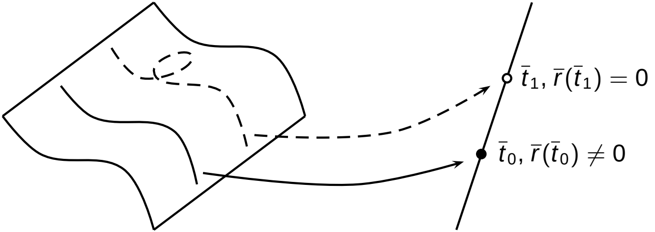
Computing zeta functions in families of $C_{a,b}$ curves using deformation



Ants VIII, Banff, May 18th, 2008

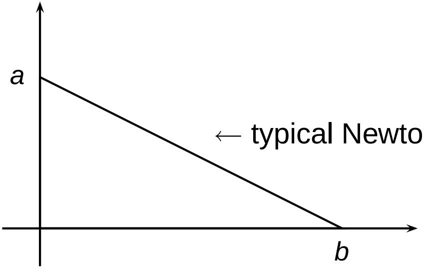
$C_{a,b}$ curves

Throughout, let k be a perfect field and fix coprime $a, b \in \mathbb{Z}_{\geq 2}$.

A $C_{a,b}$ curve is a nonsingular curve in $\mathbb{A}^2_k$ defined by

$$y^a + c_{b,0}x^b + \sum_{ai+bj<ab} c_{i,j}x^i y^j \quad \in k[x,y],$$

with $c_{b,0} \neq 0$.



$\leftarrow$ typical Newton polytope $\Delta_{a,b}$

$C_{a,b}$ curves

Properties:

- There is a unique point at infinity, which is dominated by a single place P_∞ and

$$\mathrm{div}_\infty x = aP_\infty, \quad \mathrm{div}_\infty y = bP_\infty.$$

- Since $\gcd(a, b) = 1$, the Weierstrass semigroup of P_∞

$$\{-\mathrm{ord}_{P_\infty} f \,|\, \mathrm{div}_\infty f = iP_\infty \text{ for some } i \in \mathbb{N}\}$$

  equals $a\mathbb{N} + b\mathbb{N}$.
- Riemann-Roch $\rightsquigarrow$ the genus equals $(a-1)(b-1)/2$.
- Conversely, every curve having a rational place with semigroup $a\mathbb{N} + b\mathbb{N}$ is $C_{a,b}$.

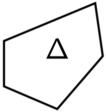
$C_{a,b}$ curves

...as generalizations of hyperelliptic curves.

- Every hyperelliptic curve of genus g having a rational Weierstrass point is $C_{2,2g+1}$.

...as steppingstones to nondegenerate curves.

- $C_{a,b}$ curves are smooth degree ab curves in weighted projective space $\mathbb{P}(b,a,1)$, which is an example of a toric surface.



$\longrightarrow$ toric surface $\mathbb{P}_\Delta$

e.g. $\mathbb{P}_{\Delta_{a,b}} = \mathbb{P}(b,a,1)$

The zeta function

Let $\mathbb{F}_q$ be a finite field, and let

$$\overline{C}(x,y) = y^a + \overline{c}_{b,0}x^b + \sum_{ai+bj<ab} \overline{c}_{i,j}x^i y^j \quad \in \mathbb{F}_q[x,y]$$

define a $C_{a,b}$ curve.

This talk is about the efficient computation of the zeta function

$$Z_{\overline{C}}(T) = \exp\left(\sum_{k=1}^{\infty} \#\overline{C}(\mathbb{F}_{q^k})\frac{T^k}{k}\right) \quad \in \mathbb{Q}[[T]]$$

which turns out to be a rational function and hence a finite, computable object.

The zeta function

Theorem (Weil):

One can write

$$Z_{\overline{C}}(T) = \frac{P(T)}{1 - qT}$$

for a degree $2g = (a-1)(b-1)$ polynomial $P(T) \in \mathbb{Z}[T]$.
Moreover, one can write

$$P(T) = \prod_{i=1}^{2g} (1 - \alpha_i T)$$

where the $\alpha_i \in \mathbb{C}$ are algebraic integers such that

- $|\alpha_i| = \sqrt{q}$ (Riemann hypothesis)
- $\alpha_i \alpha_{2g-i} = q$ (Poincaré duality).

