A proof of Bary-Soroker & Kozma's irreducibility theorem

Irreducibility of random polynomials study group, Week 5

Robin Visser
Mathematics Institute
University of Warwick

11 February 2022

Main theorem

Theorem (Bary-Soroker, Kozma (2017))

Let L be a positive integer divisible by at least 4 distinct primes (e.g. $L = 210$). Let

$$\mathbf{f} := X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$$

be a random polynomial over $\mathbb{Z}$, where $\mathbf{a}_0, \ldots, \mathbf{a}_{n-1}$ are independent random variables taking values uniformly in $\{1, \ldots, L\}$. Then

$$\mathbb{P}(\mathbf{f} \text{ is irreducible}) \to 1 \quad \text{as } n \to \infty$$

Sketch

- Let $\mathbf{f}_p$ denote the reduction of $\mathbf{f}$ mod p, for any prime p dividing L.

Sketch

- Let $\mathbf{f}_p$ denote the reduction of $\mathbf{f}$ mod p, for any prime p dividing L.
- Then $\mathbf{f}_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $\mathbf{f}_p$ being independent for different primes $p|L$ (by Chinese Remainder Theorem).

Sketch

- Let $\mathbf{f}_p$ denote the reduction of $\mathbf{f}$ mod p, for any prime p dividing L.
- Then $\mathbf{f}_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $\mathbf{f}_p$ being independent for different primes $p|L$ (by Chinese Remainder Theorem).
- Note that, for any prime p, $\mathbf{f}_p$ irreducible $\implies$ $\mathbf{f}$ irreducible.

Sketch

- Let $\mathbf{f}_p$ denote the reduction of $\mathbf{f}$ mod p, for any prime p dividing L.
- Then $\mathbf{f}_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $\mathbf{f}_p$ being independent for different primes $p|L$ (by Chinese Remainder Theorem).
- Note that, for any prime p, $\mathbf{f}_p$ irreducible $\implies$ $\mathbf{f}$ irreducible.
    - More specifically, if $\mathbf{f}_p$ has irreducible factors of degrees $d_1, \ldots, d_r$, then the Galois group of $\mathbf{f}$ (over $\mathbb{Q}$) has an element with cycle lengths $d_1, \ldots, d_r$.

Sketch

- Let $\mathbf{f}_p$ denote the reduction of $\mathbf{f}$ mod p, for any prime p dividing L.
- Then $\mathbf{f}_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $\mathbf{f}_p$ being independent for different primes $p|L$ (by Chinese Remainder Theorem).
- Note that, for any prime p, $\mathbf{f}_p$ irreducible $\implies$ $\mathbf{f}$ irreducible.
  - More specifically, if $\mathbf{f}_p$ has irreducible factors of degrees $d_1, \ldots, d_r$, then the Galois group of $\mathbf{f}$ (over $\mathbb{Q}$) has an element with cycle lengths $d_1, \ldots, d_r$.
- We show that the probability that $\mathbf{f}_p$ is reducible is small.

Sketch

- Let $\mathbf{f}_p$ denote the reduction of $\mathbf{f}$ mod p, for any prime p dividing L.
- Then $\mathbf{f}_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $\mathbf{f}_p$ being independent for different primes $p|L$ (by Chinese Remainder Theorem).
- Note that, for any prime p, $\mathbf{f}_p$ irreducible $\implies$ $\mathbf{f}$ irreducible.
    - More specifically, if $\mathbf{f}_p$ has irreducible factors of degrees $d_1, \ldots, d_r$, then the Galois group of $\mathbf{f}$ (over $\mathbb{Q}$) has an element with cycle lengths $d_1, \ldots, d_r$.
- We show that the probability that $\mathbf{f}_p$ is reducible is small.
- Therefore, we hope to show that the probabilities that $\mathbf{f}_{p_1}, \mathbf{f}_{p_2}, \mathbf{f}_{p_3}, \mathbf{f}_{p_4}$ are all (compatibly w.r.t. cycle lengths) reducible, for four distinct primes $p_1, \ldots, p_4$ dividing L, is *very* small.

Sketch

- Let $\mathbf{f}_p$ denote the reduction of $\mathbf{f}$ mod p, for any prime p dividing L.
- Then $\mathbf{f}_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $\mathbf{f}_p$ being independent for different primes $p|L$ (by Chinese Remainder Theorem).
- Note that, for any prime p, $\mathbf{f}_p$ irreducible $\implies$ $\mathbf{f}$ irreducible.
    - More specifically, if $\mathbf{f}_p$ has irreducible factors of degrees $d_1, \ldots, d_r$, then the Galois group of $\mathbf{f}$ (over $\mathbb{Q}$) has an element with cycle lengths $d_1, \ldots, d_r$.
- We show that the probability that $\mathbf{f}_p$ is reducible is small.
- Therefore, we hope to show that the probabilities that $\mathbf{f}_{p_1}, \mathbf{f}_{p_2}, \mathbf{f}_{p_3}, \mathbf{f}_{p_4}$ are all (compatibly w.r.t. cycle lengths) reducible, for four distinct primes $p_1, \ldots, p_4$ dividing L, is *very* small.
- We prove this by considering the small and large divisors separately.

Proof for 12 primes

Proof for 12 primes

- Let L be divisible by 12 distinct primes (e.g. $L = 7\,420\,738\,134\,810$), and let $\mathbf{f}$ be a random polynomial with i.i.d. uniform random coefficients in $\{1, \ldots, L\}$.

Proof for 12 primes

- Let L be divisible by 12 distinct primes (e.g. $L = 7\,420\,738\,134\,810$), and let $\mathbf{f}$ be a random polynomial with i.i.d. uniform random coefficients in $\{1, \ldots, L\}$.
- For 12 distinct primes $p_1, \ldots, p_{12}$ dividing L, let $\mathbf{f}_{p_i} := \mathbf{f} \bmod p_i$.

Proof for 12 primes

- Let L be divisible by 12 distinct primes (e.g. $L = 7\,420\,738\,134\,810$), and let $\mathbf{f}$ be a random polynomial with i.i.d. uniform random coefficients in $\{1, \ldots, L\}$.
- For 12 distinct primes $p_1, \ldots, p_{12}$ dividing L, let $\mathbf{f}_{p_i} := \mathbf{f} \bmod p_i$.
- Let $k < n$. By Meisner [3], the probability that $\mathbf{f}_{p_i}$ has a divisor of degree k is $k^{-\delta+o(1)}$ where $\delta = 1 - \frac{1+\log\log 2}{\log 2} = 0.086\ldots$.

