COUNTING MATRICES OVER FINITE RANK MULTIPLICATIVE GROUPS: EXPANDED APPENDIX

AARON MANNING

Abstract. This note contains the missing proofs from the publication [1].

Contents

1. Introduction

For a finite subset $\mathcal{A}$ of a field $\mathbb{K}$, we define $\mathcal{M}_n(\mathcal{A})$ to be the set of $n \times n$ matrices with entries from $\mathcal{A}$.

Further, define the subset of matrices in $\mathcal{M}_n(\mathcal{A})$ with a given characteristic polynomial $f \in \mathbb{K}[T]$,

$$\mathcal{P}_n(\mathcal{A}; f) = \{\mathbf{X} \in \mathcal{M}_n(\mathcal{A}) : \det(TI_n - \mathbf{X}) = f\}. \tag{1.1}$$

Let $\mathbb{K}$ be a field of characteristic zero, Γ a rank ρ subgroup of the multiplicative group $\mathbb{K}^*$, and cA a finite subset of Γ. In the article [1] by the present author and collaborators, we give bounds on the cardinality of $\mathcal{P}_n(\mathcal{A}; f)$ in in this setting, asymptotically with respect to $A = \#\mathcal{A}$. The corresponding result [1, Theorem 2.4] is reproduced

Date: 4 September 2026.

below as Theorem 1.1, and refers to the function

$$\begin{aligned}\alpha(n) = \frac{n(n-1)}{2} + \max\Bigg\{ \left\lfloor \frac{n-1}{2} \right\rfloor + \left\lfloor \frac{n(n-1)}{4} \right\rfloor, \\ \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n(n-1)}{4} - \frac{1}{2} \right\rfloor \Bigg\}.\end{aligned} \tag{1.2}$$

Theorem 1.1. *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 $n \geqslant 3$, and $\mathcal{A} \subseteq \Gamma$ of finite cardinality A, we have*

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

where $\alpha(n)$ is given by (1.2), and the implied constant may depend on n and ϱ.

As mentioned in [1, Remark 2.5], tighter bounds which depend on the coefficients of T^{n-1} and T^{n-2} of $f \in \mathbb{K}[T]$ can be given. It is also the case that, for dimensions n, tighter bounds can be obtained in the case $\mathbb{K} = \mathbb{R}$.

For brevity, the proofs of these claims were omitted from the original article. The purpose of this note is to provide the details omitted from those proofs.

2. Proofs From [1, Appendix B]

2.1. **Results.** We begin by restating the results from [1, Appendix B] which we prove.

It is convenient to define

$$\beta(n) = \frac{3}{4}n^2 - \frac{1}{4}n. \tag{2.1}$$

We first have [1, Theorem B.1], given below.

Theorem 2.1. *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 $n \geqslant 3$, and $\mathcal{A} \subseteq \Gamma$ of finite cardinality A, we have*

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

where $\beta(n)$ is given by (2.1) and furthermore

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

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

and

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

Reproduced below is [1, Theorem B.2], which we also prove here.

Theorem 2.2. *Suppose Γ is a rank ϱ subgroup of $\mathbb{R}^*$ and $n \geqslant 3$ 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 $2c_{n-2} = c_{n-1}^2$,*

$$\#\mathcal{P}_n(\mathcal{A}; f) \ll A^{\beta(n)} \cdot \begin{cases} A^{-2}, & n \equiv 0 \pmod 4, \\ A^{-3/2}, & n \equiv 1 \pmod 4, \end{cases}$$

  where $\beta(n)$ is given by (2.1);
- *if $c_{n-1} = c_{n-2} = 0$ and $n = 5$,*

$$\#\mathcal{P}_5(\mathcal{A}; f) \ll A^{\beta(5)-3/2}.$$

2.2. **Setup from the existing proof.** To avoid reproducing the common parts of the argument, we describe here the point of the proof of [1, Theorem 2.4] from which we continue.

The proof of [1, Theorem 2.4] proceeds by providing an upper bound on the set of matrices $X = (x_{i,j})_{i,j=1}^{n} \in \mathcal{M}_n(\mathcal{A})$ for which the coefficients c_{n-1} and c_{n-2} of the characteristic polynomial

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

are fixed.

Given that

$$c_{n-1} = -\operatorname{tr} \mathbf{X} \qquad \text{and} \qquad c_{n-2} = \frac{1}{2}((\operatorname{tr} \mathbf{X})^2 - \operatorname{tr} \mathbf{X}^2), \tag{2.2}$$

it is equivalent (up to a constant) to fix $t_1 = \operatorname{tr} X$ and $t_2 = \operatorname{tr} X^2$.

