Electron. Commun. Probab. **21** (2016), no. 49, 1–6.
DOI: 10.1214/16-ECP7
ISSN: 1083-589X

ELECTRONIC COMMUNICATIONS in PROBABILITY

Truncation of Haar random matrices in $\mathrm{GL}_N(\mathbb{Z}_m)$*

Yanqi Qiu†

Abstract

The asymptotic law of the truncated $S \times S$ random submatrix of a Haar random matrix in $\mathrm{GL}_N(\mathbb{Z}_m)$ as N goes to infinity is obtained. The same result is also obtained when $\mathbb{Z}_m$ is replaced by any commutative compact local ring whose maximal ideal is topologically closed.

Keywords: random matrix; invertible matrix; commutative compact local ring; truncation; asymptotic law.
AMS MSC 2010: Primary 60B20, Secondary 15B33; 60B10.
Submitted to ECP on February 26, 2016, final version accepted on June 23, 2016.

1 Introduction

In the theory of random matrices, some particular attention is payed recently to the asymptotic distributions of the truncated $S \times S$ upper-left corners of a large $N \times N$ random matrices from different matrix ensembles (CUE, COE, Haar Unitary Ensembles, Haar Orthogonal Ensembles), see [6, 4, 2, 1].

In the present paper, we consider the truncation of a Haar random matrix in $\mathrm{GL}_N(\mathbb{Z}_m)$ with $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. This research is motivated by its application in a forthcoming paper on the classification of ergodic measures on the space of infinite p-adic matrices, where the asymptotic law of a fixed size truncation of the Haar random matrix from the group of $N \times N$ invertible matrices over the ring of p-adic integers is essentially used and is derived from a particular case of our main result, Theorem 3.1. Remark that the ring of p-adic integers is isomorphic to the inverse limit of the rings $\mathbb{Z}_{p^n}$.

2 Notation

Fix a positive integer $m \in \mathbb{N}$. Consider the ring $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$. Let $\mathbb{Z}_m^\times$ be the multiplicative group of invertible elements of the ring $\mathbb{Z}_m$. For any $N \in \mathbb{N}$, denote by $M_N(\mathbb{Z}_m)$ the matrix ring over $\mathbb{Z}_m$ and denote by $\mathrm{GL}_N(\mathbb{Z}_m)$ the finite group of $N \times N$ invertible matrices over $\mathbb{Z}_m$. Note that we have

$$\mathrm{GL}_N(\mathbb{Z}_m) = \Big\{ A \in M_N(\mathbb{Z}_m) \Big| \det A \in \mathbb{Z}_m^\times \Big\}.$$

*This work is supported by the grant IDEX UNITI - ANR-11-IDEX-0002-02, financed by Programme "Investissements d'Avenir" of the Government of the French Republic managed by the French National Research Agency.

†CNRS, Institut de Mathématiques de Toulouse, Université Paul Sabatier, 118 Route de Narbonne, F-31062 Toulouse Cedex 9, France. E-mail: yqi.qiu@gmail.com

Let $\mathcal{U}_N(m)$ denote the uniform distribution on $M_N(\mathbb{Z}_m)$ and let $\mu_N(m)$ denote the uniform distribution on $\mathrm{GL}_N(\mathbb{Z}_m)$. Note that $\mu_N(m)$ is the normalized Haar measure of the group $\mathrm{GL}_N(\mathbb{Z}_m)$.

The cardinality of any finite set E is denoted by $|E|$.

