

Arithmetic statistics of rational matrices of bounded height

Muhammad (Afif) Afifurrahman

joint work with Vivian Kuperberg (ETH Zürich), Alina Ostafe and Igor E. Shparlinski

School of Mathematics and Statistics
University of New South Wales, Sydney, Australia

UNSW Number Theory Seminar, 1 May 2024

Motivation: the integer matrices

- Consider a set of matrices \mathcal{M} . We would like to count the number of matrices in \mathcal{M} with a given rank, determinant, or characteristic polynomial.
- There have been a lot of works on the statistics of matrices in $\mathcal{M}_n(\mathbb{Z}; H)$, the set of $n \times n$ integer matrices with entries bounded by H in absolute value.
- Katznelson (1994) gave an asymptotic formula on the number of matrices in $\mathcal{M}_n(\mathbb{Z}; H)$ with a given rank.
- Katznelson (1993), Duke-Rudnick-Sarnak (1994), and Shparlinski (2010) gave bounds on the number of matrices in $\mathcal{M}_n(\mathbb{Z}; H)$ with a given determinant.
- Ostafe and Shparlinski (2022) bounded the number of matrices in $\mathcal{M}_n(\mathbb{Z}; H)$ with a given characteristic polynomial.
- We also have similar results on matrices over finite fields; see Fisher (1966) and Reiner (1961).

From integer matrices to rational matrices

- A natural extension of this family of problems is to replace integer matrices with rational matrices (of restricted height).
- We consider two different sets of rational numbers in our work,

$$\mathcal{F}(H) = \{a/b : a, b \in \mathbb{Z}, 0 \leq |a|, b \leq H, \gcd(a, b) = 1\},$$
$$\mathcal{E}(H) = \{1/a : a \in \mathbb{Z}, 1 \leq |a| \leq H\}.$$

These are *Farey fractions* and *Egyptian/unit fractions* with height at most H .

- Their cardinalities are

$$\#\mathcal{F}(H) \sim \frac{12}{\pi^2} H^2, \quad \#\mathcal{E}(H) \sim 2H.$$

- Based on these sets, define

$$\mathcal{M}_{m,n}(\mathbb{Q}; H) = \{A = (a_{i,j})_{1 \leq i,j \leq n} : a_{i,j} \in \mathcal{F}(H), i = 1, \dots, m, j = 1, \dots, n\}$$

as the set of $m \times n$ matrices whose entries are Farey fractions of height at most H .

- We also define $\mathcal{M}_{m,n}(\mathbb{Z}^{-1}; H)$ as the set of $m \times n$ matrices whose entries are Egyptian fractions of height at most H .
- We note that

$$\#\mathcal{M}_{m,n}(\mathbb{Q}; H) \sim \left(\frac{12}{\pi^2}\right)^{mn} H^{2mn}, \quad \#\mathcal{M}_{m,n}(\mathbb{Z}^{-1}; H) \sim (2H)^{mn}.$$

The problem over rational matrices

- We consider the problem of bounding the numbers of matrices in $\mathcal{M}_n(\mathbb{Q}; H)$ and $\mathcal{M}_n(\mathbb{Z}^{-1}; H)$ which have a given rank, determinant, or characteristic polynomial.
- Obstacle in working over rational numbers: Additions of two rational numbers of height H can result in a number of height H^2 .
- Another obstacle: The sets $\mathcal{F}(H)$ and $\mathcal{E}(H)$ are not “discrete” and do not seem to yield to methods of geometry of numbers (e.g. counting over lattices).
- We will be working with mn variables, each between $[-H, H]$.
- Some main tools of our problems for general dimensions are: using Laplace expansions over the rows of the matrices, using the divisor bound ($\tau(n) \ll n^{o(1)}$) and bounding the number of solutions of the related equations over Farey fractions or Egyptian fractions.
- Furthermore, we can improve our results for small n by working with the variables directly.

- We are only concerned about the order of magnitude in our bounds.
- We use the notation

$$U \ll V \iff V \gg U \iff |U| \leq cV$$

for some positive constant c that only depends on the dimension m and n .

