Pacific Journal of Mathematics

UPPER BOUNDS OF ROOT DISCRIMINANT LOWER BOUNDS

SIMAN WONG

Volume 277 No. 1 September 2015

PACIFIC JOURNAL OF MATHEMATICS
Vol. 277, No. 1, 2015
dx.doi.org/10.2140/pjm.2015.277.241

UPPER BOUNDS OF ROOT DISCRIMINANT LOWER BOUNDS

SIMAN WONG

For any rational number $t \in [0, 1]$, define the logarithmic Martinet function $\beta(t)$ to be the liminf of the logarithm of the root discriminant of number fields K with $r_1(K)/[K:\mathbb{Q}] = t$ as $[K:\mathbb{Q}]$ goes to infinity. Under the generalized Riemann hypothesis for Dedekind zeta functions of number fields, we show that $\beta(t) < 14.55$ for a dense subset of rational numbers $t \in [0, 1]$. We also study unconditional estimates of the growth of root discriminants by studying how the polynomial discriminant behaves under perturbation of coefficients, and by using Pisot numbers.

1. Introduction

Let K be a number field of degree n_K and absolute discriminant d_K. Denote by $r_1(K)$ and $r_2(K)$ the number of real and complex conjugate pairs of embeddings of K, and by $rd_K := |d_K|^{1/n_K}$ the *root discriminant* of K. By analyzing the explicit formula for the Dedekind zeta function $\zeta_K(s)$ of K, Stark [1974] shows that[1] as $n_K \to \infty$,

$$\log(rd_K) \geq \frac{r_1(K)}{n_K} \log(4\pi e^C) + \frac{2r_2(K)}{n_K} \log(2\pi e^C) + o(1), \tag{1}$$

where C is the Euler constant. Note that $rd_L = rd_K$ if L/K is a finite extension unramified at all finite places. This suggests that root discriminant lower bounds can be used to study ideal class groups and, more generally, numbers fields and Galois representations with restricted ramifications; see [Fontaine 1985; Masley 1978; Tate 1994] for a sample of the wide range of applications of root discriminant lower bounds.

In view of such applications, there are extensive works on sharpening root discriminant lower bounds. Let $I_\mathbb{Q} = \mathbb{Q} \cap [0, 1]$. Inspired by [Hajir and Maire 2001] and [Martinet 1978], to help us focus on the asymptotic nature of (1) we define the *logarithmic Martinet function* $\beta : I_\mathbb{Q} \to \mathbb{R}_{>0} \cup \{\infty\}$ as follows. For $t \in I_\mathbb{Q}$, let $R_{n,t}$

Siman Wong's work is supported in part by NSF grant DMS-0901506.
MSC2010: primary 11R29; secondary 11R37, 11R21.
Keywords: Chebotarev density theorem, class field towers, Pisot numbers, root discriminants.

[1] The asymptotic constants in this paper depend only on those quantities (if any) adorning the corresponding $\ll$ sign.

be the minimal root discriminant for number fields of degree n and with r_1 real embeddings such that $r_1/n = t$. Then

$$\beta(t) := \liminf_{n\to\infty} R_{n,t}.$$

Note that $\beta(t)$ is finite[2] for any $t \in I_{\mathbb{Q}}$: first, find a number field $K_t/\mathbb{Q}$ with $r_1(K)/n_K = t$ (see for example the proof of Theorem 1.2 below for an explicit construction). Next, let $L_1 \subset L_2 \subset \cdots$ be a totally real class field tower. Then the compositums $L_i K_t$ have bounded root discriminants and satisfy $r_1(L_i K_t)/n_{L_i K_t} = t$. We also know that $\beta(t) > 0$ for all $t \in I_{\mathbb{Q}}$; this follows from

$$\beta(t) \geq t \log(4\pi e^C) + (1-t)\log(2\pi e^C) = t \log 2 + \log(2\pi e^C),$$

which is a restatement of (1). By using a smooth form of the explicit formula and with a careful choice of kernel, this lower bound has since been improved to

$$\beta(t) \geq t \log(4\pi e^{1+C}) + (1-t)\log(4\pi e^C) = t + \log(4\pi e^C),$$

and the two constants are optimal within the framework of the explicit formula and without additional inputs about the zeros of $\zeta_K(s)$ and prime ideals of the number fields. Assuming the generalized Riemann hypothesis (GRH) for $\zeta_K(s)$, the optimal conditional lower bound from the explicit formula approach is

$$\beta(t) \geq t \log(8\pi e^{C+\pi/2}) + (1-t)\log(8\pi e^C) = \tfrac{\pi}{2} t + \log(8\pi e^C). \tag{2}$$

See [Odlyzko 1990] for a survey of the literature. Aside from this finiteness result and the aforementioned lower bounds, little is known about this function β. For example, it is not known if β is bounded on $I_{\mathbb{Q}}$ (the finiteness result for $\beta(t)$ sketched earlier depends on K_t). Hajir and Maire [2001] raise a number of interesting (and, as these authors put it, probably very difficult) questions:

- Does β extend to a continuous function on [0, 1] (which would imply that β is bounded on $I_{\mathbb{Q}}$)?
- Is β monotonically increasing?
- Is there a root discriminant lower bound of the form
$$\log(rd_K) \geq \frac{r_1(K)}{n_K}\beta(1) + \frac{2r_2(K)}{n_K}\beta(0) + o(1)?$$
- Very optimistically, is it true that $\beta(t)$ is a linear function in t and, even more boldly, do we have $\beta(t) = t\beta(1) + (1-t)\beta(0)$?

By constructing explicit Hilbert class field towers, Martinet [1978] shows that $\beta(0) < 4.53$ and $\beta(1) < 6.97$, and Hajir and Maire [2002] refine this method to

[2] We thank Professor Hajir for showing us this argument.

give $\beta(0) < 4.41$ and $\beta(1) < 6.87$; Martin [2006] has made further improvement on $\beta(t)$ for $t \in \{\frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{3}{5}, \frac{5}{7}, 1\}$. As a comparison, note that, by (2), under GRH we have $\beta(0) \geq 3.80$ and $\beta(1) \geq 5.37$. In this paper we give a conditional proof that $\beta(t)$ is bounded by an explicit universal constant for a dense subset of $t \in I_{\mathbb{Q}}$.