Proof for 12 primes

- Let L be divisible by 12 distinct primes (e.g. $L = 7\,420\,738\,134\,810$), and let $\mathbf{f}$ be a random polynomial with i.i.d. uniform random coefficients in $\{1, \dots, L\}$.
- For 12 distinct primes $p_1, \dots, p_{12}$ dividing L, let $\mathbf{f}_{p_i} := \mathbf{f} \bmod p_i$.
- Let $k < n$. By Meisner [3], the probability that $\mathbf{f}_{p_i}$ has a divisor of degree k is $k^{-\delta+o(1)}$ where $\delta = 1 - \frac{1+\log\log 2}{\log 2} = 0.086\dots$.
- By independence, the probability that $\mathbf{f}$ has a divisor of degree k is

$$\begin{aligned}\mathbb{P}(\mathbf{f}\ \textit{has factor of degree}\ k) &\leq \prod_{i=1}^{12} \mathbb{P}(\mathbf{f}_{p_i}\ \textit{has factor of degree}\ k) \\ &= k^{-12\delta+o(1)} = k^{-1.03\ldots+o(1)}\end{aligned}$$

Proof for 12 primes

- By summing over sufficiently large k (say $k \geq n^{1/10}$), we obtain the bound

$$\mathbb{P}(\mathbf{f} \textit{ has factor of degree} \geq n^{1/10}) \ll \sum_{k \geq n^{1/10}} k^{-1.03\ldots+o(1)} \ll n^{-0.003\ldots+o(1)}$$

Proof for 12 primes

- By summing over sufficiently large k (say $k \geq n^{1/10}$), we obtain the bound

$$\mathbb{P}(\mathbf{f} \textit{ has factor of degree} \geq n^{1/10}) \ll \sum_{k \geq n^{1/10}} k^{-1.03\ldots+o(1)} \ll n^{-0.003\ldots+o(1)}$$

- Finally, by showing that the small divisors contribute negligibly, this proves that $\mathbb{P}(\mathbf{f} \textit{ reducible}) \to 0$ as $n \to \infty$.

Small divisors (Lemma 7)

Lemma ("small divisors are negligible")

Let $L \geq 2$ *and* $\mathbf{f} = X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$ *where as before* $\mathbf{a}_i$ *are i.i.d uniform random variables. Then there exists a* $\omega : \mathbb{N} \to \mathbb{N}$ *with* $\lim_{n\to\infty} \omega(n) = \infty$ *such that*

$$\mathbb{P}(\mathbf{f} \textit{ has a divisor of degree} \leq \omega(n)) \to 0 \quad \textit{as } n \to \infty$$

Several proofs of this lemma exist:

Small divisors (Lemma 7)

Lemma ("small divisors are negligible")

Let $L \geq 2$ *and* $\mathbf{f} = X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$ *where as before* $\mathbf{a}_i$ *are i.i.d uniform random variables. Then there exists a* $\omega : \mathbb{N} \to \mathbb{N}$ *with* $\lim_{n\to\infty} \omega(n) = \infty$ *such that*

$$\mathbb{P}(\mathbf{f} \textit{ has a divisor of degree} \leq \omega(n)) \to 0 \quad \textit{as } n \to \infty$$

Several proofs of this lemma exist:

- $\omega(n) = n/\log n$, Konyagin 1999.
- $\omega(n) = \sqrt{\log n}$, O'Rourke, Wood 2016.
- ω exists, Kozma, Zeitouni, 2013.
- $\omega(n) = \theta n$, Bary-Soroker, Koukoulopoulos, Kozma, 2020.

Proof of Lemma 7

Observation 1

Let $L \geq 1$. Then for every d, there are only finitely many irreducible polynomials of degree d which can divide a monic polynomial (of arbitrary degree) with coefficients in $\{1, \ldots, L\}$.

Proof of Lemma 7

Observation 1

Let $L \geq 1$. Then for every d, there are only finitely many irreducible polynomials of degree d which can divide a monic polynomial (of arbitrary degree) with coefficients in $\{1, \ldots, L\}$.

- Let $p(x) := X^d + b_{d-1}X^{d-1} + \cdots + b_1 X + b_0 \in \mathbb{Z}[x]$ be such a polynomial which divides some f with coefficients in $\{1, \ldots, L\}$, and let $z \in \overline{\mathbb{Z}}$ be a root of p.

Proof of Lemma 7

Observation 1

Let $L \geq 1$. Then for every d, there are only finitely many irreducible polynomials of degree d which can divide a monic polynomial (of arbitrary degree) with coefficients in $\{1, \ldots, L\}$.

- Let $p(x) := X^d + b_{d-1}X^{d-1} + \cdots + b_1 X + b_0 \in \mathbb{Z}[x]$ be such a polynomial which divides some f with coefficients in $\{1, \ldots, L\}$, and let $z \in \overline{\mathbb{Z}}$ be a root of p.
- As z divides a polynomial with coefficients in $\{1, \ldots, L\}$, then $|z| \leq L + 1$, otherwise

$$|z|^n > |L+1|^n > \sum_{i=0}^{n-1} |a_i z^i| \geq |f(z) - z^n|$$

Proof of Lemma 7

Observation 1

Let $L \geq 1$. Then for every d, there are only finitely many irreducible polynomials of degree d which can divide a monic polynomial (of arbitrary degree) with coefficients in $\{1, \ldots, L\}$.

- Let $p(x) := X^d + b_{d-1}X^{d-1} + \cdots + b_1 X + b_0 \in \mathbb{Z}[x]$ be such a polynomial which divides some f with coefficients in $\{1, \ldots, L\}$, and let $z \in \overline{\mathbb{Z}}$ be a root of p.
- As z divides a polynomial with coefficients in $\{1, \ldots, L\}$, then $|z| \leq L + 1$, otherwise

$$|z|^n > |L+1|^n > \sum_{i=0}^{n-1} |a_i z^i| \geq |f(z) - z^n|$$

- We can similarly derive a contradiction if $|z| < \frac{1}{L+1}$.