- We also write $U = V^{o(1)}$ if, for a fixed $\varepsilon > 0$, $V^{-\varepsilon} \leq U \leq V^\varepsilon$ for sufficiently big V .

Matrices with given rank

For $n \geq m$, let

$$\mathcal{L}_{m,n,r}(\mathfrak{A}; H) = \{A \in \mathcal{M}_{m,n}(\mathfrak{A}; H) : \text{rank } A = r\}.$$

with $\mathfrak{A} \in \{\mathbb{Q}, \mathbb{Z}^{-1}\}$. For the lower bound, we have

$$\#\mathcal{L}_{m,n,r}(\mathbb{Q}; H) \gg H^{2nr}, \quad \#\mathcal{L}_{m,n,r}(\mathbb{Z}^{-1}; H) \gg H^{nr}$$

from matrices whose last $m - r$ rows are identical to the first row,

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{r,1} & a_{r,2} & \dots & a_{r,n} \\ a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{1,1} & a_{1,2} & \dots & a_{1,n} \end{pmatrix}.$$

For the case of integer matrices, Katznelson (1994) proved that $\#\mathcal{L}_{m,n,r}(\mathbb{Z}; H)$ is asymptotically $cH^{nr} \log H$, for some $c > 0$ not depending on H .

MA, Kuperberg, Ostafe, Shparlinski (2024)

For $n \geq m > r$ we have

$$\#\mathcal{L}_{m,n,r}(\mathbb{Q}; H) \leq \begin{cases} H^{2mr+nr+n-r^2-r+o(1)}, & \text{if } 2m \geq n+r, \\ H^{2nr+2m-2r+o(1)}, & \text{if } 2m < n+r. \end{cases}$$

In particular, when $m = n$,

$$\#\mathcal{L}_{n,n,r}(\mathbb{Q}; H) \leq H^{3nr+n-r^2-r+o(1)}.$$

Sketch of the proof: given rank, $\#\mathcal{L}_{m,n,r}(\mathbb{Q}; H)$

Consider a matrix A with entries in $\mathcal{F}(H)$ and rank r :

$$\left(\begin{array}{c|c} A_r & C_1 \\ \hline B_r & C_2 \end{array} \right).$$

- We fix an invertible $r \times r$ matrix A_r in H^{2r^2} ways.
- Key observation: each of the other rows of A can be represented as a unique linear combination of the first r rows of A .
- We count the possible number of choices of the $(n-r) \times r$ matrix B_r and $r \times (n-r)$ matrix C_1 based on the number t of nonzero coefficients of the corresponding linear combination.
- We will have a unique choice for the rest of the entries.

- In particular, to bound the number of choices for C_1 , we need to bound the number of solutions of equations of the form

$$\rho_1(h)a_{1,j} + \dots + \rho_r(h)a_{r,j} - a_{h,j} = 0,$$

with $t + 1$ nonzero coefficients $\rho_i(h)$ and $a_{1,j}, \dots, a_{r,j}, a_{h,j} \in \mathcal{F}(H)$ for some indices h and j .

- We eventually have

$$L_{n,r}(\mathbb{Q}; H) \leq H^{2r^2} \sum_{t=1}^r H^{2t(n-r)} (H^{2r-t+1+o(1)})^{n-r} \leq H^{r(3n-r-1)+n+o(1)}.$$

- These arguments can be applied, with relevant modifications, to give an upper bound for $L_{m,n,r}(\mathbb{Z}^{-1}; H)$.

Matrices with given rank: $\#\mathcal{L}_{m,n,r}(\mathbb{Z}^{-1}; H)$

MA, Kuperberg, Ostafe, Shparlinski (2024)

- If $r = 1$,

$$\#\mathcal{L}_{m,n,1}(\mathbb{Z}^{-1}; H) \leq H^{n+o(1)}.$$

- If $r = 2$,

$$\#\mathcal{L}_{m,n,2}(\mathbb{Z}^{-1}; H) \ll \begin{cases} H^{7+o(1)}, & \text{if } (m, n) = (3, 3), \\ H^{2n+m-3+o(1)}, & \text{if } (m, n) \neq (3, 3). \end{cases}$$

- If $r \geq 3$,

$$\#\mathcal{L}_{m,n,r}(\mathbb{Z}^{-1}; H) \ll \begin{cases} H^{(n-r)(r+1)/2+mr+o(1)}, & \text{if } 2m \geq n+r, \\ H^{nr+m-r}, & \text{if } 2m < n+r. \end{cases}$$

We have matching lower bounds for $r = 1$ and $(m, r) = (3, 2)$, $n > 3$.

