Eigenvalues of Random Matrices over Finite Fields

Kent Morrison

Department of Mathematics
California Polytechnic State University
San Luis Obispo, CA 93407
kmorriso@calpoly.edu

September 5, 1999

Abstract

We determine the limiting distribution of the number of eigenvalues of a random $n \times n$ matrix over $\mathbf{F}_q$ as $n \to \infty$. We show that the $q \to \infty$ limit of this distribution is Poisson with mean 1. The main tool is a theorem proved here on asymptotic independence for events defined by conjugacy class data arising from distinct irreducible polynomials. The proof of this theorem uses the cycle index for matrices developed by Kung and Stong. Several examples are given to illustrate the use of the asymptotic independence theorem. These include previous results about derangements and about cyclic and semi-simple matrices.

1 The Cycle Index for $\mathrm{M}_n(q)$

For a prime power q let $\mathbf{F}_q$ denote the field with q elements. Let $\mathrm{M}_n(q)$ be the space of $n \times n$ matrices over $\mathbf{F}_q$ and let $\mathrm{GL}_n(q)$ be the group of invertible matrices.

To define the cycle index for $\mathrm{M}_n(q)$ we recall the rational canonical form of a matrix (see, for example, [8]). Each matrix $\alpha \in \mathrm{M}_n(q)$ gives rise to a finite dimensional $\mathbf{F}_q[z]$-module isomorphic to a direct sum

$$\bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l_i} \mathbf{F}_q[z]/(\phi_i^{\lambda_{i,j}})$$

where $\phi_1, \ldots, \phi_k$ are distinct monic irreducible polynomials; for each i, $\lambda_{i,1} \geq \lambda_{i,2} \geq \cdots \geq \lambda_{i,l_i}$ is a partition of $n_i = \sum_j \lambda_{i,j}$. If α is $n \times n$, then $n = \sum_i n_i \deg \phi_i = \sum_{i,j} \lambda_{i,j} \deg \phi_i$. Let λ_i denote the partition of n_i given by the $\lambda_{i,j}$ and define $|\lambda_i| = n_i$. The conjugacy class of α in $\mathrm{M}_n(q)$ is determined by the data consisting of the finite list of distinct monic irreducible polynomials $\phi_1, \ldots, \phi_k$ and the partitions $\lambda_1, \ldots, \lambda_k$.

We introduce an indeterminate $x_{\phi,\lambda}$ for each pair of a monic irreducible polynomial ϕ and a partition λ of some non-negative integer. The conjugacy class data for α is encoded into the product

$$x_{\phi_1,\lambda_1} \ldots x_{\phi_k,\lambda_k}.$$

We can write this more economically if we define $\lambda_\phi(\alpha)$ to be the (possibly empty) partition corresponding to ϕ in the rational canonical form for α. We regard the empty partition as the

1991 Mathematics Subject Classification. Primary 05A16, 15A33, 60C05; Secondary 15A18, 15A21
Key words and phrases. Asymptotic probability, cycle index.

only partition of 0. Set the corresponding indeterminates $x_{\phi,\emptyset} = 1$ for all ϕ. Then we can use $\prod_\phi x_{\phi,\lambda_\phi(\alpha)}$ for the monomial corresponding to α. Following Kung [7]and Stong [10], we define the **cycle index** of $\mathrm{M}_n(q)$ to be

$$1 + \sum_{n=1}^{\infty} \frac{u^n}{|\mathrm{GL}_n(q)|} \sum_{\alpha \in \mathrm{M}_n(q)} \prod_{\phi} x_{\phi,\lambda_\phi(\alpha)}.$$

(The first definition of the cycle index due to Kung used indeterminates $x_{m,\lambda}$ for m a positive integer m and λ a partition of m. But this definition did not distinguish among different irreducible polynomials of the same degree. Stong later modified the definition of the cycle index to be the one used in this paper.) Kung and Stong proved the following factorization holds.

Theorem 1

$$1 + \sum_{n=1}^{\infty} \frac{u^n}{|\mathrm{GL}_n(q)|} \sum_{\alpha \in \mathrm{M}_n(q)} \prod_{\phi} x_{\phi,\lambda_\phi(\alpha)} = \prod_{\phi} \sum_{\lambda} \frac{x_{\phi,\lambda} u^{|\lambda| \deg \phi}}{c_\phi(\lambda)}$$

where $c_\phi(\lambda)$ is the order of the group of module automorphisms of the $\mathbf{F}_q[z]$-module $\bigoplus_j \mathbf{F}_q[z]/(\phi^{\lambda_j})$.

Proof On the left side $\sum_{\alpha \in \mathrm{M}_n(q)} \prod_\phi x_{\phi,\lambda_\phi(\alpha)}$ is the sum of all monomials corresponding to all $n \times n$ matrices. Split this sum according to the conjugacy classes. Let $\phi_1, \ldots, \phi_k$ and $\lambda_1, \ldots, \lambda_k$ be the data of one conjugacy class. The monomial $\prod x_{\phi_i,\lambda_i}$ occurs with the coefficient equal to the size of the conjugacy class, namely $|\mathrm{GL}_n(q)|/|G|$, where G is the centralizer of an element in the conjugacy class. But G is isomorphic to the the subgroup of automorphisms of the $\mathbf{F}_q[z]$-module $\bigoplus_i \bigoplus_j \mathbf{F}_q[z]/(\phi_i^{\lambda_{i,j}})$. An automorphism preserves the the ϕ_i-primary component and so $|G| = \prod c_{\phi_i}(\lambda_i)$. Then

$$\frac{1}{|\mathrm{GL}_n(q)|} \sum_{\alpha} \prod_{\phi} x_{\phi,\lambda_\phi(\alpha)}$$

has the monomial $\prod x_{\phi_i,\lambda_i}$ occurring with coefficient

$$\frac{1}{c_{\phi_1}(\lambda_1) \ldots c_{\phi_k}(\lambda_k)}$$

which is exactly how the same monomial appears in the right hand side. □

In dealing with the cycle index for $\mathrm{M}_n(q)$ we have found Fulman's [4] notation and presentation most useful. There are several basic tools necessary for working with the cycle index. We give them as a sequence of lemmas as in [4]. First, from Kung [7] we get a formula for $c_\phi(\lambda)$ contained in the next lemma. See that paper for the proof.

