Enumeration of totally real number fields of bounded root discriminant

John Voight

Department of Mathematics and Statistics
University of Vermont
Burlington, VT 05401
jvoight@gmail.com

Abstract. We enumerate all totally real number fields F with root discriminant $\delta_F \leq 14$. There are 1229 such fields, each with degree $[F:\mathbb{Q}] \leq 9$.

In this article, we consider the following problem.

Problem 1. Given $B \in \mathbb{R}_{>0}$, enumerate the set $NF(B)$ of totally real number fields F with root discriminant $\delta_F \leq B$, up to isomorphism.

To solve Problem 1, for each $n \in \mathbb{Z}_{>0}$ we enumerate the set

$$NF(n,B) = \{F \in NF(B) : [F:\mathbb{Q}] = n\}$$

which is finite (a result originally due to Minkowski). If F is a totally real field of degree $n = [F:\mathbb{Q}]$, then by the Odlyzko bounds [27], we have $\delta_F \geq 4\pi e^{1+\gamma} - O(n^{-2/3})$ where γ is Euler's constant; thus for $B < 4\pi e^{1+\gamma} < 60.840$, we have $NF(n,B) = \emptyset$ for n sufficiently large and so the set $NF(B)$ is finite. Assuming the generalized Riemann hypothesis (GRH), we have the improvement $\delta_F \geq 8\pi e^{\gamma+\pi/2} - O(\log^{-2} n)$ and hence $NF(B)$ is conjecturally finite for all $B < 8\pi e^{\gamma+\pi/2} < 215.333$. On the other hand, for B sufficiently large, the set $NF(B)$ is infinite: Martin [23] has constructed an infinite tower of totally real fields with root discriminant $\delta \approx 913.493$ (a long-standing previous record was held by Martinet [25] with $\delta \approx 1058.56$). The value

$$\liminf_{n\to\infty} \min\{\delta_F : F \in NF(n,B)\}$$

is presently unknown. If B is such that $\#NF(B) = \infty$, then to solve Problem 1 we enumerate the set $NF(B) = \bigcup_n NF(n,B)$ by increasing degree.

Our restriction to the case of totally real fields is not necessary: one may place alternative constraints on the signature of the fields F under consideration (or even analogous p-adic conditions). However, we believe that Problem 1 remains one of particular interest. First of all, it is a natural boundary case: by comparison, Hajir-Maire [14, 15] have constructed an unramified tower of totally complex number fields with root discriminant ≈ 82.100, which comes within a factor 2 of the GRH-conditional Odlyzko bound of $8\pi e^{\gamma} \approx 44.763$. Secondly, in studying certain problems in arithmetic geometry and number theory—for example, in the enumeration of arithmetic Fuchsian groups [21] and the computational investigation of the Stark conjecture and its generalizations—provably complete and extensive tables of totally real fields are useful, if not outright essential. Indeed, existing strategies for finding towers with small root discriminant as above often start by finding a good candidate base field selected from existing tables.

The main result of this note is the following theorem, which solves Problem 1 for $\delta = 14$.

Theorem 2. *We have* $\#NF(14) = 1229$.

The complete list of these fields is available online [35]; the octic and nonic fields ($n = 8, 9$) are recorded in Tables 3–4 in §4, and there are no dectic fields ($NF(14, 10) = \emptyset$). For a comparison of this theorem with existing results, see §1.2.

The note is organized as follows. In §1, we set up the notation and background. In §2, we describe the computation of primitive fields $F \in NF(14)$; we compare well-known methods and provide some improvements. In §3, we discuss the extension of these ideas to imprimitive fields, and we report timing details on the computation. Finally, in §4 we tabulate the fields F.

The author wishes to thank: Jürgen Klüners, Noam Elkies, Claus Fieker, Kiran Kedlaya, Gunter Malle, and David Dummit for useful discussions; William Stein, Robert Bradshaw, Craig Citro, Yi Qiang, and the rest of the Sage development team for computational support (NSF Grant No. 0555776); and Larry Kost and Helen Read for their technical assistance.

1 Background

1.1 Initial bounds

Let F denote a totally real field of degree $n = [F : \mathbb{Q}]$ with discriminant d_F and root discriminant $\delta_F = d_F^{1/n}$. By the unconditional Odlyzko bounds [27] (see also Martinet [24]), if $n \geq 11$ then $\delta_F > 14.083$, thus if $F \in NF(14)$ then $n \leq 10$.

Table 1. Degree and Root Discriminant Bounds

n	2	3	4	5	6	7	8	9	10
B_O	> 2.223	3.610	5.067	6.523	7.941	9.301	10.596	11.823	12.985
B_O (GRH)	> 2.227	3.633	5.127	6.644	8.148	9.617	11.042	12.418	13.736
Δ	30	25	20	17	16	15.5	15	14.5	14

The lower bounds for δ_F in the remaining degrees are summarized in Table 1: for each degree $2 \leq n \leq 10$, we list the unconditional Odlyzko bound $B_O =$

$B_O(n)$, the GRH-conditional Odlyzko bound (for comparison only, as computed by Cohen-Diaz y Diaz-Olivier [7]), and the bound $\delta_F \le \Delta$ that we employ.

1.2 Previous work

There has been an extensive amount of work done on the problem of enumerating number fields—we refer to [18] for a discussion and bibliography.

1. The KASH and PARI groups [16] have computed tables of number fields of all signatures with degrees ≤ 7: in degrees $6, 7$, they enumerate totally real fields up to discriminants $10^7, 15 \cdot 10^7$, respectively (corresponding to root discriminants $14.67, 14.71$, respectively).
2. Malle [22] has computed all totally real primitive number fields of discriminant $d_F \le 10^9$ (giving root discriminants $31.6, 19.3, 13.3, 10$ for degrees $6, 7, 8, 9$). This was reported to take several years of CPU-time on a SUN workstation.
3. The database by Klüners-Malle [17] contains polynomials for all transitive groups up to degree 15 (including possible combinations of signature and Galois group); up to degree 7, the fields with minimal (absolute) discriminant with given Galois group and signature have been included.
4. Roblot [30] constructs abelian extensions of totally real fields of degrees 4 to 48 (following Cohen-Diaz y Diaz-Olivier [6]) with small root discriminant.

