The Degree of the Splitting Field of a Random Polynomial over a Finite Field

John D. Dixon and Daniel Panario

School of Mathematics and Statistics
Carleton University, Ottawa, Canada
{jdixon,daniel}@math.carleton.ca

Submitted: Aug 30, 2004; Accepted: Sep 22, 2004; Published: Sep 30, 2004
Mathematics Subject Classifications: 11T06, 20B99

Abstract

The asymptotics of the order of a random permutation have been widely studied. P. Erdös and P. Turán proved that asymptotically the distribution of the logarithm of the order of an element in the symmetric group S_n is normal with mean $\frac{1}{2}(\log n)^2$ and variance $\frac{1}{3}(\log n)^3$. More recently R. Stong has shown that the mean of the order is asymptotically $\exp(C\sqrt{n/\log n} + O(\sqrt{n}\log\log n/\log n))$ where $C = 2.99047\ldots$. We prove similar results for the asymptotics of the degree of the splitting field of a random polynomial of degree n over a finite field.

1 Introduction

We consider the following problem. Let $\mathbb{F}_q$ denote a finite field of size q and consider the set $\mathcal{P}_n(q)$ of monic polynomials of degree n over $\mathbb{F}_q$. What can we say about the degree over $\mathbb{F}_q$ of the splitting field of a random polynomial from $\mathcal{P}_n(q)$? Because we are dealing with finite fields and there is only one field of each size, it is well known that the degree of the splitting field of $f(X) \in \mathcal{P}_n(q)$ is the least common multiple of the degrees of the irreducible factors of $f(X)$ over $\mathbb{F}_q$. Thus the problem can be rephrased as follows.

Let λ be a partition of n (denoted $\lambda \vdash n$) and write λ in the form $\left[1^{k_1}2^{k_2}\ldots n^{k_n}\right]$ where λ has k_s parts of size s. We shall say that a polynomial is of shape λ if it has k_s irreducible factors of degree s for each s. Let $w(\lambda, q)$ be the proportion of polynomials in $\mathcal{P}_n(q)$ which have shape λ. If we define $m(\lambda)$ to be the least common multiple of the sizes of the parts of λ, then the degree of the splitting field over $\mathbb{F}_q$ of a polynomial of shape λ is $m(\lambda)$. The average degree of a splitting field is given by

$$E_n(q) := \sum_{\lambda \vdash n} w(\lambda, q)m(\lambda).$$

An analogous problem arises in the symmetric group S_n. A permutation in S_n is of type $\lambda = \left[1^{k_1}2^{k_2}...n^{k_n}\right]$ if it has exactly k_s cycles of length s for each s, and its order is then equal to $m(\lambda)$. If $w(\lambda)$ denotes the proportion of permutations in S_n which are of type λ, then the average order of a permutation in S_n is equal to

$$E_n := \sum_{\lambda \vdash n} w(\lambda) m(\lambda).$$

We can think of $m(\lambda)$ as a random variable where λ ranges over the partitions of n and the probability of λ is $w(\lambda, q)$ and $w(\lambda)$ in the respective cases.

Properties of the random variable $m(\lambda)$ (and related random variables) under the distribution $w(\lambda)$ have been studied by a number of authors, notably by Erdös and Turán in a series of papers [1, 2, 3] and [4]. In particular, the main theorem of [3] shows that in this case the distribution of $\log m(\lambda)$ is approximated by a normal distribution with mean $\frac{1}{2}(\log n)^2$ and variance $\frac{1}{3}(\log n)^3$ in a precise sense. In our notation the theorem reads as follows. For each real x define

$$\Psi_n(x) := \left\{ \lambda \vdash n \mid \log m(\lambda) \leq \frac{1}{2}(\log n)^2 + \frac{x}{\sqrt{3}}(\log n)^{3/2} \right\}.$$

Then for each $x_0 > 0$:

$$\sum_{\lambda \in \Psi_n(x)} w(\lambda) \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt \text{ as } n \to \infty \text{ uniformly for } x \in [-x_0, x_0].$$

