Counting solutions to equations over finite fields

Jan Tuitman (KU Leuven)

November 23, 2016

Finite Fields

A field is a set of numbers in which one can add, substract, multiply and divide like $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.

Finite Fields

A field is a set of numbers in which one can add, substract, multiply and divide like $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.

A finite field is a field with a finite number of elements. This number of elements is always a prime power and for every prime power $q = p^a$ there exists exactly one field $\mathbb{F}_q$ with q elements.

Finite Fields

A field is a set of numbers in which one can add, substract, multiply and divide like $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.

A finite field is a field with a finite number of elements. This number of elements is always a prime power and for every prime power $q = p^a$ there exists exactly one field $\mathbb{F}_q$ with q elements.

For p prime:

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \qquad (\text{ integers modulo } p).$$

For $q = p^a$:

$$\mathbb{F}_q = \mathbb{F}_p[x]/f(x) \qquad (\text{ where } f \in \mathbb{F}_p[x] \text{ irreducible of degree } a).$$

Finite Fields

A field is a set of numbers in which one can add, substract, multiply and divide like $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.

A finite field is a field with a finite number of elements. This number of elements is always a prime power and for every prime power $q = p^a$ there exists exactly one field $\mathbb{F}_q$ with q elements.

For p prime:

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \qquad (\text{ integers modulo } p).$$

For $q = p^a$:

$$\mathbb{F}_q = \mathbb{F}_p[x]/f(x) \qquad (\text{ where } f \in \mathbb{F}_p[x] \text{ irreducible of degree } a).$$

Note that $\mathbb{F}_{q_1} \subset \mathbb{F}_{q_2}$ if and only if $q_2 = q_1^k$ for some $k \in \mathbb{N}$.

Zeta functions

Let $f_1, \ldots, f_m \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$ be homogeneous polynomials.

Zeta functions

Let $f_1, \ldots, f_m \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$ be homogeneous polynomials.

The zero locus $f_1 = f_2 = \ldots = f_m = 0$ defines a projective algebraic variety

$$X \subset \mathbb{P}^n_{\mathbb{F}_q}$$

in projective n-space (identifying points that are multiples).

Zeta functions

Let $f_1, \ldots, f_m \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$ be homogeneous polynomials.

The zero locus $f_1 = f_2 = \ldots = f_m = 0$ defines a projective algebraic variety

$$X \subset \mathbb{P}^n_{\mathbb{F}_q}$$

in projective n-space (identifying points that are multiples).

For any $k \in \mathbb{N}$, let $X(\mathbb{F}_{q^k})$ denote the set of points of X with coordinates in $\mathbb{F}_{q^k}$ and $|X(\mathbb{F}_{q^k})|$ its cardinality.

Zeta functions

Let $f_1, \ldots, f_m \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$ be homogeneous polynomials.

The zero locus $f_1 = f_2 = \ldots = f_m = 0$ defines a projective algebraic variety

$$X \subset \mathbb{P}^n_{\mathbb{F}_q}$$

in projective n-space (identifying points that are multiples).

For any $k \in \mathbb{N}$, let $X(\mathbb{F}_{q^k})$ denote the set of points of X with coordinates in $\mathbb{F}_{q^k}$ and $|X(\mathbb{F}_{q^k})|$ its cardinality.

The zeta function of X is the formal power series

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

Counting points

From the Weil conjectures (which are a theorem) it is known that the zeta function is not just a formal power series, but a rational function:

$$Z(X,T) = g(T)/h(T) \qquad (\text{ with } f, g \in \mathbb{Z}[T]).$$

Counting points

From the Weil conjectures (which are a theorem) it is known that the zeta function is not just a formal power series, but a rational function:

$$Z(X,T) = g(T)/h(T) \qquad (\text{ with } f, g \in \mathbb{Z}[T]).$$

Hence it is given by a finite amount of data, so in principle can be computed.

Computing the zeta function efficiently is often referred to as point counting.

Counting points

From the Weil conjectures (which are a theorem) it is known that the zeta function is not just a formal power series, but a rational function:

$$Z(X,T) = g(T)/h(T) \qquad (\text{ with } f, g \in \mathbb{Z}[T]).$$

Hence it is given by a finite amount of data, so in principle can be computed.