Improving the bound of $L_{m,n,r}(\mathbb{Z}^{-1}, H)$ for small ranks

- For the case $r = 1, 2$, we improve the upper bounds with a different argument, based on the fact that all $(r + 1) \times (r + 1)$ submatrices of the related matrix are singular.
- For $r = 2$, $3 \leq i \leq m$, $3 \leq j \leq n$, consider the singular submatrix

$$\begin{pmatrix} 1/a_{1,1} & 1/a_{1,2} & 1/a_{1,j} \\ 1/a_{2,1} & 1/a_{2,2} & 1/a_{2,j} \\ 1/a_{i,1} & 1/a_{i,2} & 1/a_{i,j} \end{pmatrix}.$$

- We bound the number of possible entries in this submatrix using the Laplace expansion with respect to the last row and column, dividing the cases base on the structure of the main matrix.
- We have

$$\begin{aligned} \#\mathcal{L}_{m,n,2}(\mathbb{Z}^{-1}; H) &\leq H^{m+n+1+o(1)} + H^{2n+m-3+o(1)} \\ &\quad + H^{2m+n-3+o(1)} + H^{m+n+o(1)} \\ &= \begin{cases} H^{7+o(1)}, & \text{if } (m, n) = (3, 3), \\ H^{2n+m-3+o(1)}, & \text{if } (m, n) \neq (3, 3). \end{cases} \end{aligned}$$

- Similar arguments, but simpler, are used for the case $r = 1$.

Matrices with given determinant

Let

$$\mathcal{D}_n(\mathfrak{A}; H, \delta) = \{A \in \mathcal{M}_{n,n}(\mathfrak{A}; H) : \det A = \delta\}.$$

For the lower bound, we have

$$\#\mathcal{D}_n(\mathbb{Q}; H, 0) \gg H^{2n^2-2n}, \quad \#\mathcal{D}_n(\mathbb{Z}^{-1}; H, 0) \gg H^{n^2-n}, \quad \#\mathcal{D}_n(\mathbb{Q}; H, 1) \gg H^{n^2+o(1)},$$

attained by matrices of the form

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n} \\ a_{n-1,1} & \cdots & a_{n-1,n} \end{pmatrix}, \quad \begin{pmatrix} p_1/p_2 & a_{1,2} & \cdots & a_{1,n-1} & a_{1,n} \\ 0 & p_2/p_3 & \cdots & a_{2,n} & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & p_{n-1}/p_n & a_{n-1,n} \\ 0 & 0 & \cdots & 0 & p_n/p_1 \end{pmatrix}.$$

with p_i are different primes in $[1, H]$.

Matrices with given determinant

For integer matrices, we have, from Shparlinski (2010),

$$\#\mathcal{D}_n(\mathbb{Z}; H, \delta) \ll H^{n^2-n} \log H.$$

MA, Kuperberg, Ostafe, Shparlinski (2024)

For all $n \geq 2$ and $\delta \in \mathbb{Q}$,

$$\#\mathcal{D}_n(\mathbb{Q}; H, \delta) \leq \begin{cases} H^{4+o(1)}, & \text{if } n = 2, \\ H^{2n^2-n+o(1)}, & \text{if } n \geq 3. \end{cases}$$

$$\#\mathcal{D}_n(\mathbb{Z}^{-1}; H, \delta) \leq \begin{cases} H^{o(1)}, & \text{if } n = 2, \delta \neq 0, \\ H^{2+o(1)}, & \text{if } n = 2, \delta = 0, \\ H^{7+o(1)}, & \text{if } n = 3, \\ H^{n^2-n/2-1/(2n-2)+o(1)}, & \text{if } n \geq 4, \delta \neq 0, \\ H^{n^2-n/2+o(1)}, & \text{if } n \geq 4, \delta = 0. \end{cases}$$

