Characterizing algebraic curves using p-adic norms

Shuang-Yen Lee

1 Introduction

We know that a compact Riemann surface is determined by its Jacobian variety, known as the Torelli theorem. The Torelli theorem holds for curves over an arbitrary ground field k, this may be found in the appendix by J-P.Serre [1].

As a generalization of the Torelli theorem in higher differential forms, Royden proved in [2] that a Riemann surface can be determined by a norm $\|\cdot\|$ on the vector space quadratic differentials $H^0(X, K_X^{\otimes 2})$, where the norm is defined by

$$\|\alpha\| := \int_X |\alpha|.$$

I found out that the proof could be generalized to p-adic integral over a p-adic field and the estimation would be easier than the proof in [2]. However, a p-adic field is not algebraically closed, so there will be some argument on counting points that is different from the case over the complex numbers. Let K be a p-adic field and let $\mathcal{O}_K$ be the ring of integers. For a smooth projective curve X over $\mathcal{O}_K$, we define a norm $\|\cdot\|_K$ on the space of r-differential forms $V_K = H^0(X, K_X^{\otimes r})$ by

$$\|\alpha\|_K = \left(\int_{X(\mathcal{O}_K)} |\alpha|^{1/r}\right)^r.$$

The main result is

Theorem 1.1. Let X and X' be smooth projective curves over a $\mathcal{O}_K$ of genus $g \geq 3$, $r \geq 2$ a positive integer, V, V' the spaces $H^0(X, K_X^{\otimes r})$, $H^0(X', K_{X'}^{\otimes r})$, respectively. Let

$$\Phi : (V(K), \|\cdot\|_K) \to (V'(K), \|\cdot\|'_K)$$

be an isometry. Suppose that the residue field of K has more than $4g^2$ elements. Then there is an isomorphism $\varphi : X' \to X$ and some $u \in \mathcal{O}_K^\times$ such that $\Phi = u \cdot \varphi_K^*$.

2 p-adic norms

For a p-adic field K, let

- $\mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$ be the ring of integers,
- $\mathfrak{m}_K = \{x \in K \mid |x| < 1\} = (\pi_K)$ the maximal ideal of $\mathcal{O}_K$,
- $v : K^\times \to \mathbb{Z}$ the valuation on K, and
- $\mathbb{F}_q = \mathcal{O}_K/\mathfrak{m}_K$ the residue field.

Fix a positive integer r. Let X be a smooth projective curve over $\mathcal{O}_K$ requiring $X(K)$ to be nonempty, it follows from the valuative criterion for properness [4] that

$$X(\mathcal{O}_K) = X(K) \neq \varnothing.$$

We have defined a norm $\|\cdot\|_K$ on the space of differential r-forms $V_K = H^0(X, K_X^{\otimes r})$ by

$$\|\alpha\|_K = \left(\int_{X(\mathcal{O}_K)} |\alpha|^{1/r}\right)^r.$$

The following proposition gives some information about the "smoothness" of the normed space $(V_K, \|\cdot\|_K)$.

Proposition 2.1. Let α, $\beta \in V_K \setminus \{0\}$, $(\alpha)_0 = n_1P_1 + \cdots + n_\ell P_\ell$ the zero of α and let $N = \max\{n_1, \ldots, n_\ell\}$.

(i) We have

$$\|\alpha + t\beta\|_K - \|\alpha\|_K = O(|t|^{1/N+1/r}).$$

(ii) If $N = n_1 > n_i$ for all $i > 1$, then we can choose β so that $\|\alpha + t\beta\|_K - \|\alpha\|_K$ is not $O(|t|^\rho)$ for any

$$\rho > \frac{1}{N} + \frac{1}{r}.$$

Proof. If we define

$$\|\alpha\| = \int_X |\alpha|^{1/r},$$

note that

$$\|\alpha + t\beta\| - \|\alpha\| = O(|t|^\rho) \iff \|\alpha + t\beta\|_K - \|\alpha\|_K = O(|t|^\rho)$$

