An Algorithm in Computational Algebraic Number Theory
Locating Fields of Signature \([p, 0]\) Satisfying a Given Property

Jason B. Hill
University of Colorado at Boulder

De Brún Workshop on Computational Algebra
National University of Ireland, Galway  July 31, 2008
Introduction

First, allow me to say ... 

I don’t claim to be a number theorist (at least not as of today, the 31st of July, 2008 in Galway),
Introduction

First, allow me to say ...

I don’t claim to be a number theorist (at least not as of today, the 31st of July, 2008 in Galway), but I do tend to like creating algorithms to solve challenging problems,
Introduction

First, allow me to say ...

I don’t claim to be a number theorist (at least not as of today, the 31st of July, 2008 in Galway), but I do tend to like creating algorithms to solve challenging problems, such as the problem of creating an opening sentence for my talk that contains twenty a’s, six b’s, eight c’s, six d’s, fifty-two e’s, twelve f’s, eleven g’s, thirteen h’s, twenty-eight i’s, two j’s, three k’s, seventeen l’s, seven m’s, thirty-six n’s, twenty-six o’s, four p’s, one q, fifteen r’s, forty-seven s’s, forty-six t’s, six u’s, nine v’s, nine w’s, seven x’s, twelve y’s, one z, and a single!
Prerequisites and Info

This talk is aimed at those with a “basic” understanding of:

- Field theory: finite extensions of $\mathbb{Q}$.
- Linear algebra: characteristic/minimal polynomials.
- Galois theory: automorphisms of finite extensions.
Prerequisites and Info

This talk is aimed at those with a “basic” understanding of:

- Field theory: finite extensions of $\mathbb{Q}$.
- Linear algebra: characteristic/minimal polynomials.
- Galois theory: automorphisms of finite extensions.

This research was the result of a question posed by David S. Dummit in connection to work by him and others on the proper formulation of a strong variant of Stark’s Conjectures.
Some Notation:

Number Field: A finite extension of \( \mathbb{Q} \). For example, the field \( \mathbb{K} = \mathbb{Q}(\sqrt{2}) \) is a number field of degree 2.

Signature: Let \( \mathbb{K} \) be a number field of degree \( n \) and let \( r \) and \( s \) be the number of real and complex conjugate embeddings of \( \mathbb{K} \), respectively. Then \( n = r + 2s \) and we refer to \( [r, s] \) as the signature of \( \mathbb{K} \).

\( \mathbb{Q}(i) \) has signature \( [0, 1] \).

\( \mathbb{Q}(\sqrt{2}) \) has signature \( [2, 0] \).

The number field given by the roots of \( x^3 + x^2 - x - 3 \) has signature \( [1, 1] \).
Some Notation:

- **Number Field**: A finite extension of $\mathbb{Q}$. For example, the field $K = \mathbb{Q}(\sqrt{2})$ is a number field of degree 2.
Some Notation:

- **Number Field:** A finite extension of $\mathbb{Q}$. For example, the field $K = \mathbb{Q}(\sqrt{2})$ is a number field of degree 2.

- **Signature:** Let $K$ be a number field of degree $n$ and let $r$ and $s$ be the number of real and complex conjugate embeddings of $K$, respectively. Then $n = r + 2s$ and we refer to $[r, s]$ as the signature of $K$. 
Some Notation:

- **Number Field**: A finite extension of $\mathbb{Q}$. For example, the field $K = \mathbb{Q}(\sqrt{2})$ is a number field of degree 2.

- **Signature**: Let $K$ be a number field of degree $n$ and let $r$ and $s$ be the number of real and complex conjugate embeddings of $K$, respectively. Then $n = r + 2s$ and we refer to $[r, s]$ as the signature of $K$.
  - $\mathbb{Q}(i)$ has signature $[0, 1]$.
  - $\mathbb{Q}(\sqrt{2})$ has signature $[2, 0]$.
  - The number field given by the roots of $X^3 + X^2 - X - 3$ has signature $[1, 1]$. 
Denote the Following:

Given a number field $K$, let
Denote the Following:

Given a number field $K$, let

- $\mathcal{O}_K$ be the ring of algebraic integers in $K$,
Denote the Following:

Given a number field $K$, let

- $\mathcal{O}_K$ be the ring of algebraic integers in $K$,
- $U_K$ be the (multiplicative) unit group of $\mathcal{O}_K$.  

Denote the Following:

Given a number field $K$, let
- $\mathcal{O}_K$ be the ring of algebraic integers in $K$,
- $U_K$ be the (multiplicative) unit group of $\mathcal{O}_K$.
- $d(K)$ be the field discriminant of $K$. (see next slide)
The Discriminant:

Consider a number field $K$ of signature $[r, s]$. 
The Discriminant:

Consider a number field $K$ of signature $[r, s]$.

- $d(K) \in \mathbb{Z}$ is a numerical invariant of $K$. 
The Discriminant:

Consider a number field $K$ of signature $[r, s]$.