Theorem 1.1. *Assume the generalized Riemann hypothesis for the Dedekind zeta functions of number fields. Fix a fraction* $a/(3^b m) \in I_{\mathbb{Q}}$ *with* $a, b, m > 0$ *and* $3 \nmid m$ *(we allow* $3 \mid a$*). Then there exist an infinite sequence of Galois extensions* $K_1 \subsetneq K_2 \subsetneq \cdots$ *such that* $r_1(K_i)/n_{K_i} = a/(3^b m)$ *for all* i*, and such that* $\log(rd_{K_i})$ *is at most*

$$19.59316 + \tfrac{m-1}{m}(2\log m + 2\log\log m + 6.813445) + O\Big(\tfrac{\log n_{K_i} + \log m}{m \cdot n_{K_i}}\Big).$$

Corollary. Assume the generalized Riemann hypothesis for the Dedekind zeta functions of number fields. Then for any fraction $a/(3^b m) \in I_{\mathbb{Q}}$ with $a, b, m > 0$ and $3 \nmid m$ (we allow $3 \mid a$), we have

$$\beta\Big(\tfrac{a}{3^b m}\Big) \leq 19.59316 + \tfrac{m-1}{m}(2\log m + 2\log\log m + 6.813445). \qquad \square$$

A natural way to construct number fields with a prescribed ratio $r_1(K)/n_K$ is to take the square root of a totally real algebraic integer with the appropriate number of positive embeddings. To bound the root discriminant of the field generated by such a square root, we need to keep the absolute norm of this element small. We achieve that by applying the GRH form of the effective Chebotarev density theorem to the narrow class field of an explicit infinite 3-class field tower of a real quadratic field. This produces infinitely many fields for which $r_1(K)/n_K$ take on a fixed rational value with 3-power denominator; to handle ratios with general denominators m we compose the extensions constructed above with a totally real Galois extension of degree m. Because of this last step[3] we are not able to show that $\beta(t)$ is uniformly bounded on $I_{\mathbb{Q}}$ (which would have to be the case *if* β does extend to a continuous function on [0, 1]). Since fractions with 3-power denominators are dense in $I_{\mathbb{Q}}$, Theorem 1.1 does show that $\beta(t)$ is informally bounded on a dense subset of $I_{\mathbb{Q}}$.

Remark. Our proof of Theorem 1.1 readily generalizes to function fields (for which the GRH is true unconditionally).

We do not know how to prove unconditionally that $\beta(t)$ is bounded by a universal constant for all $t \in I_{\mathbb{Q}}$. If we replace in the proof of Theorem 1.1 the conditional

[3]We thank Professor Hajir for suggesting this compositum construction. We can also directly construct totally real infinite m-class field tower using the Golod–Shafarevich construction [Roquette 1967]. This results in an upper bound $\beta(a/m) \leq c_1 \log m + c_2$ for some absolute constants c_i, just like Theorem 1.1, but these constants would be weaker than those in Theorem 1.1.

effective Chebotarev density theorem with the unconditional one, our argument only gives

$$\log(rd_{K_i}) \ll (c^{n_{K_i}})/n_{K_i} \tag{3}$$

for some absolute constant $c > 0$. We have the following unconditional improvement.

Theorem 1.2. *There exists an absolute constant $c > 0$ such that for any $t \in I_{\mathbb{Q}}$, there exist infinitely many number fields K_i (depending on t) of unbounded degree such that $r_1(K_i)/n_{K_i} = t$ and $\log(rd_{K_i}) \le cn_{K_i} \log(n_{K_i})$.*

To prove this unconditional result, we start with a polynomial $f(x)$ that splits completely over $\mathbb{Z}$. We can easily estimate the discriminant of f, and by prescribing the signs of the roots of f appropriately we can guarantee that the ratio of the number of real roots of $f(x^2)$ to the degree of $f(x^2)$ takes on any given value in $I_{\mathbb{Q}}$. To achieve irreducibility we perturb the constant term and study its effect on the discriminant and signature.

Remark. The proof of Theorems 1.1 and 1.2 come down to finding in a totally real number field algebraic integers of small absolute norm and with a prescribed number of positive embeddings. If we try to tackle this problem using Minkowski's convex body theorem, the obvious construction leads to an estimate comparable to the unconditional Chebotarev estimate (3). It would be interesting to find a geometry of numbers proof of the two theorems here.

Remark. The constants in Theorem 1.1 can be improved, but not anywhere near the records of Martinet and Hajir–Maire; to streamline the exposition we forgo such refinements. In a similar vein we leave out explicit value for the constant in Theorem 1.2.

In connection with their study on arithmetic lattices in simple Lie groups of bounded covolume, Belolipetsky and Lubotzky [2012] use Pisot numbers to construct an infinite sequence of number fields of unbounded degree with a fixed number of complex places and bounded root discriminant. On the other hand, computational data suggest that number fields with a large number of complex places tend to have large class numbers, and hence (at least heuristically) large root discriminant. The following result is the first step towards affirming this circle of ideas (and the only result we know of in this direction).

Theorem 1.3. *There exists an infinite sequence of number fields T_ℓ with $n_{T_\ell} = \ell + 1$ and $r_1(T_\ell) \in \{1, 2\}$, such that $\log(rd_{T_\ell}) \le \log(\ell + 1) + \log 3/(\ell + 1)$.*

2. Conditional estimate

For any number field $L \neq \mathbb{Q}$, denote by h_L, R_L, w_L and $\mathcal{O}_L$ its class number, regulator, number of roots of unity in K, and the ring of integers of K.

Lemma 2.1. *For any number field L with $n_L \geq 36$, we have the estimate*

$$h_L \leq 4|d_L|^{\frac{1}{2}\left(1.710172+\frac{1.292958}{\log(|d_L|^{1/2})}\right)}.$$

Proof. We prove this by finding explicit numerical values for the constants in the argument in [Lang 1986, p. 322], which is a preliminary step in the proof of the Brauer–Siegel theorem. Before we proceed with the elementary but somewhat tedious computation, we will briefly explain the idea behind the proof of the lemma.