Lemma 2 *Let λ be the partition of n given by $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$. Let m_i be the number of parts of size i. Let $d_i = m_1 + 2m_2 + \cdots + im_i + i(m_{i+1} + \cdots + m_n)$. Then*

$$c_\phi(\lambda) = \prod_{i=1}^{n} \prod_{j=1}^{m_i} (q^{d_i \deg \phi} - q^{(d_i - j) \deg \phi}).$$

Note In the Ferrers diagram of λ consisting of λ_i boxes in row i, one can see that d_i is the number of boxes in the first i columns.

Lemma 3 (Stong [10]) *Fix a monic irreducible ϕ. Then*

$$\sum_{\lambda} \frac{u^{|\lambda| \deg \phi}}{c_\phi(\lambda)} = \prod_{r \geq 1} \left(1 - \frac{u^{\deg \phi}}{q^{r \deg \phi}}\right)^{-1}.$$

Proof It is sufficient to prove this when $\deg \phi = 1$ because of the way $c_\phi(\lambda)$ depends on the degree of ϕ. Furthermore, since $c_\phi(\lambda)$ just depends on the degree, it is sufficient to prove it for $\phi(z) = z$. Now we are dealing with

$$\sum_{\lambda} \frac{u^{|\lambda|}}{c_\phi(\lambda)}$$

which we split into an outer sum over n and an inner sum over the partitions of n

$$\sum_{\lambda} \frac{u^{|\lambda|}}{c_\phi(\lambda)} = 1 + \sum_{n \geq 1} \sum_{|\lambda|=n} \frac{u^n}{c_\phi(\lambda)}.$$

To evaluate the inner sum we note that $|\mathrm{GL}_n(q)| \sum_{|\lambda|=n} \frac{1}{c_\phi(\lambda)}$ is the number of nilpotent matrices of size $n \times n$. Fine and Herstein [3] proved that the number of $n \times n$ nilpotent matrices is $q^{n(n-1)}$. Therefore,

$$\sum_{|\lambda|=n} \frac{1}{c_\phi(\lambda)} = \frac{1}{q^n(1 - \frac{1}{q}) \ldots (1 - \frac{1}{q^n})}.$$

Next we use a formula from Hardy and Wright [6, Theorem 349, p. 280]. For $|a| < 1$, $|y| < 1$, the coefficient of a^n in the infinite product

$$\prod_{r \geq 1} \frac{1}{(1 - ay^r)}$$

is

$$\frac{y^n}{(1-y)(1-y^2)\ldots(1-y^n)}.$$

With this formula let $a = u$ and $y = \frac{1}{q}$ to see that the u^n coefficient of

$$\prod_{r \geq 1} \frac{1}{1 - \frac{u}{q^r}}$$

is

$$\frac{1}{q^n(1 - \frac{1}{q}) \ldots (1 - \frac{1}{q^n})}.$$

□

A key lemma for evaluating asymptotic probabilities is found in Wilf [11, Lemma B, p. 144] or Fulman [4]. For a power series $f(u) = \sum_n a_n u^n$, we let $[[u^n]]f(u)$ mean the coefficient of u^n.

Lemma 4 *If f is analytic at $u = 0$ and the power series for f converges at $u = 1$, then*

$$\lim_{n \to \infty} [[u^n]] \frac{f(u)}{1-u} = f(1).$$

Proof Multiply $f(u) = \sum_{n\geq 0} a_n u^n$ by $(1-u)^{-1} = 1 + u + \cdots + u^n + \ldots$. The coefficient of u^n is $\sum_{k=0}^{n} a_k$. Now let n go to infinity. □

Lemma 5

$$\prod_{\phi}\left(1 - \frac{u^{\deg\phi}}{q^{r\deg\phi}}\right) = 1 - \frac{u}{q^{r-1}}$$

Proof Let $r = 1$. Then

$$\prod_{\phi}(1 - \frac{u^{\deg\phi}}{q^{\deg\phi}})^{-1} = \prod_{\phi}\sum_{k\geq 0}\left(\frac{u}{q}\right)^{k\deg\phi}$$

Expanding this product we use unique factorization of polynomials in $\mathbf{F}_q[z]$ to see that the coefficient of $(\frac{u}{q})^n$ is q^n because the coefficient in question is the number of monic polynomials of degree n. Thus,

$$\prod_{\phi}\sum_{k\geq 0}\left(\frac{u}{q}\right)^{k\deg\phi} = \sum_{n\geq 0} q^n\left(\frac{u}{q}\right)^n = \frac{1}{1-u}.$$

Now replace u by $\frac{u}{q^{r-1}}$. □

Lemma 6

$$\prod_{\phi}\sum_{\lambda}\frac{u^{|\lambda|\deg\phi}}{c_\phi(\lambda)} = \prod_{r\geq 0}\left(1 - \frac{u}{q^r}\right)^{-1}.$$

Proof Follows easily from the previous lemmas. □

2 Asymptotic Probability

We will consider a subset $\mathcal{A} \subset \bigcup_{n\geq 1}\mathrm{M}_n(q)$ as an event, although strictly speaking it is a family of events parameterized by n. For each n we have the event $\mathcal{A}\cap\mathrm{M}_n(q)$ contained in the finite probability space $\mathrm{M}_n(q)$. Define the **asymptotic probability** of $\mathcal{A}$ as

$$\hat{\mathrm{P}}(\mathcal{A}) := \lim_{n\to\infty}\frac{|\mathcal{A}\cap\mathrm{M}_n(q)|}{|\mathrm{M}_n(q)|},$$

if this limit exists. We are particularly interested in events that are defined by conjugacy class data. Let L be any subset of the set of all partitions of all non-negative integers and let ψ be a monic irreducible polynomial over $\mathbf{F}_q$. Define the event $\mathcal{E}(\psi, L)$ to be the set of square matrices $\{\alpha|\lambda_\psi(\alpha) \in L\}$. For example, the invertible matrices are $\mathcal{E}(\psi, L)$ where $\psi(z) = z$ and L is the singleton set consisting of the empty partition; in this case, $\hat{\mathrm{P}}(\mathcal{E}(\psi, L)) = \prod_{r\geq 1}(1 - \frac{1}{q^r})$.