- $d(K) \in \mathbb{Z}$ is a numerical invariant of $K$.
- $[r, s]$ determines the sign of $d(K)$. 
The Discriminant:

Consider a number field $K$ of signature $[r, s]$.

- $d(K) \in \mathbb{Z}$ is a numerical invariant of $K$.
- $[r, s]$ determines the sign of $d(K)$.
- $d(K)$ gives information about the arithmetic structure of $\mathcal{O}_K$. In general, a smaller $|d(K)|$ value implies that calculations in $\mathcal{O}_K$ and $U_K$ will be easier.
The Discriminant:

Consider a number field $K$ of signature $[r, s]$.

- $d(K) \in \mathbb{Z}$ is a numerical invariant of $K$.
- $[r, s]$ determines the sign of $d(K)$.
- $d(K)$ gives information about the arithmetic structure of $\mathcal{O}_K$. In general, a smaller $|d(K)|$ value implies that calculations in $\mathcal{O}_K$ and $U_K$ will be easier.
- Hermite: Up to isomorphism, there are only finitely many number fields satisfying any given finite discriminant bound.
As a Consequence:

Thus, given a property $P$ that number fields of signature $[r, s]$ may computationally satisfy, we have one of the following situations:
As a Consequence:

Thus, given a property $P$ that number fields of signature $[r, s]$ may computationally satisfy, we have one of the following situations:

1. A number field $K$ of signature $[r, s]$ having unique smallest (abs. value) discriminant satisfying $P$ exists.
As a Consequence:

Thus, given a property $P$ that number fields of signature $[r, s]$ may computationally satisfy, we have one of the following situations:

1. A number field $K$ of signature $[r, s]$ having unique smallest (abs. value) discriminant satisfying $P$ exists.
2. No number field of signature $[r, s]$ satisfies $P$. 
The Structure of Unit Groups

Given a number field $K$ of signature $[r, s]$:
The Structure of Unit Groups

Given a number field $K$ of signature $[r, s]$:

- If $r + s > 1$ then $|U_K| = \infty$. 
The Structure of Unit Groups

Given a number field $K$ of signature $[r, s]$: 

- If $r + s > 1$ then $|U_K| = \infty$. 
- $\text{Tor}(U_K) \neq \emptyset$. 


The Structure of Unit Groups

Given a number field \( K \) of signature \([r, s]\):

- If \( r + s > 1 \) then \(|U_K| = \infty\).
- \( \text{Tor}(U_K) \neq \emptyset \).
- In fact, \( U_K \) is finitely generated as a \( \mathbb{Z} \)-module and we have the following famous structure theorem:
The Structure of Unit Groups

Given a number field $K$ of signature $[r, s]$:  
- If $r + s > 1$ then $|U_K| = \infty$.  
- $\text{Tor}(U_K) \neq \emptyset$.  
- In fact, $U_K$ is finitely generated as a $\mathbb{Z}$–module and we have the following famous structure theorem:

**Dirichlet’s Unit Theorem:**  

$$U_K \cong \mu(K) \bigoplus \mathbb{Z}^{r+s-1}$$

where $\mu(K)$ is a finite cyclic group generated by the root of unity $\zeta$. We refer to a full set of generators of $U_K$ as a set of fundamental units.
Problem Statement

**Initial Question:** Consider some number field $K$ having signature $[5, 0]$ and fundamental units $\epsilon_0 = -1, \epsilon_1, ..., \epsilon_4$. Is it possible that for $1 \leq i, j \leq 4$

$$|\text{sgn}(\epsilon_i) - \text{sgn}(\sigma \epsilon_i)| = |\text{sgn}(\epsilon_j) - \text{sgn}(\sigma \epsilon_j)|$$

for all $\sigma \in \text{Gal}(K/\mathbb{Q})$? Umm... what??
Problem Statement

**Initial Question:** Consider some number field $K$ having signature $[5, 0]$ and fundamental units $\epsilon_0 = -1, \epsilon_1, \ldots, \epsilon_4$. Is it possible that for $1 \leq i, j \leq 4$

$$|\text{sgn}(\epsilon_i) - \text{sgn}(\sigma \epsilon_i)| = |\text{sgn}(\epsilon_j) - \text{sgn}(\sigma \epsilon_j)|$$

for all $\sigma \in \text{Gal}(K/\mathbb{Q})$? Umm... what??

Let’s restate this in terms that are more computationally adequate. This requires the definition of what we will call *Unit Group Rank*. 

---

An Algorithm in Computational Algebraic Number Theory

- Introduction
- Problem Statement

---

**Problem Statement**

- Initial Question: Consider some number field $K$ having signature $[5, 0]$ and fundamental units $\epsilon_0 = -1, \epsilon_1, \ldots, \epsilon_4$. Is it possible that for $1 \leq i, j \leq 4$

$$|\text{sgn}(\epsilon_i) - \text{sgn}(\sigma \epsilon_i)| = |\text{sgn}(\epsilon_j) - \text{sgn}(\sigma \epsilon_j)|$$

for all $\sigma \in \text{Gal}(K/\mathbb{Q})$? Umm... what??

