QUANTITATIVE HILBERT IRREDUCIBILITY AND ALMOST PRIME VALUES OF POLYNOMIAL DISCRIMINANTS

THERESA C. ANDERSON, AYLA GAFNI, ROBERT J. LEMKE OLIVER, DAVID LOWRY-DUDA, GEORGE SHAKAN, AND RUIXIANG ZHANG

Abstract. We study two polynomial counting questions in arithmetic statistics via a combination of Fourier analytic and arithmetic methods. First, we obtain new quantitative forms of Hilbert's Irreducibility Theorem for degree n polynomials f with $\mathrm{Gal}(f) \subseteq A_n$. We study this both for monic polynomials and non-monic polynomials. Second, we study lower bounds on the number of degree n monic polynomials with almost prime discriminants, as well as the closely related problem of lower bounds on the number of degree n number fields with almost prime discriminants.

1. Introduction

The study of statistics for objects of algebraic interest has been a source of rich and deep advances in mathematics. One of the goals of a recent AIM workshop was to make progress on counting problems by further incorporating Fourier analytic techniques into arithmetic statistics. This project grew out of that workshop and is an effort in that direction.

In this paper, we use analytic and arithmetic methods in tandem to study a variety of arithmetic statistics related to polynomial counts. We hope to see further and more refined applications of similar ideas in other counting problems in the future. We focus on two primary applications, both involving counting polynomials of certain types. First, we study a quantitative version of *Hilbert's Irreducibility Theorem* (HIT). A precise statement follows below, but our version gives upper bounds for the number of degree n polynomials whose Galois groups are subgroups of A_n. Our techniques apply equally well to monic and non-monic polynomials, so we examine both.

To state our version of HIT, we need a few definitions. For $n \geqslant 3$, define

$$V_n(H) = \{f(x) \in \mathbb{Z}[x] : f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, a_n \neq 0, \mathrm{ht}(f) \leqslant H\},$$

where we define the *height* of a polynomial f, $\mathrm{ht}(f)$, as the maximum of the absolute value of the coefficients. Let $V_n^{\mathrm{mon}}(H) \subset V_n(H)$ denote the subset of monic polynomials, and let

$$E_n^{\mathrm{mon}}(H) = |\{f(x) \in V_n^{\mathrm{mon}}(H), \mathrm{Gal}(f) \neq S_n\}|.$$

Van der Waerden [vdW36] gave the first explicit bound for $E_n^{\mathrm{mon}}(H)$ and conjectured that $E_n^{\mathrm{mon}}(H) \ll_n |V_n^{\mathrm{mon}}(H)|/H$. Gallagher [Gal73] used the large sieve to improve van der Waerden's bound to $E_n^{\mathrm{mon}}(H) \ll_n H^{n-1/2}(\log H)^{1-\gamma_n}$, where γ_n is a sequence of positive numbers satisfying $\gamma_n \sim (2\pi n)^{-1/2}$. Zywina [Zyw10] further improved this by removing the power of $\log H$, and the record is work of Dietmann [Die13] who shows that

$$E_n^{\mathrm{mon}}(H) \ll_n H^{n-2+\sqrt{2}+\epsilon}, \tag{1.1}$$

and of Chow and Dietmann [CD20], who solve van der Waerden's conjecture when $n \leqslant 4$.

Significantly stronger bounds are known for the number $E_n^{\mathrm{mon}}(H)'$ of monic polynomials with Galois group isomorphic to neither S_n nor A_n. There have been a number of recent results on this problem, including work of Zywina [Zyw10] and Dietmann [Die12]. The record on this problem is the *very* recent work of Chow and Dietmann [CD21], who show using the determinant method that

$$E_n^{\mathrm{mon}}(H)' \ll_n H^{n-1.017}, \quad n \notin \{7, 8, 10\},$$

which resolves van der Waerden's conjecture in these degrees, apart from bounding the number of polynomials whose Galois group is A_n. Their methods also essentially apply when $n \in \{7, 8, 10\}$, but save a power of H smaller than 1.

Date: July 8, 2021.

Here, we improve the bounds on polynomials f where $\mathrm{Gal}(f) \subseteq A_n$. To be precise, let V_n denote the set of degree n polynomials over $\mathbb{Z}$, and let $V_n^{\mathrm{mon}} \subset V_n$ denote the set of monic degree n polynomials. For $H \geqslant 1$, define

$$E_n(H; A_n) := |\{f \in V_n(H) : \mathrm{Gal}(f) \subseteq A_n\}|.$$

Define $E_n^{\mathrm{mon}}(H; A_n)$ by restricting to monic polynomials. We use a combination of arithmetic and analytic techniques to prove the following.

Theorem 1.1. *Let $n \geqslant 3$ be an integer and let $H \geqslant 2$. Then for any $\epsilon > 0$,*

$$E_n(H; A_n) \ll_{n,\epsilon} H^{n+\frac{1}{3}+\frac{8}{9n+21}+\epsilon}$$

and

$$E_n^{\mathrm{mon}}(H; A_n) \ll_{n,\epsilon} H^{n-\frac{2}{3}+\frac{2}{3n+3}+\epsilon}. \tag{1.2}$$

For $n \geqslant 8$, the bound (1.2) improves on Dietmann's bound (1.1) for the number of monic polynomials whose Galois group is contained in A_n. Combined with the work of Chow and Dietmann, this improves the overall estimate on the error term in HIT to $E_n^{\mathrm{mon}}(H) \ll_{n,\epsilon} H^{n-\frac{2}{3}+\frac{2}{3n+3}+\epsilon}$. We also note that Bhargava has announced a proof of van der Waerden's conjecture using different methods.

Our approach to Theorem 1.1 is inspired by Gallagher's sieve theoretic approach (which also underlies Zywina's work), but instead of using the large sieve, we introduce a modification to the classical Selberg sieve in §4. This modification allows us to connect the local conditions appearing in the sieve more properly to the Möbius function over finite fields, provided we count the relevant polynomials with certain arithmetic weights, and is the key novelty in Theorem 1.1. We estimate the local density of the modified conditions by means of Poisson summation, with work of Porritt [Por18] on bounds for the the Fourier transform of the Möbius function appearing to control the error.

Our second application concerns lower bounds on the number of degree n polynomials with *almost prime* discriminants, i.e. discriminants with relatively few distinct prime factors. We draw inspiration from the following result of Taniguchi and Thorne [TT20a], who were in turn inspired by the folklore conjecture that there should be infinitely many fields of prime discriminant in every degree; this is known only for quadratic extensions, however.

Theorem ([TT20a])**.** *There is an absolute constant $C_3 > 0$ such that for each $X > 2$, there exist at least $C_3 X/\log X$ cubic fields whose discriminant is squarefree, bounded above by X, and has at most 3 prime factors, and there is an absolute constant $C_4 > 0$ such that for each $X > 2$, there exist at least $C_4 X/\log X$ quartic fields whose discriminant is squarefree, bounded above by X, and has at most 8 prime factors.*

The cubic case improved an earlier result of Belabas and Fouvry [BF99] which had 3 prime factors replaced by 7.

In §5, we first study the number of polynomials whose discriminants are almost prime. We prove an almost prime discriminant result for all $n \geqslant 3$ that obtains discriminants with fewer prime factors than [TT20a] if $n = 4$.

Theorem 1.2. *Let $n \geqslant 3$, and let $H \geqslant 2$. For any $r \geqslant 2n-3$, we have*

$$\#\{f \in P_n^{\mathrm{mon}}(H) : \omega(\mathrm{Disc}(f)) \leqslant r\} \gg_{n,r} \frac{H^n}{\log H},$$

where $\omega(\mathrm{Disc}(f))$ denotes the number of distinct primes dividing the discriminant of the polynomial f.

As the discriminant of a number field cut out by an irreducible polynomial divides that of the polynomial, we can use lower bounds for counts of almost prime polynomial discriminants to get lower bounds for almost prime number field discriminants. To make this comparison effective, we use results from [LT20b] that bound the number of different polynomials of a given height that cut out the same number field. This allows us to prove the following theorem. We state a more precise version as Theorem 5.2.

Theorem 1.3. *Let $n \geqslant 3$, and let $X \geqslant 2$. There is a constant $\delta_n > 0$ depending only on n, such that for any $r \geqslant 2n-3$, we have*

$$\#\{F/\mathbb{Q} : [F:\mathbb{Q}] = n, \mathrm{Disc}(F) \leqslant X, \omega(\mathrm{Disc}(F)) \leqslant r\} \gg_n X^{\frac{1}{2}+\delta_n},$$

where $\omega(\mathrm{Disc}(F))$ denotes the number of distinct primes dividing the discriminant of the field F.

In the quartic case $n = 4$, Theorem 1.3 improves on the quality of the almost primes produced by Taniguchi and Thorne (achieving $r = 5$ as opposed to $r = 8$), but at the expense of obtaining a worse lower bound on the number of such fields. In fact, the lower bounds obtained by Taniguchi and Thorne are of the expected order of magnitude for the number of prime discriminant fields, which is $\asymp_n X/\log X$ for every n, while Theorem 1.3 falls short. The reason for this is that to prove their theorem, Taniguchi and Thorne use group actions on *prehomogeneous vector spaces*. They are then able to count certain lattice points related to the desired field counts, utilizing deep parameterization theorems and Poisson summation. Their method is powerful, but as it relies on parametrizations via prehomogenous vector spaces, it is only currently available for degrees less than or equal to 5. It is interesting to note that they are sometimes able to explicitly compute all Fourier transforms [TT20b], but can prove their results using rougher estimates.

To get a result for all $n \geqslant 3$, we use a different approach that involves studying an underlying Fourier transform directly and the *almost prime sieve*. Our analysis centers on the Fourier transform of the squarefree indicator function. For small degrees, it may be possible to include additional arithmetic ingredients to improve our results.

Finally, to reach a wide audience, we have erred on the side of writing more details and explanations. We hope for this to be an engaging, understandable paper.

Acknowledgements

TCA is supported by NSF DMS 1954407. DLD is supported by the Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation via the Simons Foundation grant 546235. This work is partially supported by the DFG (EXC-2047/1 - 390685813), while AG was in residence at the Hausdorff Institute of Mathematics in Bonn, Germany. RZ is supported by the NSF grant DMS-1856541, DMS1926686 and by the Ky Fan and Yu-Fen Fan Endowment Fund at the Institute for Advanced Study.

This collaboration arose out of an AIM workshop on Fourier analysis, arithmetic statistics, and discrete restriction organized by the first author, Frank Thorne, and Trevor Wooley. The authors thank AIM for the supportive working environment. They would also like to thank Will Sawin for helping strengthen this paper, and Manjul Bhargava, Kevin Hughes, Hong Wang, and Jiuya Wang for useful conversations.

2. Polynomials over finite fields

We begin in this section by collecting some basic facts from algebraic number theory on the reduction modulo primes of integer polynomials. (See for example [Jac85, §4.16] as a reference).

Lemma 2.1. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial, and let $\mathrm{Disc}(f) \in \mathbb{Z}$ denote its polynomial discriminant. Then $\mathrm{Disc}(f) = 0$ if and only if $f(x)$ has a repeated factor (which happens over $\mathbb{C}$ if and only if it happens over $\mathbb{Z}$). Moreover if p is a prime number not dividing the leading coefficient of f, then $p \mid \mathrm{Disc}(f)$ if and only if $f(x) (\mathrm{mod}\, p)$ has repeated factors.*

Notice that if $f(x) \in \mathbb{Z}[x]$ is irreducible, then it has no repeated factors (since it has only one!). It follows that $\mathrm{Disc}(f)$ must be non-zero, and thus can be divisible by only finitely many primes. In particular, it will have repeated factors $(\mathrm{mod}\, p)$, or be of smaller degree, only for those finitely many primes. For all of the others, we have the following connection between factorization types and Galois groups.

Lemma 2.2. *Suppose $f(x) \in \mathbb{Z}[x]$ is irreducible with degree n. Let $G \subseteq S_n$ be its Galois group, thought of as permuting the roots of $f(x)$. Suppose p is a prime not dividing the leading coefficient of $f(x)$ for which $f(x) (\mathrm{mod}\, p)$ has no repeated factor. Write*

$$f(x) = f_1(x) \dots f_r(x) (\mathrm{mod}\, p),$$

where each $f_i(x)$ is irreducible $(\mathrm{mod}\, p)$.

Then there is an element of G with cycle type $(\deg f_1)(\deg f_2) \cdots (\deg f_r)$. In fact, this is true for any of the Frobenius elements associated to p.

In particular, if $\mathrm{Gal}(f) \subseteq A_n$, then the reduction of f at any prime subject to Lemma 2.2 must correspond to an even cycle type. As we are approaching our main theorem via sieves, it is the complementary notion that is of most interest to us:

Definition 2.3. We say a polynomial $f(x) \in \mathbb{F}_p[x]$ is *odd* if it has no repeated roots and the permutations with cycle type corresponding to the factorization type of $f(x)$ are odd. Equivalently, $f(x)$ is odd if it has no repeated factors and the number of its irreducible factors with even degree is odd.

Lemma 2.4. *A degree n polynomial over $\mathbb{F}_p$ is odd precisely if $\mu_p(f) = (-1)^{n+1}$, where $\mu_p(f)$ is the Möbius function over $\mathbb{F}_p[x]$.*

Proof. Suppose a squarefree polynomial f of degree n over $\mathbb{F}_p$ has factorization type $\lambda_1 \cdots \lambda_r$. Let $N_{\text{odd}} = \#\{i : \lambda_i \text{ odd}\}$ and $N_{\text{even}} = \#\{i : \lambda_i \text{ even}\}$ count the number of odd and even λ_i. Then f is odd if N_{even} is odd, i.e. if

$$(-1)^{N_{\text{even}}} = -1.$$

However, notice that $N_{\text{even}} = r - N_{\text{odd}}$ and that $N_{\text{odd}} \equiv n \pmod 2$. Thus

$$(-1)^{N_{\text{even}}} = (-1)^{r-n} = \mu(f)(-1)^n.$$

The result follows. □

Since we are primarily interested in the reduction of integer polynomials f, when the leading coefficient of f is not ± 1 the degree of the reduction of f may be smaller than that of f. Consequently, for a polynomial $f \in \mathbb{F}_p[x]$, we define

$$\mu_{p,n}(f) = \begin{cases} \mu_p(f), & \text{if } \deg(f) = n, \\ 0, & \text{if } \deg(f) \neq n, \end{cases} \tag{2.1}$$

Given an integer polynomial $f \in \mathbb{Z}[x]$, we define $\mu_{p,n}(f)$ in the expected manner by means of the reduction of $f \pmod p$. It follows from the above discussions that $\mu_{p,n}(f) = 0$ if and only if p divides the product of the leading coefficient of f with discriminant of f. Consequently, we define the quantity $\text{LDisc}(f)$ to be this product.

To end this section, we summarize the above discussion in the following lemma.

Lemma 2.5. *Let $f \in \mathbb{Z}[x]$ be a polynomial of degree $n > 0$ with $\text{Gal}(f) \subseteq A_n$. Then $\mu_{p,n}(f) \neq (-1)^{n+1}$ for every prime p.*

3. Fourier transforms of polynomials over finite fields

Given a squarefree integer d, let $V_n(\mathbb{Z}/d\mathbb{Z})$ denote the vector space of polynomials over $\mathbb{Z}/d\mathbb{Z}$ with degree at most n, and let $V_n^{\text{mon}}(\mathbb{Z}/d\mathbb{Z})$ denote the subset of those that are monic of degree equal to n. We identify the dual of $V_n(\mathbb{Z}/d\mathbb{Z})$ with $(\mathbb{Z}/d\mathbb{Z})^{n+1}$ and the dual of $V_n^{\text{mon}}(\mathbb{Z}/d\mathbb{Z})$ with $(\mathbb{Z}/d\mathbb{Z})^n$. We define the pairing between $V_n(\mathbb{Z}/d\mathbb{Z})$ and $(\mathbb{Z}/d\mathbb{Z})^{n+1}$ coefficient-wise; namely, if $f(x) = \sum_{i=0}^n a_i x^i$ and $\mathbf{u} = (u_0, \dots, u_n) \in (\mathbb{Z}/d\mathbb{Z})^{n+1}$, we define

$$\langle f, \mathbf{u} \rangle := \sum_{i=0}^n a_i u_i.$$

We define the pairing $\langle \cdot, \cdot \rangle_{\text{mon}}$ between $V_n^{\text{mon}}(\mathbb{Z}/d\mathbb{Z})$ and $(\mathbb{Z}/d\mathbb{Z})^n$ analogously. We will typically omit "mon" from the notation if it's clear that we are working with monic polynomials. If $\psi \colon V_n(\mathbb{Z}/d\mathbb{Z}) \to \mathbb{C}$ is a function, we define its Fourier transforms

$$\widehat{\psi}(\mathbf{u}) := \frac{1}{d^{n+1}} \sum_{f \in V_n(\mathbb{Z}/d\mathbb{Z})} \psi(f) e_d(\langle f, \mathbf{u} \rangle), \quad e_d(x) := e^{\frac{2\pi i x}{d}}$$

for $\mathbf{u} \in (\mathbb{Z}/d\mathbb{Z})^{n+1}$ and

$$\widehat{\psi}^{\text{mon}}(\mathbf{v}) := \frac{1}{d^n} \sum_{f \in V_n^{\text{mon}}(\mathbb{Z}/d\mathbb{Z})} \psi(f) e_d(\langle f, \mathbf{u} \rangle)$$

for $\mathbf{v} \in (\mathbb{Z}/d\mathbb{Z})^n$. Exploiting the natural map $V_n(\mathbb{Z}/d\mathbb{Z}) \to \prod_{p|d} V_n(\mathbb{F}_p)$, we will be primarily interested in functions of the form $\psi_d := \prod_{p|d} \psi_p$, where $\psi_p \colon V_n(\mathbb{F}_p) \to \mathbb{C}$. For such functions, the Fourier transform has a corresponding factorization.

Lemma 3.1. *Let d be a squarefree integer. For each prime $p \mid d$, let $\psi_p \colon V_n(\mathbb{F}_p) \to \mathbb{C}$, and for any $f \in V_n(\mathbb{Z}/d\mathbb{Z})$, define $\psi_d(f) := \prod_{p|d} \psi_p(f)$. Define ψ_p^{mon} analogously. There are units $\alpha_p \in \mathbb{F}_p^\times$ such that for any $\mathbf{u} \in \mathbb{Z}^{n+1}$ and any $\mathbf{v} \in \mathbb{Z}^n$,*

$$\widehat{\psi}_d(\mathbf{u}) = \prod_{p|d} \widehat{\psi}_p(\alpha_p \mathbf{u}) \quad \text{and} \quad \widehat{\psi}_d^{\mathrm{mon}}(\mathbf{v}) = \prod_{p|d} \widehat{\psi}_p^{\mathrm{mon}}(\alpha_p \mathbf{v}).$$

Proof. This follows from the Chinese remainder theorem, and the proof is the same in the general and monic cases. We give the proof for the general case. It suffices to prove the lemma for a squarefree factorization $d = d_1 d_2$. A polynomial $f \in V_n(\mathbb{Z}/d\mathbb{Z})$ projects to $f_1 \in V_n(\mathbb{Z}/d_1\mathbb{Z})$ and $f_2 \in V_n(\mathbb{Z}/d_2\mathbb{Z})$. Conversely, given two such polynomials f_1, f_2, there is a unique polynomial $f \in V_n(\mathbb{Z}/d\mathbb{Z})$ congruent to each, namely

$$f = f_1 d_2 \overline{d_2} + f_2 d_1 \overline{d_1},$$

where $\overline{d_2}$ is any choice of the multiplicative inverse of $d_2 (\mathrm{mod}\, d_1)$, with $\overline{d_1}$ defined analogously. Then

$$\begin{aligned}\widehat{\psi}_d(\mathbf{u}) &= \frac{1}{d^{n+1}} \sum_{f_1 \in V_n(\mathbb{Z}/d_1\mathbb{Z})} \sum_{f_2 \in V_n(\mathbb{Z}/d_2\mathbb{Z})} \psi_{d_1}(f_1)\psi_{d_2}(f_2) e_d(\langle f_1 d_2 \overline{d_2} + f_2 d_1 \overline{d_1}, \mathbf{u}\rangle) \\ &= \widehat{\psi}_{d_1}(\overline{d_2}\mathbf{u})\widehat{\psi}_{d_2}(\overline{d_1}\mathbf{u}).\end{aligned}$$

The lemma follows. □

In subsequent sections, Fourier transforms of this type will naturally appear after an application of Poisson summation on the integer lattices $\mathbb{Z}^{n+1}$ and $\mathbb{Z}^n$. The next two lemmas will be used to control the Fourier side of this application.

Lemma 3.2. *Let d be squarefree and suppose $\psi_d(f) = \prod_{p|d} \psi_p(f)$ is a function where each ψ_p satisfies $\widehat{\psi}_p(\mathbf{u}) \ll p^{-\alpha}$ for some $0 < \alpha < n$ and every $\mathbf{u} \not\equiv \mathbf{0} (\mathrm{mod}\, p)$, and further that $\widehat{\psi}_p(\mathbf{0}) \ll 1$. Then for any $X \geqslant 1$,*

$$\sum_{\substack{\mathbf{u} \in \mathbb{Z}^{n+1} \setminus \mathbf{0} \\ |u_i| \leqslant X \forall i}} \widehat{\psi}_d(\mathbf{u}) \ll X^{n+1} d^{-\alpha}.$$

Here, the sum is over $\mathbf{u} = (u_0, u_1, \ldots, u_n) \in \mathbb{Z}^{n+1} \setminus 0$ where each coordinate satisfies $|u_i| \leqslant X$. Each vector $\mathbf{u}$ is regarded in $(\mathbb{Z}/d\mathbb{Z})^{n+1}$ via the projection map.

Similarly, if $\psi_d^{\mathrm{mon}}(f) = \prod_{p|d} \psi_p^{\mathrm{mon}}(f)$ where $\widehat{\psi}_p^{\mathrm{mon}}(\mathbf{v}) \ll p^{-\beta}$ for some $0 < \beta < (n-1)$ and every $\mathbf{v} \not\equiv \mathbf{0} (\mathrm{mod}\, p)$, and further that $\widehat{\psi}_p(\mathbf{0}) \ll 1$, then

$$\sum_{\substack{\mathbf{v} \in \mathbb{Z}^{n} \setminus \mathbf{0} \\ |v_i| \leqslant X \forall i}} \widehat{\psi}_d^{\mathrm{mon}}(\mathbf{v}) \ll X^{n} d^{-\beta}.$$

Proof. We prove only the general case, the monic case following mutatis mutandis. There are fewer than X^{n+1} choices of $\mathbf{u}$ such that $\mathbf{u} \not\equiv 0 \bmod p$ for each prime divisor p of d. Thus the total contribution from these $\mathbf{u}$ is no larger than the asserted quantity by Lemma 3.1 and our assumption that $\widehat{\psi}_p(\mathbf{u}) \ll p^{-\alpha}$.

It only remains to consider those $\mathbf{u}$ that are congruent to $\mathbf{0}$ modulo at least one prime divisor of d. For each nontrivial divisor m of d, let U_m denote the set of $\mathbf{u} \in \mathbb{Z}^{n+1} \setminus \mathbf{0}$ such that m is the maximal divisor of d with $\mathbf{u} \equiv 0 (\mathrm{mod}\, m)$. Stated differently, to each $\mathbf{u}$ we associate the maximal $m \mid d$ such that $\mathbf{u} \equiv 0 (\mathrm{mod}\, m)$ and we partition these $\mathbf{u}$ into sets U_m.

For each $\mathbf{u} \in U_m$, Lemma 3.1 gives that

$$\widehat{\psi}_d(\mathbf{u}) = \widehat{\psi}_m(\mathbf{0})\widehat{\psi}_{d/m}(c\mathbf{u}) \ll m^\alpha d^{-\alpha},$$

where c is some unit depending on $\mathbf{u}$. As $\# U_m \ll (X/m)^{n+1}$, it follows that

$$\sum_{\substack{\mathbf{u} \in U_m \\ |u_i| \leqslant X \forall i}} \widehat{\psi}_d(\mathbf{u}) \ll \left(\frac{m}{d}\right)^\alpha \left(\frac{X}{m}\right)^{n+1} \ll \frac{X^{n+1}}{d^\alpha m^{n+1-\alpha}}.$$

As d is squarefree, we have that

$$\sum_{m|d} \frac{1}{m^{n+1-\alpha}} = \prod_{p|d} \left(1 + \frac{1}{p^{n+1-\alpha}}\right),$$

which is absolutely bounded since $\alpha < n$. This proves the claim. □

Lemma 3.3. *Make the same assumptions as in Lemma 3.2. If $\phi\colon \mathbb{R}^{n+1} \to \mathbb{R}$ is Schwartz, then for any $X > 0$,*

$$\sum_{\mathbf{u}\in\mathbb{Z}^{n+1}} \widehat{\psi}_d(\mathbf{u})\phi(\mathbf{u}/X) = \widehat{\psi}_d(\mathbf{0})\phi(\mathbf{0}) + O_\phi(X^{n+1}d^{-\alpha}),$$

and if $\mathbb{R}^n \to \mathbb{R}$ is Schwartz, then

$$\sum_{\mathbf{v}\in\mathbb{Z}^{n}} \widehat{\psi}_d(\mathbf{v})\phi(\mathbf{v}/X) = \widehat{\psi}^{\mathrm{mon}}_d(\mathbf{0})\phi(\mathbf{0}) + O_\phi(X^{n}d^{-\beta})$$

for any $X > 0$.

Proof. This follows from Lemma 3.2 and partial summation. □

Finally, we consider the functions that will be of interest to us in the next section, recalling relatively recent work of Porritt [Por18] on the function field analogue of bounds for sums $\max_\theta|\sum_{n\leqslant x}\mu(n)e(n\theta)|$. There is also work of Bienvenu and Lê [BL19] that is qualitatively of the same quality as Porritt's, but less precise for our particular purpose. Additionally, there is also work of Dietmann, Ostafe, and Shparlinski [DOS19] that exploits cancellation in the Fourier transform of the Möbius function in a closely related sieve problem; see in particular [DOS19, Lemma 2.7, Lemma 3.4].

Lemma 3.4. *Let $n \geqslant 3$, p be prime, and define*

$$\psi_p(f) := \frac{1 + (-1)^{n+1}\mu_{p,n}(f)}{2},$$

where $\mu_{p,n}$ is as in (2.1). Then $\widehat{\psi}_p(\mathbf{0}) = \widehat{\psi}^{\mathrm{mon}}_p(\mathbf{0}) = 1/2$ and $\widehat{\psi}_p(\mathbf{u}), \widehat{\psi}^{\mathrm{mon}}_p(\mathbf{u}) \ll_n p^{\frac{1-n}{4}}$ for $\mathbf{u} \not\equiv \mathbf{0} (\mathrm{mod}\, p)$.

Proof. The claim about $\widehat{\psi}_p(\mathbf{0})$ and $\widehat{\psi}^{\mathrm{mon}}_p(\mathbf{0})$ follows from the classical fact that

$$\sum_{f\in V_n(\mathbb{F}_p)} \mu_p(f) = \sum_{f\in V^{\mathrm{mon}}_n(\mathbb{F}_p)} \mu_p(f) = 0$$

for any $n \geqslant 2$. For $\mathbf{u} \not\equiv \mathbf{0}$, the claim about $\widehat{\psi}^{\mathrm{mon}}_p(\mathbf{u})$ follows from [Por18, Theorem 1]. For $\widehat{\psi}_p(\mathbf{u})$, we note that if $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{F}_p[x]$ with $a_n \in \mathbb{F}_p^\times$, then $\mu_p(f) = \mu_p(f/a_n)$. Consequently,

$$\widehat{\psi}_p(\mathbf{u}) = \frac{1}{p}\sum_{c\in\mathbb{F}_p^\times} \widehat{\psi}^{\mathrm{mon}}_p(c\mathbf{u}),$$

which again may be bounded by [Por18, Theorem 1]. □

Combining Lemma 3.3 with Lemma 3.4, we immediately obtain the following corollary.

Corollary 3.5. *Let $n \geqslant 3$, let $\psi_p(f) = \frac{1+(-1)^{n+1}\mu_{p,n}(f)}{2}$ for each prime p, and for squarefree d, let $\psi_d(f) = \prod_{p|d}\psi_p(f)$. If $\phi\colon \mathbb{R}^{n+1} \to \mathbb{R}$ is Schwartz, then for any $X > 0$ and any squarefree d,*

$$\sum_{\mathbf{u}\in\mathbb{Z}^{n+1}} \widehat{\psi}_d(\mathbf{u})\phi(\mathbf{u}/X) = \frac{\phi(\mathbf{0})}{2^{\omega(d)}} + O_\phi(X^{n+1}d^{\frac{1-n}{4}}),$$

where $\omega(d)$ denotes the number of distinct prime divisors of d. Similarly, if $\phi\colon \mathbb{R}^n \to \mathbb{R}$ is Schwartz, then for any $X > 0$ and any squarefree d,

$$\sum_{\mathbf{v}\in\mathbb{Z}^{n}} \widehat{\psi}_d(\mathbf{v})\phi(\mathbf{v}/X) = \frac{\phi(\mathbf{0})}{2^{\omega(d)}} + O_\phi(X^{n}d^{\frac{1-n}{4}}).$$

4. A modified Selberg sieve

In this section, we introduce a modified version of the classical Selberg sieve. Out goal is to prove the following version, which we later specialize using the results from the previous section.

Proposition 4.1. *Let n be a positive integer, H and D be real with $H, D \geqslant 1$, $\phi\colon V_n(\mathbb{R}) \to \mathbb{R}$ be non-negative, and $\{\lambda_d\}$ be a sequence of real numbers indexed by squarefree integers $d \leqslant D$, with $\lambda_1 = 1$. Then*

$$\sum_{\substack{f\in V_n(\mathbb{Z})\\ \mathrm{Gal}(f)\subseteq A_n\\ \mathrm{LDisc}(f)\neq 0}} \frac{\phi(f/H)}{2^{\omega(\mathrm{LDisc}(f))}} \leqslant \sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2} \sum_{f\in V_n(\mathbb{Z})} \phi(f/H) \prod_{p\mid[d_1,d_2]} \left(\frac{1+(-1)^{n+1}\mu_{p,n}(f)}{2}\right). \tag{4.1}$$

This proposition can be viewed as a generalization of the Selberg sieve. Before giving the proof, we first describe what can be obtained by the classical Selberg sieve. (For a treatment of the classical Selberg sieve, see [FI10, §7].) As in the statement of the proposition, we'll assume λ_d is a sequence of real numbers indexed by squarefree $d \leqslant D$ with $\lambda_1 = 1$.

Using the classical Selberg sieve, we would start with the fact that

$$\sum_{f\in V_n(\mathbb{Z})} \phi(f/H) \left(\sum_{d: f(\bmod p) \text{ is odd}, \forall p\mid d} \lambda_d\right)^2 \geqslant 0. \tag{4.2}$$

On one hand, expanding the left hand side of (4.2) we see it is equal to

$$\sum_{d_1,\, d_2} \lambda_{d_1}\lambda_{d_2} \sum_{f\in V_n(\mathbb{Z}): f(\bmod p) \text{ is odd for every } p\mid[d_1,d_2]} \phi(f/H).$$

On the other hand, when $f \in V_n(\mathbb{Z})$ and $\mathrm{Gal}(f) \subseteq A_n$, by Lemma 2.2 we see that $f(\bmod p)$ is never odd for prime p and thus $\sum_{d: f(\bmod p) \text{ is odd}, \forall p\mid d} \lambda_d = \lambda_1 = 1$. By the non-negativity of ϕ, we see (4.2) is at least

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

Hence we have

$$\sum_{\substack{f\in V_n(\mathbb{Z})\\ \mathrm{Gal}(f)\subseteq A_n}} \phi(f/H) \leqslant \sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2} \sum_{f\in V_n(\mathbb{Z}): f(\bmod p) \text{ is odd for every } p\mid[d_1,d_2]} \phi(f/H). \tag{4.3}$$

The inequality (4.2) in Proposition 4.1 should be compared with (4.1).

We initially attempted to use (4.3) instead of (4.1), but the results are less satisfactory. The main reason is that the characteristic function $1^{\mathrm{odd}}_{p,n}$ of odd polynomials in $\mathbb{F}_p[x]$ of degree n have very large Fourier coefficients away from 0.

This is due to the fact (following from Lemma 2.4) that $1^{\mathrm{odd}}_{p,n} = \frac{(-1)^{n+1}\mu_{p,n}+\mu^2_{p,n}}{2}$, since $\mu^2_{p,n}$ is supported on square-free polynomials of degree exactly n. As noted in Section 3, we expect the Fourier transform of $\mu_{p,n}$ to behave well (i.e. be small) away from 0, but one can show that $\mu^2_{p,n}$ has large Fourier coefficients away from 0 (see Remark 5.5 for a similar phenomenon in the monic case).

In order to circumvent this issue, we modify the Selberg sieve to produce the key inequality (4.1). The right hand side of (4.1) maintains the strong Fourier decay of $\mu_{p,n}(f)$ (as shown in Lemma 3.4 and Corollary 3.5) in the local computations after Poisson summation.

Compared to the classical Selberg sieve, the right hand side of (4.1) has more complicated local factors $\frac{1+(-1)^{n+1}\mu_{p,n}(f)}{2}$ that can take the value $1/2$ in addition to the typical 1 and 0. On the left hand side, we have a mild divisor-bound-type loss $2^{-\omega(\mathrm{LDisc}(f))}$. This factor does not meaningfully detract from this application.

We now prove Proposition 4.1.

Proof. The fundamental idea of this proof is to use certain non-negative definite quadratic forms instead of the complete square $(\sum \lambda_d)^2$.

For each $f \in V_n(\mathbb{Z})$, define the quadratic form Q_f in the variables $\{\lambda_d\}$

$$Q_f(\{\lambda_d\}) = \sum_{d_1 d_2} \prod_{p|[d_1,d_2]} \left(\frac{1+(-1)^{n+1}\mu_{p,n}(f)}{2}\right) \lambda_{d_1}\lambda_{d_2}.$$

We claim that each Q_f is non-negative definite. To see this, temporarily extend Q_f to a form on more variables $\{\lambda_d : d \text{ squarefree, every prime factor of } d \text{ is } \leqslant D\}$ using the same definition above. By definition the (d_1, d_2)-entry q_{f,d_1,d_2} of the matrix of Q_f is equal to $\prod_{p|[d_1,d_2]} \left(\frac{1+(-1)^{n+1}\mu_{p,n}(f)}{2}\right)$. In other words, if we write $\nu_{p,n}(f) = \frac{1+(-1)^{n+1}\mu_{p,n}(f)}{2}$, then

$$q_{f,d_1,d_2} = \left(\prod_{p\leqslant D, p\nmid d_1, p\nmid d_2} 1\right) \cdot \left(\prod_{p\leqslant D, p\nmid d_1, p|d_2} \nu_{p,n}(f)\right) \cdot \left(\prod_{p\leqslant D, p|d_1, p\nmid d_2} \nu_{p,n}(f)\right) \cdot \left(\prod_{p\leqslant D, p|d_1, p|d_2} \nu_{p,n}(f)\right).$$

Hence the matrix of the (extended) form Q_f is a tensor product of matrices $M_p (p \leqslant D \text{ prime})$ with $M_p = \begin{pmatrix} 1 & \nu_{p,n}(f) \\ \nu_{p,n}(f) & \nu_{p,n}(f) \end{pmatrix}$. More explicitly, $M_p = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ for $\mu_{p,n}(f) = (-1)^{n+1}$, $M_p = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ for $\mu_{p,n}(f) = (-1)^n$ and $M_p = \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ for $\mu_{p,n}(f) = 0$. From this we see the (extended) form Q_f is non-negative definite. Since the original Q_f is obtained by specifying all $\lambda_d = 0$ for $d > D$ in the extended form, the original form is also non-negative definite.

We now show that whenever $\mathrm{Gal}(f) \subseteq A_n$ and $\mathrm{LDisc}(f) \neq 0$, we have $Q_f \geqslant 2^{-\omega(\mathrm{LDisc}(f))}\lambda_1^2 = 2^{-\omega(\mathrm{LDisc}(f))}$. It suffices to show this for the extended form Q_f as described just above. When $\mathrm{Gal}(f) \subseteq A_n$ and $\mathrm{LDisc}(f) \neq 0$, Lemma 2.5 gives that $\mu_{p,n}(f) \neq (-1)^{n+1}$. Hence $M_p = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ for $p \nmid \mathrm{LDisc}(f)$ and $M_p = \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ for $p \mid \mathrm{LDisc}(f)$. Note that as matrices $\begin{pmatrix} 1 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} \geqslant \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix} \geqslant 0$, where $A \geqslant B$ means that $A - B$ is non-negative definite. Hence as a tensor product, the matrix of the (extended) form Q_f is $\geqslant \begin{pmatrix} 2^{-\omega(\mathrm{LDisc}(f))} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$, which shows that

$$Q_f \geqslant 2^{-\omega(\mathrm{LDisc}(f))}\lambda_1^2. \tag{4.4}$$

The remainder of the proposition is now straightforward. The right hand side of (4.1) is equal to $\sum_{f\in V_n(\mathbb{Z})} \phi(f/H)Q_f$. On the other hand, applying the lower bound (4.4) gives precisely the left hand side of (4.1). □

A similar proof gives also the monic version, which we record as the following proposition.

Proposition 4.2. *Let n be a positive integer, H and D be real with $H, D \geqslant 1$, $\phi\colon V_n^{\mathrm{mon}}(\mathbb{R}) \to \mathbb{R}$ be non-negative, and $\{\lambda_d\}$ be a sequence of real numbers indexed by squarefree integers $d \leqslant D$, with $\lambda_1 = 1$. Then*

$$\sum_{\substack{f\in V_n^{\mathrm{mon}}(\mathbb{Z}) \\ \mathrm{Gal}(f)\subseteq A_n \\ \mathrm{Disc}(f)\neq 0}} \frac{\phi(f/H)}{2^{\omega(\mathrm{Disc}(f))}} \leqslant \sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2} \sum_{f\in V_n^{\mathrm{mon}}(\mathbb{Z})} \phi(f/H) \prod_{p|[d_1,d_2]} \left(\frac{1+(-1)^{n+1}\mu_p(f)}{2}\right).$$

Proof of Theorem 1.1

Next, we use Proposition 4.1 to prove Theorem 1.1.

Theorem 4.3. *Let $n \geqslant 3$ be an integer and let H be real. Define $V_n(\mathbb{Z}; H)$ to be the set of polynomials $f = \sum a_i x^i$ in $V_n(\mathbb{Z})$ with $\max|a_i| \leqslant H$. Define $V_n^{\mathrm{mon}}(\mathbb{Z}; H)$ similarly. Then*

$$\sum_{\substack{f\in V_n(\mathbb{Z};H) \\ \mathrm{Gal}(f)\subseteq A_n \\ \mathrm{LDisc}(f)\neq 0}} \frac{1}{2^{\omega(\mathrm{LDisc}(f))}} \ll_n H^{n+\frac{1}{3}+\frac{8}{9n+21}} (\log H)^{\frac{4}{3n+7}}$$

and

$$\sum_{\substack{f\in V_n^{\mathrm{mon}}(\mathbb{Z};H)\\ \mathrm{Gal}(f)\subseteq A_n\\ \mathrm{Disc}(f)\neq 0}} \frac{1}{2^{\omega(\mathrm{Disc}(f))}} \ll_n H^{n-\frac{2}{3}+\frac{2}{3n+3}}(\log H)^{\frac{4}{3n+3}}.$$

Proof. Choose a Schwartz function $\phi\colon V_n(\mathbb{R})\to\mathbb{R}$ that is greater than or equal to 1 on polynomials whose coefficients lie in $[-1,1]$. For $f\in V_n(\mathbb{Z})$, we let

$$\psi_d(f)=\prod_{p\mid d}\left(\frac{1+(-1)^{n+1}\mu_{p,n}(f)}{2}\right).$$

We apply Proposition 4.1. The sum over f on the right-hand side of (4.1) can be written as

$$\sum_{f\in V_n(\mathbb{Z})}\phi(f/H)\psi_{[d_1,d_2]}(f)=H^{n+1}\sum_{\mathbf{u}\in\mathbb{Z}^{n+1}}\widehat{\phi}\left(\frac{\mathbf{u}H}{[d_1,d_2]}\right)\widehat{\psi}_{[d_1,d_2]}(\mathbf{u})$$

by Poisson summation. By Corollary 3.5, the right-hand side is equal to

$$\frac{H^{n+1}\widehat{\phi}(\mathbf{0})}{2^{\omega([d_1,d_2])}}+O_{\phi,n}([d_1,d_2]^{\frac{3n+5}{4}}).$$

As d_1 and d_2 are squarefree, one can check that $2^{\omega([d_1,d_2])}=\tau(d_1)\tau(d_2)/\tau((d_1,d_2))$, where τ is the divisor function. Substituting this into the full expression from Proposition 4.1, we obtain

$$\sum_{\substack{f\in V_n(\mathbb{Z};H)\\ \mathrm{Gal}(f)\subseteq A_n\\ \mathrm{LDisc}(f)\neq 0}}\frac{1}{2^{\omega(\mathrm{LDisc})(f)}}\leqslant H^{n+1}\widehat{\phi}(0)\sum_{d_1,d_2}\frac{\lambda_{d_1}\lambda_{d_2}}{\tau(d_1)\tau(d_2)}\tau\big((d_1,d_2)\big)+O_{\phi,n}(\sum_{d_1,d_2}|\lambda_{d_1}\lambda_{d_2}|[d_1,d_2]^{\frac{3n+5}{4}}). \tag{4.5}$$

As in the classical Selberg sieve, we diagonalize the quadratic form appearing in the first term to obtain

$$\begin{aligned}\sum_{d_1,d_2}\frac{\lambda_{d_1}\lambda_{d_2}}{\tau(d_1)\tau(d_2)}\tau\big((d_1,d_2)\big)&=\sum_{d_1,d_2}\frac{\lambda_{d_1}\lambda_{d_2}}{\tau(d_1)\tau(d_2)}\sum_{e\mid(d_1,d_2)}1\\&=\sum_e\left(\sum_{d\equiv 0(\mathrm{mod}\,e)}\frac{\lambda_d}{\tau(d)}\right)^2\\&=:\sum_e\xi_e^2,\end{aligned}$$

say, where the ξ_e are again supported on squarefree integers $e\leqslant D$. A Möbius inversion argument shows that

$$\lambda_d=\mu(d)\tau(d)\sum_{e\equiv 0(\mathrm{mod}\,d)}\mu(e)\xi_e. \tag{4.6}$$

Thus the constraint that $\lambda_1=1$ becomes the condition

$$\sum_e\mu(e)\xi_e=1.$$

This prompts us to choose ξ_e proportional to $\mu(e)$,

$$\xi_e=\frac{\mu(e)}{C},\quad C:=\sum_{e\leqslant D}\mu(e)^2,$$

so that

$$\sum_e\xi_e^2=1/C\ll 1/D.$$

The first term in (4.5) is thus

$$O_{\phi,n}(\frac{H^{n+1}}{D}).$$

To understand the second term, we note that the choice $\xi_e = \mu(e)/C$ in (4.6) shows that the terms λ_d satisfy

$$|\lambda_d| \leqslant \tau(d) \sum_{\substack{e \leqslant D \\ e \equiv 0 (\mathrm{mod}\, d)}} \frac{\mu(e)^2}{C} \ll \frac{\tau(d)}{d}.$$

Therefore, the second term in (4.5) is

$$\ll_{\phi,n} \sum_{d_1,d_2} \frac{\tau(d_1)\tau(d_2)[d_1,d_2]^{\frac{3n+5}{4}}}{d_1 d_2} \ll_{\phi,n} D^{\frac{3n+5}{2}} (\log D)^2.$$

Combining these two bounds, we find that

$$\sum_{\substack{f \in V_n(\mathbb{Z};H) \\ \mathrm{Gal}(f) \subseteq A_n \\ \mathrm{LDisc}(f) \neq 0}} \frac{1}{2^{\omega(\mathrm{LDisc})(f)}} \ll_{\phi,n} \frac{H^{n+1}}{D} + D^{\frac{3n+5}{2}} (\log D)^2.$$

This is optimized by choosing $D = H^{\frac{2n+2}{3n+7}} (\log H)^{\frac{-4}{3n+7}}$, which yields the first claim.

For the monic case, an analogous proof using Proposition 4.2 instead of Proposition 4.1 shows that

$$\sum_{\substack{f \in V_n^{\mathrm{mon}}(\mathbb{Z};H) \\ \mathrm{Gal}(f) \subseteq A_n \\ \mathrm{Disc}(f) \neq 0}} \frac{1}{2^{\omega(\mathrm{Disc}(f))}} \ll_{\phi,n} \frac{H^n}{D} + D^{\frac{3n+1}{2}} (\log D)^2.$$

Choosing $D = H^{\frac{2n}{3n+3}} (\log H)^{\frac{-4}{3n+3}}$ gives the second claim. □

5. Almost prime discriminants

In this section, we apply a weighted almost prime sieve as in [FI10, §25] to obtain lower bounds on almost prime values of polynomial discriminants, in a manner in spirit with the earlier sections of this paper. Specifically, we prove

Theorem 5.1. *Let $n \geqslant 3$, and let $H \geqslant 2$. For any $r \geqslant 2n-3$, we have*

$$\#\{f \in V_n^{\mathrm{mon}}(\mathbb{Z}) : \mathrm{ht}(f) \leqslant H, \omega(\mathrm{Disc}(f)) \leqslant r\} \gg_{n,r} \frac{H^n}{\log H},$$

where $\omega(\mathrm{Disc}(f))$ denotes the number of distinct primes dividing the discriminant of the polynomial f.

Since the discriminant of a field cut out by an irreducible polynomial divides that of the polynomial, this also yields lower bounds for the number of degree n number fields with almost prime discriminant.

Theorem 5.2. *Let $n \geqslant 3$, and let $X \geqslant 2$. For any $r \geqslant 2n-3$, we have*

$$\#\{F/\mathbb{Q} : [F:\mathbb{Q}] = n, \mathrm{Disc}(F) \leqslant X, \omega(\mathrm{Disc}(F)) \leqslant r\} \gg_{n,r} \frac{X^{\frac{1}{2}}}{\log^n X},$$

where $\omega(\mathrm{Disc}(F))$ denotes the number of distinct primes dividing the discriminant of the polynomial F. Moreover, if c_n is any constant for which

$$\#\{F/\mathbb{Q} : [F:\mathbb{Q}] = n, \mathrm{Gal}(\widetilde{F}/\mathbb{Q}) \simeq S_n, \mathrm{Disc}(F) \leqslant X\} \ll_n X^{c_n},$$

then we additionally have

$$\#\{F/\mathbb{Q} : [F:\mathbb{Q}] = n, \mathrm{Disc}(F) \leqslant X, \omega(\mathrm{Disc}(F)) \leqslant r\} \gg_{n,r,\epsilon} X^{\frac{1}{2} + \frac{1}{2c_n n(n-1)-2} - \epsilon}.$$

Remark 5.3. It is expected that the choice $c_n = 1$ is admissible for every n in Theorem 5.2, but this is unknown for every $n \geqslant 6$. For $n \geqslant 6$, the smallest known admissible constants are due to Schmidt [Sch95] and Lemke Oliver and Thorne [LT20a]. It follows from these that the choices $c_n = \frac{n+2}{4}$ and $c_n = 1.6(\log n)^2$ are admissible for every $n \geqslant 6$, for example.

In preparation to apply the almost prime sieve, we recall from Lemma 2.1 that given a monic polynomial $f(x) \in \mathbb{Z}[x]$, a prime p divides the discriminant of f if and only if $f(\mathrm{mod}\, p)$ is not squarefree.

Lemma 5.4. *Let $n \geqslant 3$ and let p be prime. Define $\psi_p \colon V_n^{\mathrm{mon}}(\mathbb{F}_p) \to \mathbb{C}$ by setting $\psi_p(f) = 1$ if f is not squarefree and 0 otherwise. Then $\widehat{\psi}_p^{\mathrm{mon}}(\mathbf{0}) = 1/p$, where $\widehat{\psi}_p^{\mathrm{mon}}$ is defined as in §3, and*

$$\widehat{\psi}_p^{\mathrm{mon}}(\mathbf{v}) \ll p^{-2}$$

for $\mathbf{v} \neq \mathbf{0}$.

Proof. For $n \geqslant 2$, the number of monic, squarefree polynomials of degree n over $\mathbb{F}_p$ is $p^n - p^{n-1}$. Thus the number of polynomials that are not squarefree is p^{n-1}, which yields the claim about $\widehat{\psi}_p^{\mathrm{mon}}(\mathbf{0})$, since

$$\widehat{\psi}_p^{\mathrm{mon}}(\mathbf{0}) = \frac{1}{p^n} \sum_{\substack{f \in V_n^{\mathrm{mon}} \\ f \text{ not squarefree}}} 1.$$

For $\mathbf{v} \neq \mathbf{0}$, we note that $\psi_p(f) = 1 - \mathbf{1}_{\mathrm{sf}}(f)$, where $\mathbf{1}_{\mathrm{sf}}$ is the characteristic function of squarefree polynomials. Thus for $\mathbf{v} \neq \mathbf{0}$, $\widehat{\psi}_p^{\mathrm{mon}}(\mathbf{v}) = -\widehat{\mathbf{1}}_{\mathrm{sf}}^{\mathrm{mon}}(\mathbf{v})$. Mimicking the combinatorial, inclusion-exclusion proof counting squarefree integers, we obtain

$$\begin{aligned}
\widehat{\psi}_p^{\mathrm{mon}}(\mathbf{v}) &= \frac{-1}{p^n} \sum_{\substack{f \in V_n^{\mathrm{mon}}(\mathbb{F}_p) \\ f \text{ squarefree}}} e_p(\langle f, \mathbf{v} \rangle_{\mathrm{mon}}) \\
&= \frac{-1}{p^n} \sum_{0 \leqslant d \leqslant n/2} \sum_{g \in V_d^{\mathrm{mon}}(\mathbb{F}_p)} \mu(g) \sum_{f \in V_{n-2d}^{\mathrm{mon}}(\mathbb{F}_p)} e_p(\langle f g^2, \mathbf{v} \rangle_{\mathrm{mon}}) \\
&= \frac{-1}{p^n} \sum_{0 \leqslant d \leqslant n/2} \sum_{g \in V_d^{\mathrm{mon}}(\mathbb{F}_p)} \mu(g) \sum_{f \in V_{n-2d}^{\mathrm{mon}}(\mathbb{F}_p)} e_p(\langle f, T_{g^2} \mathbf{v} \rangle_{\mathrm{mon}}),
\end{aligned}$$

where $T_{g^2} \colon \mathbb{F}_p^n \to \mathbb{F}_p^{n-2d}$ is the map adjoint to the (linear) map corresponding to multiplication by g^2. The interior sum is a complete sum over all polynomials of degree $n - 2d$, and hence is 0 unless $T_{g^2}\mathbf{v} = \mathbf{0}$. When $T_{g^2}\mathbf{v} = \mathbf{0}$, the interior summation is p^{n-2d}. Noting also that $T_1 \mathbf{v} = \mathbf{v} \neq \mathbf{0}$, it follows that

$$\widehat{\psi}_p^{\mathrm{mon}}(\mathbf{v}) = - \sum_{1 \leqslant d \leqslant n/2} \sum_{\substack{g \in V_d^{\mathrm{mon}}(\mathbb{F}_p) \\ T_{g^2}\mathbf{v} = \mathbf{0}}} \frac{\mu(g)}{p^{2d}}.$$

We can trivially bound the sum over $d \geqslant 2$ by ignoring the condition that $T_{g^2}\mathbf{v} = \mathbf{0}$,

$$\sum_{2 \leqslant d \leqslant n/2} \sum_{g \in V_d^{\mathrm{mon}}(\mathbb{F}_p)} \frac{1}{p^{2d}} \leqslant \sum_{2 \leqslant d \leqslant n/2} \frac{1}{p^d} \ll \frac{1}{p^2},$$

which is sufficient. If $d = 1$, then $g = x + \alpha$ for some $\alpha \in \mathbb{F}_p$, and the $(n-2) \times n$ matrix T_{g^2} may be written as

$$T_{(x+\alpha)^2} = \begin{pmatrix}
\alpha^2 & 2\alpha & 1 & 0 & \cdots & 0 \\
0 & \alpha^2 & 2\alpha & 1 & \cdots & 0 \\
\vdots & 0 & \ddots & \ddots & \ddots & 0 \\
0 & \cdots & 0 & \alpha^2 & 2\alpha & 1
\end{pmatrix}.$$

Since $\mathbf{v} \neq \mathbf{0}$, the equation $T_{g^2}\mathbf{v} = \mathbf{0}$ becomes a system of at most quadratic equations in α. This system may or may not have any solutions in α, but by considering a single non-zero equation, it follows that it admits at most 2. Thus the contribution from terms with $d = 1$ is at most $2p^{-2}$, which is sufficient. □

Remark 5.5. Using the argument of Lemma 5.4 but being more careful, it is possible to be more precise about the phases $\mathbf{v}$ at which the Fourier transform $|\widehat{\psi}_p^{\mathrm{mon}}(\mathbf{v})| \gg p^{-2}$, and in general, to identify the phases at which the Fourier transform admits worse than the expected squareroot cancellation. We do not presently see a way to exploit this in our proof of Theorems 5.1 and 5.2, however.

We are now ready to prove Theorem 5.1. We apply the almost prime sieve as described by Friedlander and Iwaniec [FI10, Theorem 25.1]. For convenient reference, we restate that result here.

Proposition 5.6 (Theorem 25.1 of [FI10]). *Let $\{a_n\}$ be a sequence of non-negative numbers which satisfy the linear sieve conditions* [FI10, (1.2), (5.38)],

$$\sum_{\substack{m\leqslant x\\ m\equiv 0 \bmod d}} a_m = g(d)X + R_d(x), \qquad \text{and} \qquad \prod_{w\leqslant p<z} \big(1-g(p)\big)^{-1} \leqslant K\Big(\frac{\log z}{\log w}\Big), \tag{5.1}$$

for a constant $K>1$ and any $z>w\geqslant 2$, and where X is a good approximation to $\sum_{m\leqslant x} a_n$. Suppose that the remainder terms $r_d(x)$ satisfy [FI10, (25.7)]

$$R(x,D|N) := \sum_{d\leqslant D}\Big|\sum_{n\leqslant N}\alpha_n R_{dn}(x)\Big| \ll X(\log x)^{-3} \tag{5.2}$$

for any complex coefficients $|\alpha_n|\leqslant 1$, and where D, N satisfy [FI10, (25.25)]

$$D\geqslant N^{3^r}, \quad DN\geqslant x^{1/\Delta_r+\epsilon}, \tag{5.3}$$

in which

$$\Delta_r := r + \frac{1}{\log 3}\log\big(\tfrac{3}{4}(1+3^{-r})\big).$$

Let $P(z):=\prod_{p<z}p$ and $V(z):=\prod_{p<z}(1-g(p))$. Then

$$\sum_{\substack{n\leqslant x\\ (n,P(z))=1\\ \omega(n)\leqslant r}} a_n \asymp XV(x)$$

for $z=(DN)^{\frac{1}{4}}$, and the implied constant depends on r and ϵ.

Remark 5.7. There is a small typo in the statement of this theorem in [FI10]. In their theorem statement, D and N need to satisfy (25.25), and not (25.27). Note also that they use the notation $\nu(\cdot)$ instead of $\omega(\cdot)$.

Proof of Theorem 5.1. We apply the almost prime sieve as stated in Proposition 5.6.

Let $\phi\colon \mathbb{R}^n\to\mathbb{R}$ be a non-negative Schwartz function supported on $[-1,1]^n$. For $H\geqslant 2$, let $\phi_H(\mathbf{v}) = \phi(\mathbf{v}/H)$. Abusing notation, by identifying $V_n^{\mathrm{mon}}(\mathbb{R})$ with $\mathbb{R}^n$, we may regard ϕ and ϕ_H as Schwartz functions on $V_n^{\mathrm{mon}}(\mathbb{R})$. For any integer $m\geqslant 1$, let

$$a_m := \sum_{\substack{f\in V_n^{\mathrm{mon}}(\mathbb{Z})\\ \mathrm{Disc}(f)=\pm m}} \phi_H(f).$$

Since the discriminant of a polynomial in $V_n^{\mathrm{mon}}(\mathbb{Z})$ of height at most H is $O_n(H^{2n-2})$, the sequence a_m is supported on integers $m\leqslant x$ for some $x\asymp_n H^{2n-2}$. Let $d\geqslant 1$ be a squarefree integer and define $\psi_d := \prod_{p\mid d}\psi_p$, where ψ_p is as in Lemma 5.4. Lemma 2.1 implies that $p\mid \mathrm{Disc}(f)$ exactly when $\psi_p(f)=1$. It follows from Poisson summation that

$$\begin{aligned}\sum_{\substack{m\leqslant x\\ d\mid m}} a_m &= \sum_{f\in V_n^{\mathrm{mon}}(\mathbb{Z})} \phi_H(f)\psi_d(f)\\ &= H^n\sum_{\mathbf{v}\in\mathbb{Z}^n}\hat{\phi}\left(\frac{\mathbf{v}H}{d}\right)\widehat{\psi}_d^{\mathrm{mon}}(\mathbf{v})\\ &= \frac{H^n}{d}\hat{\phi}(\mathbf{0}) + O_\phi(d^{n-2}),\end{aligned}$$

where the last line follows from Lemma 5.4 and Lemma 3.3. Recalling Mertens' famous theorem that $\prod_{p\leqslant x}(1-\frac{1}{p}) = (e^{-\gamma}+o(1))/\log x$, we see that $\{a_m\}$ satisfies the linear sieve conditions (5.1) with $g(d)=1/d$ and $X=H^n\hat{\phi}(\mathbf{0})$.

Moreover, the remainders

$$R_d(x) := \sum_{\substack{m\leqslant x\\ d\mid m}} a_m - \frac{H^n}{d}\hat{\phi}(\mathbf{0})$$

evidently satisfy

$$R(x,D|1) \leqslant \sum_{d\leqslant D}|R_d(x)| \ll_\phi D^{n-1}$$

for any $D \geqslant 1$. This is $\ll X/(\log x)^3$ provided that $D \ll_n H^{n/(n-1)}/(\log H)^{3/(n-1)} \asymp x^{n/2(n-1)^2}/(\log x)^{3/(n-1)}$. For any such D and $N = 1$, we thus have that $\{a_m\}$ satisfies (5.2).

