The Smith normal form distribution of a random integer matrix

Yinghui Wang[1]† and Richard P. Stanley[2]‡

[1] *Department of Mathematics, Columbia University, New York, New York 10027*
[2] *Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139*

Abstract. We show that the density μ of the Smith normal form (SNF) of a random integer matrix exists and equals a product of densities μ_{p^s} of SNF over $\mathbb{Z}/p^s\mathbb{Z}$ with p a prime and s some positive integer. Our approach is to connect the SNF of a matrix with the greatest common divisors (gcds) of certain polynomials of matrix entries, and develop the theory of multi-gcd distribution of polynomial values at a random integer vector. We also derive a formula for μ_{p^s} and determine the density μ for several interesting types of sets.

Résumé. Nous montrons ue la densité μ de la forme normale de Smith (FNS) d'une matrice entière aléatoire existe et vaut le produit des densités μ_{p^s} de la FNS sur $\mathbb{Z}/p^s\mathbb{Z}$ avec p premier et s un entier positif. Notre approche est de relier la FNS d'une matrice avec les plus grand commun diviseurs (pgcds) de certains polynômes des entrées de la matrice, et de développer la théorie de la distribution du multi-pgcd de polynômes évalués sur un vecteur entier aléatoire. Nous obtenons aussi une formule pour μ_{p^s} et déterminons la densité μ pour plusieurs types d'ensembles intéressants.

Keywords. Smith normal form, random integer matrix, greatest common divisor distribution

1 Introduction

Let M be a nonzero $n \times m$ matrix over a commutative ring R (with identity), and r be the rank of M. If there exist invertible $n \times n$ and $m \times m$ matrices P and Q such that the product PMQ is a diagonal matrix with diagonal entries $d_1, d_2, \ldots, d_r, 0, 0, \ldots, 0$ satisfying that $d_i \mid d_{i+1}$ for all $1 \leq i \leq r-1$, then PMQ is the *Smith normal form (SNF)* of M. In general, the SNF does not exist. It does exist when R is a *principal ideal ring*, i.e., a ring (not necessarily an integral domain) for which every ideal is principal. This class of rings includes the integers $\mathbb{Z}$ and their quotients $\mathbb{Z}/q\mathbb{Z}$, which are the rings of interest to us here. In fact, for the rings $\mathbb{Z}/q\mathbb{Z}$ we are particularly concerned with the case $q = p^s$, a prime power. For principal ideal rings, the diagonal entries are uniquely determined (up to multiplication by a unit) by $g_{i-1}d_i = g_i$ $(1 \leq i \leq r)$, where $g_0 = 1$ and g_i is the greatest common divisor (gcd) of all $i \times i$ minors of M. As an algebraic interpretation, we have the following correspondence between the SNF and the cokernel of M: coker $M \simeq R/d_1R \oplus R/d_2R \oplus \cdots \oplus R/d_rR \oplus R^{n-r}$.

† Email: `yinghui@math.columbia.edu, yinghui@alum.mit.edu`.

‡ Email: `rstan@math.mit.edu`. Partially supported by NSF grant DMS-1068625.

There has been a huge amount of research on eigenvalues of random matrices over a field (see, e.g., Akemann et al. 2011, Anderson et al. 2010, Fulman 2002, Mehta 2004). Less attention has been paid to the SNF of a random matrix over a principal ideal ring (or more general rings for which SNF always exists). Some basic results in this area are known, but they appear in papers not focused on SNF per se. We develop the theory in a systematic way, collecting previous work in this area, sometimes with simplified proofs, and providing new results.

We shall define the *density* μ of SNF of a random $n \times m$ integer matrix as the limit (if exists) as $k \to \infty$ of $\mu^{(k)}$, the density of SNF of a random $n \times m$ matrix with entries independent and uniformly distributed over $\{-k, -k+1, \dots, k\}$ (see Definition 3.1 below for a precise definition).

As a motivating example, the probability that $d_1 = 1$ for a random $n \times m$ integer matrix is the probability that the nm matrix entries are relatively prime, or equivalently, that nm random integers are relatively prime, and thus equals $1/\zeta(nm)$, where $\zeta(\cdot)$ is the Riemann zeta function.

If we regard the minors of an $n \times m$ matrix as polynomials of the nm matrix entries with integer coefficients, then the SNF of a matrix is uniquely determined by the gcds of the values of these polynomials (recall the definition of SNF from the beginning). This inspires us to study the theory of multi-gcd distribution of polynomial values.

Given a collection of relatively prime polynomials in $\mathbb{Z}[x_1, x_2, \dots, x_d]$, let $g(x)$ be the gcd of the values of these polynomials at $x = (x_1, x_2, \dots, x_d)$. We shall define the *density* λ of $g(x)$ of a random d-dimensional integer vector x as the limit (if exists) as $k \to \infty$ of $\lambda^{(k)}$, the density of $g(x)$ with x uniformly distributed over $\{-k, -k+1, \dots, k\}^d$ (see Definition 2.1 for a precise definition).

In the spirit of previous work in number theory such as Ekedahl (1991), Poonen (2003), Poonen and Stoll (1999) and the Cohen-Lenstra heuristics (Cohen and Lenstra 1984a,b), one might conjecture that λ exists and equals the product of density λ_p of $g(x)$ over $(\mathbb{Z}/p\mathbb{Z})^d$ over all primes p. In fact, we prove this conjecture with the more general density λ_{p^s} of $g(x)$ over $\mathbb{Z}/p^s\mathbb{Z}$ for sets of form (2.2) (see Theorem 2.6), with the aid of a result in number theory Poonen and Stoll (1999, Lemma 21). Note that the special case that $s = 0$ or 1 follows from Ekedahl (1991, Theorem 2.3) directly. In particular, this result applies to the probability that $g(x) = 1$, in other words, that the polynomial values are relatively prime. Furthermore, all these results hold for the multi-gcd distribution of polynomial values, namely, when $g(x)$ is a vector whose components are the gcds of the values of given collections of polynomials at x.

