The number of non-S_5 quintic extensions of bounded discriminant

Manjul Bhargava, Alina Carmen Cojocaru, and Frank Thorne

April 16, 2015

Abstract

We prove that the number of quintic fields K having associated Galois group strictly contained in S_5 and $|\operatorname{Disc}(K)| < X$ is $\mathrm{O}_\varepsilon(X^{\frac{39}{40}+\varepsilon})$. Indeed, we give four different short proofs (one of them due to Shankar and Tsimerman [ShTs], and the rest new) that this number is $\mathrm{O}_\varepsilon(X^{1-\delta})$ for some $\delta > 0$.

As a consequence, we prove that the number of S_5-quintic fields K with $|\operatorname{Disc}(K)| < X$ is $c(S_5)X + O(X^{\frac{79}{80}+\varepsilon})$ for an explicit constant $c(S_5)$, improving upon a result of the first author [Bh3] and Shankar and Tsimerman [ShTs]. We also obtain a power-saving error term in the case where the quintic fields in question are restricted to obey a specified finite list of splitting conditions.

1 Introduction

A central problem in arithmetic statistics is that of understanding the asymptotic number of number fields with a given Galois group and bounded discriminant. For a permutation group $G \subset S_n$, let $N_n(X, G)^{\blacksquare}$ denote the number of isomorphism classes of number fields K of degree n such that the Galois closure of K over $\mathbb{Q}$ has Galois group isomorphic to G (as a permutation group on the embeddings of K into $\bar{\mathbb{Q}}$). The aim is then to understand the behavior of $N_n(X, G)$ as $X \to \infty$ for various groups G.

In [Bh3, Thm. 1, p. 1559] it was shown that the total number of quintic number fields having absolute discriminant at most X is asymptotically equal to cX, where $c = c(S_5)$ is given by

$$c(S_5) := \frac{13}{120} \prod_p \left(1 + \frac{1}{p^2} - \frac{1}{p^4} - \frac{1}{p^5}\right) > 0.$$

Furthermore, in [Bh3, Thm. 4, p. 1561] it was shown that 100% of these quintic fields have associated Galois group S_5, i.e. that

$$N_5(X, S_5) \sim c(S_5)\, X. \tag{1}$$

Consequently,

$$N_5(X, G) = \mathrm{o}(X)$$

for the other four possible G, namely A_5, C_5, D_5, and F_5. (See [Co, p. 369] for a proof that these are the only possible G; here F_5 denotes the *Frobenius group*, given by the presentation $F_5 := \langle \sigma, \tau : \sigma^5 = \tau^4 = 1, \tau\sigma\tau^{-1} = \sigma^2 \rangle$.)

In applications it becomes important to understand the growth of the $N_5(X,G)$ much better and it is desirable to at least have a power-saving estimate in X. This is perhaps especially interesting in the case $G = A_5$; for example, via the work of Deligne and Serre [DeSe], A_5-quintic fields are naturally associated to certain weight one holomorphic cuspidal newforms, referred to as "of icosahedral type". Information on $N_5(X, A_5)$ thus gives information about the existence and the number of weight one icosahedral cuspforms. Indeed, along these lines Rohrlich [Ro] has applied our results to prove that self-dual Artin representations of dimension two have density zero among all two-dimensional Artin representations.

The purpose of this article is precisely to prove such an estimate:

Theorem 1 *For G any proper transitive subgroup of S_5, i.e. $G \in \{C_5, D_5, F_5, A_5\}$, we have*

$$N_5(X,G) \ll_\varepsilon X^{\frac{39}{40}+\varepsilon}.$$

Such a bound, with an error term $\ll X^{\frac{199}{200}+\varepsilon}$, was proved (although not highlighted) in work of Shankar and Tsimerman [ShTs] using the Selberg sieve.

For $G = C_5$ and $G = D_5$, stronger results are in fact known. It was proved by Cohen, Diaz y Diaz, and Olivier [CoDiOl1] that $N_5(X, C_5) \sim c(C_5)X^{1/4}$ (with an explicit and complicated constant $c(C_5)$), by means of Kummer theory and class field theory. For $G = D_5$, an upper bound of $N_5(X, D_5) \ll X^{3/4+\varepsilon}$ was proved by Klüners [Kl]; he also proved that $N_5(X, D_5) \ll X^{1/2}$ (the expected order of magnitude) conditionally on a form of the Cohen-Lenstra heuristics.

For both $G = A_5$ and $G = F_5$, the results are apparently new. In the A_5 case, the authors are unfamiliar with any other approach which seems likely to yield comparable or stronger bounds on $N_5(X,G)$. In the F_5 case, it seems possible that the techniques used by Klüners could be adapted to prove some sort of upper bound on $N_5(X, F_5)$, but we don't investigate this here.

The order of growth

$$N_5(X,G) \sim c(G)X^{\frac{1}{2}} \log X \tag{2}$$

was conjectured for $G = A_5$ and $G = F_5$ by Malle [Ma]; we refer to this paper and its references for heuristics and general conjectures of a similar type.

Our methods also would yield results for quartic or cubic extensions; however, in these cases there is little prospect of improving on known results. The relevant groups are C_4, D_4, V_4, A_4, and C_3; we refer to [CoDiOl2] for a survey covering all cases except A_4, with complete references. For $G = A_4$ it was proved by Wong [Wo] that $N_4(X, A_4) \ll X^{\frac{5}{6}+\epsilon}$. If we were to adapt the methods of this paper to quartic fields, we might hope to obtain upper bounds $\ll X^{\frac{11}{12}}$; as the quartic analogue of the lattice $V_{\mathbb{Z}}$ described in Section 2 is 12-dimensional (see [Bh1]), error terms $\asymp X^{\frac{11}{12}}$ would naturally occur throughout our analysis, so that this seems to be a natural bottleneck for any of the techniques applied here.

For some work on higher degree fields, see Ellenberg-Venkatesh [ElVe] and Dummit [Du].

Shankar and Tsimerman's objective in proving a form of Theorem 1 was to prove a power saving error term (also of $\mathrm{O}(X^{\frac{199}{200}+\varepsilon})$) for $N_5(X, S_5)$, and here we improve upon their results:

Theorem 2 *We have*

$$N_5(X, S_5) = c(S_5) + \mathrm{O}(X^{\frac{79}{80}+\varepsilon}).$$

Moreover, we will mildly generalize their results by allowing for 'local specifications', for example counting only those fields in which a fixed, finite set of primes is ramified; see Theorem 13 for a precise statement. This generalization is motivated by works of Martin and Pollack [MaPo], Yang [Ya], Cho and Kim [ChKi], and others which applied similar results in the cubic and/or quartic cases to obtain a variety of interesting results. Moreover, for quintic fields such a generalization was previously obtained in independent works of Cho and Kim [ChKi2] and Lemke Oliver and Thorne [LOTh], again with (differing) applications, and so here we improve upon the error terms proved there.