The zeta function

Consequences:

- The absolute values of the coefficients of $P(T)$ are bounded by

$$B = \binom{2g}{g} q^g,$$

  so it suffices to compute $P(T)$ modulo some $N > 2B$.
- One can recover $\#\overline{C}(\mathbb{F}_{q^k})$ as $q^k - \sum_{i=1}^{2g} \alpha_i^k$.

Theorem (Tate):

Let $\mathrm{Jac}(\overline{C})$ be the Jacobian variety of $\overline{C}$. Then

$$\#\mathrm{Jac}(\overline{C})(\mathbb{F}_q) = P(1).$$

State of the art

Two main applications in mind:

1. Direct: given a concrete curve $\overline{C}(x, y)$, efficiently determine $\#\overline{C}(\mathbb{F}_q)$, $\#\mathrm{Jac}(\overline{C})(\mathbb{F}_q)$, ...
2. Indirect: find a curve with almost prime order Jacobian, for use in cryptographic applications based on the discrete logarithm problem.

State of the art before this research:

1. Denef-Vercauteren's generalization of Kedlaya's algorithm for hyperelliptic curves over fields of small characteristic.

   E.g. computation of $Z_{\overline{C}}(T)$ for a $C_{3,4}$ curve $\overline{C}$ over $\mathbb{F}_{2^{60}}$ took about 1.5 hours on a home PC.

2. Repeated application of the above algorithm.

   Would take a couple of days to find a $C_{3,4}$ Jacobian suitable for use in cryptography.

Monsky-Washnitzer cohomology (absolute)

Write $\#\mathbb{F}_q = q = p^n$ where p is the field characteristic.

Let $\mathbb{Q}_q$ be the unramified degree n extension of $\mathbb{Q}_p$.

Let $\mathbb{Z}_q = \{\alpha \in \mathbb{Q}_q \mid \nu_p(\alpha) \geq 0\}$ be its valuation ring. It is a complete DVR with local parameter p and residue field $\mathbb{F}_q$.

Choose

$$C(x,y) = y^a + c_{b,0}x^b + \sum_{ai+bj<ab} c_{i,j}x^i y^j \quad \in \mathbb{Z}_q[x,y]$$

such that it reduces to $\overline{C}(x,y)$ modulo p $\rightsquigarrow$ this automatically defines a $C_{a,b}$ curve over $\mathbb{Q}_q$.

Monsky-Washnitzer cohomology (absolute)

Write

$$\mathbb{Z}_q\langle C\rangle^\dagger = \frac{\mathbb{Z}_q\langle x, y\rangle^\dagger}{(C(x, y))}$$

where $\mathbb{Z}_q\langle x, y\rangle^\dagger$ is the overconvergent power series ring

$$\left\{ \sum_{i,j\in\mathbb{N}} a_{ij}x^iy^j \,\middle|\, \exists \rho \in]0, 1[: \frac{|a_{ij}|_p}{\rho^{i+j}} \to 0 \text{ if } i+j \to \infty \right\}$$

(converge fast enough for their integrals to converge as well).

Note that there is a natural reduction mod p map

$$\pi : \mathbb{Z}_q\langle C\rangle^\dagger \to \mathbb{F}_q[\overline{C}].$$

Monsky-Washnitzer cohomology (absolute)

Theorem (Monsky, Washnitzer):

There exists a $\mathbb{Z}_q$-algebra endomorphism $\mathcal{F}_q$ on $\mathbb{Z}_q\langle C\rangle^\dagger$ that makes the following diagram commutative:

$$\begin{array}{ccc} \mathbb{Z}_q\langle C\rangle^\dagger & \xrightarrow{\mathcal{F}_q} & \mathbb{Z}_q\langle C\rangle^\dagger \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{F}_q[\overline{C}] & \xrightarrow{\overline{a}\mapsto\overline{a}^q} & \mathbb{F}_q[\overline{C}]. \end{array}$$

The map $\mathcal{F}_q$ is called a lift of Frobenius.

There is a constructive proof, and $\mathcal{F}_q(x)$ and $\mathcal{F}_q(y)$ can be effectively approximated using Newton iteration.

