Squarefree values of polynomial discriminants I

Manjul Bhargava[1] · **Arul Shankar[2]** ·
Xiaoheng Wang[3]

Abstract We determine the density of monic integer polynomials of given
degree $n > 1$ that have squarefree discriminant; in particular, we prove for
the first time that the lower density of such polynomials is positive. Similarly,
we prove that the density of monic integer polynomials $f(x)$, such that $f(x)$
is irreducible and $\mathbb{Z}[x]/(f(x))$ is the ring of integers in its fraction field, is
positive, and is in fact given by $\zeta(2)^{-1}$. It also follows from our methods that
there are $\gg X^{1/2+1/n}$ monogenic number fields of degree n having associated
Galois group S_n and absolute discriminant less than X, and we conjecture that
the exponent in this lower bound is optimal.

1 Introduction

The pupose of this paper is to determine the density of monic integer poly-
nomials of given degree whose discriminant is squarefree. For polynomials

✉ Manjul Bhargava
bhargava@math.princeton.edu

Arul Shankar
ashankar@math.toronto.edu

Xiaoheng Wang
x46wang@uwaterloo.ca

[1] Department of Mathematics, Princeton University, Princeton, NJ 08544, USA

[2] Department of Mathematics, University of Toronto, Toronto, ON M5S 2E4, Canada

[3] Department of Pure Mathematics, University of Waterloo, Waterloo, ON N2L 3G1,
Canada

$f(x) = x^n + a_1x^{n-1} + \cdots + a_n$, the term $(-1)^i a_i$ represents the sum of the i-fold products of the roots of f. It is thus natural to order monic polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ by the height $H(f) := \max\{|a_i|^{1/i}\}$ (see, e.g., [4,18,23]). We determine the density of monic integer polynomials of degree n having squarefree discriminant with respect to the ordering by this height, and show that the density is positive. The existence of infinitely many monic integer polynomials of each degree having squarefree discriminant was first demonstrated by Kedlaya [14]. However, it has not previously been known whether the density exists or even that the lower density is positive.

To state the theorem, define the constants $\lambda_n(p)$ by

$$\lambda_n(p) = \begin{cases} 1 & \text{if } n = 1, \\ 1 - \dfrac{1}{p^2} & \text{if } n = 2, \\ 1 - \dfrac{3p^{n-1} - p^{n-2} + (-1)^n(p-1)^2}{p^n(p+1)} & \text{if } n \geq 3 \end{cases} \tag{1}$$

for $p \neq 2$; also, let $\lambda_1(2) = 1$ and $\lambda_n(2) = 1/2$ for $n \geq 2$. Then a result of Yamamura [26, Proposition 3] states that $\lambda_n(p)$ is the density of monic polynomials of degree n over $\mathbb{Z}_p$ having discriminant indivisible by p^2. Let $\lambda_n := \prod_p \lambda_n(p)$, where the product is over all primes p. We prove:

Theorem 1.1 *Let $n \geq 1$ be an integer. Then when monic integer polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ of degree n are ordered by $H(f) := \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}$, the density having squarefree discriminant $\Delta(f)$ exists and is equal to $\lambda_n > 0$.*

Our method of proof implies that the theorem remains true even if we restrict only to those polynomials of a given degree n having a given number of real roots.

It is easy to see from the definition of the $\lambda_n(p)$ that the λ_n rapidly approach a limit λ as $n \to \infty$, namely,

$$\lambda = \lim_{n \to \infty} \lambda_n = \frac{1}{2} \cdot \prod_{p \geq 3} \left(1 - \frac{3p-1}{p^2(p+1)}\right) \approx 30.7056\%. \tag{2}$$

Therefore, as the degree tends to infinity, the probability that a random monic integer polynomial has squarefree discriminant tends to $\lambda \approx 30.7056\%$.

In algebraic number theory, one often considers number fields that are defined as a quotient ring $K_f := \mathbb{Q}[x]/(f(x))$ for some irreducible integer polynomial $f(x)$. The question naturally arises as to whether $R_f := \mathbb{Z}[x]/(f(x))$ gives the ring of integers of K_f. Our second main theorem states that this is in fact the case for most polynomials $f(x)$. We prove:

Theorem 1.2 *Let $n > 1$ be an integer. Then when monic integer polynomials $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ of degree n are ordered by $H(f)$, the density of polynomials f such that $\mathbb{Z}[x]/(f(x))$ is the ring of integers in its fraction field is $\prod_p (1 - 1/p^2) = \zeta(2)^{-1}$.*

Note that $\zeta(2)^{-1} \approx 60.7927\%$. Since a density of 100% of monic integer polynomials are irreducible (and indeed have associated Galois group S_n) by Hilbert's irreducibility theorem, it follows that $\approx 60.7927\%$ of monic integer polynomials f of any given degree $n > 1$ have the property that f is irreducible and $\mathbb{Z}[x]/(f(x))$ is the maximal order in its fraction field. The quantity

$$\rho_n(p) := 1 - \frac{1}{p^2} \tag{3}$$

represents the density of monic integer polynomials of degree $n > 1$ over $\mathbb{Z}_p$ such that $\mathbb{Z}_p[x]/(f(x))$ is the maximal order in $\mathbb{Q}_p[x]/(f(x))$. The determination of this beautiful p-adic density, and its independence of n, is due to Hendrik Lenstra (see [1, Proposition 3.5]). Theorem 1.2 again holds even if we restrict to polynomials of degree n having a fixed number of real roots.

If the discriminant of an order in a number field is squarefree, then that order must be maximal. Thus the irreducible polynomials counted in Theorem 1.1 are a subset of those counted in Theorem 1.2. The additional usefulness of Theorem 1.1 in some arithmetic applications is that if $f(x)$ is a monic irreducible integer polynomial of degree n with squarefree discriminant, then not only is $\mathbb{Z}[x]/(f(x))$ maximal in the number field $\mathbb{Q}[x]/(f(x))$ but the associated Galois group is necessarily the symmetric group S_n (see, e.g., [15,16,20,25] for further details and applications).

We prove both Theorems 1.1 and 1.2 with power-saving error terms. More precisely, let $V_n(\mathbb{Z})$ denote the subset of $\mathbb{Z}[x]$ consisting of all monic integer polynomials of degree n. Then it is easy to see that

$$\#\{f \in V_n(\mathbb{Z}) : H(f) < X\} = 2^n X^{\frac{n(n+1)}{2}} + O\left(X^{\frac{n(n+1)}{2}-1}\right).$$

We prove

$$\#\{f \in V_n(\mathbb{Z}) : H(f) < X \text{ and } \Delta(f) \text{ squarefree}\}$$
$$= \lambda_n \cdot 2^n X^{\frac{n(n+1)}{2}} + O_\varepsilon\left(X^{\frac{n(n+1)}{2}-\frac{1}{5}+\varepsilon}\right);$$

$$\#\{f \in V_n(\mathbb{Z}) : H(f) < X \text{ and } \mathbb{Z}[x]/(f(x)) \text{ maximal}\}$$
$$= \frac{6}{\pi^2} \cdot 2^n X^{\frac{n(n+1)}{2}} + O_\varepsilon\left(X^{\frac{n(n+1)}{2}-\frac{1}{5}+\varepsilon}\right) \tag{4}$$

for $n > 1$.

These asymptotics imply Theorems 1.1 and 1.2. Since it is known that the number of reducible monic polynomials of a given degree n is of a strictly smaller order of magnitude than the error terms above (see Proposition 4.3), it does not matter whether we require f to be irreducible in the above asymptotic formulae.

Recall that a number field K is called *monogenic* if its ring of integers is generated over $\mathbb{Z}$ by one element, i.e., if $\mathbb{Z}[\theta]$ gives the maximal order of K for some $\theta \in K$. As a further application of our methods, we obtain the following corollary to Theorem 1.1:

Corollary 1.3 *Let $n > 1$. The number of isomorphism classes of number fields of degree n and absolute discriminant less than X that are monogenic and have associated Galois group S_n is $\gg X^{1/2+1/n}$.*

We note that our lower bound for the number of monogenic S_n-number fields of degree n improves slightly the best-known lower bounds for the number of S_n-number fields of degree n, due to Ellenberg and Venkatesh [9, Theorem 1.1], by simply forgetting the monogenicity condition in Corollary 1.3. We conjecture that the exponent in our lower bound in Corollary 1.3 for monogenic number fields of degree n is optimal.

As is illustrated by Corollary 1.3, Theorems 1.1 and 1.2 give a powerful method to produce number fields of a given degree having given properties or invariants. We give one further example of interest. Given a number field K of degree n with r real embeddings $\xi_1, \ldots, \xi_r$ and s complex conjugate pairs of complex embeddings $\xi_{r+1}, \bar{\xi}_{r+1}, \ldots, \xi_{r+s}, \bar{\xi}_{r+s}$, the ring of integers $\mathcal{O}_K$ may naturally be viewed as a lattice in $\mathbb{R}^n$ via the map $x \mapsto (\xi_1(x), \ldots, \xi_{r+s}(x)) \in \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$. We may thus ask about the length of the shortest vector in this lattice generating K.

In their final remark [9, Remark 3.3], Ellenberg and Venkatesh conjecture that the number of number fields K of degree n whose shortest vector in $\mathcal{O}_K$ generating K is of length less than Y is $\asymp Y^{(n-1)(n+2)/2}$. They prove an upper bound of this order of magnitude. We use Theorem 1.2 to prove also a lower bound of this size, thereby proving their conjecture:

Corollary 1.4 *Let $n > 1$. The number of isomorphism classes of number fields K of degree n whose shortest vector in $\mathcal{O}_K$ generating K has length less than Y is $\asymp Y^{(n-1)(n+2)/2}$. The same is true if we further impose the condition that the Galois group of the normal closure of K is S_n.*

Finally, we remark that our methods allow the analogues of all of the above results to be proven with any finite set of local conditions imposed at finitely many places (including at infinity); the orders of magnitudes in these theorems are then seen to remain the same—with different (but easily computable in the cases of Theorems 1.1 and 1.2) positive constants—provided that no local

conditions are imposed that force the set being counted to be empty (i.e., no local conditions are imposed at p in Theorem 1.1 that force p^2 to divide the discriminant, no local conditions are imposed at p in Theorem 1.2 that cause $\mathbb{Z}_p[x]/(f(x))$ to be non-maximal over $\mathbb{Z}_p$, and no local conditions are imposed at p in Corollary 1.3 that cause such number fields to be non-monogenic locally). In fact, we can even impose certain infinite sets of local conditions (see Theorem 4.1).

We now briefly describe our methods. It is easily seen that the desired densities in Theorems 1.1 and 1.2, if they exist, must be bounded above by the Euler products $\prod_p \lambda_n(p)$ and $\prod_p(1 - 1/p^2)$, respectively. The difficulty is to show that these Euler products are also the correct lower bounds. As is standard in sieve theory, to demonstrate the lower bound, a "tail estimate" is required to show that not too many discriminants of polynomials f are divisible by p^2 when p is large relative to the discriminant $\Delta(f)$ of f (here, large means larger than $\Delta(f)^{1/(n-1)}$, say).

For any prime p, and a monic integer polynomial f of degree n such that $p^2 \mid \Delta(f)$, we say that p^2 *strongly divides* $\Delta(f)$ if $p^2 \mid \Delta(f + pg)$ for any integer polynomial g of degree n; otherwise, we say that p^2 *weakly divides* $\Delta(f)$. Then p^2 strongly divides $\Delta(f)$ if and only if f modulo p has at least two distinct multiple roots in $\bar{\mathbb{F}}_p$, or has a root in $\mathbb{F}_p$ of multiplicity at least 3; and p^2 weakly divides $\Delta(f)$ if $p^2 \mid \Delta(f)$ but f modulo p has only one multiple root in $\mathbb{F}_p$ and this root is a simple double root.

For any squarefree positive integer m, let $\mathcal{W}_m^{(1)}$ (resp. $\mathcal{W}_m^{(2)}$) denote the set of monic integer polynomials in $V_n(\mathbb{Z})$ whose discriminant is strongly divisible (resp. weakly divisible) by p^2 for every prime factor p of m. Then we prove tail estimates for $\mathcal{W}_m^{(1)}$ and $\mathcal{W}_m^{(2)}$ separately, as follows.

Theorem 1.5 *For any positive real number M and any $\epsilon > 0$, we have*

(a) $\displaystyle\#\bigcup_{\substack{m > M \\ m \text{ squarefree}}} \{f \in \mathcal{W}_m^{(1)} : H(f) < X\}$

$$= O_\epsilon(X^{n(n+1)/2+\epsilon}/M) + O(X^{n(n+1)/2-1});$$

(b) $\displaystyle\#\bigcup_{\substack{m > M \\ m \text{ squarefree}}} \{f \in \mathcal{W}_m^{(2)} : H(f) < X\}$

$$= O_\epsilon(X^{n(n+1)/2+\epsilon}/M) + O_\epsilon(X^{n(n+1)/2-1/5+\epsilon}),$$

where the implied constants are independent of M and X.

To prove our main theorems, we will use Theorem 1.5 with $M = X^{1/2}$.

The power savings in the error terms above also have applications towards determining the distributions of low-lying zeros in families of Dedekind zeta functions of monogenic degree-n fields; see [21, §5.2].

We prove the estimate in the strongly divisible case (a) of Theorem 1.5 by geometric techniques, namely, a quantitative version of the Ekedahl sieve ([8], [2, Theorem 3.3]). While the proof of [2, Theorem 3.3] uses homogeneous heights, and considers the union over all primes $p > M$, the same proof also applies in our case of weighted homogeneous heights, and a union over all squarefree $m > M$. Since the last coefficient a_n is in a larger range than the other coefficients, we in fact obtain a smaller error term than in [2, Theorem 3.3].

