A bound on a moment-like quantity in random matrix theory

Nikita Lvov[*]

May 8, 2025

Abstract

In this short note we prove a general inequality for random matrices with i.i.d entries over local rings. This inequality will prove central in the forthcoming dynamic proof of universality for random matrices over local rings. This inequality bounds a quantity, that measures the average number of surjections to a module M from the cokernel of a random matrix, in a certain large deviation regime. Thus, the quantity we bound is related to, but is distinct from the M-moment of the cokernel of the random matrix.

1 Introduction

Let R be a local ring and let u be a fixed integer. Suppose that $\mathcal{M}_{n,n+u}$ is a random matrix whose entries are i.i.d. random variables, denoted by ξ_{ij}. Then

$$coker(\mathcal{M}_{n,n+u})$$

is a random R-module. Let M be a finite R-module. The *M-moment* of the random module $coker(\mathcal{M}_{n,n+u})$ is defined to be:

$$\mathbb{E}\Big(\#Sur\big(coker(\mathcal{M}_{n,n+u}), M\big)\Big). \tag{1.1}$$

The moment method, pioneered in [Woo17], uses the calculation of M-moments for all M as $n \to \infty$ to determine the asymptotic distribution of $coker(\mathcal{M}_{n,n+u})$. This method has by now been used to establish the universality of cokernels of random matrices in a wide range of settings. See [Woo23, §2 and §3] for a fairly recent survey.

In a forthcoming paper, we re-prove and extend some known universality results using a different approach to random matrix theory, based on the Lindeberg Replacement Technique ([TV11] [Lin22]). This is a close relative of the approach in [Map13]. Our approach does not use the moment method, but nonetheless requires a bound on a quantity, (1.4), that is closely connected to (1.1). This paper will focus on bounding the quantity (1.4), which we define below.

[*] nikita.lvov@mail.mcgill.ca

The quantity that we wish to bound. To put our estimate in context, we give a rough outline of how one would go about calculating the moment (1.1). By a standard manipulation, (1.1) can be re-written as a sum over $f \in Sur(R^n, M)$:

$$\sum_{f \in Sur(R^n,M)} \mathbb{P}\Big(f\left(\mathcal{M}_{n,n+u}\right) = 0\Big) \tag{1.2}$$

where $f(\mathcal{M}) = 0$ means that the evaluation of f on every column vector of $\mathcal{M}$ is 0.

When applying the moment method,

(A) we wish to establish that for *most* f, and under certain mild conditions on the distribution of ξ,

$$\mathbb{P}(f(\mathcal{M}_{n,n+u}) = 0) \approx \frac{1}{|M|^{n+u}}, \tag{1.3}$$

(B) it is necessary to show that those f for which (1.3) does not hold, have a negligible contribution to the sum (1.2).

In our approach, we are interested *solely* in the part (B), i.e. the contribution of those f for which

$$\mathbb{P}\big(f(\mathcal{M}_{n,n+u}) = 0\big)$$

is atypically large. Specifically, we are interested in the quantity:

$$\sum_{f \in Sur(R^n,M)} \max\left(\mathbb{P}\big(f(\mathcal{M}_{n,n+u}) = 0\big) - \left(\frac{1+\epsilon_0}{|M|}\right)^{n+u}, 0\right) \tag{1.4}$$

The main theorem we establish is that under the condition that R is a local ring, and under certain conditions[1] on ξ, (1.4) decreases exponentially with n, for any ϵ_0:

Theorem 1.1. *Suppose that R is a local ring. Suppose that the support of ξ is not concentrated on the translate of a subring or the translate of an ideal of R. Then, for any finite module M, (1.4) decreases exponentially with n.*

We give a quantitative statement below.

Definition. Define β such that:

$$\max\left(\left|\left|\xi \mod \mathfrak{m}\right|\right|_{l^\infty}, \frac{1}{char(R/\mathfrak{m})}\right) = 1 - \beta$$

where $\mathfrak{m}$ is the maximal ideal of R and l^∞ refers to the l^∞ (or *sup*) norm of the probability distribution, that ξ induces on $R/\mathfrak{m}$.

[1] We believe these conditions to be necessary.