Monsky-Washnitzer cohomology (absolute)

Consider the module of differentials

$$D^1(\mathbb{Z}_q\langle C\rangle^\dagger) = \frac{\mathbb{Z}_q\langle C\rangle^\dagger dx + \mathbb{Z}_q\langle C\rangle^\dagger dy}{\left(\frac{\partial C}{\partial x}dx + \frac{\partial C}{\partial y}dy\right)}$$

and let $d : \mathbb{Z}_q\langle C\rangle^\dagger \to D^1(\mathbb{Z}_q\langle C\rangle^\dagger)$ be the usual exterior derivation. Then define the cohomology space

$$H^1_{MW}(\overline{C}/\mathbb{Q}_q) = \frac{D^1(\mathbb{Z}_q\langle C\rangle^\dagger)}{d(\mathbb{Z}_q\langle C\rangle^\dagger)} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q.$$

Note that $\mathcal{F}_q$ induces a $\mathbb{Q}_q$-vector space morphism

$$\mathcal{F}_q^* : H^1_{MW}(\overline{C}/\mathbb{Q}_q) \to H^1_{MW}(\overline{C}/\mathbb{Q}_q) : fdg \mapsto \mathcal{F}_q(f)d\mathcal{F}_q(g).$$

Monsky-Washnitzer cohomology (absolute)

Theorem (Monsky, Washnitzer):

$H^1_{MW}(\overline{C}/\mathbb{Q}_q)$ is a $2g$-dimensional vector space on which $\mathcal{F}_q^*$ acts bijectively. Moreover, if $\chi(T)$ is its characteristic polynomial, then

$$Z_{\overline{C}}(T) = \frac{T^{2g}\chi(1/T)}{1-qT}.$$

Denef and Vercauteren prove that

$$\mathcal{B} = \{x^r y^s dx \mid r = 0, \ldots, b-2; s = 1, \ldots, a-1\}$$

is a basis for $H^1_{MW}(\overline{C}/\mathbb{Q}_q)$ and give an explicit procedure to reduce a given 1-form modulo exact differential forms.

Computing the zeta function (absolute)

Algorithm to compute $Z_{\overline{C}}(T)$:

1. Compute $\mathcal{F}_q(x)$ and $\mathcal{F}_q(y)\ldots$
2. Use this to determine $\mathcal{F}_q^*(x^r y^s dx)$ for all $x^r y^s dx \in \mathcal{B}\ldots$
3. Reduce modulo exact differential forms to end up in terms of $\mathcal{B}$ again $\rightsquigarrow$ matrix of $\mathcal{F}_q^*\ldots$
4. Compute characteristic polynomial $\chi(T)$ and recover $Z_{\overline{C}}(T)\ldots$

$\ldots$ modulo a sufficiently large p-adic precision.

Differential reduction takes q steps!!

$\rightsquigarrow$ One splits q^{th} power Frobenius into n copies of p^{th} power Frobenius

$\rightsquigarrow$ resulting algorithm takes $O(n^3p)$ steps.

Computing the zeta function (absolute)

Step

2. Use $\mathcal{F}_q(x)$ and $\mathcal{F}_q(y)$ to determine $\mathcal{F}_q^*(x^r y^s dx) = \mathcal{F}_q(x)^r \mathcal{F}_q(y)^s d\mathcal{F}_q(x)$ for all $x^r y^s dx \in \mathcal{B}$...

accounts for about 80% of the computation and makes the algorithm slow in practice.

$\rightsquigarrow$ in contrast with Kedlaya's original algorithm for hyperelliptic curves, where it is possible to choose $\mathcal{F}_q(x) = x^q$ and only compute $\mathcal{F}_q(y)$ using Newton iteration

$\rightsquigarrow$ 2 minutes versus 1.5 hours

The deformation idea

Different approach (Lauder):

1. Consider a 1-parameter family of $C_{a,b}$ curves

$$\overline{C}(x,y,t) = y^a + \overline{c}_{b,0}(t)x^b + \sum_{ai+bj<ab} \overline{c}_{i,j}(t)x^i y^j \quad \in \mathbb{F}_q[t][x,y],$$

   and suppose that $\overline{C}(x,y,0)$ has an easy-to-compute matrix of Frobenius $F_q(0)$;

2. Compute a relative matrix of Frobenius $F_q(t)$ from $F_q(0)$ by solving a differential equation of the type

$$N(t)F_q(t) - \frac{d}{dt}F_q(t) = qt^{q-1}F_q(t)N(t^q)$$

   (here $N(t)$ is a matrix of the Gauss-Manin connection);

3. Evaluate $F_q(t)$ in the point of interest.

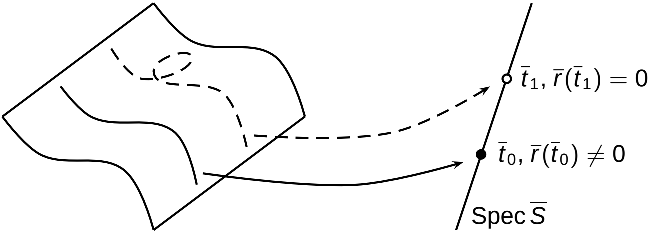
The deformation idea

Two advantages:

- One circumvents the costly computation of a lift of Frobenius;
- Once $F_q(t)$ is computed, evaluation at different values of t is cheap $\rightsquigarrow$ highly speeds up the search for a $C_{a,b}$ curve with almost prime order Jacobian.