Proof of Lemma 7

- Using the bound $|z_j| \leq L + 1$ for all roots z_j of p, we can apply standard relations between the coefficients b_i and the roots z_i, we obtain the bound

$$|b_{d-k}| = \left| \sum_{1 \leq i_1 < \cdots < i_k \leq d} \prod_{j=1}^{k} z_{i_j} \right| \leq \binom{d}{k} (L+1)^k$$

for each $k = 1, \ldots, d - 1$.

Proof of Lemma 7

- Using the bound $|z_j| \leq L+1$ for all roots z_j of p, we can apply standard relations between the coefficients b_i and the roots z_i, we obtain the bound

$$|b_{d-k}| = \left| \sum_{1 \leq i_1 < \cdots < i_k \leq d} \prod_{j=1}^{k} z_{i_j} \right| \leq \binom{d}{k} (L+1)^k$$

  for each $k = 1, \ldots, d-1$.

- Thus, there are only finitely many possibilities for each coefficients b_i, and so finitely many possible irreducible polynomials $p(x)$.

  (e.g. a rather crude bound is $(2(L+1))^{d^2}$)

Proof of Lemma 7

Observation 2

Let p be some fixed irreducible polynomial, and $\mathbf{f}$ as defined in Theorem 1. Then

$$\mathbb{P}(p \textit{ divides } \mathbf{f}) = O(\frac{1}{\sqrt{n}})$$

Proof of Lemma 7

Observation 2

Let p be some fixed irreducible polynomial, and $\mathbf{f}$ as defined in Theorem 1. Then

$$\mathbb{P}(p \textit{ divides } \mathbf{f}) = O(\frac{1}{\sqrt{n}})$$

This essentially follows from the classical Littlewood-Offord bound, a weak form of which states the following:

Littlewood-Offord (1943) (simplified)

Let $n \geq 1$, and let $x_1, \ldots, x_n$ be any non-zero complex numbers.
Let $\epsilon_1, \ldots, \epsilon_n$ be i.i.d. uniform random variables in $\{-1, +1\}$. Then the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is $O(\frac{1}{\sqrt{n}})$

Proof of Lemma 7

Observation 2

Let p be some fixed irreducible polynomial, and $\mathbf{f}$ as defined in Theorem 1. Then

$$\mathbb{P}(p \textit{ divides } \mathbf{f}) = O(\frac{1}{\sqrt{n}})$$

This essentially follows from the classical Littlewood-Offord bound, a weak form of which states the following:

Littlewood-Offord (1943) (simplified)

Let $n \geq 1$, and let $x_1, \ldots, x_n$ be any non-zero complex numbers.
Let $\epsilon_1, \ldots, \epsilon_n$ be i.i.d. uniform random variables in $\{-1, +1\}$. Then the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is $O(\frac{1}{\sqrt{n}})$

- More generally, Littlewood-Offord actually obtained a bound for the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n \in I$ for a given bounded set I.

Proof of (weak) Littlewood-Offord

- We may assume wlog that x_i are real and furthermore that $x_i > 0$ for all i.

Proof of (weak) Littlewood-Offord

- We may assume wlog that x_i are real and furthermore that $x_i > 0$ for all i.
- Let $\mathcal{A} := \left\{A \subseteq \{1, \ldots, n\} \mid \sum_{i \in A} x_i - \sum_{j \notin A} x_j = 0\right\}$.

Proof of (weak) Littlewood-Offord

- We may assume wlog that x_i are real and furthermore that $x_i > 0$ for all i.
- Let $\mathcal{A} := \left\{A \subseteq \{1, \ldots, n\} \mid \sum_{i \in A} x_i - \sum_{j \notin A} x_j = 0\right\}$.
- We note that $\mathcal{A}$ is an anti-chain, i.e. for all distinct $A, B \in \mathcal{A}$, $A \not\subseteq B$.

Proof of (weak) Littlewood-Offord

- We may assume wlog that x_i are real and furthermore that $x_i > 0$ for all i.
- Let $\mathcal{A} := \left\{A \subseteq \{1, \ldots, n\} \mid \sum_{i \in A} x_i - \sum_{j \notin A} x_j = 0\right\}$.
- We note that $\mathcal{A}$ is an anti-chain, i.e. for all distinct $A, B \in \mathcal{A}$, $A \not\subseteq B$.
- Thus, by Sperner's lemma, $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$, which by Stirling, has bound $O(\frac{2^n}{\sqrt{n}})$.

Proof of (weak) Littlewood-Offord

- We may assume wlog that x_i are real and furthermore that $x_i > 0$ for all i.
- Let $\mathcal{A} := \left\{A \subseteq \{1, \ldots, n\} \mid \sum_{i \in A} x_i - \sum_{j \notin A} x_j = 0\right\}$.
- We note that $\mathcal{A}$ is an anti-chain, i.e. for all distinct $A, B \in \mathcal{A}$, $A \not\subseteq B$.
- Thus, by Sperner's lemma, $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$, which by Stirling, has bound $O(\frac{2^n}{\sqrt{n}})$.
- Therefore, the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is $O(\frac{1}{\sqrt{n}})$.

Proof of (weak) Littlewood-Offord

- We may assume wlog that x_i are real and furthermore that $x_i > 0$ for all i.
- Let $\mathcal{A} := \left\{A \subseteq \{1, \ldots, n\} \mid \sum_{i \in A} x_i - \sum_{j \notin A} x_j = 0\right\}$.
- We note that $\mathcal{A}$ is an anti-chain, i.e. for all distinct $A, B \in \mathcal{A}$, $A \not\subseteq B$.
- Thus, by Sperner's lemma, $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$, which by Stirling, has bound $O(\frac{2^n}{\sqrt{n}})$.
- Therefore, the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is $O(\frac{1}{\sqrt{n}})$.

Remark: This is sharp! (at least for arbitrary $x_i \in \mathbb{C}$), as if $x_1 = \cdots = x_n = 1$, then the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is equivalent to the probability that a one-dimensional random walk starting at 0, ends at 0 after n steps. This is $\Theta(\binom{n}{n/2}/2^n) = \Theta(\frac{1}{\sqrt{n}})$.