In particular, the mean of the random variable $\log m(\lambda)$ is asymptotic to $\frac{1}{2}(\log n)^2$, but this does *not* imply that $\log E_n$ (the log of the mean of $m(\lambda)$) is asymptotic to $\frac{1}{2}(\log n)^2$ and indeed it is much larger. The problem of estimating E_n was raised in [4], and the first asymptotic expression for $\log E_n$ was obtained by Goh and Schmutz [6]. The result of Goh and Schmutz was refined by Stong [9] who showed that

$$\log E_n = C\sqrt{\frac{n}{\log n}} + O\left(\frac{\sqrt{n}\log\log n}{\log n}\right),$$

where $C = 2.99047...$ is an explicitly defined constant.

The object of the present paper is to prove analogous theorems for the random variable $m(\lambda)$ under the distribution $w(\lambda, q)$. Actually, it turns out that these theorems hold for several important classes of polynomials which we shall now describe. Consider the classes:

- $\mathcal{M}_1(q)$: the class of all monic polynomials over $\mathbb{F}_q$. In this class the number of polynomials of degree n is q^n for each $n \geq 1$.
- $\mathcal{M}_2(q)$: the class of all monic square-free polynomials over $\mathbb{F}_q$. In this class the number of polynomials of degree n is $(1 - q^{-1})q^n$ for each n.

- $\mathcal{M}_3(q)$: the class of all monic square-free polynomials over $\mathbb{F}_q$ whose irreducible factors have distinct degrees. In this class the number of polynomials of degree n is $a(n,q)q^n$ where, for each q, $a(n,q) \to a(q) := \prod_{k \geq 1}(1 + i_k(q)q^{-k})\exp(-1/k)$ as $n \to \infty$ where $i_k(q)$ is the number of monic irreducible polynomials of degree k over $\mathbb{F}_q$ (see [7] Equation (1) with $j = 0$).

For $x > 0$ define

$$\Phi_n(x) := \left\{ \lambda \vdash n \mid \left| \log m(\lambda) - \frac{1}{2}(\log n)^2 \right| > \frac{x}{\sqrt{3}}(\log n)^{3/2} \right\}.$$

Then for each of the classes of polynomials described above we have a weak analogue of the theorem of Erdös and Turán quoted above, and an exact analogue of Stong's theorem.

Theorem 1 *Fix one of the classes $\mathcal{M}_i(q)$ described above. For each $\lambda \vdash n$, let $w(\lambda, q)$ denote the proportion of polynomials in this class whose factorizations have shape λ. Then there exists a constant $c_0 > 0$ (independent of the class) such that for each $x \geq 1$ there exists $n_0(x)$ such that*

$$\sum_{\lambda \in \Phi_n(x)} w_i(\lambda, q) \leq c_0 e^{-x/4} \text{ for all } q \text{ and all } n \geq n_0(x). \tag{1}$$

In particular, almost all $f(X)$ of degree n in $\mathcal{M}_i(q)$ have splitting fields of degree $\exp((\frac{1}{2} + o(1))(\log n)^2)$ over $\mathbb{F}_q$ as $n \to \infty$.

Theorem 2 *Let C be the same constant as in the Goh-Schmutz-Stong theorem. Then in each of the classes described above the average degree $E_n(q)$ of a splitting field of a polynomial of degree n in that class satisfies*

$$\log E_n(q) = C\sqrt{\frac{n}{\log n}} + O\left(\frac{\sqrt{n}\log\log n}{\log n}\right) \text{ uniformly in } q.$$

