Counting points on curves: the general case

Jan Tuitman, KU Leuven

May 7, 2015

Zeta functions

Suppose that

- $\mathbf{F}_q$ finite field of cardinality $q = p^n$.
- $X/\mathbf{F}_q$ a smooth proper algebraic curve of genus g.

Recall that the zeta function of X is defined as

$$Z(X,T) = \exp\Big(\sum_{i=1}^{\infty} |X(\mathbf{F}_{q^i})| \frac{T^i}{i}\Big).$$

It follows from the Weil conjectures that $Z(X,T)$ is of the form

$$\frac{\chi(T)}{(1-T)(1-qT)},$$

where $\chi(T) \in \mathbf{Z}[T]$ of degree $2g$, with inverse roots that

- have absolute value $q^{\frac{1}{2}}$
- are permuted by the map $x \to q/x$.

Computing zeta functions

Problem

How to compute $Z(X, T)$ *efficiently?*

Answer

Using p-adic cohomology!

Applications

- *Cryptography:* $|Jac_X(\mathbf{F}_q)| = \chi(1)$ *and the DLP on* $Jac_X(\mathbf{F}_q)$ *is easy when its order only has small prime factors.*
- *Arithmetic statistics: collecting data on (generalised) Sato-Tate distributions etc.*

p-adic cohomology?

Definition

$\mathbf{Q}_q$: *unique unramified extension of* $\mathbf{Q}_p$ *of degree* n.

Fact

One can define p-adic (or rigid) cohomology spaces $H^i_{rig}(X)$:

- *finite dimensional vector spaces over* $\mathbf{Q}_q$
- *with an action of the p-th power Frobenius map* $F_p : X \to X$

such that

$$\chi(T) = \det(1 - T\,\mathrm{F}_p^n \,|H^1_{rig}(X)).$$

Remark

We will not define p-adic cohomology spaces in general (for separated schemes!), but we will see the definition in a special case.

p-adic precision

A priori we can only compute $\chi(T)$ to finite p-adic precision.

However, because of the bounds on the absolute values of the coefficients of $\chi(T)$ coming from the Weil conjectures, this polynomial can be determined exactly if it is known to high enough p-adic precision.

The loss of p-adic precision in various steps of the algorithm has to be analysed and bounded explicitly. This tends to be rather technical! The better the bound, the faster the algorithm.

Kedlaya's algorithm

Theorem (Kedlaya, 2002)

Suppose p is odd and let $X/\mathbf{F}_q$ be a hyperelliptic curve of the form $y^2 = f(x)$ with $f \in \mathbf{F}_q[x]$ with $\deg(f) = 2g+1$ and $\gcd(f, f') = 1$. Then $Z(X,T)$ can be computed in

$$\begin{aligned} &\textit{time:} && \tilde{\mathcal{O}}(pg^4 n^3) \\ &\textit{space:} && \tilde{\mathcal{O}}(pg^3 n^3) \end{aligned}$$

Remark

Implemented in Magma, also for $p = 2$ and even degree models.

Goal

Extend this algorithm to all curves.

Our algorithm

Theorem (Tuitman, 2014)

Suppose $Q \in \mathbf{F}_q[x,y]$ irreducible and monic in y that admits a good lift to characteristic 0 (see Assumption below). Let the degrees of Q in x,y be d_y, d_x, respectively and let $X/\mathbf{F}_q$ denote the smooth projective curve birational to $Q(x,y)=0$. Then $Z(X,T)$ can be computed in

$$\textit{time: } \tilde{\mathcal{O}}(p d_x^6 d_y^4 n^3)$$
$$\textit{space: } \tilde{\mathcal{O}}(p d_x^4 d_y^3 n^3)$$

(ignoring the computation of some integral bases in function fields).

Remark

Implemented in Magma, the code can be found at: https://perswww.kuleuven.be/jan_tuitman

Some notation

Definition

$\mathbf{Z}_q$: *the ring of integers of* $\mathbf{Q}_q$
σ : *the (unique) lift* $\in \mathrm{Gal}(\mathbf{Q}_q/\mathbf{Q}_p)$ *of the p-th power map on* $\mathbf{F}_q$

Definition

Let $\mathcal{Q} \in \mathbf{Z}_q[x]$ *be a lift of* Q *that is still monic of degree* d_x *in* y.

