PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY

SINGULARITY OF RANDOM SYMMETRIC MATRICES REVISITED

MARCELO CAMPOS, MATTHEW JENSSEN, MARCUS MICHELEN, AND JULIAN SAHASRABUDHE

(Communicated by Qi-Man Shao)

Abstract. Let M_n be drawn uniformly from all ± 1 symmetric $n \times n$ matrices. We show that the probability that M_n is singular is at most $\exp(-c(n\log n)^{1/2})$, which represents a natural barrier in recent approaches to this problem. In addition to improving on the best-known previous bound of Campos, Mattos, Morris and Morrison of $\exp(-cn^{1/2})$ on the singularity probability, our method is different and considerably simpler: we prove a "rough" inverse Littlewood-Offord theorem by a simple combinatorial iteration.

1. Introduction

Let A_n denote a random $n \times n$ matrix drawn uniformly from all matrices with $\{-1, 1\}$ coefficients. It is an old problem, of uncertain origin,[1] to determine the probability that A_n is singular. While a few moments of consideration reveals a natural *lower* bound of $(1 + o(1))n^2 2^{-n+1}$, which comes from the probability that two rows or columns are equal up to sign, it is widely believed that in fact

$$\mathbb{P}(\det A_n = 0) = (1 + o(1))n^2 2^{-n+1}\,. \tag{1}$$

This singularity probability was first shown to tend to zero in 1967 by Komlós [10], who obtained the bound $\mathbb{P}(\det(A_n) = 0) = O(n^{-1/2})$. The first exponential upper bound was established by Kahn, Komlós, and Szemerédi [9] in 1995 with subsequent improvements on the exponent by Tao and Vu [17, 18] and Bourgain, Vu and Wood [1]. In 2018, Tikhomirov [20] settled this conjecture up to lower order terms by showing $\mathbb{P}(\det(A_n) = 0) = (1/2 + o(1))^n$. Very recently, a closely related problem was resolved by Jain, Sah and Sawhney [8], who showed that the analogue of (1) holds when the entries of A_n are i.i.d. discrete variables of finite support that are not uniform on their support. The conjecture (1) remains open for matrices with mean-zero $\{-1, 1\}$ entries.

The focus of this paper is on the analogous question for *symmetric* random matrices. In particular, let M_n denote a uniformly drawn matrix among all $n \times n$ symmetric matrices with entries in $\{-1, 1\}$. In this setting it is also widely believed that $\mathbb{P}(\det M_n = 0) = \Theta(n^2 2^{-n})$ as in the asymmetric case [2, 3, 22] although here much less is known. For instance, the fact that $\mathbb{P}(\det M_n = 0) = o(1)$, was only resolved in 2005 by Costello, Tao and Vu [3]. Subsequent superpolynomial

Received by the editors January 17, 2021, and, in revised form, August 3, 2021.
2020 *Mathematics Subject Classification.* Primary 60B20.
The first author was partially supported by CNPq.
The third author was partially supported by NSF grant DMS-2137623.

[1]See [9] for a short discussion on the history of this conjecture

upper bounds of the form n^{-C} for all C and $\exp(-n^c)$ were proven respectively by Nguyen [12] and Vershynin [21] by different techniques: Nguyen used an inverse Littlewood-Offord theorem for quadratic forms based on previous work by Nguyen and Vu [11, 13], while Vershynin used a more geometric approach pioneered by Rudelson and Vershynin [14–16].

A combinatorial approach developed by Ferber, Jain, Luh and Samotij [5] was applied by Ferber and Jain [4] in 2018 to prove that $\mathbb{P}(\det M_n = 0) \leq \exp\big(-cn^{1/4}(\log n)^{1/2}\big)$. Another combinatorial approach was taken by Campos, Mattos, Morris and Morrison [2] who achieved the bound $\mathbb{P}(\det M_n = 0) \leq \exp\left(-cn^{1/2}\right)$. Their argument centers around an inverse Littlewood-Offord theorem inspired by the method of hypergraph containers.

The proofs of [2, 4, 21] all follow the same general shape: divide all potential vectors v for which we could have $M_n v = 0$ into "structured" and "unstructured" vectors, show that the unstructured vectors do not contribute, and union bound over the structured vectors. The main difficulty (and novelty) in these proofs arises in a careful understanding of the contribution of the *structured* vectors.

While we have this method to thank for the recent successes on this problem, an important limitation was pointed out in [2, Section 2.2] who argued that this method could not provide any improvement to the singularity probability beyond $\exp(-c\sqrt{n \log n})$, provided the randomness in the matrix is not "reused". Here we show that this natural barrier is attainable.

Theorem 1. *Let M_n be drawn uniformly from all $n \times n$ symmetric matrices with entries in $\{-1, 1\}$. Then for $c = 2^{-13}$ and n sufficiently large*

$$\mathbb{P}(\det(M_n) = 0) \leq \exp\left(-c\sqrt{n \log n}\right).$$

Indeed, our proof of Theorem 1 follows the shape of [2,4,21] and improves upon these results primarily by proving an improved and considerably simpler "rough" inverse Littlewood-Offord theorem. This theorem parallels Theorem 2.1 in [2] and improves upon it by replacing the use of Fourier analysis in [2] with a simple combinatorial algorithm. This proof additionally gives us more information in our inverse theorem, which allows for a simplified application to the proof of Theorem 1.

To state our rough inverse theorem, we need a few notions. For a vector $v \in \mathbb{Z}_p^n$ and $\mu \in [0, 1]$, we define the random variable $X_\mu(v) := \varepsilon_1 v_1 + \cdots + \varepsilon_n v_n$, where $\varepsilon_i \in \{-1, 0, 1\}$ are i.i.d. and $\mathbb{P}(\varepsilon_i = 1) = \mathbb{P}(\varepsilon_i = -1) = \mu/2$. Also define $\rho_\mu(v) = \max_x \mathbb{P}(X_\mu(v) = x)$ and[2] let $|v|$ denote the number of non-zero entries of v. Finally for $T \subseteq [n]$, let $v_T := (v_i)_{i \in T}$.