Proof of Lemma 7

Back to the original proof:

- Let p be some fixed irreducible polynomial, and let $z \in \mathbb{C}$ be a root of p.

Proof of Lemma 7

Back to the original proof:

- Let p be some fixed irreducible polynomial, and let $z \in \mathbb{C}$ be a root of p.
- Applying the (generalised) Littlewood-Offord bound with the random variables $\mathbf{a}_i$ and $x_i = z^i$. Then we have

$$\mathbb{P}(p \textit{ divides } \mathbf{f}) = \mathbb{P}(z^n + \mathbf{a}_{n-1} z^{n-1} + \cdots + \mathbf{a}_0 = 0) = O\left(\frac{1}{\sqrt{n}}\right)$$

Proof of Lemma 7

Back to the original proof:

- Let p be some fixed irreducible polynomial, and let $z \in \mathbb{C}$ be a root of p.
- Applying the (generalised) Littlewood-Offord bound with the random variables $\mathbf{a}_i$ and $x_i = z^i$. Then we have

$$\mathbb{P}(p \textit{ divides } \mathbf{f}) = \mathbb{P}(z^n + \mathbf{a}_{n-1} z^{n-1} + \cdots + \mathbf{a}_0 = 0) = O\left(\frac{1}{\sqrt{n}}\right)$$

- Thus, for any fixed degree $d \geq 1$, we have

$$\mathbb{P}(\mathbf{f} \textit{ has a divisor of degree } d) \ll \frac{(2L+2)^{d^2}}{\sqrt{n}}$$

Proof of Lemma 7

- Therefore, for any fixed $W > 0$, we have

$$\begin{aligned}\mathbb{P}(\mathbf{f} \textit{ has a divisor of degree } \leq W) &\ll \frac{1}{\sqrt{n}} \sum_{d=1}^{W} (2L+2)^{d^2} \\ &\leq \frac{1}{\sqrt{n}} W (2L+2)^{W^2}\end{aligned}$$

which tends to 0 as $n \to \infty$.

Proof of Lemma 7

- Therefore, for any fixed $W > 0$, we have

$$\mathbb{P}(\mathbf{f} \textit{ has a divisor of degree } \leq W) \ll \frac{1}{\sqrt{n}} \sum_{d=1}^{W} (2L+2)^{d^2} \leq \frac{1}{\sqrt{n}} W (2L+2)^{W^2}$$

  which tends to 0 as $n \to \infty$.
- The result also holds if W grows sufficiently slowly (e.g. $\omega(n) = (\log n)^{1/3}$ works). $\square$

Large divisors (Lemma 8)

Lemma (Bary-Soroker, Kozma (2017))

Let $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \boldsymbol{\sigma}_3, \boldsymbol{\sigma}_4$ be 4 independent uniform permutations in S_n. For $i \in \{1, \ldots, 4\}$ and $\ell \leq n$ we define $\mathbf{E}_{i,\ell}$ as the event that ℓ can be written as a sum of lengths of cycles of $\boldsymbol{\sigma}_i$. Then for all $k < n$,

$$\mathbb{P}\Big(\bigcup_{\ell=k}^{2k} \bigcap_{i=1}^{4} \mathbf{E}_{i,\ell}\Big) \leq Ck^{-c}$$

for some effective constant c, C independent of n and k.
Furthermore, for an additional parameter λ,

$$\mathbb{P}\Big(\bigcup_{\ell=k}^{2k} \bigcup_{\lambda_1=0}^{\lambda} \cdots \bigcup_{\lambda_4=0}^{\lambda} \bigcap_{i=1}^{4} \mathbf{E}_{i,\ell-\lambda_i}\Big) \leq C(\lambda+1)^4 k^{-c}$$

Proof of Lemma 8

- Wlog let k be sufficiently large, and let $\lambda < \frac{k}{2}$. Let $0 < \epsilon < \frac{1}{2}$.

Proof of Lemma 8

- Wlog let k be sufficiently large, and let $\lambda < \frac{k}{2}$. Let $0 < \epsilon < \frac{1}{2}$.
- Define $\mathbf{B}_{i,k,\epsilon}$ as the event that $\boldsymbol{\sigma}_i$ has at least $(1+\epsilon)\log k$ cycles whose sizes are less than k.

Proof of Lemma 8

- Wlog let k be sufficiently large, and let $\lambda < \frac{k}{2}$. Let $0 < \epsilon < \frac{1}{2}$.
- Define $\mathbf{B}_{i,k,\epsilon}$ as the event that $\boldsymbol{\sigma}_i$ has at least $(1+\epsilon)\log k$ cycles whose sizes are less than k.
- We shall use the following two facts (maybe proven later?):

(P1) $\mathbb{P}(\mathbf{B}_{i,k,\epsilon}) \ll k^{-\epsilon^2/3}$.
(P2) $\mathbb{P}(\mathbf{E}_{i,k} \backslash \mathbf{B}_{i,k,\epsilon}) \ll k^{\log 2 - 1 + 2\epsilon}$.

Proof of Lemma 8

- Wlog let k be sufficiently large, and let $\lambda < \frac{k}{2}$. Let $0 < \epsilon < \frac{1}{2}$.
- Define $\mathbf{B}_{i,k,\epsilon}$ as the event that $\boldsymbol{\sigma}_i$ has at least $(1+\epsilon)\log k$ cycles whose sizes are less than k.
- We shall use the following two facts (maybe proven later?):

(P1) $\mathbb{P}(\mathbf{B}_{i,k,\epsilon}) \ll k^{-\epsilon^2/3}$.
(P2) $\mathbb{P}(\mathbf{E}_{i,k} \backslash \mathbf{B}_{i,k,\epsilon}) \ll k^{\log 2 - 1 + 2\epsilon}$.

