Math. Proc. Camb. Phil. Soc. (1993), 114, 507
Printed in Great Britain

How random is the characteristic polynomial of a random matrix?

BY JENNIE C. HANSEN†
Actuarial Mathematics and Statistics Department, Heriot-Watt University, Edinburgh, Scotland

AND ERIC SCHMUTZ†
Mathematics and Computer Science Department, Drexel University, Philadelphia, PA 19104, *USA*

(*Received* 26 *October* 1992; *revised* 6 *January* 1993)

Abstract

Every monic, degree n polynomial in $\mathbf{F}_q[x]$ is the characteristic polynomial of at least one $n \times n$ matrix (with entries in the finite field $\mathbf{F}_q$), but they do not appear with equal frequency. There is no a priori reason that the characteristic polynomial of a typical matrix should resemble a typical monic degree n polynomial. Nevertheless, we prove a precise version of the following heuristic statement: 'Excepting its small factors, the characteristic polynomial of a random matrix is random.'

1. *Introduction*

Is the characteristic polynomial of a random matrix random? More precisely, let U_n be the set of monic degree n polynomials in $\mathbf{F}_q[x]$, and let $Q_n^{(1)}$ be the uniform probability measure on U_n. Let $GL(n, q)$ denote the set of $n \times n$ invertible matrices with entries in $\mathbf{F}_q$. Define $Q_n^{(2)}$ on U_n by

$$Q_n^{(2)}(\{f\}) := \frac{1}{|GL(n,q)|}|\{A \in GL(n,q) : f \text{ is the characteristic polynomial of } A\}|.$$

Are $Q_n^{(1)}$ and $Q_n^{(2)}$ close in any reasonable sense?

In one sense, the answer is certainly no. For example, if $\mathscr{P}_n$ is the set of monic degree n polynomials in $\mathbf{F}_q[x]$ that have a non-zero constant term, then

$$Q_n^{(1)}(\mathscr{P}_n) = 1 - 1/q.$$

On the other hand,

$$Q_n^{(2)}(\mathscr{P}_n) = 1.$$

Nevertheless, in many ways the characteristic polynomial of a random invertible matrix does resemble a typical monic polynomial. This vague statement will be made precise, and then proved. Since random polynomials are well understood (see, for example, [1]), this could simplify the proofs of many theorems about random matrices. Thus theorems about the characteristic polynomials of random matrices are reducible to theorems about random polynomials.

To state our main result, we need some notation. A monic polynomial in $\mathbf{F}_q[x]$ will be called irreducible if it cannot be factored as a product of two monic polynomials in $\mathbf{F}_q[x]$ of smaller degree. For $f \in \mathbf{F}_q[x]$, let $a_i = a_i(f)$ be the number of monic irreducible factors of degree i that f has, counted with multiplicity. Given $l = l(n)$, let $\mathbf{A}_n = (a_{l-1}, a_{l-2}, \ldots, a_{n-1}, a_n)$. Our main result is:

THEOREM 1. *There are positive constants c_1 and c_2 such that, for all positive integers l and n that satisfy $c_1 \log n \leqslant l \leqslant n$, and for all $B \subset N^{n-l}$,*

$$|Q_n^{(1)}(\mathbf{A}_n \in B) - Q_n^{(2)}(\mathbf{A}_n \in B)| < c_2/l.$$

Some applications are given in Section 6.

2. *Preliminaries*

For the reader's convenience, we provide the statements of several theorems that are used in this paper. The first of these is a key identity of Stong. To state it, we need some definitions and some familiarity with linear algebra. Two matrices in $GL(n, q)$ are similar if and only if they have the same rational canonical form. To specify the rational canonical form, (*a*) one must list the monic irreducible polynomials that divide the characteristic polynomial, and (*b*) for each of these irreducible polynomials, one must specify an integer partition. If p is a monic irreducible polynomial, and if λ is an integer partition, define $I_{p,\lambda}(A)$ to be 1 if p appears, associated with the partition λ, in the rational canonical form for A. Otherwise, define $I_{p,\lambda}(A)$ to be 0. Finally, for any prime number p, and for any positive integers j and a, define

