Timing Analysis of Targeted Hunter Searches

John W. Jones[1] and David P. Roberts[2]

[1] Department of Mathematics, Arizona State University, Box 871804
Tempe, AZ 85287
jj@asu.edu

[2] Department of Mathematics, Hill Center, Rutgers University
New Brunswick, NJ 08903
davrobts@math.rutgers.edu

Abstract. One can determine all primitive number fields of a given degree and discriminant with a finite search of potential defining polynomials. We develop an asymptotic formula for the number of polynomials which need to be inspected which reflects both archimedean and non-archimedean restrictions placed on the coefficients of a defining polynomial.

Several authors have used Hunter's theorem to find a defining polynomial

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbf{Z}[x]$$

for each primitive degree n field of absolute discriminant D less than or equal to some cutoff Δ. The method requires a computer search over all vectors $(a_1, \ldots, a_n)$ satisfying certain bounds.

In [JR1] we explained that one is sometimes particularly interested in the fields with $D = \Delta$, especially when all primes dividing D are very small. To find just these fields by a Hunter search, one imposes not only archimedean inequalities on the a_i as above, but also p-adic inequalities for each prime p dividing D. This is an example of a *targeted* search, the target being D.

In this paper we investigate the *search volume* of such Hunter searches, which approximates the number of polynomials one is required to inspect. We find that these search volumes have the form

$$\begin{aligned} \text{Search Volume}_n(D \leq \Delta) &= C(n,\infty)\Delta^{(n+2)/4} \\ \text{Search Volume}_n(D = \Delta) &= \left(\prod_{p^d || D} C\left(n,p^d\right)\right) C(n,\infty)\Delta^{(n-2)/4} \quad . \end{aligned}$$

In Section 1 we work over $\mathbf{R}$. The constant $C(n,\infty)$ is a sum of constants $C\left(n,\infty^d\right)$, one for each possible signature $r+2d=n$. We identify the constant $C\left(n,\infty^0\right)$ using a Selberg integral; the remaining integrals are harder and we evaluate them in the cases $n \leq 7$.

In Sections 2 and 3 we work over $\mathbf{Q}_p$. The constant $C\left(n,p^d\right)$ is a sum of constants $C\left(n,p^d,K\right)$, one for each possible p-adic completion K with discriminant

p^d. Evaluating $C\left(n, p^d, K\right)$ requires evaluating an Igusa integral. We evaluate a few cases exactly and get a reasonable simple upper bound in all cases.

In Sections 4 and 5 we work over $\mathbf{Q}$. Section 4 describes Hunter's theorem and gives an asymptotic formula for the number of defining polynomials of a degree n algebra within a given search radius. In Section 5 we prove the above search volume formulas, and discuss how our results apply in practice.

We have carried out all targeted searches for $n \leq 5$, and D of the form $p^a q^b$ with p and q primes ≤ 19. Complete tables are available at [J1]. Our computations here show that the enormously harder case $n = 6$ is feasible too. Search results will appear at [J1] as they become available.

We now fix some notation. Let F be a field of characteristic zero; typically $F = \mathbf{Q}$ or one of its completions $\mathbf{Q}_v$ in this paper. We work with finite dimensional F-algebras K. Here, all algebras are assumed to be separable. So, K factors canonically as a product of fields, $K = \prod K_i$.

We will work with monic degree n polynomials

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in F[x] \ .$$

Often we think of such polynomials as simply elements $(a_1, \ldots, a_n)$ of F^n. If $f(x)$ is separable, then we call $f(x)$ a defining polynomial for the F-algebra $K = F[x]/f(x)$. The factorization $K = \prod K_i$ is induced by the factorization $f(x) = \prod f_i(x)$ into irreducibles, via $K_i = F[x]/f_i(x)$.

Conversely, let K be an algebra and $y \in K$. Let $f_y(x)$ be the characteristic polynomial of y acting on K by multiplication. Basic algebraic facts about the map $c : K \to F^n$ defined by $y \mapsto f_y$ underlie many of our considerations. For example, c induces a surjection

$$(\text{Regular elements of } K) \to (\text{Defining polynomials for } K)$$

with $\mathrm{Aut}(K)$ acting freely and transitively on the fibers. This accounts for the presence of $|\mathrm{Aut}(K)|$ in many formulas.

If $f(x) = \prod_{i=1}^n (x - y_i)$ we put $D(f) = \prod_{i<j} (y_i - y_j)^2$ and think of D as a polynomial function of the a_j, as usual. Finally, if $F \subseteq \mathbf{C}$ we let $T_2(f) = \sum_{i=1}^n |y_i|^2$.