for any $\rho > 0$ since $\|\alpha\| > 0$. So it suffices to estimate

$$\|\alpha + t\beta\| - \|\alpha\|.$$

For a zero of α, say P, write

$$\alpha(u) = \big(a_n u^n + a_{n+1} u^{n+1} + \cdots\big)\, du^r, \ a_n \neq 0$$
$$\beta(u) = \big(b_m u^m + b_{m+1} u^{m+1} + \cdots\big)\, du^r, \ b_m \neq 0$$

locally in a neighborhood of P (with $P = 0$). Take ε small enough so that the expressions converge in $B_P(\varepsilon)$. Then we can take ε smaller so that

$$|a_n| > |a_{n+k} u^k|, \quad |b_m| > |b_{m+k} u^k|$$

for all $k \geq 1$ and $u \in B_P(\varepsilon)$ and that $B_P(\varepsilon)$ are pairwise disjoint for all zero P. Then we take t small enough so that $|\alpha + t\beta| = |\alpha|$ outside these P's neighborhoods. For $|t| \ll 1$, we get

$$\|\alpha + t\beta\| - \|\alpha\| = \int_X |\alpha + t\beta|^{1/r} - |\alpha|^{1/r} = \sum_i \int_{B_{P_i}(\varepsilon)} |\alpha + t\beta|^{1/r} - |\alpha|^{1/r}.$$

So for (i) and (ii) it suffices to show that

$$\int_{B_{P_i}(\varepsilon)} |\alpha + t\beta|^{1/r} - |\alpha|^{1/r} = O(|t|^{1/r + 1/n_i})$$

In $B_P(\varepsilon)$,

$$|\alpha(u)| = |a_n||u|^n\, du^r, \quad |\beta(u)| = |b_m||u|^m\, du^r.$$

If $m \geq n$, we get

$$|\alpha(u) + t\beta(u)|^{1/r} - |\alpha(u)|^{1/r} = 0 \quad \forall u \in B_P(\varepsilon)$$

for $|t| < |a_m|/|b_n|$. If $m < n$, let

$$\delta = \left(\frac{|t||b_m|}{|a_n|}\right)^{1/(n-m)},$$

we get

$$\frac{|(\alpha + t\beta)(u)|^{1/r} - |\alpha(u)|^{1/r}}{du} = \begin{cases} 0, & \text{if } |u| > \delta \\ ?, & \text{if } |u| = \delta \\ (|t||b_m||u|^m)^{1/r} - (|a_n||u|^n)^{1/r}, & \text{if } |u| < \delta. \end{cases}$$

Thus,

$$\int_{B_P(\varepsilon)} |\alpha + t\beta|^{1/r} - |\alpha|^{1/r} = \int_{|u|=\delta} |\alpha + t\beta|^{1/r} - |\alpha|^{1/r} + \int_{|u|<\delta} (|t||b_m||u|^m)^{1/r} - (|a_n||u|^n)^{1/r}\, du.$$

Let $q^{-(s+1)} < \delta \le q^{-s}$, we get

$$\begin{aligned} B &= \int_{|u|<\delta} (|t||b_m||u|^m)^{1/r} - (|a_n||u|^n)^{1/r}\, du \\ &= |t|^{1/r}|b_m|^{1/r}\frac{(q-1)q^{-(s+1)(1+m/r)}}{q-q^{-m/r}} - |a_n|^{1/r}\frac{(q-1)q^{-(s+1)(1+n/r)}}{q-q^{-n/r}}. \end{aligned}$$

