THE CORANK OF A RECTANGULAR RANDOM INTEGER
MATRIX.

SHAKED KOPLEWITZ

Abstract. We show that under reasonable conditions, a random $n \times (2 + \epsilon)n$ integer matrix is surjective on $\mathbb{Z}^n$ with probability $1 - O(e^{-c n})$. We also conjecture that this should hold for $n \times (1 + \epsilon)n$, and provide a counterexample to show that our “reasonableness” conditions are necessary.

1. Introduction

In [2], Bourgain, Vu, and Wood show that, given an $n \times n$ random matrix $A$ whose entries take the values $+1, -1$ independently with probability $\frac{1}{2}$, the probability that $A$ is singular is bounded by $(\frac{1}{\sqrt{2}} + o(1))^n$. In particular, this implies that $A$ is injective (as a map $A : \mathbb{Z}^n \to \mathbb{Z}^n$) with probability $1 - O(e^{-cn})$ for some constant $c > 0$. In this paper, we ask:

**Question** Let $A : \mathbb{Z}^m \to \mathbb{Z}^n$ be a random integer matrix (for $m \geq n$). What is the probability that $A$ is surjective?

Our main result is the following:

**Theorem 1.** Let $A$ be an $\epsilon$-balanced $n \times (2 + \delta)n$ random matrix with entries $|A_{ij}| = O(2^{n^k})$ for some constant $k$. Then $A$ is surjective with probability $1 - O(e^{-cn})$ for some constant $c > 0$ as $n \to \infty$.

We recall the definition of $\epsilon$-balanced in Section 2.

Some type of independence assumption like $\epsilon$-balancedness is clearly necessary to avoid trivial counterexamples, such as the entries of $A$ all being equal with probability 1. We will also show in Section 3 that the bound on the size is also necessary, for any $m$, by giving a counterexample when the entries are allowed to be of size up to $e^{3nm}$.

We also show the following holds, as a direct consequence of the results of Wood in [3]:

**Theorem 2.** Let $A$ be an $\epsilon$-balanced random $n \times (n + u)$ matrix, with $\epsilon$ and $u \geq 1$ constants, then

$$\limsup_{n \to \infty} P(A \text{ is surjective}) \leq \prod_{p \text{ prime}} \prod_{k=1}^\infty (1 - p^{-k-u}) = \prod_{k=u+1}^\infty \zeta(k)^{-1}.$$  

If $u = 0$, then $\lim_{n \to \infty} P(A \text{ is surjective}) = 0$.

In particular, both results hold for 0-1 Bernoulli random matrices, in which the entries are independently chosen to be 1 with probability $q$ and 0 otherwise, for constant $0 < q < 1$.

1991 Mathematics Subject Classification. 05,15.
Key words and phrases. cokernel group, random matrix, Cohen-Lenstra heuristics.
We conjecture that under the conditions of Theorem 2,
\[ \lim_{n \to \infty} P(A \text{ is surjective}) = \prod_{k=\nu+1}^{\infty} \zeta(k)^{-1}. \]
In particular, we guess the following:

**Conjecture 1.** Let \( A \) be an \( \epsilon \)-balanced \( n \times (1+\delta)n \) random matrix for constant \( \epsilon, \delta > 0 \), with entries bound by \( n^k \) for some constant \( k > 0 \). Then \( \lim_{n \to \infty} P(A \text{ is surjective}) = 1 \).

Since the time of the original writing, this conjecture has been proved by Nguyen and Wood in [7]. See section 6 for some of their results.

Finally, we ask what we can prove under stronger assumptions. The strongest possible case would be when the entries of the matrix are ‘uniformly distributed’ in \( \mathbb{Z} \). However, there is no uniform distribution over \( \mathbb{Z} \). Our approach to resolving this is to use the Haar measure over the profinite completion \( \hat{\mathbb{Z}} \), which will give us the following theorem:

**Theorem 3.** Let \( u \geq 0 \) be constant, and let \( A : \hat{\mathbb{Z}}^{n+u} \to \hat{\mathbb{Z}}^n \) be a random matrix, whose entries are independent identically distributed random variables given by the Haar measure on \( \hat{\mathbb{Z}} \). Then if \( u > 0 \),

\[ \lim_{n \to \infty} P(A \text{ is surjective}) = \prod_{k=\nu+1}^{\infty} \zeta(k)^{-1}. \]

If \( u = 0 \), this probability converges to zero.

