ISRAEL JOURNAL OF MATHEMATICS 91 (1995), 349–371

THE ORDER OF A TYPICAL MATRIX WITH ENTRIES IN A FINITE FIELD*

BY

ERIC SCHMUTZ

Mathematics and Computer Science Department
Drexel University, Philadelphia, PA 19104, USA
e-mail: eschmutz@mcs.drexel.edu

ABSTRACT

If A is an invertible $n \times n$ matrix with entries in the finite field $\mathbb{F}_q$, let $\mathbf{T}_n(A)$ be its minimum period or exponent, i.e. its order as an element of the general linear group $\mathrm{GL}(n, q)$. The main result is, roughly, that $\mathbf{T}_n(A) = q^{n-(\log n)^{2+o(1)}}$ for almost every A.

1. Introduction

Let $\mathcal{G}_n$ be the group of invertible $n \times n$ matrices with entries in the finite field $\mathbb{F}_q$. For $A \in \mathcal{G}_n$, let $\mathbf{T}_n(A)$ be the order or minimum period of A, i.e., the smallest $m > 0$ such that A^m is the identity matrix. Recently Stong [23] estimated the expected order:

$$\frac{1}{|\mathcal{G}_n|} \sum_{A \in \mathcal{G}_n} \mathbf{T}_n(A) = \frac{q^n}{n^{1+o(1)}}.$$

Although the average order is $q^{n-(\log n)^{1+o(1)}}$, most of the contribution to this average is from a small set of matrices with exceptionally large orders. It is therefore reasonable to ask how large the order is for a *typical* matrix. A rough statement of the main result in this paper (Theorem 13 and its corollary) is that almost every element of $\mathcal{G}_n$ has order $q^{n-(\log n)^{2+o(1)}}$.

Theorem 13 will be reduced to a seemingly different question about random polynomials. Let $\mathcal{U}_n$ be the set of monic degree n polynomials in $\mathbb{F}_q[\lambda]$, and let

* Supported by N.S.F. (D.M.S. 9101753).
Received November 17, 1992 and in revised form September 14, 1993

$\mathcal{P}_n$ be the set of polynomials in $\mathcal{U}_n$ that have non-zero constant terms. Suppose $f = \lambda^n - a_{n-1}\lambda^{n-1} - a_{n-2}\lambda^{n-2} - \cdots - a_1\lambda - a_0$ is in $\mathcal{P}_n$. Let C_f be the companion matrix of f, i.e.

$$C_f := \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & & \cdots & 0 \\ \cdot & \cdot & \cdot & & & & \cdots & 0 \\ \cdot & \cdot & \cdot & & & & \cdots & \cdot \\ \cdot & \cdot & \cdot & & & & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & & \cdots & 0 & 1 \\ a_0 & a_1 & a_2 & \cdots & & \cdots & a_{n-2} & a_{n-1} \end{pmatrix}$$

Then C_f is an element of $\mathcal{G}_n$. Abusing notation slightly, we call $\mathbf{T}_n(C_f)$ the **order** of f and write $\mathbf{T}_n(f)$. If $f \in \mathcal{U}_n$, then there is a unique $v \geq 0$ and $g \in \mathcal{P}_{n-v}$ such that $f = \lambda^v g$. We extend $\mathbf{T}_n$ to $\mathcal{U}_n$ by defining $\mathbf{T}_n(f) = \mathbf{T}_{n-v}(g)$. Theorem 1 states, roughly, that for almost every $f \in \mathcal{U}_n$, $\mathbf{T}_n(f) = q^{n-(\log n)^{2+o(1)}}$. The tool that enables us to efficiently reduce Theorem 13 to Theorem 1 is an approximation theorem of Jennie Hansen and mine. A rough and informal statement of this theorem is that, except for its small factors, the characteristic polynomial of a typical matrix in $\mathcal{G}_n$ resembles a typical monic degree n polynomial.

2. Preliminaries

Let $Q_n^{(1)}$ be the uniform probability measure on $\mathcal{U}_n$. Let $Q_n^{(2)}$ be the probability measure on $\mathcal{U}_n$ that is induced by the uniform measure on $\mathcal{G}_n$, namely

$$Q_n^{(2)}(\{f\}) = \frac{1}{|\mathcal{G}_n|}\left|\left\{A \in \mathcal{G}_n\colon f \text{ is the characteristic polynomial of } A\right\}\right|.$$

Let $\epsilon_n := \frac{1}{\log\log\log n}$. Our first goal is to prove

THEOREM 1: *Let* $\mathcal{B}_n := \left\{f\colon q^{n-(\log n)^{2+\epsilon_n}} \leq \mathbf{T}_n(f) \leq q^{n-(\log n)^{2-\epsilon_n}}\right\}$. *There is a constant* N_q *such that, for all* $n \geq N_q$,

$$1 - \epsilon_n \leq Q_n^{(1)}(\mathcal{B}_n) \leq 1.$$

(The corresponding result for $Q_n^{(2)}$ is Theorem 13.) The proof of Theorem 1 will not be completed until the end of Section 6. In the remainder of this section, some basic number theoretic facts are collected for future reference. The first of these basic facts is "well known"[21]:

THEOREM 2: *Let $f \in \mathcal{U}_n$ factor as $f = \lambda^v p_1^{r_1} p_2^{r_2} \cdots p_\omega^{r_\omega}$, where the p_i's are distinct, monic, irreducible polynomials in $\mathbb{F}_q[\lambda]$ that are all different from λ and have respective degrees $d_1 \le d_2 \le \cdots \le d_\omega$. Let τ_i be the order of p_i (i.e. the order that any root of p_i has in the splitting field of p_i). Finally, let p be the characteristic, let $\rho := \max\{r_1, \ldots, r_\omega\}$, and let t be the least postive integer for which $p^t \ge \rho$. Then*

$$\mathbf{T}_n(f) = p^t \cdot \mathrm{LCM}(\tau_1, \tau_2, \ldots, \tau_\omega).$$

Theorem 2 provides an expression for $\mathbf{T}_n(f)$ that is exact but difficult to handle. Lemma 3 provides bounds for $\mathbf{T}_n(f)$ that are more convenient. But first we need some notation. Let $\Omega_d(f)$ denote the number (counted with multiplicity) of irreducible factors of f whose degree is divisible by d. For $d > 1$, let $\mathbf{w}_d = \mathbf{w}_d(f) := \max\bigl(0, -1 + \Omega_d(f)\bigr)$. For $d = 1$, let $\mathbf{w}_1(f) = \max\bigl(0, -1 + \Omega_1(f) - v\bigr)$. (As before, v is the integer for which λ^v divides f, but λ^{v+1} does not.) Finally let $\Phi_d = \Phi_d(q)$ denote the d'th cyclotomic polynomial evaluated at q. Then, in the notation of Theorem 2, we have

LEMMA 3: *For all $f \in \mathcal{U}_n$,*

$$\frac{\tau_1 \cdot \tau_2 \cdots \tau_\omega}{\prod_d \Phi_d^{\mathbf{w}_d}} \le \mathrm{LCM}(\tau_1, \tau_2, \ldots, \tau_\omega) \le \frac{(q^{d_1} - 1) \cdot (q^{d_2} - 1) \cdots (q^{d_\omega} - 1)}{\prod_d \Phi_d^{\mathbf{w}_d}}.$$

Proof: The upper bound was observed by Stong [23]. It is a consequence of the fact that τ_i divides $q^{d_i} - 1$, and the identity

$$(2) \qquad \mathrm{LCM}(q^{d_1} - 1, q^{d_2} - 1, \ldots, q^{d_\omega} - 1) = \frac{(q^{d_1} - 1)(q^{d_2} - 1) \cdots (q^{d_\omega} - 1)}{\prod_d \Phi_d^{\mathbf{w}_d}}.$$

For the lower bound, we need some definitions. For all primes ℓ, and for all positive integers $i \le \omega$ define:

$\beta(\ell, i) :=$ the largest k for which ℓ^k divides τ_i,
$\gamma(\ell, i) :=$ the largest k for which ℓ^k divides $q^{d_i} - 1$,
$B(\ell) := \max\{\beta(\ell, 1), \beta(\ell, 2), \ldots, \beta(\ell, \omega)\}$, and
$\Gamma(\ell) = \max\{\gamma(\ell, 1), \gamma(\ell, 2), \ldots, \gamma(\ell, \omega)\}$.