The Brauer–Siegel theorem gives an asymptotic estimate for

$$\frac{\log(h_L R_L)}{\log(|d_L|^{1/2})}$$

as we run through an infinite sequence of number fields L with $n_L/\log|d_L| \to 0$. More precisely, the crucial exponent $\frac{1}{2}$ shows up in the main term of the asymptotic estimate, and $n_L/\log|d_L|$ appears in the error term. But if we are willing to weaken the main term of Brauer–Siegel, we can actually make this $n_L/\log|d_L|$ term go away (there are additional error terms).

We now resume the proof of the lemma. The residue at $s=1$ of $\zeta_L(s)$ is equal to

$$\kappa(L) = 2^{r_1(L)}(2\pi)^{r_2(L)} h_L R_L/(w_L|d_L|^{1/2}).$$

Take the logarithm of both sides, recall that $|d_L| > 1$ if $L \neq \mathbb{Q}$ and we get

$$\frac{\log(h_L R_L)}{\log(|d_L|^{1/2})} = \frac{\log(\kappa(L)) - r_1(L)\log 2 - r_2(L)\log(2\pi) + \log(w_L)}{\log(|d_L|^{1/2})} + 1. \tag{4}$$

Next, combining the functional equation of $\zeta_L(s)$ with the positivity of the integral representation of $\zeta_L(s)$ for real $s > 1$, we find that (see [Lang 1986, Lemma XVI.1])

$$(2^{-2r_2(L)}\pi^{-n_L}\cdot|d_L|)^{s/2}\Gamma\left(\tfrac{s}{2}\right)^{r_1(L)}\Gamma(s)^{r_2(L)}\cdot\zeta_L(s)\cdot s(s-1) \geq \kappa(L)|d_L|^{1/2}(2\pi)^{-r_2(L)},$$

so

$$\begin{aligned}\kappa(L) &\leq 2^{-r_2(L)s}\pi^{-n_L s/2}(2\pi)^{r_2(L)}|d_L|^{(s-1)/2}\Gamma\left(\tfrac{s}{2}\right)^{r_1(L)}\Gamma(s)^{r_2(L)}\zeta_L(s)\cdot s(s-1)\\ &\leq 2^{r_2(L)(1-s)}\pi^{r_2(L)-n_L s/2}|d_L|^{(s-1)/2}\Gamma\left(\tfrac{s}{2}\right)^{r_1(L)}\Gamma(s)^{r_2(L)}\zeta_{\mathbb{Q}}(s)^{n_L}\cdot s(s-1).\end{aligned}$$

Set $s = 1 + 1/\alpha$ with $\alpha > 0$. Then

$$\zeta_L\left(1+\tfrac{1}{\alpha}\right) \leq \zeta_{\mathbb{Q}}\left(1+\tfrac{1}{\alpha}\right)^{n_L} = \left(1+\sum_{m=2}^{\infty}\frac{1}{m^{1+\frac{1}{\alpha}}}\right)^{n_L} \leq \left(1+\int_1^{\infty}\frac{dt}{t^{1+\frac{1}{\alpha}}}\right)^{n_L} = (1+\alpha)^{n_L}.$$

Thus

$$\begin{aligned}
&\log(\kappa(L))\\
&\quad\le -\frac{r_2(L)}{\alpha}\log 2+\bigl(r_2(L)-\tfrac{1}{2}n_L\bigl(1+\tfrac{1}{\alpha}\bigr)\bigr)\log\pi+r_1(L)\log\Gamma\bigl(\tfrac{1}{2}+\tfrac{1}{2\alpha}\bigr)\\
&\qquad +r_2(L)\log\Gamma\bigl(1+\tfrac{1}{\alpha}\bigr)+\tfrac{1}{\alpha}\log|d_L^{1/2}|+n_L\log(1+\alpha)+\log\bigl(1+\tfrac{1}{\alpha}\bigr)-\log\alpha\\
&\quad = r_2(L)\bigl(\log\Gamma\bigl(1+\tfrac{1}{\alpha}\bigr)+\log\pi-\tfrac{\log 2}{\alpha}\bigr)+n_L\bigl(\log(1+\alpha)-\tfrac{\log\pi}{2}\bigl(1+\tfrac{1}{\alpha}\bigr)\bigr)\\
&\qquad +r_1(L)\log\Gamma\bigl(\tfrac{1}{2}+\tfrac{1}{2\alpha}\bigr)+\tfrac{1}{\alpha}\log|d_L^{1/2}|+\log\bigl(1+\tfrac{1}{\alpha}\bigr)-\log\alpha.
\end{aligned}$$

Substitute this into the right side of (4) and we get that

$$\begin{aligned}
\frac{\log(h_L R_L)}{\log(|d_L|^{1/2})}\le 1+\tfrac{1}{\alpha}+\frac{1}{\log(|d_L|^{1/2})}&\Bigl(r_2(L)\bigl(\log\Gamma\bigl(1+\tfrac{1}{\alpha}\bigr)-\bigl(1+\tfrac{1}{\alpha}\bigr)\log 2\bigr)\\
&+n_L\bigl(\log(1+\alpha)-\tfrac{\log\pi}{2}\bigl(1+\tfrac{1}{\alpha}\bigr)\bigr)+r_1(L)\bigl(\log\Gamma\bigl(\tfrac{1}{2}+\tfrac{1}{2\alpha}\bigr)-\log 2\bigr)\\
&+\log\bigl(1+\tfrac{1}{\alpha}\bigr)-\log\alpha+\log w_L\Bigr).
\end{aligned}$$

We check that if $\alpha>\alpha_0:=0.23048745595$ then the coefficients of the $r_1(L)$ term and the $r_2(L)$ term above are both negative. Thus for $\alpha>\alpha_0$,

$$\frac{\log(h_L R_L)}{\log(|d_L|^{1/2})}\le 1+\tfrac{1}{\alpha}+\frac{n_L\bigl(\log(1+\alpha)-\tfrac{\log\pi}{2}\bigl(1+\tfrac{1}{\alpha}\bigr)\bigr)+\log\bigl(1+\tfrac{1}{\alpha}\bigr)-\log\alpha+\log w_L}{\log(|d_L|^{1/2})}.$$

