ISSN 0001-4346, Mathematical Notes, 2021, Vol. 109, No. 6, pp. 843–848. © Pleiades Publishing, Ltd., 2021.
Russian Text © The Author(s), 2021, published in Matematicheskie Zametki, 2021, Vol. 109, No. 6, pp. 803–809.

On the Growth of the Number of Determinants with Restricted Entries

L. M. Arutyunyan[1,2*]

[1] *Lomonosov Moscow State University, Moscow, 119991 Russia*

[2] *Moscow Center of Fundamental and Applied Mathematics, Moscow, 119991 Russia*

Received January 20, 2018; in final form, January 26, 2021; accepted February 2, 2021

Abstract—We study the problem about the number of distinct determinants of matrices with entries from a fixed set.

DOI: 10.1134/S0001434621050175

Keywords: *sum-product phenomenon, determinants*.

1. INTRODUCTION AND MAIN RESULTS

The problem we consider is a particular case of the following question, which is quite typical in additive combinatorics. One considers a function of several variables and explores how big is the image of the function as the arguments run along a finite set A; see [1], [2].

We consider the following formulation of this problem. Let A be a finite subset of a field $\mathbb{F}$, and let $D_n(A)$ be the set of all determinants of matrices with entries in A, namely,

$$D_n(A) = \{D \in \mathbb{F} \mid \exists\, a_{ij} \in A,\ 1 \le i,j \le n,\ \det((a_{ij})) = D\},$$

where the symbol (a_{ij}) denotes the matrix with elements a_{ij}. How big is the set $D_n(A)$ compared to the set A?

Some related problems were considered in [3]–[5], in particular, the problem of the distribution of determinants. A continuous counterpart of the problem under examination was presented in [6]. The quantities $|D_n(A)|$ for $n = 3, 4$ were studied in [7]. For example, it was proved that the condition $|A| > \sqrt{q}$ implies $|D_3(A)| > q/2$, and $D_4(A) = \mathbb{F}_q$ (here q is a prime power and $\mathbb{F}_q$ is the field of order q). Some other related questions were also studied there. The set $D_2(A) = AA - AA$ has also attracted great attention in recent years (see [2], [8], and references therein).

It was proved in [3] that, for a set A which is a subset of the field $\mathbb{F} = \mathbb{F}_p$, i.e., a field whose cardinality is equal to a prime p, under certain restrictions on the cardinality of A, there exists a $c > 0$ for which

$$|D_n(A)| \ge (\log|A|)^{-c}|A|^{3+1/45-137/(45\times 2^{n/2})}.$$

There are also some other related results in the mentioned paper.

We will prove that, for $\mathbb{F} = \mathbb{F}_p$, where p is a prime, and an arbitrary subset A, the value of the power grows without bound as the size of matrices tends to infinity; more precisely,

$$|D_n(A)| \ge \frac{1}{8}\min(|A|^{c\log n}, p),$$

where $c > 0$ is an effective universal constant. In particular, the constant $c = 1/10$ is suitable; see Corollary 3.

The theorem remains true for an arbitrary field of characteristic zero (of course, one can consider p on the right-hand side to be $+\infty$ in this case); see Remark 2. An analogous theorem is also true for an arbitrary finite field $\mathbb{F}_q$, where $q = p^r$, under a natural additional assumption.

*E-mail: Lavrentin@ya.ru

Theorem 1. *Let $A \subset \mathbb{F}_q$, $q = p^r$, be such that A is not contained in a multiplicative shift of a proper subfield. Then*

$$|D_n(A)| \geq \min(|A|^{C \log n}, q).$$

for some universal constant $C > 0$.

All mentioned results remain true for the set of permanents instead of the set of determinants; see Remark 3.

2. MAIN DEFINITIONS

For any sets A and B, natural number n, and an element of a field a_0 of a field $\mathbb{F}$, the following operations are defined:

$$A + B = \{a + b \mid a \in A,\, b \in B\}, \qquad AB = \{ab \mid a \in A,\, b \in B\},$$
$$a_0 * A = \{a_0 a,\, a \in A\},$$
$$nA = \{a_1 + a_2 + \cdots + a_n \mid a_1, \ldots, a_n \in A\}, \qquad A^n = \{a_1 a_2 \cdots a_n \mid a_1, \ldots, a_n \in A\}.$$

The symbol 0_n denotes the zero matrix of size $n \times n$.

By $\log n$ we denote the logarithm of n to base 2.

3. PROOF OF THE MAIN RESULT

First, we want to reduce our problem to the case when the set A includes the numbers 0 and 1. We need the following lemma for this purpose.