Then we apply this theory to the SNF distribution of a random integer matrix to show that the density μ (of SNF of a random $n \times m$ integer matrix) equals a product of some densities μ_{p^s} of SNF over $\mathbb{Z}/p^s\mathbb{Z}$ for sets of form (3.2) (Theorem 3.5). We also derive a formula for μ_{p^s} (Theorem 3.2), which allows us to compute μ_{p^s} and hence μ explicitly (Theorem 4.2). Some special cases of this formula coincide with Stanley (2011, Exercise 1.192(b)) and Friedman and Washington (1989, pp. 233, 236). Another paper related to our work is Wood (2015).

On the strength of these results, we determine the value of μ for some interesting types of sets, specifically, matrices with first few diagonal entries given, matrices with diagonal entries all equal to 1, and square matrices with at most $\ell\,(= 1, 2, \dots, n)$ diagonal entries not equal to 1, i.e., whose corresponding cokernel has at most ℓ generators; further, for the last set we establish the asymptotics of μ as $\ell \to \infty$. In the case of $\ell = 1$ (which is equivalent to the matrix having a cyclic cokernel), our results echo those in Ekedahl (1991, Section 3) via a different approach. We also show that μ of a finite set is 0, and that the probability that a random integer matrix is full rank is 1, which agrees with Katznelson (1993, Theorem 1) in the case of square matrices.

Additionally, we find the maximum and minimum of $\mu_{p^s}(D)$ over all diagonal matrices D; whereas regarding it as a function of p, s, m, n and D, we find its monotonicity properties and limiting behaviors.

The remainder of this extended abstract is organized as follows. Section 2 develops the theory of multi-gcd distribution of polynomial values. Section 3 applies this theory to the SNF distribution and derives a formula for μ_{p^s}. Finally, Section 4 computes the density μ for several types of sets.

For a complete version of this extended abstract, see Wang and Stanley (2015).

We shall assume throughout that p represents a prime, p_j is the j-th smallest prime, and $\prod_p$ means a product over all primes p.

2 Multi-gcd distribution of polynomial values

Suppose that d and h are positive integers and $F_1, F_2, \ldots, F_h \in \mathbb{Z}[x_1, x_2, \ldots, x_d]$ are nonzero polynomials. Let

$$g(x) := \gcd(F_1(x), F_2(x), \cdots, F_h(x)), \quad x \in \mathbb{Z}^d$$

be the gcd of the values $F_1(x), F_2(x), \ldots, F_h(x)$, and $g(x) = 0$ if $F_j(x) = 0$ for all $1 \le j \le h$.

We shall define the *density of $g(x)$ of a random d-dimensional integer vector x* as the limit (if exists) of the density of $g(x)$ with x uniformly distributed over $\{-k, -k+1, \ldots, k\}^d =: \mathbb{Z}^d_{(k)}$ as $k \to \infty$, precisely as follows.

Definition 2.1. (i) For $\mathcal{Z} \subseteq \mathbb{Z}$, we denote by $\lambda^{(k)}(\mathcal{Z})$ the probability that $g(x) \in \mathcal{Z}$ with x uniformly distributed over $\mathbb{Z}^d_{(k)}$. If $\lim_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) = \lambda(\mathcal{Z})$ exists, then we say that the *probability that $g(x) \in \mathcal{Z}$ with x a random d-dimensional integer vector* is $\lambda(\mathcal{Z})$. If this is the case, then $\lambda(\mathcal{Z}) \in [0,1]$ since $\lambda^{(k)}(\mathcal{Z}) \in [0,1]$ for all k.

(ii) We define similarly the gcd distribution over the ring of integers mod p^s: for prime p and positive integer s, we denote by $\lambda^{(k)}_{p^s}(\mathcal{Z})$ the probability that $g(x) \in \mathcal{Z} \,(\text{mod } p^s)$ (up to multiplication by a unit) with x uniformly distributed over $\mathbb{Z}^d_{(k)}$, and by $\lambda_{p^s}(\mathcal{Z})$ the probability that $g(x) \in \mathcal{Z} \,(\text{mod } p^s)$ (up to multiplication by a unit) with x uniformly distributed over $(\mathbb{Z}/p^s\mathbb{Z})^d$.

More generally, for a finite set $\mathcal{P}$ of prime and positive integer pairs (p, s) (with p a prime and s a positive integer), we denote

$$P_{\mathcal{P}} := \prod_{(p,s)\in\mathcal{P}} p^s$$

and by $\lambda^{(k)}_{P_{\mathcal{P}}}(\mathcal{Z})$ the probability that $g(x) \in \mathcal{Z} \,(\text{mod } P_{\mathcal{P}})$ (up to multiplication by a unit) with x uniformly distributed over $\mathbb{Z}^d_{(k)}$, and by $\lambda_{P_{\mathcal{P}}}(\mathcal{Z})$ the probability that $g(x) \in \mathcal{Z} \,(\text{mod } P_{\mathcal{P}})$ (up to multiplication by a unit) with x uniformly distributed over $(\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z})^d$. Note that $\lambda_{P_{\mathcal{P}}}(\mathcal{Z})$ is the number of solutions to $g(x) \in \mathcal{Z} \,(\text{mod } P_{\mathcal{P}})$ (up to multiplication by a unit) divided by $P^d_{\mathcal{P}}$. The situation discussed in the previous paragraph is the special case that $\mathcal{P}$ consists of only one element (p, s) and $P_{\mathcal{P}} = p^s$.

(iii) The above definitions also extend to the distribution of multi-gcds. Suppose that $\mathcal{U} = \{U_i\}_{i=1}^w$ is a collection of w nonempty subsets U_i of $\{F_1, F_2, \ldots, F_h\}$. Let

$$g_i(x) := \gcd\left(F(x) : F \in U_i\right), \quad x \in \mathbb{Z}^d \tag{2.1}$$

and

$$g(x) := (g_1, g_2, \ldots, g_w)(x) \in \mathbb{Z}^w,$$

then we adopt the definitions of functions $\lambda^{(k)}$, λ, $\lambda_{P_{\mathcal{P}}}^{(k)}$ and $\lambda_{P_{\mathcal{P}}}$ for $\mathcal{Z} \subseteq \mathbb{Z}^d$ with a slight modification: replace "up to multiplication by a unit" with "up to multiplication of the components of g by units".