- By noting that $\mathbf{B}_{i,\ell,\epsilon}$ implies $\mathbf{B}_{i,2k,\epsilon/2}$ for sufficiently large k and $\ell \in [k/2, 2k]$, we therefore obtain the bound

$$\mathbb{P}\Big(\bigcup_{\ell=k}^{2k} \bigcap_{i=1}^{4} \mathbf{E}_{i,\ell}\Big) \leq \sum_{i=1}^{4} \mathbb{P}(\mathbf{B}_{i,2k,\epsilon/2}) + \sum_{\ell=k}^{2k} \prod_{i=1}^{4} \mathbb{P}(\mathbf{E}_{i,\ell} \backslash \mathbf{B}_{i,\ell,\epsilon})$$

Proof of Lemma 8

- Applying the bounds (P1) and (P2), this gives us

$$\mathbb{P}\Big(\bigcup_{\ell=k}^{2k}\bigcap_{i=1}^{4}\mathbf{E}_{i,\ell}\Big) \ll 4k^{-\epsilon^2/12} + k^{1+4(\log 2-1+2\epsilon)}$$

Proof of Lemma 8

- Applying the bounds (P1) and (P2), this gives us

$$\mathbb{P}\Big(\bigcup_{\ell=k}^{2k}\bigcap_{i=1}^{4}\mathbf{E}_{i,\ell}\Big) \ll 4k^{-\epsilon^2/12} + k^{1+4(\log 2-1+2\epsilon)}$$

- By letting ϵ be small enough (e.g. $\epsilon = 0.02$), we have that $1 + 4(\log 2 - 1 + 2\epsilon) < 0$, and thus the first result holds for

$$c = \min(\epsilon^2/12, -1 - 4(\log 2 - 1 + 2\epsilon))$$

Proof of Lemma 8

The second estimate can be obtained by essentially the same argument:

$$
\begin{aligned}
P := \mathbb{P}\Big(\bigcup_{\ell=k}^{2k}\bigcup_{\lambda_1=0}^{\lambda}\cdots\bigcup_{\lambda_4=0}^{\lambda}\bigcap_{i=1}^{4}\mathbf{E}_{i,\ell-\lambda_i}\Big) &\leq \\
&\leq \sum_{i=1}^{4}\mathbb{P}(\mathbf{B}_{i,2k,\epsilon/2}) + \sum_{\ell=k}^{2k}\sum_{\lambda_1=0}^{\lambda}\cdots\sum_{\lambda_4=0}^{\lambda}\prod_{i=1}^{4}\mathbb{P}(\mathbf{E}_{i,\ell-\lambda_i}\backslash\mathbf{B}_{i,\ell-\lambda_i,\epsilon}) \\
&\ll 4k^{-\epsilon^2/12} + (\lambda+1)^4\sum_{\ell=k/2}^{2k} k^{4(\log 2-1+2\epsilon)} \\
&\ll (\lambda+1)^4 k^{-c}
\end{aligned}
$$

where as before $c = \min(\epsilon^2/12, -1-4(\log 2 - 1 + 2\epsilon))$. $\square$

Proof of main theorem

Theorem (Bary-Soroker, Kozma (2017))

Let L be a positive integer divisible by at least 4 distinct primes. Let $\mathbf{f} = X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$ where $\mathbf{a}_0, \ldots, \mathbf{a}_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(\mathbf{f}$ is irreducible$) \to 1$,as $n \to \infty$.

Proof of main theorem

Theorem (Bary-Soroker, Kozma (2017))

Let L be a positive integer divisible by at least 4 distinct primes. Let $\mathbf{f} = X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$ where $\mathbf{a}_0, \ldots, \mathbf{a}_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(\mathbf{f}$ is irreducible$) \to 1$,as $n \to \infty$.

- Fix some k sufficiently large. We shall consider divisors of degree $k < \ell < 2k$.

Proof of main theorem

Theorem (Bary-Soroker, Kozma (2017))

Let L be a positive integer divisible by at least 4 distinct primes. Let $\mathbf{f} = X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$ where $\mathbf{a}_0, \ldots, \mathbf{a}_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(\mathbf{f}$ is irreducible$) \to 1$, as $n \to \infty$.

- Fix some k sufficiently large. We shall consider divisors of degree $k < \ell < 2k$.
- Let $p_1, \ldots, p_4$ be 4 distinct primes dividing L, and define $\mathbf{f}_{p_i}$ as the reduction of $\mathbf{f}$ mod p_i.

Proof of main theorem

Theorem (Bary-Soroker, Kozma (2017))

Let L be a positive integer divisible by at least 4 distinct primes. Let $\mathbf{f} = X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$ where $\mathbf{a}_0, \ldots, \mathbf{a}_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(\mathbf{f}$ is irreducible$) \to 1$,as $n \to \infty$.

- Fix some k sufficiently large. We shall consider divisors of degree $k < \ell < 2k$.
- Let $p_1, \ldots, p_4$ be 4 distinct primes dividing L, and define $\mathbf{f}_{p_i}$ as the reduction of $\mathbf{f}$ mod p_i.
- For $r = 1, \ldots, 4$, define $\mathbf{X}_r$ as the random tuple which takes the value $(\mathbf{m}_{1,r}, \mathbf{m}_{2,r}, \ldots)$ where $\mathbf{m}_{i,r}$ is the number of irreducible factors of $\mathbf{f}_{p_r}$ of degree i.

Proof of main theorem

Theorem (Bary-Soroker, Kozma (2017))

Let L be a positive integer divisible by at least 4 distinct primes. Let $\mathbf{f} = X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$ where $\mathbf{a}_0, \ldots, \mathbf{a}_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(\mathbf{f}$ is irreducible$) \to 1$, as $n \to \infty$.

- Fix some k sufficiently large. We shall consider divisors of degree $k < \ell < 2k$.
- Let $p_1, \ldots, p_4$ be 4 distinct primes dividing L, and define $\mathbf{f}_{p_i}$ as the reduction of $\mathbf{f}$ mod p_i.
- For $r = 1, \ldots, 4$, define $\mathbf{X}_r$ as the random tuple which takes the value $(\mathbf{m}_{1,r}, \mathbf{m}_{2,r}, \ldots)$ where $\mathbf{m}_{i,r}$ is the number of irreducible factors of $\mathbf{f}_{p_r}$ of degree i.
- Analogously, let $\boldsymbol{\sigma}$ be a random permutation in S_n, and define $\mathbf{Y}$ as the random tuple $(\mathbf{n}_1, \mathbf{n}_2, \ldots)$ where $\mathbf{n}_i$ is the number of cycles of $\boldsymbol{\sigma}$ of length i.

