

PERMANENTS OF RANDOM MATRICES OVER FINITE FIELDS

ZACH HUNTER, MATTHEW KWAN, AND LISA SAUERMANN

ABSTRACT. Fix a finite field $\mathbb{F}_q$ and let $A \in \mathbb{F}_q^{n \times n}$ be a uniformly random $n \times n$ matrix over $\mathbb{F}_q$. The asymptotic distribution of the determinant $\det(A)$ is well-understood, but the asymptotic distribution of the permanent $\text{per}(A)$ is still something of a mystery. In this paper we make a first step in this direction, proving that $\text{per}(A)$ is significantly more uniform than $\det(A)$.

1. INTRODUCTION

Two important matrix parameters are the *determinant* and *permanent*: for an $n \times n$ matrix $A = (a_{i,j})$, they are defined as

$$\det(A) = \sum_{\pi \in S_n} \text{sign}(\pi) \prod_{i=1}^n a_{i,\pi(i)} \quad \text{and} \quad \text{per}(A) = \sum_{\pi \in S_n} \prod_{i=1}^n a_{i,\pi(i)}. \quad (1.1)$$

If we fix a finite field $\mathbb{F}_q$ and let $A \in \mathbb{F}_q^{n \times n}$ be a uniformly random $n \times n$ matrix over $\mathbb{F}_q$, it is easy to compute the limiting distribution of $\det(A)$ (this is essentially equivalent to computing the number of invertible matrices over $\mathbb{F}_q$, which goes all the way back to Galois [30, p. 280]).

Fact 1.1. *For a prime power q , let*

$$\alpha_q = 1 - \prod_{i=1}^{\infty} (1 - q^{-i}).$$

Then, for a uniformly random $n \times n$ matrix $A \in \mathbb{F}_q^{n \times n}$ and any $x \in \mathbb{F}_q$, we have

$$\lim_{n \rightarrow \infty} \Pr[\det(A) = x] = \begin{cases} \alpha_q & \text{if } x = 0 \\ (1 - \alpha_q)/(q - 1) & \text{otherwise.} \end{cases}$$

Notably, this limiting distribution is *not* uniform over $\mathbb{F}_q$: the determinant is significantly more likely to take the value zero than any other value. For example, when $q = 3$ we have $\alpha_q \approx 0.44$, which is significantly larger than $1/q = 1/3$. Roughly speaking, this is because the event $\{\det(A) = 0\}$ describes the rows of A being linearly dependent: if we reveal A row-by-row, and at some step we discover that a row lies in the span of the previous rows, this tells us that $\det(A) = 0$ regardless of what happens in future rows. On the other hand, if after revealing the second-last row we still haven't discovered a linear dependence relation between the rows, then it is easy to see that the conditional distribution of $\det(A)$ is uniform over $\mathbb{F}_q$.

Unlike the determinant, the permanent does not seem to have any linear-algebraic meaning (unless our field has characteristic 2, in which case the determinant and permanent are equal). It is tempting to conjecture that, if $\mathbb{F}_q$ does not have characteristic 2, then the permanent of a uniformly random matrix over $\mathbb{F}_q$ is asymptotically uniform, as follows.

Conjecture 1.2. *Fix a finite field $\mathbb{F}_q$ of odd characteristic. Then, for a uniformly random $n \times n$ matrix $A \in \mathbb{F}_q^{n \times n}$, and any $x \in \mathbb{F}_q$, we have*

$$\lim_{n \rightarrow \infty} \Pr[\text{per}(A) = x] = \frac{1}{q}.$$

Zach Hunter was supported by SNSF grant 200021-228014. Matthew Kwan was supported by ERC Starting Grant ‘‘RAND-STRUCT’’ No. 101076777. Lisa Sauer mann was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – CRC 1720 – 539309657.

This conjecture seems to have been floating around the community for a while, but we are not completely sure about its origins. Permanents of random matrices over finite fields have received quite some interest in the computer science community (see e.g. [3, 8–10, 20]), due to a phenomenon called *random self-reducibility*, but surprisingly we were not able to find any study of the asymptotic distribution of $\text{per}(A)$ in this literature. The earliest reference we could find was in the open problem session of a 2017 workshop on combinatorics at the Mathematisches Forschungsinstitut Oberwolfach [16], in which Swastik Kopparty asked for the limiting distribution of the permanent over $\mathbb{F}_3$. The $\mathbb{F}_3$ case of [Conjecture 1.2](#) also appears explicitly in a recent paper by Scheinerman [29] (backed by quite convincing computational evidence), and the general case of [Conjecture 1.2](#) appeared in a very recent paper of Ghasemi, Gross and Kopparty [11]. See also a related conjecture by Esperet [7] (motivated by questions in graph theory).

Note that, by symmetry (through rescaling any row), $\text{per}(A)$ is equally likely to take any nonzero value. Thus, in order to understand the distribution of $\text{per}(A)$ it suffices to understand $\Pr[\text{per}(A) = 0]$. More specifically, the assertion of [Conjecture 1.2](#) is equivalent to $\lim_{n \rightarrow \infty} \Pr[\text{per}(A) = 0] = 1/q$.

Although we are not able to prove [Conjecture 1.2](#), we are at least able to prove that the permanent is (asymptotically) *more* uniform than the determinant, as follows (recall that $\lim_{n \rightarrow \infty} \Pr[\det(A) = 0] = \alpha_q > 1/q$ and observe that $\alpha_q - 1/q$ has order of magnitude $1/q^2$).

Theorem 1.3. *Fix a finite field $\mathbb{F}_q$ of odd characteristic. For a uniformly random $n \times n$ matrix $A \in \mathbb{F}_q^{n \times n}$, we have*

$$\Pr[\text{per}(A) = 0] \geq \frac{1}{q} \tag{1.2}$$

for all n , and we have the **strict** inequality

$$\limsup_{n \rightarrow \infty} \Pr[\text{per}(A) = 0] < \alpha_q. \tag{1.3}$$

Moreover, for all $n \geq 3$ we have

$$\Pr[\text{per}(A) = 0] \leq \frac{1}{q} + \frac{C}{q^3} \tag{1.4}$$

for some absolute constant C .

For $n = 2$ one has $\Pr[\text{per}(A) = 0] = 1/q + \Theta(1/q^2)$, so the assumption $n \geq 3$ in (1.4) cannot be omitted.

We remark that a theorem in a similar spirit was previously proved by Budrevich and Guterman [2] (see also the simpler proof in [1], and the earlier work [5]): restated in probabilistic language, their main result was that for any finite field $\mathbb{F}_q$ of odd characteristic, and any $n \geq 3$, the zero-permanent probability is strictly less than the zero-determinant probability. However, the gap they established between these two probabilities tends to zero very rapidly as $n \rightarrow \infty$. Budrevich and Guterman were motivated by *Pólya's permanent problem* (see e.g. [25, 27, 33]), which asks to what extent it is possible to re-express the permanent of a matrix in terms of a determinant. The gap established in [2] shows that there is no bijective “converter” $f : \mathbb{F}_q^{n \times n} \rightarrow \mathbb{F}_q^{n \times n}$ such that $\text{per}(A) = \det(f(A))$ for all $A \in \mathbb{F}_q^{n \times n}$. Note that [Theorem 1.3](#) implies the stronger result that there is no such converter that works for *almost* all $A \in \mathbb{F}_q^{n \times n}$.

1.1. General distributions. It turns out that [Fact 1.1](#) is *universal*, in the sense that the distribution of the determinant of a random matrix $A \in \mathbb{F}_q^{n \times n}$ does not depend very strongly on the distribution of the entries of A . For example, it is known that for *any* non-constant distribution μ over a finite field $\mathbb{F}_p$ of prime order, if $A \in \mathbb{F}_p^{n \times n}$ is a random matrix with independent μ -distributed entries, then $\lim_{n \rightarrow \infty} \Pr[\det(A) = 0] = \alpha_p$. This seems to have been first proved in 1990 by Charlap, Rees and Robbins [4], though similar theorems with more restrictive assumptions were proved much earlier by Kozlov [18] and Kovalenko and Levitskaja [17], and a very general theorem over arbitrary finite fields (necessarily with a more technical statement) was later proved by Kahn and Komlós [15]. See also [6, 21, 23, 24, 26, 36, 37] for some more recent work on universality of various algebraic properties for random matrices over finite fields.

We can prove a theorem in the spirit of [Theorem 1.3](#) for arbitrary (non-constant) distributions over finite fields of prime order, as follows.

Theorem 1.4. *Fix a finite field $\mathbb{F}_p$ of prime order $p \geq 3$. Then, there is $\delta_p > 0$ such that the following holds. Let μ be a probability distribution over $\mathbb{F}_p$ supported on more than one value. If $A \in \mathbb{F}_p^{n \times n}$ is a random*

matrix with independent μ -distributed entries, then for every $z \in \mathbb{F}_p$ we have

$$\limsup_{n \rightarrow \infty} \Pr[\text{per}(A) = z] \leq \alpha_p - \delta_p \quad (1.5)$$

and

$$\frac{1}{p} - \frac{C}{p^3} \leq \liminf_{n \rightarrow \infty} \Pr[\text{per}(A) = z] \leq \limsup_{n \rightarrow \infty} \Pr[\text{per}(A) = z] \leq \frac{1}{p} + \frac{C}{p^3}. \quad (1.6)$$

for some absolute constant C .