2 Properties of $w(\lambda, q)$

First consider the value of $w(\lambda, q)$ for each of the three classes. Let $i_s = i_s(q)$ denote the number of monic irreducible polynomials of degree s over $\mathbb{F}_q$. Then (see, for example, [8]) we have $q^s = \sum_{d|s} d i_d$ so a simple argument shows that

$$\frac{q^s}{s} \geq i_s \geq \frac{q^s}{s}(1 + 2q^{-s/2})^{-1}.$$

Let $\lambda \vdash n$ have the form $\left[1^{k_1}...n^{k_n}\right]$. Since $\mathcal{P}_n(q)$ contains q^n polynomials, and there are $\binom{i_s+k-1}{k}$ ways to select k irreducible factors of degree s, we have

$$w(\lambda, q) = \frac{1}{q^n}\prod_{s=1}^{n}\binom{i_s + k_s - 1}{k_s} = \prod_{s=1}^{n} q^{-sk_s}\binom{i_s + k_s - 1}{k_s} \text{ in } \mathcal{M}_1(q).$$

Similarly, since there are $(1-q^{-1})q^n$ polynomials of degree n in $\mathcal{M}_2(q)$, and there are $\binom{i_s}{k}$ ways to select k distinct irreducible factors of degree s, in this case we have

$$w(\lambda, q) = \frac{1}{(1-q^{-1})q^n} \prod_{s=1}^{n} \binom{i_s}{k_s} = \frac{1}{(1-q^{-1})} \prod_{s=1}^{n} q^{-sk_s} \binom{i_s}{k_s} \text{ in } \mathcal{M}_2(q).$$

Finally, since there are $a(n,q)q^n$ polynomials of degree n in $\mathcal{M}_3(q)$ and each of these polynomials has at most one irreducible factor of each degree, we get

$$w(\lambda, q) = \frac{1}{a(n,q)q^n} \prod_{s=1}^{n} \binom{1}{k_s} i_s^{k_s} = \frac{1}{a(n,q)} \prod_{s=1}^{n} q^{-sk_s} \binom{1}{k_s} i_s^{k_s} \text{ in } \mathcal{M}_3(q)$$

when each part in λ has multiplicty ≤ 1, and $w(\lambda, q) = 0$ otherwise. As is well known we also have

$$w(\lambda) = \frac{1}{1^{k_1} 2^{k_2} \ldots n^{k_n} k_1! k_2! \ldots k_n!}.$$

We shall use the notation Π_n to denote the set of all partitions of n, $\Pi_{n,k}$ to denote the set of partitions $\left[1^{k_1} 2^{k_2} \ldots n^{k_n}\right]$ in which each $k_i < k$ and $\Pi'_{n,k}$ to denote the complementary set of partitions.

It is useful to note that in $\mathcal{M}_1(q)$ and $\mathcal{M}_2(q)$ we have $w(\lambda, q) \to w(\lambda)$ as $q \to \infty$. However, this behaviour is not uniform in λ. Indeed for each of these two classes the ratio $w(\lambda, q)/w(\lambda)$ is unbounded above and below for fixed q if we let λ range over all partitions of n and $n \to \infty$. This means we have to be careful in deducing our theorems from the corresponding results for $w(\lambda)$. In $\mathcal{M}_3(q)$, we have $w(\lambda, q) = 0$ whenever $\lambda \in \Pi'_{n,2}$, and a simple computation shows that $a(n,q)w(\lambda, q) \to w(\lambda)$ as $q \to \infty$ whenever $\lambda \in \Pi_{n,2}$.

Lemma 3 *There exists a constant $a_0 > 0$ such that*

$$1 \leq \frac{1}{1-q^{-1}} \leq a_0 \text{ and } 1 \leq \frac{1}{a(n,q)} \leq a_0$$

for all $n \geq 1$ and all prime powers $q > 1$.

Proof. The first inequality is satisfied whenever $a_0 \geq 2$, so it is enough to prove that the set of all $a(n,q)$ has a strictly positive lower bound.

We shall use results from [7, Theorems 1 and 2]. In our notation [7] shows that $a(q)$ increases monotonically with q starting with $a(2) = 0.3967\ldots$, and that for some absolute constant c we have $|a(n,q) - a(q)| \leq c/n$ for all $n \geq 1$. In particular, $a(n,q) \geq a(q) - c/n \geq a(2) - c/n$. Thus $a(n,q) \geq \frac{1}{2}a(2) > 0$ for all q whenever $n > n_0 := \lfloor 2c/a(2) \rfloor$.

