Pacific
Journal of
Mathematics

COUNTING MATRICES OVER FINITE RANK MULTIPLICATIVE GROUPS

AARON MANNING, ALINA OSTAFE AND IGOR E. SHPARLINSKI

Volume 340 No. 1 January 2026

PACIFIC JOURNAL OF MATHEMATICS
Vol. 340, No. 1, 2026
https://doi.org/10.2140/pjm.2026.340.115

COUNTING MATRICES OVER FINITE RANK MULTIPLICATIVE GROUPS

AARON MANNING, ALINA OSTAFE AND IGOR E. SHPARLINSKI

Motivated by recent works on statistics of matrices over sets of number theoretic interest, we study matrices with entries from arbitrary finite subsets $\mathcal{A}$ of finite rank multiplicative groups in fields of characteristic zero. We obtain upper bounds, in terms of the size of $\mathcal{A}$, on the number of such matrices of a given rank, with a given determinant and with a prescribed characteristic polynomial. In particular, in the case of ranks, our results can be viewed as a statistical version of work by Alon and Solymosi (2023).

1. Introduction

1.1. ***Motivation and set-up.*** For a finite subset $\mathcal{A}$ of a field $\mathbb{K}$, we define $\mathcal{M}_{m,n}(\mathcal{A})$ to be the set of $m \times n$ matrices with entries from $\mathcal{A}$. It is also convenient to omit one of the subscripts when $m = n$, writing $\mathcal{M}_n(\mathcal{A}) = \mathcal{M}_{n,n}(\mathcal{A})$. Various counting questions regarding matrices in $\mathcal{M}_{m,n}(\mathcal{A})$ where $\mathcal{A}$ is a set of arithmetic significance have been studied in a number of works. Here we are interested in the case when m and n are fixed and the size of $\mathcal{A}$ grows, that is, when

$$A = \#\mathcal{A} \to \infty.$$

Thus this is dual to the set-up when $\mathcal{A}$ is fixed, typically $\mathcal{A} = \{0, 1\}$ or $\mathcal{A} = \{-1, 1\}$,

---

MSC2020: 11C20, 15B36, 60B20.

Keywords: matrices over finite rank multiplicative groups, rank, determinant, characteristic polynomial.

and $m, n \to \infty$, which has also received a lot of attention; see [11; 17; 19; 25; 26; 32; 36; 37; 41; 42; 51] as well as the survey [52].

The direction originates from the case of $\mathcal{A} = \mathbb{K} = \mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field of q elements [13; 24; 27; 28; 29; 44; 45; 54].

In characteristic zero, the most studied case is the case of integer entries, bounded (in, say, $\mathcal{L}^2$ or $\mathcal{L}^\infty$ norms) by some parameter $H \to \infty$. This direction originates from works of Duke, Rudnick and Sarnak [18], Eskin, Mozes and Shah [22] and Katznelson [33; 34]; see also [10; 21; 30; 47; 48; 53] for further developments of these techniques, based on geometry of numbers and homogeneous dynamics. More recently, several different approaches to problems of arithmetic statistics for matrices have emerged [1; 2; 3; 4; 5; 9; 14; 16; 15; 20; 31; 38; 39; 43; 50]. These works are based on a variety of other techniques, including some inputs from Diophantine geometry and analytic number theory. In particular, these new ideas have given the means to approach various counting question for matrices with rational entries whose numerators and denominators are bounded by a given height H, see [4], and for matrices with entries which are polynomial values of integers from $[-H, H]$, see [9; 39], in the same regime of fixed m and n and $H \to \infty$.

There is also an emerging direction of studying matrices with entries from a completely general set, where, surprisingly some nontrivial bounds are possible [8; 35; 40; 49].

More precisely, most of the above works study the following three subsets of $\mathcal{M}_{m,n}(\mathcal{A})$:

- matrices of given determinant $d \in \mathbb{K}$,

$$\mathcal{D}_n(\mathcal{A}; d) = \{\boldsymbol{X} \in \mathcal{M}_n(\mathcal{A}) : \det \boldsymbol{X} = d\}, \tag{1-1}$$

- matrices with a given characteristic polynomial $f \in \mathbb{K}[T]$,

$$\mathcal{P}_n(\mathcal{A}; f) = \{\boldsymbol{X} \in \mathcal{M}_n(\mathcal{A}) : \det(T I_n - \boldsymbol{X}) = f\}, \tag{1-2}$$

- matrices of given rank $r \in \mathbb{N}$,

$$\mathcal{R}_{m,n}(\mathcal{A}; r) = \{\boldsymbol{X} \in \mathcal{M}_{m,n}(\mathcal{A}) : \operatorname{rank} \boldsymbol{X} = r\}. \tag{1-3}$$

As with $\mathcal{M}_n(\mathcal{A})$, we also adopt the notation $\mathcal{R}_n(\mathcal{A}; r) = \mathcal{R}_{n,n}(\mathcal{A}; r)$.

Here we consider the above questions in a new setting, when the set $\mathcal{A}$ is an arbitrary finite subset of a multiplicative subgroup Γ of finite rank in a field $\mathbb{K}$ of characteristic zero. Besides the aforementioned works, our motivation also comes from a result of Alon and Solymosi [6, Theorem 1], which shows that $n \times n$ matrices with entries from finitely generated subgroups Γ of $\mathbb{C}^*$ have a rank growing with their dimension n. In our notation, the result of [6, Section 4] can be formulated as $\mathcal{R}_n(\mathcal{A}; r) = \varnothing$, provided $r < (c_1 \log n)^{c_2}$ for some positive constants c_1 and c_2, depending only on n and the rank of Γ.

It is also interesting to note that both the approach of Alon and Solymosi [6] and our approach are based on the celebrated *Subspace Theorem* of Schmidt [46]. More precisely we use its implication for the number of nondegenerate solutions to linear equations solved over Γ, given in the currently strongest form by Amoroso and Viada [7, Theorem 6.2]. This in turn has been used in [12, Corollary 16] to estimate the total number of solutions; see Section 3 for details.

We emphasise that our bounds on the above quantities $\mathcal{D}_n(\mathcal{A};\, d)$ and $\mathcal{P}_n(\mathcal{A};\, f)$ are uniform with respect to d and f, and the implied constants, while the bounds on $\mathcal{R}_{m,n}(\mathcal{A};\, r)$ may only depend on the dimensions m and n of a matrix, and the rank ϱ of Γ. In Lemmas 3.2, 3.3, and 3.4 on the number of solutions to linear equations, the implied constant may only depend on the number of summands n and the rank ϱ of Γ.

1.2. ***Notation.*** We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are equivalent to $|U| \leqslant cV$ for some positive constant c, which, as above, may depend only on m, n and ϱ throughout this work.

We also write $U \asymp V$ as a shorthand for when both $U \ll V$ and $V \ll U$ hold.

When S is a finite set, we use $\#S$ to denote its cardinality.

Throughout this work we also use

$$A = \#\mathcal{A}$$

to denote the cardinality of $\mathcal{A}$.

Finally, $\mathbb{F}_q$ denotes the finite field of q elements and I_n denotes the $n \times n$ identity matrix.

1.3. ***Trivial upper bounds.*** Before we formulate our results, we record the following trivial bounds, which we use as benchmarks to illustrate the strength of our results.

Clearly, for any $n \geq 1$ and $\mathcal{A} \subseteq \mathbb{K}$ of cardinality A,

$$\#\mathcal{D}_n(\mathcal{A};\, d) \ll A^{n^2-1}. \tag{1-4}$$

In fact, for $\mathcal{A} = \mathbb{K} = \mathbb{F}_q$ the bound (1-4) is tight. However, recent work by Shkredov and Shparlinski [49] shows that a better bound is possible for real matrices when $n \geq 3$, without any further restrictions on the entries.

Also, for $f = T^n + c_{n-1}T^{n-1} + \cdots + c_0 \in \mathbb{K}[T]$,

$$\#\mathcal{P}_n(\mathcal{A};\, f) \ll A^{n^2-2}. \tag{1-5}$$

Indeed, writing $\boldsymbol{X} = (x_{i,j})_{i,j=1}^n$ and using $f = \det(TI_n - \boldsymbol{X})$ we see that $\boldsymbol{X}$ has a fixed trace $\operatorname{tr} \boldsymbol{X} = -c_{n-1}$, and hence we can express $x_{n,n}$ via other diagonal elements. After this the equation $\det \boldsymbol{X} = (-1)^n c_0$ becomes an algebraic equation in $n^2 - 1$

variables. This equation is nontrivial as one can see by specialising all nondiagonal elements of $\boldsymbol{X}$ to 0.