For convenience, we shall always assume that the notion $g(x) \in \mathcal{Z} \pmod{P_{\mathcal{P}}}$ implies the *equivalence of multiplication of its components by units* and that the random vector x is *uniformly distributed* on its range (if known, e.g., $\mathbb{Z}_{(k)}^d$ or $(\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z})^d$).

Remark 2.2. The density $\lambda_p(\cdot)$ defined above in Definition 2.1 (ii) is consistent with the normalized *Haar measure* on $\mathbb{Z}_p^d$, as in Poonen and Stoll (1999).

In this section, we establish the properties of $\lambda_{P_{\mathcal{P}}}$ and λ, the existence of λ, and a connection between λ and the λ_{p^s}'s.

Theorem 2.3 (Multi-gcd distribution over $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$)**.** *For any $\mathcal{Z} \subseteq \mathbb{Z}^w$, we have*

$$\lim_{k\to\infty} \lambda_{P_{\mathcal{P}}}^{(k)}(\mathcal{Z}) = \lambda_{P_{\mathcal{P}}}(\mathcal{Z}) = \prod_{(p,s)\in\mathcal{P}} \lambda_{p^s}(\mathcal{Z}) \,.$$

We show some properties of the density λ of set unions, subtractions and complements. They are very useful in determining the value of λ for specific sets.

Theorem 2.4. (i) *Suppose that $\{\mathcal{Z}_\alpha\}_{\alpha\in\mathcal{A}}$ are pairwise disjoint subsets of $\mathbb{Z}^w$ such that $\lambda(\mathcal{Z}_\alpha)$ exists for all $\alpha \in \mathcal{A}$. If $\mathcal{A}$ is a finite set, then $\lambda\left(\cup_{\alpha\in\mathcal{A}} \mathcal{Z}_\alpha\right) = \sum_{\alpha\in\mathcal{A}} \lambda(\mathcal{Z}_\alpha)$.*

(ii) *Suppose that $\mathcal{Z}' \subseteq \mathcal{Z} \subseteq \mathbb{Z}^w$ such that $\lambda(\mathcal{Z}')$ and $\lambda(\mathcal{Z})$ both exist, then $\lambda(\mathcal{Z}\setminus\mathcal{Z}') = \lambda(\mathcal{Z}) - \lambda(\mathcal{Z}')$. In particular, for the complement $\mathcal{Z}^c$ of $\mathcal{Z}$ in $\mathbb{Z}^w$, we have $\lambda(\mathcal{Z}^c) = 1 - \lambda(\mathcal{Z})$.*

(iii) *Suppose that $\mathcal{Y} \in \mathbb{Z}^w$ such that $\lambda(\mathcal{Y}) = 0$, then for any $\mathcal{Z} \subseteq \mathcal{Y}$, we have $\lambda(\mathcal{Z}) = 0$.*

We show that the density λ exists and in fact, equals the product of some λ_{p^s}'s.

Assumption 2.5. For all $1 \le i \le w$, we have

$$\gcd(F_1, F_2, \ldots, F_h) = \gcd\left(F : F \in U_i\right) = 1 \text{ in } \mathbb{Q}[x_1, x_2, \ldots, x_d] \,.$$

Theorem 2.6 (Connection between λ and λ_{p^s})**.** *Suppose that Assumption 2.5 holds. Given positive integers $r \le w$ and y_i, $1 \le i \le r$, let $y = \prod_{j=1}^\infty p_j^{s_j}$ with p_j the j-th smallest prime and s_j nonnegative integers, $j = 1, 2, \ldots$ such that $y_i \,|\, y$ for all $1 \le i \le r$, then the probability $\lambda(\mathcal{Z})$ exists for*

$$\mathcal{Z} = \left\{(z_1, z_2, \ldots, z_w) \in \mathbb{Z}_+^w : \; z_i = y_i \,, \; \forall\, i \le r\right\} , \tag{2.2}$$

and in fact,

$$\lambda(\mathcal{Z}) = \prod_{j=1}^\infty \lambda_{p_j^{s_j+1}}(\mathcal{Z}) \,.$$

To prove Theorem 2.6, we use Theorem 2.3 and the following result in number theory.

Lemma 2.7. (Poonen 2003, Lemma 5.1 or Poonen and Stoll 1999, Lemma 21) *Suppose that $F, G \in \mathbb{Z}[x_1, x_2, \ldots, x_d]$ are relatively prime as elements of $\mathbb{Q}[x_1, x_2, \ldots, x_d]$. Let $\nu_\ell^{(k)}$ be the probability that $p \,|\, F(x), G(x)$ for some prime $p > \ell$ with x uniformly distributed over $\mathbb{Z}_{(k)}^d$, i.e.,*

$$\nu_\ell^{(k)} := \#\left\{x \in \mathbb{Z}_{(k)}^d : \; \exists\,\text{prime}\, p > \ell \text{ s.t. } p \,|\, F(x), G(x)\right\} / \,(2k+1)^d.$$

Then

$$\lim_{\ell\to\infty} \limsup_{k\to\infty} \nu_\ell^{(k)} = 0 \,.$$

3 SNF distribution

Let $m \leq n$ be two positive integers. We shall define the *density* of SNF of a random $n \times m$ integer matrix as the limit (if exists) of the density of SNF of a random $n \times m$ matrix with entries independent and uniformly distributed over $\mathbb{Z}_{(k)}$ as $k \to \infty$ (see Definition 3.1 below for a precise definition).

