Hyperelliptic curves over function fields

The arithmetic of hyperelliptic curves

David Kurniadi Angdinata

University College London

Friday, 28 November 2025

Global function fields

A *function field* $F = k(C)$ is that of a *nice* [1] curve C over a base field k. When $k = \mathbb{F}_q$ is a finite field of size q, this is a *global function field*.

A *ring of integers* $\mathcal{O}_F$ of a global function field F is the ring of sections over an open affine $U \subseteq C$, in which case $C \setminus U$ are its *infinite places*. This is a Dedekind domain, so it has a potentially infinite class group.

A *place* $v \in V_F$ of a global function field F is the Galois orbit of a point $x \in C(\overline{k})$, or equivalently a maximal ideal of a ring of integers $\mathcal{O}_F$. The localisation of $\mathcal{O}_F$ at v is a non-archimedean discrete valuation ring.

Example

If $C = \mathbb{P}^1$ and $k = \mathbb{F}_q$, then $F = \mathbb{F}_q(t)$ is a global function field, and the ring of integers $\mathcal{O}_F = \mathbb{F}_q[t]$ has a unique infinite place $1/t \in V_F$ with valuation $\mathrm{ord}_{1/t} : F \to \mathbb{Z} \cup \{\infty\}$ given by $\mathrm{ord}_{1/t}(f/g) = \deg g - \deg f$.

[1] smooth proper geometrically irreducible

Curves and Jacobians

Let X be a nice curve of genus g_X over the function field F of a nice curve C of genus g_C over a base field k. Associated to X is a principally polarised abelian variety of dimension g_X over F called its *Jacobian* J_X.

There is a unique abelian variety A_X over k, called the F/k-**trace** of J_X, and a unique morphism $\tau_X : A_X \times_k F \to J_X$, such that for any abelian variety A over k with a morphism $\tau : A \times_k F \to J_X$, there is a unique morphism $\psi : A \to A_X$ such that $\tau_X \circ (\psi \times_k F) = \tau$.

Theorem (Lang–Néron)

If F is a finitely generated regular field extension of k, then the Mordell–Weil group $J_X(F)/\tau_X(A_{J_k} \times_k F)$ is finitely generated.

If $J_X \times_F K \cong A \times_{\overline{k}} K$ for some abelian variety A over $\overline{k}$ and some finite extension K of F, then J_X is called **isotrivial**. If J_X is a non-isotrivial elliptic curve, then $A_X = 0$, which recovers the Mordell–Weil theorem.

A hyperelliptic curve

Example

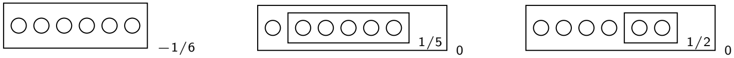
Let X be the hyperelliptic curve over $F = \mathbb{F}_{13}(t)$ given by

$$y^2 = f(x) := x^6 + x^5 + t.$$

Then J_X is non-isotrivial, and in fact geometrically irreducible.

Since the roots of $f'(x) = 6x^5 + 5x^4$ are only $x = 0$ and $x = -5/6$, it is unramified everywhere except possibly at $1/t$, at t, and at $t - 5^5/6^6$, and in fact tamely ramified everywhere since $2g_X + 1 = 5 < 13$.

The cluster pictures of X at $1/t$, at t, and at $t - 5^5/6^6$ are respectively:



A simple computation shows that $\mathfrak{f}(J_X) = (1/t)^5 \cdot t^4 \cdot (t - 5^5/6^6)$.

L-functions

Let k be finite, and let ρ be a nice [2] ℓ-adic representation of F for some fixed auxiliary prime $\ell \neq \mathrm{char}(k)$. The **L-function** of ρ is given by

$$L(\rho, T) := \prod_{v \in V_F} \det(1 - T \cdot \varphi_v \mid \rho^{I_v})^{-1},$$

which is the L-function of J_X when $\rho = \rho_{J_X} := H^1_{\text{ét}}(\overline{X}, \mathbb{Q}_\ell)$ and $T = q^{-s}$.

Theorem (Deligne–Grothendieck)

The numerator of the rational function $L(\rho, T)$ is precisely $\det(1 - T \cdot \phi_q \mid H^1_{\text{ét}}(\overline{C}, \mathcal{F}_\rho))$ *for some constructible sheaves $\mathcal{F}_\rho$ on C, and*

$$\dim H^1_{\text{ét}}(\overline{C}, \mathcal{F}_\rho) = \deg \mathfrak{f}(\rho) + (2g_C - 2)\dim \rho + 2\dim \rho^{\mathrm{Gal}(\overline{k}F/F)}.$$

Here, $\mathcal{F}_\rho$ is the pushforward of a lisse sheaf on an open subset of C where ρ is unramified, and its stalk at any place $v \in V_F$ is precisely ρ^{I_v}.