Remark. For simplicity we have stated [Theorem 1.4](#) only for prime fields, but our proof approach surely can be adapted to arbitrary finite fields, under some kind of non-degeneracy assumption on the distributions of the entries. Unfortunately, our proof approach does not seem to be compatible with the weakest non-degeneracy conditions in the literature. For example, Kahn and Komlós [15] proved that as long as μ is a distribution over a finite field $\mathbb{F}_q$ that is not supported on an affine translate of a subfield of $\mathbb{F}_q$, then for a random matrix A with independent μ -distributed entries we have $\lim_{n \rightarrow \infty} \Pr[\det(A) = 0] = \alpha_q$. In this very general setting we do not even know how to prove the inequality $\limsup_{n \rightarrow \infty} \Pr[\text{per}(A) = x] \leq \alpha_q$.

Remark. In combinatorial random matrix theory, perhaps the most intensively studied class of random matrices is the class of random *sign matrices*. Letting $A \in \{-1, 1\}^{n \times n}$ be a uniformly random $n \times n$ matrix with ± 1 entries, in spectacular recent work, Tikhomirov [32] proved that $\Pr[\det(A) = 0] = (1/2 + o(1))^n$ (see also the surveys [12, 28, 34, 35]). There has been quite some interest in permanents of random sign matrices (see e.g. [13, 19, 22, 31]), but still much less is known about permanents than determinants. It seems quite plausible that $\text{per}(A)$ and $\det(A)$ have very similar behaviour, but it is worth noting that (1.6) gives one of the first ways in which the distributions of $\text{per}(A)$ and $\det(A)$ *differ*: their statistics mod p are quite different, for all primes $p \geq 3$.

1.2. Overview of the paper and proofs. It would be possible to give a unified proof of [Theorems 1.3](#) and [1.4](#), but we found it to be clearer to present the proofs separately.

In [Section 2](#) we give the short proof of [Theorem 1.3](#). We reveal the rows of our random matrix one-by-one and study the permanents of submatrices as we go, inductively showing that “nonzero permanents are at least as likely as nonzero determinants”. Then, in the final few rows we proceed slightly differently, exploiting a certain symmetry property of the permanent.

In [Section 3](#) we prove [Theorem 1.4](#). The overall strategy is the same, but we need to additionally exploit the fact that if we add a large number of independent μ -distributed random variables, the result is nearly uniform. So, if we can simultaneously keep track of the permanents of many submatrices, we can “simulate” the uniform case in the μ -distributed setting. This requires a few additional ideas.

2. PROOF FOR THE UNIFORM CASE

In this section we prove [Theorem 1.3](#). First, it is easy to see that the permanent enjoys an analogue of the minor expansion formula for the determinant, as we record below. This fact will allow us to study permanents recursively.

Fact 2.1. *For any matrix $A \in \mathbb{F}_q^{k \times k}$, we have*

$$\text{per}(A) = \sum_{i=1}^k \text{per}(A'_i) x_i,$$

where A'_i is the $(k-1) \times (k-1)$ submatrix of A obtained by deleting the last row and the i th column, and x_i is the entry of A in the last row and the i th column.

Now, the following lemma shows that nonzero permanent-minors “grow at least as well” as nonzero determinant-minors, each time we reveal an additional row (note that for a uniformly random matrix $A \in \mathbb{F}_q^{n \times n}$, when conditioning on linearly independent outcomes of the first $n-s$ rows, the probability that the next row is in their span is precisely q^{-s}).

Definition 2.2. *In the setting of [Theorem 1.3](#), for any $0 \leq s \leq n$, let $A^{\uparrow s}$ be the $(n-s) \times n$ submatrix of A obtained by deleting the last s rows. Let $\mathcal{E}(s)$ be the event that $A^{\uparrow s}$ contains a $(n-s) \times (n-s)$ submatrix with nonzero permanent.*

Lemma 2.3. *For any $s \in \{1, \dots, n\}$, and any outcome of $A^{\uparrow s}$ satisfying $\mathcal{E}(s)$, we have*

$$\Pr[\mathcal{E}(s-1) \mid A^{\uparrow s}] \geq 1 - q^{-s}.$$

Proof. Throughout this proof, we implicitly condition on the outcome of $A^{\uparrow s}$ (i.e., we treat it as a non-random object). That is to say, we only work with the randomness of the last (i.e., $(n-s+1)$ -th) row of $A^{\uparrow(s-1)}$. Denote the entries of this row by $x_1, \dots, x_n$.

Without loss of generality, we may assume that the $(n-s) \times (n-s)$ submatrix of $A^{\uparrow s}$ formed by the last $n-s$ columns has nonzero permanent. Under this assumption, we will actually only need to use the randomness of $x_1, \dots, x_s$: fix arbitrary outcomes of $x_{s+1}, \dots, x_n$, and for the rest of the proof we also implicitly condition on these outcomes.

For $i \in \{1, \dots, s\}$, write t_i for the permanent of the $(n-s+1) \times (n-s+1)$ matrix obtained from $A^{\uparrow(s-1)}$ by deleting all of the first s columns except the i th. Then (recalling that we are in a conditional probability space where the only relevant source of randomness is the entries $x_1, \dots, x_s$, and recalling [Fact 2.1](#)), note that $t_1, \dots, t_s$ are all independent, and t_i is a bijective affine-linear transformation of x_i . This means that $t_1, \dots, t_s$ are independent random variables that are uniform on $\mathbb{F}_q$. The desired result follows, noting that $\mathcal{E}(s-1)$ can only fail if $t_1 = \dots = t_s = 0$. $\square$

Iterating [Lemma 2.3](#) shows that the permanent is *at least* as uniform as the determinant, as follows.

Corollary 2.4. *For any $s \in \{1, \dots, n\}$ we have*

$$\Pr[\mathcal{E}(s-1)] \geq \prod_{i=s}^n (1 - q^{-i}),$$

and in particular

$$\Pr[\text{per}(A) = 0] = 1 - \Pr[\mathcal{E}(0)] \leq 1 - \prod_{i=1}^n (1 - q^{-i}) \leq \alpha_q.$$

Proof. We have

$$\Pr[\mathcal{E}(s-1)] \geq \prod_{i=s}^n \Pr[\mathcal{E}(i-1) \mid \mathcal{E}(i)] \geq \prod_{i=s}^n (1 - q^{-i}),$$

using [Lemma 2.3](#) and the fact that $\Pr[\mathcal{E}(n)] = 1$ (the empty matrix has permanent 1). $\square$

We will also need the following elementary lemma about 3×3 matrices.

Lemma 2.5. *Fix a finite field $\mathbb{F}_q$ of odd characteristic, and let $B \in \mathbb{F}_q^{3 \times 3}$ be a symmetric 3×3 matrix whose diagonal entries are all zero and whose off-diagonal entries are all nonzero. Then $\text{rank}(B) = 3$.*

Proof. Write $B = (b_{i,j})$, and observe that $\det(B) = 2b_{1,2}b_{1,3}b_{2,3} \neq 0$. $\square$

The last ingredient we will need is Mantel's theorem from extremal graph theory (see e.g. [\[14, Theorem 4.6\]](#)).

Theorem 2.6. *If a graph on n vertices has more than $n^2/4$ edges, then it contains a triangle.*

Now we are ready to prove [Theorem 1.3](#).

Proof of Theorem 1.3. First, the desired *lower* bound in [\(1.2\)](#) is near-trivial. Indeed, by [Fact 2.1](#), the permanent of A is a linear combination of entries of A in the last row, where the coefficients are the permanents of the $(n-1) \times (n-1)$ submatrices of $A^{\uparrow 1}$. Given an outcome of $A^{\uparrow 1}$ satisfying $\mathcal{E}(1)$, at least one of the coefficients of this linear combination is nonzero. The entries of the last row of A are independent random variables uniform in $\mathbb{F}_q$, so this linear combination is itself uniform in $\mathbb{F}_q$. Thus, we obtain (noting that we always have $\text{per}(A) = 0$ if the event $\mathcal{E}(1)$ does not hold)

$$\Pr[\text{per}(A) = 0] = (1/q) \Pr[\mathcal{E}(1)] + \Pr[\mathcal{E}(1)^c] \geq 1/q.$$

For the rest of the proof we focus on upper-bounding $\limsup_{n \rightarrow \infty} \Pr[\text{per}(A) = 0]$ to show first [\(1.3\)](#) and then [\(1.4\)](#). For this, we will use [Lemma 2.3](#), but we will treat the last two rows slightly differently. To this end, we define a symmetric matrix $H = (h_{i,j}) \in \mathbb{F}_q^{n \times n}$ that encodes the permanents of $(n-2) \times (n-2)$

submatrices in $A^{\uparrow 2}$: for $i \neq j$, let $h_{i,j}$ be the permanent of the submatrix of $A^{\uparrow 2}$ obtained by deleting columns i and j , and for each i let $h_{i,i} = 0$. Let $\vec{x} \in \mathbb{F}_q^n$ be the last row of $A^{\uparrow 1}$ (i.e., the second-last row of A). Then, via [Fact 2.1](#), it is not hard to see that the entries of $H\vec{x}$ are the permanents of the $(n-1) \times (n-1)$ submatrices in $A^{\uparrow 1}$. Thus, $\mathcal{E}(1)$ holds if and only if $H\vec{x} = \vec{0}$.