As in the proof of [1, Theorem 2.4], from the identities

$$t_1 = \sum_{i=1}^{n} x_{i,i}, \tag{2.3}$$

and

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

one obtains

$$\frac{1}{2}\left(t_2 - \sum_{i=1}^{n} x_{i,i}^2\right) = \sum_{1 \leqslant i < j \leqslant n} x_{i,j}x_{j,i}. \tag{2.4}$$

At this point the cases split depending on whether

$$t_2 = \sum_{i=1}^{n} x_{i,i}^2 \tag{2.5}$$

holds, where, in the case that it does, the number of matrices of fixed trace and traced squared is bounded by

$$\mathfrak{ABC} \ll A^{\frac{n(n-1)}{2} + \left\lfloor \frac{n(n-1)}{4} \right\rfloor} \cdot \begin{cases} A^{\left\lfloor \frac{2n}{5} \right\rfloor}, & (t_1, t_2) = (0,0), \\ A^{\left\lfloor \frac{n-1}{2} \right\rfloor}, & \text{otherwise,} \end{cases} \tag{2.6}$$

and in the case where (2.5) does not hold, it is bounded by

$$\mathfrak{ADE} \ll A^{\frac{n(n-1)}{2} + \left\lfloor \frac{n(n-1)}{4} - \frac{1}{2} \right\rfloor} \cdot \begin{cases} A^{\left\lfloor \frac{n}{2} \right\rfloor}, & t_1 = 0, \\ A^{\left\lfloor \frac{n-1}{2} \right\rfloor}, & t_1 \neq 0. \end{cases} \tag{2.7}$$

Our proofs continue with this set up in mind.

2.3. **Proof of Theorem 2.1.**

Proof. As in the proof of [1, Theorem 2.4] (Theorem 1.1 here), we split into cases depending on whether (2.5) holds, with the bounds (2.6) and (2.7) in the case it does and does not respectively.

We define the functions

$$\begin{aligned}
\delta(n) &= \left\lfloor \frac{2n}{5} \right\rfloor + \frac{n(n-1)}{2} + \left\lfloor \frac{n(n-1)}{4} \right\rfloor, \\
\theta(n) &= \left\lfloor \frac{n-1}{2} \right\rfloor + \frac{n(n-1)}{2} + \left\lfloor \frac{n(n-1)}{4} \right\rfloor, \\
\gamma(n) &= \left\lfloor \frac{n}{2} \right\rfloor + \frac{n(n-1)}{2} + \left\lfloor \frac{n(n-1)}{4} - \frac{1}{2} \right\rfloor, \\
\text{and} \quad \omega(n) &= \left\lfloor \frac{n-1}{2} \right\rfloor + \frac{n(n-1)}{2} + \left\lfloor \frac{n(n-1)}{4} - \frac{1}{2} \right\rfloor,
\end{aligned}$$

for each of the four bounds which appear in (2.6) and (2.7), such that we may rewrite (2.6) and (2.7) as

$$\mathfrak{ABC} \ll \begin{cases} A^{\delta(n)}, & t_1 = t_2 = 0, \\ A^{\theta(n)}, & \text{otherwise}, \end{cases} \qquad \text{and} \qquad \mathfrak{ADE} \ll \begin{cases} A^{\gamma(n)}, & t_1 = 0, \\ A^{\omega(n)}, & t_1 \neq 0, \end{cases}$$

respectively.

By considering the possible values of n over each congruence class modulo 4, it is straightforward (although tedious) to show that

$$\theta(n) = \frac{3}{4}n^2 - \frac{1}{4}n - \begin{cases} 1, & n \equiv 0,3 \pmod 4, \\ 1/2, & n \equiv 1 \pmod 4, \\ 3/2, & n \equiv 2 \pmod 4, \end{cases} \tag{2.8}$$

and

$$\gamma(n) = \frac{3}{4}n^2 - \frac{1}{4}n - \begin{cases} 1, & n \equiv 0,3 \pmod 4, \\ 3/2, & n \equiv 1 \pmod 4, \\ 1/2, & n \equiv 2 \pmod 4, \end{cases} \tag{2.9}$$

Likewise, considering congruence classes modulo 20 it also follows that

$$\delta(n) = \frac{15n^2 - 7n}{20} - \frac{1}{10} \begin{cases} 0, & n \equiv 0,5 \pmod{20}, \\ 2, & n \equiv 8,13 \pmod{20}, \\ 4, & n \equiv 1,16 \pmod{20}, \\ 5, & n \equiv 10,15 \pmod{20}, \\ 6, & n \equiv 4,9 \pmod{20}, \\ 7, & n \equiv 3,18 \pmod{20}, \\ 8, & n \equiv 12,17 \pmod{20}, \\ 9, & n \equiv 6,11 \pmod{20}, \\ 11, & n \equiv 14,19 \pmod{20}, \\ 13, & n \equiv 2,7 \pmod{20}, \end{cases} \tag{2.10}$$