3 Main result

Fix a positive integer $S \in \mathbb{N}$. If X is a $N \times N$ matrix (in what follows, the range of the coefficients of X can vary), then we denote by $X[S]$ the truncated upper-left $S \times S$ corner of X, i.e.,

$$X[S] := (X_{ij})_{1 \le i,j \le S}. \tag{3.1}$$

Let $X^{(N)}(m)$ be a random matrix sampled with respect to the normalized Haar measure of $\mathrm{GL}_N(\mathbb{Z}_m)$, that is, the probability distribution $\mathcal{L}(X^{(N)}(m))$ of the random matrix $X^{(N)}(m)$ satisfies

$$\mathcal{L}(X^{(N)}(m)) = \mu_N(m).$$

By adapting the notation (3.1), we denote by $X^{(N)}(m)[S]$ the truncated upper-left $S \times S$ corner of the random matrix $X^{(N)}(m)$, i.e.,

$$X^{(N)}(m)[S] := \left(X^{(N)}(m)_{ij}\right)_{1 \le i,j \le S}.$$

Theorem 3.1. *The probability distribution $\mathcal{L}(X^{(N)}(m)[S])$ of the truncated random matrix $X^{(N)}(m)[S]$ converges weakly, as N tends to infinity, to the uniform distribution $\mathcal{U}_S(m)$ on $M_S(\mathbb{Z}_m)$.*

Now we are going to prove Theorem 3.1.

For any positive integer $u \in \mathbb{N}$, we write $Q_u : \mathbb{Z} \to \mathbb{Z}_u = \mathbb{Z}/u\mathbb{Z}$ the quotient map. If v is another positive integer such that u divides v, then since $v\mathbb{Z} \subset u\mathbb{Z} = \ker(Q_u)$, the map Q_u induces in a unique way a map $Q_u^v : \mathbb{Z}_v \to \mathbb{Z}_u$. Note that the map $Q_u^v : \mathbb{Z}_v \to \mathbb{Z}_u$ is surjective and

$$\left|(Q_u^v)^{-1}(x)\right| = \frac{v}{u}, \forall x \in \mathbb{Z}_u, \tag{3.2}$$

that is, for each element $x \in \mathbb{Z}_u$, the cardinality of the pre-image of x is v/u.

By slightly abusing the notation, for any matrix $A = (a_{ij})_{1 \le i,j \le N}$ in $M_N(\mathbb{Z})$, we set

$$Q_u(A) := (Q_u(a_{ij}))_{1 \le i,j \le N}.$$

Similarly, for any matrix $B = (b_{ij})_{1 \le i,j \le N}$ in $M_N(\mathbb{Z}_v)$, we set

$$Q_u^v(B) := (Q_u^v(b_{ij}))_{1 \le i,j \le N}.$$

By the prime factorization theorem, we may write in a unique way

$$m = p_1^{r_1} \cdots p_s^{r_s}, \tag{3.3}$$

where $p_1, \cdots, p_s$ are distinct prime numbers and $r_1, \cdots, r_s$ are positive integers. By the Chinese remainder theorem, we have an isomorphism of the following two rings:

$$\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{r_s}}. \tag{3.4}$$

A natural isomorphism is provided by the map $\phi : \mathbb{Z}_m \longrightarrow \mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{r_s}}$ defined by

$$\phi(x) = (Q^m_{p_1^{r_1}}(x), \cdots, Q^m_{p_s^{r_s}}(x)), \quad \forall x \in \mathbb{Z}_m. \tag{3.5}$$

Simple case: Let us first assume that in the factorization (3.3), we have $s = 1$. For simplifying the notation, let us write $m = p^r$.

We write $\mathbb{F}_p$ for the finite field $\mathbb{Z}/p\mathbb{Z}$. We have the following characterization of $\mathrm{GL}_N(\mathbb{Z}_{p^r})$.

Theorem 3.2 ([3, Theorem 3.6]). *A matrix M is in $\mathrm{GL}_N(\mathbb{Z}_{p^r})$ if and only if $Q_p^{p^r}(M) \in \mathrm{GL}_N(\mathbb{F}_p)$.*

Given a matrix $W \in M_S(\mathbb{Z}_{p^r})$ such that $Q_p^{p^r}(W) \in \mathrm{GL}_S(\mathbb{F}_p)$, then a moment of thinking allows us to write

$$\left|\left\{X \in \mathrm{GL}_N(\mathbb{F}_p) : X(S) = Q_p^{p^r}(W)\right\}\right| = p^{S(N-S)} \cdot \prod_{j=0}^{N-S-1} (p^N - p^{S+j}), \tag{3.6}$$

where $p^{S(N-S)}$ the number of choices of $(X_{ij})_{1\le i\le S,\, S+1\le j\le N}$ with coefficients in $\mathbb{F}_p$ and $\prod_{j=0}^{N-S-1}(p^N - p^{S+j})$ is the number of choices of $(X_{ij})_{S+1\le i\le N,\, 1\le j\le N}$.