To illustrate the mildly unusual nature of the problem of estimating $N_5(X, G)$, we give not one, but four approaches leading to various error terms in Theorem 1: Heath-Brown's square sieve (for $G \in \{C_5, D_5, A_5\}$ only), Selberg's sieve (following [ShTs]), Turán's sieve, and Bhargava's recent quantitative version of Ekedahl's geometric sieve. All of these approaches apply Bhargava's parametrization (Theorem 3) of quintic rings by lattice points in a 40-dimensional vector space, and error terms of order $X^{\frac{39}{40}}$ naturally appear in various counts for these lattice points. This does not rule out the possibility of further improving the necessary error terms, but, for the moment, it appears rather difficult.

We begin in Section 2 with a description of Bhargava's parametrization [Bh2] of quintic rings and fields, as well as his counting results [Bh3] which we apply in our sieves. In Section 2 we also prove that non-S_5-quintic field discriminants must be squarefull.

This brings us to our various sieve estimates. With the exception of the square sieve, where we exclude $G = F_5$, all of our proofs will handle all $G \neq S_5$ simultaneously. In Section 3 we use Heath-Brown's square sieve to prove that $N_5(X, G) \ll X^{\frac{119}{120}}(\log X)^{\frac{2}{3}}$. In Section 3 we use the Selberg sieve to prove that $N_5(X, G) \ll X^{\frac{199}{200}+\epsilon}$; this result is due to Shankar and Tsimerman [ShTs] and we present it here in a slightly modified form. In Section 5 we show that the Turán sieve yields a better error term of $N_5(X, G) \ll X^{\frac{119}{120}}(\log X)^{\frac{2}{3}}$; this is perhaps surprising, in view of the fact that the Turán sieve is simpler and requires less input than the Selberg sieve.

In Section 6 we prove our strongest result that $N_5(X, G) \ll X^{39/40+\varepsilon}$, using Ekedahl and Bhargava's geometric sieve [Bh4]. In contrast to the other proofs, we must go 'under the hood' and work with Bhargava's proofs in [Bh3] rather than just his end results.

Finally, we conclude in Section **??** by proving Theorem 2. The main input is our improved result that $N_5(X, G) \ll X^{39/40+\varepsilon}$, so essentially all we must do is repeat the end of Shankar and Tsimerman's proof. However, we simultaneously formulate and prove an easy generalization to counting S_5-field extensions with finitely many prescribed 'local conditions'.

2 Parametrization of quintic rings and fields

We briefly recall the main results of [Bh2] and [Bh3] needed to prove Theorems 1 and 2. For any commutative ring T (with unit), let V_T denote the space $T^4 \otimes \wedge^2 T^5$ of quadruples $v = (A, B, C, D)^t$ of 5×5 skew-symmetric matrices with entries in T and let $a_{12} = a_{12}(v)$ denote the $(1, 2)$ entry of A. The group $G_T := \mathrm{GL}_4(T) \times \mathrm{SL}_5(T)$ acts on V_T via

$$(\gamma_4, \gamma_5) \cdot (A, B, C, D)^t := \gamma_4 \left(\gamma_5 A \gamma_5^t, \gamma_5 B \gamma_5^t, \gamma_5 C \gamma_5^t, \gamma_5 D \gamma_5^t\right)^t.$$

When $T = \mathbb{Z}$, the action of $G_\mathbb{Z}$ on $V_\mathbb{Z}$ gives rise to a natural invariant polynomial in 40 variables and of degree 40, called the *discriminant* and denoted Disc, which generates the whole ring of polynomial invariants.

For T a field, the orbits of G_T on V_T were first classified by Wright and Yukie [WrYu] and were shown to be in a natural correspondence with étale degree 5 extensions of T. For $T = \mathbb{Z}$, the orbits of $G_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$ were classified by Bhargava [Bh2] in terms of quintic rings and their sextic resolvent rings as follows.

Theorem 3 (Bhargava [Bh2, p. 54])
The $G_{\mathbb{Z}}$-orbits on $V_{\mathbb{Z}}$ are in canonical bijection with the isomorphism classes of pairs (R, S), where R is a quintic ring and S is a sextic resolvent ring of R. In this bijection, for an orbit $v \in G_{\mathbb{Z}}\backslash V_{\mathbb{Z}}$ and its associated quintic ring $R(v)$ we have $\operatorname{Disc}(v) = \operatorname{Disc}(R(v))$. *Furthermore, every isomorphism class of a quintic ring R occurs in this bijection, and every isomorphism class of a maximal quintic ring occurs exactly once.*

Here, a *quintic ring* R is a commutative ring (with unit) isomorphic to $\mathbb{Z}^5$ as a $\mathbb{Z}$-module. A *sextic resolvent ring* S is defined in [Bh2, §5]; this definition will not be needed in what follows. The *discriminant* $\operatorname{Disc} R$ of a ring R is defined as usual by $\det(\operatorname{Tr}(\alpha_i\alpha_j))$ for a $\mathbb{Z}$-basis (α_i) of R, where $\operatorname{Tr}(\alpha)$ is the trace of the endomorphism on R defined by multiplication by α. For complete definitions and details, see the original source, [Bh2].

An orbit v is called *irreducible* if $R(v)$ is an integral domain. For such v, we denote by $K(v)$ the fraction field of $R(v)$ and by $G(v)$ the Galois group over $\mathbb{Q}$ of $\widehat{K(v)}$.

Essentially following [Bh3, p. 1568-9], we write

$$N^+(V_{\mathbb{Z}}, X) := \#'\{v \in G_{\mathbb{Z}}\backslash V_{\mathbb{Z}} \;:\; 0 < |\operatorname{Disc}(v)| < X\}, \tag{3}$$

$$N^{\square}(X) := \#'\{v \in G_{\mathbb{Z}}\backslash V_{\mathbb{Z}} \;:\; v \text{ irreducible, } |\operatorname{Disc}(v)| \text{ squarefull, } 0 < |\operatorname{Disc}(v)| < X\}, \tag{4}$$

where in each case the dash indicates that each irreducible v is counted by the weight $|\operatorname{Stab}_{G_{\mathbb{Z}}}(v)|^{-1}$, equal to 1 for any v corresponding to the maximal order of any non-Galois quintic field, and that each *reducible* v has a weight in $[0, |\operatorname{Stab}_{G_{\mathbb{Z}}}(v)|^{-1}]$, which may depend on both v and X. We only care that this weight is nonnegative; we explain its definition and purpose in Theorem 6.

Our interest in bounding $N^{\square}(X)$ is explained by the following lemma:

Lemma 4 *Let $G \in \{A_5, C_5, D_5, F_5\}$ and let $v \in G_{\mathbb{Z}}\backslash V_{\mathbb{Z}}$ irreducible such that $G(v) \simeq G$. If $G \not\simeq F_5$, then* $\operatorname{Disc}(v)$ *is a square; if $G \simeq F_5$, then $p^2 |\operatorname{Disc}(v)$ for any prime $p|\operatorname{Disc}(v)$. In particular, in either case,* $\operatorname{Disc}(v)$ *is squarefull.*

Proof: Let $K = K(v)$. If $G \in \{C_5, D_5, A_5\}$, then $G \leq A_5$ and hence, by [DuFo, p. 610], $\operatorname{Disc}(K)$ must be a square.

