On the computation of automorphisms of a Nilpotent Galois extension of number field

B. Allombert

IMB
CNRS/Université Bordeaux 1

18/12/2018

Introduction

Let $T \in \mathbb{Z}[X]$ be a monic irreducible polynomial and assume that T is totally split over the splitting field $L = \mathbb{Q}[X]/(T)$. This is equivalent to say that $L/\mathbb{Q}$ is a Galois extension.
The set S of roots of T over L are in bijection with the group $\mathrm{Gal}(L/\mathbb{Q})$:

$$\begin{array}{rcl} S & \to & (\mathbb{Q}[X]/(T) \to L) \\ \alpha & \mapsto & (P(X) \mapsto P(\alpha)) \end{array}$$

The goal is to compute the set S and its group structure.

Factorization over number fields

Let p be prime number such that T is squarefree modulo p. Let P be the set of maximal ideals of $\mathcal{O}_K$ above p so that $p\mathcal{O}_L = \prod_{\mathfrak{p}\in P}\mathfrak{p}$, $g = |P|$ and f the residual degree.
Classical polynomial method (nfroots) : Pick an element $\mathfrak{p}$ of P, find the solutions of

$$T(S) = 0 \pmod{\mathfrak{p}} ,$$

lift them to $L_{\mathfrak{p}}$ and try to identify them as algebraic number using LLL (Lenstra).
Problem : Since we are using a single prime ideal, the precision is huge and LLL will is very costly.
Fundamental remark : When $\mathfrak{p}$ is inert it is much easier, no LLL is needed it is only a matter of recognizing the rational coefficients.

Frobenius lift

For any $\mathfrak{p} \in P$, there exists an unique $\phi \in G$ such that

$$\phi(x) = x^p \pmod{\mathfrak{p}}$$

(the Frobenius element). G acts transitively on P, so $P = \{\tau(\mathfrak{p}) | \tau \in G\}$. For all $\tau \in G$ we have

$$\tau\phi\tau^{-1}(x) = x^p \pmod{\tau(\mathfrak{p})}$$

In particular if ϕ is in the center of G, then

$$\phi(x) = x^p \pmod{\tau(\mathfrak{p})}$$

for all τ and so by Chinese remainder theorem,

$$\phi(x) = x^p \pmod{p\mathbb{Z}_L}\ .$$

Lifting algorithm

In my thesis I give a detailed algorithm for the following problem.

Let Φ the natural map from G to

$$A = Aut(\mathbb{Z}_L/p\mathbb{Z}_L) \cong Aut(\mathbb{F}_p[X]/T)\ .$$

There exist an a polynomial-time algorithm that determines whether an element $a \in A$ is in the image of Φ and if so returns the corresponding element s of S. If some precomputation depending only on G and p are performed, the algorithm is very efficient.

$$A \cong Aut(\mathbb{F}_p[X]/T) \cong C_f \wr \mathfrak{S}_g$$

If p is inert, then Φ is an isomorphism, otherwise it is only one-to-one, A being of order $f^g g!$ which is much larger than n. If p is totall split, then $A = \mathfrak{S}_n$. This allows to represent the elements of G by simple permutation, which makes composing them much faster.

The Abelian case

Acciaro-Klüners algorithm :
Apply the previous algorithm to the Frobenius

$$\phi(x) = x^p \pmod{p, T}$$

for various primes p until either it fails (then we know the group is not abelian) or until we have a set of generators (then we know the group is abelian).
Polynomial-time under GRH.

The supersolvable case

In my thesis, I describe an algorithm (used by galoisinit) that works for supersolvable groups, but is not polynomial-time. In practice, the smallest groups where the algorithm is too slow to be useful are of order $125 = 5^3$ and are nilpotent.

A group G is supersolvable if

- G is trivial or
- G admits a non-trivial cyclic normal subgroup F such that G/F is supersolvable.

A group G is nilpotent if

- G is trivial or
- G admits a non-trivial cyclic central subgroup F such that G/F is nilpotent.

p-groups are always nilpotent.

