Enumeration of totally real number fields of bounded root discriminant

John Voight
University of Vermont

Algorithmic Number Theory Symposium (ANTS) VIII
Banff, Alberta
18 May 2008

Problem

Problem

Problem

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

Problem

Problem

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

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

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

which is finite (Minkowski).

Problem

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

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

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

which is finite (Minkowski).

By the Odlyzko bounds, for

$$B < 4\pi e^{1+\gamma} < 60.840$$

Problem

Problem

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

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

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

which is finite (Minkowski).

By the Odlyzko bounds, for

$$B < 4\pi e^{1+\gamma} < 60.840$$

(or $B < 8\pi e^{\gamma+\pi/2} < 215.333$ on the GRH),

Problem

Problem

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

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

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

which is finite (Minkowski).

By the Odlyzko bounds, for

$$B < 4\pi e^{1+\gamma} < 60.840$$

(or $B < 8\pi e^{\gamma+\pi/2} < 215.333$ on the GRH), we have $NF(n, B) = \emptyset$ for n sufficiently large and so the set $NF(B)$ is finite.

Existing tables

Existing tables

1. There are tables of number fields computed by the Pari group (late 1990s) and the KASH group (QaoS, 2005).

Existing tables

1. There are tables of number fields computed by the Pari group (late 1990s) and the KASH group (QaoS, 2005). These tables contain fields of all signatures with $n \leq 7$ and varying discriminant bound and sporadic fields in degrees 8 and 9.

Existing tables

1. There are tables of number fields computed by the Pari group (late 1990s) and the KASH group (QaoS, 2005). These tables contain fields of all signatures with $n \leq 7$ and varying discriminant bound and sporadic fields in degrees 8 and 9.
2. Malle (ANTS VII) computed all totally real primitive number fields of discriminant $d_F \leq 10^9$.

Existing tables

1. There are tables of number fields computed by the Pari group (late 1990s) and the KASH group (QaoS, 2005). These tables contain fields of all signatures with $n \leq 7$ and varying discriminant bound and sporadic fields in degrees 8 and 9.
2. Malle (ANTS VII) computed all totally real primitive number fields of discriminant $d_F \leq 10^9$. This was reported to take several years of CPU time on a SUN workstation.

Existing tables

1. There are tables of number fields computed by the Pari group (late 1990s) and the KASH group (QaoS, 2005). These tables contain fields of all signatures with $n \leq 7$ and varying discriminant bound and sporadic fields in degrees 8 and 9.
2. Malle (ANTS VII) computed all totally real primitive number fields of discriminant $d_F \leq 10^9$. This was reported to take several years of CPU time on a SUN workstation.
3. Klüners and Malle (2001) created a database for number fields, containing representative polynomials for all transitive Galois groups up to degree 15.

Existing tables

1. There are tables of number fields computed by the Pari group (late 1990s) and the KASH group (QaoS, 2005). These tables contain fields of all signatures with $n \leq 7$ and varying discriminant bound and sporadic fields in degrees 8 and 9.
2. Malle (ANTS VII) computed all totally real primitive number fields of discriminant $d_F \leq 10^9$. This was reported to take several years of CPU time on a SUN workstation.
3. Klüners and Malle (2001) created a database for number fields, containing representative polynomials for all transitive Galois groups up to degree 15.
4. Tables of totally real fields with small root discriminant (Roblot),

Existing tables

1. There are tables of number fields computed by the Pari group (late 1990s) and the KASH group (QaoS, 2005). These tables contain fields of all signatures with $n \leq 7$ and varying discriminant bound and sporadic fields in degrees 8 and 9.
2. Malle (ANTS VII) computed all totally real primitive number fields of discriminant $d_F \leq 10^9$. This was reported to take several years of CPU time on a SUN workstation.
3. Klüners and Malle (2001) created a database for number fields, containing representative polynomials for all transitive Galois groups up to degree 15.
4. Tables of totally real fields with small root discriminant (Roblot), fields with prescribed ramification (Jones),

Existing tables

1. There are tables of number fields computed by the Pari group (late 1990s) and the KASH group (QaoS, 2005). These tables contain fields of all signatures with $n \leq 7$ and varying discriminant bound and sporadic fields in degrees 8 and 9.
2. Malle (ANTS VII) computed all totally real primitive number fields of discriminant $d_F \leq 10^9$. This was reported to take several years of CPU time on a SUN workstation.
3. Klüners and Malle (2001) created a database for number fields, containing representative polynomials for all transitive Galois groups up to degree 15.
4. Tables of totally real fields with small root discriminant (Roblot), fields with prescribed ramification (Jones), ...

