Markov chains arising in the study of random matrices over pro-finite local rings

Nikita Lvov*

February 18, 2025

Abstract

Recent work of the author investigates certain random processes, valued in abelian p-groups, that naturally arise in the study of Haar random matrices over $\mathbb{Z}_p$. Non-trivially, it was found that these processes are reversible Markov chains. In this short note, we give a simple alternative derivation of this fact. The new derivation also proves that this phenomenon is not specific to $\mathbb{Z}_p$, but generalizes to Haar random matrices over any profinite local ring.

1 Introduction

Perhaps, the first and simplest instance of a Markov chain appearing in the study of random matrices, is the evolution of the corank of the principal minors of a large random matrix over a finite field.

Random matrices over finite fields Let k be a finite field. Consider an infinite matrix $\mathcal{M}$, whose entries are indexed by $\mathbb{N} \times \mathbb{N}$ and are independent *uniformly distributed* random variables in k. Let $\mathcal{M}_{n,n}$ be the top-left $n \times n$ corner of $\mathcal{M}$. Then

$$corank(\mathcal{M}_{n,n}) \tag{1.1}$$

is a random process valued in $\mathbb{N}$. Using standard arguments in linear algebra, one can deduce the following interesting features of this process:

- (1.1) is a Markov chain, i.e. a random walk on $\mathbb{N}$ (with certain explicit transition propabilities, that depend on the cardinality of k.)
- This Markov chain is recurrent, and hence converges to its unique stationary distribution.

Finally, we remark that this Markov chain is also *reversible*, for trivial reasons, since every Markov chain on $\mathbb{N}$ is reversible.

*nikita.lvov@mail.mcgill.ca

Random matrices over $\mathbb{Z}_p$ A non-trivial generalization of the above facts to matrices over $\mathbb{Z}_p$ was studied in [Lvo24].

Theorem. [Lvo24, Theorem 1.1]

$$coker\Big(Haar_{n,n}(\mathbb{Z}_p)\Big) \tag{1.2}$$

is a *reversible* Markov chain on abelian p-groups.

Remark. The process (1.2) is a direct generalization of the process (1.1). Indeed, the cokernel is a direct generalization of the corank, as for a matrix M over a finite field k,

$$coker(M) \cong k^{corank(M)}$$

.

In fact, in [Lvo24, Theorem 1.1], we describe the generator of this Markov chain explicitly. In its most elementary form, the Markov chain (1.2) is generated by the following operation:

(A) Given an abelian p-group G, mod out by a uniformly random element of G.

(B) Take the product of $\mathbb{Z}_p$.[1]

(C) Finally, mod out by a Haar random element of this product.

Futhermore, in [Lvo24, Lemma 2.3] we construct an explicit weighted graph Γ, such that the Markov chain is realized as a symmetric random walk on Γ. Finally, the last chapter of [Lvo24, Section 3], together with [LP], gives a complete explicit solution to the spectral problem for this Markov chain.

Main results of this paper: random matrices over pro-finite local rings and a unified approach The theorem [Lvo24, Theorem 1.1] is unsatisfactory in two respects:

- It is not a priori clear why the Markov property and the reversibility property hold.
  - There are related Markov chains that arise in the study of symmetric and anti-symmetric matrices over $\mathbb{Z}_p$. These Markov chains are also turn out to reversible. In each case, this is shown by a computation. However, the seeming ubiquity of this phenomenon begs for a unified approach.
- We can ask what happens for higher-dimensional rings. The approach of [Lvo24] does not directly generalize to this case.

[1] Steps (A) and (B) together are equivalent to the following single step - pick a uniformly random extension of G by $\mathbb{Z}_p$. The equivalence is a consequence of [Lvo24, Lemma 1.3].