Then

$$\tau_1 \tau_2 \cdots \tau_\omega = \prod_{\text{primes } \ell} \ell^{\beta(\ell,1) + \beta(\ell,2) + \ldots + \beta(\ell,\omega)},$$

and

$$(3)\quad \mathrm{LCM}(\tau_1,\tau_2,\dots,\tau_\omega)=\prod_{\text{primes }\ell}\ell^{B(\ell)}=\frac{\tau_1\cdot\tau_2\cdots\tau_\omega}{\prod_{\text{primes}\ell}\ell^{-B(\ell)+\beta(\ell,1)+\beta(\ell,2)+\dots+\beta(\ell,\omega)}}.$$

From (2) we have

$$(4)\qquad \prod_d \Phi_d^{w_d}=\prod_{\text{primes }\ell}\ell^{-\Gamma(\ell)+\gamma(\ell,1)+\gamma(\ell,2)+\cdots+\gamma(\ell,\omega)}.$$

Comparing (3) and (4), we see that it is sufficient to verify that, for all primes ℓ,

$$-\Gamma(\ell)+\gamma(\ell,1)+\gamma(\ell,2)+\cdots+\gamma(\ell,\omega)\ge -B(\ell)+\beta(\ell,1)+\beta(\ell,2)+\cdots+\beta(\ell,\omega).$$

Because τ_i divides $q^{d_i}-1$ $(i=1,\dots,\omega)$, we must have $\gamma(\ell,j)\ge\beta(\ell,j)$ for all $j\le\omega$. If we choose j_ℓ so that $\gamma(\ell,j_\ell)=\Gamma(\ell)$, then we have

$$\begin{aligned}-\Gamma(\ell)+\gamma(\ell,1)+\gamma(\ell,2)+\cdots+\gamma(\ell,\omega)&=\sum_{\substack{j=1\\ j\ne j_\ell}}^{\omega}\gamma(\ell,j)\\ &\ge\sum_{\substack{j=1\\ j\ne j_\ell}}^{\omega}\beta(\ell,j)=-\beta(\ell,j_\ell)+\sum_{j=1}^{\omega}\beta(\ell,j)\ge -B(\ell)+\sum_{j=1}^{\omega}\beta(\ell,j).\end{aligned}$$

∎

It is clear from Lemma 3 that we shall need estimates for the cyclotomic polynomials evaluated at q. The following crude estimates suffice.

LEMMA 4: *For all prime powers q and all positive integers d,*

$$q^{\frac{1}{2}\varphi(d)}<\Phi_d<q^{2\varphi(d)}.$$

Proof: The lower bound is proved in Kiss and Phong [19]. The upper bound is undoubtedly known, but I do not know a reference. An easy proof can be based on the identity

$$\Phi_d=\prod_{\substack{a=1\\ \mathrm{GCD}(a,d)=1}}^{d}(q-e^{2\pi ia/q}).$$

We have

$$\left|\Phi_d(q)\right|=q^{\varphi(d)}\prod_{\substack{a=1\\ \mathrm{GCD}(a,d)=1}}^{d}\left|\left(1-\frac{1}{q}e^{2\pi ia/q}\right)\right|.$$

Then, using the fact that

$$\left|\left(1-\frac{1}{q}e^{2\pi ia/q}\right)\right| \le \left(1+\frac{1}{q}\right),$$

we get

$$\Phi_d \le \left(q\left(1+\frac{1}{q}\right)\right)^{\varphi(d)}$$

Since $q(1+\frac{1}{q}) < q^2$, we have $\Phi_d < q^{2\varphi(d)}$. ∎

Finally, we remark that the probability of a polynomial depends only on the degrees of its irreducible factors and their multiplicities. More precisely, suppose that $f = \lambda^v \prod_{i=1}^{\omega} p_i^{r_i}$ and $g = \lambda^v \prod_{i=1}^{\omega} q_i^{r_i}$ are the canonical factorizations of f and g respectively, and suppose that degree(p_i)=degree(q_i) for $i = 1, 2, \ldots, \omega$. Obviously $Q_n^{(1)}(\{f\}) = Q_n^{(1)}(\{g\})$. It is less obvious, but no less true, that $Q_n^{(2)}(\{f\}) = Q_n^{(2)}(\{g\})$. (See, for example, Gerstenhaber [13].)

3. Small divisors

Let $\omega_d(f)$ denote the number of different irreducible monic polynomials that divide f and whose degree is divisible by d. For example, if $f \in \mathcal{P}_n$, then $\omega_1 = \omega$. Otherwise $\omega_1 = \omega + 1$, the number of distinct irreducible factors that f has. Theorem 5 tells us how large the ω_d's typically are. For related results, see Barbour, Arratia and Tavaré [1], Car [4], Gao and Richmond [12], Flajolet and Odlyzko [9], Flajolet and Soria [10–11], Hansen [16], Stong [24].

THEOREM 5: *Let*

$$\mu = \mu(d,n) := \frac{1}{d}\log\left(\frac{n}{d}\right),$$

and let $\sigma = \sigma(d,n) := \sqrt{\mu}$. *Let* D_n *be a sequence of positive real numbers with* $D_n = o(\log n)$. *If* $d = d(n) \le D_n$, *then for any fixed real number* t, *and for* $i = 1$ *or* 2,

$$Q_n^{(i)}\left(\frac{\omega_d - \mu}{\sigma} \le t\right) = \frac{(1+o(1))}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-s^2/2} ds$$

as $n \to \infty$. *Furthermore, there is an absolute constant* N_0 *such that, for any* $\delta > 0$, *and for all* $n \ge N_0$, *we have*

$$Q_n^{(i)}\left(|\omega_d - \mu| > \delta\mu\right) < 2e^{-\delta\mu/2\sigma}.$$

(The constant N_0 can be chosen uniformly for all $d \leq D_n$.)

Proof: Define $I_d(p) := 1$ if the degree of p (denoted $||p||$) is divisible by d, and $I_d(p) := 0$ otherwise. Let

$$F(x,y) := \prod_p (1 + y^{I_d(p)} \sum_{m \geq 1} \left(\frac{x}{q}\right)^{m||p||}),$$

where the product is over all monic irreducible polynomials. Note that $Q_n^{(1)}(\omega_d = k)$ is the coefficient of $x^n y^k$ in $F(x,y)$. Let $M_n(t) = [\![x^n]\!]F(x,e^t) = E_n^{(1)}(e^{t\omega_d})$ be the "moment generating function" for ω_d. (Here $[\![x^n]\!]$ means "the coefficient of x^n in..."). It is well known [5] that the first part of Theorem 5 (for $i = 1$) will follow if one can prove that, for any fixed real number t,

$$e^{-\mu t/\sigma} M_n(t/\sigma) = e^{t^2/2}(1 + o(1)) \tag{5}$$

as $n \to \infty$. In fact, a little bit more than this is true. Given $t_0 > 0$, we find that (5) holds uniformly for all t in the interval $-t_0 \leq t \leq t_0$. The proof will be similar to that of the main theorem in [14]. Some parts of the proof are omitted to avoid repetition. Let $\varepsilon(d)$ be the number of monic polynomials in $\mathbb{F}_q[\lambda]$ that are irreducible over $\mathbb{F}_q$ and have degree d. For future reference, we record the well known fact that

$$\frac{q^d}{d}(1 - q^{1-d/2}) \leq \varepsilon(d) \leq \frac{q^d}{d}. \tag{6}$$

Then we have

$$M_n(t) = [\![x^n]\!] \prod_{k \equiv 0(d)} \left(1 + e^t \sum_{m \geq 1} \left(\frac{x}{q}\right)^{mk}\right)^{\varepsilon(k)} \cdot \prod_{k \not\equiv 0(d)} \left(1 + \sum_{m \geq 1} \left(\frac{x}{q}\right)^{mk}\right)^{\varepsilon(k)}.$$