In particular, Theorem 3, along with the observation that the probability that \( A \) is surjective monotonically increases with \( u \), implies the following corollary:

**Corollary 4.** Let \( u(n) \) be a sequence such that \( \lim_{n \to \infty} u(n) = \infty \), and let \( A : \hat{\mathbb{Z}}^{n+u(n)} \to \hat{\mathbb{Z}}^n \) be a random matrix, whose entries are independent identically distributed random variables given by the Haar measure on \( \hat{\mathbb{Z}} \). Then

\[ \lim_{n \to \infty} P(A \text{ is surjective}) = 1 \]

In particular, this implies that a random \( n \times cn \) matrix over \( \hat{\mathbb{Z}} \) with \( c > 1 \) will be surjective with probability \( \to 1 \).

Another natural approach is to take \( A = A_{n,m,k} \) to be the matrix whose entries are independent identically distributed random variables uniformly distributed in \(-k, \ldots, k\), and take \( k \to \infty \). The authors of [5] show that

\[ \lim_{k \to \infty} P(A_{n,m,k} \text{ is surjective}) = P(A_{n,m} \text{ is surjective}), \]

where \( A_{n,m} \) is a random \( n \times m \) matrix over \( \hat{\mathbb{Z}} \).

**Acknowledgements.** The author is grateful to Sam Payne, Nathan Kaplan, and Van H. Vu for their many helpful suggestions along the way.

This work was partially supported by NSF CAREER DMS-1149054.

2. Results for \( n \times (n+u) \) Matrices for Constant \( u \)

In this section, we prove Theorem 2. We will rely on the following lemma:

**Lemma 5.** A matrix \( A : \mathbb{Z}^m \to \mathbb{Z}^n \) is surjective if and only if \( A/p : (\mathbb{Z}/p\mathbb{Z})^m \to (\mathbb{Z}/p\mathbb{Z})^n \) is surjective for every prime \( p \). Here \( A/p \) is the matrix over \( \mathbb{Z}/p\mathbb{Z} \) given by \((A/p)_{ij} = A_{ij} \pmod{p}\).
Proof. Clearly, if \( A : \mathbb{Z}^m \to \mathbb{Z}^n \) is surjective, so is \( A/p : (\mathbb{Z}/p\mathbb{Z})^m \to (\mathbb{Z}/p\mathbb{Z})^n \) for every \( p \).

Conversely, assume \( A/p : (\mathbb{Z}/p\mathbb{Z})^m \to (\mathbb{Z}/p\mathbb{Z})^n \) is surjective for every \( p \). Then \( A/p \) has rank \( n \), and in particular contains an \( n \times n \) submatrix \( B/p \leq A/p \) with nonzero determinant. As \( \det(B/p) = \det(B) \pmod{p} \), this implies that \( \det(B) \) is nonzero. This implies that the columns of \( B \), considered as vectors over \( \mathbb{Q} \), generate \( \mathbb{Q}^n \) as a vector space, and hence \( B(\mathbb{Z}^n) \) is a full-rank lattice. But \( A(\mathbb{Z}^m) \) is an abelian group containing \( B(\mathbb{Z}^n) \), so it must also be a full-rank lattice. In particular, \( D = |\mathbb{Z}^n/A\mathbb{Z}^m| \) is finite, and \( D \) divides \( |\det(B)| \).

But \( p \nmid |\det(B)| \), hence \( p \nmid D \). As this hold for every prime \( p \), we get \( D = 1 \), so \( \mathbb{Z}^n = A\mathbb{Z}^m \), which completes the proof. \( \square \)

In particular, this theorem implies that a square matrix is surjective if it is nonsingular at every prime \( p \). In contrast, a square matrix is injective if it is nonsingular at any prime \( p \).

It is worth noting that the random matrices of \([2]\), whose entries are \( \pm 1 \), are never surjective, since \( A/2 \) is the all-ones matrix.

