Counting Polynomials with Small Galois Group

David Lowry-Duda

March 2021

ICERM
November 2021 Meeting of Simons AGNTC

I'll describe a series of ideas that began at an AIM workshop on Arithmetic Statistics, Discrete Reduction, and Fourier Analysis in February of this year. The focus was to gather analysts, number theorists, and geometers together in order to apply ideas from harmonic analysis to questions in arithmetic.

The focus is the set of ideas leading to [AGO$^+$], *Quantitative Hilbert irreducibility and almost prime values of polynomial discriminants* in collaboration with Theresa Anderson, Ayla Gafni, Robert Lemke Oliver, George Shakan, and Ruixiang Zhang (half number theorists, half analysts). I also touch on forthcoming work that also includes Jiuya Wang and Kevin Hughes.

Polynomials with small Galois group

Our goal is to count polynomials (over $\mathbb{Z}$) with small Galois group (as extensions over $\mathbb{Q}$).

It's well known that a "generic" polynomial of degree n will almost surely have Galois group S_n. We can state this quantitatively, but we need to introduce some notation. Define $V_n(\mathbb{Z})$ to be the set of degree n polynomials over $\mathbb{Z}$, and $V_n^{\mathrm{mon}}(\mathbb{Z})$ the subset of *monic* degree n polynomials. Also define

$$V_n(H) := \{f \in V_n(\mathbb{Z}) : f = a_n x^n + \cdots + a_0, a_n \neq 0, \mathrm{ht}(f) \leq H\},$$

where the *height* of f, $\mathrm{ht}(f)$, is the maximum of the absolute values of the coefficients. Define $V_n^{\mathrm{mon}}(H)$ analogously. Finally, let

$$E_n^{\mathrm{mon}}(H) := \#\{f \in V_n^{\mathrm{mon}}(H) : \mathrm{Gal}(f) \neq S_n\}$$

Then $|V_n^{\mathrm{mon}}(H)| \sim H^n$. Van der Waerden [vdW36] showed that

$$E_n^{\mathrm{mon}}(H) = o(|V_n^{\mathrm{mon}}(H)|) \qquad (1936)$$

and conjectured that

$$E_n^{\mathrm{mon}}(H) \ll |V_n^{\mathrm{mon}}(H)|/H \approx H^{n-1}. \qquad (\textit{conjecture})$$

We call this van der Waerden's Conjecture.

There has been a long history of work towards van der Waerden's Conjecture, including the development of the large sieve (Gallagher), larger sieve (Zywina), and probabilistic Galois theory (Dietmann).

Of particular note is recent work of Chow and Dietmann [Die13, CD20, CD21]. They show that

$$\#\{f \in V_n^{\mathrm{mon}}(H) : \mathrm{Gal}(f) = G\} \ll H^{n-1+\delta_G+\epsilon},$$

where $\delta_G = 1/|S_n/G|$ is the (reciprocal of the) index of G in S_n. It turns out that a completely elementary argument shows that if $G < S_n$ and $G \neq S_n, A_n$, then $|S_n/G| \geq n$.

Morally, this means that we have bounds of the shape $H^{n-1+\frac{1}{n}+\epsilon}$ for all subgroups *except* A_n. Using a different argument, they show that for the particular case of A_n they can show there are at most $O(H^{n-1+(\sqrt{2}-1)+\epsilon})$ polynomials with Galois group A_n, and this was the record bound in the literature.

Remark

This *was* true. A few months ago, Bhargava announced that he can prove van der Waerden's conjecture up to ϵ factor.

To summarize our approach: we introduce a modified version of the Selberg sieve and use number theoretic properties as input to a harmonic analytic argument. Our main quantitative result in this direction is the following.

Theorem (TA, AG, RLO, DLD, GS, RZ)

Let $n \geq 3$ and $H \geq 2$. Then

$$E_n^{\mathrm{mon}}(H) \ll H^{n-\frac{2}{3}+\frac{2}{3n+3}+\epsilon}.$$

And to do this, it suffices really to estimate

$$\#\{f \in V_n^{\mathrm{mon}}(H) : \mathrm{Gal}(f) \subseteq A_n\}$$

by the work of Dietmann noted above.

Recognizing f with $\mathrm{Gal}(f) \subseteq A_n$

Let $f \in \mathbb{Z}[x]$, and let $\mathrm{Disc}(f) \in \mathbb{Z}$ be its discriminant. Then $\mathrm{Disc}(f) = 0$ iff f has a repeated factor, and $\mathrm{Disc}(f) \equiv 0 \bmod p$ exactly when $f \bmod p$ has repeated factors.

Further, suppose that f is monic irreducible of degree n and $G = \mathrm{Gal}(f) \subset S_n$. Write

$$f(x) = f_1(x) \cdots f_r(x) \pmod{p},$$

where each $f_i(x)$ is irreducible mod p. Then there is an element of G with cycle type $(\deg f_1) \cdots (\deg f_r)$ (regarded as a permutation group).

If $\mathrm{Gal}(f) \subset A_n$, then the reduction of f at any prime must correspond to a permutation of even cycle type. We will sieve out polynomials that *are not* of even type.

