Pure and Applied Mathematics Quarterly
Volume 19, Number 1, 45–60, 2023

A proof of van der Waerden's Conjecture on random Galois groups of polynomials

Manjul Bhargava

Abstract: Of the $(2H+1)^n$ monic integer polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ with $\max\{|a_1|, \ldots, |a_n|\} \le H$, how many have associated Galois group that is not the full symmetric group S_n? There are clearly $\gg H^{n-1}$ such polynomials, as may be obtained by setting $a_n = 0$. In 1936, van der Waerden conjectured that $O(H^{n-1})$ should in fact also be the correct upper bound for the count of such polynomials. The conjecture has been known previously for degrees $n \le 4$, due to work of van der Waerden and Chow and Dietmann.

In this expository article, we outline a proof of van der Waerden's Conjecture for all degrees n.*

1. Introduction

Let $E_n(H)$ denote the number of monic integer polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ of degree n with $|a_i| \le H$ for all i such that the Galois group $\mathrm{Gal}(f)$ is not S_n. There are clearly $\gg H^{n-1}$ such polynomials, as can be seen by setting $a_n = 0$. In 1936, van der Waerden made the tantalizing conjecture that $O(H^{n-1})$ should in fact also be the correct upper bound for the count of such polynomials. In other words, the probability that a monic polynomial with coefficients bounded by H in absolute value has Galois group not isomorphic to S_n is $\asymp 1/H$.

Hilbert irreducibility implies that $E_n(H) = o(H^n)$, i.e., 100% of monic polynomials of degree n are irreducible and have Galois group S_n. In 1936, van der Waerden [25] proved the first quantitative version of this statement by demonstrating that

$$E_n(H) = O(H^{n - \frac{1}{6(n-2)\log\log H}}).$$

Received December 13, 2022.

*This article is the text of the announcement of and talk on this result given on the occasion of Don Zagier's 70th birthday celebration in the Number Theory Web Seminar on July 1, 2021. Some details and arguments have been added for readability and completeness. Happy birthday, Don!

The first power-saving bound was obtained by Knobloch [17] (1956) who proved that

$$E_n(H) = O(H^{n-\frac{1}{18n(n!)^3}});$$

successive improvements to Knobloch's bound were then given by Gallagher [15] (1973) who proved using his large sieve that

$$E_n(H) = O(H^{n-1/2+\epsilon}),$$

Zywina [28] (2010) who using a "larger sieve" refined this to

$$E_n(H) = O(H^{n-1/2}),$$

Dietmann [13] (2010) who proved using resolvent polynomials and the determinant method that

$$E_n(H) = O(H^{n-2+\sqrt{2}}),$$

and Anderson, Gafni, Lemke Oliver, Lowry-Duda, Shakan, and Zhang [1] (2021) who prove using a Selberg-style sieve that

$$E_n(H) = O(H^{n-\frac{2}{3}+\frac{8}{9n+21}+\epsilon}).$$

(For more on the uses of the large sieve in this and related problems, see the works of Cohen [9] and Serre [23].)

The purpose of this article is to prove that, indeed, $E_n(H) = O(H^{n-1})$, as was conjectured by van der Waerden:

Theorem 1. *We have* $E_n(H) = O(H^{n-1})$.

More generally, for any permutation group $G \subset S_n$ on n letters, let $N_n(G,H)$ denote the number of monic integer polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ with $|a_i| \leq H$ for all i such that $\mathrm{Gal}(f) \cong G$. Then the above theorem amounts to proving that $N_n(G,H) = O(H^{n-1})$ for all permutation groups $G < S_n$.

The methods we describe can in fact be used to give the best known bounds on $N_n(G,H)$ for various individual Galois groups G (see [7] for details), and can also be used to prove a number of other variations of Theorem 1. In this expository article, unlike [7], we make a beeline towards proving just Theorem 1, van der Waerden's Conjecture, in full. Reading this shorter exposition may also be useful as a precursor to reading the more general and more detailed article [7].

2. Preliminaries

2.1. Known results for intransitive and imprimitive groups

That $N_n(G,H) = O(H^{n-1})$ holds for **intransitive** groups G was already shown by van der Waerden, using the fact that polynomials having such Galois groups are exactly those that factor over $\mathbb{Q}$. In fact, an exact asymptotic of the form

$$\sum_{G \subset S_n \text{ intransitive}} N_n(G,H) = c_n H^{n-1} + O(H^{n-2})$$

for an explicit constant $c_n > 0$ was obtained by Chela [10].

Meanwhile, Widmer [27] has given excellent bounds in the case of **imprimitive** Galois groups G, using the fact that polynomials having such Galois groups are exactly those that correspond to number fields having a nontrivial subfield. (A permutation group G is said to be *primitive* if it does not preserve any nontrivial partition of $\{1, \dots, n\}$, and is *imprimitive* otherwise.) Specifically, Widmer proves that

$$\sum_{G \subset S_n \text{ transitive but imprimitive}} N_n(G,H) = O(H^{n/2+2}).$$

Chow and Dietmann [11] showed that van der Waerden's Conjecture holds for $n \leq 4$. Hence, to prove Theorem 1, it suffices to show that $N_n(G,H) = O(H^{n-1})$ for **primitive** permutation groups $G \neq S_n$ for all $n \geq 5$.

