Counting products of integer matrices with bounded height

Muhammad (Afif) Afifurrahman

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

6 September 2023

Motivation: the scalar case (Erdős)

$\times$	1	2	$\ldots$	H
1	1	2	$\ldots$	H
2	2	4	$\ldots$	$2H$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
H	H	$2H$	$\ldots$	H^2

- **Erdős multiplication table problem** (1955): How many distinct numbers are there in this table, as $H \to \infty$?
- Trivially there are less than H^2 numbers, but what is the correct (asymptotical) answer?
- Erdős conjectured that this quantity is $O(H^2/(\log H)^{\alpha})$, for some positive α.
- Ford gave the asymptotical formula of this quantity in 2008.

Motivation: the scalar case (Ford, Koukoulopoulos)

What about more variables? How many numbers are there asymptotically in the set

$$\mathcal{A}_m(H) = \{a_1 a_2 \dots a_m \colon 1 \leq a_i \leq H \text{ for } i = 1, \dots, m\}?$$

Koukoulopoulos (2010), the case $m = 2$ corresponds to Ford (2008)

For $m \geq 2$, let $\rho = (m+1)^{1/m}$ and $Q(u) := u \log u - u + 1$. We have

$$\#\mathcal{A}_m(H) \asymp \frac{H^m}{(\log H)^{Q(\frac{1}{\log \rho})} (\log \log H)^{\frac{3}{2}}}.$$

A matrix analogue

- We replace the integers $1 \leq a_i \leq H$ in the multiplication table problem with matrices A_i of bounded height H.
- In this setting, we have the following problem analogue: how many elements are there in

$$\{A_1 \dots A_m \colon A_i \in X\},$$

where X is some set of $n \times n$ matrices of bounded height H, as $H \to \infty$?
- In this talk, we are interested in the case where $X := \mathcal{M}_n(\mathbb{Z}; H)$ is the set of integer matrices with entries bounded by H in absolute value.
- These problems are in line with Ostafe and Shparlinski's 2022 paper on multiplicatively dependent tuples of matrices in $\mathcal{M}_n(\mathbb{Z}; H)$.
- The main obstacles in passing from numbers to matrices: matrix noncommutativity and the absence of a prime number factorisation analogue for matrices.

Notation:

$$\mathcal{M}_n(\mathbb{Z};H) := \{(a_{ij})_{i,j=1}^{n} \colon a_{ij} \in \mathbb{Z}, |a_{ij}| \le H \text{ for } i,j = 1,\dots,n\}.$$

We have $\mathcal{M}_n(\mathbb{Z};H) = (2H+1)^{n^2} \asymp H^{n^2}$. We now can state the first problem as follows:

Problem 1

Give nontrivial upper and lower bounds for

$$\#\mathcal{W}_{m,n}(\mathbb{Z};H) := \#\{A_1 \dots A_m \colon A_1, \ \dots, A_m \in \mathcal{M}_n(\mathbb{Z};H)\},$$

as $H \to \infty$ and m and n fixed.

In this talk, we are only focused on the order of the bounds. Trivial bounds: $H^{n^2} \ll \#\mathcal{W}_{m,n}(\mathbb{Z};H) \ll H^{mn^2}$.

Related questions while bounding $\#\mathcal{W}_{m,n}(\mathbb{Z}; H)$

Problem 2

Give nontrivial upper and lower bounds for

$$\#\mathcal{T}_m(\mathcal{M}_n(\mathbb{Z}; H), C) := \#\{(A_1, \dots, A_m) \in \mathcal{M}_n(\mathbb{Z}; H)^m : A_1 \dots A_m = C\}$$

for a fixed C **uniformly**.
Trivial bound: $\#\mathcal{T}_m(\mathcal{M}_n(\mathbb{Z}; H), C) \ll H^{mn^2-1}$.

Problem 3

Give nontrivial upper and lower bounds for

$$\#\mathcal{U}_m(\mathcal{M}_n(\mathbb{Z}; H)) := \#\{(A_1, \dots, A_m, B_1, \dots, B_m) \in \mathcal{M}_n(\mathbb{Z}; H)^{2m} : A_1 \dots A_m = B_1 \dots B_m\}$$

Trivial bounds: $H^{mn^2} \ll \#\mathcal{U}_m(\mathcal{M}_n(\mathbb{Z}; H)) \ll H^{2mn^2}$.

Previous results on $\mathcal{M}_n(\mathbb{Z}; H)$

Katznelson (1993), Shparlinski (2010)

Fix an integer d. Then, **uniformly** on d there are $O(H^{n^2-n}\log H)$ matrices in $\mathcal{M}_n(\mathbb{Z}; H)$ of determinant d.
If $d = 0$, then the number of matrices in $\mathcal{M}_n(\mathbb{Z}; H)$ with determinant 0 is in order of magnitude $H^{n^2-n}\log H$.

If we fix $d \neq 0$, Duke-Rudnick-Sarnak actually give an asymptotical formula of the number in $\mathcal{M}_n(\mathbb{Z}; H)$ with determinant d as $H \to \infty$, with main term of order H^{n^2-n}. However, this result is not uniform with respect to d.

Katznelson (1994)

The number of matrices in $\mathcal{M}_n(\mathbb{Z}; H)$ of rank k is in order of magnitude $H^{nk+o(1)}$.

The equation $A_1 \dots A_m = C$

We give some bounds on $\#\mathcal{T}_m(\mathcal{M}_n(\mathbb{Z}; H), C)$, the number of tuples $(A_1, \dots, A_m) \in \mathcal{M}_n(\mathbb{Z}; H)^m$ that satisfies the equation

$$A_1 \dots A_m = C.$$

The bounds are uniform with respect to C.