Lemma 1. *Let $|A| \geq 2$. Then $D_{2n}(A) \supset b_0 * D_n(A - A)$ for some $b_0 \in \mathbb{F} \setminus \{0\}$.*

Proof. Let M_0 be an $n \times n$ matrix with entries in A such that $\det(M_0) \neq 0$. As M_0 one can always take a matrix of the form

$$\begin{pmatrix} b & b & b & \ldots & b & b \\ a & b & a & \ldots & a & a \\ a & a & b & \ldots & a & a \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a & a & a & \ldots & b & a \\ a & a & a & \ldots & a & b \end{pmatrix},$$

where $b \in A \setminus \{0\}$ and $a \in A \setminus \{b\}$. Let now M_1 and M_2 be matrices of size $n \times n$ with entries from the set A. Then $D_{2n}(A)$ contains the determinant of the following block matrix:

$$\begin{pmatrix} M_0 & M_1 \\ M_0 & M_2 \end{pmatrix}.$$

The determinant of this matrix is equal to the determinant of the difference of the matrices M_2 and M_1 multiplied by the determinant of the matrix M_0. Indeed, it is easy to obtain a corner of zeros:

$$\det \begin{pmatrix} M_0 & M_1 \\ M_0 & M_2 \end{pmatrix} = \det \begin{pmatrix} M_0 & M_1 \\ 0_n & M_2 - M_1 \end{pmatrix} = \det(M_0) \det(M_2 - M_1).$$

Therefore, we have the inclusion $D_{2n}(A) \supset \det(M_0) * D_n(A - A)$. □

Corollary 1. *Let $|A| \geq 2$. Then there is a set A' with the properties*

$$A' = -A', \qquad A' \supset \{0, 1\}, \qquad |A'| \geq |A|,$$

and $|D_{2n}(A)| \geq |D_n(A')|$.

Proof. For A' one can take the set $(b_1)^{-1} * (A - A)$, where b_1 is an arbitrary element of the set $(A - A) \setminus \{0\}$. By the previous lemma, we have

$$D_{2n}(A) \supset b_0 * D_n(A - A) = b_0(b_1)^n * D_n(A'). \quad \square$$

Theorem 2. *Let $A = -A$, $A \supset \{0, 1\}$. Then, for any $m, n \in \mathbb{N}$,*

$$D_{m(n-1)+1}(A) \supset nA^m.$$

Proof. Before the general case of arbitrary m and n, we consider the case where $m = 3$ and $n = 2, 3, 4$ (it is enough to take a diagonal matrix for $n = 1$). We have

$$n = 2\colon \quad \det \begin{pmatrix} 0 & b_1 & b_2 & b_3 \\ a_1 & 1 & 0 & 0 \\ a_2 & 0 & 1 & 0 \\ a_3 & 0 & 0 & 1 \end{pmatrix} = -(a_1b_1 + a_2b_2 + a_3b_3).$$

Taking arbitrary elements of A for a_i and b_i, $i = 1, 2, 3$, we obtain $D_4(A) \supset 3A^2$.

Further, we have

$$n = 3\colon \quad \det \begin{pmatrix} 0 & c_1 & 0 & c_2 & 0 & c_3 & 0 \\ 0 & 1 & b_1 & 0 & 0 & 0 & 0 \\ a_1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & b_2 & 0 & 0 \\ a_2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & b_3 \\ a_3 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = a_1b_1c_1 + a_2b_2c_2 + a_3b_3c_3.$$

Substituting different $a_i, b_i, c_i \in A$ into this formula, we obtain $D_{3(2-1)+1}(A) \supset 3A^3$.

Now let us consider a matrix for $3A^4$. We have

$$\det \begin{pmatrix} 0 & d_1 & 0 & 0 & d_2 & 0 & 0 & d_3 & 0 & 0 \\ 0 & 1 & c_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & b_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & c_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & b_2 & 0 & 0 & 0 \\ a_2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & c_3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & b_3 \\ a_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = -(a_1b_1c_1d_1 + a_2b_2c_2d_2 + a_3b_3c_3d_3).$$

For mA^n one can write down the necessary matrix in the following way. Let $a = \{a_1, \dots, a_n\}$, where $a_i = (a_{i,1}, \dots, a_{i,n})$. Let us define a matrix $M(a_i)$ as

$$M(a_i) = \begin{pmatrix} 1 & a_{i,n-1} & 0 & \dots & 0 & 0 \\ 0 & 1 & a_{i,n-2} & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & a_{i,2} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Now we can define a block matrix $\mathcal{M}(a)$:

$$\mathcal{M}(a) = \left(\begin{array}{c|cccccc|c|cccccc} 0 & a_{1,n} & 0 & 0 & \dots & 0 & \dots & a_{m,n} & 0 & 0 & \dots & 0 \\ \hline 0 & & & & & & \dots & & & & & \\ 0 & & & & & & \dots & & & & & \\ \vdots & & & M(a_1) & & & \dots & & & 0_{n-1} & & \\ 0 & & & & & & \dots & & & & & \\ a_{1,1} & & & & & & \dots & & & & & \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline 0 & & & & & & \dots & & & & & \\ 0 & & & & & & \dots & & & & & \\ \vdots & & & 0_{n-1} & & & \dots & & & M(a_m) & & \\ 0 & & & & & & \dots & & & & & \\ a_{m,1} & & & & & & \dots & & & & & \end{array}\right)$$