Furthermore, for any $n \ge m \ge r \ge 1$ and $\mathcal{A} \subseteq \mathbb{K}$ of finite cardinality A,

$$\#\mathcal{R}_{m,n}(\mathcal{A}; r) \ll A^{nr+mr-r^2}. \tag{1-6}$$

Indeed, without loss of generality, we can assume that the top left $r \times r$ submatrix of $\boldsymbol{X} \in \mathcal{M}_{m,n}(\mathcal{A})$ is nonsingular. Then we see that after fixing nr elements in the top r rows of $\boldsymbol{X}$ and, the $(m-r)r$ remaining elements in the first r columns of $\boldsymbol{X}$, the remaining elements are uniquely defined.

2. Main results

2.1. ***Matrices of given rank.*** Recall the definition of $\mathcal{R}_{m,n}(\mathcal{A}; r)$ given in (1-3) as the set of $m \times n$ matrices over $\mathcal{A}$ of rank r.

Theorem 2.1. *Let $\mathbb{K}$ be a field of characteristic zero, and Γ a rank ϱ subgroup of $\mathbb{K}^*$. If $n, m \ge 2$ with $n \ge m \ge r > 0$, for any finite subset $\mathcal{A}$ of Γ with cardinality A, we have*

$$\#\mathcal{R}_{m,n}(\mathcal{A}; r) \ll \begin{cases} A^{nr+m-r} & \text{if } 2m \le n+r, \\ A^{nr+m-r+\lfloor (r-1)/2 \rfloor (2m-n-r)} & \text{otherwise.} \end{cases}$$

When $2m > n+r$, Theorem 2.1 gives us a saving against the trivial bound (1-6), of

$$\frac{A^{nr+mr-r^2}}{A^{nr+m-r+\lfloor (r-1)/2 \rfloor (2m-n-r)}} = \begin{cases} A^{(n-r)(r-1)/2} & \text{for } r \text{ odd}, \\ A^{r(n-r)/2+(m-n)} & \text{for } r \text{ even}. \end{cases}$$

When $2m \le n+r$, the bound of Theorem 2.1 is tight. For instance, take $\mathbb{K} = \mathbb{Q}$, $\Gamma = \langle 2 \rangle$ and $\mathcal{A}_k = \{2^s : 1 \le s \le 2k\}$, defining $A_k = \#\mathcal{A}_k = 2k$. In this case we have $k^{nr} \asymp A_k^{nr}$ ways of fixing the first r rows with elements of the form 2^s for $1 \le s \le k$. We then have $k^{m-r} \asymp A_k^{m-r}$ ways of choosing all the other rows to be 2^s multiplied by the first row for each $1 \le s \le k$ (to guarantee elements stay within $\mathcal{A}_k$). Thus the number of matrices of rank at most r satisfies

$$\sum_{j=1}^{r} \#\mathcal{R}_{m,n}(\mathcal{A}_k; j) \asymp A_k^{nr+m-r}. \tag{2-1}$$

Therefore

$$\begin{aligned} \#\mathcal{R}_{m,n}(\mathcal{A}_k; r) &= \sum_{j=1}^{r} \#\mathcal{R}_{m,n}(\mathcal{A}_k; j) - \sum_{j=1}^{r-1} \#\mathcal{R}_{m,n}(\mathcal{A}_k; j) \\ &\gg \sum_{j=1}^{r} \#\mathcal{R}_{m,n}(\mathcal{A}_k; j) + O(A_k^{n(r-1)+m-(r-1)}) \gg A_k^{nr+m-r}. \end{aligned}$$

2.2. ***Matrices of given determinant.*** We recall the definition of $\mathcal{D}_n(\mathcal{A}; d)$ given in (1-1) as the set of $n \times n$ matrices over $\mathcal{A}$ with determinant d.

Theorem 2.2. *Let $\mathbb{K}$ be a field of characteristic zero, and Γ a rank ϱ subgroup of $\mathbb{K}^*$. For any $d \in \mathbb{K}$ and finite subset $\mathcal{A}$ of Γ with cardinality A,*

$$\#\mathcal{D}_n(\mathcal{A}; d) \ll \begin{cases} A^{n^2-\lceil n/2\rceil} & \text{if } d = 0, \\ A^{n^2-\lceil (n+1)/2\rceil} & \text{if } d \neq 0. \end{cases}$$

Clearly Theorem 2.2 always improves the bound (1-4) (and also the stronger bound from [49]), except when $n = 2$ and $d = 0$, in which case the bound is tight. Indeed, specialising the lower bound (2-1) to the case when $m = n$ and $r = n - 1$, we immediately see that

$$\#\mathcal{D}_n(\mathcal{A}; 0) \gg A^{n^2-n+1}.$$

Hence for $d = 0$, Theorem 2.2 is tight when $n = 2$ and $n = 3$.

2.3. ***Matrices of given characteristic polynomial.*** Recall the definition of $\mathcal{P}_n(\mathcal{A}; f)$ given in (1-2) as the set of $n \times n$ matrices over $\mathcal{A}$ with characteristic polynomial f.

We first consider the case $n = 2$ separately, due to the compatibility of the formulae for the trace and determinant in this case, which allows for a tighter bound to be acquired than in the general case.

Theorem 2.3. *Let $\mathbb{K}$ be a field of characteristic zero, and Γ a rank ϱ subgroup of $\mathbb{K}^*$. For any $d, t \in \mathbb{K}$ not both zero, and finite subset $\mathcal{A}$ of Γ with cardinality A,*

$$\#\mathcal{P}_2(\mathcal{A}; T^2 - tT + d) \ll A.$$

We do not specify a bound in Theorem 2.3 when $d = t = 0$ because in this case, the trivial bound of $O(A^2)$ is tight. This can be seen with the following construction. Let $\mathcal{A}_k = \{\pm 2^s : 0 \le s < k\}$, with $A_k = \#\mathcal{A}_k = 2k$. A matrix $\boldsymbol{X} = (x_{i,j})_{i,j=1}^2$ is in $\mathcal{P}_2(\mathcal{A}_k; T^2)$ if and only if

$$\det \boldsymbol{X} = x_{1,1}x_{2,2} - x_{1,2}x_{2,1} = 0 \quad \text{and} \quad \operatorname{tr} \boldsymbol{X} = x_{1,1} + x_{2,2} = 0,$$

or equivalently,

$$x_{1,1}^2 = -x_{1,2}x_{2,1} \quad \text{and} \quad x_{1,1} = -x_{2,2}.$$

By writing $x_{1,1} = 2^{a+b}$, $x_{1,2} = 2^{2a}$ and $x_{2,1} = -2^{2b}$ with nonnegative integers $a, b < k/2$, we see that

$$\#\mathcal{P}_2(\mathcal{A}_k; T^2) \gg A_k^2.$$

We now turn our attention to the case $n \ge 3$. Our bound is based on fixing only the coefficients of T^{n-1} and T^{n-2} in the characteristic polynomial $f \in \mathbb{K}[T]$, as motivated by the techniques of [4]. While we do not present a matching lower bound, the strength of [4, Theorem 2.3] which uses this approach indicates its unexpected power.

Before stating Theorem 2.4 for fixed characteristic polynomial, we introduce the function

$$\alpha(n) = \frac{n(n-1)}{2} + \max\left\{ \left\lfloor \frac{n-1}{2} \right\rfloor + \left\lfloor \frac{n(n-1)}{4} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n(n-1)}{4} - \frac{1}{2} \right\rfloor \right\}. \tag{2-2}$$

Theorem 2.4. *Let $\mathbb{K}$ be a field of characteristic zero, and Γ a rank ϱ subgroup of $\mathbb{K}^*$. For any monic polynomial f of degree $n \ge 3$, and any $\mathcal{A} \subseteq \Gamma$ of finite cardinality A, we have*

$$\#\mathcal{P}_n(\mathcal{A}; f) \ll A^{\alpha(n)}$$

where $\alpha(n)$ is given by (2-2).

We note that

$$\lim_{n\to\infty} \alpha(n)/n^2 = \tfrac{3}{4}.$$

Direct calculations show that Theorem 2.4 improves (1-5) and also the bound

$$\#\mathcal{P}_n(\mathcal{A}; f) \ll \#\mathcal{D}_n(\mathcal{A}; (-1)^n c_0) \ll \begin{cases} A^{n^2-\lceil n/2\rceil} & \text{if } f(0) = 0, \\ A^{n^2-\lceil (n+1)/2\rceil} & \text{if } f(0) \neq 0, \end{cases}$$

which follows from Theorem 2.2.

Remark 2.5. In the proof of Theorem 2.4 we derive more precise bounds which depend on some properties of the coefficients of X^{n-1} and X^{n-2} from f. See Appendix B, where these bounds are presented.

Finally, we observe that Theorems 2.3 and 2.4 imply upper bounds on the number of *cyclotomic* matrices $\boldsymbol{X} \in \mathcal{M}_n(\mathcal{A})$, that is, matrices with $\boldsymbol{X}^k = I_n$ for some positive integer k.

