AMSI
AUSTRALIAN MATHEMATICAL SCIENCES INSTITUTE

National Collaboration in the Mathematical Sciences

Understanding hard cases in the general class group algorithm

Makoto Suwama
Supervisor: Dr. Steve Donnelly
The University of Sydney

February 2014

1 Introduction

This report has studied the general class group algorithm implemented in Magma Computer Algebra System, in particular the cases where the algorithm struggled to find a new relation to generate the class group. We will begin by introducing some definitions and results in the first couple of sections to help define the class group. Then present the definition of the class group and the algorithm for generating it in the subsequent sections, and finally concluding with the description of the hard case with some data.

2 Number fields

The term ring in this report means a commutative ring with a multiplicative identity 1 unless explicitly stated otherwise.

Definition 2.1 (Algebraic numbers) *A complex number α is called* algebraic *if it is algebraic over $\mathbb{Q}$, that is, if it satisfies a non-zero polynomial with the coefficients in $\mathbb{Q}$.*

Definition 2.2 (Number field) *A* number field *is a subfield $K \subset \mathbb{C}$ such that $[K : \mathbb{Q}]$ is finite.*

Postal Address: 111 Barry Street
c/- The University of Melbourne
Victoria 3010 Australia

Email: enquiries@amsi.org.au
Phone: +61 3 8344 1777
Fax: +61 3 9349 4106
Web: www.amsi.org.au

In particular every element in a number field is algebraic.

Now if K is a number field then there exist finitely many algebraic numbers $\alpha_1, \alpha_2, ..., \alpha_n$ such that $K = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ due to the degree of the extension being finite. We can also strengthen this observation.

Theorem 2.3 *If K is a number field then $K = \mathbb{Q}(\theta)$ for some algebraic number θ.*

We now define a subring of a number field that is analogue to $\mathbb{Z}$ inside $\mathbb{Q}$.

Definition 2.4 *An algebraic number α is called* algebraic integer *if it satisfies a monic polynomial with the coefficients in $\mathbb{Z}$. We will denote the set of algebraic integers to be $\mathcal{B}$.*

In particular this is equivalent to the minimal polynomial of α over $\mathbb{Q}$ having coefficients in $\mathbb{Z}$.

Definition 2.5 *The* ring of integers*(or the maximal order) $\mathcal{O}_K$ of a number field K is $\mathcal{O}_K := K \cap \mathcal{B}$.*

In particular the ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$.

From here on, K denotes an arbitrary number field and $\mathcal{O}$ its ring of integers.

Definition 2.6 *A basis for $\mathcal{O}$ as a $\mathbb{Z}$-module is called an* integral basis *for K(or for $\mathcal{O}$).*

In particular, an integral basis of K is also a basis of K as a $\mathbb{Q}$-vector space.

Theorem 2.7 *Every number field K has an integral basis, and $\mathcal{O}$ is a free $\mathbb{Z}$- module of rank n equal to the degree of K.*

Now a number field K is a subfield of $\mathbb{C}$, thus we can consider the embeddings of K into $\mathbb{C}$.

Proposition 2.8 *Let K be a number field of degree n. Then there exists n distinct monomorphisms*

$$\sigma_i : K \to \mathbb{C}, \quad 1 \leq i \leq n.$$

Call σ_i's, the embeddings of K.
We will let s be the number of real embeddings, that is, the number of embeddings σ such that $\sigma(K) \subset \mathbb{R}$. And call the other embeddings complex and use $2t$ for the number of them.

Using the embeddings and the integral basis, we can define the discriminant of a number field.

Definition 2.9 *Let K be a number field of degree n with the embeddings $\{\sigma_1, \sigma_2, ..., \sigma_n\}$ and an integral basis $\{\alpha_1, \alpha_2, ..., \alpha_n\}$.*
We define the discriminant *of K (or $\mathcal{O}$) to be the square of the discriminant of $n \times n$ matrix whose (i,j)-entry is $\sigma_i(\alpha_j)$. That is*

$$\Delta_K := \left(\det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \right)^2$$

By Theorem 2.7 and Proposition 2.8 the discriminant always exists and is an invariant of the number field.