Let’s restate this in terms that are more computationally adequate. This requires the definition of what we will call *Unit Group Rank*. 

---

10
Definition of Unit Group Rank

Let $K$ be a number field of signature $[p, 0]$ for prime $p$ with fundamental units $\zeta = -1, \epsilon_1, ..., \epsilon_{p-1}$ and embeddings $\sigma_j \in \text{Gal}(\overline{K}/\mathbb{Q})$. Define

$$M_1 = \begin{bmatrix}
\zeta & \epsilon_1 & \cdots & \epsilon_{p-1} \\
|\zeta| & |\epsilon_1| & \cdots & |\epsilon_{p-1}|
\end{bmatrix}
\begin{bmatrix}
\sigma_1(\zeta) & \sigma_1(\epsilon_1) & \cdots & \sigma_1(\epsilon_{p-1}) \\
|\sigma_1(\zeta)| & |\sigma_1(\epsilon_1)| & \cdots & |\sigma_1(\epsilon_{p-1})|
\end{bmatrix}
\begin{bmatrix}
\vdots & \ddots & \vdots \\
|\sigma_{p-1}(\zeta)| & |\sigma_{p-1}(\epsilon_1)| & \cdots & |\sigma_{p-1}(\epsilon_{p-1})|
\end{bmatrix}. $$
Definition of Unit Group Rank

Thus, $M_1$ is a matrix over the multiplicative group of order 2. We define the matrix $M_2$ over the additive group of order 2 as follows. Let

$$M_2(i, j) = \begin{cases} 
0 & \text{if } M_1(i, j) = 1 \\
1 & \text{if } M_2(i, j) = -1
\end{cases}$$
An Algorithm in Computational Algebraic Number Theory

Introduction

Problem Statement

Definition of Unit Group Rank

Thus, $M_1$ is a matrix over the multiplicative group of order 2. We define the matrix $M_2$ over the additive group of order 2 as follows. Let

$$M_2(i,j) = \begin{cases} 
0 & \text{if } M_1(i,j) = 1 \\
1 & \text{if } M_2(i,j) = -1 
\end{cases}$$

The **unit group rank** of the number field $K$ is defined as the (row) rank of $M_2$. 

The Question Becomes: Is it possible for a number field of signature $[5,0]$ to have a unit group rank of 1?
Definition of Unit Group Rank

Thus, $M_1$ is a matrix over the multiplicative group of order 2. We define the matrix $M_2$ over the additive group of order 2 as follows. Let

$$M_2(i, j) = \begin{cases} 
0 & \text{if } M_1(i, j) = 1 \\
1 & \text{if } M_2(i, j) = -1 
\end{cases}$$

The unit group rank of the number field $K$ is defined as the (row) rank of $M_2$.

The Question Becomes: Is it possible for a number field of signature $[5, 0]$ to have a unit group rank of 1?
An Example:

For example, the field $K$ of signature [5, 0] generated by $\alpha$ a root of the polynomial

$$X^5 - 2X^4 - 6X^3 + 8X^2 + 8X + 1$$

has a system of fundamental units given by

$$\zeta = -1,$$
$$\epsilon_1 = \alpha,$$
$$\epsilon_2 = \alpha^2 - 2\alpha,$$
$$\epsilon_3 = \alpha^2 - 2\alpha - 2,$$
$$\epsilon_4 = \alpha^4 - 2\alpha^3 - 6\alpha^2 + 9\alpha + 7.$$
An Example (cont.):

In this case, we find

\[
M_1 = \begin{bmatrix}
-1 & 1 & -1 & 1 & -1 \\
-1 & 1 & -1 & -1 & 1 \\
-1 & 1 & -1 & -1 & 1 \\
-1 & 1 & 1 & -1 & 1 \\
-1 & 1 & 1 & -1 & 1
\end{bmatrix}, \quad M_2 = \begin{bmatrix}
1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 0
\end{bmatrix}.
\]

Therefore, \( K \) has unit group rank 3.
Previously Known:

Previously Known Cases for Unit Group Ranks of Totally Real Quintic Number Fields:
Previously Known Cases for Unit Group Ranks of Totally Real Quintic Number Fields:

- 5: Millions known.
Previously Known:

Previously Known Cases for Unit Group Ranks of Totally Real Quintic Number Fields:

- 5: Millions known.
- 4: Hundreds of thousands known.
Previously Known:

Previously Known Cases for Unit Group Ranks of Totally Real Quintic Number Fields:

- 5: Millions known.
- 4: Hundreds of thousands known.
- 3: Only 2 instances known.
An Algorithm in Computational Algebraic Number Theory

Introduction

Problem Statement

Previously Known:

Previously Known Cases for Unit Group Ranks of Totally Real Quintic Number Fields:

- 5: Millions known.
- 4: Hundreds of thousands known.
- 3: Only 2 instances known.
- 2: No instances known.
Previously Known:

Previously Known Cases for Unit Group Ranks of Totally Real Quintic Number Fields:

- 5: Millions known.
- 4: Hundreds of thousands known.
- 3: Only 2 instances known.
- 2: No instances known.
- 1: No instances known. (Conjectured to not exist.)
Previously Known:

Previously Known Cases for Unit Group Ranks of Totally Real Quintic Number Fields:

- 5: Millions known.
- 4: Hundreds of thousands known.
- 3: Only 2 instances known.
- 2: No instances known.
- 1: No instances known. (Conjectured to not exist.)