The roots of unity in K form a cyclic group, so w_L is the largest positive integer w for which K contains a primitive w-root of unity. Thus n_L is divisible by

$$w_L\prod_{p\mid w_L}\frac{p-1}{p}\ge\frac{w_L}{2}\prod_{\substack{p\mid w_L\\ p>2}}\frac{2}{3}\ge\frac{w_L}{2}\Bigl(\frac{2}{3}\Bigr)^{\frac{\log w_L}{\log 3}}=\frac{1}{2}w_L^{\frac{\log 2}{\log 3}}.$$

Thus $w_L\le(2n_L)^{\log 3/\log 2}\le 3{n_L}^{1.6}$, whence $\log w_L\le 1.6\log n_L+\log 3$. We check that $0.1x>\log x$ for $x\ge 36$, so for $n_L\ge 36$ and $\alpha>\alpha_0$,

$$\frac{\log(h_L R_L)}{\log(|d_L|^{1/2})}\le 1+\tfrac{1}{\alpha}+\frac{n_L\bigl(\log(1+\alpha)+0.1-\tfrac{\log\pi}{2}\bigl(1+\tfrac{1}{\alpha}\bigr)\bigr)+\log\bigl(1+\tfrac{1}{\alpha}\bigr)-\log\alpha+\log 3}{\log(|d_L|^{1/2})}.$$

We check that $\log(1+\alpha)+0.1-(\log\pi/2)\bigl(1+\frac{1}{\alpha}\bigr)$ vanishes at $\alpha_1 := 1.408110244096$. Set $\alpha = \alpha_1$ and we get

(5)
$$\frac{\log(h_L R_L)}{\log(|d_L|^{1/2})} \le 1+\tfrac{1}{\alpha_1}+\frac{\log\bigl(1+\frac{1}{\alpha_1}\bigr)-\log\alpha_1+\log 3}{\log(|d_L|^{1/2})} = 1.710172+\frac{1.292958}{\log(|d_L|^{1/2})}.$$

Friedman [1989, Theorem B] shows that $R_L > \frac{1}{4}$ for all $L \ne \mathbb{Q}$ except for the following three totally complex sextic fields:

L	d_L	R_L	h_L	w_L
$x^6-x^5+2x^4-2x^3+2x^2-2x+1$	-10051	0.20521	1	2
$x^6-x^5-x^4+2x^3-x+1$	-10571	0.21320	1	2
$x^6-3x^5+5x^4-5x^3+5x^2-3x+1$	-12671	0.23722	1	2

Set $R_L > \frac{1}{4}$ and we get, except possibly for these three fields,

(6)
$$\log(\tfrac{1}{4}h_L) < \log(|d_L|^{1/2})\biggl(1.710172+\frac{1.292958}{\log(|d_L|^{1/2})}\biggr).$$

Exponentiate both sides and we get

$$h_L \le 4|d_L|^{\frac{1}{2}\left(1.710172+\frac{1.292958}{\log(|d_L|^{1/2})}\right)},$$

which is the estimate in the lemma. And since $h_L = 1$ for these three fields, this estimate is applicable as well. □

Lemma 2.2. *Assume the generalized Riemann hypothesis for the Dedekind zeta functions of number fields. Then for any totally real number field L of degree $m \ge 18$ and for any integer $0 \le m' \le m$, there exists a quadratic extension $L_{m'}/L$ with signature $(r_1, r_2) = (2m-2m', m')$ and*

$$\log(rd_{L_{m'}}) \le 1.855086\log(rd_L)+3.372400+\frac{\log\log|d_L|+\log 280}{n_L}.$$

Proof. Denote by $C_{L,n}$ the narrow ray class group of L (of modulus $\mathcal{O}_L$), and by $H_{L,n}$ the corresponding narrow ray class field of L. Denote by $\mathcal{O}_L^\times$ the group of units of $\mathcal{O}_L$ and by $\mathcal{O}_{L,+}^\times$ the subgroup of totally positive units. Then

$$\begin{aligned}\#C_{L,n} &= h_L\cdot 2^{[L:\mathbb{Q}]}/[\mathcal{O}_L^\times : \mathcal{O}_{L,+}^\times] \qquad \text{by [Lang 1986, Theorem VI.2]}\\ &\le h_L\cdot 2^{[L:\mathbb{Q}]}.\end{aligned}$$

Since $H_{L,n}/L$ is unramified at all finite places,

(7)
$$|d_{H_{L,n}}| = |d_L|^{[H_{L,n}:L]} \le |d_L|^{h_L\cdot 2^{[L:\mathbb{Q}]}}.$$

Denote by $\phi_1, \ldots, \phi_m$ the distinct real embeddings of L. Apply the GRH form of the effective Chebotarev density theorem ([Lagarias and Odlyzko 1977, Corollary 1.2]; see [Oesterlé 1979, Theorem 4] for a version with explicit constants) to the Galois extension $H_{L,n}/L$ and we see that for any integer $0 \le m' \le m$, there exists a prime ideal $\mathfrak{p}_{m'} \subset \mathcal{O}_L$ such that

(i) $\mathrm{Norm}_{L/\mathbb{Q}}(\mathfrak{p}_{m'}) \le 70(\log |d_{H_{L,n}}|)^2$, and

(ii) $\mathfrak{p}_{m'}$ is principal and is generated by an element $\pi_{m'} \in \mathcal{O}_L$ with $\phi_i(\pi_{m'}) > 0$ if and only if $i \le m'$.