Proof of main theorem

- Now first, we let $\mathbf{B}_k$ be the event that for some $r = 1, \ldots, 4$ and some $i < \log^2 k$ we have $\mathbf{m}_{i,r} < \log^2 k$

Proof of main theorem

- Now first, we let $\mathbf{B}_k$ be the event that for some $r = 1, \ldots, 4$ and some $i < \log^2 k$ we have $\mathbf{m}_{i,r} < \log^2 k$
- We have the bound $\mathbb{P}(\mathbf{B}_k) \ll 4 \log^2 k \, e^{-c \log^2 k}$ (next week), thus $\mathbf{B}_k$ occurs negligibly.

Proof of main theorem

- Now first, we let $\mathbf{B}_k$ be the event that for some $r = 1, \ldots, 4$ and some $i < \log^2 k$ we have $\mathbf{m}_{i,r} < \log^2 k$
- We have the bound $\mathbb{P}(\mathbf{B}_k) \ll 4 \log^2 k \, e^{-c \log^2 k}$ (next week), thus $\mathbf{B}_k$ occurs negligibly.
- Let $\mathbf{R}_k$ be the event that for some $k \leq \ell < 2k$ and some $\lambda_r < \log^6 k$ we can write

$$\ell - \lambda_r = \sum_{i > \log^2 k} i \ell_{i,r}, \quad \ell_{i,r} \leq \mathbf{m}_{i,r}$$

for all $r = 1, \ldots, 4$.

Proof of main theorem

- Now first, we let $\mathbf{B}_k$ be the event that for some $r = 1, \ldots, 4$ and some $i < \log^2 k$ we have $\mathbf{m}_{i,r} < \log^2 k$
- We have the bound $\mathbb{P}(\mathbf{B}_k) \ll 4 \log^2 k \, e^{-c \log^2 k}$ (next week), thus $\mathbf{B}_k$ occurs negligibly.
- Let $\mathbf{R}_k$ be the event that for some $k \leq \ell < 2k$ and some $\lambda_r < \log^6 k$ we can write

$$\ell - \lambda_r = \sum_{i > \log^2 k} i \ell_{i,r}, \quad \ell_{i,r} \leq \mathbf{m}_{i,r}$$

  for all $r = 1, \ldots, 4$.
- Similarly, let $\mathbf{S}_k$ be the event that for some $k \leq \ell < 2k$ and some $\lambda < \log^6 k$ we can write

$$\ell - \lambda = \sum_{i > \log^2 k} i \ell_i, \quad \ell_i \leq \mathbf{n}_i.$$

Proof of main theorem

- We now use that $\mathbf{X}_r$ and $\mathbf{Y}$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(\mathbf{R}_k) - \mathbb{P}(\mathbf{S}_k)| \ll 1/\log^2 k$.

Proof of main theorem

- We now use that $\mathbf{X}_r$ and $\mathbf{Y}$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(\mathbf{R}_k) - \mathbb{P}(\mathbf{S}_k)| \ll 1/\log^2 k$.
- By Lemma 8, we have $\mathbb{P}(\mathbf{S}_k) \ll k^{-c} \log^{24} k$.

Proof of main theorem

- We now use that $\mathbf{X}_r$ and $\mathbf{Y}$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(\mathbf{R}_k) - \mathbb{P}(\mathbf{S}_k)| \ll 1/\log^2 k$.
- By Lemma 8, we have $\mathbb{P}(\mathbf{S}_k) \ll k^{-c} \log^{24} k$.
- This implies $\mathbb{P}(\mathbf{R}_k) \ll 1/\log^2 k$.

Proof of main theorem

- We now use that $\mathbf{X}_r$ and $\mathbf{Y}$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(\mathbf{R}_k) - \mathbb{P}(\mathbf{S}_k)| \ll 1/\log^2 k$.
- By Lemma 8, we have $\mathbb{P}(\mathbf{S}_k) \ll k^{-c}\log^{24} k$.
- This implies $\mathbb{P}(\mathbf{R}_k) \ll 1/\log^2 k$.
- Now, let $\mathbf{Q}_k$ be the event that for some $k \leq \ell < 2k$ we can write $\ell = \sum i\ell_{i,r}$ for some $\ell_{i,r} \leq \mathbf{m}_{i,r}$, for all $r = 1, \ldots, 4$.

Proof of main theorem

- We now use that $\mathbf{X}_r$ and $\mathbf{Y}$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(\mathbf{R}_k) - \mathbb{P}(\mathbf{S}_k)| \ll 1/\log^2 k$.
- By Lemma 8, we have $\mathbb{P}(\mathbf{S}_k) \ll k^{-c} \log^{24} k$.
- This implies $\mathbb{P}(\mathbf{R}_k) \ll 1/\log^2 k$.

- Now, let $\mathbf{Q}_k$ be the event that for some $k \leq \ell < 2k$ we can write $\ell = \sum i\ell_{i,r}$ for some $\ell_{i,r} \leq \mathbf{m}_{i,r}$, for all $r = 1, \ldots, 4$.
- As $\mathbf{Q}_k \backslash \mathbf{B}_k$ is contained in the event $\mathbf{R}_k$, this implies $\mathbb{P}(\mathbf{Q}_k \backslash \mathbf{B}_k) \ll 1/\log^2 k$.

Proof of main theorem

- We now use that $\mathbf{X}_r$ and $\mathbf{Y}$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(\mathbf{R}_k) - \mathbb{P}(\mathbf{S}_k)| \ll 1/\log^2 k$.
- By Lemma 8, we have $\mathbb{P}(\mathbf{S}_k) \ll k^{-c} \log^{24} k$.
- This implies $\mathbb{P}(\mathbf{R}_k) \ll 1/\log^2 k$.

- Now, let $\mathbf{Q}_k$ be the event that for some $k \leq \ell < 2k$ we can write $\ell = \sum i\ell_{i,r}$ for some $\ell_{i,r} \leq \mathbf{m}_{i,r}$, for all $r = 1, \ldots, 4$.
- As $\mathbf{Q}_k \backslash \mathbf{B}_k$ is contained in the event $\mathbf{R}_k$, this implies $\mathbb{P}(\mathbf{Q}_k \backslash \mathbf{B}_k) \ll 1/\log^2 k$.
- Finally, as $\mathbf{B}_k$ is negligible, we have $\mathbb{P}(\mathbf{Q}_k) \ll 1/\log^2 k$.