3. Linear equations in finite rank multiplicative groups

3.1. ***Counting nondegenerate solutions.*** We start with the best known bound in the case of arbitrarily many summands in an arbitrary field of characteristic zero due to Amoroso and Viada [7, Theorem 6.2], however as in [12] the previous bound of Evertse, Schlickewei and Schmidt [23] is also suitable for our purpose (as well as other bounds of this kind).

Let $\mathbb{K}$ be a field of characteristic zero, and let Π be a subgroup of $(\mathbb{K}^*)^n$. We say that a solution to the equation

$$a_1x_1 + \cdots + a_nx_n = 1, \quad (x_1, \ldots, x_n) \in \Pi, \tag{3-1}$$

is nondegenerate if

$$\sum_{i\in\mathcal{I}} a_ix_i \neq 0$$

for all $\mathcal{I} \subseteq \{1, 2, \ldots, n\}$.

Lemma 3.1. *Let $\mathbb{K}$ be a field of characteristic zero, and Π a rank ϱ subgroup of $(\mathbb{K}^*)^n$. For any $a_1, \dots, a_n \in \mathbb{K}^*$, the number of nondegenerate solutions to* (3-1) *is at most* $(8n)^{4n^4(n+\varrho+1)}$.

3.2. ***Counting arbitrary solutions.*** Since the entries of our matrices are drawn from a subgroup Γ of $\mathbb{K}^*$, we specialise Lemma 3.1 to the case $\Pi = \Gamma^n$.

The following result is essentially [12, Corollary 16]. Although it is presented in [12] for $\mathbb{K} = \mathbb{C}$ with integer coefficients, it extends to arbitrary fields of characteristic zero in the natural way.

Lemma 3.2. *Let $\mathbb{K}$ be a field of characteristic zero, and Γ a rank ϱ subgroup of $\mathbb{K}^*$. Suppose that $\mathcal{A} \subseteq \Gamma$ is a finite set of cardinality A. For any $a_1, \dots, a_n \in \mathbb{K}^*$, the number of solutions to*

$$a_1x_1 + \cdots + a_nx_n = 0, \quad x_1, \dots, x_n \in \mathcal{A},$$

is $O(A^{\lfloor n/2 \rfloor})$.

It is easy to see that the bound of Lemma 3.2 is tight, since for any choice of Γ and $\mathcal{A}$, if $n = 2k$ then we can choose

$$a_1 = \cdots = a_k = 1 \quad \text{and} \quad a_{k+1} = \cdots = a_{2k} = -1,$$

allowing us to construct $A^k = A^{\lfloor n/2 \rfloor}$ solutions by setting $x_i = x_{k+i}$ for all $i \in \{1, \dots, k\}$. If $n = 2k + 1$, then we may similarly consider

$$a_1 = \cdots = a_{k-1} = 1, \quad a_k = \cdots = a_{2k} = -1, \quad \text{and} \quad a_{2k+1} = 2,$$

which allows us to once again construct $A^k = A^{\lfloor n/2 \rfloor}$ solutions by setting $x_i = x_{k+i-1}$ for all $i \in \{1, \dots, k-1\}$ and $x_{2k-1} = x_{2k} = x_{2k+1}$.

For problems such as counting matrices of a given nonzero determinant, we also require a non-homogeneous (and a slightly stronger) version of Lemma 3.2 where the right-hand side of the corresponding equation is an arbitrary $a_0 \in \mathbb{K}^*$. We derive it as an application of Lemma 3.2, which we use to handle the vanishing subsums present in degenerate solutions.

Lemma 3.3. *Let $\mathbb{K}$ be a field of characteristic zero, and Γ a rank ϱ subgroup of $\mathbb{K}^*$. Suppose that $\mathcal{A} \subseteq \Gamma$ is a finite set of cardinality A. For any $a_0, a_1, \dots, a_n \in \mathbb{K}^*$, the number of solutions to*

$$a_1x_1 + \cdots + a_nx_n = a_0, \quad x_1, \dots, x_n \in \mathcal{A},$$

is $O(A^{\lfloor (n-1)/2 \rfloor})$.

Proof. Dividing all coefficients of the above equation by a_0 we see that it is sufficient to consider the equation

$$a_1x_1 + \cdots + a_nx_n = 1, \quad x_1, \dots, x_n \in \mathcal{A}. \tag{3-2}$$

Let $\mathfrak{A}$ denote the number of solutions to (3-2), and for each such solution $\boldsymbol{x} = (x_1, \dots, x_n)$, associate a subset $\mathcal{I}(\boldsymbol{x}) \subseteq \{1, \dots, n\}$ with the largest cardinality such that

$$\sum_{i \in \mathcal{I}(\boldsymbol{x})} a_i x_i = 0.$$

For each $\mathcal{I} \subseteq \{1, \dots, n\}$, let $\mathfrak{A}_{\mathcal{I}}$ denote the number of solutions of (3-2) such that $\mathcal{I}(\boldsymbol{x}) = \mathcal{I}$. As such, there is a particular set $\mathcal{J}$ which maximises the number of corresponding solutions such that

$$\mathfrak{A} = \sum_{\mathcal{I} \subsetneq \{1,\dots,n\}} \mathfrak{A}_{\mathcal{I}} \ll \mathfrak{A}_{\mathcal{J}}.$$

Considering now just solutions $\boldsymbol{y}$ for which $\mathcal{I}(\boldsymbol{y}) = \mathcal{J}$ in the interest of bounding $\mathfrak{A}_{\mathcal{J}}$, we may split (3-2) into the maximal degenerate part

$$\sum_{i \in \mathcal{J}} a_i x_i = 0 \tag{3-3}$$

and nondegenerate part

$$\sum_{i \in \{1,\dots,n\} \setminus \mathcal{J}} a_i x_i = 1. \tag{3-4}$$

Because solutions to (3-4) are nondegenerate by construction, the number of solutions is $\mathfrak{B} \ll 1$ by Lemma 3.1 with $\Pi = \Gamma^{n-\#\mathcal{J}}$.

By construction, $\#\mathcal{J} \le n-1$ and hence the number of solutions $\mathfrak{C}$ to (3-3) satisfies

$$\mathfrak{C} \ll A^{\lfloor (n-1)/2 \rfloor}$$

by Lemma 3.2 (except at $n = 1$, in which case the theorem we presently prove is trivial). This leads to the overall bound

$$\mathfrak{A} \ll \mathfrak{A}_{\mathcal{J}} \ll \mathfrak{B}\mathfrak{C} \ll A^{\lfloor (n-1)/2 \rfloor},$$

concluding the proof. □

As we saw when illustrating the tightness of Lemma 3.2, for the appropriate choice of $a_1, \dots, a_{n-1}$ we have $A^{\lfloor (n-1)/2 \rfloor}$ solutions to

$$a_1 x_1 + \cdots + a_{n-1} x_{n-1} = 0.$$

Choosing now $a_n = 1$ and $a_0 = x_n$ for some fixed $x_n \in \mathcal{A}$, we see that Lemma 3.3 is also tight.

We also require a bound on the number of solutions to a rather special system of two equations with elements of Γ.

Lemma 3.4. *Let $\mathbb{K}$ be a field of characteristic zero, and Γ a rank ϱ subgroup of $\mathbb{K}^*$. Suppose that $\mathcal{A} \subseteq \Gamma$ is a finite set of cardinality A. The number of solutions to the system of equations*

$$x_1 + \cdots + x_n = x_1^2 + \cdots + x_n^2 = 0, \quad x_1, \ldots, x_n \in \mathcal{A}, \tag{3-5}$$

is $O(A^{\lfloor 2n/5 \rfloor})$.

Proof. For each partition

$$\{1, \ldots, n\} = \bigsqcup_{i=1}^{h} \mathcal{I}_i$$

into $h \geq 1$ disjoint sets $\mathcal{I}_j$, with $\#\mathcal{I}_j \geq 2$, $j = 1, \ldots, h$, we count solutions to $x_1 + \cdots + x_n = 0$, which form nondegenerate solutions to each of the equations

$$\sum_{i \in \mathcal{I}_j} x_i = 0, \quad j = 1, \ldots, h.$$

Fixing one term of each equation and counting solutions in the remainder using Lemma 3.1, there are $O(A^h)$ such solutions.

Let k be the number of sets $\mathcal{I}_j$ with $\#\mathcal{I}_j = 2$, where, without loss of generality, we can assume that

$$\mathcal{I}_j = \{2j - 1, 2j\}, \quad j = 1, \ldots, k.$$

Hence $h \leq k + \lfloor (n - 2k)/3 \rfloor$ and thus there are at most

$$T_1 \ll A^{k + \lfloor (n-2k)/3 \rfloor} = A^{\lfloor (n+k)/3 \rfloor} \tag{3-6}$$

such solutions.