– Aside from intrinsic interest, such a gneralization would be desirable, as 2-dimensional rings (e.g. $\mathbb{Z}_p[x]$) arise even in the study of p-adic random matrices. For example, to understand the characterstic polynomial of a p-adic matrix $\mathcal{M}$, one is led to consider $det(\mathcal{M} - Ix)$, which is most naturally understood through $coker(\mathcal{M} - Ix)$, the cokernel of a random matrix over $\mathbb{Z}_p[x]$.[2]

In this paper we prove the following theorem.

Theorem 1.1. *Let R be a finite or profinite local ring. Then $coker(Haar_{n,n+u}(R))$ is a reversible Markov chain, for any $u \in \mathbb{Z}$.*

Remark. In fact, we prove more. The random variable $coker(Haar_{n,m}(R))$ is a "two-dimensional" Markov chain, governed by a certain family of transition operators. We refer to §6 for more details.

Remark. By itself, the *Markov property* is not surprising, and can be deduced from the following two facts:

- Suppose that a module is defined as a set of generators satisfying linear relations. Adding another Haar random relation has the effect of modding out by a Haar random element of this module.
- The module $\mathrm{coker}(M)$ is uniquely determined by $\mathrm{coker}(M^T)$ and the dimensions of M.

Indeed, the first fact tells us what happens to the cokernel when we add a Haar random column vector to a matrix. The second fact shows that this infomation is sufficient to determine what happens when we add a Haar random row vector.

However, the approach in this paper can be generalized to prove the Markov property, as well as reversibility, for *symmetric* matrices over R. In this situation, the origin of the Markov property is a priori much less evident.

Remark. In this paper, contrary to [Lvo24], the generator of the Markov chain is not described explicitly. Rather, the Markov property is deduced from invariance properties of the Haar measure, as we briefly elaborate below.

1.1 Approach

Here, we say a few words about our approach. We will define an equivalence relation on matrices over R, not necessarily square, of arbitrary dimension:

$$M_1 \sim M_2$$

if and only if there exist n and m such that:

[2]Of course, this matrix is not Haar random, but many classes of random matrices can be proven to behave asymptotically in the same way as Haar random matrices. This is the universality phenomenon, that is discussed in particular in [Woo23, Section 3].

$$\left[\begin{array}{c|c} M_1 & 0 \\ \hline 0 & \mathbb{I}_n \end{array}\right] = g^T \left[\begin{array}{c|c} M_2 & 0 \\ \hline 0 & \mathbb{I}_m \end{array}\right] g' \qquad \text{for some } g, g' \in GL(R) \quad (1.3)$$

This equivalence relation has the property that two matrices are equivalent if and only if they have the same cokernel *and* the difference between the number of columns and the number of rows is the same for both matrices.

However, the equivalence relation turns out to be more convenient to work with, without any reference to the cokernel. Indeed, it follows almost immediately from the invariance properties of the Haar measure that

$$Haar_{n,n+u}(R)$$

induces a reversible Markov chain on equivalence classes of matrices, under the equivalence relation (1.3). Theorem 1.1 can then be deduced as a corollary.

There are two other reasons why it is preferable to work with equivalence classes of matrices rather than the modules that parametrize them.

- This point of view will add flexibility, as we can mildly modify the equivalence relation. Indeed, although we do not elaborate on this in the present paper, all the results go through if we consider a weaker equivalence relation than (1.3), namely if we replace the group $GL(R)$ by $SL(R)$.
- Most importantly, the point of view also has the potential of readily generalizing to the study of matrices with symmetry, such as symmetric, anti-symmetric, or Hermitian matrices. In these cases, the equivalence classes are not parametrized by modules, but by modules with extra information. Rather than pin down this extra information, it seems more convenient to work with the equivalence classes directly.

We will write $\mathbf{c}(M)$ to denote the equivalence class of M.

