LOCAL SOLUBILITY OF HYPERELLIPTIC CURVES

OMRI FARAGGI

Abstract. We give a condition for a hyperelliptic curve $C$ over a local field $K$ to be locally soluble, on the condition that $C$ obtains semistable reduction after a tame extension of $K$, and that the residue field $k$ is sufficiently large relative to the genus of the curve. The condition is presented in terms of the cluster picture of $C$, a combinatorial object which determines much of the local arithmetic of $C$.

Table of contents

1. Introduction 1
2. The Condition 2
3. Examples 4
Appendix A. Cluster Pictures 4
References 5

1. Introduction

Let $C : y^2 = f(x)$ be a hyperelliptic curve of genus $g \geq 2$ over a local field $K$ with residue $k$ of characteristic $p > 2$. In this note we give a condition for $C$ to have a $K$-rational point in terms of the cluster picture of $C$, given that $C$ has tame reduction — in other words, it obtains semistable reduction after a tame extension of $K$. The cluster picture $\Sigma$ of $C$ is a combinatorial object which contains the data of the $p$-adic distances between the roots of the defining polynomial $f$. This removes dependency on the exact nature of $f$, and cluster pictures have been used used to calculate the Galois representation, semistable model, conductor and minimal discriminant of $C$ in [6], the minimal snc model if $C$ has tame reduction in [7], the Tamagawa number in [2], the root number in [4] and finally differentials in [8] and [10]. A survey article is available at [1]. Since our condition is in terms of the cluster picture of $C$, it allows us to determine whether families of hyperelliptic curves are locally soluble, rather than having to consider individual curves. With some additional work, this should allow us to determine what proportion of hyperelliptic curves of a given genus are locally soluble. This follows on from work such as [3] and [5].

Throughout the note the hyperelliptic curve $C$ will always be defined by an equation $y^2 = f(x)$ and $\mathcal{R}$ will denote the set of roots of $f$. In particular, it cannot be a degree 2 cover of a $\mathbb{P}^1$ with no point. The absolute Galois group $G_K = \text{Gal}(\overline{K}/K)$ acts on the roots of $\mathcal{R}$ and hence there is an induced action on the cluster picture of $C$.

Date: February 2021.
Here we state the main result of this note. A knowledge of cluster pictures is required, and so a brief exposition for the uninitiated is available in Appendix A for more details the reader is encouraged to turn to [3] or [1].

Lemma 2.1. Let \( C : y^2 = f(x) \) be a hyperelliptic curve with tame reduction over a local field \( K \) and let \( \mathcal{X} \) be a regular snc model of \( C \). Suppose that the residue field of \( K \) has size \( q > 2(g(C)^2 - 1) \). Then any smooth component \( \Gamma \) of the special fibre which is fixed by Frobenius has a smooth \( k \)-rational point.

Proof. Assume \( f \) has odd degree, since the even case is dealt with similarly. Note that any smooth component fixed by Frobenius must be defined over \( k \). The Hasse-Weil bound then states that \(|\# \Gamma(k) - (q + 1)| \leq 2g(\Gamma)\sqrt{q} \), and hence \( \Gamma(k) \) is non-empty if \( q > 2(g(\Gamma)^2 - 1) \). Since \( g(\Gamma) \leq g(C) \), we are done if \( C \) is a smooth model.

Now assume \( C \) is a semistable model. If \( \Gamma \) is genus 0 then it has \( k \)-points, so assume it has positive genus and comes from a principal cluster \( s \). Let \( I \) be the number of intersection points of other components. Then \( \Gamma \) has a smooth \( k \)-rational point if \( q - I > 2(g(\Gamma)^2 - 1) \), and hence it has a smooth \( k \)-point if \( 2g(C)^2 - I > 2g(\Gamma)^2 \). Suppose \( s = R \) is odd, and that \( s \) has \( s_e \) children of size 1, \( s_o \) proper odd children and \( s_e \) proper even children. Then by [6] Theorem 8.5, \( I = s_e + 2s_o \) and \( 2g(C) + 1 = s_o + s_e \). We also know that \( 2g(C) + 1 = \deg(f) \geq s_o + 3s_e \). Putting these together the result follows, and similarly if \( s \) is even or \( s \neq R \).

Now assume \( C \) has tame reduction. A similar argument works using [1] Theorem 7.12,7.18], noting that since \( G \) is a smooth component it has \( e_s = 1 \) and its only intersection points are loops or linking chains to other principal components.

