Computations of and with Units

Claus Fieker

University of Sydney
claus@maths.usyd.edu.au

Overview

The Unit Group of a number field is one of the most important invariants
of the unit group has a long and interesting history - which I mainly ig

The computation of the full unit group naturally has two parts:

- Computation of a large group $U \leq U_K$ of units
  - Generation of Units
  - Find dependencies to compute U
- Show that we have the full group
  - Derive a lower bound on the regulator to derive $b > (U_K : U)$
  - Show that for all $p < b$ that $p \nmid (U_K : U)$

Notation

Let K be a number field of degree $n := (K : \mathbb{Q})$ over $\mathbb{Q}$.

Fix embeddings $(.)^{(i)} : K \longrightarrow \mathbb{R}$ $(1 \leq i \leq r_1)$ or $\mathbb{C}$ $(r_1 < i \leq n =$
sort them in the usual way. Then $T_2 : K \longrightarrow \mathbb{R} : x \mapsto \sum_{i=1}^{n} |x^{(i)}|^2$
form.

Define a logarithmic map $L : K^* \longrightarrow \mathbb{R}^{r_1+r_2} : x \mapsto (\log(|x^{(i)}|))_{1\leq i}$

And define the unit rank $r := r_1 + r_2 - 1$.

Dirichlet

We have the Dirichlet unit theorem:

$$U_K / \langle \zeta \rangle = \bigtimes_{i=1}^{r} \langle \epsilon_i \rangle \cong \mathbb{Z}^r$$

Computing U_K means the computation of a so called set of Fund

$\{\epsilon_1, \ldots, \epsilon_r\}$.

Part I: Given a (finite) set of units S, find the sub-group U of U_K gene

Part II: Decide if we have the full group.

Part I

Suppose ϵ_1, . . ., ϵ_s are independent units and ϵ is arbitrary.

Decide if ϵ is independent

If ϵ is dependent, find a relation between the units.

In theory, all is trivial: the units are $\mathbb{Z}$-independent if and only if their
L are $\mathbb{R}$-linearly independent. So, to solve problem 1, we only need to
system over $\mathbb{R}$.

Zero

How do we decide if a real number is zero (on a computer)?

In general we cannot possible decide by looking at a finite approxima
number if it is zero, but if we restrict to algebraic integers we can:

Let x be an algebraic integer. Then either x is a torsion unit or there
embedding i such that $|x^{(i)}| \geq 1 + \frac{1}{6}\frac{\log n}{n^2}$

Alternatively, for a non-torsion unit we have:

$$\|L(x)\|_2 \geq \frac{21}{128}\frac{\log n}{n^2}$$

A Quadratic Form

Given s (independent) units, we can define a quadratic form on $\mathbb{Z}^s$:

$$(x_1, \ldots, x_s) \mapsto \|L(\prod_{i=1}^{s} \epsilon_i^{x_i})\|_2^2$$

Using a variant of the Cholesky Decomposition (quadratic supplement)

pute $q_{i,j} \in \mathbb{R}$ such that

$$Q(x_1, \ldots, x_s) = \sum_{i=1}^{s} q_{i,i}(x_i + \sum_{j=i+1}^{s} q_{i,j} x_j)^2$$

A Quadratic Form

$$Q(x_1, \ldots, x_s) = \sum_{i=1}^{s} q_{i,i}(x_i + \sum_{j=i+1}^{s} q_{i,j}x_j)^2$$

We can easily check that

$$d(Q) = \prod_{i=1}^{s} q_{i,i}$$

Since Q is tied to the units, we see that $Q(x_1, \ldots, x_s) \geq M_1(Q) \geq$

A Quadratic Form

$$Q(x_1, \ldots, x_s) = \sum_{i=1}^{s} q_{i,i}(x_i + \sum_{j=i+1}^{s} q_{i,j}x_j)^2$$

Using a suitable permutation of the x_i, we can achieve

- A numerically stable algorithm with rigorous error bounds to comp
- A sorting of the diagonal elements: $q_{1,1} \geq \ldots \geq q_{s,s}$

If we combine this with the lower bound for $M_1(Q)$, we have a lower discriminant $d(Q)$. Since $d(Q) \neq 0 \iff \epsilon_1, \ldots, \epsilon_s$ are independe this to detect independence.

Finding Dependencies

We are in the following situation:

- A system of independent units $\epsilon_1, \ldots, \epsilon_s$
- A unit ϵ such that there exists a dependency

Problem: How do we find the dependency?