On the other hand, since we now have $x_{2j} = -x_{2j-1}$ for $j \leq k$, the equation $x_1^2 + \cdots + x_n^2 = 0$ becomes

$$2 \sum_{j=1}^{k} x_{2j-1}^2 + \sum_{j=2k+1}^{n} x_j^2 = 0,$$

which by Lemma 3.2 has at most

$$T_2 \ll A^{\lfloor (n-k)/2 \rfloor} \tag{3-7}$$

solutions, after which the remaining variables x_{2j}, $j = 1, \ldots, k$, are uniquely defined.

Choosing, for each $k \in \{0, \ldots, \lfloor n/2 \rfloor\}$, one of the bounds (3-6) or (3-7), whichever is smaller, we deduce that the number of solutions to (3-5) is $O(A^{\kappa_n})$, where

$$\kappa_n = \max_{k \in \{0, \ldots, \lfloor n/2 \rfloor\}} \min\bigl\{ \lfloor (n+k)/3 \rfloor, \lfloor (n-k)/2 \rfloor \bigr\}.$$

By noticing that if $k \le n/5$ then $(n+k)/3 \le 2n/5$, and similarly that if $k \ge n/5$ then $(n-k)/2 \le 2n/5$, it follows that

$$\kappa_n \le \frac{2n}{5},$$

and by the integrality of κ_n the result follows. $\square$

Remark 3.5. It is not difficult to further show that $\kappa_n = \lfloor 2n/5 \rfloor$ in the proof of Lemma 3.4, with the maximum attained at $k = \lfloor n/5 \rfloor$.

4. Proofs of main results

4.1. ***Proof of Theorem 2.1.*** Our proof employs several ideas introduced in [39, Theorem 2.1], with the appropriate alterations made to use Lemmas 3.2 and 3.3, which are the new tools available in our setting.

As in the derivation of (1-6), we simplify by counting the size of the set $\mathcal{R}^*_{m,n}(\mathcal{A}; r)$ of matrices in $\mathcal{R}_{m,n}(\mathcal{A}; r)$ in which the top left $r \times r$ submatrix is nonsingular.

For arbitrary $\boldsymbol{X} = (x_{i,j})_{i,j=1}^{n} \in \mathcal{R}^*_{m,n}(\mathcal{A}; r)$, we may write $\boldsymbol{X}$ as the block matrix

$$\boldsymbol{X} = \begin{bmatrix} \boldsymbol{X}_1 & \boldsymbol{X}_2 \\ \boldsymbol{X}_3 & \boldsymbol{X}_4 \end{bmatrix},$$

where

$$\boldsymbol{X}_1 = (x_{i,j})_{i,j=1}^{r}$$

is the $r \times r$ nonsingular submatrix which exists by assumption.

There are at most

$$\mathfrak{A} \ll A^{r^2}$$

possible values for the entries of $\boldsymbol{X}_1$.

Observe that for each integer $k \in \{r+1, \dots, m\}$, the k-th row of $\boldsymbol{X}$ is a unique linear combination of the first r rows, given by coefficients $\rho_1(k), \dots, \rho_r(k) \in \mathbb{K}$. We say that $\boldsymbol{X}_3$, the matrix immediately below $\boldsymbol{X}_1$, is of type $t \in \{1, \dots, r\}$ if t is the largest number of nonzero values among the coefficients $\rho_1(k), \dots, \rho_r(k)$ taken over each $k \in \{r+1, \dots, m\}$. Suppose that, in particular the h-th row is such that t of the coefficients are nonzero, that is, h corresponds with the row which maximises the value of t. Without loss of generality we assume that it is the first t coefficients $\rho_1(h), \dots, \rho_t(h)$ which are nonzero. It is therefore possible to choose a nonsingular $t \times t$ submatrix of

$$(x_{i,j})_{1 \le i \le t, 1 \le j \le r},$$

which we assume, without loss of generality, to be

$$(x_{i,j})_{i,j=1}^{t}.$$

This means that each of the A^t choices for $(x_{h,1},\dots,x_{h,t})$ defines fully the coefficients $(\rho_1(h),\dots,\rho_t(h))$ and subsequently $(\rho_1(h),\dots,\rho_r(h))$ by including the zero values. Thus the values of $x_{h,j}$ for $j\in\{t+1,\dots,r\}$ are also fixed, that is, the rest of the corresponding row of $\boldsymbol{X}_3$. Since h has been chosen to maximise the value of t, we can apply the same bound to each row of $\boldsymbol{X}_3$ to deduce that for each $\boldsymbol{X}_1$ there are

$$\mathfrak{B}_t=\prod_{j=r+1}^{m} A^t \ll A^{t(m-r)}$$

corresponding possible matrices $\boldsymbol{X}_3$ of type t.

Given such an h as described above, for each column indexed by $j\in\{r+1,\dots,n\}$ we have an equation

$$\rho_1(h)x_{1,j}+\cdots+\rho_r(h)x_{r,j}=x_{h,j} \tag{4-1}$$

determining the value of $x_{h,j}$ in terms of the value in the j-th column of the first r rows.

Solving this equation in $(x_{1,j},\dots,x_{r,j},x_{h,j})$ for each j as described above fixes the upper right $r\times(n-r)$ submatrix $\boldsymbol{X}_2$, along with the remainder of the h-th row. This means that for each $i\in\{r+1,\dots,m\}\setminus\{h\}$ the analogous equation

$$\rho_1(i)x_{1,j}+\cdots+\rho_r(i)x_{r,j}=x_{i,j},$$

with potentially fewer nonzero coefficients, has a fixed left-hand side, and thus $x_{i,j}$ on the right-hand side is uniquely determined.

Let $\mathfrak{C}_t$ be the maximum number of solutions to (4-1) where there are exactly t nonzero coefficients amongst $\rho_1(h),\dots,\rho_r(h)$ in variables $(x_{1,j},\dots,x_{r,j},x_{h,j})$ for each $j\in\{r+1,\dots,n\}$. Given that we require $n-r$ such equations for each j to count all remaining values of $\boldsymbol{X}$, summing over all possibles types t, we have an overall bound of

$$\#\mathcal{R}_{m,n}(\mathcal{A};r)\ll\#\mathcal{R}^{*}_{m,n}(\mathcal{A};r)\ll\mathfrak{A}\sum_{t=1}^{r}\mathfrak{B}_t\mathfrak{C}_t^{n-r}. \tag{4-2}$$

Subtracting $x_{h,j}$ from both sides of (4-1), we have an equation of the same form as in Lemma 3.2 with $t+1$ nonzero coefficients, and so we have

$$\mathfrak{C}_t\ll A^{\lfloor (t+1)/2\rfloor+r-t},$$

where the factor of $A^{r-t}=A^{(r+1)-(t+1)}$ counts the number of solutions in the “free” variables corresponding to the zero coefficients.

Now, computing the bound in (4-2) we have

$$\begin{aligned}\#\mathcal{R}_{m,n}(\mathcal{A};r) &\ll \mathfrak{A}\sum_{t=1}^{r}\mathfrak{B}_t\mathfrak{C}_t^{n-r} \ll A^{r^2}\sum_{t=1}^{r}A^{t(m-r)}(A^{\lfloor (t+1)/2\rfloor+r-t})^{n-r}\\ &\ll \sum_{t=1}^{r}A^{r^2+t(m-r)+\lfloor (t+1)/2\rfloor(n-r)+(r-t)(n-r)}\\ &\ll \max_{t\in\{1,\dots,r\}}A^{r^2+t(m-r)+\lfloor (t+1)/2\rfloor(n-r)+(r-t)(n-r)}.\end{aligned}$$

By defining

$$\delta(n,m,r,t)=r^2+t(m-r)+\left\lfloor\frac{t+1}{2}\right\rfloor(n-r)+(r-t)(n-r),$$

we may write

$$\#\mathcal{R}_{m,n}(\mathcal{A};r)\ll\max_{t\in\{1,\dots,r\}}A^{\delta(n,m,r,t)}. \tag{4-3}$$

Simplifying, we find that

$$\begin{aligned}\delta(n,m,r,t)&=mt+\left\lfloor\frac{t+1}{2}\right\rfloor(n-r)-nt+nr\\ &=nr+t\left(m-\frac{n+r}{2}\right)+\begin{cases}\frac{n-r}{2} & \text{for } t \text{ odd},\\ 0 & \text{for } t \text{ even}.\end{cases}\end{aligned}$$