Definition

Let $\Delta(x) \in \mathbf{Z}_q[x]$ *be the resultant of* $\mathcal{Q}$ *and* $\frac{\partial \mathcal{Q}}{\partial y}$ *with respect to* y *and* $r(x) \in \mathbf{Z}_q[x]$ *the squarefree polynomial* $r = \Delta/(\mathrm{gcd}(\Delta, \frac{d\Delta}{dx}))$.

Some more notation

Definition

We denote

$$\mathcal{S} = \mathbf{Z}_q[x, \frac{1}{r}], \qquad \mathcal{R} = \mathbf{Z}_q[x, \frac{1}{r}, y]/(\mathcal{Q})$$

and write $\mathcal{V} = \operatorname{Spec} \mathcal{S}$, $\mathcal{U} = \operatorname{Spec} \mathcal{R}$, *so that* x *defines a finite étale morphism from* $\mathcal{U}$ *to* $\mathcal{V}$.

Remark

Note that we have taken out the (fibres of) the singularities of the plane model $\mathcal{Q}(x, y) = 0$ *and the ramification points of the finite map* x *to the projective line.*

A good lift to characteristic 0?

Assumption

- *There exists a smooth proper curve $\mathcal{X}$ over $\mathbf{Z}_q$ and a smooth relative divisor $\mathcal{D}_{\mathcal{X}}$ on $\mathcal{X}$ such that $\mathcal{U} = \mathcal{X} \setminus \mathcal{D}_{\mathcal{X}}$.*
- *There exists a smooth relative divisor $\mathcal{D}_{\mathbf{P}^1}$ on $\mathbf{P}^1_{\mathbf{Z}_q}$ such that $\mathcal{V} = \mathbf{P}^1_{\mathbf{Z}_q} \setminus \mathcal{D}_{\mathbf{P}^1}$.*

Remark

It is not entirely clear when a lift $\mathcal{Q}$ satisfying this Assumption exists. However we can say the following:

- *For a generic Q a random lift $\mathcal{Q}$ usually satisfies it.*
- *Starting from $\mathcal{Q} \in \mathbf{Z}_q[x, y]$ it is satisfied for all but finitely many p.*
- *If $x : X \to \mathbf{P}^1_{\mathbf{F}_q}$ is wildly ramified, then a lift $\mathcal{Q}$ satisfying it does not exist.*

Overconvergent rings

Definition

We define

$$\mathbf{Z}_q\langle x, 1/r\rangle^\dagger = \{ \sum_{i,j \in \mathbf{Z}_{\geq 0}} a_{ij} \frac{x^i}{r^j} | a_{ij} \in \mathbf{Z}_q, \exists \rho \in \mathbf{R}_{>1} : \lim_{i+j \to \infty} |a_{ij}| \rho^{i+j} = 0 \}$$

$$\mathbf{Z}_q\langle x, 1/r, y\rangle^\dagger = \{ \sum_{i,j,k \in \mathbf{Z}_{\geq 0}} a_{ijk} \frac{x^i y^j}{r^k} | a_{ijk} \in \mathbf{Z}_q, \exists \rho \in \mathbf{R}_{>1} : \lim_{i+j+k \to \infty} |a_{ijk}| \rho^{i+j+k} = 0 \}$$

and let

$$\mathcal{S}^\dagger = \mathbf{Z}_q\langle x, 1/r\rangle \qquad \mathcal{R}^\dagger = \mathbf{Z}_q\langle x, 1/r, y\rangle^\dagger / (\mathcal{Q})$$

denote the rings of overconvergent functions on $\mathcal{V}$ and $\mathcal{U}$.

Example: hyperelliptic curves

$\mathcal{Q} = y^2 - f(x)$ with $f \in \mathbf{Z}_q[x]$ monic of degree $2g+1$ such that $\gcd(f, f') = 1$

$r = \Delta = f(x) = y^2$

$R^\dagger = \mathbf{Z}_q\langle x, 1/r, y\rangle^\dagger/(\mathcal{Q}) = \mathbf{Z}_q\langle x, y, y^{-1}\rangle^\dagger/(\mathcal{Q})$

$\mathcal{U} = \{\mathcal{Q}(x,y) = 0\} - \{y = 0\}$

Assumption on good lift to characteristic 0 is satisfied since $\gcd(f, f') = 1$

Rigid cohomology

Definition

We define the overconvergent Kähler differentials

$$\Omega^1_{\mathcal{R}^\dagger} = \frac{R^\dagger dx \oplus R^\dagger dy}{d\mathcal{Q}}$$

and the overconvergent De Rham complex

$$\Omega^\bullet_{\mathcal{R}^\dagger}: \quad 0 \longrightarrow \mathcal{R}^\dagger \xrightarrow{d} \Omega_{\mathcal{R}^\dagger} \longrightarrow 0.$$