Theorem 1.2. *For any positive ϵ', (1.4) is bounded above by*

$$O\Big((1-\beta)^n(1+\epsilon')^n\Big). \tag{1.5}$$

The implied constant depends on ϵ', M and u, and the minimal non-zero value of

$$\mathbb{P}(\xi \equiv r \mod ann\, M)\, r \in R. \tag{1.6}$$

Remark. More succinctly, we could say that the implied constant depends only on ϵ', M and u, and the distribution of $\mathbb{P}(\xi \equiv r \mod \operatorname{ann} M)$. We have chosen the formulation above to be precise. In the sequel, we will use the symbol

$$\alpha$$

to denote (1.6).

Remark. Although we will prove Theorem 1.2 for all M, in our application to random matrices, we will need to know the result only for the modules M that satisfy:

$$Hom(k, M) \cong k$$

where k is the residue field of R.

1.1 Approach

First of all, we can use independence to rewrite (1.4) as

$$\sum_{\substack{m_i \in M \\ span(m_i)=M}} \max\left(\prod_j \mathbb{P}\left(\sum_i m_i\xi_{ij} = 0\right) - \left(\frac{1+\epsilon_0}{|M|}\right)^{n+u}, 0\right) \leq$$

$$\leq \sum_{\substack{m_i \in M \\ span(m_i)=M}} \max\left(\prod_j \Big|\Big|\sum_i m_i\xi_{ij}\Big|\Big|_{l^\infty} - \left(\frac{1+\epsilon_0}{|M|}\right)^{n+u}, 0\right) =$$

$$= \sum_{\substack{m_i \in M \\ span(m_i)=M}} \max\left(\Big|\Big|\sum_i m_i\xi_{i1}\Big|\Big|_{l^\infty}^{n+u} - \left(\frac{1+\epsilon_0}{|M|}\right)^{n+u}, 0\right) \tag{1.7}$$

For notational convenience, we will denote ξ_{i1} as ξ_i.

Remark. We will henceforth be interested in proving that the sum (1.7) is bounded above by (1.5). Theorem 1.2 will immediately follow from this bound.

Remark. As we are now only interested in (1.7), we can make a simplifying assumption.

- Note that the value of (1.7) does not change if we translate the distribution of ξ by $r \in R$, or if we multiply the distribution by a unit in R. Furthermore, the condition that ξ is not supported on the translate of a subring also does not change under these operations.

- Note that the support of ξ is not concentrated on the translate of an ideal. Hence it must contain two elements whose difference is not in $\mathfrak{m}$ and is hence a unit. Therefore, after translating and multiplying by a unit, we can arrange for the support of the new random variable to contain 0 and 1.

Hence, in bounding (1.7), we can assume, from now on, that

$$\text{the support of } \xi \text{ contains 0 and 1.} \tag{1.8}$$

1.2 Strategy

Definition. For the rest of this paper, we choose ϵ such that

$$0 < \epsilon < \epsilon_0$$

We estimate (1.7) by separating the sum into three components, based on the Fourier transform of the random variable:

$$\sum_i m_i \xi_i. \tag{1.9}$$

Type 1 We will say that $\{m_i\}$ is of Type 1 if the non-trivial values of the Fourier transform of

$$\sum_i m_i \xi_i$$

are bounded above by $\epsilon/|M|$ in absolute value.

Type 2 We say that $\{m_i\}$ is of Type 2 if all the values of the Fourier transform of

$$\sum_i m_i \xi_i$$

are *either* 1 *or* are bounded above by $\epsilon/|M|$ in absolute value.

Type 3 Otherwise, we say that $\{m_i\}$ is of Type 3.

If $\{m_i\}$ is of type j, for $j = 1, 2, 3$ we will write $\{m_i\} \in \mathcal{C}_j$.

We will call the values of the Fourier transform "small", if they are bounded above by $\epsilon/|M|$. We will call the values of the Fourier transform "large" if they are not "small" and do not have absolute value equal to 1. Finally, we remark that because of (1.8), all the random variables we consider in subsequent sections contain 0 in their support. Therefore, if the Fourier transform of such a variable has absolute value 1, then it must equal 1.

In the ensuing sections, we will bound the contributions from $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_3$, separately. Indeed, as we shall see, $\mathcal{C}_1$ does not contribute, and the contributions from $\mathcal{C}_2$ and $\mathcal{C}_3$ are each bounded above by (1.5).

1.3 Outline

In the first section, we will define the notion of ϵ-equidistribution and establish some basic facts. In the subsequent sections, we analyze successively the contributions from $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_3$.