It follows that, for any matrix $W \in M_S(\mathbb{Z}_{p^r})$, we have

$$\left|\left\{X \in \mathrm{GL}_N(\mathbb{F}_p) : X(S) = Q_p^{p^r}(W)\right\}\right| \le p^{S(N-S)} \prod_{j=0}^{N-S-1} (p^N - p^{S+j}). \tag{3.7}$$

We also have for any matrix $W \in M_S(\mathbb{Z}_{p^r})$,

$$\left|\left\{X \in \mathrm{GL}_N(\mathbb{F}_p) : X(S) = Q_p^{p^r}(W)\right\}\right| \ge \prod_{i=0}^{S-1} (p^{N-S} - p^i) \prod_{j=0}^{N-S-1} (p^N - p^{S+j}), \tag{3.8}$$

where $\prod_{i=0}^{S-1}(p^{N-S} - p^i)$ is the number of choices of $(X_{ij})_{1\le i\le S,\, S+1\le j\le N}$ with coefficients in $\mathbb{F}_p$ such that

$$\mathrm{rank}\Big[(X_{ij})_{1\le i\le S,\, S+1\le j\le N}\Big] = S.$$

Recall that $X^{(N)}(m)$ is a random matrix sampled with respect to the Haar measure of $\mathrm{GL}_N(\mathbb{Z}_m) = \mathrm{GL}_N(\mathbb{Z}_{p^r})$. By combining (3.2), (3.7) and (3.8), we see that the cardinality

$$n_N(W) := \left|\left\{X \in \mathrm{GL}_N(\mathbb{Z}_{p^r}) : X(S) = W\right\}\right|$$

satisfies the relation

$$p^{r-1} \prod_{i=0}^{S-1} (p^{N-S} - p^i) \prod_{j=0}^{N-S-1} (p^N - p^{S+j}) \le n_N(W) \le p^{r-1} p^{S(N-S)} \prod_{j=0}^{N-S-1} (p^N - p^{S+j}).$$

As a consequence, for any $W_1, W_2 \in M_S(\mathbb{Z}_{p^r})$, the following relation holds:

$$\frac{\prod_{i=0}^{S-1}(p^{N-S} - p^i)}{p^{S(N-S)}} \le \frac{\mathbb{P}(X^{(N)}(m)[S] = W_1)}{\mathbb{P}(X^{(N)}(m)[S] = W_1)} \le \frac{p^{S(N-S)}}{\prod_{i=0}^{S-1}(p^{N-S} - p^i)}. \tag{3.9}$$

Hence we get

$$\lim_{N\to\infty} \frac{\mathbb{P}(X^{(N)}(m)[S] = W_1)}{\mathbb{P}(X^{(N)}(m)[S] = W_1)} = 1. \tag{3.10}$$

Since the set $M_S(\mathbb{Z}_m)$ is finite, the above equality (3.10) implies that $\mathcal{L}(X^{(N)}(m)[S])$ converges weakly, as N tends to infinity, to the uniform distribution $\mathcal{U}_S(m)$ on $M_S(\mathbb{Z}_m)$.