We now introduce a simple concept that is key to our rough inverse Littlewood-Offord theorem. For a vector $w = (w_1, \ldots, w_d)$ we define the *neighbourhood* of w (relative to μ) as

$$N_\mu(w) := \{x \in \mathbb{Z}_p : \mathbb{P}(X_\mu(w) = x) > 2^{-1}\mathbb{P}(X_\mu(w) = 0)\}, \tag{2}$$

which is the set of places where our random walk is "likely" to terminate, relative to 0. The following result, which is our "rough" Littlewood-Offord theorem, says that if $v \in \mathbb{Z}_p^n$ and $\rho_\mu(v)$ is large then there is a small subvector x of v so that $v_i \in N_\mu(x)$ for many $i \in [n]$.

[2]We will also write $\rho_1(v) = \rho(v)$.

Theorem 2. *Let $\mu \in (0,1/4]$, $k,n \in \mathbb{N}$, p be prime and $v \in \mathbb{Z}_p^n$. Set $d = \frac{2}{\mu}\log \rho_\mu(v)^{-1}$, suppose that $|v| \geq kd$ and $\rho_\mu(v) \geq \frac{2}{p}$. Then there exists $T \subseteq [n]$ with $|T| \leq d$ so that if we set $w = v_T$ then $v_i \in N_\mu(w)$ for all but at most kd values of $i \in [n]$ and*

$$|N_\mu(w)| \leq \frac{256}{(\mu k)^{1/5}} \cdot \frac{1}{\rho_\mu(v)}\,.$$

In practice we will not apply Theorem 2 directly, but rather in two parts (Lemmas 7 and 8). The first can be found in Section 6 and uses Fourier analysis in the style of Halász [6], whose influential techniques pervade the literature. The second is a novel (and simple) iterative application of a greedy algorithm. This can be found in Section 2 along with the proof of Theorem 2.

In what follows we discuss the proof of Theorem 1. In addition to illustrating the method of [2, 4] in a little more detail, we hope the reader will get some feeling for why Theorem 2 is so integral to the problem.

1.1. **Discussion of proof.** The event 'M_n is singular' can, somewhat daftly, be expressed as $\bigcup_{v\in\mathbb{R}^n\setminus\{0\}}\{Mv = 0\}$. To reduce the size of this unwieldy union, we notice that it is sufficient to consider all non-zero $v \in \mathbb{Z}^n$ and then reduce modulo p, for a prime $p \approx \exp\left(c(n\log n)^{1/2}\right)$. Since the probability that Mv is zero is certainly bounded by the probability Mv is zero modulo p, it is enough for us to upper bound the probability of the event $\bigcup_{v\in\mathbb{Z}_p^n\setminus\{0\}}\{Mv = 0\}$, where all operations are taken over the field of p elements.

Having reduced our event to a union of a finite number of sets, it is temping to greedily apply the union bound to the events $\{Mv = 0\}$, for non-zero $v \in \mathbb{Z}_p^n$. Unfortunately in our case, a small wrinkle arises with vectors for which $\rho(v) \approx 1/p$; that is, very close to the "mixing" threshold. To get around this, we again follow [2, 4] and use a lemma that allows us to safely exclude all v with $\rho(v) < cn/p$ from our union bound, at the cost of working with a slightly different event which, in practice, adds little difficulty to our task. In particular, to prove Theorem 1, it will be enough to establish the following.

Theorem 3. *Let $c = 1/800$, $n \in \mathbb{N}$ sufficiently large and $p \leq \exp(c\sqrt{n\log n})$ prime. Then for $\beta = \Theta(n/p)$ we have*

$$\sum_{v:\rho(v)\geq\beta} \max_{w\in\mathbb{Z}_p^n} \mathbb{P}(Mv = w) \leq e^{-cn}\,. \tag{3}$$

To bound the sum on the left hand side of (3), we invoke our inverse Littlewood-Offord result (Theorem 2, in the form of Lemmas 4 and 7).

We will in fact first sketch a proof of Theorem 3 under the stricter assumption that $p \leq \exp(c\sqrt{n})$ and then show how to recover the missing $\sqrt{\log n}$ factor. We do this for two reasons. Firstly, the proof under the stricter assumption on p already contains the key ideas, and so we feel this is the clearest way to present the argument. Secondly, the reader can extract a very short proof of the bound $\mathbb{P}(\det(M_n) = 0) \leq \exp\left(-c\sqrt{n}\right)$ if they so desire.

In Section 5, we provide the short derivation of Theorem 1 from Theorem 3 and [2, Lemma 2.1].

Remark. Simultaneously to our work, Jain, Sah and Sawhney [7] obtained an upper bound on the singularity probability of the form $\exp(-cn^{1/2}(\log n)^{1/4})$ and a bound on the lower tail of the least singular value for symmetric random matrices with subgaussian entries.

2. An inverse Littlewood-Offord lemma

In this section we present one of the key ideas of this paper, namely a greedy algorithm which furnishes us with a simple yet powerful inverse Littlewood-Offord result.

To go further, we introduce a little notation. Let $\mathbb{Z}_p^*$ denote the set of all vectors of finite dimension with entries in $\mathbb{Z}_p$. For $v = (v_1, \dots, v_k), w = (w_1, \dots, w_l) \in \mathbb{Z}_p^*$, let $vw := (v_1, \dots, v_k, w_1, \dots, w_l)$ denote the *concatenation* of v and w and let v^k denote the concatenation of k copies of v. For $v \in \mathbb{Z}_p^n$ and $T \subseteq [n]$, let $v_T := (v_i)_{i \in T}$ and say that w is a *subvector* of v if $w = v_T$ for some $T \subseteq [n]$. We also define $|v|$ to be the size of the *support* of v, the number of non-zero coordinates.

