Universality results for random matrices over finite local rings

Nikita Lvov*

May 10, 2025

Abstract

Let R be a finite local ring. We prove a quantitative universality statement for the cokernel of random matrices with i.i.d. entries valued in R. Rather than use the moment method, we use the Lindeberg replacement technique. This approach also yields a universality result for several invariants that are finer than the cokernel, such as the span and the determinant.

1 Introduction

We are interested in cokernels of random matrices over finite and profinite local rings. Firstly, we discuss the case when the entries of the matrices are uniformly distributed and independent.

Matrices with uniformly random entries

1. First, let $\mathcal{U}_{n,m}$ be an $n \times m$ matrix over $\mathbb{Z}_p$, whose entries are sampled uniformly at random. A theorem of Friedman and Washington describes the asymptotic distribution of $coker(\mathcal{U}_{n,n})$:

   Theorem. [FW89, Proposition 1]

   $$\lim_{n\to\infty} \mathbb{P}\Big(coker(\mathcal{U}_{n,n}) \cong A\Big) = \frac{c_0}{|Aut(A)|} \tag{1.1}$$

   where

   $$c_0 = \prod_{i=1}^{\infty}\left(1 - \frac{1}{p^i}\right)$$

   The distribution (1.1) on p-groups is known as the Cohen-Lenstra distribution [CL84].

*nikita.lvov@mail.mcgill.ca

2. The derivation that establishes [FW89, Proposition 1] can be generalized to non-square matrices to give:

$$\lim_{n\to\infty} \mathbb{P}\Big(coker(\mathcal{U}_{n,n+u}) \cong A\Big) = \frac{c_u}{|A|^u |Aut(A)|} \qquad \text{for } u \geq 0 \tag{1.2}$$

where

$$c_u = \prod_{i=u+1}^{\infty} \left(1 - \frac{1}{p^i}\right)$$

3. Finally, from the recent work of Sawin and Wood [SW24, Lemma 6.7 and Lemma 6.6], we can deduce a formula valid for any *finite* local ring R. We consider an $n \times (n+u)$ matrix over R, whose entries are independent and uniformly distributed. We again denote this matrix as $\mathcal{U}_{n,n+u}$. [SW24, Lemma 6.7] implies that for $u > 0$, and any finite local ring R,

$$\lim_{n\to\infty} \mathbb{P}(coker(\mathcal{U}_{n,n+u}) = A) = \frac{1}{|A|^u |Aut(A)|} \prod_{i=d(A)+u+1}^{\infty} \left(1 - \frac{1}{q^i}\right) \tag{1.3}$$

where q is the cardinality the residue field of R. $d(A)$ is defined to be the difference between the number of relations and the number of elements in the minimal presentation of A, negative if there are more relations than elements[1].

In fact, (1.1) and (1.2) can both be deduced from (1.3).

1.1 Universality; the results of this paper

As found in the work of Maples, Wood and Nguyen ([Map13], [Woo19], [NW21]), the conclusion of (1.1) continues to hold when we replace the matrix $\mathcal{U}_{n,n}$ by *any* i.i.d. random matrix, under the necessary condition that the distribution of the entries is non-degenerate modulo p. This is an instance of the general phenomenon of universality. We refer to [Woo23] for a survey.

Henceforth, R will be a fixed finite local ring, and u will be an integer. The integer u may be negative.

In this paper, we consider a $n \times (n+u)$ random matrix $\mathcal{M}_{n,n+u}$ over R. We assume that the entries are i.i.d. random variables. We assume that their distribution is not concentrated on the translate of a subring, or the translate of an ideal of R.

We prove an estimate, which we call the column-swapping estimate, (Theorem 2.2). This estimate will immediately imply the following universality theorem:

.

[1] For example, $d(R^3) = 3$.

Theorem 1.1. *Let $\mathcal{M}_{n,n+u}$ and $\mathcal{U}_{n,n+u}$ be the random matrices previously defined. We have the following asymptotic statements:*

(A) For any $u \in \mathbb{Z}$, the total variation distance between

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

tends to 0 as $n \to \infty$.