Theorem 7

$$\hat{\mathrm{P}}(\mathcal{E}(\psi, L)) = \prod_{r\geq 1}\left(1 - \frac{1}{q^{r\deg\psi}}\right)\sum_{\lambda\in L}\frac{1}{c_\psi(\lambda)}$$

Proof Beginning with the cycle index and its factorization we use the lemmas above.

$$\begin{aligned}
\hat{\mathrm{P}}(\mathcal{E}(\psi, L)) &= \lim_{n\to\infty} \frac{|\mathrm{GL}_n(q)|}{|\mathrm{M}_n(q)|}[[u^n]] \left\{ \left(\prod_{\phi\neq\psi} \sum_{\lambda} \frac{u^{|\lambda|\deg\phi}}{c_\phi(\lambda)} \right) \sum_{\lambda\in L} \frac{u^{|\lambda|\deg\psi}}{c_\psi(\lambda)} \right\} \\
&= \prod_{r\geq 1} \left(1-\frac{1}{q^r}\right) \lim_{n\to\infty}[[u^n]] \left\{ \frac{\prod_\phi \sum_\lambda \frac{u^{|\lambda|\deg\phi}}{c_\phi(\lambda)}}{\sum_\lambda \frac{u^{|\lambda|\deg\psi}}{c_\psi(\lambda)}} \sum_{\lambda\in L} \frac{u^{|\lambda|\deg\psi}}{c_\psi(\lambda)} \right\} \\
&= \prod_{r\geq 1} \left(1-\frac{1}{q^r}\right) \lim_{n\to\infty}[[u^n]] \left\{ \frac{\prod_{r\geq 0}\left(1-\frac{u}{q^r}\right)^{-1}}{\prod_{r\geq 1}\left(1-\frac{u^{\deg\psi}}{q^{r\deg\psi}}\right)^{-1}} \sum_{\lambda\in L} \frac{u^{|\lambda|\deg\psi}}{c_\psi(\lambda)} \right\} \\
&= \prod_{r\geq 1} \left(1-\frac{1}{q^r}\right) \lim_{n\to\infty}[[u^n]] \left\{ \frac{1}{1-u} \frac{\prod_{r\geq 1}\left(1-\frac{u}{q^r}\right)^{-1}}{\prod_{r\geq 1}\left(1-\frac{u^{\deg\psi}}{q^{r\deg\psi}}\right)^{-1}} \sum_{\lambda\in L} \frac{u^{|\lambda|\deg\psi}}{c_\psi(\lambda)} \right\} \\
&= \prod_{r\geq 1} \left(1-\frac{1}{q^r}\right) \frac{\prod_{r\geq 1}\left(1-\frac{1}{q^r}\right)^{-1}}{\prod_{r\geq 1}\left(1-\frac{1}{q^{r\deg\psi}}\right)^{-1}} \sum_{\lambda\in L} \frac{1}{c_\psi(\lambda)} \\
&= \prod_{r\geq 1} \left(1-\frac{1}{q^{r\deg\psi}}\right) \sum_{\lambda\in L} \frac{1}{c_\psi(\lambda)}
\end{aligned}$$

□

Theorem 8 (Asymptotic Coprime Independence) *If ψ_1 and ψ_2 are distinct monic irreducible polynomials over $\mathbf{F}_q$ and L_1 and L_2 are subsets of all partitions of non-negative integers, then*

$$\hat{\mathrm{P}}(\mathcal{E}(\psi_1, L_1) \cap \mathcal{E}(\psi_2, L_2)) = \hat{\mathrm{P}}(\mathcal{E}(\psi_1, L_1))\hat{\mathrm{P}}(\mathcal{E}(\psi_2, L_2))$$

Proof

$$\begin{aligned}
&\hat{\mathrm{P}}(\mathcal{E}(\psi_1, L_1) \cap \mathcal{E}(\psi_2, L_2)) \\
&= \lim_{n\to\infty} \frac{|\mathrm{GL}_n(q)|}{|\mathrm{M}_n(q)|}[[u^n]] \left\{ \left(\prod_{\phi\neq\psi_1,\psi_2} \sum_{\lambda} \frac{u^{|\lambda|\deg\phi}}{c_\phi(\lambda)} \right) \sum_{\lambda\in L_1} \frac{u^{|\lambda|\deg\psi_1}}{c_{\psi_1}(\lambda)} \sum_{\lambda\in L_2} \frac{u^{|\lambda|\deg\psi_2}}{c_{\psi}(\lambda)} \right\} \\
&= \prod_{r\geq 1} \left(1-\frac{1}{q^r}\right) \lim_{n\to\infty}[[u^n]] \left\{ \frac{\prod_\phi \sum_\lambda \frac{u^{|\lambda|\deg\phi}}{c_\phi(\lambda)}}{\sum_\lambda \frac{u^{|\lambda|\deg\psi_1}}{c_{\psi_1}(\lambda)} \sum_\lambda \frac{u^{|\lambda|\deg\psi_2}}{c_{\psi_1}(\lambda)}} \sum_{\lambda\in L_1} \frac{u^{|\lambda|\deg\psi_1}}{c_{\psi_1}(\lambda)} \sum_{\lambda\in L_2} \frac{u^{|\lambda|\deg\psi_2}}{c_{\psi_2}(\lambda)} \right\} \\
&= \prod_{r\geq 1} \left(1-\frac{1}{q^r}\right) \times \\
&\quad \lim_{n\to\infty}[[u^n]] \left\{ \frac{\prod_{r\geq 0}\left(1-\frac{u}{q^r}\right)^{-1}}{\prod_{r\geq 1}\left(1-\frac{u^{\deg\psi_1}}{q^{r\deg\psi_1}}\right)^{-1} \prod_{r\geq 1}\left(1-\frac{u^{\deg\psi_2}}{q^{r\deg\psi_2}}\right)^{-1}} \sum_{\lambda\in L_1} \frac{u^{|\lambda|\deg\psi_1}}{c_{\psi_1}(\lambda)} \sum_{\lambda\in L_2} \frac{u^{|\lambda|\deg\psi_2}}{c_{\psi_2}(\lambda)} \right\} \\
&= \prod_{r\geq 1} \left(1-\frac{1}{q^{r\deg\psi_1}}\right) \prod_{r\geq 1} \left(1-\frac{1}{q^{r\deg\psi_2}}\right) \sum_{\lambda\in L_1} \frac{1}{c_{\psi_1}(\lambda)} \sum_{\lambda\in L_2} \frac{1}{c_{\psi_2}(\lambda)} \\
&= \hat{\mathrm{P}}(\mathcal{E}(\psi_1, L_1))\hat{\mathrm{P}}(\mathcal{E}(\psi_2, L_2)).
\end{aligned}$$

□

Since $\hat{\mathrm{P}}$ is not a probability measure on a sample space, we do not have countable additivity of $\hat{\mathrm{P}}$. It is countable additivity that implies that the probability of a countable intersection of independent events is the product of the probabilities of the events. In light of that it is notable that we do have such a result for a countable intersection of events of the form $\mathcal{E}(\psi_i, L_i)$. This corollary allows us to consider asymptotic probabilities for events defined by conditions on each monic, irreducible polynomial in $\mathbf{F}_q[z]$.