The estimate in the weakly divisible case (b) of Theorem 1.5 is considerably more difficult. Our main idea is to embed polynomials f, whose discriminant is *weakly* divisible by p^2, into a larger space that has more symmetry, such that the invariants under this symmetry are given exactly by the coefficients of f; moreover, we arrange for the image of f in the bigger space to have discriminant *strongly* divisible by p^2. We then count in the bigger space.

More precisely, we make use of the representation of $G = \mathrm{SO}_n$ on the space $W = W_n$ of symmetric $n \times n$ matrices, as studied in [4,23]. We fix A_0 to be the $n \times n$ symmetric matrix with 1's on the anti-diagonal and 0's elsewhere. The group $G = \mathrm{SO}(A_0)$ acts on W via the action $g \cdot B = gBg^t$ for $g \in G$ and $B \in W$. Define the *invariant polynomial* of an element $B \in W$ by

$$f_B(x) = (-1)^{n(n-1)/2} \det(A_0 x - B).$$

Then f_B is a monic polynomial of degree n. It is known (see [3, §4]) that the ring of polynomial invariants for the action of G on W is freely generated by the coefficients of the invariant polynomial. Define the *discriminant* $\Delta(B)$ and *height* $H(B)$ of an element $B \in W$ by $\Delta(B) = \Delta(f_B)$ and $H(B) = H(f_B)$. This representation of G on W was used in [4,23] to study 2-descent on the hyperelliptic curves $C : y^2 = f_B(x)$.

A key step of our proof of Theorem 1.5(b) is the construction, for every positive squarefree integer m, of a map

$$\sigma_m : \mathcal{W}_m^{(2)} \to \frac{1}{4} W(\mathbb{Z}),$$

such that $f_{\sigma_m(f)} = f$ for every $f \in \mathcal{W}_m^{(2)}$; here $\frac{1}{4} W(\mathbb{Z}) \subset W(\mathbb{Q})$ is the lattice of elements B whose coefficients have denominators dividing 4. In our construction, the image of σ_m in fact lies in a special subspace W_0 of W; namely, if $n = 2g + 1$ is odd, then W_0 consists of symmetric matrices $B \in W$ whose top left $g \times g$ block is 0, and if $n = 2g + 2$ is even, then W_0 consists of symmetric matrices $B \in W$ whose top left $g \times (g + 1)$ block is 0. We

associate to any element of W_0 a further polynomial invariant which we call the Q-*invariant* (which is a relative invariant for the subgroup of $SO(A_0)$ that fixes W_0). Next, we show that for elements B in the image of σ_m, we have $|Q(B)| = m$. Finally, even though the discriminant polynomial of $f \in \mathcal{W}_m^{(2)}$ is *weakly* divisible by p^2, the discriminant polynomial of its image $\sigma_m(f)$, when viewed as a polynomial on $W_0 \cap \frac{1}{4} W(\mathbb{Z})$, is *strongly* divisible by p^2. This is the ey point of our construction.

To obtain Theorem 1.5(b), it thus suffices to estimate the number of $G(\mathbb{Z})$-equivalence classes of elements $B \in W_0 \cap \frac{1}{4} W(\mathbb{Z})$ of height less than X having Q-invariant larger than M. This can be reduced to a geometry-of-numbers argument in the spirit of [4,23], although the current count is more subtle in that we are counting certain elements in a cuspidal region of a fundamental domain for the action of $G(\mathbb{Z})$ on $W(\mathbb{R})$. The $G(\mathbb{Q})$-orbits of elements $B \in W_0 \cap W(\mathbb{Q})$ are called *distinguished orbits* in [4,23], as they correspond to the identity 2-Selmer elements of the Jacobians of the corresponding hyperelliptic curves $y^2 = f_B(x)$ over $\mathbb{Q}$; these were not counted separately by the geometry-of-numbers methods of [4,23], as these elements lie deeper in the cusps of the fundamental domains. We develop a method to count those elements in the cusp having bounded height and Q-invariant larger than M, following the arguments of [4,23] while using the invariance and algebraic properties of the Q-invariant polynomial. This yields Theorem 1.5(b), which then allows us to carry out the sieves required to obtain Theorems 1.1 and 1.2.

Corollary 1.3 can be deduced from Theorem 1.1 roughly as follows. Let $g \in V_n(\mathbb{R})$ be a monic real polynomial of degree n and nonzero discriminant having r real roots and $2s$ complex roots. Then $\mathbb{R}[x]/(g(x))$ is isomorphic to $\mathbb{R}^n \cong \mathbb{R}^r \times \mathbb{C}^s$ via its real and complex embeddings. Let θ denote the image of x in $\mathbb{R}[x]/(g(x))$ and let R_g denote the lattice formed by taking the $\mathbb{Z}$-span of $1, \theta, \ldots, \theta^{n-1}$. Suppose further that there exist monic integer polynomials h_i of degree i for $i = 1, \ldots, n-1$ such that $1, h_1(\theta), h_2(\theta), \ldots, h_{n-1}(\theta)$ is the unique Minkowski-reduced basis of R_g; we say that the polynomial $g(x)$ is *strongly quasi-reduced* in this case. Note that if g is an integer polynomial, then the lattice R_g is simply the image of the ring $\mathbb{Z}[x]/(g(x)) \subset \mathbb{R}[x]/(g(x))$ in $\mathbb{R}^n$ via its archimedean embeddings.

When ordered by their heights, we prove that 100% of monic integer polynomials $g(x)$ are strongly quasi-reduced. We furthermore prove that two distinct strongly quasi-reduced integer polynomials $g(x)$ and $g^*(x)$ of degree n with vanishing x^{n-1}-term necessarily yield non-isomorphic rings R_g and R_{g^*}. The proof of the positive density result of Theorem 1.1 then produces $\gg X^{1/2+1/n}$ strongly quasi-reduced monic integer polynomials $g(x)$ of degree n having vanishing x^{n-1}-term, squarefree discriminant, and height less than $X^{1/(n(n-1))}$. These therefore correspond to $\gg X^{1/2+1/n}$ non-isomorphic monogenic rings

of integers in S_n-number fields of degree n having absolute discriminant less than X, and Corollary 1.3 follows.

A similar argument proves Corollary 1.4. Suppose $f(x)$ is a strongly quasi-reduced irreducible monic integer polynomial of degree n with squarefree discriminant $\Delta(f)$. Elementary estimates show that if $H(f) < Y$, then $\|\theta\| \ll Y$, and so the shortest vector in the ring of integers generating the field also has length bounded by $O(Y)$. The above-mentioned result on the number of strongly quasi-reduced irreducible monic integer polynomial of degree n with squarefree discriminant, vanishing x^{n-1}-coefficient, and height bounded by Y then gives the desired lower bound of $\gg Y^{(n-1)(n+2)/2}$. We give full proofs of Corollaries 1.3 and 1.4 in Section 5.

In a subsequent paper [6] (Part II), we prove the corresponding results for non-monic integer polynomials of degree n ordered by the maximum of the absolute values of the coefficients. Namely, we determine the density of such polynomials having squarefree discriminant and the density corresponding to maximal orders. The treatment of non-monic integer polynomials in Part II builds on the ideas here, but involves a number of new ideas due to the fact that there exist non-monic integer polynomials $f(x)$ of degree n for which there are no symmetric integer matrices A and B such that $f(x) = \det(Ax - B)$! (See [5].) This complication requires additional methods to adapt the proof to the non-monic case. The non-monic case has a number of applications as well, including new results towards counting number fields and also to the resolution of a conjecture of Poonen [17] on an arithmetic Bertini theorem for the projective line. The main theorems of this paper are the analogous results for the affine line. The results in [17], building on work of Granville [12], imply versions of Theorems 1.1 and 1.2 conditional on the ABC Conjecture.

This paper is organized as follows. In Sects. 2 and 3, we begin by collecting some algebraic facts about the representation $2 \otimes g \otimes (g+1)$ of $\mathrm{SL}_2 \times \mathrm{GL}_g \times \mathrm{GL}_{g+1}$ and we define the Q-invariant, which is a relative polynomial invariant for this action. We then apply geometry-of-numbers techniques as described above to prove the critical estimates of Theorem 1.5, handling the cases of n odd and n even separately. In Sect. 4, we then show how our main theorems, Theorems 1.1 and 1.2, can be deduced from Theorem 1.5. Finally, in Sect. 5, we prove Corollary 1.3 on the number of monogenic S_n-number fields of degree n having bounded absolute discriminant, as well as Corollary 1.4 on the number of rings of integers in number fields of degree n whose shortest vector generating the number field is of bounded length.

2 A uniformity estimate for odd degree monic polynomials

In this section, we prove the estimate of Theorem 1.5(b) when $n = 2g + 1$ is odd, for any $g \geq 1$.

2.1 Invariant theory for the fundamental representation: SO_n on the space W of symmetric $n \times n$ matrices

Let A_0 denote the $n \times n$ symmetric matrix with 1's on the anti-diagonal and 0's elsewhere. The group $G = SO(A_0)$ acts on W via the action

$$\gamma \cdot B = \gamma B \gamma^t.$$

We recall some of the arithmetic invariant theory for the representation W of $n \times n$ symmetric matrices of the split orthogonal group G; see [4] for more details. The ring of polynomial invariants for the action of $G(\mathbb{C})$ on $W(\mathbb{C})$ is freely generated by the coefficients of the *invariant polynomial $f_B(x)$ of B*, defined by

$$f_B(x) := (-1)^g \det(A_0 x - B)$$

(see [3, §4]). We define the *discriminant* Δ on W by $\Delta(B) = \Delta(f_B)$, and the $G(\mathbb{R})$-invariant *height* of elements in $W(\mathbb{R})$ by $H(B) = H(f_B)$.

Let k be any field of characteristic not 2. For a monic polynomial $f(x) \in k[x]$ of degree n such that $\Delta(f) \neq 0$, let C_f denote the smooth hyperelliptic curve $y^2 = f(x)$ of genus g and let J_f denote the Jacobian of C_f. Then C_f has a rational Weierstrass point at infinity. The stabilizer of an element $B \in W(k)$ with invariant polynomial $f(x)$ is naturally isomorphic to $J_f[2](k)$ by [4, Proposition 5.1], and hence has cardinality at most $\#J_f[2](\bar{k}) = 2^{2g}$, where $\bar{k}$ denotes a separable closure of k.

We say that an element (or the $G(k)$-orbit of an element) $B \in W(k)$ with $\Delta(B) \neq 0$ is *k-distinguished* if there exists a g-dimensional subspace defined over k that is isotropic with respect to both A_0 and B. If B is k-distinguished, then the set of these g-dimensional subspaces over k is in bijection with $J_f[2](k)$ by [4, Proposition 4.1], and so it too has cardinality at most 2^{2g}.

In fact, it is known (see [4, Proposition 5.1]) that the elements of $J_f[2](k)$ are in natural bijection with the even-degree factors of f defined over k. (Note that the number of even-degree factors of f over $\bar{k}$ is indeed 2^{2g}.) In particular, if f is irreducible over k, then the group $J_f[2](k)$ is trivial.

Now let W_0 be the subspace of W consisting of matrices whose top left $g \times g$ block is zero. Then elements B in $W_0(k)$ with nonzero discriminant are all evidently k-distinguished since the g-dimensional subspace Y_g spanned by the first g basis vectors is isotropic with respect to both A_0 and B. Let G_0 denote the subgroup of G consisting of elements γ such that γ^t preserves Y_g. Then G_0 acts on W_0.

An element $\gamma \in G_0$ has the block matrix form

$$\gamma = \begin{pmatrix} \gamma_1 & 0 \\ \delta & \gamma_2 \end{pmatrix} \in \begin{pmatrix} M_{g \times g} & 0 \\ M_{(g+1) \times g} & M_{(g+1) \times (g+1)} \end{pmatrix}, \tag{5}$$

so $\gamma \in G_0$ transforms the top right $g \times (g+1)$ block of an element $B \in W_0$ as follows:

$$(\gamma \cdot B)^{\text{top}} = \gamma_1 B^{\text{top}} \gamma_2^t,$$

where we use the superscript "top" to denote the top right $g \times (g+1)$ block of any given element in W_0. It will be convenient for us to view $(A_0^{\text{top}}, B^{\text{top}})$ as an element of the representation $V_g = 2 \otimes g \otimes (g+1)$ of the group $H_g := \text{SL}_2 \times \text{GL}_g \times \text{GL}_{g+1}$. We have a map $\theta : G_0 \rightarrow H_g$ sending γ expressed in (5) to $(1, \gamma_1, \gamma_2)$. Then we have

$$(A_0^{\text{top}}, (\gamma \cdot B)^{\text{top}}) = \theta(\gamma) \cdot (A_0^{\text{top}}, B^{\text{top}})$$

for $\gamma \in G_0$ and $B \in W_0$.

Next, we construct a relative polynomial invariant for the action of H_g on V_g as follows. We write any $2 \times g \times (g+1)$ matrix v in V_g as a pair (A, B) of $g \times (g+1)$ matrices. Let $M_v(x, y)$ denote the vector of $g \times g$ minors of $Ax - By$, where x and y are indeterminates; in other words, the i-th coordinate of the vector $M_v(x, y)$ is given by $(-1)^{i-1}$ times the determinant of the matrix obtained by removing the i-th column of $Ax - By$. Then $M_v(x, y)$ is a vector of length $g+1$ consisting of binary forms of degree g in x and y, each of which has $g+1$ coefficients. Taking the determinant of the resulting $(g+1) \times (g+1)$ matrix of coefficients of these $g+1$ binary forms in $M_v(x, y)$ then yields a polynomial $Q = Q(v)$ in the coordinates of V_g, which is a relative invariant for the action of H_g. Explicitly, we have

$$Q((\gamma_0, \gamma_1, \gamma_2) \cdot v) = \det(\gamma_1)^{g+1} \det(\gamma_2)^g Q(v). \qquad (6)$$

Indeed, it follows from the definition that the Q-invariant is invariant under the action of the subgroup $\text{SL}_2 \times \text{SL}_g \times \text{SL}_{g+1}$. (Alternatively, the group $\text{SL}_2 \times \text{SL}_g \times \text{SL}_{g+1}$ has no nontrivial characters.) Moreover, we may work over the algebraic closure and write γ_1 and γ_2 as products of scalar matrices and matrices with determinant 1. Finally one can easily check (6) when γ_1 and γ_2 are scalar matrices.

We then define the Q-*invariant* of $B \in W_0$ to be the Q-invariant of $(A_0^{\text{top}}, B^{\text{top}})$:

$$Q(B) := Q(A_0^{\text{top}}, B^{\text{top}}). \qquad (7)$$

Then the Q-invariant is also a relative invariant for the action of G_0 on W_0, since for any $\gamma \in G_0$ expressed in the form (5), we have

$$Q(\gamma \cdot B) = \det(\gamma_1) Q(B). \qquad (8)$$

In fact, we may extend the definition of the Q-invariant to an even larger subset of $W(\mathbb{Q})$ than $W_0(\mathbb{Q})$. We have the following proposition.

Proposition 2.1 *Let $B \in W_0(\mathbb{Q})$ be an element whose invariant polynomial $f(x)$ is irreducible over $\mathbb{Q}$. Then for every $B' \in W_0(\mathbb{Q})$ such that B' is $G(\mathbb{Z})$-equivalent to B, we have $Q(B') = \pm Q(B)$.*

Proof Suppose $B' = \gamma \cdot B$ with $\gamma \in G(\mathbb{Z})$ and $B, B' \in W_0(\mathbb{Q})$. Then Y_g and $\gamma^t Y_g$ are both g-dimensional subspaces over $\mathbb{Q}$ isotropic with respect to both A_0 and B. Since f is irreducible over $\mathbb{Q}$, we have that $J_f[2](\mathbb{Q})$ is trivial, and so these two subspaces must be the same. We conclude that $\gamma \in G_0(\mathbb{Z})$, and thus $Q(\gamma \cdot B) = \pm Q(B)$ by (8). $\qquad\square$

We may thus define the $|Q|$-*invariant* for any element $B \in W(\mathbb{Q})$ that is $G(\mathbb{Z})$-equivalent to some element $B' \in W_0(\mathbb{Q})$ and whose invariant polynomial is irreducible over $\mathbb{Q}$; indeed, we set $|Q|(B) := |Q(B')|$. By Proposition 2.1, this definition of $|Q|(B)$ is independent of the choice of B'. Note that all such elements $B \in W(\mathbb{Q})$ are $\mathbb{Q}$-distinguished.

2.2 Embedding $\mathcal{W}_m^{(2)}$ into $\frac{1}{2}W(\mathbb{Z})$

We begin by describing those monic integer polynomials in $V_n(\mathbb{Z})$ that lie in $\mathcal{W}_m^{(2)}$, i.e., the monic integer polynomials that have discriminant weakly divisible by p^2 for all $p \mid m$.

Proposition 2.2 *Let m be a positive squarefree integer, and let f be a monic integer polynomial whose discriminant is weakly divisible by p^2 for all $p \mid m$. Then there exists an integer ℓ such that $f(x + \ell)$ has the form*

$$f(x + \ell) = x^n + b_1 x^{n-1} + \cdots + b_{n-2}x^2 + b_{n-1}x + b_n \qquad (9)$$

for some integers $b_1, \ldots, b_n$ where m divides b_{n-1} and m^2 divides b_n.

Proof Since m is squarefree, by the Chinese Remainder Theorem it suffices to prove the assertion in the case that $m = p$ is prime. Since p divides the discriminant of f, the reduction of f modulo p must have a repeated factor $h(x)^e$ for some polynomial $h \in \mathbb{F}_p[x]$ and some integer $e \geq 2$. As the discriminant of f is not strongly divisible by p^2, we see that h is linear and $e = 2$. By replacing $f(x)$ by $f(x + \ell)$ for some integer ℓ, if necessary, we may assume that the repeated factor is x^2, i.e., we may assume that $f(x)$ has the form

$$f(x) = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n$$

for some integers $b_1, \ldots, b_n$ such that p divides b_{n-1} and b_n. It remains now to show that p^2 divides b_n.

Viewing the discriminant $\Delta(f)$ as a polynomial in b_n, we write

$$\Delta(f) = b_n \Delta_1 + \Delta_2,$$

for polynomials $\Delta_1 \in \mathbb{Z}[b_1, \ldots, b_n]$ and $\Delta_2 \in \mathbb{Z}[b_1, \ldots, b_{n-1}]$. Next we set b_n to 0 and observe that b_{n-1}^2 divides Δ_2. Indeed, the discriminant of f is equal to the resultant $\mathrm{Res}(f(x), f'(x))$ of $f(x)$ and $f'(x)$. When $b_n = 0$, the only nonzero entry in the last column of the matrix whose determinant computes $\mathrm{Res}(f(x), f'(x))$ is b_{n-1} appearing in the last row. The corresponding minor after removing the last row and column has two nonzero entries in its last column, both of which equal to b_{n-1}. This implies that we can pull out another factor of b_{n-1} from the determinant of this minor. Hence there is a polynomial $\Delta_3 \in \mathbb{Z}[b_1, \ldots, b_{n-1}]$ such that

$$\Delta(f) = b_n \Delta_1 + b_{n-1}^2 \Delta_3. \tag{10}$$

Since p divides b_{n-1} and b_n, we see that $p^2 \mid \Delta(f)$ if and only if $p^2 \mid b_n \Delta_1$. If p^2 does not divide b_n, then p divides Δ_1, which implies that p^2 divides $\Delta(f)$ strongly, a contradiction. Therefore, we have that p^2 divides b_n. $\qquad\square$

Proposition 2.2 identifies the p^2 hidden in the coefficients of a monic polynomial f when p^2 weakly divides $\Delta(f)$. We next construct a matrix in $\frac{1}{2}W_0(\mathbb{Z})$ with invariant polynomial f and where the two p's in p^2 are split apart. For any integers $m, c_1, \ldots, c_n$, consider the matrix

$B_m(c_1, \ldots, c_n)$

$$= \begin{pmatrix}
 & & & & & & & & m & & 0 \\
 & & & & & & & \cdot^{\cdot^{\cdot}} & & \cdot^{\cdot^{\cdot}} & \\
 & & & & & & 1 & 0 & & & \\
 & & & & & 1 & 0 & & & & \\
 & & & & 1 & -c_1 & -c_2/2 & & & & \\
 & & & 1 & 0 & -c_2/2 & -c_3 & -c_4/2 & & & \\
 & & \cdot^{\cdot^{\cdot}} & 0 & & & -c_4/2 & -c_5 & & \cdot^{\cdot} & \\
 m & \cdot^{\cdot^{\cdot}} & & & & & & \cdot^{\cdot} & & \cdot^{\cdot} & -c_{n-1}/2 \\
 0 & & & & & & & & -c_{n-1}/2 & -c_n
\end{pmatrix}$$

$$\tag{11}$$

in $\frac{1}{2}W_0(\mathbb{Z})$. It follows from a direct computation that

$$f_{B_m(c_1,\ldots,c_n)}(x) = x^n + c_1 x^{n-1} + \cdots + c_{n-2}x^2 + mc_{n-1}x + m^2 c_n.$$

We compute the Q-invariant of $B_m(c_1, \ldots, c_n)$. Let $v = (A_0^{\text{top}}, B_m(c_1, \ldots, c_n)^{\text{top}})$ be the corresponding element in V_g. The vector $M_v(x, y)$ of length $g + 1$ of minors of $A_0^{\text{top}} x - B_m(c_1, \ldots, c_n)^{\text{top}} y$ is

$$M_v(x, y) = \begin{pmatrix} x^g \\ x^{g-1}y \\ \vdots \\ xy^{g-1} \\ my^g \end{pmatrix}.$$

Computing the determinant of the $(g + 1) \times (g + 1)$ matrix of coefficients of $M_v(x, y)$ then gives

$$Q(B_m(c_1, \ldots, c_n)) = Q(v) = m.$$

For any integer ℓ, we have

$$\begin{aligned} f_{B_m(c_1, \ldots, c_n) + \ell A_0}(x) &= (-1)^g \det(A_0(x - \ell) - B_m(c_1, \ldots, c_n)) \\ &= f_{B_m(c_1, \ldots, c_n)}(x - \ell), \end{aligned} \tag{12}$$

and by the SL_2-invariance of the Q-invariant,

$$Q(B_m(c_1, \ldots, c_n) + \ell A_0) = Q(B_m(c_1, \ldots, c_n)) = m. \tag{13}$$

Theorem 2.3 *Let m be a positive squarefree integer. There exists a map $\sigma_m : \mathcal{W}_m^{(2)} \to \frac{1}{2} W_0(\mathbb{Z})$ such that for every $f \in \mathcal{W}_m^{(2)}$,*

$$f_{\sigma_m(f)} = f, \qquad Q(\sigma_m(f)) = m. \tag{14}$$

Proof Let f be any element of $\mathcal{W}_m^{(2)}$. By Proposition 2.2, there exists an integer ℓ and integers $c_1, \ldots, c_n$ such that

$$f(x + \ell) = x^n + c_1 x^{n-1} + \cdots + c_{n-2} x^2 + m c_{n-1} x + m^2 c_n.$$

We set $\sigma_m(f) = B_m(c_1, \ldots, c_n) + \ell A_0$. Then (14) follows from (12) and (13). □

We remark that the integer ℓ in the proof of Theorem 2.3 is unique modulo m since it is the unique double root of $f(x)$ modulo every prime factor p of m. Since the invariant polynomial of $\sigma_m(f)$ recovers f, we see that no two elements in the image of σ_m are in the same $G(\mathbb{Z})$-orbit (or even $G(\mathbb{C})$-orbit). Furthermore, by the definition of discriminant on W, we have that

$\Delta(\sigma_m(f)) = \Delta(f)$ is divisible by p^2 for every prime factor p of m. If one varies the coefficients of $\sigma_m(f)$ by multiples of p while keeping the top left $g \times g$ block 0, one can show that p^2 still divides the discriminant of the resulting matrix. In other words, the matrix $\sigma_m(f)$, as an element of $\frac{1}{2}W_0(\mathbb{Z})$, has discriminant *strongly divisible* by p^2. It then seems natural to use the Ekedahl sieve to handle this strongly divisible case. However, the Ekedahl sieve does not apply when the polynomial is not squarefree as a polynomial and as we will show in the sequel, as polynomials in the coordinates of W_0, the discriminant Δ is divisible by Q^2. Instead, we will count elements in $\frac{1}{2}W_0(\mathbb{Z})$ having large Q-invariant using geometry-of-numbers techniques.

More precisely, let $\mathcal{L}$ be the set of elements $v \in \frac{1}{2}W(\mathbb{Z})$ satisfying the following conditions: v is $G(\mathbb{Z})$-equivalent to some element in $\frac{1}{2}W_0(\mathbb{Z})$ and the invariant polynomial of v is irreducible over $\mathbb{Q}$. Then by the remark following Proposition 2.1, we may view $|Q|$ as a function also on $\mathcal{L}$. Using $\mathcal{W}_m^{(2),\mathrm{irr}}$ to denote the set of irreducible polynomials in $\mathcal{W}_m^{(2)}$, we then have the following immediate consequence of Theorem 2.3:

Theorem 2.4 *Let $m > 0$ be a squarefree integer. There exists an injective map*

$$\bar{\sigma}_m : \mathcal{W}_m^{(2),\mathrm{irr}} \to G(\mathbb{Z})\backslash\mathcal{L}$$

such that $f_{\bar{\sigma}_m(f)} = f$ for every $f \in \mathcal{W}_m^{(2),\mathrm{irr}}$. Moreover, for every element B in the $G(\mathbb{Z})$-orbit of an element in the image of $\bar{\sigma}_m$, we have $|Q|(B) = m$.

The number of reducible monic integer polynomials having height less than X is of a strictly smaller order of magnitude than the total number of such polynomials (see, e.g., Proposition 4.3). Thus, for our purposes of proving Theorem 1.5(b), it will suffice to count elements in $\mathcal{W}_m^{(2),\mathrm{irr}}$ of height less than X over all $m > M$, which by Theorem 2.4 we may do by counting these special $G(\mathbb{Z})$-orbits on $\mathcal{L} \subset \frac{1}{2}W(\mathbb{Z})$ having height less than X and $|Q|$-invariant greater than M. More precisely, let $N(\mathcal{L}; M; X)$ denote the number of $G(\mathbb{Z})$-equivalence classes of elements in $\mathcal{L}$ whose $|Q|$-invariant is greater than M and whose height is less than X. Then, by Theorem 2.4, to obtain an upper bound for the left hand side in Theorem 1.5(b), it suffices to obtain the same upper bound for $N(\mathcal{L}; M; X)$.

2.3 Counting $G(\mathbb{Z})$-orbits in $\frac{1}{2}W(\mathbb{Z})$

The counting problem for the representation W of G is studied in [4]. In this section, we recall some of the set up and results of [4].

We remark first that the representation studied in [4] is the subspace of W consisting of symmetric matrices with anti-trace 0. Since this is a linear condition on the anti-diagonal entries, each of which has weight 1 when restricted to the action of the maximal torus (see also (19)), the only difference in not imposing this condition is an extra factor of X in the count. We will in fact make use of the anti-trace-0 version in Sect. 5 in our application to counting fields.

To count $G(\mathbb{Z})$-orbits in a lattice $\frac{1}{2}W(\mathbb{Z})$ in $W(\mathbb{R})$, one begins by constructing fundamental domains for the action of $G(\mathbb{Z})$ on the set of elements in $W(\mathbb{R})$ with nonzero discriminant. A fundamental domain R for the action of $G(\mathbb{R})$ on the set of elements in $W(\mathbb{R})$ with nonzero discriminant and height less than 1 is obtained in [4, §9.1]. The exact shape of R is not important. What is important is that R is (absolutely) bounded. Next a fundamental domain $\mathcal{F}$ for the left multiplication action of $G(\mathbb{Z})$ on $G(\mathbb{R})$ is written down in [4, §9.2]. This is done using the Iwasawa decomposition of $G(\mathbb{R})$ as

$$G(\mathbb{R}) = N(\mathbb{R})TK,$$

where N is a unipotent group consisting of lower triangular matrices, K is compact, and T is the split torus of G given by

$$T = \left\{ \begin{pmatrix} t_1^{-1} & & & & & & \\ & \ddots & & & & & \\ & & t_g^{-1} & & & & \\ & & & 1 & & & \\ & & & & t_g & & \\ & & & & & \ddots & \\ & & & & & & t_1 \end{pmatrix} : t_1, \ldots, t_g \in \mathbb{R} \right\}.$$

We may also make the following change of variables. For $1 \leq i \leq g - 1$, set

$$s_i = t_i / t_{i+1},$$

and set $s_g = t_g$. It follows that for $1 \leq i \leq g$, we have $t_i = s_i s_{i+1} \cdots s_g$. We denote an element of T with coordinates t_i (resp. s_i) by (t) (resp. (s)). A fundamental set for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$ can then be taken to be contained in a *Siegel set*, i.e., contained in $N'T'K$, where N' consists of elements in $N(\mathbb{R})$ whose coefficients are absolutely bounded and $T' \subset T$ consists of elements in $(s) \in T$ with $s_i \geq c$ for some positive constant c.

For any $h \in G(\mathbb{R})$, since $\mathcal{F}h$ remains a fundamental domain for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$, the set $(\mathcal{F}h) \cdot (XR)$ (when viewed as a multiset) is a finite cover of a fundamental domain for the action of $G(\mathbb{Z})$ on the elements in $W(\mathbb{R})$

with nonzero discriminant and height bounded by X. The degree of the cover depends only on the size of stabilizer in $G(\mathbb{R})$ and is thus absolutely bounded by 2^{2g}. The presence of these stabilizers is in fact the reason we consider $\mathcal{F}h \cdot XR$ as a multiset. Hence, we have

$$N(\mathcal{L}; M; X) \ll \#\{B \in ((\mathcal{F}h) \cdot (XR)) \cap \mathcal{L} : |Q|(B) > M\}. \quad (15)$$

Let $\mathcal{G}_1$ be a compact left K-invariant set in $G(\mathbb{R})$ which is the closure of a nonempty open set. Averaging (15) over $h \in \mathcal{G}_1$ and exchanging the order of integration as in [4, §10.1], we obtain

$$N(\mathcal{L}; M; X) \ll \int_{\gamma \in \mathcal{F}} \#\{B \in ((\gamma\mathcal{G}_1) \cdot (XR)) \cap \mathcal{L} : |Q|(B) > M\} d\gamma, \quad (16)$$

where the implied constant depends only on $\mathcal{G}_1$ and R, and where $d\gamma$ is a Haar measure on $G(\mathbb{R})$ given by

$$d\gamma = dn \, \delta(s) d^\times s \, dk,$$

where dn is a Haar measure on the unipotent group $N(\mathbb{R})$, dk is a Haar measure on the compact group K, $d^\times s$ is given by

$$d^\times s := \prod_{i=1}^g \frac{ds_i}{s_i},$$

and

$$\delta(s) = \prod_{k=1}^g s_k^{k^2 - 2kg}; \quad (17)$$

see [4, (10.7)].

Since $s_i \geq c$ for every i, there exists a compact subset N'' of $N(\mathbb{R})$ containing $(t)^{-1} N'(t)$ for all $t \in T'$. Since N'', K, $\mathcal{G}_1$ are compact and R is bounded, the set $E = N'' K \mathcal{G}_1 R$ is bounded. Then we have

$$N(\mathcal{L}; M; X) \ll \int_{s_i \gg 1} \#\{B \in ((s) \cdot XE) \cap \mathcal{L} : |Q|(B) > M\} \delta(s) d^\times s. \quad (18)$$

We denote the coordinates on W by b_{ij}, for $1 \leq i \leq j \leq n$. These coordinates are eigenvectors for the action of T on W^*, the dual of W. Denote the T-weight of a coordinate α on W, or more generally a product α of powers of such coordinates, by $w(\alpha)$. An elementary computation shows that

$$
w(b_{ij}) = \begin{cases}
t_i^{-1} t_j^{-1} & \text{if } i, j \leq g \\
t_i^{-1} & \text{if } i \leq g, \ j = g + 1 \\
t_i^{-1} t_{n-j+1} & \text{if } i \leq g, \ j > g + 1 \\
1 & \text{if } i = j = g + 1 \\
t_{n-j+1} & \text{if } i = g + 1, \ j > g + 1 \\
t_{n-i+1} t_{n-j+1} & \text{if } i, j > g + 1.
\end{cases}
\tag{19}
$$

Then the (i, j)-entry of any $B \in (s) \cdot XE$ is bounded by $X w(b_{ij})$, up to a multiplicative constant depending only on $\mathcal{G}_1$ and R.

Let W^{dist} denote the subset of $W(\mathbb{Q})$ consisting of $\mathbb{Q}$-distinguished elements. Then $\mathcal{L}$ is a subset of W^{dist}. It is shown in [4, §10.2] that most of the lattice points in W^{dist} lie inside the subspace W_{00} consisting of symmetric matrices B whose (i, j)-entries are 0 whenever $i + j < n$. More precisely, we have the following estimates from [4, Propositions 10.5 and 10.7]:

Proposition 2.5 *We have*

$$
\int_{s_i \gg 1} \#\{B \in ((s) \cdot XE) \cap (\tfrac{1}{2} W(\mathbb{Z}) \setminus \tfrac{1}{2} W_{00}(\mathbb{Z})) : b_{11} = 0\} \delta(s) d^{\times} s
$$
$$
= O_\epsilon(X^{n(n+1)/2 - 1 + \epsilon})
\tag{20}
$$

$$
\int_{s_i \gg 1} \#\{B \in ((s) \cdot XE) \cap \mathcal{L} : b_{11} \neq 0\} \delta(s) d^{\times} s
$$
$$
= o(X^{n(n+1)/2}).
\tag{21}
$$

Therefore, to prove Theorem 1.5(b) when n is odd, it remains to obtain a power-saving improvement of (21) and estimate

$$
\int_{s_i \gg 1} \#\{B \in ((s) \cdot XE) \cap \mathcal{L} \cap \tfrac{1}{2} W_{00}(\mathbb{Z}) : |Q|(B) > M\} \delta(s) d^{\times} s. \tag{22}
$$

2.4 Proof of Theorem 1.5(b) for odd n

We begin with a power-saving improvement of (21).

Proposition 2.6 *We have*

$$
\int_{s_i \gg 1} \#\{B \in ((s) \cdot XE) \cap W^{\text{dist}} \cap \tfrac{1}{2} W(\mathbb{Z}) : b_{11} \neq 0\} \delta(s) d^{\times} s
$$
$$
= O_\epsilon(X^{n(n+1)/2 - 1/5 + \epsilon}).
$$

Proof We note that the *p*-adic density of elements in $W(\mathbb{Z}_p)$ that are $\mathbb{Q}_p$-distinguished is bounded uniformly away from 1. In fact, this density is bounded above by $1 - \frac{g}{2g+1} + O(1/p)$ by [4, §10.7]. Then an application of the Selberg sieve exactly as in [22] yields the result. □

We now estimate (22). The *Q*-invariant can also be given a weight by viewing the torus *T* as sitting inside G_0 and using (8). Namely,

$$w(Q) = \prod_{k=1}^{g} t_k^{-1} = \prod_{k=1}^{g} s_k^{-k}. \tag{23}$$

Since the polynomial *Q* is homogeneous of degree $g(g+1)/2$ in the coefficients of W_0, we see that the *Q*-invariant of any $B \in (s) \cdot XE$ is bounded by $X^{g(g+1)/2}w(Q)$, up to a multiplicative constant depending only on $\mathcal{G}_1$ and R.

Although we shall not use this fact directly, the points in $((s) \cdot XE) \cap \frac{1}{2}W_{00}(\mathbb{Z})$ with irreducible invariant polynomial occur predominantly when the coordinates s_i are so large that they force any (half-)integral point of $(s) \cdot XE$ to lie inside W_{00}; this can be deduced by following the proof of Proposition 2.5 and using Proposition 2.6. On the other hand, since the weight of the *Q*-invariant is a product of negative powers of s_i, the *Q*-invariants of points in $((s) \cdot XE) \cap \frac{1}{2}W_{00}(\mathbb{Z})$ become large when the coordinates s_i are small. It is the tension between these two requirements that underlies the proof of the following proposition, which gives the desired power-saving estimate for the number of elements in $((s) \cdot XE) \cap \frac{1}{2}W_{00}(\mathbb{Z})$ having large $|Q|$-invariant.

Proposition 2.7 *We have*

$$\int_{s_i \gg 1} \#\{B \in ((s) \cdot XE) \cap \mathcal{L} \cap \tfrac{1}{2}W_{00}(\mathbb{Z}) : |Q|(B) > M\}\delta(s)d^\times s$$
$$= O\left(\frac{1}{M}X^{n(n+1)/2}\log X\right).$$

Proof First note that if an element in $\frac{1}{2}W_{00}(\mathbb{Z})$ has (i, j)-coordinate 0 for some $i + j = n$, then the element has discriminant 0 and hence is not in $\mathcal{L}$. Since the weight of $b_{i,n-i}$ is s_i^{-1}, to count points in $\mathcal{L}$ it suffices to integrate only in the region where $s_i \ll X$ for all *i*. Furthermore, the condition on the $|Q|$-invariant implies that it suffices to integrate only in the region where $X^{g(g+1)/2}w(Q) \gg M$.

Let *S* denote the set of coordinates of W_{00}, i.e., $S = \{b_{ij} : i + j \geq n\}$. For (s) in the range $1 \ll s_i \ll X$, we have $Xw(\alpha) \gg 1$ for all $\alpha \in S$. Hence the number of lattice points in $(s) \cdot (XE)$ for (s) in this range is $\ll \prod_{\alpha \in S}(Xw(\alpha))$.

Therefore,

$$
\int_{s_i \gg 1} \#\{B \in ((s) \cdot (XE)) \cap \mathcal{L} \cap \tfrac{1}{2} W_{00}(\mathbb{Z}) : |Q(B)| > M\}\delta(s)d^\times s
$$

$$
\ll \int_{1 \ll s_i \ll X,\ X^{g(g+1)/2}w(Q) \gg M} \prod_{\alpha \in S}(Xw(\alpha))\delta(s)d^\times s
$$

$$
\ll \int_{1 \ll s_i \ll X,\ X^{g(g+1)/2}w(Q) \gg M} X^{n(n+1)/2-g^2} \prod_{k=1}^{g} s_k^{2k-1} d^\times s
$$

$$
\ll \frac{1}{M}\int_{s_i=1}^{X} X^{n(n+1)/2-g^2+g(g+1)/2}w(Q)\prod_{k=1}^{g} s_k^{2k-1}d^\times s
$$

$$
\ll \frac{1}{M}\int_{s_i=1}^{X} X^{n(n+1)/2-g(g-1)/2}\prod_{k=1}^{g} s_k^{k-1}d^\times s
$$

$$
\ll \frac{1}{M}X^{n(n+1)/2}\log(X),
$$

where the second inequality follows from the definition (17) of $\delta(s)$ and the computation (19) of the weights of the coordinates b_{ij}, the third inequality follows from the fact that $X^{g(g+1)/2}w(Q) \gg M$, the fourth inequality follows from the computation of the weight of Q in (23), and the $\log X$ factor comes from the integration over s_1.   □

The estimate in Theorem 1.5(b) for odd n now follows from Theorem 2.4 and Propositions 2.5, 2.6 and 2.7, in conjunction with the bound on the number of reducible polynomials proved in Proposition 4.3.

3 A uniformity estimate for even degree monic polynomials

In this section, which is structured similarly to Sect. 2, we prove the estimate of Theorem 1.5(b) when $n = 2g + 2$ is even, for any $g \geq 1$.

3.1 Invariant theory for the fundamental representation: SO_n on the space W of symmetric $n \times n$ matrices

Let A_0 denote the $n \times n$ symmetric matrix with 1's on the anti-diagonal and 0's elsewhere. The group $SO(A_0)$ acts on W via the action

$$
\gamma \cdot B = \gamma B \gamma^t.
$$

The central μ_2 acts trivially and so the action descends to an action of $G = \mathrm{SO}(A_0)/\mu_2$.

We recall some of the arithmetic invariant theory of the representation W of $n \times n$ symmetric matrices of the (projective) split orthogonal group $G = \mathrm{PSO}_n$. See [23] for more details. The ring of polynomial invariants over $\mathbb{C}$ is freely generated by the coefficients of the *invariant polynomial*

$$f_B(x) := (-1)^{g+1} \det(A_0 x - B)$$

(see [23, §2.1, 2.2]). We define the *discriminant* Δ and *height* H on W as the discriminant and height of the invariant polynomial.

Let k be a field of characteristic not 2. For any monic polynomial $f(x) \in k[x]$ of degree n such that $\Delta(f) \neq 0$, let C_f denote the smooth hyperelliptic curve $y^2 = f(x)$ of genus g and let J_f denote its Jacobian. Then C_f has two rational non-Weierstrass points at infinity that are conjugate by the hyperelliptic involution. The stabilizer of an element $B \in W(k)$ with invariant polynomial $f(x)$ is isomorphic to $J_f[2](k)$ by [24, Proposition 2.33], and hence has cardinality at most $\#J_f[2](\bar{k}) = 2^{2g}$, where $\bar{k}$ denotes a separable closure of k.

We say that an element (or the $G(k)$-orbit of an element) $B \in W(k)$ with $\Delta(B) \neq 0$ is *distinguished* if there exists a flag $Y' \subset Y$ defined over k where Y is $(g+1)$-dimensional isotropic with respect to A_0 and Y' is g-dimensional isotropic with respect to B. If B is distinguished, then the set of these flags is in bijection with $J_f[2](k)$ by [24, Proposition 2.32], and so it too has cardinality at most 2^{2g}.

In fact, it is known (see [5, Proposition 22]) that the elements of $J_f[2](k)$ are in natural bijection with the even degree factorizations of f defined over k. (Note that the number of such factorizations of f over $\bar{k}$ is indeed 2^{2g}.) In particular, if f is irreducible over k and does not factor as $g(x)\bar{g}(x)$ over some quadratic extension of k, then the group $J_f[2](k)$ is trivial.

Let W_0 be the subspace of W consisting of matrices whose top left $g \times (g+1)$ block is zero. Then elements B in $W_0(k)$ with nonzero discriminant are all distinguished since the $(g+1)$-dimensional subspace Y_{g+1} spanned by the first $g+1$ basis vectors is isotropic with respect to A_0 and the g-dimensional subspace $Y_g \subset Y_{g+1}$ spanned by the first g basis vectors is isotropic with respect to B. Let G_0 be the parabolic subgroup of G consisting of elements γ such that γ^t preserves the flag $Y_g \subset Y_{g+1}$. Then G_0 acts on W_0.

An element $\gamma \in G_0$ has the block matrix form

$$\gamma = \begin{pmatrix} \gamma_1 & 0 & 0 \\ \delta_1 & \alpha & 0 \\ \delta_2 & \delta_3 & \gamma_2 \end{pmatrix} \in \begin{pmatrix} M_{g \times g} & 0 & 0 \\ M_{1 \times g} & M_{1 \times 1} & M_{1 \times (g+1)} \\ M_{(g+1) \times g} & M_{(g+1) \times 1} & M_{(g+1) \times (g+1)} \end{pmatrix}, \quad (24)$$

so $\gamma \in G_0$ acts on the top right $g \times (g + 1)$ block of an element $B \in W_0$ by

$$\gamma.B^{\text{top}} = \gamma_1 B^{\text{top}} \gamma_2^t,$$

where we use the superscript "top" to denote the top right $g \times (g + 1)$ block of any given element of W_0. We may thus view $(A_0^{\text{top}}, B^{\text{top}})$ as an element of the representation $V_g = 2 \otimes g \otimes (g + 1)$. As before, we define the *Q-invariant* of $B \in W_0$ as the Q-invariant of $(A_0^{\text{top}}, B^{\text{top}})$:

$$Q(B) := Q(A_0^{\text{top}}, B^{\text{top}}). \tag{25}$$

Then the Q-invariant is a relative invariant for the action of G_0 on W_0, i.e., for any $\gamma \in G_0$ in the form (24), we have by (6),

$$Q(\gamma.B) = \det(\gamma_1)^{g+1} \det(\gamma_2)^g Q(B) = \det(\gamma_1)\alpha^{-g} Q(B). \tag{26}$$

In fact, we may extend the definition of the Q-invariant to an even larger subset of $W(\mathbb{Q})$ than $W_0(\mathbb{Q})$. We have the following proposition.

Proposition 3.1 *Let $B \in W_0(\mathbb{Q})$ be an element whose invariant polynomial $f(x)$ is irreducible over $\mathbb{Q}$ and, when $n \geq 4$, does not factor as $g(x)\bar{g}(x)$ over some quadratic extension of $\mathbb{Q}$. Then for every $B' \in W_0(\mathbb{Q})$ such that B' is $G(\mathbb{Z})$-equivalent to B, we have $Q(B') = \pm Q(B)$.*

Proof The assumption on the factorization property of $f(x)$ implies that $J_f[2](\mathbb{Q})$ is trivial. The proof is now identical to that of Proposition 2.1. □

We may thus define the $|Q|$-*invariant* for any element $B \in W(\mathbb{Q})$ that is $G(\mathbb{Z})$-equivalent to some $B' \in W_0(\mathbb{Q})$ and whose invariant polynomial is irreducible over $\mathbb{Q}$ and does not factor as $g(x)\bar{g}(x)$ over any quadratic extension of $\mathbb{Q}$; indeed, we set $|Q|(B) := |Q(B')|$. By Proposition 3.1, this definition of $|Q|(B)$ is independent of the choice of B'. We note again that all such elements $B \in W(\mathbb{Q})$ are distinguished.

3.2 Embedding $\mathcal{W}_m^{(2)}$ into $\frac{1}{4}W(\mathbb{Z})$

Let m be a positive squarefree integer and let f be an monic integer polynomial whose discriminant is weakly divisible by m^2. Then as proved in §2.2, there exists an integer ℓ such that $f(x + \ell)$ has the form

$$f(x + \ell) = x^n + c_1 x^{n-1} + \cdots + c_{n-2}x^2 + mc_{n-1}x + m^2 c_n.$$

Consider the following matrix:

$B_m(c_1, \ldots, c_n)$

$$
=
\begin{pmatrix}
 & & & & & & & & & m & & 0 \\
 & & & & & & & & \ddots & & \ddots & \\
 & & & & & & & 1 & & \ddots & & \\
 & & & & & & 1 & 0 & & & & \\
 & & & & & 1 & -c_1/2 & & & & & \\
 & & & & 1 & -c_1/2 & c_1^2/4 - c_2 & -c_3/2 & & & & \\
 & & & 1 & 0 & & -c_3/2 & -c_4 & -c_5/2 & & & \\
 & & \iddots & & & & & -c_5/2 & -c_6 & \ddots & & \\
 & m & \iddots & & & & & & \ddots & \ddots & & -c_{n-1}/2 \\
 0 & & \iddots & & & & & & & & -c_{n-1}/2 & -c_n
\end{pmatrix}.
$$

$$(27)$$

It follows from a direct computation that

$$
f_{B_m(c_1,\ldots,c_n)}(x) = x^n + c_1 x^{n-1} + \cdots + c_{n-2} x^2 + m c_{n-1} x + m^2 c_n.
$$

We set $\sigma_m(f) := B_m(c_1, \ldots, c_n) + \ell A_0 \in \frac{1}{4} W(\mathbb{Z})$. Then evidently $f_{\sigma_m(f)} = f$. A direct computation again shows that $Q(B_m(c_1, \ldots, c_n)) = m$. Since the Q-invariant on $2 \otimes g \otimes (g+1)$ is SL_2-invariant, we conclude that

$$
Q(\sigma_m(f)) = m.
$$

Theorem 3.2 *Let m be a positive squarefree integer. There exists a map $\sigma_m : \mathcal{W}_m^{(2)} \to \frac{1}{4} W(\mathbb{Z})$ such that for every $f \in \mathcal{W}_m^{(2)}$,*

$$
f_{\sigma_m(f)} = f, \qquad Q(\sigma_m(f)) = m. \tag{28}
$$

Let $\mathcal{L}$ be the set of elements $v \in \frac{1}{4} W(\mathbb{Z})$ that are $G(\mathbb{Z})$-equivalent to some elements of $\frac{1}{4} W_0(\mathbb{Z})$ and such that the invariant polynomial of v is irreducible over $\mathbb{Q}$ and does not factor as $g(x)\bar{g}(x)$ over some quadratic extension of $\mathbb{Q}$. Then by the remark following Proposition 3.1, we may view $|Q|$ as a function also on $\mathcal{L}$. Let $\mathcal{W}_m^{(2),\mathrm{irr}}$ denote the set of polynomials in $\mathcal{W}_m^{(2)}$ that are irreducible over $\mathbb{Q}$ and do not factor as $g(x)\bar{g}(x)$ over any quadratic extension of $\mathbb{Q}$. Then we have the following immediate consequence of Theorem 3.2:

Theorem 3.3 *Let m be a positive squarefree integer. There exists an injective map*

$$
\bar{\sigma}_m : \mathcal{W}_m^{(2),\mathrm{irr}} \to G(\mathbb{Z}) \backslash \mathcal{L}
$$

such that $f_{\bar{\sigma}_m(f)} = f$ for every $f \in \mathcal{W}_m^{(2)}$. Furthermore, every element in every orbit in the image of $\bar{\sigma}_m$ has $|Q|$-invariant m.

The number of monic integer polynomials having height less than X that are reducible or factor as $g(x)\bar{g}(x)$ over some quadratic extension of $\mathbb{Q}$ is of a strictly smaller order of magnitude than the total number of such polynomials (see, e.g., Proposition 4.3). Thus to prove Theorem 1.5(b), it suffices to count the number of elements in $\mathcal{W}_m^{(2),\mathrm{irr}}$ having height less than X over all $m > M$, which, by Theorem 3.3, we may do by counting $G(\mathbb{Z})$-orbits on $\mathcal{L} \subset \frac{1}{4}W(\mathbb{Z})$ having height less than X and $|Q|$-invariant greater than M. More precisely, let $N(\mathcal{L}; M; X)$ denote the number of $G(\mathbb{Z})$-equivalence classes of elements in $\mathcal{L}$ whose $|Q|$-invariant is greater than M and whose height is less than X. We obtain a bound for $N(\mathcal{L}; M; X)$ using the same method as in Sect. 2.

3.3 Counting $G(\mathbb{Z})$-orbits in $\frac{1}{4}W(\mathbb{Z})$

The counting problem for the representation W of G is studied in [23]. In this section, we recall some of the set up and results of [23].

Let R be a fundamental domain for the action of $G(\mathbb{R})$ on the elements of $W(\mathbb{R})$ having nonzero discriminant and height bounded by 1 as constructed in [23, §4.1]. Let $\mathcal{F}$ be a fundamental set for the left multiplication action of $G(\mathbb{Z})$ on $G(\mathbb{R})$ obtained using the Iwasawa decomposition of $G(\mathbb{R})$. More explicitly, we have

$$G(\mathbb{R}) = N(\mathbb{R})TK,$$

where N is a unipotent group consisting of lower triangular matrices, K is compact, and T is the split torus of G given by

$$T = \left\{ \begin{pmatrix} t_1^{-1} & & & & & \\ & \ddots & & & & \\ & & t_{g+1}^{-1} & & & \\ & & & t_{g+1} & & \\ & & & & \ddots & \\ & & & & & t_1 \end{pmatrix} \right\}.$$

We may also make the following change of variables. For $1 \le i \le g$, define s_i to be

$$s_i = t_i/t_{i+1},$$

and let $s_g = t_g t_{g+1}$. We denote an element of T with coordinates t_i (resp. s_i) by (t) (resp. (s)). We may take $\mathcal{F}$ to be contained in a *Siegel set*, i.e., contained in $N'T'K$, where N' consists of elements in $N(\mathbb{R})$ whose coefficients are

absolutely bounded and $T' \subset T$ consists of elements in $(s) \in T$ with $s_i \geq c$ for some positive constant c.

Let $\mathcal{G}_1$ be a compact left K-invariant set in $G(\mathbb{R})$ which is the closure of nonempty open set. Then as in Sect. 2, we have

$$N(\mathcal{L}; M; X) \ll \int_{\gamma \in \mathcal{F}} \#\{B \in ((\gamma\mathcal{G}_1) \cdot (XR)) \cap \mathcal{L} : |Q|(B) > M\}d\gamma, \quad (29)$$

where the implied constant depends only on $\mathcal{G}_1$ and R, and where $d\gamma$ is a Haar measure on $G(\mathbb{R})$ given by

$$d\gamma = dn \, \delta(s)d^\times s \, dk,$$

where dn is a Haar measure on the unipotent group $N(\mathbb{R})$, dk is a Haar measure on the compact group K, $d^\times s$ is given by

$$d^\times s := \prod_{i=1}^{g+1} \frac{ds_i}{s_i},$$

and $\delta(s)$ is given by

$$\delta(s) = \prod_{k=1}^{g-1} s_k^{k^2-2kg-k} \cdot (s_g s_{g+1})^{-g(g+1)/2}; \quad (30)$$

see [23, (20)].

Since $s_i \geq c$ for every i, there exists a compact subset N'' of $N(\mathbb{R})$ containing $(t)^{-1}N'(t)$ for all $t \in T'$. Since N'', K, G_0 are compact and R is bounded, the set $E = N''KG_0R$ is bounded. Then we have

$$N(\mathcal{L}; M; X) \ll \int_{s_i \gg 1} \#\{B \in ((s) \cdot XE) \cap \mathcal{L} : |Q|(B) > M\}\delta(s)d^\times s. \quad (31)$$

As before, we denote the coordinates of W by b_{ij}, for $1 \leq i \leq j \leq n$, and we denote the T-weight of a coordinate α on W, or a product α of powers of such coordinates, by $w(\alpha)$. We compute the weights of the coefficients b_{ij} to be

$$w(b_{ij}) = \begin{cases} t_i^{-1}t_j^{-1} & \text{if } i, j \leq g+1 \\ t_i^{-1}t_{n-j+1} & \text{if } i \leq g+1, \ j > g+1 \\ t_{n-i+1}t_{n-j+1} & \text{if } i, j > g+1. \end{cases} \quad (32)$$

Then the (i, j)-entry of any $B \in (s) \cdot XE$ is bounded by $Xw(b_{ij})$, up to a multiplicative constant depending only on $\mathcal{G}_1$ and R.

Let $W_{00} \subset W$ denote the space of symmetric matrices B such that $b_{ij} = 0$ for $i + j < n$. Let W^{dist} denote the subset of $W(\mathbb{Q})$ consisting of $\mathbb{Q}$-distinguished elements. Then $\mathcal{L}$ is a subset of W^{dist}. It was shown in [23, §4.2] that most of the lattice points in W^{dist} lie inside W_{00}. More precisely, we have the following estimates from [23, Proposition 21 and 23].

Proposition 3.4 *We have*

$$\int_{s_i \gg 1} \#\{B \in ((s) \cdot XE) \cap (\tfrac{1}{4}W(\mathbb{Z}) \setminus \tfrac{1}{4}W_{00}(\mathbb{Z})) : b_{11} = 0\}\delta(s)d^\times s$$
$$= O_\epsilon(X^{n(n+1)/2-1+\epsilon}) \tag{33}$$

$$\int_{s_i \gg 1} \#\{B \in ((s) \cdot XE) \cap \mathcal{L} : b_{11} \neq 0\}\delta(s)d^\times s$$
$$= o(X^{n(n+1)/2}). \tag{34}$$

Therefore, to prove Theorem 1.5(b) when $n = 2g + 2$ is even, it remains to obtain a power saving improvement of (34) and estimate

$$\int_{s_i \gg 1} \#\{B \in ((s) \cdot XE) \cap \mathcal{L} \cap \tfrac{1}{4}W_{00}(\mathbb{Z}) : |Q|(B) > M\}\delta(s)d^\times s. \tag{35}$$

3.4 Proof of Theorem 1.5(b) for even n

We begin with a power saving improvement of (34).

Proposition 3.5 *We have*

$$\int_{s_i \gg 1} \#\{B \in ((s) \cdot XE) \cap W^{\text{dist}} \cap \tfrac{1}{4}W(\mathbb{Z}) : b_{11} \neq 0\}\delta(s)d^\times s$$
$$= O_\epsilon(X^{n(n+1)/2-1/5+\epsilon}).$$

Proof In the proof of [23, Proposition 23], it is shown that the p-adic density of elements in $W(\mathbb{Z}_p)$ that are $\mathbb{Q}_p$-distinguished is bounded uniformly away from 1. Then an application of the Selberg sieve exactly as in [22] yields the result. □

We now estimate (35). The Q-invariant can also be given a weight by viewing the torus T as sitting inside G_0 and using (26). Namely,

$$w(Q) = (t_1 \cdots t_g)^{-1}t_{g+1}^g = \prod_{k=1}^{g} s_k^k. \tag{36}$$

Since the polynomial Q is homogeneous of degree $g(g+1)/2$ in the coefficients of W_0, we see that the Q-invariant of any $B \in (s) \cdot XE$ is bounded by $X^{g(g+1)/2} w(Q)$, up to a multiplicative constant depending only on G_0 and R.

Proposition 3.6 *We have*

$$\int_{s_i \gg 1} \#\{B \in ((s) \cdot (XE)) \cap \mathcal{L} \cap \tfrac{1}{4} W_{00}(\mathbb{Z}) : |Q|(B) > M\} \delta(s) d^\times s$$
$$= O(X^{n(n+1)/2} \log^2 X / M).$$

Proof Analogous to the proof of Proposition 2.7, in order for the set $\{B \in ((s) \cdot (XE)) \cap \mathcal{L} \cap \tfrac{1}{4} W_{00}(\mathbb{Z}) : |Q|(B) > M\}$ to be nonempty, the following conditions must be satisfied:

$$\begin{aligned} X s_i^{-1} &\gg 1, \\ X s_g s_{g+1}^{-1} &\gg 1, \\ X^{g(g+1)/2} w(Q) &\gg M. \end{aligned} \tag{37}$$

Let S denote the set of coordinates of W_{00}, i.e., $S = \{b_{ij} : i + j \geq n\}$. Let $T_{X,M}$ denote the set of (s) satisfying $s_i \gg 1$ and the conditions of (37). Then we have

$$\int_{s_i \gg 1} \#\{B \in ((s) \cdot (XE)) \cap \mathcal{L} \cap \tfrac{1}{2} W_{00}(\mathbb{Z}) : |Q|(B) > M\} \delta(s) d^\times s$$

$$\ll \int_{(s) \in T_{X,M}} \Big(\prod_{\alpha \in S} (X w(\alpha)) \Big) \delta(s) d^\times s$$

$$\ll \int_{(s) \in T_{X,M}} X^{n(n+1)/2 - g(g+1)} \prod_{k=1}^{g-1} s_k^{2k-1} \cdot s_g^{g-1} s_{g+1}^g d^\times s$$

$$\ll \frac{1}{M} \int_{(s) \in T_{X,M}} X^{n(n+1)/2 - g(g+1)/2} w(Q) \prod_{k=1}^{g-1} s_k^{2k-1} \cdot s_g^{g-1} s_{g+1}^g d^\times s$$

$$\ll \frac{1}{M} \int_{(s) \in T_{X,M}} X^{n(n+1)/2 - g(g+1)/2} \prod_{k=1}^{g-1} s_k^{k-1} \cdot s_g^{-1} s_{g+1}^g d^\times s$$

$$\ll \frac{1}{M} \int_{(s) \in T_{X,M}} X^{n(n+1)/2 - g(g+1)/2 + g} \prod_{k=1}^{g-1} s_k^{k-1} \cdot s_g^{g-1} d^\times s$$

$$\ll \frac{1}{M} X^{n(n+1)/2} \log^2(X),$$

where the first inequality follows from the fact that $Xw(b_{ij}) \gg 1$ for all $b_{ij} \in S$ when (s) is in the range $1 \ll s_i \ll X$, the second inequality follows from the definition (30) of $\delta(s)$ and the computation (32) of the weights of the coordinates b_{ij}, the third inequality follows from the fact that $X^{g(g+1)/2}w(Q) \gg M$, the fourth inequality follows from the computation of the weight of Q in (36), the fifth inequality comes from multiplying by the factor $(Xs_g s_{g+1}^{-1})^g \gg 1$, and the $\log^2 X$ factor in the last inequality comes from the integrals over s_1 and s_{g+1}. □

The estimate in Theorem 1.5(b) for even n now follows from Theorem 3.3 and Propositions 3.4, 3.5 and 3.6, in conjunction with the bound on the number of reducible polynomials proved in Proposition 4.3.

4 Proof of the main theorems

In this section, we prove a result from which Theorems 1.1 and 1.2 immediately follow. Let $\Sigma = (\Sigma_v)_v$ be a collection of sets $\Sigma_v \subset V_n(\mathbb{Z}_v)$ indexed by places v of $\mathbb{Q}$, such that Σ_p is defined by congruence conditions modulo some power of p for any finite prime p and $\Sigma_\infty \subset V_n(\mathbb{R})$ consists of all degree-n polynomials f such that the number of real roots of f lies in some fixed nonempty subset of $\{0, \ldots, n\}$. Such a set is called a collection of local specifications. Associate to each collection Σ the subset $\mathcal{V}(\Sigma)$ of $V_n(\mathbb{Z})$ consisting of all elements f that satisfy $f \in \Sigma_v$ for all places v. For any positive integer κ, we say that a collection Σ of local specifications is κ-acceptable if Σ_p is defined by congruence conditions modulo p^κ for all primes p; and for all sufficiently large primes p, the sets Σ_p contain every element $f \in V_n(\mathbb{Z}_p)$ with $p^2 \nmid \Delta(f)$. The local specifications corresponding to Theorems 1.1 and 1.2 are 2-acceptable. For a set $S \subset V_n(\mathbb{Z})$, let S_X denote the set of elements in S with height bounded by X. Then we have the following theorem:

Theorem 4.1 *Let κ be a positive integer and let Σ be a κ-acceptable collection of local specifications. Then*

$$\#\mathcal{V}(\Sigma)_X = \mathrm{Vol}(\Sigma_{\infty, H<1}) \prod_p \mathrm{Vol}(\Sigma_p) \cdot X^{n(n+1)/2} + O_\epsilon(X^{n(n+1)/2 - \min\{1/5, 1/(2\kappa)\} + \epsilon}),$$

where $\Sigma_{\infty, H<1}$ is the set of elements in Σ_∞ having height less than 1*, the volumes of sets in $V_n(\mathbb{Z}_p)$ (resp. $V_n(\mathbb{R})$) are computed with respect to the Haar-measures normalized so that $V_n(\mathbb{Z}_p)$ has volume* 1 *(resp. $V_n(\mathbb{Z})$ has covolume* 1*), and where the implied constant depends only on n and Σ.*

This section is organized as follows. First in §4.1 we prove some estimates for the number of reducible elements in $V_n(\mathbb{Z})$ having bounded height. Then in §4.2, we prove a uniformity estimate on polynomials whose discriminants are

divisible by a large square. We then prove Theorem 4.1 by using this uniformity estimate and a squarefree sieve, from which we then deduce Theorems 1.1 and 1.2.

4.1 Estimates on reducible forms

Let $V_n(\mathbb{Z})$ denote the set of monic integer polynomials of degree n. Let $V_n(\mathbb{Z})^{\text{red}}$ denote the subset of polynomials that are reducible or when $n \geq 4$, factor as $g(x)\bar{g}(x)$ over some quadratic extension of $\mathbb{Q}$. We first give a power saving bound for the number of polynomials in $V_n(\mathbb{Z})^{\text{red}}$ having bounded height. We start with the following lemma.

Lemma 4.2 *The number of elements in $V_n(\mathbb{Z})_X$ that have a rational linear factor is bounded by $O(X^{n(n+1)/2-n+1} \log X)$.*

Proof Consider the polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in V_n(\mathbb{Z})_X.$$

First, note that the number of such polynomials with $a_n = 0$ is bounded by $O(X^{n(n+1)/2-n})$. Next, we assume that $a_n \neq 0$. There are $O(X^{n(n+1)/2-n+1})$ possibilities for the $(n-1)$-tuple $(a_1, a_2, \ldots, a_{n-2}, a_n)$. If $a_n \neq 0$ is fixed, then there are $O(\log X)$ possibilities for the linear factor $x - r$ of $f(x)$, since $r \mid a_n$. By setting $f(r) = 0$, we see that the values of $a_1, a_2, \ldots, a_{n-2}, a_n$, and r determine a_{n-1} uniquely. The lemma follows. □

Following arguments of Dietmann [7], we now prove that the number of reducible monic integer polynomials of bounded height is negligible, with a power-saving error term.

Proposition 4.3 *We have*

$$\#V_n(\mathbb{Z})_X^{\text{red}} = O(X^{n(n+1)/2-n+1} \log X).$$

Proof First, by [7, Lemma 2], we have that

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + t \tag{38}$$

has Galois group S_n over $\mathbb{Q}(t)$ for all $(n-1)$-tuples $(a_1, \ldots, a_{n-1})$ aside from a set S of cardinality $O(X^{(n-1)(n-2)/2})$. Hence, the number of n-tuples $(a_1, \ldots, a_n)$ with height bounded by X such that the Galois group of $x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + t$ over $\mathbb{Q}(t)$ is not S_n is $O(X^{(n-1)(n-2)/2} X^n) = O(X^{n(n+1)/2-n+1})$.

Next, let H be a subgroup of S_n that arises as the Galois group of the splitting field of a polynomial in $V_n(\mathbb{Z})$ with no rational root. For reducible polynomials, we have from [7, Lemma 4] that H has index at least $n(n-1)/2$ in S_n. When $n \geq 4$ is even and the polynomial factors as $g(x)\bar{g}(x)$ over a quadratic extension, the splitting field has degree at most $2(n/2)!$ and so the index of the corresponding Galois group in S_n is again at least $n(n-1)/2$. For fixed $a_1, \ldots, a_{n-1}$ such that the polynomial (38) has Galois group S_n over $\mathbb{Q}(t)$, an argument identical to the proof of [7, Theorem 1] implies that the number of a_n with $|a_n| \leq X^n$ such that the Galois group of the splitting field of $x^n + a_1 x^{n-1} + \cdots a_n$ over $\mathbb{Q}$ is H is bounded by

$$O_\epsilon\left(X^\epsilon \exp\left(\frac{n}{[S_n : H]} \log X + O(1)\right)\right) = O(X^{2/(n-1)+\epsilon}).$$

In conjunction with Lemma 4.2, we thus obtain the estimate

$$\#V_n(\mathbb{Z})_X^{\text{red}} = O(X^{n(n+1)/2-n+1} \log X) + O(X^{n(n+1)/2-n+1})$$
$$+ O_\epsilon(X^{n(n+1)/2-n+2/(n-1)+\epsilon}),$$

and the proposition follows. □

4.2 Proof of Theorem 4.1

Recall that we proved the estimates of Theorem 1.5(b) for odd and even n in §2 and §3, respectively. The estimate of Theorem 1.5(a) is a direct consequence of [2, Theorem 3.5, Lemma 3.6] since the discriminant polynomial on V_n is irreducible. For any positive squarefree integer m, let $\mathcal{W}_m$ denote the set of all elements in $V_n(\mathbb{Z})$ whose discriminants are divisible by m^2. We now prove the following direct consequence of Theorem 1.5.

Theorem 4.4 *Let $\mathcal{W}_{m,X}$ denote the set of elements in $\mathcal{W}_m$ having height bounded by X. For any positive real number M, we have*

$$\sum_{\substack{m > M \\ m \text{ squarefree}}} \#\mathcal{W}_{m,X} = O_\epsilon(X^{n(n+1)/2+\epsilon}/\sqrt{M}) + O_\epsilon(X^{n(n+1)/2-1/5+\epsilon}). \quad (39)$$

Proof Note first that an element $f \in V_n(\mathbb{Z})$ belongs to at most $O(X^\epsilon)$ different sets $\mathcal{W}_m$, since m is a divisor of $\Delta(f)$. Hence it suffices to prove the bound (39) for the number of elements in the union of $\mathcal{W}_{m,X}$ over all squarefree integers $m > M$. Now suppose f is an element in this union. Let k_1 denote the product of all the primes p where p^2 strongly divides $\Delta(f)$ and let k_2

denote the product of all the primes p where p^2 weakly divides $\Delta(f)$. Then $f \in \mathcal{W}_{k_1}^{(1)} \cap \mathcal{W}_{k_2}^{(2)}$ with $k_1 k_2 > M$. In other words,

$$\bigcup_{\substack{m > M \\ m \text{ squarefree}}} \mathcal{W}_{m,X} \subset \bigcup_{\substack{k_1 > \sqrt{M} \\ k_1 \text{ squarefree}}} \mathcal{W}_{k_1,X}^{(1)} \cup \bigcup_{\substack{k_2 > \sqrt{M} \\ k_2 \text{ squarefree}}} \mathcal{W}_{k,X}^{(2)}.$$

The theorem now follows from Parts (a) and (b) of Theorem 1.5. □

We remark that the $\sqrt{M}$ in the denominator in (39) can be improved to M. However we will be using Theorem 4.4 for $M = X^{1/\kappa}$ (where $\kappa = 2$ for the application to Theorems 1.1 and 1.2) in which case the second term $O_\epsilon(X^{n(n+1)/2-1/5+\epsilon})$ sometimes dominates. We outline here how to improve the denominator to M for the sake of completeness. Break up $\mathcal{W}_m$ into sets $\mathcal{W}_{m_1}^{(1)} \cap \mathcal{W}_{m_2}^{(2)}$ for positive squarefree integers m_1, m_2 with $m_1 m_2 = m$ as above. Break the ranges of m_1 and m_2 into dyadic ranges. For each range, we count the number of elements in $\mathcal{W}_{m_1}^{(1)} \cap \mathcal{W}_{m_2}^{(2)}$ by embedding each $\mathcal{W}_{m_2}^{(2)}$ into $\frac{1}{4}W(\mathbb{Z})$ as in Sects. 2 and 3. Earlier, we bounded the cardinality of the image of $\mathcal{W}_{m_2,X}^{(2)}$ by splitting $\frac{1}{4}W(\mathbb{Z})$ up into two pieces: $\frac{1}{4}W_{00}(\mathbb{Z})$ and $\frac{1}{4}W(\mathbb{Z}) \setminus \frac{1}{4}W_{00}(\mathbb{Z})$. The bound on the second piece does not depend on m_2 and continues to be $O_\epsilon(X^{n(n+1)/2-1/5+\epsilon})$. However for the first piece, we now impose the further condition that elements in $\frac{1}{4}W_{00}(\mathbb{Z})$ are strongly divisible by p^2 for all prime factors p of m_1 and apply the quantitative version of the Ekedahl sieve as in [2]. This gives the desired additional $1/m_1$ saving, improving the bound to

$$O_\epsilon(X^{n(n+1)/2+\epsilon}/M) + O_\epsilon(X^{n(n+1)/2-1/5+\epsilon}).$$

The reason for counting in dyadic ranges of m_1 and m_2 is that for both the strongly and weakly divisible cases, we count not for a fixed m but sum over all $m > M$.

Let $(\Sigma_v)_v$ be a κ-acceptable collection of local specifications. Let N denote a positive integer such that for every prime $p > N$, the set Σ_p contains every element $f \in V_n(\mathbb{Z}_p)$ with $p^2 \nmid \Delta(f)$. Let P denote the product of all primes $p \leq N$. For squarefree integers m, we let $\mathcal{W}_m(\Sigma)$ denote the set of elements f such that $f \notin \Sigma_p$ for all $p \mid m$ and let m' denote the product of all the prime factors of m that are larger than N. Then $m' \geq m/P$ and $\mathcal{W}_m(\Sigma) \subset \mathcal{W}_{m'}$. Since P depends only on Σ, we may assume that $\log X > P$ in what follows. In other words, we have

$$\sum_{\substack{m > X^{1/\kappa} \\ m \text{ squarefree}}} \#\mathcal{W}_m(\Sigma)_X \leq \sum_{\substack{m' > X^{1/\kappa-\epsilon} \\ m' \text{ squarefree}}} \#\mathcal{W}_{m',X}. \tag{40}$$

For each prime p, let $\theta(p)$ denote $\mathrm{Vol}(\Sigma_p)$, let $\theta(\infty)$ denote $\mathrm{Vol}(\Sigma_{\infty, H<1})$, and set $\bar{\theta}(p) := 1 - \theta(p)$. We define $\bar{\theta}(m) = \prod_{p|m} \bar{\theta}(m)$ for squarefree integers m. Let μ denote the Möbius function. We have

$$
\begin{aligned}
\#\mathcal{V}(\Sigma)_X &= \sum_{m \geq 1} \mu(m) \#\mathcal{W}_m(\Sigma)_X \\
&= \sum_{m=1}^{X^{1/\kappa}} \mu(m)\theta(\infty)\bar{\theta}(m) X^{n(n+1)/2} + O\left(\sum_{m=1}^{X^{1/\kappa}} X^{n(n+1)/2-n}\right) \\
&\quad + O\left(\sum_{m > X^{1/\kappa}} \#\mathcal{W}_m(\Sigma)_X\right) \\
&= \theta(\infty) \prod_p \theta(p) \cdot X^{n(n+1)/2} + O_\epsilon(X^{n(n+1)/2-1/(2\kappa)+\epsilon}) \\
&\quad + O_\epsilon(X^{n(n+1)/2-1/5+\epsilon}),
\end{aligned}
\tag{41}
$$

where the final equality follows from (40) and Theorem 4.4. This concludes the proof of Theorem 4.1.

Finally note that Theorems 1.1 and 1.2 follow from Theorem 4.1 since the corresponding families are 2-acceptable, and the constants λ_n and $\zeta(2)^{-1}$ appearing in these theorems are equal simply to $\prod_p \lambda_n(p)$ and $\prod_p \rho_n(p)$, respectively.

5 A lower bound on the number of degree-n number fields that are monogenic/have a short generating vector

Let $g \in V_n(\mathbb{R})$ be a monic real polynomial of degree n and nonzero discriminant with r real roots and $2s$ complex roots. Then $\mathbb{R}[x]/(g(x))$ is naturally isomorphic to $\mathbb{R}^n \cong \mathbb{R}^r \times \mathbb{C}^s$ as $\mathbb{R}$-vector spaces via its real and complex embeddings (where we view $\mathbb{C}$ as $\mathbb{R} + \mathbb{R}\sqrt{-1}$). The $\mathbb{R}$-vector space $\mathbb{R}[x]/(g(x))$ also comes equipped with a natural basis, namely $1, \theta, \theta^2, \ldots, \theta^{n-1}$, where θ denotes the image of x in $\mathbb{R}[x]/(g(x))$. Let R_g denote the lattice spanned by $1, \theta, \ldots, \theta^{n-1}$. In the case that g is an integral polynomial in $V_n(\mathbb{Z})$, the lattice R_g may be identified with the ring $\mathbb{Z}[x]/(g(x)) \subset \mathbb{R}[x]/(g(x)) \subset \mathbb{R}^n$.

Since $g(x)$ gives a lattice in $\mathbb{R}^n$ in this way, we may ask whether this basis is reduced in the sense of Minkowski, with respect to the usual inner product on $\mathbb{R}^n$.[1] More generally, for any monic real polynomial $g(x)$ of degree n and nonzero discriminant, we may ask whether the basis $1, \theta, \theta^2, \ldots, \theta^{n-1}$ is Minkowski-reduced for the lattice R_g, up to a unipotent upper-triangular

---

[1] Recall that a $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ of a lattice L is called *Minkowski-reduced* if successively for $i = 1, \ldots, n$ the vector α_i is the shortest vector in L such that $\alpha_1, \ldots, \alpha_i$ can be extended to a $\mathbb{Z}$-basis of L. Most lattices have a unique Minkowski-reduced basis.

transformation over $\mathbb{Z}$ (i.e., when the basis $[1 \ \theta \ \theta^2 \ \cdots \ \theta^{n-1}]$ is replaced by $[1 \ \theta \ \theta^2 \ \cdots \ \theta^{n-1}]A$ for some upper triangular $n \times n$ integer matrix A with 1's on the diagonal).

More precisely, given $g \in V_n(\mathbb{R})$ of nonzero discriminant, let us say that the corresponding basis $1, \theta, \theta^2, \ldots, \theta^{n-1}$ of $\mathbb{R}^n$ is *quasi-reduced* if there exist monic integer polynomials h_i of degree i, for $i = 1, \ldots, n-1$, such that the basis $1, h_1(\theta), h_2(\theta), \ldots, h_{n-1}(\theta)$ of R_g is Minkowski-reduced (so that the basis $1, \theta, \theta^2, \ldots, \theta^{n-1}$ is Minkowski-reduced up to a unipotent upper-triangular transformation over $\mathbb{Z}$). By abuse of language, we then call the polynomial g *quasi-reduced* as well. We say that g is *strongly quasi-reduced* if in addition $\mathbb{Z}[x]/(g(x))$ has a unique Minkowski-reduced basis.

The relevance of being strongly quasi-reduced is contained in the following lemma.

Lemma 5.1 *Let $g(x)$ and $g^*(x)$ be distinct monic integer polynomials of degree n and nonzero discriminant that are strongly quasi-reduced and whose x^{n-1}-coefficients vanish. Then $\mathbb{Z}[x]/(g(x))$ and $\mathbb{Z}[x]/(g^*(x))$ are non-isomorphic rings.*

Proof Let θ and θ^* denote the images of x in $\mathbb{Z}[x]/(g(x))$ and $\mathbb{Z}[x]/(g^*(x))$, respectively. By the assumption that g and g^* are strongly quasi-reduced, we have that $1, h_1(\theta), h_2(\theta), \ldots, h_{n-1}(\theta)$ and $1, h_1^*(\theta^*), h_2^*(\theta^*), \ldots, h_{n-1}^*(\theta^*)$ are the unique Minkowski-reduced bases of $\mathbb{Z}[x]/(g(x))$ and $\mathbb{Z}[x]/(g^*(x))$, respectively, for some monic integer polynomials h_i and h_i^* of degree i for $i = 1, \ldots, n-1$.

If $\phi : \mathbb{Z}[x]/(g(x)) \rightarrow \mathbb{Z}[x]/(g^*(x))$ is a ring isomorphism, then by the uniqueness of Minkowski-reduced bases for these rings, ϕ must map Minkowski basis elements to Minkowski basis elements, i.e., $\phi(h_i(\theta)) = h_i^*(\theta^*)$ for all i. In particular, this is true for $i = 1$, so $\phi(\theta) = \theta^* + c$ for some $c \in \mathbb{Z}$, since h_1 and h_1^* are monic integer linear polynomials. Therefore θ and $\theta^* + c$ must have the same minimal polynomial, i.e., $g(x) = g^*(x - c)$; the assumption that θ and θ^* both have trace 0 then implies that $c = 0$. It follows that $g(x) = g^*(x)$, a contradiction. We conclude that $\mathbb{Z}[x]/(g(x))$ and $\mathbb{Z}[x]/(g^*(x))$ must be non-isomorphic rings, as desired. $\square$

The condition of being quasi-reduced is fairly easy to attain:

Lemma 5.2 *If $g(x)$ is a monic real polynomial of nonzero discriminant, then $g(\rho x)$ is quasi-reduced for any sufficiently large $\rho > 0$.*

Proof This is easily seen from the Iwasawa-decomposition description of Minkowski reduction. Consider the fundamental domain $\mathcal{F}_{SL}$ for the action of $SL_n(\mathbb{Z})$ on $SL_n(\mathbb{R})$ given by

$$\mathcal{F}_{SL} = \{\gamma = \nu\tau\kappa : \ \nu \in N' \ \tau \in T'; \kappa \in SO_n(\mathbb{R})\},$$

where N' denotes a compact subset (depending on τ) of the group of lower-triangular matrices and T' is the group of diagonal matrices $(t_1, \ldots, t_n)$ with $t_i \leq c\, t_{i+1}$ for all i and some absolute constant $c = c_n > 0$. Given an n-ary positive definite integer-valued quadratic form Q, viewed as a symmetric $n \times n$ matrix, we write $Q = \gamma I_n \gamma^T$, where I_n is the sum-of-n-squares diagonal quadratic form and $\gamma = \nu\tau \in \mathrm{SL}_n(\mathbb{R})$ is unique up to right multiplication by an element in $\mathrm{SO}_n(\mathbb{R})$. The condition that Q is Minkowski reduced is equivalent to the condition that γ belongs to $\mathcal{F}_{\mathrm{SL}}$. The condition that Q be quasi-reduced is simply then that $t_i \leq c\, t_{i+1}$ (with no condition on ν).

Consider the natural isomorphism $\mathbb{R}[x]/(g(x)) \to \mathbb{R}[x]/(g(\rho x))$ of étale $\mathbb{R}$-algebras defined by $x \to \rho x$. If θ denotes the image of x in $\mathbb{R}[x]/(g(x))$, then $\rho\theta$ is the image of x in $\mathbb{R}[x]/(g(\rho x))$ under this isomorphism. Let Q_1 be the Gram matrix of the lattice basis $1, \theta, \theta^2, \ldots, \theta^{n-1}$ in $\mathbb{R}^n$ and Q_ρ be the Gram matrix of the lattice basis $1, \rho\theta, \rho^2\theta^2, \ldots, \rho^{n-1}\theta^{n-1}$ in $\mathbb{R}^n$. If the element $\tau \in T$ corresponding to $g(x)$ is $(t_1, \ldots, t_n)$, then the element $\tau_\rho \in T$ corresponding to $g(\rho x)$ is $(t_1, \rho t_2, \rho^2 t_3, \ldots, \rho^{n-1} t_n)$. This is because $Q_\rho = \Lambda Q_1 \Lambda^T$, where Λ is the diagonal matrix $(1, \rho, \rho^2, \ldots, \rho^{n-1})$; therefore, if $Q_1 = (\nu\tau\kappa)I_n(\nu\tau\kappa)^T$, then

$$Q_\rho = (\Lambda\nu\tau\kappa)I_n(\Lambda\nu\tau\kappa)^T = (\nu'(\Lambda\tau)\kappa)I_n(\nu'(\Lambda\tau)\kappa)^T$$

for some $\nu' \in N$ depending on Λ, so $\tau_\rho = \Lambda\tau$. For sufficiently large ρ, we then have $\rho^{i-1}t_i \leq c\rho^i t_{i+1}$ for all $i = 1, \ldots, n-1$, as desired. □

Lemma 5.2 implies that most monic irreducible integer polynomials are strongly quasi-reduced:

Lemma 5.3 *A density of* 100% *of irreducible monic integer polynomials* $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ *of degree n, when ordered by height* $H(f) := \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}$, *are strongly quasi-reduced.*

Proof Let $\epsilon > 0$, and let B be a compact region in $\mathbb{R}^n \cong V_n(\mathbb{R})$ consisting of monic real polynomials of nonzero discriminant and height less than 1 such that

$$\mathrm{Vol}(B) > (1 - \epsilon)\mathrm{Vol}(\{f \in V_n(\mathbb{R}) : H(f) < 1\}).$$

For each $f \in B$, by Lemma 5.2 there exists a minimal finite constant $\rho_f > 0$ such that $f(\rho x)$ is quasi-reduced for any $\rho > \rho_f$. The function ρ_f is continuous in f, and thus by the compactness of B there exists a finite constant $\rho_B > 0$ such that $f(\rho x)$ is quasi-reduced for any $f \in B$ and $\rho > \rho_B$.

Now consider the weighted homogeneously expanding region $\rho \cdot B$ in $\mathbb{R}^n \cong V_n(\mathbb{R})$, where a real number $\rho > 0$ acts on $f \in B$ by $(\rho \cdot f)(x) = f(\rho x)$.

Note that $H(\rho \cdot f) = \rho H(f)$. For $\rho > \rho_B$, we have that all polynomials in $\rho \cdot B$ are quasi-reduced, and

$$\text{Vol}(\rho \cdot B) > (1 - \epsilon)\text{Vol}(\{f \in V_n(\mathbb{R}) : H(f) < \rho\}).$$

Letting ρ tend to infinity shows that the density of monic integer polynomials f of degree n, when ordered by height, that have nonzero discriminant and are strongly quasi-reduced is greater than $1 - \epsilon$. Since ϵ was arbitrary, and 100% of integer polynomials are irreducible, the lemma follows. □

We have the following variation of Theorem 1.1.

Theorem 5.4 *Let $n \geq 1$ be an integer. Then when monic integer polynomials $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ of degree n with $a_1 = 0$ are ordered by $H(f) := \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}$, the density having squarefree discriminant $\Delta(f)$ exists and is equal to $\kappa_n = \prod_p \kappa_n(p) > 0$, where $\kappa_n(p)$ is the density of monic polynomials $f(x)$ over $\mathbb{Z}_p$ with vanishing x^{n-1}-coefficient having discriminant indivisible by p^2.*

Indeed, the proof of Theorem 1.1 applies also to those monic integer polynomials having vanishing x^{n-1}-coefficient without any essential change; one simply replaces the representation W (along with W_0 and W_{00}) by the codimension-1 linear subspace consisting of symmetric matrices with anti-trace 0, but otherwise the proof carries through in the identical manner. The analogue of Theorem 5.4 holds also if the condition $a_1 = 0$ is replaced by the condition $0 \leq a_1 < n$; in this case, $\kappa_n = \prod_p \kappa_n(p) > 0$ is replaced by the same constant $\lambda_n = \prod_p \lambda_n(p) > 0$ of Theorem 1.1, since for any monic degree-n polynomial $f(x)$ there is a unique constant $c \in \mathbb{Z}$ such that $f(x + c)$ has x^{n-1}-coefficient a_1 satisfying $0 \leq a_1 < n$.

Lemmas 5.1 and 5.3 and Theorem 5.4 imply that 100% of monic integer irreducible polynomials having squarefree discriminant and vanishing x^{n-1}-coefficient (or those having x^{n-1}-coefficient non-negative and less than n), when ordered by height, yield *distinct* degree-n fields. Since polynomials of height less than $X^{1/(n(n-1))}$ have absolute discriminant $\ll X$, and since number fields of degree n and squarefree discriminant always have associated Galois group S_n, we see that the number of S_n-number fields of degree n and absolute discriminant less than X is $\gg X^{(2+3+\cdots+n)/(n(n-1))} = X^{1/2+1/n}$. We have proven Corollary 1.3.

Remark 5.5 The statement of Corollary 1.3 holds even if one specifies the real signatures of the monogenic S_n-number fields of degree n, with the identical proof. It holds also if one imposes any desired set of local conditions on the degree-n number fields at a finite set of primes, so long as these local conditions do not contradict local monogeneity.

Remark 5.6 We conjecture that a positive proportion of monic integer polynomials of degree n with x^{n-1}-coefficient non-negative and less than n and absolute discriminant less than X have height $O(X^{1/(n(n-1))})$, where the implied O-constant depends only on n. That is why we conjecture that the lower bound in Corollary 1.3 also gives the correct order of magnitude for the upper bound.

In fact, let C_n denote the $(n-1)$-dimensional Euclidean volume of the $(n-1)$-dimensional region R_0 in $V_n(\mathbb{R}) \cong \mathbb{R}^n$ consisting of all polynomials $f(x)$ with vanishing x^{n-1}-coefficient and absolute discriminant less than 1. Then the region R_z in $V_n(\mathbb{R}) \cong \mathbb{R}^n$ of all polynomials $f(x)$ with x^{n-1}-coefficient equal to z and absolute discriminant less than 1 also has volume C_n, since R_z is obtained from R_0 via the volume-preserving transformation $x \mapsto x + z/n$. Since we expect that 100% of monogenic number fields of degree n can be expressed as $\mathbb{Z}[\theta]$ in exactly one way (up to transformations of the form $\theta \mapsto \pm\theta + c$ for $c \in \mathbb{Z}$), in view of Theorem 1.2 we conjecture that the number of monogenic number fields of degree n and absolute discriminant less than X is asymptotic to

$$\frac{nC_n}{2\zeta(2)} X^{1/2+1/n}. \tag{42}$$

When $n = 3$, a Mathematica computation shows that we have $C_3 = \frac{2^{1/3}(3+\sqrt{3})}{45} \frac{\Gamma(1/2)\Gamma(1/6)}{\Gamma(2/3)}$.

Finally, we turn to the proof of Corollary 1.4. Following [9], for any algebraic number x, we write $\|x\|$ for the maximum of the archimedean absolute values of x. Given a number field K, write $s(K) = \inf\{\|x\| : x \in \mathcal{O}_K, \mathbb{Q}(x) = K\}$. We consider the number of number fields K of degree n such that $s(K) \leq Y$.

As already pointed out in [9, Remark 3.3], an upper bound of $\ll Y^{(n-1)(n+2)/2}$ is easy to obtain. Namely, a bound on the archimedean absolute values of an algebraic number x gives a bound on the archimedean absolute values of all the conjugates of x, which then gives a bound on the coefficients of the minimal polynomial of x. Counting the number of possible minimal polynomials satisfying these coefficient bounds gives the desired upper bound.

To obtain a lower bound of $\gg Y^{(n-1)(n+2)/2}$, we use Lemmas 5.1 and 5.3 and Theorem 5.4. Suppose $f(x) = x^n + a_2 x^{n-2} + \cdots + a_n$ is an irreducible monic integer polynomial of degree n. Let θ denote a root of $f(x)$. If $H(f) \leq Y$, then $|\theta| \ll Y$; this follows, e.g., from Fujiwara's bound [10]:

$$\|\theta\| \leq \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_{n-1}|^{1/(n-1)}|, |a_n/2|^{1/n}\}.$$

Therefore, if $H(f) \leq Y$, then

$$s(\mathbb{Q}[x]/(f(x))) \leq \|\theta\| \ll Y. \tag{43}$$

Now Lemma 5.3 and Theorem 5.4 imply that there are $\gg Y^{(n-1)(n+2)/2}$ such polynomials $f(x)$ of height less than Y that have squarefree discriminant and are also strongly quasi-reduced. Lemma 5.1 and (43) then imply that these polynomials define distinct S_n-number fields K of degree n with $s(K) \leq Y$. This completes the proof of Corollary 1.4.

References

1. Ash, A., Brakenhoff, J., Zarrabi, T.: Equality of polynomial and field discriminants. Exp. Math. **16**, 367–374 (2007)
2. Bhargava, M.: The geometric sieve and the density of squarefree values of polynomial discriminants and other invariant polynomials. http://arxiv.org/abs/1402.0031
3. Bhargava, M., Gross, B.: Arithmetic invariant theory, symmetry: representation theory and its applications. Progr. Math. **257**, 33–54 (2014)
4. Bhargava, M., Gross, B.: The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point. Automorphic representations and L-functions. Tata Inst. Fundam. Res. Stud. Math., Mumbai, vol. 22, pp. 23–91 (2013)
5. Bhargava, M., Gross, B., Wang, X.: A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension. J. Am. Math. Soc. **30**, 451–493 (2017)
6. Bhargava, M., Shankar, A., Wang, X.: Squarefree values of polynomial discriminants II (in preparation)
7. Dietmann, R.: On the distribution of Galois groups. Mathematika **58**, 35–44 (2012)
8. Ekedahl, T.: An infinite version of the Chinese remainder theorem. Comment. Math. Univ. St. Paul. **40**, 53–59 (1991)
9. Ellenberg, J., Venkatesh, A.: The number of extensions of a number field with fixed degree and bounded discriminant. Ann. Math. **163**(2), 723–741 (2006)
10. Fujiwara, M.: Über die obere Schranke des absoluten Betrages der Wurzeln einer algebraischen Gleichung. Tohoku Math. J. **10**, 167–171 (1916)
11. Gelfond, I.M., Kapranov, M.M., Zelevinsky, A.V.: Discriminants, Resultants and Multidimensional Determinants. Springer, New York (1994)
12. Granville, A.: ABC allows us to count squarefrees. Int. Math. Res. Notices. **19**, 991–1009 (1998)
13. Iwaniec, H., Kowalski, E.: Analytic Number Theory, vol. 53. Amer. Math. Soc. Colloq. Publ., Providence (2004)
14. Kedlaya, K.S.: A construction of polynomials with squarefree discriminants. Proc. Am. Math. Soc. **140**, 3025–3033 (2012)
15. Kondo, T.: Algebraic number fields with the discriminant equal to that of a quadratic number field. J. Math. Soc. Japan **47**(1), 31–36 (1995)
16. Nakagawa, J.: On the Galois group of a number field with square free discriminant. Comment. Math. Univ. St. Paul. **37**, 95–98 (1988)
17. Poonen, B.: Bertini theorems over finite fields. Ann. Math. 1099–1127 (2004)
18. Poonen, B., Stoll, M.: Most odd degree hyperelliptic curves have only one rational point. Ann. Math. **180**(3), 1137–1166 (2014)

19. Sato, M., Kimura, T.: A classification of irreducible prehomogeneous vector spaces and their relative invariants. Nagoya Math. J. **65**, 1–155 (1977)
20. Scholz, A.: Aufgabe 208, Jahresber. Deutsch Math.-Verein., vol. XLV (1935), 2. Abt. Heft 9/11, 110; Lösung der Aufgabe 208, Jahresber. Deutsch Math.-Verein., vol. XLVII (1937), 2. Abt. Heft 5/8, 47
21. Shankar, A., Södergren, A., Templier, N.: Sato-Tate equidistribution of certain families of Artin L-functions. https://arxiv.org/abs/1507.07031
22. Shankar, A., Tsimerman, J.: Counting S_5-fields with a power saving error term. Forum Math. Sigma **2**, e13 (2014)
23. Shankar, A., Wang, X.: Rational points on hyperelliptic curves having a marked non-Weierstrass point. Compositio Mathematica **154**(1), 188–222 (2018)
24. Wang, X..: Pencils of quadrics and Jacobians of hyperelliptic curves. Ph.D thesis, Harvard (2013)
25. Yamamura, K.: On unramified Galois extensions of real quadratic number fields. Osaka J. Math. **23**(2), 471–478 (1986)
26. Yamamura, K.: Some analogue of Hilbert's irreducibility theorem and the distribution of algebraic number fields. J. Fac. Sci. Univ. Tokyo Sect. IA Math. **38**(1), 99–135 (1991)