On the other hand, as we noted above, in $\mathcal{M}_3(q)$, $a(n,q)w(\lambda, q) \to w(\lambda)$ as $q \to \infty$ whenever $\lambda \in \Pi_{n,2}$ and is 0 otherwise. Thus

$$a(n,q) = \sum_{\lambda \in \Pi_n} a(n,q) w(\lambda, q) \to \sum_{\lambda \in \Pi_{k,2}} w(\lambda) = b(n), \text{ say, as } q \to \infty.$$

Evidently, $b(n) > 0$ (it is the probability that a permutation in S_n has all of its cycles of different lengths). Define $b_0 := \min\{b(n) \mid n = 1, 2, ..., n_0\}$. Then the limit above shows that there exists q_0 such that $a(n,q) \geq \frac{1}{2}b_0$ whenever $n = 1, 2, ..., n_0$ and $q > q_0$.

Finally, choose $a_0 \geq 2$ such that $1/a_0$ is bounded above by $\frac{1}{2}a(2)$, $\frac{1}{2}b_0$ and all $a(n,q)$ with $n = 1, 2, ..., n_0$ and $q \leq q_0$. This value of a_0 satisfies the stated inequalities. ∎

We next examine some properties of the $w(\lambda, q)$ which we shall need later. In what follows, if $\lambda := \left[1^{k_1}...n^{k_n}\right] \in \Pi_n$ and $\mu := \left[1^{l_1}...m^{l_m}\right] \in \Pi_m$, then the join $\lambda \vee \mu$ denotes the partition of $m + n$ with $k_s + l_s$ parts of size s. We shall say that λ and μ are *disjoint* if $k_s l_s = 0$ for each s.

Lemma 4 *Let a_0 be a constant satisfying the conditions in Lemma 3. Then for each class $\mathcal{M}_i(q)$ we have $w(\lambda \vee \mu, q) \leq a_0 w(\lambda, q)w(\mu, q)$ for all λ and μ. On the other hand, if λ and μ are disjoint, then $w(\lambda \vee \mu, q) \geq a_0^{-2} w(\lambda, q)w(\mu, q)$.*

We also have $w(\lambda \vee \mu) \leq w(\lambda)w(\mu)$, with equality holding when λ and μ are disjoint.

Proof. First note that in each of the classes, $w(\lambda \vee \mu, q)$ is 0 if either $w(\lambda, q)$ or $w(\mu, q)$ is 0. Suppose neither of the latter is 0 and put $r := w(\lambda \vee \mu, q)/w(\lambda, q)w(\mu, q)$.

First consider the class $\mathcal{M}_1(q)$. Then r can be written as a product of terms of the form

$$\binom{i_s + k_s + l_s - 1}{k_s + l_s} \Big/ \binom{i_s + k_s - 1}{k_s}\binom{i_s + l_s - 1}{l_s}.$$

The numerator of this ratio counts the number of ways of placing $k_s + l_s$ indistinguishable items in i_s distinguishable boxes. The denominator counts the number of ways of doing this when k_s of the items are of one type and l_s are another, and so is at least as great as the numerator. Hence we conclude that $r \leq 1 < a_0$ in this case. Moreover, when λ and μ are disjoint then each term is equal to 1 and so $r = 1 \geq a_0^{-2}$. This proves the claim for the class $\mathcal{M}_1(q)$. Taking limits as $q \to \infty$ also gives a proof of the final statement.

