Irreducibility of random polynomials of large degree

Dimitris Koukoulopoulos[1]

Joint work with Lior Bary-Soroker[2] and Gady Kozma[3]

[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?*

Roots

$$f(x) = \sum_{j=0}^{n} a_j x^j \quad \text{with } a_0 a_n \neq 0$$

$$\text{roots} \quad z_j = r_j e^{i\theta_j} \quad (j = 1, 2, \dots, n)$$

$$L = L(f) = \log\left(\frac{|a_0| + |a_1| + \cdots + |a_n|}{\sqrt{|a_0 a_n|}}\right)$$

Theorem

1. *Erdős-Turan (1948):* $\left|\#\{j : \theta_j \in [\alpha, \beta]\} - \frac{\beta - \alpha}{2\pi} \cdot n\right| \leqslant 16\sqrt{nL}.$
2. *Hughes-Nikeghbali (2008):* $n \geqslant \#\{j : |r_j - 1| \leqslant \varepsilon\} \geqslant n - 2L/\varepsilon.$

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.

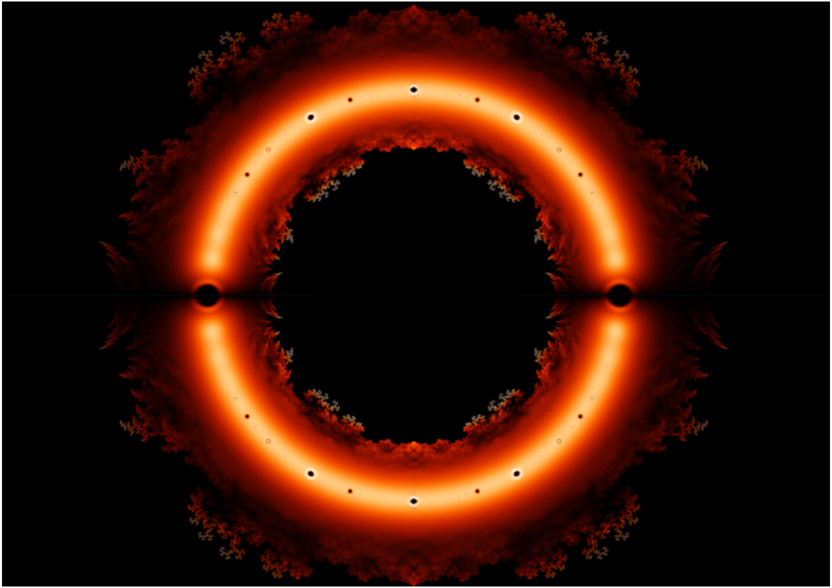

Figure: Roots of ± 1 polynomials of degree $\leqslant 24$ (S. Derbyshire)
Google “Baez Roots”

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

$$M(f) := |a_n| \prod_{j=1}^{n} \max\{1, |z_j|\} = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log|f(e^{i\theta})|\mathrm{d}\theta\right)$$

Fact: If $f(x) \in \mathbb{Z}[x]$, then $M(f) \geqslant 1$ with "=" if-f f is product of cyclotomics.

Conjecture (Lehmer (1933))

There exists a universal constant $c > 1$ such that $M(f) \geqslant c$ 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 $M(f) \geqslant 1 + c\left(\frac{\log\log n}{\log n}\right)^3$.

Irreducibility & Galois groups of random polynomials

Question

(a) $\mathbb{P}\big(f(x) = \textit{irreducible}\big) = ?$ *(b)* $\mathbb{P}\big(\operatorname{Gal}(f) = G\big) = ?$

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

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

In fact, $\mathbb{P}(\operatorname{Gal}(f) = \mathcal{S}_{n-k}) \sim 1/2^{k+1}$ for each fixed $k \geqslant 0$ (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 μ on $\mathbb{Z}$.

- μ 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: $\mathrm{Gal}(f) = \mathcal{S}_n$ w.h.p.(=with high probability)
- Advantage when H is large: reduce modulo many large primes.

0,1 polynomials

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

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 $\mathcal{A}_n$ or $\mathcal{S}_n$.

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

$f(x)$ has Galois group $\mathcal{A}_n$ or $\mathcal{S}_n$ with probability $\geqslant 0.003736$.

The argument of Breuillard-Varjú

(It works for any non-singular μ of compact support.)