If we let

$$\Psi_k(x) = 1 + \sum_{m \geq 1} \left(\frac{x}{q}\right)^{mk},$$

then it is known [4] (and perhaps obvious [25]) that

$$\prod_k \Psi_k^{\varepsilon(k)} = \frac{1}{1-x}.$$

We also have

$$M_n(t) = [\![x^n]\!] \frac{1}{1-x} \prod_{k \equiv 0(d)} \left(\frac{1}{\Psi_k} + e^t\left(1 - \frac{1}{\Psi_k}\right)\right)^{\varepsilon(k)}.$$

If we set $z = z(n,d) = e^{t/\sigma} - 1$, then

$$M_n(t/\sigma) = [\![x^n]\!]\frac{1}{1-x}\prod_{k\equiv 0(d)}\left(1+z\left(1-\frac{1}{\Psi_k}\right)\right)^{\varepsilon(k)}. \tag{7}$$

Until now, all generating functions have been treated as formal power series. For x in the open unit disc, define

$$\delta_n(x) := \sum_{k\equiv 0(d)}\varepsilon(k)\log\left(1+z\left(1-\frac{1}{\Psi_k}\right)\right) - z\sum_{k\equiv 0(d)}\frac{x^k}{k},$$

where log denotes the principal branch of the logarithm. This requires the comment that $z = O(t_0/\sigma) = o(1)$, and also that

$$1-\frac{1}{\Psi_k} = \left(\frac{x}{q}\right)^k + O\left(\frac{x^{2k}}{q^{2k}}\right) = O(1).$$

Thus

$$e^{\delta_n(x)} = (1-x^d)^{z/d}\prod_{k\equiv 0(d)}\left(1+z\left(1-\frac{1}{\Psi_k}\right)\right)^{\varepsilon(k)}.$$

As in [14], we can analytically continue δ_n to a disc with any radius less than $\sqrt{q}$. To be definite, let D be the closed disc of radius $(1+\sqrt{2})/2$, and let Δ_n denote the extension of δ_n to D. The extended functions $\Delta_n(x)$ are uniformly bounded on D, and for all $x \in D$, $\Delta_n(x) \to 0$ as $n \to \infty$. Returning to (7), we have

$$M_n(t/\sigma) = [\![x^n]\!]\frac{e^{\Delta_n(x)}}{(1-x)(1-x^d)^{z/d}} = B^{(n)} + R^{(n)},$$

where

$$B^{(n)} := [\![x^n]\!]\frac{e^{\Delta_n(1)}}{(1-x)(1-x^d)^{z/d}},$$

and

$$R^{(n)} := [\![x^n]\!]\frac{e^{\Delta_n(x)} - e^{\Delta_n(1)}}{(1-x)(1-x^d)^{z/d}}.$$

It is relatively easy to estimate $B^{(n)}$:

$$B^{(n)} = e^{\Delta_n(1)}\sum_{k=0}^{n}[\![x^k]\!](1-x^d)^{-z/d} = e^{\Delta_n(1)}\sum_{m=0}^{\lfloor n/d\rfloor}[\![u^m]\!](1-u)^{-z/d}$$
$$= e^{\Delta_n(1)}\binom{\lfloor\frac{n}{d}\rfloor + \frac{z}{d}}{\lfloor\frac{n}{d}\rfloor} = e^{\Delta_n(1)}\lfloor n/d\rfloor^{z/d}(1+o(1)).$$

Recall that

$$\Delta_n(1) = o(1) \quad \text{and} \quad z = \frac{t}{\sigma} + \frac{t^2}{2\sigma^2} + O\Big(\frac{t_0^3}{\sigma^3}\Big).$$

Hence

$$e^{-t\mu/\sigma} B^{(n)} = e^{t^2/2}(1 + o(1)).$$

Using arguments similar to those in [14], one can prove that $R^{(n)} = o(B^{(n)})$. This completes the proof of the first part of the lemma for $i = 1$.

The computations are analagous for $i = 2$, but are slightly more complicated. In place of the generating function $F(x, y)$, one has

$$\prod_p \Big(1 + y^{I_d(p)} \sum_{j=1}^{\infty} \frac{q^{||p||j(j-1)} x^{||p||j}}{(q^{||p||j} - 1)(q^{||p||(j-1)} - 1) \cdots (q^{||p||} - 1)}\Big).$$

The details are omitted because the argument is almost identical to that in [14].

For the second part of Theorem 5, begin with the observation that, for $i = 1$ or 2,

$$Q_n^{(i)}\Big(\omega_d - \mu > \delta\mu\Big) = Q_n^{(i)}\Big(\exp\Big(\frac{\omega_d}{\sigma}\Big) > e^{(1+\delta)\mu/\sigma}\Big).$$

On the other hand, for any $y > 0$, and any non-negative random variable $\mathbf{X}$, $E_n^{(i)}(\mathbf{X}) \geq y \cdot Q_n^{(i)}(\mathbf{X} \geq y)$. In particular, taking $y = e^{(\delta+1)\mu/\sigma}$ and $\mathbf{X} = e^{\omega_d/\sigma}$, we get

$$Q_n^{(i)}\Big(\omega_d - \mu > \delta\mu\Big) \leq e^{-(\delta+1)\mu/\sigma} E_n^{(i)}\Big(\exp\Big(\frac{\omega_d}{\sigma}\Big)\Big) = e^{-\delta\mu/\sigma} E_n^{(i)}\Big(\exp\Big(\frac{\omega_d - \mu}{\sigma}\Big)\Big).$$

However, by (5) (and its analog for $i = 2$) we have

$$E_n^{(i)}\Big(\exp\Big(\frac{\omega_d - \mu}{\sigma}\Big)\Big) = \sqrt{e} + o(1).$$

Similar arguments yield

$$Q_n^{(i)}\Big(\omega_d - \mu < -\delta\mu\Big) < (\sqrt{e} + o(1))e^{-\delta 2\mu/\sigma}. \qquad \blacksquare$$

If we let $D_n := \lfloor (\log n)^{1-\epsilon_n/2} \rfloor$, then we have

COROLLARY: *Let $\mathcal{A}_n$ be the event that the inequalities $|\mathbf{w}_d - \mu| < \frac{1}{2}\mu$ are all satisfied ($d = 1, 2, \ldots, D_n$). Then, for $i = 1$ or 2,*

$$Q_n^{(i)}(\mathcal{A}_n) = 1 + o(\epsilon_n).$$

Proof: Observe that, for all d,

$$|\mathbf{w}_d - \mu| \le |\omega_d - \mu| + |\mathbf{w}_d - \omega_d|.$$

It follows directly from Theorem 5 that

$$Q_n^{(i)}\Big(|\omega_d - \mu| > \frac{1}{4}\mu \text{ for some } d \le D_n\Big) = o(\epsilon_n).$$

It therefore suffices to prove that

$$Q_n^{(i)}\Big(|\mathbf{w}_d - \omega_d| < \frac{1}{4}\mu \text{ for all } d \le D_n\Big) = 1 + o(\epsilon_n).$$

To this end, define $\alpha = \alpha_d(f)$ to be the number of irreducible factors of degree d, counted with multiplicity, that the characteristic polynomial of f has. Let

$$\mathcal{C}_n := \Big\{f\colon \alpha_k(f) \le \frac{1}{\epsilon_n^2} \text{ for all } k \text{ and } \alpha_k \le 1 \text{ for } k > \frac{1}{\epsilon_n^2}\Big\}.$$