Say we could find a totally real quintic number field having a unit group rank of 1. We would like to find the one having the smallest field discriminant.
One possible approach is to use a “table building” technique.

That is, use an existing algorithm to generate an instance of every number field of degree 5 satisfying some discriminant bound. Sort the results by signature and then sort the relevant fields by unit group rank.
Hunter’s Theorem

Hunter’s Theorem: Let $K$ be a number field of degree $n$ over $\mathbb{Q}$ and let $\gamma_n$ be Hermite’s Constant for dimension $n$. Then there exists some $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ with the following properties:
Hunter’s Theorem

**Hunter’s Theorem**: Let $K$ be a number field of degree $n$ over $\mathbb{Q}$ and let $\gamma_n$ be Hermite’s Constant for dimension $n$. Then there exists some $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ with the following properties:

1. If $\sigma_i(\alpha)$ denotes the conjugates of $\alpha$ in $\mathbb{C}$, then

\[
\sum_{i=1}^{n} |\sigma_i(\alpha)|^2 \leq \frac{1}{n} \text{Tr}_{K/\mathbb{Q}}(\alpha)^2 + \gamma_{n-1} \left( \frac{|d(K)|}{n} \right)^{1/(n-1)}
\]
Hunter’s Theorem

Hunter’s Theorem: Let $K$ be a number field of degree $n$ over $\mathbb{Q}$ and let $\gamma_n$ be Hermite’s Constant for dimension $n$. Then there exists some $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ with the following properties:

1. If $\sigma_i(\alpha)$ denotes the conjugates of $\alpha$ in $\mathbb{C}$, then

$$\sum_{i=1}^{n} |\sigma_i(\alpha)|^2 \leq \frac{1}{n} \text{Tr}_{K/\mathbb{Q}}(\alpha)^2 + \gamma_{n-1} \left( \frac{|d(K)|}{n} \right)^{1/(n-1)}$$

2. $0 \leq \text{Tr}_{K/\mathbb{Q}}(\alpha) \leq n/2$. 
Using Hunter’s Theorem:

Hence, suppose a number field $K$ of degree $n$ satisfies $|d(K)| < B$. Then there exists some $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ such that...
Using Hunter’s Theorem:

Hence, suppose a number field $K$ of degree $n$ satisfies $|d(K)| < B$. Then there exists some $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ such that

$$\sum_{i=1}^{n} |\sigma_i(\alpha)|^2 \leq \frac{1}{n} \text{Tr}_{K/Q}(\alpha)^2 + \gamma_{n-1} \left( \frac{|d(K)|}{n} \right)^{1/(n-1)} \leq \frac{n}{4} + \gamma_{n-1} \left( \frac{B}{n} \right)^{1/(n-1)}$$
Using Hunter’s Theorem:

Hence, suppose a number field $K$ of degree $n$ satisfies $|d(K)| < B$. Then there exists some $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ such that

$$
\sum_{i=1}^{n} |\sigma_i(\alpha)|^2 \leq \frac{1}{n} \text{Tr}_{K/Q}(\alpha)^2 + \gamma_{n-1} \left( \frac{|d(K)|}{n} \right)^{1/(n-1)} \leq \frac{n}{4} + \gamma_{n-1} \left( \frac{B}{n} \right)^{1/(n-1)}
$$

If we denote the characteristic polynomial of $\alpha$ by

$$
C_{\alpha,Q}(X) = X^n - a_1 X^{n-1} + \cdots + (-1)^n a_n = \prod_{i=1}^{n} (X - \sigma_i(\alpha)),
$$

then we may use Hunter’s Theorem to start to bound the relevant coefficients.
Using Hunter’s Theorem:

Using elementary symmetric polynomials, the arithmetic–
geometric mean inequality, and some ideas from field theory, we find:

\[ |a_k| \leq \binom{n}{k} \left( \frac{a_1^2}{n} + \gamma_{n-1} \left( \frac{B}{n} \right)^{1/(n-1)} \right)^{k/2}. \]

For the constant term of the characteristic polynomial we find:

\[ |a_n|^{2/n} = \left( \prod_{i=1}^{n} |\sigma_i(\alpha)|^2 \right)^{1/n} \leq \frac{\left( \frac{a_1^2}{n} + \gamma_{n-1} \left( \frac{B}{n} \right)^{1/(n-1)} \right)}{n}. \]
A Lesson in Inefficiency:

For example, to generate an instance of all quintic number fields (up to isomorphism) satisfying the discriminant bound $|d(K)| < 14,642$, we compute all fields given by a root of

$$m_{\alpha, \mathbb{Q}}(X) = X^5 - a_1 X^4 + a_2 X^3 - a_3 X^2 + a_4 X - a_5$$
A Lesson in Inefficiency:

For example, to generate an instance of all quintic number fields (up to isomorphism) satisfying the discriminant bound $|d(K)| < 14,642$, we compute all fields given by a root of

$$m_{\alpha, \mathbb{Q}}(X) = X^5 - a_1 X^4 + a_2 X^3 - a_3 X^2 + a_4 X - a_5$$

where

$$0 \leq a_1 \leq 2, \quad |a_2| \leq 112, \quad |a_3| \leq 374, \quad |a_4| \leq 627 \quad \text{and} \quad |a_5| \leq 7.$$
A Lesson in Inefficiency:

For example, to generate an instance of all quintic number fields (up to isomorphism) satisfying the discriminant bound $|d(K)| < 14,642$, we compute all fields given by a root of

$$m_{\alpha,\mathbb{Q}}(X) = X^5 - a_1 X^4 + a_2 X^3 - a_3 X^2 + a_4 X - a_5$$

where

$$0 \leq a_1 \leq 2, \quad |a_2| \leq 112, \quad |a_3| \leq 374, \quad |a_4| \leq 627 \quad \text{and} \quad |a_5| \leq 7.$$

This results in a list of 9,517,449,375 polynomials.
A Lesson in Inefficiency:

For example, to generate an instance of all quintic number fields (up to isomorphism) satisfying the discriminant bound $|d(K)| < 14,642$, we compute all fields given by a root of

$$m_{\alpha, \mathbb{Q}}(X) = X^5 - a_1 X^4 + a_2 X^3 - a_3 X^2 + a_4 X - a_5$$

where

$$0 \leq a_1 \leq 2, \quad |a_2| \leq 112, \quad |a_3| \leq 374, \quad |a_4| \leq 627 \quad \text{and} \quad |a_5| \leq 7.$$  

This results in a list of 9,517,449,375 polynomials. Many are reducible and can be removed.
A Lesson in Inefficiency:

For example, to generate an instance of all quintic number fields (up to isomorphism) satisfying the discriminant bound $|d(K)| < 14,642$, we compute all fields given by a root of

$$m_{\alpha, \mathbb{Q}}(X) = X^5 - a_1 X^4 + a_2 X^3 - a_3 X^2 + a_4 X - a_5$$

where

$$0 \leq a_1 \leq 2, \quad |a_2| \leq 112, \quad |a_3| \leq 374, \quad |a_4| \leq 627 \quad \text{and} \quad |a_5| \leq 7.$$ 

This results in a list of 9,517,449,375 polynomials. Many are reducible and can be removed. Others result in isomorphic fields and can be removed.
A Lesson in Inefficiency:

For example, to generate an instance of all quintic number fields (up to isomorphism) satisfying the discriminant bound $|d(K)| < 14,642$, we compute all fields given by a root of

$$m_{\alpha,Q}(X) = X^5 - a_1 X^4 + a_2 X^3 - a_3 X^2 + a_4 X - a_5$$

where

$$0 \leq a_1 \leq 2, \quad |a_2| \leq 112, \quad |a_3| \leq 374, \quad |a_4| \leq 627 \quad \text{and} \quad |a_5| \leq 7.$$

This results in a list of 9,517,449,375 polynomials. Many are reducible and can be removed. Others result in isomorphic fields and can be removed. In the end, only one totally real quintic number field results from this list.
Problems with the Table Building Approach:

This approach has two very big problems:
Problems with the Table Building Approach:

This approach has two very big problems:

- Computationally very inefficient: We only wish to spend time analyzing fields of the correct signature.
Problems with the Table Building Approach:

This approach has two very big problems:

- Computationally very inefficient: We only wish to spend time analyzing fields of the correct signature.
- Discriminant bound doesn’t exist: We don’t even know that a field with the property exists, so we have no bound.
Problems with the Table Building Approach:

This approach has two very big problems:

- Computationally very inefficient: We only wish to spend time analyzing fields of the correct signature.
- Discriminant bound doesn’t exist: We don’t even know that a field with the property exists, so we have no bound.

Let’s create an algorithm that solves these problems and:

- Spend no computation time whatsoever on other signatures.
- Requires no discriminant bound. (Once an instance of a field with the signature and property required is found, then we obtain a bound. Until then, develop a method to search with increasing discriminant bounds without repeating calculations.)
A New Approach:

We wish to generate all number fields (up to isomorphism) satisfying an increasing discriminant bound and having signature $[p, 0]$ for prime $p$. For a number field given by a root of $m \alpha, \mathbb{Q}(X) = X^p - a_1X^{p-1} + \cdots + (-1)^p a_p = p \prod_{i=1}^{\sigma_i(\alpha)}$,

Hunter's Theorem tells us how to bound $a_1$ independently of discriminant bounds. We can use some relatively simple calculus for the other coefficients, and then "reverse engineer" the discriminant bound by using Hunter's Theorem.
A New Approach:

- We wish to generate all number fields (up to isomorphism) satisfying an increasing discriminant bound and having signature $[p, 0]$ for prime $p$. 
A New Approach:

- We wish to generate all number fields (up to isomorphism) satisfying an increasing discriminant bound and having signature $[p, 0]$ for prime $p$.

