Irreducibility of random polynomials of large degree

Dimitris Koukoulopoulos

Joint work with Lior Bary-Soroker and Gady Kozma

1 Université de Montréal
2 Tel Aviv University
3 Weizman Institute

Greek Mathematical Seminar
16 June 2021
The structure of random polynomials

Question

Pick a polynomial $f(x)$ at random. What can we say about its algebraic structure?

- Distribution of roots?
- Factorization?
- Galois group?
Theorem

1. Erdős-Turan (1948): \[ \left| \# \{ j : \theta_j \in [\alpha, \beta] \} - \frac{\beta - \alpha}{2\pi} \cdot n \right| \leq 16\sqrt{nL}. \]

2. Hughes-Nikeghbali (2008): \[ n \geq \# \{ j : |r_j - 1| \leq \varepsilon \} \geq n - 2L/\varepsilon. \]

Corollary

If \((f_j)_{j=1}^{\infty}\) is a family of polynomials such that \[ \frac{L(f_j)}{\deg(f_j)} \to 0, \] then almost all their roots are close to the unit circle, and their angles are roughly uniformly distributed around it.
**Figure:** Roots of $\pm 1$ polynomials of degree $\leq 24$ (S. Derbyshire)

Google "Baez Roots"
Roots of unity

\[ f(x) = \sum_{j=0}^{n} a_j x^j = a_n(x - z_1) \cdots (x - z_n), \quad a_0 a_n \neq 0 \]

Mahler measure

\[ M(f) := |a_n| \prod_{j=1}^{n} \max\{1, |z_j|\} = \exp \left( \frac{1}{2\pi} \int_{0}^{2\pi} \log |f(e^{i\theta})| \, d\theta \right) \]

**Fact:** If \( f(x) \in \mathbb{Z}[x] \), then \( M(f) \geq 1 \) with “=” if \( f \) is product of cyclotomics.

**Conjecture (Lehmer (1933))**

There exists a universal constant \( c > 1 \) such that \( M(f) \geq c \) for all \( f(x) \) that have integer coefficients and that are non-cyclotomic.

**Theorem (Dobrowolski (1979))**

If \( f(x) \in \mathbb{Z}[x] \) is non-cyclotomic of deg \( n \), then \( M(f) \geq 1 + c \left( \frac{\log \log n}{\log n} \right)^3 \).
Irreducibility & Galois groups of random polynomials

Question

(a) \( \mathbb{P}(f(x) = \text{irreducible}) = ? \)

(b) \( \mathbb{P}(\text{Gal}(f) = G) = ? \)

Heuristic: Factoring imposes many relations on coefficients. Unless there are obvious roots, polynomials tend to be irreducible.

Example

If we sample among all 0,1 polynomials, we expect

\[ \mathbb{P}(f(x) = \text{reducible}) = \mathbb{P}(f(0) = 0) + o_{n \to \infty}(1) \sim \frac{1}{2}. \]

In fact, \( \mathbb{P}(\text{Gal}(f) = S_{n-k}) \sim \frac{1}{2^{k+1}} \) for each fixed \( k \geq 0 \) (i.e., according to how many initial coeff’s vanish, the Galois group is as complex as possible).
Sampling polynomials

\[ f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \]

with \( a_j \) sampled according to a probability measure \( \mu \) on \( \mathbb{Z} \).

- \( \mu \) is often the uniform measure on a finite set \( \mathcal{N} \subseteq \mathbb{Z} \).

- Long history when \( n \) is fixed, \( \mathcal{N} = [-H, H] \cap \mathbb{Z} \) with \( H \to \infty \):
  - van der Waarden (1936), Gallagher (1973), Kuba (2009), Dietmann (2013), Chow-Dietmann (2020)

**Conclusion:** \( \text{Gal}(f) = S_n \) w.h.p. (=with high probability)

- Advantage when \( H \) is large: reduce modulo many large primes.
0,1 polynomials

\[ f(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + 1 \quad \text{with } a_j \in \{0, 1\} \]

**Conjecture (Odlyzko-Poonen (1993))**

\( f(x) \) is irreducible w.h.p.

**Theorem (Konyagin (1999))**

\( f(x) \) is irreducible with probability \( \gg 1 / \log n \).