2.2. Primitive Galois groups that are not S_n

We now use the following result of Jordan on primitive permutation groups.

Proposition 2 (Jordan)**.** *If $G \subset S_n$ is a primitive permutation group on n letters that contains a transposition, then $G = S_n$.*

Proof. Suppose that $G \subset S_n$ is a primitive permutation group on n letters containing a transposition. Define an equivalence relation $\sim$ on $\{1, \dots, n\}$ by defining $i \sim j$ if the transposition $(i\, j) \in G$. Then the action of G clearly preserves the equivalence relation $\sim$ on $\{1, \dots, n\}$. However, since G is primitive, it cannot preserve any nontrivial partition of $\{1, \dots, n\}$. Therefore, we must have $i \sim j$ (i.e., $(i\, j) \in G$) for all i, j, and so $G = S_n$ since S_n is generated by its transpositions. $\square$

Hence a primitive permutation group $G \neq S_n$ cannot contain a transposition. This has the following consequence for the discriminants of polynomials $f \in \mathbb{Z}[x]$ of degree n whose associated Galois group is not S_n:

Corollary 3. *Let f be an integer polynomial of degree n, and let $K_f := \mathbb{Q}[x]/(f(x))$. If $\mathrm{Gal}(f) \neq S_n$ is primitive, then the discriminant $\mathrm{Disc}(K_f)$ is squarefull.*

Proof. The Galois group $G = \mathrm{Gal}(f)$ acts on the n embeddings of K_f into its Galois closure. Suppose $p \mid \mathrm{Disc}(K_f)$, and p factors in K_f as $\prod P_i^{e_i}$, where P_i has residue field degree f_i. If p is tamely ramified in K_f, then any generator $g \in G \subset S_n$ of an inertia group $I_p \subset G$ at p is the product of disjoint cycles consisting of f_1 cycles of length e_1, f_2 cycles of length e_2, etc. Since G does not the contain a transposition, we must have $e_i > 2$ for some i or $e_i = 2$ and $f_i > 1$ for some i, or $e_i = e_j = 2$ for some $i \neq j$; thus the discriminant valuation $v_p(\mathrm{Disc}(K_f)) = \sum(e_i - 1)f_i$ is at least 2 in that case. If p is wildly ramified, then automatically the discriminant valuation $v_p(\mathrm{Disc}(K_f))$ is at least 2. Therefore, $\mathrm{Disc}(K_f)$ is squarefull. $\square$

3. Proof of van der Waerden's Conjecture (Theorem 1)

We first prove the "weak version" of the conjecture, namely, that $E_n(H) = O_\epsilon(H^{n-1+\epsilon})$.

To accomplish this, we divide the set of irreducible monic integer polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$, such that $|a_i| < H$ for all i and $\mathrm{Gal}(f) < S_n$ is primitive, into three subsets. Let again $K_f := \mathbb{Q}[x]/(f(x))$.

We consider the following three cases:

- **Case I:** The product C of the ramified primes in K_f is at most H, but the absolute discriminant $D = |\mathrm{Disc}(K_f)|$ is greater than H^2.
- **Case II:** The absolute discriminant $D = |\mathrm{Disc}(K_f)|$ is at most H^2.
- **Case III:** The product C of the ramified primes in K_f is greater than H.

We estimate the sizes of each of these sets in turn.

3.1. Case I: $C \leq H$ and $D > H^2$

We first consider those f for which the product C of ramified primes in $K_f := \mathbb{Q}[x]/(f(x))$ is at most H, but the absolute discriminant D of $K = K_f$ is greater than H^2.

By Corollary 3, D is squarefull as we have assumed that $\mathrm{Gal}(f) < S_n$ is primitive. Given such a D, the polynomials f such that $|\mathrm{Disc}(K_f)| = D$ satisfy congruence conditions modulo $C = \mathrm{rad}(D)$ of density $O(\prod_{p|C} c/p^{v_p(D)}) = O(c^{\omega(D)}/D)$ for a suitable constant $c > 0$. Since $C < H$, the number of such f can be counted directly within the box $\{|a_i| < H\}$ of sidelength H; we immediately have the estimate $O(H^n c^{\omega(D)}/D)$ for the number of such f.

Summing $O(H^n c^{\omega(D)}/D)$ over all squarefull $D > H^2$ gives the desired estimate $O_\epsilon(H^{n-1+\epsilon})$ in this case:

$$\sum_{D>H^2 \text{ squarefull}} O(H^n c^{\omega(D)}/D) = O_\epsilon(H^{n-1+\epsilon}). \tag{1}$$

3.2. Case II: $D \leq H^2$

We next consider those f for which the absolute discriminant D of K_f is at most H^2.

