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

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbf{Z}[x]$$

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

$$\text{Search Volume}_n(D \leq \Delta) = C(n,\infty)\Delta^{(n+2)/4}$$

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

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 $C(n, p^d, K)$ 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

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

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