We then have

$$H^1_{rig}(U) = H^1(\Omega^\bullet_{\mathcal{R}^\dagger} \otimes \mathbf{Q}_q) = \mathrm{coker}(d) \otimes \mathbf{Q}_q.$$

Frobenius lift I

Theorem

There exists a Frobenius lift $\mathrm{F}_p : \mathcal{R}^\dagger \to \mathcal{R}^\dagger$ for which $\mathrm{F}_p(x) = x^p$.

Proof.

To find $\mathrm{F}_p(1/r)$ and $\mathrm{F}_p(y)$ we solve the equations

$$\begin{aligned} \mathrm{F}_p(1/r) r^\sigma(x^p) &= 1, & \qquad \mathrm{F}_p(1/r) &\equiv r^{-p} \bmod p, \\ \mathcal{Q}^\sigma(x^p, \mathrm{F}_p(y)) &= 0, & \qquad \mathrm{F}_p(y) &\equiv y^p \bmod p, \end{aligned}$$

by Hensel lifting.

Let $s(x,y) = \Delta(x)/\frac{\partial \mathcal{Q}}{\partial y} \in \mathbf{Z}_q[x,y]/(\mathcal{Q})$ and choose $m \in \mathbf{Z}_{\geq 0}$ such that there exists $g(x) \in \mathbf{Z}_q[x]$ so that $r(x)^m = g(x)\Delta(x)$.

Frobenius lift II

Define sequences $(\alpha_i)_{i \geq 0}, (\beta_i)_{i \geq 0}$ with $\alpha_i \in \mathcal{S}^\dagger, \beta_i \in \mathcal{R}^\dagger$, by the following recursion:

$$\begin{aligned}
\alpha_0 &= r^{-p}, \\
\beta_0 &= y^p, \\
\alpha_{i+1} &= \alpha_i(2 - \alpha_i r^\sigma(x^p)) && \mod p^{2^{i+1}}, \\
\beta_{i+1} &= \beta_i - \mathcal{Q}^\sigma(x^p, \beta_i) s^\sigma(x^p, \beta_i) g^\sigma(x^p) \alpha_i^m && \mod p^{2^{i+1}}.
\end{aligned}$$

Then take

$$\mathrm{F}_p(x) = x^p, \qquad \mathrm{F}_p(1/r) = \lim_{i \to \infty} \alpha_i, \qquad \mathrm{F}_p(y) = \lim_{i \to \infty} \beta_i,$$

Integral bases

Assumption

Matrices $W^0 \in Gl_{d_x}(\mathbf{Z}_q[x, 1/r])$ *and* $W^\infty \in Gl_{d_x}(\mathbf{Z}_q[x, 1/x, 1/r])$ *are given such that, if we denote* $b^0_j = \sum_{i=0}^{d_x-1} W^0_{i+1,j+1} y^i$ *and* $b^\infty_j = \sum_{i=0}^{d_x-1} W^\infty_{i+1,j+1} y^i$ *for all* $0 \leq j \leq d_x - 1$*, then:*

- $[b^0_0, \ldots, b^0_{d_x-1}]$ *is an integral basis for* $\mathbf{Q}_q(x, y)$ *over* $\mathbf{Q}_q[x]$*,*
- $[b^\infty_0, \ldots, b^\infty_{d_x-1}]$ *is an integral basis for* $\mathbf{Q}_q(x, y)$ *over* $\mathbf{Q}_q[1/x]$*.*

Let $W \in Gl_{d_x}(\mathbf{Z}_q[x, 1/x])$ be the matrix defined by $W = (W^0)^{-1} W^\infty$.

Remark

Good algorithms are available to compute integral bases in function fields (in Magma). We exclude this from our complexity estimates, in practice it takes neglible time and space.

Connection matrix I

Proposition

Let $G^0 \in M_{d_x \times d_x}(\mathbf{Z}_q[x, 1/r])$ *denote the matrix such that*

$$db_j^0 = \sum_{i=0}^{d_x-1} G^0_{i+1,j+1} b_i^0 dx,$$

for all $0 \leq j \leq d_x - 1$. *Let* $x_0 \neq \infty$ *be a geometric point of* $\mathbf{P}^1(\bar{\mathbf{Q}}_q)$. *Then the matrix* $G^0 dx$ *has at most a simple pole at* x_0.