The number of isomorphism classes of number fields $K = K_f$ of degree n and absolute discriminant at most H^2 is $O((H^2)^{(n+2)/4}) = O(H^{(n+2)/2})$, by a result of Schmidt [22].[1] For all $n > 2$, Schmidt's estimate was recently improved to $O(H^{(n+2)/2-\kappa_n})$ for a small $\kappa_n > 0$ in joint work with Shankar and Wang [8] (see also the work of Anderson, Gafni, Hughes, Lemke Oliver, and Thorne [2]). By a result of Lemke Oliver and Thorne [20], each isomorphism class of number field K of degree n can arise for at most $O(H \log^{n-1} H/ |\mathrm{Disc}(K)|^{1/(n(n-1))})$ monic integer polynomials f of degree n.

Thus the total number of f that arise in this case is at most

$$O(H^{(n+2)/2-\kappa_n} \cdot H \log^{n-1} H) = O(H^{n-1})$$

when $n \geq 6$. The exact asymptotic results known for the density of discriminants of quintic fields [4] immediately gives $O(H^2 \cdot H \log^4 H) = O(H^{n-1})$ when $n = 5$ as well.

3.3. Case III: $C > H$

Finally, we consider those f for which the product C of ramified primes in K_f is greater than H.

[1] Improved results for n sufficiently large have been obtained by Ellenberg and Venkatesh [14], Couveignes [12], and most recently, Lemke Oliver and Thorne [19].

Fix such an f. By Corollary 3, for every prime $p \mid C$, the polynomial f has either at least a triple root or at least a pair of double roots modulo p. Therefore, changing f by a multiple of p does not change the fact that $p^2 \mid \mathrm{Disc}(f)$. (We thus say that "$\mathrm{Disc}(f)$ is a multiple of p^2 for mod p reasons" in this case.)

Proposition 4. *If $h(x_1,\ldots,x_n)$ is an integer polynomial, such that $h(c_1,\ldots,c_n)$ is a multiple of p^2, and indeed $h(c_1+pd_1,\ldots,c_n+pd_n)$ is a multiple of p^2 for all $(d_1,\ldots,d_n)\in\mathbb{Z}^n$, then $\frac{\partial}{\partial x_n}h(c_1,\ldots,c_n)$ is a multiple of p.*

Proof. Write $h(c_1,\ldots,c_{n-1},x_n)$ as

$$h(c_1,\ldots,c_n)+\tfrac{\partial}{\partial x_n}h(c_1,\ldots,c_n)(x_n-c_n)+(x_n-c_n)^2r(x)\,.$$

Since the first and third terms are multiples of p^2 whenever $x_n\equiv c_n \pmod p$, the second term must be a multiple of p^2 as well, implying that $\frac{\partial}{\partial x_n}h(c_1,\ldots,c_n)$ is a multiple of p. □

Applying Proposition 4 to $h(a_1,\ldots,a_n)=\mathrm{Disc}(f)$, where $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$, we immediately conclude that $\frac{\partial}{\partial a_n}\mathrm{Disc}(f)$ is a multiple of C. Since both $\mathrm{Disc}(f)$ and $\frac{\partial}{\partial a_n}\mathrm{Disc}(f)$ are multiples of C for our choice of f, the resultant of $\mathrm{Disc}(f)$ and $\frac{\partial}{\partial a_n}\mathrm{Disc}(f)$, i.e., the *double discriminant*

$$\mathrm{DD}(a_1,\ldots,a_{n-1}):=\mathrm{Disc}_{a_n}(\mathrm{Disc}_x(f(x))),$$

must also be a multiple of C for this choice of f. (An examination of the polynomial $f(x)=x^n+a_{n-1}x+a_n$ shows that $\mathrm{DD}(a_1,\ldots,a_{n-1})$ does not identically vanish.)

Let $f\in\mathbb{Z}[x]$ be a polynomial for which the product C of ramified primes in K_f is greater than H. For such an f, we have proven that the polynomial $\mathrm{DD}(a_1,\ldots,a_{n-1})$ is a multiple of C. The number of possible $a_1,\ldots,a_{n-1}\in[-H,H]^{n-1}$ such that

$$\mathrm{DD}(a_1,\ldots,a_{n-1})=0$$

is $O(H^{n-2})$, and so the total number of f with $\mathrm{DD}(a_1,\ldots,a_{n-1})=0$ is $O(H^{n-1})$.

Let us now fix $a_1,\ldots,a_{n-1}$ such that $\mathrm{DD}(a_1,\ldots,a_{n-1})\neq 0$. Then $\mathrm{DD}(a_1,\ldots,a_{n-1})$ has at most $O_\epsilon(H^\epsilon)$ factors $C>H$. Once C is determined by $a_1,\ldots,a_{n-1}$, the number of solutions for $a_n \pmod C$ to

$$\mathrm{Disc}(f)\equiv 0 \pmod C$$

is

$$(\deg_{a_n}(\mathrm{Disc}(f)))^{\omega(C)} = O_\epsilon(H^\epsilon).$$

Since $C > H$, the number of $a_n \in [-H, H]$ is also $O_\epsilon(H^\epsilon)$, and so the total number of f in this case is again $O_\epsilon(H^{n-1+\epsilon})$.