Proposition 2.2. Let \( X \) be a curve over a local field \( K \) and let \( \mathcal{X} \) be a regular snc model of \( X \). Then \( X \) has a \( K \)-rational point if and only if \( \mathcal{X}_k \) has a component of multiplicity 1 which is fixed by Frobenius and has a smooth \( k \)-rational point.

Proof. By [3] Corollary 9.1.32] there is a reduction map red : \( X(K) \rightarrow \mathcal{X}_k(k) \) landing in the smooth locus of \( \mathcal{X}_k \), which is onto since \( K \) is henselian. Therefore \( X(K) \) is empty if and only if the smooth locus of \( \mathcal{X}_k(k) \) is empty. Since the smooth locus of \( \mathcal{X}_k(k) \) consists of points lying on components of multiplicity 1 which are fixed by Frobenius, the result follows.

Theorem 2.3. Let \( C \) be a hyperelliptic curve with tame reduction over a local field \( K \) and let \( C \) be the minimal snc model of \( C \). If \( R \) is principal, then \( C_k \) has a component of multiplicity 1 fixed by Frobenius precisely if at least one of the follow occurs:

(i) there is a principal cluster \( s \) fixed by \( G_K \) with \( e_s = 1 \), and if in addition \( s \) is übereven, the character \( \epsilon_s \) is trivial on \( G_K \);
(ii) there is a principal cluster \( s \) fixed by \( G_K \) (and \( \epsilon_s \) trivial if \( s \) übereven) with \( e_s > 1 \) and at least one of the following:
   (a) \( s = R \) and either \( R \) is odd or \( R \) is even and \( \epsilon_R \) is the trivial character,
   (b) \( s \) has a stable child of size 1 or \( g(s) = 0 \), \( s \) is not übereven and \( s \) has no proper stable odd child,
   (c) \( s \) has no stable proper child, \( \lambda_s \in \mathbb{Z} \), \( v_K(e_s) \) is even and either \( g(s) > 0 \) or \( s \) is übereven,
   (d) the children of size 1 of \( s \) are fixed by \( G_K \);
(iii) there is a pair of principal clusters \( s' < s \), both fixed by \( G_K \), either with \( s' \) odd and \( [-r_s - \delta_s/2, -\lambda_s] \cap \mathbb{Z} \not= \emptyset \), or \( s' \) even, the character \( \epsilon_{s'} \) trivial on \( G_K \) and \( [-d_{s'}, -d_s] \cap \mathbb{Z} \not= \emptyset \);
(iv) there is a twin \( t \) fixed by \( G_K \) and either:
   (a) the character \( \epsilon_t \) is trivial and \( [-d_t, -d_{P(t)}] \cap \mathbb{Z} \not= \emptyset \),
   (b) the character \( \epsilon_t \) is trivial on inertia, \( \epsilon_t(Frob) = -1 \), \( d_t \in \mathbb{Z} \) and \( v_t \in 2\mathbb{Z} \) or,
   (c) the character \( \epsilon_t \) is non-trivial on inertia and \( v_K(e_t) \) even;
If \( R \) is not principal, then \( C \) has a component of multiplicity 1 fixed by Frobenius in the cases above, and the additional following cases:

(v) there is a c-twin \( s < t \) fixed by \( G_K \) and either:
(a) the character \( \epsilon_1 \) is trivial and \([-d_s, -d_t] \cap \mathbb{Z} \neq \emptyset \),
(b) the character \( \epsilon_1 \) is trivial on inertia, \( \epsilon_1(Frob) = -1 \), \( d_t \in \mathbb{Z} \) and \( \nu_t \in 2\mathbb{Z} \) or,
(c) the character \( \epsilon_1 \) is non-trivial on inertia and trivial on Frobenius;
(vi) the top cluster \( R = s_1 \sqcup s_2 \) is not principal and either:
(a) \( s_1 \) is odd, fixed by \( G_K \) and \([-\lambda_R - \delta_{s_1}/2, -\lambda_R] \cap \mathbb{Z} \neq \emptyset \),
(b) \( s_1 \) is odd, fixed by inertia but not Frobenius and \( d_R \in \mathbb{Z} \),
(c) \( s_1 \) is odd, inertia swaps \( s_1 \) and \( s_2 \) and \( \epsilon_R(Frob) = 1 \),
(d) \( s_1 \) is even, fixed by \( G_K \), \( \epsilon_{s_1} \) is trivial and \([-d_{s_1}, -d_R] \cap \mathbb{Z} \neq \emptyset \),
(e) \( s_1 \) is even, fixed by inertia but not Frobenius, \( \epsilon_{s_1} \) is trivial and \( d_R \in \mathbb{Z} \),
(f) \( s_1 \) is even, inertia swaps \( s_1 \) and \( s_2 \), \( \epsilon_{s_1} \) is trivial and \( \epsilon_R(Frob) = 1 \).

Proof. For brevity, call components of multiplicity 1 which are fixed by Frobenius good. If \( C \) has a good component, it must either by a principal component of part of a chain of rational curves. We investigate these cases separately, beginning with principal components. The principal components are parametrised by principal clusters \(^1\) and by [7, Theorem 7.12] a good component must come from a principal cluster \( s \) fixed by \( G_K \). In addition, \( s \) must have \( e_s = 1 \), i.e. \( d_s \in \mathbb{Z} \) and \( \nu_s \in 2\mathbb{Z} \), and if \( s \) is even, the character \( \epsilon_s \) must be trivial. In all these cases we do indeed have a good component. This is case (i).

We are left to find the cases where there is a good component in a chain of rational curves. Chains of rational curves appear in several flavours: linking chains between principal components, loops (including the crosses of crossed tails). A principal cluster \( s \) fixed by Galois with \( e_s > 1 \) contributes tails to the special fibre. If \( s = R \) then the \( \infty \)-tails will have a good component if \( R \) is odd or if \( R \) is even and the character \( \epsilon_R \) is trivial by the first three rows of the first table in [7, Theorem 7.18], noting that \( \epsilon_R(Frob) \) swaps the \( \infty \)-tails if and only if it is \(-1 \) by Theorem [7, Theorem 7.21]. If \( s \) is a general principal cluster then a \((0, 0)\)-tail exists if (ii)(b) is satisfied and it will always have a good component An \((s_s = 0)\)-tail will have a good component so long as \( \lambda_s \in \mathbb{Z} \) and \( v_K(e_s) \) is even — the former ensures that there are two \((x_s = 0)\)-tails by Theorem [7, Theorem 7.18] and the latter that they are fixed by Frobenius, by [7, Theorem 7.21]. A \((y_s = 0)\)-tail will have a good component if and only if the singletons of \( s \) are fixed by Galois. This is case (ii).

Suppose \( L \) is a linking chain arising from a pair of orbits \( X' < X \). By [7, Theorem 7.18], the lowest common multiple of multiplicities of the components of \( L \) is \(|X'|\), so \( X = s, X' = s' \) must be clusters fixed by Galois. If \( s' \) is odd then \( L \) has a good component if and only if \([-\lambda_s - \delta_{s'}/2, -\lambda_s] \cap \mathbb{Z} \neq \emptyset \). If \( s' \) is even then \( L \) has a good component if and only if \( \epsilon_{s'} \) is trivial and \([-d_{s'}, -d_s] \cap \mathbb{Z} \neq \emptyset \). This is because \( \sigma \in G_K \) swaps the two linking chains connecting \( \Gamma_{s, L} \) and \( \Gamma_{s', L} \) if and only if \( \epsilon_{s'}(\sigma) = -1 \) (This is case (iii)).

Now suppose \( L \) is a loop arising from an orbit of twins. By the same argument as above, this must in fact arise from a twin \( t \) fixed by Galois with \( e_t \) trivial on inertia. If \( e_t \) is further trivial on Frobenius then \( L \) will have a good component if and only if it has a component of multiplicity 1, which occurs precisely when \([-d_t, -d_{P(t)}] \cap \mathbb{Z} \neq \emptyset \). If \( e_t(Frob) = -1 \) then Frobenius inverts the loop, but there can still be a component fixed by Frobenius if \( L \) is a loop of odd length. This happens precisely when \( d_t \) is an integer.

If \( T \) is instead a crossed tail, it must arise from a twin \( t \) fixed by Galois with \( e_t \) non-trivial on inertia. In this case, the crosses of \( T \) have multiplicity 1, and by they are fixed by Frobenius if and only if \( v_K(e_t) \) is even. This and the previous paragraph is case (iv).

Cases (v) and (vi), where \( R \) is a non-principal cluster, are dealt with similarly. 

\(^1\)Except in crossed tails but these always have even multiplicity.
Corollary 2.4. Let $C$ be a hyperelliptic curve with tame reduction over a local field $K$ with residue field $k$ of characteristic $p > 2$. Suppose that $|k| = q$ is such that $q > 2(g(C)^2 - 1)$. Then $C$ has a $K$-rational point in precisely the cases described in Theorem 2.3.

Proof. By Lemma 2.1 any smooth components of the special fibre fixed by Frobenius have a $k$-point. By Theorem 2.3, a smooth component fixed by Frobenius exists and hence by Proposition 2.4, $C$ has a $K$-rational point.

\[ \Box \]

3. Examples

We give some examples to illustrate our theorem. All curves are over $\mathbb{Q}_p$, with $p$ sufficiently large so that all multiplicity 1 components of the special fibre which are fixed by Frobenius have points.

Example 3.1. Let $C : y^2 = (x^4 - p^{17})(x^3 - p^2)$. We immediately observe that $\mathcal{R}$ is principal, odd and $\epsilon_\mathcal{R} > 1$, so $C$ must have a $K$-rational point by condition (ii)(a).

Example 3.2. Let $C : y^2 = p((x - 1)^2 + p^2)((x - \zeta_3)^2 + p^2)((x - \zeta_3^2)^2 + p^2)$, with $p \equiv -1 \mod 3$ and $\zeta_3$ a fixed cubic root of unity. The cluster picture of $C$ is shown in Figure 1. There is a unique principal cluster $\mathcal{R}$, which is übereven. However, $\epsilon_\mathcal{R} = 2$ and $\epsilon_\mathcal{R}(\sigma) = (−1)_{\mathcal{R}}\epsilon_\mathcal{R}(\sigma) = -1$ for $\sigma$ a generator of $\text{Gal}(\overline{\mathbb{Q}}_{3^k}/\mathbb{Q}_p)$ and so $\epsilon_\mathcal{R}$ is non-trivial. Therefore condition (i) and (ii) are not satisfied. Since there is only 1 principal cluster (iii) is not satisfied. Therefore we are left to check (iv). But the three twins are permuted by Frobenius and hence (iv) is not satisfied. Therefore $C$ has no $K$-rational points. This can also be seen from looking at the minimal nsc model — the components of multiplicity 1 are the crosses of the three crossed tails. But the crossed tails are permuted by Frobenius as the corresponding clusters are, so there is no component of multiplicity 1 fixed by Frobenius.

Figure 1. Cluster picture and minimal nsc model of $C : y^2 = p((x - 1)^2 + p^2)((x - \zeta_3)^2 + p^2)((x - \zeta_3^2)^2 + p^2)$.

Example 3.3. Let $C : y^2 = p(x^3 - p^2)((x - 1)^3 - p^2)$. This is a hyperelliptic curve of Namikawa-Ueno type $\Pi - \Pi' - \alpha$. The cluster picture of $C$ is shown in Figure 2. The two principal clusters $\mathcal{s}_1$ and $\mathcal{s}_2$ have $e_{\mathcal{s}_1} = 6$ and so (i) does not apply. Quick inspection reveals that (ii)-(v) don’t either. Continuing, we see that the top cluster $\mathcal{R} = \mathcal{s}_1 \sqcup \mathcal{s}_2$ is not principal and $\mathcal{s}_1$ is odd and fixed by Galois. However, $[−\lambda_{\mathcal{R}} - \delta_{\mathcal{s}_1}/2, -\lambda_{\mathcal{R}}] = [-11/6, -3/2]$ which does not contain an integer. Therefore condition (vi) does not give us a $K$-rational point, and therefore $C$ cannot have any $K$-rational points. This can also be seen from the minimal nsc model as there is no component of multiplicity 1.

Appendix A. Cluster Pictures

We briefly collate some definitions concerning clusters for the convenience of the reader.

Definition A.1. Let $C : y^2 = f(x)$ be a hyperelliptic curve over $K$, with $\mathcal{R}$ the set of roots of $f$. A cluster is a non-empty subset $\mathcal{s} \subseteq \mathcal{R}$ of the form $\mathcal{s} = D \cap \mathcal{R}$ for some disc $D = z + \pi^n \mathcal{O}_K$, where $z \in \overline{K}$ and $n \in \mathbb{Q}$. If $\mathcal{s}$ is a cluster and $|\mathcal{s}| > 1$, $\mathcal{s}$ is a proper cluster and we define its depth

$$d_{\mathcal{s}} = \min_{r, r' \in \mathcal{s}} v_K(r - r').$$

The cluster picture $\Sigma$ is the set of all clusters of the roots of $f$. 