1 Archimedean Volumes

Let A be a degree n algebra over $\mathbf{R}$. So, we can simply take $A = \mathbf{R}^r \times \mathbf{C}^d$ for some $r + 2d = n$. The characteristic polynomial of $y \in A$ is

$$f_y(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in \mathbf{R}[x] \ .$$

Let A^0 be the set of elements of A with trace 0, and consider the corresponding space of polynomials

$$P^0(A, r) = \left\{ f_y \in \mathbf{R}[x] \ : \ y \in A^0 \text{ and } T_2(f_y) \leq r^2 \right\} \ .$$

We measure the volume of $P^0(A, r)$ with respect to the usual volume form $da_2 \cdots da_n$.

Proposition 1.1.

$$\mathrm{vol}(P^0(A,r)) = \mathrm{vol}(P^0(A,1))\ r^{(n+2)(n-1)/2}$$

Proof. One has a linear map

$$\begin{aligned} L\colon P^0(A,1) &\to P^0(A,r) \\ (a_2,\ldots,a_n) &\mapsto (r^2 a_2,\ldots,r^n a_n)\ . \end{aligned}$$

The Jacobian of this map is r to the power

$$\sum_{j=2}^{n} j = \frac{(n+2)(n-1)}{2}\ .$$

□

This simple observation is the most important point in analyzing Hunter searches.

We work more generally with

$$\zeta_A(s) := \int_{P^0(A,1)} |D|^{s-\frac{1}{2}}\ da_2\cdots da_n\ .$$

The desired volume $\mathrm{vol}(P^0(A,1))$ is just the special value $\zeta_A(1/2)$. A general formula for $\zeta_A(s)$ would be desirable, since it would give one the moments of the polynomial discriminants encountered in a Hunter search. For example, to compute the average polynomial discriminant encountered one needs the number $\zeta_A(3/2)$, as well as $\zeta_A(1/2)$.

Let $A^0(1)$ be the unit ball in A^0; it is a degree $|\mathrm{Aut}(A)|$ cover of $P^0(A,1)$ via the characteristic polynomial map c. One can pull back the defining integral to $A^0(1)$; at this step the Jacobian $|D|^{1/2}$ enters the integrand. One can next extend the integral to the full unit ball $A(1)$. Using the homogeneity of the integrand, one can replace the sharp radial cutoff $\rho \le 1$ by an integral over all of A against a Gaussian $e^{-\rho^2/2}$. The net result is

$$\zeta_A(s) = \frac{2^{n(s-ns-1)/2}}{|\mathrm{Aut}(A)|\ \sqrt{\pi n}\ \left(\dfrac{(ns+1)(n-1)}{2}\right)!} \int_A e^{-\rho^2/2}|D|^s\omega\ .$$

Here ω is the standard volume form on A, giving the unit ball $\rho \le 1$ its usual volume $\pi^{n/2}/(n/2)!$. Also $|\mathrm{Aut}(\mathbf{R}^r \times \mathbf{C}^d)| = r!d!2^d$.

Proposition 1.2.

$$\mathrm{vol}(P^0(\mathbf{R}^n,1)) = \frac{2^{-n(n-5)/4}\prod_{j=1}^{n}(j/2)!}{n!\sqrt{\pi n}\left(\dfrac{(n+2)(n-1)}{4}\right)!}$$

Proof. In the case $A = \mathbf{R}^n$ the roots $y_1,\ldots,y_n$ are coordinates on A and $\omega = dy_1 \cdots dy_n$. A special case of Selberg's integral is

$$\int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} e^{-r^2/2} |D|^s \, dy_1 \cdots dy_n = (2\pi)^{n/2} \prod_{j=1}^{n} \frac{(js)!}{s!} \ ;$$

see e.g. [M1], 17.6.7. Evaluating at $s = 1/2$ this becomes $2^{3n/2} \prod_{j=1}^{n} (j/2)!$, yielding the proposition. □

Proposition 1.3. *The ratios* $\mathrm{vol}(P^0(\mathbf{R}^r \times \mathbf{C}^d, 1))/\mathrm{vol}(P^0(\mathbf{R}^n, 1))$ *for* $n \leq 7$ *are as follows.*