General case: It is clear that, for any $N \in \mathbb{N}$, the isomorphism ϕ defined in (3.5) induces in a natural way a ring isomorphism:

$$\phi_N : M_N(\mathbb{Z}_m) \xrightarrow{\simeq} M_N(\mathbb{Z}_{p_1^{r_1}}) \oplus \cdots \oplus M_N(\mathbb{Z}_{p_s^{r_s}}). \tag{3.11}$$

The restriction of ϕ_N on $\mathrm{GL}_N(\mathbb{Z}_m)$ induces a group isomorphism:

$$\phi_N : \mathrm{GL}_N(\mathbb{Z}_m) \xrightarrow{\simeq} \mathrm{GL}_N(\mathbb{Z}_{p_1^{r_1}}) \oplus \cdots \oplus \mathrm{GL}_N(\mathbb{Z}_{p_s^{r_s}}). \tag{3.12}$$

Obviously, we have

$$(\phi_N)_*(\mathcal{U}_N(m)) = \mathcal{U}_N(p_1^{r_1}) \otimes \cdots \otimes \mathcal{U}_N(p_s^{r_s}) \tag{3.13}$$

and

$$(\phi_N)_*(\mu_N(m)) = \mu_N(p_1^{r_1}) \otimes \cdots \otimes \mu_N(p_s^{r_s}). \tag{3.14}$$

In particular, if $X^{(N)}(p_1^{r_1}), \cdots, X^{(N)}(p_s^{r_s})$ are independent Haar random matrices in $\mathrm{GL}_N(\mathbb{Z}_{p_1^{r_1}}), \cdots, \mathrm{GL}_N(\mathbb{Z}_{p_s^{r_s}})$ respectively, then the random matrix

$$\phi_N^{-1}(X^{(N)}(p_1^{r_1}) \oplus \cdots \oplus X^{(N)}(p_s^{r_s}))$$

is a Haar random matrix in $\mathrm{GL}_N(\mathbb{Z}_m)$. Moreover, we have

$$\phi_N^{-1}(X^{(N)}(p_1^{r_1}) \oplus \cdots \oplus X^{(N)}(p_s^{r_s}))[S] = \phi_S^{-1}(X^{(N)}(p_1^{r_1})[S] \oplus \cdots \oplus X^{(N)}(p_s^{r_s})[S]).$$

Hence $X^{(N)}(m)[S]$ and $\phi_S^{-1}(X^{(N)}(p_1^{r_1})[S] \oplus \cdots \oplus X^{(N)}(p_s^{r_s})[S])$ are identically distributed. By the previous result, we know that for any $i = 1, \cdots, s$, the law of $X^{(N)}(p_i^{r_i})[S]$ converges weakly to the uniform distribution $\mathcal{U}_S(p_i^{r_i})$ on $M_S(\mathbb{Z}_{p_i^{r_i}})$. It follows that the law of $X^{(N)}(m)[S]$ converges weakly to

$$(\phi_S^{-1})_*(\mathcal{U}_S(p_1^{r_1}) \otimes \cdots \otimes \mathcal{U}_S(p_s^{r_s})) = \mathcal{U}_S(m).$$

We thus complete the proof of Theorem 3.1.

4 A generalization

Let $\mathbb{F}_q$ denote the finite field with cardinality $q = p^n$. Consider the Haar random matrix $Z^{(N)}$ in $\mathrm{GL}_N(\mathbb{F}_q)$. Then we have

Theorem 4.1. *The probability distribution $\mathcal{L}(Z^{(N)}[S])$ of the truncated random matrix $Z^{(N)}[S]$ converges weakly, as N tends to infinity, to the uniform distribution on $M_S(\mathbb{F}_q)$.*

Proof. By combinatorial arguments, we have a similar estimate as (3.9) and the proof of Theorem 4.1 then follows immediately. Here we omit the details. □

Let $(\mathscr{A}, +, \cdot)$ be a topological commutative ring with identity which is compact, thus by assumption, the two operations $+, \cdot : \mathscr{A} \times \mathscr{A} \to \mathscr{A}$ are both continuous. Assume also that $\mathscr{A}$ is a local ring. Recall that by local ring, we mean that $\mathscr{A}$ admits a unique maximal ideal. Let us denote the maximal ideal of $\mathscr{A}$ by $\mathfrak{m}$. If we denote by $\mathscr{A}^\times$ the multiplicative group of the $\mathscr{A}$, then we have $\mathfrak{m} = \mathscr{A} \setminus \mathscr{A}^\times$. Moreover, let us assume that $\mathfrak{m}$ is closed.