Definition A.2. A cluster $s \in \Sigma_X$ is odd (resp. even) if $|s|$ is odd (resp. even). A child $s' < s$ is a maximal subcluster of $s$, and its relative depth is $\delta_{s'} = d_{s'} - d_s$. The cluster $s$ is even if all its children are even. It is a twin if $|s| = 2$ and principal if $|s| \geq 3$, except if either $s = R$ is even and has exactly two children, or if $s$ has a child of size $2g$. It is a cotwin if it has a child of size $2g$ whose complement is not a twin.

Definition A.3. Let $D$ be a $p$-adic disk. Then

$$\nu_D(f) = v_K(c_f) + \sum_{r \in R} \min(d_D, v_K(z_D - r)),$$

and for a cluster $s$, $\nu_s = \nu_D(s)$.  

Definition A.4. Let $s$ be a proper cluster. Then $e_s \in \mathbb{Z}$ is the smallest integer such that $e_s d_s \in \mathbb{Z}$ and $e_s \nu_s \in 2\mathbb{Z}$.

Definition A.5. Let $s \in \Sigma$ be a proper cluster. Then the genus of $s$, $g(s)$, is such that $2g(s) + 1$ or $2g(s) + 2$ equals the number of odd children of $s$.

Definition A.6 (Invariants and Characters). For $\sigma \in G_K$ let

$$\chi(\sigma) \equiv \frac{\sigma(\pi)}{\pi} \mod m.$$  

For a proper cluster $s \in \Sigma_C$ define

$$\lambda_s = \frac{\nu_s}{2} - d_s \sum_{s' < s} \left\lfloor \frac{|s'|}{2} \right\rfloor.$$  

Define $\theta_s = \sqrt{c_f \prod_{r \not\in s} (z_D - r)}$. If $s$ is either even or a cotwin, we define $\epsilon_s : G_K \to \{ \pm 1 \}$ by

$$\epsilon_s(\sigma) \equiv \frac{\sigma(\theta_s)}{\theta_s^{(\sigma)s'}} \mod m.$$  

For all other clusters $s$ set $\epsilon_s(\sigma) = 0$.

Definition A.7. Let $s' < s$ be clusters in $\Sigma$. Then $s'$ is a stable child of $s$ if the stabiliser of $s$ also stabilises $s'$.

References

[1] Alex J. Best, L. Alexander Betts, Matthew Bisatt, Raymond van Bommel, Vladimir Dokchitser, Omri Faraggi, Sabrina Kunzeleier, Céline Maistret, Adam Morgan, Simone Muselli, and Sarah Nowell. A user’s guide to the local arithmetic of hyperelliptic curves. Bulletin of the London Mathematical Society, to appear.

[2] L. Alexander Betts. On the computation of Tamagawa numbers and Néron component groups of Jacobians of semistable hyperelliptic curves. Journal of Number Theory, to appear.

[3] Manjul Bhargava, John Cremona, and Tom Fisher. The proportion of genus one curves over $\mathbb{Q}$, defined by a binary quartic that everywhere locally have a point. International Journal of Number Theory, 17(4):903–923, May 2021.

[4] Matthew Bisatt. Clusters, inertia, and root numbers. arXiv preprint arXiv:1902.08981, 2019.

[5] J. E. Cremona and M. Sadek. Local and global densities for Weierstrass models of elliptic curves. arXiv preprint arXiv:2003.08454, 2020.

[6] Tim Dokchitser, Vladimir Dokchitser, Céline Maistret, and Adam Morgan. Arithmetic of hyperelliptic curves over local fields. arXiv preprint arXiv:1808.02936, 2018.
[7] Omri Faraggi and Sarah Nowell. Models of hyperelliptic curves with tame potentially semistable reduction. *Transactions of the London Mathematical Society*, 7(1):49–95, 2020.

[8] Sabrina Kunzweiler. Differential forms on hyperelliptic curves with semistable reduction. *Research in Number Theory*, 6, 06 2020.

[9] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics (0-19-961947-6). Oxford University Press, 2006.

[10] Simone Muselli. Models and integral differentials of hyperelliptic curves. *arXiv preprint arXiv:2003.01830*, 2020.