The Geometric Sieve and Asymptotics for Counting Number Fields

Arav Karighattam

Abstract. The asymptotics for the number of field extensions of $\mathbb{Q}$ with a fixed Galois group are not known in general, but Malle has conjectures for them. However, in many specific cases, such as for all abelian groups, as well as for some select non-Galois extensions, the conjectures have been proved. In this paper we review some recent results and some aspects of their proofs, such as the geometric sieve. For the case of $S_r \times A$ extensions that we consider, we review the methods for using the asymptotics for fields with fixed Galois groups to find the asymptotics for the fields whose Galois group is the product of the two groups. In particular, we need a uniformity theorem, to find an upper bound for the number of extensions ramified at large primes, because in the proof we will be summing over ramification conditions. The main tool which is used here is the geometric sieve, which is used to count points on varieties, and relate that to this problem by using the parametrization of quintic rings which writes the discriminant as a polynomial defined on a vector space, and by finding a subscheme in which the polynomial must have certain divisibility conditions. More specifically, we will review a result which estimates the growth of the number of lattice points on a fixed variety in a given region, with the size of region as the region expands. We will also review a result to convert the problem of counting orbits on vector spaces such that a given polynomial satisfies a prescribed set of congruence conditions into a problem of computing an integral over an appropriate fundamental domain of a group action. The integrand in this case will be of the form in which the first result will be applicable.

1 Introduction

To understand the primes in a field extension $K/\mathbb{Q}$, we may consider the discriminant Disc K of the extension, which has the property that the primes dividing the discriminant are the primes ramified in the extension. A way of determining the distribution of isomorphism classes of number fields, using a more analytic approach, is to consider those with a fixed Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ (or an analogue for non-Galois extensions, which will be mentioned below) whose discriminant is bounded by some number X, and find the asymptotics in the limit $X \to \infty$. This would be a measure of the number of additional properties of number fields with Galois group G in addition to its discriminant. For example, for quadratic fields, there is only one field for a given discriminant D (namely $K = \mathbb{Q}(\sqrt{D})$). For $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ extensions, note that, for example, Disc $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = 64a^2b^2$ when a and b are squarefree, $\gcd(a,b) = 1$, and $a \equiv b \equiv 3 \pmod 4$, as $\{1, \sqrt{a}, \sqrt{b}, \frac{1+\sqrt{ab}}{2}\}$ is an integral basis. The number of such extensions with Disc $K = 64p_1^2p_2^2 \cdots p_n^2$ with $p_i \equiv 3 \pmod 4$ is then at least 2^{n-1} (these take the form $K = \mathbb{Q}(\sqrt{P}, \sqrt{\alpha})$ where $P = p_1p_2 \cdots p_n$ and α is any product of the primes p_i). More generally, the allowed discriminants are the squares of squarefree integers multiplied by a small power of 2 depending on modulo 4 congruence conditions on the discriminants of the three quadratic subfields. As the number of extensions with a fixed discriminant with n prime factors tends to infinity with n, we see that the number of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ extensions should grow asymptotically faster than $\sqrt{X}$. (Note that as remarked in [16], the number of squarefree integers less than x is $O(x)$, hence we see the number of allowed discriminants up to X is $O(\sqrt{X})$.) However, the number of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ extensions $K/\mathbb{Q}$ with a given discriminant Disc $K = X$ is $o(X^{\varepsilon})$ for any $\varepsilon > 0$ so the number of extensions will grow much slower than X.

The asymptotics for the number of Galois extensions of $\mathbb{Q}$ with a given Galois group G with discriminant at most X have been conjectured by Malle [13]. For more general non-Galois extensions K with Galois closure L, we may consider as in [13] the subgroup $G_K \leq S_{[K:\mathbb{Q}]}$ resulting from the action of $\mathrm{Gal}(L/\mathbb{Q})$ on the set of embeddings $K \to L$. Using the notation from [17], for any group G with an embedding $G \to S_n$, we would like to find the asymptotics of

$$N(G, X) := |\{K/\mathbb{Q} : |\text{Disc } K| \leq X,\, G_K \cong G \text{ as permutation groups}\}|,$$

where by $G_K \cong G$ as permutation groups we mean that there is an automorphism $\phi \in \text{Aut } S_n$ such that $\phi(G_K) = G$. In the case of Galois extensions, note that there is a natural embedding $G \to S_{|G|}$ for any finite group G. There happens to be one restriction on embeddings $G \to S_n$ that are isomorphic to groups of the form G_K as permutation groups, in particular, that the action of G on the set $\{1, 2, \ldots, n\}$ is transitive. For the group G_K, this follows from the result in Galois theory that all subfields of the Galois closure L of K which are isomorphic to K are actually Galois conjugates of K. Malle's conjecture over $\mathbb{Q}$ for general (not necessarily Galois) extensions is the following.

Conjecture 1. (Malle, 2004) [13] *Let $G \to S_n$ be an embedding such that G acts transitively on the set $\{1, 2, \dots, n\}$. Let O_g be the number of orbits in $\{1, 2, \dots, n\}$ under the action of the cyclic subgroup $\langle g\rangle \leq G$. Consider the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on the group generated by a primitive $|G|$-th root of unity ζ; this extends to an action on G by the function $g \to \zeta^{|G|/\mathrm{ord}\, g}$. Let $A(G) = \min\limits_{g\in G\setminus\{1\}} (n - O_g)$ and let $b(G)$ be the number of orbits of the set of conjugacy classes $\{[g] : n - O_g = a(G)\}$ under the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Then*

$$N(G, X) \sim CX^{1/A(G)} \log^{b(G)-1} X$$

as $X \to \infty$ for some constant C depending only on G. (Note that $n - O_g$ is typically called the index of g.)

This conjecture was actually stated in [13] for arbitrary base fields k, where the constant c can also depend on k, and the constant b is modified slightly. In particular, as the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of conjugacy classes of G, we may restrict the action to the absolute Galois group of k and define $b(G, k)$ as the number of orbits of the set of conjugacy classes $|g| : n - O_g = A(g)$ under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$. In this paper, although much work has been done over arbitrary base fields, we will be reviewing results and their proofs only over the base field $\mathbb{Q}$.

Let us evaluate this expression for the case $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ that we were considering earlier. First, as all elements have order 2, the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on G is trivial. Then the natural embedding $G \to S_{|G|}$ which sends each element $g \in G$ to the permutation on the elements of G corresponding to multiplication by g, has image $\{1, (12)(34), (13)(24), (14)(23)\} \subseteq S_4$, so that $O_g = 2$ for all nontrivial $g \in G$. As G is abelian, we deduce that $A(G) = 2$ and $b(G) = 3$, so that Malle's conjecture predicts that $N(G, X) \sim CX^{1/2} \log^2 X$ for some constant C, which agrees with the earlier analysis.

Note that for Galois field extensions, Wright [18] proved the conjecture for all abelian groups G (in fact over general number field bases k). In this case, the embedding of G as a permutation group is the natural one, and the size of an orbit O_g for any $g \in G$ is simply the index $[G : \langle g\rangle] = |G|/\mathrm{ord}\, g$. Then if p is the smallest prime factor of $|G|$, O_g is maximized for nontrivial g when g has order p, so that $A(G) = |G|(1 - 1/p)$. As remarked in [13], we may deduce that $b(G) = (|G[p]| - 1)/[\mathbb{Q}(\zeta) : \mathbb{Q}]$ where ζ is the primitive p-th root of unity; this is because O_g is maximized if and only if g is a nontrivial element of $G[p]$, and the subgroup $\langle g\rangle$ for any such g has orbits of size $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then Malle's conjecture for abelian groups G embedded naturally in $S_{|G|}$ is

$$N(G, X) \sim CX^{\frac{p}{(p-1)|G|}} \log^{\frac{|G[p]|-1}{[\mathbb{Q}(\zeta):\mathbb{Q}]}} X$$

for some constant C. Wright proved this and a more general result with specified ramification conditions (see Section 2). A similar result for extensions $K/\mathbb{Q}$ which are direct products of non-Galois S_r degree-r extensions and abelian Galois extensions (that is, in the earlier notation, $G_K \cong S_r \times H$ where H is abelian and $S_i \times H$ is regarded as a permutation group acting on the set $\{1, 2, \dots, r\} \times H$) has been proven in [14, 17] in the cases $r = 3, 4, 5$. For these permutation groups it turns out that the constants $A(G)$ and $b(G)$ take much simpler forms. Following [17], if p is the smallest prime divisor of $|H|$ and $(g, h) \in S_r \times H$, the number of orbits $O_{(g,h)}$ is simply the product $O_g O_h$ of the number of orbits of g in $\{1, 2, \dots, r\}$ and the number of orbits of h in A. By noting that O_g is maximized for nontrivial $g \in S_r$ when g is a transposition and O_h is maximized for nontrivial $h \in H$ when h has order p, we deduce that the maximum value of $O_{(g,h)}$ occurs when g is a transposition and $h = 1$, so that $A(S_r \times H) = |H|$. Since all transpositions in S_r form a single conjugacy class, $b(S_r \times H) = 1$, and Malle's conjecture in this case becomes the following theorem.