(B) The total variation distance between the joint distribution of

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

and the joint distribution of

$$coker(\mathcal{U}_{n,n}), \, det(\mathcal{U}_{n,n})$$

tends to 0 as $n \to \infty$.

(C) Both of the above statements hold if we replace the cokernel by the span of the column vectors.

In all of the above cases, the total variation distance is bounded above by $O(\theta^n)$, for any θ satisfying (2.4). The implicit constant depends on θ, u, R and the distribution of the entries of $\mathcal{M}_{n,n+u}$.

Statement (A) has the following corollary:

Corollary. *When $u \geq 0$, the asymptotic value of $\mathbb{P}(coker(\mathcal{M}_{n,n+u}))$ is given by (1.3).*

Statement (B) has the following corollary:

Corollary. *$det(\mathcal{M}_{n,n})$ has the same asymptotic distribution as $det(\mathcal{U}_{n,n})$.*

1.2 Method of Proof

Most current proofs of universality for random matrices, over finite and pro-finite rings, use the moment method, which first appeared in [Woo17]. We use a different approach, the Lindeberg replacement technique of [TV11], inspired by [Lin22]. The idea of this technique is to replace a column vector of $\mathcal{M}_{n,n+u}$ by a uniformly random vector. Somewhat surprisingly, this does not significantly alter the distribution of the cokernel of the random matrix or the distribution of the other invariants (Theorem 2.1). Replacing all the columns by independent uniformly random vectors allows us to conclude 1.1.

Remark. In an upcoming note, we will reinterpret the "column-swapping estimate" from a dynamical point of view - the estimate will imply that cokernels of minors *approximately* form a Markov chain. We will see that the dynamic perspective naturally allows us to prove finer universality results, using equidistribution theorems for Markov chains.

1.3 Related work

The earliest papers treating universality problems for random matrices over the p-adics were [Map13] , [Woo17] and [NW21] . In the decade that followed their appearance, there has been a surge of results on this topic. We again refer to [Woo23] for a survey. Nearly all of this work has been driven by the moment method, introduced by Wood in the seminal article on symmetric p-adic matrices [Woo17].

As noted previously, we instead use the Lindeberg replacement technique. In the context of random matrices over the real and complex numbers, this method was introduced by Tao and Vu in [TV11]; in the latter article, it is used to prove universality of local eigenvalue statistics of random matrices over $\mathbb{R}$ and $\mathbb{C}$. The LRT has also been used to prove universality for the distribution of the logarithm of the determinant of a random matrix over $\mathbb{R}$ in [NV14].

For rings other than $\mathbb{R}$ or $\mathbb{C}$, this approach seems to have been pursued only in the case of finite fields. In particular, for symmetric matrices over finite fields, a strategy equivalent to a replacement strategy was suggested in an unpublished note of Maples [Map]. We also remark that although some ideas of Tao and Vu are used in the paper [Map13], the approach therein seems to be different.

1.3.1 Outline

In §2, we state the column-swapping estimate and derive some of its consequences, such as Theorem 1.1. In §3, we prove the column-swapping estimate, by reducing it to two inequalities, proven in [Lvoa] and [Lvob], respectively.

2 The column-swapping estimate and its consequences

Definition. Let ξ be a random variable on R with the same distribution as the entries of $\mathcal{M}_{n,n+u}$.

Definition. Let $\mathbf{v_1}$ be a random vector whose entries are independent and have the same distribution as ξ.

Definition. Let $\mathbf{v_0}$ be a uniformly distributed random vector.

Definition. Suppose that B is a submodule of the module R^n and that $\mathbf{v}$ is a random element of R^n. Then by

$$\mathrm{proj}_B \mathbf{v},$$

we denote the sum of $\mathbf{v}$ and an independent uniformly distributed random element of B.

Remark. Intuitively, we get $\mathrm{proj}_B \mathbf{v}$ by "averaging out" $\mathbf{v}$ over B-cosets.