We see that

$$\left(\frac{|t||b_m|}{|a_n|}\right)^{1/(n-m)} \le q^{-s} \le \left(\frac{|t||b_m|}{|a_n|}\right)^{1/(n-m)} \cdot q^{1-1/(n-m)},$$

so

$$B = O(|t|^{(1+n/r)/(n-m)})$$

and not $O(|t|^\rho)$ for $\rho > (1+n/r)/(n-m)$. In fact, when $n=1$, $m=0$,

$$B = \left(\frac{q^{1/r}-1}{q^{1+1/r}-1} \cdot \frac{|b_m|^{1+1/r}}{|a_n|}\right)|t|^{1+1/r},$$

and when $n > 1$,

$$B = (q-1)\left(\frac{(y/q)^{1+m/r}}{q-q^{-m/r}} - \frac{(y/q)^{1+n/r}}{q-q^{-n/r}}\right)\left(\frac{(|t||b_m|)^{(1+n/r)/(n-m)}}{|a_n|^{(1+m/r)/(n-m)}}\right),$$

where

$$y = q^{\left\{\frac{v(tb_m/a_n)}{n-m}\right\}} \in [1, q).$$

Note that $n > m$ implies that

$$\frac{1-q^{-(1+n/r)}}{1-q^{-(1+m/r)}} > 1 > \left(\frac{y}{q}\right)^{(n-m)/r} \implies \frac{(y/q)^{1+m/r}}{q-q^{-m/r}} - \frac{(y/q)^{1+n/r}}{q-q^{-n/r}} > 0.$$

It is much harder to compute

$$A = \int_{|u|=\delta} |\alpha(u) + t\beta(u)|^{1/r} - |\alpha(u)|^{1/r},$$

but it is obvious that $A = O(|t|^{(1+n/r)/(n-m)})$ by the same reason.

So we get

$$\int_{B_P(\varepsilon)} |\alpha + t\beta|^{1/2} - |\alpha|^{1/2} = A + B = O(|t|^{(1+n/r)/(n-m)}).$$

This proves (i). If $v(tb_m) \not\equiv v(a_n) \pmod{(n-m)}$, we have $A = 0$. When $n - m > 1$, this shows that

$$\int_{B_P(\varepsilon)} |\alpha + t\beta|^{1/2} - |\alpha|^{1/2} = A + B$$

is not $O(|t|^\rho)$ for any

$$\rho > \frac{1 + n/r}{n - m}$$

by taking t such that $v(tb_m) \not\equiv v(a_n) \pmod{(n-m)}$. Suppose that $N = n_1 > n_i$ for all $i > 1$, note that

$$\dim L(rK) = (r+1)(g-1) > (r+1)(g-1) - 1 = \dim L(rK - P_1)$$

for $r > 1$ and

$$\dim L(rK) = g > g - 1 = L(rK - P_1)$$

for $r = 1$ by Riemann-Roch theorem, so $L(rK - P_1) \subsetneqq L(rK)$. We simply take

$$\beta \in L(rK) \setminus L(rK - P_1)$$

so that $m = 0$ and get (ii). ■

Remark. We give an estimate of A when $v(tb_m) \equiv v(a_n) \pmod{(n-m)}$ requiring $n - m < p$. We know that on $|u| = \delta$,

$$\frac{|\alpha(u) + t\beta(u)|}{du^r} \leq \frac{|\alpha(u)|}{du^r}$$

and the inequality is strict if and only if

$$\begin{aligned} 0 \equiv \frac{\alpha(u) + t\beta(u)}{du^r} &\equiv a_n u^n + tb_m u^m \pmod{\mathfrak{m}_K^{v(tb_m\delta^m)+1}} \\ \Longleftrightarrow \left(\frac{u}{\pi_K^s}\right)^{(n-m)} &\equiv x := -\frac{tb_m}{a_n}\pi^{-s(n-m)} \pmod{\mathfrak{m}_K}. \end{aligned}$$

Since $n - m < p$, by Hensel's lemma, for each $z \in \mathfrak{m}_K$ there exists a unique $|u| = \delta$ such that

$$\left(\frac{u}{\pi_K^s}\right)^{(n-m)} = x + z = z - \frac{tb_m}{a_n}\pi^{-s(n-m)} \Longleftrightarrow a_n u^n + tb_m u^m = z a_n \pi^{s(n-m)}.$$