We now recall the following definition from \([3]\):

**Definition.** A random variable \( y \) taking values in a ring \( T \) is \( \epsilon \)-balanced if for every maximal ideal \( \mathfrak{p} \) of \( T \) and every \( r \in T/\mathfrak{p} \), we have \( \mathbb{P}(y \equiv r \pmod{\mathfrak{p}}) \leq (1 - \epsilon) \). In particular, if \( T \) is a field, \( y \) is \( \epsilon \)-balanced if for every \( r \in T \), we have \( \mathbb{P}(y = r) \leq (1 - \epsilon) \).

A random matrix is \( \epsilon \)-balanced if its entries are independent and \( \epsilon \)-balanced.

In particular, a matrix whose entries are independent identically distributed Bernoulli random variables equal to 0 with probability \( 1 > q > 0 \) and 1 otherwise is \( \epsilon \)-balanced, for \( \epsilon = \min(q, 1 - q) \).

For any abelian group \( G \) and prime \( p \), define \( G_p \) to be a \( p \)-Sylow subgroup. If \( P \) is a set of primes, define \( G_P = \prod_{p \in P} G_p \). We now recall the following theorem of Wood:

**Theorem 6** (Corollary 3.4 of \([3]\)). Let \( \epsilon > 0 \) and let \( A \) be an \( \epsilon \)-balanced \( n \times (n + u) \) random matrix. Let \( G \) be a finite abelian group and let \( P \) be a finite set of primes including all those dividing \( |G| \). Then:

\[
\lim_{n \to \infty} \mathbb{P}(\mathbb{Z}^n/(A\mathbb{Z}^{n+u}))_p \simeq G = \frac{1}{|G|^u|\text{Aut}(G)|} \prod_{p \in P} \prod_{k=1}^{\infty} (1 - p^{-k-u}).
\]

Using this, we now prove Theorem 2.

**Proof of Theorem 2.** Let \( A : \mathbb{Z}^{n+u} \to \mathbb{Z}^n \) be an \( \epsilon \)-balanced random matrix. By Lemma 2, \( A \) is surjective only if \( A/p \) is surjective for every prime \( p \). This is equivalent to \( (\mathbb{Z}^n/(A\mathbb{Z}^{n+u}))_p \), being the trivial group for every prime \( p \).

Let \( P \) be a finite set of primes. Then by Theorem 2 with \( G = 1 \),

\[
\lim_{n \to \infty} \mathbb{P}(\mathbb{Z}^n/(A\mathbb{Z}^{n+u}))_p \simeq 1 \quad \text{for all } p \in P = \prod_{p \in P} \prod_{k=1}^{\infty} (1 - p^{-k-u}).
\]

But for any finite set \( P \), this is an upper bound on \( \lim \sup \mathbb{P}(A \text{ is surjective}) \). Taking \( P \) to be increasingly large gives us the theorem. \( \square \)
3. Surjectivity of random $n \times (2 + \delta)n$ matrices

In this section, we prove Theorem 4. First, we recall the following theorem from [3]:

**Theorem 7.** Let $A$ be an $\epsilon$-balanced $n \times m$ random matrix over a field $\mathbb{F}_p$ with $m \geq (1 + \delta)n$ for some constant $\delta > 0$. Then $A$ has full rank with probability at least $1 - e^{-cn}$ for some constant $c$ depending only on $\epsilon, \delta$. In particular, $c$ is independent of $\mathbb{F}_p$.

The proof bounds the probability that each row is dependent on the previous rows, similarly to the proof of Lemma [5].

In particular, This implies the following corollary:

**Corollary 8.** Let $A$ be an $\epsilon$-balanced $n \times m$ random matrix over $\mathbb{Z}$ with $m \geq (1+\delta)n$ for some constant $\delta > 0$. Then there exists a constant $c$ depending only on $\epsilon, \delta$, such that with probability $\geq 1 - e^{-\epsilon \cdot n}$, $A$ contains an $n \times n$ submatrix $A'$ with nonzero determinant.

**Proof.** Using Theorem [7] for $A/2$ gives us that

$$\mathbb{P}(\text{rank}(A/2) = n) \geq 1 - e^{-c\epsilon n}.$$ 

But if $A/2$ has rank $n$, it must contain a full rank $n \times n$ submatrix $A'/2$. Hence $\det(A') \neq 0 \pmod{2}$, and in particular $\det(A') \neq 0$. \hfill \Box

We are now ready to prove Theorem 4.