Monsky-Washnitzer cohomology (relative)

$\overline{C}(x,y,t)$ defines a flat family over an open subset $\operatorname{Spec} \mathbb{F}_q[t, \overline{r}(t)^{-1}]$ of the affine t-line.



Choose

$$C(x,y,t) = y^a + c_{b,0}(t)x^b + \sum_{ai+bj<ab} c_{i,j}(t)x^i y^j \quad \in \mathbb{Z}_q[t][x,y]$$

such that it reduces to $\overline{C}(x,y,t)$ modulo p.
Choose $r(t) \in \mathbb{Z}_q[t]$ such that it reduces to $\overline{r}(t)$ modulo p

Monsky-Washnitzer cohomology (relative)

Write

$$\mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger \langle C\rangle^\dagger = \frac{\mathbb{Z}_q\langle t, z, x, y\rangle^\dagger}{(zr(t) - 1, C(x, y))}$$

where $\mathbb{Z}_q\langle x, y\rangle^\dagger$ is the overconvergent power series ring

$$\left\{ \sum_{i,j,k,\ell \in \mathbb{N}} a_{ijk\ell} x^i y^j t^k z^\ell \,\middle|\, \exists \rho \in]0,1[: \frac{|a_{ijk\ell}|_p}{\rho^{i+j+k+\ell}} \to 0 \text{ if } i+j+k+\ell \to \infty \right\}$$

(converge fast enough for their integrals to converge as well).

Note that there is a natural reduction mod p map

$$\pi : \mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger \langle C\rangle^\dagger \to \mathbb{F}_q[t, \bar{r}(t)^{-1}][\overline{C}].$$

Monsky-Washnitzer cohomology (relative)

Theorem:

There exists a $\mathbb{Z}_q$-algebra endomorphism $\mathcal{F}_q$ on $\mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger$ that makes the following diagram commutative:

$$\begin{array}{ccc} \mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger & \xrightarrow{\mathcal{F}_q} & \mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{F}_q[t, \bar{r}(t)^{-1}][\overline{C}] & \xrightarrow{\bar{a}\mapsto\bar{a}^q} & \mathbb{F}_q[t, \bar{r}(t)^{-1}][\overline{C}] \end{array}$$

such that $\mathcal{F}_q(t) = t^q$. The map $\mathcal{F}_q$ is called a lift of Frobenius.

There is a constructive proof, and explicit bounds on the convergence rates of $\mathcal{F}_q(x)$, $\mathcal{F}_q(y)$, $\mathcal{F}_q(z)$ and $\mathcal{F}_q(t)$ can be given.

Monsky-Washnitzer cohomology (relative)

Consider the module of differentials

$$D^1(\mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger) = \frac{\mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger dx + \mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger dy}{\left(\frac{\partial C}{\partial x}dx + \frac{\partial C}{\partial y}dy\right)}$$

and let $d : \mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger \to D^1(\mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger)$ be the exterior derivation with t fixed. Then define the cohomology space

$$H^1_{MW}(\overline{C}/S^\dagger) = \frac{D^1(\mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger)}{d(\mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger)} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q,$$

where $S^\dagger = \mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$.
Note that $\mathcal{F}_q$ induces a $\mathbb{Q}_q$-linear morphism

$$\mathcal{F}_q^* : H^1_{MW}(\overline{C}/S^\dagger) \to H^1_{MW}(\overline{C}/S^\dagger) : fdg \mapsto \mathcal{F}_q(f)d\mathcal{F}_q(g).$$

Monsky-Washnitzer cohomology (relative)

Theorem:

$H^1_{MW}(\overline{C}/S^\dagger)$ is a free $2g$-dimensional module. For every $\bar{t}_0 \in \mathbb{F}_q$ for which $\bar{r}(\bar{t}_0) \neq 0$, let $\hat{t}_0 \in \mathbb{Z}_q$ be its Teichmüller representative. Then $H^1_{MW}(\overline{C}/S^\dagger)$ mod $t - \hat{t}_0$ can be identified with

$$H^1_{MW}(\overline{C}(x, y, \bar{t}_0) \,|\, \mathbb{Q}_q)$$

on which the action of Frobenius is given by $\mathcal{F}_q^*(\hat{t}_0)$.