Theorem 2.1 (MA, 2023)

$$\#\mathcal{T}_m(\mathcal{M}_n(\mathbb{Z}; H), C) \le \begin{cases} H^{(m-1)(n^2-n)+o(1)}, & \text{if } C \text{ is nonsingular, for all } m, \\ H^{n^2+o(1)}, & \text{if } C \ne O_n \text{ is singular and } m = 2, \\ H^{mn^2-n}, & \text{if } C \ne O_n \text{ is singular and } m > 2. \end{cases}$$

If $C = O_n$ (the zero $n \times n$ matrix), we have

$$H^{(m-1)n^2} \ll \#\mathcal{T}_m(\mathcal{M}_n(\mathbb{Z}; H), O_n) \le H^{(m-1)n^2+o(1)}.$$

Sketch of the proof: $A_1 \dots A_m = C$

- For nonsingular C: For a fixed $(A_1, \dots, A_{m-1})$ we have a unique A_m. We also have

$$\det(A_1) \dots \det(A_m) = \det(C).$$

  Next, we use a bound on the divisor function, then use Shparlinski's determinant bound.
- For singular $C \neq O_n$ and $m = 2$: We rewrite the equation $AB = C$ as

$$\left(\begin{array}{c|c} X_1 & V_1 \\ \hline W_1 & Y_1 \end{array}\right) \left(\begin{array}{c|c} X_2 & V_2 \\ \hline W_2 & Y_2 \end{array}\right) = \left(\begin{array}{c|c} X & V \\ \hline W & Y \end{array}\right),$$

  then bound the number of solutions based on rank A.
- For singular $C \neq O_n$ and $m > 2$: One of the matrices in

$$A_1 \dots A_m = C$$

  must be singular.

Sketch of the proof: $A_1 \dots A_m = O_n$

- Lower bound:

$$O_n A_2 \dots A_m = O_n,$$

then we have at least $H^{(m-1)n^2}$ solutions.

- Upper bound: From Sylvester's rank inequality, we have $(m-1)n \geq \sum_{i=1}^{m} \operatorname{rank} A_i$. Applying Katznelson's rank theorem, we have

$$\#\mathcal{T}_m(\mathcal{M}_n(\mathbb{Z}; H), O_n) \leq \sum_{\substack{0 \leq k_1, \dots, k_m \leq n \\ k_1 + \dots + k_m \leq (m-1)n}} H^{nk_1 + o(1)} \cdot \ldots \cdot H^{nk_m + o(1)} \leq H^{(m-1)n^2 + o(1)}.$$

- These two bounds match, up to an error factor $H^{o(1)}$.

The equation $A_1 \dots A_m = B_1 \dots B_m$

We can use the previous results to derive some upper bounds for $\#\mathcal{U}_m(\mathcal{M}_n(\mathbb{Z}; H))$ and $\#\mathcal{U}_m(\mathcal{M}_n^*(\mathbb{Z}; H))$, the number of solutions of equation

$$A_1 \dots A_m = B_1 \dots B_m,$$

where $A_i, B_i \in \mathcal{M}_n(\mathbb{Z}; H)$ or $\mathcal{M}_n^*(\mathbb{Z}; H)$ (the set of all invertible matrices in $\mathcal{M}_n(\mathbb{Z}; H)$), respectively.

Corollary 2.2 (MA, 2023)

For all $m, n \geq 2$, we have

$$\#\mathcal{U}_m(\mathcal{M}_n^*(\mathbb{Z}; H)) \leq H^{(2m-1)n^2-(m-1)n+o(1)}.$$

We also have

$$\#\mathcal{U}_m(\mathcal{M}_n(\mathbb{Z}; H)) \leq \begin{cases} H^{3n^2-n+o(1)}, & \text{if } m = 2, \\ H^{2mn^2-2n+o(1)}, & \text{if } m > 2. \end{cases}$$

The product set: Lower bound

We recall that our main problem is to bound

$$\#\mathcal{W}_{m,n}(\mathbb{Z}; H) = \#\{A_1 \dots A_m \colon A_1, \ \dots, A_m \in \mathcal{M}_n(\mathbb{Z}; H)\}.$$

From our previous result, for a fixed invertible C there are at most $H^{(m-1)(n^2-n)+o(1)}$ solutions for the equation

$$A_1 \dots A_m = C.$$

This implies there are at least $H^{n^2+mn-n+o(1)}$ different invertible matrices C in the set. This improves the trivial lower bound H^{n^2}.

The product set: Upper bound

For the upper bound, we use Koukolopoulos' result on integer product set and Shparlinski's determinant result.

Theorem 2.3 (MA, 2023)

For all $m, n \geq 2$, we have

$$H^{n^2+mn-n+o(1)} \leq \#\mathcal{W}_{m,n}(\mathbb{Z}; H) = O\left(\frac{H^{mn^2}}{(\log H)^{Q(\frac{1}{\log \rho})-1}(\log\log H)^{\frac{3}{2}}}\right),$$

where $\rho = m^{1/(m-1)}$ and $Q(u) := u\log u - u + 1$.

If $Q(\frac{1}{\log \rho}) \geq 1$, we have $\#\mathcal{W}_{m,n}(\mathbb{Z}; H) = o(H^{mn^2})$. Unfortunately, this is only true if $m \geq 6$. However, we believe this is also true for $2 \leq m \leq 5$.

Thank you

M. Afifurrahman, “Some counting questions for matrix products”, *Bull. Aust. Math. Soc*, to appear. Preprint available at arXiv:2306:04885.