**Proof of Theorem 4.** Let $A$ be a random $n \times (2 + \delta)n$ matrix. We split it into two submatrices $A = (B, C)$, where $B$ and $C$ are $n \times (1 + \frac{\delta}{2})n$. Note that $B$ and $C$ are both $\epsilon$-balanced.

As $B$ is $\epsilon$-balanced, by Corollary [5] with probability at least $1 - e^{-\epsilon n}$, it contains a submatrix $B'$ such that $\det(B') \neq 0$, where $c$ depends only on $\epsilon, \delta$.

We can also bound the size of $|\det(B')|$. Recall that the entries of $A$, hence in particular the entries $B'_{ij}$ of $B'$, are all bounded by $O(2^{n^k})$ for some constant $k$. Assume that $|B'_{ij}| \leq 2^{n^k}$. As the determinant is the sum of $n!$ products of permutations of the $B'_{ij}$, we can bound $|\det(B')| \leq (n!)(2^{n^k})^n \leq 2^{n^{k'}}$ for a sufficiently large constant $k'$. If $|\det(B')|$ is nonzero, the number of prime divisors of $|\det(B')|$ is bounded by $\log_2(|\det(B')|) \leq n^{k'}$.

Let $P$ denote the set of prime divisors of $|\det(B')|$. By Theorem [4] for every $p \in P$, $C/p$ is surjective over $\mathbb{Z}/p\mathbb{Z}$ with probability at least $1 - e^{-c'n}$ for some $c'$ depending only on $\epsilon, \delta$. If $\det(B')$ is nonzero, then $|P| \leq n^{k'}$, so the probability that $C/p$ is surjective over every $p \in P$ is at least $1 - n^{k'}e^{-c'n}$. As $\det(B')$ is nonzero with probability at least $1 - e^{-c'n}$, the probability that $C/p$ is surjective for every $p \in P$ is at least $1 - (n^{k'} + 1)e^{-c'n} \geq 1 - e^{-an}$ for some constant $a > 0$.

But if this holds, then $A$ is surjective: $B'/p$ is surjective over every $p \notin P$, and $C/p$ is surjective over every $p \in P$. Hence $A/p$ is surjective over every prime $p$, so by Lemma [5] $A$ is surjective. \hfill \Box

4. Counterexample with large entries

In this section, we show that the bound on the size of the entries given in Theorem 4 is necessary by showing a distribution of the entries with size bounded
by \(e^{3nm}\), where the probability that a matrix is surjective goes to zero (In fact, the entries will be bounded by \(e^{n^2\log(n)m2^{\alpha m}}\)). Note that this depends on \(m\), so taking \(m\) to be a large function of \(n\) cannot resolve this need for a bound on the size of the entries.

Let \(P\) be the set of the first \(2^{nm}n\) primes. For each \(i, j\) we choose a subset \(P_{i,j}' \subseteq P\) independently at random by taking \(p \in P_{i,j}'\) independently with probability \(\frac{1}{2}\) for every \(p \in P\). We let \(A_{ij} = \prod_{p \in P_{i,j}'} p\).

\(A\) is \(\mathcal{Z}\)-balanced for \(\epsilon = \frac{1}{2}\): At a prime \(p \in P\), this is obvious, since \(\mathbb{P}(A_{ij} \equiv 0 \text{ (mod } p)) = \frac{1}{2}\). for \(p \notin P\), this follows by noting that when we choose whether to put the last prime of \(P\) in \(P'\), we choose whether or not to change \(A_{ij}\) (mod \(p\)) with probability \(\frac{1}{2}\).

To see the bound on the size of \(A_{ij}\), note that \(A_{ij}\) is bounded by the product of the first \(2^{nm}n\) primes. In general, the product of the first \(k\) primes is bounded by \(e^{2k\log(k)}\) (see for example [1]). Taking \(k = 2^{nm}n\), we see that

\[
|A_{ij}| \leq e^{2^{nm}n \log(2^{nm}n)} \leq e^{n^2 \log(n)m2^{nm+1}} \leq e^{3nm}
\]

for all sufficiently large \(n\).

Finally, for every \(p \in P\). If all the entries of \(A\) are zero mod \(p\), then \(A\) is not surjective. For each \(p \in P\), this occurs independently with probability \(2^{-nm}\). As there are \(2^{nm}n\) primes in \(P\), the probability of being surjective is at most \((1 - 2^{-nm})^{2^{nm}n} = ((1 - 2^{-nm})^{2^{nm}})^n \leq e^{-n} \rightarrow 0\). This shows that the conclusion of Theorem [1] does not hold in this case.

### 5. Random matrices over \(\mathbb{F}\)

In this section, we prove Theorem [4]

First, recall that \(\mathbb{F} = \prod_p \mathbb{Z}_p\), and that the Haar measure on \(\mathbb{F}\) is the product of the Haar measures on \(\mathbb{Z}_p\). Furthermore, the matrix \(A : \mathbb{F}^m \rightarrow \mathbb{F}^n\) is the direct product of the matrices \(A_p : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p^n\). Where \(A_p\) is the \(n \times m\) matrix given by taking the \(\mathbb{Z}_p\)-part of the coefficients of \(A\). In particular, \(A\) is surjective only if \(A_p\) is surjective for every \(p\).

When the entries of \(A\) are independent random variables in \(\mathbb{F}\), the \(A_p\) are all independent random matrices whose values are independent uniformly distributed random variables in \(\mathbb{Z}_p\). Hence

\[
\mathbb{P}(A \text{ is surjective}) = \prod_p \mathbb{P}(A_p \text{ is surjective}).
\]

The main part of the proof of Theorem [4] is the following lemma:

**Lemma 9.** Let \(A_p\) be a random \(n \times m\) matrix, with \(m \geq n\), whose entries are independent and uniformly distributed in \(\mathbb{Z}_p\). Then

\[
\mathbb{P}(A_p \text{ is surjective}) = \prod_{k=m+1-n}^{m} (1 - p^{-k}).
\]

**Proof.** First, recall that \(A_p\) is surjective on \(\mathbb{Z}_p^n\) only if \(A_p/p\) is surjective on \(\mathbb{Z}_p/p\mathbb{Z}_p^n = \mathbb{Z}/p\mathbb{Z}^n\). Hence we can consider \(A_p/p\). Note that its entries are independent and uniformly distributed in \(\mathbb{Z}/p\mathbb{Z}\).
As a matrix over a field, $A_p/p$ is surjective only if it has rank $n$, which happens only if its $n$ rows are independent. We prove by induction that the probability of the first $r$ rows being independent is $\prod_{k=m+1-r}^n (1 - p^{-k})$.

Let $u_1, \ldots, u_n$ be the rows of $A_p/p$. For $r = 1$, $u_1$ is independent only if it is nonzero. As it has $m$ independent entries, this happens with probability $1 - p^{-m}$. Now assume the claim for $r$. The first $r+1$ rows, $u_1, \ldots, u_{r+1}$ are independent only if $u_1, \ldots, u_r$ are independent and $u_{r+1}$ is independent of them. By the assumption, the probability that the first $u_1, \ldots, u_r$ rows are independent is $\prod_{k=m+1-r}^n (1-p^{-k})$.

If the first $u_1, \ldots, u_r$ rows are independent, there exists some set $I$ of $r$ columns such that $u_1|I, \ldots, u_r|I$ are independent. Then there are unique coefficients $a_1, \ldots, a_r$ such that $u_{r+1}|I = \sum a_i u_i|I$, and $u_{r+1}$ is dependent on $u_1, \ldots, u_r$ only if $(u_{r+1})_j = \sum a_i (u_i)_j$ for every $j \notin I$. Since $(u_{r+1})_j$ is independent of the rest of the matrix, this happens with probability $\frac{1}{p}$. As there are $m - r$ values for $j \notin I$, this implies that the probability that $u_{r+1}$ is dependent on $u_1, \ldots, u_r$ is $p^{-r}$ only if its $m - r$ columns are independent. The first $r$ rows are independent only if its $r$ columns are independent. We prove by induction that the probability of

\[
(1 - p^{-(m-r)}) \prod_{k=m+1-r}^n (1 - p^{-k}) = \prod_{k=m+1-(r+1)}^n (1 - p^{-k}),
\]

which completes the proof. \hfill \Box

We now prove Theorem 3.

**Proof of Theorem 3.** Let $A$ be a random $n \times (n + u)$ matrix over $\hat{\mathbb{Z}}$. As we saw,

\[
\mathbb{P}(A \text{ is surjective}) = \prod_p \mathbb{P}(A_p \text{ is surjective}) = \prod_{p} \prod_{k=1+u}^{n+u} (1 - p^{-k})
\]

\[
= \prod_{k=1+u}^{n+u} \prod_{p} (1 - p^{-k})
\]

\[
= \prod_{k=1+u}^{n+u} \zeta(k)^{-1} \to \prod_{k=1+u}^{\infty} \zeta(k)^{-1}.
\]

The last two lines hold when $u > 0$. When $u = 0$, $\prod_p (1 - p^{-1}) = 0$, so the product converges to zero. \hfill \Box

6. **Further results**

Since the original writing of this paper, a number of the results conjectured here have been proven. In [7], Nguyen and Wood prove Conjecture 1.

**Theorem 10** (Theorem 1.4 of [7]). For integers $n, u \geq 0$, let $A_{n \times (n + u)}$ be an integral $n \times (n + u)$ matrix with entries i.i.d copies of an $\alpha_n$-balanced random integer $\zeta_n$, with $\alpha_n \geq n^{-1+\epsilon}$ and $|\zeta_n| \leq n^T$ for any fixed parameters $0 < \epsilon < 1$ and $T > 0$ not depending on $n$. Then

\[
\lim_{\min n, u \to \infty} \mathbb{P}(A_{n \times (n + u)} \text{ is surjective}) = 1.
\]

In fact, they prove stronger results. Their main theorem is the following:
Theorem 11 (Theorem 1.1 of [7]). Let \( n, u, A_{n \times (n+u)} \) be as above, and let \( B \) be a fixed finite abelian group. Then for any fixed \( u \),

\[
\lim_{n \to \infty} \mathbb{P}(\text{coker} A_{n \times (n+u)} \cong B) = \frac{1}{|B||\text{Aut}(B)|} \prod_{k=u+1}^{\infty} \zeta(k)^{-1}.
\]

And these two imply the following corollary:

Corollary 12 (Theorem 1.5 of [7]). Let \( n, u, A_{n \times (n+u)} \) be as above. For any fixed \( u \geq 0 \):

\[
\lim_{n \to \infty} \mathbb{P}(A_{n \times (n+u)} \text{ is surjective}) = \prod_{k=u+1}^{\infty} \zeta(k)^{-1}.
\]

Finally, in [6], Nguyen and Paquette give some bounds on the speed of convergence for the probability of the matrix being surjective. In particular, they prove:

Theorem 13 (Theorem 1.4 (5) of [6]). Let \( n, u, A_{n \times (n+u)} \) be as above, and assume that \( \alpha_n \geq \frac{\log^{O(1)}(n)}{n} \). Then

\[
\mathbb{P}(A_{n \times (\lfloor (1+o(1))n \rfloor)} \text{ is surjective}) = 1 - O\left(n^{-\omega(1)}\right).
\]

References

[1] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. Illinois Journal of Mathematics, 6:64–94, 1962.

[2] Jean Bourgain, Van H Vu, and Philip Matchett Wood. On the singularity probability of discrete random matrices. Journal of Functional Analysis, 258(2):559–603, 2010.

[3] Shaked Koplewitz. \( p \)-parts of sandpile groups of random bipartite graphs, in preparation. 2016.

[4] Kenneth Maples. Singularity of random matrices over finite fields. arXiv preprint arXiv:1012.2372, 2010.

[5] Gérard Maze, Joachim Rosenthal, and Urs Wagner. Natural density of rectangular unimodular integer matrices. Linear Algebra and its Applications, 434(5):1319–1324, 2011.

[6] Hoi H Nguyen and Elliot Paquette. Surjectivity of near square random matrices. arXiv preprint arXiv:1802.00001, 2018.

[7] Hoi H Nguyen and Melanie Matchett Wood. Random integral matrices: universality of surjectivity and the cokernel. arXiv preprint arXiv:1806.00596, 2018.

[8] Melanie Matchett Wood. Random integral matrices and the Cohen-Lenstra heuristics. arXiv preprint arXiv:1504.04391, 2015.

Mathematics Department, Yale University, New Haven, CT 06511

E-mail address: shaked.koplewitz@gmail.com