Observe that, by the invariance of the cokernel under the action of $SL(R)$, the distribution of

$$\text{coker}\left[\begin{array}{c|c} \quad \mathcal{M}_{n,n+u} \quad & \mathbf{v} \end{array}\right]$$

remains invariant if we add a uniformly random element of $im(\mathcal{M}_{n,n+u})$ to $\mathbf{v}$.

Hence, it follows that the total variation distance:

$$d_{TV}\left(coker\left[\begin{array}{c|c} \quad \mathcal{M}_{n,n+u} \quad & \mathbf{v_1} \end{array}\right], coker\left[\begin{array}{c|c} \quad \mathcal{M}_{n,n+u} \quad & \mathbf{v_0} \end{array}\right]\right) \tag{2.1}$$

is equal to the total variation distance between

$$coker\left[\begin{array}{c|c} \mathcal{M}_{n,n+u} & \text{proj}_{im(\mathcal{M}_{n,n+u})}\mathbf{v_1} \end{array}\right]$$

and

$$coker\left[\begin{array}{c|c} \mathcal{M}_{n,n+u} & \text{proj}_{im(\mathcal{M}_{n,n+u})}\mathbf{v_0} \end{array}\right]$$

Therefore, (2.1) is bounded by:

$$\sum_{M} \mathbb{P}(\mathcal{M}_{n,n+u} = M) d_{TV}\left(\text{proj}_{im(M)}\mathbf{v_1}, \text{proj}_{im(M)}\mathbf{v_0}\right) \tag{2.2}$$

Remark. Of course, $\text{proj}_{im(M)}\mathbf{v_0}$ has the same distribution as $\mathbf{v_0}$. Therefore, we can replace it by $\mathbf{v_0}$, if we wish.

It therefore suffices to bound (2.2). The preceding discussion serves to motivate the following theorem, which is the central result of this paper: we first state the theorem in qualitative form:

Theorem 2.1 (Qualitative form of the column-swapping estimate)**.** *Suppose that $\mathcal{M}_{n,n+u}$ is a random matrix with i.i.d. random entries, which are sampled from a distribution that is*

- *not concentrated on the translate of an ideal of R,*
- *not concentrated on the translate of a subring of R.*

Then there exists $\theta < 1$ such that

$$\sum_{M} \mathbb{P}(\mathcal{M}_{n,n+u} = M) d_{TV}\left(proj_{im(M)}\mathbf{v_1}, proj_{im(M)}\mathbf{v_0}\right) \leq$$

$$\leq O(\theta^n) \tag{2.3}$$

where θ is a constant that depends on R, and on the distribution of the entries of $\mathcal{M}_{n,n+u}$.

Moreover, the same estimate continues to hold if some of the entries of $\mathcal{M}_{n,n+u}$ are replaced by independent uniformly distributed random variables.

Quantitative form Below, we give the quantitative form of Theorem 2.1. In order to do so, we must first introduce some definitions. Let ξ be a random variable that has the same *distribution* as the entries of $\mathcal{M}_{n,n+u}$.

Definition. Define ($\xi \mod \mathfrak{m}$) to be the random variable that is induced by ξ on $R/\mathfrak{m}$.

- Denote by $\left|\left|\xi \mod \mathfrak{m}\right|\right|_{l^2}$ the l^2 norm of the distribution of ($\xi \mod \mathfrak{m}$).
- Denote by $\left|\left|\xi \mod \mathfrak{m}\right|\right|_{l^\infty}$ the l^∞ norm of the distribution of ($\xi \mod \mathfrak{m}$).
- Let $char(R/\mathfrak{m})$ denote the characteristic of the field $R/\mathfrak{m}$.