Stucture

It follows that in both case there is a family of generators $(g_i)_{i=1}^n$, a tower of subgroups $G_i = \langle g_1, \ldots, g_i \rangle$ such that $G = G_n$ and $g_i \pmod{G_{i-1}}$ is normal (resp. central) in G/G_{i-1}. Furthermore

- for all $h \in G$, $[h, g_i] \in G_i$ (resp. $[h, g_i] \in G_{i-1}$),
- the order of $g_i \pmod{G_i}$ is noted o_i and is called the relative order of g_i,
- an element of G can be written uniquely as a product $g_1^{e_1} \ldots g_n^{e_n}$ with $0 \leq e_j < o_j$ for $1 \leq j \leq n$.

The nilpotent case

If G is nilpotent, then $Z(G)$ is non trivial, so we can try to find $\mathfrak{p}$ non totally split such that the Frobenius ϕ is in $Z(G)$ in which case :

$$\phi(x) = x^p \pmod{\tau\mathfrak{p}}$$

for all τ of G and so

$$\phi(x) = x^p \pmod{p, T}$$

which we can lift to a solution in L with the above algorithm. If the algorithm returns false, we try another prime p. Under the Čebotarev density theorem, the probability of success is $(|Z(G)| - 1)/(|G| - 1)$ if we reject totally split primes (which occurs with probability $1/|G|$).

Lifting

The problem is actually to get the other solutions.
In my thesis, I explain how to compute the fixed field K of L by ϕ. $H = G/\langle\phi\rangle = \mathrm{Gal}(K/\mathbb{Q})$ is also nilpotent so we can apply the algorithm recursively. From this, we will recover the automorphisms of K, the generators of H as a nilpotent group, and for each generators a prime ideal of K such that the generator is the Frobenius of such prime.

Lifting

So let $\sigma \in H$ that is the Frobenius of some prime ideal $\mathfrak{q}$ in K above some prime $p \in \mathbb{Z}$. We pick a prime ideal $\mathfrak{p}$ above $\mathfrak{q}$ in L and extend σ to L to the Frobenius of $\mathfrak{p}$. Since ϕ is central, we have for all k

$$\sigma(x) = x^p \pmod{\phi^k(\mathfrak{p})}$$

so by Chinese remainder,

$$\sigma(x) = x^p \pmod{\mathfrak{q}\mathbb{Z}_L}$$

and so for any τ

$$\tau\sigma\tau^{-1}(x) = x^p \pmod{\tau(\mathfrak{q})\mathbb{Z}_L}$$

Bracket formula

We obtain the important formula :

$$[\tau, \sigma](x)^{p^{f-1}} = \sigma^{-1}(x) \pmod{\tau(\mathfrak{q})\mathbb{Z}_L}$$

Now assuming we have already computed $[\tau, \sigma]$ for all τ, we obtain the quantity $\sigma^{-1}(x)$ modulo all the conjugates of $\mathfrak{q}$, and so we can apply our algorithm to recover σ.
So we should start with $F = \langle \phi \rangle$, find σ such that $[G, \sigma] \subseteq F$, lift it, add it to F and continue...
Howeve since we do not know yet the group G, we have no way to compute the bracket $[\tau, \sigma]$. To solve this problem with a polynomial number of guesses we use the presentations of nilpotent groups (Ph. Hall).

Polycyclic presentation

A nilpotent polycyclic presentation over the free generators $g_1, \ldots, g_n$ is given by

- Relative orders $(o_i)_{i=1}^n$
- Powers $(u_i)_{i=1}^n$ (u_i is a word in $g_1, \ldots, g_{i-1}$)
- Brackets $(w_{j,i})_{1 \leq i < j \leq n}$ ($w_{j,i}$ is a word in $g_1, \ldots, g_{i-1}$)

$$G = \langle g_1, \ldots, g_n | \forall 1 \leq i < j \leq n \qquad g_i^{o_i} = u_i, [g_j, g_i] = w_{j,i} \rangle$$

$$D_8 : \langle g_1, g_2, g_3 | g_1^2 = g_3^2 = 1, g_2^2 = g_1, [g_1, g_2] = [g_1, g_3] = 1, [g_2, g_3] = g_1 \rangle$$

$$H_8 : \langle g_1, g_2, g_3 | g_1^2 = 1, g_2^2 = g_3^2 = g_1, [g_1, g_2] = [g_1, g_3] = 1, [g_2, g_3] = g_1 \rangle$$

A reduced word is a word of the form $g_1^{e_1}...g_n^{e_n}$ with $0 \leq e_j < o_j$ for $1 \leq j \leq n$. Every elements of G can be represented uniquely as a reduced word.