Existing tables

1. There are tables of number fields computed by the Pari group (late 1990s) and the KASH group (QaoS, 2005). These tables contain fields of all signatures with $n \leq 7$ and varying discriminant bound and sporadic fields in degrees 8 and 9.
2. Malle (ANTS VII) computed all totally real primitive number fields of discriminant $d_F \leq 10^9$. This was reported to take several years of CPU time on a SUN workstation.
3. Klüners and Malle (2001) created a database for number fields, containing representative polynomials for all transitive Galois groups up to degree 15.
4. Tables of totally real fields with small root discriminant (Roblot), fields with prescribed ramification (Jones), ...

From (2) we could determine $NF(10)$ if we also separately compute imprimitive fields;

Existing tables

1. There are tables of number fields computed by the Pari group (late 1990s) and the KASH group (QaoS, 2005). These tables contain fields of all signatures with $n \leq 7$ and varying discriminant bound and sporadic fields in degrees 8 and 9.
2. Malle (ANTS VII) computed all totally real primitive number fields of discriminant $d_F \leq 10^9$. This was reported to take several years of CPU time on a SUN workstation.
3. Klüners and Malle (2001) created a database for number fields, containing representative polynomials for all transitive Galois groups up to degree 15.
4. Tables of totally real fields with small root discriminant (Roblot), fields with prescribed ramification (Jones), ...

From (2) we could determine $NF(10)$ if we also separately compute imprimitive fields; the latter two are in a different spirit.

Main result

Main result

Theorem

$\#NF(14) = 1229.$

Main result

Theorem

$\#NF(14) = 1229.$

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

Degree 10

Degree 10

Conjecture

Let $F = \mathbb{Q}(\alpha)$ *where* α *is a root of the polynomial*

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

Degree 10

Conjecture

Let $F = \mathbb{Q}(\alpha)$ *where* α *is a root of the polynomial*

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

Then F *is the totally real field of degree* 10 *with smallest discriminant* $d_F = 443952558373 = 61^2 397^2 757$.

Degree 10

Conjecture

Let $F = \mathbb{Q}(\alpha)$ *where* α *is a root of the polynomial*

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

Then F *is the totally real field of degree* 10 *with smallest discriminant* $d_F = 443952558373 = 61^2 397^2 757$.

The number field F (though not this polynomial) already appears in the tables of Klüners-Malle.

Degree 10

Conjecture

Let $F = \mathbb{Q}(\alpha)$ *where* α *is a root of the polynomial*

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

Then F *is the totally real field of degree* 10 *with smallest discriminant* $d_F = 443952558373 = 61^2 397^2 757$*.*

The number field F (though not this polynomial) already appears in the tables of Klüners-Malle. It is a quadratic extension of the second smallest totally real quintic field, of discriminant 24217 (an S_5 extension).

Motivation and applications

Motivation and applications

As we have seen, many of the existing tables are either old, incomplete, or in a different spirit.

Motivation and applications

As we have seen, many of the existing tables are either old, incomplete, or in a different spirit.

The complete list of these fields is available online at `http://www.cems.uvm.edu/~voight/nf-tables/`.

Motivation and applications

As we have seen, many of the existing tables are either old, incomplete, or in a different spirit.

The complete list of these fields is available online at `http://www.cems.uvm.edu/~voight/nf-tables/`. Our algorithm is included in Sage 3.0.

Motivation and applications

As we have seen, many of the existing tables are either old, incomplete, or in a different spirit.

The complete list of these fields is available online at `http://www.cems.uvm.edu/~voight/nf-tables/`. Our algorithm is included in Sage 3.0.

One may place alternative constraints on the signature of the fields F under consideration or even analogous p-adic conditions.

Motivation and applications

As we have seen, many of the existing tables are either old, incomplete, or in a different spirit.

The complete list of these fields is available online at `http://www.cems.uvm.edu/~voight/nf-tables/`. Our algorithm is included in Sage 3.0.

One may place alternative constraints on the signature of the fields F under consideration or even analogous p-adic conditions. However, totally real fields are interesting for many reasons.

Motivation and applications: Towers

Motivation and applications: Towers

Recall that assuming the GRH, for $B < 215.333$ the set $NF(B)$ is finite.

Motivation and applications: Towers

Recall that assuming the GRH, for $B < 215.333$ the set $NF(B)$ is finite. Martin has constructed an infinite tower of totally real fields with root discriminant $\delta \approx 913.493$.

Motivation and applications: Towers

Recall that assuming the GRH, for $B < 215.333$ the set $NF(B)$ is finite. Martin has constructed an infinite tower of totally real fields with root discriminant $\delta \approx 913.493$. The value

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

is presently unknown.

