SINGULARITY OF RANDOM SYMMETRIC MATRICES REVISITED

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

ABSTRACT. Let $M_n$ be drawn uniformly from all $\pm 1$ 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.

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\footnote{See \cite{9} for a short discussion on the history of this conjecture}, to determine the probability that $A_n$ is singular. While a few moments of consideration reveals a natural lower bound of $(1 + o(1))n^22^{-n+1}$, which comes from the probability that two rows or columns are equal up to sign, it is widely believed that in fact

\begin{equation}
\Pr(\det A_n = 0) = (1 + o(1))n^22^{-n+1}.
\end{equation}

This singularity probability was first shown to tend to zero in 1967 by Komlós \cite{10}, who obtained the bound $\Pr(\det(A_n) = 0) = O(n^{-1/2})$. The first exponential upper bound was established by Kahn, Komlós, and Szemerédi \cite{9} in 1995 with subsequent improvements on the exponent by Tao and Vu \cite{17,18} and Bourgain, Vu and Wood \cite{1}. In 2018, Tikhomirov \cite{20} settled this conjecture up to lower order terms by showing $\Pr(\det(A_n) = 0) = (1/2 + o(1))^n$. Very recently, a closely related problem was resolved by Jain, Sah and Sawhney \cite{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 $\Pr(\det M_n = 0) = \Theta(n^22^{-n})$ as in the asymmetric case \cite{2,3,22} although here much less is known. For instance, the fact that $\Pr(\det M_n = 0) = o(1)$, was only resolved in 2005 by Costello, Tao and Vu \cite{8}. Subsequent superpolynomial upper bounds of the form $n^{-C}$ for all $C$ and $\exp(-n^c)$ were proven respectively by

\footnote{The first named author is partially supported by CNPq.}
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, 15, 16].

A combinatorial approach developed by Ferber, Jain, Luh and Samotij [5] was applied by Ferber and Jain [4] in 2018 to prove that
\[ P(\det M_n = 0) \leq \exp(-cn^{1/4}(\log n)^{1/2}) \]
Another combinatorial approach was taken by Campos, Mattos, Morris and Morrison [2] who achieved the bound
\[ P(\det M_n = 0) \leq \exp(-cn^{1/2}) \] 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
\[ P(\det(M_n) = 0) \leq \exp(-c\sqrt{n\log n}) \]

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].

To state this, 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 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 \(\mu\)) as*
\[ N_\mu(w) := \{x \in \mathbb{Z}_p : \mathbb{P}(X_\mu(w) = x) > 2^{-1}\mathbb{P}(X_\mu(w) = 0)\}, \]
which is the set of places where our random walk is “likely” to terminate, relative to 0.

\[ \text{We will also write } \rho_1(v) = \rho(v). \]
Theorem 2. Let $\mu \in (0, 1/4]$, $k, n \in \mathbb{N}$, $p$ prime and $v \in \mathbb{Z}_p^n$. Set $d = \frac{2}{p} \log \rho(v)^{-1}$, suppose that $|v| \geq kd$ and $\rho(v) \geq \frac{k}{p}$. 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

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

In addition to controlling the number of such vectors $v$ with prescribed $\rho(v)$, Theorem 2 gives some further information on the structure of the sets that the $v_i$ belong to, which makes for a simplified application of Theorem 2 in the proof of Theorem 1.

The proof of Theorem 2 has two parts. The first can be found in Section 4 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 [4, 2] 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 $p \approx \exp \left( \frac{c}{2} \sqrt{n \log n} \right)$. 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 tempting 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 [4, 2] 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.

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

$$\sum_{v: \rho(v) \geq \beta} \max_{w \in \mathbb{Z}_p^n} \mathbb{P}(Mv = w) \leq e^{-cn}$$  \hspace{1cm} (3)$$

then for $c' = 2^{-13}$

$$\mathbb{P}(\det(M_n) = 0) \leq \exp(-c' \sqrt{n \log n}).$$
This is essentially Lemma 2.1 in [2], but is implicit in the earlier work of [4] who proved this using the earlier ideas of [3]. We provide the short formal derivation of Lemma 3 from Lemma 2.1 of [2] in Section 3.

With Lemma 3 in hand, our task is now clear: we need to bound the sum on the left hand side of (3). To do this, we invoke our inverse Littlewood-Offord result (Theorem 2, in the form of Lemmas 5 and 6) and prove the following.

**Theorem 4.** 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

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

**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. **Proof of Theorem 2**

In this section we prove Theorem 2 modulo a key Fourier lemma which we postpone to Section 4.