Remark. Observe that, under the hypotheses of Theorem 2.1,

$$\max\left(\left|\left|\xi \mod \mathfrak{m}\right|\right|_{l^2}, \left|\left|\xi \mod \mathfrak{m}\right|\right|_{l^\infty}, \frac{1}{char(R/\mathfrak{m})}\right) < 1.$$

Theorem 2.2 (Quantitative form of the column-swapping estimate)**.** *If θ satisfies*

$$\max\left(\left|\left|\xi \mod \mathfrak{m}\right|\right|_{l^2}, \left|\left|\xi \mod \mathfrak{m}\right|\right|_{l^\infty}, \frac{1}{char(R/\mathfrak{m})}\right) < \theta < 1 \tag{2.4}$$

then, (2.3) holds; the proportionality constant implicit in (2.3) depends on u, θ, R and on the smallest non-zero value of:

$$I\!P(\xi = r) \quad , \quad r \in R$$

Intuitive meaning of Theorem 2.1 Theorem 2.1 captures the following intuitively plausible fact. An i.i.d. random vector should be approximately equidistributed in the quotient of R^n by $n+u$ other i.i.d. random vectors, with high probability.

2.1 Corollaries of Theorem 2.2

Deduction of Theorem 1.1 Theorem 1.1 is an immediate consequence of Theorem 2.2.

Proof. Indeed, by the discussion preceding Theorem 2.1, the inequality (2.3) implies that:

$$d_{TV}\left(coker\left[\begin{array}{c|c} \mathcal{M}_{n,n+u} & \mathbf{v_1}\end{array}\right], coker\left[\begin{array}{c|c} \mathcal{M}_{n,n+u} & \mathbf{v_0}\end{array}\right]\right) \leq$$

$$\leq O(\theta^n) \tag{2.5}$$

Remark. Recall that the inequality in (2.3) remains valid if we replace some of the entries of $\mathcal{M}_{n,n+u}$ by independent, uniformly random variables. Hence, (2.5) also remains valid.

By the preceding remark, we can apply the inequality (2.5) iteratively to conclude that

$$\lim_{n\to\infty} d_{TV}\Big(coker(\mathcal{M}_{n,n+u+1}), coker(\mathcal{U}_{n,n+u+1})\Big) = 0 \tag{2.6}$$

for any $u \in \mathbb{Z}$. $\square$

Finer invariants To conclude (2.5), all we have used about the cokernel function is its invariance under the right action of SL_{n+u}. Therefore, (2.5) remains valid if we replace the cokernel by any other SL_{n+u} invariant, such as the span of the column vectors of $\mathcal{M}_{n,n+u}$. In particular,

- We have

  $$\lim_{n\to\infty} d_{TV}\Big(span(\mathcal{M}_{n,n+u}), span(\mathcal{U}_{n,n+u})\Big) = 0$$

- The total variation distance between the joint distribution of

  $$span(\mathcal{M}_{n,n})\,,\, det(\mathcal{M}_{n,n})$$

  and the joint distribution of

  $$span(\mathcal{U}_{n,n})\,,\, det(\mathcal{M}_{n,n})$$

  tends to 0.

Rate of convergence We observe that the rate of convergence is

$$(n+u)O(\theta^n)$$

which may be rewritten as

$$O(\theta^n)$$

for a slightly larger θ in the range (2.4). Once again, the implicit constant depends only on u, R, θ and the smallest non-zero value of

$$\mathbb{P}(\xi = r) \qquad r \in R$$

This proves the rest of Theorem 1.1

Upper-Triangular Matrices We will finally observe a consequence of Theorem 2.2 that will be useful in an upcoming note, where Theorem 2.2 will be combined with a Markovian perspective to deduce other universality results.

Definition. Define T_n to be the group of upper triangular matrices with 1's on the diagonal and let t be the map to the double quotient

$$Mat_{k,l} \to T_k \backslash Mat_{k,l} / T_l$$

Corollary. *(of Theorem 2.2)*

$$d_{TV}\left(t\left[\begin{array}{c|c} \quad\mathcal{M}_{n,n+u}\quad & \mathbf{v_1} \end{array}\right], t\left[\begin{array}{c|c} \quad\mathcal{U}_{n,n+u}\quad & \mathbf{v_0} \end{array}\right]\right) \leq O(\theta^n)$$

