-5+o(1)}.$$

The proof relies on counting matrices with given determinant or characteristic polynomial and modular reduction for an appropriately chosen prime.

(III) Multiplicative dependence: Motivation

We say that $\mathbf{a} = (a_1, \ldots, a_s) \in \mathbb{C}^s$ is multiplicatively dependent if there is a non-zero vector $(k_1, \ldots, k_s) \in \mathbb{Z}^s$ for which

$$a_1^{k_1} \cdots a_s^{k_s} = 1.$$

Pappalardi, Sha, Shparlinski & Stewart (**2018**): an asymptotic formula for the number of multiplicatively dependent s-tuples of integers in the cube $[-H, H]^s$, and similar results for algebraic numbers of bounded degree/in a given number field, and of height at most H.

Stewart (**2019**), *Konyagin, Sha, Shparlinski & Stewart* (**2020**): studied the distribution of multiplicatively dependent vectors in $\mathbb{R}^n$ and $\mathbb{C}^n$.

In the matrix setting, we say that $(A_1, \ldots, A_s) \in \mathcal{M}_n(\mathbb{Z})^s$ is *multiplicatively dependent* if there is a non-zero vector $(k_1, \ldots, k_s) \in \mathbb{Z}^s$ such that

$$A_1^{k_1} \ldots A_s^{k_s} = I_n,$$

where I_n is the $n \times n$ identity matrix.

Comment

The matrix version of this problem looks *typographically* very similarly however it is of very different spirit and requires different tools due to:

- Non-commutativity of matrix multiplication (e.g., multiplicative dependence may change if the entries of $(A_1, \ldots, A_s)$ are permuted).
- One of the main tools used in the number case: the existence and uniqueness of prime number factorisation, is missing.
- Non-commutativity suggests the following, alternative definition of multiplicative dependence, which we call *non-freeness*. We say that $(A_1, \ldots, A_s) \in \mathcal{M}_n(\mathbb{Z})^s$ is **not free** if there is a nontrivial word (i.e., without occurrences of $A_i A_i^{-1}$) of length $L \geq 1$ of the form

$$A_{i_1}^{\pm 1} \cdots A_{i_L}^{\pm 1} = I_n.$$

What do we count?

We are interested in the following quantities:

$$\mathcal{N}_{n,s}(H) = \{(A_1, \ldots, A_s) \in \mathcal{M}_n(\mathbb{Z}; H)^s : \ (A_1, \ldots, A_s) \text{ is mult. dep.}\};$$

$$\mathcal{N}^*_{n,s}(H) = \{(A_1, \ldots, A_s) \in \mathcal{N}_{n,s}(H) : \\ (A_1, \ldots, A_s) \text{ is mult. dep. of maximal rank}\},$$

where maximal rank $=$ any sub-tuple $(A_{i_1}, \ldots, A_{i_t})$ of length $t < s$ with $1 \le i_1 < \ldots < i_t \le s$ is mult. indep.;

$$\mathcal{F}_{n,s}(H) = \{(A_1, \ldots, A_s) \in \mathcal{M}_n(\mathbb{Z}; H)^s : \ (A_1, \ldots, A_s) \text{ is non-free}\}.$$

Goal

We want good lower and upper bounds for:

- $\#\mathcal{N}_{n,s}(H)$, mult. dep. matrices; $\checkmark$
- $\#\mathcal{N}_{n,s}(H)^*$, mult. dep. matrices of maximal rank; $\checkmark$
- $\#\mathcal{F}_{n,s}(H)$, non-free matrices. **???** *(see K. Bulinski's talk)*

For $n = 1$ these questions are **exactly** the same as studied by *Pappalardi, Sha, Shparlinski & Stewart* (**2018**).

However, the matrix setting is very different and needs new ideas.

Observation

Taking determinants in

$$A_1^{k_1} \cdots A_s^{k_s} = I_n \quad \text{and} \quad A_{i_1}^{\pm 1} \cdots A_{i_L}^{\pm 1} = I_n$$

helps to overcome both obstructions.

Generally speaking we *want* results which are **stronger** than what this approach gives.

. . . this does not mean we can always get such results, but in some cases we can indeed.

Here is how the above approach works.

- Taking determinants we obtain a multiplicative relation between $\det A_1, \ldots, \det A_s$.
- Count the number of s-tuples of integers in $[-n!H^n, n!H^n]$ which are multiplicatively dependent.
- Finally, we need to estimate the number of matrices $A \in \mathcal{M}_n(\mathbb{Z}; H)$ with a given determinant.
- However, to go beyond this approach and obtain stronger results, we need to count matrices with a given characteristic polynomial.