- Reduction algorithm (Ph. Hall) : Use the bracket relation $g_j g_i = w_{i,j} g_i gj$ to reorder the terms. Whenever $g_i^{o_i}$ appears, replace by u_i. It terminate because all letters of $w_{i,j}$ and u_i come before i.
- Multiplication : we concatenate the words and reduce the result.
- Quotient : the presentation of $G/\langle g_1 \rangle$ is obtained by removing the letter g_1 from w and u.

We assume we have been able to find the words u and w modulo g_1. Since g_1 is in the center the word u and w are just missing some power of g_1 at the start.
We proceed in order. g_k modulo $\langle g_1 \rangle$ is the Frobenius of some prime ideal $\mathfrak{q}_k \in K$ above some pime p_k, so we pick some prime ideal $\mathfrak{p}_k \in L$ above $\mathfrak{q}_k$, and we lift g_k to its Frobenius.

$$g_k(x) = x^{p_k} \pmod{\mathfrak{p}_k}$$

$$[h, g_k](x) = g_k^{-1}(x)^{p_k} \pmod{h(\mathfrak{p}_k)}$$

w	g_3	g_4	g_5
g_2	$w_{3,2}$	$w_{4,2}$	$w_{5,2}$
g_3		$w_{4,3}$	$w_{5,3}$
g_4			$w_{5,4}$

Let us assume we already determined the group G_{k-1} and the relations $w_{i,j}$ for $1 \leq j \leq k-1$ and $i > j$. We want to find g_k. We will try all possible lifts of the $w_{i,k}$ for all $k < i \leq n$, where lifing means adding some power of g_1 to the word.

Let R a set of representative of $H/\langle g_k \rangle$. We can take for R the set of reduced words that do not involve g_1 and g_k.
For each $h \in R$ we need to compute $[h, g_k]$. We proceed as follow : we write $h = h_l h_r$ where h_l is the part with generators of index $i < k$, and h_r is the part with generators of index $i > k$.
Since g_k is in the center of G_n/G_{k-1}, it exists h_l' and h_l'' in G_{k-1} such that $hg_k = h_l' g_k h_r \ g_k h = h_l'' g_k h_r$
and moreover the computation of the words h_l' and h_l'' only requires the knowledge of the $w_{i,j}$ for $1 \leq j \leq k$ and $i > j$.

We obtain $[h, g_k] = h'_l (h''_l)^{-1}$. This way we can write $[h, g_k]$ as a product of the elements g_j for $1 \leq j \leq k-1$ which we have already computed.
We compute $[h, g_k]$ for all $h \in H$, and we apply the Chinese remainder to the formulas for all $h \in H$

$$[h, g_k](x) = g_k^{-1}(x)^{p_k} \pmod{h\mathfrak{p}_k}$$

and we use the lifting algorithm to recover g_k.
At this point we can compute $g_k^{o_k}$ to lift u_k.

Complexity

We can reduce the problem to a group of order p^n where all the relatives orders are p. We see that the number of choice to try to find g_2 is p^{n-2}, p^{n-3} for g_3 etc. which leads to a total number of choice of $(p^{n-1} - p)/(p - 1)$ which is less that the order of the group.
If the group is abelian, then this algorithm is slightly faster than Acciaro-Klüners algorithm.

The super-solvable case

Let assume $\langle\phi\rangle$ is normal instead of central. Then for all τ there exists k such that $\tau\phi\tau^{-1} = \phi^k$ and so

$$\phi^k(x) = x^p \pmod{\tau(\mathfrak{q})\mathbb{Z}_L}$$

which leads to

$$\phi(x) = x^{p^l} \pmod{\tau(\mathfrak{q})\mathbb{Z}_L}$$

for l such that $lk = 1 \pmod{f}$.

We recover ϕ by trying all the admissible functions from P to $(\mathbb{Z}/f\mathbb{Z})^\times$.

This is subexponential in the worse case of $C_p \rtimes C_{p-1}$, there is $(p-2)!$ possible functions to test.

However the lifting part is in exponential time (α^n with $\alpha \leq 5^{4/25} \sim 1.29370$), so ideally we would like to find a better way for lifting.