2 The notion of ϵ-equidistribution

Definition. We say that a random variable ζ is ϵ-equidistributed on a finite abelian group G if every non-trivial Fourier coefficient of ζ is bounded above by $\epsilon/|G|$.

Lemma 2.1. *If ζ is ϵ-equidistributed on G, then*

$$\Big|\Big|\zeta\Big|\Big|_{l^\infty} = \max_{g\in G} I\!P(\zeta = g) \leq \frac{1+\epsilon}{|G|}$$

Proof. This follows readily from the inverse Fourier transform. □

We say that a G-valued random variable is ϵ-equidistributed on a subgroup π of G if ζ is supported on π and ϵ-equidistributed on π. In §5, we will use the following estimate.

Theorem 2.2. *Suppose that ζ_1 and ζ_2 are G-valued random variables. Now suppose that ζ_2 is ϵ-equidistributed on a subgroup π of G. Then,*

$$I\!P(\zeta_1 + \zeta_2 = g) \leq (1+\epsilon)\left(\frac{I\!P(\zeta_1 \equiv g \mod \pi)}{|\pi|}\right)$$

Lemma 2.3. *If ζ and ζ' are two independent random variables supported on π, and ζ is ϵ-equidistributed on π, then $\zeta+\zeta'$ is ϵ-equidistributed on π.*

Proof. (of Lemma 2.3) This follows from the multiplicativity of the Fourier transform. □

Proof. (of Theorem 2.2) We rewrite

$$\mathbb{P}(\zeta_1 + \zeta_2 = g) = \mathbb{P}(\zeta_1 - g + \zeta_2 = 0) =$$

$$\mathbb{P}\big(\zeta_1 - g + \zeta_2 \equiv 0 \mod \pi | \zeta_1 \equiv g \mod \pi\big)\mathbb{P}\big(\zeta_1 \equiv g \mod \pi\big)$$

After we condition on $\zeta_1 - g \cong 0 \mod \pi$, both $\zeta_1 - g$ and ζ_2 are independent random variables supported on π. Hence, we can apply Lemma 2.3 to deduce Theorem 2.2. □

3 Sum over $\mathcal{C}_1$

Lemma 3.1. *If $\{m_i\} \in \mathcal{C}_1$,*

$$\Big|\Big|\sum_i m_i\xi_i\Big|\Big|_{l^\infty}^{n+u} < \left(\frac{1+\epsilon_0}{|M|}\right)^{n+u}$$

Corollary. *If $\{m_i\} \in \mathcal{C}_1$, $\{m_i\}$ does not contribute to (1.7).*

Proof. Suppose that $\{m_i\} \in \mathcal{C}_1$. Therefore, the non-trivial Fourier coefficients of

$$\sum m_i \xi_i \tag{3.1}$$

are bounded uniformly in absolute value by $\frac{\epsilon}{|M|}$. Then, by Lemma 2.1,

$$\left|\left|\sum m_i \xi_i\right|\right|_{l^\infty} \leq \frac{1+\epsilon}{|M|}$$

and therefore:

$$\left|\left|\sum m_i \xi_i\right|\right|_{l^\infty}^{n+u} \leq \left(\frac{1+\epsilon}{|M|}\right)^{n+u} < \left(\frac{1+\epsilon_0}{|M|}\right)^{n+u}$$

□

4 Sum over $\mathcal{C}_2$

Recall that ξ_i are identically distributed R-valued random variables, whose support is not contained in the translate of any proper subring of R. By (1.8), we can assume that the support of ξ_i contains 0 and 1.

Recall that $\mathcal{C}_2$ is defined to consist of n-tuples of elements of M, spanning M, such that:

- Every Fourier coefficient of the random variable

  $$\sum_i m_i \xi_i$$

  is either equal to 1, or bounded above in absolute value by:

  $$\frac{\epsilon}{|M|}.$$

- At least one non-trivial Fourier coefficient is equal to 1.

We have the following theorem:

Theorem 4.1.

$$\sum_{\{m_i\} \in \mathcal{C}_2} \left|\left|\sum_i m_i \xi_i\right|\right|_{l^\infty}^{n+u} \lesssim \left(\frac{1+\epsilon}{char(R/\mathfrak{m})}\right)^n$$

where the implied constant depends only on M and u.