Theorem 2. (Masri-Thorne-Tsai-Wang) [14, 17] *If G is the product $S_r \times A$ with a permutation action on the set $\{1, 2, \dots, r\} \times A$, there exists a constant C depending only on G such that*

$$N(G, X) \sim CX^{1/|A|}$$

in the limit $X \to \infty$.

To find the asymptotics for $S_r \times A$ extensions, with the embedding $S_r \times A \to S_{r|A|}$ mentioned above, following [17], one of the necessary steps is to obtain *uniformity theorems*, which give upper bounds for the number of non-Galois S_r degree-r extensions with certain ramification conditions. These theorems show that the number of S_r degree-r extensions of $\mathbb{Q}$ with discriminant bounded by X which are totally ramified (or overramified for $r = 4$, where overramified will be defined shortly) at some primes $p_1, p_2, \ldots, p_m$ is uniformly smaller for larger q. More specifically, for any positive squarefree integer q, we may define [17]

$$N_q(G, X) := |\{K/\mathbb{Q} : |\text{Disc } K| \leq X,\, G_K \cong G \text{ as permutation groups,} \\ K \text{ totally ramified or overramified at } p\ \forall p|q\}|,$$

where overramified applies to $r = 4$ and totally ramified applies to $r = 3, 5$. Here a prime p is overramified in an S_4 non-Galois quartic extension $K/\mathbb{Q}$ (as defined in [1]) if p splits in K as a product of primes all of whose exponents are greater than 1. Then we have the following theorem, for which the proof in the case $r = 5$ will be outlined in Section 5.

Theorem 3. *For any positive squarefree integer q and for any $\varepsilon > 0$, we have the following estimates for $N_q(S_r, X)$ as $X \to \infty$:*

(a) (Datkovsky-Wright, 1988) [9] $N_q(S_3, X) = O(X/q^{2-\varepsilon})$

(b) (Bhargava, 2005) [1] $N_q(S_4, X) = O(X/q^{2-\varepsilon})$

(c) (Wang, 2017) [17] $N_q(S_5, X) = O(X/q^{4/15-\varepsilon})$

In the sections below, we will explain how to combine the asymptotics for non-Galois S_r degree r extensions and for abelian A extensions into the asymptotics for $S_r \times A$ degree $r|A|$ extensions below with restrictions on A (in particular, we assume that $|A|$ is relatively prime to $r!$, which is slightly stricter than the conditions in [17]). We will also need a uniformity result for Galois A-extensions, this time for all ramification types (see Section 2).

There are two methods used in the proof of Theorem 3, the first method for $r = 3$ and 4 uses class field theory, and the case $r = 5$ uses the *geometric sieve* in [4]. The geometric sieve consists of two main steps. The first step, the Ekedahl sieve (used in [16] for instance), is used to count the number of values of a polynomial that are not multiples of p^k for appropriate integers k and primes p. In the applications in [3, 16], this is used to count the number of squarefree values of a polynomial, whereas to prove Theorem 3, we will be parametrizing non-Galois S_5 quintic extensions using a polynomial, and using the Ekedahl sieve to apply the ramification conditions. For the case of computing the density of squarefree values of a polynomial, the Ekedahl sieve method in [16] uses the ABC conjecture. For the specific polynomials that are associated with counting non-Galois S_r degree-r extensions for $r = 3, 4$ and 5, the ABC conjecture does not need to be assumed by instead proving a series of conditions relating the polynomials to the orbits of vector spaces under the action of a group variety [4]. We will be explaining some of these tools in Section 4.

2 Products of Number Fields

Consider the product of two number fields K and L, we would like to relate the discriminants of K and L with the discriminant of the compositum KL, in order to use asymptotics for non-Galois S_r degree r extensions and for abelian extensions, for example, to compute the asymptotics for $S_r \times A$ degree $r|A|$ extensions. We will follow [17] throughout this section unless otherwise noted.

In general, there could be two problems in counting such number fields. The first is that the degree of KL may not be the product of the degrees of K and L. However, we note that if K is a non-Galois S_r degree-r extension, L is a Galois A-extension for A an abelian group whose order is relatively prime to $r!$, and K' is the Galois closure of K, we find that $K' \cap L = \mathbb{Q}$ as $[K' \cap L : \mathbb{Q}] \mid \gcd\big([K' : \mathbb{Q}], [L : \mathbb{Q}]\big) = \gcd(r!, |A|) = 1$. For such extensions, the Fundamental Theorem of Galois Theory implies that $[K'L : \mathbb{Q}] = [K' : \mathbb{Q}][L : \mathbb{Q}]$, and by taking explicit bases we may see that the degree of KL is the product of the degrees of K and L as field extensions of $\mathbb{Q}$, and further, that $G_{KL} = G_K \times G_L$. (It is important to consider the Galois closure of K, note that, for example, the extensions $\mathbb{Q}(\sqrt[3]{2})$ and $Q(\zeta_3)$ have relatively prime degrees and $\mathbb{Q}$ is their intersection, but the compositum is a Galois extension with Galois group S_3.)

The second problem is that the product of the rings of integers $\mathcal{O}_K$ and $\mathcal{O}_L$ of K and L is not necessarily equal to $\mathcal{O}_{KL}$, so we cannot easily extend integral bases on $\mathcal{O}_K$ and $\mathcal{O}_L$ to $\mathcal{O}_{KL}$. This can be seen, for example, for the fields $K = \mathbb{Q}(\sqrt{3})$ and $L = \mathbb{Q}(\sqrt{7})$, when the algebraic integer $\frac{1+\sqrt{21}}{2} \notin \mathcal{O}_K\mathcal{O}_L$. Instead, the product $\mathcal{O}_K\mathcal{O}_L$ becomes a possibly non-maximal order in KL. This problem, unlike the previous one, does occur for the $S_r \times A$ extensions that we are considering, and the rest of this section will discuss the resolution of this problem.

First, we compute the discriminant of the order $\mathcal{O}_K\mathcal{O}_L$ for number fields K and L with degrees k and ℓ over $\mathbb{Q}$, such that $K \cap L = 1$. If $\{r_1, r_2, \ldots, r_k\}$ and $\{s_1, s_2, \ldots, s_\ell\}$ are integral bases for $\mathcal{O}_K$ and $\mathcal{O}_L$, as $\mathcal{O}_K\mathcal{O}_L$ is an order in a field of degree $k\ell$ over $\mathbb{Q}$, the product $\{r_i s_j | 1 \leq i \leq k, 1 \leq j \leq \ell\}$ is an integral basis for $\mathcal{O}_K\mathcal{O}_L$, and the discriminant is $\det(\mathrm{Tr}_{\mathcal{O}_K\mathcal{O}_L}(r_{i_1}s_{j_1}r_{i_2}s_{j_2}))_{(i_1,j_1),(i_2,j_2)\in S}$ where $S = \{1, 2, \ldots, k\}\{1, 2, \ldots, \ell\}$ (using the trace definition of the determinant [2, 15]). Note that the matrix that we are taking a determinant of has indices in S. Now

$$\mathrm{Tr}_{\mathcal{O}_K\mathcal{O}_L}(r_{i_1}s_{j_1}r_{i_2}s_{j_2}) = \mathrm{Tr}_{\mathcal{O}_K}(r_{i_1}r_{i_2})\mathrm{Tr}_{\mathcal{O}_L}(s_{j_1}s_{j_2}),$$

The determinant can be naturally expressed as a sum over all permutations of S, we will show that we only need to sum over those permutations arising as a product of permutations in S_k and S_ℓ (here for $\alpha \in S_k$ and $\beta \in S_\ell$, define the product $\alpha\beta$ by $\alpha\beta(i,j) = (\alpha(i), \beta(j))$). Indeed, if σ is a permutation of S that does not arise as a product in this way, we may assume that $\pi(\sigma(i,j)) \neq \pi(\sigma(i,j'))$ for some i, where π is the projection to the first coordinate. For t the transposition $((i,j)(i,j'))$, the permutation $\sigma \circ t$ yields a term which is the negative of the term corresponding to σ in the discriminant. Using this reduction, we may explicitly compute that

$$\mathrm{Disc}\ \mathcal{O}_K\mathcal{O}_L = (\mathrm{Disc}\ \mathcal{O}_K)^\ell(\mathrm{Disc}\ \mathcal{O}_L)^k.$$

The key step in [17] used is to determine the differences between Disc KL and $(\mathrm{Disc}\ K)^\ell(\mathrm{Disc}\ L)^k$ for a finite range of primes $p < M$. More specifically, for any $M > 0$, let $\mathrm{Disc}_{(p)} F$ be the largest power of p dividing Disc F for any number field F, and define

$$\mathrm{Disc}_M KL = \prod_{p<M} \mathrm{Disc}_{(p)} KL \prod_{p\geq M} (\mathrm{Disc}_{(p)} K)^\ell(\mathrm{Disc}_{(p)} L)^k.$$

As Disc KL | Disc $\mathcal{O}$ for any order $\mathcal{O} \subseteq \mathcal{O}_{KL}$ ([15], Proposition I.2.12), the quantity $\mathrm{Disc}_M KL$ is an upper bound for Disc KL, and is equal to Disc KL for any M which is larger than all of the ramified primes in $KL/\mathbb{Q}$.