$d \backslash n$	3	4	5	6	7
0	1	1	1	1	1
1	5	18	58	179	543
2		9	$134\frac{1}{3}$	1355	11875
3				$451\frac{2}{3}$	$17466\frac{1}{3}$

Proof. Let

$$I = \prod_{1 \leq i < j \leq n} (y_i - y_j)$$

be the indicated square root of D. We need to compute

$$\int_{\mathbf{R}^r \times \mathbf{C}^d} e^{-\rho^2/2} |I| \, \omega \ .$$

Taking $y_{r+1}, \ldots, y_{r+d}$ as coordinates on $\mathbf{C}^d$ and writing $y_k = (u_k + iv_k)/\sqrt{2}$ one has

$$\rho^2 = \sum_{j=1}^{r} y_j^2 + \sum_{k=1}^{d} (u_k^2 + v_k^2)$$

$$\omega = dy_1 \cdots dy_r \, du_1 \cdots du_d \, dv_1 \cdots dv_d$$

$$|I| = f(y_1, \ldots, y_r, u_1, \ldots, u_d, v_1, \ldots, v_d) \prod_{1 \leq i < j \leq r} |y_i - y_j| \prod_{k=1}^{d} |v_k|$$

with f a polynomial. One can expand f and integrate out the u_k's and the v_k's using

$$\int_0^{\infty} e^{-x^2/2} x^j \, dx = 2^{(j-1)/2} \left(\frac{j-1}{2} \right)!$$

$2d$ times on each term. One is left with an integral of the form

$$\int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} e^{-(y_1^2 + \ldots + y_r^2)/2} \left(\prod_{1 \leq i < j \leq r} |y_i - y_j| \right) g(y_1, \ldots, y_r) \, dy_1 \cdots dy_r$$

with $g(y_1, \ldots, y_r)$ a symmetric polynomial in the y_i. Here the absolute values pose a problem. For $r \leq 3$ this obstruction can be surmounted in an elementary way and one can again integrate term-by-term. When $d = 1$ the moment formulas in [M1], Section 17.8 suffice. This covers all cases with $n \leq 7$. □

The case of cubics $f(x) = x^3 + a_2x + a_3$ is illustrative. The two regions $P^0(A, 1)$ are shown in Figure 1. In the case $A = \mathbf{R} \times \mathbf{C}$, let $r^2 = y_1^2 + |y_2|^2 + |y_3|^2$

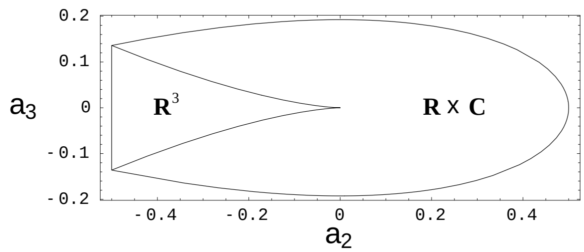

Fig. 1. The sets $P^0(A, 1)$ for cubics $f(x) = x^3 + a_2x + a_3$

and express the real root y_1 as rt. Then the defining integral for $\zeta_{\mathbf{R}\times\mathbf{C}}(s)$ can be evaluated by changing variables from (a_2, a_3) to $0 \le r \le 1$, $-\sqrt{2/3} \le t \le \sqrt{2/3}$. The result is

$$\zeta_{\mathbf{R}\times\mathbf{C}}(s) = \frac{\sqrt{\pi}\, 2^{-s-1} 3^{2s-\frac{1}{2}} (s-1/2)!}{(1+3s)\; s!}\; {}_2F_1\left(-2s, \frac{1}{2}+s; 1+s; \frac{2}{3}\right) \quad .$$

The presence of the hypergeometric function ${}_2F_1$ indicates that the general $\zeta_{\mathbf{R}^r\times\mathbf{C}^d}(s)$ is more complicated than the general $\zeta_{\mathbf{R}^n}(s)$.

2 Ultrametric Masses

The set of isomorphism classes of degree n algebras A over $\mathbf{Q}_p$ is much more complicated than in the archimedean case $v = \infty$. A starting point for analyzing this set is a mass formula, due to Krasner and Serre [S1]. Here is a quick summary, more details being contained in [R2].

The mass of A is by definition $m_A := 1/|\operatorname{Aut}(A)|$. Let $\mathbf{Q}_p^{\text{un}}$ be a maximal unramified extension of $\mathbf{Q}_p$ and put $A^{\text{un}} = A \otimes \mathbf{Q}_p^{\text{un}}$. Call two algebras A_1 and A_2 geometrically equivalent if $A_1^{\text{un}} \cong A_2^{\text{un}}$. Then, the sum of m_A over A in a geometric equivalence class is 1.

Let m_{n,p^d} be the sum of m_A over all totally ramified A of degree n and discriminant p^d. Then, in the tame case $p \nmid n$, the only non-vanishing m_{n,p^d} is $m_{n,p^{n-1}} = 1$. The first few wild cases are shown in Table 1. Other wild cases are more complicated, but are also governed by the Krasner-Serre mass formula $\sum_d m_{n,p^d}\, p^{n-1-d} = 1$.

The general case reduces to the totally ramified case just summarized. Given A, from the canonical factorization $A^{\text{un}} = \prod A_i^{\text{un}}$ one gets an unordered collection of (n_i, d_i). The sum of m_A over algebras A giving rise to these (n_i, d_i) is $\prod m_{n_i,p^{d_i}}$. In particular, the degree partition $\lambda_A = (n_1, n_2, \ldots)$ is a complete geometric invariant of a tame algebra.

Table 1. Masses for low degree wildly ramified algebras

$$m_{p,p^d} = \begin{cases} p-1 & \text{if } p \le d \le 2p-2 \\ p & \text{if } d = 2p-1 \\ 0 & \text{else} \end{cases}$$

d	$m_{4,2^d}$	$m_{6,2^d}$	$m_{6,3^d}$
4	1		
5			
6	2	1	2
7			2
8	4	2	
9	4		6
10	4	4	6
11	8	8	9

Let $M(n, p^d)$ be the sum of m_A over all p-adic algebras with degree n and discriminant p^d. The above discussion is sufficient for computing $M(n, p^d)$ for $n \le 7$. The integers $M(n, p^d)$ appear in Corollary 3.3 and also the table in Section 5.

3 Ultrametric Volumes

Let A be a degree n algebra over $\mathbf{Q}_p$, with ring of integers $\mathcal{O}$, and discriminant p^{d_A}. Define

$$P(A) = \{f_y(x) \in \mathbf{Z}_p[x] : y \in \mathcal{O}\} \ .$$

We measure volumes with $da_1 \cdots da_n$, so that all of $\mathbf{Z}_p^n$ gets volume 1.

Proposition 3.1. *With $Z_A(t)$ as defined in the proof below,*

(i) $\mathrm{vol}(P(A)) = \dfrac{Z_A(1/p)}{|\operatorname{Aut}(A)|\ p^{d_A}}$

(ii) $Z_A(1/p) \le 1$.

Proof. Let ω be Haar measure on A, normalized so that $\omega(\mathcal{O}) = 1$. We use the characteristic polynomial map $c\colon \mathcal{O} \to P(A)$. Pulled back to $\mathcal{O}$, the polynomial discriminant function D factors as $p^{d_A} I^2$. Here, I is a polynomial function on $\mathcal{O}$ with $\mathbf{Z}_p$ coefficients. Note, $\mathbf{Z}_p[y]$ has index $1/|I(y)|_p$ in $\mathcal{O}$.

The Jacobian function $c^*(da_1 \cdots da_n)/\omega$ is $p^{-d_A}|I|_p$. On regular elements, i.e. elements on which I is non-zero, c has degree $\operatorname{Aut}(A)$. So

$$\begin{aligned} \zeta_A(s) := \int_{P(A)} |D|_p^{s-\frac{1}{2}}\ da_1 \cdots da_n &= \frac{1}{|\operatorname{Aut}(A)|} \int_{\mathcal{O}} |p^{d_A} I^2|_p^{s-\frac{1}{2}}\ p^{-d_A}\ |I|_p\ \omega \\ &= \frac{1}{|\operatorname{Aut}(A)|\ p^{d_A(\frac{3}{2}-s)}} \int_{\mathcal{O}} |I|_p^{2s}\ \omega \\ &= \frac{Z_A(p^{-2s})}{|\operatorname{Aut}(A)|\ p^{d_A(\frac{3}{2}-s)}} \ . \end{aligned}$$

Here we have defined

$$Z_A(t) = \sum_{j=0}^{\infty} \omega(\mathcal{O}[j]) t^j$$

with $\mathcal{O}[j]$ the set of $y \in \mathcal{O}$ with $|I(y)|_p = 1/p^j$. Plugging in $s = 1/2$ gives part (i).

To prove part (ii), we note that $Z_A(t)$ is a power series with positive coefficients such that $Z_A(1) = \omega(\mathcal{O}) = 1$. It is an increasing function on $[0,1]$ and so $Z_A(1/p) \leq 1$. □

The function $Z_A(t)$ is an example of an Igusa zeta function [D1]. Thus, it is known to be in $\mathbf{Q}(t)$.

Proposition 3.1 and its proof make no reference to the classification of p-adic algebras sketched in Section 2. Define

$$P(\lambda) = \bigcup_{\lambda_A = \lambda} P(A)$$
$$P(n, p^d) = \bigcup_{d_A = d} P(A) \ .$$

Summing over A with $\lambda_A = \lambda$ in Proposition 3.1 and using the Krasner-Serre mass formula gives Corollary 3.2 below. Summing over A with $d_A = d$ in Proposition 3.1 and using the definition of $M(n, p^d)$ gives Corollary 3.3.

Corollary 3.2. *For λ a partition of n,*

$$\mathrm{vol}(P(\lambda)) \leq \frac{1}{p^{n-\ell(\lambda)}} \ .$$

where $\ell(\lambda)$ denotes the length of λ.

Corollary 3.3. *For $d \in \mathbf{Z}_{\geq 0}$,*

$$\mathrm{vol}\left(P\left(n, p^d\right)\right) \leq \frac{M(n, p^d)}{p^d} \ .$$

On the other hand, one can also prove Corollary 3.2 directly, using neither the Krasner-Serre mass formula, nor Proposition 3.1.

Direct proof of Corollary 3.2. Write $\lambda = (\lambda_1, \ldots, \lambda_{\ell(\lambda)})$, with each $\lambda_i > 0$. Let $P(\lambda)_1 \subset \mathbf{F}_p^n$ be the reduction of $P(\lambda) \subset \mathbf{Z}_p^n$. For e a positive integer, let μ_e be the number of i such that $\lambda_i = e$. Very simply,

$$P(\lambda)_1 = \left\{ \prod_e f_e(x)^e \right\}$$

where $f_e(x) \in \mathbf{F}_p[x]$ is monic of degree μ_e. To give an element of $P(\lambda)_1$ is to give the coefficients of the f_e. There are $\sum \mu_e = \ell(\lambda)$ coefficients, and so $P(\lambda)_1$ is $p^{\ell(\lambda)}/p^n$ of $\mathbf{F}_p^n$. □

It would be nice to compute $Z_A(1/p)$ exactly. To do this it seems necessary to compute all of $Z_A(t)$. We have succeeded when n is prime and A is a field; the results in the unramified case U and the totally ramified case R are

$$Z_U(t) = \frac{1 - \dfrac{1}{p^{n-1}}}{1 - \dfrac{t^{n(n-1)/2}}{p^{n-1}}} \qquad Z_R(t) = \frac{\left(1 - \dfrac{1}{p}\right)\left(1 - \dfrac{t^{(n-1)^2/2}}{p^{n-1}}\right)}{\left(1 - \dfrac{t^{(n-1)/2}}{p}\right)\left(1 - \dfrac{t^{n(n-1)/2}}{p^{n-1}}\right)} .$$

We have also computed several more difficult $Z_A(t)$, sometimes directly, and sometimes making use of the stationary phase formula [D1], Theorem 3.4. The resulting formulas are quite complicated.

4 The Search Set

Let K be a degree n algebra over $\mathbf{Q}$ with absolute discriminant D. With respect to the quadratic form T_2, one has an orthogonal decomposition $K = K^0 \oplus \mathbf{Q}$, K^0 being the subspace of traceless elements.

Let $\mathcal{O}$ be the ring of integers in K. Let $\mathcal{O}'$ be the projection of $\mathcal{O}$ to K^0. As a lattice in the Euclidean space $K^0 \otimes \mathbf{R}$, $\mathcal{O}'$ has covolume $\sqrt{D/n}$.

Let g_m be the smallest real number so that every lattice in Euclidean space $\mathbf{R}^m$ with covolume V has a non-zero vector of length $\leq (g_m V^2)^{1/(2m)}$. The value of g_m is known ([CS1], Table 1.2) for $m \leq 8$.

m	1	2	3	4	5	6	7	8
g_m	1	$1\frac{1}{3}$	2	4	8	$21\frac{1}{3}$	64	256

In the literature one often sees Hermite's constant $\gamma_m = \sqrt[m]{g_m}$ instead of g_m.