If we regard the minors of an $n \times m$ matrix as polynomials of the nm matrix entries with integer coefficients, then the SNF of a matrix is uniquely determined by the values of these polynomials. Specifically, let $x_1, x_2, \dots, x_{nm}$ be the nm entries of an $n \times m$ matrix, F_j's be the minors of an $n \times m$ matrix as elements in $\mathbb{Z}[x_1, x_2, \dots, x_{nm}]$, U_i be the set of $i \times i$ minors $(1 \leq i \leq m)$, then the SNF of this matrix is the diagonal matrix whose i-th diagonal entry is 0 if $g_i(x) = 0$ and $g_i(x)/g_{i-1}(x)$ otherwise, where $x = (x_1, x_2, \dots, x_{nm})$ and $g_i(x)$ is defined in (2.1).

In this spirit, the multi-gcd distribution as well as the results in Sections 2 have analogues for the SNF distribution of a random integer matrix. This section presents these analogues and the next section will use them to compute the density μ for some interesting types of sets.

Conventionally, the SNF is only defined for a nonzero matrix; however, for convenience, we shall define the SNF of a zero matrix to be itself, so that SNF is well-defined for all matrices. This definition does not change the density (if exists) of SNF of a random $n \times m$ integer matrix since the probability of a zero matrix with entries from $\mathbb{Z}_{(k)}$ is $1/(2k+1)^{nm}$, which converges to 0 as $k \to \infty$.

We denote the SNF of an $n \times m$ matrix M by $\mathrm{SNF}(M) = (\mathrm{SNF}(M)_{i,j})_{n\times m}$ and let $\mathbb{S}$ be the set of all candidates for SNF of an $n \times m$ integer matrix, i.e., the set of $n \times m$ diagonal matrices whose diagonal entries $(d_1, d_2, \dots, d_m)$ are nonnegative integers such that d_{i+1} is a multiple of d_i, $i = 1, 2, \dots, m-1$.

For ease of notation, we shall always assume that the matrix entries are *independent and uniformly distributed* on its range (if known, e.g., $\mathbb{Z}_{(k)}$ or $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$), and that the notion $\mathrm{SNF}(M) \in \mathcal{S}$ or $\mathrm{SNF}(M) = D$ (mod $P_{\mathcal{P}}$) for some $\mathcal{S} \subseteq \mathbb{S}$, $D \in \mathbb{S}$ and $P_{\mathcal{P}} = \prod_{(p,s)\in\mathcal{P}} p^s \in \mathbb{Z}_+$ implies the *equivalence of multiplication of the entries of M by units* in $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$, thus we can assume for convenience that the entries of $\mathrm{SNF}(M)$ (mod $P_{\mathcal{P}}$) are zero or divisors of $P_{\mathcal{P}}$.

Definition 3.1. (i) For $\mathcal{S} \subseteq \mathbb{S}$, we denote by $\mu^{(k)}(\mathcal{S})$ the probability that $\mathrm{SNF}(M) \in \mathcal{S}$ with entries of M from $\mathbb{Z}_{(k)}$. If $\lim_{k\to\infty} \mu^{(k)}(\mathcal{S}) = \mu(\mathcal{S})$ exists, then we say that the *probability that* $\mathrm{SNF}(M) \in \mathcal{S}$ *with M a random $n \times m$ integer matrix* is $\mu(\mathcal{S})$. If this is the case, then $\mu(\mathcal{S}) \in [0,1]$ since $\mu^{(k)}(\mathcal{S}) \in [0,1]$ for all k.

(ii) We define similarly the SNF distribution over the ring of integers mod p^s: for prime p and positive integer s, we denote by $\mu_{p^s}^{(k)}(\mathcal{S})$ the probability that the $\mathrm{SNF}(M) \in \mathcal{S} \pmod{p^s}$ with entries of M from $\mathbb{Z}_{(k)}$, and by $\mu_{p^s}(\mathcal{S})$ the probability that $\mathrm{SNF}(M) \in \mathcal{S} \pmod{p^s}$ with entries of M from $\mathbb{Z}/p^s\mathbb{Z}$.

More generally, for a finite set $\mathcal{P}$ of prime and positive integer pairs (p, s) (with p a prime and s a positive integer), we denote by $\mu_{P_{\mathcal{P}}}^{(k)}(\mathcal{S})$ the probability that $\mathrm{SNF}(M) \in \mathcal{S} \pmod{P_{\mathcal{P}}}$ with entries of M from $\mathbb{Z}_{(k)}$, and by $\mu_{P_{\mathcal{P}}}(\mathcal{S})$ the probability that $\mathrm{SNF}(M) \in \mathcal{S} \pmod{P_{\mathcal{P}}}$ with entries of M from $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$. Note that $\mu_{P_{\mathcal{P}}}(\mathcal{S})$ is the number of matrices M over $P_{\mathcal{P}}$ such that $\mathrm{SNF}(M) \in \mathcal{S} \pmod{P_{\mathcal{P}}}$ divided by $P_{\mathcal{P}}^{nm}$. The situation discussed in the previous paragraph is the special case that $\mathcal{P}$ consists of only one element (p, s) and $P_{\mathcal{P}} = p^s$.

In this section, we establish a formula for μ_{p^s}, discuss the properties of $\mu_{P_{\mathcal{P}}}$ and μ, show the existence of μ and represent it as a product of μ_{p^s}'s.

We have the following analogue of Theorem 2.3 for SNFs. We also derive a formula for μ_{p^s} from Feng et al. (2013, Theorem 1) (or Feng et al. 2014, Theorem 2).