Lemma 4.2. *Suppose that $\{m_i\} \in \mathcal{C}_2$. There is a proper additive subgroup $\pi_{\{m_i\}}$ of M such that:*

- *The random variables $m_i \xi_i$ are supported on $\pi_{\{m_i\}}$.*
- *We have the bound*

  $$\left|\left|\sum_i m_i \xi_i\right|\right|_{l^\infty} \leq \frac{1+\epsilon}{|\pi_{\{m_i\}}|}$$

Proof. Indeed, if a non-trivial Fourier coefficient is equal to 1, then the random variable:

$$\sum_i m_i \xi_i \tag{4.1}$$

is supported on the kernel of the corresponding homomorphism to $\mathbb{C}^*$. Therefore, the support of (4.1) is contained in a proper additive subgroup of M. Denote by $\pi_{\{m_i\}}$ the smallest additive subgroup that contains the support of (4.1).

Claim. *The Fourier coefficients of (4.1), regarded as a random variable valued in $\pi_{\{m_i\}}$ are a subset of the Fourier coefficients of (4.1), regarded as a random variable valued in M.*

The claim follows from the fact that $\mathbb{Q}/\mathbb{Z}$ is injective in the category of abelian groups. Therefore, any homomorphism in $Hom(\pi, \mathbb{C}^*) \cong Hom(\pi_m, \mathbb{Q}/\mathbb{Z})$ can be extended to a homomorphism in $Hom(M, \mathbb{C}^*) \cong Hom(M, \mathbb{Q}/\mathbb{Z})$.

It follows from the claim that all the non-trivial Fourier coefficients of (4.1), regarded as a random variable valued in $\pi_{\{m_i\}}$, are either equal to 1 or bounded above by $\epsilon \Big/ |M|$. But by the minimality of $\pi_{\{m_i\}}$, none of the non-trivial Fourier coefficients can be equal to 1. It follows that the random variable (4.1) is ϵ-equidistributed on $\pi_{\{m_i\}}$. Therefore, by Lemma 2.1

$$\Big|\Big| \sum_i m_i \xi_i \Big|\Big|_{l^\infty} \leq \frac{1+\epsilon}{|\pi_{\{m_i\}}|}$$

□

Corollary.

$$\sum_{\{m_i\} \in \mathcal{C}_2} \Big|\Big| \sum_i m_i \xi_i \Big|\Big|_{l^\infty}^{n+u} \leq \sum_{\{m_i\} \in \mathcal{C}_2} \left(\frac{1+\epsilon}{|\pi_{\{m_i\}}|} \right)^{n+u} \tag{4.2}$$

The right hand side of (4.2) is bounded above by:

$$\sum_{\substack{\pi \subset M \\ \pi \neq M}} \left(\frac{1+\epsilon}{|\pi|} \right)^{n+u} \# \left\{ \{m_i\} \subset \mathcal{C}_2 \Big| support \left(\sum_i m_i \xi_i \right) \in \pi \right\} \leq$$

$$\leq \sum_{\substack{\pi \subset M \\ \pi \neq M}} \left(\frac{1+\epsilon}{|\pi|} \right)^{n+u} \# \left\{ \{m_i\} \Big| span\{m_i\} = M; support \left(\sum_i m_i \xi_i \right) \in \pi \right\}$$

Lemma 4.3. *Suppose that the n-tuple $\{m_i\}$ spans M, and*

$$support \left(\sum_i m_i \xi_i \right) \in \pi.$$

If $\pi \neq M$, then π is not an R-module.

Proof. Because the support of ξ_i contains 0 and 1, it follows that the support of

$$\sum_i m_i \xi_i$$

contains m_i for all i. It follows that $m_i \in \pi$. The smallest R-module that contains m_i for all i is M. Hence, if $\pi \neq M$, then π is not an R-module. □

Lemma 4.4. *Suppose that S is a subset of R that contains* 1 *and that is not contained in any proper subring of R. Suppose that π is any additive subgroup of M. Then,*

$$\left\{ m \in M \middle| mS \in \pi \right\} \in \pi$$

where equality holds if and only if π is an R-module.

