A dynamic point of view on universality for random matrices over finite local ring

Nikita Lvov*

May 31, 2025

Abstract

We consider the corners process for an i.i.d. matrix. When the distribution of the entries is uniform, this process is a Markov chain, and hence the ergodic theorem for Markov chains can be applied. This implies, in particular, that for uniformly distributed p-adic random matrices, the cokernels of the corners are distributed according to the Cohen-Lenstra measure, almost surely. The purpose of this note is to show that the conclusion of the ergodic theorem also holds for i.i.d matrices, provided that the distribution of the entries is not concentrated on the translate of a subring, or the translate of an ideal.

1 Introduction

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]. More generally,

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

where

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

*nikita.lvov@mail.mcgill.ca

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 $\mathcal{U}_{n,n+u}$. Now, [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]. We denote the measure on the right hand side of (1.3) as μ_u.

μ_u

The expressions (1.1) and (1.2) can both be deduced from (1.3).

Ergodic averages in the uniform case. We slightly refine the above set-up. $\mathcal{U}$ will denote an infinite random matrix over $\mathbb{Z}_p$, whose entries are sampled uniformly and independently at random. Denote by $\mathcal{U}_{n,m}$ the top left $n \times m$ corner of $\mathcal{U}$.

From [Lvoa], it follows that the random groups $\mathrm{coker}(\mathcal{U}_{n,n+u})$ form a recurrent Markov chain. In [Lvoa], we denote the generator of this Markov chain as Δ_u; by (1.3) , the stationary measure of this Markov chain is μ_u. From the ergodic theorem for Markov chains, it follows that:

Δ_u

$$\frac{1}{N} \sum_{i=1}^{N} \mathbb{1}_{(coker(\mathcal{U}_{i,i+u})=A)} \xrightarrow{N\to\infty} \mu_u(A) \text{ a.s.} \tag{1.4}$$

1.1 Random matrices with i.i.d. entries that are not necessarily uniformly distributed.

Let $\mathcal{M}$ be an infinite random matrix over R whose entries are i.i.d. random variables, subject to the condition that their distribution is not supported on the translate of a subring of R or the translate of an ideal.

Let $\mathcal{M}_{n,m}$ denote the top left $n \times m$ corner of $\mathcal{M}$. The next theorem states that the asymptotic distribution of $coker(\mathcal{M}_{n,n+u})$ is the same as the asymptotic distribution of $coker(\mathcal{U}_{n,n+u})$. This is an example of universality.

$\mathcal{M}_{n,m}$

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

Theorem. [Lvob] The equality (1.3) continues to hold when $\mathcal{U}_{n,n+u}$ is replaced by $\mathcal{M}_{n,n+u}$.

Remark. For $R \cong \mathbb{Z}/p^N\mathbb{Z}$, this theorem appeared in the work of Maples and Wood, [Map13] [Woo19], with stronger results proven by Nguyen and Wood [NW21]. When R is the quotient of a DVR, this is proven by Yan, under a slightly different assumption on the distribution of the entries [Yan23].

The main result: universality for ergodic averages. In this note, we prove another manifestation of universality; we show that (1.4) also holds when $\mathcal{U}_{n,n+u}$ is replaced by $\mathcal{M}_{n,n+u}$.

Theorem 1.1. *Let $\mathcal{M}_{i,i+u}$ be the top left $i \times i+u$ corner of $\mathcal{M}$, where $\mathcal{M}$ is the infinite random matrix defined above. Then,*

$$\frac{1}{N}\sum_{i=1}^{N} \mathbb{1}_{(coker(\mathcal{M}_{i,i+u})=A)} \xrightarrow{N\to\infty} \mu_u(A) \text{ a.s.} \tag{1.5}$$

We deduce this from [Lvoa] and [Lvob]. Indeed, as mentioned previously, [Lvoa] implies that

$$\dots \quad , \quad coker(\mathcal{U}_{i,i+u}) \quad , \quad coker(\mathcal{U}_{i+1,i+u+1}) \quad , \quad \dots$$

is a Markov chain generated by a certain operator, Δ_u, while [Lvob] implies that the process

$$\dots \quad , \quad coker(\mathcal{M}_{i,i+u}) \quad , \quad coker(\mathcal{M}_{i+1,i+u+1}) \quad , \quad \dots \tag{1.6}$$

is "approximately" a Markov chain generated by Δ_u, in a certain quantitative sense. This allows us to deduce (1.5) from the ergodic theorem for Markov chains.