Again

$$\mathcal{B} = \{x^r y^s dx \,|\, r = 0, \ldots, b-2; s = 1, \ldots, a-1\}$$

is a basis for $H^1_{MW}(\overline{C}/S^\dagger)$ and there is an explicit procedure to reduce a given 1-form modulo exact differential forms.

The Gauss-Manin connection

If we don't let t be constant, then we have a map

$$d : D^1(\mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger) \to D^2(\mathbb{Z}_q\langle t, r(t)^{-1}\rangle^\dagger\langle C\rangle^\dagger).$$

One can always write $d\omega = \varphi \wedge dt$, which induces a well-defined map

$$\nabla : H^1_{MW}(\overline{C}/S^\dagger) \to H^1_{MW}(\overline{C}/S^\dagger)$$

that satisfies

$$\nabla \circ \mathcal{F}_q^* = qt^{q-1} \circ \mathcal{F}_q^* \circ \nabla.$$

On the level of matrices, this reads

$$N(t)F_q(t) - \frac{d}{dt}F_q(t) = qt^{q-1}F_q(t)N(t^q).$$

Computing the zeta function (relative)

Computing the zeta function of a concrete curve $\overline{C}_1(x,y)$:

1. Put the curve in a family

$$\overline{C}(x,y,t) = (1-t)\overline{C}_0(x,y) + t\overline{C}_1(x,y)$$

   where $\overline{C}_0(x,y)$ is a superelliptic curve defined over $\mathbb{F}_p$...
2. Compute $F_q(0)$ using known techniques (Gaudry-Gürel)...
3. Compute Gauss-Manin connection N...
4. Solve the differential equation

$$N(t)F_q(t) - \frac{d}{dt}F_q(t) = qt^{q-1}F_q(t)N(t^q)$$

   and compute $F_q(1)$...
5. Compute characteristic polynomial and recover $Z_{\overline{C}}(T)$...

Computing the zeta function (relative)

Finding a $C_{a,b}$ curve with almost prime order Jacobian:

1. Consider a 'random' family $\overline{C}(x, y, t) \in \mathbb{F}_p[t][x, y]$ with superelliptic $\overline{C}(x, y, 0)$...
2. Compute $F_q(0)$ using known techniques (Gaudry-Gürel)...
3. Compute Gauss-Manin connection N...
4. Solve the differential equation
$$N(t)F_q(t) - \frac{d}{dt}F_q(t) = qt^{q-1}F_q(t)N(t^q)\ldots$$
to find $F_q(t)$
5. For randomly chosen $\bar{t}_0 \in \mathbb{F}_q$, compute $F_q(\hat{t}_0)$ and its characteristic polynomial $\chi(T)$, until $\chi(1)$ is almost prime.

Computing the zeta function (relative)

Implementation results:

- Direct application: not yet implemented. . .
  - Expected: only slight improvement upon Denef and Vercauteren's algorithm.
  - But: roughly same running time to be expected for nondegenerate curves (ongoing work by Tuitman).
- Indirect application:

equation	$\mathbb{F}_{p^n}$	g	precomp	time/curve	memory
$Y^3 + X^4 + (t+1)XY + 1$	2^{59}	3	553s	14.5s	56MB
$Y^3 + X^5 + X^2 + t + 1$	2^{43}	4	135s	6.5s	22MB
$Y^3 + X^4 + (t+1)XY + 1$	3^{37}	3	1064s	13s	54MB
$Y^3 + X^5 + XY + tY + 1$	3^{29}	4	4128s	22s	91MB
$Y^3 - X^4 + tX^2 + t - 1$	5^{23}	3	30.5s	2s	23MB
$Y^3 - X^5 - X^2 + tX - 1$	5^{19}	4	837s	20s	56MB
$Y^3 + X^4 + tX - 1$	5^{200}	3	515s	538s	288MB

$\rightsquigarrow$ finding $C_{a,b}$ curves with almost prime order Jacobian is now a matter of minutes instead of days