Gonality preserving lifts of low genus curves

Jan Tuitman

UNSW, 24-07-2017

§1 Introduction

Let $\bar{C}/\mathbb{F}_q$ be a smooth projective curve of genus g

Def The *zeta function* of $\bar{C}$ is defined as:

$$Z(\bar{C},T) = \exp\left(\sum_{i=1}^{\infty} |X(\mathbb{F}_{q^i})| \frac{T^i}{i}\right)$$

Facts (Weil)

- $$Z(\bar{C},T) = \frac{\chi(T)}{(1-T)(1-qT)}.$$
- $$\chi(T) = \prod_{i=1}^{2g} (1-\alpha_i T) \quad \text{with } |\alpha_i| = \sqrt{q}$$
- the α_i are permuted under $\alpha \longmapsto \frac{q}{\alpha}$

Problem Compute $Z(\bar{C},T)$ effectively (fast)

Applications

- Experimental data for conjectures (Sato-Tate, BSD, Lang-Trotter, Langlands program)
- Cryptography (and coding theory)

  Let J be Jacobian of $\bar{C}$, then $|J(\mathbb{F}_q)| = \chi(1)$

  If $|J(\mathbb{F}_q)|$ has small prime factors then the discrete logarithm problem of $J(\mathbb{F}_q)$ is easy

Thm (Kedlaya 2001)

Let $q = p^n$ with p odd and $\bar{C}$ the smooth projective curve birational to:

$$y^2 = f(x)$$

with $f \in \mathbb{F}_q[x]$ monic, separable of degree $2g+1$.

Then $Z(\bar{C}, T)$ can be computed in time

$$O((pg^4n^3)^{1+\varepsilon})$$

This has been extended to all hyperelliptic curves and is implemented in magma.

Thm (T, 2015)

Let $q = p^n$ and $\bar{C}$ the smooth projective curve birational to

$$\bar{Q}(x,y) = 0$$

with $\bar{Q} \in \mathbb{F}_q[x,y]$ monic in y and irreducible.

Suppose that a good lift Q of $\bar{Q}$ to $\mathbb{Z}_q[x,y]$ is known. ($\mathbb{Z}_q$ is the ring of integers of $\mathbb{Q}_q$, the unique unramified extension of $\mathbb{Q}_p$ of degree n)

Then $Z(\bar{C}, T)$ can be computed in time

$$O((pd_x^6 d_y^4 n^3)^{1+\varepsilon})$$

where d_x, d_y are the degrees of Q in y, x.

So how do we find a good lift? Can we d_x to be as small as possible?

§2 A lifting problem

Def The gonality γ of $\bar{C}/\mathbb{F}_q$ is the minimal degree of a noncanstant $\mathbb{F}_q$ rational map to $\mathbb{P}^1$. Same for the geometric gonality but with $\mathbb{F}_q$ rational replaced by $\bar{\mathbb{F}}_q$ rational.

Ex hyperelliptic $\Leftrightarrow$ gonality $= 2$ ($y^2 = f(x)$, x is the gonal map)

Problem

Let K be a number field of degree n which is inert at p, i.e such that $\mathcal{O}_K/(p) \simeq \mathbb{F}_q$

Given $\bar{C}/\mathbb{F}_q$ find $f \in \mathcal{O}_K[x,y]$ such that:

(i) Its reduction mod p $\bar{f}$ defines a curve birational to $\bar{C}$

(ii) The curve $C \subset \mathbb{A}^2_K$ defined by f has the same (geometric) genus as $\bar{C}$

(iii) The degree in y equals the gonality of $\bar{C}$ (so $\bar{C}$ has the same gonality as C and x is gonal map)

Rem We will always assume that q is odd

Rem A solution to this problem is not guaranteed to be a good lift for the point counting, but it almost always is (after making it monic) we will use the following theorem:

<u>Thm (Baker's bound)</u>

The genus of C is at most the number of interior points in the <u>Newton polygon</u> of f (same for $\bar{C}$ and $\bar{f}$). This bound is generically satisfied (e.g. when f is <u>nondegenerate</u>.