1.2 Outline

In §2, we make some remarks on the equivalence relation (1.3). In §3, we show that the equivalence class, to which a matrix M belongs, is determined by $coker(M)$ and by the difference between the number of rows and the number of columns of M. In §4, we show that the process induced by $Haar_{n.n+u}$ on equivalence classes is a Markov chain. In §5, we show that this Markov chain is recurrent. This is done by reducing to the finite field case. We also draw a connection to the recent work of Sawin and Wood, [SW24]. In §6, we define other transition operators, and show that a certain Markov chain is reversible. These results will imply that the process $coker(Haar_{n,n+u})$ is also a reversible Markov chain. In §7, we comment on the relation of the transition operators defined in [Lvo24] to the transition operators defined in this paper. Lastly, in §8, we discuss what happens when we change the ring R.

1.3 Previous work

The finite field case appears in many papers and it is difficult to find a precise attribution. The $\mathbb{Z}_p$ case was studied by Roger Van Peski, who computed, in particular, the joint distribution of $coker(Haar_{n,N})$ and $coker(Haar_{n,N+k})$ in [VP21, Theorem 1.3, part 2].

1.4 Acknowledgements

The general proof of reversibility was inspired by a fruitful e-mail exchange with Roger Van Peski.

2 The equivalence classes

$(R, \mathfrak{m})$ is a complete local ring with a finite residue field. $G \stackrel{\text{def}}{=\!=} GL(R)$.

We recall that, in §1.1, we have defined an equivalence relation, where $M_1 \sim M_2$ if and only if there exist n and m such that:

$$\left[\begin{array}{c|c} M_1 & 0 \\ \hline 0 & \mathbb{I}_n \end{array}\right] = g^T \left[\begin{array}{c|c} M_2 & 0 \\ \hline 0 & \mathbb{I}_m \end{array}\right] g' \qquad \text{for some } g, g' \in GL$$

Definition. For $u \in \mathbb{Z}$, $\mathcal{C}_u$ is the set of equivalence classes of matrices such that $\#\text{cols} - \#\text{rows} = u$

Recall that, given a matrix M, we denote by $\mathbf{c}(M)$ the equivalence class to which M belongs.

Remark. $\mathcal{C}_u$ has a distinguished element, i.e. the equivalence class of

$$\left[\begin{array}{c} 1 \end{array}\right] \text{ or } \left[\begin{array}{c} 1 \\ \mathbf{0} \end{array}\right] \text{ or } \left[\begin{array}{cc} 1 & \mathbf{0} \end{array}\right]$$

We will denote this equivalence class as $O_u(R)$.

Lemma 2.1. *A matrix M over R belongs to the equivalence class $O_u(R)$ if and only if $M \mod \mathfrak{m}$ belongs to $O_u(k)$.*

Proof. A square matrix over R is invertible if and only if its reduction $\mod \mathfrak{m}$ is invertible. Lemma 2.1 can be deduced from this fact using row and column operations. □

3 The cokernel map

Theorem 3.1. *The map*

$$C_u \xrightarrow{coker} R - \mathbf{mod}$$

is well-defined and injective

Proof. It follows from the definition of the equivalence relation that the map is well-defined. The injectivity follows from the uniqueness of minimal free resolutions of modules over local rings, [Eis95, Theorem 20.2]. □

Lemma 3.2. *coker*$(O_u(R)) \cong R^{|u|}$ *if* $u < 0$ *and coker*$(O_u(R))$ *is trivial if* $u \geq 0$.

Proof. This follows from the definition of $O_u(R)$. □

4 A random operator and a Markov chain on $\mathcal{C}_u$

First, we specify what we mean by a *random operator* from a set X to a set Y.

Definition. A random operator from X to Y is a linear operator from measures on X to measures on Y, that sends probability measure to probability measures.

Remark. The pro-finite ring R is equipped with a canonical measure, alternatively called the uniform measure, or the additive Haar measure.

Definition. We say an R-valued random variable is Haar random if it is distributed according to the Haar measure on R.

In this section, we will write $*$ to denote a Haar random entry in a matrix. If $*$ appears more than once, the corresponding entries will be *independent* Haar random variables.

