Fast multiquadratic classgroup computation

Jean-Francois Biasse[1] and Christine van Vredendaal[2]

[1] University of South Florida
Department of Mathematics and Statistics,
4020 E Fowler Avenue, Tampa, Florida, USA 33620
biasse@lix.polytechnique.fr

[2] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, NL
c.v.vredendaal@tue.nl

Abstract. Should have an abstract.

Keywords: multiquadratic fields

1 Introduction

Some intro should go here.

2 Preliminaries

2.1 Multiquadratic Fields

Definition 2.1 *Let d be squarefree integer d other than 1. The field*

$$\mathcal{K} = \mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Q}, \}$$

is called a quadratic field and has degree 2 over $\mathbb{Q}$.

These fields have all have signature $(2, 0)$ and therefore the unit group of any order in $\mathcal{K}$ is finitely generated by 1 generator of infinite order. This unit can be computed efficiently using the continued fraction method(see [2]). For the ring of integers $\mathcal{O}_\mathcal{K}$ of a field $\mathcal{K}$, we denote its the unit group by $\mathcal{O}_\mathcal{K}^\times$. For a quadratic field this group is isomorphic to $\mu(\mathcal{O}) \times \mathbb{Z}$ and generated by the fundamental unit ϵ. Here $\mu(\mathcal{O})$ is the finite cyclic group of roots of unity in $\mathcal{O}$.

Author list in alphabetical order; see https://www.ams.org/profession/leaders/culture/CultureStatement04.pdf. This work was supported by the Netherlands Organisation for Scientific Research (NWO) under grants 613.001.011 and 639.073.005 and other stuff? Calculations were carried out on the Saber cluster of the Cryptographic Implementations group at Technische Universiteit Eindhoven.

Definition 2.2 *Let $d_1, d_2, \ldots, d_n$ be squarefree integers that are multiplicatively independent modulo squares (i.e. they are independent in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$). The field*

$$L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n}),$$

is called a multiquadratic field and has degree $N = 2^n$ over $\mathbb{Q}$. Its Galois group $\mathrm{Gal}(L/\mathbb{Q})$ *is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$.*

2.2 Class Groups

2.3 How to Compute Class Groups

Definition 2.3 (relations) *We denote the relation of a field L of the principal ideal (α) as $\mathcal{R}_L((\alpha))$. $\mathcal{R}_L((\alpha)) = (\alpha, \boldsymbol{e})$ if and only if*

$$(\alpha) = \prod_{1 \le i \le B} \mathfrak{p}_i^{e_i},$$

where $\mathfrak{p}_i$ are prime ideals of L. The relations of L form a multiplicative group; a minimal set that forms the basis of this group is denoted by $\mathcal{R}el(L)$.

3 Theorems and proofs and properties needed for the algorithm

3.1 Relation subfield equation

Let $\mathcal{C}l_L, \mathcal{C}l_{K_\sigma}, \mathcal{C}l_{K_\tau}, \mathcal{C}l_{K_{\sigma\tau}}$ be the classgroups of respectively a multiquadratic field L and its 3 (multi)-quadratic subfields as defined before. Then we have a natural mapping $\phi : \mathcal{C}l_{K_\sigma} \times \mathcal{C}l_{K_\tau} \times \mathcal{C}l_{K_{\sigma\tau}} \to \mathcal{C}l_L$ defined by

$$\phi([\mathcal{I}_\sigma]_{K_\sigma}, [\mathcal{I}_\tau]_{K_\tau}, [\mathcal{I}_{\sigma\tau}]_{K_{\sigma\tau}}) = [(\mathcal{I}_\sigma \mathcal{I}_\tau \mathcal{I}_{\sigma\tau})\mathcal{O}_L]_L$$

where $\mathcal{I}_\ell$ is an ideal of K_ℓ for $\ell \in \{\sigma, \tau, \sigma\tau\}$ and $[\cdot]_\ell$ is a function that maps an ideal to its representative in the classgroup of ℓ.

Lemma 3.1 ([4]) *The kernel and cokernel of the map ϕ defined above are elementary 2-groups.*

Q1: does this hold for index 2 multiquadratic subfields of a multiquadratic field?
A1: do we even need it? I don't think so.

Definition 3.2 *Let $\mathcal{R}el(L), \mathcal{R}el(K_\sigma), \mathcal{R}el(K_\tau), \mathcal{R}el(K_{\sigma\tau})$ Then we have a natural mapping $\psi : \mathcal{R}el(K_\sigma) \times \mathcal{R}el(K_\tau) \times \mathcal{R}el(K_{\sigma\tau}) \to \mathcal{R}el(L)$ defined by*

$$\psi(\mathcal{R}_{K_\sigma}(\mathcal{I}_\sigma), \mathcal{R}_{K_\tau}(\mathcal{I}_\tau), \mathcal{R}_{K_{\sigma\tau}}(\mathcal{I}_{\sigma\tau}) = \mathcal{R}_L((\mathcal{I}_\sigma \mathcal{I}_\tau \mathcal{I}_{\sigma\tau})\mathcal{O}_L)$$

where $\mathcal{I}_\ell$ is a principal ideal of K_ℓ for $\ell \in \{\sigma, \tau, \sigma\tau\}$.