Computing the zeta function efficiently is often referred to as point counting.

Most of my research is about computing $Z(X,T)$, or equivalently the $|X(\mathbb{F}_{q^k})|$ efficiently (in terms of complexity and in practice).

Counting points

From the Weil conjectures (which are a theorem) it is known that the zeta function is not just a formal power series, but a rational function:

$$Z(X,T) = g(T)/h(T) \qquad (\text{ with } f, g \in \mathbb{Z}[T]).$$

Hence it is given by a finite amount of data, so in principle can be computed.

Computing the zeta function efficiently is often referred to as point counting.

Most of my research is about computing $Z(X,T)$, or equivalently the $|X(\mathbb{F}_{q^k})|$ efficiently (in terms of complexity and in practice).

Computing zeta functions is very central and important problem in mathematics, as we will now explain with some examples.

Sato-Tate conjecture

Let C be a (smooth) projective curve of genus g defined over $\mathbb{Q}$.

Sato-Tate conjecture

Let C be a (smooth) projective curve of genus g defined over $\mathbb{Q}$.

For every prime p let C_p denote the curve over $\mathbb{F}_p$ obtained by reducing (the equations of) C modulo p. For all but a finite number of p:

$$Z(C_p, T) = \frac{\chi_p(T)}{(1-T)(1-qT)}$$

for some polynomial $\chi_p(T) \in \mathbb{Z}[T]$ of degree $2g$.

Sato-Tate conjecture

Let C be a (smooth) projective curve of genus g defined over $\mathbb{Q}$.

For every prime p let C_p denote the curve over $\mathbb{F}_p$ obtained by reducing (the equations of) C modulo p. For all but a finite number of p:

$$Z(C_p, T) = \frac{\chi_p(T)}{(1-T)(1-qT)}$$

for some polynomial $\chi_p(T) \in \mathbb{Z}[T]$ of degree $2g$.

How is the polynomial $\chi_p(T/\sqrt{p})$ distributed when p varies?

Sato-Tate conjecture

Let C be a (smooth) projective curve of genus g defined over $\mathbb{Q}$.

For every prime p let C_p denote the curve over $\mathbb{F}_p$ obtained by reducing (the equations of) C modulo p. For all but a finite number of p:

$$Z(C_p, T) = \frac{\chi_p(T)}{(1-T)(1-qT)}$$

for some polynomial $\chi_p(T) \in \mathbb{Z}[T]$ of degree $2g$.

How is the polynomial $\chi_p(T/\sqrt{p})$ distributed when p varies?

Conjectural answer: as the (reverse) characteristic polynomial of a random conjugacy class of a certain compact group. So far only known for $g = 1$ (elliptic curves).

Sato-Tate conjecture

Let C be a (smooth) projective curve of genus g defined over $\mathbb{Q}$.

For every prime p let C_p denote the curve over $\mathbb{F}_p$ obtained by reducing (the equations of) C modulo p. For all but a finite number of p:

$$Z(C_p, T) = \frac{\chi_p(T)}{(1-T)(1-qT)}$$

for some polynomial $\chi_p(T) \in \mathbb{Z}[T]$ of degree $2g$.

How is the polynomial $\chi_p(T/\sqrt{p})$ distributed when p varies?

Conjectural answer: as the (reverse) characteristic polynomial of a random conjugacy class of a certain compact group. So far only known for $g = 1$ (elliptic curves).

Andrew Sutherland (with coauthors) computed $\chi_p(T)$ for C with $g = 2$ and found all predicted distributions! Methods become impractical for more general curves.

Sato-Tate conjecture

Let C be a (smooth) projective curve of genus g defined over $\mathbb{Q}$.

For every prime p let C_p denote the curve over $\mathbb{F}_p$ obtained by reducing (the equations of) C modulo p. For all but a finite number of p:

$$Z(C_p, T) = \frac{\chi_p(T)}{(1-T)(1-qT)}$$

for some polynomial $\chi_p(T) \in \mathbb{Z}[T]$ of degree $2g$.