The first two of these allow us only to determine $NF(10)$ (if we also separately compute the imprimitive fields); the latter two, though very valuable for certain applications, are in a different spirit than our approach. Therefore our theorem substantially extends the complete list of fields in degrees 7–9.

2 Enumeration of totally real fields

2.1 General methods

The general method for enumerating number fields is well-known (see Cohen [4, §9.3]). We define the Minkowski norm on a number field F by $T_2(\alpha) = \sum_{i=1}^{n} |\alpha_i|^2$ for $\alpha \in F$, where $\alpha_1, \alpha_2, \dots, \alpha_n$ are the conjugates of α in $\mathbb{C}$. The norm T_2 gives $\mathbb{Z}_F$ the structure of a lattice of rank n. In this lattice, the element 1 is a shortest vector, and an application of the geometry of numbers to the quotient lattice $\mathbb{Z}_F/\mathbb{Z}$ yields the following result.

Lemma 3 (Hunter). *There exists $\alpha \in \mathbb{Z}_F \setminus \mathbb{Z}$ such that $0 \le \mathrm{Tr}(\alpha) \le n/2$ and*

$$T_2(\alpha) \le \frac{\mathrm{Tr}(\alpha)^2}{n} + \gamma_{n-1} \left(\frac{|d_F|}{n} \right)^{1/(n-1)}$$

where γ_{n-1} is the $(n-1)$th Hermite constant.

Remark 4. The values of the Hermite constant are known for $n \leq 8$ (given by the lattices $A_1, A_2, A_3, D_4, D_5, E_6, E_7, E_8$): we have $\gamma_n^n = 1, 4/3, 2, 4, 8, 64/3, 64, 256$ (see Conway and Sloane [9]) for $n = 1, \dots, 8$; the best known upper bounds for $n = 9, 10$ are given by Cohn and Elkies [8].

Therefore, if we want to enumerate all number fields F of degree n with $|d_F| \leq B$, an application of Lemma 3 yields $\alpha \in \mathbb{Z}_F \setminus \mathbb{Z}$ such that $T_2(\alpha) \leq C$ for some $C \in \mathbb{R}_{>0}$ depending only on n, B. We thus obtain bounds on the power sums

$$|S_k(\alpha)| = \left| \sum_{i=1}^{n} \alpha_i^k \right| \leq T_k(\alpha) = \sum_{i=1}^{n} |\alpha_i|^k \leq nC^{k/2},$$

and hence bounds on the coefficients $a_i \in \mathbb{Z}$ of the characteristic polynomial

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

of α by Newton's relations:

$$S_k + \sum_{i=1}^{k-1} a_{n-1} S_{k-i} + k a_{n-k} = 0. \tag{1}$$

This then yields a finite set $NS(n, B)$ of polynomials $f(x) \in \mathbb{Z}[x]$ such that every F is represented as $\mathbb{Q}[x]/(f(x))$ for some $f(x) \in NS(n, B)$, and in principle each $f(x)$ can then be checked individually. We note that it is possible that α as given by Hunter's theorem may only generate a subfield $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subsetneq F$ if F is imprimitive: for a treatment of this case, see §3.

The size of the set $NS(n, B)$ is $O(B^{n(n+2)/4})$ (see Cohen [4, §9.4]), and the exponential factor in n makes this direct method impractical for large n or B. Note, however, that it is sharp for $n = 2$: we have $NF(2, B) \sim (6/\pi^2)B^2$ (as $B \to \infty$), and indeed, in this case one can reduce to simply listing squarefree integers. For other small values of n, better algorithms are known: following Davenport-Heilbronn, Belabas [2] has given an algorithm for cubic fields; Cohen-Diaz y Diaz-Olivier [7] use Kummer theory for quartic fields; and by work of Bhargava [3], in principle one should similarly be able to treat the case of quintic fields. No known method improves on this asymptotic complexity for general n, though some possible progress has been made by Ellenberg-Venkatesh [12].

2.2 Improved methods for totally real fields

We now restrict to the case that F is totally real. Several methods can then be employed to improve the bounds given above—although we only improve on the implied constant in the size of the set $NS(n, B)$ of examined polynomials, these improvements are essential for practical computations.

Basic bounds. From Lemma 3, we have $0 \le a_{n-1} = -\operatorname{Tr}(\alpha) \le \lfloor n/2 \rfloor$ and

$$a_{n-2} = \frac{1}{2}a_{n-1}^2 - \frac{1}{2}T_2(\alpha) \ge \frac{1}{2}\left(1 - \frac{1}{n}\right)a_{n-1}^2 - \frac{\gamma_{n-1}}{2}\left(\frac{B}{n}\right)^{1/(n-1)}.$$

For an upper bound on a_{n-2}, we apply the following result.

Lemma 5 (Smyth [32]). *If γ is a totally positive algebraic integer, then*

$$\operatorname{Tr}(\gamma) > 1.7719[\mathbb{Q}(\gamma) : \mathbb{Q}]$$

unless γ is a root of one of the following polynomials:

$$x-1, x^2-3x+1, x^3-5x^2+6x-1, x^4-7x^3+13x^2-7x+1, x^4-7x^3+14x^2-8x+1.$$

Remark 6. The best known bound of the above sort is due to Aguirre-Bilbao-Peral [1], who give $\operatorname{Tr}(\gamma) > 1.780022[\mathbb{Q}(\gamma) : \mathbb{Q}]$ with 14 possible explicit exceptions. For our purposes (and for simplicity), the result of Smyth will suffice.