The sign conditions mean that $L_{m'} := L(\sqrt{\pi_{m'}})$ has exactly $2m'$ real embeddings. Since $\pi_{m'}$ is a uniformizer, $L_{m'}/L$ is a quadratic extension unramified outside $\mathfrak{p}_{m'}$ and 2. Let $\mathfrak{Q} \subset \mathcal{O}_{L_{m'}}$ be a prime lying above 2 that *ramifies* in $L_{m'}/L$. By [Serre 1979, Remark 1 on p. 58], the exponent of $\mathfrak{Q}$ in the different ideal of $L_{m'}/L$ is at most $1 + \mathrm{ord}_{\mathfrak{Q}}(2)$. Consequently, $\mathrm{Disc}(L_{m'}/L)$ divides $\mathfrak{p}_{m'} \prod_{\mathfrak{q}|2} \mathfrak{q}^{1+\mathrm{ord}_{\mathfrak{q}}(2)} = \mathfrak{p}_{m'} \prod_{\mathfrak{q}|2} \mathfrak{q} \cdot 2\mathcal{O}_L$, so in particular

$$\mathrm{Disc}(L_{m'}/L) \quad \text{divides} \quad \mathfrak{p}_{m'} \cdot 2^2 \mathcal{O}_L. \tag{8}$$

Thus

$$\begin{aligned} |d_{L_{m'}}| &= \mathrm{Norm}_{L/\mathbb{Q}}(\mathrm{Disc}(L_{m'}/L)) \cdot |d_L|^{[L_{m'}:L]} \\ &\le \mathrm{Norm}_{L/\mathbb{Q}}(\mathfrak{p}_{m'} \cdot 2^2 \mathcal{O}_L) \cdot d_L^2 && \text{by (8)} \\ &\le \left[70 \cdot h_L \cdot 2^{n_L} \log |d_L| \cdot 2^{2n_L}\right]^2 \cdot d_L^2 && \text{by (7).} \end{aligned}$$

Since $n_{L_{m'}} = 2n_L$, the logarithm of the root discriminant of $L_{m'}$ is bounded by

$$\log(rd_{L_{m'}}) \le \frac{\log 70}{n_L} + \frac{\log h_L}{n_L} + \log 2 + \frac{\log\log |d_L|}{n_L} + \log 4 + \log(rd_L).$$

Since $n_{L_{m'}} \ge 36$, apply Lemma 2.1 and we get

$$\begin{aligned} \log(rd_{L_{m'}}) \le \frac{\log |d_L|}{2n_L}\left(1.710172 + \frac{1.292958}{\log(|d_L|^{1/2})}\right) + \frac{\log 4}{n_L} \\ + \frac{\log 70}{n_L} + \log 2 + \frac{\log\log |d_L|}{n_L} + \log 4 + \log(rd_L) \\ \le 1.855086 \log(rd_L) + 3.372400 + \frac{\log\log |d_L| + \log 280}{n_L}. \end{aligned}$$
□

Remark. The proof of the lemma (and its subsequent application) does not require that the element $\pi_{m'}$ be a generator of a prime ideal; it is enough that it is not a square, has small norm, and has the prescribed number of positive embeddings. Thus the use of the conditional effective Chebotarev density theorem is an overkill; instead we could apply the GRH form of the Perron formula to the Hecke L-series of the narrow class group $C_{L,n}$ and sieve out the desired positivity conditions using orthogonality relations. But this alternative argument still requires the GRH and would lengthen the proof, so we opt for a streamlined approach via the conditional effective Chebotarev density theorem.

Proof of Theorem 1.1. Schmithals [1980] shows that the elementary 3-class group of the real quadratic field $k = \mathbb{Q}(\sqrt{3321607})$ has rank 3. Combining this with refinement of earlier work of Koch and Venkov [1975] and Schoof [1986] shows that k has an infinite 3-class field tower. Set $K_0 := k$ and denote by K_{i+1} the 3-Hilbert class field of K_i, all viewed as subfields of a fixed algebraic closure of $\mathbb{Q}$. Since K_0 is totally real and every $[K_{i+1} : K_i]$ is odd, that means every K_i is totally real.

Since K_i/k is unramified for all $i \geq 1$, we have

(9)
$$rd_{K_i} = rd_k = \sqrt{39345017}, \qquad \frac{\log\log |d_{K_i}|}{n_{K_i}} = \frac{\log(n_{K_i}/2)}{n_{K_i}} + \frac{\log\log\sqrt{39345017}}{n_{K_i}}.$$

Fix $i \geq 18$; then for any integer $0 \leq m' \leq n_{K_i}$, Lemma 2.2 furnishes an extension $K_{i,m'}/\mathbb{Q}$ of degree $2n_{K_i}$ with signature $(2n_{K_i} - 2m', m')$ and

(10)
$$\begin{aligned}\log(rd_{K_{i,m'}}) &\leq 1.855086\log(rd_k) + 3.372400 + O\Big(\frac{\log n_{K_i}}{n_{K_i}}\Big)\\ &= 19.593159 + O\Big(\frac{\log n_{K_i}}{n_{K_i}}\Big).\end{aligned}$$

We now consider the $m = 1$ case of the theorem, so fix $t = a/3^b \in I_{\mathbb{Q}}$ with $b > 0$ and $0 \leq a \leq 3^b$ (we allow $3 \mid a$). Since the K_i are 3-class field towers of k, for i sufficiently large we have $3^b \mid n_{K_i}$, so for such i we can choose $0 \leq m' \leq [K_i : \mathbb{Q}]$ so that $2m'/n_{K_{i,m'}} = m'/n_{K_i} = t$. Apply (10) and we are done.

Now, let $m > 1$ be coprime to 3. Then $\phi(6m) = 2\phi(2m) < 2m$, so by [Washington 1982, Proposition 2.7],

$$|d_{\mathbb{Q}(\zeta_{6m})}| \leq \frac{(6m)^{\phi(6m)}}{2^{\phi(6m)}3^{\phi(6m)/2}} = m^{\phi(6m)}3^{\phi(6m)/2} < m^{2m}3^m = (\sqrt{3}m)^{2m}.$$

The GRH form of the effective Chebotarev density theorem then furnishes a prime $p \equiv 1 \pmod{6m}$ with

$$\begin{aligned}p &\leq 70(\log |d_{\mathbb{Q}(\zeta_{6m})}|)^2\\ &< 70\big(\log(\sqrt{3}m)^{2m}\big)^2\\ &\leq 70 \cdot 4m^2(\log m + \log\sqrt{3})^2\end{aligned}$$

which is to say (since $m \geq 2$)