If $G \simeq F_5$, there exists a unique subfield F of $\hat{K}$ of degree 4 over $\mathbb{Q}$. By the *Brauer relation*

$$\zeta(s)^4 \zeta_{\hat{K}}(s) = \zeta_K(s)^4 \zeta_F(s)$$

(see [FrTa, Theorems 73 and 75]), we have $\operatorname{Disc}(\hat{K}) = \operatorname{Disc}(K)^4 \operatorname{Disc}(F)$ (as can be seen, for example, by inspecting the functional equations of both sides). Thus

$$\operatorname{Disc}(K) = \operatorname{Disc}(F)\mathcal{N}_{F/\mathbb{Q}}(\mathfrak{f}(\hat{K}/F)),$$

where $\mathfrak{f}(\hat{K}/F)$ is the conductor of $\hat{K}/F$.

For each prime p dividing $\mathrm{Disc}(F)$, since $F/\mathbb{Q}$ is cyclic we must have $p^2 \mid \mathrm{Disc}(F)$, and thus $p^2 \mid \mathrm{Disc}(K)$. Suppose now that $p \mid \mathrm{Disc}(K)$ but $p \nmid \mathrm{Disc}(F)$. Then every prime of $\mathcal{O}_F$ above p must be ramified, hence totally ramified, in $\hat{K}/F$. This implies that the ramification degrees of p satisfy $e_p(\hat{K}/\mathbb{Q}) = e_p(K/\mathbb{Q}) = 5$, and hence that $p^4 \mid \mathrm{Disc}(K)$. □

In light of this result, for any transitive proper subgroup $G < S_5$ we have

$$N_5(X, G) \leq N^{\Box}(X).$$

We will also apply the following additional characterization.

Lemma 5 *If K is a quintic field with $\mathrm{Gal}(\hat{K}/\mathbb{Q}) \in \{A_5, C_5, D_5, F_5\}$, then no prime p can have splitting type (1112) in K; i.e., we cannot have $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ where $\mathfrak{p}_1$ has residue class degree 2 over $p\mathbb{Z}$ and the remaining $\mathfrak{p}_i$ have residue class degree 1.*

Proof: If any prime had this splitting type, then $\mathrm{Gal}(\hat{K}/\mathbb{Q})$ would contain a transposition; since $\mathrm{Gal}(\hat{K}/\mathbb{Q})$ also contains a 5-cycle it would then be all of S_5. □

For any $G_{\mathbb{Z}}$-invariant subset S of $V_{\mathbb{Z}}$ defined by congruence conditions modulo m for some integer $m \geq 1$, we write

$$N^+(S, X) := \#'\{v \in G_{\mathbb{Z}}\backslash S \ : \ v \text{ irreducible}, \ 0 < |\mathrm{Disc}(v)| < X\}, \tag{5}$$

and we write $\delta(S)$ for the proportion of elements of $V_{\mathbb{Z}/m\mathbb{Z}}$ whose lifts belong to S. The following counting theorem establishes that $\delta(S)$ is the 'density' of S:

Theorem 6 (Bhargava [Bh3, (26)-(27), pp. 1585–1586])
With the definitions above, if $m \ll X^{1/40}$ and $m\delta(S) \gg 1$, then

$$N^+(S, X) = C\delta(S)X + \mathrm{O}\left(m\delta(S)X^{39/40}\right) \tag{6}$$

with

$$C := \frac{1}{2} \cdot \left(\frac{1}{8} + \frac{1}{12} + \frac{1}{120}\right) \cdot \zeta(2)^2\zeta(3)^2\zeta(4)^2\zeta(5) \tag{7}$$

and where the implied constant in (6) *is absolute.*

Proof: This result is stated in [Bh3] for $N(S, X)$ instead of $N^+(S, X)$, i.e., using the notation of [Bh3, p. 1568], for $v \in G_{\mathbb{Z}}\backslash V_{\mathbb{Z}}$ which are *irreducible*. The result as stated is ideally suited for our purposes, but **Manjul please confirm** there is a typo in [Bh3]. Instead, the result in [Bh3] is proved for all $v \in G_{\mathbb{Z}}\backslash V_{\mathbb{Z}}$, irreducible or not, with the extra condition that the first coordinate $a_{12}(v)$ is nonzero.

This condition on $a_{12}(v)$ depends on the actual element $v \in V_{\mathbb{Z}}$ and not just its $V_{\mathbb{Z}}$-orbit, so v is chosen to lie in $\mathcal{F}w$, where $\mathcal{F}$ is a fundamental domain for the action of $G_{\mathbb{Z}}$ on $G_{\mathbb{R}}$, so that for any nonsingular w, $\mathcal{F}w$ is a fundamental domain for the action of $G_{\mathbb{Z}}$ on the $G_{\mathbb{R}}$-orbit $V_{\mathbb{R}}^{(i)}$ of w, of which there are three. The element w is, in turn, chosen to lie in $V_{\mathbb{R}}^{(i)} \cap H$ for a fixed compact set H. Each element v is then given a weighting of $|\mathrm{Stab}_{G_{\mathbb{Z}}}(v)|^{-1}$ times the measure of the set of

$w \in V_{\mathbb{R}}^{(i)} \cap H$ for which the unique $G_{\mathbb{Z}}$-representative of v in $\mathcal{F}w$ has $a_{12} \neq 0$, normalized so that the total measure of $V_{\mathbb{R}}^{(i)} \cap H$ is 1. For reducible orbits we only care that this weight is nonnegative.

For irreducible orbits, Lemma 11 of [Bh3] establishes that the difference between $|\operatorname{Stab}_{G_{\mathbb{Z}}}(v)|^{-1}$ and this normalized weight, totalled over all irreducible $v \in G_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$ with $|\operatorname{Disc}(v)| < X$, is $O(X^{\frac{39}{40}})$. Therefore, subject to the condition $m\delta(S) \gg 1$ stated in our version of Bhargava's theorem, the error in (6) $\gg X^{\frac{39}{40}}$ so that for irreducible elements we may replace this complicated weight with $|\operatorname{Stab}_{G_{\mathbb{Z}}}(v)|^{-1}$, as stated in the definition of $N^{+}(S, X)$. □

The following choices of S will allow us to sieve for squares:

Proposition 7 *Let q be the product of k distinct odd primes, and for each prime $p \mid q$ let S_p denote one of the following three sets:*

- *Write $S_p^{\pm}$ for the set of $v \in G_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$ for which $\left(\frac{\operatorname{Disc}(v)}{p}\right) = \pm 1$;*
- *Write $S_p(1112) = T_p(1112)$ (using the notation of [Bh2, Section 12]) for the set of $v \in G_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$ for which p has splitting type (1112).*

Then

$$\delta\left(\cap_{p|q} S_p\right) = \prod_{p|q} \delta_p$$

with

$$\begin{aligned}
\delta_p^{+} = \delta_p^{-} &:= \frac{1}{2} \cdot \frac{(p-1)^8 p^{16} (p+1)^4 (p^2+1)^2 (p^2+p+1)^2 (p^4+p^3+p^2+p+1)}{p^{40}} \\
&= \frac{1}{2} \cdot \Big(1 - p^{-1} + \mathrm{O}(p^{-2})\Big),
\end{aligned}$$

$$\delta_p(1112) := \frac{1}{12} \cdot \frac{(p-1)^8 p^{16} (p+1)^4 (p^2+1)^2 (p^2+p+1)^2 (p^4+p^3+p^2+p+1)}{p^{40}}.$$

Proof: The proof can be extracted from [Bh2, Bh3] and we outline it below. First, observe that by the Chinese remainder theorem it suffices to assume that $q = p$ is an odd prime. In [Bh2, p. 90], Bhargava introduced the sets $T_p(\sigma)$ for

$$\sigma \in \{(11111), (1112), (113), (122), (23), (14), (5)\},$$

defined such that $v \in V_{\mathbb{Z}}$ is in $T_p(\sigma)$ iff $R(v)$ satisfies

$$R(v)/(p) \simeq \mathbb{F}_{p^{f_1}} \oplus \cdots \oplus \mathbb{F}_{p^{f_k}}, \quad \sigma = (f_1 \ldots f_k).$$

A classical theorem of Stickelberger implies that $\operatorname{Disc}(v)$ is a quadratic residue modulo p if and only if k is odd, i.e., if

$$\sigma \in \{(11111), (113), (122), (5)\}, \tag{8}$$

and a quadratic nonresidue if and only if

$$\sigma \in \{(1112), (23), (14)\}. \tag{9}$$

Therefore, the density (for $q = p$) is given by the total of the densities of the $T_p(\sigma)$, where $\sigma = (1112)$ or ranges over the set in (8) or (9) respectively. These densities are computed in [Bh2, Lemma 20], and this completes the proof. □

3 Proof via the square sieve

In this section we shall explore that A_5-, D_5-, and C_5- extensions have square discriminants and prove the bound

$$N_5(X,G) \ll X^{\frac{119}{120}}(\log X)^{\frac{2}{3}} \tag{10}$$

for each of these G.

A natural tool for detecting squares is the classical Legendre symbol. In appropriate settings, this tool can be used successfully towards estimating, from above, the number of squares in a finite sequence. Indeed, such a procedure is illustrated by what is now referred to as the *square sieve*, a version of which we now recall.

Proposition 8 (Heath-Brown [HB])
Let $\mathcal{A}$ denote any multiset of nonzero integers of absolute value at most X, and let $\mathcal{P}$ be any finite set of primes with $e^{|\mathcal{P}|} > X$. If $S(\mathcal{A})$ denotes the number of squares in $\mathcal{A}$, then we have

$$S(\mathcal{A}) \ll \frac{|\mathcal{A}|}{|\mathcal{P}|} + \frac{1}{|\mathcal{P}|^2}\sum_{p\neq p'\in\mathcal{P}}\left|\sum_{n\in\mathcal{A}}\left(\frac{n}{pp'}\right)\right|. \tag{11}$$

Heath-Brown's proof is by obtaining upper and lower bounds for the quantity $\sum_{a\in\mathcal{A}}\left(\sum_{p\in\mathcal{P}}\left(\frac{a}{p}\right)\right)^2$; see also [CoMu, p. 21] for a slight variation.

For our application, let $\mathcal{A}$ be the weighted multiset of discriminants $\mathrm{Disc}(v)$ counted by $N^+(V_{\mathbb{Z}},X)$ with $G(v)\in\{A_5,D_5,C_5\}$, and let $\mathcal{P}$ consist of all odd primes $< z$ for some parameter $z = z(X) \ll X^{\frac{1}{80}}$. It is immediate from Theorem 6 and Proposition 7 that

$$\left|\sum_a\left(\frac{a}{pp'}\right)\right| \ll pp'X^{\frac{39}{40}},$$

whence, by Proposition 8,

$$\begin{aligned} N_5(X,A_5)+N_5(X,D_5)+N_5(X,C_5) &\ll S(\mathcal{A}) \\ &\ll \frac{|\mathcal{A}|}{|\mathcal{P}|} + \frac{1}{|\mathcal{P}|^2}\sum_{p\neq p'\in\mathcal{P}}\left|\sum_{a\in\mathcal{A}}\left(\frac{a}{pp'}\right)\right| \\ &\ll \frac{X\log X}{z} + X^{\frac{39}{40}}z^2; \end{aligned}$$

we conclude by taking $z \asymp X^{\frac{1}{120}}(\log X)^{\frac{1}{3}}$.

4 Proof via the Selberg sieve

The basic idea to be explored in this section is that quintic rings $R(v)$ with splitting types modulo a prime p forbidden by the condition $G(v) \not\simeq S_5$ have density equal to a constant in $(0,1)$; then a natural tool to use for estimating $N_5(X,G)$ for $G \not\simeq S_5$ is a "small sieve".

In a recent paper [ShTs], Shankar and Tsimerman used this idea and the Selberg sieve to prove that

$$N_5(X, S_5) = c(S_5)\, X + \mathrm{O}_\varepsilon\left(X^{\frac{199}{200}+\varepsilon}\right), \quad \forall \varepsilon > 0. \tag{12}$$

Their proof naturally shows, for each $G \in \{A_5, C_5, D_5, F_5\}$, including $G = F_5$ which was omitted in the previous section, that

$$N_5(X, G) \ll_\varepsilon X^{\frac{199}{200}+\varepsilon} \ \ \forall \varepsilon > 0, \tag{13}$$

and we recall their proof in a slightly different formulation. In the next section we show that this error term can be improved by substituting the Turán sieve for the Selberg sieve, while leaving intact the basic structure of the proof.

We recall the general statement of the Selberg sieve. Let $\mathcal{A}$ be a finite multiset of integers, $\mathcal{P}$ a set of primes, and z a parameter to be determined later. Write $P(z)$ for the product of the primes in $\mathcal{P}$ less than z, for each $p \in \mathcal{P}$ choose an arbitrary subset $\mathcal{A}_p \subseteq \mathcal{A}$, and for each $q \mid P(z)$ define $\mathcal{A}_q := \bigcap_{p|q} \mathcal{A}_p$. We assume that there exist $X > 0$ and a multiplicative function $g(q) : \mathbb{Z}^+ \to (0, 1)$ such that

$$\mathcal{A}_q = g(q)X + R_q,$$

and we write

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, z) := \#\Bigg(\mathcal{A} \backslash \bigcup_{p|P(z)} \mathcal{A}_p\Bigg). \tag{14}$$

Proposition 9 (Selberg; [CoMu, p. 119]) *With the notation above, we have*

$$S(\mathcal{A}, \mathcal{P}, z) \ll \frac{X}{V(z)} + \sum_{\substack{q_1, q_2 \le z \\ q_1, q_2 | P(z)}} |R_{[q_1, q_2]}|,$$

where

$$V(z) := \sum_{\substack{q \le z \\ q | P(z)}} \prod_{p|q} \frac{g(p)}{1 - g(p)}.$$

To apply this to our problem, choose $\mathcal{A} := \mathcal{A}(X)$ as before, let $\mathcal{P}$ be the set of odd primes, and let z be a parameter to be determined later. Define

$$\mathcal{A}_q := \{v \in \mathcal{A} : v \in T_p(1112) \text{ for all } p \mid q\},$$

so that by construction $N^{\square}(X) \le \mathcal{S}(\mathcal{A}, \mathcal{P}, z)$ for any choice of the parameter z. Each error term $R_{[q_1,q_2]}$ is $\mathrm{O}(q_1 q_2 X^{39/40})$ by Theorem 6, and for each $q \mid P(z)$ we have

$$\prod_{p|q} \frac{\delta}{1-\delta} = \prod_{p|q} \Big(\frac{\frac{1}{12} - \frac{1}{12}p^{-1}}{\frac{11}{12} + \frac{1}{12}p^{-1}} + \mathrm{O}(p^{-2}) \Big) = \prod_{p|q} \frac{1}{11} \Big(1 - \frac{12}{11}p^{-1} + \mathrm{O}(p^{-2}) \Big) \gg M(z)^{-1} \prod_{p \le z} (1 - \frac{12}{11}p^{-1}) \gg z^{-\varepsilon},$$

where $M(z)$ is the maximum of $11^{\omega(n)}$ taken over all $n \le z$. Therefore $V(z) \gg z^{1-\varepsilon}$ and

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, z) \ll \frac{X}{z^{1-\varepsilon}} + \mathrm{O}(X^{39/40} z^4),$$

and upon choosing $z = X^{1/200}$ we obtain a bound $\ll X^{199/200+\varepsilon}$.

5 Proof via the Turán sieve

In this section we shall explore a similar idea to the previous section, and instead obtain the improved bound

$$N_5(X,G) \ll X^{\frac{119}{120}} (\log X)^{\frac{2}{3}}.$$

In place of the Selberg sieve, we use a much simpler sieve emerging from Turán's normal order method:

Proposition 10 (Turán; [CoMu, p. 48]) *With the same notation and terminology introduced for the Selberg sieve, we have*

$$S(\mathcal{A},\mathcal{P},z) \leq \frac{X}{U(z)} + \frac{2}{U(z)} \sum_{p \mid P(z)} |R_p| + \frac{1}{U(z)^2} \sum_{\substack{p_1,p_2 \mid P(z) \\ p_1 \neq p_2}} |R_{p_1 p_2}|,$$

where

$$U(z) := \sum_{p \mid P(z)} g(p).$$

Note that, unlike the Selberg sieve, the Turán sieve only requires the first two steps in the inclusion-exclusion formula, and in particular does not require bounds for $|R_d|$ for general squarefree d.

We now prove that $N^{\square}(X) \ll X^{\frac{119}{120}} (\log X)^{2/3}$. We choose $\mathcal{P}$ as in our proof of the Selberg sieve, so that $U(z) \gg \frac{z}{\log z}$ and Proposition 10 implies that

$$S(\mathcal{A},\mathcal{P},z) \ll \frac{X \log z}{z} + zX^{\frac{39}{40}} + z^2 X^{\frac{39}{40}}$$

and with $z = X^{1/120} (\log X)^{1/3}$ we obtain

$$N^{\square}(X) \leq S(\mathcal{A},\mathcal{P},z) \ll X^{\frac{119}{120}} (\log X)^{\frac{2}{3}}.$$

6 Proof via the geometric sieve

In this section we exploit Lemma 4, which established that non-S_5-quintic field discriminants must be squarefull. This will lead to the full version of Theorem 1 via the Ekedahl-Bhargava *geometric sieve* described in [Bh4]. Note that this section will not depend on Theorem 6 or on any direct analogue thereof in [Bh3], although of course similar ideas are involved.

We begin with a geometric characterization of squarefull discriminants. Choose arbitrarily any of the 40 coordinates of $V_{\mathbb{Z}}$ and label it x; then, write $Y \subseteq \mathbb{A}^{40}_{\mathbb{Z}}$ for the subscheme

$$Y := \left\{ v \ : \ \mathrm{Disc}(v) = \frac{\partial \, \mathrm{Disc}}{\partial x}(v) = 0 \right\},$$

which has codimension 2 in $\mathbb{A}^{40}_{\mathbb{Z}}$.

Lemma 11 *Suppose that $v \in V_{\mathbb{Z}}$ corresponds to a maximal quintic order with $G(v) \not\simeq S_5$. Then $v \in Y(\mathbb{F}_p)$ for each prime $p \mid \mathrm{Disc}(v)$; equivalently, $v \in Y(\mathbb{Z}/q\mathbb{Z})$ for each squarefree $q \mid \mathrm{Disc}(v)$.*

Proof: If $p \mid \operatorname{Disc}(x)$, then $p^2 \mid \operatorname{Disc}(v)$ by Lemma 4. Since v corresponds to a maximal order, it follows by the arguments in [Bh4, Section 4.2] that $p^2 \mid \operatorname{Disc}(v')$ for any $v' \equiv v \pmod{p}$, i.e. that v is *strongly a multiple of* p^2. (In [Bh4, look up] this is proved by assuming that v is a weak multiple of p^2 and finding $g \in G_{\mathbb{Q}}$ with $gv \in V_{\mathbb{Z}}$ and $\operatorname{Disc}(gv) = p^{-2} \operatorname{Disc}(v)$; the quintic ring corresponding to gv will properly contain that corresponding to v, contradicting maximality.)

The result is now a special case of [Bh4, Lemma 3.6]. $\square$

The idea of the geometric sieve is that the number of pairs (v, p), where v is a lattice point in a fixed compact set B, and p is a large prime for which $v \in Y(\mathbb{F}_p)$, can be bounded using algebro-geometric methods. In adapting this idea we must count not only large primes, but also more generally large squarefree integers q; we will characterize squarefull field discriminants by the fact that they are *divisible* by large squares.

A more substantial hurdle is that there is no compact fundamental domain B for the action of $G_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$. Therefore, we will adapt a method which Bhargava applied in [Bh3] to count quintic rings by averaging over many fundamental domains. We will thus need to apply the geometric sieve, not to a fixed set B, but uniformly to a range of B. Indeed, the possibility of such an approach was suggested in Remark 4.2 of [Bh4] and we carry out the details here.

For a parameter $M = M(X) \gg X^{\frac{1}{40}}$, we write S_M for the set of all $v \in V_{\mathbb{Z}}$ of nonzero discriminant, with multiplicity equal to the number of squarefree integers $q > M$ for which $q^2 \mid \operatorname{Disc}(v)$. This multiplicity is $\ll_{\varepsilon} X^{\epsilon}$ whenever $|\operatorname{Disc}(v)| < X$, and we must incorporate this additional X^{ϵ} factor into all error terms counting such v.

By Bhargava's method, explicitly by (10) of [Bh3], we have

$$N(S_M, X) \; = \; C \int_{g \in \mathcal{F}} \#\{v \in S_M \cap gH : v \text{ irreducible}, |\operatorname{Disc}(v)| < X\} \, dg \tag{15}$$

for any fundamental domain $\mathcal{F}$ for the action of $G_{\mathbb{Z}}$ on $G_{\mathbb{R}}$ by left multiplication. Here

$$H := \{v \in V_{\mathbb{R}} : |\operatorname{Disc}(v)| \geq 1, ||v|| \leq J\}$$

for a Euclidean norm $|| \cdot ||$ fixed under the action of K (defined shortly), J is a constant chosen to be large enough such that H has positive volume, and C is a constant depending only on the choice of H.

For any quintic field K it follows from [Ser, Remark 1, p. 58] that $v_p(\operatorname{Disc}(K)) \leq 4$ for each $p \neq 5$ and $v_5(\operatorname{Disc}(K)) \leq 9$, where $v_p(\cdot)$ denotes the p-adic valuation. Therefore, by construction we have

$$N^{\square}(X) \leq N^{\square}(5^5 M^4) + N(S_M, X) \ll M^4 + N(S_M, X),$$

and so, given an appropriately small choice of M, bounds for $N^{\square}(X)$ will follow from bounds for $N(S_M, X)$.

Now, following [Bh3, p. 1567], we choose a particular fundamental domain $\mathcal{F}$ of the form

$$\mathcal{F} = \{nak\lambda \; : \; n \in N'(a), \; a \in A', \; k \in K, \; \lambda \in \Lambda\},$$

where

$$
\begin{aligned}
K &= \{\text{special orthogonal transformations in } G_{\mathbb{R}}\};\\
A' &= \{a(s_1,s_2,\ldots,s_7) : s_1,s_2,\ldots,s_7 \geq c\}, \text{ for an absolute constant } c\in(0,1), \text{ and}\\
& \quad a(s) = \left(\begin{pmatrix} s_1^{-3}s_2^{-1}s_3^{-1} &&& \\ & s_1s_2^{-1}s_3^{-1} && \\ && s_1s_2s_3^{-1} & \\ &&& s_1s_2s_3^3 \end{pmatrix}, \begin{pmatrix} s_4^{-4}s_5^{-3}s_6^{-2}s_7^{-1} &&&& \\ & s_4s_5^{-3}s_6^{-2}s_7^{-1} &&& \\ && s_4s_5^2s_6^{-2}s_7^{-1} && \\ &&& s_4s_5^2s_6^3s_7^{-1} & \\ &&&& s_4s_5^2s_6^3s_7^4 \end{pmatrix}\right);\\
\bar{N}' &= \{n(u_1,u_2,\ldots,u_{16}) : u=(u_1,u_2,\ldots,u_{16})\in\nu(a)\}, \text{ where}\\
& \quad n(u) = \left(\begin{pmatrix} 1 &&& \\ u_1 & 1 && \\ u_2 & u_3 & 1 & \\ u_4 & u_5 & u_6 & 1 \end{pmatrix}, \begin{pmatrix} 1 &&&& \\ u_7 & 1 &&& \\ u_8 & u_9 & 1 && \\ u_{10} & u_{11} & u_{12} & 1 & \\ u_{13} & u_{14} & u_{15} & u_{16} & 1 \end{pmatrix}\right);\\
\Lambda &= \{\lambda : \lambda > 0\}, \text{ where}\\
& \quad \lambda \text{ acts by } \left(\begin{pmatrix} \lambda &&& \\ & \lambda && \\ && \lambda & \\ &&& \lambda \end{pmatrix}, \begin{pmatrix} 1 &&&& \\ & 1 &&& \\ && 1 && \\ &&& 1 & \\ &&&& 1 \end{pmatrix}\right).
\end{aligned}
$$

In the above, $\nu(a)\subseteq\mathbb{R}^{16}$ is absolutely bounded and depends only on the value of $a\in A'$, and we write $N' = \cup_{a\in A'}N'(a)$.

We now write

$$(16)\quad N_{12}(S_M,X) \;=\; C\int_{g\in\mathcal{F}} \#\{v\in S_M\cap gH : v \text{ irreducible},\ a_{12}(v)\neq 0,\ |\operatorname{Disc}(v)|<X\}\,dg,$$

and by [Bh3, Lemma 11] we have

$$N(S_M,X) = N_{12}(S_M,X) + O(X^{\frac{39}{40}+\varepsilon}).$$

We will prove that $N_{12}(S_M,X) \ll X^{\frac{39}{40}+\varepsilon}$ by bounding the integrand [1]

$$(17)\qquad \#\{v\in S_M\cap n(u)a(s)\lambda kH : v \text{ irreducible},\ a_{12}(v)\neq 0,\ |\operatorname{Disc}(v)|<X\}$$

in (16), uniformly for $g\in\mathcal{F}$.

We introduce some simplifications by enlarging the set $\mathcal{F}$ to a bigger set $\mathcal{F}'\subset G_{\mathbb{R}}$. We first allow $n(u)$ to vary over N' instead of just $N'(a)$. Moreover, a simple explicit computation shows that $N'A'\subseteq c^{20}A'N'$, and we thus have $\mathcal{F}'\subseteq c^{20}\Lambda A'N'K$.

We may, as in [Bh3], restrict λ to the interval $(c', c^{-20}X^{1/40})$ for an absolute constant c'; otherwise gH will contain no points with absolute discriminant in $[1,X)$. Moreover, as in (21) of [Bh3] we may restrict A' to the set $A''(\lambda)$ of $a(s)=(s_1,\cdots,s_7)$ for which

$$(18)\qquad s_1^3s_2s_3s_4^3s_5^6s_6^4s_7^2 \leq J'\lambda,$$

[1] **Manjul:** On p. 1567 of [Bh3] you use the notation $\bar{N}'$, for which I just wrote N'. Also, you write $n(u)$ on the same page and $\bar{n}(u)$ in (10) of p. 1569; I am guessing you meant the same thing throughout and I simply wrote $n(u)$ here.

for an absolute constant J' (determined in terms of J); otherwise gH will contain only points with $a_{12} = 0$.

Therefore, a uniform upper bound for the quantity in (17) is given by any uniform bound for

$$\#\{v \in S_M \cap \lambda a' N' KH : |\operatorname{Disc}(v)| < X\}$$

uniformly in $\lambda \in (c', c^{-20}X^{1/40})$, $a' \in A''(\lambda)$. We have $KH = H$, and we replace H with the closure H' of the convex hull of $N'KH$, which is a bounded subset of $V_{\mathbb{R}}$. We will use the geometric sieve to prove, uniformly in λ and a', that

$$\#\{v \in S_M \cap \lambda a' H' : |\operatorname{Disc}(v)| < X\} \ll \lambda^{39+\varepsilon}. \tag{19}$$

Granting this for now, the integrand in (15) is $\ll \lambda^{39+\varepsilon}$. By a computation essentially identical to that of (22) of [Bh3], we obtain that the integral, and therefore $N^{\square}(X)$, is $\ll X^{\frac{39}{40}+\varepsilon}$.

It remains to prove (19). For this, we introduce the geometric sieve in the form of Theorem 3.5 of [Bh4]:

Theorem 12 *Let B be a compact region in $\mathbb{R}^n$ having finite measure, and let Y be any closed subscheme of $\mathbb{A}^n_{\mathbb{Z}}$ of codimension $k \geq 2$ such that the Zariski closure of the projection of Y onto the first $n-k+j$ coordinates has codimension j in $\mathbb{A}^{n-k+j}$ for $j = 0, \ldots, k$. Let r and M be positive real numbers, and let $t = \operatorname{diag}(t_1, \ldots, t_n)$ be a diagonal element of $\mathrm{SL}_n(\mathbb{R})$. Suppose that $\kappa > 0$ is a constant such that $rt_i \geq \kappa$ for all i and $t_i \geq \kappa$ for all $i > n-k$. Then we have*

$$\#\{a \in rtB \cap \mathbb{Z}^n \mid a \pmod{p} \in Y(\mathbb{F}_p) \text{ for some prime } p > M\} = O\left(\frac{r^n}{M^{k-1}\log M} + r^{n-k+1}\right). \tag{20}$$

We apply this theorem with $B = H'$, $n = 40$, $k = 2$, $r = \lambda$, and $t = \rho(a')$ where $\rho : \mathrm{GL}_4(\mathbb{R}) \times \mathrm{SL}_5(\mathbb{R}) \to \mathrm{GL}_{40}(\mathbb{R})$ is the representation associated to the action of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$. The conditions of the theorem are satisfied with $\kappa = \min(c^{25}, J^{-1})$.

If we wished to count pairs (v, q) with $q > M$ *prime*, we would choose any $M \in (X^{1/40}, X^{39/160})$ and obtain the desired upper bound of $\mathrm{O}(\lambda^{39/40+\varepsilon})$ in (19).

To count squarefree integers $q > M$, one modifies the proof of Theorem 12; this introduces an additional factor of $O_{\varepsilon}(X^{\varepsilon})$ into the error terms. At various points, the argument in [Bh4] uses the bound $\mathrm{O}(1)$ for the number of prime factors $> r$ of nonzero values of appropriate polynomials, or the number of roots $\pmod{p}$ when all but one of the variables are specialized to specific values (and the resulting polynomial is not identically zero $\pmod{p}$). In each case, replacing the prime p with a squarefree integer q replaces this $\mathrm{O}(1)$ with a factor $\ll_{\varepsilon} X^{\varepsilon}$, and otherwise the argument is identical.

This therefore completes the proof of Theorem 1.

7 Counting S_5-fields with a power saving error term – previous version

To do. It seems that we cannot go beyond $X^{119/120}$, unless we find some way to deal with the reducible rings.

In this section we prove Theorem 2. As mentioned earlier, our result is a quantitative improvement of a theorem of Shankar and Tsimerman [ShTs], and our proof will follow theirs.

Simultaneously, we introduce an (easy) generalization to allow local specifications. To define these, we first recall a couple of definitions from [ShTs] and [Bh2]. We write $W_d \subseteq V_{\mathbb{Z}}$ for the set of elements corresponding to quintic orders that are nonmaximal at each prime dividing d, and $U_d \subseteq V_{\mathbb{Z}}$ for be complement of W_d. By [Bh3, **to be filled in**] it is known that W_d and U_d are defined by congruence conditions modulo d^2. (**I'm not sure about this**)

By a *set of local specifications* $\mathcal{S}$ *with conductor* N, we mean the following. N will denote a squarefree integer, and for each prime $p \mid N$, we choose one or more of the sets $U_p(\sigma)$ described in Section 12 of [Bh3], where $U_p(\sigma) = U_p \cap T_p(\sigma)$ with $T_p(\sigma)$ defined as in the proof of Proposition 7. We then restrict our count to those fields which have the splitting type described by $U_p(\sigma)$. For each p, the *local density* $\widetilde{\delta}_p$ is the sum of the selected $\delta(U_p(\sigma))$, divided by the sum of all of the $\delta(U_p(\sigma))$; formulas for these $\delta(U_p(\sigma))$ are given in Lemma 20 of [Bh3]. (In [Bh3] the notation $\mu(U_p(\sigma))$ is used in place of $\delta(U_p(\sigma))$; here we have chosen to use δ to avoid a conflict with the Möbius function.) The density $\widetilde{\delta}(\mathcal{S})$ of $\mathcal{S}$ is then defined to be $\widetilde{\delta}(\mathcal{S}) := \prod_{p|N} \widetilde{\delta}_p$.

We may also allow a 'local specification at infinity', by which we mean a restriction to those S_5-fields having 0, 1, or 2 pairs of complex conjugate embeddings respectively. In this case we multiply $\widetilde{\delta}(\mathcal{S})$ by $\frac{1}{26}$, $\frac{5}{13}$, and $\frac{15}{26}$ respectively, corresponding to the relative proportions in the version of Theorem 6 stated in [Bh3].

We write $N_5(X, S_5, \mathcal{S})$ for the count of S_5-quintic fields K satisfying the local specifications described by S.

Theorem 13 *Write* $E(N) := \max(1, N\delta(\mathcal{S})^{1/2})$. *Then we have*

$$N_5(X, S_5, \mathcal{S}) = \widetilde{\delta}(\mathcal{S})c(S_5)X + \mathrm{O}(E(N)X^{\frac{79}{80}+\varepsilon}).$$

The case $\mathcal{S} = \emptyset$ and $N = 1$ is Theorem 2.