Sketch of the proof: given determinant, $\#\mathcal{D}_n(\mathfrak{A}; H, \delta)$

For $n = 2$, we expand the equation directly. An example for $\#\mathcal{D}_2(\mathbb{Q}; H, \delta)$:

$$\begin{vmatrix} a_1/b_1 & a_2/b_2 \\ a_3/b_3 & a_4/b_4 \end{vmatrix} = r/s \iff rb_1b_2b_3b_4 + sa_2a_3b_1b_4 = sa_1a_4b_2b_3.$$

We then fix some elements in the last equation and use the divisor bound ($\tau(n) \ll n^{o(1)}$) to bound the number of choices for other variables.

For $n \geq 3$ and $\delta = 0$, we use the rank bound to get

$$\#\mathcal{D}_n(\mathfrak{A}; H, 0) \ll \sum_{r=0}^{n-1} L_{n,r}(\mathfrak{A}; H) \ll \begin{cases} H^{2n^2-n+o(1)}, & \text{if } \mathfrak{A} = \mathbb{Q}, \\ H^{n^2-n/2+o(1)}, & \text{if } \mathfrak{A} = \mathbb{Z}^{-1}. \end{cases}$$

Sketch of the proof: given determinant, $\#\mathcal{D}_n(\mathfrak{A}; H, \delta)$

When $\delta \neq 0$, we fix all rows, except the first, of $A \in \mathcal{D}_n(\mathfrak{A}; H, \delta)$ and use Laplace expansion on the first row of A to get an equation of the form

$$\sum_{j=1}^n Q_j a_{1,j} = Q_0,$$

with $a_{1,j} \in \mathcal{F}(H)$ or $\mathcal{E}(H)$, for $j = 1, \dots, n$. We then bound the number of solutions of this equation. For the case $\mathfrak{A} = \mathbb{Q}$, we use a result of Shparlinski (2017), and for $\mathfrak{A} = \mathbb{Z}^{-1}$, we derive a new result on a related problem.

Shparlinski (2017)

Let $H_1, \dots, H_n \geq 1$ and let $(Q_0, Q_1, \dots, Q_n) \in \mathbb{Z}^{n+1}$ with $1 \leq |Q_i| \leq \exp(H^{o(1)})$, $i = 1, \dots, n$, where $H = \max_{i=1}^n H_i$. Then, the equation

$$\sum_{i=1}^n Q_i x_i = Q_0,$$

has at most $H_1 \cdots H_n (\log H)^{2n-1+o(1)}$ solutions with $x_i \in \mathcal{F}(H_i)$, $i = 1, \dots, n$.

This implies

$$\#\mathcal{D}_n(\mathbb{Q}; H, \delta) \ll H^{2n(n-1)} \cdot H^{n+o(1)} = H^{2n^2-n+o(1)}.$$

A new result on the equation $\sum Q_i/x_i = Q_0$

If $\mathfrak{A} = \mathbb{Z}^{-1}$, the problem of bounding the number of solutions of the previous equation is equivalent to the following problem, to which we give a new result.

Lemma (MA, Kuperberg, Ostafe, Shparlinski (2024))

Let $(Q_0, Q_1, \dots, Q_n) \in \mathbb{Z}^{n+1}$ with $1 \leq |Q_i| \leq H^{O(1)}$ for $i = 1, \dots, n$. Then, the equation

$$\sum_{i=1}^n \frac{Q_i}{x_i} = Q_0,$$

has at most $H^{n/2+o(1)}$ solutions $(1/x_1, \dots, 1/x_n) \in \mathcal{E}(H)^n$.

If $Q_0 \neq 0$, we may replace the exponent $n/2 + o(1)$ with $n/2 - 1/(2n-2) + o(1)$.

Furthermore, for $n = 2$, we can replace the exponent with $o(1)$ and $1 + o(1)$ if $Q_0 = 0$ and $Q_0 \neq 0$, respectively. Also, for $n = 3$, we can replace the exponent with $1 + o(1)$.

The known lower bound when $Q_0 = 0$ is $H^{\lfloor n/2 \rfloor + o(1)}$.

