MATHEMATICS OF COMPUTATION
Volume 78, Number 266, April 2009, Pages 1109–1117
S 0025-5718(08)02178-9
Article electronically published on August 22, 2008

A TARGETED MARTINET SEARCH

ERIC D. DRIVER AND JOHN W. JONES

Abstract. Constructing number fields with prescribed ramification is an important problem in computational number theory. In this paper, we consider the problem of computing all imprimitive number fields of a given degree which are unramified outside of a given finite set of primes S by combining the techniques of targeted Hunter searches with Martinet's relative version of Hunter's theorem. We then carry out this algorithm to generate complete tables of imprimitive number fields for degrees 4 through 10 and certain sets S of small primes.

An important problem in the study of fields is to determine all number fields of a fixed degree having a prescribed ramification structure. This paper will focus on finding all imprimitive number fields of a given degree unramified outside of a finite set of primes.

Hunter's theorem has been used extensively for computing all primitive number fields of a given degree with absolute discriminant below a given bound. In [13], Martinet gives a version of Hunter's theorem suitable for relative extensions which has been used to carry out similar searches for imprimitive fields [4, 5, 16, 17, 18, 19]. Note, however, that for even modest degree fields and small sets of primes, such as $S = \{2, 3\}$, using a standard Hunter search to find all fields unramified outside S can become computationally burdensome. This can be ameliorated by carrying out a targeted Hunter search where one searches for all fields with specific discriminants, but only those possible for fields unramified away from S. This approach was introduced in [6] and refined in [7] to determine all sextic and septic fields with $S = \{2, 3\}$, respectively. It has subsequently been used to investigate fields of degrees 8 and 9 ramified at a single prime in [11, 12].

In this paper, we combine Martinet's theorem with the targeted search technique to form what we call a *targeted Martinet search*. We then demonstrate the algorithm by using it to compute complete tables of imprimitive decic fields with prescribed ramification.

Section 1 describes the process of conducting a number field search based on Martinet's theorem. The size of the relative extensions considered in applications here are larger than those in the literature. Section 2 describes how targeting can be used with a search described in Section 1, with details on combining congruences and archimedean bounds given in Section 3. Finally, Section 4 summarizes the results of several searches carried out using the methods in this paper.

Received by the editor August 20, 2007 and, in revised form, May 13, 2008.
2000 *Mathematics Subject Classification.* Primary 11Y40; Secondary 11-04.

1. Martinet's theorem and Archimedean bounds

If K is a number field, $\mathcal{O}_K$ will be its ring of integers and $d_K \in \mathbb{Z}$ will denote its discriminant. Hermite's constant for j-dimensional lattices will be denoted γ_j.

A standard approach to computing complete tables of degree n extensions of $\mathbb{Q}$ with discriminant $|d_K| \leq B$ for some bound B is to use Hunter's theorem. This approach is only guaranteed to find all primitive extensions, i.e., those with no intermediary fields. We will be interested in imprimitive extensions and will make use of Martinet's generalization of Hunter's theorem for relative extensions [13].

Theorem 1 (Martinet)**.** *Let K be a number field of degree m over $\mathbb{Q}$ and let L be a finite extension of K of relative degree $n = [L : K]$. Let $\sigma_1, \ldots, \sigma_m$ denote the embeddings of K into $\mathbb{C}$. Then there exists $\alpha \in \mathcal{O}_L - \mathcal{O}_K$ such that*

$$\sum_{i=1}^{mn} |\alpha_i|^2 \leq \frac{1}{n} \sum_{j=1}^{m} |\sigma_j(\mathrm{Tr}_{L/K}(\alpha))|^2 + \gamma_{m(n-1)} \left(\frac{|d_L|}{n^m |d_K|} \right)^{1/m(n-1)},$$

where the α_i's are the conjugates of α. Furthermore, α can be chosen arbitrarily modulo addition by elements of $\mathcal{O}_K$ and also modulo multiplication by roots of unity in $\mathcal{O}_K$.