Then

$$\det(\mathcal{M}(a)) = (-1)^{n+1} \sum_{i=1}^{m} \prod_{j=1}^{n} a_{i,j}.$$

Indeed, all nonzero elements of the matrix $\mathcal{M}(a)$ in the rows from $(i-1)(n-1)+2$ to $i(n-1)+1$ lie only in the first column and in the block with $M(a_i)$. Moreover, in the first column, we can choose only one of the m elements $a_{i,1}$. Suppose that we have chosen $a_{i_0,1}$ in the first column. Then we cannot pick an element of the last row in the block with $M(a_{i_0})$; thus, in the last column, we must pick the element $a_{i_0,2}$ Further, we cannot pick elements of the last two rows in the third column, so that we inevitably choose $a_{i_0,3}$ in that column, and so on. Finally, we pick the element $a_{i_0,n-1}$ in the second column of the block with $M(a_{i_0})$. Now, in the column with index $(i_0-1)(n-1)+1$ of the original matrix, we can pick only $a_{i_0,n}$. The product of the entries already chosen equals $\prod_{j=1}^{n} a_{i_0,j}$. Now if one removes the rows and columns with already chosen entries from the matrix, there remains an upper triangular matrix with all diagonal elements equal to 1. It is also easy to show that the sign of the permutation corresponding to the chosen entries is always the same (although, this is inessential for our considerations, because the set A is symmetric with respect to zero). Thus, picking a with all possible $a_{i,j} \in A$, we obtain $D_{m(n-1)+1}(A) \supset mA^n$. □

Remark 1. It is easy to see that the following generalization of the previous statement takes place. Under the assumptions of the previous theorem, let

$$k = m_1(n_1-1) + m_2(n_2-1) + \dots + m_j(n_j-1);$$

then

$$D_k(A) \supset m_1A^{n_1} + m_2A^{n_2} + \dots + m_jA^{n_j}.$$

Corollary 2. *For an arbitrary set A,*

$$|D_{2(m(n-1)+1)}(A)| \geq |m(A-A)^n|.$$

The main result is a consequence of the following lemma (see [9]).

Lemma 2. *For an arbitrary $A \subset \mathbb{F}_p$,*

$$|8^nA^n - 8^nA^n| \geq \frac{1}{8}\min(|A|^n, p).$$

Proof. In Sec. 5 of [9], it was proved that if $|A| \geq 5$ and $N_n = 5 \cdot 4^n/24 - 1/3$, then

$$|N_n A^n - N_n A^n| \geq \frac{3}{8} \min\left(|A|^n, \frac{p-1}{2}\right).$$

The required estimate is obvious for $|A| = 0$ and $|A| = 1$, and for $|A| \geq 2$, we have $|4A| \geq 5$ by the Cauchy–Davenport theorem, and so

$$|8^n A^n - 8^n A^n| \geq |4^n N_n A^n - 4^n A^n| \geq |N_n (4A)^n - N_n (4A)^n| \geq \frac{3}{8} \min\left(|A|^n, \frac{p-1}{2}\right),$$

which gives the desired result, because $p - 1 \geq p/3$ for $p \geq 3$, and the case $p = 2$ is trivial.

Lemma 2, together with Corollary 2, gives

$$D_{8^{n+1}}(A) \geq \frac{1}{8} \min(|A|^n, p),$$

which implies the main result. □

Corollary 3. *The following estimate holds*:

$$D_n(A) \geq \frac{1}{8} \min(|A|^{0.1 \log n}, p).$$

Proof. It is easy to see that

$$|D_n(A)| \geq \frac{1}{8} \min(|A|^{(\log n)/(\log 8) - 2}).$$

For $n \leq 2^{10}$, we have $(1/10) \log n \leq 1$, and for $n \geq 2^{10}$, we have $(\log n)/(\log 8) - 2 \geq (1/10) \log n$. □

Remark 2. The above result remains true for fields of characteristic 0, since statements like Lemma 2 remain true in this case (moreover, their proofs become easier).

Remark 3. In [3] and [10], a problem similar to ours but for permanents instead of determinants was considered. In particular, it was proved there that the number of distinct permanents of matrices with entries in a set A is at least $|A|^{2-1/6+o(1)}$, where $o(1)$ tends to zero with the growth of matrix size. It is not hard to see that the results obtained here give the same estimate as in Corollary 3 but for permanents. Indeed, in the matrices appearing in Theorem 2, the signs of all permutations which give nonzero products of elements are the same. So the permanents of these matrices can differ from their determinants only in sign.