2 The corner process is approximately a Markov chain

We use the symbol "$*$" to denote independent uniformly random variables. Let T denote the group of upper triangular matrices with 1's on the diagonal, and denote by t the map

$$t : Mat \to T \backslash Mat / T$$

that takes a matrix to its orbit under the action of $T \times T$. Finally, denote by d_{TV} the total variation distance. The inequality [Lvob, (2.5)] implies that

$$d_{TV}\left(t\left[\begin{array}{ccc|c} & \mathcal{M}_{n,n+u} & & * \\ & & & \vdots \\ & & & * \\ \hline * & \dots & * & * \end{array}\right], t\left[\begin{array}{c} \mathcal{M}_{n+1,n+u+1} \end{array}\right]\right) < O(\theta^n)$$

θ

where $\theta < 1$ is an explicit constant (defined in [Lvob, Theorem 2.2]), that depends only on the distribution of the entries of $\mathcal{M}$ and on the cardinality of the residue field of R.

Lemma 2.1. *The total variation distance between*

$$\left(\ \dots, \quad coker(\mathcal{M}_{i,i+u}), \quad \dots, \quad coker(\mathcal{M}_{n,n+u}), \quad coker(\mathcal{M}_{n+1,n+u+1}) \ \right)$$

and

$$\left(\ \dots, \quad coker(\mathcal{M}_{i,i+u}), \quad \dots, \quad coker(\mathcal{M}_{n,n+u}), \quad \Delta_u coker(\mathcal{M}_{n,n+u}) \ \right)$$

is bounded above by $O(\theta^n)$.

Definition. Denote by X_n the following process, indexed by $i \in \mathbb{N}$:

$$\Big(\quad \dots \quad , coker(\mathcal{M}_{i,i+u}), \quad \dots \quad , coker(\mathcal{M}_{n,n+u}),$$

$$\Delta_u coker(\mathcal{M}_{n,n+u}), \quad \dots \quad , \Delta_u^{i-n} coker(\mathcal{M}_{n,n+u}), \quad \dots \quad \Big)$$

Corollary. *(of Lemma 2.1)*

$$d_{TV}(X_n, X_{n+1}) < O(\theta^n) \tag{2.1}$$

Theorem 2.2. *X_n converges to X_∞ in total variation. More precisely:*

$$d_{TV}(X_n, X_\infty) < O(\theta^n) \tag{2.2}$$

Proof. (2.1) implies that for any k,

$$d_{TV}(X_n, X_{n+k}) < O(\theta^n)$$

where the implicit constant is different from the one in (2.1). Hence, X_n is a Cauchy sequence in the total variation topology.

Now, the space of probability measures, endowed with the total variation topology, is complete. Therefore, there exits Y such that

$$d_{TV}(X_n, Y) \leq O(\theta^n)$$

For any k, the pushforward of the distribution of Y to the first k coordinates must coincide with the pushforward of the distribution of X_∞ to the first k coordinates. As this is true for any k, X_∞ must have the same distribution as Y. □

2.1 Corollaries

Corollary. *The asymptotic distribution of $coker(\mathcal{M}_{i,i+u})$ is μ_u.*

Proof. In the limit $i \to \infty$, the distribution of $(X_n)_i$ converges to μ_u in total variation, because Δ_u generates a recurrent Markov chain. By Theorem 2.2,

$$d_{TV}\Big((X_n)_i, (X_\infty)_i\Big) < O(\theta^n)$$

We take the *limsup* as $i \to \infty$ to get:

$$\limsup_{i\to\infty} d_{TV}\Big(\,\mu_0\,,\,(X_\infty)_i\,\Big) < O(\theta^n)$$

and then take the limit as $n \to \infty$. This shows that the distribution of $(X_\infty)_i$ must also converge to μ_u. This proves the corollary. □

Remark. The statement of the corollary was previously demonstrated in [Lvob], with an explicit convergence rate. The result is proven again here, in order to show that it can be deduced from a dynamic perspective.

The next corollary is the main result of this note.

Corollary (Theorem 1.1)**.**

$$\frac{1}{N}\sum_{i=1}^{N} \mathbb{1}_{(coker(\mathcal{M}_{i,i+u})=A)} \xrightarrow{N\to\infty} \mu_u(A) \ \ a.s. \tag{2.3}$$

Proof. By the ergodic theorem for Markov chains, for any n,

$$\mathbb{P}\left(\frac{1}{N}\sum_{i=1}^{N} \mathbb{1}_{((X_n)_i=A)} \xrightarrow{N\to\infty} \mu_u(A)\right) = 1$$

Hence, by (2.2),

$$\mathbb{P}\left(\frac{1}{N}\sum_{i=1}^{N} \mathbb{1}_{((X_\infty)_i=A)} \xrightarrow{N\to\infty} \mu_u(A)\right) \geq 1 - O(\theta^n)$$

Taking $n \to \infty$ proves (2.3). □

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.

[Lvoa] Nikita Lvov. Markov chains arising in the study of random matrices over pro-finite local rings. preprint.

[Lvob] Nikita Lvov. Universality results for random matrices over finite local rings. preprint.

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

[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, 2024.

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

[Yan23] Eric Yan. Universality for cokernels of Dedekind domain valued random matrices. *arXiv*, math.NT/2301.09196, 2023.