Counting multiplicatively dependent matrices of maximal rank

Recall:

$$\mathcal{N}^*_{n,s}(H) = \{(A_1, \ldots, A_s) \in \mathcal{N}_{n,s}(H) : \\ (A_1, \ldots, A_s) \text{ is mult. dep. of maximal rank}\}.$$

A.O. & Shparlinski (2022)

We have

$$H^{sn^2 - \lceil s/2 \rceil n + o(1)} \geq \#\mathcal{N}^*_{n,s}(H) \geq \begin{cases} H^{(s-1)n^2/2 + n/2 + o(1)}, & \text{if } s \text{ is even}, \\ H^{(s-1)n^2/2 + o(1)}, & \text{if } s \text{ is odd}. \end{cases}$$

Idea of proof: Upper bound

- Let $(A_1, \ldots, A_s) \in \mathcal{M}_n(\mathbb{Z}; H)^s$ be such that

$$A_1^{k_1} \ldots A_s^{k_s} = I \qquad \text{for some } k_1, \ldots, k_s \in \mathbb{Z} \setminus \{0\} \textit{ (max. rank!)}$$

$$\Downarrow$$

$$\prod_{i \in \mathcal{I}} (\det A_i)^{|k_i|} = \prod_{j \in \mathcal{J}} (\det A_j)^{|k_j|}, \qquad (\star)$$

with $\mathcal{I} \cup \mathcal{J} = \{1, \ldots, s\}$, $\mathcal{I} \cap \mathcal{J} = \emptyset$ and $|k_h| > 0$, $h = 1, \ldots, s$.

- Fix $\mathcal{I}$ and $\mathcal{J}$ as above and count s-tuples for which $(\star)$ is possible with these sets $\mathcal{I}$ and $\mathcal{J}$ and some exponents $|k_h| > 0$, $h = 1, \ldots, s$. Let $I = \#\mathcal{I}$ and $J = \#\mathcal{J}$.
- Assume $J \le I$ (and thus $I \ge \lceil s/2 \rceil$) and fix J matrices A_j, $j \in \mathcal{J}$, trivially in at most

$$\mathfrak{A}_1 = O\left(H^{Jn^2}\right)$$

ways.

- Let

$$Q = \prod_{j \in \mathcal{J}} \det A_j .$$

- $\det A_i$, $i \in \mathcal{I}$, are factored from the prime divisors of Q and thus one can show that each of them can take at most $H^{o(1)}$ values.

$$\Downarrow$$

Shparlinski (**2010**): each of the matrices A_i can take at most $H^{n^2-n+o(1)}$ values. Hence the total number of choices for the I-tuple $(A_i)_{i\in\mathcal{I}}$ is at most

$$\mathfrak{A}_2 = H^{In^2-In+o(1)}.$$

$$\Downarrow$$

Total number of s-tuples $(A_1, \ldots, A_s) \in \mathcal{M}_n(\mathbb{Z}; H)^s$ satisfying $(\star)$ for at least one choice of the exponents is at most

$$\mathfrak{A}_1\mathfrak{A}_2 = H^{Jn^2+In^2-In+o(1)} = H^{sn^2-\lceil s/2\rceil n+o(1)}.$$

Lower bound

Assume $s = 2r$ (similar construction also works for $s = 2r + 1$).

- One can show *inductively* that there are $K^{sn^2+o(1)}$ choices for s-tuples $(B_1, \ldots, B_s) \in \mathcal{M}_n(\mathbb{Z}; K)^s$ of non-singular matrices such that for every $j = 2, \ldots, s$, $\det B_j$ contains a prime divisor which does not divide $\det B_1 \ldots \det B_{j-1}$.
- Let $K = \left\lfloor (H/n)^{1/2} \right\rfloor$. For any choice of $(B_1, \ldots, B_s) \in \mathcal{M}_n(\mathbb{Z}; K)^s$ as above, we define

$$A_{2i-1} = B_{2i-1}B_{2i}, \qquad A_{2i} = B_{2i+1}B_{2i}, \qquad i = 1, \ldots, r,$$

where we also set $B_{2r+1} = B_{s+1} = B_1$. Clearly

$$A_1 A_2^{-1} \ldots A_{2r-1} A_{2r}^{-1} = I.$$

$$\Downarrow$$

$$(A_1, \ldots, A_s) \in \mathcal{N}^*_{n,s}(H).$$

- In principle different choices $(B_1, \ldots, B_s)$ can lead to the same $(A_1, \ldots, A_s)$ in the above construction.

$$\Downarrow$$

We need to eliminate possible repetitions.