The almost prime sieve (Proposition 5.6) then shows that for any r for which (5.3) is satisfied, we have the asymptotic

$$\sum_{\substack{m \leqslant x \\ \omega(m) \leqslant r}} a_m \geqslant \sum_{\substack{m \leqslant x \\ (m, P(z))=1 \\ \omega(m) \leqslant r}} a_m \asymp_{n,\phi} \frac{H^n}{\log H},$$

and (5.3) is satisfied when

$$\frac{1}{\Delta_r} < \frac{n}{2(n-1)^2}, \quad \Delta_r := r + \frac{1}{\log 3} \log\left(\frac{3}{4}(1 + 3^{-r})\right). \tag{5.4}$$

Noting that $r + \frac{\log(3/4)}{\log 3} < \Delta_r < r$, and that $\frac{\log(3/4)}{\log 3} = -0.26\ldots$, the condition (5.4) is satisfied if

$$r > \frac{2(n-1)^2}{n} + 0.27 = 2n - 3.73 + \frac{2}{n}.$$

In particular, for $n \geqslant 3$, this is true when $r \geqslant 2n - 3$. Since

$$\#\{f \in V_n^{\mathrm{mon}}(\mathbb{Z}) : \mathrm{ht}(f) \leqslant H, \omega(\mathrm{Disc}(f)) \leqslant r\} \gg_\phi \sum_{\substack{m \leqslant x \\ \omega(m) \leqslant r}} a_m,$$

the theorem follows. □

To go from Theorem 5.1 to Theorem 5.2, notice that the lower bound in Theorem 5.1 is larger than the error term in the Hilbert irreducibility theorem. Consequently, the same lower bound holds for the number of irreducible polynomials with almost prime discriminant, as well as for the number of S_n polynomials with almost prime discriminant. In particular, almost all of the polynomials produced by Theorem 5.1 cut out S_n fields of degree n with almost prime discriminant. To prove Theorem 5.2, the key is to understand the number of different polynomials that cut out the same field. For this, we recall a result of Lemke Oliver and Thorne [LT20b].

Lemma 5.8. *Let F be a number field of degree n, and let*

$$M_F(H) = \#\{f \in \mathbb{Z}[x] : \mathbb{Q}[x]/(f(x)) \simeq F, \mathrm{ht}(f) \leqslant H\}.$$

Then $M_F(H) \ll_n H(\log H)^{n-1} \mathrm{Disc}(F)^{\frac{-1}{n^2-n}}$, and in particular $M_F(H) \ll_n H(\log H)^{n-1}$.

Proof. This follows by combining [LT20b, Theorem 2.1] and [LT20b, Lemma 3.1]. □

Proof of Theorem 5.2. We first prove the statement with the lower bound $\gg_{n,r} X^{1/2}$, as it is almost immediate from Theorem 5.1, which produces $\gg_{n,r} H^n/\log H$ irreducible polynomials with Galois group S_n whose discriminants have at most r prime factors, and Lemma 5.8, which implies that at most $H(\log H)^{n-1}$ of these polynomials can cut out the same field. In particular, there will be $\gg_{n,r} H^{n-1}/(\log H)^n$ different fields produced, each of which has discriminant $O_n(H^{2n-2})$. Choosing $H = cX^{1/(2n-2)}$ for a suitable constant c yields the claim.

To obtain the second claim of the theorem, let c_n be as in the statement of the theorem and suppose $H \geqslant 2$. Then for any $Y \geqslant 1$, there holds

$$\sum_{\substack{[F:\mathbb{Q}]=n \\ \mathrm{Gal}(\tilde{F}/\mathbb{Q}) \simeq S_n \\ \mathrm{Disc}(F) \leqslant Y}} M_F(H) \ll_n H(\log H)^{n-1} Y^{c_n - \frac{1}{n^2-n}}$$

from Lemma 5.8 and partial summation. For any $\epsilon > 0$, it follows there is a choice of Y satisfying

$$Y \asymp_{n,\epsilon} H^{\frac{n(n-1)^2}{c_n n(n-1)-1} - \epsilon}$$

such that

$$\sum_{\substack{[F:\mathbb{Q}]=n \\ \mathrm{Disc}(F) \leqslant Y}} M_F(H) \ll_{n,\epsilon} H^{n-\epsilon}.$$

This is smaller than the lower bound produced by Theorem 5.1 on the number of polynomials with almost prime discriminant, almost all of which are irreducible with Galois group S_n by Hilbert irreducibility. Thus, almost all of the polynomials produced by Theorem 5.1 cut out degree n S_n extensions $F/\mathbb{Q}$ of discriminant at least Y. For such fields F, we have $M_F(H) \ll_n H(\log H)^{n-1}Y^{-\frac{1}{n^2-n}}$ by Lemma 5.8. Dividing the total number of polynomials by this upper bound on the multiplicity, we find

$$\#\{F/\mathbb{Q} : [F:\mathbb{Q}] = n, \mathrm{Gal}(\widetilde{F}/\mathbb{Q}) \simeq S_n, \omega(\mathrm{Disc}(F)) \leqslant r, \mathrm{Disc}(F) \ll_n H^{2n-2}\} \gg_{n,r,\epsilon} H^{n-1}(\log H)^{-n}Y^{\frac{1}{n^2-n}}$$
$$\gg_{n,r,\epsilon} H^{n-1+\frac{n-1}{c_n n(n-1)-1}-\epsilon}.$$

Again choosing $H = cX^{\frac{1}{2n-2}}$ for a suitable constant c, the result follows. □

References

[BF99] K. Belabas and E. Fouvry. Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier. *Duke Math. J.*, 98(2):217–268, 1999.

[BL19] Pierre-Yves Bienvenu and Thái Hoàng Lê. Linear and quadratic uniformity of the Möbius function over $\mathbb{F}_q[t]$. *Mathematika*, 65(3):505–529, 2019.

[CD20] Sam Chow and Rainer Dietmann. Enumerative Galois theory for cubics and quartics. *Adv. Math.*, 372:107282, 37, 2020.

[CD21] Sam Chow and Rainer Dietmann. Towards van der Waerden's conjecture, 2021. Preprint available at https://arxiv.org/abs/2106.14593.

[Die12] Rainer Dietmann. On the distribution of Galois groups. *Mathematika*, 58(1):35–44, 2012.

[Die13] Rainer Dietmann. Probabilistic Galois theory. *Bull. Lond. Math. Soc.*, 45(3):453–462, 2013.

[DOS19] Rainer Dietmann, Alina Ostafe, and Igor E. Shparlinski. Discriminants of fields generated by polynomials of given height, 2019. Preprint available at https://arxiv.org/abs/1909.00135.

[FI10] John Friedlander and Henryk Iwaniec. *Opera de Cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.

[Gal73] P. X. Gallagher. The large sieve and probabilistic Galois theory. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 91–101, 1973.

[Jac85] Nathan Jacobson. *Basic algebra. I.* W. H. Freeman and Company, New York, second edition, 1985.

[LT20a] Robert J. Lemke Oliver and Frank Thorne. Upper bounds on number fields of given degree and bounded discriminant, 2020. Preprint available at https://arxiv.org/abs/2005.14110.

[LT20b] Robert J. Lemke Oliver and Frank Thorne. Upper bounds on polynomials with small Galois group. *Mathematika*, 66(4):1054–1059, 2020.

[Por18] Sam Porritt. A note on exponential-Möbius sums over $\mathbb{F}_q[t]$. *Finite Fields and Their Applications*, 51:298–305, 2018.

[Sch95] Wolfgang M. Schmidt. Number fields of given degree and bounded discriminant. *Astérisque*, 228(4):189–195, 1995. Columbia University Number Theory Seminar (New York, 1992).

[TT20a] Takashi Taniguchi and Frank Thorne. Levels of distribution for sieve problems in prehomogeneous vector spaces. *Math. Ann.*, 376(1):1537–1559, 1 2020.

[TT20b] Takashi Taniguchi and Frank Thorne. Orbital exponential sums for prehomogeneous vector spaces. *Amer. J. Math.*, 142(1):177–213, 2020.

[vdW36] B L van der Waerden. Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt. *Monatsh. Math. Phys.*, 43(1):133–147, 1936.

[Zyw10] David Zywina. Hilbert's irreducibility theorem and the larger sieve, 2010. Unpublished. Preprint available at https://arxiv.org/abs/1011.6465.