3.4. Conclusion

We have thus proven the following theorem:

Theorem 5. *Let $E_n(H)$ denote the number of monic integer polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ of degree n with $|a_i| \leq H$ for all i such that* $\mathrm{Gal}(f)$ *is not S_n. Then $E_n(H) = O_\epsilon(H^{n-1+\epsilon})$.*

3.5. Removing the ϵ

Removing the ϵ in Theorem 5 turns out to be just as much work as proving Theorem 5.

To remove the ϵ in Case I, we replace the condition

$$C \leq H \text{ and } D > H^2$$

by

$$C \leq H^{1+\delta} \text{ and } D > H^{2+2\delta}$$

for some small $\delta = \delta_n > 0$.

The resulting congruence conditions in Case I are now modulo an integer C that is potentially larger than the sidelength H of the box. However, using Fourier analysis (see Subsection 3.6), we show sufficient equidistribution of the residue classes modulo C that we are counting to extend the validity of the count $O(H^n c^{\omega(D)}/D)$ even when $C < H^{1+\delta}$. Specifically, using Fourier analysis, we prove:

Lemma 6. *Let $0 < \delta < 1/(2n-1)$. For each $i = 1, \ldots, m$, let $k_i > 1$ be a positive integer. Let D be a positive integer with prime factorization $D = p_1^{k_1} \cdots p_m^{k_m}$ such that $C = p_1 \cdots p_m < H^{1+\delta}$. Then the number of monic integer polynomials f of degree n in $[-H, H]^n$ such that $|\mathrm{Disc}(K_f)| = D$ is at most $O(c^{\omega(C)}H^n/D)$.*

The estimate $O(H^n c^{\omega(C)}/D)$ of Lemma 6, summed over all squarefull $D > H^{2+2\delta}$, then gives $O(H^{n-1-\delta+\epsilon})$; this thereby removes the ϵ in (1).

We now replace the condition

$$D \le H^2$$

in Case II by

$$D \le H^{2+2\delta}.$$

Since we had already proven a power saving in this case, the total estimate in this case, even with this small change, is still $O(H^{n-1})$.

Finally, we turn to Case III, and replace the condition

$$C > H$$

by

$$C > H^{1+\delta}.$$

Thus Cases I, II, and III again cover all possibilities.

Note that there are two sources of the ϵ in our original treatment of Case III:

(i) The first source is that the number of factors C of $\mathrm{DD}(a_1, \ldots, a_{n-1})$ is $O(H^\epsilon)$.

(ii) The second source is that, for each choice of $a_1, \ldots, a_{n-1}$ such that $\mathrm{DD}(a_1, \ldots, a_{n-1}) \neq 0$, and each choice of factor $C \mid \mathrm{DD}(a_1, \ldots, a_{n-1})$, there are $O((n-1)^{\omega(C)}) = O(H^\epsilon)$ choices for a_n.

We remove the ϵ's in these arguments as follows. We choose a suitable factor C' of C that is between $H^{1+\delta/2}$ and $H^{1+\delta}$ in size, in which case we can handle it by a method analogous to Case I (with C' in place of C). Otherwise, we can choose a factor $C' > H$ of C all of whose prime divisors are greater than $H^{\delta/2}$, in which case we can handle it by the same method as in Case III above (with C' in place of C)—but with no ϵ occurring because C' will have at most a bounded number of prime factors!

To be more precise, we break into two subcases:

Subcase (i): $\boldsymbol{A = \prod_{\substack{p \mid C \\ p > H^{\delta/2}}} p \le H}$

In this subcase, C has a factor B between $H^{1+\delta/2}$ and $H^{1+\delta}$, with $A \mid B \mid C$. Let B be the largest such factor. Let $D' := \prod_{p \mid B} p^{v_p(D)}$. Then $D' > H^{2+\delta}$. We now carry out the argument of Case I, with B in place of C, and D'

in place of D. (Note that D determines C determines B determines D'.) Summing $O(c^{\omega(D')}H^n/D')$ over all squarefull $D' > H^{2+\delta}$ then gives the desired estimate $O(H^{n-1})$ in this subcase:

$$\sum_{D'>H^{2+\delta}\text{ squarefull}} O(c^{\omega(D')}H^n/D') = O_\epsilon(H^{n-1-\delta/2+\epsilon}) = O(H^{n-1}).$$

Subcase (ii): $\boldsymbol{A = \prod_{\substack{p\mid C\\ p>H^{\delta/2}}} p > H}$

In this subcase, we carry out the original argument of Case III, with C replaced by A. We have $A \mid \mathrm{DD}(a_1,\ldots,a_{n-1}) := \mathrm{Disc}_{a_n}(\mathrm{Disc}_x(f(x)))$.

Fix $a_1,\ldots,a_{n-1}$ such that $\mathrm{DD}(a_1,\ldots,a_{n-1}) \neq 0$. Being bounded above by a fixed power of H, we see that $\mathrm{DD}(a_1,\ldots,a_{n-1})$ can have at most a **bounded** number of possibilities for the factor A (since all prime factors of A are bounded below by a fixed positive power of H)!