(11)
$$p < 70 \cdot 13m^2 \log^2 m.$$

Denote by M_m the unique degree m subfield of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. The conductor-discriminant formula gives $|d_{M_m}| \le p^{m-1}$, so by (11),

$$\log|d_{M_m}| \le (m-1)(2\log m + 2\log\log m + \log(70\cdot 13)). \tag{12}$$

The only finite prime that ramifies in $K_i/\mathbb{Q}$ (resp. $M_m/\mathbb{Q}$) is $39345017 \equiv 2 \pmod 3$ (resp. $p \equiv 1 \pmod 3$), so K_i and M_m are linearly disjoint over $\mathbb{Q}$. It follows that

$$[K_iM_m : \mathbb{Q}] = m\cdot n_{K_i} \quad \text{and} \quad |d_{K_iM_m}| = |d_{K_i}|^m |d_{M_m}|^{n_{K_i}}.$$

Thus

$$\log|d_{K_iM_m}| = m\log|d_{K_i}| + n_{K_i}\log|d_{M_m}|, \tag{13}$$

whence, by (9) and (12),

$$\begin{aligned}\log(rd_{K_iM_m}) &= \log(rd_{K_i}) + \log(rd_{M_m})\\ &\le 8.743940 + \tfrac{m-1}{m}(2\log m + 2\log\log m + 6.813445).\end{aligned}$$

Both terms on the right side of (13) are greater than 1. Since $x+y \le xy$ if both $x, y \ge 1$, it follows from (13) that

$$\begin{aligned}\frac{\log\log|d_{K_iM_m}|}{n_{K_iM_m}} &= \frac{\log m + \log\log|d_{K_i}| + \log n_{K_i} + \log\log|d_{M_m}|}{m\cdot n_{K_i}}\\ &\le 2\frac{\log n_{K_i}}{m\cdot n_{K_i}} + O\left(\frac{\log m}{m\cdot n_{K_i}}\right), \qquad \text{by (9), (12).}\end{aligned}$$

Since $[\mathbb{Q}(\zeta_p) : M_m]$ is even, M_m is fixed by the unique order-2 element of the cyclic group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. That means M_m, and hence K_iM_m, is totally real. Apply Lemma 2.2 and we see that for any $0 \le m \le m\cdot n_{K_i}$ there exists an extension $K_{i,m'}$ with signature $(2m\cdot n_{K_i} - 2m', m')$ and

$$\begin{aligned}\log(rd_{K_{i,m'}}) \le 1.855096\big(8.743940 + \tfrac{m-1}{m}(2\log m + 2\log\log m + 6.813445)\big)\\ +3.372400 + O\left(\frac{\log n_{K_i} + \log m}{m\cdot n_{K_i}}\right),\end{aligned}$$

and Theorem 1.1 follows for general $m > 1$. □

3. Unconditional estimate

Fix an integer $n \ge 1$. For each $0 \le j \le n$, pick $\sigma_j \in \{\pm 1\}$ and define

$$f_n(x) := \prod_{i=1}^{n}(x - (2i)\sigma_i), \qquad g_n(x) := f_n(x) + 2.$$

Lemma 3.1. *For $n \geq 6$, the roots γ_i of $g_n(x)$ are all real and pairwise distinct, and up to relabeling we have $|\gamma_j - (2j)\sigma_j| < 1$ for all i. In particular, $g_n(x)$ has as many positive roots as $f_n(x)$.*

Proof. For any $1 \leq j \leq n$ we can write

$$f_n(x) = (x-(2j)\sigma_j)\prod_{i\neq j}(x-(2i)\sigma_i). \tag{14}$$

Since $|(2i)\sigma_i - (2j)\sigma_j| \geq 2|i-j|$ for all $i \neq j$, if $|x-(2j)\sigma_j| \leq 1$ then the product on the right side of (14) does not change sign and has absolute value at least $\prod_{i\neq j}(2|i-j|-1)$. This latter product is taken over $n-1$ odd integers between 1 and $2n-3$, with each odd integer appearing at most twice. So if $|x-(2j)\sigma_j| \leq 1$ and $n \geq 3$, then

$$\Big|\prod_{j\neq i}(x-(2i)\sigma_i)\Big| \geq \prod_{\ell=1}^{[\frac{n-1}{2}]}(2\ell-1)^2 \geq \Big(2\Big[\frac{n-1}{2}\Big]-1\Big)^2 \geq \Big(\frac{n-3}{2}\Big)^2.$$

To recapitulate, for $|x-(2j)\sigma_j| \leq 1$ and $n \geq 3$, the polynomial $f_n(x)$ is equal to $x-(2j)\sigma_j$ times a product that, within this closed interval, takes on a constant sign and has absolute value at least $((n-3)/2)^2$. Note that $x-(2j)\sigma_j$ takes values ∓ 1 at $(2j)\sigma_j \pm 1$. So for $n \geq 6$, one of $f_n((2j)\sigma_j \pm 1)$ is $\leq -\frac{9}{4}$ and the other is $\geq \frac{9}{4}$. Thus $g_n(x) := f_n(x)+2$ takes a negative value at exactly one of the two end points of the *closed* interval

$$[(2j)\sigma_j - 1, (2j)\sigma_j + 1]$$

and it takes positive value in the middle. By continuity, $g_n(x)$ must have a root in one of the *open* intervals

$$((2j)\sigma_j - 1, (2j)\sigma_j) \quad \text{or} \quad ((2j)\sigma_j, (2j)\sigma_j + 1). \tag{15}$$

As we run through all $1 \leq j \leq n$, these $2n$ *open* intervals are pairwise disjoint, and the two open intervals in (15) are both contained in the positive x-axis if and only if $\sigma_j > 0$. That means if $n \geq 6$, then the degree-n polynomial $g_n(x)$ has exactly n distinct real roots, and its unique root in the union of the intervals in (15) has the same sign as σ_j. This completes the proof of the lemma. □

Lemma 3.2. *As $n\to\infty$ we have the estimate* $\log|\mathrm{disc}(g_n(x^2))| \ll n^2 \log n$.