If $2m\le n+r$, then the maximum value of δ over t corresponds to

$$t=1. \tag{4-4}$$

If $2m>n+r$, then $\delta(n,m,r,t)$ is strictly monotonically increasing over integers t of the same parity. Thus it suffices to check the two possibilities $t\in\{r,r-1\}$. As such, we consider that

$$\begin{aligned}&\delta(n,m,r,r)-\delta(n,m,r,r-1)\\ &\qquad=r\left(m-\frac{n+r}{2}\right)-(r-1)\left(m-\frac{n+r}{2}\right)+(-1)^{r+1}\frac{n-r}{2}\\ &\qquad=\left(m-\frac{n+r}{2}\right)+(-1)^{r+1}\frac{n-r}{2}\\ &\qquad=\begin{cases}m-r & \text{for } r \text{ odd},\\ m-n & \text{for } r \text{ even}.\end{cases}\end{aligned}$$

In particular, for odd r, we have $\delta(n,m,r,r)\ge\delta(n,m,r,r-1)$, while for even r, we have $\delta(n,m,r,r)\le\delta(n,m,r,r-1)$. Therefore the choice of t which maximises δ is given by

$$t=\begin{cases}r & \text{if } r \text{ is odd},\\ r-1 & \text{if } r \text{ is even},\end{cases}$$

or equivalently

$$t = 2\left\lfloor \frac{r-1}{2} \right\rfloor + 1. \tag{4-5}$$

Therefore, in the case when $2m \le n + r$, with the choice of t in (4-4),

$$\delta(n, m, r, t) = nr + \left(m - \frac{n+r}{2}\right) + \frac{n-r}{2} = nr + m - r,$$

while for $2m > n + r$, with the choice of t in (4-5), we have

$$\begin{aligned} \delta(n, m, r, t) &= nr + \left(2\left\lfloor \frac{r-1}{2} \right\rfloor + 1\right)\left(m - \frac{n+r}{2}\right) + \frac{n-r}{2} \\ &= nr + m - r + \left\lfloor \frac{r-1}{2} \right\rfloor (2m - n - r). \end{aligned}$$

Substituting these into (4-3), we conclude the proof.

4.2. ***Proof of Theorem 2.2.*** For the case when $d = 0$, we may write $\mathcal{D}_n(\mathcal{A}; 0)$ as the set of matrices which have rank strictly less than n. Therefore,

$$\#\mathcal{D}_n(\mathcal{A}; 0) = \sum_{r=1}^{n-1} \#\mathcal{R}_n(\mathcal{A}; r).$$

Applying now Theorem 2.1 (when $2m > n + r$, which in our case $m = n$ is equivalent to $r < n$), we deduce

$$\begin{aligned} \#\mathcal{D}_n(\mathcal{A}; 0) &\ll \sum_{r=1}^{n-1} A^{nr+n-r+\lfloor (r-1)/2 \rfloor (n-r)} \\ &\ll \max_{r \in \{1,\dots,n-1\}} A^{nr+n-r+\lfloor (r-1)/2 \rfloor (n-r)}. \end{aligned} \tag{4-6}$$

Defining

$$\delta(n, r) = nr + n - r + \left\lfloor \frac{r-1}{2} \right\rfloor (n - r)$$

for the exponent in the above expression, we have

$$\begin{aligned} \delta(n, r) &= nr + n - r + \frac{r}{2}(n - r) + (r - n) \cdot \begin{cases} \frac{1}{2} & \text{if } r \text{ is odd,} \\ 1 & \text{if } r \text{ is even,} \end{cases} \\ &= r\left(\frac{3}{2}n - \frac{r}{2} - 1\right) + n + (r - n) \cdot \begin{cases} \frac{1}{2} & \text{if } r \text{ is odd,} \\ 1 & \text{if } r \text{ is even.} \end{cases} \end{aligned}$$

Straightforward computations similar to those in the proof of Theorem 2.1 show that $\delta(n, r)$ is increasing over integers r of the same parity, and that as a function of $r \in \{1, \dots, n-1\}$, it is maximised at $r = n - 1$. Substituting this back in (4-6) we deduce

$$\#\mathcal{D}_n(\mathcal{A}; 0) \ll A^{n^2 - \lceil n/2 \rceil}, \tag{4-7}$$

proving the case $d = 0$.

Suppose now that $d \neq 0$. Take a matrix $\boldsymbol{X} \in \mathcal{D}_n(\mathcal{A}; d)$ and consider the Laplace expansion for the determinant across the first row given by

$$\det \boldsymbol{X} = d = \sum_{j=1}^{n} (-1)^{j+1} x_{1,j} \det \boldsymbol{X}_{1,j}, \tag{4-8}$$

where $\boldsymbol{X}_{1,j}$ is the submatrix of $\boldsymbol{X}$ obtained by removing the first row and the j-th column.

Suppose firstly that none of the minors $\det \boldsymbol{X}_{1,j}$ in (4-8) are zero. In this case, we have at most

$$\mathfrak{A} \ll A^{n^2-n}$$

possibilities for the bottom $n-1$ rows of $\boldsymbol{X}$. Given that none of the minors are zero, we solve (4-8) in the variables $x_{1,j}$ in

$$\mathfrak{B} \ll A^{\lfloor (n-1)/2 \rfloor}$$

ways by Lemma 3.3, leading to an overall bound of

$$\mathfrak{A}\mathfrak{B} \ll A^{n^2-n+\lfloor (n-1)/2 \rfloor} = A^{n^2-\lceil (n+1)/2 \rceil}. \tag{4-9}$$

Now, suppose that at least one of the minors $\det \boldsymbol{X}_{1,j}$ is zero, which now excludes the possibility $n = 2$. We can assume, without loss of generality, that in particular, $\det \boldsymbol{X}_{1,1} = 0$. Thus, there are at most

$$\mathfrak{C} = \#\mathcal{D}_{n-1}(\mathcal{A}; 0) \ll A^{(n-1)^2-\lceil (n-1)/2 \rceil} = A^{n^2-2n+1-\lceil (n-1)/2 \rceil}$$

possibilities for $\boldsymbol{X}_{1,1}$ by (4-7).

We can then fix the elements $x_{1,1}, x_{2,1}, \ldots, x_{n,1}$ in

$$\mathfrak{D} = A^n$$

ways, leaving only the first row less the top left entry unfixed. Under these assumptions, (4-8) becomes

$$d = \sum_{j=2}^{n} (-1)^{j+1} x_{1,j} \det \boldsymbol{X}_{1,j}. \tag{4-10}$$

Let $\mathfrak{E}_t$ be the number of solutions to (4-10) under the assumption that exactly t of the matrix minors are nonzero. We assume, without loss of generality, that it is the first t coefficients of the variables $x_{1,2}, \ldots, x_{1,(t+1)}$ which are nonzero.

If $t = 1$ then

$$d = -x_{1,2} \det \boldsymbol{X}_{1,2},$$

where $\det \boldsymbol{X}_{1,2} \neq 0$ is already fixed. This defines $x_{1,2}$ uniquely, while the remaining variables can be fixed in A^{n-2} ways leading to a bound of

$$\mathfrak{E}_1 \ll A^{n-2}.$$

If $t = 2$, then we have an equation

$$d = -x_{1,2} \det \boldsymbol{X}_{1,2} + x_{1,3} \det \boldsymbol{X}_{1,3}$$

with $O(1)$ solutions by Lemma 3.3, while the remaining elements can be fixed in A^{n-3} ways leading to a bound of

$$\mathfrak{E}_2 \ll A^{n-3}.$$

If $3 \le t \le n-1$, which may only happen when $n \ge 4$, we can solve for the nonzero coefficients in $A^{\lfloor (t-1)/2 \rfloor}$ by Lemma 3.3 ways and the remaining coefficients in A^{n-1-t} ways leading to

$$\mathfrak{E}_t \ll A^{n-1-t+\lfloor (t-1)/2 \rfloor}.$$

We observe that for $t = 1$ this also formally coincides with the above bound on $\mathfrak{E}_1$.

Combining these, we have a total bound on the number of matrices in $\mathcal{D}_n(\mathcal{A}; d)$ which have a singular submatrix in the Laplace expansion as

$$\begin{aligned} \mathfrak{C}\mathfrak{D}\mathfrak{E}_t &\ll A^{n^2-2n+1-\lceil (n-1)/2 \rceil} \cdot A^n \cdot \begin{cases} A^{n-3} & \text{if } t = 2, \\ A^{n-1-t+\lfloor (t-1)/2 \rfloor} & \text{if } t = 1 \text{ or } 3 \le t \le n-1, \end{cases} \\ &= \begin{cases} A^{n^2-\lceil (n+3)/2 \rceil} & \text{if } t = 2, \\ A^{n^2-\lceil (n-1)/2 \rceil - t + \lfloor (t-1)/2 \rfloor} & \text{if } t = 1 \text{ or } 3 \le t \le n-1. \end{cases} \end{aligned}$$

One can easily check that the expression is maximised at $t = 1$. Therefore, for $1 \le t \le n-1$ we have

$$\mathfrak{C}\mathfrak{D}\mathfrak{E}_t \ll A^{n^2-\lceil (n+1)/2 \rceil}. \tag{4-11}$$

Hence, combining (4-9) and (4-11), we have overall

$$\#\mathcal{D}_n(\mathcal{A}; d) = \mathfrak{A}\mathfrak{B} + \sum_{t=2}^{n-1} \mathfrak{C}\mathfrak{D}\mathfrak{E}_t \ll A^{n^2-\lceil (n+1)/2 \rceil},$$

concluding the proof.