Once A is determined by $a_1,\ldots,a_{n-1}$, then the number of solutions for $a_n \pmod{A}$ to

$$\mathrm{Disc}(f) \equiv 0 \pmod{A}$$

is

$$O((n-1)^{\omega(A)}) = O(1).$$

Since $A > H$, the total number of f in this subcase is also $O(H^{n-1})$.

This completes the proof of Theorem 1, assuming the truth of Lemma 6.

3.6. Proof of Lemma 6

For a ring R, let V_R^1 denote the set of monic polynomials of degree n over R, which we may identify with R^n. For a function $\Psi_q : V^1_{\mathbb{Z}/q\mathbb{Z}} \to \mathbb{C}$, let $\widehat{\Psi_q} : V^{1*}_{\mathbb{Z}/q\mathbb{Z}} \to \mathbb{C}$ be its Fourier transform defined by the usual formula

$$\widehat{\Psi_q}(x) = \frac{1}{q^n}\sum_{g\in V^{1*}_{\mathbb{Z}/q\mathbb{Z}}} \Psi_q(g)\exp\left(\frac{2\pi i[f,g]}{q}\right),$$

where V_R^{1*} denotes the R-dual of V_R^1. If Ψ_q is the characteristic function of a set $S \subset V^1_{\mathbb{Z}/q\mathbb{Z}}$, then upper bounds on the maximum $M(\Psi_q)$ of $|\widehat{\Psi}_q(g)|$ over all nonzero g constitutes a measure of equidistribution of S in suitable boxes of monic integer polynomials of degree n. This is because, for any Schwartz function ϕ approximating the characteristic function of the box $[-1,1]^n$, the twisted Poisson summation formula gives

$$\begin{aligned}(2)\qquad &\sum_{f=(a_1,\ldots,a_n)\in V_{\mathbb{Z}}^1} \Psi_q(a_1,\ldots,a_n)\phi(a_1/H,a_2/H,\ldots,a_n/H)\\ &= H^n \sum_{g=(b_1,\ldots,b_n)\in V_{\mathbb{Z}}^{1*}} \widehat{\Psi_q}\,(b_1,\ldots,b_n)\widehat{\phi}\,(b_1H/q,b_2H/q\ldots,b_nH/q)\,.\end{aligned}$$

For suitable ϕ, the left side of (2) will be an upper bound for the number of elements in S in the box $[-H,H]^n$. The $g=0$ term is the expected main term, while the rapid decay of $\widehat{\phi}$ implies that the error term is effectively bounded by H^n times the sum of $|\widehat{\Psi_q}(g)|$ over all $0\neq g\in V_{\mathbb{Z}}^*$ whose coordinates are of size at most $O(q^{1+\epsilon}/H)$, and this in turn can be bounded by $O(H^n(q^{1+\epsilon}/H)^nM(\Psi_q))=O(q^{n+\epsilon}M(\Psi_q))$.

In this subsection, we show that the monic polynomials of degree n over $\mathbb{F}_p$, having splitting type containing a given splitting type σ, are very well distributed in boxes. We accomplish this by demonstrating cancellation in the Fourier transform of certain corresponding weighted characteristic functions, using Weil's bounds [26] on exponential sums.

To state the result precisely, we shall need the following definitions.

- If a monic polynomial f (over $\mathbb{Z}$, or over $\mathbb{F}_p$) factors modulo p as $\prod_{i=1}^r P_i^{e_i}$, with P_i monic irreducible and $\deg(P_i)=f_i$, then the *splitting type* (f,p) of f is defined to be $(f_1^{e_1}\cdots f_r^{e_r})$.
- The *index* $\mathrm{ind}(f)$ of f modulo p (or the *index* of the splitting type (f,p) of f) is then defined to be $\sum_{i=1}^r(e_i-1)f_i$.
- More abstractly, we call any expression σ of the form $(f_1^{e_1}\cdots f_r^{e_r})$ a *splitting type*.
- The *index* $\mathrm{ind}(\sigma)$ of σ is defined to be $\sum_{i=1}^r(e_i-1)f_i$.
- Finally, $\#\mathrm{Aut}(\sigma)$ is defined to be $\prod_i f_i$ times the number of permutations of the factors $f_i^{e_i}$ that preserve σ. (See [5, §2] for the motivation for this definition.)

Proposition 7. *Let $\sigma = (f_1^{e_1} \cdots f_r^{e_r})$ be a splitting type with* $\operatorname{ind}(\sigma) = k$. *Let $w_{p,\sigma} : V^1_{\mathbb{F}_p} \to \mathbb{C}$ be defined by*

$w_{p,\sigma}(f) :=$ the number of r-tuples $(P_1, \ldots, P_r)$, up to the action of the group of permutations of $\{1, \ldots, r\}$ preserving σ, such that the P_i are distinct irreducible monic polynomials with $\deg P_i = f_i$ for each i and $P_1^{e_1} \cdots P_r^{e_r} \mid f$.

Then

$$\widehat{w_{p,\sigma}}(g) = \begin{cases} \dfrac{p^{-k}}{\operatorname{Aut}(\sigma)} + O(p^{-k-1}) & \text{if } g = 0; \\[2ex] O(p^{-k-1/2}) & \text{if } g \neq 0. \end{cases}$$

Proof. We have

$$\widehat{w_{p,\sigma}}(g) = \frac{1}{p^n} \sum_{f \in V^1_{\mathbb{F}_p}} e^{2\pi i [f,g]/p} w_{p,\sigma}(f) \tag{3}$$

$$= \frac{1}{p^n} \sum_{P_1,\ldots,P_r} \sum_{P_1^{e_1} \cdots P_r^{e_r} \mid f} e^{2\pi i [f,g]/p}. \tag{4}$$

When $g = 0$, evaluating (4) gives $\widehat{w_{p,\sigma}}(0) = (p^{-k}/\#\operatorname{Aut}(\sigma)) + O(p^{-k-1})$. This is because 1) the number of possibilities for $P_1, \ldots, P_r$ is $(1/\#\operatorname{Aut}(\sigma)) \times p^{\sum e_i} + O(p^{\sum e_i - 1})$, and 2) the number of $f \in V^1_{\mathbb{F}_p}$ such that $P_1^{e_1} \cdots P_r^{e_r}$ divides f is $p^{n - \sum e_i f_i}$. We conclude that

$$\widehat{w_{p,\sigma}}(0) = \frac{1}{p^n} \left(\frac{p^{\sum e_i}}{\#\operatorname{Aut}(\sigma))} + O(p^{\sum e_i - 1}) \right) p^{n - \sum e_i f_i} = \frac{p^{-k}}{\operatorname{Aut}(\sigma)} + O(p^{-k-1}).$$

When $g \neq 0$, we apply the Weil bound [26] on exponential sums to establish cancellation in and thereby obtain a nontrivial estimate on (4) as follows. As already noted, the total number of f (counted with multiplicity) in the double sum in (4) is $\asymp \frac{p^{n-k}}{\#\operatorname{Aut}(\sigma)}$. We partition these polynomials $f(x)$ into orbits of size p under the action of translation $x \mapsto x + c$ for $c \in \mathbb{F}_p$. We then consider the elements of each orbit together in (4). Given such a polynomial $f(x)$, if $g \neq 0$ and $p > n$, then $[f(x+c), g]$ is a nonconstant univariate polynomial $Q(c)$ in c of degree at most n. In that case, the contribution in (4) corresponding to $f(x)$ and its translates $f(x + c)$ add up to

$$\sum_{c \in \mathbb{F}_p} e^{2\pi i [f(x+c), g]} = \sum_{c \in \mathbb{F}_p} e^{2\pi i Q(c)}$$

which is at most $(n-1)p^{1/2}$ in absolute value by the Weil bound. Summing over the $O(p^{n-k-1})$ equivalence classes of these $f(x)$ under the action of translation $x \mapsto x+c$ then yields

$$|\widehat{w_{p,\sigma}}(g)| = O(p^{-n}p^{n-k-1}p^{1/2}) = O(p^{-k-1/2}),$$

which improves upon the trivial bound $O(p^{-k})$, as desired. $\square$

Corollary 8. *Let D be a positive integer with prime factorization $D = p_1^{k_1}\cdots p_m^{k_m}$ and let $C = p_1\cdots p_m$. The number of integral monic polynomials of degree n in $[-H,H]^n$ that modulo p_i have index at least k_i for $i=1,\ldots,m$ is $O(c^{\omega(C)}H^n/D) + O_\epsilon(C^{n-1/2+\epsilon}/D)$.*

Proof. First, we note that the values of the $\mathbb{Z}/C\mathbb{Z}$-Fourier transform are simply products of values of the $\mathbb{F}_{p_i}$-Fourier transforms (one value for each i).

Let ϕ be a smooth function with compact support that is identically 1 on $[-1,1]^n$. Let $\Psi : V^1_{\mathbb{Z}/C\mathbb{Z}} \to \mathbb{R}$ be defined by $\Psi = \prod_i(\sum_{\sigma:\mathrm{ind}(\sigma)\geq k} w_{p_i,\sigma})$. By twisted Poisson summation (2), we have

$$\begin{aligned}
& \sum_{f\in V^1_{\mathbb{Z}}} \Psi(f)\phi(f/H) \\
= \quad & H^n \sum_{g\in V^{1*}_{\mathbb{Z}}} \widehat{\Psi}(g)\widehat{\phi}\left(\frac{gH}{C}\right) \\
\ll \quad & H^n\widehat{\Psi}(0)\widehat{\phi}(0) + H^n \sum_{g\in\left[-\frac{C^{1+\epsilon}}{H},\frac{C^{1+\epsilon}}{H}\right]^n\cap V^{1*}_{\mathbb{Z}}\setminus\{0\}} \left|\widehat{\Psi}(g)\right| + H^n \sum_{g\notin\left[-\frac{C^{1+\epsilon}}{H},\frac{C^{1+\epsilon}}{H}\right]^n\cap V^{1*}_{\mathbb{Z}}} \left|\widehat{\phi}\left(\frac{gH}{C}\right)\right| \\
\ll_{\epsilon,N} \quad & c^{\omega(C)}H^n/D + H^n \sum_{g\in\left[-\frac{C^{1+\epsilon}}{H},\frac{C^{1+\epsilon}}{H}\right]^n\cap V^{1*}_{\mathbb{Z}}\setminus\{0\}} \left|\widehat{\Psi}(g)\right| + H^n \sum_{g\notin\left[-\frac{C^{1+\epsilon}}{H},\frac{C^{1+\epsilon}}{H}\right]^n\cap V^{1*}_{\mathbb{Z}}} \left(\frac{\|g\|H}{C}\right)^{-N}
\end{aligned}$$