Let $U = \#\{u_0 \in \mathbb{F}_q \mid u_0^{n-m} = x\}$, we get

$$\begin{aligned} A &= U \cdot \frac{\delta}{q} \cdot |a_n|^{1/r} \delta^{n/r} \left[(1-q^{-1})(q^{-1/r}-1) + (q^{-1}-q^{-2})(q^{-2/r}-1) + \cdots \right. \\ &\quad \left. + O\left(\max_{k\geq 1} \max \left\{ \left| \frac{a_{n+k}}{a_n} \right|, \left| \frac{b_{m+k}}{b_m} \right| \right\} \delta^k \right) \right] \\ &= U|a_n|^{1/2} \delta^{1+n/2} \left(\frac{1-q^{1/r}}{q^{1+1/r}-1} \right) (1+O(\delta)), \\ &= U \left(\frac{1-q^{1/r}}{q^{1+1/r}-1} \right) (1+O(|t|^{1/(n-m)})) \left(\frac{(|t||b_m|)^{(1+n/r)/(n-m)}}{|a_n|^{(1+m/r)/(n-m)}} \right). \end{aligned}$$

If $n = 1$, we get $U = 1$, so

$$A + B = O(|t|^{2+1/r}).$$

When $N = 1$, this gives a sharper estimate

$$\|\alpha + t\beta\|_K - \|\alpha\|_K = O(|t|^{2+1/r}).$$

3 Dual r-canonical curve

Let X be a curve over $\overline{\mathbb{Q}}_p$ of genus $g \geq 3$, $V = H^0(X, K_X^{\otimes r})$. We have the r-canonical embedding

$$\phi = |rK| : X \to \mathbb{P}(V)^\vee$$

when $r \geq 2$ or X non-hyperelliptic. We define the dual r-canonical map

$$\psi : X \to \mathbb{P}(V)$$

by sending $P \in X$ to the osculating hyperplane $H_P \in \mathbb{P}(V)$ of $\phi(X)$ at $\phi(P)$. Explicitly, write $V = \langle \alpha_1, \ldots, \alpha_m \rangle_{\overline{\mathbb{Q}}_p}$, where

$$m = \dim V = \begin{cases} (r+1)(g-1), & \text{if } r > 1 \\ g, & \text{if } r = 1, \end{cases}$$

we get

$$\phi(P) = [\alpha_1(P) : \cdots : \alpha_m(P)].$$

The osculating hyperplane H_P is

$$\left[\langle \phi(P), \phi'(P), \ldots, \phi^{(k)}(P) \rangle_{\overline{\mathbb{Q}}_p} \right] = \ker \begin{pmatrix} \alpha_1(P) & \cdots & \alpha_m(P) \\ \vdots & \ddots & \vdots \\ \alpha_1^{(k)}(P) & \cdots & \alpha_m^{(k)}(P) \end{pmatrix} \in \mathbb{P}(V)$$

for some k. If we take α so that $\mathrm{ord}_P(\alpha)$ is maximal (which is unique up to a scalar, otherwise $h^0(rK - (\mathrm{ord}_P(\alpha)+1)P) \geq 2-1=1$), then $\alpha(P) = \cdots = \alpha^{(k)}(P) = 0$ and hence we get $H_P = [\alpha]$. Since

$$h^0(rK - (m-1)P) \geq m - (m-1) = 1,$$

we have $\mathrm{ord}_P(\alpha) \geq m-1$. If $r > 1$, it follows from

$$2(m-1) > r(2g-2) = \deg rK_X \iff g > 2$$

that ψ is injective. If $r = 1$ and $\psi(P) = \psi(Q)$ with P, Q distinct, then

$$K_X = (g-1)P + (g-1)Q,$$

so ψ is either a generically injecitve map or a $2-1$ map. If ψ is $2-1$, then for generic $P \in X$, there's another point $Q \in X$ such that

$$K_X = (g-1)P + (g-1)Q.$$

Theorem 3.1. Let X be an algebraic curve over a characteristic 0 field of genus g, and let Q be a g^r_d on X, i.e., a linear system on X of degree d, with $r = \dim Q$. Then

$$\sum_{P\in X} w_P(Q) = (r+1)(d+rg-r),$$

where

$$w_P(Q) = \sum_{i=1}^{r+1}(n_i - i),$$

and $n_1 < n_2 < \cdots < n_{r+1}$ denote the gap numbers. In particular, there are only finitely many $P \in X$ such that $Q(-(r+1)P) \neq \varnothing$.