Now consider the class $\mathcal{M}_2(q)$. In this case $r/(1 - q^{-1})$ can be written as a product of terms of the form

$$\binom{i_s}{k_s + l_s} \Big/ \binom{i_s}{k_s}\binom{i_s}{l_s}.$$

The numerator counts the number of ways to choose $k_s + l_s$ out of i_s items, whilst the denominator is at least as large as $\binom{i_s}{k_s}\binom{i_s - k_s}{l_s}$ which counts the number of ways to choose $k_s + l_s$ items when k_s are of one type and l_s are another type. This shows that each term is at most 1 and so $r \leq (1 - q^{-1}) \leq a_0$ as required. Again, in this case, when the partitions are disjoint, each term is equal to 1 and so $r = 1 - q^{-1} \geq a_0^{-2}$. This proves the claim for the class $\mathcal{M}_2(q)$, and the proof for the class $\mathcal{M}_3(q)$ is similar (in this case $w(\lambda \vee \mu, q)$ is 0 unless λ and μ are disjoint). ∎

Lemma 5 *For all partitions of the form $[s^k]$ and all q we have*

$$w(\left[s^k\right], q) \leq a_0 \frac{k+1}{(2s)^k}$$

in each of the classes $\mathcal{M}_i(q)$.

Proof. Fix q and k and define

$$v_s := \frac{q^{-sk}}{k!}\prod_{j=0}^{k}\left(\frac{q^s}{s}+j\right).$$

Since $i_s \le q^s/s$ we have $w(\left[s^k\right],q) \le a_0 v_s$ for each of the three classes. We also note that

$$v_1 = \frac{1}{k!}\prod_{j=0}^{k-1}(1+j/q) \le \frac{1}{k!}\prod_{j=0}^{k-1}(1+j/2) = \frac{k+1}{2^k}.$$

Finally since

$$v_{s+1}/v_s = q^{-k}\prod_{j=0}^{k-1}\frac{q^{s+1}/(s+1)+j}{q^s/s+j} \le q^{-k}\prod_{j=0}^{k-1}\frac{qs}{s+1} = \left(\frac{s}{s+1}\right)^k,$$

we obtain $w(\left[s^k\right],q) \le a_0 v_s \le a_0 s^{-k} v_1$ so the result follows. ■

Lemma 6 *Let $\lambda = \left[1^{k_1}...n^{k_n}\right]$ be a partition of n. The following are true for each of the classes $\mathcal{M}_i(q)$.*

(a) If each $k_s \le k$ for some fixed integer $k > 0$, then $w(\lambda,q) \le a_0 e^{2k(k-1)} w(\lambda)$.

(b) There exists a constant c_1 such that, if each $k_s \le 1$, then $w(\lambda,q) \ge c_1 w(\lambda)$.

Proof. (a) For each of the classes we have

$$w(\lambda,q) \le a_0 \prod_{s=1}^{n}\frac{1}{q^{sk_s}}\frac{1}{k_s!}(i_s+k_s-1)^{k_s}.$$

Using the bound $i_s \le q^s/s$ we obtain

$$\begin{aligned} w(\lambda,q) &\le a_0 \prod_{s=1}^{n}\frac{1}{s^{k_s}k_s!}\left(1+\frac{s(k_s-1)}{q^s}\right)^{k_s} \\ &\le a_0 w(\lambda)\exp\left(\sum_{s=1}^{n} sk_s(k_s-1)q^{-s}\right). \end{aligned}$$

Since $\sum_{s=1}^{\infty} sq^{-s} \le \sum_{s=1}^{\infty} s2^{-s} = 2$, this proves (a).

(b) Similarly, for partitions with no two parts of the same size we have (for any of the classes)

$$\begin{aligned} w(\lambda,q) &\ge \prod_{s=1}^{n}\frac{1}{q^{sk_s}} i_s^{k_s} \ge \prod_{s=1}^{n}\frac{1}{s^{k_s}k_s!}\left(\frac{1}{1+2q^{-s/2}}\right)^{k_s} \\ &\ge w(\lambda)\exp\left(-2\sum_{s=1}^{n} k_s q^{-s/2}\right) \end{aligned}$$

so the lower bound follows with $c_1 := \exp\left(-2\sum_{s=1}^{\infty} 2^{-s/2}\right) = 0.007999$. ■

Recall that the set $\Pi_{n,k}$ consists of all partitions of n in which each part has multiplicity $< k$, and $\Pi'_{n,k}$ consists of the remaining partitions.