Proof. The inclusion holds because $1 \in S$. If π is an R-module, then we have equality. Conversely, suppose that we have equality. Then,

$$\pi S = \pi.$$

Therefore, S is contained in the stabilizer of π, which is a subring of R. Since S is not contained in any proper subring of R, the stabilizer of π must be R. □

Corollary. *Suppose that π is not an R-module. Then,*

$$\# \left\{ \{m_i\} \middle| support(m_i \xi_i) \in \pi \right\} \leq \left(\frac{|\pi|}{char(R/\mathfrak{m})} \right)^n$$

Proof. Indeed,

$$\# \left\{ \{m_i\} \middle| support(m_i \xi_i) \in \pi \right\} \leq \# \left\{ m \in M \middle| m\xi \in \pi \right\}^n$$

By Lemma 4.4, and because π is not an R-module,

$$\left\{ m \in M \middle| m\xi \in \pi \right\} \tag{4.3}$$

is a proper subgroup of π. If $p = char(R/\mathfrak{m})$, M is a p-group and hence π is a p-group, Therefore, (4.3) is bounded above by $|\pi|/p$ and the result follows. □

Proof of Theorem 4.1 We combine the estimates above to get:

$$\sum_{m \in \mathcal{C}_2} \left| \left| m_i \xi_i \right| \right|_{l^\infty}^{n+u} \leq$$

$$\leq \sum_{\substack{\pi \subset M \\ \pi \notin \mathbf{R-mod}}} \# \left\{ \{m_i\} \middle| support(m_i \xi_i) \in \pi \right\} \left(\frac{1+\epsilon}{|\pi|} \right)^{n+u} \leq$$

$$\leq \sum_{\substack{\pi \subset M \\ \pi \notin \mathbf{R-mod}}} \left(\frac{|\pi|}{|char(R/\mathfrak{m})|}\right)^n \left(\frac{1+\epsilon}{|\pi|}\right)^{n+u} \lesssim$$

$$\lesssim \left(\frac{1+\epsilon}{char(R/\mathfrak{m})}\right)^{n+u}$$

where the implied constant depends only on M and on u.

5 Sum over $\mathcal{C}_3$

Recall that we say that $\{m_i\}$ belongs to $\mathcal{C}_3$ if *at least one* Fourier coefficient of the random variable

$$\sum_i m_i \xi_i$$

has absolute value smaller than 1 but larger than $\epsilon/|M|$.

Theorem 5.1.

$$\sum_{m \in \mathcal{C}_3} \left|\left|\sum_i m_i \xi_i\right|\right|_{l^\infty}^{n+u} \lesssim (1+\epsilon)^{2n+u}(1-\beta)^{n+u}$$

where the implied constant depends on u, ϵ, M, and the distribution of

$$(\xi \mod ann\, M)$$

.

5.1 Preliminary Theorem

This section will be devoted to the proof of the auxiliary Theorem 5.3. Before stating Theorem 5.3, we need a lemma.

Lemma 5.2. *There exists a positive integer T, depending only on ϵ, M and the distribution of $(\xi \mod ann\, M)$, such that for any $m \in M$, any Fourier coefficient of $m\xi$ is either equal to* 1 *or has absolute value less than:*

$$\left(\frac{\epsilon}{|M|}\right)^{1/T}$$

Proof. To prove the lemma, it is sufficient to show that every Fourier coefficient of $m\xi$ is either 1 or bounded above in absolute value by some absolute constant, say $\mathbf{C}$, that depends only on the distribution of $(\xi \mod \operatorname{ann} M)$. But every Fourier coefficient of $m\xi$ occurs as a Fourier coefficient of $(\xi \mod \operatorname{ann} M)$. The set of Fourier coefficients of $(\xi \mod \operatorname{ann} M)$ is a finite set that depends only on the distribution of $(\xi \mod \operatorname{ann} M)$. Hence, the result follows.

□

Definition. Define α to be the smallest non-zero value of $\mathbb{P}(\xi \equiv r \mod \operatorname{ann} M)$ as r ranges over $R \mod \operatorname{ann} M$.

Remark. Although, this is not very important for the proof, we remark that we can compute an explicit upper bound on $\mathbf{C}$, from α and from the minimal value of e such that $p^e M = 0$.

Theorem 5.3. *Given $\{m_i\} \in \mathcal{C}_3$, there exists an additive subgroup $\pi \in M$ such that*

- *We have the inequality:*

$$\Big|\Big|\sum_i m_i \xi_i\Big|\Big|_{l^\infty} \leq \frac{(1-\alpha)(1+\epsilon)}{|\pi|}.$$

- *When π is an R-module, we have the stronger inequality:*

$$\Big|\Big|\sum_i m_i \xi_i\Big|\Big|_{l^\infty} \leq \frac{(1-\beta)(1+\epsilon)}{|\pi|}.$$

- *$m_i \in \pi$ for all but $T|M|$ indices i.*

π is not necessarily unique.

