Computing the Hilbert class field of quartic CM fields

Jared Asuncion - Universite de Bordeaux / Universiteit Leiden

Motivation

Compute the largest unramified abelian extension of a number field.

By compute, we mean: find an algorithm that gives a set α of algebraic numbers such that $K(\alpha)$ is equal to $H_K(1)$, the Hilbert class field of K.

Unramified extension: all places of K are unramified in L

- **unramified** prime ideals (finite places)

example
$L = \mathbb{Q}(i)$
$K = \mathbb{Q}$

× $(2) = (2, 1+i)^2$
✓ $(3) = (3)^1$
✓ $(5) = (5, i+2)^1(5, i+3)^1$

- **unramified** embeddings (infinite places)

✓ real emb in $K \rightsquigarrow$ real emb in L
× real emb in $K \rightsquigarrow$ complex emb in L
✓ complex emb in $K \rightsquigarrow$ complex emb in L

Abelian extension: Galois extension whose Galois group is abelian

- class field theory (20th century) $\rightsquigarrow$ existence of set of fields $\{H_K^+(m) : m \in \mathbb{Z}_{>0}\}$ satisfying
  1. $\mathrm{Gal}(H_K^+(m)/K) \cong \mathrm{Cl}_K^+(m)$, a group described in terms of ideals of $\mathcal{O}_K$
  2. $\forall$ abelian exts L/K which do not ramify at infinite places of K $\exists m$ s.t. $L \subseteq H_K(m)$.
     $\forall$ abelian exts L/K $\exists m$ s.t. $L \subseteq H_K^+(m)$.

What do we know?

Let $m \in \mathbb{Z}_{>0}$.

✓ $H_{\mathbb{Q}}^+(m) = \mathbb{Q}(\exp(2\pi i \cdot 1/m))$
(...by Kronecker-Weber Theorem, 19th century)

✓ $H_K^+(m)$; $K = \mathbb{Q}(\sqrt{D}), D \in \mathbb{Q}, D < 0$
(...by class field theory + CM theory)

- $H_K^+(m)$ $K = \mathbb{Q}(\sqrt{D})$, $D > 0$
  (...solved if Stark's conjectures are true [13, 8])
- $H_K^+(m)$ when K is a quartic CM field
  (...what this poster is about)

CM Theory

CM field: $K = K_0(\sqrt{\delta})$ s.t.

- K_0 totally real
- $\delta \in K_0$ s.t. $\delta \ll 0$

Reflex field: K^r, a field related to K and a *CM type* Φ of K.

Main Theorem of CM [10]:
For each $m \in \mathbb{Z}_{>0}$...

- ...we can compute the following abelian extension of K:
  $$\mathrm{CM}_K(m) := K(j_{A,m}) \text{ s.t.}$$
  - $\mathrm{CM}_K(m) \subseteq H_K(m)$
  - $j_{A,m}$, set of invariants associated to the m-torsion points of a principally polarized abelian variety A with $\mathrm{End}\, A \cong \mathcal{O}_{K^r}$ (CM by $\mathcal{O}_{K^r}$) of type Φ.
- ...we can find the subgroup:
  $$J_m \leq G := \mathrm{Gal}(H_K(m)/K)$$
  s.t. $H_K(m)^{J_m} = \mathrm{CM}_K(m)$.

A theorem of Shimura

Shimura [11]: Given K, primitive quartic CM field (i.e. degree 4 CM field that is either cyclic Galois or not Galois),
then $\exists\ m \in \mathbb{Z}_{>0}$ such that

$$H_K(1) \subseteq H_{K_0}(m)\,\mathrm{CM}_K(m) \qquad (\star_m)$$

holds .... what can we say about such m?

An integer m for which $\star_m$ holds.

Theorem (Asuncion). Let K be a primitive quartic CM field. Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that

1. $|\mathrm{Cl}_K(1)/\langle S\rangle|$ is odd
2. S contains all prime ideals of $\mathcal{O}_K$ above 2
3. S contains at least three elements

Let P be the set of rational primes p below the prime ideals in S. Then, $\star_m$ holds for $m = 4\prod_{p\in P} p$.

Key points of proof:

- to find S: unramified-outside-S emb. problem [3]
- to determine valuation at each $\mathfrak{p} \in S$: [2]

Given an integer m, does $\star_m$ hold?

Assume K, primitive quartic CM field.

1. Express $\star_m \rightsquigarrow$ in terms of Galois theory:
   $$G(H_K(1)) \supseteq G(KH_{K_0}(m)) \cap G(\mathrm{CM}_K(m))$$
   where $G(F) := \mathrm{Gal}(H_K(m)/F)$.
   Class field theory can compute groups $\cong$ to:
   ✓ $G(H_K(1))$ ✓ $G(H_{K_0}(m))$
2. [1, 5] study group related to $G(\mathrm{CM}_K(1))$.
   We generalize method to find $G(\mathrm{CM}_K(m))$.
3. Compute $\cap$ and check $\supseteq$ to answer question.