Theorem 3.2 (SNF distribution over $\mathbb{Z}/P_{\mathcal{P}}$). (i) *Given a prime p, a positive integer s and a sequence of integers $0 = a_0 \le a_1 \le \cdots \le a_s \le a_{s+1} = m$, let $\boldsymbol{a} := (a_1, a_2, \ldots, a_s)$ and $D_{\boldsymbol{a}} \in \mathbb{S}$ be the diagonal matrix with exactly $(a_i - a_{i-1})$ p^{i-1}'s, i.e., a_i non-p^i-multiples, $1 \le i \le s$ on its diagonal. Then we have*

$$\mu_{p^s}(\{D_{\boldsymbol{a}}\}) = p^{-\sum_{i=1}^{s}(n-a_i)(m-a_i)} \cdot \frac{[p,n][p,m]}{[p,n-a_s][p,m-a_s]\prod_{i=1}^{s}[p,a_i-a_{i-1}]}\,, \tag{3.1}$$

where

$$[p,0] = 1, \quad [p,\ell] := \prod_{j=1}^{\ell}\left(1 - p^{-j}\right)\,, \quad \ell \in \mathbb{Z}_+\,.$$

(ii) *For any $\mathcal{S} \subseteq \mathbb{S}$, we have*

$$\mu_{P_{\mathcal{P}}}(\mathcal{S}) = \sum_{D \in \mathcal{S} \,(\mathrm{mod}\, P_{\mathcal{P}})} \mu_{P_{\mathcal{P}}}(\{D\})$$

and

$$\lim_{k\to\infty} \mu_{P_{\mathcal{P}}}^{(k)} = \mu_{P_{\mathcal{P}}}(\mathcal{S}) = \prod_{(p,s)\in\mathcal{P}} \mu_{p^s}(\mathcal{S})\,.$$

The properties of λ of set unions, subtractions and complements in Section 2 also carry over to SNFs. They are useful in determining the value of μ for some specific sets (for instance, the singleton set of the identity matrix as in Section 4.3).

Theorem 3.3. (i) *Suppose that $\{\mathcal{S}_\alpha\}_{\alpha\in\mathcal{A}}$ are pairwise disjoint subsets of $\mathbb{S}$ such that $\mu(\mathcal{S}_\alpha)$ exists for all $\alpha \in \mathcal{A}$. If $\mathcal{A}$ is a finite set, then $\mu\left(\cup_{\alpha\in\mathcal{A}} \mathcal{S}_\alpha\right) = \sum_{\alpha\in\mathcal{A}} \mu(\mathcal{S}_\alpha)$.*

(ii) *Suppose that $\mathcal{S}' \subseteq \mathcal{S} \subseteq \mathbb{S}$ such that $\mu(\mathcal{S}')$ and $\mu(\mathcal{S})$ both exist, then $\mu(\mathcal{S} \setminus \mathcal{S}') = \mu(\mathcal{S}) - \mu(\mathcal{S}')$. In particular for the complement $\mathcal{S}^c$ of $\mathcal{S}$ in $\mathbb{S}$, we have $\mu(\mathcal{S}^c) = 1 - \mu(\mathcal{S})$.*

(iii) *Suppose that $\mathcal{T} \in \mathbb{S}$ such that $\mu(\mathcal{T}) = 0$, then for any $\mathcal{S} \subseteq \mathcal{T}$, we also have $\mu(\mathcal{S}) = 0$.*

Theorem 2.6 has an analogue for SNFs as well, by virtue of the following well-known lemma (see Bôcher 1964, Theorem 61.1 for an easy proof).

Lemma 3.4. *Fix a positive integer r. The determinant of an $r \times r$ matrix as a polynomial of its r^2 entries $x_1, x_2, \ldots, x_{r^2}$ is irreducible in $\mathbb{Q}[x_1, x_2, \ldots, x_{r^2}]$.*

For any $i \le m \wedge (n-1)$ (i.e., min $\{m, n-1\}$, recalling that $m \le n$), the set U_i contains at least two different minors, which are both irreducible as polynomials of the entries on the strength of Lemma 3.4 and therefore relatively prime. Hence Assumption 2.5 holds with $w = m \wedge (n-1)$. This allows us to apply Theorem 2.6 to SNFs and obtain the following analogue.

Theorem 3.5 (Connection between μ and μ_{p^s}). *Given positive integers $r \le m\wedge(n-1)$ and $d_1 \,|d_2\,| \cdots |\, d_r$, let $z = \prod_{j=1}^{\infty} p_j^{s_j}$ with p_j the j-th smallest prime and s_j nonnegative integers, $j = 1, 2, \ldots$ such that $d_r \mid z$, then the probability $\mu(\mathcal{S})$ exists for*

$$\mathcal{S} = \{D := (D_{i,j})_{n\times m} \in \mathbb{S} :\ D_{i,i} = d_i\,,\ \forall\, i \le r\}\,, \tag{3.2}$$

and in fact

$$\mu(\mathcal{S}) = \prod_{j=1}^{\infty} \mu_{p_j^{s_j+1}}(\mathcal{S})\,. \tag{3.3}$$

Remark 3.6. (i) The right-hand side of (3.3) is well-defined since $\mu_{p^s}(\cdot) \in [0,1]$ for all p and s.

(ii) We have assumed that $r \leq m \wedge (n-1)$; in fact, we have $\mu(\mathcal{S}) = 0$ otherwise. Recall that $m \leq n$ and note that $r \leq m$, thus in the case of $r > m \wedge (n-1)$, we must have $r = m = n$. As a result, any matrix M with $\mathrm{SNF}(M) \in \mathcal{S}$ satisfies $|M| = \pm d_n$. We will show later that the probability that the determinant of a random $n \times n$ integer matrix equals $\pm c$ is 0 for all constant c (Theorem 4.3).

(iii) We have also assumed that the d_i's are positive; in fact, we have $\mu(\mathcal{S}) = 0$ otherwise. If $d_i = 0$ for some i, then all $i \times i$ minors of any matrix M with $\mathrm{SNF}(M) \in \mathcal{S}$ are zero. Applying Theorem 4.3 to $c = 0$ yields the desired result.

4 Applications

Now we apply Theorems 3.2 and 3.5 to compute the density μ explicitly for the following subsets of $\mathbb{S}$: matrices with first few diagonal entries given (i.e., with the form of (3.2)), full rank matrices, a finite subset, matrices with diagonal entries all equal to 1, and square matrices with at most $\ell\,(= 1, 2, \ldots, n)$ diagonal entries not equal to 1.

4.1 Density of the set (3.2)

For the set $\mathcal{S}$ of (3.2), we take $z = d_r$ in Theorem 3.5, then it suffices to compute $\mu_{p^{s+1}}(\mathcal{S})$ for each $(p, s) = (p_j, s_j)$. In $\bmod p^{s+1}$, the set $\mathcal{S}$ has $m - r + 1$ elements. Further, since formula (3.1) gives the density $\mu_{p^{s+1}}$ of each element of $\mathcal{S}$, one can take the sum over $\mathcal{S}$ to get an expression for $\mu_{p^{s+1}}(\mathcal{S})$ (Theorem 3.2), and compute this sum explicitly when $m - r$ is small, such as in Theorems 4.6 and 4.7 below. However, this sum is hard to compute when $m - r$ is large, for instance, when m is large and r is fixed; in this case, we recast $\mathcal{S}$ as the difference between a subset of $\mathbb{S}$ and the union of other $r - 1$ subsets such that for each of these r sets, its density $\mu_{p^{s+1}}$ is given directly by (3.1).

We work out two examples to illustrate this idea, and then deal with the general case (see Wang and Stanley 2015 for details). Our approach first reproduces the result mentioned at the beginning: the probability that $d_1 = 1$ is $1/\zeta(nm)$. Here is another example.

Theorem 4.1 (Example)**.** *Let $\mathcal{S}$ be the set of* (3.2) *with $r = 2$, $d_1 = 2$ and $d_2 = 6$, then we have*

$$\mu(\mathcal{S}) = \mu_{2^2}(\mathcal{S})\, \mu_{3^2}(\mathcal{S}) \prod_{p>3} \mu_p(\mathcal{S}),$$

where

$$\mu_{2^2}(\mathcal{S}) = 2^{-nm}\left(1 - 2^{-nm} - 2^{-(n-1)(m-1)} \cdot \frac{(1-2^{-n})(1-2^{-m})}{1-2^{-1}}\right),$$

$$\mu_{3^2}(\mathcal{S}) = 3^{-(n-1)(m-1)}\left(1 - 3^{-(n-1)(m-1)}\right)\frac{(1-3^{-n})(1-3^{-m})}{1-3^{-1}},$$

$$\mu_p(\mathcal{S}) = 1 - p^{-nm} - p^{-(n-1)(m-1)} \cdot \frac{(1-p^{-n})(1-p^{-m})}{1-p^{-1}} = 1 - \sum_{(n-1)(m-1)}^{(n-1)m} p^{-i} + \sum_{n(m-1)+1}^{nm-1} p^{-i}.$$

In general, we obtain the following formula.

Theorem 4.2 (General case)**.** *Let $\mathcal{S}$ be the set of* (3.2) *in Theorem 3.5 with* $d_r = \prod_{j=1}^{\infty} p_j^{s_j}$*, then for* $(p, s) = (p_j, s_j)$*,* $j = 1, 2, \ldots$*, we have*

$$\mu_{p^{s+1}}(\mathcal{S}) = p^{-\sum_{i=1}^{s}(n-\tilde{a}_i)(m-\tilde{a}_i)} \cdot \frac{[p,n][p,m]}{[p,n-\tilde{a}_s][p,m-\tilde{a}_s]\prod_{i=1}^{s}[p,\tilde{a}_i-\tilde{a}_{i-1}]}$$
$$-\sum_{\ell=\tilde{a}_s}^{r-1} p^{-(n-\ell)(m-\ell)-\sum_{i=1}^{s}(n-\tilde{a}_i)(m-\tilde{a}_i)} \cdot \frac{[p,n][p,m]}{[p,n-\ell][p,m-\ell][p,\ell-\tilde{a}_s]\prod_{i=1}^{s}[p,\tilde{a}_i-\tilde{a}_{i-1}]},$$

where $\tilde{a}_i$ $(0 \le i \le s)$ *is the number of non-*p^i*-multiples among* $d_1, d_2, \ldots, d_r$ *(thus* $\tilde{a}_s \le r-1$*). In particular, when* $s = 0$ *(which holds for all but finitely many* j*'s), we have*

$$\mu_p(\mathcal{S}) = 1 - \sum_{\ell=0}^{r-1} p^{-(n-\ell)(m-\ell)} \cdot \frac{[p,n][p,m]}{[p,n-\ell][p,m-\ell][p,\ell]} .$$

The value of $\mu(\mathcal{S})$ *is then given by Theorem 3.5 with* $z = d_r$*.*

4.2 The determinant

The determinant of an $m \times m$ matrix can be regarded as a polynomial G of its m^2 entries. Note that G is not a constant since it takes values 1 and 0 for the identity matrix and the zero matrix, respectively. Thus we can apply to G the well-known result that the probability that a nonzero polynomial at a random integer vector equals zero is 0 (see Poonen 2003, Lemma 4.1) and obtain the following.

Theorem 4.3. *Let* c *be an integer. The probability that the determinant equals* c *for an* $m \times m$ *matrix with entries from* $\mathbb{Z}_{(k)}$ *goes to* 0 *as* $k \to \infty$*; in other words, the density of the determinant of a random* $m \times m$ *integer matrix is always* 0*.*

This result agrees with Katznelson (1993, Theorem 1) for the case of $c = 0$ and Duke et al. (1993, Theorem 1.2 and Example 1.6) for the case of $c \neq 0$. It leads to the next two theorems. The first of them shows that the probability that a random $n \times m$ integer matrix is full rank is 1.

Theorem 4.4. *If* $\mathcal{S} \subseteq \mathbb{S}$ *satisfies* $D_{m,m} = 0$ *for all* $D = (D_{i,j})_{n\times m} \in \mathcal{S}$*, then we have* $\mu(\mathcal{S}) = 0$*; in other words, the probability that an* $n \times m$ *matrix with entries from* $\mathbb{Z}_{(k)}$ *is full rank goes to* 1 *as* $k \to \infty$*.*

When $m = n$, we generalize Theorem 4.4 to $\mathcal{S}$ with finitely many values of $D_{m,m}$'s.