We will use the notation in Martinet's theorem for the remainder of this paper. We also use the standard notation $T_2(\alpha) := \sum_{i=1}^{mn} |\alpha_i|^2$.

1.1. Archimedean bounds.

Let $\alpha \in \mathcal{O}_L - \mathcal{O}_K$ be the element given by Martinet's theorem and let $f_{\alpha,K}(x) \in \mathcal{O}_K[x]$ be the characteristic polynomial for α over K. We write

$$f_{\alpha,K}(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

where each $a_i \in \mathcal{O}_K$. If $\omega_1, \omega_2, \ldots, \omega_m$ is an integral basis for $K/\mathbb{Q}$, then we may write $a_i = \sum_{j=1}^{m} a_{ij} \omega_j$ where each $a_{ij} \in \mathbb{Z}$. When working with a_i in this basis, we will denote the column vector $(a_{i1}, \ldots, a_{im})^T$ by $\vec{a}_i$. Note that

$$\langle \vec{a}_i, \vec{a}_i \rangle = \sum_{j=1}^{m} |\sigma_j(a_i)|^2$$

is a positive definite quadratic form on $\vec{a}_i$. Here, we will mainly report on upper bounds for $\langle \vec{a}_i, \vec{a}_i \rangle$. More details can be found in [4, 10, 16, 17].

For the coefficient a_1, one can shift the components so that $-\lfloor \frac{n-1}{2} \rfloor \leq a_{1j} \leq \lfloor \frac{n}{2} \rfloor$ for each j and $0 \leq a_{11} \leq \lfloor \frac{n}{2} \rfloor$. If a_{11} through a_{1k} are all zero, we may normalize the next coefficient $0 \leq a_{1,k+1} \leq \lfloor \frac{n}{2} \rfloor$. Finally, whenever $m = 2$ we observe that any search with a given a_1 is the equivalent to one that uses the Galois conjugate of a_1, so we may remove any a_1 from our list of candidates whose Galois conjugate is already on the list. A short table of explicit values for a_1 can be found in [10, §2.1] for degree $[L : \mathbb{Q}] = mn \leq 10$.

Once the value for a_1 has been fixed, we have an exact numerical value for Martinet's bound:

$$T_2(\alpha) \leq C_{a_1} := \frac{1}{n} \sum_{j=1}^{m} |\sigma_j(a_1)|^2 + \gamma_{m(n-1)} \left(\frac{|d_L|}{n^m |d_K|} \right)^{1/m(n-1)}.$$

It may be possible to replace a_1 with an equivalent element for which $\sum_{j=1}^{m} |\sigma_j(a_1)|^2$ is smaller, and hence gives a more efficient bound C_{a_1}. This improvement was

incorporated into Martinet-type searches for nonics in [5]. In the most interesting case here, namely when the base field is quadratic (i.e. $m = 2$), it is not hard to prove that the values for a_1 given in [10] are already optimal in this regard.

For the constant coefficient a_n, there is a standard bound derived from the arithmetic/geometric mean inequality, yielding

$$\langle \vec{a}_n, \vec{a}_n \rangle \leq \left(\frac{C_{a_1}}{n} \right)^n. \tag{1}$$

To bound the other coefficients, we first bound the power sum $s_k = \sum_{j=1}^n \alpha_j^k$, and then inductively use Newton's formula to get bounds on a_k. The power sums s_k satisfy

$$\langle \vec{s}_k, \vec{s}_k \rangle \leq C_{a_1}^k. \tag{2}$$

Given a_i and s_i for $i \in \{1, 2, \ldots, k-1\}$, set $\vec{b} = -\sum_{j=1}^{k-1} a_{k-j} s_j$. Then the coefficient a_k satisfies the relation

$$\vec{a}_k = \frac{1}{k}(\vec{b} - \vec{s}_k).$$

1.2. **The method of Pohst.** It is possible to improve the bounds on s_k when $k \geq 3$ based on a method of M. Pohst [15]. Define