Define

$$r_D = \left(\frac{g_{n-1} D}{n}\right)^{1/(2n-2)} .$$

One gets immediately that in $\mathcal{O}'$ there is a non-zero vector y' of length $\leq r_D$. The subalgebra $\mathbf{Q}(y')$ of K strictly contains $\mathbf{Q}$; so if K is a primitive field, $\mathbf{Q}(y')$ is automatically all of K.

Henceforth in this paper we take $n \geq 3$ to avoid trivialities. By replacing y' by $-y'$ one can assume that $a_3' \geq 0$ in its characteristic polynomial. As j varies from 0 to $n-1$, exactly one of $y = y' - j/n$ is in $\mathcal{O}$. This element y has characteristic polynomial $f_y \in P(r_D)$; here the *search set* $P(r)$ is the set of polynomials

$$f(x) = \prod_{i=1}^{n} (x - y_i) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in \mathbf{Z}[x]$$

satisfying the two conditions

(*i*) trace condition:

$$a_1 \in \{0, \ldots, n-1\} \text{ and } a_3 \geq \frac{(n-2)a_1 a_2}{n} - \frac{(n-1)(n-2)a_1^3}{3n^2}$$

(*ii*) length condition:

$$T_2(f) \leq \frac{a_1^2}{n} + r^2 \ .$$

Proposition 4.1. *Let K be a degree n algebra over $\mathbf{Q}$ with absolute discriminant D. Let $m(K, \Delta)$ be the number of defining polynomials for K in $P(r_\Delta)$.*

(*i*) *If K is a primitive field and $D \leq \Delta$, then $m(K, \Delta) \geq 1$.*
(*ii*) *For general K,*

$$m(K, \Delta) \sim \frac{m_n}{|\operatorname{Aut}(K)|} \sqrt{\frac{\Delta}{D}} \quad \text{with} \quad m_n = \frac{\sqrt{g_{n-1}}\ \pi^{(n-1)/2}}{2\left(\frac{n-1}{2}\right)!}$$

as $\Delta \to \infty$.

Proof. Part (*i*) is essentially Hunter's theorem, see e.g. [C1], Theorem 6.4.1. It is proved by our discussion above. Our trace condition is a modification of the standard one. We make this modification in order to fully exploit the involution $y' \mapsto -y'$, thereby making $|P(r)|$ as small as possible.

For Part (*ii*), let $\mathcal{O}'_{\Delta,+}$ be the subset of $\mathcal{O}'$ consisting of elements y' with length $\leq r_\Delta$ and $a_3' \geq 0$. Let $\mathcal{O}'_{\text{reg},\Delta,+}$ be the subset of $\mathcal{O}'_{\Delta,+}$ consisting of regular elements. Then

$$\begin{aligned} |\operatorname{Aut}(K)|\ m(K, \Delta) = |\mathcal{O}'_{\text{reg},\Delta,+}| \sim |\mathcal{O}'_{\Delta,+}| &\sim \frac{(\text{Volume of ball of radius } r_\Delta)}{2\ (\text{Covolume of } \mathcal{O}')} \\ &= \frac{(r_\Delta \sqrt{\pi})^{n-1} / \left(\frac{n-1}{2}\right)!}{2\sqrt{D/n}} = \frac{\sqrt{g_{n-1}}\pi^{(n-1)/2}}{2\left(\frac{n-1}{2}\right)!} \sqrt{\frac{\Delta}{D}} \end{aligned}$$

as $\Delta \to \infty$. □

Part (*ii*) relates to the phenomenon that searches tend to find several defining polynomials for each primitive field sought, as well as defining polynomials for non-primitive fields. For $3 \leq n \leq 9$ one has

n	3	4	5	6	7	8	9
m_n	1.8	3.0	4.9	7.4	11.9	18.9	32.5

to one decimal place.

5 Timing Analysis

To incorporate targeting into the formalism, let S be a finite set of places of $\mathbf{Q}$ containing ∞. For $v \in S$, let A_v be a degree n algebra over $\mathbf{Q}_v$. Let

$$P(\{A_v\}, r) = \{f(x) \in P(r) : \mathbf{Q}_v[x]/f(x) \cong A_v \text{ for } v \in S\} \ .$$

From Proposition 4.1, $P(\{A_v\}, r_\Delta)$ contains a defining polynomial for every primitive degree n field K with absolute discriminant $D \leq \Delta$ and $K_v \cong A_v$, $v \in S$.

