Fake Real Quadratic Orders

Hongyan Wang

December 3, 2016

1 Introduction

The FRQO library contains the implementation of various subroutines utilized for the test of the Cohen-Lenstra heuristics and the Ankeny-Artin-Chowla conjecture. FRQO is maintained by Hongyan Wang, and is an appendix to the Master's thesis *Fake Real Quadratic Orders* [Wan16], written under the supervision of Renate Scheidler and Michael J. Jacobson, Jr. It is highly recommended to read the thesis before utilizing the library.

2 Dependencies on FRQO

FRQO depends on several libraries and specifications that need to be present on your system prior to the installation. These libraries are:

- GMP, *gmplib.org*. The GNU multiple precision arithmetic library;
- optarith, *github.com/maxwellsayles/liboptarith*. Optimized arithmetic operations for 32, 64 and 128 bit integers. Includes optimized implementations of many different extended GCD algorithms;
- qform, *github.com/maxwellsayles/libqform*. Ideal class group arithmetic in imaginary quadratic fields.
- LMFDB, *lmfdb.org/NumberField/QuadraticImaginaryClassGroups*. Tabulations of class groups of imaginary quadratic fields for $|D|$ up to 2^{40}.

Before installing, make sure that each of those libraries is installed. Our computations are based on Mosunov's data base of the tabulation of class groups of imaginary quadratic fields for $|D|$ up to 2^{40} [Mos15]. Make sure you have downloaded these files before installing the library.

3 Building and using FRQO

The easiest way to use FRQO is to build it using **make**. The **make** command creates an executable file, **frqo**. To run the program, use the command **./frqo** *index*.

4 Files

The FRQO library contains the following files:

- **myfunctions.c** contains functions utilized to compute orders of ideals in imaginary quadratic fields. This is mainly for the test of the Cohen-Lenstra heuristics.

- **generator.c** contains routines utilized for the computation of the fundamental unit of a fake real quadratic order. This is mainly for the test of the Ankeny-Artin-Chowla conjecture.

- The files entitled **myfunctions.h** and **generator.h** contain declarations of all the subroutines implemented in files listed above;

- The **main.c** file contains the implementation of a command line program for the test of the Cohen-Lenstra heuristics and the Ankeny-Artin-Chowla conjecture.

5 Setup

Before installing the FRQO library, make sure that all the libraries that FRQO depends on are installed while the data base of the tabulation of class groups of imaginary quadratic fields are downloaded (see Section 2). Pay a particular attention to the **optarith** library. Before installing it, ensure that there are enough primes defined in files primes.c, primes.h, and their quadratic residues are precomputed in **sqrtmodp_list.c**, **sqrtmodp_list.h**. Several functions of the FRQO library heavily rely on these precomputed values. If you observed that there are not enough primes suitable for your needs, please compile the program **gen_sqrtmodp.cc** located in the folder **code_gen**. Run this program by providing to it the total number of primes you wish to generate as a parameter. It will generate two new files, **sqrtmodp_list.c** and **sqrtmodp_list.h**. Replace the old files with this name by the new ones, and then build the optarith library again with these new files.

In order to prepare the FRQO library for compilation, please edit the **main.c**.

- **myprimes** defines the list of primes we want to deal with;

- **folder** defines the location of the data base of the tabulation of class groups of imaginary quadratic fields;

- **name** defines the names and locations of output files.

In addition, modify the location of libraries and header files in **Makefile**.

6 Tests of Conjectures

Our program is based on Mosunov's tabulation of class groups of imaginary quadratic fields for $|D|$ up to 2^{40} [Mos15]. The data are stored in four folders according to the congruence class of $|D|$ modulo 8 or 16. These four folders are cl3mod8, cl7mod8, cl4mod16 and cl8mod16.

Each folder contains 4096 compressed files with indices $0, 1, 2, ..., 4095$. The file with index l contains data for $l \cdot 2^{28} < |D| < (l+1) \cdot 2^{28}$. For example, the file cl7mod8.45.gz contains data for $45 \cdot 2^{28} < |D| < 46 \cdot 2^{28}$ with $|D| \equiv 7 \mod 8$. For file cl$A$mod$M.I$.gz, where $(A, M) = (3, 8), (7, 8), (4, 16)$ or $(8, 16)$ and $I = 0, 1, ..., 4095$, after we decompress the file, it has the following format:

- There is one line for each discriminant
- Discriminants are listed in ascending order (in absolute value)
- Line i for i^{th} discriminant D_i has the form $a\ b\ c_1 c_2 ... c_t$
- $|D_i| = |D_{i-1}| + aM$, $h(\mathbb{Q}(D_i)) = b$, invariant factors for the class group are $[c_1, c_2, ..., c_t]$ and $b = c_1 c_2 ... c_t$
- $|D_1|$ is given by $|D_1| = I \cdot 2^{28} + a_1$ where a_1 is the first number in line 1

For our computation, we simply need the first two columns of each line. Since the discriminants in the files with the same index are in the same interval, we perform our computation index by index. For each index, we read files from four folders and conduct computation for each discriminant.

7 File Formats

Each index generates two files, **fac_idx_cohen** and **fac_idx_aac**, corresponding to the Cohen-Lenstra heuristics and the Ankeny-Artin-Chowla conjecture, respectively. **fac_idx_cohen** contains m lines where m is the number primes in the array **myprimes**. The kth line corresponds to the kth prime number, p_k, and contains two integers, n_1 and n_2. n_1 is the number of fake real quadratic orders for idx$\cdot 2^{28} \leq |D| \leq$ (idx+1) $\cdot\, 2^{28}$ and $p = p_k$, while n_2 is the number of fake real quadratic orders for which the odd part of the class number equals one for idx$\cdot 2^{28} \leq |D| \leq$ (idx+1) $\cdot\, 2^{28}$ and $p = p_k$. Then the proportion of fake real quadratic orders for which the odd part of the class number equals one can be computed by accumulating the counters for each prime.

For example, **fac_0_cohen** looks like the following table

27198208	20993865
30597983	23603950
33997786	26202651
35697664	27503039
37397587	28779368
...	...

So for $p = p_1$, the proportion of $\mathcal{O}_{K,p}$ for which the odd part of the class number equals one for $|D|$ up to 2^{28} can be computed by $20993865/27198208 \approx 0.77$.

fac_idx_aac is use to record counterexamples to the Ankeny-Artin-Chowla conjecture for all primes in **myprimes** with idx$\cdot 2^{28} \leq |D| \leq (\text{idx}+1) \cdot 2^{28}$. Each line represents one counterexample and has the form "$D \quad p$". For example **fac_0_aac** looks like

-3	7
-3	1009
-89716079	11

The first line implies that $\mathcal{O}_{K,7}$ is violates the Ankeny-Artin-Chowla conjecture where $K = \mathbb{Q}(\sqrt{-3})$.

8 Examples

To run the program for index=0, we simply use the command line

./frqo 0

To run the program for index=4095, we use the command line

./frqo 4095

References

[Mos15] Anton S. Mosunov. Unconditional class group tabulation of imaginary quadratic fields to 2^{40}. *Master's Thesis, University of Calgary*, 2015.

[Wan16] Hongyan Wang. Fake real quadratic orders. *Master's Thesis, University of Calgary*, 2016.