Excluding these finitely many cases, we apply Lemma 5 to the totally positive algebraic integer α^2, using the fact that $T_2(\alpha) = \operatorname{Tr}(\alpha^2)$, to obtain the upper bound $a_{n-2} < a_{n-1}^2/2 - 0.88595n$.

Rolle's theorem. Now, given values $a_{n-1}, a_{n-2}, \dots, a_{n-k}$ for the coefficients of $f(x)$ for some $k \ge 2$, we deduce bounds for a_{n-k-1} using Rolle's theorem—this elementary idea can already be found in Takeuchi [33] and Klüners-Malle [18, §3.1]. Let

$$f_i(x) = \frac{f^{(n-i)}(x)}{(n-i)!} = g_i(x) + a_{n-i}$$

for $i = 0, \dots, n$. Consider first the case $k = 2$. Then

$$g_3(x) = \frac{n(n-1)(n-2)}{6}x^3 + \frac{(n-1)(n-2)}{2}a_{n-1}x^2 + (n-2)a_{n-2}x.$$

Let $\beta_1 < \beta_2$ denote the roots of $f_2(x)$. Then by Rolle's theorem,

$$f_3(\beta_1) = g_3(\beta_1) + a_{n-3} > 0 \quad \text{and} \quad f_3(\beta_2) = g_3(\beta_2) + a_{n-3} < 0$$

hence $-g_3(\beta_1) < a_{n-3} < -g_3(\beta_2)$. In a similar way, if $\beta_1^{(k)} < \dots < \beta_k^{(k)}$ denote the roots of $f_k(x)$, then we find that

$$-\min_{\substack{1 \le i \le k \\ i \not\equiv k\ (2)}} g_{k+1}(\beta_i^{(k)}) < a_{n-k-1} < -\max_{\substack{1 \le i \le k \\ i \equiv k\ (2)}} g_{k+1}(\beta_i^{(k)}).$$

Lagrange multipliers. We can obtain further bounds as follows. We note that if the roots of f are bounded below by $\beta_0^{(k)}$ (resp. bounded above by $\beta_{k+1}^{(k)}$), then

$$f_k(\beta_0^{(k)}) = g_k(\beta_0^{(k)}) + a_{n-k} > 0$$

(with a similar inequality for $\beta_{k+1}^{(k)}$), and these combine with the above to yield

$$-\min_{\substack{0\le i\le k+1\\ i\not\equiv k\ (2)}} g_{k+1}(\beta_i^{(k)}) < a_{n-k-1} < -\max_{\substack{0\le i\le k+1\\ i\equiv k\ (2)}} g_{k+1}(\beta_i^{(k)}). \tag{2}$$

We can compute $\beta_0^{(k)}, \beta_{k+1}^{(k)}$ by the method of Lagrange multipliers, which were first introduced in this general context by Pohst [29] (see Remark 7). The values $a_{n-1}, \dots, a_{n-k} \in \mathbb{Z}$ determine the power sums s_i for $i = 1, \dots, k$ by Newton's relations (1). Now the set of all $x = (x_i) \in \mathbb{R}^n$ such that $S_i(x) = s_i$ is closed and bounded, and therefore by symmetry the minimum (resp. maximum) value of the function x_n on this set yields the bound $\beta_0^{(k)}$ (resp. $\beta_{k+1}^{(k)}$). By the method of Lagrange multipliers, we find easily that if $x \in \mathbb{R}^n$ yields such an extremum, then there are at most $k-1$ distinct values among $x_1, \dots, x_{n-1}$, from which we obtain a finite set of possibilities for the extremum x.

For example, in the case $k = 2$, the extrema are obtained from the equations

$$(n-1)x_1 + x_n = s_1 = -a_{n-1} \quad \text{and} \quad (n-1)x_1^2 + x_n^2 = s_2 = a_{n-1}^2 - 2a_{n-2}$$

which yields simply

$$\beta_0^{(2)}, \beta_3^{(2)} = \frac{1}{n}\left(-a_{n-1} \pm (n-1)\sqrt{a_{n-1}^2 - 2\left(1 + \frac{1}{n-1}\right)a_{n-2}}\right).$$

(It is easy to show that this always improves upon the trivial bounds used by Takeuchi [33].) For $k = 3$, for each partition of $n-1$ into 2 parts, one obtains a system of equations which via elimination theory yield a (somewhat lengthy but explicitly given) degree 6 equation for x_n. For $k \ge 4$, we can continue in a similar way but we instead solve the system numerically, e.g., using the method of homotopy continuation as implemented by the package PHCpack developed by Verschelde [34]; in practice, we do not significantly improve on these bounds whenever $k \ge 5$, and even for $k = 5$, if n is small then it often is more expensive to compute the improved bounds than to simply set $\beta_0^{(k)} = \beta_0^{(k-1)}$ and $\beta_{k+1}^{(k)} = \beta_k^{(k-1)}$.

Remark 7. Pohst's original use of Lagrange multipliers, which applies to number fields of arbitrary signature, instead sought the extrema of the power sum S_{k+1} to bound the coefficient a_{n-k-1}. The bounds given by Rolle's theorem for totally real fields are not only easier to compute (especially in higher degree) but in most cases turn out to be strictly stronger. We similarly find that many other bounds typically employed in this situation (e.g., those arising from the positive definiteness of T_2 on $\mathbb{Z}[\alpha]$) are also always weaker.

2.3 Algorithmic details

Our algorithm to solve Problem 1 then runs as follows. We first apply the basic bounds from §2.2 to specify finitely many values of a_{n-1}, a_{n-2}. For each such pair, we use Rolle's theorem and the method of Lagrange multipliers to bound each of the coefficients inductively. Note that if $k \geq 3$ is odd and $a_{n-1} = a_{n-3} = \cdots = a_{n-(k-2)} = 0$, then replacing α by $-\alpha$ we may assume that $a_{n-k} \geq 0$.