Remark 4.2. If $m = p_1^{r_1} \cdots p_s^{r_s}$ with $s \geq 2$, then the ring $\mathbb{Z}_m$ is not local. Thus the results in §3 are not a particular case of Theorem 4.6.

Denote by $\nu_{\mathscr{A}}$ the normalized Haar measure on the compact additive group $(\mathscr{A}, +)$.

Lemma 4.3 ([5, Lemma 3])**.** *The quotient ring $\mathscr{A}/\mathfrak{m}$ is a finite field.*

As a consequence, there exists a positive integer $q = p^n$ with p a prime number and n a positive integer, such that $|\mathscr{A}/\mathfrak{m}| = q$ and $\mathscr{A}/\mathfrak{m} \simeq \mathbb{F}_q$. Let $\{a_i : i = 0, \cdots, q-1\}$ be a subset of $\mathscr{A}$ which forms a complete set of representatives of $\mathscr{A}/\mathfrak{m}$, assume moreover that $a_0 = 0 \in \mathscr{A}$.

From now on, as a set, we will identify $\{a_i : i = 0, \cdots, q-1\}$ with $\mathbb{F}_q$. For instance, under this identification, we may write

$$\mathscr{A} = \bigsqcup_{i=0}^{q-1} (a_i + \mathfrak{m}) = \bigsqcup_{x \in \mathbb{F}_q} (x + \mathfrak{m}),$$

we also identify the following subset of $M_N(\mathscr{A})$:

$$\Big\{ X = (X_{ij})_{1 \leq i,j \leq N} \Big| X_{ij} \in \{a_i : 0 \leq i \leq q-1\}, \det X \in \mathscr{A}^\times \Big\} \tag{4.1}$$

with the set $\mathrm{GL}_N(\mathbb{F}_q)$.

Since $\mathscr{A}^\times$ is closed, indeed, the group of invertible matrices over $\mathscr{A}$:

$$\mathrm{GL}_N(\mathscr{A}) = \Big\{ A \in M_N(\mathscr{A}) \Big| \det A \in \mathscr{A}^\times \Big\},$$

as a closed subset of $M_N(\mathscr{A})$, is compact. As a consequence, we may speak of Haar random matrix in $\mathrm{GL}_N(\mathscr{A})$, let $Y^{(N)}$ be such a random matrix. We would like to study the asymptotic law of the truncated random matrix $Y^{(N)}[S]$ as N goes to infinity.

Lemma 4.4. *We have*

$$\mathrm{GL}_N(\mathscr{A}) = \bigsqcup_{X \in \mathrm{GL}_N(\mathbb{F}_q)} (X + M_N(\mathfrak{m})), \tag{4.2}$$

where we identify $\mathrm{GL}_N(\mathbb{F}_q)$ *with the set given by* (4.1).

Proof. It is easy to see that for any $X \in \mathrm{GL}_N(\mathbb{F}_q)$ and any $X' \in M_N(\mathfrak{m})$, we have

$$\det(X + X') \equiv \det X (\bmod \mathfrak{m}),$$

and hence $\det(X + X') \in \mathscr{A}^\times$. This implies that the set on the right hand side of (4.2) is contained in $\mathrm{GL}_N(\mathscr{A})$. Conversely, an element $A \in \mathrm{GL}_N(\mathscr{A}) \subset M_N(\mathscr{A})$ corresponds naturally to a matrix $X_A \in M_N(\mathscr{A})$ all of whose coefficients are in $\mathbb{F}_q$ (identified with $\{a_i : 0 \leq i \leq q-1\}$) such that

$$A \equiv X_A (\bmod \mathfrak{m}) \text{ and } \det A \equiv \det X_A (\bmod \mathfrak{m}).$$

As a consequence, $\det X_A \in \mathscr{A}^\times$ and hence $X_A \in \mathrm{GL}_N(\mathbb{F}_q)$. This shows that $\mathrm{GL}_N(\mathscr{A})$ is contained in the set on the right hand side of (4.2).