We conclude this section on number fields by introducing a multiplicative function norm.

Definition 2.10 *Let K be a number field of degree n and $\sigma_1, \sigma_2, ..., \sigma_n$ be the embeddings. Define the* norm *of α in K to be*

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

3 Ideals

In the ring of integers $\mathcal{O}$, the prime factorisation of elements do not hold like in $\mathbb{Z}$. As a result, working with elements in this ring may not be appropriate. Instead, we are going to work with ideals of this ring.

Definition 3.1 *Let $\mathfrak{a}, \mathfrak{b}$ be ideals of a ring R, then the product of $\mathfrak{a}$ and $\mathfrak{b}$ is defined as* $\mathfrak{ab} := \{\sum_{i=1}^{n} \alpha_i \beta_i : \alpha_i \in \mathfrak{a}, \beta_i \in \mathfrak{b}\}$

Definition 3.2 *Let $\mathfrak{p}$ be a proper ideal of a ring R. $\mathfrak{p}$ is a prime ideal if $\mathfrak{bc} \subseteq \mathfrak{a} \implies$ either $\mathfrak{b} \subseteq \mathfrak{a}$ or $\mathfrak{c} \subseteq \mathfrak{a}$*

Definition 3.3 *Let $\mathfrak{a}$ be a $\mathcal{O}$-submodule of a number field K. $\mathfrak{a}$ is called a* fractional ideal *of $\mathcal{O}$ if there is a non-zero element $c \in \mathcal{O}$ such that $c\mathfrak{a} \subseteq \mathcal{O}$, that is, $c\mathfrak{a}$ is an ideal of $\mathcal{O}$.*
Define the set of all non-zero fractional ideals of $\mathcal{O}$ to be $\mathcal{F}$.

Theorem 3.4 *$\mathcal{F}$ is an abelian group under multiplication.*

Theorem 3.5 *Every non-zero ideal of the ring of integers $\mathcal{O}$ can be written as a product of prime ideals, unique up to the order of factors.*

Essentially, the prime factorisation of ideals is the reason we are working with ideals rather then elements of the ring.

Like the previous section we are going to conclude this section by introducing norm, but this time on ideals.

Definition 3.6 *Let $\mathfrak{a}$ be an ideal of the ring of integers $\mathcal{O}$. Define* norm *of $\mathfrak{a}$ as*

$$N(\mathfrak{a}) := |\mathcal{O} : \mathfrak{a}|$$

Proposition 3.7 *Let α be an element in the ring of integers $\mathcal{O}$, then*

$$|N(\alpha)| = N(<\alpha>)$$

4 Class Group

Lemma 4.1 *Let $\mathcal{P} := \{\mathfrak{a} \in \mathcal{F} : \exists c \in \mathcal{O}$ such that $c^{-1}\mathfrak{a}$ is a principal ideal$\}$.*
Then $\mathcal{P}$ is a normal subgroup of $\mathcal{F}$.

Theorem 4.2 *Let the* class group *of $\mathcal{O}$ to be the quotient group*

$$\mathcal{C}l(\mathcal{O}) := {}^{\mathcal{F}}\!/_{\mathcal{P}}$$

and call $h(\mathcal{O}) := |\mathcal{C}l(\mathcal{O})|$ the class number *of $\mathcal{O}$.*
Then $\mathcal{C}l(\mathcal{O})$ is an abelian group of finite order.

Corollary 4.3 *$\mathcal{O}$ is a principal ideal domain if and only if $\mathcal{C}l(\mathcal{O})$ is a trivial group.*

Theorem 4.4 *Every coset of $\mathcal{P}$ in $\mathcal{F}$ contains an ideal $\mathfrak{a}$ with*

$$N(\mathfrak{a}) \leq M_{st}\sqrt{|\Delta|}$$

where $M_{st} := \left(\frac{4}{\pi}\right)^t \frac{(s+2t)!}{(s+2t)^{s+2t}}$ *and,*

s and $2t$ are the number of real and complex embeddings from Proposition 2.8.