Connection matrix II

Proof.

Note that $\mathrm{ord}_P(dx/(x-x_0)) = -1$ at every $P \in \mathcal{X} \setminus \mathcal{U}$ lying over x_0. At every such P and for all $0 \leq i \leq d_x - 1$ we clearly have $\mathrm{ord}_P(db_i^0) \geq 0$, so that $\mathrm{ord}_P((x-x_0)db_i^0) - \mathrm{ord}_P(dx) \geq 1$. Since $[b_0^0, \ldots, b_{d_x-1}^0]$ is an integral basis for $\mathbf{Q}_q(x,y)$ over $\mathbf{Q}_q[x]$, we conclude that $(x-x_0)G^0$ does not have a pole at x_0, so that $G^0 dx$ has at most a simple pole there. $\square$

Exponents I

Definition

Let $x_0 \in \mathbf{P}^1(\bar{\mathbf{Q}}_q) \setminus \infty$ be a geometric point. The exponents of $G^0 dx$ at x_0 are defined as the eigenvalues of the residue matrix

$$G_{-1}^{x_0} = (x - x_0) G^0|_{x=x_0}$$

.

Proposition

The exponents of $G^0 dx$ at any geometric point $x_0 \in \mathbf{P}^1(\bar{\mathbf{Q}}_q) \setminus \infty$ are elements of $\mathbf{Q} \cap \mathbf{Z}_p$ and are contained in the interval $[0, 1)$.

Exponents II

Proof.

Let $\lambda \in \bar{\mathbf{Q}}_q$ denote an exponent of $G^0 dx$ at $x_0 \neq \infty$. Then there exists $f = \sum_{i=0}^{d_x-1} a_i b_i^0$ with $a_0, \ldots, a_{d_x-1} \in \bar{\mathbf{Q}}_q$ such that

$$df = \left(\frac{\lambda f}{x - x_0} + g \right) dx \tag{1}$$

as 1-forms on $\mathcal{U} \otimes \bar{\mathbf{Q}}_q$, where $g \in \mathcal{O}(\mathcal{U} \otimes \bar{\mathbf{Q}}_q)$ satisfies $\operatorname{ord}_P(g) \geq 0$ at all points $P \in x^{-1}(x_0)$. Note that for at least one $P \in x^{-1}(x_0)$ we have $\operatorname{ord}_P(f) < \operatorname{ord}_P(x - x_0)$, since otherwise $f/(x - x_0)$ would be integral over $\mathbf{Q}_q[x]$. For such a P, dividing by f in (1) and taking residues, we obtain

$$\operatorname{ord}_P(f) = \lambda \operatorname{ord}_P(x - x_0) = \lambda e_P.$$

Since $0 \leq \operatorname{ord}_P(f) < \operatorname{ord}_P(x - x_0)$, we see that $\lambda \in \mathbf{Q} \cap [0, 1)$. It follows from the Assumption on good lifts that $\lambda \in \mathbf{Z}_p$. □

Pole order reduction I

Proposition

For all $\ell \in \mathbf{Z}_{\geq 1}$ and every vector $w \in \mathbf{Q}_q[x]^{\oplus d_x}$, there exist vectors $u, v \in \mathbf{Q}_q[x]^{\oplus d_x}$ with $\deg(v) < \deg(r)$, such that

$$\frac{\sum_{i=0}^{d_x-1} w_i b_i^0}{r^\ell} \frac{dx}{r} = d\left(\frac{\sum_{i=0}^{d_x-1} v_i b_i^0}{r^\ell}\right) + \frac{\sum_{i=0}^{d_x-1} u_i b_i^0}{r^{\ell-1}} \frac{dx}{r}.$$

Remark

By repeatedly applying this proposition, we can represent any cohomology class $\in H^1_{rig}(U)$ by a 1-form that is logarithmic at all points $P \in \mathcal{X} \setminus \mathcal{U}$ with $x(P) \neq \infty$.

Pole order reduction II

Proof.