For each polynomial $f \in NS(n, B)$ that emerges from these bounds, we test it to see if it corresponds to a field $F \in NF(n, B)$. We treat each of these latter two tasks in turn.

Calculation of real roots. In the computation of the bounds (2), we use Newton's method to iteratively compute approximations to the roots $\beta_i^{(k)}$, using the fact that the roots of a polynomial are interlaced with those of its derivative, i.e. $\beta_{i-1}^{(k-1)} < \beta_i^{(k)} < \beta_i^{(k-1)}$ for $i = 1, \ldots, k$. Note that by Rolle's theorem, we will either find a simple root in this open interval or we will converge to one of the endpoints, say $\beta_i^{(k)} = \beta_i^{(k-1)}$, and then necessarily $\beta_i^{(k)} = \beta_i^{(k-1)}$ as well, which implies that $f_k(x)$ is not squarefree and hence the entire coefficient range may be discarded immediately. It is therefore possible to very quickly compute an approximate root which differs from the actual root $\beta_i^{(k+1)}$ by at most some fixed $\epsilon > 0$. We choose ϵ small enough to give a reasonable approximation but not so small as to waste time in Newton's method (say, $\epsilon = 10^{-4}$). We deal with the possibility of precision loss by bounding the value $g_{k+1}(\beta_i^{(k)})$ in (2) using elementary calculus; we leave the details to the reader.

Testing polynomials. For each $f \in NS(n, B)$, we test each of the following in turn.

1. We first employ an "easy irreducibility test": We rule out polynomials f divisible by any of the factors: $x, x \pm 1, x \pm 2, x^2 \pm x - 1, x^2 - 2$. In the latter three cases, we first evaluate the polynomial at an approximation to the values $(1 \pm \sqrt{5})/2, \sqrt{2}$, respectively, and then evaluate f at these roots using exact arithmetic. (Some benefit is gained by hard coding this latter evaluation.)
2. We then compute the discriminant $d = \operatorname{disc}(f)$. If $d \leq 0$, then f is not a real separable polynomial, so we discard f.
3. If $F = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(f(x)) \in NF(n, B)$, then for some $a \in \mathbb{Z}$ we have $B_O(n)^n < d_F = d/a^2 < B^n$ where B_O is the Odlyzko bound (see §1). Therefore using trial division we can quickly determine if there exists such an $a^2 \mid d$; if not, then we discard f.
4. Next, we check if f is irreducible, and discard f otherwise.
5. By the preceding two steps, an a-maximal order containing $\mathbb{Z}[\alpha]$ is in fact the maximal order $\mathbb{Z}_F$ of the field F. If $\operatorname{disc}(\mathbb{Z}_F) = d_F > B$, we discard f.
6. Apply the POLRED algorithm of Cohen-Diaz y Diaz [5]: embed $\mathbb{Z}_F \subset \mathbb{R}^n$ by Minkowski (as in §1.1) and use LLL-reduction [20] to compute a small

element $\alpha_{\rm red} \in \mathbb{Z}_F$ such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha_{\rm red}) = F$. Add the minimal polynomial $f_{\rm red}(x)$ of $\alpha_{\rm red}$ to the list $NF(n, B)$ (along with the discriminant d_F), if it does not already appear.

We expect that almost all isomorphic fields will be identified in Step 6 by computing a reduced polynomial. For reasons of efficiency, we wait until the space $NS(n, B)$ has been exhausted to do a final comparison with each pair of polynomials with the same discriminant to see if they are isomorphic. Finally, we add the exceptional fields coming from Lemma 5, if relevant.

Remark 8. Although Step 1 is seemingly trivial, it rules out a surprisingly significant number of polynomials f—indeed, nearly all reducible polynomials are discarded by this step in higher degrees. Indeed, if $T_2(f) = \sum_i \alpha_i^2$ (where α_i are the roots of f) is small compared to $\deg(f) = n$, then f is likely to be reducible and moreover divisible by a polynomial g with $T_2(g)$ also small. It would be interesting to give a precise statement which explains this phenomenon.

2.4 Implementation details

For the implementation of our algorithm, we use the computer algebra system Sage [31], which utilizes PARI [28] for Steps 4–6 above. Since speed was of the absolute essence, we found that the use of Cython (developed by Stein and Bradshaw) allowed us to develop a carefully optimized and low-level implementation of the bounds coming from Rolle's theorem and Lagrange multiplier method 2. We used the DSage package (due to Qiang) which allowed for the distribution of the compution to many machines; as a result, our computational time comes from a variety of processors (Opteron 1.8GHz, Athlon Dual Core 2.0GHz, and Celeron 2.53GHz), including a cluster of 30 machines at the University of Vermont.

In low and intermediate degrees, where we expect comparatively many fields, we find that the running time is dominated by the computation of the maximal order (Step 5), followed by the check for irreducibility (Step 4); this explains the ordering of the steps as above. By contrast, in higher degrees, where we expect few fields but must search in an exponentially large space, most of the time is spent in the calculation of real roots and in Step 1. Further timing details can be found in Table 2 in §3.2.

3 Imprimitive fields

In this section, we extend the ideas of the previous section to imprimitive fields F, i.e. those fields F containing a nontrivial subfield. Suppose that F is an extension of E with $[F : E] = m$ and $[E : \mathbb{Q}] = d$. Since $\delta_F \geq \delta_E$, if $F \in NF(B)$ then $E \in NF(B)$ as well, and thus we proceed by induction on E. For each such subfield E, we proceed in an analogous fashion. We let

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

be the minimal polynomial of an element $\alpha \in \mathbb{Z}_F$ with $F = E(\alpha)$ and $a_i \in \mathbb{Z}_E$.

3.1 Extension of bounds

Basic bounds We begin with a relative version of Hunter's theorem. We denote by E_∞ the set of infinite places of E.