Consider the random operator from $\mathrm{Mat}(R)$ to $\mathrm{Mat}(R)$, defined as

$$M \to \left[\begin{array}{c|c} M & \begin{matrix}*\\ \vdots \\ *\end{matrix} \\ \hline \begin{matrix}* & \dots & *\end{matrix} & * \end{array}\right] \tag{4.1}$$

Theorem 4.1. *(4.1) defines a random operator from* $\mathcal{C}_u$ *to* $\mathcal{C}_u$*, for all* u*.*

Proof of Theorem 4.1 We will prove Theorem 4.1 by proving Lemma 4.2 and Lemma 4.3. Together, these will imply Theorem 4.1. We will write

$$M_1 \sim M_2 \tag{4.2}$$

to denote that M_1 and M_2 are in the same class in $\mathcal{C}_u$. If M_1 and M_2 are random matrices, (4.2) will mean that the two matrices induce the same distribution on $\mathcal{C}_u$.

Lemma 4.2.

$$\left[\begin{array}{c|c|c} M & \mathbf{0} & \begin{matrix}*\\ \vdots \\ *\end{matrix} \\ \hline \mathbf{0} & \mathbf{I} & \begin{matrix}*\\ \vdots \\ *\end{matrix} \\ \hline \begin{matrix}* & \dots & *\end{matrix} & \begin{matrix}* & \dots & *\end{matrix} & * \end{array}\right] \sim \left[\begin{array}{c|c|c} M & \mathbf{0} & \begin{matrix}*\\ \vdots \\ *\end{matrix} \\ \hline \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \hline \begin{matrix}* & \dots & *\end{matrix} & \mathbf{0} & * \end{array}\right] \sim$$

$$\sim \left[\begin{array}{ccc|c} & M & & \begin{matrix}*\\ \vdots \\ *\end{matrix} \\ \hline * & \dots & * & * \end{array}\right]$$

Proof. It suffices to prove

$$\left[\begin{array}{ccc|c} & \mathbf{I} & & \begin{matrix}*\\ \vdots \\ *\end{matrix} \\ \hline * & \dots & * & * \end{array}\right] \sim \left[\begin{array}{ccc|c} & \mathbf{I} & & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hline 0 & \dots & 0 & * \end{array}\right]$$

Observe that

$$\left[\begin{array}{c|c} \mathbf{I} & \mathbf{v} \\ \hline \mathbf{w}^T & c \end{array}\right] \left[\begin{array}{c|c} \mathbf{I} & \mathbf{0} \\ \hline \mathbf{0} & c - \mathbf{w}^T\mathbf{v} \end{array}\right]$$

Now suppose that c, $\mathbf{v}$ and $\mathbf{w}$ are independent and Haar random. In particular c is Haar random and independent of $\mathbf{w}^T\mathbf{v}$.

Claim. *The sum of two independent random variables is Haar random if one of them is Haar random.*

The claim is a consequence of the fact the Haar distribution is invariant by translations. It follows that $c - \mathbf{w}^T\mathbf{v}$ is Haar random. This proves Lemma 4.2. □

Lemma 4.3.

$$\left[\begin{array}{ccc|c} & g^T M g' & & \begin{matrix}*\\ \vdots \\ *\end{matrix} \\ \hline * & \dots & * & * \end{array}\right] \sim \left[\begin{array}{ccc|c} & M & & \begin{matrix}*\\ \vdots \\ *\end{matrix} \\ \hline * & \dots & * & * \end{array}\right]$$

Proof. It suffices to show:

$$\left[\begin{array}{ccc|c} & g^T M g' & & \begin{matrix}*\\ \vdots \\ *\end{matrix} \\ \hline * & \dots & * & * \end{array}\right] = \left[\begin{array}{ccc|c} & g & & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hline 0 & \dots & 0 & 1 \end{array}\right]^T \left[\begin{array}{ccc|c} & M & & \begin{matrix}*\\ \vdots \\ *\end{matrix} \\ \hline * & \dots & * & * \end{array}\right] \left[\begin{array}{ccc|c} & g' & & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hline 0 & \dots & 0 & 1 \end{array}\right]$$