The proof of the theorem may be found in [3]. Apply the this to the case $Q = |rK_X| = g^{m-1}_{r(2g-2)}$, we see that $|2K - dP| = \varnothing$ and hence $\mathrm{ord}_P(\psi(P)) = m-1$ for generic $P \in X$. We call P an r-Weierstrass point if $\mathrm{ord}_P(\psi(P)) \geq m$. Let

$$W = \{P \in X \mid \mathrm{ord}_P(\psi(P)) \geq m\}$$

be the set of r-Weierstrass points. For $P \in W$, let

$$L_P = \{[\alpha] \in \mathbb{P}(V) \mid \mathrm{ord}_P(\alpha) \geq m-1\},$$

then $\psi(P) \in L_P$.

Lemma 3.2. The dual r-canonical curve $\psi(X)$ is not contained in any hyperplane of P.

Proof. Let H be a hyperplane of $\mathbb{P}(V)$, then H is a $g^{m-2}_{r(2g-2)}$. Then (3.1) shows that there are only a finite number of points of X at which there is an $[\alpha] \in H$ with a zero of order at least $m-1$. Thus the dual r-canonical curve is not contained in H. ∎

4 Proof of the main result

Let

$$S = \{[\alpha] \in \mathbb{P}(V) \mid \exists P \in X \text{ s.t. } \operatorname{ord}_P(\alpha) \geq m-1\} \subseteq \mathbb{P}(V),$$

then it is clear that

$$S = \psi(X) \cup \bigcup_{P \in W} L_P.$$

Define $\theta : S \to X$ by sending $\alpha \in S$ to the unique point $P \in X$ such that $\operatorname{ord}_P(\alpha) \geq m-1$. Then $\theta \circ \psi = \mathrm{id}_X$ and $\theta^{-1}(P)$ is always a linear space (of dimension ≥ 1 if and only if $P \in W$).

From (2.1) we see that the set $S(K)$ is the set of those $[\alpha]$ for which there is $\beta \in V_K$ so that

$$\|\alpha + t\beta\|_K - \|\alpha\|_K$$

is not $O(|t|^\rho)$ for any $\rho > \frac{1}{2} + \frac{1}{m-1}$.

Proposition 4.1. Let X and X' be smooth projective curves over $\mathcal{O}_K$ of genus $g \geq 3$, r a positive integer, V, V' the spaces $H^0(X, K_X^{\otimes r})$, $H^0(X', K_{X'}^{\otimes r})$, respectively, and let

$$\Phi : (V(K), \|\cdot\|_K) \to (V'(K), \|\cdot\|'_K)$$

be an isometry. Suppose that $q > 4g^2$ and ψ, ψ' are injective (which is always true for $r \geq 2$). Then there is an isomorphism $\varphi_K : X'_K \to X_K$ and some $u \in \mathcal{O}_K^\times$ such that $\Phi = u \cdot \varphi_K^*$.

Proof. From $q > 4g^2$ we get $q + 1 > 2g\sqrt{q}$. It follows from the Riemann hypothesis for curves [4] that $X(\mathbb{F}_q)$ are nonempty. Consider the mod $\mathfrak{m}_K$-reduction

$$h : X(\mathcal{O}_K) \to X(\mathbb{F}_q).$$

For any $\overline{x} \in X(\mathbb{F}_q)$, the preimage $h^{-1}(\overline{x})$ of $\overline{x}$ in $X(\mathcal{O}_K)$ is isomorphic to $\mathfrak{m}$ in K-analytic sense, hence $X(K) = X(\mathcal{O}_K)$ (by the valuative criterion for properness) contains infinitely many points. Similarly, $X'(K)$ contains infinitely many points.