In other words the map ψ takes relations of the subfields of L and maps them to relations in L. We now look at what that mapping looks like.

Theorem 3.3 *Let $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ be a multiquadratic field. Let K_σ be a (multi)-quadratic subfield fixed by σ. Without loss of generality assume $[L : K_\sigma] = 2$. Let $\mathcal{R}_{K_\sigma}((\alpha)) = (\alpha, \boldsymbol{e})$ be a relation of K_σ. Then $(\alpha, \boldsymbol{e}') = \mathcal{R}_L((\alpha))$ is a relation of L with $\boldsymbol{e}' = (e_1\boldsymbol{f}_1|e_2\boldsymbol{f}_2|\ldots|e_B\boldsymbol{f}_B)$, where $\boldsymbol{f}_i$ are the ramification indices such that prime ideals $\mathfrak{p}_i$ of L factor as $\prod_{f_j \in \boldsymbol{f}_i} \mathfrak{P}_j^{f_j}$.*

Proof. Suppose for $\alpha \in K_\sigma$ we have the relation given by

$$(\alpha) = \prod_{1 \le i \le B} \mathfrak{p}_i^{e_i},$$

where B is the cardinality of the factor base of K_σ and $\mathfrak{p}_i$ its prime ideals. Then

$$N_{K_\sigma : \mathbb{Q}}(\alpha) = \prod_{1 \le i \le b} p_i^{e'_i},$$

where b is the number of different primes that the prime ideals lie over.

Then because we have $\alpha \in L$ and $[L : K_\sigma] = 2$

$$N_{L:\mathbb{Q}}(\alpha) = \prod_{1 \le i \le B} p_i^{2e'_i},$$

which means that α is B-smooth in L. We also know that for each prime ideal $\mathfrak{p}_i \in K_\sigma$ holds

$$\mathfrak{p}_i \mathcal{O}_{\mathcal{L}} = \prod_{1 \le j \le B'} \mathfrak{P}_j^{f_j},$$

where the $\mathfrak{P}_j$ are the prime ideals of L that lie over $\mathfrak{p}_i$ and the f_j are the ramification indices. Let $\boldsymbol{f}_i$ be the vector of ramification indices for $\mathfrak{p}_i$. From this follows

$$\begin{aligned}(\alpha) &= \prod_{1 \le i \le B} \mathfrak{p}_i^{e_i} \\ &= \prod_{1 \le i \le B} \prod_{1 \le j \le B'} \mathfrak{P}_j^{e_i f_j}.\end{aligned}$$

Therefore $(\alpha, (e_1\boldsymbol{f}_1|e_2\boldsymbol{f}_2|\ldots|e_B\boldsymbol{f}_B))$ is a relation in L. □

Q2: are all primes unramified in multiquadratic fields?
A2: seems to be the case, is this easy to see/show? maybe only for specific primes
TODO: simplify the proof if this is the case.

Corollary 3.4 *The set $U = \mathcal{R}el(K_\sigma) \cup \mathcal{R}el(K_\tau) \cup \mathcal{R}el(K_{\sigma\tau})$ covers all relations that result from pricipal ideals in the subgroup $\mathcal{P}(K_\sigma) \times \mathcal{P}(K_\tau) \times \mathcal{P}(K_\sigma \tau)$ of $\mathcal{P}(L)$.*

Lemma 3.5 *Let L be a real multiquadratic field and let σ, τ be distinct non-identity automorphisms of L. Define $\sigma\tau = \sigma \circ \tau$. For $\ell \in \{\sigma, \tau, \sigma\tau\}$ let K_ℓ be the subfield of L fixed by ℓ. Define $U = \mathcal{R}el(K_\sigma) \cup \mathcal{R}el(K_\tau) \cup \sigma(\mathcal{R}el(K_{\sigma\tau}))$. Here $\sigma(\mathcal{R}el(K_{\sigma\tau})) = \bigcup_{(\alpha, \boldsymbol{e}) \in \mathcal{R}el(K_{\sigma\tau})} \mathcal{R}_{K_{\sigma\tau}}(\sigma(\alpha))$.*
Then

$$(\mathcal{R}el(L))^2 \leq U \leq \mathcal{R}el(L),$$

where $(\mathcal{R}el(L))^2$ denotes the relations that span $(\mathcal{C}l_L)^2$.

Proof. The relations in $\mathcal{R}el(K_\sigma), \mathcal{R}el(K_\tau)$ and $\mathcal{R}el(K_{\sigma\tau})$ span respectively the principal ideals in $\mathcal{P}(K_\sigma), \mathcal{P}(K_\tau)$ and $\mathcal{P}(K_{\sigma\tau})$, which in turn are subgroups of $\mathcal{P}(L)$. The automorphism σ on $\mathcal{P}(K_{\sigma\tau})$ preserves $\mathcal{P}(K_{\sigma\tau})$, so $\sigma(\mathcal{P}(K_{\sigma\tau}))$ is also a subgroup of $\mathcal{P}(L)$. From this the second inclusion follows.