Motivation and applications: Towers

Recall that assuming the GRH, for $B < 215.333$ the set $NF(B)$ is finite. Martin has constructed an infinite tower of totally real fields with root discriminant $\delta \approx 913.493$. The value

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

is presently unknown.

By comparison, Hajir-Maire have constructed an unramified tower of totally complex number fields with root discriminant ≈ 82.100,

Motivation and applications: Towers

Recall that assuming the GRH, for $B < 215.333$ the set $NF(B)$ is finite. Martin has constructed an infinite tower of totally real fields with root discriminant $\delta \approx 913.493$. The value

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

is presently unknown.

By comparison, Hajir-Maire have constructed an unramified tower of totally complex number fields with root discriminant ≈ 82.100, which comes within a factor 2 of the GRH-conditional Odlyzko bound of $8\pi e^{\gamma} \approx 44.763$.

Motivation and applications: Towers

Recall that assuming the GRH, for $B < 215.333$ the set $NF(B)$ is finite. Martin has constructed an infinite tower of totally real fields with root discriminant $\delta \approx 913.493$. The value

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

is presently unknown.

By comparison, Hajir-Maire have constructed an unramified tower of totally complex number fields with root discriminant ≈ 82.100, which comes within a factor 2 of the GRH-conditional Odlyzko bound of $8\pi e^{\gamma} \approx 44.763$.

Totally real octics of moderate discriminant are good candidates as the base field for such a tower

Motivation and applications: Towers

Recall that assuming the GRH, for $B < 215.333$ the set $NF(B)$ is finite. Martin has constructed an infinite tower of totally real fields with root discriminant $\delta \approx 913.493$. The value

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

is presently unknown.

By comparison, Hajir-Maire have constructed an unramified tower of totally complex number fields with root discriminant ≈ 82.100, which comes within a factor 2 of the GRH-conditional Odlyzko bound of $8\pi e^\gamma \approx 44.763$.

Totally real octics of moderate discriminant are good candidates as the base field for such a tower (coming from the Golod-Shafarevich bound).

Motivation and applications: Towers

Recall that assuming the GRH, for $B < 215.333$ the set $NF(B)$ is finite. Martin has constructed an infinite tower of totally real fields with root discriminant $\delta \approx 913.493$. The value

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

is presently unknown.

By comparison, Hajir-Maire have constructed an unramified tower of totally complex number fields with root discriminant ≈ 82.100, which comes within a factor 2 of the GRH-conditional Odlyzko bound of $8\pi e^{\gamma} \approx 44.763$.

Totally real octics of moderate discriminant are good candidates as the base field for such a tower (coming from the Golod-Shafarevich bound). In joint work with Martin, we are now searching for a better tower.

Motivation and applications: Arithmetic

Motivation and applications: Arithmetic

In studying certain enumerative problems in arithmetic geometry and number theory, one often reduces to a bound on the root discriminant and concludes finiteness using the Odlyzko bounds.

Motivation and applications: Arithmetic

In studying certain enumerative problems in arithmetic geometry and number theory, one often reduces to a bound on the root discriminant and concludes finiteness using the Odlyzko bounds. Therefore, provably complete and extensive tables of totally real fields are useful (if not essential).

Motivation and applications: Arithmetic

In studying certain enumerative problems in arithmetic geometry and number theory, one often reduces to a bound on the root discriminant and concludes finiteness using the Odlyzko bounds. Therefore, provably complete and extensive tables of totally real fields are useful (if not essential).

For example, using our tables we enumerated all Shimura curves of genus at most two.

Motivation and applications: Arithmetic

In studying certain enumerative problems in arithmetic geometry and number theory, one often reduces to a bound on the root discriminant and concludes finiteness using the Odlyzko bounds. Therefore, provably complete and extensive tables of totally real fields are useful (if not essential).

For example, using our tables we enumerated all Shimura curves of genus at most two. A *Shimura curve* is a generalization of a modular curve,

Motivation and applications: Arithmetic

In studying certain enumerative problems in arithmetic geometry and number theory, one often reduces to a bound on the root discriminant and concludes finiteness using the Odlyzko bounds. Therefore, provably complete and extensive tables of totally real fields are useful (if not essential).

For example, using our tables we enumerated all Shimura curves of genus at most two. A *Shimura curve* is a generalization of a modular curve, given by taking the quotient $X_0^{\mathfrak{D}}(\mathfrak{N}) = \Gamma_0^{\mathfrak{D}}(\mathfrak{N}) \backslash \mathfrak{H}$

Motivation and applications: Arithmetic

In studying certain enumerative problems in arithmetic geometry and number theory, one often reduces to a bound on the root discriminant and concludes finiteness using the Odlyzko bounds. Therefore, provably complete and extensive tables of totally real fields are useful (if not essential).

