Arithmetic of hyperelliptic curves over local fields

T. Dokchitser, V. Dokchitser, C. Maistret, A. Morgan

University of Bristol/King's College London

September 5, 2017

Setup

$p \neq 2$ prime;

$K/\mathbb{Q}_p$ finite extension;

C/K a hyperelliptic curve of genus g,

$$C : \qquad y^2 = f(x) \qquad = c \prod_{r \in R} (x - r).$$

For purposes of the presentation assume that

- $deg(f) = 2g + 1$ or $2g + 2 \quad \neq 1, 2, 4$
- $f(x) \in \mathcal{O}_K[x]$, $c \in \mathcal{O}_K^\times$ and $f(x) \bmod \pi_K$ is not of the form $(x - z)^n$, $\quad (x - z_1)^n (x - z_2)^m$, $\quad (x - z_1)(x - z_2)(x - z_3)^n$ or $h(x)^2$.

Cluster

A *cluster* $\mathfrak{s}$ is a non-empty subset of R cut out by a p-adic disc:

$$\mathfrak{s} = R \cap Disc(z_{\mathfrak{s}}, d) = \{r \in R \mid v(r - z_{\mathfrak{s}}) \geq d\}, \qquad \text{for some } z_{\mathfrak{s}} \in \overline{\mathbb{Q}}_p, d \in \mathbb{Q}.$$

Depth

The *depth* of $\mathfrak{s}$ is

$$d_{\mathfrak{s}} = \min_{r,r' \in \mathfrak{s}} v(r - r')$$

child/parent

If $\mathfrak{s}' \subsetneq \mathfrak{s}$ is a maximal subcluster, we call $\mathfrak{s}'$ the *child* of $\mathfrak{s}$ and $\mathfrak{s}$ the *parent* of $\mathfrak{s}'$.

$\mathfrak{s}_{odd}$

For a cluster $\mathfrak{s}$ we write $\mathfrak{s}_{odd}$ for the set of its children that have odd size.

Theorem (Semistability criterion)

The curve C/K is semistable if and only if the following hold:

(i) $K(R)/K$ has ramification degree at most 2,

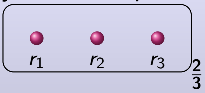
(ii) Every cluster of size ≥ 2 is inertia invariant,

(iii) Every cluster $\mathfrak{s}$ of size ≥ 3 has $d_{\mathfrak{s}} \in \mathbb{Z}$ and

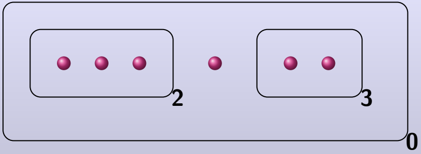
$$\nu_{\mathfrak{s}} = |\mathfrak{s}| d_{\mathfrak{s}} + \sum_{r \notin \mathfrak{s}} v(r_0 - r) \in 2\mathbb{Z} \qquad \text{for any } r_0 \in \mathfrak{s}.$$

Example ($p \neq 3$)

$$y^2 = x^3 - p^2$$



$$y^2 = (x-1)(x-1+p^2)(x-1-p^2) \cdot (x-2) \cdot x(x-p^3)$$



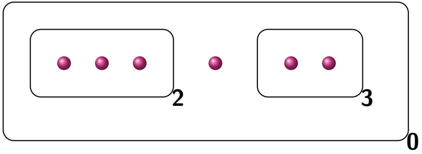
$$\nu_R = 6 \times 0 + 0 \in 2\mathbb{Z}$$
$$\nu_{\mathfrak{s}} = 3 \times 2 + 3 \times 0 \in 2\mathbb{Z}$$

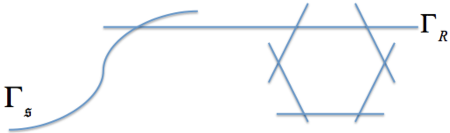
Theorem(Special fiber of the minimal regular model $\overline{C}_{min}$)

Suppose that C/K is semistable. Then $\overline{C}_{min}$ is given by

- an (explicit) curve $\Gamma_{\mathfrak{s}}$ for each cluster $\mathfrak{s}$ of size ≥ 3;
  genus $g_{\mathfrak{s}}$ where $|\mathfrak{s}_{odd}| = 2g_{\mathfrak{s}}+1$ or $2g_{\mathfrak{s}}+2$;
  $\Gamma_{\mathfrak{s}}$ is a union of two $\mathbb{P}^1$s if $\mathfrak{s}_{odd}$ is empty;
- $\mathfrak{t}$ child of $\mathfrak{s}$ with $|\mathfrak{t}| \geq 3$ odd — a chain of $\mathbb{P}^1$s from $\Gamma_{\mathfrak{s}}$ to $\Gamma_{\mathfrak{t}}$ of length $\frac{d_{\mathfrak{t}}-d_{\mathfrak{s}}}{2}-1$,
- $\mathfrak{t}$ child of $\mathfrak{s}$ with $|\mathfrak{t}| \geq 3$ even — two chains of $\mathbb{P}^1$s from $\Gamma_{\mathfrak{s}}$ to $\Gamma_{\mathfrak{t}}$ of length $d_{\mathfrak{t}}-d_{\mathfrak{s}}-1$,
- $\mathfrak{t}$ child of $\mathfrak{s}$ with $|\mathfrak{t}| = 2$ — a chain of $\mathbb{P}^1$s from $\Gamma_{\mathfrak{s}}$ to itself of length $2(d_{\mathfrak{t}}-d_{\mathfrak{s}})-1$.