for any integer N; the bound on the third summand holds because ϕ is smooth and thus is N-differentiable for any integer N, and so $\widehat{\phi}(g) \ll_N \|g\|^{-N}$ (see, e.g., [24, Chapter 5 (Theorem 1.3)]). By choosing N sufficiently large, the third term can be absorbed into the first term.

We now estimate the second term using Proposition 7:

$$\begin{aligned}
&H^n \sum_{g\in\left[-\frac{C^{1+\epsilon}}{H},\frac{C^{1+\epsilon}}{H}\right]\cap V_{\mathbb{Z}}^{1*}\setminus\{0\}} \left|\widehat{\Psi}(g)\right| \\
\ll\quad & H^n c^{\omega(C)} \sum_{q|C} \sum_{\substack{g\in\left[-\frac{C^{1+\epsilon}}{H},\frac{C^{1+\epsilon}}{H}\right]^n\cap V_{\mathbb{Z}}^{1*}\setminus\{0\}\\ (\mathrm{ct}(g),C)=q}} q^{1/2}\prod_{i=1}^m p_i^{-k_i-1/2} \\
\ll_\epsilon\quad & H^n \sum_{q|C} \frac{C^{n+\epsilon}}{q^n H^n}\cdot q^{1/2}\prod_{i=1}^m p_i^{-k_i-1/2} \\
\ll_\epsilon\quad & C^\epsilon \prod_{i=1}^m p_i^{n-k_i-1/2} \\
\ll_\epsilon\quad & C^{n-1/2+\epsilon}/D,
\end{aligned}$$

where the content $\mathrm{ct}(g)$ of g denotes the largest integer such that $g/\mathrm{ct}(g) \in V_{\mathbb{Z}}^{1*}$. This yields the desired result. □

We now complete the proof of the key lemma, Lemma 6. Suppose f is a monic integer polynomial of degree n such that $|\mathrm{Disc}(K_f)| = D = \prod p_i^{k_i}$. Then (aside from primes $p \mid n$ where there may be wild ramification) the index of $f \pmod{p_i}$ is at least k_i. By Corollary 8, the number of monic integer polynomials f of degree n such that the index of $f \pmod{p_i}$ is at least k_i for all i, and the product $C = \prod p_i$ of ramified primes in K_f satisfies $C < H^{1+\delta}$, is

$$\begin{aligned}
O(c^{\omega(C)}H^n/D) + O_\epsilon(C^{n-1/2+\epsilon}/D) &= O(c^{\omega(C)}H^n/D) + O_\epsilon((H^{1+\delta})^{n-1/2+\epsilon}/D)\\
&= O(c^{\omega(C)}H^n/D)
\end{aligned}$$

since $\delta < 1/(2n-1)$. This completes the proof of Lemma 6 (and thus also Theorem 1). □

4. Related results and variations

We note that the non-monic case (the subject of van der Waerden's original conjecture) can be handled in essentially the same way, in order to prove that the number of integer-coefficient polynomials of degree n with coefficients bounded in absolute value by H whose Galois group is not S_n is $E_n^*(H) = O(H^n)$.

Other results that can be proven using extensions of the methods described in this article:

- If $G \neq S_n$ or A_n:
  - If $n \geq 10$, then $N_n(G,H) = O(H^{n-2})$;
  - If $n \geq 28$, then $N_n(G,H) = O(H^{n-3})$;
  - For sufficiently large n, we have $E_n(H) = O(H^{n-cn/\log^2 n})$ where c is an absolute constant.
- For p a prime, if $G = C_p$ (the cyclic group of order p), then $N_n(C_p,H) = O(H^2)$.
- If G is a regular permutation group on n letters, then $N_n(G,H) = O(H^{3n/11+1.164})$.
- We have $N_{11}(M_{11},H) = O(H^{8.686})$, where M_{11} is the Mathieu group on 11 letters.
- (A question of Serre) The number of monic even integer polynomials

$$g(x) = x^{2n} + a_1 x^{2n-2} + a_2 x^{2n-4} + \cdots + a_n$$

  with $|a_i| < H$ for all i whose Galois group is not the Weyl group $W(B_n) \cong S_2^n \rtimes S_n$ is $\asymp H^{n-1/2}$, and the number for which it is also not the Weyl group $W(D_n)$ is $\asymp H^{n-1}$.