$$[p^a]_j := \prod_{i=0}^{j-1} (p^{aj} - p^{ai}).$$

It is well known that $|GL(n, q)| = [q]_n$. The vector space cycle index is a polynomial in the variables $x_{p,\lambda}$ that is defined by

$$Z_n(q, X) := \frac{1}{[q_n]} \sum_A \prod_{p,\lambda} x_{p,\lambda}^{J_{p,\lambda}(A)},$$

where the product is over all monic irreducible polynomials in $F_q[x]$, with the exception of $p(z) = z$. One can regard $Z_n(q, X)$ as a monstrous probability generating function: there is one monomial for each similarity class (orbit), and the coefficient of each term is the proportion of matrices in $GL(n, q)$ that are in that similarity class.

Now consider the formal power series

$$G(u, q, X) := 1 + \sum_{n=1}^{\infty} Z_n(q, X)\, u^n.$$

If p is a polynomial, let $|p|$ be its degree. If $\lambda = \{1^{(m_1)}, 2^{(m_2)}, \ldots, n^{(m_n)}\}$ is a partition of $j = |\lambda|$ with m_i parts of size i $(i = 1, 2, \ldots, n)$, let

$$d_i = m_1 + 2m_2 + \ldots + (i-1)\, m_{i-1} + i m_i + i m_{i+1} + \ldots + i m_j.$$

Then we have the following formal power series identity of Kung and Stong [7, 13].

THEOREM 2 (Stong).

$$G(u,q,X)=\prod_{p}\left[1+\sum_{\lambda}\frac{x_{p,\lambda}\,u^{|\lambda|\cdot|p|}}{c_{|p|}(\lambda)}\right],$$

where p runs over all monic irreducible polynomials (except $p(z)=z$), and

$$c_m(\lambda):=\prod_{i}\prod_{k=1}^{m_i}(q^{md_i}-q^{m(d_i-k)}).$$

Next, for $d>1$, let $\epsilon(d)$ denote the number of monic irreducible polynomials of degree d. Set $\epsilon(1):=q-1$. We have the following well known inequalities. (See, for example Berlekamp[2], p. 80.)

LEMMA 3. *For all integers $d>1$,*

$$\frac{q^d}{d}(1-q^{1-d/2})\leqslant\epsilon(d)\leqslant\frac{q^d}{d}.$$

3. *Largest irreducible factor*

Let $\mathbf{L}_r(f)$ denote the rth largest of the degrees of f's irreducible factors. More precisely, if f factors in $\mathbf{F}_q[x]$ as

$$f=\prod_{i=1}^{\nu}p_i,$$

where the p_is are (not necessarily distinct) monic irreducible polynomials, and if $|p_i|\geqslant|p_j|$ for all $i\leqslant j$, then define $\mathbf{L}_r(f):=|p_r|$. Then, for any positive integer l, we have

$$\begin{aligned}Q_n^{(1)}(\mathbf{L}_1\leqslant l)&=[u^n]\left(1-\frac{u}{q}\right)^{-q}\prod_{d=2}^{l}\left(1-\frac{u^d}{q^d}\right)^{-\epsilon(d)}\\&=[u^n]\frac{1}{1-u}\prod_{d=l+1}^{\infty}\left(1-\frac{u^d}{q^d}\right)^{\epsilon(d)}.\end{aligned}\tag{1}$$

As usual, $[u^n]$ means 'the coefficient of u^n in...'. See Wilf[14] for an excellent introduction to generating functions.) To get a corresponding expression for monic polynomials make the following substitution in the vector space cycle index:

$$x_{p,\lambda}:=\begin{cases}1, & \text{if } |p|\leqslant l,\\ 0, & \text{otherwise.}\end{cases}$$

Let

$$\Phi_d=\Phi_d(u)=1+\sum_{\lambda}\frac{u^{|\lambda|d}}{c_d(\lambda)},$$

where the sum is over all integer partitions. (Recall that $|\lambda|$ is the integer that λ partitions.) In this way we get

$$Q_n^{(2)}(\mathbf{L}_1\leqslant l)=[u^n]\prod_{d=1}^{l}\Phi_d^{\epsilon(d)}=[u^n]\frac{1}{1-u}\prod_{d=l+1}^{\infty}\Phi_d^{-\epsilon(d)}.\tag{2}$$

The probabilities in (1) and (2) could be estimated for various ranges of l using

contour integration ([11]). Our goal here is more modest: we prove that two probabilities are approximately the same without actually determining this probability.