For example, using our tables we enumerated all Shimura curves of genus at most two. A *Shimura curve* is a generalization of a modular curve, given by taking the quotient $X_0^{\mathfrak{D}}(\mathfrak{N}) = \Gamma_0^{\mathfrak{D}}(\mathfrak{N})\backslash\mathfrak{H}$ where $\Gamma_0^{\mathfrak{D}}(\mathfrak{N})$ is the group of units of reduced norm 1 in a quaternion algebra over a totally real field F which is split at a unique real place.

Motivation and applications: Arithmetic

In studying certain enumerative problems in arithmetic geometry and number theory, one often reduces to a bound on the root discriminant and concludes finiteness using the Odlyzko bounds. Therefore, provably complete and extensive tables of totally real fields are useful (if not essential).

For example, using our tables we enumerated all Shimura curves of genus at most two. A *Shimura curve* is a generalization of a modular curve, given by taking the quotient $X_0^{\mathfrak{D}}(\mathfrak{N}) = \Gamma_0^{\mathfrak{D}}(\mathfrak{N})\backslash\mathfrak{H}$ where $\Gamma_0^{\mathfrak{D}}(\mathfrak{N})$ is the group of units of reduced norm 1 in a quaternion algebra over a totally real field F which is split at a unique real place. There are exactly 858 such curves.

Motivation and applications: Arithmetic

In studying certain enumerative problems in arithmetic geometry and number theory, one often reduces to a bound on the root discriminant and concludes finiteness using the Odlyzko bounds. Therefore, provably complete and extensive tables of totally real fields are useful (if not essential).

For example, using our tables we enumerated all Shimura curves of genus at most two. A *Shimura curve* is a generalization of a modular curve, given by taking the quotient $X_0^{\mathfrak{D}}(\mathfrak{N}) = \Gamma_0^{\mathfrak{D}}(\mathfrak{N})\backslash\mathfrak{H}$ where $\Gamma_0^{\mathfrak{D}}(\mathfrak{N})$ is the group of units of reduced norm 1 in a quaternion algebra over a totally real field F which is split at a unique real place. There are exactly 858 such curves.

We also recently enumerated all CM-extensions K/F with *higher relative class number* at most sixteen,

Motivation and applications: Arithmetic

In studying certain enumerative problems in arithmetic geometry and number theory, one often reduces to a bound on the root discriminant and concludes finiteness using the Odlyzko bounds. Therefore, provably complete and extensive tables of totally real fields are useful (if not essential).

For example, using our tables we enumerated all Shimura curves of genus at most two. A *Shimura curve* is a generalization of a modular curve, given by taking the quotient $X_0^{\mathfrak{D}}(\mathfrak{N}) = \Gamma_0^{\mathfrak{D}}(\mathfrak{N}) \backslash \mathfrak{H}$ where $\Gamma_0^{\mathfrak{D}}(\mathfrak{N})$ is the group of units of reduced norm 1 in a quaternion algebra over a totally real field F which is split at a unique real place. There are exactly 858 such curves.

We also recently enumerated all CM-extensions K/F with *higher relative class number* at most sixteen, generalizing the Gauss class number 1 problem to higher K-groups.

Motivation and applications: Asymptotics of number fields

Motivation and applications: Asymptotics of number fields

Finally, work of Bhargava has renewed interest in the asymptotics of number fields with fixed Galois group.

Motivation and applications: Asymptotics of number fields

Finally, work of Bhargava has renewed interest in the asymptotics of number fields with fixed Galois group. Bhargava (2005–) counts the number of cubic, quartic, quintic fields up to discriminant X and obtains an asymptotic in terms of local densities.

Motivation and applications: Asymptotics of number fields

Finally, work of Bhargava has renewed interest in the asymptotics of number fields with fixed Galois group. Bhargava (2005–) counts the number of cubic, quartic, quintic fields up to discriminant X and obtains an asymptotic in terms of local densities. It would be interesting to investigate the convergence of the data and the error term.

Motivation and applications: Asymptotics of number fields

Finally, work of Bhargava has renewed interest in the asymptotics of number fields with fixed Galois group. Bhargava (2005–) counts the number of cubic, quartic, quintic fields up to discriminant X and obtains an asymptotic in terms of local densities. It would be interesting to investigate the convergence of the data and the error term.

Also, in joint work with Dummit, we are investigating the *signature rank* of totally real quintic fields, the $\mathbb{F}_2$-rank of the group of totally positive units modulo squares $\mathbb{Z}_{F,+}^{*}/\mathbb{Z}_{F}^{*2}$.