[2] almost everywhere unramified and pure and self-dual of some integral weight

Artin formalism

Let K be a finite extension of F. Artin's formalism gives a factorisation

$$L(J_X/K, s) := L(\rho_{J_X/K}, q^{-s}) = \prod_{\chi \in \widehat{G}} L(\rho_{J_X} \otimes \chi, q^{-s}),$$

where $\widehat{G}$ is the character group of the Galois closure of K over F.

At the level of étale cohomology, there are also canonical isomorphisms

$$H^1_{\text{ét}}(\overline{C}, \mathcal{F}_{\rho_{J_X/K}}) \cong \bigoplus_{\chi \in \widehat{G}} H^1_{\text{ét}}(\overline{C}, \mathcal{F}_{\rho_{J_X} \otimes \chi}),$$

which respects the action of ϕ_q. Furthermore, if $\widehat{G}$ can be partitioned into subsets $o \subseteq \widehat{G}$, then there are canonical isomorphisms

$$H^1_{\text{ét}}(\overline{C}, \mathcal{F}_{\rho_{J_X/K}}) \cong \bigoplus_{o \subseteq \widehat{G}} H^1_{\text{ét}}(\overline{C}, \mathcal{F}_{\rho_{J_X} \otimes (\bigoplus_{\chi \in o} \chi)}).$$

Geometric vanishing

By Poincaré duality, the Tate twist $H^1_{\text{ét}}(\overline{C}, \mathcal{F}_{\rho_{J_X}(1)\otimes(\bigoplus_{\chi\in o}\chi)})$ admits a ϕ_q-invariant non-degenerate symmetric bilinear pairing for any $o \subseteq \widehat{G}$.

Lemma (Ulmer)

Let $W_1, \ldots, W_{2n}$ be finite-dimensional vector spaces with odd $\dim W_0$, *and let $\phi : \bigoplus_{i=1}^{2n} W_i \to \bigoplus_{i=1}^{2n} W_i$ be a linear map with $\phi(W_i) = W_{i+1}$ for all $i \in \mathbb{Z}/2n$, such that $\bigoplus_{i=1}^{2n} W_i$ admits a ϕ_q-invariant non-degenerate symmetric bilinear pairing that induces an isomorphism $W_n \cong W_0^*$. Then*

$$1 - T^{2n} \textit{ divides } \det(1 - T\cdot\phi \mid \textstyle\bigoplus_{i=1}^{2n} W_i).$$

In particular, for each subset $o \subseteq \widehat{G}$ satisfying appropriate assumptions,

$$1 - (qT)^{2n} \text{ divides } \det(1 - T\cdot\phi_q \mid H^1_{\text{ét}}(\overline{C}, \mathcal{F}_{\rho_{J_X}\otimes(\bigoplus_{\chi\in o}\chi)})),$$

which increments the order of vanishing of $L(J_X/K, s)$.

A Frobenius action

Example (Ulmer)

Let $F = \mathbb{F}_{13}(t)$, and let $K = \mathbb{F}_{13}(\sqrt[170]{t})$. Then $\mathrm{Gal}(\overline{\mathbb{F}_{13}}(t)/\mathbb{F}_{13}(t)) \cong \widehat{\mathbb{Z}}$ is generated by ϕ_{13}, which acts naturally on $\widehat{G} \cong \mathbb{Z}/170$ by

$$\phi_{13}^i \cdot \chi := (\sigma \mapsto \chi(\phi_{13}^i(\sigma))),$$

which translates to multiplication by $13^{-1} \equiv -13 \mod 170$.

Let $\widehat{G} \cong \mathbb{Z}/170$ be partitioned by the 44 orbits of this action given by the singletons $\{0\}$ and $\{85\}$, and $\{\pm n, \pm 13n\}$ for each $n \in \mathbb{N}$.

Let X be as before. If the order of $\chi \in \widehat{G}$ is sufficiently large,

$$\dim H^1_{\text{ét}}(\overline{C}, \mathcal{F}_{\rho_{J_X}(1)\otimes\chi}) \equiv \deg \mathfrak{f}(\rho_{J_X}(1) \otimes \chi) \equiv \deg \mathfrak{f}(\rho_{J_X}) \mod 2,$$

which is odd. Thus the previous lemma applies, and the order of vanishing of $L(J_X/K, s)$ at $s = 1$ is at least $44 - c$ for some small $c \in \mathbb{N}$.

The Birch–Swinnerton-Dyer conjecture

Conjecture (Birch–Swinnerton-Dyer)

The order of vanishing of $L(J_X, s)$ at $s = 1$ is $\mathrm{rk}(J_X)$, with leading term

$$\lim_{s\to 1} \frac{L(J_X, s)}{(s-1)^{\mathrm{rk}(J_X)}} = \frac{\mathrm{Reg}(J_X)\cdot \#\text{Ш}(J_X)\cdot \mathrm{Tam}(J_X)}{\#\,\mathrm{tor}(J_X)^2}.$$

This implicitly assumes that $\text{Ш}(J_X)$ is finite, which by the exact sequence

$$0 \to J_X(F)\otimes \mathbb{Z}_\ell \to \varprojlim_n \mathrm{Sel}_{\ell^n}(J_X) \to T_\ell \text{Ш}(J_X) \to 0,$$

implies that the first map is an isomorphism.