Finally, by the definition of the set $\mathrm{GL}_N(\mathbb{F}_q)$ in (4.2), it is clear that all the subsets $X + M_N(\mathfrak{m}), X \in \mathrm{GL}_N(\mathbb{F}_q)$ are disjoint. □

As an immediate consequence of Lemma 4.4, we have the following corollary. First recall that we have identified $\mathrm{GL}_N(\mathbb{F}_q)$ with the set (4.1), hence the random matrix $Z^{(N)}$ may be considered as a random matrix sampled uniformly from the set (4.1). Note that $M_N(\mathfrak{m}) \simeq \mathfrak{m}^{N \times N}$ is equipped with the uniform probability

$$(q^{-1} \nu_{\mathscr{A}}|_{\mathfrak{m}})^{\otimes (N \times N)}. \tag{4.3}$$

Corollary 4.5. *Assume that we are given a random matrix* $U^{(N)}$ *sampled uniformly from* $M_N(\mathfrak{m})$, *which is independent from the random matrix* $Z^{(N)}$. *The the random matrix*

$$Z^{(N)} + U^{(N)}$$

is a Haar random matrix in $\mathrm{GL}_N(\mathscr{A})$.

Note that the distributions of the two random matrices $U^{(S)}$ and $U^{(N)}[S]$ coincide.

Theorem 4.6. *The probability distribution $\mathcal{L}(Y^{(N)}[S])$ of the truncated random matrix $Y^{(N)}[S]$ converges weakly, as N tends to infinity, to the uniform distribution $\nu_{\mathscr{A}}^{\otimes(S\times S)}$ on $M_S(\mathscr{A})$.*

Proof. By Corollary 4.5, the random matrices $Y^{(N)}[S]$ and $Z^{(N)}[S]+U^{(N)}[S]$ are identically distributed. Now by Theorem 4.1, the probability distribution $\mathcal{L}(Z^{(N)}[S])$ converges weakly, as N goes to infinity, to the uniform distribution on $M_S(\mathbb{F}_q)$, hence the probability distribution $\mathcal{L}(Y^{(N)}[S]) = \mathcal{L}(Z^{(N)}[S]+U^{(N)}[S])$ converges weakly, as N goes to infinity, to the probability distribution of the random matrix

$$V^{(S)} + U^{(S)},$$

where $V^{(S)}$ and $U^{(S)}$ are independent, $V^{(S)}$ is sampled uniformly from $M_S(\mathbb{F}_q)$ and $U^{(S)}$ is sampled uniformly from $M_N(\mathfrak{m})$. We complete the proof of Theorem 4.6 by noting that $V^{(S)}+U^{(S)}$ is uniformly distributed on $M_S(\mathscr{A})$. $\square$

References

[1] Zhishan Dong, Tiefeng Jiang, and Danning Li: Circular law and arc law for truncation of random unitary matrix. *J. Math. Phys.*, 53(1):013301, 14, 2012. MR-2919538

[2] Yan V. Fyodorov and Boris A. Khoruzhenko: A few remarks on colour-flavour transformations, truncations of random unitary matrices, Berezin reproducing kernels and Selberg-type integrals. *J. Phys. A*, 40(4):669–699, 2007. MR-2303596

[3] Christopher J. Hillar and Darren L. Rhea: Automorphisms of finite abelian groups. *Amer. Math. Monthly*, 114(10):917–923, 2007. MR-2363058

[4] J. Novak: Truncations of random unitary matrices and Young tableaux. *Electron. J. Combin.*, 14(1):Research Paper 21, 12, 2007. MR-2285825

[5] Seth Warner: Compact noetherian rings. *Math. Ann.*, 141:161–170, 1960. MR-0118749

[6] Karol Życzkowski and Hans-Jürgen Sommers: Truncations of random unitary matrices. *J. Phys. A*, 33(10):2045–2057, 2000. MR-1748745