<u>Cor</u> If $\bar{f}$ satisfies Baker's bound then any lift f with the same Newton polygon satisfies (i, ii).

<u>Pf</u> The genus can only go down under reduction mod p.

§3 Some algebraic geometry

a divisor on $\overline{C}/\mathbb{F}_q$ is a finite formal sum:

$$D = \sum_{P \in \overline{C}(\overline{\mathbb{F}}_q)} n_P P$$

such a D is defined over $\mathbb{F}_q$ if it is fixed by $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$

The degree of D is $\sum_{P \in \overline{C}(\overline{\mathbb{F}}_q)} n_P$ effective if al $n_P \geq 0$.

To a function $\varphi \in \overline{\mathbb{F}}_q(\overline{C})$ one associates its divisor:

$$\mathrm{div}(\varphi) = \sum_{P \in \overline{C}(\overline{\mathbb{F}}_q)} \mathrm{ord}_P(\varphi) P$$

and similarly for a meromorphic differential ω on $\overline{C}$.

To a divisor D one associates
The vector space

$$L(D) = \{ f \in \overline{\mathbb{F}}_q(\overline{C}) \mid \mathrm{div}(f) \geq -D \}$$

The canonical divisor K is the divisor of any meromorphic ω on $\overline{C}$, this is well defined up to a $\mathrm{div}(\varphi)$.

Thm (Riemann-Roch)
$\dim L(D) - \dim L(K-D) = \deg D - g + 1$

From a divisor D one gets a map to projective space

$$\overline{C}_{\overline{\mathbb{F}}_q} \longrightarrow \mathbb{P}^{\dim L(D)-1}_{\overline{\mathbb{F}}_q}$$
$$P \longmapsto (\varphi_1(P) : \cdots : \varphi_m(P))$$

if $L(D) = 2$ then degree map = degree divisor

well defined if D is base point free. This map is defined over $\mathbb{F}_q$ if D is.

$K : \overline{C} \longrightarrow \mathbb{P}^{g-1}_{\mathbb{F}_q}$ is the canonical map associated to K.

§4 Hyperelliptic curves

$\underline{g=0}$ $\quad \bar{C} \cong \mathbb{P}^1$ since $|\bar{C}(\mathbb{F}_q)| = q+1 > 0$ $\quad \gamma = 1$

$\underline{g=1}$ $\quad \bar{C}$ elliptic since $|\bar{C}(\mathbb{F}_q)| \geq q+1-2\sqrt{q} > 0$ $\quad \gamma = 2$

Weierstrass form : $\bar{f} = y^2 - \bar{h}(x)$

eft : $f = y^2 - h(x)$

$\underline{g=2}$ and geometrically hyperelliptic in general

$K : C \xrightarrow{2 \to 1}$ smooth $g=0$ curve in $\mathbb{P}^{g-1}$

but the $g=0$ curve again has a point so $\cong \mathbb{P}^1$ $\quad \gamma = 2$

Again : $\bar{f} = y^2 - \bar{h}(x)$

$f = y^2 - h(x)$

from now on we exclude hyperelliptic case.

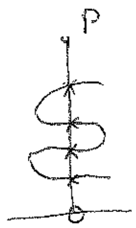
§5 $g=3$

Assume $\bar{C}$ is not hyperelliptic

$K \hookrightarrow \mathbb{P}^2$ as plane quartic $F(X,Y,Z) = 0$

two cases:

① $|\bar{C}(\mathbb{F}_q)| = \emptyset$, $\gamma = 4$, (projection from point outside curve)



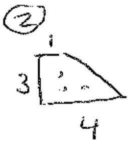
② $|\bar{C}(\mathbb{F}_q)| \neq \emptyset$, $\gamma = 3$, (projection from point $P \in C(\mathbb{F}_q)$)

$P \in$ $\quad (D = K - P)$

In case ② move P to $(0:1:0)$ using $\mathrm{Aut}(\mathbb{P}^2)$, so Y^4 does not appear in F.