Motivation and applications: Asymptotics of number fields

Finally, work of Bhargava has renewed interest in the asymptotics of number fields with fixed Galois group. Bhargava (2005–) counts the number of cubic, quartic, quintic fields up to discriminant X and obtains an asymptotic in terms of local densities. It would be interesting to investigate the convergence of the data and the error term.

Also, in joint work with Dummit, we are investigating the *signature rank* of totally real quintic fields, the $\mathbb{F}_2$-rank of the group of totally positive units modulo squares $\mathbb{Z}_{F,+}^{*}/\mathbb{Z}_F^{*2}$. For this application, we need very large tables of (totally real) quintics.

Motivation and applications: Asymptotics of number fields

Finally, work of Bhargava has renewed interest in the asymptotics of number fields with fixed Galois group. Bhargava (2005–) counts the number of cubic, quartic, quintic fields up to discriminant X and obtains an asymptotic in terms of local densities. It would be interesting to investigate the convergence of the data and the error term.

Also, in joint work with Dummit, we are investigating the *signature rank* of totally real quintic fields, the $\mathbb{F}_2$-rank of the group of totally positive units modulo squares $\mathbb{Z}_{F,+}^{*}/\mathbb{Z}_F^{*2}$. For this application, we need very large tables of (totally real) quintics. This work is motivated by the Stark conjecture.

Results and timings

Results and timings

For good measure (and for our applications), we actually compute $NF(n, B) \leq \Delta(n)$ as follows.

Results and timings

For good measure (and for our applications), we actually compute $NF(n, B) \leq \Delta(n)$ as follows.

n	2	3	4	5	6	7	8	9	10
$\Delta(n)$	30	25	20	17	16	15.5	15	14.5	14
f	443	4922	57721	244600	3242209	$1.7 \cdot 10^7$	$1.2 \cdot 10^8$	$9.5 \cdot 10^8$	$2.5 \cdot 10^9$
F	273	630	1273	674	802	301	164	15	0
CPU time	0.2s	2.2s	26.8s	1m25s	17m3s	2h59m	1d4.5h	17d21h	193d
Imprim f	0	0	7059	0	62532	0	239404	15658	945866
Imprim F	0	0	702	0	420	0	100	6	0
CPU time	-	-	4m22s	-	8m38s	-	1h56m	16m53s	11h27m
Total fields	273	630	1578	674	827	301	164	15	0

The CPU time is relative to the processor of a desktop machine (Opteron 1.8GHz, Athlon Dual Core 2.0GHz, and Celeron 2.53GHz).

Method: Hunter's theorem

Method: Hunter's theorem

We follow the well-known method for enumerating $NF(n, B)$, with a few new tricks.

Method: Hunter's theorem

We follow the well-known method for enumerating $NF(n, B)$, with a few new tricks.

First, we use the geometry of numbers (Hunter's theorem):

Method: Hunter's theorem

We follow the well-known method for enumerating $NF(n, B)$, with a few new tricks.

First, we use the geometry of numbers (Hunter's theorem): there exists $\alpha \in \mathbb{Z}_F \setminus \mathbb{Z}$ such that $0 \leq \mathrm{Tr}(\alpha) \leq n/2$ and

Method: Hunter's theorem

We follow the well-known method for enumerating $NF(n, B)$, with a few new tricks.

First, we use the geometry of numbers (Hunter's theorem): there exists $\alpha \in \mathbb{Z}_F \setminus \mathbb{Z}$ such that $0 \leq \mathrm{Tr}(\alpha) \leq n/2$ and

$$T_2(\alpha) = \sum_{i=1}^{n} |\alpha_i|^2 \leq C(n, B)$$

for an explicit bound $C(n, B)$.

Method: Hunter's theorem

We follow the well-known method for enumerating $NF(n, B)$, with a few new tricks.

First, we use the geometry of numbers (Hunter's theorem): there exists $\alpha \in \mathbb{Z}_F \setminus \mathbb{Z}$ such that $0 \leq \mathrm{Tr}(\alpha) \leq n/2$ and

$$T_2(\alpha) = \sum_{i=1}^{n} |\alpha_i|^2 \leq C(n, B)$$

for an explicit bound $C(n, B)$. This gives bounds on the coefficients $a_i \in \mathbb{Z}$ of the characteristic polynomial of α

Method: Hunter's theorem

We follow the well-known method for enumerating $NF(n, B)$, with a few new tricks.