Finding Dependencies

Solutions:

- Compute a dependency over $\mathbb{R}$, normalize it, compute a "bound"
  nued fractions to find a rational dependency.
- Compute dependencies in suitable residue class fields, use Chinese
  and finally, find a rational dependency using rational reconstructio
- Use MLLL in the real-lattice
- Use (M)LLL in a derived integral-lattice

Problem in most cases are numerical: one needs to control all numeri
last possibility is theoretically unproven (Leopold-conjecture) and untri

Karim's approach

Karim Belabas suggested the following approach:

Let $M \in \mathbb{R}^{s\times s} \in \mathrm{Gl}(s, \mathbb{R})$ be arbitrary. One can compute an intege

$A := \lfloor \lambda M \rceil \lfloor \lambda M^t \rceil$ is a symmetric, positive definite integral matrix.

If λ is large enough, then the LLL applied to A should behave simil

applied to MM^t. in particular, a short vector can be obtained this wa

Scaling and Rounding

Our approach is slightly different. We start by the following: Let M

symmetric and positive definite, then $M_\lambda := \lfloor \lambda M \rceil + \lceil \frac{s}{2} \rceil I_s \in$

symmetric and positive definite for all $\lambda > 0$.

It is then easy to see that if $x^t M x = 0$ for some $x \in \mathbb{Z}^s$ we get $x^t M$

- independent of λ.

On the other hand, if $x^t M x > 0$ then obviously, $x^t M_\lambda x \cong \lambda x^t M x$

Therefore, if λ is large enough, the first basis vector of an integral LLL

for M_λ will correspond to our dependency.

Part II

We assume that somehow we have a maximal system of independent

a subgroup $U \leq U_K$ of finite index.

We suspect that $U = U_K$ and we want to show this.

We know $(U_K : U) = \frac{\operatorname{Reg} U}{\operatorname{Reg} U_K}$ - but we don't know $\operatorname{Reg} U_K$.

Aim: Find a "good" lower bound $R \leq \operatorname{Reg} U_K$

Then one needs to show that for all primes $p \leq \frac{\operatorname{Reg} U}{R}$ our candidate U

in U_K.

Remak

The strategy is to find a "good" lower bound on the size of the smalle
unit. This is attempted through a mixture of explicitly searching for s
by solving a global minimization problem:

Suppose $T_2(\epsilon) > K$ and $T_2(\epsilon^{-1}) > K$ for some K. Find a "gooc
that $Q(\epsilon) \geq q(K)$.

By combining the explicit results for all units ϵ such that $T_2(\epsilon) \leq K$
$q(K)$ for all others, we derive a lower bound on $d(Q) = \mathrm{Reg}\, U_K$ v
theorem on successive minima.

An extremal Problem

Consider the minimization problem: Minimize

$$\sum_{i=1}^{n} x_i^2$$

under the constraints

- $\sum_{i=1}^{n} x_i = 0$
- $\sum_{i=1}^{n} \exp(2x_i) \geq K$
- $\sum_{i=1}^{n} \exp(-2x_i) \geq K$

Interpretation: $x_i := \log |\epsilon^{(i)}|$

Reduction

It is immediately clear, that

- A solution has positive and negative coordinates
- A solution has at most three different coordinates
- The solution becomes at most smaller if we omit for example the l

Pohst showed that under the additional assumption that we have at leas

coordinates, no zero coordinates and without the last constraint, th

bounded from below by

$$M_{K,0} := \frac{n}{4} \operatorname{arcosh}^2 \frac{K}{n}$$

In case n even, this corresponds to a vector $(x, \ldots, x, -x, \ldots, -x$

Last Case

The remaining case of zero coordinates is handled by "reduction": If a
zero, we reduce n and K and use the last step again.

It remains to find the minimum of

$$M_{K,j} := \frac{n-j}{4}\operatorname{arcosh}^2\frac{K-j}{n-j}$$

for $j \in [0..n-2]$.

By computing partial derivatives we can show that this function is decr
$K > n(1+\sqrt{2})$ and the minimum is thus in $j = n-2$.

Improvements

To improve the bound we need to exclude the possibility of zero coordina

into the field, this means simply that we need to exclude units that ha

of absolute value $\mathbf{1}$.

In general, as we will see next, we cannot exclude this. However, it is

conjugates cannot be of absolute value $\mathbf{1}$, so that $n - j \geq r_1$ and j

real fields.

Special Units

Let K be a totally real field of degree n. Using Minkowski's lattice th

easily find an algebraic integer x such that $x^{(1)} > 2$ and $|x^{(i)}| \leq 2$ f

Then $L := K(y)$ for $y^2 + xy + 1$ has a unit y such that the $2n$

conjugates are of absolute value 1.