How is the polynomial $\chi_p(T/\sqrt{p})$ distributed when p varies?

Conjectural answer: as the (reverse) characteristic polynomial of a random conjugacy class of a certain compact group. So far only known for $g = 1$ (elliptic curves).

Andrew Sutherland (with coauthors) computed $\chi_p(T)$ for C with $g = 2$ and found all predicted distributions! Methods become impractical for more general curves.

Computing zeta functions is also important for gathering experimental data on e.g. the generalised Birch and Swinnerton-Dyer conjecture and the Langlands program.

Cryptography

Let C be a (smooth) projective curve over a finite field $\mathbb{F}_q$.

One can associate to C a finite abelian group $J_C(\mathbb{F}_q)$ called the the Jacobian of C (its rational points).

Cryptography

Let C be a (smooth) projective curve over a finite field $\mathbb{F}_q$.

One can associate to C a finite abelian group $J_C(\mathbb{F}_q)$ called the the Jacobian of C (its rational points).

Let $P, Q \in J_C(\mathbb{F}_q)$ and $k \in \mathbb{N}$ be such that $kP = Q$, where kP means adding k copies of P in the group $J_C(\mathbb{F}_q)$.

Cryptography

Let C be a (smooth) projective curve over a finite field $\mathbb{F}_q$.

One can associate to C a finite abelian group $J_C(\mathbb{F}_q)$ called the the Jacobian of C (its rational points).

Let $P, Q \in J_C(\mathbb{F}_q)$ and $k \in \mathbb{N}$ be such that $kP = Q$, where kP means adding k copies of P in the group $J_C(\mathbb{F}_q)$.

Now given C and P, Q, one can ask for k. This is called the discrete logarithm problem and used in the Diffie-Hellman key exchange protocol.

Cryptography

Let C be a (smooth) projective curve over a finite field $\mathbb{F}_q$.

One can associate to C a finite abelian group $J_C(\mathbb{F}_q)$ called the the Jacobian of C (its rational points).

Let $P, Q \in J_C(\mathbb{F}_q)$ and $k \in \mathbb{N}$ be such that $kP = Q$, where kP means adding k copies of P in the group $J_C(\mathbb{F}_q)$.

Now given C and P, Q, one can ask for k. This is called the discrete logarithm problem and used in the Diffie-Hellman key exchange protocol.

In general very hard, but when the order of $J_C(\mathbb{F}_q)$ only has small prime factors it is easy! However, $|J_C(\mathbb{F}_q)|$ can be read off from the zeta function $Z(C, T)$.

Cryptography

Let C be a (smooth) projective curve over a finite field $\mathbb{F}_q$.

One can associate to C a finite abelian group $J_C(\mathbb{F}_q)$ called the the Jacobian of C (its rational points).

Let $P, Q \in J_C(\mathbb{F}_q)$ and $k \in \mathbb{N}$ be such that $kP = Q$, where kP means adding k copies of P in the group $J_C(\mathbb{F}_q)$.

Now given C and P, Q, one can ask for k. This is called the discrete logarithm problem and used in the Diffie-Hellman key exchange protocol.

In general very hard, but when the order of $J_C(\mathbb{F}_q)$ only has small prime factors it is easy! However, $|J_C(\mathbb{F}_q)|$ can be read off from the zeta function $Z(C, T)$.

Computing zeta functions of curves is also important for constructing good error correcting codes (coming from curves with many points).

Curves

Let C be a smooth projective curve over $\mathbb{F}_q$ with $q = p^a$ given by an affine plane (possibly singular) birational model $Q(x, y) = 0$ (not homogeneous) of degrees d_x, d_y in y and x.

Curves

Let C be a smooth projective curve over $\mathbb{F}_q$ with $q = p^a$ given by an affine plane (possibly singular) birational model $Q(x, y) = 0$ (not homogeneous) of degrees d_x, d_y in y and x.

Suppose that Q admits a good lift to characteristic zero (rather technical).

Curves

Let C be a smooth projective curve over $\mathbb{F}_q$ with $q = p^a$ given by an affine plane (possibly singular) birational model $Q(x, y) = 0$ (not homogeneous) of degrees d_x, d_y in y and x.

Suppose that Q admits a good lift to characteristic zero (rather technical).

Theorem (T,2014)

For all $\epsilon > 0$, the zeta function $Z(C, T)$ can be computed in time

$$O((pd_x^6 d_y^4 a^3)^{1+\epsilon}).$$

Curves

Let C be a smooth projective curve over $\mathbb{F}_q$ with $q = p^a$ given by an affine plane (possibly singular) birational model $Q(x, y) = 0$ (not homogeneous) of degrees d_x, d_y in y and x.

Suppose that Q admits a good lift to characteristic zero (rather technical).

Theorem (T,2014)

For all $\epsilon > 0$, the zeta function $Z(C, T)$ can be computed in time

$$O((pd_x^6 d_y^4 a^3)^{1+\epsilon}).$$

Kiran Kedlaya (2001) did this for hyperelliptic curves $Q = y^2 - f(x)$. People tried to extend this algorithm to more general curves without much succes. In practice remained limited to hyperelliptic and superelliptic curves $(y^k = f(x))$.

Curves

Let C be a smooth projective curve over $\mathbb{F}_q$ with $q = p^a$ given by an affine plane (possibly singular) birational model $Q(x, y) = 0$ (not homogeneous) of degrees d_x, d_y in y and x.

Suppose that Q admits a good lift to characteristic zero (rather technical).

Theorem (T,2014)

For all $\epsilon > 0$, the zeta function $Z(C, T)$ can be computed in time

$$O((pd_x^6 d_y^4 a^3)^{1+\epsilon}).$$

Kiran Kedlaya (2001) did this for hyperelliptic curves $Q = y^2 - f(x)$. People tried to extend this algorithm to more general curves without much succes. In practice remained limited to hyperelliptic and superelliptic curves ($y^k = f(x)$).

In contrast to other extensions of Kedlaya's algorithm, my algorithm is general, practical and completely implemented (by me, in Magma).

Curves

Let C be a smooth projective curve over $\mathbb{F}_q$ with $q = p^a$ given by an affine plane (possibly singular) birational model $Q(x, y) = 0$ (not homogeneous) of degrees d_x, d_y in y and x.

Suppose that Q admits a good lift to characteristic zero (rather technical).

Theorem (T,2014)

For all $\epsilon > 0$, the zeta function $Z(C, T)$ can be computed in time

$$O((pd_x^6 d_y^4 a^3)^{1+\epsilon}).$$

Kiran Kedlaya (2001) did this for hyperelliptic curves $Q = y^2 - f(x)$. People tried to extend this algorithm to more general curves without much succes. In practice remained limited to hyperelliptic and superelliptic curves $(y^k = f(x))$.

In contrast to other extensions of Kedlaya's algorithm, my algorithm is general, practical and completely implemented (by me, in Magma).

Together with Wouter Castryck I showed (2016) how to find a good lift to characteristic zero of lowest possible degrees for all curves of genus $g \leq 5$.

Hypersurfaces

Let X be a projective variety over $\mathbb{F}_q$ with $q = p^a$ defined by a single (sufficiently general) homogeneous polynomial $P \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$ of degree d and let ω be an exponent for matrix multiplication.

Hypersurfaces

Let X be a projective variety over $\mathbb{F}_q$ with $q = p^a$ defined by a single (sufficiently general) homogeneous polynomial $P \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$ of degree d and let ω be an exponent for matrix multiplication.

Theorem (Pancratz-T,2013)

For all $\epsilon > 0$, the zeta function $Z(X, T)$ can be computed in time

$$O((pd^{(\omega+4)n}e^{(\omega+1)n}a^3)^{1+\epsilon}).$$

Hypersurfaces

Let X be a projective variety over $\mathbb{F}_q$ with $q = p^a$ defined by a single (sufficiently general) homogeneous polynomial $P \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$ of degree d and let ω be an exponent for matrix multiplication.

Theorem (Pancratz-T,2013)

For all $\epsilon > 0$, the zeta function $Z(X,T)$ can be computed in time

$$O((pd^{(\omega+4)n}e^{(\omega+1)n}a^3)^{1+\epsilon}).$$

Improvement of Alan Lauder's deformation method (2004) which has p^2 instead of p and $\omega + 5$ instead of $\omega + 4$.

Hypersurfaces

Let X be a projective variety over $\mathbb{F}_q$ with $q = p^a$ defined by a single (sufficiently general) homogeneous polynomial $P \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$ of degree d and let ω be an exponent for matrix multiplication.

Theorem (Pancratz-T,2013)

For all $\epsilon > 0$, the zeta function $Z(X, T)$ can be computed in time

$$O((pd^{(\omega+4)n} e^{(\omega+1)n} a^3)^{1+\epsilon}).$$

Improvement of Alan Lauder's deformation method (2004) which has p^2 instead of p and $\omega + 5$ instead of $\omega + 4$.

Unlike Lauder's, our algorithm is completely implemented (in C using FLINT). Implementation possible because we improved precision bounds by orders of magnitude.

The most important example of this are the bounds from 'effective bounds on convergence of Frobenius structures on connections' (Kedlaya-T,2012).

p-adic cohomology

The field $\mathbb{Q}_p$ of p-adic numbers defined as the completion (as a metric space) of $\mathbb{Q}$ with respect to the norm

$$\left| \frac{a}{b} \right| = p^{\mathrm{ord}_p(b) - \mathrm{ord}_p(a)}$$

where ord_p denotes the number of factors p in the prime factorisation of an integer. For $q = p^a$ one can define $\mathbb{Q}_q$ as the unique unramified extension of degree a of $\mathbb{Q}_p$.

p-adic cohomology

The field $\mathbb{Q}_p$ of p-adic numbers defined as the completion (as a metric space) of $\mathbb{Q}$ with respect to the norm

$$\left|\frac{a}{b}\right| = p^{\mathrm{ord}_p(b)-\mathrm{ord}_p(a)}$$

where ord_p denotes the number of factors p in the prime factorisation of an integer. For $q = p^a$ one can define $\mathbb{Q}_q$ as the unique unramified extension of degree a of $\mathbb{Q}_p$.

For a projective variety X over $\mathbb{F}_q$ with $q = p^a$, one can define rigid cohomology spaces $H^i_{\mathrm{rig}}(X)$, which are finite dimensional $\mathbb{Q}_q$ vector spaces with an action F_q^* of the q-th power map F_q, such that

$$Z(X,T) = \prod_{i=0}^{2\dim X} \det(1 - T\,\mathrm{F}_q^* | H^i_{\mathrm{rig}}(X))^{(-1)^{i+1}}$$

We compute the $H^i_{\mathrm{rig}}(X)$ with the matrices of F_q^* and then deduce the zeta function.

p-adic cohomology

The field $\mathbb{Q}_p$ of p-adic numbers defined as the completion (as a metric space) of $\mathbb{Q}$ with respect to the norm

$$\left|\frac{a}{b}\right| = p^{\mathrm{ord}_p(b)-\mathrm{ord}_p(a)}$$

where ord_p denotes the number of factors p in the prime factorisation of an integer. For $q = p^a$ one can define $\mathbb{Q}_q$ as the unique unramified extension of degree a of $\mathbb{Q}_p$.

For a projective variety X over $\mathbb{F}_q$ with $q = p^a$, one can define rigid cohomology spaces $H^i_{\mathrm{rig}}(X)$, which are finite dimensional $\mathbb{Q}_q$ vector spaces with an action F_q^* of the q-th power map F_q, such that

$$Z(X,T) = \prod_{i=0}^{2\dim X} \det(1 - T\,\mathrm{F}_q^* | H^i_{\mathrm{rig}}(X))^{(-1)^{i+1}}$$

We compute the $H^i_{\mathrm{rig}}(X)$ with the matrices of F_q^* and then deduce the zeta function.

In the hypersurface case, we first deform X to a simpler (diagonal) hypersurface to compute $H^i_{\mathrm{rig}}(X)$ and F_q^* (using Gauss–Manin connections).

Large p & average polynomial time

So far I have only mentioned my own algorithms. For fixed characteristic p these represent the state of the art.

Large p & average polynomial time

So far I have only mentioned my own algorithms. For fixed characteristic p these represent the state of the art.

However, input size of the problem is about:

- $\log(p) d_x d_y a$ in the curve case
- $\log(p) d^n a$ in the hypersurface case.

The complexity of my algorithms is quasilinear in p, hence exponential in $\log(p)$.

Large p & average polynomial time

So far I have only mentioned my own algorithms. For fixed characteristic p these represent the state of the art.

However, input size of the problem is about:

- $\log(p) d_x d_y a$ in the curve case
- $\log(p) d^n a$ in the hypersurface case.

The complexity of my algorithms is quasilinear in p, hence exponential in $\log(p)$.

Used to be the case for all algorithms (apart from Schoof-Pila, which is restriced to curves, in practice even to genus $g \leq 2$).

Large p & average polynomial time

So far I have only mentioned my own algorithms. For fixed characteristic p these represent the state of the art.

However, input size of the problem is about:

- $\log(p) d_x d_y a$ in the curve case
- $\log(p) d^n a$ in the hypersurface case.

The complexity of my algorithms is quasilinear in p, hence exponential in $\log(p)$.

Used to be the case for all algorithms (apart from Schoof-Pila, which is restriced to curves, in practice even to genus $g \leq 2$).

Recently, David Harvey has introduced algorithms with complexity quasilinear in $p^{1/2}$ (2007) and even average polynomial time (2014), i.e. time polynomial in $\log(p)$ per prime p computing for enough primes p simultaneously.

However, Harvey's complexity in terms of (d_x, d_y, d, n, a) is a lot worse.

Large p & average polynomial time

So far I have only mentioned my own algorithms. For fixed characteristic p these represent the state of the art.

However, input size of the problem is about:

- $\log(p) d_x d_y a$ in the curve case
- $\log(p) d^n a$ in the hypersurface case.

The complexity of my algorithms is quasilinear in p, hence exponential in $\log(p)$.

Used to be the case for all algorithms (apart from Schoof-Pila, which is restriced to curves, in practice even to genus $g \leq 2$).

Recently, David Harvey has introduced algorithms with complexity quasilinear in $p^{1/2}$ (2007) and even average polynomial time (2014), i.e. time polynomial in $\log(p)$ per prime p computing for enough primes p simultaneously.

However, Harvey's complexity in terms of (d_x, d_y, d, n, a) is a lot worse.

My main goal is to combine Harvey's methods with mine and get the best of both. I am currently writing this down for the hypersurface case.

Coleman integration

I am computing cohomology spaces, which have other applications as well! The most important of these is to Coleman integration and the Chabauty method.

Coleman integration

I am computing cohomology spaces, which have other applications as well! The most important of these is to Coleman integration and the Chabauty method.

Let:

- X a smooth projective curve over $\mathbb{Q}_p$ (of good reduction)
- $P, Q \in X(\mathbb{Q}_p)$ points of X with coordinates in $\mathbb{Q}_p$
- $\omega \in \Omega^1(X)$ a regular 1-form

Coleman integration

I am computing cohomology spaces, which have other applications as well! The most important of these is to Coleman integration and the Chabauty method.

Let:

- X a smooth projective curve over $\mathbb{Q}_p$ (of good reduction)
- $P, Q \in X(\mathbb{Q}_p)$ points of X with coordinates in $\mathbb{Q}_p$
- $\omega \in \Omega^1(X)$ a regular 1-form

Robert Coleman (1985) defined a path independent line integral:

$$\int_P^Q \omega.$$

Coleman integration

I am computing cohomology spaces, which have other applications as well! The most important of these is to Coleman integration and the Chabauty method.

Let:

- X a smooth projective curve over $\mathbb{Q}_p$ (of good reduction)
- $P, Q \in X(\mathbb{Q}_p)$ points of X with coordinates in $\mathbb{Q}_p$
- $\omega \in \Omega^1(X)$ a regular 1-form

Robert Coleman (1985) defined a path independent line integral:

$$\int_P^Q \omega.$$

This is nontrivial since over $\mathbb{Q}_p$ (totally disconnected) we do not have analytic continuation to fix the integration constants.

The Chabauty method

This is particulary interesting since Coleman used it to reformulate the Chabauty method:

The Chabauty method

This is particulary interesting since Coleman used it to reformulate the Chabauty method:

Theorem

Let $\mathcal{X}$ be a curve of genus $g \geq 2$ over $\mathbf{Q}$, J the Jacobian of $\mathcal{X}$, p a prime of good reduction and $X = \mathcal{X} \otimes \mathbf{Q}_p$. Moreover, let r be the Mordell-Weil rank of $\mathcal{X}$ and suppose that $r < g$. Then there exists $\omega \in \Omega^1(X)$ such that $\int_P^Q \omega = 0$ for all $P, Q \in \mathcal{X}(\mathbf{Q})$.

The Chabauty method

This is particulary interesting since Coleman used it to reformulate the Chabauty method:

Theorem

Let $\mathcal{X}$ be a curve of genus $g \geq 2$ over $\mathbf{Q}$, J the Jacobian of $\mathcal{X}$, p a prime of good reduction and $X = \mathcal{X} \otimes \mathbf{Q}_p$. Moreover, let r be the Mordell-Weil rank of $\mathcal{X}$ and suppose that $r < g$. Then there exists $\omega \in \Omega^1(X)$ such that $\int_P^Q \omega = 0$ for all $P, Q \in \mathcal{X}(\mathbf{Q})$.

So by computing Coleman integrals, one might sometimes be able to find rational points, or prove that we have found all of them.

The Chabauty method

This is particulary interesting since Coleman used it to reformulate the Chabauty method:

Theorem

Let $\mathcal{X}$ be a curve of genus $g \geq 2$ over $\mathbf{Q}$, J the Jacobian of $\mathcal{X}$, p a prime of good reduction and $X = \mathcal{X} \otimes \mathbf{Q}_p$. Moreover, let r be the Mordell-Weil rank of $\mathcal{X}$ and suppose that $r < g$. Then there exists $\omega \in \Omega^1(X)$ such that $\int_P^Q \omega = 0$ for all $P, Q \in \mathcal{X}(\mathbf{Q})$.

So by computing Coleman integrals, one might sometimes be able to find rational points, or prove that we have found all of them.

Remark

The nonabelian Chabauty method of Minhyong Kim tries to get rid of the assumption $r < g$. This still involves (iterated) Coleman integrals!

Coleman integration on general curves

For hyperelliptic curves Kedlaya's algorithm has been adapted (2010) to compute Coleman integrals and do Chabauty as well by Jennifer Balakrishnan (with coauthors).

Coleman integration on general curves

For hyperelliptic curves Kedlaya's algorithm has been adapted (2010) to compute Coleman integrals and do Chabauty as well by Jennifer Balakrishnan (with coauthors).

This was not extended to other curves, because there was no practical Kedlaya type algorithm for more general curves.

Coleman integration on general curves

For hyperelliptic curves Kedlaya's algorithm has been adapted (2010) to compute Coleman integrals and do Chabauty as well by Jennifer Balakrishnan (with coauthors).

This was not extended to other curves, because there was no practical Kedlaya type algorithm for more general curves.

Over the past year together with Balakrishnan I have adapted my algorithm for curves to compute both single and iterated Coleman integrals for all curves including a complete implementation.

This should be out very soon!

Coleman integration on general curves

For hyperelliptic curves Kedlaya's algorithm has been adapted (2010) to compute Coleman integrals and do Chabauty as well by Jennifer Balakrishnan (with coauthors).

This was not extended to other curves, because there was no practical Kedlaya type algorithm for more general curves.

Over the past year together with Balakrishnan I have adapted my algorithm for curves to compute both single and iterated Coleman integrals for all curves including a complete implementation.

This should be out very soon!

My next goal: apply this to nonabelian Chabauty, i.e. in cases with $r \geq g$, where the theory is less clear. I have already started working on the modular curve $X_{ns}(13)$.