DISTRIBUTION OF COKERNELS OF \((n+u) \times n\) MATRICES OVER \(\mathbb{Z}_p\)

LING-SANG TSE

Abstract. Let \(n, u \geq 0\), \(M\) be a \((n+u) \times n\) matrix over \(\mathbb{Z}_p\), and \(G\) be a finite abelian \(p\)-group group. We find that the probability that the cokernel of \(M\) is isomorphic to \(\mathbb{Z}_p^u \oplus G\) as \(n\) goes to infinity is exactly what is expected from Cohen-Lenstra heuristics for the classical case when \(u\) is negative.

1. Outline of the paper

The goal of this paper is to prove the following theorem:

**Theorem 1.1.** Let \(n, u \geq 0\), \(M\) be a randomly chosen \((n+u) \times n\) matrix over \(\mathbb{Z}_p\), and \(G\) be a finite abelian \(p\)-group group. Then

\[
\lim_{n \to \infty} \mathbb{P}(\text{coker } M \cong \mathbb{Z}_p^u \oplus G) = \prod_{i=1}^\infty \left(1 - \frac{p^{-i-u}}{|G|^u |\text{Aut } G|}\right).
\]

Notation: For the rest of this paper, let \(n, u \geq 0\), \(M\) be a randomly chosen \((n+u) \times n\) matrix over \(\mathbb{Z}_p\), and \(G\) be a finite abelian \(p\)-group group. Also, let \(\mu\) be the standard Haar measure on the set of \((n+u) \times n\) matrices over \(\mathbb{Z}_p\) such that \(\mu(\{(n+u) \times n\ \text{matrices over } \mathbb{Z}_p\}) = 1\).

We prove Theorem 1.1 using the following lemmas:

**Lemma 1.2.** For any \((n+u) \times n\) matrix \(M\) over \(\mathbb{Z}_p\), the probability that \(M\) has rank \(n\) is 1.

**Lemma 1.3.** If \(M\) is a random \((n+u) \times n\) over \(\mathbb{Z}_p\), then

\[
\lim_{n \to \infty} \mathbb{E}_\mu(\#\text{Sur (coker } M, G)) = |G|^u
\]

Note that from Lemma 1.2 the probability that \(M\) has cokernel isomorphic to \(\mathbb{Z}_p^u \oplus T\) for some abelian \(p\)-group \(T\) is 1, so what the lemma really meant to say is \(\lim_{n \to \infty} \mathbb{E}_\mu(\#\text{Sur (}\mathbb{Z}_p^u \oplus T, G)) = |G|^u\).

**Lemma 1.4.** If \(M\) is a random \((n+u) \times n\) over \(\mathbb{Z}_p\), then

\[
\lim_{n \to \infty} \mathbb{E}_\mu(\#\text{Sur ((coker } M)[p^\infty], G)) = |G|^u
\]

Similarly as in Lemma 1.3, what Lemma 1.4 meant is \(\lim_{n \to \infty} \mathbb{E}_\mu(\#\text{Sur (}T, G)) = |G|^u\).

2. Proofs

**Proof of Lemma 1.2** An alternate, more combinatorial, proof of this lemma is presented in the appendix in A.1. Here, we present a much nicer proof.
An \((n + u) \times n\) matrix has rank \(n\) if and only if it has an \(n \times n\) submatrix with rank \(n\), so it is sufficient to show that the probability that an \(n \times n\) matrix has rank \(n\) is 1.

Claim 1.2.1: Fix a polynomial \(f\) in \(\mathbb{Z}_p\) over \(n\) variables. The probability of picking a random point \((a_1, \ldots, a_n)\) in \((\mathbb{Z}_p)^n\) so that \(f\) vanishes at \((a_1, \ldots, a_n)\) is 0.

Proof of Claim 1.2.1 by induction: If \(n\) is 1, this is clear because the polynomial has finitely many roots.

Assume this is true for \(n - 1\) variables, and let \(f\) be a polynomial in \(n\) variables over \(\mathbb{Z}_p\). At any given given point in \((a_1, \ldots, a_n) \in (\mathbb{Z}_p)^n\), consider \(g(x_n) := f(a_1, \ldots, a_{n-1}, x_n)\) as a polynomial in the one variable \(x_n\). The coefficients of \(g(x_n)\) are polynomials in \(n - 1\) variables, so by induction, the probability of picking a random point \((a_1, \ldots, a_n)\) in \((\mathbb{Z}_p)^n\) so that all of the coefficients of the corresponding polynomial \(g(x_n)\) are 0 is 0. Thus, the probability that \(g(x_n)\) is a non-trivial polynomial is 1, so as in the 1 variable case, the probability that \(g(a_n) = f(a_1, \ldots, a_n) = 0\) is 0. This completes the proof of Claim 1.2.1.

An \(n \times n\) matrix has rank \(n\) if and only if its determinant is 0, and the determinant of an \(n \times n\) matrix is a fixed polynomial in \(n^2\) variables evaluated at a random point in \((\mathbb{Z}_p)^{n^2}\). Thus, by Claim 1.2.1, the probability that an \(n \times n\) matrix has rank \(n\) is 0.

Proof of Lemma 1.3 Let \(M\) be a random \((n + u) \times n\) matrix over \(\mathbb{Z}_p\). We have

\[
\mathbb{E}_\mu \#(\text{Sur (coker } M, G)) = \int \sum_{\{M: \mathbb{Z}_p^n \to \mathbb{Z}_p^{n+u}\}} \sum_{\{\phi: \text{coker } M \to G\}} 1
\]

\[
= \sum_{\{\phi: \mathbb{Z}_p^{n+u} \to G\}} \int \sum_{\{M: \mathbb{Z}_p^n \to \mathbb{Z}_p^{n+u}\} \text{ such that im } M \subseteq \ker \phi} d\mu
\]

\[
= \sum_{\{\phi: \mathbb{Z}_p^{n+u} \to G\}} |G|^{-n}
\]

The last equality follows because \(\ker \phi\) has index \(|G|\) in \(\mathbb{Z}_p^{n+u}\), so the probability that any of the basis element maps into \(\ker \phi\) is \(|G|^{-1}\). \(M\) is determined by where the \(n\) basis elements are mapped to, so the probability that \(\text{im } M \subseteq \ker \phi\) is \(|G|^{-n}\).

Therefore, we have

\[
\lim_{n \to \infty} \mathbb{E}_\mu \#(\text{Sur (coker } M, G)) = \lim_{n \to \infty} \sum_{\{\phi: \mathbb{Z}_p^{n+u} \to G\}} |G|^{-n}
\]

\[
= \lim_{n \to \infty} \sum_{\{\phi: \mathbb{Z}_p^{n+u} \to G\}} |G|^{-n}
\]

\[
= \frac{|G|^{n+u}}{|G|^n}
\]

\[
= |G|^u
\]

The second last equality follows because as \(n \to \infty\), \(#\text{Hom } (\mathbb{Z}_p^{n+u}, G) \sim \#\text{Sur } (\mathbb{Z}_p^{n+u}, G)\)
(We present a proof of this in the appendix in A.2).
DISTRIBUTION OF COKERNELS OF \((n+u) \times n\) MATRICES OVER \(\mathbb{Z}_p\)

This completes the proof of lemma 1.3.

Proof of Lemma 1.4

As in the note beneath the statement of Lemma 1.3, let \(\mathbb{Z}_p^u \oplus T\) be the cokernel of an \((n+u) \times n\) matrix. We have

\[
\sum_{H \leq G} \# \text{Sur} \left( \mathbb{Z}_p^u \oplus T, H \right) = \# \text{Hom} \left( \mathbb{Z}_p^u \oplus T, G \right)
= \# \text{Hom} \left( \mathbb{Z}_p^u, G \right) \# \text{Hom} \left( T, G \right)
= |G|^u \left( \sum_{H \leq G} \# \text{Sur} \left( T, H \right) \right)
\]

Therefore,

\[
\# \text{Sur} \left( T, G \right) = \sum_{H \leq G} \frac{\# \text{Sur} \left( \mathbb{Z}_p^u \oplus T, H \right)}{|G|^u} - \sum_{H \leq G} \# \text{Sur} \left( T, H \right)
\]

We prove Lemma 1.4 by inducting on the order of \(|G|\).

If \(G\) is the trivial group, then it is clear that \(\mathbb{E}_\mu \left( \# \text{Sur} \left( \text{coker} \ M \right)[p^\infty] \right) = |G|^u = 1\).

We proceed with the induction, and assume that the hypothesis is true for any group of order less than \(|G|\).

\[
\mathbb{E}_\mu \left( \# \text{Sur} \left( T, G \right) \right) = \sum_{H \leq G} \frac{\mathbb{E}_\mu \left( \# \text{Sur} \left( \mathbb{Z}_p^u \oplus T, H \right) \right)}{|G|^u} - \sum_{H \leq G} \mathbb{E}_\mu \left( \# \text{Sur} \left( T, H \right) \right)
= \sum_{H \leq G} \frac{|H|^u}{|G|^u} - \sum_{H \leq G} |H|^{-u}
\]

where the second equality follows by Lemma 1.3 and by the induction hypothesis.

Claim 1.4.1: If \(n \mid |G|\),

\[
\# \left\{ \text{subgroups of } G \text{ of order } n \right\} = \# \left\{ \text{subgroups of } \hat{G} \text{ of index } n \right\}
\]

Proof of Claim 1.4.1: We show

\[
\# \left\{ \text{subgroups of } G \text{ of order } n \right\} = \# \left\{ \text{subgroups of } \hat{G} \text{ of index } n \right\}
= \# \left\{ \text{subgroups of } G \text{ of index } n \right\}
\]

To show the second equality, we may define an isomorphism \(\phi_2\) from \(G\) to \(\hat{G}\): For a cyclic group \(G_0\) with generator \(\alpha_0\), we map \(\alpha_0\) to the character \(\alpha_0 \mapsto e^{2\pi i/|G|}\). Then for a general finite abelian group \(G\), we decompose \(G\) into a product of cyclic groups and extend the map the natural way by taking the product of the maps on the cyclic groups. It is easy to check that \(\phi_2\) is a well-defined isomorphism, so the second equality follows.
To show the first equality, we define a bijective map of sets $\phi_1$ mapping a subgroup of $G$ of order $n$ to a subgroup of $\hat{G}$ of index $n$. Let $H^\perp := \{ \chi \in \hat{G} \mid \chi(h) = 1 \text{ for all } h \in H \}$, and we define $\phi_1$ by $\phi_1(H) = H^\perp$. By the universal property of quotients, given a character $\chi \in \hat{G}$, $H$ is contained in the kernel of $\chi$ if and only if there exists a homomorphism $\overline{\chi} : G/H \to \mathbb{C}$ such that $\chi(g) = \overline{\chi}(\overline{g})$ for all $g \in G$. Thus, every $\chi \in H^\perp$ corresponds to a character $\overline{\chi} \in \hat{G}/H$ by reduction mod $H$, and so $H^\perp \cong \hat{G}/H$. As in the previous paragraph, $\hat{G}/H \cong G/H$, and it is easy to check that $H^\perp$ is a subgroup of $\hat{G}$, so $H^\perp$ is a subgroup of $\hat{G}$ of index $n$. Thus $\phi_1$ is well-defined and is injective.

It remains to check that $\phi_2$ is a bijection: By definition of $(H^\perp)^\perp$, $H \subseteq (H^\perp)^\perp$ (where we treat $h \in H \subseteq \hat{G}$ as evaluation at $h$). Since $|(H^\perp)^\perp| = |H|$, we have $(H^\perp)^\perp = H$.

The proof of Claim 1.4.1 is complete.

Therefore,

$$
\mathbb{E}_\mu (\# \text{Sur} (T, G)) = \sum_{H \leq G} \frac{|H|^u}{|G|^u} - \sum_{H \leq G} \frac{|H|^{-u}}{|G|^{-u}} = |G|^{-u}
$$

This completes the proof of Lemma 1.4, and we can finally prove our main theorem.

**Proof of Theorem 1.1.** We apply the following theorem, due to Wood:

**Theorem 2.1.** [4, Theorem 8.3] Let $X_n$ be a sequence of random variables taking values in finitely generated abelian groups. Let $a$ be a positive integer and $A$ be the set of (isomorphism classes of) abelian groups with exponent dividing $a$. Suppose that for every $G \in A$, we have

$$
\lim_{n \to \infty} \mathbb{E}(\# \text{Sur} (X_n, G)) \leq |\wedge^2 G|.
$$

Then for every $H \in A$, the limit $\lim_{n \to \infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \cong H)$ exists, and for all $G \in A$ we have

$$
\sum_{H \in A} \lim_{n \to \infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \cong H) \# \text{Sur}(H, G) \leq |\wedge^2 G|.
$$

Suppose $Y_n$ is a sequence of random variables taking values in finitely generated abelian groups such that for every $G \in A$, we have

$$
\lim_{n \to \infty} \mathbb{E}(\# \text{Sur}(Y_n, G)) \leq |\wedge^2 G|.
$$

Then, we have that for every $H \in A$

$$
\lim_{n \to \infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \cong H) = \lim_{n \to \infty} \mathbb{P}(Y_n \otimes \mathbb{Z}/a\mathbb{Z} \cong H).
$$

Pick random finite $p$-groups $Y_n$ with probability

$$
\prod_{i=1}^\infty (1 - p^{-i-u}) \frac{1}{|G|^{i-u} |\text{Aut} G|},
$$

and denote the expectation values with respect to this probability measure $\mathbb{E}_Y$. 
By Theorem 3.20 in [Majumder],
\[
\sum_{G \text{ is a } p\text{-group}} \frac{1}{|G^u| \cdot |\text{Aut } G|} = \prod_{i=1}^{\infty} (1 - p^{-i-u})^{-1},
\]
so this is a well-defined probability distribution.

We apply the following theorem, also due to Wood, to get
\[
\lim_{n \to \infty} \mathbb{E}_\mu(\#\text{Sur}(T, G)) = \lim_{n \to \infty} \mathbb{E}_Y(\#\text{Sur}(Y, G)) = |G|^{-u}
\]

Theorem 2.2. [5, Theorem 3.2] Let \(Y\) be a random \(p\)-group chosen with probability
\[
\prod_{i=1}^{\infty} (1 - p^{-i-u})
\]
Then for every finite abelian group \(G\) with exponent dividing \(a\), we have
\[
\mathbb{E}(\#\text{Sur}(Y, G)) = |G|^{-u}
\]

Let \(a = p|G|\), and we apply Theorem 2.1 to get
\[
\lim_{n \to \infty} P(\text{rank } M \cong n) = \prod_{i=1}^{\infty} (1 - p^{-i-u})
\]
and so
\[
\lim_{n \to \infty} P(\text{coker } M \cong \mathbb{Z}_p^u \oplus G) = \prod_{p \in P} \prod_{i=1}^{\infty} (1 - p^{-i-u})
\]
This completes the proof of Theorem 1.1. Similarly, we may get the following corollary for a matrix over \(\mathbb{Z}\):

Corollary 2.3. Let \(n, u \geq 0\), \(M\) be a randomly chosen \((n+u) \times n\) matrix over \(\mathbb{Z}\), \(G\) be a finite abelian group, and \(P\) be the set of primes dividing \(|G|\). Then
\[
\lim_{n \to \infty} P(\text{coker } M \cong \mathbb{Z}_p^u \oplus G) = \prod_{p \in P} \prod_{i=1}^{\infty} (1 - p^{-i-u})
\]

3. APPENDIX

A.1 Alternative proof of Lemma 1.2

We prove Lemma 1.2 by showing the following:

1. The rank of \(M\) is equal to \(n\) if and only if \(\exists e > 0\) such that \((p^e \mathbb{Z})^n \subset \text{im } M\). To be precise, what is meant by \((p^e \mathbb{Z})^n \subset \text{im } M\) in the rest of this proof is whether there exists an embedding of \((p^e \mathbb{Z})^n\) into \(\text{im } M\).

Then by Nakayama’s lemma, for all \(e \geq 0\), \(e' > e\), \(\mathbb{P}(\text{rank } M = n) \geq \mathbb{P}\left(\frac{p^e \mathbb{Z}^n}{p^{e'} \mathbb{Z}^n} \subset \text{im } M \text{ (mod } p^{e'})\right)\).

2. If \(e' > e > 0\), \(\mathbb{P}(\frac{p^e \mathbb{Z}}{p^{e'} \mathbb{Z}}^n \subset \text{im } M) \geq \left(\frac{(n+u)!}{u!}\right)^{1/n} p^{-ue-u-e-1}\), which goes to 0 as \(e\) goes to infinity.

Step 1: We show that the rank of \(M\) is equal to \(n \iff \exists e > 0\) such that \((p^e \mathbb{Z})^n \subset \text{im } M\).
(\implies)

\[ \text{rank } M = n \]

\[ \iff \exists \text{ an } n \times n \text{ matrix of minor with nonvanishing determinant} \]

\[ \iff \text{im } M \text{ is minimally generated by } \{v_i\}_{i=1}^n \text{ for some } v_i = (v_{ij})_{1 \leq j \leq n} \in \mathbb{Z}_p^n \]

Let \( e = \max \{ \text{ord}_p (v_{ij}) \} \). Then

\[ \text{im } M \text{ is minimally generated by } \{v_i\}_{i=1}^n \iff (p^e\mathbb{Z}_p)^n \subset \text{im } M \]

(\implies) Let \( e_i \) be the standard \( i^{th} \) basis vector. We may assume that there exists \( e > 0 \) such that \( p^e e_i \in \text{im } M \) for all \( i \) satisfying \( 1 \leq i \leq n \). Then for all \( i \), there exist \( v_1, \ldots, v_n \in \mathbb{Z}_p^n \) such that \( Mv_i = p^e e_i \). Then \( M(p^{-e}v_i) = e_i \) for all \( i \) (if we extend the action of \( M \) to \( \mathbb{Q}_p^n \), so there exists an \( n \times n \) matrix of minors of \( M \) such that \( \det M \neq 0 \). It follows that the rank \( M \) is \( n \). \( \bullet \)

Step 2: We finish the proof by showing that if \( e' > e > 0 \), then

\[ \mathbb{P} \left( \left( \frac{p^e\mathbb{Z}}{p^{e'}\mathbb{Z}} \right)^n \subset \text{im } M \right) \geq p^{-(n-1)n+(n+u)^2} \prod_{i=1}^{n+u} (1 - p^{-i}). \]

Let \( \tilde{M} \in \left( \frac{\mathbb{Z}}{p^e\mathbb{Z}} \right)^{(n+u)\times n} \), and suppose \( \left( \frac{p^e\mathbb{Z}}{p^{e'}\mathbb{Z}} \right)^n \nsubseteq \text{im } \tilde{M} \). Then we may post-compose \( M \) with an automorphism of \( \left( \frac{p^e\mathbb{Z}}{p^{e'}\mathbb{Z}} \right)^{(n+u)\times n} \) fixing \( \left( \frac{p^{e+1}\mathbb{Z}}{p^{e'}\mathbb{Z}} \right)^{(n+u)\times n} \) such that \( \text{im } \tilde{M} \) does not contain any of the vectors in the set \( \{(0, \ldots, 0, p^e, 0, \ldots, 0)\}_{i=n-1}^{n+u} \), with the \( p^e \) in the \( i^{th} \) place.

Counting the number of choices for \( \phi \circ \tilde{M} \) is equivalent to counting the number of \((n+u)\times n\) matrices of the form

\[
\begin{bmatrix}
\frac{Z}{p^e\mathbb{Z}} & \cdots & \frac{Z}{p^e\mathbb{Z}} \\
\frac{Z}{p^{e'}\mathbb{Z}} & \cdots & \frac{Z}{p^{e'}\mathbb{Z}} \\
\frac{Z}{p^{e'-1}\mathbb{Z}} & \cdots & \frac{Z}{p^{e'-1}\mathbb{Z}} \\
\frac{Z}{p^{e'-1}\mathbb{Z}} & \cdots & \frac{Z}{p^{e'-1}\mathbb{Z}}
\end{bmatrix},
\]

with \( n-1 \) rows of \( \frac{Z}{p^e\mathbb{Z}} \) at the top and \( u+1 \) rows of \( \frac{Z}{p^{e'-1}\mathbb{Z}} \). There are \( p^{n((n-1)e' + (n+1)(e'-e-1))} \) of them. Choosing \( \phi \) is equivalent to choosing an automorphism of \( \left( \frac{\mathbb{Z}}{p^e\mathbb{Z}} \right)^{n+u} \), and there are \( p^{(n+u)^2} \prod_{i=1}^{n+u} (1 - p^{-i}) \) of them.

There are \( p^{n(n+u)e'} \) homomorphisms from \( \left( \frac{\mathbb{Z}}{p^e\mathbb{Z}} \right)^n \) to \( \left( \frac{\mathbb{Z}}{p^{e'}\mathbb{Z}} \right)^{n+u} \) in total. Therefore,
DISTRIBUTION OF COKERNELS OF \((n+u) \times n\) MATRICES OVER \(\mathbb{Z}_p\)

\[
\mathbb{P}\left(\left(\frac{p^u \mathbb{Z}}{p^u \mathbb{Z}}\right)^n \not\subseteq \text{im } M\right) \leq \frac{p^{n(n-1)e'+(u+1)(e'-e-1)}p^{(n+u)^2} \prod_{i=1}^{n+u} (1 - p^{-1})}{p^{n(n+u)e'}}
\]

\[= p^{-e(n-1)n+(n+u)^2} \prod_{i=1}^{n+u} (1 - p^{-i}),\]

which goes to 0 as \(e\) goes to \(\infty\).

Therefore, for all \(e \geq 0, e' > e,\)

\[\mathbb{P}(\text{rank } M = n) \geq \mathbb{P}\left(\left(\frac{p^u \mathbb{Z}}{p^u \mathbb{Z}}\right)^n \subseteq \text{im } M\right),\]

which goes to 1 as \(e\) goes to \(\infty\).

A.2 Proof of \(#\text{Hom } (\mathbb{Z}_p^{n+u}, G) \sim \#\text{Sur } (\mathbb{Z}_p^{n+u}, G):\)

We have

\[\# \text{ Sur } (\mathbb{Z}_p^{n+u}, G) = \#\{\tilde{\phi} : \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{n+u} \rightarrow G \mid \tilde{\phi} = 0\}
= (p^{n+u} - 1)(p^{n+u} - p) \cdots (p^{n+u} - p^{k-1}) \#\{\phi : \mathbb{Z}_p^{n+u} \rightarrow G \mid \tilde{\phi} = 0\}
= p^{(n+u)k}(1 - p^{-(n+u)}) \cdots (1 - p^{-(n+u)+k-1}) \#\{\phi : \mathbb{Z}_p^{n+u} \rightarrow G \mid \tilde{\phi} = 0\}
= \# \text{ Hom } (\mathbb{Z}_p^{n+u}, G)(1 - p^{-(n+u)})(1 - p^{-(n+u)+1}) \cdots (1 - p^{-(n+u)+k-1}),\]

which goes to \(#\text{Hom } (\mathbb{Z}_p^{n+u}, G)\) as \(n\) goes to \(\infty\).

Acknowledgements

I would like to thank my PhD advisor Jacob Tsimerman for his insightful comments and helpful discussions in writing this paper.

References

[1] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), volume 1068 of Lecture Notes in Math., pages 3362. Springer, Berlin, 1984.
[2] Johannes Lengler, The CohenLenstra heuristic for finite abelian groups, PhD thesis, Universit"{a}t des Saarlandes, Saarbr"{u}cken, Germany, 2009.
[3] Pritam Majumder, Uniqueness of factorization in quadratic fields, Master’s thesis, Indian Institute of Technology Kanpur, India, 2014.
[4] Melanie Matchett Wood. The distribution of sandpile groups of random graphs. \texttt{arXiv:1402.5149 [math]}, February 2014.
[5] Melanie Matchett Wood. Random Integral Matrices and the Cohen Lenstra heuristics. \texttt{arXiv:1504.04391 [math]}, April 2015.