To go further, we introduce a little notation. Let \( \mathbb{Z}_p^n \) denote the set of all vectors of finite dimension with entries in \( \mathbb{Z}_p \). For \( v = (v_1, \ldots, v_k), w = (w_1, \ldots, w_l) \in \mathbb{Z}_p^n \), let \( vw := (v_1, \ldots, v_k, w_1, \ldots, w_l) \) 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 \( w \in \mathbb{Z}_p^n \), 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 \( X_\mu \) is most likely to be found at 0 (see e.g. [19] Corollary 7.12),

\[
\rho_\mu(w) = \mathbb{P}(X_\mu(w) = 0).
\]

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 \( N(w) \). 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

\[
|N(w)| \leq \frac{2}{\rho_\mu(w)}.
\]
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 \( \rho_{\mu} \) [19 Corollary 7.12]: if \( w, v \in \mathbb{Z}_p^* \) where \( w \) is a subvector of \( v \), then
\[
\rho(v) \leq \rho_{\mu}(w) .
\]

**Lemma 5.** 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
\[
|T| \leq \frac{2}{\mu} \log \frac{1}{\rho_{\mu}(v)}. \tag{6}
\]

**Proof.** We build a sequence of sets \( T_1, \ldots, T_d \subseteq [n] \) 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 \( v_{T_t} = (x_1, \ldots, x_t) \). Pick \( i \in [n]\setminus T_t \) such that
\[
\rho_{\mu}(x_1 \ldots xTv_i) \leq (1 - \mu/2)\rho_{\mu}(x_1 \ldots x_t). \tag{7}
\]

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 \( v_T = (x_1, \ldots, x_d) \). By the termination condition, we have that for \( i \in [n]\setminus T \)
\[
\rho_{\mu}(x_1 \ldots xTv_i) > (1 - \mu/2)\rho_{\mu}(x_1 \ldots x_t). \tag{8}
\]

Conditioning on the coefficient of \( v_i \) and using that \( \mathbb{P}(X_{\mu}(x_1 \ldots x_d) = v_i) = \mathbb{P}(X_{\mu}(x_1 \ldots x_d) = -v_i) \) by symmetry, we can rewrite the left hand side to obtain
\[
\mu\mathbb{P}(X_{\mu}(x_1 \ldots x_d) = v_i) + (1 - \mu)\rho_{\mu}(x_1 \ldots x_d) > (1 - \mu/2)\rho_{\mu}(x_1 \ldots x_d). \tag{9}
\]

Rearranging shows \( v_i \in N(v_T) \). For the bound on \( d = |T| \), observe that by (5), inequality (7) and the fact that \( \rho_{\mu}(x_1) = (1 - \mu) \) we have
\[
\rho_{\mu}(v) \leq \rho_{\mu}(x_1 \ldots x_d) \leq (1 - \mu/2)^d \leq e^{-\mu d/2}. \tag{10}
\]

The next lemma shows that we can improve Lemma 5 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. In fact, if one only wanted to prove a bound of the form \( \exp(-cn^{1/2}) \) using our method, one needs only to use Lemma 5 along with a simplified Fourier argument.
For this lemma we need the following property of \( \rho_\mu \), which can be found in [19, Corollary 7.12]. Let \( w_1, \ldots, w_k \in \mathbb{Z}_p^* \) and \( \mu \in (0,1/2) \) then

\[
\rho_\mu(w_1 \cdots w_k) \leq \max_{j \in [k]} \rho_\mu(w_j^k).
\]

**Lemma 6.** Let \( \mu \in (0,1/4], n \in \mathbb{N} \) and \( v \in \mathbb{Z}_p^* \). Set \( d = \frac{2}{\mu} \log \rho_\mu(v)^{-1} \) and let \( k \in \mathbb{N} \) be such that \( kd \leq n \). Then there exists \( T \subseteq S \subseteq [n] \) with \( |T| \leq d \), \( |S| \leq kd \) such that \( v_i \in N(v_T) \) for all \( i \notin S \) and \( \rho_\mu(v_S) \leq \rho_\mu(v_T^k) \).

**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 \( v_{T_j} = (x_1, \ldots, x_{d(j)}) \) given by Lemma 5 applied to \( v_{A_j} \) and let

\[
A_{j+1} = A_j \setminus T_j \quad \text{and} \quad S = \bigcup_{j=1}^k T_j.
\]

By Lemma 5 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 \( 1 \leq j \leq k+1 \), \( v_i \in N(v_{T_j}) \) for all \( i \notin S \) and \( 1 \leq j \leq k \). Note also that \( |T_j| \leq d \) for all \( 1 \leq j \leq k \).