PROPOSITION 4. *There is a constant c_3 such that, for all positive integers n and l,*

$$|Q_n^{(1)}(\mathbf{L}_1 \leqslant l) - Q_n^{(2)}(\mathbf{L}_1 \leqslant l)| \leqslant \frac{c_3 l}{q^l}.$$

Proof. Let

$$D_l(u) = 1 - \prod_{m=l+1}^{\infty} \left(\Phi_m \cdot \left(1 - \left(\frac{u^m}{q^m}\right)\right)\right)^{-\epsilon(m)}.$$

Then from (1) and (2) we have

$$Q_n^{(1)}(\mathbf{L}_1 \leqslant l) - Q_n^{(2)}(\mathbf{L}_1 \leqslant l) = [u^n] \frac{1}{1-u} \prod_{m=l+1}^{\infty} \left(1 - \frac{u^m}{q^m}\right)^{\epsilon(m)} \cdot D_l(u)$$

$$= [u^n] D_l(u) \left(1 - \frac{u}{q}\right)^{-q} \prod_{d=2}^{l} \left(1 - \frac{u^d}{q^d}\right)^{-\epsilon(d)}. \tag{3}$$

Until now we have regarded our generating functions as formal power series. In order to regard them as analytic functions, we need more information about the Φ_m s. First we record the following identities from Stong [13].

$$\Phi_m(u) = 1 + \sum_{j=1}^{\infty} \frac{q^{mj(j-1)} u^{mj}}{[q^m]_j}$$

$$\frac{1}{\Phi_m} = 1 + \sum_{j \geqslant 1} \frac{(-1)^j u^{mj}}{(q^{mj}-1)(q^{m(j-1)}-1)\dots(q^m-1)}. \tag{4}$$

There is a constant m_0 such that, for all $m \geqslant m_0$,

$$\sum_{j=1}^{\infty} \frac{q^{mj(j-1)}}{]q^m]_j} < 1.$$

We may and do assume that the constant c_1 in Theorem 1 is larger than m_0. Hence, for all $m \geqslant l$, and for $|u| \leqslant 1$, one has $0 < |\Phi_m(u) - 1| < 1$. Since $\phi_m \neq 0$, we can define

$$\Delta_m(u) = \epsilon(m) \log \Phi_m + \epsilon(m) \log\left(1 - \frac{u^m}{q^m}\right).$$

Observe that, uniformly for $|u| \leqslant 1$, we have

$$\Delta_m(u) = \epsilon(m)\left\{\left(\frac{u^m}{q^m - 1} + O\left(\frac{1}{q^{2m}}\right)\right) + \left(\frac{-u^m}{q^m} + O\left(\frac{1}{q^{2m}}\right)\right)\right\}.$$

Invoking Lemma 3, we get $\Delta_m(u) = O(q^{-m})$ uniformly for $|u| \leqslant 1$. Hence, for $|u| \leqslant 1$. we have

$$D_l(u) = 1 - \exp\left[\sum_{m=l+1}^{\infty} \Delta_m(u)\right] = O(q^{-l}).$$

Since $$Q_n^{(1)}(\mathbf{L}_1 \leqslant l) - Q_n^{(2)}(\mathbf{L}_1 \leqslant l) = [u^n] D_l(u) \left(1 - \frac{u}{q}\right)^{-q} \prod_{d=2}^{l} \left(1 - \frac{u^d}{q^d}\right)^{-\epsilon(d)},$$

where $D_l(u) = O(q^{-l})$ uniformly for $|u| \leqslant 1$, we can estimate

$$|Q_n^{(1)}(\mathbf{L}_1 \leqslant l) - Q_n^{(2)}(\mathbf{L}_1 \leqslant l)| \leqslant \frac{c}{q^l} \cdot \max_{|u| \leqslant 1} \left| \left(1-\frac{u}{q}\right)^{-q} \prod_{d=2}^{l} \left(1-\frac{u^d}{q^d}\right)^{-\epsilon(d)} \right| = O\left(\frac{l}{q^l}\right). \quad \blacksquare$$

4. *Exceptional sets*

In this section we prove three technical lemmas. These lemmas will enable us to disregard various exceptional sets whose contribution is negligible.