- For a number field given by a root of

$$m_{\alpha, \mathbb{Q}}(X) = X^p - a_1 X^{p-1} + \cdots + (-1)^p a_p = \prod_{i=1}^{p} (X - \sigma_i(\alpha)),$$

Hunter’s Theorem tells us how to bound $a_1$ independently of discriminant bounds.
A New Approach:

- We wish to generate all number fields (up to isomorphism) satisfying an increasing discriminant bound and having signature \([p, 0]\) for prime \(p\).

- For a number field given by a root of

\[
m_{\alpha, \mathbb{Q}}(X) = X^p - a_1 X^{p-1} + \cdots + (-1)^p a_p = \prod_{i=1}^{p} (X - \sigma_i(\alpha)),
\]

Hunter’s Theorem tells us how to bound \(a_1\) independently of discriminant bounds.

- We can use some relatively simple calculus for the other coefficients, and then “reverse engineer” the discriminant bound by using Hunter’s Theorem.
What We Already Know:
What We Already Know:

- For signature $[5, 0]$ fields, we already know $0 \leq a_1 \leq 2$. 

...
What We Already Know:

- For signature [5, 0] fields, we already know $0 \leq a_1 \leq 2$.
- The minimal polynomial in question is of degree 5, with 5 distinct real roots.
What We Already Know:

- For signature $[5, 0]$ fields, we already know $0 \leq a_1 \leq 2$.
- The minimal polynomial in question is of degree 5, with 5 distinct real roots.
- Hence, the first, second and third derivatives of this polynomial are separable with real roots.
What We Already Know:

- For signature $[5, 0]$ fields, we already know $0 \leq a_1 \leq 2$.
- The minimal polynomial in question is of degree 5, with 5 distinct real roots.
- Hence, the first, second and third derivatives of this polynomial are separable with real roots.
- The third derivative is given by

  $$m''_{\alpha, \mathbb{Q}}(\alpha) = 60X^2 - 24a_1X + 6a_2$$

  and will have two real roots precisely when $a_2 < 2a_1^2/5$. 
What We Already Know:

- For signature $[5, 0]$ fields, we already know $0 \leq a_1 \leq 2$.
- The minimal polynomial in question is of degree 5, with 5 distinct real roots.
- Hence, the first, second and third derivatives of this polynomial are separable with real roots.
- The third derivative is given by
  \[
m'''_{\alpha, \mathbb{Q}}(\alpha) = 60X^2 - 24a_1 X + 6a_2
  \]
  and will have two real roots precisely when $a_2 < 2a_1^2/5$.
- In the worst case, we find $a_2 \leq 1$. 
The Main Idea – Heart of the Algorithm:

- We iterate on $a_2$ downward from $a_2 = 1$.
- In each of the cases $a_1 = 0, 1, 2$:
  1. Using the given $a_1$ and $a_2$, integrate $m'''_{\alpha, \mathbb{Q}}(\alpha)$.
  2. Calculate the range of $a_3$ values for which $m''_{\alpha, \mathbb{Q}}(\alpha)$ has only distinct real roots.
  3. The idea is: It can only be pushed up or down so far before a root becomes complex.
  4. Iterate over that range doing the following:
  5. Using the given $a_1, a_2, a_3$, integrate $m''_{\alpha, \mathbb{Q}}(\alpha)$.
  6. Calculate the range of $a_4$ values for which $m'_{\alpha, \mathbb{Q}}(\alpha)$ has only distinct real roots.
  7. Iterate over that range...
The Main Idea – Heart of the Algorithm:

- We iterate on \( a_2 \) downward from \( a_2 = 1 \).
- In each of the cases \( a_1 = 0, 1, 2 \):
  1. Using the given \( a_1 \) and \( a_2 \), integrate \( m'''_{\alpha, \mathbb{Q}}(\alpha) \).
  2. Calculate the range of \( a_3 \) values for which \( m''_{\alpha, \mathbb{Q}}(\alpha) \) has only distinct real roots.
  3. The idea is: It can only be pushed up or down so far before a root becomes complex.
  4. Iterate over that range doing the following:
  5. Using the given \( a_1, a_2, a_3 \), integrate \( m''_{\alpha, \mathbb{Q}}(\alpha) \).
  6. Calculate the range of \( a_4 \) values for which \( m'_{\alpha, \mathbb{Q}}(\alpha) \) has only distinct real roots.
  7. Iterate over that range...
- This results in a “tree” of coefficient values, dependent on (in this order)
  \[ a_2, a_1, a_3, a_4, a_5 \]
Using the Algorithm to Find Fields:

1. Using this "tree" approach, we iterate \( a^2 \) downward until an instance of a field with our property is found. Once located, we use that field's discriminant to calculate the lower bound for \( a^2 \) using Hunter's Theorem, and continue in the same fashion until either 1. That bound is reached. (The field in question is the lowest discriminant field satisfying the signature and property.) or 2. Another field with smaller discriminant is found and we recalculate the \( a^2 \) bound.

We can also use some isomorphism limiting algorithms (e.g., POLREDABS) before calculating number field properties in order to limit repeat calculations.
Using the Algorithm to Find Fields:

- Using this “tree” approach, we iterate $a_2$ downward until an instance of a field with our property is found.
Using the Algorithm to Find Fields:

- Using this “tree” approach, we iterate \( a_2 \) downward until an instance of a field with our property is found.
- Once located, we use that field’s discriminant to calculate the lower bound for \( a_2 \) using Hunter’s Theorem, and continue in the same fashion until either
  1. That bound is reached. (The field in question is the lowest discriminant field satisfying the signature and property.)
  2. Another field with smaller discriminant is found and we recalculate the \( a_2 \) bound.
Using the Algorithm to Find Fields:

- Using this “tree” approach, we iterate $a_2$ downward until an instance of a field with our property is found.
- Once located, we use that field’s discriminant to calculate the lower bound for $a_2$ using Hunter’s Theorem, and continue in the same fashion until either
  1. That bound is reached. (The field in question is the lowest discriminant field satisfying the signature and property.)
  2. Another field with smaller discriminant is found and we recalculate the $a_2$ bound.
- We can also use some isomorphism limiting algorithms (e.g., POLREDABS) before calculating number field properties in order to limit repeat calculations.
Testing the Algorithm

A general form of the algorithm (for signature \([p, 0]\) with \(p\) a prime) was coded in the PARI/GP environment. Given a signature \([p, 0]\) and a property \(P\), the algorithm finds a smallest discriminant field of signature \([p, 0]\) satisfying \(P\).
Testing the Algorithm

- A general form of the algorithm (for signature \([p, 0]\) with \(p\) a prime) was coded in the PARI/GP environment.
A general form of the algorithm (for signature $[p, 0]$ with $p$ a prime) was coded in the PARI/GP environment.

Given a signature $[p, 0]$ and a property $P$, the algorithm finds a smallest discriminant field of signature $[p, 0]$ satisfying $P$. 
Examples:

The following queries were made, results were given and verified in QaoS:
Examples:

The following queries were made, results were given and verified in QaoS:

- The smallest discriminant totally real quintic number field having an abelian Galois group:

  The algorithm terminates at $a_2 = -6$ and finds the unique field having discriminant 14,641:

  $$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$$

  This is the smallest discriminant for any totally real quintic number field.
Testing the Algorithm

The smallest discriminant totally real quintic number field having class number 2:

When $a^2 = -7$, the algorithm returns the field generated by a root of $X^5 - 2X^4 - 7X^3 + 8X^2 + 5X - 1$ with field discriminant 10,940,453. The calculated lower bound for $a^2$ is found to be $-28$.

When $a^2 = -11$, the field given by $X^5 - 11X^3 - 9X^2 + 14X + 9$ with discriminant 4,010,276 is found. The new lower bound for $a^2$ is -22, and no smaller discriminant fields are found.
The smallest discriminant totally real quintic number field having class number 2:

When \( a_2 = -7 \) the algorithm returns the field generated by a root of

\[ X^5 - 2X^4 - 7X^3 + 8X^2 + 5X - 1 \]

with field discriminant 10,940,453. The calculated lower bound for \( a_2 \) is found to be \(-28\).
The smallest discriminant totally real quintic number field having class number 2:

When \( a_2 = -7 \) the algorithm returns the field generated by a root of

\[
X^5 - 2X^4 - 7X^3 + 8X^2 + 5X - 1
\]

with field discriminant 10,940,453. The calculated lower bound for \( a_2 \) is found to be \(-28\). When \( a_2 = -11 \) the field given by

\[
X^5 - 11X^3 - 9X^2 + 14X + 9
\]

with discriminant 4,010,276 is found. The new lower bound for \( a_2 \) is \(-22\), and no smaller discriminant fields are found.
An Algorithm in Computational Algebraic Number Theory

Testing the Algorithm

The smallest discriminant totally real quintic number field having regulator greater than 100 but less than 101:

\[ X^5 - X^4 - 11X^3 + 7X^2 + 18X + 6 \]

The smallest discriminant totally real number field of odd prime degree having a non-cyclic simple Galois group:

\[ X^5 + X^4 - 11X^3 - X^2 + 12X + 4 \]

(A5)

The smallest discriminant totally real number field of odd prime degree greater than 5 having a primitive Galois group:

\[ X^7 - X^6 - 6X^5 + 4X^4 + 10X^3 - 4X^2 - 4X + 1 \]

(S7)
The smallest discriminant totally real quintic number field having regulator greater than 100 but less than 101:

\[ X^5 - X^4 - 11X^3 + 7X^2 + 18X + 6 \]
The smallest discriminant totally real quintic number field having regulator greater than 100 but less than 101:

\[ X^5 - X^4 - 11X^3 + 7X^2 + 18X + 6 \]