Since Φ is an isometry, $S(K)$ sends to $S'(K)$ under the linear map $\overline{\Phi} : \mathbb{P}(V(K)) \xrightarrow{\sim} \mathbb{P}(V'(K))$. Extend $\overline{\Phi}$ to $\overline{\Phi}_{\overline{\mathbb{Q}}_p} : \mathbb{P}(V) \xrightarrow{\sim} \mathbb{P}(V')$, we may assume that S, S' are contained in the same projective space $\mathbb{P}^{3g-4}$ and we have

$$C(K) \cup \bigcup_{P \in W} L_P(K) = S(K) = S'(K) = C'(K) \cup \bigcup_{P' \in W'} L_{P'}(K),$$

where $C = \psi(X)$, $C' = \psi'(X')$. By (3.2),

$$|C' \cap L_P| < \infty \implies |C'(K) \cap L_P(K)| < \infty.$$

Then $|X'(K)| = \infty$ gives $|C(K) \cap C'(K)| = \infty$ and hence $|C \cap C'| = \infty$, thus $C = C'$ since they are both irreducible. Therefore,

$$\varphi_{\overline{\mathbb{Q}}_p} = \theta \circ \overline{\Phi}_{\overline{\mathbb{Q}}_p}^{-1} \circ \psi' : X'_{\overline{\mathbb{Q}}_p} \to X_{\overline{\mathbb{Q}}_p}$$

is an isomorphism. Since $\varphi_{\overline{\mathbb{Q}}_p}$ is defined over K, we get an isomorphism $\varphi_K : X'_K \to X_K$. Since $\overline{\Phi} = \overline{\varphi}_K^*$, we get $\Phi = u \cdot \varphi_K^*$ for some $u \in K$. Then $|u| = 1$ since both Φ and φ_K^* are isometries. ■

Using the following theorem, stated in [5], we can prove that the isomorphism $\varphi_K : X'_K \to X_K$ lifts to an isomorphism $\varphi : X' \to X$. This is also an arithmetic version of the theorem stated in [6].

Theorem 4.2. Let $(R, \mathfrak{m})$ be a discrete valuation ring with the quotient field K; let V and W be smooth projective varieties, defined over K, and T the graph of an isomorphism, defined over K, between V and W. Let X (resp. Y) be an ample divisor on V (resp. W), both rational over K, such that $Y = T(X)$. Let

$$(V, W, X, Y, T) \to (V', W', X', Y', T')$$

be the mod $\mathfrak{m}$-reduction and assume that V', W' are smooth and that X' (resp. Y') is also ample on V' (resp. W'). Then T' is the graph of an isomorphism between V' and W', if one of the V', W' is not ruled.

5 Future work

The proof above only works for $g \geq 3$ and $q > 4g^2$. For $g = 2$, the dual r-canonical would be a $\mathbb{P}^1$ with 6 Weierstrass point on it. Since K is not algebraically closed, the Weierstrass points may not be K-rational. A way to solve this is to take an extension $K \subset L$, so that the Weierstrass points are L-rational and try to compare the norms $\|\cdot\|_K$ and $\|\cdot\|_L$. If we can compare the norms $\|\cdot\|_K$ and $\|\cdot\|_L$, we can also take an extension so that the condition $q > 4g^2$ is satisfied.

Acknowledgement

This is an undergraduate thesis, which is supervised by professor Chin-Lung Wang.

References

[1] K. Lauter, and J-P. Serre. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. Journal of Algebraic Geometry 10 (2001), 19-36. `arXiv:math/0104247 [math.AG]`

[2] H. L. Royden, Automorphisms and Isometries of Teichmilller Space. Advances in the Theory of Riemann Surfaces. (AM-66), Volume 66.

[3] R. Miranda. Algebraic curves and Riemann surfaces, 1995.

[4] R. Hartshorne. Algebraic geometry, 1977.

[5] Matsusaka, T., and David Bryant Mumford. 1964. Two fundamental theorems on deformations of polarized varieties. American Journal of Mathematics 86(3): 668-684.

[6] C. L. Wang. Cohomology Theory in Birational Geometry. J. Differential Geom. 60(2): 345-354 (February, 2002). DOI: 10.4310/jdg/1090351105