Dehomogenizing w.r.t Z gives f supported on:

① 

② 

Both satisfy Baker's bound so a naive eft will do.

Can optimise still more and make polygon ② smaller.

$\underline{g=4}$

Assume $\bar{C}$ is non-hyperelliptic, so $K: \bar{C} \hookrightarrow \mathbb{P}^3$

$\deg(K) = 2g-2 = 6$

By Riemann-Roch:

$\ell(2K) = 12-4+1 = 9$

However, there are 10 degree 2 monomials on $\mathbb{P}^3$

$\Rightarrow$ $\exists$ $\boxed{\text{unique quadric}}$ $\bar{S}_2 \in \mathbb{F}_q[X,Y,Z,W]$ that vanishes on $\bar{C}$

Again by Riemann-Roch:

$\ell(3K) = 18-4+1 = 15$

There are 20 degree 3 monomials on $\mathbb{P}^3$, the degree 3 multiples of $\bar{S}_2$ have dimension 4, so $\boxed{\text{one new cubic}}$ $\bar{S}_3 \in \mathbb{F}_q[X,Y,Z,W]$ that vanishes on $\bar{C}$.

One can show that $\bar{C}$ is defined by $\bar{S}_2, \bar{S}_3$ so is a complete intersection.

A naive lift of $\bar{S}_2, \bar{S}_3$ will satisfy (i), (ii) but have $\boxed{\gamma = 2g-2 = 6}$

We can do a lot better.

Let $\bar{M} \in \mathbb{F}_q^{4\times 4}$ be the matrix s.t. $S_2 = (X,Y,Z,W)\bar{M}(X,Y,Z,W)^t$

$\overset{\shortparallel}{\bar{M}^t}$

Let χ_2 be the quadratic character on $\mathbb{F}_q$ then there are 3
(0 if 0, 1 if square, -1 otherwise)
cases:

① $\chi_2(\det \bar{M}) = 0$ $\boxed{\gamma = 3}$

② $\chi_2(\det \bar{M}) = 1$ square $\boxed{\gamma = 3}$

③ $\chi_2(\det \bar{M}) = -1$ non-square $\boxed{\gamma = 4}$ (5 if $\bar{C}(\mathbb{F}_{q^2}) = 0$)
(only when $q \le 7$)

case 1 $\quad \chi_2(\det \bar{M}) = 0$

use $\mathrm{Aut}(\mathbb{P}^3)$ to take $\bar{S}_2$ to $ZW - X^2 \quad (= \mathbb{P}(1,2,1))$

project from $(0:0:0:1)$ on XYZ plane i.e. eliminate W

to obtain $\bar{S}_3(X^2, XZ, Z^2, X^2) \qquad W = \frac{X^2}{Z}$

dehomogenize w.r.t Z

$\rightsquigarrow \bar{f}$ with Newton polygon

Baker's bound is satisfied
so take a naive lift $f \in \mathcal{O}_K[x,y]$.

case 2 $\quad \chi_2(\det \bar{M}) = 1$

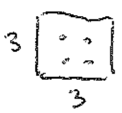
use $\mathrm{Aut}(\mathbb{P}^3)$ to take $\bar{S}_2$ to $XY - ZW \quad (\simeq \mathbb{P}^1 \times \mathbb{P}^1)$

again project from $(0:0:0:1)$ on XYZ plane

to obtain $\bar{S}_3(XZ, YZ, Z^2, XY)$

dehomogenise w.r.t Z

$\rightsquigarrow \bar{f}$ with Newton polygon



Baker's bound is satisfied
so take a naive lift $f \in \mathcal{O}_K[x,y]$

case 3 $\quad$ cannot find a plane model satisfying Baker's bound.

assume $q > 7$ so that $\bar{C}(\mathbb{F}_{q^2}) \neq \emptyset$

take $\bar{P} \in \bar{C}(\mathbb{F}_{q^2})$ and let $\bar{P}'$ be its Galois conjugate