Proof of Theorem 5.3

We will need a lemma:

Lemma 5.4. *Given any $m \in Hom(R^n, M)$, there exists a set of indices $\mathcal{I}$ of size at most $T|M|$, such that*

1. *The Fourier coefficients of the random variable:*

$$\sum_{i \notin \mathcal{I}} m_i \xi_i \tag{5.1}$$

   are all either "small" or equal to 1.

2. *Furthermore, there is an additive subgroup of M that contains*

$$support(m_i \xi_i) \qquad \text{for all } i \notin \mathcal{I},$$

   but does not contain

$$support(m_i \xi_i) \qquad \text{for any } i \in \mathcal{I}.$$

Proof. We proceed iteratively, starting with the empty set. The iteration step is as follows. Suppose that we have an index set $\mathcal{J}$ that satisfies the second condition of the lemma, e.g. the set $\emptyset$. Further suppose that some Fourier coefficient of

$$\sum_{i \notin J} m_i \xi_i$$

is *large.* Then the kernel of this Fourier coefficient contains:

$$support(m_i \xi_i)$$

for all but at most T indices i. Adding these indices to $\mathcal{J}$, we obtain a new index set $\mathcal{J}'$. This index set has the property that the smallest subgroup of M that contains:

$$support(m_i \xi_i) \qquad \text{for all } i \notin \mathcal{J}'$$

does not contain

$$support(m_i\xi_i) \qquad \text{for any } i \in \mathcal{J}'.$$

As the support of

$$\sum_{i\in\mathcal{J}'} m_i\xi_i$$

is strictly contained inside the support of

$$\sum_{i\in\mathcal{J}} m_i\xi_i,$$

the iteration must halt after at most $|M|$ steps. Therefore the final index set has cardinality at most $|M|T$. □

Let π be the smallest subgroup that contains the support of:

$$\left(\sum_{i\notin\mathcal{I}} m_i\xi_i\right). \tag{5.2}$$

The Fourier coefficient of the restriction of (5.2) are either equal to 1 or "small". Therefore,

$$\sum_{i\notin\mathcal{I}} m_i\xi_i$$

is ϵ-equidistributed on π.

Remark. The non-uniqueness of π, stated in Theorem 5.3 is due to the non-uniqueness of our choice of $\mathcal{I}$.

Lemma 5.5. *For any $i \in \mathcal{I}$, the random variable $m_i\xi_i \mod \pi$ takes at least two distinct values with non-zero probability. Furthermore,*

- *We have the bound*

$$\left|\left|m_i\xi_i \mod \pi\right|\right|_{l^\infty} \leq 1-\alpha.$$

- *If π an R-module, we have the stronger bound*

$$\left|\left|m_i\xi_i \mod \pi\right|\right|_{l^\infty} \leq \left|\left|\xi \mod \mathfrak{m}\right|\right|_{l^\infty} \leq 1-\beta.$$

Proof. The support of ξ contains 0. Hence the random variable induced by $m_i\xi_i$ on M/π takes the value 0 with positive probability. Moreover, the support of $m_i\xi_i$ is not contained in π. Hence, the random variable induced by $m_i\xi_i$ on M/π also a takes a non-zero value with positive probability. This proves the first part of the lemma.

The probability that this induced random variable takes any given value is a sum of terms of the form: $\mathbb{P}(\xi_i = r)$. Hence this probability is either 0 or it is bounded below by α. Therefore, since the induced random variable takes at least two distinct values with non-zero probability, each non-zero probability must be at least α. This proves the second part of the lemma.

Lastly, if π is an R-module, then

$$\Big|\Big| m_i\xi_i \mod \pi \Big|\Big|_{l^\infty} = \max_{m\in M} \mathbb{P}\big(m_i\xi_i \equiv m \mod \pi\big) =$$
$$= \max_{r\in R} \mathbb{P}\big(\xi \equiv r \mod (\pi : m_i)\big) \leq$$
$$\leq \max_{r\in R} \mathbb{P}\big(\xi \equiv r \mod \mathfrak{m}\big) =$$
$$= \Big|\Big|\xi \mod \mathfrak{m}\Big|\Big|_{l^\infty} \leq 1-\beta$$

where we have used the notation $(\pi : m_i)$ to denote the ideal

$$\{r\in R | rm_i \in \pi\}$$

. This is a proper ideal of R, as π does not contain the support of $m_i\xi_i$. □

Proof. (of Theorem 5.3) We combine Theorem 2.2 and Lemma 5.5.