Theorem 4.5. *Suppose that* $m = n$ *and* $\mathcal{S} \subset \mathbb{S}$*, then we have* $\mu(\mathcal{S}) = 0$ *if the set* $\{D_{n,n} : D = (D_{i,j})_{n\times n} \in \mathcal{S}\}$ *is finite; in particular, this holds for any finite subset* $\mathcal{S} \subset \mathbb{S}$*.*

4.3 Probability that all diagonal entries of the SNF are 1

Theorems 4.5 and 3.3 (iii) imply that the probability that all diagonal entries of an SNF are 1 is 0 if $m = n$; however, we find that this probability is positive if $m < n$ by applying Theorems 3.2 and 3.5.

Theorem 4.6. *Let* E *be the* $n \times m$ *diagonal matrix whose diagonal entries are all* 1*. If* $m < n$*, then*

$$\mu(\{E\}) = \frac{1}{\prod_{i=n-m+1}^{n}\zeta(i)} \to \begin{cases} 1, & \text{if } m \text{ is fixed} \\ \frac{1}{\prod_{i=n-m+1}^{\infty}\zeta(i)}, & \text{if } n-m \text{ is fixed} \end{cases}, \quad \text{as } n \to \infty .$$

4.4 Probability that at most ℓ diagonal entries of the SNF are not 1

Assume that $m = n$. We provide a formula for the probability that an SNF has at most ℓ diagonal entries not equal to 1, and a formula for the limit of this probability as $n \to \infty$. When $\ell = 1$, this limit is the reciprocal of a product of values of the Riemann zeta function at positive integers and equals 0.846936. As $\ell \to \infty$, we prove that this limit converges to 1 and find its asymptotics (see (4.1)).

We shall say that an SNF is *cyclic* if it has at most one diagonal entry not equal to 1, i.e., if the corresponding cokernel is cyclic. Denote the set of $n \times n$ cyclic SNFs by $\mathcal{T}_n$. We compute the probability $\mu(\mathcal{T}_n)$ of having a cyclic SNF, and show that this probability strictly decreases to $0.846936\cdots$ as $n \to \infty$.

Theorem 4.7 (Cyclic SNFs)**.** *We have*
(i)

$$\mu(\mathcal{T}_n) = \frac{1}{\prod_{i=2}^{n} \zeta(i)} \cdot \prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^n}\right) =: Z_n\,;$$

(ii) Z_n is strictly decreasing in n;
(iii)

$$Z_2 = \frac{1}{\zeta(4)} = \frac{90}{\pi^4} = 0.923938\cdots\,;$$

(iv)

$$\lim_{n\to\infty} Z_n = \frac{1}{\zeta(6)\prod_{i=4}^{\infty}\zeta(i)} = 0.846936\cdots\,.$$

Remark 4.8. Theorem 4.7 (i), (iv) and the numerical value of (iii) are first obtained in Ekedahl (1991, Section 3). We use a slight different approach and provide a complete and more detailed proof.

Now we consider the SNFs with at most $\ell\,(\le n)$ diagonal entries not equal to 1, i.e., whose corresponding cokernel has at most ℓ generators. Denote the set of such $n \times n$ SNFs by $\mathcal{T}_n(\ell)$. In particular, we have $\mu(\mathcal{T}_n(n)) = 1$. The above discussion on cyclic SNFs is for the case $\ell = 1$. We compute $\mu(\mathcal{T}_n(\ell))$ and its limit as $n \to \infty$, show that this limit increases to 1 as $\ell \to \infty$, and establish its asymptotics.

We start with a lemma which plays an important role in our proof.

Lemma 4.9. *For any positive number $x \le 1/2$, the positive sequence $\{[1/x, k]\}_{k=1}^{\infty}$ is decreasing and thus has a limit as $k \to \infty$:*

$$C(x) := (1-x)\,(1-x^2)\cdots \in \left[e^{-2x/(1-x)}, 1\right).$$

This also implies that $C(x) \uparrow 1$ as $x \to 0$, and $[1/x, k] \in [e^{-2x/(1-x)}, 1)$ for all $x \in (0, 1/2]$ and $k \ge 1$.

In particular, when $x = 1/p$, we have

$$[p,k] \downarrow C_p := C(1/p) \in \left[e^{-2/(p-1)}, 1\right) \subseteq \left[e^{-2}, 1\right), \text{ as } k \to \infty,$$

$C_p \to 1$ as $p \to \infty$, and $[p,k] \in [e^{-2/(p-1)}, 1)$ for all p and $k \ge 1$.

Theorem 4.10 (ℓ generators)**.** *We have*

$$\mu(\mathcal{T}_n(\ell)) = \prod_p Z_n(p,\ell) = \frac{1}{\prod_{i=2}^{n}\zeta(i)} \prod_p Y_n(p,\ell)$$

where

$$Z_n(p,\ell) = \mu_p(\mathcal{T}_n(\ell)) = [p,n]\sum_{i=0}^{\ell} \frac{p^{-i^2}[p,n]}{[p,i]^2[p,n-i]}\,, \quad Y_n(p,\ell) = [p,1]\sum_{i=0}^{\ell} \frac{p^{-i^2}[p,n]}{[p,i]^2[p,n-i]}\,,$$

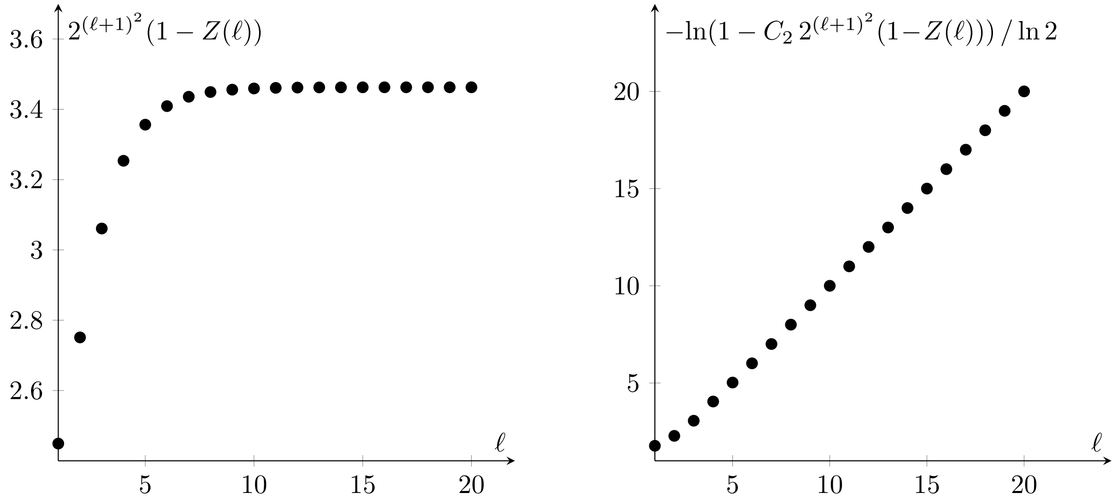
and

$$Z(\ell) := \lim_{n\to\infty} \mu(\mathcal{T}_n(\ell)) = 1 - C_2^{-1}\cdot 2^{-(\ell+1)^2}\left[1 - 2^{-\ell} + O\left(4^{-\ell}\right)\right] \text{ as } \ell\to\infty\,, \tag{4.1}$$

where $C_2^{-1} = [(1-2^{-1})(1-2^{-2})\cdots]^{-1} = 3.46275\cdots$, *and* $Z(\ell)\uparrow 1$ *as* $\ell\to\infty$.

Figure 1 and Table 1 below illustrate the asymptotics (4.1) of $Z(\ell)$ and the fast rate of convergence.

Fig. 1: Asymptotics of $Z(\ell)$



Tab. 1: Asymptotics of $Z(\ell)$

ℓ	$Z(\ell)$	$1-Z(\ell)$	$2^{(\ell+1)^2}(1-Z(\ell))$	$-\ln[1 - C_2\,2^{(\ell+1)^2}(1-Z(\ell))]\,/\ln 2$
1	0.84693590174	$1.5306409827\times 10^{-1}$	2.4490255722	1.7722561143
2	0.99462688354	$5.3731164573\times 10^{-3}$	2.7510356262	2.2825533991
3	0.99995329508	$4.6704924839\times 10^{-5}$	3.0608539542	3.1070346720
4	0.99999990304	$9.6964549316\times 10^{-8}$	3.2535903764	4.0492638585
5	0.99999999995	$4.8841345825\times 10^{-11}$	3.3563517281	5.0244160399
6	1.00000000000	$6.0557728677\times 10^{-15}$	3.4090970538	6.0122065228
7	1.00000000000	$1.8625553206\times 10^{-19}$	3.4358081323	7.0061041819
8	1.00000000000	$1.4265758896\times 10^{-24}$	3.4492488532	8.0030523343
9	1.00000000000	$2.7262958680\times 10^{-30}$	3.4559905935	9.0015262279
10	1.00000000000	$1.3012691691\times 10^{-36}$	3.4593668192	10.000763129

Acknowledgements

The authors are grateful to Professor Bjorn Poonen for advice on the literature on the subject of this paper.

References

G. Akemann, J. Baik, and P. Di Francesco. *The Oxford Handbook of Random Matrix Theory*. Oxford University Press, Oxford, 2011.

G.W. Anderson, A. Guionnet, and O. Zeitouni. *An Introduction to Random Matrices*. Cambridge University Press, Cambridge, 2010.

M. Bôcher. *Introduction to Higher Algebra*. Dover Publications, Inc., New York, 1964.

H. Cohen and H.W. Lenstra, Jr. Heuristics on class groups. *Number theory (New York 1982)*, Lecture Notes in Math. 1052: 26–36, Springer, Berlin, 1984.

H. Cohen and H.W. Lenstra, Jr. Heuristics on class groups of number fields. *Number theory (Noordwijkerhout 1983)*, Lecture Notes in Math. 1068: 33–62, Springer, Berlin, 1984.

W. Duke, Z. Rudnick, and P. Sarnak. Density of integer points on affine homogeneous varieties. *Duke Math. J.* 71(1): 143–179, 1993.

T. Ekedahl. An infinite version of the Chinese remainder theorem. *Comment. Math. Univ. St. Paul.* 40(1): 53–59, 1991.

C. Feng, R.W. Nóbrega, F.R. Kschischang, and D. Silva. Communication over finite-ring matrix channels. *Proc. IEEE Int. Symp. Information Theory (ISIT)*, 2890–2894, 2013.

C. Feng, R.W. Nóbrega, F.R. Kschischang, and D. Silva. Communication over finite-chain-ring matrix channels. *IEEE Trans. Inform. Theory* 60(10): 5899–5917, 2014.

E. Friedman and L.C. Washington. On the distribution of divisor class groups of curves over a finite field. *Théorie des nombres (Quebec, PQ, 1987)*, 227–239, de Gruyter, Berlin, 1989.

J. Fulman. Random matrix theory over finite fields. *Bull. Amer. Math. Soc. (N.S.)* 39(1): 51–85, 2002.

Y.R. Katznelson. Singular matrices and a uniform bound for congruence groups of $SL_n(\mathbf{Z})$. *Duke Math. J.* 69(1), 121–136, 1993.

M.L. Mehta. *Random Matrices*. Third ed. Elsevier/Academic Press, Amsterdam, 2004.

B. Poonen. Squarefree values of multivariable polynomials. *Duke Math. J.* 118(2): 353–373, 2003.

B. Poonen and M. Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)* 150(3): 1109–1149, 1999.

R.P. Stanley. *Enumerative Combinatorics*. Vol. 1, second ed., Cambridge University Press, Cambridge, 2011.

Y. Wang and R.P. Stanley. The Smith normal form distribution of a random integer matrix *Preprint*, 2015. Available at http://arxiv.org/abs/1506.00160.

M.M. Wood. Random integral matrices and the Cohen Lenstra Heuristics. *Preprint*, 2015. Available at http://arxiv.org/abs/1504.04391.