If we fix an outcome of $A^{\uparrow 2}$ such that $\text{rank}(H) \geq 3$, then, conditionally on this outcome of $A^{\uparrow 2}$, the random vector $H\vec{x}$ is uniform on some linear subspace of $\mathbb{F}_q^n$ with dimension at least 3. So,

$$\Pr[\mathcal{E}(1) \mid \text{rank}(H) \geq 3] = \Pr[H\vec{x} = \vec{0} \mid \text{rank}(H) \geq 3] \geq 1 - q^{-3}. \quad (2.1)$$

Note that [\(2.1\)](#) gives a stronger bound than the $s = 2$ case of [Lemma 2.3](#). The idea for the rest of the proof is to show that $\text{rank}(H) \geq 3$ with non-negligible probability, so we can use [\(2.1\)](#) to improve on the proof of [Corollary 2.4](#).

Consider the graph G on the vertex set $\{1, \dots, n\}$ where ij is an edge if $h_{i,j} \neq 0$. The probability that a given pair ij does not form an edge of G is at most α_q , by [Corollary 2.4](#) (applied to an $(n-2) \times (n-2)$ random matrix). A direct calculation shows that $\alpha_q < 0.45$ (using $q \geq 3$). Thus, by Markov's inequality, the probability that our graph G has at least $\binom{n}{2} - n^2/4$ non-edges is at most

$$\frac{\alpha_q \cdot \binom{n}{2}}{\binom{n}{2} - n^2/4} = 2\alpha_q + o(1) \leq 0.9$$

(assuming, as we may, that n is sufficiently large). If this does not occur, then by Mantel's theorem ([Theorem 2.6](#)) G contains a triangle. This triangle corresponds to a 3×3 principal submatrix of H whose diagonal entries are all zero and whose off-diagonal entries are all nonzero, so $\text{rank}(H) \geq 3$ by [Lemma 2.5](#). In summary, letting $\mathcal{F}$ be the event that $\text{rank}(H) \geq 3$, we have proved that

$$\Pr[\mathcal{F}] \geq 1 - 2\alpha_q - o(1) \geq 0.1.$$

Now, we have

$$\begin{aligned} \Pr[\mathcal{E}(1)] &\geq \Pr[\mathcal{E}(1) \mid \mathcal{F}] \Pr[\mathcal{F}] + \Pr[\mathcal{E}(1) \mid \mathcal{E}(2) \setminus \mathcal{F}] \Pr[\mathcal{E}(2) \setminus \mathcal{F}] \\ &\geq (1 - q^{-3}) \Pr[\mathcal{F}] + (1 - q^{-2})(\Pr[\mathcal{E}(2)] - \Pr[\mathcal{F}]) \\ &\geq (1 - q^{-2}) \Pr[\mathcal{E}(2)] + \Pr[\mathcal{F}](q^{-2} - q^{-3}) \\ &\geq \prod_{i=2}^n (1 - q^{-i}) + \frac{q^{-2}}{20}. \end{aligned}$$

In the second line we used [\(2.1\)](#) to lower-bound $\Pr[\mathcal{E}(1) \mid \mathcal{F}]$ and we used [Lemma 2.3](#) to lower-bound $\Pr[\mathcal{E}(1) \mid \mathcal{E}(2) \setminus \mathcal{F}]$. In the last line we used [Corollary 2.4](#) to lower-bound $\Pr[\mathcal{E}(2)]$.

Using [Lemma 2.3](#), it follows that

$$\Pr[\text{per}(A) \neq 0] = \Pr[\mathcal{E}(0)] \geq \Pr[\mathcal{E}(0) \mid \mathcal{E}(1)] \Pr[\mathcal{E}(1)] \geq (1 - q^{-1}) \Pr[\mathcal{E}(1)] \geq \prod_{i=1}^n (1 - q^{-i}) + \frac{q^{-2}}{50} \geq 1 - \alpha_q + \frac{q^{-2}}{50}$$

and hence $\limsup_{n \rightarrow \infty} \Pr[\text{per}(A) = 0] \leq \alpha_q - q^{-2}/50 < \alpha_q$, proving [\(1.3\)](#).

For [\(1.4\)](#) we use a similar approach. First, note that the probability that a given pair ij does not form an edge of G can also be bounded via [Corollary 2.4](#) by $1 - \prod_{i=1}^{n-2} (1 - q^{-i}) \leq \sum_{i=1}^{n-2} q^{-i} \leq 2q^{-1}$. Thus, again applying Markov's inequality as before, the probability that G has at least $\binom{n}{2} - n^2/4$ non-edges is at most

$$\frac{2q^{-1} \cdot \binom{n}{2}}{\binom{n}{2} - n^2/4} = 2q^{-1} \cdot \frac{2(n-1)}{n-2} \leq 8q^{-1},$$

recalling the assumption $n \geq 3$. Thus, we obtain $\Pr[\mathcal{F}] \geq 1 - 8q^{-1}$.

From [Corollary 2.4](#) we furthermore obtain $\Pr[\mathcal{E}(2)] \geq \prod_{i=3}^n (1 - q^{-i}) \geq 1 - \sum_{i=3}^n q^{-i} \geq 1 - 2q^{-3}$. Then, the same argument as above shows that

$$\Pr[\mathcal{E}(1)] \geq (1 - q^{-2}) \Pr[\mathcal{E}(2)] + \Pr[\mathcal{F}](q^{-2} - q^{-3}) \geq (1 - q^{-2})(1 - 2q^{-3}) + (1 - 8q^{-1})(q^{-2} - q^{-3}) \geq 1 - 11q^{-3}$$

and consequently

$$\Pr[\text{per}(A) \neq 0] \geq (1 - q^{-1}) \Pr[\mathcal{E}(1)] \geq (1 - q^{-1})(1 - 11q^{-3}) \geq 1 - q^{-1} - 11q^{-3}. \quad \square$$

Remark. Here we obtained a separation between the permanent and determinant by considering the last two rows in a special way. One can improve our bounds further by considering the last s rows in a special way, for $s > 2$. In particular, with a finite amount of casework for a given value of s , it seems that one can improve the error term $O(q^{-3})$ to $O(q^{-s-1})$. (We worked out the details of this for $s = 3$, and intend to include them in a future companion note to this paper, but the casework seems to become exponentially more complicated for larger and larger s .)

3. PROOF FOR GENERAL DISTRIBUTIONS

Now, we turn to the proof of [Theorem 1.4](#). Throughout this section, we fix a prime $p \geq 3$ and a probability distribution μ over $\mathbb{F}_p$ supported on more than one value, and we let $A \in \mathbb{F}_p^{n \times n}$ be a random matrix with independent μ -distributed entries.

To prove [Theorem 1.4](#), we need to adapt the proof of [Theorem 1.3](#) to consider *many* submatrices with nonzero permanent, simultaneously. We will consider submatrices satisfying a certain “complement-disjointness” property, as follows.

Definition 3.1. For any $0 \leq s \leq n$, let $A^{\uparrow s}$ be the submatrix of A obtained by deleting the last s rows. For a set $I \subseteq \{1, \dots, n\}$ of size s , let $\text{per}(A; I)$ be the permanent of the $(n-s) \times (n-s)$ submatrix of $A^{\uparrow s}$ obtained by deleting the columns indexed by I . For a positive integer ℓ , let $\mathcal{E}(s, \ell)$ be the event that there are ℓ disjoint sets $I_1, \dots, I_\ell$, each of size s , such that $\text{per}(A; I_i) \neq 0$ for each $i = 1, \dots, \ell$.

In the proof of [Theorem 1.3](#) (specifically, in [Lemma 2.3](#)), we conditioned on an outcome of $A^{\uparrow s}$ which has a submatrix with nonzero permanent, and studied the probability that $A^{\uparrow(s-1)}$ has a larger submatrix with nonzero permanent. [Lemma 2.3](#) was stated only for random matrices with uniform entries; it would be possible to consider general entry distributions, but this would change the probability bound. The following lemma considers a similar situation where we condition on $A^{\uparrow s}$ having *many* submatrices with nonzero permanent, and we would like $A^{\uparrow(s-1)}$ to have *many* larger submatrices with nonzero permanent. Unfortunately, the two meanings of “many” here are rather different from each other, but in this more “robust” situation we are able to obtain probability bounds which are essentially independent of the entry distribution (i.e., we obtain approximately the same $1 - p^{-s}$ bound as in [Lemma 2.3](#), regardless of the entry distribution).