Recall that $rG^0 \in M_{d_x \times d_x}(\mathbf{Z}_q[x])$. Note that since r is separable, r' is invertible in the ring $\mathbf{Q}_q[x]/(r)$. One checks that v has to satisfy the $d_x \times d_x$ linear system

$$\left(\frac{rG^0}{r'} - \ell I\right) v \equiv \frac{w}{r'} \pmod{r}$$

over $\mathbf{Q}_q[x]/(r)$. However, since $\ell \geq 1$ is not an exponent of $G^0 dx$, we have that $\det(\ell I - rG^0/r')$ is invertible in $\mathbf{Q}_q[x]/(r)$, so that this system has a unique solution v. We take

$$u = \frac{w - \left(rG^0 - \ell r' I\right) v}{r} - \frac{dv}{dx}.$$

□

Precision loss

Proposition

Let $\omega \in \Omega^1(\mathcal{U})$ *be of the form*

$$\omega = \frac{\sum_{i=0}^{d_x-1} w_i y^i}{r^\ell} \frac{dx}{r},$$

with $\ell \in \mathbf{Z}_{\geq 1}$ *and* $\deg(w) < \deg(r)$*. We define*

$$e = \max\{e_P | P \in \mathcal{X} \setminus \mathcal{U}, x(P) \neq \infty\},$$

where e_P *denotes the ramification index of* x *at* P*.*

If we represent the class of ω *in* $H^1_{rig}(U)$ *by* $\left(\sum_{i=0}^{d_x-1} u_i y^i\right) \frac{dx}{r}$*, with* $u \in \mathbf{Q}_q[x]^{\oplus d_x}$*, then*

$$p^{\lfloor \log_p(\ell e) \rfloor} u \in \mathbf{Z}_q[x]^{\oplus d_x}.$$

What about $x = \infty$?

At the points $P \in \mathcal{X} \setminus \mathcal{U}$ with $x(P)$ we have an analogous procedure to reduce pole orders, by working with respect to $[b^{\infty}_0, \ldots, b^{\infty}_{d_x-1}]$.

Computing a basis for $H^1_{\mathrm{rig}}(U)$ is now a matter of linear algebra!

The class of any 1-form $\omega \in \Omega^1(\mathcal{U} \otimes \mathbf{Q}_q)$ can be reduced to this basis using pole order reduction.

Computing a basis for $H^1_{\mathrm{rig}}(U)$

Theorem

Define the following $\mathbf{Q}_q$-vector spaces:

$$
\begin{aligned}
E_0 &= \left\{ \left(\sum_{i=0}^{d_x-1} u_i(x) b_i^0 \right) \frac{dx}{r} \quad : u \in \mathbf{Q}_q[x]^{\oplus d_x} \right\}, \\
E_\infty &= \left\{ \left(\sum_{i=0}^{d_x-1} u_i(x,1/x) b_i^\infty \right) \frac{dx}{r} \quad : u \in \mathbf{Q}_q[x,1/x]^{\oplus d_x}, \mathrm{ord}_\infty(u) > \mathrm{ord}_0(W) - \deg(r) + 1 \right\}, \\
B_0 &= \left\{ \sum_{i=0}^{d_x-1} v_i(x) b_i^0 \quad : v \in \mathbf{Q}_q[x]^{\oplus d_x} \right\}, \\
B_\infty &= \left\{ \sum_{i=0}^{d_x-1} v_i(x,1/x) b_i^\infty \quad : v \in \mathbf{Q}_q[x,1/x]^{\oplus d_x}, \mathrm{ord}_\infty(v) > \mathrm{ord}_0(W) \right\}.
\end{aligned}
$$

Then $E_0 \cap E_\infty$ and $d(B_0 \cap B_\infty)$ are finite dimensional $\mathbf{Q}_q$-vector spaces and

$$H^1_{rig}(U) \cong (E_0 \cap E_\infty)/d(B_0 \cap B_\infty).$$

Computing a basis for $H^1_{\text{rig}}(X)$

We are interested in X and not in U. Moreover, the dimension of $H^1_{\text{rig}}(U)$ is usually a lot larger than that of $H^1_{\text{rig}}(X)$.

Theorem

Let z_P denote a local parameter at $P \in \mathcal{X} \setminus \mathcal{U}$. We have an exact sequence

$$0 \longrightarrow H^1_{rig}(X) \longrightarrow H^1_{rig}(U) \xrightarrow{(res_0 \oplus res_\infty)} \bigoplus_{P \in \mathcal{X} \setminus \mathcal{U}} \mathcal{O}_{\mathcal{X},P}/(z_P) \otimes \mathbf{Q}_q.$$

The kernels of res_0 and res_∞ can be computed without having to compute the Laurent series expansions at all $P \in \mathcal{X} \setminus \mathcal{U}$