Corollary 9 *For distinct, monic, irreducible polynomials ψ_i, and arbitrary subsets of partitions L_i, $i = 1, 2, \ldots$*

$$\hat{\mathrm{P}}\left(\bigcap_{i=1}^{\infty} \mathcal{E}(\psi_i, L_i)\right) = \prod_{i=1}^{\infty} \hat{\mathrm{P}}(\mathcal{E}(\psi_i, L_i)).$$

Proof The proof follows that of the theorem. □

In order to consider probability questions involving invertible matrices, rather than all matrices, the next theorem is quite useful, because it shows that the asymptotic conditional probability of an event (conditioned on invertibility) is typically the same as the asymptotic unconditioned probability. For events $\mathcal{A}_1$ and $\mathcal{A}_2$, we define the asymptotic conditional probability of $\mathcal{A}_1$ given $\mathcal{A}_2$ as

$$\hat{\mathrm{P}}(\mathcal{A}_1|\mathcal{A}_2) := \lim_{n\to\infty} \frac{|\mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathrm{M}_n(q)|}{|\mathcal{A}_2 \cap \mathrm{M}_n(q)|} = \lim_{n\to\infty} \frac{\mathrm{P}(\mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathrm{M}_n(q))}{\mathrm{P}(\mathcal{A}_2 \cap \mathrm{M}_n(q))}$$

Theorem 10 *Let $\{\psi_i\}_{i\in I}$ be a finite or countable set of distinct, monic, irreducible polynomials in $\mathbf{F}_q[z]$, none of which is equal to z. Let L_i, $i \in I$, be subsets of partitions and let $\mathcal{E}_i = \mathcal{E}(\psi_i, L_i)$. Then*

$$\hat{\mathrm{P}}(\bigcap_i \mathcal{E}_i | \text{ invertible}) = \hat{\mathrm{P}}(\bigcap_i \mathcal{E}_i)$$

Proof A matrix α is invertible if $\lambda_z(\alpha) = \emptyset$. Therefore, the subset of invertible matrices is $\mathcal{E}(z, \{\emptyset\})$ which we will denote by $\mathcal{E}_0$.

$$\begin{aligned}
\hat{\mathrm{P}}(\bigcap_{i\geq 1} \mathcal{E}_i | \text{invertible}) &= \lim_{n\to\infty} \frac{\mathrm{P}(\bigcap_{i\geq 1} \mathcal{E}_i \cap \mathcal{E}_0 \cap \mathrm{M}_n(q))}{\mathrm{P}(\mathcal{E}_0 \cap \mathrm{M}_n(q))} \\
&= \frac{\lim_{n\to\infty} \mathrm{P}(\bigcap_{i\geq 1} \mathcal{E}_i \cap \mathcal{E}_0 \cap \mathrm{M}_n(q))}{\lim_{n\to\infty} \mathrm{P}(\mathcal{E}_0 \cap \mathrm{M}_n(q))} \\
&= \frac{\hat{\mathrm{P}}(\bigcap_{i\geq 1} \mathcal{E}_i)\hat{\mathrm{P}}(\mathcal{E}_0)}{\hat{\mathrm{P}}(\mathcal{E}_0)} \\
&= \hat{\mathrm{P}}(\bigcap_{i\geq 1} \mathcal{E}_i)
\end{aligned}$$

□

Let X be a real or integer valued function on the union of the $\mathrm{M}_n(q)$. We will refer to such an X as a random variable although it is actually a family of random variables, one for each discrete probability space $\mathrm{M}_n(q)$. An important example, to be treated in detail in section 4, is the dimension of the kernel. Now for a random variable X taking values in $\mathbf{N} = \{0, 1, 2, \ldots\}$. we consider the asymptotic probabilities $\hat{\mathrm{P}}(X = k)$ for each $k \in \mathbf{N}$. These may or may not define a probability distribution on $\mathbf{N}$ because of the limiting process. A trivial example of not being a probability distribution is given by X being the size of the matrix. In this case $\hat{\mathrm{P}}(X = k) = 0$ for

all k. But for random variables expressed in terms of conjugacy class data we have the following theorem.

Theorem 11 *If f is a function from partitions to $\mathbf{N}$ and X is the random variable defined by $X(\alpha) = f(\lambda_\phi(\alpha))$ for a fixed monic, irreducible polynomial ϕ, then*

$$\sum_{k\geq 0} \hat{\mathrm{P}}(X = k) = 1.$$

Proof We let $L_k = f^{-1}(k)$ and then $\mathcal{E}(\phi, L_k)$ is the event that $X = k$. By Theorem 7

$$\hat{\mathrm{P}}(X = k) = \hat{\mathrm{P}}(\mathcal{E}(\phi, L_k)) = \prod_{r\geq 1}\left(1 - \frac{1}{q^{r\deg\phi}}\right)\sum_{\lambda\in L_k}\frac{1}{c_\phi(\lambda)}.$$

Summing over k gives us

$$\sum_{k\geq 0}\hat{\mathrm{P}}(X = k) = \prod_{r\geq 1}\left(1 - \frac{1}{q^{r\deg\phi}}\right)\sum_{k\geq 0}\sum_{\lambda\in L_k}\frac{1}{c_\phi(\lambda)}.$$

Now the sum $\sum_{k\geq 0}\sum_{\lambda\in L_k}\frac{1}{c_\phi(\lambda)}$ is the sum over all partitions. By Lemma 3

$$\sum_{\lambda}\frac{1}{c_\phi(\lambda)} = \prod_{r\geq 1}\left(1 - \frac{1}{q^{r\deg\phi}}\right)^{-1}.$$

□

3 The Number of Eigenvalues

For each $a \in \mathbf{F}_q$ define the "random variable" X_a to be the dimension of the a-eigenspace, that is, $X_a(\alpha) = \dim\ker(\alpha - aI)$. Thus, X_a is the geometric multiplicity of a as an eigenvalue. This theorem gives the asymptotic distribution of X_a. Notice that the most likely multiplicity is 1.