- $\mathbb{E}_{x\leqslant p\leqslant 2x}\Big[\#\{\omega\in\mathbb{Z}/p\mathbb{Z} : f(\omega)\equiv 0 \pmod p\}\Big] \sim \#\{\text{irr. factors of } f\}$
- $\mathbb{E}_{f\in\mathcal{F}}\mathbb{E}_{x\leqslant p\leqslant 2x}\Big[\#\{\omega\in\mathbb{Z}/p\mathbb{Z} : f(\omega)\equiv 0 \pmod p\}\Big]$
  $= \mathbb{E}_{x\leqslant p\leqslant 2x}\Bigg[\sum_{\omega\in\mathbb{Z}/p\mathbb{Z}} \mathbb{P}_{f\in\mathcal{F}}\Big(f(\omega)\equiv 0 \pmod p\Big)\Bigg]$
- Given ω, 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 ω, the walk mixes as soon as $n \geqslant (\log p)(\log\log p)^{3+\varepsilon}$. So $\mathbb{P}(f(\omega)\equiv 0 \pmod p) \sim \frac{1}{p}$ for **most** ω.
- 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 $\mu \neq$ *Dirac mass, compactly supported. There is* $\theta = \theta(\mu) > 0$ *s.t.*

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

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

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

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

Let μ *be unif. on* $\mathcal{N}$*. Then* $\mathbb{P}\big(\mathrm{Gal}(f) \in \{\mathcal{A}_n, \mathcal{S}_n\} \bigm| f(0) \neq 0\big) \sim 1$ *when:*

(a) $\mathcal{N} = \{1, 2, \dots, H\}$ *for some* $H \geqslant 35$.

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

(c) $\mathcal{N} = \{n^s : 1 \leqslant n \leqslant N\}$ *with s odd and* $N \geqslant N_0(s)$.

The proof in a nutshell when $\mathcal{N} = \{1, 2, \ldots, 210\}$

- Eliminating factors of small degree (Konyagin's argument):
  - $\mathbb{P}\Big(a_0 + a_1\omega + \cdots + a_{n-1}\omega^{n-1} = -\omega^n\Big) \ll n^{-1/2} \quad \forall \omega \in \mathbb{C} \setminus \{0\}.$

    Use when $\omega = e^{2\pi i \frac{k}{\ell}}$ with $0 \leqslant k < \ell \leqslant n^{1/10}$.
  - For non-cyclotomic factors of degree $\leqslant n^{1/10}$, 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 $\mathbb{P}(f_p$ 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:

$$\mathbb{P}(f \text{ has factor of deg } k) \lesssim k^{-r \times 0.086} \leqslant k^{-1.032} \quad \text{if } r \geqslant 12.$$

  - 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** $m \leqslant n$. 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 $\mathcal{N} = \{1, 2, \ldots, 211\}$?

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

- 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:

$$\sum\sum\sum\sum_{\substack{\boldsymbol{g}=(g_2,g_3,g_5,g_7) \\ \deg(g_p)\leqslant(\frac{1}{2}+\varepsilon)n \\ x\nmid g_p(x)\ \forall p}} \left| \mathbb{P}\left(f : \begin{array}{l} g_2|f_2,\ g_3|f_3 \\ g_5|f_5,\ g_7|f_7 \end{array} \right) - \frac{1}{\prod_{p\leqslant 7} p^{\deg(g_p)}} \right| \ll \frac{1}{n^{10}}.$$

What about $\mathcal{N} = \{0, 1\}$?

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

$$\sum\sum\sum\sum_{\substack{\boldsymbol{g}=(g_2,\dots,g_7)\\ \deg(g_p)=k_p,\, x\nmid g_p(x)\ \forall p}} \sum\sum\sum\sum_{\substack{\boldsymbol{f}=(f_2,\dots,f_7)\\ (f_p,g_p)=1\ \forall p}} \prod_{0\leqslant j<n} |\hat{\mu}(\psi_{210}(x^j\boldsymbol{f}/\boldsymbol{g}))|$$

$$\leqslant \sum\sum\sum\sum_{\substack{\boldsymbol{g}=(g_2,g_3,g_5,g_7)\\ \deg(g_p)=k_p,\, x\nmid g_p(x)\ \forall p}} \sum\sum\sum\sum_{\substack{\boldsymbol{f}=(f_2,\dots,f_7)\\ (f_p,g_p)=1\ \forall p}} \prod_{0\leqslant j<n/s} |\hat{\mu}(\psi_{210}(x^j\boldsymbol{f}/\boldsymbol{g}))|^s.$$

Gain: replace μ by $\underbrace{\mu * \cdots * \mu}_{s \text{ times}}$ that is more regular (think CLT).

Loss: replace n by n/s, so this limits $k_p \leqslant n/s$ 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 $\mathrm{Gal}(f) \in \{\mathcal{A}_n, \mathcal{S}_n\}$.
- $f(x)$ irreducible iff $\mathrm{Gal}(f)$ is transitive
- Łuczak-Pyber : $\dfrac{\#\mathcal{T}_n}{\#\mathcal{S}_n} = o(1), \quad \text{where} \quad \mathcal{T}_n = \bigcup_{\substack{G \leqslant \mathcal{S}_n \text{ transitive} \\ G \neq \mathcal{A}_n, \mathcal{S}_n}} G.$
- **New goal:** construct $g_f \in \mathrm{Gal}(f)$ that behaves quasi-uniformly in $\mathcal{S}_n$, so that the odds that it lies in $\mathcal{T}_n$ are small by Łuczak-Pyber (and thus so are the odds that $\mathrm{Gal}(f) \neq \mathcal{A}_n, \mathcal{S}_n$).
- Take g_f to be the Frobenius automorphism modulo a prime p for which the measure μ is sufficiently well-distributed

Thank you!