- When $(A_1, \ldots, A_s)$ and B_1 are fixed then the other matrices $B_2, \ldots, B_s$ are uniquely defined.
- Hence each s-tuple $(A_1, \ldots, A_s)$ comes from at most $K^{n^2-n+o(1)}$ different choices of $(B_1, \ldots, B_s) \in \mathcal{M}_n(\mathbb{Z}; K)^s$

$$\Downarrow$$

$$\#\mathcal{N}_{n,s}^*(H) \geq K^{sn^2-n^2+n+o(1)} = H^{n((s-1)n+1)/2+o(1)}$$

for an even s.

Background on totients

Recall that m is called a *totient* if it is a value of the Euler function $m = \varphi(k)$ for some integer k.

Since $1 = \varphi(1)$ is a totient, each integer can be represented as a sum of some number $h \geq 1$ of totients and hence we can define

$$w(n) = \max \left\{ \sum_{j=1}^{h} \varphi(k_j)^2 : \; n = \sum_{j=1}^{h} \varphi(k_j) \right\},$$

where the maximum is taken over all such representations of all possible lengths $h \geq 1$.

In particular, by *Baker, Harman & Pintz* (**2001**) on prime gaps:

$$n^2 \geq w(n) \geq \left(n - n^{21/40}\right)^2 \geq n^2 - 2n^{61/40}$$

for a sufficiently large n.

Counting multiplicatively dependent matrices

Recall that $R_n(H; f)$ is the number of matrices $A \in \mathcal{M}_n(\mathbb{Z}; H)$ with a given characteristic polynomial $f \in \mathbb{Z}[X]$ and γ_n is the largest real number such that uniformly over polynomials f we have

$$R_n(H; f) \le H^{n^2 - n - \gamma_n + o(1)}, \qquad \text{as } H \to \infty.$$

A.O. & Shparlinski (2022)

With γ_n as above, we have

$$H^{sn^2 - n - \min\{n, \gamma_n\} + o(1)} \ge \#\mathcal{N}_{n,s}(H) \ge H^{(s-1)n^2 + w(n)/2 - n/2}.$$

Upper bound

If any multiplicative relation between $(A_1, \ldots, A_s) \in \mathcal{M}_n(\mathbb{Z}; H)^s$ involves at least $r \geq 3$ matrices, we use our bound on $\mathcal{N}^*_{n,r}(H) \leq H^{rn^2-2n+o(1)}$. The total contribution from such s-tuples is

$$H^{rn^2-2n+o(1)} H^{(s-r)n^2} = H^{sn^2-2n+o(1)}.$$

For s-tuples $(A_1, \ldots, A_s) \in \mathcal{M}_n(\mathbb{Z})^s$ with a multiplicative relation between two matrices, call them A and B, we get an equation of the type

$$A^k = B^m, \qquad \text{for some } (k, m) \in \mathbb{Z}^2 \setminus \{(0,0)\}.$$

Despite that k and m *are not fixed*, one can show that there are $H^{o(1)}$ possibilities for $\mathrm{Spectrum}\, A$ when $\mathrm{Spectrum}\, B$ is fixed.

This allows us to invoke our bound on $R_n(H; f) \leq H^{n^2-n-\gamma_n+o(1)}$. The total contribution from such s-tuples is

$$H^{n^2} H^{n^2-n-\gamma_n+o(1)} H^{(s-2)n^2} = H^{sn^2-n-\gamma_n+o(1)}.$$

Construction for the lower bound (simplified)

Let $\Phi_k(X)$ be the kth cyclotomic polynomial, of degree $\varphi(k) = m \le n$. Since Φ_k is monic & irreducible by *Eskin, Mozes & Shah* (**1996**) there are

$$R_m(H; \Phi_k) \gg H^{m(m-1)/2}$$

matrices $B \in \mathcal{M}_m(\mathbb{Z}; H)$ for which $\Phi_k(B) = 0$: $\Longrightarrow B^k = I$. Then

$$A = \begin{pmatrix} I_{n-m} & \mathbf{0} \\ \mathbf{0} & B \end{pmatrix} \Longrightarrow A^k = I_n.$$