Theorem (Artin–Tate, Milne, Schneider, Bauer, Kato–Trihan)

The rank conjecture is equivalent to the finiteness of $\text{Ш}(J_X)[\ell^\infty]$ for any prime ℓ, in which case the leading term conjecture also holds.

Invariants of surfaces

For any nice curve X over F, there is a unique irreducible proper regular relatively minimal surface $\mathcal{X} \to C$ over k, whose generic fibre is X.

If S is a proper regular surface over k, its **Picard** and **Brauer groups** are

$$\mathrm{Pic}(S) := H^1_{\text{ét}}(S, \mathbb{G}_m), \qquad \mathrm{Br}(S) := H^2_{\text{ét}}(S, \mathbb{G}_m).$$

The **Néron–Severi group** $\mathrm{NS}(S)$ is the image of $\mathrm{Pic}(S)$ in the quotient of $\mathrm{Pic}(\overline{S})$ by its subgroup of divisors algebraically equivalent to zero.

Theorem (Shioda–Tate)

If f_v is the number of irreducible components of the fibre $\mathcal{X}_v$ at v, then

$$\mathrm{rk}(\mathrm{NS}(\mathcal{X})) - \mathrm{rk}(J_X) = 2 + \sum_v (f_v - 1).$$

Theorem (Grothendieck)

There is a canonical isomorphism $\mathrm{Br}(\mathcal{X}) \xrightarrow{\sim} Ш(J_X)$.

The Tate conjecture

Analogously to J_X, there is an exact sequence

$$0 \to \mathrm{NS}(\mathcal{X}) \otimes \mathbb{Z}_\ell \xrightarrow{c_\ell} \varprojlim_n H^2_{\text{ét}}(\overline{\mathcal{X}}, \mu_{\ell^n})^{G_k} \to T_\ell \operatorname{Br}(\mathcal{X}) \to 0,$$

so the finiteness of $Ш(J_X)[\ell^\infty]$ reduces to c_ℓ being an isomorphism.

Conjecture (Tate)

The cycle class map c_ℓ is an isomorphism for any prime ℓ. Equivalently,

$$\mathrm{rk}(\mathrm{NS}(\mathcal{X})) = -\operatorname{ord}_{s=1} \zeta(\mathcal{X}, s).$$

In particular, this is independent of ℓ. It turns out that

$$-\operatorname{ord}_{s=1} \zeta(\mathcal{X}, s) - \operatorname{ord}_{s=1} L(J_X, s) = 2 + \sum_v (f_v - 1),$$

so the rank conjecture is equivalent to the Tate conjecture.

A Delsarte surface

Tate's conjecture is known to hold for rational surfaces, abelian surfaces, elliptic K3 surfaces, and surfaces dominated by a product of nice curves.

Example (Ulmer)

Let X be as before. It defines a *Delsarte* surface $\mathcal{X} \subseteq \mathbb{P}^3_{[z:t:x:y]}$ given by

$$z^4y^2 - x^6 - zx^5 - z^5t = 0,$$

which is dominated by the *Fermat* surface $S \subseteq \mathbb{P}^3_{[y_0:y_1:y_2:y_3]}$ given by

$$y_0^2 + y_1^2 + y_2^2 + y_3^2 = 0,$$

by the rational map $S \to \mathcal{X}$ given by

$$[y_0 : y_1 : y_2 : y_3] \mapsto \left[\frac{y_2^{12}}{y_1^{10}} : y_3^2 : \frac{y_2^{10}}{y_1^8} : \frac{5y_0y_2^6}{y_1^5}\right].$$

In particular, the Tate conjecture holds for $\mathcal{X}$. Thus the rank conjecture, and hence the full Birch–Swinnerton-Dyer conjecture, holds for J_X.

Unbounded ranks

The previous examples generalise to families of hyperelliptic curves.

Theorem (Ulmer [3])

For any $g, p, r \in \mathbb{N}$ with p prime, there is a non-isotrivial geometrically irreducible hyperelliptic curves X of genus g over $\mathbb{F}_p(t)$ such that

$$\operatorname{ord}_{s=1} L(J_X, s) = \operatorname{rk}(J_X) \geq r.$$

For instance, X could be chosen to be

$$\begin{cases} y^2 + xy = x^{2g+1} + t^{p^n+1}x & \text{if } p = 2, \\ y^2 = x^{2g+1} + x^{2g} + tx & \text{if } 2 < p \mid (2g+1), \\ y^2 = x^{2g+2} + x^{2g+1} + tx & \text{if } 2 < p \mid (2g+2), \\ y^2 = x^{2g+2} + x^{2g+1} + t & \text{otherwise}, \end{cases}$$

in which case $r \geq (p^n + 1)/2n - c$ for some $c \in \mathbb{N}$ independent of n.

[3] Douglas Ulmer (2007) *L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields*