An introduction to rigid cohomology
(Oxford – 2017)

Bernard Le Stum

Université de Rennes 1

December 11, 2017

Contents

Counting points

The Zeta function

Using cohomology

Computing cohomology

Frobenius action

Rigid cohomology

Counting points

Let $\mathbb{F}_q$ be a finite field with q elements (q a power of a prime p) and X an algebraic variety over $\mathbb{F}_q$. We want to do the following:

- Compute the number of rational points ($\mathbb{F}_q$-points) of X

We will denote it by $N(X) := |X(\mathbb{F}_q)|$.

Example (always assuming q is odd)

We may consider the affine plane curve X defined by

$$y^2 = x^3 + x, \quad y \neq 0$$

inside $\mathbb{A}^2_{\mathbb{F}_q}$, or its projective closure $\overline{X}$ defined by

$$y^2 z = x^3 + xz^2$$

inside $\mathbb{P}^2_{\mathbb{F}_q}$.

Example (continuing)

Of course, we have

$$N(\overline{X}) = N(X) + |\{a \in \mathbb{F}_q, a^3 + a = 0\}| + |\{a \in \mathbb{F}_q, a^3 = 0\}|$$

$$= \begin{cases} N(X) + 2 & \text{if} \quad i \notin \mathbb{F}_q \quad (q \equiv -1 \mod 4) \\ N(X) + 4 & \text{if} \quad i \in \mathbb{F}_q \quad (q \equiv 1 \mod 4). \end{cases}$$

Before going any further, recall from the exact sequence

$$1 \to \{\pm 1\} \to \mathbb{F}_q^\times \to (\mathbb{F}_q^\times)^2 \to 1,$$

that there are exactly $\frac{q-1}{2}$ squares in $\mathbb{F}_q^\times$.

We consider now the first case which concerns $q = 3, 7, 27, \ldots$ and can easily be done in a very general way. Since -1 is not a square in $\mathbb{F}_q$, we see that, given any $a \in \mathbb{F}_q^\times$, then

either a or $-a$ is a square but not both.

Example (continuing)

For the same reason,

either $a^3 + a$ or $(-a)^3 + (-a) = -(a^3 + a)$ is a square but not both.

Thus we see that it happens exactly $\frac{q-1}{2}$ times that $a^3 + a$ has the form b^2. And when this happens, we get exactly 2 possibilities for b. It follows that $N(X) = q - 1$ and therefore $N(\overline{X}) = q + 1$.

The second case which concerns $q = 5, 9, 25, 49, \ldots$ is a lot more complicated. For example, if $q = 5$, we may draw the following table

a	-2	-1	1	2
a^2	-1	1	1	-1
a^3	2	-1	1	-2
$a^3 + a$	0	-2	2	0

It follows that no element of the form $a^3 + a$ can be a non zero square and therefore $N(X) = 0$ so that $N(\overline{X}) = 4$.

Example (continuing)

We can also work out the case of $\mathbb{F}_9 := \mathbb{F}_3[i]$. On easily computes

$$a^3 + a = \overline{a} + a = 2\mathrm{Re}(a) = -\mathrm{Re}(a) \in \mathbb{F}_3$$

and see that it is a non zero square in $\mathbb{F}_9$ if and only if $\mathrm{Re}(a) \neq 0$. Thus we obtain 6 possibilities for a and therefore $N(X) = 12$ so that $N(\overline{X}) = 16$.

The Zeta function

If $\mathbb{F}_{q^r}/\mathbb{F}_q$ is a finite extension, and X is any algebraic variety over $\mathbb{F}_q$, we will write

$$N_r(X) := |X(\mathbb{F}_{q^r})| \quad (= N(X \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}))\,.$$

And we define the *Zeta function* of X as

$$Z(X,t) = \exp\left(\sum_1^\infty N_r(X)\frac{t^r}{r}\right).$$

If we can compute it, we will recover

$$N(X) = \left(\frac{\mathrm{d}\log Z(X,t)}{\mathrm{d}t}\right)_{|0},$$

and more generally, all other $N_r(X)$ by looking at the coefficients of $\log Z(X,t)$.

Thus, what we want to do now is the following:

- Compute the Zeta function of X

Example

Let us first verify that if X is defined over $\mathbb{F}_q$ by

$$y^2 = x^3 + x, \quad y \neq 0$$

and $\overline{X}$ denotes its projective closure as before, then we have

$$Z(\overline{X}, t) = \begin{cases} \frac{Z(X,t)}{(1-t)^2(1-t^2)} & \text{if} \quad q \equiv -1 \mod 4 \\ \frac{Z(X,t)}{(1-t)^4} & \text{if} \quad q \equiv 1 \mod 4. \end{cases}$$

Since $Z(\overline{X}, t) = Z(X, t) \times Z(\overline{X} \setminus X, t)$, we simply have to identify the numerator with $Z(\overline{X} \setminus X, t)$.

Example (continuing)

Note that an equation $x = a$ has exactly 1 solution in $\mathbb{F}_{q^r}$ for each r and therefore, the Zeta function of a rational point is

$$\exp\left(\sum_1^\infty \frac{t^r}{r}\right) = \exp\left(-\log(1-t)\right) = \frac{1}{1-t}.$$

This gets rid of the second case where there are 4 rational points.

However, when $q \equiv -1 \mod 4$, then $x^2 + 1$ has no solution in $\mathbb{F}_{q^r}$ for r odd and exactly 2 solutions for r even. Thus the corresponding Zeta function is

$$\exp\left(\sum_1^\infty 2\frac{t^{2k}}{2k}\right) = \frac{1}{1-t^2}.$$

And the first case is settled as well.

Example (continuing)

When $q = 3$, we can deduce the first terms of the Zeta functions of our affine and projective curves above from our previous computations.

More precisely, we have $N_1(X) = 3 - 1 = 2$ and $N_3(X) = 27 - 1 = 26$ and we did directly $N_2(X) = 12$ so that

$$Z(X, t) \equiv \exp(2t + 12\frac{t^2}{2} + 26\frac{t^3}{3}) \equiv 1 + 2t + 8t^2 + 34t^3 \mod t^4.$$

Also, we have $N_1(\overline{X}) = 3 + 1 = 4$ and $N_3(\overline{X}) = 27 + 1 = 28$ and $N_2(\overline{X}) = 12 + 4 = 16$ so that

$$Z(\overline{X}, t) \equiv \exp(4t + 16\frac{t^2}{2} + 28\frac{t^3}{3}) \equiv 1 + 4t + 16t^2 + 52t^3 \mod t^4.$$

Alternatively, one can derive this by dividing out the previous one by $(1 - t)^2(1 - t^2)$ (exercise !).

Using cohomology

We can use étale ([4]) or rigid ([1]) cohomology in order to compute the Zeta function. We will do rigid cohomology here.

Theorem (Étesse-LS)

If X is a smooth algebraic variety of pure dimension d over $\mathbb{F}_q$, then

$$Z(X,t) = \prod_{i=0}^{2d} \det\left(1 - tq^d (F^*)^{-1}_{|H^i_{\mathrm{rig}}(X)}\right)^{(-1)^{i+1}}.$$

Therefore, what we want to do now is the following:

- Compute the rigid cohomology of X
- Compute the action of Frobenius

Example

We will see below how to compute the action of Frobenius on the rigid cohomology of our elliptic curve X. As a consequence, the Zeta function of $\overline{X}$ will have the following form:

$$Z(\overline{X}, t) = \frac{1 - at + qt^2}{(1-t)(1-qt)}.$$

In particular, the Zeta function is completely determined once we know $N(\overline{X}) = q + 1 - a$ (use logarithmic derivative).

When $q \equiv -1 \mod 4$, we saw that $N(\overline{X}) = q + 1$. Thus, we get $a = 0$ and an easy computation shows that

$$Z(\overline{X}, t) \equiv 1+(q+1)t+(q^2+2q+1)t^2+(q^3+2q^2+2q+1)t^3 \mod t^4$$

which is a generalization of the above formula (case $q = 3$).

Example (continuing)

As an application, we may choose $q = 7$ and get

$$\log Z(\overline{X}, t) = 8t + 32t^2 \mod t^3.$$

We recover $N(\overline{X}) = 8$ and discover $N_2(\overline{X}) = 64$ so that $N_2(X) = 60$. Thus, the equation $y^2 = x^3 + x$ has 60 solutions with $y \neq 0$ over $\mathbb{F}_7[i]$.

We can also do the case $q = 5$. We know that $N(\overline{X}) = 4$ so that $4 = 5 + 1 - a$ and thus $a = 2$. In other words, we have

$$Z(\overline{X}, t) = \frac{1 - 2t + 5t^2}{(1 - t)(1 - 5t)}.$$

It follows that

$$\log Z(\overline{X}, t) = 4t + 16t^2 \mod t^3$$

form which we recover $N(\overline{X}) = 4$ but we also discover $N_2(\overline{X}) = 32$

Computing cohomology

The true power of rigid cohomology is that we can define it whenever we are in a suitable geometric situation and show afterwards that this is well defined.

Assume for example that there exists a scheme $\mathcal{X}$ over $\mathbb{Z}_q$ (unramified lifting of $\mathbb{F}_q$ over $\mathbb{Z}_p$) such that

$$X = \mathcal{X} \otimes_{\mathbb{Z}_q} \mathbb{F}_q$$

and a smooth proper scheme $\overline{\mathcal{X}}$ over $\mathbb{Z}_q$ such that $\mathcal{X}$ is the complement of a relative normal crossing divisor with smooth components. Then, one can define

$$H^*_{\mathrm{rig}}(X) := H^*_{\mathrm{dR}}(\mathcal{X} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q).$$

Recall that de Rham cohomology is obtained by differentiating functions. We can work out an example right now.

Example

We consider again the affine curve $y^2 = x^3 + x, y \neq 0$. We will have

$$H^*_{\mathrm{rig}}(X) := H^*(A \xrightarrow{\mathrm{d}} A\mathrm{d}x)$$

(meaning $H^0_{\mathrm{rig}}(X) = \ker \mathrm{d} : A \to A\mathrm{d}x$ and $H^1_{\mathrm{rig}}(X) = A\mathrm{d}x/\mathrm{d}A$) with

$$A := \mathbb{Q}_q[x, y, \frac{1}{y}]/(y^2 - x^3 - x) \quad \text{and} \quad \mathrm{d}y = \frac{3x^2+1}{2y}\mathrm{d}x.$$

Actually, it is convenient to set $B := \mathbb{Q}_q[x, \frac{1}{x^3+x}]$, so that

$$A = B \oplus By \quad \text{and} \quad \mathrm{d}y = \frac{3x^2+1}{2(x^3+x)}y\mathrm{d}x.$$

We may then split the computation in two parts:

$$H^*_{\mathrm{rig}}(X) := H^*(B \xrightarrow{\mathrm{d}} B\mathrm{d}x) \oplus H^*(By \xrightarrow{\mathrm{d}} By\mathrm{d}x).$$

Example (continuing)

Any element of B can be written in a unique way as a finite sum

$$f(x) = \sum P_k(x)(x^3 + x)^k$$

with $\deg P_k \leq 2$. All terms can be integrated unless $k = -1$ and we obtain

$$H^1(B \xrightarrow{\mathrm{d}} B\mathrm{d}x) \simeq \mathbb{Q}_q \frac{\mathrm{d}x}{y^2} \oplus \mathbb{Q}_q x \frac{\mathrm{d}x}{y^2} \oplus \mathbb{Q}_q x^2 \frac{\mathrm{d}x}{y^2}.$$

The second part requires some more work but one finds

$$H^1(By \xrightarrow{\mathrm{d}} By\mathrm{d}x) \simeq \mathbb{Q}_q \frac{\mathrm{d}x}{y} \oplus \mathbb{Q}_q x \frac{\mathrm{d}x}{y}.$$

Using standard properties of rigid cohomology, one can show that this last vector space is actually identical to $H^1_{\mathrm{rig}}(\overline{X})$.

Frobenius action

The *Frobenius map* on an $\mathbb{F}_q$-variety X is the identity on the underlying topological space but it raises functions to the q-th power.

Unfortunately, the map $f \mapsto f^q$ on X does not lift to $\mathcal{X}$ in general.

Example

The endomorphism

$$F : (x, y) \mapsto (x^q, y^q)$$

of the affine plane over $\mathbb{Z}_q$ does not keep $\mathcal{X}$ stable in the example above:

$$(x^q)^3 + x^q = x^{3q} + x^q \neq (x^3 + x)^q = (y^q)^2$$

There is a solution: one may replace $\mathcal{X}$ with its p-adic completion $\widehat{\mathcal{X}}$. In other words, we can replace polynomials with series that converge on the closed p-adic ball of radius one.

Example

In the case of the curve $y^2 = x^3 + x, y \neq 0$, we would replace A with

$$\widehat{A} := \mathbb{Q}_q\{x, y, 1/y\}/(y^2 - x^3 - x)$$

where

$$\mathbb{Q}_q\{x, y, 1/y\} = \left\{ \sum_{i \in \mathbb{N}, j \in \mathbb{Z}} a_{i,j} x^i y^j, a_{i,j} \to 0 \right\}$$

(which means that $a_{i,j}$ must be divisible by any high power of p when i or $|j|$ are big enough).

We may then define

$$F : (x, y) \mapsto \left(x^q, y^q \sqrt{\frac{x^{3q} + x^q}{(x^3 + x)^q}} \right)$$

in order to get a lifting of Frobenius to $\widehat{A}$. We need to give a meaning to this square root.