Proof. For any polynomial $G(x)$, from the definition of polynomial discriminant we see that

$$|\mathrm{disc}(G(x^2))| = |\mathrm{disc}(G(x))|^2 \cdot 2^{\deg G} \cdot |\text{constant term of } G(x)|.$$

Consequently,

$$\log|\operatorname{disc}(g_n(x^2))| \le 2\log|\operatorname{disc}(g_n(x))| + 2n\log 2 + \sum_{i=1}^{n}\log(2i)$$
$$\ll \log|\operatorname{disc}(g_n(x))| + n\log n.$$

By Lemma 3.1, if $n \ge 6$ then the roots of $g_n(x)$ are pairwise distinct and each one is of distance less than 1 from exactly one of the $(2j)\sigma_j$. Thus

$$\log|\operatorname{disc}(g_n(x))| \le \sum_{1\le i\ne j\le n} 2\log|2i+2j+2| \ll n^2\log(2n+2) \ll n^2\log n.$$

Combine this with (16) and the lemma follows. □

Proof of Theorem 1.2. Given $0 \le n' \le n$, choose $\sigma_j \in \{\pm 1\}$ $(0 \le j \le n)$ so that exactly n' of them are positive. With respect to these σ_j, the corresponding polynomial $g_n(x^2)$ is Eisenstein at 2, and so it is irreducible over $\mathbb{Q}$. By construction it has exactly $2n'$ real embedding. Denote by $N_n/\mathbb{Q}$ the degree $2n$ extension defined by a root of $g_n(x^2)$. It is totally real if $n \ge 6$, by Lemma 3.1. By Lemma 3.2, we have $\log(rd_{N_n}) \ll n_{N_n}\log(n_{N_n})$, and the theorem follows. □

4. Small root discriminants via Pisot numbers

A real algebraic integer θ is called a Pisot number if every conjugate of θ other than θ itself has absolute value less than 1 (these other conjugates need not be real). A celebrated theorem of Salem [1944] says that the set of Pisot numbers is a closed subset of the real line.

Lemma 4.1. *Any integer $a \ge 2$ is a nonisolated limit point of the set of Pisot numbers.*

Proof. This is a standard fact about Pisot numbers; we give the details following the hint in [Salem 1963, p. 21] since we need the explicit polynomials later on. Consider the polynomial

$$f_{n,a}(x) = x^n(x-a) - 1.$$

Clearly $f_{n,a}(0) \ne 0$, and

$$f_{n,a}\left(\frac{an}{n+1}\right) = \left(\frac{an}{n+1}\right)^n\left(\frac{an}{n+1} - a\right) - 1 = \left(\frac{n}{n+1}\right)^n\left(\frac{-a^{n+1}}{n+1}\right) - 1 < 0.$$

Thus the roots of the derivative $f'_{n,a}(x) = (n+1)x^{n-1}(x - an/(n+1))$ are not roots of $f_{n,a}$, whence $f_{n,a}$ is separable. Since $f_{n,a}(a) = -1$ and

$$f_{n,a}(a+1/n) = \frac{(a+1/n)^n}{n} - 1 > \frac{(1+1)^n - n}{n} \ge \frac{(n\cdot 1^{n-1}\cdot 1) - n}{n} \ge 0 \quad \text{for } n \ge 2,$$

it follows that $f_{n,a}$ has a real root in the interval $(a, a+1/n)$ for $n \geq 2$. And since $f'_{n,a}$ has no root in $(a, a+1/n)$, the mean value theorem implies that $f_{n,a}$ has a *unique* real root $\theta_{n,a}$ in this interval. Our next step is to show that the remaining roots of $f_{n,a}$ all have absolute value less than 1.

First, suppose $a > 2$. By Rouché's theorem, the number of roots of $f_{n,a}$ inside the unit circle is equal to that of az^n, counted with multiplicity. For future reference, note that up until this point our argument does not require that a be an integer.

Take $a > 2$ to be an integer. Since $f_{n,a}$ has degree $n+1$, combine the conclusion of the two paragraphs above and it follows that $\theta_{n,a}$ is a Pisot number for all $n \geq 2$. And since $\lim_{n\to\infty} \theta_{n,a} = a$, we see that a is a nonisolated limit point of the set of Pisot numbers.

Now, fix $n \geq 2$, and let $a \to 2$ from the right side. By the conclusion of the second paragraph (which is valid for $a > 2$), it follows that $f_{n,2}$ has n roots with absolute value at most 1. Suppose it does have a root ζ with absolute value 1. Then $\zeta - \zeta^{-n} = 2$, which is impossible. Thus for any fixed $n \geq 2$, all roots of $f_{n,2}$ except for $\theta_{n,2}$ have absolute value less than 1. We can now continue as in the case of integer $a > 2$ above, and the lemma follows. □

Proof of Theorem 1.3. First, note that $f_{n,a}$ is irreducible over $\mathbb{Q}$; otherwise by Gauss's lemma, it has a nontrivial monic irreducible factor over $\mathbb{Z}$ with all roots having absolute value less than 1, which is impossible. Thus $T_n := \mathbb{Q}(\theta_{n,2})$ is an extension of $\mathbb{Q}$ of degree $n+1$.

Since $f_{n,2}(0) = -1$ and since $f'_{n,2}$ is negative on the interval (0, 1), that means $f_{n,2}$ has no real root on the interval [0, 1]. Thus $\theta_{n,2}$ is the only real root of $f_{n,2}$ on the positive real axis. Since $f'_{n,2}$ has no root on the negative real axis, the mean value theorem implies that $f_{n,2}$ has at most one negative real root. Consequently, $f_{n,2}$ has at most two real roots. Since $f_{n,2}$ does have at least one real root and since $\deg(f_{n,2}) = n+1$, it follows that $r_1(T_n) = 1$ or 2 depending on whether n is even or odd. It remains to bound the root discriminant of T_n.