3 Proof of the column-swapping estimate

We wish to bound

$$\sum_{M} \mathbb{P}(\mathcal{M}_{n,n+u} = M) d_{TV}\left(\text{proj}_{im(M)}\mathbf{v_1}, \text{proj}_{im(M)}\mathbf{v_0}\right) \tag{3.1}$$

Let ν_i denote the distribution of $\mathbf{v}_i$. Note that

$$d_{TV}\left(\text{proj}_{im(M)}\mathbf{v_1}, \text{proj}_{im(M)}\mathbf{v_0}\right)$$

can be rewritten as

$$\left|\left|\text{proj}_{im(M)}(\nu_1 - \nu_0)\right|\right|_{l^1}$$

Hence, to prove Theorem 2.2, it suffices to bound:

$$\sum_{M} \mathbb{P}(\mathcal{M}_{n,n+u} = M)\left|\left|\text{proj}_{im(M)}(\nu_1 - \nu_0)\right|\right|_{l^1}$$

We will now see that Theorem 2.2 can be deduced from the following estimate:

Lemma 3.1. *For any arbitrary signed measure ν on R^n, we have the inequality:*

$$\begin{aligned} &\sum_{M} \mathbb{P}\left(\mathcal{M}_{n,n+u} = M\right) \left|\left|proj_{im(M)}\nu\right|\right|_{l^1} \leq \\ &\leq \sum_{I \subset R} O\left((1+\epsilon)^n \left|\left|\nu \mod I\right|\right|_{l^2}\right) + \\ O\left((1+\epsilon)^n \max\left[\left|\left|\xi \mod \mathfrak{m}\right|\right|_{l^\infty}, \frac{1}{char(R/\mathfrak{m})}\right]^n\right) \end{aligned} \tag{3.2}$$

where the implied constants depend on R, u, ϵ, and the minimal non-zero value of $\mathbb{P}(\xi = r)$, for $r \in R$.

The deduction of Theorem 2.2 from Lemma 3.1 In order to deduce Theorem 2.2, we will apply the bound in Lemma 3.1 to the case when

$$\nu = \nu_1 - \nu_0$$

First of all, note that

- The total mass of the measure $\nu_1 - \nu_0$ is 0:

$$\nu_1 - \nu_0 \mod R = 0 \tag{3.3}$$

- Hence, $\nu_1 - \nu_0$ is orthogonal to ν_0.

It follows that

$$\left|\left|\nu \mod I\right|\right|_{l^2} = \left|\left|\nu_1 - \nu_0 \mod I\right|\right|_{l^2} \leq \left|\left|\nu_1 \mod I\right|\right|_{l^2}$$

due to orthogonality. Since the l^2 norm of a probability measure cannot decrease under pushforward, the last line is bounded by:

$$\left|\left|\nu_1 \mod \mathfrak{m}\right|\right|_{l^2} = \left|\left|\xi \mod \mathfrak{m}\right|\right|_{l^2}^n$$

The last equality holds because ν_1 is a product measure. Hence $\nu_1 \mod \mathfrak{m}$ is a product measure. The norm of product measure is the product of the norms of the factors.

The remainder of this paper is devoted to the proof of Lemma 3.1.

3.0.1 Decomposing measures on modules

We recall the decomposition of measures on finite R-modules, described in [Lvob]. Recall that, given a signed measure ν on a finite module $\mathbf{M}$, and a submodule $N \subset \mathbf{M}$, we denote by $\text{proj}_N \nu$ the average of ν over N-cosets of $\mathbf{M}$. Finally, denote by ω the dualizing module of R.

Lemma 3.2. *[Lvob, Theorem 1.1 and Lemma 11.1] Given a finite R-module* $\mathbf{M}$*,*

- *Any signed measure ν on $\mathbf{M}$ admits a decomposition into orthogonal components parametrized by $\chi \in Hom(\mathbf{M}, \omega)/R^*$:*

$$\nu = \sum_{\chi} \nu_\chi$$

  where

  1. *The signed measures ν_χ are constant on $ker(\chi)$-cosets.*
  2. *$proj_N \nu_\chi = 0$ over any N that is not contained in $ker(\chi)$.*

- *We have the upper bound:*

$$\left|\left|\nu_\chi\right|\right|_{l^1} \leq \sqrt{|im\chi|} \tag{3.4}$$

Remark.