Unless specified otherwise, take $\mu = 1/4$ for definiteness. We recall the key definition introduced in (2). For $w \in \mathbb{Z}_p^*$, we define the *neighbourhood* of w as

$$N(w) := \{x \in \mathbb{Z}_p : \mathbb{P}(X_\mu(w) = x) > 2^{-1}\mathbb{P}(X_\mu(w) = 0)\}.$$

This is motivated by the fact that for $\mu \in [0, 1/2]$, the walk X_μ is most likely to be found at 0 (see e.g. [19, Corollary 7.12]), i.e.

$$\rho_\mu(w) = \mathbb{P}(X_\mu(w) = 0)\,. \tag{4}$$

Hence, we may think of $N(w)$ as the set of all values of the random walk $X_\mu(w)$, which are at least half as likely as the most likely value. We can also easily control the size of $N(w)$ in terms of $\rho_\mu(w)$. Indeed,

$$1 \geq \sum_{x \in N(w)} \mathbb{P}(X_\mu(w) = x) > \frac{1}{2}|N(w)| \cdot \mathbb{P}(X_\mu(w) = 0) = \frac{1}{2}|N(w)|\rho_\mu(w)$$

and so

$$|N(w)| \leq \frac{2}{\rho_\mu(w)}\,. \tag{5}$$

We now turn to our greedy algorithm which, given a vector $v \in \mathbb{Z}_p^*$, returns a short subvector w of v such that each coordinate of v is contained in $N(w)$. The following simple lemma can be interpreted as an inverse Littlewood-Offord result in its own right, and is *almost* as good as Theorem 2; however it only gives a bound of $|N(w)| \leq 1/\rho_\mu(w) \leq 1/\rho_\mu(v)$, which is lacking the crucial factor of $k^{-1/5}$. For this lemma we use the monotonicity of ρ_μ [19, Corollary 7.12]: if $w, v \in \mathbb{Z}_p^*$ where w is a subvector of v, then

$$\rho_\mu(v) \leq \rho_\mu(w)\,. \tag{6}$$

Lemma 4. *For $\mu \in (0, 1/4]$ and $n \in \mathbb{N}$, let $v \in \mathbb{Z}_p^n$. Then there exists $T \subseteq [n]$, such that $v_i \in N(v_T)$ for all $i \notin T$, $\rho_\mu(v_T) \leq (1 - \mu/2)^{|T|}$ and so*

$$|T| \leq \frac{2}{\mu} \log \frac{1}{\rho_\mu(v)}.$$

Proof. We build a sequence of sets $T_1, \dots, T_d \subseteq [n]$ with $|T_i| = i$ via the following greedy process. Let $T_1 = \{1\}$. Given $T_t \subseteq [n]$ with $|T_t| = t$ for $t \geq 1$, let $v_{T_t} = (x_1, \dots, x_t)$. Pick $i \in [n] \backslash T_t$ such that

$$\rho_\mu(x_1 \dots x_t v_i) \leq (1 - \mu/2)\rho_\mu(x_1 \dots x_t)\,. \tag{7}$$

If no such i exists we terminate the process and set $T = T_t$. Suppose this process runs for d steps producing $T \subseteq [n]$ such that $v_T = (x_1, \dots, x_d)$. By the termination condition, we have that for $i \in [n] \backslash T$

$$\rho_\mu(x_1 \dots x_d v_i) > (1 - \mu/2)\rho_\mu(x_1 \dots x_d)\,.$$

Conditioning on the coefficient of v_i and using that $\mathbb{P}(X_\mu(x_1 \dots x_d) = v_i) = \mathbb{P}(X_\mu(x_1 \dots x_d) = -v_i)$ by symmetry, we can rewrite the left hand side to obtain

$$\mu\mathbb{P}(X_\mu(x_1 \dots x_d) = v_i) + (1-\mu)\rho_\mu(x_1 \dots x_d) > (1 - \mu/2)\rho_\mu(x_1 \dots x_d)\,.$$

Rearranging shows $v_i \in N(v_T)$. For the bound on $d = |T|$, observe that by (6), inequality (7) and the fact that $\rho_\mu(x_1) = (1 - \mu)$ we have

$$\rho_\mu(v) \le \rho_\mu(x_1 \dots x_d) \le (1 - \mu/2)^d \le e^{-\mu d/2}\,.$$

$\square$

3. A weak version of Theorem 3

In this section we sketch how a weak version of Theorem 3 follows from Lemma 4. This section is not needed for the proof of Theorem 1, but is included to illustrate some of the key ideas. Moreover, the bound $\mathbb{P}(\det(M_n) = 0) \le \exp(-c\sqrt{n})$ follows easily from Theorem 6 and Lemma 9 and so we obtain a particularly short proof of this result.

First we need the following strengthening of the monotonicity property (6). This type of lemma abounds in the literature, first appearing in [9]. Since the proof is a simplification of the Fourier arguments in the proof Lemma 12, we omit the details.

Lemma 5. *For $\alpha > 0$ there is a ν, $K > 0$ so that for all v with $\rho_\mu(v) = \Omega(n/p)$ and $|v| \ge K$ we have*

$$\rho_\mu(v) \le \alpha\rho_\nu(v)\,.$$

Theorem 6. *There exists $c > 0$ such that for $n \in \mathbb{N}$ sufficiently large, $p \le \exp(c\sqrt{n})$ prime and $\beta = \Theta(n/p)$ we have*

$$\sum_{v:\rho(v)\ge\beta} \max_{w\in\mathbb{Z}_p^n} \mathbb{P}(Mv = w) = e^{-\Omega(n)}\,. \tag{8}$$

Proof. Let $\alpha = 2^{-16}$, let $\nu \in (0, 1/4]$ and $K > 0$ be given by Lemma 5 and set $d = \frac{2}{\nu}\log p$. Let $c > 0$ be a constant taken sufficiently small so that the bounds in the following proof hold. We will use Lemma 4 to count the number of possible v with $\rho(v) \ge \beta$: for each such v, there must be a subset $T \subset [n]$ so that $v_i \in N_\nu(v_T)$ for all $i \notin T$. More formally, let $\mathcal{V} = \{v \in \mathbb{Z}_p^n \setminus \{0\} : \rho(v) \ge \beta\}$ and for $v \in \mathcal{V}$, let $f(v) := (T, v_T)$ where $T \subset [n]$ is the set obtained by applying Lemma 4 to v (with $\mu = \nu$). Let $\mathcal{S} := f(\mathcal{V})$.