LEMMA 5. *For $A \in GL(n,q)$, let $\mathbf{R}_n(A,l)$ be the number distinct monic irreducible polynomials that*

(i) *have degree larger than l, and*

(ii) *have square dividing the characteristic polynomial of A.*

Then the number of matrices A in $GL(n,q)$ for which $\mathbf{R}_n(A,l) > 0$ is at most $c_4/lq^l|GL(n,q)|$, where c_4 is a positive constant that is independent of l and n.

Proof. Let $F(u,X)$ be the generating function that is obtained from the cycle index G by setting

$$x_{p,\lambda} = \begin{cases} 1, & \text{if } |\lambda| = 1 \text{ or } |p| \leqslant l, \\ X, & \text{otherwise.} \end{cases}$$

Then $F(u,1) = 1/(1-u)$. If $E_n^{(i)}$ denotes expectation with respect to $Q_n^{(i)}$, then

$$E_n^{(2)}(\mathbf{R}_n) = [u^n] \frac{\partial F}{\partial X}\bigg|_{X=1} = [u^n] \frac{1}{1-u} \sum_{m>l} \frac{\epsilon(m)}{\Phi_m(u)} \left(\sum_{j \geqslant 2} \frac{q^{mj(j-1)} u^{mj}}{[q^m]_j} \right).$$

By (4), this is at most

$$[u^n] \frac{1}{1-u} \left\{ \sum_{m>l} \epsilon(m) M(u) \left(\sum_{j \geqslant 2} \frac{q^{mj(j-1)} u^{mj}}{[q^m]_j} \right) \right\},$$

where

$$M(u) := 1 + \sum_{j \geqslant 1} \frac{u^{mj}}{(q^{mj}-1)(q^{m(j-1)}-1)\dots(q^m-1)}.$$

Since the function inside the large braces has non-negative coefficients, we have

$$E_n^{(2)}(\mathbf{R}_n) \leqslant \sum_{m>l} \epsilon(m) M(1) \left(\sum_{j \geqslant 2} \frac{q^{mj(j-1)}}{[q^m]_j} \right) \leqslant \sum_{m>l} \frac{q^m}{m} O\left(\frac{1}{q^{2m}}\right) = O\left(\frac{1}{lq^l}\right). \quad \blacksquare$$

Recall that $\alpha_d(f)$ is the number of irreducible factors of degree d, counted with multiplicity, that f has. We have

LEMMA 6. *At least $(1+O(1/l))|GL(n,q)|$ matrices in $GL(n,q)$ have the property that, for all $d > l$, $\alpha_d \leqslant 1$.*

Proof. Let $\mathbf{X}_n(A)$ be the number of pairs of distinct monic irreducible polynomials that divide the characteristic polynomial of A and have a common degree greater than l, i.e.

$$\mathbf{X}_n(A) = \sum_{d>l} \sum_{\lambda_1,\lambda_2} \sum_{\substack{p_1 \neq p_2 \\ \deg p_1 = \deg p_2 = d}} I_{p_1,\lambda_1} I_{p_2,\lambda_2}.$$

By Lemma 5, it suffices to show that $\mathbf{X}_n(A) = 0$ for all but $O(|q|_n/l)$ matrices in $GL(n, q)$. Suppose that p_1 and p_2 are distinct irreducibles of degree m, and suppose that λ_1 and λ_2 are integer partitions. Then, as in Stong[13], p. 176, one can use Theorem 2 to get

$$E_n(I_{p_1,\lambda_1} I_{p_2,\lambda_2}) = [u^n] \frac{u^{|\lambda_1|m+|\lambda_2|m}}{(1-u)\, c_m(\lambda_1)\, c_m(\lambda_2)\, \Phi_m^2}.$$