Lemma 7 *For all classes $\mathcal{M}_i(q)$, and all n and q*

$$\sum_{\lambda \in \Pi'_{n,k}} w(\lambda, q) \leq a_0^2 \frac{k+1}{2^{k-1}} \text{ whenever } k \geq 2.$$

Similarly

$$\sum_{\lambda \in \Pi'_{n,k}} w(\lambda) \leq \frac{k+1}{2^{k-1}} \text{ whenever } k \geq 2.$$

Proof. Each $\lambda \in \Pi'_{n,k}$ can be written in the form $[s^k] \vee \mu$ for some $\mu \vdash n - ks$ in at least one way. Hence using Lemmas 4 and 5 we obtain

$$\sum_{\lambda \in \Pi'_{n,k}} w(\lambda, q) \leq \sum_{s=1}^{n/k} \sum_{\mu \vdash n-ks} w([s^k] \vee \mu, q) \leq a_0 \sum_{s=1}^{n/k} w([s^k], q) \sum_{\mu \vdash n-ks} w(\mu, q)$$
$$= a_0 \sum_{s=1}^{n/k} w([s^k], q) \leq a_0^2 \sum_{s=1}^{\infty} \frac{k+1}{(2s)^k} \leq a_0^2 \frac{k+1}{2^{k-1}}.$$

This proves the stated inequality. The corresponding inequality for $w(\lambda)$ is similar. ∎

3 Proof of Theorem 1

Since $\Phi_n(x)$ and $\Psi_n(x) \setminus \Psi_n(-x)$ are complementary sets for $x > 0$, and the error function is even, the theorem of Erdös and Turán quoted in the Introduction shows that for fixed $x > 0$:

$$W_n(x) := \sum_{\lambda \in \Phi_n(x)} w(\lambda) \to \eta(x) \text{ as } n \to \infty,$$

where

$$\eta(x) := \frac{1}{\sqrt{2\pi}} \left\{ \int_{-\infty}^{-x} e^{-t^2/2} dt + \int_x^{\infty} e^{-t^2/2} dt \right\} = \frac{2}{\sqrt{2\pi}} \int_x^{\infty} e^{-t^2/2} dt.$$

A simple integration by parts shows (see, for example, [5, Chap. 7]) that

$$\eta(x) < \frac{2e^{-x^2/2}}{\sqrt{2\pi} x} \text{ for } x > 0.$$

Thus, for $x \geq 1$, there exists $n_0(x) > 0$ such that $W_n(x) < e^{-x^2/2}$ whenever $n > n_0(x)$.

Define $\Phi_{n,k}(x) := \Phi_n(x) \cap \Pi_{n,k}$ and $\Phi'_{n,k}(x) := \Phi_n(x) \cap \Pi'_{n,k}$. Now using Lemma 6 we have, for each of the classes $\mathcal{M}_i(q)$, that

$$W_{n,k}(x, q) := \sum_{\lambda \in \Phi_{n,k}(x)} w(\lambda, q) \leq a_0 e^{2k(k-1)} \sum_{\lambda \in \Phi_{n,k}(x)} w(\lambda) \leq a_0 e^{2k(k-1)} W_n(x).$$

On the other hand Lemma 7 shows that for $k \geq 1$:

$$W'_{n,k}(x,q) := \sum_{\lambda \in \Phi'_{n,k}(x)} w(\lambda, q) \leq \sum_{\lambda \in \Pi'_{n,k}(x)} w(\lambda, q) \leq a_0^2 \frac{k+1}{2^{k-1}} < 8a_0^2 e^{-(k+1)/2}.$$

Thus for $x \geq 1$, $k \geq 1$ and $n \geq n_0(x)$ we have

$$\sum_{\lambda \in \Phi_n(x)} w(\lambda, q) = W_{n,k}(x,q) + W'_{n,k}(x,q) < a_0 e^{2k(k-1)} e^{-x^2/2} + 8a_0^2 e^{-(k+1)/2}.$$

If $x \geq 2$, then we can choose $k := \lfloor x/2 \rfloor$ and obtain

$$e^{2k(k-1)} e^{-x^2/2} + 8a_0 e^{-(k+1)/2} < e^{-x} + 8a_0 e^{-x/4} < (1 + 8a_0) e^{-x/4},$$

uniformly in x. Thus taking $c_0 := a_0(1 + 8a_0)$ we obtain (1) for $x \geq 2$. However, by adjusting the value of c_0 if necessary we can ensure that the inequality (1) is also valid for x with $1 \leq x < 2$. Then the inequality is valid for all $x \geq 1$.