Remark 4.1. We note that while the bound of Theorem 2.2 for $d \neq 0$ is dominated by (4-9), we can eliminate the other bottleneck coming from (4-11), which corresponds to the case $t = 1$, by showing that this case is impossible. Since this general argument can be useful for other similar questions, we present it in Appendix A; see Proposition A.1.

4.3. *Proofs of Theorems 2.3 and 2.4.*

4.3.1. *The case $n = 2$ (Theorem 2.3).* For each matrix

$$\boldsymbol{X} = \begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix} \in \mathcal{P}_2(\mathcal{A};\, T^2 - tT + d),$$

the entries are related to the coefficients of the characteristic polynomial by the equations

$$x_{1,1}x_{2,2} - x_{1,2}x_{2,1} = d = \det \boldsymbol{X} \tag{4-12}$$

and

$$x_{1,1} + x_{2,2} = t = \operatorname{tr} \boldsymbol{X}. \tag{4-13}$$

Suppose firstly that $t = 0$ and $d \neq 0$. Hence by (4-13) we have $x_{1,1} = -x_{2,2}$, which, when substituted into (4-12) yields

$$-(x_{1,1})^2 - x_{1,2}x_{2,1} = d.$$

For each possible value of $x_{1,2}$, we have an equation in $(x_{1,1})^2$ and $x_{2,1}$ with $O(1)$ solutions by Lemma 3.3, solving over the set $\mathcal{A} \cup \{x^2 : x \in \mathcal{A}\}$, which contains no more than twice the number of elements in $\mathcal{A}$. This induces at most two values for $x_{1,1}$ and then for each of these, a unique value of $x_{2,2}$ by (4-13). Hence up to a constant, the value of $x_{1,2}$ determines the rest of the matrix, so there are only $O(A)$ such matrices.

Now, suppose that $t \neq 0$. The equation (4-13) has $O(1)$ solutions in $x_{1,1}$ and $x_{2,2}$ by Lemma 3.3. Assuming these values are now fixed, we trivially have $O(A)$ solutions to (4-12) in $x_{1,2}$ and $x_{2,1}$ because either value uniquely determines the other. Thus there exist $O(A)$ such matrices.

4.3.2. *The case $n \geq 3$ (Theorem 2.4).* We construct an upper bound on $\#\mathcal{P}_n(\mathcal{A};\, f)$ by acquiring an upper bound on the larger set of matrices $\boldsymbol{X} = (x_{i,j})_{i,j=1}^n \in \mathcal{M}_n(\mathcal{A})$ for which only the coefficients c_{n-1} and c_{n-2} of the characteristic polynomial

$$f = \det(TI_n - \boldsymbol{X}) = \sum_{k=0}^{n} c_k T^k$$

are fixed.

Given that c_{n-1} and c_{n-2} are given by

$$c_{n-1} = -\operatorname{tr} \boldsymbol{X} \quad \text{and} \quad c_{n-2} = \tfrac{1}{2}((\operatorname{tr} \boldsymbol{X})^2 - \operatorname{tr} \boldsymbol{X}^2), \tag{4-14}$$

we may instead equivalently fix $t_1 = \operatorname{tr} \boldsymbol{X}$ and $t_2 = \operatorname{tr} \boldsymbol{X}^2$.

Fixing t_1 leads to an equation

$$t_1 = \sum_{i=1}^{n} x_{i,i}, \tag{4-15}$$

while fixing t_2 we have

$$t_2 = \sum_{i=1}^{n} \sum_{j=1}^{n} x_{i,j} x_{j,i} = \sum_{i=1}^{n} x_{i,i}^2 + 2 \sum_{1 \le i < j \le n} x_{i,j} x_{j,i},$$

which leads to the equation

$$\frac{1}{2}\left(t_2 - \sum_{i=1}^{n} x_{i,i}^2 \right) = \sum_{1 \le i < j \le n} x_{i,j} x_{j,i}. \tag{4-16}$$

We first note that there are at most

$$\mathfrak{A} \ll A^{n(n-1)/2}$$

possibilities for the elements $x_{i,j}$ for $1 \le i < j \le n$.

We begin by first counting the set of matrices for which

$$t_2 = \sum_{i=1}^{n} x_{i,i}^2, \tag{4-17}$$

and within this consider two cases,

$$(t_1, t_2) = (0, 0) \quad \text{and} \quad (t_1, t_2) \ne (0, 0).$$

If $(t_1, t_2) = (0, 0)$, then the number of possible values for the main diagonal is $A^{\lfloor 2n/5 \rfloor}$ by Lemma 3.4. If either $t_1 \ne 0$ or $t_2 \ne 0$, then we may solve (4-15) or (4-17) respectively for all the $x_{i,i}$ in $A^{\lfloor (n-1)/2 \rfloor}$ ways by Lemma 3.3, where in the second case we count the solutions over $\{x^2 : x \in \mathcal{A}\} \subseteq \Gamma$ which is no larger than $\mathcal{A}$, thus fixing each $x_{i,i}$ up to a constant. This means that overall the number of possibilities for the main diagonal is given by

$$\mathfrak{B} \ll \begin{cases} A^{\lfloor 2n/5 \rfloor} & \text{if } (t_1, t_2) = (0, 0), \\ A^{\lfloor (n-1)/2 \rfloor} & \text{otherwise.} \end{cases}$$

From (4-17), the left-hand side of (4-16) is zero and hence the number of possibilities for $x_{i,j}$ with $1 \le j < i \le n$ is

$$\mathfrak{C} \ll A^{\lfloor n(n-1)/4 \rfloor}$$

by Lemma 3.2.

This means that the set of matrices with a fixed trace and trace squared which satisfy (4-17) is given by

$$\mathfrak{A}\mathfrak{B}\mathfrak{C} \ll A^{n(n-1)/2 + \lfloor n(n-1)/4 \rfloor} \cdot \begin{cases} A^{\lfloor 2n/5 \rfloor} & \text{if } (t_1, t_2) = (0, 0), \\ A^{\lfloor (n-1)/2 \rfloor} & \text{otherwise.} \end{cases} \tag{4-18}$$

Now we consider the complementary case to (4-17) of matrices for which

$$t_2 \neq \sum_{i=1}^{n} x_{i,i}^2. \tag{4-19}$$

By considering solutions to (4-15), we can see that the number of possibilities for $x_{1,1}, \dots, x_{n,n}$ is

$$\mathfrak{D} \ll \begin{cases} A^{\lfloor n/2 \rfloor} & \text{if } t_1 = 0, \\ A^{\lfloor (n-1)/2 \rfloor} & \text{if } t_1 \neq 0, \end{cases}$$

by Lemma 3.2 and Lemma 3.3 respectively.

Now, in this case, from (4-19), the left-hand side of (4-16) is nonzero and hence the number of possibilities for $x_{i,j}$ with $1 \le j < i \le n$ is

$$\mathfrak{E} \ll A^{\lfloor n(n-1)/4 - 1/2 \rfloor}$$

by Lemma 3.3.

Thus the number of matrices of a fixed trace and trace squared satisfying (4-19) is

$$\mathfrak{A}\mathfrak{D}\mathfrak{E} \ll A^{n(n-1)/2 + \lfloor n(n-1)/4 - 1/2 \rfloor} \cdot \begin{cases} A^{\lfloor n/2 \rfloor} & \text{if } t_1 = 0, \\ A^{\lfloor (n-1)/2 \rfloor} & \text{if } t_1 \neq 0. \end{cases} \tag{4-20}$$

Clearly, the second bound in (4-20) is always dominated by the first bound in (4-20). One also checks that for $n \ge 3$ we have $\lfloor 2n/5 \rfloor \le \lfloor (n-1)/2 \rfloor$. Hence, the first bound in (4-18) is always dominated by the second one.

Therefore, the bounds (4-18) and (4-20) imply

$$\mathcal{P}_n(\mathcal{A}; f) \ll A^{\alpha(n)},$$

where $\alpha(n)$ is given by (2-2).

5. Further questions

There are various possible generalisations and extensions of the problems we consider here. Firstly, it is quite natural to consider special types of matrices such as those with symmetry constraints including symmetric, skew symmetric, or Hermitian matrices, as considered in [18; 21; 27]. We expect these questions require new ideas. For instance, the method of fixing the trace and trace of the square as in Theorem 2.4 lends itself particularly poorly to counting symmetric matrices.