$$T_k := \sum_{j=1}^n |\alpha_j|^k,$$

where the α_j's are the roots of $f_{\alpha,K}$. Clearly, $|s_k| \leq T_k$. Suppose that a_n has been fixed and let t_2 be a bound for T_2. The method of Pohst uses Lagrange multipliers to minimize the bounds on T_k ($3 \leq k \leq n-1$) subject to the constraints that $\sum_{j=1}^n |\alpha_j|^2 \leq t_2$ and $\prod_{j=1}^n |\alpha_j| = |a_n|$. A more detailed description can be found in [3, p. 458].

In carrying out number field searches based on Martinet's theorem, there is little need for better bounds on the s_k when $n = 2$ or 3. The only other case in the literature is where $n = 4$, in which case Pohst's theorem is applied to the degree mn polynomial $\mathrm{Norm}_{K/\mathbb{Q}}(f_{\alpha,K})$ (see e.g., [17]). Here, the need for good archimedean bounds was more pressing for the $n = 5$ cases under consideration. We find it useful to apply Pohst's theorem to both the degree mn polynomial and individually to $f_{\alpha,K}$ and its conjugates. We explain the derivation of the latter bounds below.

For the i-th conjugate polynomial of $f_{\alpha,K}$, we define

$$T_k^{(i)} := \sum_{j=1}^n |\sigma_{ij}(\alpha)|^k \qquad (1 \leq i \leq m).$$

In order to get a bound $t_2^{(\ell)}$ for $T_2^{(\ell)}$, we use the Martinet bound to give us

$$T_2^{(\ell)} = \sum_{j=1}^n |\sigma_{\ell j}(\alpha)|^2 \leq C_{a_1} - \sum_{\substack{i=1 \\ i \neq \ell}}^m \sum_{j=1}^n |\sigma_{ij}(\alpha)|^2. \tag{3}$$

Next, from the arithmetic/geometric mean inequality we have

$$\sum_{j=1}^n |\sigma_{ij}(\alpha)|^2 \geq n \left[\prod_{j=1}^n |\sigma_{ij}(\alpha)|^2 \right]^{1/n} = n|\sigma_i(a_n)|^{2/n}.$$

Substituting this into (3), we finally get

$$T_2^{(\ell)} \leq C_{a_1} - n \sum_{\substack{i=1 \\ i \neq \ell}}^{m} |\sigma_i(a_n)|^{2/n}.$$

Now let $t_k^{(i)}$ be the bound for $T_k^{(i)}$ obtained by applying the method of Pohst to the ith conjugate polynomial; we then have $|\sigma_i(s_k)| \leq t_k^{(i)}$. Combining these bounds together we get

$$\langle \vec{s}_k, \vec{s}_k \rangle = \sum_{i=1}^{m} |\sigma_i(s_k)|^2 \leq \sum_{i=1}^{m} \left[t_k^{(i)} \right]^2.$$

2. Targeting

For the number field K, if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ we denote the completion of K by $K_\mathfrak{p}$, and p the prime below $\mathfrak{p}$. Then $\mathcal{O}_\mathfrak{p}$ will denote the ring of integers of $K_\mathfrak{p}$ and $\mathcal{P}_\mathfrak{p}$ the maximal ideal of $\mathcal{O}_\mathfrak{p}$. The factorization $\mathfrak{p}\mathcal{O}_L$ will be denoted $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ and f_i will denote the residue field degrees. Notations for completions $L_\mathfrak{P}$ are analogous to those for K described above. Finally, if S is our set of integral primes, then we let S_K denote the set of prime ideals of $\mathcal{O}_K$ which lie above some $p \in S$.