The following result can be easily derived from Corollary 3.

Corollary 4. *Let $\delta \in (0, 1)$. Then $D_n(A) = \mathbb{F}_p$ if $|A| \geq p^\delta$, $n \geq 8e^{10/\delta}$.*

The case of a field $\mathbb{F}_q$, $q = p^r$, can be handled in a similar way by using results of [11], from which one can easily derive a generalization of Lemma 2 to the case of an arbitrary finite field. Below we give a simplified version of Lemma 18 from the cited paper.

Corollary 5. *Let $A \subset \mathbb{F}_q$, $q = p^r$, be such that A is not contained in a multiplicative shift of a proper subfield and $|A| < q^{1/4}$. Then*

$$|6^n A^{2n} - 6^n A^{2n}| \geq \min(q^{1/4}, |A|^n).$$

The proof of an analog of Lemma 2 also uses Proposition 1 from the paper cited above. Below we formulate its simplified version.

Corollary 6. *Let $A \subset \mathbb{F}_q$, $q = p^r$, be such that A is not contained in a multiplicative shift of a proper subfield. Then the following estimate is true*:

$$|16A^3 - 16A^3| \geq \min(q, |A|^2).$$

Combining the last two corollaries, one obtains the following statement.

Lemma 3. *Let $A \subset \mathbb{F}_q$, $q = p^r$, be such that A is not contained in a multiplicative shift of a proper subfield. Then the following estimate is true*:

$$|6^{9(n+2)}A^{18n} - 6^{9(n+2)}A^{18n}| \geq \min(q, |A|^n).$$

Theorem 1 can be proved similarly to Corollary 3 but with the use of Lemma 3 instead of Lemma 2.

Obviously, $|D_n(A)| \leq |A|^{n^2}$. The following example shows that the upper bound is much sharper than the trivial one for some sets. For simplicity, we consider it in a field of characteristic zero.

Example. If the estimate $|D_n(A)| \geq C(n)|A|^{n^\alpha}$ with some $C(n) > 0$ is true for every set $A \subset \mathbb{R}$, then α cannot exceed 1. Indeed, if $A = \{1, \ldots, m\}$, then, since $A^n \subset [1, \ldots, m^n]$, we have

$$D_n(A) \subset [-n!\,m^n, n!\,m^n], \qquad \text{so that} \quad |D_n(A)| \leq C'(n)m^n \leq C'(n)|A|^n.$$

ACKNOWLEDGMENTS

The author expresses thanks to I. D. Shkredov for the formulation of the problem and great support throughout the whole research. The author is also grateful to the referee, who suggested considering the fields $\mathbb{F}_{p^r}$, where $r > 1$, and for other useful remarks.

FUNDING

This work was supported by the Grant of the Government of the Russian Federation (contract no. 14. W03.31.0031).

REFERENCES

1. T. C. Tao and V. H. Vu, *Additive Combinatorics*, in *Cambridge Stud. Adv. Math.* (Cambridge Univ. Press, Cambridge, 2006), Vol. 105.
2. B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev, and I. D. Shkredov, "New results on sum-product type growth over fields," Mathematika **65** (3), 588–642 (2019); `arXiv:1702.01003` (2017).
3. 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), 405–417 (2019); `arXiv:1801.03432` (2018).
4. L. A. Vinh, "Distribution of determinant of matrices with restricted entries over finite fields," J. Comb. Number Theory **1** (3), 203–212 (2010).
5. O. Ahmadi and I. E. Shparlinski, "Distribution of matrices with restricted entries over finite fields," Indag. Math. (N. S.) **18** (3), 327–337 (2007).
6. A. Greenleaf, A. Iosevich, and M. Mourgoglou, "On volumes determined by subsets of Euclidean space," Forum Math. **27** (1), 635 (2015); `arXiv:1110.6790` (2011).
7. D. Covert, D. Hart, A. Iosevich, D. Koh, and M. Rudnev, "Generalized incidence theorems, homogeneous forms and sum-product estimates in finite fields," Eur. J. Comb. **31** (1), 306–319 (2010).
8. M. Rudnev, "On the number of incidences between planes and points in three dimensions," Combinatorica **38** (1), 219–254 (2018).
9. A. A. Glibichuk and S. V. Konyagin, "Additive properties of product sets in fields of prime order," in *CRM Proc. Lecture Notes,* Vol. 43: *Additive Combinatorics* (Amer. Math. Soc., Providence, RI, 2007), pp. 279–286.
10. L. A. Vinh, "On the permanents of matrices with restricted entries over finite fields," SIAM J. Discrete Math. **26** (3), 997–1007 (2012).
11. A. A. Glibichuk, "Sums of powers of subsets of an arbitrary finite field," Izv. Math. **75** (2), 253–285 (2011).