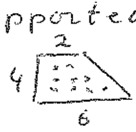
$\bar{\ell}$ line through $\bar{P}$ and $\bar{P}'$

use $\mathrm{Aut}(\mathbb{P}^3)$ to send $\bar{\ell}$ to $X = Z = 0 \qquad (D = K - P - P')$

$\bar{S}_3(0, Y, 0, W) = (\bar{a}Y + \bar{b}W)\,\bar{S}_2(0, Y, 0, W)$

Lift such that $\quad S_3(0, Y, 0, W) = (aY + bW)\,S_2(0, X, 0, W)$

Eliminate W and dehomogenize w.r.t. $Z \to f$ supported on



again we can optimise, make polygons smaller etc

We have also worked out the $g = 5$ case completely, obtaining lifts with $r = 3$ or $r = 4$ again apart from some very rare cases.

$\boxed{\text{Extra}}$

$\underline{g = 5}$

There are 2 cases

trigonal: canonical embedding cut out by 3 quadrics $\overline{S_{21}}, \overline{S_{22}}, \overline{S_{23}}$ and 2 cubics $\overline{S_{31}}\ \overline{S_{32}}$ in $\mathbb{P}^4$

non trigonal: canonical embedding complete intersection of 3 quadrics in $\mathbb{P}^4$

trigonal case

The three quadrics cut out a surface scroll of type $(1,2)$ which can be put into the form:

$$X^2 - ZV \qquad XY - ZW \qquad XW - YV$$

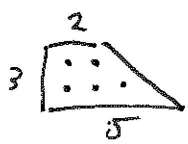
using $\mathrm{Aut}(\mathbb{P}^4)$. However, this is not so easy as before (Lie algebra method).

eliminating V, W gives

$$S_{3,i}(XZ, YZ, Z^2, X^2, XY) \qquad \text{for } i = 1, 2 ..$$

dehomogenizing w.r.t Z gives two polynomials $\overline{f_1}, \overline{f_2} \in \mathbb{F}_q[x,y]$.

Their gcd $\overline{f}$ defines the curve and has Newton polygon:



which satisfies Baker's bound, so an arbitrary lift will do.

<u>nontrigonal</u>

the family of quadrics vanishing on $\bar{C}$ will contain singular fibres.

Let $\bar{M}_i \in \mathbb{F}_q^{5\times 5}$, $\bar{M}_i^t = M_i$, be the matrix associated to $\bar{S}_{2,i}$.

Let $D(\bar{C})$ be the discriminant curve of $\bar{C}$ i.e.:

$$\det(\lambda_1 \bar{M}_1 + \lambda_2 \bar{M}_2 + \lambda_3 \bar{M}_3) = 0 \quad \text{in} \quad \mathbb{P}^2 = \mathrm{Proj}\ \mathbb{F}_q[\lambda_1, \lambda_2, \lambda_3]$$

For $P \in D(\bar{C})$ let
$$\chi(P) = \begin{cases} -\ \chi_2(\text{product of nonzero eigenvalues if rank quadric} = 4) \\ -\ 0 \quad \text{otherwise} \end{cases}$$

<u>Then</u>: $\bar{C}$ has gonality 4 $\iff$ $D(\bar{C})(\mathbb{F}_q)$ contains a point P with $\chi(P) \in \{0, 1\}$ (so not -1).

construction if $\chi(P) = 1$ (generic case):

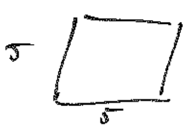
we can put the quadric corresponding to P in the form:

$$\bar{S} = XY - ZW$$

cone over $\mathbb{P}^1 \times \mathbb{P}^1$, top $(0:0:0:0:1)$

we take $S = XY - ZW$ and lift the other 2 quadrics arbitrarily.

Projecting from the top we obtain a curve in $\mathbb{P}^1 \times \mathbb{P}^1$ defined by $\bar{f} \in \mathbb{F}_q[x,y]$ with Newton polygon:



This does not satisfy Baker's bound, but no problem.