Motivated by recent work on counting commuting pairs of matrices [14; 40], one can also ask about an upper bound on the number of commuting pairs $\boldsymbol{XY} = \boldsymbol{YX}$ with $\boldsymbol{X}, \boldsymbol{Y} \in \mathcal{M}_n(\mathcal{A})$. Once can also ask about multiplicative dependencies in s-tuples of matrices from $\mathcal{M}_n(\mathcal{A})$, similarly to questions studied in [16; 31]. For example, Theorem 2.2 combined with Theorems 2.3 and 2.4 enables us to apply some ideas from [31] for such questions (at least for sets $\mathcal{A} \subseteq \mathbb{Z}$).

Since the work of Blomer and Li [9] is a part of our motivation, it is natural to investigate the same type of applications as in [9] and thus study the statistics of gaps between values of linear forms in elements of finite rank multiplicative subgroups of $\mathbb{R}^*$. One can also generalise the results here to matrices with polynomials entries, evaluated on elements of $\mathcal{A} \subseteq \Gamma$, similarly to [9; 39].

Finally, one can ask about similar questions over fields of positive characteristic, for example for subsets of finitely generated multiplicative group in the field of rational functions over a finite field.

Appendix A. Vanishing minors in Laplace expansion

Proposition A.1. *Let $\mathbb{K}$ be a field, and suppose $n \geq 2$. For any nonsingular matrix $X \in \mathcal{M}_n(\mathbb{K})$ with nonzero entries, the Laplace expansion about any row or column has at most $n-2$ zero minors.*

We also remark that the assumption that X has nonzero entries is stronger than necessary. It is sufficient to require that the span of the rows or columns not including the one being expanded about contains a vector with no zero entries.

Proof. Without loss of generality, we can consider expansion about the top row. Let $X = (x_{i,j})_{i,j=1}^{n} \in \mathcal{M}_n(\mathbb{K})$, and similarly define

$$\widetilde{X} = \begin{bmatrix} x_{n,1} & x_{n,2} & \cdots & x_{n,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,n} \end{bmatrix} \in \mathcal{M}_n(\mathbb{K})$$

as the matrix obtained by replacing the first row of X with the bottom row. Clearly $\widetilde{X}$ is singular, and hence the Laplace expansion about the first row yields

$$0 = \det \widetilde{X} = \sum_{j=1}^{n} (-1)^{j+1} x_{n,j} \det X_{1,j}, \tag{A-1}$$

where, as before, $X_{1,j}$ is the submatrix of X obtained by removing the first row and the j-th column of X, or equivalently $\widetilde{X}$.

It is impossible for $\det X_{1,j}$ to be zero for all $j \in \{1, \dots, n\}$, otherwise $\det X = 0$, contradicting the assumed nonsingularity of X. It is likewise impossible for exactly $n-1$ of the cofactors $\det X_{1,j}$ to be zero, otherwise, because in this case, since all the $x_{n,j}$ are nonzero, the right-hand side of (A-1) is also nonzero.

Therefore, at most $n-2$ of the cofactors may be zero. □

Appendix B. Tighter bounds from the proof of Theorem 2.4

By careful consideration of the bounds in (4-18) and (4-20) over distinct cases based on the value of t_1, t_2, and n, determining the particular maximum in each instance, one can prove a tighter bound on $\#\mathcal{P}_n(\mathcal{A}; f)$ than that of Theorem 2.4. We present this bound below, without proof.

It is convenient to define

$$\beta(n) = \tfrac{3}{4}n^2 - \tfrac{1}{4}n. \tag{B-1}$$

Theorem B.1. *Let $\mathbb{K}$ be a field of characteristic zero, and Γ a rank ϱ subgroup of $\mathbb{K}^*$. For any monic polynomial*

$$f = \sum_{k=0}^{n} c_k T^k \in \mathbb{K}[T]$$

of degree $n \geq 3$, and $\mathcal{A} \subseteq \Gamma$ of finite cardinality A, we have

$$\#\mathcal{P}_n(\mathcal{A}; f) \ll A^{\beta(n)} \cdot \begin{cases} A^{-\lambda(n)} & \text{if } c_{n-1} = c_{n-2} = 0, \\ A^{-\mu(n)} & \text{if } c_{n-1} = 0 \text{ and } c_{n-2} \neq 0, \\ A^{-\nu(n)} & \text{if } c_{n-1} \neq 0, \end{cases}$$

where $\beta(n)$ is given by (B-1) *and furthermore*

$$\lambda(n) = \begin{cases} 1 & \text{if } n \equiv 0, 3 \pmod 4, \\ \frac{3}{2} & \text{if } n \equiv 1 \pmod 4 \text{ and } n \neq 5, \\ \frac{1}{2} & \text{if } n \equiv 2 \pmod 4 \text{ or } n = 5, \end{cases}$$

$$\mu(n) = \begin{cases} 1 & \text{if } n \equiv 0, 3 \pmod 4, \\ \frac{1}{2} & \text{if } n \equiv 1, 2 \pmod 4, \end{cases}$$

$$\nu(n) = \begin{cases} 1 & \text{if } n \equiv 0, 3 \pmod 4, \\ \frac{1}{2} & \text{if } n \equiv 1 \pmod 4, \\ \frac{3}{2} & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

In the case when $\mathbb{K} = \mathbb{R}$ we can further improve the bound in a few particular cases by noticing that when $t_2 = 0$, the left-hand side of (4-16) must be nonzero, allowing the use of Lemma 3.3 rather than possibly Lemma 3.2. This leads to the following result.

Theorem B.2. *Suppose Γ is a rank ϱ subgroup of $\mathbb{R}^*$ and $n \geq 3$ with $n \equiv 0, 1 \pmod 4$. For any monic polynomial*

$$f = \sum_{k=0}^{n} c_k T^k \in \mathbb{R}[T]$$

of degree n and $\mathcal{A} \subseteq \Gamma$ of finite cardinality A, we have:

- *If* $c_{n-1} \neq 0$ *and* $2c_{n-2} = c_{n-1}^2$,
$$\#\mathcal{P}_n(\mathcal{A};\, f) \ll A^{\beta(n)} \cdot \begin{cases} A^{-2} & \text{if } n \equiv 0 \pmod 4, \\ A^{-3/2} & \text{if } n \equiv 1 \pmod 4, \end{cases}$$
where $\beta(n)$ *is given by* (B-1).
- *If* $c_{n-1} = c_{n-2} = 0$ *and* $n = 5$,
$$\#\mathcal{P}_5(\mathcal{A};\, f) \ll A^{\beta(5)-3/2}.$$

Note that for $n \equiv 2, 3 \pmod 4$, the fact that $\Gamma \subseteq \mathbb{R}^*$ does not offer any advantage.

Acknowledgement

The authors would like to thank the referee for the careful reading of the manuscript and useful comments.

This work was supported, in part, by the Australian Research Council grants DP230100530 and DP230100534. Ostafe also gratefully acknowledges the hospitality and support of the Max Planck Institute for Mathematics and Institut des Hautes Études Scientifiques, where parts of her work have been carried out.

References

[1] A. Abrams, Z. Landau, J. Pommersheim, and N. Srivastava, “On eigenvalue gaps of integer matrices”, *Math. Comp.* **94**:352 (2025), 853–862. MR

[2] M. Afifurrahman, “Some counting questions for matrix products”, *Bull. Aust. Math. Soc.* **110**:1 (2024), 32–43. MR

[3] M. Afifurrahman, “A uniform formula on the number of integer matrices with given determinant and height”, preprint, 2024. arXiv 2407.08191

[4] M. Afifurrahman, V. Kuperberg, A. Ostafe, and I. E. Shparlinski, “Statistics of ranks, determinants and characteristic polynomials of rational matrices”, *Forum Math.* **37**:4 (2025), 1259–1289. MR

[5] O. Ahmadi and I. E. Shparlinski, “Distribution of matrices with restricted entries over finite fields”, *Indag. Math.* (*N.S.*) **18**:3 (2007), 327–337. MR

[6] N. Alon and J. Solymosi, “Rank of matrices with entries from a multiplicative group”, *Int. Math. Res. Not.* **2023**:14 (2023), 12383–12399. MR

[7] F. Amoroso and E. Viada, “Small points on subvarieties of a torus”, *Duke Math. J.* **150**:3 (2009), 407–442. MR

[8] L. M. Arutyunyan, “On the growth of the number of determinants with restricted entries”, *Mat. Zametki* **109**:6 (2021), 803–809. In Russian; translated in *Mathem. Notes*, **109** (2021), 843–848. MR

[9] V. Blomer and J. Li, “Correlations of values of random diagonal forms”, *Int. Math. Res. Not.* **2023**:23 (2023), 20296–20336. MR

[10] V. Blomer and C. Lutsko, “Hyperbolic lattice point counting in unbounded rank”, *J. Reine Angew. Math.* **812** (2024), 257–274. MR

[11] J. Bourgain, V. H. Vu, and P. M. Wood, “On the singularity probability of discrete random matrices”, *J. Funct. Anal.* **258**:2 (2010), 559–603. MR

[12] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski, “Multiplicative congruences with variables from short intervals”, *J. Anal. Math.* **124** (2014), 117–147. MR

[13] R. P. Brent and B. D. McKay, “Determinants and ranks of random matrices over Z_m”, *Discrete Math.* **66**:1-2 (1987), 35–49. MR

[14] T. Browning, W. Sawin, and V. Y. Wang, “Pairs of commuting integer matrices”, preprint, 2024. arXiv 2409.01920

[15] K. Bulinski and I. E. Shparlinski, “Counting elements of the congruence subgroup”, *Canad. Math. Bull.* **67**:4 (2024), 955–969. MR

[16] K. Bulinski, A. Ostafe, and I. E. Shparlinski, “Counting embeddings of free groups into $\mathrm{SL}_2(\mathbb{Z})$ and its subgroups”, To appear in *Ann. Scuola Normale Pisa*.