Proof: Define U'_N to be the subset of $U_N := \cap_{p|N} U_p$ corresponding to the set of local specifications $\mathcal{S}$, which is defined modulo N^2. We have, exactly following the end of [ShTs], that

$$\begin{aligned}
N(\cap_{p\nmid N} U_p \cap U'_N \cap V_{\mathbb{Z}}, X) &= \sum_{(d,N)=1} \mu(d) N(W_d \cap U'_N \cap V_{\mathbb{Z}}, X) \\
&= \sum_{\substack{d<T \\ (d,N)=1}} \Big(C\mu(d)\delta(W_d)\delta(U'_N)X + \mathrm{O}(X^{\frac{39}{40}} d^{\varepsilon} E(N)^2) \Big) + \sum_{d>T} O_{\varepsilon}(X/d^{2-\varepsilon}) \\
&= \delta(U'_N)C \sum_{(d,N)=1} \mu(d)\delta(W_d)X + O_{\varepsilon}(X/T^{1-\varepsilon} + X^{\frac{39}{40}} T^{1+\varepsilon} E(N)^2) \\
&= \delta(U'_N)C \sum_{p\nmid N} (1 - \delta(W_d))X + O_{\varepsilon}(X/T^{1-\varepsilon} + X^{\frac{39}{40}} T^{1+\varepsilon} E(N)^2).
\end{aligned}$$

Choosing $T = X^{1/80} E(N)^{-1/2}$, we obtain that there are $\widetilde{\delta}(\mathcal{S})c(S_5)X + O_{\varepsilon}(E(N)X^{\frac{79}{80}+\varepsilon})$ maximal quintic orders, satisfying the conditions described by $\mathcal{S}$, with discriminant bounded by X. (We use the fact that $\widetilde{\delta}(\mathcal{S}) \cdot \prod_{p|N} \delta(U_p) = \delta(U'_N)$.) By Theorem 1 the number of maximal quintic non-S_5 orders is $\ll X^{\frac{39}{40}+\varepsilon}$, so that the number of S_5-quintic fields K with $|\operatorname{Disc}(K)| < X$ is also $\widetilde{\delta}(S)c(S_5)X + O_{\varepsilon}(E(N)X^{\frac{79}{80}+\varepsilon})$. □

Questions for Manjul

- In (10) of [Bh3], do $n(u)$ and $\bar{n}(u)$ mean the same thing?
- We were a little bit unsure about Theorem 6. The proof looks like it counts reducible rings also, and excludes those v with $a_{12} = 0$. This is the version applied in Arul and Jacob's paper. Are they equivalent, or are both indepently true? It looks like one implies the other if $\delta(S) \gg m^{-1}$ (which is the case for all $\delta(S)$ we consider here, and this condition is incorporated implicitly into the definition of $E(N)$ of Theorem 13) – what if $\delta(S) < m^{-1}$?

  The formulation given here is the one given in your paper (i.e. excluding reducible rings, and allowing $a_{12} = 0$). This seems to be the easiest formulation, and indeed it seems like Arul and Jacob could have simplified their proof by using this version instead. Is everything along these lines correct?

Acknowledgments

(to write properly) Robert Lemke Oliver, Akshay Venkatesh, Melanie Matchett Wood, ...

References

[Bh1] M. Bhargava, *Higher composition laws III: The parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), no. 3, 1329–1360.

[Bh2] M. Bhargava, *Higher composition laws IV: The parametrization of quintic rings,* Ann. of Math. (2) **167** (2008), no. 1, 53–94.

[Bh3] M. Bhargava, *The density of discriminants of quintic rings and fields,* Ann. of Math. (2) **72** (2010), no. 3, 1559–1591.

[Bh4] M. Bhargava, *The geometric sieve and the density of squarefree values of invariant polynomials,* preprint, `http://arxiv.org/abs/1402.0031`.

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

[ChKi] P. Cho and H. Kim, *Low lying zeros of Artin L-functions*, Math. Z. **279** (2015), no. 3-4, 669–688.

[ChKi2] P. Cho and H. Kim, *Central limit theorem for Artin L-functions*, preprint, 2014.

[CoDiOl1] H. Cohen, F. Diaz y Diaz, and M. Olivier, *On the density of discriminants of cyclic extensions of prime degree*, J. reine angew. Math. **550** (2002), 169–209.

[CoDiOl2] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Counting discriminants of number fields*, J. Théor. Nombres Bordeaux **18** (2006), 573–593.

[CoMu] A.C. Cojocaru and M.R. Murty, *An introduction to sieve methods and their applications,* London Mathematical Society Student Texts **66**, Cambridge University Press (2006).

[Co] D. Cox, *Galois theory*, second edition, Wiley, Hoboken, NJ (2012).

[DeSe] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530 (1975).

[DuFo] D. Dummit and R. Foote, *Abstract algebra*, third edition, Wiley, Hoboken, NJ (2004).

[Du] E. Dummit, *Counting Number Field Extensions of Given Degree, Bounded Discriminant, and Specified Galois Closure*, Ph.D. thesis, University of Wisconsin, 2014. (Currently available at `http://www.math.rochester.edu/people/faculty/edummit/papers/thesis-whole_aug8.pdf`.)

[ElVe] J. Ellenberg and A. Venkatesh, *The number of extensions of a number field with fixed degree and bounded discriminant*, Ann. of Math. **163** (2), 723–741 (2006).

[FrTa] A. Fröhlich and M. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics **27**, Cambridge University Press (1993).

[HB] D. R. Heath-Brown, *The square sieve and consecutive square-free numbers*, Math. Ann. **266** (1984), no. 3, 251–259.

[Kl] J. Klüners, *Asymptotics of number fields and the Cohen-Lenstra heuristics*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 607–615.

[LOTh] R. Lemke Oliver and F. Thorne, *The number of ramified primes in number fields of small degree*, preprint, `http://arxiv.org/abs/1408.1018`.

[Ma] G. Malle, *On the distribution of Galois groups II,* Experiment. Math. **13** (2004), 129–135.

[MaPo] G. Martin and P. Pollack, *The average least character non-residue and further variations on a theme of Erdős*, J. Lond. Math. Soc. (2), **87** (2013), no. 1, 22–42.

[Ro] D. Rohrlich, *Self-dual Artin representations,* Automorphic representations and L-functions, 455–499, Tata Inst. Fundam. Res. Stud. Math. **22**, Tata Inst. Fund. Res., Mumbai, 2013.

[Sel] A. Selberg, *On an elementary method in the theory of primes,* Norske Vid. Selsk. Forh., Trondhjem **19** (1947), no. 18, 64–67.

[Ser] J.-P. Serre, *Local fields,* Springer, New York, 1979.

[ShTs] A. Shankar and J. Tsimerman, *Counting S_5-fields with a power saving error term,* Forum Math. Sigma **2** (2014), e13, 8 pp.

[Tu] P. Turán, ...

[Wo] S. Wong, *Densities of quartic fields with even Galois groups*, Proc. Amer. Math. Soc. **133** (2005), no. 10, 2873–2881.

[WrYu] D. J. Wright and A. Yukie, *Prehomogeneous vector spaces and field extensions,* Invent. Math. **110** (1992), 283–314.

[Ya] A. Yang, *Distribution problems associated to zeta functions and invariant theory,* Ph.D. thesis, Princeton University, 2009.

Bhargava: Department of Mathematics, Princeton University, Princeton, NJ 08544
E-mail address: bhargava@math.princeton.edu

Cojocaru: Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA;
Institute of Mathematics "Simion Stoilow" of the Romanian Academy, 21 Calea Grivitei St, Bucharest, 010702, Sector 1, Romania
E-mail address, A.C. Cojocaru: cojocaru@uic.edu

Thorne: Department of Mathematics, University of South Carolina, Columbia, SC 29208
E-mail address: thorne@math.sc.edu