To that end, we define *odd*.

Oddness

Call $f \in \mathbb{F}_p[x]$ odd if it has no repeated roots and the permutations with cycle type corresponding to the factorization type of f are odd.

Let $\mathbf{1}_p^{\mathrm{odd}}$ denote the odd indicator function mod p, and let $\mathbf{1}_d^{\mathrm{odd}}$ denote the product of the odd indicator functions on primes $p \mid d$.

This function is enough to set up (but not yet execute) a sieving argument.

Broad look on a Selberg sieve

Embed $V_n^{\mathrm{mon}}(\mathbb{Z}) \subset \mathbb{R}^n$ and define a nonnegative Schwarz function $\phi : \mathbb{R}^n \to \mathbb{R}$ that's roughly a bump function around 0. Let λ_d denote a sequence of real numbers with support on squarefree indices squarefree $d \leq D$ with $\lambda_1 = 1$. Then trivially

$$\sum_{f \in V_n^{\mathrm{mon}}(\mathbb{Z})} \phi(f/H) \left(\sum_d \mathbf{1}_d^{\mathrm{odd}}(f) \lambda_d \right)^2 \geq 0. \tag{1}$$

When $f \in V_n^{\mathrm{mon}}(\mathbb{Z})$ and $\mathrm{Gal}(f) \subseteq A_n$, we have that $\mathbf{1}_d^{\mathrm{odd}}(f) = 0$ for all $d > 1$, hence (1) is bounded below by

$$\sum_{\substack{f \in V_n^{\mathrm{mon}}(\mathbb{Z}) \\ \mathrm{Gal}(f) \subseteq A_n}} \phi(f/H).$$

Comparing with the direct expansion of (1) gives

$$\sum_{\substack{f \in V_n^{\mathrm{mon}}(\mathbb{Z}) \\ \mathrm{Gal}(f) \subseteq A_n}} \phi(f/H) \leq \sum_{d_1, d_2} \lambda_{d_1} \lambda_{d_2} \sum_{f \in V_n^{\mathrm{mon}}(\mathbb{Z})} \mathbf{1}^{\mathrm{odd}}_{[d_1, d_2]}(f) \phi(f/H).$$

This is the fundamental setup of a Selberg-type sieve: to estimate the terms on the left, we bound the RHS and then optimize the weights λ_d. I ignore λ optimization completely today, and instead describe bounding the inner sum on the RHS.

Fourier analysis

To bound the RHS, we'll use Fourier analysis and a somewhat atypical application of Poisson summation:

Lemma

Fix $d \geq 2$. Let $\phi\colon \mathbb{R}^n \longrightarrow \mathbb{C}$ be Schwartz, and let $\psi_d\colon (\mathbb{Z}/d\mathbb{Z})^n \longrightarrow \mathbb{C}$ be any function. Let $\widehat{\phi}\colon \mathbb{R}^n \longrightarrow \mathbb{C}$ and $\widehat{\psi}_d\colon (\mathbb{Z}/d\mathbb{Z})^n \longrightarrow \mathbb{C}$ denote the Fourier transforms

$$\widehat{\phi}(\mathbf{u}) = \int_{\mathbb{R}^n} e(\langle \mathbf{x}, \mathbf{u}\rangle)\phi(\mathbf{x})d\mathbf{x} \quad \text{and} \quad \widehat{\psi}_d(\mathbf{u}) = \frac{1}{d^n}\sum_{\mathbf{x}\in(\mathbb{Z}/d\mathbb{Z})^n} e_d(\langle \mathbf{x}, \mathbf{u}\rangle)\psi_d(\mathbf{x}),$$

where $e(x) = e^{-2\pi i x}$ and $e_d(x) = e^{2\pi i x/d}$. Then

$$\sum_{\mathbf{x}\in\mathbb{Z}^n} \phi(\mathbf{x})\psi_d(\mathbf{x}) = \sum_{\mathbf{u}\in\mathbb{Z}^n} \widehat{\phi}\Big(\frac{\mathbf{u}}{d}\Big)\widehat{\psi}_d(\mathbf{u}).$$

The theme is that

$$\sum_{f \in V_n^{\mathrm{mon}}(\mathbb{Z})} \mathbf{1}^{\mathrm{odd}}_{[d_1,d_2]}(f)\phi(f/H) = H^n \sum_{\mathbf{v} \in \mathbb{Z}^n} \widehat{\phi}\left(\frac{\mathbf{v}H}{[d_1,d_2]}\right) \widehat{\mathbf{1}}^{\mathrm{odd}}_{[d_1,d_2]}(\mathbf{v}),$$

and so morally what we need to do is understand $\widehat{\mathbf{1}}^{\mathrm{odd}}_{[d_1,d_2]}$ well.

In fact, one can show that $\widehat{\mathbf{1}}^{\mathrm{odd}}_{d}$ acts almost-multiplicatively in d, so it suffices to study it when d is prime.

I briefly describe two ways to study this Fourier transform.

Method 1: Group actions

Homogenize f to think of it as a binary n-ic form. The group $\mathrm{GL}(1) \times \mathrm{GL}(2)$ acts on binary forms ($\mathrm{GL}(1)$ by multiplication, and $\mathrm{GL}(2)$ by change of basis on (X, Y)).