Fix a prime ideal $\mathfrak{p} \in S_K$. Then the decomposition $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ corresponds to the decomposition of the local algebra

$$L \otimes_K K_\mathfrak{p} \cong \prod_{i=1}^{g} L_{\mathfrak{P}_i}. \tag{4}$$

At the finest level, a local target for $\mathfrak{p}$ can be a candidate for $L \otimes_K K_\mathfrak{p}$, a separable degree n algebra over $K_\mathfrak{p}$. For practical reasons, we typically consider larger targets. For the searches in Section 4, our targets consisted of unordered collections of triples (e_i, f_i, c_i) representing the ramification indices, residue field degrees, and discriminant exponents of the extensions $L_{\mathfrak{P}_i}/K_\mathfrak{p}$. Note, however, that in all cases, a local target provides sufficient information to determine the $\mathfrak{P}$-part of d_L. Combining this for all primes dividing d_K and primes in S gives d_L for applying Martinet's theorem. Then, larger targets, such as all extensions where the relative extension is unramified outside S, can then be searched by searching a series of smaller targets.

As in Section 1, $f_{\alpha,K}$ denotes the characteristic polynomial of α over K where $L = K(\alpha)$. Then $f_{\alpha,K}$ factors into irreducibles over $\mathcal{O}_{K_\mathfrak{p}}$ as $f_{\alpha,K} = h_1 \cdots h_g$ which correspond to the factorization of $L \otimes_K K_\mathfrak{p}$ in equation (4). Moreover, since α is integral over $\mathcal{O}_K$, each h_i has coefficients in $\mathcal{O}_{K_\mathfrak{p}}$. For congruences derived from this factorization, we note that for all k, we have $f_{\alpha,K} \equiv \tilde{h}_1 \cdots \tilde{h}_g \pmod{\mathfrak{p}^k}$ where we may take each $\tilde{h}_i \in \mathcal{O}_K[x]$ because $\mathcal{O}_K$ is dense in $\mathcal{O}_{K_\mathfrak{p}}$. The basic process is to simply compute congruences for the $\tilde{h}_i$ modulo $\mathfrak{p}^k$, and then multiply these polynomials to obtain congruences for $f_{\alpha,K}$ modulo $\mathfrak{p}^k$.

Let $\Gamma \subseteq \mathcal{O}_K$ be a complete set of representatives for $\mathcal{O}_K/\mathfrak{p}$ with $1 \in \Gamma$. Then we immediately have

$$h_i \equiv r_i^{e_i} \pmod{\mathcal{P}_{K_\mathfrak{p}}} \tag{5}$$

where r_i is a degree f_i monic polynomial with coefficients in Γ.

For tamely ramified primes, equation (5) suffices. When the ramification is wild, however, the congruences given by equation (5) can be improved significantly by working modulo a power of $\mathcal{P}_{K_\mathfrak{p}}$. We use Ore congruences as in [7]. We illustrate the general situation with an example.

Consider the case of a cubic extension where we have $e = p = 3$ and $f = 1$. Let ρ be a uniformizer for $K_\mathfrak{p}$, and let π be a uniformizer for $L_\mathfrak{P}$. Let e_0 be the ramification index of $\mathcal{P}_{K_\mathfrak{p}}$ over $p\mathbb{Z}_p$, so that $\nu_\pi(p) = 3e_0$. The minimal polynomial for π over $K_\mathfrak{p}$ is Eisenstein, so it can be written

$$f_\pi(x) = x^3 + \rho^{k_1}Ax^2 + \rho^{k_2}Bx + \rho C \in K_\mathfrak{p}[x],$$

where A, B, $C \in \mathcal{O}_{K_\mathfrak{p}}$. If we let d denote the exponent of $\mathcal{P}_{L_\mathfrak{P}}$ in $\mathcal{D}(L_\mathfrak{P}/K_\mathfrak{p})$, then

$$\begin{aligned} d &= \nu_\pi(f'_\pi(\pi)) \\ &= \nu_\pi(3\pi^2 + 2\rho^{k_1}A\pi + \rho^{k_2}B) \\ &= \min\{\nu_\pi(3\pi^2), \nu_\pi(2\rho^{k_1}A\pi), \nu_\pi(\rho^{k_2}B)\} \\ &= \min\{3e_0 + 2, 3k_1 + \nu_\pi(A) + 1, 3k_2 + \nu_\pi(B)\}. \end{aligned}$$

It is easy to see that we can always take $1 \le k_1 \le k_2 \le e_0 + 1$. Thus, we would work modulo $\mathfrak{p}^{k_2}$.