For a given $s = (T, u) \in \mathcal{S}$ we have $|T| \le d$ and $u \in \mathbb{Z}_p^{|T|}$. We may therefore bound

$$|\mathcal{S}| \le 2^n \cdot p^d \le 2^{(1+2c^2/\nu)n}\,. \tag{9}$$

Further, for a given $s = (T, u) \in \mathcal{S}$, we note that for every $v \in f^{-1}(s)$ we must have $v_i \in N_\nu(u)$ for every $i \notin T$ and so

$$|f^{-1}(s)| \le |N_\nu(u)|^{n-|T|} \le \left(\frac{2}{\rho_\nu(u)}\right)^{n-|T|}\,. \tag{10}$$

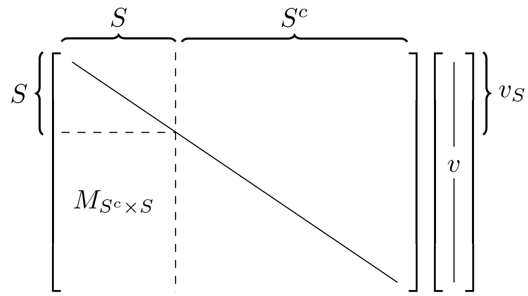

FIGURE 1. Diagram of the matrix M.

For each $v \in f^{-1}(s)$, let $T \subset S$ where $|S| = \min\{|T| + K, |v|\}$ (and $v_i \neq 0$ for all $i \in S$). We may then bound

$$\mathbb{P}(Mv = w) \leq \max_{w'} \mathbb{P}(M_{S^c\times S}(v_S) = w') \leq \rho(v_S)^{n-|S|}\,, \tag{11}$$

where for the second inequality we used that the entries of $M_{S^c\times S}$ are i.i.d. (see Figure 1). Now if $|T|+K \leq |v|$ we apply Lemma 5 to get $\rho(v_S) \leq c\rho_\nu(v_S) \leq c\rho_\nu(u)$. Then applying (10) with (11) for each $s = (T, u)$ yields

$$\begin{aligned}\sum_{\substack{v\in f^{-1}(s)\\ |v|\geq |T|+K}} \max_{w\in\mathbb{Z}_p^n} \mathbb{P}(Mv = w) &\leq |f^{-1}(s)|\rho(u)^{n-|S|}\\ &\leq \left(\frac{2}{\rho_\nu(u)}\right)^{n-|T|}(c\rho_\nu(u))^{n-|T|-K} \leq 2^{-4n}\,,\end{aligned}$$

where for the final inequality we used that $\rho_\nu(u) \geq 1/p$, and so $\rho_\nu(u)^K \geq 2^{-n}$.

Combining with (9) shows that

$$\sum_{s\in\mathcal{S}} \sum_{\substack{v\in f^{-1}(s)\\ |v|\geq |T|+K}} \max_{w\in\mathbb{Z}_p^n} \mathbb{P}(Mv = w) \leq 2^{-n}\,.$$

On the other hand if $|T| = t$ and $|v| \leq t + K$ we use that $\rho(v_S) \leq \rho_\nu(v_S) \leq \rho_\nu(u) \leq (1-\nu/2)^t$ (where the final inequality follows from Lemma 4). In this case there are $p^{t+K}\binom{n}{\leq t+K}$ choices for v. Combining this with (11) we have

$$\sum_{s\in\mathcal{S}} \sum_{\substack{v\in f^{-1}(s)\\ |v|\leq |T|+K}} \max_{w\in\mathbb{Z}_p^n} \mathbb{P}(Mv = w) \leq \sum_{t=1}^{d} p^t \binom{n}{\leq t+K}(1-\nu/2)^{t(n-d-K)} \leq (1-\nu)^{n/8}.$$

$\square$

4. THE GREEDY ALGORITHM ITERATED

In this section we show that we can strengthen Lemma 4 by applying it iteratively. This will be key to regaining this crucial $k^{-1/5}$ in Theorem 2, and will ultimately give our $\sqrt{\log n}$ gain in the exponent of the singularity probability.

For this lemma we need the following property of ρ_μ, which can be found in [19, Corollary 7.12]. Let $w_1, \dots, w_k \in \mathbb{Z}_p^*$ and $\mu \in (0, 1/2)$ then

$$\rho_\mu(w_1 \cdots w_k) \le \max_{j\in[k]} \rho_\mu\left(w_j^k\right) . \tag{12}$$

Lemma 7. *Let $\mu \in (0, 1/4]$, $n \in \mathbb{N}$ and $v \in \mathbb{Z}_p^n$. Set $d = \frac{2}{\mu}\log \rho_\mu(v)^{-1}$ and let $k \in \mathbb{N}$ be such that $kd \le n$. Then there exists $T \subseteq S \subseteq [n]$ with $|T| \le d$, $|S| \le kd$ such that $v_i \in N(v_T)$ for all $i \notin S$ and $\rho_\mu(v_S) \le \rho_\mu(v_T^k)$.*

Proof. We will define a sequence of sets $[n] = A_1 \supseteq \cdots \supseteq A_k \supseteq A_{k+1}$. Given v_{A_j}, we choose $T_j \subseteq [n]$ with $v_{T_j} = (x_1, \dots, x_{d(j)})$ given by Lemma 4 applied to v_{A_j} and let

$$A_{j+1} = A_j \setminus T_j \qquad \text{and} \qquad S = \bigcup_{j=1}^{k} T_j.$$

By Lemma 4, we have that $v_i \in N(v_{T_j})$ for all $i \in A_{j+1}$. In particular, since $S^c \subseteq A_j$ for all $1 \le j \le k+1$, $v_i \in N(v_{T_j})$ for all $i \notin S$ and $1 \le j \le k$. Note also that $|T_j| \le d$ for all $1 \le j \le k$.