Lemma 3.2. For any $s, \ell \in \mathbb{N}$ and $\varepsilon > 0$, there is $L = L_\mu(s, \ell, \varepsilon) \in \mathbb{N}$ such that the following holds for sufficiently large n . For any outcome of $A^{\uparrow s}$ satisfying $\mathcal{E}(s, L)$, we have

$$\Pr[\mathcal{E}(s-1, \ell) \mid A^{\uparrow s}] \geq 1 - p^{-s} - \varepsilon.$$

We defer the proof of [Lemma 3.2](#) to [Section 3.2](#). It is proved using an anticoncentration inequality for “robustly high-rank” linear maps (which is stated as [Lemma 3.6](#) later in this section, and may be of more general interest).

We would like to use [Lemma 3.2](#) recursively, to deduce a version of [Corollary 2.4](#) for general distributions. Unfortunately, we can only iterate [Lemma 3.2](#) a very small number of times, as each iteration requires more and more submatrices with nonzero permanent¹. So, we also need the following lemma, which serves as a starting point for applying [Lemma 3.2](#).

Lemma 3.3. For any $\varepsilon > 0$, there is $S = S_\mu(\varepsilon) \in \mathbb{N}$ such that

$$\Pr[\mathcal{E}(S, \lceil n^{0.99} \rceil)] \geq 1 - \varepsilon$$

for n sufficiently large (in terms of ε and μ).

We defer the proof of [Lemma 3.3](#) to [Section 3.1](#). The proof is a straightforward adaptation of ideas of Tao and Vu [\[31\]](#).

We can now prove a version of [Corollary 2.4](#) for general distributions.

¹We wrote [Lemma 3.2](#) in a non-quantitative way, so as written it can only be applied $O(1)$ times. With more care, it may be possible to apply it about $\log n$ times, but additional ideas are certainly required.

Corollary 3.4. *For any $s, \ell \in \mathbb{N}$ and $\varepsilon > 0$, if n is sufficiently large in terms of s, ℓ, ε and μ , then*

$$\Pr[\mathcal{E}(s-1, \ell)] \geq \prod_{i=s}^{\infty} (1 - p^{-i}) - \varepsilon,$$

and in particular

$$\Pr[\text{per}(A) = 0] = 1 - \Pr[\mathcal{E}(0, 1)] \leq \alpha_p + \varepsilon.$$

Proof. We use the quantities $S_\mu(\cdot)$ and $L_\mu(\cdot, \cdot, \cdot)$ in the statements of [Lemmas 3.2](#) and [3.3](#).

Let $S = S_\mu(\varepsilon/2)$. Let $\ell_{s-1} = \ell$ and for $i \in \{s, \dots, S\}$ let $\ell_i = L_\mu(i, \ell_{i-1}, \varepsilon/(2S))$. Then, by [Lemma 3.3](#) we have $\Pr[\mathcal{E}(S, \ell_S)] \geq \Pr[\mathcal{E}(S, \lceil n^{0.99} \rceil)] \geq 1 - \varepsilon/2$ for sufficiently large n , and hence

$$\Pr[\mathcal{E}(s-1, \ell)] \geq \Pr[\mathcal{E}(S, \ell_S)] \prod_{i=s}^S \Pr[\mathcal{E}(i-1, \ell_{i-1}) \mid \mathcal{E}(i, \ell_i)] \geq \left(1 - \frac{\varepsilon}{2}\right) \prod_{i=s}^S \left(1 - p^{-i} - \frac{\varepsilon}{2S}\right) \geq \prod_{i=s}^{\infty} (1 - p^{-i}) - \varepsilon,$$

using [Lemma 3.2](#). $\square$

Now, just as in the proof of [Theorem 1.3](#), we need to improve [Corollary 3.4](#) by some special considerations for the last two rows. In order to apply the same proof strategy, we need the following anticoncentration inequality for “robustly high rank” linear maps, which may be of general interest. To state this lemma we need a bit more notation.

Definition 3.5. *For a matrix $M \in \mathbb{F}^{m \times n}$ over a field $\mathbb{F}$, a set of rows $I \subseteq \{1, \dots, m\}$ and a set of columns $J \subseteq \{1, \dots, n\}$, let $M[I \times J]$ be the $|I| \times |J|$ submatrix obtained by deleting all rows not indexed by I and deleting all columns not indexed by J .*

Lemma 3.6. *For any $r \in \mathbb{N}$ and $\varepsilon > 0$, there is $K = K_\mu(r, \varepsilon) \in \mathbb{N}$ such that the following holds. Consider a matrix $M \in \mathbb{F}_p^{m \times n}$ and disjoint subsets $I_1, \dots, I_K \subseteq \{1, \dots, n\}$ with $\text{rank } M[\{1, \dots, m\} \times I_i] \geq r$ for each $i = 1, \dots, K$. Let $\vec{x} \in \mathbb{F}_p^n$ be a random vector with independent μ -distributed entries. Then*

$$\Pr[M\vec{x} = \vec{0}] \leq \frac{1}{p^r} + \varepsilon.$$

We defer the proof of [Lemma 3.6](#) to [Section 3.2](#). It is proved via a case distinction: either M has high rank, in which case we can easily obtain good anticoncentration bounds for $M\vec{x}$ (see [Lemma 3.10](#)), or we can approximate $M\vec{x}$ in terms of r independent random variables that are uniform over $\mathbb{F}_p$.

The second case in the proof of [Lemma 3.6](#) requires the following lemma (which we will also need for our deduction of [Theorem 1.4](#)): sums of many independent random variables are approximately uniform. Let us say that a random variable $X \in \mathbb{F}_p$ is ε -almost-uniform if $|\Pr[X = z] - 1/p| \leq \varepsilon$ for all $z \in \mathbb{F}_p$.

Lemma 3.7. *For any $\varepsilon > 0$, there is $Q = Q_\mu(\varepsilon) \in \mathbb{N}$ such that the following holds. Consider $\vec{h} \in \mathbb{F}_p^n$, such that least Q entries of $\vec{h}$ are nonzero, and consider a random vector $\vec{x} \in \mathbb{F}_p^n$ with independent μ -distributed entries. Then $\vec{h} \cdot \vec{x}$ is ε -almost-uniform.*

Proof. Let Q be very large in terms of ε and μ , and let $k = \lfloor Q/(p-1) \rfloor$. Without loss of generality we can assume that the first k entries $h_1, \dots, h_k$ of $\vec{h}$ are equal to the same nonzero value $h \in \mathbb{F}_p$. Writing $\vec{x} = (x_1, \dots, x_n)$, the sequence of partial sums

$$x_1, x_1 + x_2, \dots, x_1 + \dots + x_k$$

can be interpreted as a Markov chain, and some straightforward analysis (see e.g. [\[15, Lemma 5.1\]](#) and the remark thereafter) shows that $x_1 + \dots + x_k$ is ε -almost-uniform, provided k is sufficiently large in terms of ε and μ . Now, conditioning on any fixed outcomes for $x_{k+1}, \dots, x_n$, for any $z \in \mathbb{F}_p$, we have

$$\Pr[\vec{h} \cdot \vec{x} = z \mid x_{k+1}, \dots, x_n] = \Pr[x_1 + \dots + x_k = h^{-1}(z - h_{k+1}x_{k+1} - \dots - h_n x_n) \mid x_{k+1}, \dots, x_n] \in \left[\frac{1}{p} - \varepsilon, \frac{1}{p} + \varepsilon \right].$$

Finally, averaging over all outcomes of $x_{k+1}, \dots, x_n$ yields $\Pr[\vec{h} \cdot \vec{x} = z] \in [1/p - \varepsilon, 1/p + \varepsilon]$ for all $z \in \mathbb{F}_p$, as desired. $\square$

In the proof of [Theorem 1.4](#), we cannot apply [Lemma 3.6](#) directly. Instead, we need the following corollary.