In Section 5 (Lemma 6), it is proved that $Q_n^{(i)}(\mathcal{C}_n) = 1 + o(\epsilon_n)$. But for $f \in \mathcal{C}_n$, we have

$$|\mathbf{w}_d - \omega_d| \le \sum_{j=1}^{1/\epsilon_n^2} \frac{1}{\epsilon_n^2} < \frac{1}{4}\mu. \qquad \blacksquare$$

4. Upper bound

In Theorems 1 and 13, the upper bounds for $\mathbf{T}_n$ are relatively easy; we are already in a position to prove them. If $f \in \mathcal{U}_n$, then by Theorem 2 and Lemma 3, we have

$$\mathbf{T}_n(f) \le p^t \cdot \frac{\big(q^{d_1} - 1, q^{d_2} - 1, \ldots, q^{d_\omega} - 1\big)}{\prod_{d=1}^{\infty} \Phi_d^{\mathbf{w}_d}}. \tag{8}$$

To estimate the numerator of (8), note that

$$(q^{d_1} - 1) \cdot (q^{d_2} - 1) \cdots (q^{d_\omega} - 1) < q^{d_1 + d_2 + \cdots + d_\omega} \le q^n.$$

Also

$$p^t < q\rho \le qn = q^{O(\log n)}.$$

Finally, since $\Phi_d(q) \geq 1$ for all d, we get can get a bound for the denominator of (8) by restricting the product to d's less than $D_n := \lfloor (\log n)^{1-\epsilon_n/2} \rfloor$:

$$\prod_{d=1}^{\infty} \Phi_d^{\mathbf{w}_d} \geq \prod_{d=1}^{D_n} \Phi_d^{\mathbf{w}_d}.$$

Putting these three estimates into (8) we get, for all f in $\mathcal{U}_n$,

$$\mathbf{T}_n(f) < \frac{q^{n+O(\log n)}}{\prod_{d \leq D_n} \Phi_d^{\mathbf{w}_d}}. \tag{9}$$

Lemma 4 and the corollary to Theorem 5 together imply that, with probability $1 + o(\epsilon_n)$,

$$\prod_{d \leq D_n} q^{(\varphi(d) \log n)/4d} \leq \prod_{d \leq D_n} \Phi_d^{\mathbf{w}_d} \leq \prod_{d \leq D_n} q^{4\varphi(d) \log(n/d)}. \tag{10}$$

It is well known [18, chapter 4] that, as $y \to \infty$,

$$\sum_{d=1}^{y} \frac{\varphi(d)}{d} = \frac{6}{\pi^2} y(1 + o(1)).$$

Putting this into (10) (with $y = \xi$), we conclude that, with probability $1 + o(\epsilon_n)$,

$$q^{(\log n)^{2-3\epsilon_n/4}} < \prod_{d \leq D_n} \Phi_d^{\mathbf{w}_d} < q^{(\log n)^2}. \tag{11}$$

Putting the first inequality of (11) back into (9), we get the upper bounds in Theorem 1 and Theorem 13: for $i = 1$ or 2,

$$Q_n^{(i)}(\mathbf{T}_n < q^{n-(\log n)^{2-\epsilon_n}}) = 1 + o(\epsilon_n).$$

5. Technical lemmas

In this section we prove a series of technical lemmas. These lemmas will enable us to disregard various exceptional sets whose contribution is negligible. For any polynomial f, let $||f||$ denote its degree. In this section, $i < j$ does not imply that $||p_i|| < ||p_j||$; it is inconvenient notationally to continue with the convention of Theorem 2.

First we show that only small irreducibles appear with multiplicity larger than one. This will be used in the proof of the lower bound in §6. Let $\alpha_d(f)$ be the number of monic irreducible factors of degree d, counted with multiplicity, that f has. Then we have

LEMMA 6: *With Q_n^i- probability $1+o(\epsilon_n)$ ($i=1$ or 2), one has both $\alpha_d \le 1$ for all $d > 1/\epsilon_n^2$, and $\alpha_d \le 1/\epsilon_n^2$ for all $d \ge 1$.*

Proof: Let $\mathbf{R}_n(f)$ be the number of pairs of monic irreducible polynomials whose product divides f, and which have a common degree larger than $1/\epsilon_n^2$. In other words,

$$\mathbf{R}_n(f) := \big|\{(p_1,p_2)\colon ||p_1|| = ||p_2|| > 1/\epsilon_n^2 \text{ and } p_1p_2 \text{ divides } f\}\big|.$$

To prove the first part of the lemma, for $i=1$, it suffices to prove that $Q_n^{(1)}(\mathbf{R}_n > 0) = o(\epsilon_n)$. To this end, define $S_m := \{(p_1,p_2)\colon ||p_1|| = ||p_2|| = m\}$ to be the set of pairs of monic irreducible polynomials of degree m. Then

$$\begin{aligned} Q_n^{(1)}(\mathbf{R}_n > 0) &\le E_n^{(1)}(\mathbf{R}_n) \\ &= \sum_{m=\lfloor 1/\epsilon_n^2\rfloor+1}^{n/2} \sum_{(p_1,p_2)\in S_m} Q_n^{(1)}\Big(\{f\colon p_1p_2 \text{ divides } f\}\Big) \\ &= \sum_{m=\lfloor 1/\epsilon_n^2\rfloor+1}^{n/2} e(m)^2 \frac{q^{n-2m}}{q^n}. \end{aligned}$$

By (6) this is

$$\sum_{m=\lfloor 1/\epsilon_n^2\rfloor+1}^{n/2} O\Big(\frac{1}{m^2}\Big) = O(\epsilon_n^2).$$

Similarly for the second part of the lemma, let $\beta = \lfloor \frac{1}{\epsilon_n^2} \rfloor$. Then

$$Q_n^{(1)}(\alpha_d \ge \beta \quad \text{for some } d \ge 2) \le \sum_{d=2}^{n/\beta} \varepsilon(d)^\beta \frac{q^{n-d\beta}}{q^n}.$$

By (6), this is $o(\epsilon_n)$. For $d=1$,

$$Q_n^{(1)}(\alpha_1 > \beta) \le \frac{E_n^{(1)}(\alpha_1)}{\beta} = O\Big(\frac{1}{\beta}\Big) = o(\epsilon_n).$$

For $i=2$, we can take care of the "large degrees" using lemma 6 of [17]:

$$Q_n^{(2)}(\alpha_d \le 1 \text{ for all } d \ge 1/\epsilon_n^2) = 1 + O(1/\epsilon_n^2).$$

Then all that remains is to verify that

$$Q_n^{(2)}(\alpha_d \le 1/\epsilon_n^2 \text{ for all } d \le 1/\epsilon_n^2) = 1 + O(1/\epsilon_n^2).$$

I thank an anonymous referee for the following argument: If we set $Y := \sum_{d \le \beta} \alpha_d$, then it suffices to prove that $Q_n^{(2)}(Y > 1/\epsilon_n^2) = o(\epsilon_n)$. Using Kung and Stong's vector space cycle index [24], one can verify that

$$E(\mathbf{Y}^2) = O(\log(1/\epsilon_n^2)) = o(1/\epsilon).$$

(The details are omitted. See [24] for very similar computations.) But then

$$Q_n^{(2)}(Y > 1/\epsilon_n^2) < E(Y^2)\epsilon_n^2 = o(\epsilon). \qquad \blacksquare$$

In the remainder of this section, the only probability measure considered is $Q_n^{(1)}$. In particular, $Q_n^{(1)}$ is the implicit probability measure in the phrase "with probability $1 + o(\epsilon_n)\ldots$". It is clear from Lemma 3 that we will need to estimate the product $\prod_d \Phi_d^{\mathbf{w}_d}$. For small d's, we can use the corollary to Theorem 5 to estimate each term in the product. To deal with d's in the narrow range $(\log n)^{1-\epsilon_n} \le d \le (\log n)^{1+\epsilon_n/3}$, we need

LEMMA 7: *With probability* $1 + o(\epsilon_n)$, *one has*

$$\prod_{d=(\log n)^{1-\epsilon_n}}^{(\log n)^{1+\frac{\epsilon_n}{3}}} \Phi_d^{\mathbf{w}_d} < q^{(\log n)^{2+2\epsilon_n/3}}.$$