Definition 4.5 *Define* factor base *to be the set*
$FB := \{\mathfrak{p} < \mathcal{O} : \mathfrak{p}$ *is a prime ideal and* $N(\mathfrak{p}) \leq M_{st}\sqrt{|\Delta|}\}$.

Now by Theorem 3.5 and 4.4, we have

Proposition 4.6 $\mathcal{C}l(\mathcal{O}) = {}^{<FB>}\!/_{<FB> \cap \mathcal{P}}$

5 Class group algorithm

In the class group algorithm, we will present the class group in the form similar to Proposition 4.6. That is, treat the class group as a free abelian group generated by ideals in FB and find the relations between the generators. The relations here correspond to $< FB > \cap \mathcal{P}$ in the proposition and is a subgroup of $< FB >$.

Now the algorithm in this report is only described briefly to show the main ideas and the reader should refer to Cohen(1996) for the full detail of the algorithm.

Outline of general class group algorithm

1. Generate FB
2. Generate a product of random ideals in FB
3. Find a short element α in the generated product
4. Factorise the principal ideal generated by α
5. If the principal ideal factors over ideals in FB, record the factors as a relation
6. Repeat step 2 to 5 until the stopping condition has been met

6 Hard case

Sometimes, the relation recorded in step 5 of the algorithm may already be in the subgroup of relations already found. Such generation of old relations can happen repeatedly in some cases and in this report we have looked at two examples of such a case.

In both of the examples, the algorithm generated subgroup of index 2 of all the relations quite smoothly, but had trouble finding the relation in the other coset.

Now, going back to the algorithm, notice the generation of a relation is strongly influenced by the choice of the random ideals in step 2. Hence we have tested how the number of random ideals picked in step 2 affected which coset the generated relation belonged.

The number field we used for the first example is $\mathbb{Q}$ adjoined with the roots of $x^6 - 1269$ and adjoined the roots of $x^7 + 23810$ for the second example. We generated 1000 relations for each fixed number of random ideals used to form the product and recorded if the relation factorised over FB, and if it did, which coset it belonged.

Table 1: Distribution of the relation generated for $x^6 - 1269$

#Ideals	NS	New	Old
2	51	56	893
5	49	127	824
10	54	205	741
20	52	322	626
30	51	393	556

Table 2: Distribution of the relation generated for $x^7 + 23810$

#Ideals	NS	New	Old
2	856	1	143
5	967	1	32
10	972	1	27
20	975	2	23
30	969	4	27

In both of the tables, first column displays the number of random ideals used to form the product. Second column displays the number of relations that did not factorise

over FB (stands for non-smooth), third column the number of new relations and the last column the number of old relations generated.

In Table 1, the number of new relations clearly increased as the number of ideals increased, while the number of old relations decreased. On the other hand it is not clear whether the number of new relations increased in Table 2, as it may due to sample error. As a result, we have tested the second example again, this time generating 10000 relations each.

Table 3: Distribution of the relation generated for $x^7 + 23810$

#Ideals	NS	New	Old
2	8555	18	1427
5	9654	6	340
10	9644	9	347
20	9636	23	341
30	9629	41	330

Now it is clear that the number of new relations increased as the number of ideals increased with the exception of the case with two ideals. Although the number of new relations generated using two ideals is large, the number of old relations is also large as well. Consequently using two ideals has little benefit in this example.

In both of the examples, increasing the number of random ideals increased the chance of generating a new relation. This suggests that increasing the number of ideals may be a good strategy for increasing the chance of finding a new relation in general.

References

[1] Bosma, W. & Cannon, J. & Playoust, C. 1997, The Magma algebra system. I. The user language, *Journal of Symbolic Computation*, vol. 24, no. 3-4, pp. 235-265.

[2] Cohen, H. 1996, *A course in computational algebraic number theory*, Springer-Verlag, Berlin.

[3] Stewart, I. & Tall, D. 1979, *Algebraic Number Theory*, Chapman and Hall, London.