We will now explain how to get an upper and a lower bound for $N(S_r \times A, X)$, using the definition above. We will first need to relate the discriminant of KL with the discriminants of K and L using ramification conditions, and then we will find similar relations for $\mathrm{Disc}_M KL$. Note that the fields in question in the two lemmas below are not necessarily Galois extensions.

Lemma 4. [17] *Let F be a number field and let $p \nmid [F : \mathbb{Q}]$ be a ramified prime in the extension $F/\mathbb{Q}$. Then $Disc_{(p)} F$ only depends on the inertia group $I_p(F/\mathbb{Q}) \leq G_K \leq S_{[F:\mathbb{Q}]}$ of $F/\mathbb{Q}$ at p.*

Proof. This is a consequence of the result ([15], Theorems III.2.6 and III.2.9) that $\log_p \mathrm{Disc}_{(p)} F$ when $p \nmid [F : \mathbb{Q}]$ is the sum $\sum_j (e_j - 1)f_j$ where j varies over the primes of K under p, e_j denotes the ramification index and f_j denotes the inertia degree at the prime $\mathfrak{p}_j|p$. To compute the number of orbits in the set of embeddings $F \to \overline{\mathbb{Q}}$, we note that $F \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a direct sum of local fields (in particular it is the direct sum of the completions of F at the primes splitting at p with the completion at a prime $\mathfrak{p}_j$ occurring e_j times). The set of embeddings $F \to \overline{\mathbb{Q}}$ now corresponds to the set of $\mathbb{Q}_p$-algebra homomorphisms $F \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \overline{\mathbb{Q}}_p$ (this is similar to what is described for general rings in [2]). The $\mathbb{Q}_p$-algebra homomorphisms $\phi : F \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \overline{\mathbb{Q}}_p$ are those which are an embedding in one factor and zero on all of the others. As $|\mathrm{Gal}(\mathbb{F}_p^f/\mathbb{F}_p)| = f$ for any positive integer f, the number of orbits under the inertia group among those homomorphisms which correspond to an embedding of $F_{\mathfrak{p}_j}$ is f_j (the inertia group permutes the e_j different factors of $F_{\mathfrak{p}_j}$). The total number of orbits is then the sum $\sum_j f_j$, and as the inertia group on $F/\mathbb{Q}$ at p is defined by local conditions, this inertia group has $\sum_j f_j$ orbits. Then $\log_p \mathrm{Disc}_{(p)} F$ is $\sum_j (e_j - 1)f_j = [F : \mathbb{Q}] - \sum_j f_j$ only depends on the action of the inertia group on the $[F : \mathbb{Q}]$ embeddings $F \to \overline{\mathbb{Q}}$. □

The next lemma shows that we only need the inertia groups of two fields K and L to determine the largest power of p dividing the discriminant of the compositum KL.

Lemma 5. [17] *Let K and L be number fields of degrees r and s, respectively, such that $G_{KL} \leq S_{rs}$ is the product of $G_K \leq S_r$ and $G_L \leq S_s$. Suppose that $p \nmid [KL : \mathbb{Q}]$ is a prime. Then $Disc_{(p)} KL$ only depends on the action of inertia groups of K and L on the sets of embeddings $K \to \mathbb{Q}$ and embeddings $L \to \mathbb{Q}$.*

This lemma follows from the previous one, by noting that the inertia group of KL is a subgroup of S_{rs}, the group of permutations on the set of pairs of embeddings $K \to \overline{\mathbb{Q}}$, $L \to \overline{\mathbb{Q}}$, as the product of the inertia groups of K and L in S_r and S_s. Then the orbits under the action of the inertia group of KL are products of orbits under the action of K and orbits under the action of L, so that

$$\begin{aligned}\mathrm{Disc}_{(p)} KL &= p^{rs-(r-\log_p \mathrm{Disc}_{(p)} K)(s-\log_p \mathrm{Disc}_{(p)} L)} \\ &= p^{-(\log_p \mathrm{Disc}_{(p)} K)(\log_p \mathrm{Disc}_{(p)} L)}(\mathrm{Disc}_{(p)} K)^s(\mathrm{Disc}_{(p)} L)^r \qquad (1)\end{aligned}$$

which only depends on the desired actions of the inertia groups of K and L by Lemma 4.

Now we will count $S_r \times A$ number fields by counting the number fields with a specified set of local conditions and summing over all possible ramification types, assuming that $\gcd(r!, |A|) = 1$. By the two lemmas above, for primes $p \nmid r|A|$, $\mathrm{Disc}_{(p)} KL$ can be expressed in terms of $\mathrm{Disc}_{(p)} K$ and $\mathrm{Disc}_{(p)} L$ by specifying the inertia groups of K and L. Let $\mathfrak{S}$ denote the set of all finite sets S of primes, with a choice of subgroups $A_p \leq S_r$, $B_p \leq S_s$ for each $p \nmid r|A|$, and a choice of $\mathbb{Q}_p$-algebras $\mathfrak{A}_p$ and $\mathfrak{B}_p$ which are rank-r and rank-$|A|$ $\mathbb{Q}_p$-modules, respectively, for every $p \mid r|A|$. For any $\mathcal{S} \in \mathfrak{S}$, we will suppose that the pair of fields $(K, L) \in S$ if the set of primes at which both K and L are ramified is S, if A_p and B_p are the inertia subgroups of K and L for $p \nmid r|A|$, and if $\mathcal{A}_p$ and $\mathcal{B}_p$ are $K \otimes \mathbb{Q}_p$ and $L \otimes \mathbb{Q}_p$ for $p \mid r|A|$. Since the exponent of p in the discriminant of a field F is the sum of the valuations of the discriminants of the direct summands of $F \otimes_{\mathbb{Q}} \mathbb{Q}_p$, and $KL \otimes_{\mathbb{Q}} \mathbb{Q}_p$ can be expressed in terms of the $\mathbb{Q}_p$-algebras $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and $L \otimes_{Q} \mathbb{Q}_p$, we see that Disc KL can be expressed in terms of Disc K and Disc L, and the element of $\mathfrak{S}$ corresponding to the ramification of K and L at the primes of $\mathbb{Q}$. For some fixed $\mathcal{S} \in \mathfrak{S}$, by taking the product over all p of equation (1), and noting that the power of p on the right hand side is not equal to 1 if and only if $p \in S$,

$$\text{Disc } KL = (\text{Disc } K)^{|A|} (\text{Disc } L)^r \prod_{p \in S} p^{-(\log_p \mathrm{Disc}_{(p)} K)(\log_p \mathrm{Disc}_{(p)} L)}. \tag{2}$$

In the expression above, note that $d_{p,\mathcal{S},1} := \log_p \mathrm{Disc}_{(p)} K$ and $d_{p,\mathcal{S},2} := \log_p \mathrm{Disc}_{(p)} L$ are completely determined by p and $\mathcal{S}$.

We will now find lower and upper bounds for $N(S_r \times A)$. First, we will define $N_M(S_r \times A)$ just as we defined $N(S_r \times A)$, but with Disc KL replaced by $\mathrm{Disc}_M KL$. Note that by equation (2), if the pair of fields $(K, L) \in \mathcal{S}$, and S is the associated set of primes, Disc $KL = \mathrm{Disc}_M KL$ for all $M > \max S$. Then by equation (2),

$$\begin{aligned} N(S_r \times A, X) - N_M(S_r \times A, X) &= \sum_{\mathcal{S} \in \mathfrak{S}} |\{(K, L) \in \mathcal{S} \mid \text{Disc } KL < X, \mathrm{Disc}_M KL > X\}| \\ &\leq \sum_{\substack{\mathcal{S} \in \mathfrak{S} \\ \max S \geq M}} |\{(K, L) \in \mathcal{S} \mid \text{Disc } KL < X\}| \\ &= \sum_{\substack{\mathcal{S} \in \mathfrak{S} \\ \max S \geq M}} \left| \left\{ (K, L) \in \mathcal{S} \,\middle|\, (\text{Disc } K)^{|A|} (\text{Disc } L)^r < X \prod_{p \in S} p^{d_{p,\mathcal{S},1} d_{p,\mathcal{S},2}} \right\} \right|. \end{aligned} \tag{3}$$

We can also compute $N_M(S_r \times A, X)$ using a similar sum over ramification conditions. In this case, it turns out to be easier to consider a different set of local conditions, and to consider the set of all primes up to M (as the largest power of p dividing $\mathrm{Disc}_M KL$ is $(\mathrm{Disc}_{(p)} K)^{|A|} (\mathrm{Disc}_{(p)} L)^r$). Let $\mathfrak{S}_M$ be the denote the set of all $\mathcal{S} \in \mathfrak{S}$ with the set S to be chosen as the set of all primes less than M, and where trivial inertia groups may be chosen for any of the primes. Note that $\mathfrak{S}_M$ is a finite set, while $\mathfrak{S}$ is not. We then obtain the result

$$N_M(S_r \times A, X) = \sum_{\mathcal{S} \in \mathfrak{S}_M} \left| \left\{ (K, L) \in \mathcal{S} \,\middle|\, (\text{Disc } K)^{|A|} (\text{Disc } L)^r < X \prod_{p < M} p^{-d_{p,\mathcal{S},1} d_{p,\mathcal{S},2}} \right\} \right| \tag{4}$$

just as in equation (3).

