plain

Recognizing Hilbert Class Polynomials

Hao Chen

November 6, 2015

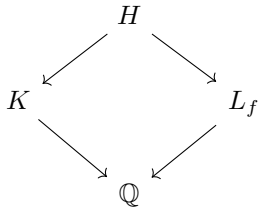
1 The problem

The problem is to develop an fast algorithm that: takes as input a polynomial $f(x) \in \mathbb{Z}[x]$, returns a negative discriminant $D < 0$ if $f(x) = H_D(x)$, and returns *Null* if f is not a Hilbert class polynomial.

2 The analysis

First, obviously, we should check if f is irreducible.

Next, we consider the field $L_f = \mathbb{Q}[x]/(f(x))$. Assume $f = H_D$, we set $K = \mathbb{Q}(\sqrt{D})$ and $H = K[x]/(f(x))$ be the corresponding ring class field of K. Consider the following diagram:



2.1 Case 1: L_f is Galois over $\mathbb{Q}$

We want to say that usually $H/\mathbb{Q}$ is the Galois closure of $L_f/\mathbb{Q}$. This is equivalent to saying that $L_f/\mathbb{Q}$ is not Galois.
Suppose L_f is Galois. Then the group $\Delta = \mathrm{Gal}(H/L_f)$ is a normal subgroup of order two in $G = \mathrm{Gal}(H/\mathbb{Q})$. Note that Δ is generated by a lift of the complex conjugation σ on K. By Cox, we know that the conjugation action of σ on $\mathrm{Gal}(H/K)$ is

$$\sigma\tau\sigma^{-1} = \tau^{-1}.$$

However, Δ is a normal subgroup of G. So $\sigma\tau = \tau\sigma$. Hence we must have that $\mathrm{Gal}(H/K)$ has exponent 2, which means that the class group $C(D)$ is elementary 2-abelian, which is equivalent to D being a "convenient number" in the sense of Euler.

Note that in this case h_D is necessarily a power of 2. Hence if $\deg f$ is not a power of 2, this can not happen.

2.2 Case 2: $L_f/\mathbb{Q}$ is not Galois

In this case, since H is the Galois closure of L_f over $\mathbb{Q}$, we know from Ralph's class that the set of ramified primes of the two extensions are the same. At the same time, we know that $S(H/\mathbb{Q})$ is contained in the primes dividing D, and it contains the primes dividing d_K.

(Question: is it true that $S(H/\mathbb{Q})$ = the primes dividing D? William states that it's true.)

An immediate consequence is

Lemma 2.1 *If $f(x) = H_D(x)$, then $d_K \mid disc(L_f)$.*

This would allow us to search over a finite list of fields. Then an algorithm is as follows:

Find all possible d_K. For each d_K, compute ring class numbers, until the class numbers gets larger than $\deg(f)$.