The coefficients of the characteristic polynomial for any $\beta \in \mathcal{P}_{L_\mathfrak{P}}$ will satisfy the same divisibility conditions as the coefficients of f_π; and any element $\beta \in \mathcal{O}_{L_\mathfrak{P}}$ is a translate by some $\gamma \in \Gamma$ of an element in $\mathcal{P}_{L_\mathfrak{P}}$. Therefore, the corresponding local factor h_i will take the form

$$\begin{aligned} h_i &= (x+\gamma)^3 + \rho^{k_1}A(x+\gamma)^2 + \rho^{k_2}B(x+\gamma) + \rho C \\ &\equiv (x+\gamma)^3 + \rho^{k_1}A(x+\gamma)^2 + \rho C \pmod{\mathcal{P}_{K_\mathfrak{p}}^{k_2}} \end{aligned}$$

for some $A, B, C \in \mathcal{O}_{K_\mathfrak{p}}$ and some $\gamma \in \Gamma$. We then write A and C as power series in ρ with coefficients from Γ to obtain explicit congruences.

3. Algorithm implementation

The bounds derived earlier take the form

$$\langle \vec{a}, \vec{a} \rangle \le B \tag{6}$$

for a positive definite quadratic form $\langle\,,\rangle$ where B is a positive real number and the column vector $\vec{a} = (a_1, \ldots, a_m)^T \in \mathbb{Z}^m$ represents the element $a = \sum_{i=1}^m a_i\omega_i$ which is either a polynomial coefficient or a power sum.

Explicitly, if $Q = [\sigma_i(\omega_j)]_{ij}$, then $\langle \vec{a}, \vec{a} \rangle = \vec{a}^{\,T}Q^HQ\vec{a}$ where Q^H denotes the conjugate transpose of Q and $\vec{a}^{\,T}$ is simply the transpose of $\vec{a}$. Since $\vec{a} \in \mathbb{Z}^m$ and $\langle \vec{a}, \vec{a} \rangle$ are real, let A be the matrix of real parts of Q^HQ, and our bound (6) becomes $\vec{a}^{\,T}A\vec{a} \le B$.

To get efficient bounds on the components of $\vec{a}$, we use the Cholesky decomposition of the quadratic form associated to A as in [2], section 2.7.3. In our applications, the lattice has very small dimension, so we used a simple approach to enumerating short vectors in the lattice. With larger lattices, one might use Fincke-Pohst instead.

Now, suppose we want to find elements $a = \sum_{i=1}^m a_i\omega_i \in \mathcal{O}_K$ which are congruent to $c = \sum_{i=1}^m c_i\omega_i \in \mathcal{O}_K$ modulo the ideal $\mathfrak{a}$. The ideal $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank

$m = [K : \mathbb{Q}]$, so there exist $\mu_j \in \mathcal{O}_K$ such that

$$\mathfrak{a} = \mu_1\mathbb{Z} + \mu_2\mathbb{Z} + \cdots + \mu_m\mathbb{Z}.$$

Each μ_j may be written $\mu_j = \sum_{i=1}^{m} \mu_{ij}\omega_i$ where $\mu_{ij} \in \mathbb{Z}$. We choose our basis for $\mathfrak{a}$ so that the matrix $M = (\mu_{ij})$ is in Hermite normal form.