Proof of main theorem

- We now use that $\mathbf{X}_r$ and $\mathbf{Y}$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(\mathbf{R}_k) - \mathbb{P}(\mathbf{S}_k)| \ll 1/\log^2 k$.
- By Lemma 8, we have $\mathbb{P}(\mathbf{S}_k) \ll k^{-c}\log^{24} k$.
- This implies $\mathbb{P}(\mathbf{R}_k) \ll 1/\log^2 k$.

- Now, let $\mathbf{Q}_k$ be the event that for some $k \le \ell < 2k$ we can write $\ell = \sum i\ell_{i,r}$ for some $\ell_{i,r} \le \mathbf{m}_{i,r}$, for all $r = 1, \ldots, 4$.
- As $\mathbf{Q}_k \backslash \mathbf{B}_k$ is contained in the event $\mathbf{R}_k$, this implies $\mathbb{P}(\mathbf{Q}_k \backslash \mathbf{B}_k) \ll 1/\log^2 k$.
- Finally, as $\mathbf{B}_k$ is negligible, we have $\mathbb{P}(\mathbf{Q}_k) \ll 1/\log^2 k$.

Therefore, $\mathbb{P}(\mathbf{f} \textit{ has divisor of degree} \in [k, 2k)) \ll \frac{1}{\log^2 k}$

Proof of main theorem

Finally, summing over all possible divisors, this proves

$$\begin{aligned}
\mathbb{P}(\mathbf{f}\ \textit{reducible}) &\le \mathbb{P}(\mathbf{f}\ \textit{has divisors of degree} \le \omega(n)) \\
&\quad + \sum_{\substack{k=\omega(n)\cdot 2^i \\ i=0,\dots,\log_2 n}} \mathbb{P}(\mathbf{f}\ \textit{has divisors of degree} \in [k, 2k)) \\
&\ll (\textit{something small}) + \sum_{\substack{k=\omega(n)\cdot 2^i \\ i=0,\dots,\log_2 n}} \frac{1}{\log^2 k} \\
&\ll \frac{1}{\log \omega(n)} - \frac{1}{\log \omega(n) + \log n} \\
&\to 0 \quad \textit{as } n \to \infty.
\end{aligned}$$

Proof of main theorem

Finally, summing over all possible divisors, this proves

$$\begin{aligned}
\mathbb{P}(\mathbf{f}\ \textit{reducible}) &\leq \mathbb{P}(\mathbf{f}\ \textit{has divisors of degree} \leq \omega(n)) \\
&\quad + \sum_{\substack{k=\omega(n)\cdot 2^i \\ i=0,\dots,\log_2 n}} \mathbb{P}(\mathbf{f}\ \textit{has divisors of degree} \in [k, 2k)) \\
&\ll (\textit{something small}) + \sum_{\substack{k=\omega(n)\cdot 2^i \\ i=0,\dots,\log_2 n}} \frac{1}{\log^2 k} \\
&\ll \frac{1}{\log \omega(n)} - \frac{1}{\log \omega(n) + \log n} \\
&\to 0 \quad \textit{as } n \to \infty.
\end{aligned}$$

E.g. Using Konyagin's bound for $\omega(n)$, we have $\mathbb{P}(\mathbf{f}\ \textit{reducible}) \ll \frac{1}{\log n}$. □

Recent developments

Theorem (Bary-Soroker, Koukoulopoulos, Kozma (2020))

Let $L \geq 35$*, and let* $\mathbf{f} = X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$ *where* $\mathbf{a}_0, \ldots, \mathbf{a}_{n-1}$ *are i.i.d random variables taking values uniformly in* $\{1, \ldots, L\}$*. Then* $\mathbb{P}(\mathbf{f}$ *is irreducible*$) \to 1$*, as* $n \to \infty$.

Recent developments

Theorem (Bary-Soroker, Koukoulopoulos, Kozma (2020))

Let $L \geq 35$, and let $\mathbf{f} = X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$ where $\mathbf{a}_0, \ldots, \mathbf{a}_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(\mathbf{f}$ is irreducible$) \to 1$, as $n \to \infty$.

- This was proven using a combination of a standard argument for $L \geq 33\,730$ and a computer-assisted proof for $35 \leq L < 33\,730$.

Recent developments

Theorem (Bary-Soroker, Koukoulopoulos, Kozma (2020))

Let $L \geq 35$, and let $\mathbf{f} = X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$ where $\mathbf{a}_0, \ldots, \mathbf{a}_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(\mathbf{f}$ is irreducible$) \to 1$, as $n \to \infty$.

- This was proven using a combination of a standard argument for $L \geq 33\,730$ and a computer-assisted proof for $35 \leq L < 33\,730$.
- Here, $\mathbf{f}_p$ does not have uniformly distributed coefficients mod p nor independence necessarily, and so Bary-Soroker–Koukoulopoulos–Kozma use p-adic Fourier Analysis and the large sieve to prove approximate equidistribution modulo 4 primes.

Recent developments

Theorem (Bary-Soroker, Koukoulopoulos, Kozma (2020))

Let $L \geq 35$, and let $\mathbf{f} = X^n + \mathbf{a}_{n-1}X^{n-1} + \cdots + \mathbf{a}_1 X + \mathbf{a}_0$ where $\mathbf{a}_0, \ldots, \mathbf{a}_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(\mathbf{f}$ is irreducible$) \to 1$, as $n \to \infty$.

- This was proven using a combination of a standard argument for $L \geq 33\,730$ and a computer-assisted proof for $35 \leq L < 33\,730$.
- Here, $\mathbf{f}_p$ does not have uniformly distributed coefficients mod p nor independence necessarily, and so Bary-Soroker–Koukoulopoulos–Kozma use p-adic Fourier Analysis and the large sieve to prove approximate equidistribution modulo 4 primes.
- Their proofs also work for general measures (under some assumptions), even for non-identically distributed coefficients.