The proof of the previous lemma is based on bounding the number of integer solutions of this equation, with $|x_i| \leq H$:

$$\text{lcm}(x_1, \dots, x_n) \mid Qx_1 \dots x_n.$$

After having the lemma, we use similar ideas as Konyagin-Korolev (2016). We count each cases with respect to a parameter U , to get

$$\#\mathcal{D}_n(\mathbb{Z}^{-1}; H, \delta) \ll H^{n/2+o(1)} U^{-1/2} + H^{n/2-1/(n-1)+o(1)} U^{1/2}.$$

Taking $U = H^{1/(n-1)}$, we have, for $\delta \neq 0$,

$$\#\mathcal{D}_n(\mathbb{Z}^{-1}; H, \delta) \ll H^{n^2-n/2-1/(2n-2)+o(1)}.$$

Matrices with given characteristic polynomial

Let $\mathcal{P}_n(\mathfrak{A}; H, f) = \{A \in \mathcal{M}_n(\mathfrak{A}; H) : \text{the characteristic polynomial of } A \text{ is } f\}$.

For integer matrices, we have, from Ostafe and Shparlinski (2022),

$$\#\mathcal{P}_n(\mathbb{Z}; H, f) \ll H^{n^2-n-1/(n-3)^2} \text{ if } n \geq 4.$$

MA, Kuperberg, Ostafe, Shparlinski (2024)

For all $n \geq 2$ and $f \in \mathbb{Q}[X]$,

$$\begin{aligned} \#\mathcal{P}_2(\mathbb{Z}^{-1}; H, X^2) &= \frac{24}{\pi^2} H \log^2 H + O(H \log H), \\ \#\mathcal{P}_n(\mathbb{Z}^{-1}; H, f) &\ll \begin{cases} H^{o(1)}, & \text{if } n = 2 \text{ and } f(X) \neq X^2, \\ H^{3+o(1)}, & \text{if } n = 3, \\ H^{n^2/2-1/(2n-2)+o(1)}, & \text{if } n \geq 4 \text{ and } f_{n-1} \neq 0, \\ H^{n^2/2+o(1)}, & \text{if } n \geq 4 \text{ and } f_{n-1} = 0, \end{cases} \end{aligned}$$

where f_{n-1} is the coefficient of X^{n-1} in f .

Sketch of the proof: given characteristic polynomial, $\#\mathcal{P}_2(\mathbb{Z}^{-1}; H, f)$

For $n = 2$, we expand the corresponding trace and determinant equation directly and use the divisor bounds ($\tau(n) \ll n^{o(1)}$).

For the special case of $\#\mathcal{P}_2(\mathbb{Z}^{-1}; H, X^2)$, by expanding the related equations,

$$\begin{pmatrix} 1/x_1 & 1/x_2 \\ 1/x_3 & 1/x_4 \end{pmatrix} \in \mathcal{P}_2(\mathbb{Z}^{-1}; H, X^2) \iff x_1^2 = -x_2x_3, x_4 = -x_1.$$

In this case, the problem is equivalent to counting the number of integer pairs (a, b) with $|a|, |b| \leq H$ such that ab is a square. de la Bretèche, Kurlberg, and Shparlinski (2021) already give an asymptotic formula for this problem, which completes the proof of our result.

Sketch of the proof: given characteristic polynomial, $\#\mathcal{P}_n(\mathfrak{A}; H, f)$

For a fixed characteristic polynomial f of A , we note that $\text{Tr } A$ and $\text{Tr } A^2$ is also fixed. The entries $(a_{i,j}) \in \mathfrak{A}$ of A would then satisfy the following system of equations:

$$\sum_{i=1}^n \frac{s_1}{a_{i,i}} = r_1, \quad (1)$$

$$\sum_{1 \leq i < j \leq n} \frac{s_2}{a_{i,j} a_{j,i}} = r_2. \quad (2)$$

We can directly apply our previous result on the number of solutions of the equation $\sum Q_i/x_i = Q_0$ to bound the number of solutions to (1). For (2) we need to modify the equation, and then apply the same result. We get

$$\#\mathcal{P}_n(\mathbb{Z}^{-1}; H, f) \ll \begin{cases} H^{3+o(1)}, & \text{if } n = 3, \\ H^{n^2/2-1/(2n-2)+o(1)}, & \text{if } n \geq 4 \text{ and } f_{n-1} \neq 0, \\ H^{n^2/2+o(1)}, & \text{if } n \geq 4 \text{ and } f_{n-1} = 0. \end{cases}$$