Corollary 3.8. *For any $r, \ell \in \mathbb{N}$ and $\varepsilon > 0$, there is $D = D_\mu(r, \ell, \varepsilon) \in \mathbb{N}$ such that the following holds. Consider a matrix $M \in \mathbb{F}_p^{n \times n}$ and disjoint subsets $I_1, \dots, I_D \subseteq \{1, \dots, n\}$ of size r with $\text{rank } M[I_i \times I_i] = r$ for each $i = 1, \dots, D$. Let $\vec{x} \in \mathbb{F}_p^n$ be a random vector with independent μ -distributed entries. Then*

$$\Pr[M\vec{x} \text{ has at most } \ell \text{ nonzero entries}] \leq \frac{2}{p^r} + \varepsilon.$$

Proof. Let $K = K_\mu(r, \varepsilon/2)$, where $K_\mu(\cdot, \cdot)$ is as in Lemma 3.6, and let $D = 2\ell K$. Consider a matrix $M \in \mathbb{F}_p^{n \times n}$ and subsets $I_1, \dots, I_D \subseteq \{1, \dots, n\}$ as in the assumptions of the corollary. Now, for $j = 1, \dots, 2\ell$, let $M_j = M[(I_{(j-1)K+1} \cup \dots \cup I_{jK}) \times \{1, \dots, n\}]$ be the $(rK) \times n$ submatrix of M consisting of the rows with indices in $I_{(j-1)K+1} \cup \dots \cup I_{jK}$. Since $\text{rank } M_j[I_{(j-1)K+i} \times I_{(j-1)K+i}] = \text{rank } M[I_{(j-1)K+i} \times I_{(j-1)K+i}] = r$ for all $i = 1, \dots, K$, the matrix M_j together with the sets $I_{(j-1)K+1}, \dots, I_{jK}$ satisfies the assumption of Lemma 3.6. Hence we obtain $\Pr[M_j\vec{x} = \vec{0}] \leq p^{-r} + \varepsilon/2$ for all $j = 1, \dots, 2\ell$.

Now, if $M\vec{x}$ has at most ℓ nonzero entries, then we must have $M_j\vec{x} = \vec{0}$ for at least $2\ell - \ell = \ell$ indices $j \in \{1, \dots, 2\ell\}$. Since the expected number of indices $j \in \{1, \dots, 2\ell\}$ with $M_j\vec{x} = \vec{0}$ is at most $(p^{-r} + \varepsilon/2) \cdot 2\ell = (2p^{-r} + \varepsilon)\ell$, by Markov's inequality we can conclude

$$\Pr[M\vec{x} \text{ has at most } \ell \text{ nonzero entries}] \leq \Pr[M_j\vec{x} = \vec{0} \text{ for at least } \ell \text{ different } j] \leq \frac{(2p^{-r} + \varepsilon)\ell}{\ell} = \frac{2}{p^r} + \varepsilon. \quad \square$$

We now show how to deduce Theorem 1.4 from Lemmas 3.2 and 3.7 and Corollaries 3.4 and 3.8. The structure of the proof is very similar to the proof of Theorem 1.3, though the notation is a bit more complicated and we need to replace certain trivial estimates with the more sophisticated lemmas collected in this section so far.

Proof of Theorem 1.4. Consider any $\varepsilon > 0$ and any $\ell \in \mathbb{N}$. We will prove that for n sufficiently large in terms of ε , ℓ and μ , we have

$$\Pr[\mathcal{E}(1, \ell)] \geq \prod_{i=2}^n (1 - p^{-i}) + (1 - 2\alpha_p)(p^{-2} - 2p^{-3}) - \varepsilon. \quad (3.1)$$

To see that this suffices, consider $\ell = Q_\mu(\varepsilon)$ (where $Q_\mu(\cdot)$ is as in Lemma 3.7). Conditioning on an outcome of $A^{\uparrow 1}$ such that $\mathcal{E}(1, \ell)$ holds, by Fact 2.1 the permanent $\text{per}(A)$ can be interpreted as a linear combination of the entries in the last row of A , where at least ℓ coefficients are nonzero. Therefore, Lemma 3.7 yields

$$\Pr[\text{per}(A) \neq z] \geq \Pr[\text{per}(A) \neq z \mid \mathcal{E}(1, \ell)] \cdot \Pr[\mathcal{E}(1, \ell)] \geq \left(1 - \frac{1}{p} - \varepsilon\right) \Pr[\mathcal{E}(1, \ell)] \geq (1 - p^{-1}) \Pr[\mathcal{E}(1, \ell)] - \varepsilon$$

and, together with (3.1), for sufficiently large n we obtain

$$\Pr[\text{per}(A) \neq z] \geq (1 - p^{-1}) \prod_{i=2}^n (1 - p^{-i}) + (1 - p^{-1})(1 - 2\alpha_p)(p^{-2} - 2p^{-3}) - 2\varepsilon \geq 1 - \alpha_p + (1 - 2\alpha_p)p^{-2}/5 - 2\varepsilon.$$

Taking $\varepsilon = (1 - 2\alpha_p)p^{-2}/20$, this implies (1.5) (with $\delta_p = (1 - 2\alpha_p)p^{-2}/10$). Furthermore, taking $\varepsilon = p^{-3}$, Lemma 3.7 yields

$$\left| \Pr[\text{per}(A) = z] - \frac{1}{p} \right| \leq \left| \Pr[\text{per}(A) = z \mid \mathcal{E}(1, \ell)] - \frac{1}{p} \right| + \Pr[\mathcal{E}(1, \ell)^c] \leq \varepsilon + \Pr[\mathcal{E}(1, \ell)^c] = \Pr[\mathcal{E}(1, \ell)^c] + p^{-3}$$

for any $z \in \mathbb{F}_p$. Using (3.1) we can compute (again for sufficiently large n)

$$\begin{aligned} \Pr[\mathcal{E}(1, \ell)^c] &= 1 - \Pr[\mathcal{E}(1, \ell)] \leq 1 - \prod_{i=2}^n (1 - p^{-i}) - (1 - 2\alpha_p)(p^{-2} - 2p^{-3}) + \varepsilon \\ &\leq \sum_{i=2}^n p^{-i} - (p^{-2} - 2p^{-3}) + 2\alpha_p p^{-2} + 2p^{-3} \\ &\leq 2p^{-3} + 2p^{-3} + 2\alpha_p p^{-2} + 2p^{-3} \leq 10p^{-3}, \end{aligned}$$

using that $\alpha_p = 1 - \prod_{i=1}^{\infty} (1 - p^{-i}) \leq \sum_{i=1}^{\infty} p^{-i} \leq 2p^{-1}$. Thus, we obtain

$$\left| \Pr[\text{per}(A) = z] - \frac{1}{p} \right| \leq 10p^{-3} + p^{-3} = 11p^{-3}$$

for any $z \in \mathbb{F}_p$, proving (1.6) with $C = 11$.

So, we just need to prove (3.1). Define the matrix $H \in \mathbb{F}_p^{n \times n}$ and the graph G as in the proof of Theorem 1.3 (encoding the permanents of $(n-2) \times (n-2)$ submatrices in $A^{\uparrow 2}$). Let $D_\mu(\cdot, \cdot, \cdot)$ be as in Corollary 3.8, and let $D = D_\mu(3, \ell, \varepsilon/4)$. By Markov's inequality and Corollary 3.4, the probability that our graph G has at least $\binom{n}{2} - n^2/4 - 3Dn$ non-edges is at most $2\alpha_p + o(1)$. If this occurs, then we can repeatedly apply Mantel's theorem (Theorem 2.6) to find D vertex-disjoint triangles. (After each time we apply Mantel's theorem to find a triangle, we delete all edges incident to the vertices of that triangle before the next application of Mantel's theorem.)

Just as in the proof of Theorem 1.3, via Lemma 2.5, a triangle in G yields a size-3 set $I \subseteq \{1, \dots, n\}$ such that $\text{rank}(H[I \times I]) = 3$. Write $\mathcal{F}^*$ for the event that there are D disjoint size-3 sets $I_1, \dots, I_D \subseteq \{1, \dots, n\}$ such that $\text{rank}(H[I_i \times I_i]) = 3$ for each $i = 1, \dots, D$; we have just proved that

$$\Pr[\mathcal{F}^*] \geq 1 - 2\alpha_p + o(1).$$

For any outcome of $A^{\uparrow 2}$ such that $\mathcal{F}^*$ holds, we can apply Corollary 3.8 to the matrix $H \in \mathbb{F}_p^{n \times n}$ and find that with probability at least $1 - 2p^{-3} - \varepsilon/4$ the vector $H\vec{x}$ has at least ℓ nonzero entries, where $\vec{x} \in \mathbb{F}_p^n$ denotes the random vector consisting of the entries in the second-last row of A . Now, the entries of $H\vec{x}$ are precisely the permanents of the $(n-1) \times (n-1)$ submatrices of $A^{\uparrow 1}$, and having at least ℓ such nonzero entries means that the event $\mathcal{E}(1, \ell)$ holds. Thus, we obtain

$$\Pr[\mathcal{E}(1, \ell) \mid \mathcal{F}^*] \geq 1 - 2p^{-3} - \varepsilon/4.$$

Now, let $L_\mu(\cdot, \cdot, \cdot)$ be as in Lemma 3.2 and write $\mathcal{E}^*(2) = \mathcal{E}(2, L_\mu(2, \ell, \varepsilon/4))$. Then by Corollary 3.4 we have

$$\Pr[\mathcal{E}^*(2)] \geq \prod_{i=3}^{\infty} (1 - p^{-i}) - \varepsilon/4$$

if n is sufficiently large.