One can show that $\mathbf{1}_p^{\mathrm{odd}}$ is invariant under this action, and then study Fourier transforms on *orbits*. There is a Heisenberg principle is in effect: if $\mathcal{O}_f$ is the orbit of a particular polynomial f, then we have that

$$\widehat{\mathbf{1}}_p^{\mathrm{odd}}(f)\sqrt{|\mathcal{O}_f|} \ll 1.$$

Thus one approach to bound the Fourier transform $\widehat{\mathbf{1}}_p^{\mathrm{odd}}$ is to classify binary n-ic form orbits. Large orbits have small Fourier transform and can be ignored, and (hopefully) small orbits can be explicitly understood.

It turns out that this was enough to produce improved bounds to van der Waerden's conjecture,

Method 1: Group actions

Homogenize f to think of it as a binary n-ic form. The group $\mathrm{GL}(1) \times \mathrm{GL}(2)$ acts on binary forms ($\mathrm{GL}(1)$ by multiplication, and $\mathrm{GL}(2)$ by change of basis on (X, Y)).

One can show that $\mathbf{1}_p^{\mathrm{odd}}$ is invariant under this action, and then study Fourier transforms on *orbits*. There is a Heisenberg principle is in effect: if $\mathcal{O}_f$ is the orbit of a particular polynomial f, then we have that

$$\widehat{\mathbf{1}}_p^{\mathrm{odd}}(f)\sqrt{|\mathcal{O}_f|} \ll 1.$$

Thus one approach to bound the Fourier transform $\widehat{\mathbf{1}}_p^{\mathrm{odd}}$ is to classify binary n-ic form orbits. Large orbits have small Fourier transform and can be ignored, and (hopefully) small orbits can be explicitly understood.

It turns out that this was enough to produce improved bounds to van der Waerden's conjecture, but we did not publish this approach. (However this is a very powerful method, and we are using it now in other problems).

Method 2: Modify the Selberg sieve

Let μ_p denote the Möbius function on $\mathbb{F}_p[x]$. Then one can show that on a monic f of degree n,

$$\mathbf{1}_p^{\mathrm{odd}}(f) = \frac{(-1)^{n+1}\mu_p(f) + \mu_p^2(f)}{2}.$$

Classical analytic number theory can bound the Fourier transform of $\mu_p(f)$ well, but generically the Fourier transform of $\mu_p^2(f)$ has large coefficients (thus is hard to understand).

Instead, we consider

$$\widetilde{\mathbf{1}}_p^{\mathrm{odd}}(f) = \frac{(-1)^{n+1}\mu_p(f) + 1}{2},$$

which can take the value $1/2$ in addition to 1 and 0.

Modified sieve

This doesn't fit into the typical Selberg sieve. But to each $f \in V_n^{\mathrm{mon}}(\mathbb{Z})$, we can define the quadratic form Q_f in variables $\{\lambda_d\}$

$$Q_f(\{\lambda_d\}) = \sum_{d_1,d_2} \prod_{p|[d_1,d_2]} \widetilde{\mathbf{1}}_p^{\mathrm{odd}}(f)\lambda_{d_1}\lambda_{d_2}.$$

We show that Q_f is nonnegative definite and bounded below,

$$Q_f \geq 2^{-\omega(\mathrm{Disc}(f))}\lambda_1^2.$$

Applying this in the construction of the sieve gives a new relation

$$\sum_{\substack{f \in V_n^{\mathrm{mon}}(\mathbb{Z}) \\ \mathrm{Gal}(f) \subseteq A_n \\ \mathrm{Disc}(f) \neq 0}} \frac{\phi(f/H)}{2^{\omega(\mathrm{Disc}(f))}} \leq \sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2} \sum_{f \in V_n^{\mathrm{mon}}(\mathbb{Z})} \phi(f/H) \prod_{p|[d_1,d_2]} \widetilde{\mathbf{1}}_p^{\mathrm{mon}}(f).$$

Then we apply the Poisson summation argument indicated above and optimize sieve weights to get our main result.

Thank you very much.

Please note that these slides (and references for the cited works) are (or will soon be) available on my website (davidlowryduda.com).

References i


Theresa C Anderson, Ayla Gafni, Robert J Lemke Oliver, David Lowry-Duda, George Shakan, and Ruixiang Zhang.
Quantitative hilbert irreducibility and almost prime values of polynomial discriminants.
Int. Math. Res. Not.
To appear. https://arxiv.org/abs/2107.02914.


Sam Chow and Rainer Dietmann.
Enumerative Galois theory for cubics and quartics.
Adv. Math., 372:107282, 37, 2020.


Sam Chow and Rainer Dietmann.
Towards van der Waerden's conjecture, 2021.
Preprint available at https://arxiv.org/abs/2106.14593.

References ii

Rainer Dietmann.
Probabilistic Galois theory.
Bull. Lond. Math. Soc., 45(3):453–462, 2013.

B L van der Waerden.
Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt.
Monatsh. Math. Phys., 43(1):133–147, 1936.