The smallest discriminant totally real number field of odd prime degree having a non-cyclic simple Galois group:

\[ X^5 + X^4 - 11X^3 - X^2 + 12X + 4 \quad (A_5) \]
The smallest discriminant totally real quintic number field having regulator greater than 100 but less than 101:

\[X^5 - X^4 - 11X^3 + 7X^2 + 18X + 6\]

The smallest discriminant totally real number field of odd prime degree having a non-cyclic simple Galois group:

\[X^5 + X^4 - 11X^3 - X^2 + 12X + 4 \quad (A_5)\]

The smallest discriminant totally real number field of odd prime degree greater than 5 having a primitive Galois group:

\[X^7 - X^6 - 6X^5 + 4X^4 + 10X^3 - 4X^2 - 4X + 1 \quad (S_7)\]
Searching for a Rank 1 Totally Real Quintic:
Searching for a Rank 1 Totally Real Quintic:

- The algorithm (PARI/GP) ran on 28 CPUs at 2.8 GHz for 12 days.
Searching for a Rank 1 Totally Real Quintic:

- The algorithm (PARI/GP) ran on 28 CPUs at 2.8 GHz for 12 days.
- In the process, some things were learned: blocks of reducible polynomials, memory requirements, etc.
Fields Having Previously Known Ranks:

The totally real quintic number field of smallest discriminant having...
Fields Having Previously Known Ranks:

The totally real quintic number field of smallest discriminant having...

Unit group rank 5:

\[ X^5 - X^4 - 4X^3 + 3X^2 + 3X - 1 \quad d = 14,641 \]
Fields Having Previously Known Ranks:

The totally real quintic number field of smallest discriminant having...

Unit group rank 5:

\[ X^5 - X^4 - 4X^3 + 3X^2 + 3X - 1 \quad d = 14,641 \]

Unit group rank 4:

\[ X^5 - 2X^4 - 3X^3 + 5X^2 + x - 1 \quad d = 36,497 \]
Fields Having Previously Known Ranks:

The totally real quintic number field of smallest discriminant having...

Unit group rank 5:
\[ X^5 - X^4 - 4X^3 + 3X^2 + 3X - 1 \quad d = 14,641 \]

Unit group rank 4:
\[ X^5 - 2X^4 - 3X^3 + 5X^2 + x - 1 \quad d = 36,497 \]

Unit group rank 3:
\[ X^5 - 2X^4 - 6X^3 + 8X^2 + 8X + 1 \quad d = 638,597 \]
The First Example of a Rank 2 Field:

The number field generated by a root $\alpha$ of the polynomial

\[ X^5 - X^4 - 21X^3 - 7X^2 + 68X + 60 \]

is the first known example of a totally real quintic having unit group rank 2.
The First Example of a Rank 2 Field:

The number field generated by a root $\alpha$ of the polynomial

$$X^5 - X^4 - 21X^3 - 7X^2 + 68X + 60$$

is the first known example of a totally real quintic having unit group rank 2.

- It has discriminant $52,315,684 = 2^2 \cdot 449 \cdot 29129$.
- The class number is 2.
- The Galois group is $S_5$. 
Success!! The First Example of a Rank 1 Field:

The number field generated by a root $\alpha$ of the polynomial

$$X^5 - 43X^3 - 5X^2 + 262X - 49$$

is the first known example of a totally real quintic having unit group rank 1.
Success!! The First Example of a Rank 1 Field:

The number field generated by a root $\alpha$ of the polynomial

$$X^5 - 43X^3 - 5X^2 + 262X - 49$$

is the first known example of a totally real quintic having unit group rank 1.

- It has discriminant

$$169,942,443,923,524 = 2^2 \cdot 4248561090881$$

- The class number is 4.

- The Galois group is $S_5$. 
Main Results

Final Results:

Main Results

Final Results:
- Rank 5: 20,075,722 (29.7%)
Main Results

Final Results:

- Rank 5: 20,075,722 (29.7%)
- Rank 4: 40,127,241 (59.3%)
Main Results

Final Results:

- Rank 5: 20,075,722 (29.7%)
- Rank 4: 40,127,241 (59.3%)
- Rank 3: 7,400,436 (10.9%)
Main Results

Final Results:

- Rank 5: 20,075,722 (29.7%)
- Rank 4: 40,127,241 (59.3%)
- Rank 3: 7,400,436 (10.9%)
- Rank 2: 38,562 (0.057%)
Main Results

Final Results:
- Rank 5: 20,075,722 (29.7%)
- Rank 4: 40,127,241 (59.3%)
- Rank 3: 7,400,436 (10.9%)
- Rank 2: 38,562 (0.057%)
- Rank 1: 8 (0.000012%)
Where to go from here...?

- This approach can be generalized to most signatures for fields of prime degree.
- Using results of M.E. Pohst, it can be generalized to certain signatures for composite degree fields.
The End

Jason.B.Hill@Colorado.edu

http://www.jasonbhill.com