First, we use the geometry of numbers (Hunter's theorem): there exists $\alpha \in \mathbb{Z}_F \setminus \mathbb{Z}$ such that $0 \leq \mathrm{Tr}(\alpha) \leq n/2$ and

$$T_2(\alpha) = \sum_{i=1}^{n} |\alpha_i|^2 \leq C(n, B)$$

for an explicit bound $C(n, B)$. This gives bounds on the coefficients $a_i \in \mathbb{Z}$ of the characteristic polynomial of α

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

Method: Hunter's theorem

We follow the well-known method for enumerating $NF(n, B)$, with a few new tricks.

First, we use the geometry of numbers (Hunter's theorem): there exists $\alpha \in \mathbb{Z}_F \setminus \mathbb{Z}$ such that $0 \leq \mathrm{Tr}(\alpha) \leq n/2$ and

$$T_2(\alpha) = \sum_{i=1}^{n} |\alpha_i|^2 \leq C(n, B)$$

for an explicit bound $C(n, B)$. This gives bounds on the coefficients $a_i \in \mathbb{Z}$ of the characteristic polynomial of α

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

(We must also deal with the possibility that F is imprimitive and $\mathbb{Q}(\alpha) \neq F$.)

Method: Analysis

Method: Analysis

This yields a finite set $NS(n, B)$ of possible $f(x) \in \mathbb{Z}[x]$

Method: Analysis

This yields a finite set $NS(n, B)$ of possible $f(x) \in \mathbb{Z}[x]$ of size $O(B^{n(n+2)/4})$.

Method: Analysis

This yields a finite set $NS(n, B)$ of possible $f(x) \in \mathbb{Z}[x]$ of size $O(B^{n(n+2)/4})$.

Conjecture (Linnik)

$\#NF(n, B) \sim c(n)B^n$ *for some* $c_n \in \mathbb{R}_{>0}$.

Method: Analysis

This yields a finite set $NS(n, B)$ of possible $f(x) \in \mathbb{Z}[x]$ of size $O(B^{n(n+2)/4})$.

Conjecture (Linnik)

$\#NF(n, B) \sim c(n)B^n$ *for some* $c_n \in \mathbb{R}_{>0}$*.*

This conjecture is known for $n = 3$ (Davenport-Heilbronn) and for $n = 4, 5$ (Bhargava).

Method: Analysis

This yields a finite set $NS(n, B)$ of possible $f(x) \in \mathbb{Z}[x]$ of size $O(B^{n(n+2)/4})$.

Conjecture (Linnik)

$\#NF(n, B) \sim c(n)B^n$ for some $c_n \in \mathbb{R}_{>0}$.

This conjecture is known for $n = 3$ (Davenport-Heilbronn) and for $n = 4, 5$ (Bhargava). For large n, the best result known is

$$\#NF(n, B) = O\left(B^{n \exp(C\sqrt{\log n})}\right)$$

for some absolute constant C (Ellenberg-Venkatesh).

Method: Analysis

This yields a finite set $NS(n, B)$ of possible $f(x) \in \mathbb{Z}[x]$ of size $O(B^{n(n+2)/4})$.

Conjecture (Linnik)

$\#NF(n, B) \sim c(n)B^n$ for some $c_n \in \mathbb{R}_{>0}$.

This conjecture is known for $n = 3$ (Davenport-Heilbronn) and for $n = 4, 5$ (Bhargava). For large n, the best result known is

$$\#NF(n, B) = O\left(B^{n\exp(C\sqrt{\log n})}\right)$$

for some absolute constant C (Ellenberg-Venkatesh). It is an open problem to make their method practical,

Method: Analysis

This yields a finite set $NS(n,B)$ of possible $f(x) \in \mathbb{Z}[x]$ of size $O(B^{n(n+2)/4})$.

Conjecture (Linnik)

$\#NF(n,B) \sim c(n)B^n$ for some $c_n \in \mathbb{R}_{>0}$.

This conjecture is known for $n = 3$ (Davenport-Heilbronn) and for $n = 4, 5$ (Bhargava). For large n, the best result known is

$$\#NF(n,B) = O\left(B^{n\exp(C\sqrt{\log n})}\right)$$

for some absolute constant C (Ellenberg-Venkatesh). It is an open problem to make their method practical, so we are left to chip away at the implied constant.

Method: Smyth's lower bound

Method: Smyth's lower bound

We now assume F is totally real and primitive.

Method: Smyth's lower bound

We now assume F is totally real and primitive.

From Hunter's theorem, we obtain an upper bound on $T_2(\alpha) = \mathrm{Tr}(\alpha^2)$.

Method: Smyth's lower bound

We now assume F is totally real and primitive.

From Hunter's theorem, we obtain an upper bound on $T_2(\alpha) = \mathrm{Tr}(\alpha^2)$. We then apply the following result of Smyth.