Let T be the T_j for which $\rho_\mu(v_{T_j}^k)$ is maximized. The first claim of the lemma follows from the above. For the second claim note that, by (12) we have

$$\rho_\mu(v_S) \le \max_{1\le j\le k} \rho_\mu(v_{T_j}^k) = \rho_\mu(v_T^k)\,.$$

□

To conclude the proof of our Theorem 2—and to understand the strength of Lemma 7—we introduce our main Fourier ingredient, the proof of which is found in Section 6.

Lemma 8. *Let $\mu \in (0, 1/4]$, $k \in \mathbb{N}$ and $v \in \mathbb{Z}_p^*$ such that $|v| \ne 0$. Then*

$$\rho_\mu(v^k) \le 64(\mu k)^{-1/5}\rho_\mu(v) + p^{-1}\,.$$

Proof of Theorem 2. Let $k, n \in \mathbb{N}$ and $v \in \mathbb{Z}_p^n$ be as in the theorem statement. By Lemma 7, there exists $T \subseteq S \subseteq [n]$ with $|T| \le d$, $|S| \le kd$ such that $v_i \in N(v_T)$ for all $i \notin S$ and $\rho_\mu(v_S) \le \rho_\mu(v_T^k)$. Moreover, since $|v| \ge kd$, the support of v_T is non-zero. Applying Lemma 8 we conclude that

$$\rho_\mu(v_S) \le \rho_\mu(v_T^k) \le 64(\mu k)^{-1/5}\rho_\mu(v_T) + p^{-1}\,.$$

By (5) and (6) we then have

$$|N_\mu(v_T)| \le \frac{2}{\rho_\mu(v_T)} \le \frac{128}{(\mu k)^{1/5}(\rho_\mu(v_S) - p^{-1})} \le \frac{256}{(\mu k)^{1/5}\rho_\mu(v)}\,,$$

where on the final bound we use that $\rho_\mu(v) \ge \frac{2}{p}$. □

5. Proof of Theorem 1

In this section we prove our main theorem, Theorem 1. We first show how Theorem 1 follows quickly from Theorem 3 and then we switch our focus to proving Theorem 3.

Define

$$q_n(\beta) := \max_{w\in\mathbb{Z}_p^n} \mathbb{P}\left(\exists\, v \in \mathbb{Z}_p^n \setminus \{0\} :\ Mv = w \text{ and } \rho(v) \ge \beta\right)$$

and note the following lemma from [2] (their Lemma 2.1).

Lemma 9. *Let $n \in \mathbb{N}$ and $p > 2$ be a prime. Then for every $\beta > 0$*

$$\mathbb{P}(\det(M_n) = 0) \leq n \sum_{m=n-1}^{2n-3} \left(\beta^{1/8} + \frac{q_m(\beta)}{\beta} \right).$$

Proof of Theorem 1 *assuming Theorem* 3. Pick a prime $p = t\exp(c\sqrt{n \log n})$ with $c = 1/800$ and $t \in [1/2, 1]$. Letting $\beta = \Theta(n/p)$, we apply the union bound and Theorem 3 to conclude that for $n - 1 \leq m \leq 2n - 3$, we have

$$q_m(\beta) \leq \sum_{v:\rho(v) \geq \beta} \max_{w \in \mathbb{Z}_p^m} \mathbb{P}(Mv = w) \leq e^{-cm}.$$

Thus, we apply Lemma 9, to obtain

$$\mathbb{P}(\det(M_n) = 0) \leq e^{-c(1+o(1))\sqrt{n \log n}/8} + e^{-cn(1+o(1))} \leq e^{-c\sqrt{n \log n}/9},$$

for n sufficiently large. $\square$

With this reduction firmly in-hand, we turn to prove Theorem 3.

Proof of Theorem 3. Throughout we assume that n is sufficiently large so that all inequalities in the proof hold, we let $k = n^{1/4}$, $d = \frac{2}{\mu} \log p \leq \frac{2}{\mu} \sqrt{n \log n}$ and define $\mathcal{V} := \{v \in \mathbb{Z}_p^n \backslash \{0\} : \rho_\mu(v) \geq \beta\}$. Our task is to bound

$$Q_n(\beta) := \sum_{v \in \mathcal{V}} \max_{w} \mathbb{P}(M_n v = w). \tag{13}$$

We start our analysis of (13) by partitioning this sum by way of a function $f : \mathcal{V} \to \mathcal{S}$. To define f, let $v \in \mathbb{Z}_p^n$ and apply Lemma 7 to obtain $S, T \subseteq [n]$. We then apply Lemma 4 to v_S to obtain a further set $T' \subseteq [n]$. We then define $f(v) = (S, T, T', v_T, v_{T'})$ and put $\mathcal{S} := f(\mathcal{V})$. We thus partition our sum (13) as

$$Q_n(\beta) = \sum_{s \in \mathcal{S}} \sum_{v \in f^{-1}(s)} \max_{w} \mathbb{P}(M_n v = w). \tag{14}$$

Note that if $s = (S, T, T', u_1, u_2) \in \mathcal{S}$, then

$$|S| \leq kd, \quad |u_1|, |u_2| \leq d, \quad \rho_\mu(u_1) \geq \beta, \quad \rho_\mu(u_2) \leq (1 - \mu/2)^{|u_2|} \text{ and } \quad u_2 \neq 0 \tag{15}$$

by Lemmas 4 and 7 together with (6), and note that we have the bound

$$|\mathcal{S}| \leq 8^n p^{2d}, \tag{16}$$

since there are 8^n choices for S, T, T' and at most p^{2d} choices for u_1, u_2.