Example (continuing)

Since

$$(x^3 + x)^q \equiv x^{3q} + x^q \mod p,$$

we can write

$$\frac{x^{3q} + x^q}{(x^3 + x)^q} = 1 + pz$$

and use

$$\sqrt{1 + pz} = \sum_{n \geq 0} \binom{n}{\frac{1}{2}} p^n z^n.$$

This series converges for $|z| < \frac{1}{|p|}$, and in particular on the closed disc of radius one.

Unfortunately, unless $\mathcal{X}$ is proper, we have

$$H^*_{\mathrm{dR}}(\widehat{\mathcal{X}} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q) \neq H^*_{\mathrm{dR}}(\mathcal{X} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q).$$

Example

$$\widehat{\mathbb{A}^1_{\mathbb{Z}_q}} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q = \mathbb{D}_{\mathbb{Q}_q}(0, 1^+)$$

and

$$H^*_{\mathrm{dR}}(\mathbb{D}_{\mathbb{Q}_p}(0, 1^+)) = H^*(\mathbb{Q}_q\{t\} \xrightarrow{\mathrm{d}} \mathbb{Q}_q\{t\}\mathrm{d}t).$$

One easily sees that the series

$$\sum_k p^k t^{p^k} \in \mathbb{Q}_q\{t\},$$

for example, is not integrable and it follows that

$$H^1_{\mathrm{dR}}(\mathbb{D}_{\mathbb{Q}_p}(0, 1^+)) \neq 0 = H^1_{\mathrm{dR}}(\mathbb{A}^1_{\mathbb{Q}_p}).$$

Actually, there exists a better object $\mathcal{X}^\dagger$ that lies between $\mathcal{X}$ and $\widehat{\mathcal{X}}$ called the *weak completion* of $\mathcal{X}$ such that

$$H^*_{\mathrm{dR}}(\mathcal{X}^\dagger \otimes_{\mathbb{Z}_q} \mathbb{Q}_q) = H^*_{\mathrm{dR}}(\mathcal{X} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q),$$

and we can still lift morphisms.

Example

In the case of the curve $y^2 = x^3 + x, y \neq 0$, we will replace A with

$$A^\dagger := \mathbb{Q}_q[x, y, 1/y]^\dagger/(y^2 - x^3 - x)$$

where

$$\mathbb{Q}_q[x, y, 1/y]^\dagger = \left\{ \sum_{i\in\mathbb{N}, j\in\mathbb{Z}} a_{i,j} x^i y^j, \exists \lambda > 1, |a_{i,j}|\lambda^{i+|j|} \to 0 \right\}$$

(overconvergent series) and the above Frobenius is actually defined on $A^\dagger$. This technique works as well for any hyperelliptic curve ([2]) and leads to efficient algorithms.

Rigid cohomology

Here is how Pierre Berthelot defines *rigid cohomology*. Let k be any field and X a variety over k. Let K be a non trivial complete ultrametric field of characteristic 0 with residue field k.

Let $X \hookrightarrow P$ be an embedding into a proper smooth (around X) formal $\mathcal{O}_K$-scheme. Let P_K be the generic fiber of P (which is an analytic K-variety). Denote by $]X[_P$ the *tube* of X in P (we have $]X[_P := \widehat{P}_K^X$ if X is closed and we can use boolean combinations in general). Let $\iota_X :]X[_P \hookrightarrow P_K$ be the inclusion map. Then, we set

$$H^*_{\mathrm{rig}}(X/K) := H^*(]X[_P, \iota_X^{-1}\Omega^\bullet_{P_K})$$

(in Huber or Berkovich sense - use $j^\dagger$ with Tate theory).

The magic of it is that rigid cohomology does not depend on the choice of the embedding (see [3] for example) !

Jean-Yves Étesse and Bernard Le Stum.
Fonctions L associées aux F-isocristaux surconvergents. I. Interprétation cohomologique.
Math. Ann., 296(3):557–576, 1993.

Kiran S. Kedlaya.
Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology.
J. Ramanujan Math. Soc., 16(4):323–338, 2001.

Bernard Le Stum.
Rigid cohomology, volume 172 of *Cambridge Tracts in Mathematics*.
Cambridge University Press, Cambridge, 2007.

James S. Milne.
Étale cohomology, volume 33 of *Princeton Mathematical Series*.
Princeton University Press, Princeton, N.J., 1980.

Extra slide

Up to my knowledge, the following result si still a conjecture:

Theorem (conjecture)

If X is affine of dimension d, then $H^i_{\mathrm{rig}}(X/K) = 0$ for $i \geq d+1$.

The result is known in the following cases:

1. X is smooth,
2. $i > d+1$,
3. $d = 1$ (and very likely $d = 2$).

– Thank you –