But this follows from the $GL_n(R)$-invariance of the Haar measure on R^n, for any n. This proves Lemma 4.2 and Theorem 4.1. □

Definition. We denote by Δ_u the random operator induced by (4.1) on $\mathcal{C}_u$.

$$M \to \left[\begin{array}{ccc|c} & & & * \\ & M & & \vdots \\ & & & * \\ \hline * & \dots & * & * \end{array}\right]$$

coker$\Big(\mathbf{Haar_{n,n+u}}\Big)$ is a Markov chain. We give a corollary of Theorem 4.1

Definition. Recall that $Haar$ be an infinite matrix, whose entries are indexed by $\mathbb{N} \times \mathbb{N}$, with Haar random variables. Recall also that $Haar_{n,n+u}$ denotes the top-left $n \times n+u$ minor.

Corollary 4.3.1. The random process coker$\Big(Haar_{n,n+u}\Big)$ is a Markov chain, generated by the operator Δ_u.

5 Positive recurrence of the Markov chain coker$\Big(Haar_{n,n+u}\Big)$

Theorem 5.1. *The Markov chain* $\mathbf{c}(Haar_{n,n+u})$ *is positive recurrent. Equivalently, the Markov chain*

$$coker(Haar_{n,n+u})$$

is positive recurrent.

We prove this by reducing to a question over the finite field k.

Lemma 5.2. $O_u(k)$ *is a positive recurrent state for the Markov chain*

$$\mathbf{c}(Haar_{n,n+u} \otimes k)$$

Proof. We prove Lemma 5.2 using two standard computations over finite fields:

- If $u \geq 0$

$$\mathbb{P}(Haar_{n,n+u}(k) \in O_u(k)) =$$

$$\mathbb{P}(dim_k columnspace(Haar_{n,n+u} \otimes k) = r) = \prod_{i=u+1}^{n+u} \left(1 - \frac{1}{|k|^i}\right)$$

- If $u < 0$

$$\mathbb{P}(Haar_{n,n+u}(k) \in O_u(k)) =$$

$$\mathbb{P}(dim_k rowspace(Haar_{n,n+u} \otimes k) = r) = \prod_{i=|u|+1}^{n} \left(1 - \frac{1}{|k|^i}\right)$$

Hence,

$$\lim_{n\to\infty} \mathbb{P}(Haar_{n,n+u}(k) \in O_r(k)) = \prod_{i=|u|+1}^{\infty} \left(1 - \frac{1}{|k|^i}\right)$$

□

Theorem 5.1 now follows from Lemma 5.2 by Lemma 2.1.

Corollary. *The operator Δ_u has a unique stationary measure and the distribution of $c_u\Big(Haar_{n,n+u}(R)\Big)$ converges to this stationary measure.*

We denote this measure as μ_u.

Explicit form of $\mu_u(R)$

Remark. From the work of Sawin and Wood, [SW24, Lemma 6.6, Lemma 6.7], it is possible to give explicit expressions for the measures $\mu_u(R)$, as a measure on modules, when $u \geq 0$. The general expression is given in [SW24, Lemma 6.7]. For the statement that their measure and our measure are the same, see the last line of the penultimate paragraph of [SW24, page 48].

6 More random operators; the proof of Theorem 1.1

In this section, we complete the proof of Theorem 1.1. Theorem 1.1 will follow by combining Corollary 6.3.1 with Corollary 4.3.1 and Theorem 3.1 in the previous section.

Consider the random operators:

$$M \to \left[\begin{array}{c} M \\ \hline * \quad \dots \quad * \end{array}\right] \text{ and } M \to \left[\begin{array}{c|c} M & * \\ & \vdots \\ & * \end{array}\right] \tag{6.1}$$

Theorem 6.1. *The two operators in (6.1) descend to random operators:*

$$d_{u-1,u} : \mathcal{C}_u \to \mathcal{C}_{u-1} \text{ and } d_{u+1,u,} : \mathcal{C}_u \to \mathcal{C}_{u+1},$$

respectively.