We will now explain how the results for S_r extensions and A extensions are combined to yield a result for $S_r \times A$ extensions. First, we will state the results for S_r and A extensions that we will need. For S_r extensions with $r = 3, 4$, or 5, the general results for arbitrary ramification conditions are given in [7], and in particular, they determine constants $C_{\mathcal{S}}$ depending on r such that

$$N_{\mathcal{S}}(S_r, X) \sim C_{\mathcal{S}} X, \tag{5}$$

where $N_{\mathcal{S}}(S_r, X)$ is the number of non-Galois S_r degree-r number fields K satisfying the set of local conditions $\mathcal{S} \in \mathfrak{S}$. Similarly, Wright [18] derived a result for $N_{\mathcal{S}}(A, X)$ (defined similarly), and found constants $D_{\mathcal{S}}$ such that

$$N_{\mathcal{S}}(A, X) \sim D_{\mathcal{S}} X^{\frac{p_0}{(p_0 - 1)|A|}} \log^{\frac{|A[p_0]| - 1}{[\mathbb{Q}(\zeta):\mathbb{Q}]}} X \tag{6}$$

for any $\mathcal{S} \in \mathfrak{S}$, where p_0 is the smallest prime divisor of $|A|$. Next, we will use the following lemma for combining distributions. For the proof, which uses partial summation, see [17].

Lemma 6. (Wang, 2017) [17] *Let $f_1, f_2 : \mathbb{N} \to \mathbb{N}$ be monotonic functions, and let $F_i(X)$ be the largest integer such that $f_i \leq X$. Suppose that C_1, C_2, r_1, r_2, s_1, and s_2 are constants such that $F_i \sim C_i X^{r_i} \log^{s_i} X$. If a and b are integers with $b > ar_2/r_1$, there is a constant C depending on C_1 and C_2 such that*

$$\left| \left\{ (x, y) \in \mathbb{N} \times \mathbb{N} \,\middle|\, f_1(x)^a f_2(y)^b < X \right\} \right| \sim C X^{r_1/a} \log^{s_1} X.$$

If r_1, r_2, s_1, s_2, a, and b are fixed, then $C \leq D C_1 C_2$ for some constant D that does not depend on C_1 and C_2.

Once these lemmas are used, we may compute the sums in equations (3) and (4). However, we will then need the uniformity theorem, Theorem 3, to show that the infinite sum in equation (3) is bounded. The most important aspect of Theorem 3 and the similar theorem for abelian extensions (for a proof of the uniformity of abelian extensions, see [17]) that has not been shown in the estimates in [7] is the explicit dependence on the squarefree integer q. Precisely, the constant $D_{\mathcal{S}} = O\big(q^{-\frac{p_0}{(p_0-1)|A|}+\varepsilon}\big)$ for any $\varepsilon > 0$. Also, the proof of the results in [7] uses many similar geometric sieve techniques, such as Lemma 11, and the consideration of fundamental domains in Section 5.

Let us combine the results above to find the desired asymptotics. For $N_M(S_r \times A, X)$ we can use equations (5) and (6) and Lemma 6 directly to find that for every $\mathcal{S} \in \mathfrak{S}_M$, there exists constants $B_{\mathcal{S}}$ and a constant C such that

$$N_M(S_r \times A, X) \sim \sum_{\mathcal{S}\in\mathfrak{S}} B_{\mathcal{S}} X^{1/|A|} = C_M X^{1/|A|}, \tag{7}$$

noting that $r > \frac{p_0}{p_0-1}$, and that the sum is finite. Here $C_M := \sum_{\mathcal{S}\in\mathfrak{S}} B_{\mathcal{S}}$.

It remains to uniformly bound $N(S_r \times A, X) - N_M(S_r \times A, X)$ as $M \to \infty$. Note that in this case we have to choose the distributions that will be input into Lemma 6 carefully; the natural choices $N_{\mathcal{S}}(S_r, X)$ and $N_{\mathcal{S}}(A, X)$ do not yield optimal bounds as the discriminant has a common factor over all fields satisfying the local conditions in $\mathcal{S}$. For each $\mathcal{S} \in \mathfrak{S}$, let $F_1(\mathcal{S}, X)$ be the number of non-Galois S_r degree-r fields satisfying the local conditions in $\mathcal{S}$ such that $\prod_{p\notin S} \operatorname{Disc}_{(p)} K < X$, and let $F_2(\mathcal{S}, X)$ be the similarly defined distribution for abelian extensions. Then by the uniformity theorems, if T denotes the set of totally ramified (or overramified primes) in S, and t is the constant such that $C_{\mathcal{S}} = O(q^{-t+\varepsilon})$ for any $\varepsilon > 0$ when $q = \prod_{p\in T} p$ (where $t = 2$ for $r = 3, 4$ and $t = 4/15$ for $r = 5$),

$$F_1(\mathcal{S}, X) = N_{\mathcal{S}}\Big(S_r, X \prod_{p\in S} p^{d_{p,\mathcal{S},1}}\Big) = O\Big(X \prod_{p\in S} p^{d_{p,\mathcal{S},1}} \prod_{p\in T} p^{-t+\varepsilon}\Big)$$

and

$$\begin{aligned} F_2(\mathcal{S}, X) = N_{\mathcal{S}}\Big(A, X \prod_{p\in S} p^{d_{p,\mathcal{S},2}}\Big) &= O\Big(X^{\frac{p_0}{(p_0-1)|A|}} \log^{\frac{|A[p_0]|-1}{[\mathbb{Q}(\zeta):\mathbb{Q}]}} X D_{\mathcal{S}} \prod_{p\in S} p^{d_{p,\mathcal{S},2}(1+\varepsilon/2)}\Big) \\ &= O\Big(X^{\frac{p_0}{(p_0-1)|A|}} \log^{\frac{|A[p_0]|-1}{[\mathbb{Q}(\zeta):\mathbb{Q}]}} X \prod_{p\in S} p^{\varepsilon d_{p,\mathcal{S},2}}\Big), \end{aligned}$$

for any $\varepsilon > 0$ where the constants do not depend on $\mathcal{S}$. By Lemma 6, we see that for sufficiently large X, there exists some constant C such that

$$\begin{aligned} &N(S_r \times A, X) - N_M(S_r \times A, X) \\ \le\ &CX^{1/|A|} \sum_{\substack{\mathcal{S}\in\mathfrak{S} \\ \max S > M}} \prod_{p\in S} p^{d_{p,\mathcal{S},1}+\varepsilon d_{p,\mathcal{S},2}+(d_{p,\mathcal{S},1}d_{p,\mathcal{S},2}-|A|d_{p,\mathcal{S},1}-rd_{r,\mathcal{S},2})/|A|} \prod_{p\in T} p^{-t+\varepsilon} \\ =\ &CX^{1/|A|} \sum_{\substack{\mathcal{S}\in\mathfrak{S} \\ \max S > M}} \prod_{p\in S} p^{-d_{p,\mathcal{S},2}(d_{p,\mathcal{S},1}-r)/|A|} \prod_{p\in T} p^{-t+\varepsilon}. \end{aligned}$$

Now we can factor out the contributions from the primes $p \mid r|A|$. This can be achieved by splitting the sum over elements of $\mathfrak{S}$ into a sum over the part of $\mathfrak{S}$ corresponding to local conditions over primes $p \nmid r|A|$, and a sum over the local conditions on primes $p \mid r|A|$, and the latter sum is finite (since we may assume that $M > r|A|$). In particular, we may bound the contribution from primes dividing $r|A|$ by some constant C'. We may replace the sum over $\mathfrak{S}$ by a sum over tuples of pairwise relatively prime squarefree integers $(q_{G,H})$ where G ranges over the subgroups of S_r and H ranges over the subgroups of $S_{|A|}$. For any $\mathcal{S} \in \mathfrak{S}$, the integer $q_{G,H}$ is the product over all $p \in S$ such that the groups corresponding to p in $\mathcal{S}$ are G and H. We may also replace the condition $\max S > M$ by the much weaker bound $\max q_{G,H} > M$.

We will now bound the exponent of p in the product. Note that by [15], Theorems III.2.6 and III.2.9, we know that there exists ramification indices e_j and inertia degrees f_j such that $d_{p,\mathcal{S},1} = \sum_j (e_j - 1) f_j$ and $\sum_j e_j f_j = r$. Likewise, there is some integer $e \mid |A|$ greater than 1 such that $d_{p,\mathcal{S},2} = |A|(e-1)/e$ (remember that we are considering Galois A-extensions, so there is only one ramification index and one inertia degree). If $r = 3$, note that the inertia group at p corresponds to a totally ramified extension if and only if $d_{p,\mathcal{S},1} = 2$ (in fact this is the maximum value of $d_{p,\mathcal{S},1}$). Then, we will assume that $\gcd(6, |A|) = 1$ (this is stricter than the assumption used in [17]; the extension to $3 \mid |A|$ uses similar methods, but requires more casework, and will be omitted here). In this case, $d_{p,\mathcal{S},2}(d_{p,\mathcal{S},1}-r)/|A| \le 4/5(2-3)$, and accounting for the factor of $p^{-t+\varepsilon}$, we note that the largest possible power of p in the product is $p^{-8/5+\varepsilon}$. For

$r = 4$, a similar argument applies, because if $d_{p,\mathcal{S},1}$ is its maximum value of 3, the inertia group corresponds to an overramified (in fact totally ramified) extension and 2 is the maximum value achieved by other inertia groups. Note that the uniformity theorem for $r = 4$ is more naturally proved for overramified extensions [1, 17], hence it is stated that way. The largest possible power of p in the product is again $p^{-8/5+\varepsilon}$. If $r = 5$, note that now $t = 4/15$ and $d_{p,\mathcal{S},2} \geq 6|A|/7$, hence the largest possible power of p in the product is $p^{-6/7}p^{-4/15+\varepsilon} = p^{-118/105+\varepsilon}$ (from the totally ramified case).

Combining all of the above results, we find that

$$\begin{aligned} N(S_r \times A, X) - N_M(S_r \times A, X) &\leq CC'X^{1/|A|} \sum_{\max(q_{G,H})>M} \prod_{G,H} q_{G,H}^{-118/105+\varepsilon} \\ &\leq CC'DX^{1/|A|}\Big[\sum_{q=1}^{\infty} q^{-118/105+\varepsilon}\Big]^{D-1} \sum_{q=M+1}^{\infty} q^{-118/105+\varepsilon} \\ &\leq CC'DX^{1/|A|}\zeta(118/105-\varepsilon)^{D-1} \sum_{q=M+1}^{\infty} q^{-118/105+\varepsilon}. \end{aligned}$$

As the series for $\zeta(-118/105+\varepsilon)$ converges for sufficiently small ε, the right hand side is well defined. Further, if we combine this with equation (7), since C_M is increasing, and the previous result bounds C_M from above, as can be seen by taking the limit supremum as $X \to \infty$ of $X^{-1/|A|}N(S_r \times A, X))$, $\lim_{M\to\infty} C_M$ exists. Taking the same limit supremum and then taking $M \to \infty$ shows that $N(S_r \times A, X) \sim \big(\lim_{M\to\infty} C_M\big)X^{1/|A|}$, which is the desired result.

In the remaining sections, we will describe the proof and necessary tools, such as the geometric sieve and the parametrization of quintic rings, behind the uniformity theorem, and then give an overview of the proof in the case $r = 5$. The cases $r = 3, 4$ in [17] which will not be covered here use class field theory methods.

3 The discriminant polynomial for non-Galois extensions

It turns out that there is a general polynomial, called f_r in [3, 17], such that for an appropriate parametrization of the rings of integers of non-Galois degree-r field extensions $K/\mathbb{Q}$ with $G_K \cong S_r$, the polynomial f_r evaluated at a field K is the discriminant of K. A suitable parametrization has been determined for $r = 3, 4, 5$, in terms of group actions on vector spaces over $\mathbb{Z}$. For the purposes of the proof of the uniformity theorem, Theorem 3, we will just describe the construction for the case $r = 5$. For the rest of this section we will be following [2].

For any extension $K/\mathbb{Q}$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$. For any commutative ring extension $R/\mathbb{Z}$ which is also a free $\mathbb{Z}$-module of rank 5 (these are generalizations of the ring of integers of a number field of degree 5 over $\mathbb{Q}$), we may choose a basis $\langle 1, r_1, r_2, r_3, r_4\rangle$. Then a commutative ring extension $R/\mathbb{Z}$ which is a free module of rank 5 (simply known as a *quintic ring*) is determined by the coefficients C^i_{jk} defining the multiplicative structure of the ring,

$$r_j r_k = C^0_{jk} + C^1_{jk}r_1 + C^2_{jk}r_2 + C^3_{jk}r_3 + C^4_{jk}r_4.$$

An arbitrary set of coefficients $\{C^i_{jk} \mid 0 \leq i \leq 4, 1 \leq j, k \leq 4\}$ will correspond to a quintic ring if it is symmetric in j and k and the associative law holds.

The parametrization of quintic rings in [2] associates to a ring R *resolvent rings* S which are rank-6 free $\mathbb{Z}$-modules, and to every pair (R, S) a quadruple of 5×5 skew-symmetric matrices up to $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ symmetry, that is, an orbit of the tensor product $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ under the action of $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$. For any element $(M_1, M_2, M_3, M_4) \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, the structure coefficients C^i_{jk} of the ring are constructed as follows. For any $2m \times 2m$ skew-symmetric matrix B, the determinant of B is the square of a polynomial of degree m in the coefficients, and the Pfaffian of B is defined as this polynomial. For $m = 2$, the Pfaffian of a 4×4 skew-symmetric matrix B happens to be

$$\mathrm{Pf}(B) = \frac{1}{2}\sum_{\sigma\in S_4} \mathrm{sgn}(\sigma)B_{\sigma(1)\sigma(2)}B_{\sigma(3)\sigma(4)} = B_{12}B_{34} + B_{14}B_{23} - B_{13}B_{24},$$

which is quadratic in the coefficients of B. For a 5×5 skew-symmetric matrix M, there are 5 natural 4×4 skew-symmetric submatrices B_i; these can be constructed from M by removing the ith row and the ith column. Then we can define a symmetric bilinear form $Q : \wedge^2\mathbb{Z}^5 \times \wedge^2\mathbb{Z}^5 \to \mathbb{Z}^5$ such that $(Q(X, X))_i = 2(-1)^{i+1}\mathrm{Pf}(B_i)$, and a quadratic form $P(X) := \frac{1}{2}Q(X, X)$. (Note that for a general quadratic form $\tilde{P}(x) = \sum_{1\leq i\leq j\leq n} A_{ij}x_ix_j$ on $\mathbb{Z}^n$, we can define a symmetric bilinear form with integer coefficients $\tilde{Q}(x, y) = \sum_{1\leq i\leq j\leq n} A_{ij}(x_iy_j + x_jy_i)$, then $2\tilde{P}(x) = \tilde{Q}(x, x)$.) Now if i, j, k are distinct and nonzero, define

$$\begin{aligned} C^i_{jk} &= \operatorname{sgn}(ijk\ell)\, P(M_j)^\intercal M_\ell\, P(M_k), \\ C^i_{jj} &= \operatorname{sgn}(ijk\ell)\, Q(M_k, M_i)^\intercal M_i\, Q(M_i, M_\ell), \end{aligned}$$

where ℓ is the integer such that $ijk\ell$ is a permutation of $1, 2, 3, 4$. For any i and j, if k is the integer such that $\{i, k\} = \{1, 2\}$ or $\{3, 4\}$, and ℓ is the integer such that $ijk\ell$ is a permutation of $1, 2, 3, 4$ as before (if it exists, otherwise set $C^j_{ij} = 0$), let

$$\begin{aligned} C^j_{ij} &= \operatorname{sgn}(ijk\ell)\, Q(M_j, M_k)^\intercal M_\ell\, P(M_i), \\ C^i_{ii} &= \operatorname{sgn}(ijk\ell)(Q(M_i, M_j)^\intercal M_k\, Q(M_\ell, M_i) \\ &\qquad - Q(M_j, M_k)^\intercal M_\ell\, P(M_i)), \\ C^0_{ij} &= \sum_{n=1}^{4} C^m_{in} C^n_{mj} - C^n_{ij} C^m_{mn}, \end{aligned}$$

where any fixed n may be chosen for the last equation. It has been shown in [2] that this set of coefficients yields a quintic ring R(M) because it satisfies the associative law (see [2] for more details), and in particular the last equation holds for all n if it just holds for one value of n.

This particular parametrization of quintic rings is useful because of the following properties of this correspondence. First, we will mention one useful lemma about the group action itself.

Lemma 7. (Bhargava, 2008) [2] *For any $v \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$, the stabilizer of v in $GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ is isomorphic to the symmetric group S_5.*

We also mention that there is an invariant polynomial f_5 for this action, and that the following theorem holds.

Theorem 8. (Bhargava, 2008) [2] *For any $M \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$, the ring $R(M)$ constructed above is invariant under the action of $GL_2(\mathbb{Z}) \times SL_4(\mathbb{Z})$. If two elements M and $\widetilde{M}$ of the vector space $V := \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$ of quadruples of 5×5 skew-symmetric matrices yield the same set of coefficients C^i_{jk}, and those coefficients correspond to a maximal quintic ring R (that is, there is no quintic ring $R' \subseteq R$), M and $\widetilde{M}$ must be in the same orbit under the action of $SL_5(\mathbb{Z})$. Further, for every maximal order R there is exactly one $M \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$ such that $R = R(M)$. Under this correspondence, for any $M \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$, Disc $R(M) = f_5(M)$.*

4 The geometric sieve

The first part of the geometric sieve [4], is an estimate of the growth of the number of lattice points satisfying a set of congruence conditions over an infinite set of primes in an expanding region, for example rB where $B \subseteq \mathbb{R}^n$ is a fixed compact region and $r \to \infty$. This part is known as the Ekedahl sieve [10], where the set of congruence conditions is replaced by an appropriate algebraic variety over $\mathbb{Z}$. We first start with the following lemma, which is useful in constructing such an algebraic variety.

Lemma 9. (Bhargava, 2014) [4] *Let f be a irreducible polynomial over $\mathbb{Z}$ in n variables (so that the greatest common divisor of the coefficients is 1), let k be any positive integer, and let p be a prime. For any $u \in \mathbb{Z}^n$, say that f is strongly a multiple of p^k at u if $f(u) \equiv f(v) \equiv 0 \pmod{p^k}$ whenever $u \equiv v \pmod{p}$. There is a subscheme $Z \subseteq \mathbb{A}^n_\mathbb{Z}$ (not depending on p) such that f is strongly a multiple of p^k at $u \in \mathbb{Z}^n$ if and only if the residue class $u \pmod{p}$ modulo p is a $\mathbb{Z}/p\mathbb{Z}$-point of Z.*

Proof. We follow the method in [4]. Since f is irreducible, f has some nonzero coefficient modulo p. Let $g \in \mathbb{Z}[x_1]$ be the polynomial $g(x_1) := f(x_1, u_2, u_3, \ldots, u_n)$; then g reduces to a nonzero polynomial in $(\mathbb{Z}/p\mathbb{Z})[x_1]$. As $g(u)$ is a multiple of p^k for all $u \equiv u_1 \pmod{p}$, by expanding g as a Taylor series $g(u) = g(u_1) + (u - u_1)(dg/dx_1)(u_1) + \ldots$ (note that this series has deg $g + 1$ terms), and inserting $u \equiv u_1 \pmod{p}$, we find that $d^m g/dx_1^m \equiv 0 \pmod{p}$ for all $0 \le m \le k - 1$. By the definition of g, we see that $\partial^m f/\partial x_1^m = 0$ for $0 \le m \le k - 1$. Then the subscheme $Z = V(\partial^m f/\partial x_1^m \mid 0 \le m \le k - 1)$ of $\mathbb{A}^n_\mathbb{Z}$ satisfies the conditions. □

We will prove a version [17] of the growth estimate for lattice points in an algebraic variety with only a finite number of congruence conditions, where in the expanding region rB, r is now a lower triangular matrix acting on $B \subseteq \mathbb{R}^n$. The proof of such estimates [3, 17] involves induction on the dimension of the space, by considering an appropriate projection $\mathbb{A}^n_\mathbb{Z} \to \mathbb{A}^{n-1}_\mathbb{Z}$, finding a uniform estimate for the number of points on a fiber over some element of $\mathbb{A}^{n-1}_\mathbb{Z}$, and summing over all the fibers (where the inductive hypothesis is used to count the number of fibers).

Theorem 10. (Wang, 2017) [17] *Suppose that Z is a closed subscheme of $\mathbb{A}^n_{\mathbb{Z}}$ whose codimension is k. Let q be a squarefree integer with m prime factors and a be a positive constant. For any lower triangular matrix $L \in GL_n(\mathbb{R})$ such that $L_{ii} \geq a$ for all i, and any compact region $B \subseteq \mathbb{R}^n$,*

$$|\{x \in LB \cap \mathbb{Z}^n \mid \overline{x} \in Z(\mathbb{Z}/q\mathbb{Z})\}| \leq C^m D \max_{S \subseteq \{1,2,\ldots,n\}, |S| \leq k} \frac{\prod_{r \notin S} L_{rr}}{q^{k-|S|}}$$

for some constant C depending only on Z, and some constant D only depending on a, B, and Z. In the above, $\overline{x}$ denotes the residue class of x.

Proof. We will prove this by induction on n, following [17]. Suppose $n \geq 1$, and $(x_1, x_2, \ldots, x_{n-1}) \in \mathbb{Z}^{n-1}$ is any point. First, we will estimate the number of points in LB which are also in the fiber over this point, and then we will use the result for $n-1$ to estimate the number of points with fibers of dimension 0 and 1, which together give the result for n. Choose some $\alpha > 1/2$ such that for all $b \in B$, $|b_n| < \alpha$. If $x := (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ has $x \in LB$ and $\overline{x} \in Z(\mathbb{Z}/q\mathbb{Z})$, there is some constant β which depends on B, L, and x_j for $1 \leq j \leq n-1$ such that $x_n \in (L_{nn}(\beta - \alpha), L_{nn}(\beta + \alpha))$. This can be seen by noting that for any $u \in B$, as L is lower triangular, $(Lu)_i$ is a linear combination of $u_1, u_2, \ldots, u_i$ with the coefficient of u_i being L_{ii}, and setting $x = Lu$ for some $u \in B$ and $-\alpha < u_n < \alpha$. If $x_1, x_2, \ldots x_{n-1}$ are fixed, so are $u_1, u_2, ..., u_{n-1}$, and $x_n = \beta' + L_{nn}u_n$ for some constant β'. If we set $\beta = \beta'/L_{nn}$ (note that $L_{nn} \geq a > 0$), we find that $|x_n - L_{nn}\beta| < L_{nn}\alpha$, as mentioned earlier.

Consider the subscheme $Z' \subseteq \mathbb{A}^1_{\mathbb{Z}}$ consisting of those x_n such that $(x_1, x_2, \ldots, x_n) \in Z$. If $\dim Z' = 1$, then an approximation in which we ignore the congruence conditions from Z entirely will be sufficient, and we note that

$$|\{x_n \mid x \in LB \cap \mathbb{Z}^n, \overline{x} \in Z(\mathbb{Z}/q\mathbb{Z})\}| < 2\alpha L_{nn} + 1 \leq \Big(2\alpha + \frac{1}{a}\Big) L_{nn}.$$

If instead $\dim Z' = 0$, then Z' is given by some equation $f(x_n) = 0$. As $f(x_n) = 0$ has at most $\deg f$ roots in $\mathbb{Z}/p\mathbb{Z}$ for every p dividing q, as q has m prime factors, the variety $Z'(\mathbb{Z}/q\mathbb{Z})$ has at most $(\deg f)^m$ points. For any given $v \in \mathbb{Z}/q\mathbb{Z}$, as

$$\begin{aligned} &|(L_{nn}(\beta - \alpha), L_{nn}(\beta + \alpha)) \cap \{x_n \in \mathbb{Z} \mid x_n \equiv v (\text{mod } q)\}| \\ &= \Big| \mathbb{Z} \cap \Big(\frac{L_{nn}(\beta - \alpha) - v}{q}, \frac{L_{nn}(\beta + \alpha) - v}{q} \Big) \Big| < \frac{2\alpha L_{nn}}{q} + 1, \end{aligned}$$

we find that

$$|\{x_n \mid x \in LB \cap \mathbb{Z}^n, \overline{x} \in Z(\mathbb{Z}/q\mathbb{Z})\}| \leq (\deg f)^m \Big[1 + \frac{2\alpha L_{nn}}{q}\Big] < 4\alpha (\deg f)^m \max\Big\{1, \frac{L_{nn}}{q}\Big\}.$$