**Theorem (Breuillard-Varjú (2019))**

Assume GRH. Then w.h.p. \( f(x) \) has Galois group \( A_n \) or \( S_n \).

**Theorem (Bary-Soroker, K., Kozma (2020+))**

\( f(x) \) has Galois group \( A_n \) or \( S_n \) with probability \( \geq 0.003736 \).
The argument of Breuillard-Varjú

(It works for any non-singular $\mu$ of compact support.)

- $\mathbb{E}_{x \leq p \leq 2x} \left[ \# \{ \omega \in \mathbb{Z}/p\mathbb{Z} : f(\omega) \equiv 0 \pmod{p} \} \right] \sim \# \{ \text{irr. factors of } f \}$

- $\mathbb{E}_{f \in \mathcal{F}} \mathbb{E}_{x \leq p \leq 2x} \left[ \# \{ \omega \in \mathbb{Z}/p\mathbb{Z} : f(\omega) \equiv 0 \pmod{p} \} \right] = \mathbb{E}_{x \leq p \leq 2x} \left[ \sum_{\omega \in \mathbb{Z}/p\mathbb{Z}} \mathbb{P}_{f \in \mathcal{F}} \left( f(\omega) \equiv 0 \pmod{p} \right) \right]

- Given $\omega$, the expression $f(\omega) - \omega^n = a_0 + a_1 \omega + \cdots + a_{n-1} \omega^{n-1}$ is a random walk in $\mathbb{Z}/p\mathbb{Z}$ of independent increments.

- Breuillard-Varjú proved that, for most $\omega$, the walk mixes as soon as $n \geq (\log p)(\log \log p)^{3+\varepsilon}$. So $\mathbb{P}(f(\omega) \equiv 0 \pmod{p}) \sim \frac{1}{p}$ for most $\omega$.

- **Problem:** in order to make effective the very first asymptotic, we need to assume the Generalized Riemann Hypothesis.
New results

Theorem 1 (Bary-Soroker, K., Kozma (2020+))

Let $\mu \neq \text{Dirac mass, compactly supported}$. There is $\theta = \theta(\mu) > 0$ s.t.

$$
\mathbb{P}(f(x) \text{ has no factors of deg } \leq \theta n \mid f(0) \neq 0) \to 1.
$$

If $\mu$ is uniform on an AP (e.g. on $\{0, 1\}$ or $\{-1, +1\}$), we further have

$$
\mathbb{P}(f(x) = \text{irreducible} \mid f(0) \neq 0) \gtrsim -\log(1 - \theta).
$$

Theorem 2 (Bary-Soroker, K., Kozma (2020+))

Let $\mu$ be unif. on $\mathcal{N}$. Then $\mathbb{P}(\text{Gal}(f) \in \{A_n, S_n\} \mid f(0) \neq 0) \sim 1$ when:

(a) $\mathcal{N} = \{1, 2, \ldots, H\}$ for some $H \geq 35$.

(b) $\mathcal{N} \subseteq \{-H, \ldots, H\}$ with $\#\mathcal{N} \geq H^{4/5}(\log H)^2$ and $H \geq H_0$.

(c) $\mathcal{N} = \{n^s : 1 \leq n \leq N\}$ with $s$ odd and $N \geq N_0(s)$. 
The proof in a nutshell when $\mathcal{N} = \{1, 2, \ldots, 210\}$

- **Eliminating factors of small degree (Konyagin’s argument):**
  - $\mathbb{P}\left(a_0 + a_1\omega + \cdots + a_{n-1}\omega^{n-1} = -\omega^n\right) \ll n^{-1/2} \quad \forall \omega \in \mathbb{C} \setminus \{0\}$.
  - Use when $\omega = e^{2\pi i \frac{k}{\ell}}$ with $0 \leq k < \ell \leq n^{1/10}$.
  - For non-cyclotomic factors of degree $\leq n^{1/10}$, use Dobrowolski’s result on the Mahler measure of non-cyclotomic polynomials.