Finally, we prove the last assertion of the theorem. Given any $\varepsilon > 0$ and $\delta > 0$, choose $x \geq 1$ so that $c_0 e^{-x/4} < \delta$, and then choose $n_1 \geq n_0(x)$ so that $x < \varepsilon\sqrt{3 \log n_1}$. Now (1) shows that for all $n \geq n_1$ the proportion of $f(X)$ of degree n in $\mathcal{M}_i(q)$ which have splitting fields whose degree lies outside of the interval $\left[\exp((\frac{1}{2} - \varepsilon)(\log n)^2), \exp((\frac{1}{2} + \varepsilon)(\log n)^2)\right]$ is bounded by $c_0 e^{-x/4} < \delta$. This is equivalent to what is stated.

4 Proof of Theorem 2

We start by proving an upper bound for $E_n(q)$. Define

$$\tilde{E}_n := \max\{E_m \mid m = 1, 2, ..., n\}.$$

(It seems likely that $\tilde{E}_n = E_n$ but we have not been able to prove this.)

Lemma 8 *There exists a constant $c_2 > 0$ such that, in each of the classes $\mathcal{M}_i(q)$, $E_n(q) \leq c_2 \tilde{E}_n$ for all q and all n.*

Proof. Let $k \geq 2$ be the least integer such that

$$a_0^2 \sum_{s=1}^{\infty} \frac{(k+1)s}{(2s)^{k-1}} \leq 1/2.$$

We shall define $c_2 := 2a_0 e^{2k(k-1)}$.

We shall prove the lemma by induction on n. Note that $E_1(q) = 1 \leq c_2 = c_2\tilde{E}_1$. Assume $n \geq 2$ and that $E_m(q) \leq c_2\tilde{E}_m$ for all $m < n$. Now Lemma 4 shows that

$$\begin{aligned} E'_{n,k}(q) := \sum_{\lambda\in\Pi'_{n,k}} w(\lambda,q)m(\lambda) &\leq \sum_{s=1}^{n/k}\sum_{\mu\vdash n-ks} w(\left[s^k\right]\vee\mu,q)m(\left[s^k\right]\vee\mu) \\ &\leq a_0\sum_{s=1}^{n/k} sw(\left[s^k\right],q)\sum_{\mu\vdash n-ks} w(\mu,q)m(\mu) \\ &= a_0\sum_{s=1}^{n/k} sw(\left[s^k\right],q)E_{n-ks}(q). \end{aligned}$$

Thus using Lemma 5, the choice of k and the induction hypothesis, we obtain

$$E'_{n,k}(q) \leq a_0^2\sum_{s=1}^{n/k}\frac{(k+1)s}{(2s)^{k-1}}c_2\tilde{E}_{n-ks} \leq \frac{1}{2}c_2\tilde{E}_n$$

because the sequence $\left\{\tilde{E}_n\right\}$ is monotonic. On the other hand, Lemma 6 shows

$$\begin{aligned} E_{n,k}(q) := \sum_{\lambda\in\Pi_{n,k}} w(\lambda,q)m(\lambda) & \\ \leq a_0e^{2k(k-1)}\sum_{\lambda\in\Pi_{n,k}} w(\lambda)m(\lambda) &\leq a_0e^{2k(k-1)}E_n \leq \frac{1}{2}c_2\tilde{E}_n \end{aligned}$$

by the choice of c_2. Hence

$$E_n(q) = E_{n,k}(q) + E'_{n,k}(q) \leq c_2\tilde{E}_n$$

and the induction step is proved. ■

To complete the proof of the theorem we must prove a lower bound for $E_n(q)$. Let Λ_n denote the set of partitions π of the form:

(i) π is a partition of some integer m with $n - r < m \leq n$ where r is the smallest prime $> \sqrt{n}$;

(ii) the parts of π are distinct and each is a multiple of a different prime $> \sqrt{n}$.