Proof: Let

$$\mathbf{Y}_n(f) := \sum_{d=(\log n)^{1-\epsilon_n}}^{(\log n)^{1+\epsilon_n/3}} \varphi(d)\mathbf{w}_d.$$

By Lemma 4, it suffices to prove that

$$Q_n^{(1)}\Big(\mathbf{Y}_n > \frac{1}{2}(\log n)^{2+2\epsilon_n/3}\Big) = o(\epsilon_n). \tag{12}$$

For any $y > 0$, $E_n^{(1)}(\mathbf{Y}_n) \ge y \cdot Q_n^{(1)}\big(\mathbf{Y}_n > y\big)$. In particular, taking $y = \frac{1}{2}(\log n)^{2+2\epsilon_n/3}$, we get

$$Q_n^{(1)}\Big(\mathbf{Y}_n > \frac{1}{2}(\log n)^{2+2\epsilon_n/3}\Big) \le \frac{E_n^{(1)}(\mathbf{Y}_n)}{\frac{1}{2}(\log n)^{2+2\epsilon_n/3}}. \tag{13}$$

Lemma 6 implies that, with probability $1 + o(\epsilon_n)$, we have $\mathbf{w}_d \le \omega_d$ for all $d > (\log n)^{1-\epsilon_n}$. We therefore get

$$\begin{aligned} &E_n^{(1)}(\mathbf{Y}_n) \\ &\le \sum_{d=(\log n)^{1-\epsilon_n}}^{(\log n)^{1+\epsilon_n/3}} \varphi(d) \sum_{m\equiv 0(d)} \sum_{\{\text{monic, irred. } p:\, \|p\|=m\}} Q_n^{(1)}\Big(\{f: p \text{ divides } f\}\Big) \\ &= \sum_{d=(\log n)^{1-\epsilon_n}}^{(\log n)^{1+\epsilon_n/3}} \varphi(d) \sum_{\substack{1\le m\le n \\ m\equiv 0(d)}} \varepsilon(m)\frac{q^{n-m}}{q^n} \\ &= \sum_{d=(\log n)^{1-\epsilon_n}}^{(\log n)^{1+\epsilon_n/3}} \varphi(d) O\Big(\frac{\log n}{d}\Big) = O((\log n)^{2+\epsilon_n/3}). \end{aligned}$$

Comparing this with (13) we get (12). ∎

For the intermediate range $(\log n)^{1+\epsilon_n/3} \le d \le (\log n)^{2+\epsilon_n/2}$, we need

LEMMA 8: *With probability* $(1 + o(\epsilon_n))$, *one has*

$$\prod_{d=(\log n)^{1+\epsilon_n/3}}^{(\log n)^{2+\epsilon_n/2}} \Phi_d^{\mathbf{w}_d} < q^{(\log n)^{2+\epsilon_n/2}}.$$

Proof: Let

$$\mathbf{W}_n = \sum_{d=(\log n)^{1+\epsilon_n/3}}^{(\log n)^{2+\epsilon_n/2}} \varphi(d)\mathbf{w}_d.$$

Again by Lemma 4, it suffices to prove that,

$$Q_n^{(1)}\Big(\mathbf{W}_n > (\log n)^{2+\epsilon_n/2}\Big) = o(\epsilon_n).$$

Because

$$Q_n^{(1)}\Big(\mathbf{W}_n > c(\log n)^{2+\epsilon_n/2}\Big) < \frac{E_n^{(1)}(\mathbf{W}_n)}{(\log n)^{2+\epsilon_n/2}},$$

it suffices to prove that $E_n^{(1)}(\mathbf{W}_n) = o(\epsilon_n(\log n)^{2+\epsilon_n/2})$. For $d > 1$,

$$\begin{aligned} E_n^{(1)}(\mathbf{w}_d) &= \sum_{j\ge 2} jQ_n^{(1)}(\Omega_d - 1 = j) = \sum_{r\ge 2}(r-1)Q_n^{(1)}(\Omega_d = r) \\ &\le \sum_{r\ge 2}(r-1)\frac{1}{r!} \sum_{\substack{(p_1,p_2,\ldots,p_r) \\ \|p_i\|\equiv 0(d)}} Q_n^{(1)}\Big(\{f: p_1p_2\ldots p_r \text{ divides } f\}\Big) + o(1), \end{aligned}$$

where the inner sum is over all ordered r-tuples of irreducible polynomials whose degree is divisible by d. We can easily estimate the inner sum:

$$\sum_{\substack{(p_1,p_2,\dots,p_r)\\ |[p_i]|\equiv 0(d)}} Q_n^{(1)}\Big(\{f\colon p_1p_2\dots,p_r \text{ divides } f\}\Big)$$

$$\leq \sum_{\substack{(m_1,m_2,\dots,m_r)\\ m_i\equiv 0(d) \text{ and } m\leq n}} \varepsilon(m_1)\varepsilon(m_2)\cdots\varepsilon(m_r)\Big(\frac{q^{n-m_1-m_2-\dots-m_r}}{q^n}\Big).$$

By (6), we have $\varepsilon(m_i)\leq q^{m_i}/m_i$. Hence the last sum is

$$\sum_{\substack{(m_1,m_2,\dots,m_r)\\ m_i\equiv 0(d) \text{ and } m\leq n}} O\Big(\frac{1}{m_1m_2\cdots m_r}\Big) = O\Big(\Big(\frac{\log n}{d}\Big)^r\Big).$$

But then

$$E_n^{(1)}(\mathbf{W}_n) = \sum_{d=(\log n)^{1+\epsilon_n/3}}^{(\log n)^{2+\epsilon_n/2}} \varphi(d)\sum_{r\geq 2}\frac{(r-1)}{r!}O\Big((\frac{\log n}{d})^r\Big)$$

$$\ll \sum_{r\geq 2}\frac{(\log n)^r}{(r-1)!}\sum_{d=(\log n)^{1+\epsilon_n/3}}^{(\log n)^{2+\epsilon_n/2}}\frac{1}{d^{r-1}}.$$

The contribution to this sum from the $r=2$ term is small enough:

$$(\log n)^2\sum_{d=(\log n)^{1+\epsilon_n/3}}^{(\log n)^{2+\epsilon_n/2}}\frac{1}{d} = O\Big((\log n)^2\log\log n\Big) = o(\epsilon_n(\log n)^{2+\epsilon_n/2}).$$

The remaining terms ($r\geq 3$) are negligible:

$$\sum_{r\geq 3}\frac{(\log n)^r}{(r-1)!}\sum_{d=(\log n)^{1+\epsilon_n/3}}^{(\log n)^{2+\epsilon_n/2}}\frac{1}{d^{r-1}}$$

$$=\sum_{r\geq 3}\frac{(\log n)^r}{(r-1)!}O\Big(\frac{1}{(\log n)^{(r-2)(1+\epsilon_n/3)}}\Big) = o(\epsilon_n(\log n)^{2+\epsilon_n/2}). \qquad \blacksquare$$

Finally, for large d's we need

LEMMA 9: *With probability* $(1+o(\epsilon_n))$, *one has* $\mathbf{w}_d = 0$ *for all* $d > (\log n)^{2+\epsilon_n/3}$.