Upper bound for $\#\mathcal{P}_n(\mathbb{Q}; H, f)$

If we replace our lemma in the previous arguments with Shparlinski's 2017 result on the corresponding equation over Farey fractions, we have an upper bound of $\#\mathcal{P}_n(\mathbb{Q}; H, f)$, $n \geq 3$.

MA, Kuperberg, Ostafe, Shparlinski (2024)

Uniformly over $f \in \mathbb{Q}[X]$, we have

$$\#\mathcal{P}_n(\mathbb{Q}; H, f) \ll \begin{cases} H^{2+o(1)}, & \text{if } n = 2, \\ H^{n^2+o(1)}, & \text{if } n \geq 3. \end{cases}$$

For $n = 2$, we note that $f(X) = (X - a_{1,1}/b_{1,1})(X - a_{2,2}/b_{2,2})$ is the characteristic polynomial of

$$\begin{pmatrix} a_{1,1}/b_{1,1} & a_{1,2}/b_{1,2} \\ 0 & a_{2,2}/b_{2,2} \end{pmatrix}.$$

Since there are H^2 choices for $a_{1,2}/b_{1,2}$, we have the matching lower bound for $\#\mathcal{P}_2(\mathbb{Q}; H, f)$. For $n \geq 3$ and f splits on \mathbb{Q} , we have $\#\mathcal{P}_n(\mathbb{Q}; H, f) \gg H^{n(n-1)}$.

Sketch of the proof: given characteristic polynomial, $\#\mathcal{P}_2(\mathbb{Q}; H, f)$

From the corresponding trace and determinant equation, we have

$$r_1 s_0 a_1 b_1 b_2 b_3 = s b_1^2 a_2 a_3 + s a_1^2 b_2 b_3 + r_0 s_1 b_1^2 b_2 b_3.$$

We paramaterize the variables with respect to c_2, c_3, d_2, d_3 and count these instead, over some dyadic interval

$$c_i \in [C_i, 2C_i], \quad d_i \in [D_i, 2D_i].$$

We first prove there are at most

$$\sqrt{C_2 C_3} H^{o(1)}$$

choices of (c_2, c_3) . Next, after fixing these, we note that the following expression is a perfect square

$$R = r_1^2 s_0^2 c^2 - 4 \frac{s_0^2 s_1^2 c^2}{c_2 c_3} \frac{a_2}{d_3} \frac{a_3}{d_2} - 4 r_0 s^2 c^2.$$

Using results from squares in arithmetic progression, and with some other arguments, we have

$$\#\mathcal{P}_2(\mathbb{Q}; H, f) \ll (C_2 C_3)^{1/2} H^{1+o(1)} (D_2 D_3)^{1/2} \ll H^{2+o(1)}.$$

- Some of our results are based on applying Laplace expansions to only one row of A . Applying the expansions to some other rows or columns might improve the results, but we need to work with more variables.
- For our proof of $\#\mathcal{P}_n(\mathfrak{A}; H, f)$, we only use two coefficients of f . However, the results is close enough to the expected lower bound.
- Improving the bound for $\#\mathcal{P}_n(\mathbb{Z}^{-1}; H, f)$ is related to bounding the number of integer solutions to the system of equations

$$\sum_{i=1}^n Q_i/x_i = Q_0 \quad \text{and} \quad \sum_{i=1}^n R_i/x_i^2 = R_0,$$

with $|x_i| \geq H$ which is an interesting problem of its own. The exponent 1 and 2 can be replaced with other numbers. Also, studying similar questions over Farey fractions are also interesting on its own.

Thank you

M. Afifurrahman, V. Kuperberg, A. Ostafe and I. E. Shparlinski, 'Statistics of ranks, determinants and characteristic polynomials of rational matrices', *Preprint*, 2024, available from <https://arxiv.org/abs/2401.10086>.