As α runs through the roots of $f_{n,2}$, we see that the absolute value of the polynomial discriminant of $f_{n,2}$ is

$$\begin{aligned}
\prod_\alpha |f'_{n,2}(\alpha)| &= \Big|\prod_\alpha \alpha\Big|^{n-1} \cdot (n+1)^{n+1} \cdot \prod_\alpha \big|\alpha - \tfrac{2n}{n+1}\big| \\
&= (n+1)^{n+1} \cdot \big|f\big(1 - \tfrac{2}{n+1}\big)\big| \\
&= (n+1)^{n+1} \cdot \big|\big(1 - \tfrac{2}{n+1}\big)^n \big(1 - \tfrac{2}{n+1} - 2\big) - 1\big| \\
&\leq 3(n+1)^{n+1} \qquad\qquad \text{for } n \geq 2,
\end{aligned}$$

and the theorem follows. □

Acknowledgements

We thank Professors Hajir and Maire for bringing this question to our attention, Professors Gunnells and Kusner for useful discussions, and the referee for detailed and constructive comments.

References

[Belolipetsky and Lubotzky 2012] M. Belolipetsky and A. Lubotzky, "Manifolds counting and class field towers", *Adv. Math.* **229**:6 (2012), 3123–3146. MR 2900437 Zbl 1241.22014

[Fontaine 1985] J.-M. Fontaine, "Il n'y a pas de variété abélienne sur $\mathbb{Z}$", *Invent. Math.* **81**:3 (1985), 515–538. MR 87g:11073 Zbl 0612.14043

[Friedman 1989] E. Friedman, "Analytic formulas for the regulator of a number field", *Invent. Math.* **98**:3 (1989), 599–622. MR 91c:11061 Zbl 0694.12006

[Hajir and Maire 2001] F. Hajir and C. Maire, "Tamely ramified towers and discriminant bounds for number fields", *Compositio Math.* **128**:1 (2001), 35–53. MR 2002g:11149 Zbl 1042.11072

[Hajir and Maire 2002] F. Hajir and C. Maire, "Tamely ramified towers and discriminant bounds for number fields, II", *J. Symbolic Comput.* **33**:4 (2002), 415–423. MR 2003h:11137 Zbl 1086.11051

[Koch and Venkov 1975] H. Koch and B. B. Venkov, "Über den p-Klassenkörperturm eines imaginär-quadratischen Zahlkörpers", pp. 57–67 in *Journées arithmétiques de Bordeaux* (Bordeaux, 1974), Astérisque **24–25**, Soc. Math. France, Paris, 1975. MR 52 #13741 Zbl 0335.12021

[Lagarias and Odlyzko 1977] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem", pp. 409–464 in *Algebraic number fields: L-functions and Galois properties* (Durham, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR 56 #5506 Zbl 0362.12011

[Lang 1986] S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics **110**, Springer, New York, 1986. MR 44 #181 Zbl 0601.12001

[Martin 2006] J. W. Martin, "Improved bounds for discriminants of number fields: improved discriminant bounds", preprint, 2006.

[Martinet 1978] J. Martinet, "Tours de corps de classes et estimations de discriminants", *Invent. Math.* **44**:1 (1978), 65–73. MR 57 #275 Zbl 0369.12007

[Masley 1978] J. M. Masley, "Class numbers of real cyclic number fields with small conductor", *Compositio Math.* **37**:3 (1978), 297–319. MR 80e:12005 Zbl 0428.12003

[Odlyzko 1990] A. M. Odlyzko, "Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results", *Sém. Théor. Nombres Bordeaux* (2) **2**:1 (1990), 119–141. MR 91i:11154 Zbl 0722.11054

[Oesterlé 1979] J. Oesterlé, "Versions effectives du théorème de Chebotarev sous l'hypothése de Riemann généralisée", pp. 165–167 in *Journées arithmétiques de Luminy* (Luminy, 1978), Astérisque **61**, Soc. Math. France, Paris, 1979. Zbl 0418.12005

[Roquette 1967] P. Roquette, "On class field towers", pp. 231–249 in *Algebraic number theory* (Brighton, 1965), edited by J. W. S. Cassels and A. Fröhlich, Thompson, Washington, DC, 1967. MR 36 #1418

[Salem 1944] R. Salem, "A remarkable class of algebraic integers: proof of a conjecture of Vijayaraghavan", *Duke Math. J.* **11** (1944), 103–108. MR 5,254a Zbl 0063.06657

[Salem 1963] R. Salem, *Algebraic numbers and Fourier analysis*, D. C. Heath, Boston, 1963. MR 28 #1169 Zbl 0126.07802

[Schmithals 1980] B. Schmithals, "Konstruktion imaginärquadratischer Körper mit unendlichem Klassenkörperturm", *Arch. Math.* (*Basel*) **34**:4 (1980), 307–312. MR 82f:12017 Zbl 0448.12008

[Schoof 1986] R. Schoof, "Infinite class field towers of quadratic fields", *J. Reine Angew. Math.* **372** (1986), 209–220. MR 88a:11121 Zbl 0589.12011

[Serre 1979] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics **67**, Springer, New York, 1979. MR 82e:12016 Zbl 0423.12016

[Stark 1974] H. M. Stark, "Some effective cases of the Brauer–Siegel theorem", *Invent. Math.* **23** (1974), 135–152. MR 49 #7218 Zbl 0278.12005

[Tate 1994] J. Tate, "The non-existence of certain Galois extensions of $\mathbb{Q}$ unramified outside 2", pp. 153–156 in *Arithmetic geometry* (Tempe, AZ, 1993), edited by N. Childress and J. W. Jones, Contemp. Math. **174**, Amer. Math. Soc., Providence, RI, 1994. MR 95i:11132 Zbl 0814.11057

[Washington 1982] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics **83**, Springer, New York, 1982. MR 85g:11001 Zbl 0484.12001

Received January 23, 2014. Revised February 13, 2015.

SIMAN WONG
DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF MASSACHUSETTS
LEDERLE GRADUATE RESEARCH TOWER
BOX 34515
AMHERST, MA 01003-9305
UNITED STATES

siman@math.umass.edu

PACIFIC JOURNAL OF MATHEMATICS

msp.org/pjm

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2015 is US $420/year for the electronic version, and $570/year for print and electronic.
Subscriptions, requests for back issues and changes of subscribers address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS

Volume 277 No. 1 September 2015