Proof: Let

$$\mathbf{B}_n(f) := \sum_{d>(\log n)^{2+\epsilon_n/2}} \left|\left\{(p_1,p_2)\colon p_i \equiv 0(d) \text{ and } p_1p_2 \text{ divides } f\right\}\right|.$$

It suffices to show that $Q_n^{(1)}(\mathbf{B}_n > 0) = o(\epsilon_n)$. A similar averaging argument works:

$$Q_n^{(1)}(\mathbf{B}_n > 0) \le E_n^{(1)}(\mathbf{B}_n) \le \sum_{d>(\log n)^{2+\epsilon_n/3}} O\Big(\frac{\log^2 n}{d^2}\Big) = o(\epsilon_n). \qquad \blacksquare$$

COROLLARY: *With probability* $1 + o(\epsilon_n)$,

$$\prod_{d>(\log n)^{2+\epsilon_n/3}} \Phi_d^{\mathbf{w}_d} = 1.$$

Finally, in proving the lower bound, we shall need information about the distribution of orders for irreducible polynomials of a given degree. For this we require

LEMMA 10: *Define* $E(d,n)$ *to be the number of monic irreducible polynomials that have degree* d *and order less than* q^d/n^ξ, *where* $\xi = \xi(n) := \lfloor(\log n)^{\epsilon_n/2}\rfloor$. *Then there is a constant* c *such that, for all sufficiently large* n, *and for all* $d \le n$,

$$E(d,n) < \frac{q^{d-c\xi}}{d}.$$

Proof: The order of any irreducible polynomial of degree d divides $q^d - 1$. Furthermore, for each m dividing $q^d - 1$, the number of monic irreducible polynomials that have of order m and degree d is at most $\varphi(m)/d$ [15, page 85]. Finally, $\varphi(m) \le m$ for all m. Combining all these facts, we get

$$E(d,n) \le \sum_{\substack{m\mid q^d-1\\ m<(q^d/n^\xi)}} \frac{\varphi(m)}{d} \le \frac{1}{d} \sum_{\substack{m\mid q^d-1\\ m<(q^d/n^\xi)}} m.$$

If $mk = q^d - 1$ and $m < q^d/n^\xi$, then $k \ge n^\xi(1 - 1/q^d) \ge \frac{1}{2}n^\xi$. Thus we have

$$E(d,n) \le \frac{1}{d} \sum_{\substack{k\mid q^d-1\\ k\ge\frac{1}{2}n^\xi}} \frac{q^d-1}{k} < \frac{q^d}{d} \sum_{\substack{k\mid q^d-1\\ k\ge\frac{1}{2}n^\xi}} \frac{1}{k}.$$

Let $P^+(k)$ denote the largest prime factor of k. We split the sum as follows:

$$\frac{q^d}{d} \sum_{\substack{k \mid q^d-1 \\ k \geq \frac{1}{2}n^\xi}} \frac{1}{k} = \frac{q^d}{d}\Big(\sum_1 \frac{1}{k} + \sum_2 \frac{1}{k}\Big),$$

where the sum $\sum_1$ is over all k for which:

(a) k divides $q^d - 1$,

(b) $k \geq \frac{1}{2}n^\xi$, and

(c) $P^+(k) > n^4$.

(In the second sum $\sum_2$ one has $P^+(k) \leq n^4$.) To estimate $\sum_1$, we further decompose it according to the size of the largest prime factor of k. Factoring k as $k = p \cdot j$, where $p = P^+(k) \geq n^4$ and $j \big| q^d - 1$, we get:

$$\sum_1 \leq \sum_{\substack{\text{primes } p > n^4 \\ p \mid q^d-1}} \sum_{j \mid q^d-1} \frac{1}{pj}.$$

Obviously $q^d - 1$ has $O_q(d) = O(n)$ prime factors [8]. We therefore have the crude estimate

$$\sum_{\substack{\text{primes } p > n^4 \\ p \mid q^d-1}} \frac{1}{p} = O_q\Big(\frac{1}{n^3}\Big).$$

Erdős [8] proved that

$$\sum_{m \mid q^d-1} \frac{1}{m} = O(\log\log d).$$

Thus

$$\sum_1 = O\Big(\frac{\log\log n}{n^3}\Big).$$

To deal with $\sum_2$, we first define $\Psi(x, y)$ to be the number of positive integers $\leq x$ having prime factors that are all less than or equal to y. Then

$$\sum_2 < \sum_{\substack{k : q^n > k \geq \frac{1}{2}n^\xi \\ P^+(k) \leq n^4}} \frac{1}{k}$$

$$= \sum_{k:\ q^n > k \geq \frac{1}{2}n^\xi} \frac{1}{k}\Big(\Psi(k, n^4) - \Psi(k-1, n^4)\Big) \leq \sum_{k : k \geq \frac{1}{2}n^\xi} \frac{\Psi(k, n^4)}{k(k+1)}.$$

It is well known [15] that there are constants c_0, c_1 such that, for all $x \geq y \geq 2$,

$$\Psi(x,y) \leq c_1 x \exp\Big(-c_0 \frac{\log x}{\log y}\Big).$$

In particular, with $y = n^4$ and $x = k$, we get

$$\sum\nolimits_2 \leq \sum_{k: k \geq \frac{1}{2} n^\epsilon} \frac{\Psi(k, n^4)}{k(k+1)} < q^{-c\xi}$$

for some constant c. ∎

6. Lower bound

Combining (11) with Lemma 7, Lemma 8, and the corollary to Lemma 9, we conclude that, with probability $1 + o(\epsilon_n)$,

$$\prod_{d=1}^{\infty} \Phi_d^{\mathbf{w}_d} < q^{(\log n)^{2+3\epsilon_n/4}}. \tag{14}$$

Therefore, by Lemma 3, we have

$$Q_n^{(1)}\Big(\mathbf{T}_n > \frac{\tau_1 \cdot \tau_2 \cdots \tau_\omega}{q^{(\log n)^{2+3\epsilon_n/4}}}\Big) = 1 + o(\epsilon_n). \tag{15}$$

In order to use (15), we need to determine how large the τ_i's are.

LEMMA 11: *Let* $\mathcal{F}_7 := \Big\{f\colon \tau_i \geq \frac{q^{d_i r_i}}{n^\xi} \text{ for all } i \leq \omega\Big\}$. *Then, for* $k = 1$ *or* 2, $Q_n^{(k)}(\mathcal{F}_7) = 1 + o(\epsilon_n)$.

Remark: Intuitively, we expect the τ_i's to be conditionally independent, given the degree sequence. When coupled with Lemma 10, this should tell us how large the τ_i's are. This heuristic is not misleading, but it is not strictly true either. In order to provide a rigorous proof, it is necessary to identify various exceptional sets whose contribution is negligible. I have not been able to simplify the proof.

Proof: Let us revert to our notational conventions from Theorem 2: irreducible factors of a polynomial f will be labelled in an order that refines the ordering by degrees. In other words, if $f = \lambda^v p_1^{r_1} p_2^{r_2} \cdots p_\omega^{r_\omega}$, and $d_i = ||p_i||$, then it is understood that $d_1 \leq d_2 \leq \cdots \leq d_\omega$. With this notational convention, we can define $L := \lfloor c \cdots \log n \rfloor$, and let

$$\gamma(f) := \min\big\{i\colon ||p_i|| > L\big\}. \tag{16}$$

(For those exceptional polynomials whose irreducible factors' degrees are all less than L, define $\gamma(f) = \omega(f)$, say. These form a small set whose probability is negligible [22], [17].) Lemma 6 implies that, with probability $1 + o(\epsilon_n)$, we have $d_i r_i \leq L$ for all $i < \gamma$. Hence, with $Q_n^{(k)}$-probability $1 + o(\epsilon_n)$, we have $q^{d_i r_i}/n^{\xi} < 1$ for all $i < \gamma$. Since the τ_i's are all positive integers, it follows immediately that, with $Q_n^{(k)}$-probability $1 + o(\epsilon_n)$, we have

$$(\forall i < \gamma) \quad \tau_i \geq \frac{q^{d_i r_i}}{n^{\xi}}. \tag{17}$$

It is therefore sufficient to prove that, with probability $1 + o(\epsilon_n)$, one has $\tau_i \geq q^{d_i r_i}/n^{\xi}$ for all i in the interval $\gamma(f) \leq i \leq \omega(f)$. Let

$$\mathcal{F}_1 := \{f: \tau_i \geq q^{d_i r_i}/n^{\xi} \quad \text{for all } i \text{ in the interval } \gamma \leq i \leq \omega\}.$$

By (17), it suffices to prove that $Q_n^{(k)}(\mathcal{F}_1) = 1 + o(\epsilon_n)$.