Proof. The proof is analogous to the proof of Theorem 4.1 above. □

Definition. We can similarly define:

$$d_{r,u} : \mathcal{C}_u \to \mathcal{C}_r \tag{6.2}$$

for any u and r in $\mathbb{Z}$. If $u > r$, then (6.2) is defined by adding $|u - r|$ random rows. If $u < r$, (6.2) is defined by adding $|u - r|$ random columns. If $u = r$, (6.2) is the identity operator.

Identities satisfied by $d_{r,u}$

Theorem 6.2. *The operators* $d_{r,u}$ *satisfy the following identites:*

(A) $d_{r,u}d_{u,s} = d_{r,s}$ *whenever* $u < r < s$ *or* $u > r > s$

(B) $d_{u,r}d_{r,u} = \Delta_u^{|u-r|}$

(C) $d_{r,u}$ *is the adjoint of* $d_{u,r}$*, with respect to the measures* μ_u *and* μ_r*.*

Proof. The first two properties follow immediately from the definitions. The last property is a consequence of Theorem 6.3 below. □

Another Markov Chain Given any $u \neq r$, the pair of operators

$$(d_{u,r}, d_{r,u}) \tag{6.3}$$

defines a Markov chain on the state space:

$$\mathcal{C}_u \cup \mathcal{C}_r$$

Theorem 6.3. *The operator (6.3) defines a reversible Markov chain on* $\mathcal{C}_u \cup \mathcal{C}_r$*.*

By taking the square of the operator (6.3), we get the following corollary of Theorem 6.3:

Corollary 6.3.1. The operator Δ_u defines a *reversible* Markov chain on $\mathcal{C}_u$.

We now prove Theorem 6.3. Without loss of generality, suppose that

$$r > u.$$

Lemma 6.4. *Suppose that* $\mathcal{M}$ *is a* $n \times n+u$ *random matrix, whose distribution is invariant under the action of* $GL_n \times GL_{n+u}$*. Then the total variation distance between the distributions of:*

$$\mathbf{c}\left[\begin{array}{c|c} \mathcal{M} & \begin{matrix} * & \dots & * \\ \vdots & \ddots & \vdots \\ * & \dots & * \end{matrix} \\ \hline & \begin{matrix} * & \dots & * \\ \vdots & \ddots & \vdots \\ * & \dots & * \end{matrix} \end{array}\right] \quad \textit{and} \quad \mathbf{c}\left[\begin{array}{c|c} \mathcal{M} & \mathbf{0} \\ \hline & \mathbf{I}_{r-u} \end{array}\right]$$

is bounded by $o(n)$*.*

Deduction of Theorem 6.3 from Lemma 6.4 First of all, observe that elementary column operations imply that:

$$\left[\begin{array}{c|c} & \mathbf{0} \\ \mathcal{M} & \hline \\ & \mathbf{I}_{r-u} \end{array}\right] \sim \left[\begin{array}{c} \\ \text{top left} \\ (n-(r-u))\times(n+u) \\ \text{corner of } \mathcal{M} \\ \\ \end{array}\right]$$

Now let $G_1 \in \mathcal{C}_r$ and $G_2 \in \mathcal{C}_u$. Take $\mathcal{M}$ to be the random matrix $Haar_{n,n+u}$, conditioned on $\mathbf{c}\Big(Haar_{n,n+u}\Big) = G_2$. Lemma 6.4 implies the following equality:

$$\mathbb{P}\left(\mathbf{c}(Haar_{n,n+r}) = G_1 \middle| \mathbf{c}(Haar_{n,n+u}) = G_2\right) =$$

$$= \mathbb{P}\left(\mathbf{c}(Haar_{n-(u-r),n+u}) = G_1 \middle| \mathbf{c}(Haar_{n,n+u}) = G_2\right) + o(n)$$