- Implemented in PARI/GP [7] by the author.

CM fields examples

- CM fields of degree 2:
  $K = K_0(\sqrt{D}), D < 0, K_0 = \mathbb{Q}$,
  $K^r = K$,
  CM type Φ (one choice up to $\sim$)
  Let E be an ell curve of type Φ s.t. $\mathrm{End}\, E \cong \mathcal{O}_{K^r}$
  - $\mathrm{CM}_K(1) = K(j(E))$
    $j(E) \rightsquigarrow j$-invariant of E
  - $\mathrm{CM}_K(m) = K(j(E))(X_m)$
    X_m is the set of 'normalized' x-coordinates of m-torsion points of E
  - $J_m = \langle 1\rangle \quad \forall m \in \mathbb{Z}_{>0}$
    $\rightsquigarrow H_K(m) = \mathrm{CM}_K(m)$ ✓
- CM fields of degree 4
  $K = K_0(\sqrt{\delta}), \delta \in K_0, \delta \ll 0$,
  $K_0 = \mathbb{Q}(\sqrt{D})$, $D > 0$.
  - **Reflex field?** We can solve it!
  - **j-invariant analogue?**
    Yes – Igusa invariants [6].
  - $J_1 = \langle 1\rangle$? No, not necessarily!

Computing $H_K(1)$ when $\star_m$ holds.

Assume K, primitive quartic CM field.

Computing $H_{K_0}(m)$.

1. Assume Stark's conjectures are true.
2. Solve for $H_{K_0}(m)$.
3. Verify if result is correct.

Computing $\mathrm{CM}_K(m)$

1. $m = 1$: use Igusa invariants, see [6, 12, 4].
2. $m = 2$: use Rosenhain invariants [15].

- $m > 2$: future work.

Computing $H_K(1)$ **if** $\star_m$ with $m \leq 2$.

1. Compute $H_{K_0}(m)$ and $\mathrm{CM}_K(m)$.
2. Compute $H_K(1)$ as a subfield of the compositum. Use Galois theory + explicit Shimura reciprocity [14].

Our SAGE [9] **Implementation**

- **...computes** $H_K(1)$ when $\star_m$ holds, for examples where $\mathrm{Cl}_K(1)$ is cyclic and degree 32 within 15 minutes
- **...vs existing Kummer theory implementations**
  PARI and MAGMA do not finish this computation within 4 hours.

References.

[1] Reinier Bröker, David Gruenewald, and Kristin Lauter. Explicit CM theory for level 2-structures on abelian surfaces. In: Algebra & Number Theory 5.4 (Dec. 2011),

[2] Henri Cohen. Advanced topics in computational number theory. Graduate Texts in Mathematics. New York: Springer, 2000.

[3] Teresa Crespo. Embedding problems with ramification conditions. In: Arch. Math. (Basel) 53.3 (1989),

[4] Régis Dupont. Fast evaluation of modular functions using Newton iterations and the AGM. In: Mathematics of Computation 80.275 (2011),

[5] Andreas Enge and Emmanuel Thomé. Computing class polynomials for abelian surfaces. In: Experimental Mathematics 23 (2014),

[6] Jun-ichi Igusa. Modular forms and projective invariants. In: American Journal of Mathematics 89.3 (1967),

[7] PARI/GP version 2.11.2. available from http://pari.math.u-bordeaux.fr/. The PARI Group. Univ. Bordeaux, 2019.

[8] Xavier-François Roblot. Stark's conjectures and Hilbert's twelfth problem. In: Experiment. Math. 9.2 (2000),

[9] W. A. Stein et al. Sage Mathematics Software (Version 9.1). http://www.sagemath.org. The Sage Development Team. 2020.

[10] Goro Shimura. Introduction to the Arithmetic Theory of Automorphic Functions. Kanô memorial lectures. Princeton University Press, 1971.

[11] Goro Shimura. On the class-fields obtained by complex multiplication of abelian varieties. In: Osaka Math. J. 14.1 (1962),

[12] Anne-Monika Spallek. Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen. In: 1994.

[13] H.M. Stark. Values of L-Functions at s = 1 I. L-Functions for quadratic forms. In: Advances in Mathematics 7.3 (1971),

[14] Marco Streng. An explicit version of Shimura's reciprocity law for Siegel modular functions. 2011. arXiv: 1201.0020 [math.NT].

[15] Paul B. van Wamelen. Examples of genus two CM curves defined over the rationals. In: Math. Comput. 68 (1999),

Credits. Poster template is a modified version of Dreuw and Deselaer's Poster template. Emojis are from Twitter's open-source emoji project, twemoji.