Firstly, consider that when $t_1 = t_2 = 0$, we have

$$\mathcal{P}_n(\mathcal{A}; f) \ll \max\left\{A^{\delta(n)}, A^{\gamma(n)}\right\}.$$

Careful consideration of each congruence class modulo 20 for the expressions in (2.10) and (2.9), we can see that $\delta(n) \leqslant \gamma(n)$ for all $n \geqslant 3$ except for $n = 5$. Hence we have overall that for $t_1 = t_2 = 0$,

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

where

$$\phi(n) = \begin{cases} 17, & n = 5, \\ 3n^2/4 - n/4 - 1, & n \equiv 0, 3 \pmod 4, \\ 3n^2/4 - n/4 - 3/2, & n \neq 5, n \equiv 1 \pmod 4, \\ 3n^2/4 - n/4 - 1/2, & n \equiv 2 \pmod 4, \end{cases}$$

which is equivalent to

$$\begin{aligned} \phi(n) &= \frac{3}{4}n^2 - \frac{1}{4}n - \begin{cases} 1, & n \equiv 0, 3 \pmod 4, \\ 3/2, & n \equiv 1 \pmod 4 \text{ and } n \neq 5, \\ 1/2, & n \equiv 2 \pmod 4 \text{ or } n = 5, \end{cases} \\ &= \beta(n) + \lambda(n) \end{aligned}$$

after extracting a common main term.

When $t_1 = 0$ and $t_2 \neq 0$, we have

$$\mathcal{P}_n(\mathcal{A}; f) \ll \max\left\{A^{\theta(n)}, A^{\gamma(n)}\right\},$$

and by comparing (2.8) against (2.9) we deduce that under these conditions,

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

where

$$\begin{aligned} \psi(n) &= \frac{3}{4}n^2 - \frac{1}{4}n - \begin{cases} 1, & n \equiv 0, 3 \pmod 4, \\ 1/2, & n \equiv 1, 2 \pmod 4. \end{cases} \\ &= \beta(n) - \mu(n). \end{aligned}$$

Finally, when $t_1 \neq 0$, we have

$$\mathcal{P}_n(\mathcal{A}; f) \ll \max\left\{A^{\theta(n)}, A^{\omega(n)}\right\} = A^{\theta(n)},$$

since $\theta(n) \leqslant \omega(n)$, and by (2.8) $\theta(n) = \beta(n) - \nu(n)$.

From the relationship (2.2) between the coefficients of the characteristic polynomial of $\mathbf{X}$ and $\operatorname{tr}\mathbf{X}$ and $\operatorname{tr}\mathbf{X}^2$, we note that $t_1 = 0$ if and only if $c_{n-1} = 0$ and $t_2 = 0$ if and only if $2c_{n-2} = c_{n-1}^2$. Putting this all together concludes the proof. □

2.4. **Proof of Theorem 2.2.**

Proof. We continue from (2.4) in the proof of Theorem 1.1 under the assumption that $t_2 = 0$, or equivalently that $2c_{n-2} = c_{n-1}^2$. As in that proof, we have at most

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

possibilites for the elements $x_{i,j}$ for $1 \leqslant i < j \leqslant n$.

Then, solving for the elements on the main diagonal from (2.3), we see that there are at most

$$\mathfrak{F} \ll \begin{cases} A^{\lfloor \frac{n}{2} \rfloor}, & t_1 = 0, \\ A^{\lfloor \frac{n-1}{2} \rfloor}, & t_1 \neq 0, \end{cases}$$

solutions by [1, Lemma 3.2] and [1, Lemma 3.3] respectively.

As we assumed that $t_2 = 0$, we can solve (2.4) for the remainder of the elements of the matrix in

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

ways.

This leads to the overall bound of

$$\#\mathcal{P}_n(\mathcal{A}; f) = \mathfrak{A}\mathfrak{F}\mathfrak{G} \ll \begin{cases} A^{\lfloor \frac{n}{2} \rfloor + \frac{n(n-1)}{2} + \lfloor \frac{n(n-1)}{4} - \frac{1}{2} \rfloor}, & t_1 = 0, \\ A^{\lfloor \frac{n-1}{2} \rfloor + \frac{n(n-1)}{2} + \lfloor \frac{n(n-1)}{4} - \frac{1}{2} \rfloor}, & t_1 \neq 0. \end{cases}$$

Simplification of this bound in the cases of interest, that is $n \equiv 0, 1 \pmod 4$ when $t_1 \neq 0$ and just $n = 5$ when $t_1 = 0$, leads to the claimed result. □

References

[1] A. Manning, A. Ostafe, and I. E. Shparlinski, 'Counting matrices over finite rank multiplicative groups', *Pacific J. Math.*, **340**(1) (2026), 115-138.