By the Markov property, the left hand side is

$$\mathbb{P}\left(G_2 \xrightarrow{d_{r,u}} G_1\right)$$

while the right hand side is

$$\mathbb{P}\left(G_1 \xrightarrow{d_{u,r}} G_2\right) \frac{\mathbb{P}(\mathbf{c}(Haar_{n+u,n+u-r}) = G_1)}{\mathbb{P}(\mathbf{c}(Haar_{n+u,n}) = G_2)} + o(n)$$

Taking the limit $n \to \infty$ yields:

$$\mathbb{P}(G_2 \xrightarrow{d_{r,u}} G_1)\mu_u(G_1) = \mathbb{P}(G_1 \xrightarrow{d_{u,r}} G_2)\mu_r(G_2)$$

6.1 The proof of Lemma 6.4

As the statement is about the distribution induced on $\mathcal{C}_r$, we can apply an element of GL to any matrix. This will not change the distribution induced on $\mathcal{C}_r$. In particular, we can apply a Haar random element of $GL_{n+u}(R)$, acting on the left.

Definition. Let $\mathcal{G}_{n+u}(R)$ denote a multiplicatively Haar random element of $GL_{n+u}(R)$.

Thus, it suffices to bound the total variation distance between the random matrices, of dimension $(n+u) \times (r-u)$:

$$\mathcal{G}_{n+u}(R) \left[\begin{array}{c} \mathbf{I}_{r-u} \\ \hline \mathbf{0} \end{array}\right] \text{ and } \left[\begin{array}{ccc} * & \dots & * \\ \vdots & \ddots & \vdots \\ * & \dots & * \\ \hline * & \dots & * \\ \vdots & \ddots & \vdots \\ * & \dots & * \end{array}\right] \tag{6.4}$$

Remark. Note that the column vectors the matrix on the left of (6.4) are the first $r-u$ column vectors of $\mathcal{G}$.

Lemma 6.5. *The distribution of the first $r-u$ vectors of $\mathcal{G}_{n+u}(R)$ is the restriction of the additive Haar measure to the set of all $(r-u)$-tuples of vectors that have full k-rank.*

Proof. First, we observe the following fact, whose proof is standard.

Lemma 6.5.1. *Let N be any natural number. Every $(r-u)$-tuple of vectors in R^N that are k-independent, can be completed to an N-tuple of k-independent vectors.*

Proof of Lemma 6.5 when R is finite: Suppose R is finite. Then $GL_{n+u}(R)$ is finite. Applying a uniformly random element of $GL_{n+u}(R)$ to

$$\left[\begin{array}{c} \mathbf{I}_{r-u} \\ \hline \mathbf{0} \end{array}\right]$$

produces a uniformly random element in the orbit

$$GL_{n+u}(R)\left[\begin{array}{c} \mathbf{I}_{r-u} \\ \hline \mathbf{0} \end{array}\right]$$

By Lemma 6.5.1, this is a uniformly random $(r-u)$-tuple of k-independent vectors in R^N. Hence, we have proven Lemma 6.5 for finite R

Proof of Lemma 6.5 when R is infinite: Now suppose that R is not finite. Then we know that Lemma 6.5 holds modulo any power of the maximal ideal. Because R is profinite, it also holds that Lemma 6.5 is true for R.

□

Thus, the total variation distance between the two random matrices is twice the probability that $r-u$ Haar random vectors over k are *not* independent.

Lemma 6.6. *The following expression gives the probability that the rank of an $(r-u)\times n+u$ Haar random matrix over k is less than (r-u).*

$$1-\prod_{i=1}^{r-u}\left(1-\frac{1}{|k|^{n+u-i+1}}\right)=o(n)$$

Proof. This is a standard calculation over finite fields. □

Combining Lemma 6.6 and Lemma 6.5 shows that the total variation distance between the random matrix distributions (6.4) is $o(n)$. By the discussion preceding (6.4), we conclude Lemma 6.4.

7 Relation with operators defined in [Lvo24]

In previous work, we defined the operators:

$$d,\ d^* \tag{7.1}$$

as certain explicit random operators on groups. Below, we give the relation of these operators to the ones studied in this paper.