- It follows that:

$$\Big|\Big|\sum_i m_i\xi_i\Big|\Big|_{l^\infty} \leq \frac{(1+\epsilon)}{|\pi|}\Big|\Big|\sum_i m_i\xi_i \mod \pi\Big|\Big|_{l^\infty} \leq$$
$$\leq \frac{(1+\epsilon)(1-\alpha)}{|\pi|}$$

- When π is an R-module, we have the better bound:

$$\Big|\Big|\sum_i m_i\xi_i\Big|\Big|_{l^\infty} \leq \frac{(1+\epsilon)}{|\pi|}\Big|\Big|\xi \mod \mathfrak{m}\Big|\Big|_{l^\infty} \leq \frac{(1+\epsilon)(1-\beta)}{|\pi|}$$

5.2 Proof of Theorem 5.1

Now, the proof of Theorem 5.1 is analogous to the proof of Theorem 4.1.

By Theorem 5.3, we can bound

$$\sum_{\{m_i\}\in\mathcal{C}_3} \Big|\Big|\sum_i m_i\xi_i\Big|\Big|^{n+u}_{l^\infty}$$

by

$$\sum_{\substack{\pi\subset M\\ \pi \text{ not an}\\ R\text{-module}}} \#\Big\{\{m_i\}\in M^n \Big| \mathit{support}(m_i\xi_i)\in\pi \text{ for all but } |M|T \text{ indices } i\Big\}\left(\frac{(1+\epsilon)(1-\alpha)}{|\pi|}\right)^{n+u}$$
$$+ \sum_{\substack{\pi\subset M\\ \pi \text{ is an}\\ R\text{-module}}} \#\Big\{\{m_i\}\in M^n \Big| \mathit{support}(m_i\xi_i)\in\pi \text{ for all but } |M|T \text{ indices } i\Big\}\left(\frac{(1+\epsilon)(1-\beta)}{|\pi|}\right)^{n+u} \tag{5.3}$$

Lemma 5.6. *For all π, we have the bound:*

$$\#\left\{\{m_i\} \in M^n \middle| \mathit{support}(m_i\xi_i) \in \pi \textit{ for all but } |M|T \textit{ indices } i\right\} \lesssim$$

$$\lesssim (1+\epsilon)^n |\pi|^n \tag{5.4}$$

where the implied constant depends on ϵ and $|M|$ and T. When π is an R-module, we have the stronger bound:

$$\#\left\{\{m_i\} \in M^n \middle| \mathit{support}(m_i\xi_i) \in \pi \textit{ for all but } |M|T \textit{ indices } i\right\} \lesssim$$

$$\lesssim (1+\epsilon)^n \left(\frac{|\pi|}{\mathit{char}(R/\mathfrak{m})}\right)^n. \tag{5.5}$$

Proof. In both cases, we have:

$$\#\left\{\{m_i\} \in M^n \middle| \mathit{support}(m_i\xi_i) \in \pi \text{ for all but } |M|T \text{ indices } i\right\} \leq$$

$$\leq \#\left\{m \in M \middle| \mathit{support}(m\xi) \in \pi\right\}^{n-|M|T} |M|^{|M|T} \binom{n}{|M|T}$$

Now, by Lemma 4.4,

$$\#\left\{m \in M \middle| \mathit{support}(m\xi) \in \pi\right\} \tag{5.6}$$

is bounded by $|\pi|$ when π is an R-module, and bounded by $\frac{|\pi|}{\mathit{char}(R/\mathfrak{m})}$ when π is not an R-module.