To this end, define

$$\mathcal{F}_2 := \{f: r_i = 1 \text{ for } \gamma \leq i \leq \omega\},$$

and

$$\mathcal{F}_3 := \{f: d_i \neq d_j \text{ for } \gamma \leq i < j \leq \omega\}.$$

Also, let $\mathcal{F}_4$ consist of those polynomials in $\mathcal{U}_n$ for which there are at most $2 \log n$ distinct irreducible factors of degree larger than L. Finally, let

$$\mathcal{F}_5 = \mathcal{F}_2 \cap \mathcal{F}_3 \cap \mathcal{F}_4.$$

By Lemma 6 and Theorem 5, we have $Q_n^{(k)}(\mathcal{F}_5) = 1 + o(\epsilon_n)$. Thus we have

$$Q_n^{(k)}(\mathcal{F}_5) = 1 + o(\epsilon_n), \quad k = 1, 2. \tag{18}$$

This will enable us to restrict our attention to $\mathcal{F}_6 \stackrel{\text{def}}{=} \mathcal{F}_1 \cap \mathcal{F}_5$. Notice that

$$Q_n^{(k)}(\mathcal{F}_1) = Q_n^{(k)}(\mathcal{F}_6) + Q_n^{(k)}(\mathcal{F}_1 \cap \mathcal{F}_5^c).$$

Certainly the second term is negligible by (18):

$$Q_n^{(k)}(\mathcal{F}_1 \cap \mathcal{F}_5^c) \leq Q_n^{(k)}(\mathcal{F}_5^c) = o(\epsilon_n).$$

It therefore suffices to prove that $Q_n^{(k)}(\mathcal{F}_6) = 1 + o(\epsilon_n)$. To this end, define

$$\mathcal{J}(a,b) := \Big\{ \langle j_i \rangle_{i=a}^{i=b} \colon L < j_a < j_{a+1} < \cdots < j_b \text{ and } \sum_{i=a}^{b} j_i \le n \Big\}.$$

For $\vec{j} = \langle j_i \rangle_{i=a}^{i=b} \in \mathcal{J}(a,b)$, let

$$A_{\vec{j}} := \big\{ f \in \mathcal{F}_2 \colon \gamma = a,\ \omega = b, \text{ and } d_i = j_i \text{ for } i = a, a+1, \ldots, b \big\}.$$

Then

$$Q_n^{(k)}(\mathcal{F}_5) = \sum_{\substack{b-a<2\log n \\ a \le b}} \sum_{\vec{j} \in \mathcal{J}(a,b)} Q_n^{(k)}(A_{\vec{j}}), \tag{19}$$

and

$$Q_n^{(k)}(\mathcal{F}_6) = \sum_{\substack{b-a<2\log n \\ a \le b}} \sum_{\vec{j} \in \mathcal{J}(a,b)} Q_n^{(k)}(A_{\vec{j}}) Q_n^{(k)}\big(\tau_i \ge q^{d_i r_i}/n^{\xi} \text{ for } \gamma \le i \le \omega \big| A_{\vec{j}}\big). \tag{20}$$

Note that, for $f \in A_{\vec{j}}$, we have $r_i = 1$ for $a \le i \le b$. Because the degrees are distinct, we have conditional independence:

$$Q_n^{(k)}\Big(\tau_i \ge \frac{q^{d_i}}{n^{\xi}} \text{ for } \gamma \le i \le \omega \Big| A_{\vec{j}}\Big) = \prod_{i=a}^{b} Q_n^{(k)}\Big(\tau_i \ge \frac{q^{d_i}}{n^{\xi}} \Big| A_{\vec{j}}\Big). \tag{21}$$

By Lemma 10 we have, for $a \le i \le b$,

$$Q_n^{(k)}\Big(\tau_i \ge \frac{q^{d_i}}{n^{\xi}} \Big| A_{\vec{j}}\Big) > \Big(1 - \frac{q^{d_i - c\xi}}{d\varepsilon(d_i)}\Big)$$

(where $\xi = \lfloor (\log n)^{\epsilon_n/2} \rfloor$ and $\epsilon_n = 1/\log\log\log n$). From (6), we have $\varepsilon(d) \ge q^d/2d$, and consequently $q^{d_i - c\xi}/d\varepsilon(d_i) < 2q^{-c\xi}$. Thus

$$\prod_{i=a}^{b} Q_n^{(k)}\Big(\tau_i \ge \frac{q^{d_i r_i}}{n^{\xi}} \Big| A_{\vec{j}}\Big) > (1 - 2q^{-c\xi})^{2\log n} = 1 + o(\epsilon_n).$$

It is important to note that the constant implicit in the $o(\epsilon_n)$ can be chosen uniformly with repsect to $\vec{j}$. If we put this into (21) and then (20), we get:

$$Q_n^{(k)}(\mathcal{F}_6) = \sum_{\substack{b-a<2\log n \\ a\le b}} \sum_{\vec{j}\in\mathcal{J}(a,b)} Q_n^{(k)}(A_{\vec{j}})(1+o(\epsilon_n))$$
$$= Q_n^{(k)}(\mathcal{F}_5)(1+o(\epsilon_n)) = 1+o(\epsilon_n). \quad \blacksquare$$

With Lemma 11 at our disposal, we can now prove the lower bound in Theorem 1. Define $\mathcal{F}_8 := \{f: \omega \le 2\log n\} \bigcap \mathcal{F}_7$. By Theorem 5 and Lemma 11, $Q_n^{(k)}(\mathcal{F}_8) = 1+o(\epsilon_n)$. But for ALL $f \in \mathcal{F}_8$,

$$\tau_1\tau_2\cdots\tau_\omega \ge \frac{q^{d_1r_1+\cdots+d_\omega r_\omega}}{n^{\omega\xi}} = \frac{q^{n-v}}{n^{\omega\xi}} \ge \frac{q^{n-v}}{n^{2\xi\log n}}.$$

Recall the definition of v: λ^v divides f but λ^{v+1} does not. To deal with v, note that for any postive integer $v_0 \le n$, $Q_n^{(1)}(v \ge v_0) = 1/q^{v_0}$. Also note that $Q_n^{(2)}(v > 0) = 0$. Let $\mathcal{F}_9 = \{f: v \le (\log\log n)^2\}$, and let $\mathcal{F}_{10} = \mathcal{F}_8 \bigcap \mathcal{F}_9$. Then $Q_n^{(k)}(\mathcal{F}_9) = 1+o(\epsilon_n)$, and consequently $Q_n^{(k)}(\mathcal{F}_{10}) = 1+o(\epsilon_n)$. But for all $f \in \mathcal{F}_{10}$,

$$\tau_1\tau_2\cdots\tau_\omega \ge \frac{q^{n-(\log\log n)^2}}{n^{2\log n\xi}} \ge q^{n-(\log n)^{2+\epsilon}}. \tag{22}$$

This completes the proof of the lower bound in Theorem 1. $\blacksquare$

7. Reduction from matrices to polynomials

We have determined the order of a typical polynomial. Our goal is to determine the order of a typical matrix. The second problem will be reduced to the first problem using an approximation theorem that is stated below. Recall that $\alpha_i(f)$ denotes the number of irreducible factors of degree i that f has. Given $\ell = \ell(n)$, let $\Lambda_n^{(\ell)} = (\alpha_{\ell+1}, \alpha_{\ell+2}, \ldots, \alpha_n)$. Then we have

THEOREM 12 ([17]): *There is an absolute constant c_0 such that, for all positve integers ℓ and n that satisfy $c_0\log n \le \ell < n$, and for all $B \subseteq N^{n-\ell}$,*

$$\left|Q_n^{(2)}(\Lambda_n^{(\ell)} \in B) - Q_n^{(1)}(\Lambda_n^{(\ell)} \in B)\right| < \frac{c_0}{\ell}.$$

Theorem 12 will be used to prove the following

THEOREM 13: *There is a constant N_q such that, for all $n \ge N_q$,*

$$1-\epsilon_n \le Q_n^{(2)}(\mathcal{B}_n) \le 1.$$

One could prove Theorem 13 directly, without using Theorem 12, if one instead used Kung and Stong's vector space cycle index identity [24]. The ideas would be very similar to those in the proof of Theorem 1, but the computations would be very long and complicated. Although our proof of Theorem 13 is not completely trivial, it is signifigantly shorter than a direct proof.