To complete the proof, we need to count the number of points $(x_1, x_2, \ldots, x_{n-1})$ that belong to each case. First, consider the closure Z' of the image of Z under the projection $\pi : \mathbb{A}^n_{\mathbb{Z}} \to \mathbb{A}^{n-1}_{\mathbb{Z}}$. By definition, $\dim Z' = \dim \pi(Z) \leq \dim Z$, hence the codimension of Z' is at least k. Consider the set $T \subseteq \mathbb{A}^{n-1}_{\mathbb{Z}}$ of points y such that $\pi^{-1}(y) \subseteq Z$ (that is, the fiber at y is one-dimensional). If $\{f_i \mid 1 \leq i \leq r\}$ is a set of defining polynomials for Z, we see that T is defined by the polynomials in $x_1, x_2, \ldots, x_{n-1}$ which are the coefficients of the polynomials f_i considered as polynomials in just x_n. Hence T is a closed subscheme of $\mathbb{A}^{n-1}_{\mathbb{Z}}$. As $T \times \mathbb{A}^1_{\mathbb{Z}} \subset Z$, we see that T has codimension at least k in $\mathbb{A}^{n-1}_{\mathbb{Z}}$. By the inductive hypothesis, we find that

$$\begin{aligned} |\{y \in \pi(LB \cap \mathbb{Z}^n) \mid \overline{y} \in Y'(\mathbb{Z}/q\mathbb{Z})\}| &= |\{y \in L'B' \cap \mathbb{Z}^{n-1} \mid \overline{y} \in Y'(\mathbb{Z}/q\mathbb{Z})\}| \\ &\leq C_1^m D_1 \max_{S \subseteq \{1,2,\ldots,n-1\}, |S| \leq k-1} \frac{\prod_{r \notin S} L_{rr}}{q^{k-1-|S|}} \end{aligned}$$

where L' is the matrix L with its nth row and column removed, $B' = \pi(B)$, C_1 is a constant depending on just Z, and D_1 is a constant depending on a, B, and Z. Similarly,

$$\begin{aligned} |\{y \in \pi(LB \cap \mathbb{Z}^n) \mid \overline{y} \in T(\mathbb{Z}/q\mathbb{Z})\}| &= |\{y \in L'B' \cap \mathbb{Z}^{n-1} \mid \overline{y} \in T(\mathbb{Z}/q\mathbb{Z})\}| \\ &\leq C_2^m D_2 \max_{S \subseteq \{1,2,\ldots,n-1\}, |S| \leq k} \frac{\prod_{r \notin S} L_{rr}}{q^{k-|S|}}, \end{aligned}$$

for constants C_2 and D_2 satisfying the same conditions as before. Hence,

$$\begin{aligned}|\{x \in LB \cap \mathbb{Z}^n \mid \overline{x} \in Z(\mathbb{Z}/q\mathbb{Z})\}| &< \Big(2\alpha + \frac{1}{a}\Big) L_{nn} |\{y \in \pi(LB \cap \mathbb{Z}^n) \mid \overline{y} \in T(\mathbb{Z}/q\mathbb{Z})\}| \\ &\quad + 4\alpha (\deg f)^m \max\Big\{1, \frac{L_{nn}}{q}\Big\} |\{y \in \pi(LB \cap \mathbb{Z}^n) \mid \overline{y} \in Y'(\mathbb{Z}/q\mathbb{Z})\}| \\ &\le C^m D \max_{S \subseteq \{1,2,\ldots,n\}, |S| \le k} \frac{\prod_{r \notin S} L_{rr}}{q^{k-|S|}},\end{aligned}$$

where $C = \max\{C_1 \deg f, C_2\}$ and $D = 4\alpha D_1 + (2\alpha + 1/a) D_2$, concluding the proof. □

The geometric sieve is a tool to calculate the number of values of a polynomial that satisfy a set of congruence conditions. In the application in [4] to finding squarefree values, the set of conditions is infinite, but for the uniformity theorem it is finite. The second step [3, 17] requires that the polynomial be an invariant for an appropriate action of a group variety on a vector space, and will use the fundamental domain of this action to count the desired number. For the uniformity theorem, a further averaging step [3, 6] is required, in particular, the following lemma will be needed.

Lemma 11. [6, 17] *Suppose that G is an affine group variety with an action on a vector space V of dimension n defined in terms of polynomials, and let f be an invariant polynomial for this action. Suppose that $V' \subseteq V$ is an orbit for this action such that the stabilizer of any element of V' is finite. Suppose also that the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$ has a fundamental domain $\mathcal{F}$. For any $x > 0$, any squarefree integer q, and any positive integer c, let $N_q(V', c, X)$ be the number of orbits of V' under the action of $G(\mathbb{Z})$ such that $|f|$ is bounded by X and f is strongly a multiple of p^c for all $p|q$. There exists a subscheme $Z \subseteq \mathbb{A}^n_{\mathbb{Z}}$ such that for any compact subset $B \subseteq V(\mathbb{R})$,*

$$N_q(V', c, X) = C \int_{\mathcal{F}} |\{x \in gB \cap V'(\mathbb{Z}) : |f(x)| \le X, \overline{x} \in Z(\mathbb{Z}/q\mathbb{Z})\}| dg \tag{8}$$

where dg is the Haar measure on $G(\mathbb{R})$, and C is some constant depending only on B and the normalization of the measure.

Proof. We follow [6] for much of the proof, and then follow [17] in rewriting the integral in terms of the subscheme $Z \subseteq A^n_{\mathbb{Z}}$. Note that some steps in [6] are not needed here as we explicitly compute the relevant integral in terms of the Haar measure of the set G_B^{-1} (defined below), and sum over the orbits later. Also, the argument in [6] is for the specific group action relevant for parametrizing non-Galois cubic fields, so we prove the more general form that would apply to quintic extensions that would be used in [17].

Choose any element $w \in V'$, and consider the subset $G_B \subseteq G(\mathbb{R})$ consisting of all $g \in G(\mathbb{R})$ such that $gw \in B \cap V'$, and define $G_B^{-1} = \{g^{-1} | g \in G_B\}$. We will now show that G_B and G_B^{-1} are compact whenever B is compact. As $G(\mathbb{R})$ embeds as a closed subset of $\mathbb{A}^m_{\mathbb{R}}$ in the analytic topology for some m, a subset of $G(\mathbb{R})$ is compact if and only if it is closed and bounded (also in the analytic topology). Since the map $G_B \to B$ is an n-fold cover of B defined by regular functions, there exists an open ball around any point of B with bounded preimage. As $B \subseteq V(\mathbb{R})$ is compact, we see that G_B is bounded and hence compact, and has finite measure. As inversion $g \to g^{-1}$ is a continuous map in the analytic topology (it is also given by regular functions since G is a group variety), G_B^{-1} is also compact and has finite measure.

We will now derive a relation to help us count the orbits where $|f|$ is bounded by X. Let S be the set of all $x \in V'$ such that $f(x)$ is strongly a multiple of p^c for all $p|q$ (as f is an invariant polynomial, S is $G(\mathbb{Z})$-invariant). Let $O(y)$ be the orbit of some $y \in S$ under the action of $G(\mathbb{Z})$, n be the size of the stabilizer of w under the action of $G(\mathbb{R})$, and $\mathcal{F}$ be the fundamental domain for the left action of $G(\mathbb{Z})$ on $G(\mathbb{R})$. If we choose $c \in G(\mathbb{R})$ such that $y = cw$ (as $G(\mathbb{R})$ is transitive), then for any $x \in O(y)$, and $g, h \in G(\mathbb{R})$, we see that $ghw = x$ if and only if there exists some g' in the stabilizer S_w of w under $G(\mathbb{R})$ and some $\alpha \in G(\mathbb{Z})$ for which $ghw = \alpha cw$ and $c^{-1}\alpha^{-1}gh = g'$, or equivalently, $g = \alpha c g' h^{-1}$. For any compact set $K \subseteq G(\mathbb{R})$, note that

$$\sum_{\alpha \in G(\mathbb{Z})} \mu(\alpha K \cap \mathcal{F}) = \sum_{\alpha \in G(\mathbb{Z})} \mu(K \cap \alpha^{-1}\mathcal{F}) = \mu(K),$$

for μ the Haar measure on $G(\mathbb{R})$ (which is left-translation invariant, see [12]), so we obtain the relation

$$\sum_{x \in O(y)} \int_{\mathcal{F}} |\{h \in G_B : ghw = x\}| \, dg = \sum_{\substack{\alpha \in G(\mathbb{Z}) \\ g' \in S_w}} \mu(\alpha c g' G_B^{-1} \cap \mathcal{F}) = \sum_{g' \in S_w} \mu(c g' G_B^{-1}) = n\mu(G_B^{-1}). \tag{9}$$

Now we will sum over all orbits of S such that $|f|$ is bounded by X. For any $g \in \mathcal{F}$, we see that

$$\sum_{x\in S,\,|f(x)|\le X} |\{h \in G_B : ghw = x\}| = n|\{x \in S \cap gB : |f(x)| \le X\}|,$$

as there are exactly n elements $h \in G_B$ such that $hw = g^{-1}x$ for any $x \in gB$. By Lemma 9, the subscheme $Z \subseteq A^n_{\mathbb{Z}}$ defined by the polynomials $\partial^j f/\partial x_n^j$ for all $0 \le j \le c-1$ has the property that

$$\{x \in S \cap gB : |f(x)| \le X\} = \{x \in gB \cap V'(\mathbb{Z}) : |f(x)| \le X,\, \overline{x} \in Z(\mathbb{Z}/q\mathbb{Z})\}.$$

Hence, summing equation (9) over the desired set of orbits gives

$$\mu(G_B^{-1})N_q(V', c, X) = \int_{\mathcal{F}} |\{x \in gB \cap V'(\mathbb{Z}) : |f(x)| \le X,\, \overline{x} \in Z(\mathbb{Z}/q\mathbb{Z})\}|\, dg,$$

so that equation (8) holds with $C = 1/\mu(G_B^{-1})$. □

5 The Uniformity Theorem for S_5 quintic extensions

We would like to find an estimate for the number of non-Galois S_5 quintic extensions of $\mathbb{Q}$ which are totally ramified at a specified set of primes, and we will count these by discriminant, so we will count those extensions whose discriminant is bounded by X. This will be a part of the error term for Malle's conjecture for non-Galois $S_5 \times A$ degree-$5|A|$ extensions of $\mathbb{Q}$, so we will not need the precise constant factor. In particular, we will show that

$$N_q(S_5, X) = O(X/q^{4/15-\varepsilon})$$

for any $\varepsilon > 0$. We will follow [17] for the rest of this section unless otherwise noted, in this outline of the proof of the uniformity theorem for $r = 5$.