We now turn to bounding a given term in the sum (14), based on which piece of the partition it is in. Let $s = (S, T, T', u_1, u_2) \in \mathcal{S}$ and $v \in f^{-1}(s)$. For any $w \in \mathbb{Z}_p^n$, we bound $\mathbb{P}(M_n v = w)$ by first revealing the rows indexed by S^c and then revealing the rows indexed by $S \backslash T'$,

$$\mathbb{P}(Mv = w) \leq \mathbb{P}\left(M_{(S\backslash T') \times [n]} v = w_{S \backslash T'} \mid M_{S^c \times [n]} v = w_{S^c}\right) \cdot \mathbb{P}(M_{S^c \times [n]} v = w_{S^c}).$$

Looking only on the off-diagonal blocks $(S \setminus T') \times T'$ and $S^c \times S$ and considering the "worst case" vectors for these blocks, we have

$$\mathbb{P}(Mv = w) \leq \max_u \mathbb{P}(M_{(S\backslash T') \times T'} v_{T'} = u) \cdot \max_u \mathbb{P}(M_{S^c \times S} v_S = u).$$

The crucial point here is that these events can be written as an intersection of independent events concerning the rows. That is

$$\mathbb{P}(Mv = w) \leq \rho(v_{T'})^{|S|-|T'|}\rho(v_S)^{n-|S|} \leq \rho_\mu(v_{T'})^{|S|-|T'|}\rho_\mu(v_S)^{n-|S|}, \tag{17}$$

where this last inequality follows from the monotonicity of ρ in the parameter μ, noted at (6).

We now bound the size of a piece of our partition $|f^{-1}(s)|$. By (5) together with Lemmas 4 and 7, the number of choices for v_{S^c} and $v_{S\setminus T'}$ are (respectively) at most

$$|N(u_1)|^{n-|S|} \leq \left(\frac{2}{\rho_\mu(u_1)}\right)^{n-|S|}, \qquad |N(u_2)|^{|S|-|T'|} \leq \left(\frac{2}{\rho_\mu(u_2)}\right)^{|S|-|T'|},$$

so that

$$|f^{-1}(s)| \leq \left(\frac{2}{\rho_\mu(u_1)}\right)^{n-|S|}\left(\frac{2}{\rho_\mu(u_2)}\right)^{|S|-|T'|}. \tag{18}$$

By (17) and the fact that $|S| \leq kd = o(n)$ (by our choice of parameters), we have

$$\sum_{v\in f^{-1}(s)} \max_w \mathbb{P}(M_n v = w) \leq 2^n\left(\frac{\rho_\mu(u_1^k)}{\rho_\mu(u_1)}\right)^{n-|S|} \leq 2^n\left(\frac{\rho_\mu(u_1^k)}{\rho_\mu(u_1)}\right)^{24n/25}. \tag{19}$$

We consider first the case where $|u_1| \neq 0$; then we may apply Lemma 8 to obtain the bound

$$\rho_\mu(u_1^k) \leq 64(\mu k)^{-1/5}\rho_\mu(u_1) + \frac{1}{p}.$$

By the bound $\rho_\mu(u_1) \geq \beta = \Theta(n/p)$, we then have

$$\frac{\rho_\mu(u_1^k)}{\rho_\mu(u_1)} \leq 64(\mu k)^{-1/5} + \Theta(n^{-1}) \leq n^{-1/24}.$$

Combining this with (16) and (19) shows that

$$\sum_{\substack{s\in\mathcal{S},\\ |u_1|\neq 0}}\sum_{v\in f^{-1}(s)} \max_w \mathbb{P}(M_n v = w) \leq |\mathcal{S}|\cdot n^{-n/25} \leq 8^n p^{2d} n^{-n/25}$$

$$\leq 8^n \exp\left(\frac{4c}{\mu}n\log n - \frac{1}{25}n\log n\right) \leq e^{-n}, \tag{20}$$

provided $c \leq \mu/200$. Now if $|u_1| = 0$ then there are at most

$$|f^{-1}(s)| \leq \left(\frac{2}{\rho_\mu(u_2)}\right)^{|S|-|T'|}$$

choices for v. Notice that $\rho_\mu(v_S) \leq \rho_\mu(u_2)$ and so

$$\sum_{v\in f^{-1}(s)} \max_w \mathbb{P}(M_n v = w) \leq \rho_\mu(u_2)^{n-|T'|}\left(\frac{1}{\rho_\mu(u_2)}\right)^{|S|-|T'|}$$

$$\leq \rho_\mu(u_2)^{n/2} \leq (1-\mu/2)^{n|u_2|/2},$$

where for the final inequality we used (15). On the other hand, by (15), the number of choices for $s = (S, T, T', u_1, u_2)$ such that $|u_1| = 0, |u_2| = t$ is at most

$$\binom{n}{\leq kd}^3 p^t \leq \exp(ct\cdot\sqrt{n\log n} + 3kd\log n).$$

Putting our bounds together, we have

$$\sum_{\substack{s\in\mathcal{S},\\ |u_1|=0,|u_2|=t}} \sum_{v\in f^{-1}(s)} \max_w \mathbb{P}(M_n v = w) \leq \exp(ct\cdot\sqrt{n\log n} + 3kd\log n - n\mu t/4)$$
$$\leq e^{-n\mu t/5}\,.$$

Summing over all $t \geq 1$ (recalling that $u_2 \neq 0$) and using (20), we conclude that

$$Q_n(\beta) = \sum_{s\in\mathcal{S}} \sum_{v\in f^{-1}(s)} \max_w \mathbb{P}(M_n v = w) \leq e^{-\mu n/6}\,,$$

as desired. □

6. Proof of Lemma 8

In this section, we pin down one final loose end, the proof of Lemma 8, which is our main Fourier lemma. For $v \in \mathbb{Z}_p^n$, and $\mu \in [0,1]$ we note a standard Fourier expression for $\rho_\mu(v)$. Define

$$f_{\mu,v}(\xi) := \prod_{i=1}^{n}((1-\mu) + \mu c_p(v_i\xi)), \tag{21}$$

where we let $c_p(x) = \cos(2\pi x/p)$. We then have

$$\rho_\mu(v) = \mathbb{E}_{\xi\in\mathbb{Z}_p} f_{\mu,v}(\xi)\,. \tag{22}$$

Clearly $|f_{\mu,v}(\xi)| \leq 1$ and for $\mu \leq 1/2$ each of the terms in the product $f_{\mu,v}(\xi)$ is non-negative. In this case it is natural to work with $\log f_{\mu,v}$. For this, we let $\|x\|_{\mathbb{T}}$ denote the distance from $x \in \mathbb{R}$ to the nearest integer and note the following bounds. For $\mu \in [0,1/4]$ we have

$$\mu\|x/p\|_{\mathbb{T}}^2 \leq -\log(1-\mu+\mu c_p(x)) \leq 32\mu\|x/p\|_{\mathbb{T}}^2\,, \tag{23}$$

which are elementary[3] and can be found in (7.1) in [19].