Hence
$$E_n(\mathbf{X}_n) \leqslant \sum_{m>l(n)} \epsilon(m)^2 \sum_{\lambda_1,\lambda_2} [u^n] \frac{u^{|\lambda_1|m+|\lambda_2|m}}{(1-u)\, c_m(\lambda_1)\, c_m(\lambda_2)\, \Phi_m^2}.$$

To estimate this, note that, for any m we have

$$\sum_{\lambda_1,\lambda_2} [u^n] \frac{u^{|\lambda_1|m+|\lambda_2|m}}{(1-u)\, c_m(\lambda_1)\, c_m(\lambda_2)\, \Phi_m^2} = [u^n] \frac{1}{(1-u)} \frac{(\Phi_m(u)-1)^2}{\Phi_m^2(u)}$$

$$\leqslant [u^n] \frac{1}{(1-u)} (\Phi_m(u)-1)^2 (M(u))^2.$$

Observe that $(\Phi_m(1)-1)$ is $O(q^{-m})$ and that $M(1)$ is bounded by a constant. Combining these estimates with Lemma 3 we get

$$E_n(\mathbf{X}_n) \leqslant \sum_{m>l(n)} O\left(\frac{1}{m^2}\right) = O\left(\frac{1}{l}\right). \quad \blacksquare$$

LEMMA 7. $Q_n^{(1)}(\alpha_d \leqslant 1 \text{ for all } d > l) = 1 + O(1/l)$.

Proof. For $f \in U_n$, let $\mathbf{P}_n(f)$ be the number of pairs of (not necessarily distinct) irreducible monic polynomials that divide f and have a common degree larger than l. It suffices to show that $Q_n^{(1)}(\mathbf{P}_n > 0) = O(1/l)$. But

$$Q_n^{(1)}(\mathbf{P}_n > 0) \leqslant E_n^{(1)}(\mathbf{P}_n) = \sum_{(p_1,p_2)} Q_n^{(1)}(p_1 p_2 \text{ divides } f).$$

Here the sum is over all pairs of monic irreducible polynomials that have a common degree that is larger than l. Evaluating the inside probability explicitly, we get

$$Q_n^{(1)}(\mathbf{P}_n > 0) \leqslant \sum_{d>l} \epsilon(d)^2 \frac{q^{n-2d}}{q^n} = O\left(\frac{1}{l}\right). \quad \blacksquare$$

5. *Approximations*

Suppose that $j_1, j_2, \ldots, j_r$ are positive integers with $j_1 > j_2 > \ldots > j_r > l$, and suppose $j_1 + j_2 + \ldots + j_r = m \leqslant n$. How many polynomials f have a factorization $f = \prod_{i=1}^{r} p_i$, such that $|p_i| = j_i$, $i = 1, 2, \ldots, r$, and such that $|p_i| \leqslant l$ for all $i > r$? For each $i \leqslant r$, there are $\epsilon(j_i)$ ways to choose the irreducible of degree j_i. Then the rest of f, namely $\prod_{i=r+1}^{r} p_i$, can be any polynomial of degree $n-m$ whose irreducible factors all have degrees less than or equal to l. Hence there are exactly $q^{n-m} Q_{n-m}^{(1)}(\mathbf{L}_1 \leqslant l)$ ways to choose 'the rest of f'. Thus

$$Q_n^{(1)}(\mathbf{L}_1 = j_1, \mathbf{L}_2 = j_2, \ldots, \mathbf{L}_r = j_r, \mathbf{L}_{r+1} \leqslant l) = \frac{\epsilon(j_1)\,\epsilon(j_2)\ldots\epsilon(j_r)}{q^m} Q_{n-m}^{(1)}(\mathbf{L}_1 \leqslant l).$$