Proposition 5.1.

$$|P(\{A_v\}, r_\Delta)| \sim \frac{n}{2} \left(\frac{g_{n-1}}{n}\right)^{(n+2)/4} \mathrm{vol}(P^0(A_\infty, 1)) \left(\prod_p \mathrm{vol}(P(A_p))\right) \Delta^{(n+2)/4}$$

as $\Delta \to \infty$.

Proof. For elements in $P(\{A_\infty\}, r_\Delta)$ there are n possible values of a_1, each giving asymptotically the same number of polynomials; this accounts for the factor n. Those with $a_1 = 0$ are the intersection of the standard lattice $\mathbf{Z}^{n-1}$ with the interior of the region $P^0(A_\infty, r_\Delta)_+$ in $\mathbf{R}^{n-1}$. The $+$ indicates the extra condition $a_3 \geq 0$, and accounts for the 2 in the denominator. Proposition 1.1 and the definition of r_Δ account for the factor $\mathrm{vol}(P^0(A_\infty, r_\Delta)) = (g_{n-1}\Delta/n)^{(n+2)/4}\mathrm{vol}(P^0(A_\infty, 1))$. Finally the ultrametric conditions account for the extra factors $\mathrm{vol}(P(A_p))$. □

The deeper Propositions 1.2 and 1.3 determine the archimedean volumes for $n \leq 7$; Proposition 3.1 bounds the ultrametric volumes in general.

Proposition 5.1 is an asymptotic formula. However one would expect, and experience shows, that it applies well when Δ is simply the product of the discriminants of the A_p's. In this restricted context, and summing over p-adic algebras with a given discriminant, the formula can be restated as follows. Define

$$C(n, \infty^d) = \frac{n}{2} \left(\frac{g_{n-1}}{n}\right)^{(n+2)/4} \mathrm{vol}\left(P^0(\mathbf{R}^{n-2d} \times \mathbf{C}^d, 1)\right)$$
$$C(n, p^d) = \mathrm{vol}\left(P\left(n, p^d\right)\right) p^d \ .$$

Then, *a Hunter search for all primitive fields of signature* $(n - 2d_\infty, d_\infty)$ *and absolute discriminant* $\prod p^{d_p}$ *requires inspection of approximately*

$$C(n, \infty^{d_\infty}) \prod_p C(n, p^{d_p}) p^{d_p(n-2)/4}$$

polynomials. (Naturally there are no such fields unless $(-1)^{d_\infty} \prod p^{d_p}$ is congruent to 0 or 1 modulo 4. If $n = 6$, some searches can be replaced by easier searches via sextic twinning [R1].)

In the literature there are several methods which allow one to implement the length inequality and target the local algebra at ∞ with little loss [BFP1],

[SPD1], [O1], [DO1]. In principal, p-adic bounds on the a_i giving only the slight loss $C(n, p^d) \leq M(n, p^d)$ of Corollary 3.3 are easy to describe since they amount to collections of congruences on the a_i. For example, in the tame case one can follow the direct proof of Corollary 3.2. In practice, for large p and/or n it can become unwieldy to implement sharp p-adic bounds as well.

Table 2 below gives what we call local difficulty ratings, namely the numbers $\log_{10}(C(n, \infty^d))$ and $\log_{10}(M(n, p^d)p^{d(n-2)/4})$. All entries are rounded to the nearest tenth. The rows labelled *All* give totals for all values of d.

