bnfinit

Loïc Grenié

26 Janvier 2012

1 The math

We want to compute the class group $\mathcal{C}\ell_K$ and the unit group of a number field K.

For any real x we define $\mathcal{B}_x$ to be the set of prime ideals of K of norm at most x. There is a theorem of Belabas, Diaz y Diaz and Friedman which gives a criterion to check if a real T is such that $\mathcal{B}_T$ contains a set of generators of $\mathcal{C}\ell_K$. We suppose we have chosen such a T.

Let $n_T = \#\mathcal{B}_T$, $\mathcal{I}_T$ be the group of ideals generated by $\mathcal{B}_T$ and

$$K_T = \{x \in K \mid (x) \in \mathcal{I}_T\}\ .$$

We identify all ideals of $\mathcal{I}_T$ with its set of exponents in $X_T = \mathbf{Z}^{\mathcal{B}_T}$. We need to find a set E of elements of K_T such that the lattice L_E they lattice they generate in X is such that

$$\mathcal{C}\ell_K \simeq X/L_E\ .$$

Moreover, if E has n elements, we can give two different facorizations of $n - n_E$ principal ideals, which means we have $n - n_E$ units. We also need to increase E up to the point where those units generate the unit group (modulo torsion units). Since $\mathcal{B}_T$ is a set of generators,the elements of E will be called relations.

We know we have finished using the analytic class number formula

$$\operatorname{res}_{s=1} \zeta_K = \lim_{s\to 1} \frac{\zeta_K(s)}{\zeta(s)} = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot h_K \cdot \operatorname{Reg}_K}{w_K \cdot \sqrt{|D_K|}}$$

where everything except h_K and Reg_K can easily be computed at initialization (we compute an approximation of the residue using the Euler products of the ζ functions).

Give E we compute $h_E = \#E/L_E$ and Reg_E which is the volume of the fundamental cell of the lattice of logarithmic embedings of the $n_E - n$ units. If E is too small the lattices are either of too small dimension or of correct dimension but with finite index with respect to the effective index. In that case,

$$\frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot h_E \cdot \operatorname{Reg}_E}{w_K \cdot \sqrt{|D_K|}}$$

will be a submultiple of $\operatorname{res}_{s=1} \zeta_K(s)$. In that case we increase E until the two parts of the equal sign agree.

2 What pari does

There is a certain number of free relations, these are the prime $p \in \mathbf{Z}$ such that $p \in K_T$.

After those, we need to find enough relations. There are two ways in PARI to find relations.

2.1 small_norm

The first function called in `bnfinit` is `small_norm`. Given an ideal I it checks some elements of $x \in I$ to see whether $x \in K_T$. The elements it checks are those with small coefficients in the ideal basis.

The function `small_norm` is called one or more times, depending on the field. The first time, it runs with $I \in \mathcal{B}_T$, i.e. all the prime ideals in the factor base. If it is not sufficient, it runs a second time, on a suitable subset B_1 of $\mathcal{B}_T$ but this time it runs with $I = \mathfrak{P}_1\mathfrak{P}$ where $\mathfrak{P}$ runs in B_1 and $\mathfrak{P}_1$ is the first element of $\mathcal{B}_T$. The third time it runs on a suitable subset $B_2 \subseteq B_1$ and takes $I = \mathfrak{P}_2\mathfrak{P}$ where $\mathfrak{P}$ runs in B_2 and $\mathfrak{P}_2$ is the second element of $\mathcal{B}_T$. This goes on as long as E is not large enough or $\mathfrak{P}_i$ has exhausted $\mathcal{B}_T$.

2.2 rnd_rel

The function `rnd_rel` is similar to `small_norm`, however the each element of the subset B_k is multiplied by an ideal

$$\mathfrak{P}_1^{n_1} \cdot \mathfrak{P}_2^{n_2} \cdots \mathfrak{P}_r^{n_r}$$

where $\mathfrak{P}_1$, ..., $\mathfrak{P}_r$ is a (slowly varying) fixed subset of $\mathcal{B}_T$ and r is a (nearly) fixed number between 3 and roughly 10. At each run of `rnd_rel` we pick a set n_1, ..., n_r of exponents.

2.3 HNF

After each run of `small_norm` or `rnd_rel` we have a set of relations, that is a set of integer vectors of X. PARI computes the HNF of the complete set of relations and does the same operations on the logarithmic embeddings of the elements of E (that's why we need the matrix U in HNF). Each zero column in the HNF matrix corresponds to a unit and the real part of the logarithmic embeddings give the generators of the unit lattice we generate so far.

At the end of the HNF reduction, we have a certain number of ideals that correspond to the pivots of the HNF. The set B_i for the next run of `small_norm` or `rnd_rel` is the complementary of the set of pivots.

3 What is needed

3.1 Some tuning

Where do we stop doing one thing ?

3.2 Good HNF

3.3 New method for finding elements

3.4 Get rid of logarithmic embeddings

4 Example

```
bnfinit(x^4-nextprime(10^8));
```