For the first inclusion, let $\mathfrak{a} = (\alpha) \in \mathcal{P}(L)$ and $(\alpha, \boldsymbol{e})$ its corresponding relation in $\mathcal{R}el(L)$. Then $N_{L:K_\ell}(\mathfrak{a}) \in \mathcal{P}(K_\ell)$ for $\ell \in \{\sigma, \tau, \sigma\tau\}$. Each non-identity automorphism of L has order 2, so in particular each $\ell \in \{\sigma, \tau, \sigma\tau\}$ has order 2 (if $\sigma\tau$ is the identity then $\sigma = \sigma\sigma\tau = \tau$, contradiction), so $N_{L:K_\ell}(\mathfrak{a}) = (\alpha \cdot \ell(\alpha))\mathcal{O}_{K_\ell}$. We also have that holds (see [1])

$$\frac{N_{L:K_\sigma}(\alpha) N_{L:K_\tau}(\alpha)}{\sigma(N_{L:K_{\sigma\tau}}(\alpha))} = \frac{\alpha \cdot \sigma(\alpha) \cdot \alpha \cdot \tau(\alpha)}{\sigma(\alpha \cdot \sigma\tau(\alpha))} = \alpha^2.$$

Hence α^2 is a linear combination of relations in $\mathcal{R}el(K_\sigma), \mathcal{R}el(K_\tau)$ and $\sigma(\mathcal{R}el(K_{\sigma\tau}))$. This holds for each $(\alpha) \in \mathcal{P}(L)$, so $(\mathcal{R}el(L))^2$ is a subgroup of U. □

4 The Algorithm

4.1 The algorithm

4.2 Heuristic running time

4.3 Open questions

Q3: What happens to $\mathcal{R}el(L)$ if σ is applied.
A3: Simple linear transformation of the relations (since we can compute $\sigma(\mathfrak{p})$ for all prime ideals)
Q4: Are there precision issues?
A4: Since we are not dealing with embeddings, I don't see any issues.
Q5: I still need to clarify how findSquares **works.**
A5:I think since all relations are essentially linear relations and squareroot of the relation in the quadratic fields, you only have to compute the characters for the relations in the quadratic fields and the you can just take linear combinations for the rest. You get a theorem like Theorem 5.2 of [1].

Algorithm 4.1: MQClassGroup(L)

```
Input: Real multiquadratic field $L$
Result: $\mathcal{C}l_L$
if $[L : \mathbb{Q}] = 1$ then
    return some error
if $[L : \mathbb{Q}] = 2$ then
    return QClassGroup($L$)
$\sigma, \tau \leftarrow$ distinct non-identity automorphisms of $L$
for $\ell \in \{\sigma, \tau, \sigma\tau\}$ do
    $K_\ell \leftarrow$ fixed field of $\ell$
    $\mathcal{R}el(K_\ell), \mathcal{C}l_{K_\ell} \leftarrow$ MQClassGroup($K_\ell$)
$U \leftarrow \mathcal{R}el(K_\sigma) \cup \mathcal{R}el(K_\tau) \cup \sigma(\mathcal{R}el(K_{\sigma\tau}))$
$\mathcal{R}el(L) \leftarrow$ findSquares($U$)
return $\mathcal{R}el(L)$, ClassGroup($\mathcal{R}el(L)$)
```

Q6: This algorithm implies that the largest prime you need is the the largest prime of the largest quadratic field. given the adjoined squareroots, the largest discriminant and therefor prime bound can be calculated. This should be usable somehow.
Q7: It also seems that for the all of one example I tried, the "The discriminant of a multiquadratic field is the product of the discriminant of its quadratic subfields". This might be dependent on which squares are adjoined, but might be something to look into.
A7: This might be only for $1 \bmod 4$ primes? Or maybe not?
Q8: Can the Biasse SAC 2017 preprocessing paper be used to make a class group precomputation to make [1] even faster? But this is only if everything works.
Q9: There are still statements in Kubota [3] that I think could help, or at least should be referenced for completeness sake. However, the German is too confusing for a novice.

5 Results

Hopefully with some implementation (maybe compare with Sage???)

References

1. Jens Bauch, Daniel J. Bernstein, Henry de Valence, Tanja Lange, and Christine van Vredendaal. Short generators without quantum computers: The case of multiquadratics. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, volume 10210 of *Lecture Notes in Computer Science*, pages 27–59, 2017.

2. Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag New York, Inc., New York, NY, USA, 1993.
3. Tomio Kubota. Über den bizyklischen biquadratischen Zahlkörper. *Nagoya Math. J.*, 10:65–85, 1956.
4. Patrick J. Sime. On the ideal class group of real biquadratic fields. *Trans. Amer. Math. Soc.*, 347:4855–48–4876, 1995.