Choosing A_1 as one of such matrices and arbitrary $A_2, \ldots, A_s$, we obtain

$$\#\mathcal{N}_{n,s}(H) \gg H^{(s-1)n^2} R_m(H; \Phi_k).$$

Remark: We can do better by putting more "roots of identity" of orders $k_1, \ldots, k_h$ along the main diagonal:

$$A = \begin{pmatrix} B_1 & & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & & B_h \end{pmatrix} \Longrightarrow A^{k_1 \ldots k_h} = I_n.$$

(IV) Boundedly generated subgroups

A group $\Gamma \le \mathrm{GL}_n(\mathbb{Q})$ is *boundedly generated* if $\exists\, A_1, \ldots, A_s \in \mathrm{GL}_n(\mathbb{Q})$:

$$\Gamma = \{A_1^{k_1} \ldots A_s^{k_s} : \; k_1, \ldots, k_s \in \mathbb{Z}\} = \langle A_1 \rangle \ldots \langle A_s \rangle.$$

Inspired by recent work of *Corvaja, Demeio, Rapinchuk, Ren & Zannier* (**2022**) on sparsity of elements of boundedly generated subgroups of $\mathrm{GL}_n(\mathbb{Q})$ we look at a dual question and count elements of the set:

$$\mathcal{G}_{n,s}(H) = \{(A_1, \ldots, A_s) \in \mathcal{M}_n(\mathbb{Z}; H) : \; \langle A_1 \rangle \ldots \langle A_s \rangle \le \mathrm{GL}_n(\mathbb{Q})\}.$$

Remark: The fact that $I_n \in \Gamma$ does not allow us to use our bounds on $\#\mathcal{N}_{n,s}(H)$ since now the choice $k_1 = \ldots = k_s = 0$ is not excluded.

A.O. & Shparlinski (2022)

For $n \ge 2$, we have

$$\#\mathcal{G}_{n,s}(H) \le H^{sn^2 - sn/3 + o(1)}.$$

Commuting matrices

As a part of the argument, we need to count, for a given matrix A, the number of matrices $B \in \mathcal{M}_n(\mathbb{Z}; H)$ which belong to the *centraliser* of A, that is, bound the cardinality of the set

$$\mathcal{C}_n(A, H) = \{B \in \mathcal{M}_n(\mathbb{Z}; H) : \ AB = BA\}.$$

A.O. & Shparlinski (2022)

Assume that A has either a row or a column with two non-zero elements. Then

$$\#\mathcal{C}_n(A, H) \ll H^{n^2-n}.$$

This also motivates a dual question of estimating the cardinality of the set

$$\mathcal{C}_n(H) = \{(A, B) \in \mathcal{M}_n(\mathbb{Z}; H)^2 : \ AB = BA\}.$$

Using *Feit and Fine* (**1960**) on counting commuting matrices over $\mathbb{F}_q$, applied with a prime $q = p$ satsifying $2H < p \ll H$, implies that $\#\mathcal{C}_n(H) \ll H^{n^2+n}$, but we seek better bounds.

(V) More questions

Of course, we want to see our bounds improved but here we formulate several other possible directions of research.

Multiplicatively dependent $\mathrm{SL}_n(\mathbb{Z})$ matrices

Our methods always exploit multiplicative relations between determinants. Thus we have *no nontrivial bounds* for $\mathrm{SL}_n(\mathbb{Z})$ matrices (for $n > 2$).

Multiplicatively dependent symmetric matrices

Shparlinski (**2010**): *nontrivial* upper bound for the number of symmetric matrices $A \in \mathcal{M}_n(\mathbb{Z}; H)$ of given determinant but it is rather *weak* and is not expected to be tight. Getting a good bound on

$$\#\{A \in \mathcal{M}_n(\mathbb{Z}; H) : \ A = A^t, \ \det A = d\}$$

can be the first step towards extending our results to symmetric matrices and is of independent interest.

Commutators

A matrix $C \in \mathcal{M}_n(\mathbb{Z})$ is called a *commutator* if $C = ABA^{-1}B^{-1}$ for some $A, B \in \mathcal{M}_n(\mathbb{Z})$.

Can we get a nontrivial bound on the number of commutators in $\mathcal{M}_n(\mathbb{Z}; H)$?

Clearly if $C = ABA^{-1}B^{-1}$, then $\det C = 1$, and thus by *Duke, Rudnick & Sarnak* (**1993**) we have at most H^{n^2-n} such matrices, which we call to be the *trivial* bound.