Method: Smyth's lower bound

We now assume F is totally real and primitive.

From Hunter's theorem, we obtain an upper bound on $T_2(\alpha) = \mathrm{Tr}(\alpha^2)$. We then apply the following result of Smyth.

Lemma (Smyth)

If θ is a totally positive algebraic integer,

Method: Smyth's lower bound

We now assume F is totally real and primitive.

From Hunter's theorem, we obtain an upper bound on $T_2(\alpha) = \mathrm{Tr}(\alpha^2)$. We then apply the following result of Smyth.

Lemma (Smyth)

If θ is a totally positive algebraic integer, then

$$\mathrm{Tr}(\theta) > 1.7719[\mathbb{Q}(\theta) : \mathbb{Q}]$$

Method: Smyth's lower bound

We now assume F is totally real and primitive.

From Hunter's theorem, we obtain an upper bound on $T_2(\alpha) = \mathrm{Tr}(\alpha^2)$. We then apply the following result of Smyth.

Lemma (Smyth)

If θ is a totally positive algebraic integer, then

$$\mathrm{Tr}(\theta) > 1.7719[\mathbb{Q}(\theta) : \mathbb{Q}]$$

with finitely many (explicitly known) exceptions.

Method: Smyth's lower bound

We now assume F is totally real and primitive.

From Hunter's theorem, we obtain an upper bound on $T_2(\alpha) = \mathrm{Tr}(\alpha^2)$. We then apply the following result of Smyth.

Lemma (Smyth)

If θ is a totally positive algebraic integer, then

$$\mathrm{Tr}(\theta) > 1.7719[\mathbb{Q}(\theta) : \mathbb{Q}]$$

with finitely many (explicitly known) exceptions.

We therefore have finitely many possibilities for the first two coefficients a_{n-1}, a_{n-2}.

Method: Rolle's theorem

Method: Rolle's theorem

Now, given values for $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$, we deduce bounds for a_{n-k-1}.

Method: Rolle's theorem

Now, given values for $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$, we deduce bounds for a_{n-k-1}. Let $f_k(x) = \frac{1}{(n-k)!} f^{(n-k)}(x) = g_k(x) + a_{n-k}$.

Method: Rolle's theorem

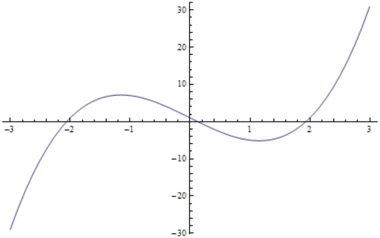
Now, given values for $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$, we deduce bounds for a_{n-k-1}. Let $f_k(x) = \frac{1}{(n-k)!} f^{(n-k)}(x) = g_k(x) + a_{n-k}$. Consider for illustration the case $k = 3$, so

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

Method: Rolle's theorem

Now, given values for $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$, we deduce bounds for a_{n-k-1}. Let $f_k(x) = \frac{1}{(n-k)!} f^{(n-k)}(x) = g_k(x) + a_{n-k}$. Consider for illustration the case $k = 3$, so

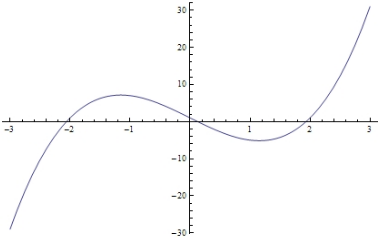
$$g_3(x) = \frac{n(n-1)(n-2)}{6} x^3 + \frac{(n-1)(n-2)}{2} a_{n-1} x^2 + (n-2) a_{n-2} x.$$



Method: Rolle's theorem

Now, given values for $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$, we deduce bounds for a_{n-k-1}. Let $f_k(x) = \frac{1}{(n-k)!} f^{(n-k)}(x) = g_k(x) + a_{n-k}$. Consider for illustration the case $k = 3$, so

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

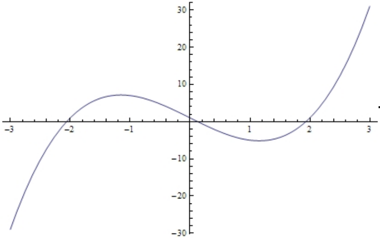


Let $\beta_1 < \beta_2$ denote the roots of $f_2(x)$.