Lemma 9 (Martinet [26]). *There exists $\alpha \in \mathbb{Z}_F \setminus \mathbb{Z}_E$ such that*

$$T_2(\alpha) \leq \frac{1}{m} \sum_{\sigma \in E_\infty} \left|\sigma\left(\operatorname{Tr}_{F/E} \alpha\right)\right|^2 + \gamma_{n-d} \left(\frac{|d_F|}{m^d |d_E|}\right)^{1/(n-d)}. \qquad (3)$$

The inequality of Lemma 9 remains true for any element of the set $\mu_E \alpha + \mathbb{Z}_E$, where μ_E denotes the roots of unity in E. This allows us to choose $\operatorname{Tr}_{F/E} \alpha = -a_{m-1}$ among any choice of representatives from $\mathbb{Z}_E/m\mathbb{Z}_E$ (up to a root of unity); we choose the value of a_{m-1} which minimizes

$$\sum_{\sigma \in E_\infty} \left|\sigma\left(\operatorname{Tr}_{F/E} \alpha\right)\right|^2 = \sum_{\sigma \in E_\infty} \sigma(a_{m-1})^2,$$

which is a positive definite quadratic form on $\mathbb{Z}_E$; such a value can be found easily using the LLL-algorithm.

Now suppose that F is totally real. Then $\sum_{\sigma \in E_\infty} |\sigma(a_{m-1})|^2 = \operatorname{Tr}_{E/\mathbb{Q}} a_{m-1}^2$, and we have 2^d or $\lceil m^d/2 \rceil$ possibilities for a_{m-1}, according as $m = 2$ or otherwise. For each value of a_{m-1}, we have $T_2(\alpha) \in \mathbb{Z}$ bounded from above by Lemma 9 and from below by Lemma 5 since $\operatorname{Tr}_{E/\mathbb{Q}}(\alpha^2) = T_2(\alpha) > 1.7719n$. If we denote $\operatorname{Tr}_{F/E} \alpha^2 = t_2$, then by Newton's relations, we have $t_2 = a_{m-1}^2 - 2a_{m-2}$, and hence $\operatorname{Tr}_{E/\mathbb{Q}} t_2 = T_2(\alpha)$ and $t_2 \equiv a_{m-1}^2 \pmod 2$. In particular, $t_2 \in \mathbb{Z}_E$ is totally positive and has bounded trace, leaving only finitely many possibilities: indeed, if we embed $\mathbb{Z}_E \hookrightarrow \mathbb{R}^d$ by Minkowski, these inequalities define a parallelopiped in the positive orthant.

Lattice points in boxes. One option to enumerate the possible values of t_2 is to enumerate all lattice points in a sphere of radius given by (3) using the Fincke-Pohst algorithm [13]. However, one ends up enumerating far more than what one needs in this fashion, and so we look to do better. The problem we need to solve is the following.

Problem 10. Given a lattice $L \subset \mathbb{R}^d$ of rank d and a convex polytope P of finite volume, enumerate the set $P \cap L$.

Here we must allow the lattice L to be represented numerically; to avoid issues of precision loss, one supposes without loss of generality that $\partial P \cap L = \emptyset$.

There exists a vast literature on the classical problem of the enumeration of integer lattice points in rational convex polytopes (see e.g., De Loera [10]), as well as several implementations [11, 19]. (In many cases, these authors are concerned primarily with simply counting the number of lattice points, but their methods equally allow their enumeration.)

In order to take advantage of these methods to solve Problem 10, we compute an LLL-reduced basis $\gamma = \gamma_1, \dots, \gamma_d$ of L, and we perform the change of variables $\phi : \mathbb{R}^d \to \mathbb{R}^d$ which maps $\gamma_i \mapsto e_i$ where e_i is the ith coordinate vector. The image $\phi(P)$ is again a convex polytope. We then compute a rational polytope Q (i.e. a polytope with integer vertices) containing $\phi(P)$ by rounding the vertices to the nearest integer point as follows. For each pair of vertices $v, w \in P$ such that the line $\ell(v, w)$ containing v and w is not contained in a proper face of P, we round the ith coordinates $\phi(v)_i$ down and $\phi(w)_i$ up if $\phi(v)_i \leq \phi(w)_i$, and otherwise round in the opposite directions. The convex hull Q of these rounded vertices clearly contains $\phi(P \cap L)$, and is therefore amenable to enumeration using the methods above.

We note that in the case where P is a parallelopiped, for each vertex v there is a unique opposite vertex w such that the line $\ell(v, w)$ is not contained in a proper face, so the convex hull Q will also form a parallelopiped.

Coefficient bounds and testing polynomials. The bounds in §2 apply *mutatis mutandis* to the relative situation. For example, given $a_{m-1}, \dots, a_{m-k}$ for $k \geq 2$, for each $v \in E_\infty$, if we let $v(g)$ denote the polynomial $\sum_i v(b_i)x^i$ for $g(x) = \sum_i b_i x^i \in E[x]$, we obtain the inequality

$$-\min_{\substack{0 \leq i \leq k+1 \\ i \not\equiv k \ (2)}} v(g_{k+1})(\beta_{i,v}^{(k)}) < v(a_{m-k-1}) < -\max_{\substack{0 \leq i \leq k+1 \\ i \equiv k \ (2)}} v(g_{k+1})(\beta_{i,v}^{(k)});$$

here, $\beta_{1,v}^{(k)}, \dots, \beta_{k,v}^{(k)}$ denote the roots of $v(f_k(x))$, and $\beta_{0,v}^{(k)}, \beta_{k+1,v}^{(k)}$ are computed in an analogous way using Lagrange multipliers. In this situation, we have a_{m-k-1} contained in an honest rectangular box, and the results of the previous subsection apply directly.

For each polynomial which satisfies these bounds, we perform similar tests to discard polynomials as in §2.3. One has the option of working always relative to the ground field or immediately computing the corresponding absolute field; in practice, for the small base fields under consideration, these approaches seem to be comparable, with a slight advantage to working with the absolute field.

3.2 Conclusion and timing

Putting together the primitive and imprimitive fields computed in §§2–3, we have proven Theorem 2. In Table 2, we list some timing details arising from the computation. Note that in high degrees (presumably because we enumerate an exponentially large space) we recover all imprimitive fields already during the search for primitive fields.

Table 2. Timing data

n	2	3	4	5	6	7	8	9	10
$\Delta(n)$	30	25	20	17	16	15.5	15	14.5	14
f	443	4922	57721	244600	3242209	1.7×10^7	1.2×10^8	9.5×10^8	2.5×10^9
Irred f	418	2523	27234	157613	2710965	1.6×10^7	1.1×10^8	9.0×10^8	2.5×10^9
f, $d_F \leq B$	418	1573	5665	4497	1288	4839	3016	506	0
F	273	630	1273	674	802	301	164	15	0
Total time	0.2s	2.2s	26.8s	1m25s	17m3s	2h59m	1d4.5h	17d21h	193d
Imprim f	0	0	7059	0	62532	0	239404	15658	945866
Imprim F	0	0	702	0	420	0	100	6	0
Time	-	-	4m22s	-	8m38s	-	1h56m	16m53s	11h27m
Total fields	273	630	1578	674	827	301	164	15	0

4 Tables of totally real fields

In Table 3, we count the number of totally real fields F with root discriminant $\delta_F \leq 14$ by degree, and separate out the primitive and imprimitive fields. We also list the minimal discriminant and root discriminant for $n \leq 9$. The polynomial

$$x^{10} - 11x^8 - 3x^7 + 37x^6 + 14x^5 - 48x^4 - 22x^3 + 20x^2 + 12x + 1$$

with $d_F = 443952558373 = 61^2 397^2 757$ and $\delta_F \approx 14.613$ is the dectic totally real field with smallest discriminant that we found—the corresponding number field (though not this polynomial) already appears in the tables of Klüners-Malle [17] and is a quadratic extension of the second smallest real quintic field, of discriminant 24217. It is reasonable to conjecture that this is indeed the smallest such field.

Table 3. Totally real fields F with $\delta_F \leq 14$

$n = [F : \mathbb{Q}]$	$\#NF(n, 14)$	Primitive F	Imprimitive F	Minimal d_F	Minimal δ_F
2	59	59	0	5	2.236
3	86	86	0	49	3.659
4	277	117	160	725	5.189
5	170	170	0	14641	6.809
6	263	104	159	300125	8.182
7	301	301	0	20134393	11.051
8	62	19	43	282300416	11.385
9	11	6	5	9685993193	12.869
10	0	0	0	443952558373?	14.613?
Total	1229	862	367	-	-

In Tables 4–5, we list the octic and nonic fields F with $\delta_F \leq 14$. For each field, we specify a maximal subfield E by its discriminant and degree—when more than one such subfield exists, we choose the one with smallest discriminant.

Table 4. Octic totally real fields F with $\delta_F \le 14$

d_F	f	$[E:\mathbb{Q}]$	d_E
282300416	$x^8-4x^7+14x^5-8x^4-12x^3+7x^2+2x-1$	4	2624
309593125	$x^8-4x^7-x^6+17x^5-5x^4-23x^3+6x^2+9x-1$	4	725
324000000	$x^8-7x^6+14x^4-8x^2+1$	4	1125
410338673	$x^8-x^7-7x^6+6x^5+15x^4-10x^3-10x^2+4x+1$	4	4913
432640000	$x^8-2x^7-7x^6+16x^5+4x^4-18x^3+2x^2+4x-1$	4	1600
442050625	$x^8-2x^7-12x^6+26x^5+17x^4-36x^3-5x^2+11x-1$	4	725
456768125	$x^8-2x^7-7x^6+11x^5+14x^4-18x^3-8x^2+9x-1$	4	725
483345053	$x^8-x^7-7x^6+4x^5+15x^4-3x^3-9x^2+1$	1	1
494613125	$x^8-x^7-7x^6+4x^5+13x^4-4x^3-7x^2+x+1$	4	725
582918125	$x^8-2x^7-6x^6+9x^5+11x^4-9x^3-6x^2+2x+1$	4	725
656505625	$x^8-3x^7-4x^6+13x^5+5x^4-13x^3-4x^2+3x+1$	4	725
661518125	$x^8-x^7-7x^6+5x^5+15x^4-7x^3-10x^2+2x+1$	2	5
707295133	$x^8-8x^6-2x^5+19x^4+7x^3-13x^2-4x+1$	1	1
733968125	$x^8-2x^7-6x^6+10x^5+11x^4-11x^3-7x^2+2x+1$	2	5
740605625	$x^8-x^7-9x^6+8x^5+21x^4-12x^3-14x^2+4x+1$	4	725
803680625	$x^8-2x^7-9x^6+12x^5+22x^4-24x^3-14x^2+14x-1$	4	725
852038125	$x^8-10x^6-5x^5+17x^4+5x^3-10x^2+1$	4	725
877268125	$x^8-3x^7-6x^6+20x^5+5x^4-25x^3-x^2+7x+1$	4	725
898293125	$x^8-x^7-9x^6+10x^5+15x^4-10x^3-9x^2+x+1$	4	725
1000118125	$x^8-3x^7-4x^6+14x^5+5x^4-19x^3-x^2+7x-1$	2	5
1024000000	$x^8-8x^6+19x^4-12x^2+1$	4	1600
1032588125	$x^8-9x^6-2x^5+23x^4+9x^3-17x^2-9x-1$	2	5
1064390625	$x^8-13x^6+44x^4-17x^2+1$	4	725
1077044573	$x^8-x^7-8x^6+8x^5+16x^4-17x^3-2x^2+5x-1$	1	1
1095205625	$x^8-3x^7-5x^6+18x^5+2x^4-23x^3+2x^2+8x-1$	2	5
1098290293	$x^8-3x^7-4x^6+16x^5+x^4-23x^3+7x^2+5x-1$	1	1
1104338125	$x^8-2x^7-8x^6+15x^5+17x^4-31x^3-9x^2+17x-1$	4	725
1114390153	$x^8-8x^6-2x^5+16x^4+3x^3-10x^2+1$	1	1
1121463125	$x^8-3x^7-4x^6+15x^5+2x^4-18x^3+5x+1$	2	5
1136700613	$x^8-x^7-7x^6+4x^5+14x^4-4x^3-8x^2+x+1$	1	1
1142440000	$x^8-3x^7-5x^6+15x^5+8x^4-15x^3-5x^2+4x+1$	4	4225
1152784549	$x^8-4x^7-x^6+15x^5-3x^4-16x^3+4x^2+4x-1$	4	1957
1153988125	$x^8-2x^7-7x^6+11x^5+12x^4-16x^3-5x^2+6x-1$	4	2525
1166547493	$x^8-x^7-7x^6+6x^5+14x^4-9x^3-9x^2+3x+1$	1	1
1183423341	$x^8-x^7-8x^6+9x^5+17x^4-20x^3-8x^2+10x-1$	4	1957
1202043125	$x^8-3x^7-4x^6+16x^5-21x^3+9x^2+2x-1$	2	5
1225026133	$x^8-3x^7-4x^6+18x^5-6x^4-17x^3+9x^2+2x-1$	1	1
1243893125	$x^8-x^7-8x^6+3x^5+18x^4-x^3-12x^2-2x+1$	2	5
1255718125	$x^8-2x^7-8x^6+19x^5+10x^4-41x^3+13x^2+10x-1$	4	725
1261609229	$x^8-2x^7-6x^6+12x^5+9x^4-19x^3-x^2+6x-1$	1	1
1292203125	$x^8-4x^7-x^6+17x^5-6x^4-21x^3+6x^2+8x+1$	4	1125
1299600812	$x^8-2x^7-6x^6+10x^5+12x^4-13x^3-8x^2+3x+1$	1	1
1317743125	$x^8-x^7-8x^6+7x^5+19x^4-14x^3-12x^2+8x-1$	2	5
1318279381	$x^8-x^7-7x^6+5x^5+14x^4-6x^3-9x^2+x+1$	1	1
1326417388	$x^8-2x^7-6x^6+10x^5+12x^4-13x^3-9x^2+4x+2$	4	2777
1348097653	$x^8-2x^7-6x^6+11x^5+11x^4-17x^3-6x^2+6x+1$	1	1
1358954496	$x^8-8x^6+20x^4-16x^2+1$	4	2048
1359341129	$x^8-8x^6-x^5+18x^4+2x^3-12x^2-x+2$	1	1
1377663125	$x^8-12x^6+33x^4-5x^3-22x^2+5x+1$	4	725
1381875749	$x^8-3x^7-4x^6+14x^5+4x^4-18x^3+x^2+5x-1$	1	1
1391339501	$x^8-3x^7-4x^6+15x^5+4x^4-22x^3+9x-1$	1	1
1405817381	$x^8-9x^6-x^5+20x^4+6x^3-12x^2-7x-1$	1	1
1410504129	$x^8-9x^6-x^5+22x^4+x^3-15x^2-x+1$	4	3981
1410894053	$x^8-2x^7-6x^6+9x^5+12x^4-11x^3-8x^2+3x+1$	1	1
1413480448	$x^8-4x^7-2x^6+16x^5-x^4-16x^3+2x^2+4x-1$	4	2048
1424875717	$x^8-x^7-7x^6+5x^5+15x^4-6x^3-10x^2+x+1$	1	1
1442599461	$x^8-3x^7-4x^6+15x^5+4x^4-21x^3-2x^2+8x+1$	4	7053
1449693125	$x^8-x^7-9x^6+10x^5+20x^4-20x^3-14x^2+11x+1$	2	5
1459172469	$x^8-4x^7-x^6+17x^5-6x^4-21x^3+8x^2+6x-1$	4	1957
1460018125	$x^8-3x^7-5x^6+13x^5+11x^4-14x^3-10x^2+x+1$	4	2525
1462785589	$x^8-2x^7-6x^6+11x^5+10x^4-17x^3-3x^2+6x-1$	1	1
1472275625	$x^8-3x^7-6x^6+19x^5+13x^4-35x^3-12x^2+13x-1$	4	725

Table 5. Nonic totally real fields F with $\delta_F \leq 14$

d_F	f	$[E:\mathbb{Q}]$	d_E
9685993193	$x^9 - 9x^7 + 24x^5 - 2x^4 - 20x^3 + 3x^2 + 5x - 1$	1	1
11779563529	$x^9 - 9x^7 - 2x^6 + 22x^5 + 5x^4 - 17x^3 - 4x^2 + 4x + 1$	1	1
16240385609	$x^9 - x^8 - 9x^7 + 4x^6 + 26x^5 - 2x^4 - 25x^3 - x^2 + 7x + 1$	3	49
16440305941	$x^9 - 2x^8 - 9x^7 + 11x^6 + 28x^5 - 18x^4 - 34x^3 + 8x^2 + 13x + 1$	3	229
16898785417	$x^9 - 2x^8 - 7x^7 + 11x^6 + 18x^5 - 17x^4 - 19x^3 + 6x^2 + 7x + 1$	1	1
16983563041	$x^9 - x^8 - 8x^7 + 7x^6 + 21x^5 - 15x^4 - 20x^3 + 10x^2 + 5x - 1$	3	361
17515230173	$x^9 - 4x^8 - 3x^7 + 29x^6 - 26x^5 - 24x^4 + 34x^3 - 2x^2 - 5x + 1$	3	49
18625670317	$x^9 - 9x^7 - x^6 + 23x^5 + 4x^4 - 19x^3 - 3x^2 + 4x + 1$	1	1
18756753353	$x^9 - 3x^8 - 4x^7 + 15x^6 + 4x^5 - 22x^4 - x^3 + 10x^2 - 1$	1	1
19936446593	$x^9 - 3x^8 - 5x^7 + 17x^6 + 7x^5 - 30x^4 - x^3 + 16x^2 - 2x - 1$	3	49
20370652633	$x^9 - 2x^8 - 8x^7 + 12x^6 + 15x^5 - 17x^4 - 8x^3 + 8x^2 + x - 1$	1	1

References

1. Julián Aguirre, Mikel Bilbao, and Juan Carlos Peral, *The trace of totally positive algebraic integers*, Math. Comp. **75** (2006), no. 253, 385–393.
2. K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no. 219, 1213–1237.
3. Manjul Bhargava, *Gauss composition and generalizations*, Algorithmic number theory (ANTS V, Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, 1–8.
4. Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Math., vol. 193, Springer-Verlag, New York, 2000.
5. Henri Cohen and Francisco Diaz y Diaz, *A polynomial reduction algorithm*, Sém. Théor. Nombres Bordeaux (2) **3** (1991), no. 2, 351–360.
6. Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *A table of totally complex number fields of small discriminants*, Algorithmic number theory (ANTS III, Portland, Oregon, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, 381–391.
7. Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *Constructing complete tables of quartic fields using Kummer theory*, Math. Comp. **72** (2003), no. 242, 941–951.
8. Henry Cohn and Noam Elkies, *New upper bounds on sphere packings I*, Ann. Math. **157** (2003), 689–714.
9. J.H. Conway and N.J.A. Sloane, *Sphere packings, lattices and groups*, 3rd. ed., Grund. der Math. Wissenschaften, vol. 290, Springer-Verlag, New York, 1999.
10. Jesús De Loera, Raymond Hemmecke, Jeremiah Tauzer, and Ruriko Yoshia, *Effective lattice point counting in rational convex polytopes*, J. Symbolic Comput. **38** (2004), no. 4, 1273–1302.
11. Jesús De Loera, *LattE: Lattice point Enumeration*, 2007, `http://www.math.ucdavis.edu/~latte/`.
12. Jordan S. Ellenberg and Akshay Venkatesh, *The number of extensions of a number field with fixed degree and bounded discriminant*, Ann. of Math. (2) **163** (2006), no. 2, 723–741.

13. U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), no. 170, 463–471.
14. Farshid Hajir and Christian Maire, *Tamely ramified towers and discriminant bounds for number fields*, Compositio Math. **128** (2001), no. 1, 35–53.
15. Farshid Hajir and Christian Maire, *Tamely ramified towers and discriminant bounds for number fields. II.*, J. Symbolic Comput. **33** (2002), no. 4, 415–423.
16. *Number field tables*, `ftp://megrez.math.u-bordeaux.fr/pub/numberfields/`.
17. Klüners-Malle, *A database for number fields*, `http://www.math.uni-duesseldorf.de/~klueners/minimum/minimum.html`.
18. Jürgen Klüners and Gunter Malle, *A database for field extensions of the rationals*, *LMS J. Comput. Math.* **4** (2001), 182–196.
19. M. Kreuzer and H. Skarke, *PALP: A Package for Analyzing Lattice Polytopes*, 2006, `http://hep.itp.tuwien.ac.at/~kreuzer/CY/CYpalp.html`.
20. A.K. Lenstra, H.W. Lenstra, L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534.
21. D.D. Long, C. Maclachlan, A.W. Reid, Arithmetic Fuchsian groups of genus zero, *Pure Appl. Math. Q.* **2** (2006), no. 2, 569–599.
22. Gunter Malle, The totally real primitive number fields of discriminant at most 10^9, *Algorithmic number theory*, *Lecture Notes in Comput. Sci.*, vol. 4076, Springer, Berlin, 2006, 114–123.
23. Jason Martin, *Improved bounds for discriminants of number fields*, submitted.
24. Jacques Martinet, *Petits discriminants des corps de nombres*, Number theory days (Exeter, 1980), *London Math. Soc. Lecture Note Ser.*, vol. 56, Cambridge Univ. Press, Cambridge-New York, 1982, 151–193.
25. Jacques Martinet, Tours de corps de classes et estimations de discriminants, *Invent. Math.* **44** (1978), 65–73.
26. Jacques Martinet, Methodes geométriques dans la recherche des petitis discriminants, *Sem. Théor. Nombres* (1983–1984), Birkhäuser-Boston, 147–179.
27. 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** (1990), no. 1, 119–141.
28. The PARI Group, *PARI/GP* (version 2.3.2), Bordeaux, 2006, `http://pari.math.u-bordeaux.fr/`.
29. Michael Pohst, *On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields*, J. Number Theory **14** (1982), no. 1, 99–117.
30. X.-F. Roblot, *Totally real fields with small root discriminant*, `http://math.univ-lyon1.fr/~roblot/tables.html`.
31. William Stein, *SAGE Mathematics Software* (version 2.8.12), The SAGE Group, 2007, `http://www.sagemath.org/`.
32. C.J. Smyth, *The mean values of totally real algebraic integers*, Math. Comp. **42** (1984), no. 166, 663–681.
33. Kisao Takeuchi, *Totally real algebraic number fields of degree 9 with small discriminant*, Saitama Math. J. **17** (1999), 63–85.
34. Jan Verschelde, *Algorithm 795: PHCpack: A general-purpose solver for polynomial systems by homotopy continuation*, ACM Transactions on Mathematical Software **25** (1999), no. 2, 251–276.
35. John Voight, *Totally real number fields*, `http://www.cems.uvm.edu/~voight/nf-tables/`.