For Lemma 10, one of the main results of this section, we need the well-known Cauchy-Davenport inequality which tells us that for $A, B \subseteq \mathbb{Z}_p$ we have $|A+B| \geq \min\{|A|+|B|-1, p\}$. Here, as usual, $A+B := \{a+b : a\in A, b\in B\}$.

A first step towards Lemma 8 is to prove it in the case when $\rho_\mu(v)$ is not too large.

Lemma 10. *Let $\mu \in (0,1/4]$, $v \in \mathbb{Z}_p^*$ and $k \in \mathbb{N}$. Then*

$$\rho_\mu(v^k) \leq \Big(\rho_\mu(v)^{\frac{k-1}{k}} + \frac{8}{\sqrt{\mu k}}\Big)\rho_\mu(v) + p^{-1}.$$

To prove this lemma, we adopt some temporary notation. Let $F = f_{\mu,v^k}$ and $G = f_{\mu,v}$, be as defined in (21) and note that $G = F^{1/k}$. We note also that F is non-negative since $\mu \leq 1/4$. Let $\ell := \frac{1}{8}(\mu k)^{1/2}$. For all $\alpha \in (0,1)$, we consider the level sets

$$A_\alpha := \{\xi\in\mathbb{Z}_p : F(\xi) > \alpha\} \qquad B_\alpha := \{\xi\in\mathbb{Z}_p : G(\xi) > \alpha\}.$$

Claim 11. For $\alpha \in (0,1)$, we have $\ell\cdot A_\alpha \subseteq B_\alpha$.

[3] For these explicit constants, note the bounds $a \leq -\log(1-a) \leq (3/2)a$ for $a \in [0,1/4]$ and $x^2 \leq 1-\cos(2\pi x) \leq 20x^2$ for $|x| \leq 1/2$.

Proof. To see this, assume $\xi_1,\ldots,\xi_\ell \in A_\alpha$ and so $G(\xi_i) = (F(\xi_i))^{1/k} > \alpha^{1/k}$ for each $i \in [\ell]$. Taking logs of both sides and applying (23) gives, for each $i \in [\ell]$,

$$\mu \sum_{j=1}^{n} \|\xi_i v_j\|_{\mathbb{T}}^2 \le -\log G(\xi_i) \le k^{-1} \log \alpha^{-1} \,. \tag{24}$$

Thus, using the triangle inequality along with (24) gives

$$\left(\sum_{j=1}^{n} \|(\xi_1 + \cdots + \xi_\ell)v_j\|_{\mathbb{T}}^2\right)^{1/2} \le \sum_{i=1}^{\ell}\left(\sum_{j=1}^{n} \|\xi_i v_j\|_{\mathbb{T}}^2\right)^{1/2} \le \ell\left(\frac{\log \alpha^{-1}}{\mu k}\right)^{1/2} .$$

It then follows from the upper bound in (23) that

$$-\log G(\xi_1 + \cdots + \xi_\ell) \le 32 \sum_{j=1}^{n} \|(\xi_1 + \cdots + \xi_\ell)v_j\|_{\mathbb{T}}^2 \le 32\frac{\ell^2}{\mu k}\log \alpha^{-1}.$$

Thus, using our choice of $\ell = \frac{1}{8}(\mu k)^{1/2}$, we have $G(\xi_1 + \cdots + \xi_\ell) > \alpha$, and so $\xi_1 + \cdots + \xi_\ell \in B_\alpha$. □

Proof of Lemma 10. Letting $g := \mathbb{E}_\xi G = \rho_\mu(v)$, we want to show that $\mathbb{E}_\xi F \le \left(g^{(k-1)/k} + \frac{8}{\sqrt{\mu k}}\right) g + p^{-1}$. We do this in two ranges. First we recall that $F^{1/k} = G$ and so

$$\mathbb{E}_\xi\left[F\mathbf{1}(F \le g)\right] \le \mathbb{E}_\xi\left[G \cdot g^{(k-1)/k}\right] = g^{\frac{2k-1}{k}}.$$

Next we treat the ξ for which $F(\xi) > g$. First note that by Markov's inequality $|B_\alpha| < p$, for all $\alpha > g$. It follows from Claim 11 and the Cauchy-Davenport inequality that $|A_\alpha| \le \ell^{-1}|B_\alpha| + 1$ for all $\alpha > g$. Thus,

$$\mathbb{E}_\xi\left[F\mathbf{1}\left(F > g\right)\right] = \int_g^1 |A_t|p^{-1}\,dt \le \ell^{-1}\int_g^1 |B_t|p^{-1}\,dt + 1/p \le g/\ell + 1/p.$$

Putting our bounds together we have

$$\rho_\mu(v^k) \le \left(g^{(k-1)/k} + \frac{8}{\sqrt{\mu k}}\right) g + 1/p = \left(\rho_\mu(v)^{(k-1)/k} + \frac{8}{\sqrt{\mu k}}\right)\rho_\mu(v) + p^{-1},$$

as desired. □

To complete our proof of Lemma 8, we need the following classical result:

Lemma 12. *If $v \in \mathbb{Z}_p^*$ with $v \ne 0$ then $\rho_\mu(v) \le \frac{64}{\sqrt{\mu|v|}} + p^{-1}$.*

Letting $d = |v|$, this lemma may be deduced by bounding $\rho_\mu(v) \le \rho_\mu(v_j^d)$ for some j by (12), noting that $\rho_\mu(v_j^d) = \rho_\mu(1^d)$ and bounding the latter either directly or using a standard local central limit theorem. Alternatively, a stronger statement may be found in [2, Lemma 2.3].