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 (8) we have

\[
\rho_\mu(v_S) \leq \max_{1 \leq j \leq k} \rho_\mu(v_{T_j}^k) = \rho_\mu(v_T^k).
\]

□

To conclude the proof of our Theorem 2—and to understand the strength of Lemma 6—we introduce our main Fourier ingredient, the proof of which is found in Section 4.

**Lemma 7.** Let \( \mu \in (0,1/4], k \in \mathbb{N} \) and \( v \in \mathbb{Z}_p^* \) such that \( |v| \neq 0 \). Then

\[
\rho_\mu(v^k) \leq 64k^{-1/5} \rho_\mu(v) + p^{-1}.
\]

**Proof of Theorem 2.** Let \( k, n \in \mathbb{N} \) and \( v \in \mathbb{Z}_p^* \) be as in the theorem statement. By Lemma 6 there exists \( T \subseteq S \subseteq [n] \) with \( |T| \leq d \), \( |S| \leq kd \) such that \( v_i \in N(v_T) \) for all \( i \notin S \) and \( \rho_\mu(v_S) \leq \rho_\mu(v_T^k) \). Moreover, since \( |v| \geq kd \), the support of \( v_T \) is non-zero. Applying Lemma 7 we conclude that

\[
\rho_\mu(v_S) \leq \rho_\mu(v_T^k) \leq 64k^{-1/5} \rho_\mu(v_T) + p^{-1}.
\]

By (5) and (6) we then have

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

where on the final bound we use that \( \rho_\mu(v) \geq \frac{2}{p} \) □
3. Proof of Theorem 1

In this section we prove Theorem 4 which, from the discussion in the introduction, implies Theorem 1. As we were a bit quick with this discussion, we take a moment to spell out the proof of this implication.

Define

\[ q_n(\beta) := \max_{w \in \mathbb{Z}_p^n} \mathbb{P}(\exists v \in \mathbb{Z}_p^n \setminus \{0\} : M \cdot v = w \text{ and } \rho(v) \geq \beta) \]

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

**Lemma 8.** Let \( n \in \mathbb{N} \) and \( p > 2 \) be a prime. Then for every \( \beta > 0 \)

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

Our Lemma 3 follows easily.

**Proof of Lemma 3.** Pick a prime \( p = t \exp(c \sqrt{n \log n}) \) with \( c = 1/800 \) and \( t \in [1/2, 1] \). Looking to apply Lemma 8 with \( \beta = \Theta(n/p) \), we apply the union bound to \( q_n(\beta) \) and our assumption for each \( n-1 \leq m \leq 2n-3 \) to bound

\[
q_n(\beta) \leq \sum_{w : \rho(v) \geq \beta} \max_{w \in \mathbb{Z}_p^n} \mathbb{P}(Mv = w) \leq e^{-cn}.
\]

Thus, we apply Lemma 8 to obtain

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

for \( n \) sufficiently large. \( \square \)

With these reductions firmly in-hand, we turn to prove Theorem 4 and therefore Theorem 1.

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

Our task is to bound

\[ Q_n(\beta) := \sum_{v \in \mathcal{V}} \max_w \mathbb{P}(M_n \cdot v = w). \tag{9} \]

We start our analysis of (9) 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 6 to obtain \( S, T \subseteq [n] \). We then apply Lemma 5 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 (9) as

\[ Q_n(\beta) = \sum_{s \in \mathcal{S}} \sum_{v \in f^{-1}(s)} \max_w \mathbb{P}(M_n \cdot v = w). \tag{10} \]
Note that if \( s = (S, T, T', w_1, w_2) \in S \), then

\[
|S| \leq kd, \quad |w_1|, |w_2| \leq d, \quad \rho_\mu(w_1) \geq \beta, \quad \rho_\mu(w_2) \leq (1 - \mu/2)|w_2| \quad \text{and} \quad w_2 \neq 0
\]

by Lemmas 5 and 6 together with (6), and note that we have the bound

\[
|S| \leq 8^n p^{2d},
\]

since there are \( 8^n \) choices for \( S, T, T' \) and at most \( p^{2d} \) choices for \( w_1, w_2 \).