Note that if the parts of π are $k_1r_1, ..., k_tr_t$ where $r_1, ..., r_t$ are distinct primes $> \sqrt{n}$ then $w(\pi)m(\pi) \geq \prod_i r_i/\left(k_ir_i\right)^1 1! = \prod_i 1/k_i$.

Consider the partitions of n which can be written in the form $\pi \vee \omega$ where $\pi \in \Lambda_n$ and $\omega \in \Pi_{n-|\pi|}$. In Sect. 3 of [9] (see especially the bottom of page 3) Stong notes (in our notation) that since π and ω are disjoint:

$$\begin{aligned} E_n &\geq \sum_{\pi\in\Lambda_n}\sum_{\omega\vdash n-|\pi|} w(\pi\vee\omega)m(\pi\vee\omega) \\ &\geq \sum_{\pi\in\Lambda_n} w(\pi)m(\pi)\sum_{\omega\vdash n-|\pi|} w(\omega) = \sum_{\pi\in\Lambda_n} w(\pi)m(\pi). \end{aligned}$$

He then proves that the last sum is greater than $E_n \exp\left(-O\left(\frac{\sqrt{n}\log\log n}{\log n}\right)\right)$.

Similarly, using Lemma 4 we obtain

$$\begin{aligned}E_n(q) &\geq \sum_{\pi\in\Lambda_n}\sum_{\omega\vdash n-|\pi|} w(\pi\vee\omega,q)m(\pi\vee\omega)\\ &\geq a_0^{-2}\sum_{\pi\in\Lambda_n} w(\pi,q)m(\pi)\sum_{\omega\vdash n-|\pi|} w(\omega,q) = a_0^{-2}\sum_{\pi\in\Lambda_n} w(\pi,q)m(\pi).\end{aligned}$$

Since each $\pi\in\Lambda_n$ has all its parts of different sizes, Lemma 6 shows that $w(\pi,q)\geq c_1 w(\pi)$, and so from the result due to Stong quoted above

$$E_n(q)\geq a_0^{-2}c_1\sum_{\pi\in\Lambda_n} w(\pi)m(\pi)\geq E_n\exp\left(-O\left(\frac{\sqrt{n}\log\log n}{\log n}\right)\right).$$

The lower bound in our theorem now follows from Stong's theorem.

References

[1] P. Erdös and P. Turán, On some problems of a statistical group theory I, *Z. Wahrschein. Verw. Gebeite* **4** (1965) 175–186.

[2] P. Erdös and P. Turán, On some problems of a statistical group theory II, *Acta Math. Acad. Sci. Hungar.* **18** (1967) 151–163.

[3] P. Erdös and P. Turán, On some problems of a statistical group theory III, *Acta Math. Acad. Sci. Hungar.* **18** (1967) 309–320.

[4] P. Erdös and P. Turán, On some problems of a statistical group theory IV, *Acta Math. Acad. Sci. Hungar.* **19** (1968) 413–435.

[5] W. Feller, "An Introduction to Probability Theory and its Applications", Vol. 1 (3rd. ed.), Wiley, New York, 1968.

[6] W. Goh and E. Schmutz, The expected order of a random permutation, *Bull. London Math. Soc.* **23** (1991) 34–42.

[7] A. Knopfmacher and R. Warlimont, Distinct degree factorizations for polynomials over a finite field, *Trans. Amer. Math. Soc.* **347** (1995) 2235–2243.

[8] R. Lidl and H. Niederreiter, "Finite Fields", Cambridge Univ. Press, 1997.

[9] R. Stong, The average order of a permutation, *Electronic J. Combinatorics* **5** (1998) #R41.