Proof of Lemma 8. If $\rho_\mu(v) \le (\mu k)^{-1/4}$ then Lemma 10 tells us that $\rho_\mu(v^k) \le 64(\mu k)^{-1/5}\rho_\mu(v) + p^{-1}$, as desired. On the other hand, if $\rho_\mu(v) > (\mu k)^{-1/4}$,

$$\rho_\mu(v^k) = \frac{64}{\sqrt{\mu k|v|}} + 1/p \le 64(\mu k)^{-1/4}\rho_\mu(v) + 1/p$$

thus completing the proof. □

References

[1] Jean Bourgain, Van H. Vu, and Philip Matchett Wood, *On the singularity probability of discrete random matrices*, J. Funct. Anal. **258** (2010), no. 2, 559–603, DOI 10.1016/j.jfa.2009.04.016. MR2557947

[2] Marcelo Campos, Letícia Mattos, Robert Morris, and Natasha Morrison, *On the singularity of random symmetric matrices*, Duke Math. J. **170** (2021), no. 5, 881–907, DOI 10.1215/00127094-2020-0054. MR4255046

[3] Kevin P. Costello, Terence Tao, and Van Vu, *Random symmetric matrices are almost surely nonsingular*, Duke Math. J. **135** (2006), no. 2, 395–413, DOI 10.1215/S0012-7094-06-13527-5. MR2267289

[4] Asaf Ferber and Vishesh Jain, *Singularity of random symmetric matrices—a combinatorial approach to improved bounds*, Forum Math. Sigma **7** (2019), Paper No. e22, 29, DOI 10.1017/fms.2019.21. MR3993806

[5] Asaf Ferber, Vishesh Jain, Kyle Luh, and Wojciech Samotij, *On the counting problem in inverse Littlewood-Offord theory*, J. Lond. Math. Soc. (2) **103** (2021), no. 4, 1333–1362, DOI 10.1112/jlms.12409. MR4273471

[6] Gábor Halász, *On the distribution of additive arithmetic functions*, Acta Arith. **27** (1975), 143–152, DOI 10.4064/aa-27-1-143-152. MR369292

[7] V. Jain, A. Sah, and M. Sawhney, *On the smallest singular value of symmetric random matrices*, preprint `arXiv:2011.02344`, 2020.

[8] V. Jain, A. Sah, and M. Sawhney, *Singularity of discrete random matrices ii*, preprint `arXiv:2010.06554`, 2020.

[9] Jeff Kahn, János Komlós, and Endre Szemerédi, *On the probability that a random* ± 1*-matrix is singular*, J. Amer. Math. Soc. **8** (1995), no. 1, 223–240, DOI 10.2307/2152887. MR1260107

[10] J. Komlós, *On the determinant of* $(0, 1)$ *matrices*, Studia Sci. Math. Hungar. **2** (1967), 7–21. MR221962

[11] Hoi Nguyen and Van Vu, *Optimal inverse Littlewood-Offord theorems*, Adv. Math. **226** (2011), no. 6, 5298–5319, DOI 10.1016/j.aim.2011.01.005. MR2775902

[12] Hoi H. Nguyen, *Inverse Littlewood-Offord problems and the singularity of random symmetric matrices*, Duke Math. J. **161** (2012), no. 4, 545–586, DOI 10.1215/00127094-1548344. MR2891529

[13] Hoi H. Nguyen and Van H. Vu, *Small ball probability, inverse theorems, and applications*, Erdös centennial, Bolyai Soc. Math. Stud., vol. 25, János Bolyai Math. Soc., Budapest, 2013, pp. 409–463, DOI 10.1007/978-3-642-39286-3_16. MR3203607

[14] Mark Rudelson and Roman Vershynin, *The Littlewood-Offord problem and invertibility of random matrices*, Adv. Math. **218** (2008), no. 2, 600–633, DOI 10.1016/j.aim.2008.01.010. MR2407948

[15] Mark Rudelson and Roman Vershynin, *Smallest singular value of a random rectangular matrix*, Comm. Pure Appl. Math. **62** (2009), no. 12, 1707–1739, DOI 10.1002/cpa.20294. MR2569075

[16] Mark Rudelson and Roman Vershynin, *Non-asymptotic theory of random matrices: extreme singular values*, Proceedings of the International Congress of Mathematicians. Volume III, Hindustan Book Agency, New Delhi, 2010, pp. 1576–1602. MR2827856

[17] Terence Tao and Van Vu, *On random* ± 1 *matrices: singularity and determinant*, Random Structures Algorithms **28** (2006), no. 1, 1–23, DOI 10.1002/rsa.20109. MR2187480

[18] Terence Tao and Van Vu, *On the singularity probability of random Bernoulli matrices*, J. Amer. Math. Soc. **20** (2007), no. 3, 603–628, DOI 10.1090/S0894-0347-07-00555-3. MR2291914

[19] Terence Tao and Van Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006, DOI 10.1017/CBO9780511755149. MR2289012

[20] Konstantin Tikhomirov, *Singularity of random Bernoulli matrices*, Ann. of Math. (2) **191** (2020), no. 2, 593–634, DOI 10.4007/annals.2020.191.2.6. MR4076632

[21] Roman Vershynin, *Invertibility of symmetric random matrices*, Random Structures Algorithms **44** (2014), no. 2, 135–182, DOI 10.1002/rsa.20429. MR3158627

[22] Van Vu, *Random discrete matrices*, Horizons of combinatorics, Bolyai Soc. Math. Stud., vol. 17, Springer, Berlin, 2008, pp. 257–280, DOI 10.1007/978-3-540-77200-2_13. MR2432537

Instituto Nacional de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, Brazil
Email address: marcelo.campos@impa.br

School of Mathematics, University of Birmingham, Birmingham, United Kingdom
Email address: m.jenssen@bham.ac.uk

Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, Chicago, Illinois 60607
Email address: michelen.math@gmail.com

Department of Pure Mathematics and Mathematics Statistics (DPMMS), University of Cambridge, Cambridge, United Kingdom
Email address: jdrs2@cam.ac.uk