Table 2. Local Difficulty Ratings

d	∞	2	3	5	7	11	13	∞	2	3	5	7	11	13
0	−3.1			**Quartics**				−5.3			**Quintics**			
1	−1.9	–	0.2	0.3	0.4	0.5	0.6	−3.5	–	0.4	0.5	0.6	0.8	0.8
2	−2.2	0.6	0.5	1.0	1.1	1.3	1.4	−3.1	0.8	0.7	1.3	1.6	1.9	2.0
3		0.8	1.2	1.0	1.3	1.6	1.7		1.0	1.6	1.9	2.2	2.6	2.8
4		0.9	1.3						1.5	2.1	–	2.5	3.1	3.3
5		1.1	1.7						1.7	2.5	3.2			
6		1.7							2.1	2.6	3.7			
7		–							–		4.3			
8		1.8							2.4		4.8			
9		2.0							2.6		5.4			
10		2.1							2.9					
11		2.6							3.4					
All	*−1.7*	*2.9*	*1.9*	*1.4*	*1.5*	*1.8*	*1.9*	*−3.0*	*3.6*	*3.0*	*5.5*	*2.7*	*3.3*	*3.5*
0	−8.1			**Sextics**				−11.4			**Septics**			
1	−5.9	–	0.5	0.7	0.8	1.0	1.1	−8.7	–	0.6	0.9	1.1	1.3	1.4
2	−5.0	0.9	1.0	1.7	2.0	2.4	2.5	−7.3	1.1	1.2	2.0	2.4	2.9	3.1
3	−5.5	1.2	2.0	2.6	3.0	3.6	3.8	−7.2	1.4	2.4	3.1	3.6	4.4	4.7
4		1.9	2.7	3.1	3.9	4.6	4.9		2.2	3.2	4.0	4.8	5.8	6.2
5		2.1	3.1	4.2	4.2	5.2	5.6		2.5	3.9	5.1	5.8	7.0	7.4
6		2.8	3.8	4.8					3.4	4.7	6.2	–	7.8	8.4
7		2.7	4.1	5.5					3.5	5.2	7.0	8.2		
8		3.5	4.8	6.2					4.3	5.9	7.9	9.2		
9		3.9	5.4	7.0					4.6	6.4	8.8	10.3		
10		4.1	5.9						5.0	7.1	9.4	11.3		
11		4.8	6.2						5.6	7.5		12.4		
12		4.7							5.7			13.5		
13		5.1							6.3			14.6		
14		5.4							6.5					
All	*−4.8*	*5.7*	*6.4*	*7.1*	*4.4*	*5.3*	*5.7*	*−6.9*	*6.8*	*7.7*	*9.5*	*14.6*	*7.9*	*8.4*

The translation from search volumes to search times requires that one incorporate a number of practical concerns as well. All told, one can expect that a degree n search with difficulty x will take longer than a degree $n-1$ search with difficulty x. For our current programs, in degrees 5 and 6 on a medium speed personal computer, the translation from volumes to times goes as follows.

For quintics, searches with difficulty rating x take us about $10^{x-7.9}$ days. For example, the search for all $2^{11}3^6 5^9$ quintics has difficulty rating $-3.0 + 3.4 + 2.6 + 5.4 = 8.4$ and took $10^{0.5} \approx 3$ days.

For sextics, searches with difficulty rating x take us about $10^{x-7.3}$ days. For example, the search for all primitive $2^{14}5^9$ sextics has difficulty rating $-4.8 + 5.4 + 7.0 = 7.6$ and took around $10^{0.3} \approx 2$ days.

In [JR1] we found all sextic fields ramified within $S = \{\infty, 2, 3\}$. Table 2 shows that a few other $\{\infty, p, q\}$ are easier, while harder cases like $\{\infty, 3, 5\}$ are feasible too.

References

[BFP1] Buchmann, J., Ford, D., and Pohst, M., *Enumeration of quartic fields of small discriminant*, Math. Comp. **61** (1993) 873–879.

[C1] Cohen, H.: A Course in Computational Algebraic Number Theory, GTM **138** Springer Verlag, 1995.

[CS1] Conway, J. and Sloane, N.: Sphere Packings, Lattices, and Groups, Springer Verlag, 1988.

[D1] Denef, J.: *Report on Igusa's local zeta function*, Séminaire Bourbaki 741, Astérisque **201-202-203**, 359–386.

[DO1] Diaz y Diaz, F. and Olivier, M., *Imprimitive ninth-degree number fields with small discriminants*, Math. Comp. **64** (1995) 305–321.

[J1] Jones, J.: *Tables of number fields with prescribed ramification*, a WWW site, `http://math.la.asu.edu/~jj/numberfields`

[JR1] Jones, J. and Roberts, D.: *Sextic number fields with discriminant* $-^j 2^a 3^b$, to appear in the Proceedings of the Fifth Conference of the Canadian Number Theory Association.

[M1] Mehta, M.: Random Matrices, 2nd edition, Academic Press, 1991.

[O1] Olivier, M., *The computation of sextic fields with a cubic subfield and no quadratic subfield*, Math. Comp. **58** (1992) 419–432.

[R1] Roberts, D.: *Twin sextic algebras*, to appear in Rocky Mountain J. Math.

[R2] Roberts, D.: *Low degree p-adic fields*, in preparation.

[S1] Serre, J.-P.: *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **286** (1978), no. 22, A1031-A1036.

[SPD1] Schwarz, A., Pohst, M., and Diaz y Diaz, F.: *A table of quintic number fields*, Math. Comp. **63** (1994) 361–376.