Example: $C : y^2=(x-1)(x-1+p^2)(x-1-p^2)\cdot(x-2)\cdot x(x-p^3)$





Consequences for semistable C/K

- The homology of the dual graph Υ_C of $\overline{C}_{min}$ is

$$H_1(\Upsilon_C, \mathbb{Z}) = \mathbb{Z}^{|A|},$$

where A is the set of clusters $\mathfrak{s} \neq R$ with $|\mathfrak{s}|$ even and $|\mathfrak{s}_{odd}| \geq 1$. Frobenius acts as an (explicit) signed permutation, and there is an explicit formula for the intersection pairing.

- A formula for the Tamagawa number of the Jacobian (A. Betts).

- A criterion for whether $C(K) = \emptyset$ for p sufficiently large.

- A criterion for whether $C(K)$ is deficient.

Theorem: ℓ-adic representation for $\ell \neq p$

As I_K-representations

$$H^1_{\acute{e}t}(C/\overline{K}, \mathbb{Q}_\ell) \quad \cong \quad H^1_{ab} \oplus (H^1_t \otimes Sp(2)), \qquad \text{with}$$

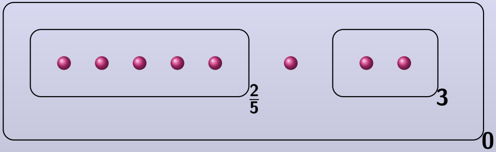
$$H^1_{ab} = \bigoplus_{\mathfrak{s}:\ |\mathfrak{s}|\geq 3,\ |\mathfrak{s}_{odd}|\geq 1} \mathrm{Ind}^{I_K}_{\mathrm{Stab}(\mathfrak{s})} V_\mathfrak{s}, \qquad H^1_t = \bigoplus_{\mathfrak{s}\neq R:\ |\mathfrak{s}|\ \text{even},\ |\mathfrak{s}_{odd}|\geq 1} \mathrm{Ind}^{I_K}_{\mathrm{Stab}(\mathfrak{s})} \epsilon_\mathfrak{s},$$

where $V_\mathfrak{s} = (\mathbb{Q}_\ell[\mathfrak{s}_{odd}] \ominus \mathbf{1} \ominus \epsilon_\mathfrak{s}) \otimes \gamma_\mathfrak{s}$ and $\epsilon_\mathfrak{s}, \gamma_\mathfrak{s}$ are explicit characters (or 0) of $\mathrm{Stab}_{I_K}(\mathfrak{s})$.

Curve and Clusters | Frobenius | Inertia

Let $p = 17, \qquad a = \sqrt{-p}$,

$C : y^2 = (x^5 - p^2)(x-2)(x-1)(x-1-p^3)$



Frobenius:

$$\begin{pmatrix} a & 0 & 0 & -a & & \\ 0 & 0 & a & -a & & \\ 0 & 0 & 0 & -a & & \\ 0 & a & 0 & -a & & \\ & & & & 1 & 0 \\ & & & & 0 & p \end{pmatrix}$$

Inertia:

$$\begin{pmatrix} 0 & 0 & 0 & -1 & & \\ 1 & 0 & 0 & -1 & & \\ 0 & 1 & 0 & -1 & & \\ 0 & 0 & 1 & -1 & & \\ & & & & 1 & * \\ & & & & 0 & 1 \end{pmatrix}$$

Consequences for the Jacobian $\mathrm{Jac}(C)/K$

• $\mathrm{Jac}(C)$ has potentially good reduction if and only if all clusters $\mathfrak{s} \neq R$ have odd size.

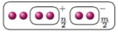
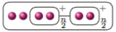
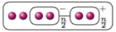
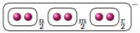
• The potential toric dimension of $\mathrm{Jac}(C)$ is the number of clusters $\mathfrak{s} \neq R$ of even size that have an odd-size child.

• A formula for the conductor.

• A formula for the local root number if the inertia action on the roots is tame (M. Bisatt).

Classification of semistable curves of genus 2 (23 types)

- Reduction type
- Cluster picture
- Dual graph of special fiber
- Monodromy pairing
- Frobenius action on dual graph
- Local Root number
- Tamagawa Number
- Deficiency

Type	C	n_v	c_v	deficient	w_v
2		0	1	✗	1
1_n^+		1	n	✗	-1
1_n^-		1	n^*	✗	1
$I_{n,m}^{+,+}$		2	nm	✗	1
$I_{n,m}^{+,-}$		2	nm^*	✗	-1
$I_{n,m}^{-,-}$		2	n^*m^*	✗	1
$I_{n\text{-}n}^{+}$		2	n	✗	-1
$I_{n\text{-}n}^{-}$		2	n^*	✗	1
$U_{n,m,r}^{+}$		2	$nm+nr+mr$	✗	1
$U_{n,m,r}^{-}$		2	$\left(\frac{nm+nr+mr}{gcd(n,m,r)}\right)^* \cdot gcd(n,m,r)^*$	$\begin{cases} ✓ & n,m,r \text{ odd} \\ ✗ & \text{else} \end{cases}$	1

Thank you!