Finally, invoking Lemma 3 and the fact that

$$\sum_{i=1}^{r} \frac{1}{q^{j_i/2}} < \sum_{d \geqslant l} \frac{1}{q^{d/2}} = O\left(\frac{1}{q^{l/2}}\right),$$

we get

$$Q_n^{(1)}(\mathbf{L}_1 = j_1, \mathbf{L}_2 = j_2, \ldots, \mathbf{L}_r = j_r, \mathbf{L}_{r+1} \leqslant l) = \frac{1}{j_1 j_2 \cdots j_r} Q_{n-m}^{(1)}(\mathbf{L}_1 \leqslant l)\left(1 + O\left(\frac{1}{q^{l/2}}\right)\right). \quad (5)$$

Next we get a similar expression for matrices. How many matrices $T \in GL(n,q)$ have a characteristic polynomial $f(x)$ with a factorization $f = \prod_{i=1}^{\nu} p_i$, such that $|p_i| = j_i$, $i = 1, 2, \ldots, r$, and such that $|p_i| \leqslant l$ for all $i > r$? If we fix a basis, and regard matrices as linear transformations, then the kernels of $p_i(T)$, $(i = 1, 2, \ldots, r)$ and of $\prod_{i=r+1}^{\nu} p_i(T)$ are T-invariant subspaces of F_q^n, whose respective dimensions are $j_1, j_2, \ldots, j_r$, and $(n-m)$. (Recall $m = j_1 + j_2 + \ldots + j_r$.) To specify T, we can (a) first specify these $r+1$ subspaces, and then (b) specify the restrictions of T to each of these subspaces. How many nonsingular linear transformations T have the property that (i) the r largest irreducible factors of its characteristic polynomial have degrees $j_1, \ldots, j_r$, and (ii) all others have degree less than or equal to l? We claim that this number is

$$\left(\frac{[q]_n}{[q]_{j_1}[q]_{j_2}\cdots[q]_{j_r}[q]_{n-m}}\right)\epsilon(j_1)\epsilon(j_2)\ldots\epsilon(j_r)\prod_{i=1}^{r}\frac{[q]_{j_i}}{(q^{j_i}-1)}\cdot\Psi(n-m,l), \quad (6)$$

where $\Psi(k,s)$ denotes the number of matrices in $GL(k,q)$ whose characteristic polynomial's irreducible factors all have degree less than or equal to s. To see this we note:

(a) There are

$$\frac{[q]_n}{[q]_{j_1}[q]_{j_2}\cdots[q]_{j_r}[q]_{n-m}}$$

ways to decompose F_q^n as a direct sum of a j_1-dimensional subspace K_1, a j_2-dimensional subspace $K_2, \ldots,$ a j_r dimensional subspace K_r, and an $(n-m)$ dimensional space K_{r+1};

(b) There are $\epsilon(j_1)\epsilon(j_2)\ldots\epsilon(j_r)$ ways to choose one irreducible polynomial of degree j_i for each $i \leqslant r$;

(c) Given K_i and p_{j_i}, there are

$$\frac{[q]_{j_i}}{(q^{j_i}-1)}$$

choices for the restriction of T to K_i; this is the number of linear transformations on K_i whose characteristic polynomial is p_i (see Gerstenhaber [3] for a proof of this);

(d) Given K_{r+1}, there are $\Psi(n-m,l)$ choices for the restriction of T to K_{r+1}.

As before, we use Lemma 3 to get

$$Q_n^{(1)}(\mathbf{L}_1 = j_1, \mathbf{L}_2 = j_2, \ldots, \mathbf{L}_r = j_r, \mathbf{L}_{r+1} \leqslant l) = \prod_{i=1}^{r}\frac{\epsilon(j_i)}{(q^{j_i}-1)} Q_{n-m}^{(2)}(\mathbf{L}_1 \leqslant l)$$

$$= \frac{1}{j_1 j_2 \cdots j_r} Q_{n-m}^{(2)}(\mathbf{L}_1 \leqslant l)\left(1 + O\left(\frac{1}{q^{l/2}}\right)\right). \quad (7)$$

Now we are in a position to prove Theorem 1.