Combining everything, and applying Lemma 3.2, we can conclude

$$\begin{aligned} \Pr[\mathcal{E}(1, \ell)] &\geq \Pr[\mathcal{E}(1, \ell) \mid \mathcal{F}^*] \Pr[\mathcal{F}^*] + \Pr[\mathcal{E}(1, \ell) \mid \mathcal{E}^*(2) \setminus \mathcal{F}^*] \Pr[\mathcal{E}^*(2) \setminus \mathcal{F}^*] \\ &\geq (1 - 2p^{-3} - \varepsilon/4) \Pr[\mathcal{F}^*] + (1 - p^{-2} - \varepsilon/4) \Pr[\mathcal{E}^*(2) \setminus \mathcal{F}^*] \\ &\geq (1 - 2p^{-3}) \Pr[\mathcal{F}^*] + (1 - p^{-2}) \Pr[\mathcal{E}^*(2) \setminus \mathcal{F}^*] - \varepsilon/2 \\ &\geq (1 - 2p^{-3}) \Pr[\mathcal{F}^*] + (1 - p^{-2}) \left(\prod_{i=3}^{\infty} (1 - p^{-i}) - \varepsilon/4 - \Pr[\mathcal{F}^*] \right) - \varepsilon/2 \\ &\geq \prod_{i=2}^{\infty} (1 - p^{-i}) + (p^{-2} - 2p^{-3}) \Pr[\mathcal{F}^*] - 3\varepsilon/4 \\ &\geq \prod_{i=2}^{\infty} (1 - p^{-i}) + (p^{-2} - 2p^{-3})(1 - 2\alpha_p + o(1)) - 3\varepsilon/4, \end{aligned}$$

and (3.1) follows for sufficiently large n . □

3.1. Growing many matrices with nonzero permanents. In this section we prove Lemma 3.3, adapting a strategy of Tao and Vu [31]. Recall the definitions in Definition 3.1. First, the following lemma is suitable to find a *single* submatrix with nonzero permanent.

Lemma 3.9. *For any $\varepsilon > 0$, there is $T = T_\mu(\varepsilon) \in \mathbb{N}$ such that the following holds. Consider any subset $J \subseteq \{1, \dots, n\}$ of size $|J| = 2T$. Then,*

$$\Pr[\text{there is a subset } I \subseteq J \text{ of size } |I| = T \text{ with } \text{per}(A; I) \neq 0] \geq 1 - \varepsilon.$$

Proof. Let $\rho = \max_{z \in \mathbb{F}_p} \mu(z) < 1$ (recalling that μ is supported on at least two values), and choose $0 < \delta < 1$ small enough such that $1 - \rho(1 + \delta) > \delta$. Furthermore choose $T > 2(1 + \delta)/(\varepsilon\delta^2)$ to be sufficiently large such that $\rho^{\delta T}/(1 - \rho) < \varepsilon/4$.

We consider a random process that attempts to construct a nested sequence of sets $I_0 \supseteq \dots \supseteq I_{n-T}$ (starting with $I_0 = \{1, \dots, n\}$, and removing an element at each step), in such a way that $\text{per}(A; I_t) \neq 0$ for all $t = 0, \dots, n - T$, and $I_{n-T} \subseteq J$. If this process succeeds, then we can take I_{n-T} as the desired set I .

Specifically, the process is defined as follows. Let $T' = 2T + \lfloor \delta T \rfloor$. For each step $t = 1, \dots, n - T'$, we define I_t as follows:

- If there is $i \in I_{t-1} \setminus J$ such that $\text{per}(A; I_{t-1} \setminus \{i\}) \neq 0$, take the minimum such i and set $I_t = I_{t-1} \setminus \{i\}$.
- Otherwise, terminate the process.

For each step $t = n - T' + 1, \dots, n - T$, we define I_t as follows:

- If there is $i \in I_{t-1} \setminus J$ such that $\text{per}(A; I_{t-1} \setminus \{i\}) \neq 0$, take the minimum such i and set $I_t = I_{t-1} \setminus \{i\}$.
- Otherwise, if there is any $i \in I_{t-1}$ such that $\text{per}(A; I_{t-1} \setminus \{i\}) \neq 0$, take the minimum such i and set $I_t = I_{t-1} \setminus \{i\}$.
- Otherwise, terminate the process.

That is to say: in each of the first $n - T'$ steps we make sure to remove an element outside J . In each of the subsequent steps we still try to remove an element outside J if possible, but if not we allow ourselves to remove some other element. Note that we always have $|I_t| = n - t$ and $\text{per}(A; I_t) \neq 0$ whenever the set I_t is defined, and also note that I_t only depends on the outcome of $A^{\uparrow(n-t)}$ (i.e., only on the first t rows of the matrix A).

It suffices to show that with probability at least $1 - \varepsilon/2$ this process does not terminate in any step before defining I_{n-T} , and to show that² $I_{n-T} \not\subseteq J$ with probability at most $\varepsilon/2$.

First, note that for any outcome of $A^{\uparrow(n-t)}$ for which $\text{per}(A; I_t) \neq 0$, we have

$$\Pr[\text{the process terminates at step } t + 1 \mid A^{\uparrow(n-t)}] \leq \begin{cases} \rho^{|I_t \setminus J|} \leq \rho^{n-t-2T} & \text{if } t < n - T' \\ \rho^{|I_t|} = \rho^{n-t} & \text{if } n - T' \leq t < n - T \end{cases}$$

The reasoning is basically the same as in the proof of [Lemma 2.3](#). Indeed, write $A = (a_{i,j})$, condition on an outcome of $A^{\uparrow(n-t)}$, and additionally condition on $a_{t+1,i}$ for all $i \notin I_t$. Then, the quantities $\text{per}(A; I_t \setminus \{i\})$, for $i \in I_t$, become independent random variables (each only depending on the outcome of $a_{t+1,i}$), which each have probability at most ρ of taking any particular value (in particular, of taking the value zero).

By a union bound, it follows that the probability that the process terminates in some step (i.e., the probability that I_{n-T} does not get defined) is at most

$$\sum_{t=0}^{n-T'-1} \rho^{n-t-2T} + \sum_{t=n-T'}^{n-T-1} \rho^{n-t} = \sum_{j=T'+1-2T}^{n-2T} \rho^j + \sum_{j=T+1}^{T'} \rho^j \leq \frac{\rho^{\lfloor \delta T \rfloor + 1} + \rho^{T+1}}{1 - \rho} \leq \frac{2\rho^{\delta T}}{1 - \rho} \leq \frac{\varepsilon}{2}.$$

Now we study the probability that $I_{n-T} \not\subseteq J$. For $t = n - T' + 1, \dots, n - T$, say step t is *bad* if $I_t \setminus J = I_{t-1} \setminus J \neq \emptyset$ (i.e., if $I_{t-1} \not\subseteq J$, and the element we remove from I_{t-1} in step t lies in J). Then for any outcome of $A^{\uparrow t}$ with $I_{t-1} \not\subseteq J$, we have

$$\Pr[t \text{ is bad} \mid A^{\uparrow t}] \leq \rho^{|I_{n-t} \setminus J|} \leq \rho,$$

and for any outcome of $A^{\uparrow t}$ with $I_{t-1} \subseteq J$ we have $\Pr[t \text{ is bad} \mid A^{\uparrow t}] = 0 \leq \rho$. Thus, the number of bad steps is stochastically dominated by a $\text{Binomial}(T' - T, \rho)$ -distributed random variable.

Now, if $I_{n-T} \not\subseteq J$, there must be an element $h \in I_{n-T} \not\subseteq J$. This means that $I_t \not\subseteq J$ for all $t = n - T' + 1, \dots, n - T$. Furthermore, at most $|I_{n-T'} \setminus J| \leq |I_{n-T'}| - |J| = T' - 2T = \lfloor \delta T \rfloor$ elements outside J get removed during the $T' - T$ steps $n - T' + 1, \dots, n - T$. This means that at least $T' - T - \lfloor \delta T \rfloor = T$ of these steps must be bad.

Thus, writing $B \sim \text{Binomial}(T' - T, \rho)$ (which has expectation $\rho(T' - T)$ and standard deviation at most $\sqrt{T' - T} \leq \sqrt{(1 + \delta)T}$), we have

$$\Pr[I_{n-T} \not\subseteq J] \leq \Pr[\text{at least } T \text{ of the steps } n - T' + 1, \dots, n - T \text{ are bad}]$$

²If we terminate in some step (so I_{n-T} is not defined), we say that the event $\{I_{n-T} \not\subseteq J\}$ does *not* occur.

$$\begin{aligned}
&\leq \Pr[B \geq T] \\
&\leq \Pr[B \geq \rho(T' - T) + \delta T] \leq \frac{(1 + \delta)T}{\delta^2 T^2} = \frac{(1 + \delta)}{\delta^2 T} \leq \frac{\varepsilon}{2},
\end{aligned}$$

noting that $\rho(T' - T) + \delta T \leq \rho(1 + \delta)T + \delta T \leq T$ by definition of T' and of δ , and using Chebyshev's inequality. $\square$

Now we show how to deduce [Lemma 3.3](#).