It follows from 1. and 2. and the definition of $\text{proj}_N \nu$ that:

$$\text{proj}_N \nu = \sum_{N \subset ker(\chi)} \nu_\chi$$

A Reduction Now we will apply the preceding decomposition to the signed measure

$$\nu \overset{\text{def}}{=\!=} \nu_1 - \nu_0$$

on R^n.

Lemma 3.2.1.

$$\sum_M I\!P(M = \mathcal{M}_{n,n+u}) \left|\left|proj_{im(M)}(\nu_1 - \nu_0)\right|\right|_{l^1} \tag{3.5}$$

is bounded above by

$$\sum_{\substack{\chi \in Hom(R^n, \omega)/R^* \\ \chi \neq 0}} \left|\left|\nu_\chi\right|\right|_{l^1} I\!P(\chi \mathcal{M}_{n,n+u} = 0) \tag{3.6}$$

Proof. By (3.2)

$$\Big|\Big|\mathrm{proj}_{im(M)}\nu\Big|\Big|_{l^1} = \Big|\Big| \sum_{\substack{\chi\in Hom(R^n,\omega)/R^* \\ im(M)\subset ker(\chi)}} \nu_\chi \Big|\Big|_{l^1} \tag{3.7}$$

Observe that

$$im(M) \in ker(\chi) \Leftrightarrow \chi\, M = 0$$

Thus, we can rewrite (3.7) as

$$\Big|\Big| \sum_{\substack{\chi\in Hom(R^n,\omega)/R^* \\ \chi\, M=0}} \nu_\chi \Big|\Big|_{l^1} \leq \sum_{\substack{\chi\in Hom(R^n,\omega)/R^* \\ \chi\, M=0}} \Big|\Big|\nu_\chi\Big|\Big|_{l^1} =$$

$$\sum_{\chi\in Hom(R^n,\omega)/R^*} \Big|\Big|\nu_\chi\Big|\Big|_{l^1} \mathbb{1}_{\{\chi\, M=0\}}$$

Therefore, (3.2) is bounded above by:

$$\sum_M \mathbb{P}\Big(\mathcal{M}_{n,n+u} = M\Big) \sum_{\chi\in Hom(R^n,\omega)/R^*} \Big|\Big|\nu_\chi\Big|\Big|_{l^1} \mathbb{1}_{\{\chi\, M=0\}}$$

$$= \sum_{\chi\in Hom(R^{n+u},\omega)/R^*} \Big|\Big|\nu_\chi\Big|\Big|_{l^1} \mathbb{P}(\chi\,\mathcal{M}_{n,n+u} = 0)$$

Proof of Lemma 3.1 We recall that ω is the dualizing module. Hence, the correspondance between submodules of ω and their annihilating ideals is 1-to-1. Denote by ω_I the submodule corresponding to I.

Hence, we can rewrite (3.6) as

$$\sum_{I\subset R} \sum_{\chi\in Sur(R^n,\omega_I)/R^*} \Big|\Big|\nu_\chi\Big|\Big|_{l^1} \mathbb{P}(\chi\,\mathcal{M}_{n,n+u} = 0)$$

Lemma 3.1 will be proven by showing the following estimate and summing over all I.

Lemma 3.2.2. *For any ideal I of R,*

$$\sum_{\chi\in Sur(R^n,\omega_I)/R^*} \Big|\Big|\nu_\chi\Big|\Big|_{l^1} \mathbb{P}(\chi\,\mathcal{M}_{n,n+u} = 0) \leq \tag{3.8}$$

$$\leq O\Big((1+\epsilon)^n \Big|\Big|\nu \mod I\Big|\Big|_{l^2}\Big) +$$

$$+O\left((1+\epsilon)^n \max\left[\Big|\Big|\xi \mod \mathfrak{m}\Big|\Big|_{l^\infty}, \frac{1}{char(R/\mathfrak{m})}\right]^n\right)$$

where the implied constants depend on u, ϵ, R and the distribution of ξ.