Now if $a \equiv c \pmod{\mathfrak{a}}$, then $a - c \in \mathfrak{a}$ which implies

$$\begin{aligned}\sum_{i=1}^{m} a_i\omega_i - \sum_{i=1}^{m} c_i\omega_i &= k_1\mu_1 + \cdots + k_m\mu_m \\ &= k_1\sum_{i=1}^{m}\mu_{i1}\omega_i + \cdots + k_m\sum_{i=1}^{m}\mu_{im}\omega_i\end{aligned}$$

for some $k_i \in \mathbb{Z}$. Equating the coefficients of the ω_i's, we get the following matrix equation:

$$\vec{a} = M\vec{k} + \vec{c}.$$

Now define $\vec{k}' = \vec{k} + M^{-1}\vec{c}$. Then

$$\vec{a} = M(\vec{k} + M^{-1}\vec{c}) = M\vec{k}'.$$

We now use the bound on $\vec{a}$ to give bounds on the k_i's. From equation (6) we get

$$(\vec{k}')^{T}(QM)^{H}(QM)\vec{k}' \le B.$$

As before, there exists an auxiliary matrix A such that $(\vec{k}')^{T}A\vec{k}' \le B$ and A is a positive definite real symmetric matrix. Using the Cholesky decomposition for A we can enumerate small vectors $\vec{k}'$, i.e., those satisfying $\langle\vec{k}', \vec{k}'\rangle_A \le B$ for the positive definite quadratic form given by A. If we write these bounds as $L_i' \le k_i' \le U_i'$, then we get the following bounds on the k_i's,

$$\lceil L_i' - c_i'\rceil \le k_i \le \lfloor U_i' - c_i'\rfloor$$

where $\vec{c}\,' = M^{-1}\vec{c}$. We will write these bounds as $L_i \le k_i \le U_i$. Note that the bounds L_i and U_i depend on the current values of $k_{i+1}, \ldots, k_m$. So to obtain all values for $\vec{k}$, we first loop over the range for k_m. The current value for k_m is used to get looping bounds for k_{m-1}. Then the current values for k_m and k_{m-1} are used to get looping bounds for k_{m-2}, and so on.

The search algorithm loops over all combinations of the k_i's, and for each combination, computing $\vec{a} = M\vec{k} + \vec{c}$. Observe that the bounds on the k_i's are smaller than the bounds on the a_i's so that the search region has been reduced. This is analogous to the one-dimensional case where one considers all elements a such that $a = c + kp$ (here $\mu_1 = p$ is the modulus of the congruence vector). If the archimedean bounds are $|a| < B$, then $k = \frac{a-c}{p}$ so that $\frac{-B-c}{p} \le k \le \frac{B-c}{p}$.

The above method is modified slightly when the bound is on a power sum instead of a polynomial coefficient. Suppose we are interested in the jth ($2 \le j \le n-1$) polynomial coefficient and we have the following bound on the jth power sum:

$$\langle\vec{s_j}, \vec{s_j}\rangle \le B.$$

From Newton's formula, we may write

$$j\vec{a_j} = \vec{b_j} - \vec{s_j}$$

where $\vec{b_j} = -\sum_{i=1}^{j-1} a_{j-i}s_i \in \mathbb{Z}^m$.

If we define

$$\vec{c}\,' := \frac{1}{j} M^{-1}(\vec{b_j} - j\vec{c})$$

and

$$\vec{k}' := \vec{c}\,' - \vec{k},$$

then we have

$$\begin{aligned} \vec{s_j} &= \vec{b_j} - j\vec{a_j} \\ &= \vec{b_j} - j(M\vec{k} + \vec{c}) \\ &= jM\left[\frac{1}{j} M^{-1}(\vec{b_j} - j\vec{c}) - \vec{k}\right] \\ &= jM\vec{k}'. \end{aligned}$$

The bound on $\vec{s_j}$ can now be used to get a bound on $\vec{k}'$:

$$\langle \vec{s_j}, \vec{s_j} \rangle = (jM\vec{k}')^H Q^H Q (jM\vec{k}') = j^2 (\vec{k}')^T (QM)^H (QM)\vec{k}'$$

$$\implies \quad \langle \vec{k}', \vec{k}' \rangle_{QM} = \frac{1}{j^2} \langle \vec{s_j}, \vec{s_j} \rangle \leq \frac{B}{j^2}.$$

As before, there exists an auxiliary matrix A such that $\langle \vec{k}', \vec{k}' \rangle_A \leq \frac{B}{j^2}$ and A is a positive definite real symmetric matrix. The rest of the algorithm remains the same.

4. Applications

The targeted Martinet search was used to construct complete tables of imprimitive number fields with prescribed ramification. We did this for degrees 4, 6, 8, 9, and 10; the results of which can be found on our websites [8, 9]. The algorithm was programmed in C using the pari library [14].

The web site [8] contains results of Hunter searches for sextic fields which were known to be complete for all Galois groups except for $C_3^2 : C_4$ and $C_3^2 : D_4$. In [6], the search for sextic fields with $S = \{2, 3\}$ was shown complete for these groups by class field theory. Using the methods of this paper, the tables were proven complete for 33 other values of S.

In this section, we consider the specific case of degree 10 fields unramified outside the set $S = \{2, 3\}$. The search was done in two parts. The first part did a search for quadratic extensions of a quintic base field, and the second part searched for quintic extensions of a quadratic base field.

The results of our quadratic over quintic search are summarized in Table 1, where the fields are sorted by Galois group. Searches involving quadratic extensions are inherently easier than quintic extensions. This is a relatively simple computation, so we completed this search in two ways, by targeted Martinet searches as described above, and by class field theory. We note that computing quadratic extensions of quintic fields by Martinet searches has appeared previously in the literature (see [18, 19]). Class field theory is especially easy to apply in this situation because it just entails taking square roots of the appropriate elements of quintic fields. This is simplified further by the fact that we are allowing ramification above 2, and that the 6 quintic base fields all have narrow class number one. This search took roughly 1.5 hours by a targeted Martinet search and 10 seconds by class field theory using a script written for `gp` [14].

TABLE 1. All decics unramified outside $S = \{2, 3\}$ and having a quintic subfield.

T_4	T_5	T_{12}	T_{22}	T_{24}	T_{25}	T_{29}	T_{37}	T_{38}	T_{39}	Total
1	6	5	30	7	7	42	91	91	546	826

Table 2 gives the results for the much more difficult quintic over quadratic search. The data is sorted vertically by quadratic base field, and horizontally by Galois group. The results are complete for all 7 of the quadratic base fields which are unramified outside $\{2, 3\}$. Run times for the first 6 base fields varied from 25 hours for the $\mathbb{Q}(\sqrt{-3})$ case to 30 days for the $\mathbb{Q}(\sqrt{2})$ case. Run times are heavily dependent on the discriminant of the base field. For the last base field $\mathbb{Q}(\sqrt{6})$, we decided to use a distributed computing approach using BOINC [1]. We found a dozen volunteer host machines, including a dual Clovertown (8 cores) and a pair of quad-core Xeon servers. The $\mathbb{Q}(\sqrt{6})$ case was finally settled after about 60 days of hard-core processing. The total processing time summed over all host machines was 41216 hours (4.7 years), justifying the need for a distributed computing approach.

TABLE 2. All decics unramified outside $S = \{2, 3\}$ and having a quadratic subfield, $\mathbb{Q}(\sqrt{d})$ with $d \in \{-1, \pm 2, \pm 3, \pm 6\}$.

K	T_4	T_5	T_{12}	T_{22}	T_{28}	T_{40}	T_{41}	T_{42}	T_{43}	Total
$\mathbb{Q}(\sqrt{-3})$		1		5		1	2		3	12
$\mathbb{Q}(\sqrt{-1})$		1		5			2		6	14
$\mathbb{Q}(\sqrt{2})$	1		2	3	1	4	7	18	31	67
$\mathbb{Q}(\sqrt{-2})$		1		5			5		41	52
$\mathbb{Q}(\sqrt{3})$		1	1	4		4	6		41	57
$\mathbb{Q}(\sqrt{-6})$		1	1	4			2		2	10
$\mathbb{Q}(\sqrt{6})$		1	1	4		3	4		61	74

ACKNOWLEDGEMENTS

We would like to thank all the volunteers who donated the idle time on their cpus, especially Greg Tucker and Bill Brown, whose multi-core servers did more than 90% of the workload. Without these volunteers, the completion of the $\mathbb{Q}(\sqrt{6})$ case would not have been possible (at least for several years).

REFERENCES

[1] BOINC, Berkeley Open Infrastructure for Network Computing. `http://boinc.berkeley.edu`
[2] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, New York, 1996. MR1228206 (94i:11105)
[3] H. Cohen, Advanced Topics in Computational Number Theory, Springer-Verlag, New York, 2000. MR1728313 (2000k:11144)
[4] F. Diaz y Diaz, Petits discriminants des corps de nombres totalement imaginaires de degré 8, J. Number Theory **25** (1987), no. 1, 34–52. MR871167 (88a:11115)
[5] F. Diaz y Diaz and M. Olivier, Imprimitive ninth-degree number fields with small discriminants, Math. Comp. 64 (1995), 305–321. MR1260128 (95c:11153)

[6] J. Jones and D. Roberts, Sextic number fields with discriminant $(-1)^j 2^a 3^b$, in Number Theory: Fifth Conference of the Canadian Number Theory Association, CRM Proceedings and Lecture Notes, 19, American Math. Soc., (1999), 141–172. MR1684600 (2000b:11142)
[7] J. Jones and D. Roberts, Septic number fields with discriminant $\pm 2^a 3^b$, Math. Comp. 72 (2003), 1975-1985. MR1986816 (2004e:11119)
[8] J. Jones, Tables of number fields with prescribed ramification, `http://math.la.asu.edu/~jj/numberfields`
[9] E. Driver, Tables of number fields with prescribed ramification, `http://hobbes.la.asu.edu/Number_Fields/Driver/FieldTables.html`
[10] E. Driver, A Targeted Martinet Search, Ph.D. Thesis, Arizona State University, December 2006.
[11] S. Lesseni, The nonexistence of nonsolvable octic number fields ramified only at one small prime, Math. Comp. **75** (2006), no. 255, 1519–1526 (electronic). MR2219042 (2007d:11121)
[12] S. Lesseni, Nonsolvable nonic number fields ramified only at one small prime, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 617–625. MR2330431
[13] J. Martinet, Méthodes géométriques dans la recherche des petits discriminants, Prog. Math. 59, Birkhäuser, Boston (1985), 147-179. MR902831 (88h:11083)
[14] PARI2, 2000. PARI/GP, Version 2.1.4. The PARI Group, Bordeaux. `http://www.parigp-home.de`
[15] M. Pohst, On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields, J. Number Theory 14 (1982), 99–117. MR644904 (83g:12009)
[16] M. Pohst, J. Martinet, and F. Diaz y Diaz, The minimum discriminant of totally real octic fields, J. Number Theory **36** (1990), no. 2, 145–159. MR1072461 (91g:11128)
[17] S. Selmane, Non-primitive number fields of degree eight and of signature $(2, 3)$, $(4, 2)$ and $(6, 1)$ with small discriminant, Math. Comp. **68** (1999), no. 225, 333–344. MR1489974 (99c:11160)
[18] S. Selmane, Quadratic extensions of totally real quintic fields, Math. Comp. 70 (2000), 837-843. MR1697649 (2001g:11167)
[19] S. Selmane, Tenth degree number fields with quintic fields having one real place, Math. Comp. 70 (2000), 845-851. MR1709158 (2001g:11196)

Department of Mathematics, Arizona State University, Tempe, Arizona 85287-1804
Current address: Lockheed Martin Corporation, P.O. Box 85, Litchfield Park, Arizona 85340

Department of Mathematics, Arizona State University, Tempe, Arizona 85287-1804