Proof of Lemma 3.3. Let $T_\mu(\cdot)$ be as in [Lemma 3.9](#) and let $S = T_\mu(\varepsilon/2)$. Let $\ell = 2\lceil n^{0.99} \rceil$ and fix disjoint subsets $J_1, \dots, J_\ell \subseteq \{1, \dots, n\}$ of size $2S$. Say J_i is *good* if there is a subset $I_i \subseteq J_i$ of size $|I_i| = S$ with $\text{per}(A; I_i) \neq 0$, and say that J_i is *bad* otherwise. Then each J_i is bad with probability at most $\varepsilon/2$ by [Lemma 3.9](#). By Markov's inequality, the probability that more than half of $J_1, \dots, J_\ell$ are bad is at most $2(\varepsilon/2) = \varepsilon$. If this does not happen, i.e. if at least $\ell/2 = \lceil n^{0.99} \rceil$ of the sets $J_1, \dots, J_\ell$ are good, then $\mathcal{E}(S, \lceil n^{0.99} \rceil)$ occurs. $\square$

3.2. Approximate uniformity for linear maps. In this section we prove [Lemma 3.6](#) and use it to deduce [Lemma 3.2](#). First, we need the following simple lemma showing anticoncentration bounds for $M\vec{x}$ in terms of the rank of M and the entry distribution of $\vec{x}$.

Lemma 3.10. *Let $\rho = \max_{z \in \mathbb{F}_p} \mu(z) < 1$, and let $\vec{x} \in \mathbb{F}_p^n$ be a vector with independent μ -distributed entries. Then for any matrix $M \in \mathbb{F}_p^{m \times n}$ and any $\vec{z} \in \mathbb{F}_p^m$, we have*

$$\Pr[M\vec{x} = \vec{z}] \leq \rho^{\text{rank } M}.$$

Proof. We can interpret $M\vec{x} = \vec{z}$ as a system of linear equations. Letting $r = \text{rank } M$, this system has exactly $n - r$ free variables. Conditioning on any entries for the entries of $\vec{x}$ corresponding to these free variables, there is at most one choice for each of the remaining r entries such that $M\vec{x} = \vec{z}$. For each of these entries, the probability of attaining the appropriate value is at most ρ , so overall $\Pr[M\vec{x} = \vec{z}]$ is at most $\rho^r = \rho^{\text{rank } M}$. $\square$

Now, we are ready to prove [Lemma 3.6](#).

Proof of Lemma 3.6. We may assume without loss of generality $\varepsilon < 1/2$. Let $\rho = \max_{z \in \mathbb{F}_p} \mu(z) < 1$ be the maximum point probability of μ , and let $R \in \mathbb{N}$ be such that $\rho^R \leq p^{-r}$. Furthermore, let $Q_\mu(\cdot)$ be as in [Lemma 3.7](#), let $Q = Q_\mu(\varepsilon/r)$ and let $K = 2p^R Q$.

First, consider the case that $\text{rank } M > R$. Then by [Lemma 3.10](#) we have

$$\Pr[M\vec{x} = \vec{0}] \leq \rho^{\text{rank } M} \leq \rho^R \leq p^{-r} + \varepsilon,$$

as desired.

So let us from now on assume that $\text{rank}(M) \leq R$. Then there is a set $I \subseteq \{1, \dots, m\}$ of size $|I| \leq R$, such that the rows indexed by I generate the row space of the matrix M . In particular, for any $i = 1, \dots, K$ the row space of the matrix $M[\{1, \dots, m\} \times I_i]$ is generated by the rows indexed by I , and so our assumption $\text{rank } M[\{1, \dots, m\} \times I_i] \geq r$ implies $\text{rank } M[I \times I_i] \geq r$. Thus, for each $i = 1, \dots, K$, the submatrix $M[I \times I_i]$ has r linearly independent columns.

Let $S \subseteq \mathbb{F}_p^I$ be the set of “popular” vectors that appear at least $K/(2p^R) = Q$ times as columns of $M[I \times \{1, \dots, n\}]$. All but at most $p^{|I|} \cdot K/(2p^R) \leq p^R \cdot K/(2p^R) = K/2$ columns of $M[I \times \{1, \dots, n\}]$ are popular, so there is an index $i \in \{1, \dots, K\}$ such that all columns of $M[I \times I_i]$ are popular vectors. This means in particular that there are r linearly independent popular vectors $\vec{v}_1, \dots, \vec{v}_r \in S \subseteq \mathbb{F}_p^I$. After reordering the columns of M , suppose without loss of generality that the first Q columns of $M[I \times \{1, \dots, n\}]$ are equal to $\vec{v}_1$, the second Q columns are equal to $\vec{v}_2$, and so on. Then, whenever we have $M\vec{x} = \vec{0}$, we obtain $M[I \times \{1, \dots, n\}]\vec{x} = \vec{0}$, and hence

$$(x_1 + \dots + x_Q)\vec{v}_1 + \dots + (x_{(r-1)Q+1} + \dots + x_{rQ})\vec{v}_r + M[I \times \{rQ+1, \dots, n\}](x_{rQ+1}, \dots, x_n)^T = M\vec{x} = \vec{0}.$$

Thus, writing $\vec{z} = -M[I \times \{rQ+1, \dots, n\}](x_{rQ+1}, \dots, x_n)^T$ and $y_j = x_{(j-1)Q+1} + \dots + x_{jQ}$ for $j = 1, \dots, r$, we obtain

$$\Pr[M\vec{x} = \vec{0}] \leq \Pr[M[I \times \{1, \dots, n\}]\vec{x} = \vec{0}] \leq \Pr[y_1\vec{v}_1 + \dots + y_r\vec{v}_r = \vec{z}].$$

Now, since $\vec{v}_1, \dots, \vec{v}_r \in F_p^I$ are linearly independent, for any outcome of $\vec{z}$ there is at most one possible outcome of $y_1, \dots, y_r \in \mathbb{F}_p$ such that $y_1 \vec{v}_1 + \dots + y_r \vec{v}_r = \vec{z}$. Note that $y_1, \dots, y_r$ are independent, and by [Lemma 3.7](#) each y_i is (ε/r) -almost-uniform, so we may conclude that

$$\Pr[M\vec{x} = \vec{0}] \leq \Pr[y_1 \vec{v}_1 + \dots + y_r \vec{v}_r = \vec{z}] \leq \left(\frac{1}{p} + \frac{\varepsilon}{r}\right)^r \leq \frac{1}{p^r} + \varepsilon. \quad \square$$

Now we show how to deduce [Lemma 3.2](#).

Proof of Lemma 3.2. For large L , fix an outcome of $A^{\uparrow s}$ satisfying $\mathcal{E}(s, L)$, so there are disjoint size- s sets $I_1, \dots, I_L$, each satisfying $\text{per}(A; I_i) \neq 0$. For each $j \in \{1, \dots, L\}$, let $\mathcal{F}_j$ be the event that $\text{per}(A; I_j \setminus \{i\}) = 0$ for all $i \in I_j$, and let X be the number of $j \in \{1, \dots, L\}$ for which $\mathcal{F}_j$ occurs. Our objective is to prove that, for sufficiently large L , we have

$$\Pr[X > L - \ell] \leq \frac{1}{p^s} + \varepsilon.$$

We will do this by studying a sufficiently high moment of X , using [Lemma 3.6](#).

Write $\vec{x}$ for the $(n-s+1)$ -th row of A . First, note that (given our outcome of $A^{\uparrow s}$), for each $j \in \{1, \dots, L\}$, the quantities $\text{per}(A; I_j \setminus \{i\})$, for $i \in I_j$, depend linearly on $\vec{x}$. We define an $s \times n$ matrix M_j to record this linear dependence (with rows indexed by I_j , and with columns indexed by $\{1, \dots, n\}$), as follows. For $i \in I_j$ and $h \notin I_j$, write $I_j - i + h$ to denote the size- s set $(I_j \setminus \{i\}) \cup \{h\}$. Then, for $i \in I_j$ and $h \in \{1, \dots, n\}$, define the (i, h) -entry of M_j to be

$$\begin{cases} \text{per}(A; I_j - i + h) & \text{if } h \notin I_j, \\ \text{per}(A; I_i) & \text{if } i = h, \\ 0 & \text{if } h \in I_j \setminus \{i\}. \end{cases}$$

It is not hard to see (using [Fact 2.1](#)) that for any $i \in I_j$, the i -entry of $M_j \vec{x}$ is precisely $\text{per}(A; I_j \setminus \{i\})$. In particular, $\mathcal{F}_j$ occurs if and only if $M_j \vec{x} = \vec{0}$. Also note that the $s \times s$ submatrix $M_j[I_j \times I_j]$ is a diagonal matrix with all entries on the diagonal being $\text{per}(A; I_i) \neq 0$, so we have $\text{rank } M_j[I_j \times I_j] = s$.