Lastly, we note that $\binom{n}{|M|T}$ is a polynomial in n. In particular, it grows slower than any exponential. Therefore,

$$\binom{n}{|M|T} \lesssim (1+\epsilon)^n$$

where the implied constant depends on ϵ, M and T. Therefore,

$$\left\{\{m_i\} \in M^n \middle| \mathit{support}(m_i\xi_i) \in \pi \text{ for all but } |M|T \text{ indices } i\right\} \lesssim$$

$$\lesssim |\pi|^n |M|^{|M|T} (1+\epsilon)^n \lesssim$$
$$\lesssim |\pi|^n (1+\epsilon)^n$$

where again the implied constant depends on ϵ, M and T. □

Finally, substituting (5.4) into (5.3) yields

$$\sum_{\{m_i\}\in\mathcal{C}_3} \left|\left|\sum_i m_i\xi_i\right|\right|_{l^\infty}^{n+u} \lesssim (1+\epsilon)^{2n+u}(1-\beta)^{n+u}$$

where the implied constant depends on ϵ, u, M and T. Recalling that T is determined by M, ϵ and the distribution of ($\xi \mod \operatorname{ann} M$), we deduce Theorem 5.1.

Deduction of Theorem 1.2 Finally, we choose ϵ such that $(1+\epsilon)^3 < (1+\epsilon')$. Combining the three estimates - Lemma 3.1, Theorem 4.1 and Theorem 5.1 - we prove that (1.7) is bounded above by (1.5). Hence, we deduce Theorem 1.2.

6 Replacing some of the entries of the matrix by independent uniformly random variables

The purpose of this section is to show that Theorem 1.2 continues to hold when we replace some of the entries of $\mathcal{M}_{n,n+u}$ by independent uniformly random variables.

Let $\bar{\mathcal{M}}$ be an $n \times n+u$ random matrix whose entries are independent random variables. $\bar{\mathcal{M}}$ is independent of $\mathcal{M}_{n,n+u}$. The entries of $\bar{\mathcal{M}}$ are not necessarily identically distributed.

Lemma 6.1. *The sum of*

$$\max\left(I\!\!P\big(f(\mathcal{M}_{n,n+u}+\bar{\mathcal{M}})=0\big)-\left(\frac{1+\epsilon_0}{|M|}\right)^{n+u},0\right) \tag{6.1}$$

over all

$$f \in Sur(R^n, M)$$

is bounded above by (1.5)

Proof. Denote the entries of $\bar{\mathcal{M}}$ by $\bar{\xi}_{ij}$. We proceed as in §1.1. By independence, we can rewrite (6.1) as:

$$\max\left(\prod_j \mathbb{P}\left(\sum_i m_i(\xi_{ij}+\bar{\xi}_{ij})=0\right)-\left(\frac{1+\epsilon_0}{|M|}\right)^{n+u},0\right) \leq$$

$$\leq \max\left(\prod_j \Big|\Big|\sum_i m_i\xi_{ij}+m_i\bar{\xi}_{ij}\Big|\Big|_{l^\infty}-\left(\frac{1+\epsilon_0}{|M|}\right)^{n+u},0\right) \leq$$

$$\leq \max\left(\prod_j \Big|\Big|\sum_i m_i\xi_{ij}\Big|\Big|_{l^\infty}-\left(\frac{1+\epsilon_0}{|M|}\right)^{n+u},0\right) \tag{6.2}$$

The last inequality holds because the l^∞ norm of a sum of two independent random variables is bounded above by the l^∞ norm of either variable. Hence the sum of (6.1) is precisely (1.7). By the last paragraph of §5.2, (1.7) is bounded above by (1.5). □

Corollary 6.1.1. Theorem 1.2 remains true if we replace some subset of the entries of $\mathcal{M}_{n,n+u}$ by independent uniformly random variables.

Proof. We apply Lemma 6.1; it suffices to let $\bar{\mathcal{M}}$ be a matrix some of whose entries are independent uniformly random variables, while the other entries are identically 0. □

References

[Lin22] J.W. Lindeberg. Eine neue herleitung des exponentialgesetzes in der wahrscheinlichkeitsrechnung. *Math. Zeit.*, 15:211–225, 1922.

[Map13] Kenneth Maples. Cokernels of random matrices satisfy the Cohen-Lenstra heuristics. *arXiv*, math.CO/1301.1239[5], 2013.

[TV11] Terence Tao and Van Vu. Random matrices: Universality of local eigenvalue statistics. *Acta Math.*, 206:127–204, 2011.

[Woo17] Melanie Matchett Wood. The distribution of sandpile groups of random graphs. *Journal of the American Mathematical Society*, 30(4):915–958, 2017.

[Woo23] Melanie Matchett Wood. Probability theory for random groups arising in number theory. In Dmitry Beliaev and Stanislav Smirnov, editors, *ICM 2022 Proceedings*, Berlin, 2023. EMS Press.