We now turn to bounding a given term in the sum (10), based on which piece of the partition it is in. Let \( s = (S, T, T', w_1, w_2) \in S \) and \( v \in f^{-1}(s) \). For any \( w \in \mathbb{Z}_p^n \), we bound \( \mathbb{P}(M_n \cdot v = w) \) by first revealing the rows indexed by \( S^c \) and then revealing the rows indexed by \( S \setminus T' \),

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

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

\[
\mathbb{P}(M \cdot v = w) \leq \max_u \mathbb{P}(M_{(S \setminus T') \times T'} \cdot v_{T'} = u) \cdot \max_u \mathbb{P}(M_{S^c \times S} \cdot v_S = u).
\]

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

\[
\mathbb{P}(M \cdot v = w) \leq \rho(v_{T'})^{|S| - |T'|} \rho(v_{S})^{n - |S|} \leq \rho_\mu(v_{T'})^{|S| - |T'|} \rho_\mu(v_{S})^{n - |S|},
\]

where this last inequality follows from the monotonicity of \( \rho \) in the parameter \( \mu \), noted at (6).

We now bound the size of a piece of our partition \(|f^{-1}(s)|\). By (5) together with Lemmas 5 and 6, the number of choices for \( v_{S^c} \) and \( v_{S \setminus T'} \) are (respectively) at most

\[
|N(w_1)|^{n - |S|} \leq \left(\frac{2}{\rho_\mu(w_1)}\right)^{n - |S|}, \quad |N(w_2)|^{|S| - |T'|} \leq \left(\frac{2}{\rho_\mu(w_2)}\right)^{|S| - |T'|},
\]

so that

\[
|f^{-1}(s)| \leq \left(\frac{2}{\rho_\mu(w_1)}\right)^{n - |S|} \cdot \left(\frac{2}{\rho_\mu(w_2)}\right)^{|S| - |T'|}.
\]

By (13) and the fact that \(|S| \leq kd = o(n)\) (by our choice of parameters), we have

\[
\sum_{v \in f^{-1}(s)} \max_w \mathbb{P}(M_n \cdot v = w) \leq 2^n \left(\frac{\rho_\mu(w_1^k)}{\rho_\mu(w_1)}\right)^{n - |S|} \leq 2^n \left(\frac{\rho_\mu(w_1^k)}{\rho_\mu(w_1)}\right)^{24n/25}.
\]

We consider first the case where \(|w_1| \neq 0\); then we may apply Lemma 7 to obtain the bound

\[
\rho_\mu(w_1^k) \leq 64(\mu k)^{-1/5} \rho_\mu(w_1) + \frac{1}{p}.
\]
By the bound $\rho_{\mu}(w_1) \geq \beta = \Theta(n/p)$, we then have
\[
\frac{\rho_{\mu}(w_k)}{\rho_{\mu}(w_1)} \leq 64(\mu k)^{-1/5} + \Theta(n^{-1}) \leq n^{-1/24}.
\]
Combining this with (12) and (15) shows that
\[
\sum_{s \in S, v \in f^{-1}(s), |w_1| \neq 0} \max_w \mathbb{P}(M_n \cdot v = w) \leq |S| \cdot n^{-n/25} \leq 8^n p^{2d_n} n^{-n/25}
\]
(16) \leq 8^n \exp \left( \frac{4c}{\mu} n \log n - \frac{1}{25} n \log n \right) \leq e^{-n},

provided $c \leq \mu/200$. Now if $|w_1| = 0$ then there are at most
\[
|f^{-1}(s)| \leq \left( \frac{2}{\rho_{\mu}(w_2)} \right)^{|S| - |T'|}
\]
choices for $v$. Notice that $\rho_{\mu}(v S) \leq \rho_{\mu}(w_2)$ and so
\[
\sum_{v \in f^{-1}(s)} \max_w \mathbb{P}(M_n \cdot v = w) \leq \rho_{\mu}(w_2)^n \left( \frac{1}{\rho_{\mu}(w_2)} \right)^{|S| - |T'|} \leq \rho_{\mu}(w_2)^n / 2 \leq \left( 1 - \frac{\mu}{2} \right)^{|w_2|/2},
\]
where for the final inequality we used (11). On the other hand, by (11), the number of choices for
$s = (S, T, T', w_1, w_2)$ such that $|w_1| = 0, |w_2| = t$ is at most
\[
\left( \frac{n}{k d} \right)^t \leq \exp(\sqrt{n \log n} + 3 k d \log n).
\]
Putting our bounds together, we have
\[
\sum_{s \in S, v \in f^{-1}(s), |w_1| = 0, |w_2| = t} \max_w \mathbb{P}(M_n \cdot v = w) \leq \exp(\sqrt{n \log n} + 3 k d \log n - n \mu t/4) \leq e^{-n \mu t/5}.
\]
Summing over all $t \geq 1$ (recalling that $w_2 \neq 0$) and using (16), we conclude that
\[
Q_n(\beta) = \sum_{s \in S} \sum_{v \in f^{-1}(s)} \max_w \mathbb{P}(M_n \cdot v = w) \leq e^{-\mu n/6},
\]
as desired. \[\square\]