Proof of P1

Let $S_n(k,\ell)$ be the set of $\pi \in S_n$ containing exactly ℓ cycles of length at most k. We can write

$$n|S_n(k,\ell)| = \sum_{\pi \in S_n(k,\ell)} \sum_{\substack{\sigma | \pi \\ \sigma \text{ a cycle}}} |\sigma|$$

By substituting $\pi = \sigma\pi'$ and noting that π' has either $\ell - 1$ or ℓ cycles of length at most k, we get

$$n|S_n(k,\ell)| \leq \sum_{j=1}^{n} \sum_{m=\ell-1}^{\ell} \sum_{\pi' \in S_{n-j}(k,m)} \sum_{\substack{\sigma \in S_n, |\sigma|=j \\ \sigma \text{ a cycle}}} j = \sum_{j=1}^{n} \sum_{m=\ell-1}^{\ell} \sum_{\pi' \in S_{n-j}(k,m)} \frac{n!}{(n-j)!}$$

Now we rearrange this sum according to the cycle type $(c_1, \ldots, c_n)$ of the permutation π' and apply the Cauchy formula:

Proof of P1

$$\begin{aligned}
n|S_n(k,\ell)| &\leq n! \sum_{j=1}^{n} \sum_{\substack{c_1,\ldots,c_n \geq 0 \\ c_1+2c_2+\cdots+nc_n = n-j \\ c_1+\cdots+c_k \in \{\ell-1,\ell\}}} \frac{1}{\prod_i c_i! i^{c_i}} \\
&\leq n! \sum_{\substack{c_1,\ldots,c_n \geq 0 \\ c_1+\cdots+c_k \in \{\ell-1,\ell\}}} \frac{1}{\prod_i c_i! i^{c_i}} \\
&= n! \Big(\frac{h_k^{\ell-1}}{(\ell-1)!} + \frac{h_k^{\ell}}{\ell!} \Big) \prod_{k<i\leq n} e^{1/i}
\end{aligned}$$

where the last inequality follows by the multinomial theorem, and where $h_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ are the harmonic numbers.

Proof of P1

By applying the bound $h_k \leq 1 + \log k$, this proves that

$$\frac{|S_n(k,\ell)}{n!} \leq \frac{e}{k} \frac{(1+\log k)^{\ell}}{\ell!} (1 + \frac{\ell}{1+\log k})$$

which we note is $O(\frac{(1+\log k)^{\ell-1}}{k(\ell-1)!})$ if $\ell \gg \log k$.
Finally, by summing over all $\ell > (1+\epsilon)\log k$, we obtain

$$\mathbb{P}(\mathbf{B}_{i,k,\epsilon}) \leq \sum_{\ell > (1+\epsilon)\log k} \frac{|S_n(k,\ell)|}{n!} \ll \sum_{\ell > (1+\epsilon)\log k} \frac{(1+\log k)^{\ell-1}}{k(\ell-1)!} \ll \frac{(1+\log k)^{(1+\epsilon)\log k - 1}}{k((1+\epsilon)\log k - 1)!}$$

$$\ll \frac{1}{k} (\frac{e}{1+e})^{(1+\epsilon)\log k}$$

Finally, by computing a Taylor expansion of $-1 + (1+\epsilon)\log(e/(1+\epsilon))$, we obtain the above is bounded by $O(k^{-\epsilon^2/3})$ if $\epsilon \leq 1/2$, which completes the proof of P1. □

Proof of P2

Fix some $\ell \leq (1+\epsilon)\log k$ and consider $\pi \in S_n(k,\ell)$
If π fixes some set X with $|X| = k$, then we denote $\pi_1 = \pi|_x$ and $\pi_2 = \pi|_{[n]\setminus X}$ for the induced permutations on X and its complement.
Then π has ℓ_1 cycles of length $\leq k$, and π_2 has ℓ_2 cycles of length $\leq k$, where $\ell_1 + \ell_2 = \ell$.
Thus, by P1, the number of such $\pi \in S_n(k,\ell)$ for a given choice of X and ℓ_1, ℓ_2 is

$$\ll \frac{(1+\log k)^{\ell_1}}{k\ell_1!} k! \cdot \frac{(1+\log k)^{\ell_2}}{k\ell_2!}(n-k)!$$

Therefore, the probability that $\pi \in S_n$ has exactly ℓ cycles of length at most k is

$$\ll \sum_{\ell_1+\ell_2=\ell} \frac{1}{k^2} \frac{(1+\log k)^{\ell}}{\ell_1!\ell_2!} = \frac{2^{\ell}(1+\log k)^{\ell}}{k^2 \ell!}$$

Proof of P2

Therefore, by summing over all $\ell \leq (1+\epsilon)\log k$, we obtain

$$\begin{aligned}
\mathbb{P}(\mathbf{E}_{i,k} \backslash \mathbf{B}_{i,k,\epsilon}) &\ll \frac{1}{k^2} \sum_{\ell \leq (1+\epsilon)\log k} \frac{2^\ell (1+\log k)^\ell}{\ell!} \\
&\ll \frac{1}{k^2} \frac{2^{(1+\epsilon)\log k}(1+\log k)^{(1+\epsilon)\log k}}{((1+\epsilon)\log k)!} \\
&\ll \frac{1}{k^{1-\log 2 - 2\epsilon}}
\end{aligned}$$

which proves P2. $\square$

References

Bary-Soroker, L., Koukoulopoulos, D., Kozma, G. (2020)
Irreducibility of random polynomials: general measures
Preprint, Available at: arXiv:2007.14567.

Bary-Soroker, L., Kozma, G. (2017)
Irreducible polynomials of bounded height
Duke Math. J. 169(4), 579-598.

Eberhard, S., Ford, K., Green, B. (2017)
Invariable generation of the symmetric group
Duke Math. J. 166(8): 1573-1590.

Konyagin, S.V. (1999)
On the number of irreducible polynomials with 0,1 coefficients
Acta Arith. 88 (1999), 333-350.

References

Kozma, G., Zeitouni, O. (2013)
On Common Roots of Random Bernoulli Polynomials,
Int. Math. Res., 18, 4334–4347.

Littlewood, J.E., Offord, A.C. (1943)
On the number of real roots of a random algebraic equation (III)
Rec. Math. [Mat. Sbornik] N.S., 12(54):3, 277–286.

Meisner, P. (2018)
Erdös' Multiplication Table Problem for Function Fields and Symmetric Groups.
Preprint, Available at: arXiv:1804.08483.

Questions?