Theorem 12 *For $k \geq 1$,*

$$\hat{\mathrm{P}}(X_a = k) = \frac{q^k}{(q-1)^2\ldots(q^k-1)^2}\prod_{r\geq 1}\left(1 - \frac{1}{q^r}\right)$$

For $k = 0$

$$\hat{\mathrm{P}}(X_a = 0) = \prod_{r\geq 1}\left(1 - \frac{1}{q^r}\right)$$

Proof It is enough to show this for $a = 0$ since $X_0(\alpha - aI) = X_a(\alpha)$. First we count the linear maps on $\mathbf{F}_q^n$ with k-dimensional kernel. The number of possible subspaces of dimension k to serve as the kernel is

$$\frac{(q^n-1)(q^n-q)\ldots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\ldots(q^k-q^{k-1})}$$

(This is a Gaussian binomial coefficient.) Having chosen a subspace to be the kernel let $v_1, \ldots, v_{n-k}$ be complementary linearly independent vectors. They must be mapped to linearly independent

vectors. Now v_1 can be mapped to any of $q^n - 1$ vectors, v_2 to any of $q^n - q$ vectors, and so on, ending with v_{n-k} mapped to any of $q^n - q^{n-k-1}$ vectors. Thus, the number of linear maps with k-dimensional kernel is

$$\frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})}(q^n-1)\dots(q^n-q^{n-k-1})$$

Dividing this by q^{n^2} we get the probability that an $n \times n$ matrix has k-dimensional kernel, which is

$$\frac{q^k}{(q-1)^2\dots(q^k-1)^2}\prod_{i=1}^{n}\left(1-\frac{1}{q^i}\right)\prod_{i=n-k+1}^{n}\left(1-\frac{1}{q^i}\right)$$

Now let $n \to \infty$. □

Since X_a is a random variable whose value on the matrix α only depends on the partition $\lambda_{z-a}(\alpha)$, it follows from Theorem 11 that the asymptotic probabilities $\rho_k := \hat{\mathrm{P}}(X_a = k)$ actually define a discrete probability distribution on the non-negative integers $k = 0, 1, 2, \dots$. However, this special case is equivalent to an identity of Euler. For a proof see Andrews [1, 2.2.9, p. 21] and substitute $1/q$ for q.

Corollary 13 *Let L_k be the set of partitions having exactly k parts and let ϕ be a monic irreducible polynomial of degree m. Then*

$$\sum_{\lambda \in L_k}\frac{1}{c_\phi(\lambda)} = \frac{q^{km}}{(q^m-1)^2\dots(q^{km}-1)^2}.$$

Proof First, for $\deg\phi = 1$ we have $\phi(z) = z - a$ for some $a \in \mathbf{F}_q$. Then $\lambda_\phi(\alpha) \in L_k$ iff $X_a(\alpha) = k$. Now use the previous theorem. For the higher degree case just replace q by q^m. □

We define $\hat{\mathrm{E}}(X_a)$ to be the limit as $n \to \infty$ of the expected value of X_a on $\mathrm{M}_n(q)$. The next theorem justifies an interchange of limits.

Theorem 14

$$\hat{\mathrm{E}}(X_a) = \sum_{k \geq 0} k\rho_k.$$

Proof Let P_n and E_n denote probability and expected value on $\mathrm{M}_n(q)$. Then

$$\begin{aligned}\hat{\mathrm{E}}(X_a) &= \lim_{n\to\infty}\mathrm{E}_n(X_a)\\ &= \lim_{n\to\infty}\sum_{k\geq 0}k\mathrm{P}_n(X_a = k)\end{aligned}$$

We use the Dominated Convergence Theorem on the measure space $\{0, 1, 2, \dots\}$ with counting measure. For each n the $k\mathrm{P}_n(X_a = k)$ define an integrable function on this measure space. From Theorem 12 we see that

$$k\mathrm{P}_n(X_a = k) < \frac{kq^k}{(q-1)^2\dots(q^k-1)^2}.$$

The right side is the kth term of a convergent series by the Ratio Test, and so Dominated Convergence implies

$$\begin{aligned}\lim_{n\to\infty}\sum_{k\geq 0} k\mathrm{P}_n(X_a=k) &= \sum_{k\geq 0}\lim_{n\to\infty} k\mathrm{P}_n(X_a=k)\\ &= \sum_{k\geq 0} k\hat{\mathrm{P}}(X_a=k)\\ &= \sum_{k\geq 0} k\rho_k.\end{aligned}$$

□

Define the random variable $X=\sum_{a\in\mathbf{F}_q} X_a$, which counts the number of eigenvalues (with multiplicity) in $\mathbf{F}_q$. Then $\hat{\mathrm{E}}(X)$ is the asymptotic expected number of eigenvalues.

Proposition 15 *The asymptotic expected number of eigenvalues of a matrix over $\mathbf{F}_q$ is*

$$q\prod_{r\geq 1}\left(1-\frac{1}{q^r}\right)\sum_{k\geq 1}\frac{kq^k}{(q-1)^2\dots(q^k-1)^2}.$$

Proof $\hat{\mathrm{E}}(X)=\hat{\mathrm{E}}\left(\sum_{a\in\mathbf{F}_q}\right)=q\hat{\mathrm{E}}(X_0)$, since the X_a are identically distributed. Therefore, $\hat{\mathrm{E}}(X)=q\sum_{k\geq 0}k\rho_k$. □

In order to describe the asymptotic distribution of the number of eigenvalues we make use of the probability generating function for the random variable X defined by

$$f_X(t)=\sum_{k=0}^{\infty}\hat{\mathrm{P}}(X=k)t^k.$$

We also have the probability generating functions for each of the X_a given by

$$f_{X_a}(t)=\sum_{k=0}^{\infty}\rho_k t^k=\sum_{k=0}^{\infty}\hat{\mathrm{P}}(X_a=k)t^k.$$

Because of the asymptotic independence of the X_a for $a\in\mathbf{F}_q$ we see that

$$f_X(t)=\prod_{a\in\mathbf{F}_q} f_{X_a}(t),$$

but the X_a are also identically distributed. Therefore

$$f_X(t)=\left(\sum_{k=0}^{\infty}\rho_k t^k\right)^q.$$

Theorem 16 *The asymptotic probability that a matrix over $\mathbf{F}_q$ has k eigenvalues in $\mathbf{F}_q$ (counted with multiplicity) is given by the coefficient of t^k in the power series*

$$\left(\sum_{k=0}^{\infty}\rho_k t^k\right)^q.$$

In other words, this asymptotic probability is

$$\sum_{k_1+\ldots k_q=k} \rho_{k_1}\rho_{k_2}\cdots\rho_{k_q}.$$

The probability of no eigenvalue is the constant term of f_X, which is $\rho_0^q = \prod_{r\geq 1}\left(1-\frac{1}{q^r}\right)^q$, and the probability of exactly one eigenvalue is the t-coefficient of f_X, which is

$$q\rho_0^{q-1}\rho_1 = \frac{1}{(1-\frac{1}{q})^2}\prod_{r\geq 1}\left(1-\frac{1}{q^r}\right)^q.$$

Example 1 For $q=2$ the values of the ρ_k are approximately

$$\begin{aligned}\rho_0 &\approx 0.289\\ \rho_1 &\approx 0.578\\ \rho_2 &\approx 0.128\\ \rho_3 &\approx 0.005.\end{aligned}$$

For $k\geq 4$, $\rho_k \approx 0$. The expected dimension of the null space is $\hat{\mathrm{E}}(X_0) = \sum_k k\rho_k \approx 0.85$ and the expected number of eigenvalues is $2\hat{\mathrm{E}}(X_0) \approx 1.7$. The distribution of the number of eigenvalues can be seen in the coefficients of the probability generating function

$$\begin{aligned}f_X(t) &= \rho_0^2 + 2\rho_0\rho_1 t + (2\rho_0\rho_2+\rho_1^2)t^2 + (2\rho_0\rho_3+2\rho_1\rho_2)t^3+\ldots\\ &\approx 0.083 + 0.334t + 0.408t^2 + 0.151t^3 + 0.022t^4 + \ldots.\end{aligned}$$

About 33% of the time a large binary matrix has just one eigenvalue and about 40% of the time it has two eigenvalues. The Maple code below simulates the sampling of 1000 random matrices of size 15 over $\mathbf{F}_2$ and finds the distribution of the dimensions of the null space.

```
n:=15:  # size of matrices
num:=1000:  # number of random matrices
A:=array(1..n,1..n):
C:=array(0..n,[seq(0,i=0..n)]):
 # C(k) is the number of matrices with k-dimensional null space
for kk to num do
  for i to n do
   for j to n do
    A[i,j]:=rand(2)():
   od;
  od;
dim := nops(Nullspace(A) mod 2):
C[dim]:=C[dim]+1:
od:
entries(C);
```

In one run there were these results, which agree with the theoretical values for ρ_k.

dim ker	0	1	2	3
proportion	.280	.567	.150	.003

The sample average is 0.876.

Theorem 17 *As $q \to \infty$ the distribution of X (the number of eigenvalues in the base field) approaches a Poisson distribution of mean 1.*

Proof The probability generating function for the Poisson distribution is $e^{-1}\sum_{k\geq 0}\frac{t^k}{k!} = e^{t-1}$. By the Continuity Theorem (see [2, p. 280]) it will suffice to show that $\lim_{q\to\infty} f_X(t) = e^{t-1}$ pointwise for $0 \leq t \leq 1$. Now,

$$\log f_X(t) = \log f_{X_0}(t)^q = q \log f_{X_0}(t) = q \log \sum_{k\geq 0} \rho_k t^k.$$

Recall that $\rho_k = \frac{q^k}{(q-1)^2 \ldots (q^k-1)^2}\rho_0$ and $\rho_0 = \prod_{r\geq 1}\left(1 - \frac{1}{q^r}\right)$. Therefore,

$$\log f_X(t) = q \log \rho_0 + q \log \left(1 + \sum_{k\geq 1} \frac{q^k}{(q-1)^2 \ldots (q^k-1)^2} t^k\right).$$

From Corollary 23 we see that $\lim_{q\to\infty} q \log \rho_0 = -1$. The second term is

$$q \log \left(1 + \frac{q}{(q-1)^2}t + \frac{q^2}{(q-1)^2(q^2-1)^2}t^2 + \ldots\right).$$

Expand using the series for $\log(1+x)$ and note that as $q \to \infty$ the only term that does not go to 0 faster than $1/q$ is $\frac{q}{(q-1)^2}t$. Thus, the limit of the second term is

$$\lim_{q\to\infty} q\frac{q}{(q-1)^2}t = t.$$

Hence $\lim_{q\to\infty} \log f_X(t) = -1 + t$ and $\lim_{q\to\infty} f_X(t) = e^{t-1}$. □

Example 2 Using Maple a simulation of 500 random matrices of size 15 by 15 over the field with 31 elements gave the following distribution of the number of eigenvalues. For comparison a Poisson distribution of mean 1 is shown.

# of eigenvalues	0	1	2	3	4	5
proportion	.350	.372	.190	.058	.026	.004
Poisson	.368	.368	.184	.061	.015	.003

The random variable X counts the number of blocks in the rational canonical form associated to the linear monic polynomials. Equivalently, it counts the sum of the dimensions of the eigenspaces of the eigenvalues in the base field. Next we consider the eigenspaces associated to eigenvalues in extension fields. Let ϕ be a monic irreducible polynomial of degree m. Define the random variable V_ϕ to be the number of parts of the partition λ_ϕ. Thus V_ϕ counts the number of blocks in the rational canonical form associated to ϕ.

Proposition 18 *The asymptotic probability that $V_\phi = k$ is*

$$\hat{\mathrm{P}}(V_\phi = k) = \frac{q^{km}}{(q^m-1)^2 \ldots (q^{km}-1)^2} \prod_{r\geq 1}\left(1 - \frac{1}{q^{rm}}\right).$$

Proof The proof follows from Theorem 7 and Corollary 13. □

Define $V_m = \sum_{\deg \phi = m} V_\phi$. Notice that V_1 is X above. Because the V_ϕ are asymptotically independent, the asymptotic probability generating function

$$f_{V_m}(t) = \prod_{\deg \phi = m} f_{V_\phi}(t),$$

where

$$f_{V_\phi}(t) = \sum_{k=0}^{\infty} \hat{\mathrm{P}}(V_\phi = k) t^k.$$

For all irreducible ϕ of degree m the functions $f_{V_\phi}(t)$ are identical and so

$$f_{V_m}(t) = \left(f_{V_\phi}(t)\right)^{\nu_m},$$

where ϕ is any fixed irreducible monic polynomial of degree m.

Theorem 19 *As $q \to \infty$ the distribution of V_m approaches a Poisson distribution of mean $1/m$.*

Proof We have $\log f_{V_m}(t) = \nu_m \log f_{V_\phi}(t)$. Recall that $\nu_m = q^m/m + O(q^{m/2})$. We can use the proof of Theorem 17 with q^m in place of q to show that

$$\lim_{q \to \infty} q^m \log f_{V_\phi}(t) = t - 1.$$

Easy estimates show that

$$\lim_{q \to \infty} \nu_m \log f_{V_\phi}(t) = \frac{1}{m}(t-1).$$

Hence, as $q \to \infty$, $f_{V_m}(t) \to e^{\frac{1}{m}(t-1)}$, which is the the probability generating function of a Poisson distribution with mean $1/m$. □

4 Other Applications and Examples

In this section we present results due to Stong and Fulman that illustrate the use of the results on asymptotic independence to find some interesting asymptotic probabilities.

Proposition 20 *For $a \in \mathbf{F}_q$ the asymptotic probability that a is not an eigenvalue is $\prod_{r \geq 1} \left(1 - \frac{1}{q^r}\right)$.*

Proof Use Theorem 7 with $\psi(z) = z - a$ and let L the singleton set containing the empty partition. Then $\sum_{\lambda \in L} \frac{1}{c_\psi(\lambda)} = 1$. □

A derangement is a permutation with no fixed points. A linear map from $\mathbf{F}_q^n$ to itself always fixes 0, so we define a **linear derangement** as an invertible linear map that has no non-zero fixed vectors.

Proposition 21 *The asymptotic probability that an invertible linear map is a linear derangement is $\prod_{r \geq 1} \left(1 - \frac{1}{q^r}\right)$.*

Proof A linear map fixes a non-zero vector precisely when it has 1 for an eigenvalue, and the proposition follows from the previous theorem and proposition. □

This probability that an invertible linear map does not fix a non-zero vector is the same as the probability that any linear map does not fix a non-zero vector, which is the same as the probability of being invertible.

Now we consider the natural action of $\mathrm{GL}_n(q)$ on projective space $\mathbf{P}^{n-1}(\mathbf{F}_q)$. Define a **projective derangement** to be an element of $\mathrm{GL}_n(q)$ that acts on $\mathbf{P}^{n-1}(\mathbf{F}_q)$ without fixed points. Since points in $\mathbf{P}^{n-1}(\mathbf{F}_q)$ are lines in $\mathbf{F}_q^n$, the fixed points of α acting on $\mathbf{P}^{n-1}(\mathbf{F}_q)$ are the lines lying in eigenspaces of α.

Proposition 22 *The asymptotic probability that an invertible linear map is a projective derangement is* $\prod_{r\geq 1}\left(1-\frac{1}{q^r}\right)^{q-1}$.

Proof To be a derangement means that there are no eigenvalues in the base field $\mathbf{F}_q$. Thus, the asymptotic probability is $\hat{\mathrm{P}}(\mathcal{E})$, where

$$\mathcal{E} = \bigcap_{a\in\mathbf{F}_q\setminus\{0\}} \mathcal{E}(z-a, L)$$

and L is the singleton containing the empty partition. By the theorem on coprime independence

$$\hat{\mathrm{P}}(\mathcal{E}) = \prod_{a\in\mathbf{F}_q\setminus\{0\}} \hat{\mathrm{P}}(\mathcal{E}(z-a, L))$$

From Proposition 20 $\hat{\mathrm{P}}(\mathcal{E}(z-a,L)) = \prod_{r\geq 1}\left(1-\frac{1}{q^r}\right)$, and so

$$\hat{\mathrm{P}}(\mathcal{E}) = \prod_{r\geq 1}\left(1-\frac{1}{q^r}\right)^{q-1}.$$

□

Recall that the probability that a permutation on n letters is a derangement approaches $1/e$ as n goes to infinity. For projective derangements we have to let the matrix size and the field size go to infinity.

Corollary 23 *The limit as $q\to\infty$ of the asymptotic probability that an invertible linear map is a projective derangement is $1/e$. That is,*

$$\lim_{q\to\infty}\prod_{r\geq 1}\left(1-\frac{1}{q^r}\right)^{q-1} = \frac{1}{e}.$$

Proposition 24 *Let a be algebraic of degree m over $\mathbf{F}_q$. Then the asymptotic probability that a is not an eigenvalue of a square matrix is* $\prod_{r\geq 1}\left(1-\frac{1}{q^{rm}}\right)$.

Proof The event we need is $\mathcal{E}(\psi, L)$ where ψ is the monic irreducible polynomial of degree m having a as a root and L is the singleton containing the empty partition. By Theorem 7

$$\hat{\mathrm{P}}(\mathcal{E}(\psi, L)) = \prod_{r\geq 1}\left(1-\frac{1}{q^{r\deg\psi}}\right)\sum_{\lambda\in L}\frac{1}{c_\psi(\lambda)}.$$

Now $\sum_{\lambda\in L}\frac{1}{c_\psi(\lambda)} = 1$ and $\deg\psi = m$. □

Proposition 25 *Let ϕ be a monic, irreducible polynomial of degree m. Then the asymptotic probability that ϕ is a factor of the characteristic polynomial of a square matrix is* $1 - \prod_{r\geq 1}\left(1 - \frac{1}{q^{rm}}\right)$.

Proof This is the complementary probability to that of the previous proposition. □

Remarks Contrast this result with the probability that ϕ divides a random monic polynomial of degree n as $n \to \infty$. For n larger than $m = \deg \phi$ this probability is $1/q^m$. In this sense the characteristic polynomial is not distributed uniformly across the monic polynomials. On the other hand, Hansen and Schmutz [5] have shown that if we disregard the small factors, then the characteristic polynomial of a random matrix is random, but the meaning of "small" is relative to the size of the matrix, growing proportionally to the logarithm of the size of the matrix.

We define $\alpha \in \mathrm{M}_n(q)$ to be **semi-simple** if the associated $\mathbf{F}_q[z]$-module is semi-simple, which means that it is isomorphic to a direct sum

$$\bigoplus_i \mathbf{F}_q[z]/(\phi_i)$$

where the ϕ_i are irreducible but not necessarily distinct. This property is also equivalent to being diagonalizable over the algebraic closure of $\mathbf{F}_q$. In terms of the conjugacy class data, α being semi-simple is equivalent to $\lambda_\phi(\alpha)$ being the empty partition or consisting only of 1's for all monic irreducible ϕ.