Proposition

Let $\omega \in \Omega^1(\mathcal{U} \otimes \mathbf{Q}_q)$ *be a 1-form of the form*

$$\omega = \left(\sum_{i=0}^{d_x - 1} u_i(x) b_i^0 \right) \frac{dx}{r},$$

with $u \in \mathbf{Q}_q[x]^{\oplus d_x}$. *For every geometric point* $x_0 \in \mathcal{D}_{\mathbf{P}^1}(\bar{\mathbf{Q}}_q) \setminus \infty$, *let the vector* $v_{x_0} \in \bar{\mathbf{Q}}_q^{\oplus d_x}$ *be defined by* $v_{x_0} = u|_{x=x_0}$. *Let* $\mathcal{E}_\lambda^{x_0}$ *denote the (generalised) eigenspace of* $G_{-1}^{x_0}$ *with eigenvalue* λ, *so that* $\bar{\mathbf{Q}}_q^{\oplus d_x}$ *decomposes as* $\bigoplus \mathcal{E}_\lambda^{x_0}$. *Then*

$$\mathit{res}_0(\omega) = 0 \quad \Leftrightarrow \quad \text{the projection of } v_{x_0} \text{ onto } \mathcal{E}_0^{x_0} \text{ vanishes for all } x_0 \in \mathcal{D}_{\mathbf{P}^1}(\bar{\mathbf{Q}}_q) \setminus \infty.$$

Remark

We have an analogous characterisation of the kernel of res_∞.

Example: hyperelliptic curves

$\mathcal{Q} = y^2 - f(x)$ with $f \in \mathbf{Z}_q[x]$ monic of degree $2g+1$ such that $\gcd(f, f') = 1$

$$W^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad W^\infty = \begin{pmatrix} 1 & 0 \\ 0 & x^{-(g+1)} \end{pmatrix}$$

A basis for $H^1_{\mathrm{rig}}(U)$ is given by

$$[x^0 \frac{dx}{y}, \dots, x^{2g-1} \frac{dx}{y}, x^0 \frac{dx}{y^2}, \dots, x^{2g} \frac{dx}{y^2}]$$

and the first $2g$ vectors form a basis for the subspace $H^1_{\mathrm{rig}}(X)$.

Our algorithm

- Determine a sufficient p-adic precision N.
- Compute a basis $[\omega_1, \ldots, \omega_{2g}]$ for $H^1_{\mathrm{rig}}(X)$.
- Compute $\mathrm{F}_p(1/r)$ and $\mathrm{F}_p(y)$ by Hensel lifting.
- Compute $\mathrm{F}_p(\omega_i)$ and reduce back to the basis $[\omega_1, \ldots, \omega_{2g}]$ for $1 \leq i \leq 2g$ to find the matrix $\mathcal{F}$ of the action of F_p on $H^1_{\mathrm{rig}}(X)$.
- Compute the matrix

  $$\mathcal{F}^{(n)} = \mathcal{F}^{\sigma^{(n-1)}} \mathcal{F}^{\sigma^{(n-2)}} \cdots \mathcal{F}$$

  of the action of F_p^n on $H^1_{\mathrm{rig}}(X)$.
- Compute $\chi(T) = \det(1 - T\,\mathrm{F}_p^n \,|\, H^1_{\mathrm{rig}}(X))$.

Some remarks

- Our bounds for N (which we have not talked about here) are very sharp. Sometimes our N matches the experimental minimal precision, often it is off by 1 or 2.
- The code is really optimised already, we do not really know to make it significantly faster anymore (apart from changing language?).
- For the latest version of the code and examples, download pcc_p and pcc_q from our website https://perswww.kuleuven.be/jan_tuitman.
- More details can be found in the papers:
  'Counting points on curves using a map to $\mathbf{P}^1$' and
  'Counting points on curves: the general case'
  on arxiv.

- Work with W. Castryck: find a good lift to characteristic 0 of lowest possible degree for all curves of genus up to 5 and $p \neq 2$ not too small. For example when X is a genus 5 curve given as the intersection of 3 quadrics in $\mathbf{P}^4$.
- Kedlaya's algorithm has been applied to other problems like computing (Φ, Γ)-modules or Coleman integrals. In the near future we want to adapt our algorithm so that it can be applied to these problems as well.
- David Harvey has made improvements to Kedlaya's algorithm so that it runs in $\tilde{\mathcal{O}}(p^{1/2})$ or even average polynomial time for g, n fixed. In the longer run we would like to try and extend these ideas to our more general setting.