For more details on these results and variations, see [7].

Acknowledgments

We are extremely grateful to Benedict Gross, Danny Neftin, Andrew O'Desky, Robert Lemke Oliver, Ken Ono, Fernando Rodriguez-Villegas, Arul Shankar, Don Zagier, and the anonymous referee for all their helpful comments and encouragement. Most of all, we thank Don Zagier for his friendship and years of inspiration—wishing him a very happy birthday and many happy returns!

References

[1] T. C. Anderson, A. Gafni, R. J. Lemke Oliver, D. Lowry-Duda, G. Shakan, and R. Zhang, Quantitative Hilbert irreducibility and almost prime values of polynomial discriminants, *Int. Math. Res. Not.* 2021, rnab296.

[2] T. C. Anderson, A. Gafni, K. Hughes, R. J. Lemke Oliver, and F. Thorne, Improved bounds on number fields of small degree, Preprint, 2022, arXiv:2204.01651.

[3] M. Bhargava, The density of discriminants of quartic rings and fields, *Ann. of Math.* **162** (2005), 1031–1063. MR2183288

[4] M. Bhargava, The density of discriminants of quintic rings and fields, *Ann. of Math.* **172** (2010), 1559–1591. MR2745272

[5] M. Bhargava, Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants, *Int. Math. Res. Not.* **2007**, Article ID rnm052. MR2354798

[6] M. Bhargava, The geometric sieve and the density of squarefree values of invariant polynomials (2014), arXiv:1402.0031v1.

[7] M. Bhargava, Galois groups of random integer polynomials and van der Waerden's Conjecture (2021), arXiv:2111.06507.

[8] M. Bhargava, A. Shankar, and X. Wang, An improvement on Schmidt's bound on the number of number fields of bounded discriminant and small degree, *Forum Math., Sigma* **10** (2022), e86, 13 pages. MR4493242

[9] S. D. Cohen, The distribution of Galois groups and Hilbert's irreducibility theorem, *Proc. Lond. Math. Soc.* (3) **43** (1981), 227–250. MR0628276

[10] R. Chela, Reducible polynomials, *J. Lond. Math. Soc.* **38** (1963), 183–188. MR0148647

[11] S. Chow and R. Dietmann, Enumerative Galois theory for cubics and quartics, *Adv. Math.* **372** (2020): 107282. MR4128571

[12] J.-M. Couveignes, Enumerating number fields, *Ann. of Math.* **192** (2019), 487–497. MR4151082

[13] R. Dietmann, Probabilistic Galois theory, *Bull. London Math. Soc.* **45** (2012), No. 3, 453–462. MR3065016

[14] J. S. Ellenberg and A. Venkatesh, The number of extensions of a number field with fixed degree and bounded discriminant, *Ann. of Math.* **163** (2006), 723–741. MR2199231

[15] P. X. Gallagher, The large sieve and probabilistic Galois theory, *Proceedings of Symposia in Pure Mathematics XXIII*, A.M.S., 1973, pp. 91–101. MR0332694

[16] R. Guralnick and K. Magaard, On the minimal degree of a primitive permutation group, *J. Algebra* **207** (1998), 127–145. MR1643074

[17] H.-W. Knobloch, Zum Hilbertschen Irreduzibilitätssatz, *Abh. Math. Sem. Univ. Hamburg* **19** (1955), 176–190. MR0067923

[18] H.-W. Knobloch, Die Seltenheit der reduziblen Polynome, *Jber. Deutsch. Math. Verein.* **59**, (1956), 12–19. MR0080071

[19] R. J. Lemke Oliver and F. Thorne, Upper bounds on number fields of given degree and bounded discriminant, *Duke Math. J.* **171** (2020), 3077–3087. MR4497223

[20] R. J. Lemke Oliver and F. Thorne, Upper bounds on polynomials with small Galois group, *Mathematika* **66** (2020), 1054–1059. MR4151870

[21] M. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, *Proc. London Math. Soc.* (3) **63** (1991), 266–314. MR1114511

[22] W. M. Schmidt, Number fields of given degree and bounded discriminant, *Astérisque* **228** (1995), No. 4, 189–195. MR1330934

[23] J-P. Serre, *Lectures on the Mordell–Weil Theorem*, Aspects of Mathematics **15**, Springer Fachmedien Wiesbaden, 1997.

[24] E. Stein and R. Shakarchi, *Fourier Analysis: An Introduction*, Princeton University Press, 2003. MR1970295

[25] B. L. van der Waerden, Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt, *Monatsh. Math. Phys.*, **43** (1936), No. 1, 133–147. MR1550517

[26] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A.* **34** (1948), 204–207. MR0027006

[27] M. Widmer, On number fields with nontrivial subfields, *International Journal of Number Theory* **7** (2011), No. 3, 695–720. MR2805576

[28] D. Zywina, Hilbert's irreducibility theorem and the larger sieve (2010), arXiv.org:1011.6465v1.

Manjul Bhargava
Princeton University
USA
E-mail: bhargava@math.princeton.edu