4. Proof of Lemma 7

In this section, we pin down one final loose end, the proof of Lemma 7 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
\[
f_{\mu,v}(\xi) := \prod_{i=1}^n ((1 - \mu) + \mu c_p(v_i, \xi)),
\]
where $c_p(v_i, \xi)$ is the inner product of $v_i$ and $\xi$ modulo $p$. We have that
\[
f_{\mu,v}(\xi) = \exp \left( -2\pi i \sum_{i=1}^n \mu v_i \xi i \right).
\]
where we let \( c_p(x) = \cos(2\pi x/p) \). We then have
\[
(18) \quad \rho_\mu(v) = \mathbb{E}_{\xi \in \mathbb{Z}_p} f_{\mu,v}(\xi).
\]
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 \(|x|_T\) 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
\[
(19) \quad \mu|x/p|_T^2 \leq -\log \left(1 - \mu + \mu c_p(x)\right) \leq 32\mu|x/p|_T^2,
\]
which are elementary and can be found in (7.1) in [19].

For the following lemma, 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 7 is to prove it in the case when \( \rho_\mu(v) \) is not too large.

**Lemma 9.** Let \( \mu \in (0, 1/4] \), \( v \in \mathbb{Z}_p^* \) and \( k \in \mathbb{N} \). Then
\[
(20) \quad \rho_\mu(v^k) \leq \left( \rho_\mu(v)^{\frac{k-1}{k}} + \frac{8}{\sqrt{\mu k}} \rho_\mu(v) \right)^k + p^{-1}.
\]
To prove this lemma, we adopt some temporary notation. Let \( F = f_{\mu,v^k} \) and \( G = f_{\mu,v} \), be as defined in (17) 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
\[
A_\alpha := \{\xi \in \mathbb{Z}_p : F(\xi) > \alpha\} \quad B_\alpha := \{\xi \in \mathbb{Z}_p : G(\xi) > \alpha\}.
\]

**Claim 10.** For \( \alpha \in (0, 1) \), we have \( \ell \cdot A_\alpha \subseteq B_\alpha \).

**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 (19) gives, for each \( i \in [\ell] \),
\[
(20) \quad \mu \sum_{j=1}^{n} \|\xi_j v_j\|_T^2 \leq -\log G(\xi_i) \leq k^{-1} \log \alpha^{-1}.
\]
Thus, using the triangle inequality along with (20) gives
\[
\left( \sum_{j=1}^{n} \|\xi_1 + \cdots + \xi_\ell v_j\|_T^2 \right)^{1/2} \leq \sum_{i=1}^{\ell} \left( \sum_{j=1}^{n} \|\xi_j v_j\|_T^2 \right)^{1/2} \leq \ell \left( \frac{\log \alpha^{-1}}{\mu k} \right)^{1/2}.
\]
It then follows from the upper bound in (19) that
\[
-\log G(\xi_1 + \cdots + \xi_\ell) \leq 32 \sum_{j=1}^{n} \|\xi_1 + \cdots + \xi_\ell v_j\|_T^2 \leq 32 \ell^2 \frac{\log \alpha^{-1}}{\mu k}.
\]

\(^3\)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 \(|x| \leq 1/2\).
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 9.** Letting $g := \mathbb{E}_\xi G = \rho_\mu(v)$, we want to show that $\mathbb{E}_\xi F \leq \left( (g^{(k-1)/k} + \frac{8}{\sqrt{\mu k}}) \right) g + p^{-1}$. We do this in two ranges. First we recall that $F^{1/k} = G$ and so

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

Next we treat the $\xi$ for which $F(\xi) > g$. First note that by Markov’s inequality $|B_\alpha| < p$, for all $\alpha > g$. It follows from Claim 10 and the Cauchy-Davenport inequality that $|A_\alpha| \leq \ell - 1 |B_\alpha| + 1$ for all $\alpha > g$. Thus,

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

Putting our bounds together we have

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

as desired. □

To complete our proof of Lemma 7, we need the following classical result:

**Lemma 11.** If $v \in \mathbb{Z}_p^*$ with $v \neq 0$ then $\rho_\mu(v) = \frac{64}{\sqrt{\mu |v|}} + p^{-1}$.

Letting $d = |v|$, this lemma may be deduced by bounding $\rho_\mu(v) \leq \rho_\mu(v^d_j)$ for some $j$ by (8), noting that $\rho_\mu(v^d_j) = \rho_\mu(1^d)$ 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 7.** If $\rho_\mu(v) \leq (\mu k)^{-1/4}$ then Lemma 9 tells us that $\rho_\mu(v^k) \leq 64(\mu k)^{-1/5} \rho_\mu(v) + p^{-1}$, as desired. On the other hand, if $\rho_\mu(v) > (\mu k)^{-1/4}$,

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

thus completing the proof. □

**References**

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

[2] M. Campos, L. Mattos, R. Morris, and N. Morrison. On the singularity of random symmetric matrices. *arXiv preprint arXiv:1904.11478*, 2019.

[3] K. P. Costello, T. Tao, and V. Vu. Random symmetric matrices are almost surely nonsingular. *Duke Math. J.*, 135(2):395–413, 2006.

[4] A. Ferber and V. Jain. Singularity of random symmetric matrices—a combinatorial approach to improved bounds. *Forum Math. Sigma*, 7:Paper No. e22, 29, 2019.
[5] A. Ferber, V. Jain, K. Luh, and W. Samotij. On the counting problem in inverse littlewood–offord theory. arXiv preprint arXiv:1904.10425, 2019.

[6] G. Halász. On the distribution of additive arithmetic functions. Acta Arithmetica, 1(27):143–152, 1975.

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

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

[9] J. Kahn, J. Komlós, and E. Szemerédi. On the probability that a random ±1-matrix is singular. J. Amer. Math. Soc., 8(1):223–240, 1995.

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

[11] H. Nguyen and V. Vu. Optimal inverse Littlewood-Offord theorems. Adv. Math., 226(6):5298–5319, 2011.

[12] H. H. Nguyen. Inverse Littlewood-Offord problems and the singularity of random symmetric matrices. Duke Math. J., 161(4):545–586, 2012.

[13] H. H. Nguyen and V. H. Vu. Small ball probability, inverse theorems, and applications. In Erdős centennial, volume 25 of Bolyai Soc. Math. Stud., pages 409–463. János Bolyai Math. Soc., Budapest, 2013.

[14] M. Rudelson and R. Vershynin. The Littlewood-Offord problem and invertibility of random matrices. Adv. Math., 218(2):600–633, 2008.

[15] M. Rudelson and R. Vershynin. Smallest singular value of a random rectangular matrix. Comm. Pure Appl. Math., 62(12):1707–1739, 2009.

[16] M. Rudelson and R. Vershynin. Non-asymptotic theory of random matrices: extreme singular values. In Proceedings of the International Congress of Mathematicians. Volume III, pages 1576–1602. Hindustan Book Agency, New Delhi, 2010.

[17] T. Tao and V. Vu. On random ±1 matrices: singularity and determinant. Random Structures Algorithms, 28(1):1–23, 2006.

[18] T. Tao and V. Vu. On the singularity probability of random Bernoulli matrices. J. Amer. Math. Soc., 20(3):603–628, 2007.

[19] T. Tao and V. H. Vu. Additive combinatorics, volume 105. Cambridge University Press, 2006.

[20] K. Tikhomirov. Singularity of random Bernoulli matrices. Ann. of Math. (2), 191(2):593–634, 2020.

[21] R. Vershynin. Invertibility of symmetric random matrices. Random Structures Algorithms, 44(2):135–182, 2014.

[22] V. Vu. Random discrete matrices. In Horizons of combinatorics, volume 17 of Bolyai Soc. Math. Stud., pages 257–280. Springer, Berlin, 2008.

INSTITUTO NACIONAL DE MATEMÁTICA PURA E APlicada (IMPA).

Email address: marcelo.campos@impa.br

UNIVERSITY OF BIRMINGHAM, SCHOOL OF MATHEMATICS.

Email address: m.jenssen@bham.ac.uk

UNIVERSITY OF ILLINOIS AT CHICAGO. DEPARTMENT OF MATHEMATICS, STATISTICS AND COMPUTER SCIENCE.

Email address: michelen.math@gmail.com

UNIVERSITY OF CAMBRIDGE. DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICS STATISTICS (DPMMS).

Email address: jdrs2@cam.ac.uk