Proof. By Equation 3.4, $|\nu_\chi|$ is bounded above by

$$\sqrt{|\omega_I|} = \sqrt{|R/I|}$$

Hence, we can separate the sum (3.8) into two parts:

$$\sqrt{|R/I|} \sum_{\chi \in Sur(R^n, \omega_I)/R^*} \max \left[\mathbb{P}(\chi\, \mathcal{M}_{n,n+u} = 0) - \left(\frac{1+\epsilon_0}{|\omega_I|} \right)^{n+u}, 0 \right] +$$

$$+ \sum_{\chi \in Sur(R^n, \omega_I)/R^*} \left|\left| \nu_\chi \right|\right|_{l^1} \left(\frac{(1+\epsilon_0)}{|\omega_I|} \right)^{n+u}$$

It remains to estimate the two terms. Fortunately, the hard work has already been done in [Lvoa] and [Lvob]:

Applying the bounds from [Lvoa] and [Lvob]

(A) By [Lvoa, Theorem 1.2], for any $\epsilon' > 0$,

$$\sum_{\chi \in Sur(R^n, \omega_I)/R^*} \max \left[\mathbb{P}(\chi \mathcal{M}_{n,n+u} = 0) - \left(\frac{1+\epsilon_0}{|\omega_I|} \right)^{n+u}, 0 \right] \leq$$

$$\leq O \left(\max \left[\frac{1}{char(R/\mathfrak{m})}, \left|\left| \xi \mod \mathfrak{m} \right|\right|_{l^\infty} \right]^n (1+\epsilon')^n \right)$$

where the implied constant depends on ϵ', R/I, u and the distribution of $\xi \mod I$.

Moreover, this inequality remains valid if we replace some of the entries of $\mathcal{M}_{n,n+u}$ by independent uniformly random variables.

(B) By [Lvob, Theorem 10.1],

$$\frac{1}{|\omega_I|^n} \sum_{\chi \in Sur(R^n, \omega_I)/R^*} \left|\left| \nu_\chi \right|\right|_{l^1} =$$

$$= \frac{1}{|\omega_I|^n} \sum_{\chi \in Sur(R^n, \omega_I)/R^*} \left|\left| \nu_\chi \right|\right|_{l^1} \leq \frac{1}{\sqrt{R/I^*}} \left|\left| \nu \mod I \right|\right|_{l^2} \tag{3.9}$$

□

References

[CL84] H. Cohen and H. W. Lenstra. Heuristics on class groups of number fields. In Hendrik Jager, editor, *Number Theory Noordwijkerhout 1983*, pages 33–62, Berlin, Heidelberg, 1984. Springer Berlin Heidelberg.

[FW89] Eduardo Friedman and Lawrence C. Washington. On the distribution of divisor class groups of curves over a finite field. In Jean M. de Koninck and Claude Levesque, editors, *Théorie des nombres / Number Theory*, pages 227–239, Berlin, New York, 1989. De Gruyter.

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

[Lvoa] Nikita Lvov. A bound on a moment-like quantity in random matrix theory. preprint.

[Lvob] Nikita Lvov. Decomposing measures on modules. preprint.

[Map] Kenneth Maples. Symmetric random matrices over finite fields. preprint.

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

[NV14] Hoi H. Nguyen and Van Vu. Random matrices, law of the determinant. *The Annals of Probability*, 42, 2014.

[NW21] Hoi H. Nguyen and Melanie Matchett Wood. Random integral matrices: Universality of surjectivity and the cokernel. *Inventiones mathematicae*, 228(1):1–76, 2021.

[SW24] Will Sawin and Melanie Matchett Wood. The moment problem for random objects in a category. *arXiv*, math.PR/2210.06279[3], 2024.

[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.

[Woo19] Melanie Matchett Wood. Random integral matrices and the Cohen-Lenstra heuristics. *American Journal of Mathematics*, 141(2):383–398, 2019.

[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.