Method: Rolle's theorem

Now, given values for $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$, we deduce bounds for a_{n-k-1}. Let $f_k(x) = \frac{1}{(n-k)!} f^{(n-k)}(x) = g_k(x) + a_{n-k}$. Consider for illustration the case $k = 3$, so

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



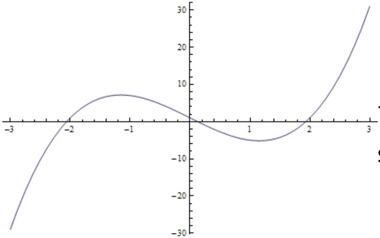
Let $\beta_1 < \beta_2$ denote the roots of $f_2(x)$.

Thus $f_3(\beta_1) = g_3(\beta_1) + a_{n-3} > 0$

Method: Rolle's theorem

Now, given values for $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$, we deduce bounds for a_{n-k-1}. Let $f_k(x) = \frac{1}{(n-k)!} f^{(n-k)}(x) = g_k(x) + a_{n-k}$. Consider for illustration the case $k = 3$, so

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



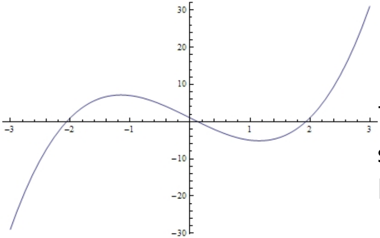
Let $\beta_1 < \beta_2$ denote the roots of $f_2(x)$.

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

Method: Rolle's theorem

Now, given values for $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$, we deduce bounds for a_{n-k-1}. Let $f_k(x) = \frac{1}{(n-k)!} f^{(n-k)}(x) = g_k(x) + a_{n-k}$. Consider for illustration the case $k = 3$, so

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



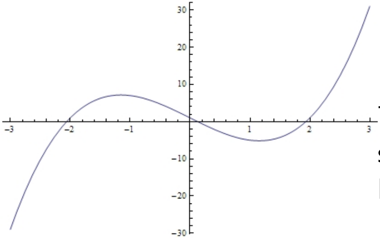
Let $\beta_1 < \beta_2$ denote the roots of $f_2(x)$.

Thus $f_3(\beta_1) = g_3(\beta_1) + a_{n-3} > 0$ and similarly $f_3(\beta_2) = g_3(\beta_2) + a_{n-3} < 0$ hence $-g_3(\beta_1) < a_{n-3} < -g_3(\beta_2)$.

Method: Rolle's theorem

Now, given values for $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$, we deduce bounds for a_{n-k-1}. Let $f_k(x) = \frac{1}{(n-k)!} f^{(n-k)}(x) = g_k(x) + a_{n-k}$. Consider for illustration the case $k = 3$, so

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



Let $\beta_1 < \beta_2$ denote the roots of $f_2(x)$.

Thus $f_3(\beta_1) = g_3(\beta_1) + a_{n-3} > 0$ and similarly $f_3(\beta_2) = g_3(\beta_2) + a_{n-3} < 0$ hence $-g_3(\beta_1) < a_{n-3} < -g_3(\beta_2)$.

In a similar way, using Lagrange multipliers (Pohst) we find a bound on the largest β_3 and smallest root β_0 of $f(x)$ which yields $f_3(\beta_3) = g_3(\beta_3) + a_{n-3} > 0$ so $-g_3(\beta_3) < a_{n-3} < -g_3(\beta_0)$.

Method: Conclusion

Method: Conclusion

The combined Rolle's theorem-Lagrange multiplier bounds are by far the best available in the case of totally real fields, in our experience.

Method: Conclusion

The combined Rolle's theorem-Lagrange multiplier bounds are by far the best available in the case of totally real fields, in our experience.

We find additional (substantial!) speedups by using an "easy irreducibility" test and other implementation tricks.

Method: Conclusion

The combined Rolle's theorem-Lagrange multiplier bounds are by far the best available in the case of totally real fields, in our experience.

We find additional (substantial!) speedups by using an "easy irreducibility" test and other implementation tricks.

Finally, we extend these ideas to the imprimitive case.

Method: Conclusion

The combined Rolle's theorem-Lagrange multiplier bounds are by far the best available in the case of totally real fields, in our experience.

We find additional (substantial!) speedups by using an "easy irreducibility" test and other implementation tricks.

Finally, we extend these ideas to the imprimitive case. We use a lattice point enumeration method which allows us to generalize the use of Rolle's theorem and Lagrange multipliers to the relative situation.

Method: Conclusion

The combined Rolle's theorem-Lagrange multiplier bounds are by far the best available in the case of totally real fields, in our experience.

We find additional (substantial!) speedups by using an "easy irreducibility" test and other implementation tricks.

Finally, we extend these ideas to the imprimitive case. We use a lattice point enumeration method which allows us to generalize the use of Rolle's theorem and Lagrange multipliers to the relative situation.

Thanks!