- **Eliminating factors of large degree:**
  - If $f$ has factor of deg $k$, so does $f_p := f \pmod{p} \quad \forall p$.
  - **Ford, Eberhard-Ford-Green, Meisner:** if $f_p$ is unif. distr. among deg $n$ monics over $\mathbb{F}_p$, then $\mathbb{P}(f_p \text{ has factor of deg } k) \approx k^{-0.086}$.
  - If $\mathcal{N} = \{1, \ldots, H\}$ and $p_1, \ldots, p_r | H$, then $f_{p_1}, \ldots, f_{p_r}$ independent:
    $$\mathbb{P}(f \text{ has factor of deg } k) \lesssim k^{-r \times 0.086} \leq k^{-1.032} \quad \text{if } r \geq 12.$$  
  - Using an idea of Pemantle-Peres-Rivin, $r = 4$ suffices.
  - Smallest $H = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ [Bary-Soroker and Kozma (2020)].
The idea of Pemantle-Peres-Rivin

\[ \nu(f_p; m) := \# \{ \text{irr. factors of } f_p \} \]

- Most \( f_p \) with a deg \( k \) factor are s.t. \( \nu(f_p; k) \sim \frac{\log k}{\log 2} \)
- But, for almost all \( f_p \), we have \( \nu(f_p; m) \sim \log m \) for all \( m \leq n \). Call this high probability event \( E_p \).
- Since \( E_p \) occurs with high probability, we may condition on it at a small loss.
- Conditionally on \( E_p \), the probability of \( f_p \) having a deg \( k \) factor is \( \approx k^{\log 2^{-1}} \approx k^{-0.3} \). Since \( 4 \times 0.3 > 1 \), four primes suffice.
What about $\mathcal{N} = \{1, 2, \ldots, 211\}$?

$$\frac{\#\{1 \leq n \leq 211 : n \equiv a \pmod{5}\}}{211} = \begin{cases} 1/5 - 1/1055 & \text{if } a = 0, \\ 1/5 + 4/1055 & \text{if } a = 1, \\ 1/5 - 1/1055 & \text{if } a = 2, \\ 1/5 - 1/1055 & \text{if } a = 3, \\ 1/5 - 1/1055 & \text{if } a = 4, \end{cases}$$

- Very small Fourier transform at all non-zero frequencies mod 5
- Analogous situation for polynomials with missing digits (work of Moses & Porritt, building on ideas of Dartyge-Mauduit & Maynard).

Adapt methods $\rightsquigarrow$ joint level of distribution for reductions mod 2,3,5,7:

$$\sum \sum \sum \sum \sum \mathbb{P}\left( f : \begin{array}{c} g_2 | f_2, \\ g_3 | f_3, \\ g_5 | f_5, \\ g_7 | f_7 \end{array} \right) - \frac{1}{\prod_{p \leq 7} p^{\deg(g_p)}} \ll \frac{1}{n^{10}}.$$
What about $\mathcal{N} = \{0, 1\}$?

Following Dartyge-Mauduit, after Fourier inversion, apply Hölder: for any $s \in \mathbb{N}$, we have

$$
\sum \sum \sum \sum \sum \sum \sum \prod |\hat{\mu}(\psi_{210}(x^j f/g))|
$$

Following Dartyge-Mauduit, after Fourier inversion, apply Hölder: for any $s \in \mathbb{N}$, we have

$$
\sum \sum \sum \sum \sum \sum \sum \prod |\hat{\mu}(\psi_{210}(x^j f/g))|
$$

Gain: replace $\mu$ by $\mu \ast \cdots \ast \mu$ that is more regular (think CLT).

Loss: replace $n$ by $n/s$, so this limits $k_p \leq n/s$ at best.
The Galois group

- We proved that $f(x)$ is irreducible w.h.p. (or with positive prob.)
- Assuming $f(x)$ is irreducible, we want to show $\text{Gal}(f) \in \{A_n, S_n\}$.
- $f(x)$ irreducible iff $\text{Gal}(f)$ is transitive
- Łuczak-Pyber: $\frac{\#T_n}{\#S_n} = o(1)$, where $T_n = \bigcup_{G \leq S_n \text{ transitive}} G \neq A_n, S_n$.
- **New goal**: construct $g_f \in \text{Gal}(f)$ that behaves quasi-uniformly in $S_n$, so that the odds that it lies in $T_n$ are small by Łuczak-Pyber (and thus so are the odds that $\text{Gal}(f) \neq A_n, S_n$).
- Take $g_f$ to be the Frobenius automorphism modulo a prime $p$ for which the measure $\mu$ is sufficiently well-distributed.
Thank you!