Let $B \subset N^{n-l}$ be given. Let B_1 be the subset of B consisting of those vectors $(a_{l+1}, a_{l+2}, \ldots, a_{n-1}, a_n)$ in N^{n-l} that have the property that each a_i is either 0 or 1. By Lemma 7. we have $Q_n^{(1)}(B-B_1) = O(1/l)$. By Lemma 6, $Q_n^{(2)}(B-B_1) = O(1/l)$. It therefore suffices to prove the following inequality:

$$|Q_n^{(1)}(\mathbf{A}_n \in B_1) - Q_n^{(2)}(\mathbf{A}_n \in B_1)| < \frac{c_5}{l}.$$

Suppose $(a_{l+1}, a_{l+2}, \ldots, a_{n-1}, a_n) \in B_1$ and $\sum_{i=l+1}^{n} a_i = r$. Let $j_1 = \max\{k: a_k > 0\}$ be the largest order of a positive a_k. Similarly let $j_2 = \max\{k: j_1 > k \text{ and } a_k > 0\}$ be the second largest, and so on. Then

$$Q_n^{(1)}((\mathbf{A}_n = (a_{l+1}, a_{l+2}, \ldots, a_{n-1}, a_n)) = Q_n^{(1)}(\mathbf{L}_1 = j_1, \mathbf{L}_2 = j_2, \ldots, \mathbf{L}_r = j_r, \mathbf{L}_{r+1} \leqslant l)$$
$$= \frac{1}{j_1 j_2 \cdots j_r} Q_{n-m}^{(1)}(\mathbf{L}_1 \leqslant l)\left(1 + O\left(\frac{1}{q^{l/2}}\right)\right).$$

By Proposition 4, this is

$$\frac{1}{j_1 j_2 \cdots j_r}\left\{Q_{n-m}^{(2)}(\mathbf{L}_1 \leqslant l) + O\left(\frac{l}{q^l}\right)\right\}\left(1 + O\left(\frac{1}{q^{l/2}}\right)\right).$$

By (7), this is

$$Q_n^{(2)}(\mathbf{L}_1 = j_1, \mathbf{L}_2 = j_2, \ldots, \mathbf{L}_r = j_r, \mathbf{L}_{r+1} \leqslant l)\left(1 + O\left(\frac{1}{q^{l/2}}\right)\right) + \frac{1}{j_1 j_2 \cdots j_r} O\left(\frac{l}{q^l}\right).$$

Because the constants implicit in our $O(\cdot)$ expressions can be chosen uniformly with respect to $(a_{l+1}, a_{l+2}, \ldots, a_{n-1}, a_n)$, we can sum over all choices of $(a_{l+1}, a_{l+2}, \ldots, a_{n-1}, a_n) \in B_1$ to get

$$Q_n^{(1)}(\mathbf{A}_n \in B_1) = Q_n^{(2)}(\mathbf{A}_n \in B_1)\left(1 + O\left(\frac{1}{q^{l/2}}\right)\right) + O\left(\frac{l}{q^l}\right) \sum_{\langle j_i \rangle} \frac{1}{j_1 j_2 \cdots}.$$

To deal with the last term, we invoke the following theorem of Lehmer [8]:

$$[u^n] \frac{1}{1-u} \prod_{j=1}^{\infty}\left(1 + \frac{u^j}{j}\right) = O(n).$$

Thus $Q_n^{(1)}(\mathbf{A}_n \in B_1) = Q_n^{(2)}(\mathbf{A}_n \in B_1) + O\left(\frac{1}{q^{l/2}} + \frac{nl}{q^l}\right) = Q_n^{(2)}(\mathbf{A}_n \in B_1) + O\left(\frac{1}{l}\right)$. ∎

6. *Applications and conclusions*

The identity of Kung and Stong has made it possible to prove many interesting results about the random matrices. Unfortunately, calculations with the cycle index tend to be quite daunting. We hope our theorem will make most of these calculations unnecessary. Below are several new and old theorems that can be quickly proved using the results in this paper.

Application 1: *Order statistics.* As before, let $\mathbf{L}_r(f)$ denote the rth largest irreducible factor's degree. (If r is larger than the number of irreducible factors, then let

$\mathbf{L}_r(f) = 0$.) Let $\Lambda_n = \langle \mathbf{L}_r/n \rangle_{r=1}^{\infty}$. It is known [6] that $Q_n^{(1)} \circ \Lambda_n^{-1}$ converges weakly to the Poisson–Dirichlet distribution on the (infinite dimensional) unit simplex. One immediate consequence of Theorem 1 is that $Q_n^{(2)} \circ \Lambda_n^{-1}$ does too.