When the associated module is cyclic we say that α is **cyclic**. In that case the associated $\mathbf{F}_q[z]$-module is isomorphic to

$$\bigoplus_i \mathbf{F}_q[z]/(\phi_i^{e_i})$$

where the ϕ_i are distinct and irreducible. Equivalently, the minimal polynomial is the same as the characteristic polynomial of α. Also equivalent to α being cyclic is that it is **regular** when considered as an element of $\mathrm{GL}_n(\bar{\mathbf{F}}_q)$, where an element of an algebraic group is regular if its centralizer has minimal dimension. In terms of the conjugacy class data, α being cyclic is equivalent to $\lambda_\phi(\alpha)$ being empty or consisting of just one part for all ϕ.

Proposition 26 *The asymptotic probability that a matrix is semi-simple and cyclic (equivalently, that the characteristic polynomial is square-free) is*

$$\prod_{r\geq 1}\left(1 - \frac{1}{q^r}\right).$$

Proof Let $L = \{\emptyset, 1\}$ be the subset containing just the empty partition and the unique partition of 1. The set of matrices that are both semi-simple and cyclic is the intersection of $\mathcal{E}(\phi, L)$ as ϕ ranges over the monic irreducible polynomials. Now $\sum_{\lambda\in L}\frac{1}{c_\phi(\lambda)} = 1 + \frac{1}{q^{\deg\phi}-1}$ and so

$$\begin{aligned}
\hat{\mathrm{P}}(\mathcal{E}(\phi, L)) &= \prod_{r\geq 1}\left(1 - \frac{1}{q^{r\deg\phi}}\right)\left(1 + \frac{1}{q^{\deg\phi} - 1}\right) \\
&= \prod_{r\geq 2}\left(1 - \frac{1}{q^{r\deg\phi}}\right)\left(1 - \frac{1}{q^{\deg\phi}}\right)\left(1 + \frac{1}{q^{\deg\phi} - 1}\right) \\
&= \prod_{r\geq 2}\left(1 - \frac{1}{q^{r\deg\phi}}\right).
\end{aligned}$$

It follows that

$$\begin{aligned}
\hat{\mathrm{P}}(\text{semi-simple and cyclic}) &= \prod_{\phi} \hat{\mathrm{P}}(\mathcal{E}(\phi, L)) \\
&= \prod_{\phi} \prod_{r \geq 2} \left(1 - \frac{1}{q^{r \deg \phi}}\right) \\
&= \prod_{r \geq 2} \prod_{\phi} \left(1 - \frac{1}{q^{r \deg \phi}}\right) \\
&= \prod_{r \geq 2} \left(1 - \frac{1}{q^{r-1}}\right) \\
&= \prod_{r \geq 1} \left(1 - \frac{1}{q^{r}}\right).
\end{aligned}$$

Here Lemma 5 is used to go from the third to the fourth line. □

Consider the next proposition in light of the fact that the asymptotic probability is $1 - \frac{1}{q}$ that a random polynomial is square-free.

Proposition 27 *The asymptotic probability that an invertible matrix is semi-simple and cyclic (equivalently, that the characteristic polynomial is square-free) is* $1 - \frac{1}{q}$.

Proof Let $L = \{\emptyset, 1\}$ as in the previous proposition. By Theorem 10 the asymptotic probability that an invertible matrix is semi-simple and cyclic is

$$\begin{aligned}
\hat{\mathrm{P}}(\text{semi-simple and cyclic} \,|\, \text{invertible}) &= \hat{\mathrm{P}} \left(\bigcap_{\phi \neq z} \mathcal{E}(\phi, L) \right) \\
&= \prod_{\phi \neq z} \hat{\mathrm{P}}(\mathcal{E}(\phi, L)) \\
&= \frac{\prod_{\phi} \hat{\mathrm{P}}(\mathcal{E}(\phi, L))}{\hat{\mathrm{P}}(\mathcal{E}(z, L))} \\
&= \frac{\hat{\mathrm{P}}(\text{semi-simple and cyclic})}{\prod_{r \geq 1} \left(1 - \frac{1}{q^r}\right) \left(1 + \frac{1}{q-1}\right)} \\
&= \frac{1}{1 + \frac{1}{q-1}} \\
&= 1 - \frac{1}{q}.
\end{aligned}$$

□

Remarks Fulman also finds the asymptotic probabilities that a matrix is semi-simple, that an invertible matrix is semi-simple, that a matrix is cyclic, and that an invertible matrix is cyclic. The calculation of the probability that a matrix is semi-simple uses Gordon's generalization of the Rogers-Ramanujan identities. There is earlier related work of Neumann and Praeger [9] on these probabilities.

Notice that the probabilites of being cyclic and semi-simple go to 1 as $q \to \infty$, which is to be expected since these properties are generic for the Zariski topology in the algebraic varieties of $n \times n$ matrices and invertible $n \times n$ matrices over the algebraic closure $\bar{\mathbf{F}}_q$.

References

[1] G. E. Andrews, *The Theory of Partitions*, Addison-Wesley, Reading, Mass., 1976.

[2] W. Feller, *An Introduction to Probability Theory and Its Applications. Vol. I.*, John Wiley & Sons, Inc., New York-London-Sydney, second ed., 1968.

[3] N. J. Fine and I. N. Herstein, *On the number of nilpotent matrices with coefficients in a finite field*, Illinois J. Math., 5 (1958), pp. 330–333.

[4] J. Fulman, *Cycle indices for the finite classical groups*, J. Group Theory, 2 (1999), pp. 251–289.

[5] J. C. Hansen and E. Schmutz, *How random is the characteristic polynomial of a random matrix*, Math. Proc. Camb. Phil. Soc., 114 (1993), pp. 507–515.

[6] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Univ. Press, New York, fifth ed., 1979.

[7] J. Kung, *The cycle structure of a linear transformation over a finite field*, Linear Algebra Appl., 36 (1981), pp. 141–155.

[8] S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., third ed., 1993.

[9] P. M. Neumann and C. E. Praeger, *Cyclic matrices over finite fields*, J. London Math. Soc., 52 (1995), pp. 263–284.

[10] R. Stong, *Some asymptotic results on finite vector spaces*, Adv. Appl. Math., 9 (1988), pp. 167–199.

[11] H. S. Wilf, *Generatingfunctionology*, Academic Press, second ed., 1994.