Proof: The upper bound for $\mathbf{T}_n$ was already proved in section 4. To prove the lower bound, observe that for all $f \in \mathcal{U}_n$, $\mathbf{T}_n(f) \geq \mathrm{LCM}(\tau_\gamma, \tau_{\gamma+1}, \ldots, \tau_\omega)$. Define $\Omega_d'(f)$ to be the number of irreducible factors of f whose degree is (a) divisible by d, and (b) larger than L. Let $\mathbf{w}_d'(f) = \max(0, -1 + \Omega_d'(f))$. Then, as in Lemma 3,

$$\mathrm{LCM}(\tau_\gamma, \tau_{\gamma+1}, \ldots, \tau_\omega) \geq \frac{\tau_\gamma \tau_{\gamma+1} \cdots \tau_\omega}{\prod_d \Phi_d^{\mathbf{w}_d'}}.$$

Let $\mathbf{D}_n(f) = \tau_\gamma \tau_{\gamma+1} \cdots \tau_\omega$. If we can prove both of the inequalities $\mathbf{D}_n \geq q^{n-(\log n)^{2+3\epsilon_n/4}}$ and $\prod_d \Phi_d^{\mathbf{w}_d'} \leq q^{(\log n)^{2+3\epsilon_n/4}}$, then we certainly also have $\mathbf{T}_n(f) \geq q^{n-(\log n)^{2+\epsilon_n}}$. By Theorem 12, we have

$$(23)\quad Q_n^{(2)}\Big(\prod_d \Phi_d^{\mathbf{w}_d'} \geq q^{(\log n)^{2+3\epsilon_n/4}}\Big) = Q_n^{(1)}\Big(\prod_d \Phi_d^{\mathbf{w}_d'} \geq q^{(\log n)^{2+3\epsilon_n/4}}\Big) + o(\epsilon_n).$$

On the other hand, using (14) and the fact that $\mathbf{w}_d' \leq \mathbf{w}_d$, we get

$$Q_n^{(1)}\Big(\prod_d \Phi_d^{\mathbf{w}_d'} \geq q^{(\log n)^{2+3\epsilon_n/4}}\Big) \leq Q_n^{(1)}\Big(\prod_d \Phi_d^{\mathbf{w}_d} \geq q^{(\log n)^{2+3\epsilon_n/4}}\Big) = o(\epsilon_n).$$

It therefore suffices to show that

$$Q_n^{(2)}(\mathbf{D}_n \geq q^{n-(\log n)^{2+3\epsilon_n/2}}) = 1 + o(\epsilon_n).$$

By Theorem 5, $Q_n^{(2)}(\omega > 2\log n) = o(\epsilon_n)$. This plus Lemma 11 imply that, with $Q_n^{(2)}$-probability $1 + o(\epsilon_n)$, we have

$$\mathbf{D}_n \geq \frac{q^{d_\gamma r_\gamma + \cdots + d_\omega r_\omega}}{n^{2\xi \log n}} \geq q^{n-(\log n)^{2+3\epsilon_n/4}}. \qquad \blacksquare$$

It is not quite true that the order of a matrix is the order of its characteristic polynomial. However, they differ by no more than a factor of nq. Hence we can also prove the following

COROLLARY: *Let $\mathcal{S}_n$ consist of those matrices $A \in \mathcal{G}_n$ for which $q^{n-(\log n)^{2+\epsilon_n}} \leq \mathbf{T}_n(A) \leq q^{n-(\log n)^{2-\epsilon_n}}$. Then*

$$Q_n^{(2)}(\mathcal{S}_n) = 1 + o(\epsilon_n).$$

Perhaps the main results in this paper could be strengthened using more sophisticated techniques from probability theory.

ACKNOWLEDGEMENT: I am grateful to Jennie Hansen for some helpful comments.

References

[1] R. Arratia, A. D. Barbour and S. Tavaré, *On random polynomials over finite fields,* Mathematical Proceedings of the Cambridge Philosophical Society **114** (1993), 347–368.

[2] R. Arratia and S. Tavaré, *Limit theorems for combinatorial structures via discrete process approximations,* Random Structures and Algorithms **3** (1992), 321–345.

[3] R. Arratia and S. Tavaré, *Independent process approximations for random combinatorial structures,* Advances in Mathematics **104** (1994), 90–154.

[4] M. Car, *Factorisation dans $\mathbf{F}_q[x]$,* Comptes Rendus de l'Academie des Sciences, Paris **294** (1982), 147–150.

[5] J. Curtiss, *A note on the theory of moment generating functions,* Annals of Mathematical Statistics **13** (1942), 430–433.

[6] P. Erdős, C. Pomerance and E. Schmutz, *Carmichael's lambda function,* Acta Arithmetica **LVIII.4** (1991), 363–385.

[7] P. Erdős and P. Turán, *On some problems of a statistical group theory III,* Acta Math. Acad. Sci. Hung. **18** (1967), 309-320.

[8] P. Erdős, *On the sum $\sum_{d|2^n-1} \frac{1}{d}$,* Israel Journal of Mathematics **9** (1971), 43–48.

[9] P. Flajolet and A. M. Odlyzko, *Singularity analysis of generating functions,* SIAM Journal on Discrete Mathematics **3** (1990), 216–240.

[10] P. Flajolet and M. Soria, *General combinatorial schemas with Gaussian limit distributions and exponential tails,* Discrete Mathematics **114** (1993), 159–180.

[11] P. Flajolet and M. Soria, *Gaussian limiting distributions for the number of components in combinatorial structures,* Journal of Combinatorial Theory, Series A **53** (1990), 165–182.

[12] Z. Gao and L. B. Richmond, *Central and local limit theorems applied to asymptotic enumertion IV: multivariate generating functions*, Journal of Computational and Applied Mathematics **41** (1992), 177–186.

[13] M. Gerstenhaber, *On the number of nilpotent matrices with coefficients in a finite field*, Illinois Journal of Mathematics **5** (1961), 330–336.

[14] W. Goh and E. Schmutz, *A Central Limit Theorem on $GL_n(F_q)$*, Random Structures and Algorithms **2** (1991), 47–53.

[15] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge University Press, 1988.

[16] J. C. Hansen, *Factorization in $GF(q^m)[x]$ and Brownian motion*, Combinatorics, Probability, and Computing **2** (1993), 285–299.

[17] J. C. Hansen and E. Schmutz, *How random is the characteristic polynomial of a random matrix?*, Mathematical Proceedings of the Cambridge Philosophical Society **114** (1993), 507–516.

[18] M. Kac, *Statistical independence in probability, analysis and number theory*, Carus Monographs No.12, MAA, 1959, p. 56.

[19] P. Kiss and B. M Phong, *On a problem of Rotkiewicz*, Mathematics of Computation **48** (1987), 751–755.

[20] V. Kolchin, *Random Mappings*, Optimization Software Inc., New York, 1986.

[21] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications **20**, Addison Wesley, 1983.

[22] A. M. Odlyzko, *Discrete logarithms in finite fields and their cryptographic significance*, Proceedings of Eurocrypt '84, Springer Lecture Notes in Computer Science **209** (1984), 225–314.

[23] R. Stong, *The average order of a matrix*, Journal of Combinatorial Theory, Series A **64** (1993), 337–343.

[24] R. Stong, *Some asymptotic results on finite vector spaces*, Advances in Applied Mathematics **9** (1988), 167–199.

[25] H. Wilf, *Generatingfunctionology*, Academic Press, New York, 1990.