Application 2: *Splitting field degree.* For $A \in GL(n,q)$, let $\mathbf{D}_n(A)$ be the degree of the splitting field of A's characteristic polynomial $\mathrm{char}(A)$, i.e. the least integer d such that $\mathrm{char}(A)$ has all its roots in $\mathbf{F}_{q^d}$. Combining the results of Nicolas [9, 10] with our theorem, one can quickly prove that

$$\frac{\log \mathbf{D}_n - \frac{1}{2}\log^2 n}{\sqrt{(\frac{1}{3}\log^3 n)}}$$

converges in distribution to a standard normal distribution.

Application 3: *Matrix orders.* For $f \in \mathcal{U}_n$, let $\mathbf{T}_n(f)$ be order of f. A rough version of the first theorem in [12] is that $\mathbf{T}_n(f) = q^{n-(\log n)^{2+o(1)}}$ for almost every f. Then, using the results in this paper, it is proved that almost every element of the general linear group $GL(n,q)$ has order $q^{n-(\log n)^{2+o(1)}}$.

Application 4: *Brownian motion.* For any $f \in U_n$, let $\mathbf{X}_n^{(1)}(t,f)$ be the number of monic irreducible factors of degree $\leqslant n^t$. For any $A \in GL(n,q)$, let $\mathbf{X}_n^{(2)}(t,A)$ be the number of monic irreducible factors of degree $\leqslant n^t$ that the characteristic polynomial of A has. Finally, let

$$\mathbf{Y}_n^{(i)}(t,A) = \frac{\mathbf{X}_n^{(i)}(t,A) - t\log n}{\sqrt{\log n}}$$

($i = 1, 2$). It is known [1, 4, 5] that, for $i = 1$ or 2, $\mathbf{Y}_n^{(i)}$ converges, in Skorohod's topology, to the standard Brownian motion process. The proofs are not easy. However, by using the results in this paper, it should be relatively easy to prove that these two theorems are equivalent; either one implies the other.

REFERENCES

[1] R. Arratia, A. D. Barbour and S. Tavaré. *On Random Polynomials over finite fields* (preprint).

[2] E. Berlekamp. *Algebraic Coding Theory* (2nd ed.). Aegean Park Press (1984).

[3] M. Gerstenhaber. On the number of nilpotent matrices with entries in a finite field. *Illinois J. Math.* 5 (2) (1961). 330–333.

[4] W. Goh and E. Schmutz. Random Matrices and Brownian Motion (to appear in Combinatorics, Probability, and Computing).

[5] J. Hansen. Factorization in $GF(q^m)[x]$ and Brownian motion (to appear in Combinatorics, Probability and Computing).

[6] J. Hansen. Order statistics for decomposable combinatorial structures (to appear in Random Structures and Algorithms).

[7] J. P. S. Kung. The cycle structure of a linear transformation over a finite field. *Linear Algebra and its Applications* 36 (1981), 141–155.

[8] D. H. Lehmer. On reciprocally weighted partitions. *Acta Arithmetica XXI* (1972), 379–388.

[9] M. Mignotte and J. L. Nicolas. Statistiques sur $\mathbf{F}_q[x]$. *Ann. Inst. Henri Poincaré* XIX no. 2 (1983), 113–121.

[10] J. L. Nicolas. A Gaussian law on $\mathbf{F}_q[x]$. *Colloq. Math. Soc. Janos Bolyai* (*Topics in classical number theory*) 34 (1984), 1127–1162.

[11] A. M. Odlyzko, *Discrete logarithms in finite fields and their cryptographic significance*, Lecture Notes in Computer Science 209 (Springer Verlag, 1984).

[12] E. Schmutz. The order of a typical matrix with entries in a finite field (submitted).

[13] R. Stong. Some asymptotic results on finite vector spaces. *Advances in applied mathematics* 9 (1988), 167–199.

[14] H. S. Wilf. *Generatingfunctionology* (Academic Press, 1990).