Now, let $K_\mu(\cdot, \cdot)$ be as in [Lemma 3.6](#) and let $K = K_\mu(s, \varepsilon/2)$. For each subset $J \subseteq \{1, \dots, L\}$ with $|J| = K$, let $M_J \in \mathbb{F}_p^{(Ks) \times n}$ be the matrix obtained by concatenating the matrices M_j for $j \in J$ below each other (i.e. the matrix whose rows are the rows of all the matrices M_j for $j \in J$). Then, M_J satisfies the conditions of [Lemma 3.6](#) with $r = s$ (since $\text{rank } M_J[\{1, \dots, Ks\} \times I_j] \geq \text{rank } M_j[I_j \times I_j] = s$ for all $j = 1, \dots, K$), and therefore

$$\Pr\left[\bigcap_{j \in J} \mathcal{F}_j\right] = \Pr[M_J \vec{x} = \vec{0}] \leq \frac{1}{p^s} + \frac{\varepsilon}{2}.$$

This implies that

$$\mathbb{E}\left[\binom{X}{K}\right] \leq \left(\frac{1}{p^s} + \frac{\varepsilon}{2}\right) \binom{L}{K},$$

so by Markov's inequality,

$$\Pr[X > L - \ell] \leq \Pr\left[\binom{X}{K} \geq \binom{L - \ell}{K}\right] \leq \left(\frac{1}{p^s} + \frac{\varepsilon}{2}\right) \binom{L}{K} \binom{L - \ell}{K}^{-1} \leq \frac{1}{p^s} + \varepsilon$$

for sufficiently large L . $\square$

REFERENCES

- [1] L. A. Bassalygo, *On the number of nonzero permanents over a finite field of odd characteristic*, Probl. Inf. Transm. **49** (2013), no. 4, 382–383, Translation of Problemy Peredachi Informatsii **49** (2013), no. 4, 95–97.
- [2] M. V. Budrevich and A. E. Guterman, *Permanent has less zeros than determinant over finite fields*, Theory and applications of finite fields, Contemp. Math., vol. 579, Amer. Math. Soc., Providence, RI, 2012, pp. 33–42.
- [3] J.-Y. Cai, A. Pavan, and D. Sivakumar, *On the hardness of permanent*, STACS 99 (Trier), Lecture Notes in Comput. Sci., vol. 1563, Springer, Berlin, 1999, pp. 90–99.
- [4] L. S. Charlap, H. D. Rees, and D. P. Robbins, *The asymptotic probability that a random biased matrix is invertible*, Discrete Math. **82** (1990), no. 2, 153–163.
- [5] G. Dolinar, A. E. Guterman, B. Kuzma, and M. Orel, *On the Polya permanent problem over finite fields*, European J. Combin. **32** (2011), no. 1, 116–132.

- [6] S. Eberhard, *The characteristic polynomial of a random matrix*, *Combinatorica* **42** (2022), no. 4, 491–527.
- [7] L. Esperet, *Antifactors in bipartite multigraphs*, arXiv preprint arXiv:2205.14904.
- [8] U. Feige and C. Lund, *On the hardness of computing the permanent of random matrices*, *Comput. Complexity* **6** (1996), no. 2, 101–132.
- [9] P. Gemmell, R. Lipton, R. Rubinfeld, M. Sudan, and A. Wigderson, *Self-testing/correcting for polynomials and for approximate functions*, Proceedings of the twenty-third annual ACM symposium on Theory of computing - STOC '91, STOC '91, ACM Press, 1991, p. 33–42.
- [10] P. Gemmell and M. Sudan, *Highly resilient correctors for polynomials*, *Inform. Process. Lett.* **43** (1992), no. 4, 169–174.
- [11] F. Ghasemi, G. Gross, and S. Kopparty, *Permanental rank versus determinantal rank of random matrices over finite fields*, arXiv preprint arXiv:2512.03221 (2025).
- [12] A. Guionnet, *Bernoulli random matrices*, European Congress of Mathematics, EMS Press, Berlin, 2023, pp. 45–71.
- [13] Z. Hunter, M. Kwan, and L. Sauerermann, *Exponential anticoncentration of the permanent*, arXiv preprint arXiv:2509.22577.
- [14] S. Jukna, *Extremal combinatorics*, Texts in Theoretical Computer Science. An EATCS Series, Springer-Verlag, Berlin, 2001, With applications in computer science.
- [15] J. Kahn and J. Komlós, *Singularity probabilities for random matrices over finite fields*, *Combin. Probab. Comput.* **10** (2001), no. 2, 137–157.
- [16] S. Kopparty, *Problem session (problem 9)*, *Combinatorics*, Oberwolfach Rep. **14** (2017), no. 1, 5–81, Abstracts from the workshop held January 1–7, 2017, Organized by Jeff Kahn, Angelika Steger and Benny Sudakov.
- [17] I. N. Kovalenko and A. A. Levitskaja, *Limiting behavior of the number of solutions of a system of random linear equations over a finite field and a finite ring*, *Dokl. Akad. Nauk SSSR* **221** (1975), no. 4, 778–781.
- [18] M. V. Kozlov, *On the rank of matrices with random Boolean elements*, *Dokl. Akad. Nauk SSSR* **169** (1966), 1013–1016.
- [19] M. Kwan and L. Sauerermann, *On the permanent of a random symmetric matrix*, *Selecta Math. (N.S.)* **28** (2022), no. 1, Paper No. 15, 29.
- [20] R. J. Lipton, *New directions in testing*, Distributed computing and cryptography (Princeton, NJ, 1989), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 2, Amer. Math. Soc., Providence, RI, 1991, pp. 191–202.
- [21] K. Luh, S. Meehan, and H. H. Nguyen, *Some new results in random matrices over finite fields*, *J. Lond. Math. Soc. (2)* **103** (2021), no. 4, 1209–1252.
- [22] P. H. Lundow and K. Markström, *Efficient computation of permanents, with applications to boson sampling and random matrices*, arXiv preprint arXiv:1904.06229.
- [23] K. Maples, *Cokernels of random matrices satisfy the Cohen-Lenstra heuristics*, arXiv preprint arXiv:1301.1239.
- [24] K. Maples, *Singularity of random matrices over finite fields*, arXiv preprint arXiv:1012.2372.
- [25] M. Marcus and H. Minc, *On the relation between the determinant and the permanent*, *Illinois J. Math.* **5** (1961), 376–381.
- [26] H. H. Nguyen and M. M. Wood, *Random integral matrices: universality of surjectivity and the cokernel*, *Invent. Math.* **228** (2022), no. 1, 1–76.
- [27] N. Robertson, P. D. Seymour, and R. Thomas, *Permanents, Pfaffian orientations, and even directed circuits*, *Ann. of Math. (2)* **150** (1999), no. 3, 929–975.
- [28] J. Sahasrabudhe, *Probabilistic combinatorics at exponentially small scales*, arXiv preprint arXiv:2512.15077.
- [29] D. Scheinerman, *Fast computation of permanents over $\mathbb{F}_3$ via $\mathbb{F}_2$ arithmetic*, arXiv preprint arXiv:2407.20205.
- [30] D. E. Smith, *A source book in mathematics*, Dover Publications, Inc., New York, 1959.
- [31] T. Tao and V. Vu, *On the permanent of random Bernoulli matrices*, *Adv. Math.* **220** (2009), no. 3, 657–669.
- [32] K. Tikhomirov, *Singularity of random Bernoulli matrices*, *Ann. of Math. (2)* **191** (2020), no. 2, 593–634.
- [33] V. V. Vazirani and M. Yannakakis, *Pfaffian orientations, 0-1 permanents, and even cycles in directed graphs*, vol. 25, 1989, *Combinatorics and complexity* (Chicago, IL, 1987), pp. 179–190.
- [34] V. H. Vu, *Combinatorial problems in random matrix theory*, Proceedings of the International Congress of Mathematicians—Seoul 2014. Vol. IV, Kyung Moon Sa, Seoul, 2014, pp. 489–508.
- [35] V. H. Vu, *Recent progress in combinatorial random matrix theory*, *Probab. Surv.* **18** (2021), 179–200.
- [36] M. M. Wood, *The distribution of sandpile groups of random graphs*, *J. Amer. Math. Soc.* **30** (2017), no. 4, 915–958.
- [37] M. M. Wood, *Random integral matrices and the Cohen-Lenstra heuristics*, *Amer. J. Math.* **141** (2019), no. 2, 383–398.

DEPARTMENT OF MATHEMATICS, ETH ZÜRICH, ZÜRICH, SWITZERLAND.

Email address: zach.hunter@math.ethz.ch

INSTITUTE OF SCIENCE AND TECHNOLOGY AUSTRIA (ISTA). AM CAMPUS 1, 3400 KLOSTERNEUBURG, AUSTRIA

Email address: matthew.kwan@ist.ac.at

INSTITUTE FOR APPLIED MATHEMATICS, UNIVERSITY OF BONN, GERMANY

Email address: sauerermann@iam.uni-bonn.de