Definition. We say a matrix over $\mathbb{Z}_p$ is singular if there is a non-trivial relation between the column vectors of M, and a non-trivial relation between the row vectors of M. If a matrix is singular, then every matrix in its equivalence class in $\mathcal{C}_u$ is also singular.

Theorem 7.1. *We have the following relations, when $R = \mathbb{Z}_p$:*

- *The restriction of $d_{-1,0}$ to non-singular equivalence classes coincides with the operator d^*, defined in [Lvo24].*
- *The restriction of $d_{0,-1}$ to non-singular equivalence classes coincides with the operator d, defined in [Lvo24].*
- *Hence, the operator $\Delta_0 \stackrel{\text{def}}{=\!=} d_{0,-1}d_{-1,0}$, defined above, coincides with the operator dd^*, when restricted to non-singular equivalence classes. (In [Lvo24], the operator dd^* is also denoted by the symbol " Δ_0 ".)*

Remark. The restriction to non-singular equivalences classes is not a serious restriction for the study of Haar random matrices over $\mathbb{Z}_p$, as in this case, the singular matrices are contained in a set of measure 0.

Proof. To prove Theorem 7.1, it suffices to show that

$$d^*\Big(\operatorname{coker}(M)\Big) = \operatorname{coker}\begin{bmatrix} M \\ \hline * & \dots & * \end{bmatrix}$$

for all non-singular $n \times n$ matrices M over $\mathbb{Z}_p$ and

$$d\Big(\operatorname{coker}(M)\Big) = \operatorname{coker}\left[\begin{array}{c|c} & * \\ M & \vdots \\ & * \end{array}\right]$$

for all non-singular $n+1 \times n$ matrices M over $\mathbb{Z}_p$. But this is shown in [Lvo24, Theorem 1.1]. □

8 Other comments

Remark. Any ring homomorphism $R \to R/I$ induces maps:

$$red_I : C_u(R) \to C_u(R/I) \tag{8.1}$$

We will call this the *reduction* map. The push-forward of reduction induces an operator from measures on $C_u(R)$ to measures on $C_u(R/I)$. Moreover, we can define the adjoint of reduction, with respect to the measures $\mu_u(R)$ and $\mu_u(R/I)$. The adjoint of reduction will be a random operator:

$$ind_I : C_u(R/I) \to C_u(R)$$

We will call this the *induction* operator.

Lemma 8.1. *The adjoint of (8.1) is explicitly given as follows. Given a matrix M over R/I, replace every entry of M by an independent Haar random element of its I-coset in R.*

Remark 8.1. On matrices, this operator is the adjoint of reduction modulo I, with respect to the Haar measure.

Proof. By arguments similar to those in the proof of Theorem 4.1, we verify that this induces a random operator from $C_u(R/I)$ to $C_u(R)$. The adjoint property follows from Remark 8.1. □

Theorem 8.2. *The operators defined above commute with the operators $d_{u,r}$.*

Proof. The commutativity can be verified on the level of matrices. □

Corollary. *The image of ind_I is a subspace of the space of signed measures on $C_\cdot(R)$ that is fixed by the operators $d_{\cdot,\cdot}$. The kernel of red_I is also a subspace of the space of signed measures on $C_\cdot(R)$ that is fixed by the operators $d_{\cdot,\cdot}$.*

References

[Eis95] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, New York, NY, 1995.

[LP] Nikita Lvov and Roger Van Peski. A note on the moment inversion problem for finite abelian p-groups. *in progress*.

[Lvo24] Nikita Lvov. A random walk on the category of finite abelian p-groups. *arXiv:math.PR/2408.06492v1*, 2024.

[SW24] Will Sawin and Melanie Matchett Wood. The moment problem for random objects in a category. *arXiv:math.PR/2210.06279v2*, 2024.

[VP21] Roger Van Peski. Limits and fluctuations of p-adic random matrix products. *Selecta Mathematica*, 27(5), October 2021.

[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.