By the results in Section 3, quintic rings can be parametrized by orbits of the vector space $V(\mathbb{Z}) = \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ under the left action of $G(\mathbb{Z}) = \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$, and the discriminant of a quintic ring is the value of the invariant polynomial f_5 of degree 40 defined on this vector space. We would like to apply Theorem 10 and Lemma 11 to bound the number $N_q(S_5, X)$, but we must first rewrite the problem in terms of strong multiples of an appropriate polynomial.

Suppose that $K/\mathbb{Q}$ is a non-Galois S_5 quintic extension totally ramified at some prime p. We claim that the discriminant polynomial f_5 is strongly a multiple of p^4 at the element $v \in V(\mathbb{Z})$ corresponding to this extension. We will perform the computation more explicitly, rather than use Theorems III.2.6 and III.2.9 of [15], as we will show that this can be determined from the congruence classes of the structure constants of $\mathcal{O}_K$ in an appropriate basis. Suppose that p ramifies as $p = \mathfrak{p}^5$ in K. As $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \cong \mathbb{Z}/p\mathbb{Z}$, for any integral basis $\{1, r_1, r_2, r_3, r_4\}$ for $\mathcal{O}_K$, we may construct an integral basis $\{1, r_1', r_2', r_3', r_4'\}$ such that $v_{\mathfrak{p}}(r_i') = i$, as follows. Choose some integer $0 \le \alpha_{00} \le p-1$ such that $\alpha_{00} \equiv r_1 \pmod{\mathfrak{p}}$, and let $r_1' = r_1 - \alpha_{00}$, then $r_1' \in \mathfrak{p}$. Next, choose some integers $0 \le \alpha_{10}, \alpha_{11} \le p-1$ such that $r_2 \equiv \alpha_{10} + \alpha_{11}r_1' \pmod{\mathfrak{p}^2}$; we may define $r_2' := r_2 - \alpha_{11}r_1' - \alpha_{10}$ which is evidently an element of $\mathfrak{p}^2$. Proceeding in this way yields a set $\{1, r_1', r_2', r_3', r_4'\}$ which is an integral basis by construction. The discriminant of the ring $\mathcal{O}_K$ (as defined in [2, 15]) is $\det \mathrm{Tr}(r_i'r_j')$ where $r_0' = 1$, and $\mathrm{Tr}(r)$ is the trace of the multiplication-by-r map. For any $0 \le k \le 4$, if we write $r_i'r_j'r_k' = \sum_{\ell=0}^4 d_{ijk\ell}r_\ell'$ for integers $d_{ijk\ell}$, then every term on the right hand side has a different $\mathfrak{p}$-adic valuation, so that $v_{\mathfrak{p}}(d_{ijkk}) \ge i + j$ and $p|\mathrm{Tr}(r_i'r_j')$ whenever $(i, j) \ne (0, 0)$. As all but one of the entries of the 5×5 matrix $(r_i'r_j')_{0\le i,j\le 4}$ are multiples of p, the discriminant of K is a multiple of p^4. To see that f_5 is strongly a multiple of p^4 at the corresponding point $v \in V(\mathbb{Z})$, pick any $w \in V(\mathbb{Z})$ with $w \equiv v \pmod{p}$. As the structure constants of the ring associated to w are congruent to the structure constants of the ring associated to v modulo p (from the explicit equations for the structure constants in Section 3), we may deduce the desired result as the trace formula [2, 15] for the discriminant only depends on the structure constants of the ring.

The next step is to check that the conditions on the group action in Lemma 11 do hold for the action of $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ on $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. We will not explicitly verify these axioms, but we will note that the following facts have been proved about this action. First, the action of $G(\mathbb{R})$ on $V(\mathbb{R})$ is known to have three orbits [3], the stabilizer of any element of $V(\mathbb{C})$ is the group S_5 (Lemma 7), and the there is a fundamental domain for the action of $G(\mathbb{R})$ on $V(\mathbb{R})$ [3].

We will now outline the proof. Recall that in the statement of Theorem 10, the lower triangular matrix is assumed to have all diagonal entries to be positive and to be larger than some fixed constant. We can then split the vector space into many regions, depending on whether certain coordinates are zero or not (see[3]). Then in each region, the integral over the fundamental domain can be bounded by applying Theorem 10 to the integrand, and then choosing an appropriate measure for the domain ([3] gives such a measure). Note at this step, we have to use the fact (see [4, 17]) that the variety defined by f_5 and its first three partial derivatives with respect to one variable does have codimension 4. Bounding this integral for each region, and summing over all of the regions, yields the theorem.

6 Other results

We briefly mention other results concerning Malle's Conjecture. The conjecture has been proven (including [5, 8]) for the embeddings $S_3 \to S_6$ (corresponding to Galois S_3 extensions, the proof uses the Davenport-Heilbronn Theorem for the asymptotics for non-Galois cubic extensions, and the fact that every S_3 extension contains a unique non-Galois cubic extension) and $D_4 \to S_4$ (by proving that the associated Dirichlet series are holomorphic in the appropriate domain). We also note that Klüners [11] came up with a counterexample to the conjecture, for a particular class of degree-6 field extensions $L/\mathbb{Q}$ for which there exists an intermediate field K with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$ and $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

Acknowledgements

I thank Prof. Melanie Wood for introducing me to this topic in a course on the distribution of class groups.

References

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

[2] M. Bhargava, *Higher Composition Laws IV: The parametrization of quintic rings*, Ann. of Math. **167** (2008), pp. 53–94

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

[4] M. Bhargava, *The geometric sieve and the density of squarefree values of invariant polynomials*, arxiv: 1402.0031

[5] M. Bhargava, M. M. Wood, *The Density of Discriminants of S_3-Sextic Number Fields*, Proc. Amer. Math. Soc., **136** (2008), No. 5, pp. 1581–1587

[6] M. Bhargava, A. Shankar, J. Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, Invent. Math. **193** (2013), pp. 439–499

[7] M. Bhargava, A. Shankar, X. Wang, *Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces*, arxiv: 1512.03035

[8] H. Cohen, F. Diaz y Diaz, M. Olivier, *Enumerating Quartic Dihedral Extensions of* $\mathbb{Q}$, Compositio Math. **133** (2002), pp. 65–93

[9] B. Datkovsky, D. Wright, *Density of discriminants of cubic extensions*, J. Reine Angew. Math. **386** (1988), pp. 116–138.

[10] T. Ekedahl, *An infinite version of the Chinese remainder theorem*, Comment. Math. Univ. St. Paul. **40** (1991), pp. 53–59

[11] J. Klüners, *A Counter Example to Malle's Conjecture on the Asymptotics of Discriminants*, C. R. Math. Acad. Sci. Paris, **340** (2005), No. 6, pp. 411–414

[12] A. W. Knapp, *Lie Groups Beyond an Introduction*, Progress in Mathematics **140**, Birkhäuser, Boston, 1996

[13] G. Malle, *On the Distribution of Galois Groups II*, Exp. Math. **13** (2004), No. 2, pp. 129–136

[14] R. Masri, F. Thorne, W.-L. Tsai, J. Wang, *Malle's Conjecture for $G \times A$, with $G = S_3, S_4, S_5$*, arxiv: 2004.04651

[15] J. Neukirch, *Algebraic Number Theory*, A Series of Comprehensive Studies in Mathematics **322**, Springer-Verlag, New York, 1999

[16] B. Poonen, *Squarefree Values of Multivariable Polynomials*, Duke Math. J. **118** (2003), No. 2, pp. 353–373

[17] J. Wang, *Malle's Conjecture for $S_n \times A$ for $n = 3, 4, 5$*, arxiv: 1705.00044

[18] D. J. Wright, *Distribution of Discriminants of Abelian Extensions*, Proc. London Math. Soc. **58** (1989), No. 3, pp. 17–50