[17] M. Campos, M. Jenssen, M. Michelen, and J. Sahasrabudhe, “The singularity probability of a random symmetric matrix is exponentially small”, *J. Amer. Math. Soc.* **38**:1 (2025), 179–224. MR

[18] W. Duke, Z. Rudnick, and P. Sarnak, “Density of integer points on affine homogeneous varieties”, *Duke Math. J.* **71**:1 (1993), 143–179. MR

[19] S. Eberhard, “The characteristic polynomial of a random matrix”, *Combinatorica* **42**:4 (2022), 491–527. MR

[20] D. El-Baz, M. Lee, and A. Strömbergsson, “Effective equidistribution of primitive rational points on expanding horospheres”, preprint, 2022. arXiv 2212.07408

[21] A. Eskin and Y. R. Katznelson, “Singular symmetric matrices”, *Duke Math. J.* **79**:2 (1995), 515–547. MR

[22] A. Eskin, S. Mozes, and N. Shah, “Unipotent flows and counting lattice points on homogeneous varieties”, *Ann. of Math.* (2) **143**:2 (1996), 253–299. MR

[23] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt, “Linear equations in variables which lie in a multiplicative group”, *Ann. of Math.* (2) **155**:3 (2002), 807–836. MR

[24] W. Feit and N. J. Fine, “Pairs of commuting matrices over a finite field”, *Duke Math. J.* **27** (1960), 91–94. MR

[25] A. Ferber, K. Luh, and G. McKinley, “Resilience of the rank of random matrices”, *Combin. Probab. Comput.* **30**:2 (2021), 163–174. MR

[26] A. Ferber, V. Jain, A. Sah, and M. Sawhney, “Random symmetric matrices: rank distribution and irreducibility of the characteristic polynomial”, *Math. Proc. Cambridge Philos. Soc.* **174**:2 (2023), 233–246. MR

[27] J. Fulman, “Random matrix theory over finite fields”, *Bull. Amer. Math. Soc.* (*N.S.*) **39**:1 (2002), 51–85. MR

[28] J. Fulman and L. Goldstein, “Stein’s method and the rank distribution of random matrices over finite fields”, *Ann. Probab.* **43**:3 (2015), 1274–1314. MR

[29] M. Gerstenhaber, “On the number of nilpotent matrices with coefficients in a finite field”, *Illinois J. Math.* **5** (1961), 330–333. MR

[30] A. Gorodnik, A. Nevo, and G. Yehoshua, “Counting lattice points in norm balls on higher rank simple Lie groups”, *Math. Res. Lett.* **24**:5 (2017), 1285–1306. MR

[31] P. Habegger, A. Ostafe, and I. E. Shparlinski, “Integer matrices with a given characteristic polynomial and multiplicative dependence of matrices”, preprint, 2022. arXiv 2203.03880

[32] V. Jain, A. Sah, and M. Sawhney, “Singularity of discrete random matrices”, *Geom. Funct. Anal.* **31**:5 (2021), 1160–1218. MR

[33] Y. R. Katznelson, “Singular matrices and a uniform bound for congruence groups of $\mathrm{SL}_n(\mathbf{Z})$”, *Duke Math. J.* **69**:1 (1993), 121–136. MR

[34] Y. R. Katznelson, “Integral matrices of fixed rank”, *Proc. Amer. Math. Soc.* **120**:3 (1994), 667–675. MR

[35] D. Koh, T. Pham, C.-Y. Shen, and L. A. Vinh, “On the determinants and permanents of matrices with restricted entries over prime fields”, *Pacific J. Math.* **300**:2 (2019), 405–417. MR

[36] S. Koplewitz, “The corank of a rectangular random integer matrix”, *Linear Algebra Appl.* **591** (2020), 160–168. MR

[37] M. Kwan and L. Sauermann, “On the permanent of a random symmetric matrix”, *Selecta Math.* (*N.S.*) **28**:1 (2022), art. id. 15, 29 pp. MR

[38] L. Mérai and I. E. Shparlinski, “Number of characteristic polynomials of matrices with bounded height”, *Linear Algebra Appl.* **712** (2025), 1–8. MR

[39] A. Mohammadi, A. Ostafe, and I. E. Shparlinski, “On some matrix counting problems”, *J. Lond. Math. Soc.* (2) **110**:6 (2024), art. id. e70044, 28 pp. MR

[40] A. Mudgal, “On commuting pairs in arbitrary sets of 2 × 2 matrices”, preprint, 2024. arXiv 2411.10404

[41] H. H. Nguyen and E. Paquette, “Surjectivity of near-square random matrices”, *Combin. Probab. Comput.* **29**:2 (2020), 267–292. MR

[42] H. H. Nguyen and M. M. Wood, “Random integral matrices: universality of surjectivity and the cokernel”, *Invent. Math.* **228**:1 (2022), 1–76. MR

[43] A. Ostafe and I. E. Shparlinski, “On the sparsity of non-diagonalisable integer matrices and matrices with a given discriminant”, preprint, 2023. arXiv 2312.12626

[44] I. Reiner, “On the number of matrices with given characteristic polynomial”, *Illinois J. Math.* **5** (1961), 324–329. MR

[45] C. Sanna, “On the distribution of the entries of a fixed-rank random matrix over a finite field”, *Finite Fields Appl.* **93** (2024), art. id. 102333, 15 pp. MR

[46] W. M. Schmidt, “Norm form equations”, *Ann. of Math.* (2) **96** (1972), 526–551. MR

[47] N. A. Shah, “Counting integral matrices with a given characteristic polynomial”, *Sankhyā Ser. A* **62**:3 (2000), 386–412. MR

[48] U. Shapira and C. Zheng, “Limiting distributions of translates of divergent diagonal orbits”, *Compos. Math.* **155**:9 (2019), 1747–1793. MR

[49] I. D. Shkredov and I. E. Shparlinski, “On the determinants of matrices with elements from arbitrary sets”, *Mathematika* **71**:2 (2025), art. id. e70018, 18 pp. MR

[50] I. E. Shparlinski, “Some counting questions for matrices with restricted entries”, *Linear Algebra Appl.* **432**:1 (2010), 155–160. MR

[51] T. Tao and V. H. Vu, “Inverse Littlewood–Offord theorems and the condition number of random discrete matrices”, *Ann. of Math.* (2) **169**:2 (2009), 595–632. MR

[52] V. H. Vu, “Recent progress in combinatorial random matrix theory”, *Probab. Surv.* **18** (2021), 179–200. MR

[53] D. Wei and F. Xu, “Counting integral points in certain homogeneous spaces”, *J. Algebra* **448** (2016), 350–398. MR

[54] M. M. Wood, “Random integral matrices and the Cohen–Lenstra heuristics”, *Amer. J. Math.* **141**:2 (2019), 383–398. MR

Received February 19, 2025. Revised August 25, 2025.

AARON MANNING
SCHOOL OF MATHEMATICS AND STATISTICS
UNIVERSITY OF NEW SOUTH WALES
SYDNEY NSW
AUSTRALIA

contact@aaronmanning.net

ALINA OSTAFE
SCHOOL OF MATHEMATICS AND STATISTICS
UNIVERSITY OF NEW SOUTH WALES
SYDNEY NSW
AUSTRALIA

alina.ostafe@unsw.edu.au

IGOR E. SHPARLINSKI
SCHOOL OF MATHEMATICS AND STATISTICS
UNIVERSITY OF NEW SOUTH WALES
SYDNEY NSW
AUSTRALIA

igor.shparlinski@unsw.edu.au