Most odd degree hyperelliptic curves have only one rational point

Michael Stoll
Universität Bayreuth

Arithmetic of abelian varieties in families
EPFL

November 12, 2012

Odd Degree Hyperelliptic Curves

We consider hyperelliptic curves of genus g of the form

$$C : y^2 = f(x) = x^{2g+1} + c_2 x^{2g-1} + c_3 x^{2g-2} + \ldots + c_{2g} x + c_{2g+1}$$

with $\underline{c} = (c_2, c_3, \ldots, c_{2g+1}) \in \mathcal{F}_g = \mathbb{Z}^{2g}$, ordered by height

$$H(\underline{c}) = \max\left\{|c_2|^{1/2}, |c_3|^{1/3}, \ldots, |c_{2g+1}|^{1/(2g+1)}\right\}.$$

Let $\mathcal{F}_{g,X} = \{\underline{c} \in \mathcal{F}_g : H(\underline{c}) < X\}$.

For a subset $S \subset \mathcal{F}_g$, we define its lower and upper density by

$$\lambda_g(S) = \liminf_{X\to\infty} \frac{\#(S \cap \mathcal{F}_{g,X})}{\#\mathcal{F}_{g,X}}, \qquad \upsilon_g(S) = \limsup_{X\to\infty} \frac{\#(S \cap \mathcal{F}_{g,X})}{\#\mathcal{F}_{g,X}}.$$

If $\lambda_g(S) = \upsilon_g(S)$, then the common value is the density $\delta_g(S)$ of S.

The Meaning of the Title

Each curve C has a rational point at infinity, denoted ∞.

Now the precise version of the statement in the title is as follows.

Theorem.
Let $\mathcal{C}_g$ be the subset of $\mathcal{F}_g$ consisting of curves C with $C(\mathbb{Q}) = \{\infty\}$. Then

$$\lim_{g \to \infty} \lambda_g(\mathcal{C}_g) = 1\,.$$

More precisely, $\quad \lambda_g(\mathcal{C}_g) = 1 - O\left(g^d 2^{-g}\right) \quad$ for some d.

This is joint work with **Bjorn Poonen**.

A First Idea

Let J denote the Jacobian of C and $\mathrm{Sel}(J)$ the 2-Selmer group of J.
We take ∞ as base-point to embed C into J.
Recall the connecting map $\delta \colon J(\mathbb{Q}) \to \mathrm{Sel}(J)$ from the Kummer sequence.

There is the following commuting diagram.

$$\begin{tikzcd}
 & J(\mathbb{Q}) \arrow[r, "\delta"] & \mathrm{Sel}(J) \arrow[dr, "r"] & \\
C(\mathbb{Q}) \arrow[ur, hook] \arrow[dr, hook] & & & J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \\
 & C(\mathbb{Q}_2) \arrow[r, hook] \arrow[urr, bend left, "s"] & J(\mathbb{Q}_2) \arrow[ur] &
\end{tikzcd}$$

If the images of r and s only meet in 0 (which is the image of ∞)
and r is injective, then $\quad C(\mathbb{Q}) \subset C(\mathbb{Q}_2) \cap 2J(\mathbb{Q})$.

This is not good enough.

A Better Idea

We look at the following 'scale-and-reduce' map.

$$\sigma\colon J(\mathbb{Q}_2) \setminus J(\mathbb{Q}_2)_{\text{tors}} \longrightarrow \frac{J(\mathbb{Q}_2)}{J(\mathbb{Q}_2)_{\text{tors}}} \setminus \{0\} \xrightarrow{\cong} \mathbb{Z}_2^g \setminus \{0\} \xrightarrow{s\&r} \mathbb{F}_2^g \setminus \{0\}$$

where the last map $s\&r$ first scales to obtain a primitive element and then reduces mod 2.

Lemma.
If the map $\sigma_S\colon \text{Sel}(J) \longrightarrow \dfrac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2) + J(\mathbb{Q}_2)_{\text{tors}}} \cong \mathbb{F}_2^g$ is injective, then

$$\sigma\bigl(J(\mathbb{Q}) \setminus J(\mathbb{Q})_{\text{tors}}\bigr) \subset \sigma_S\bigl(\text{Sel}(J)\bigr)\,.$$

Proof. Write $P \in J(\mathbb{Q}) \setminus J(\mathbb{Q})_{\text{tors}}$ as $P = 2^n P'$ with $P' \notin 2J(\mathbb{Q})$. Then $0 \neq \delta(P') \in \text{Sel}(J)$, so $\sigma(P) = \sigma(P') = \sigma_S(\delta(P'))$.

A Criterion

Corollary.
Assume that σ_S is injective. If

$$\sigma\big(C(\mathbb{Q}_2) \setminus C(\mathbb{Q}_2)_{\text{tors}}\big) \cap \sigma_S\big(\text{Sel}(J)\big) = \emptyset\,,$$

then $\qquad C(\mathbb{Q}) = C(\mathbb{Q})_{\text{tors}}$.

Proof. If $P \in C(\mathbb{Q}) \setminus C(\mathbb{Q})_{\text{tors}}$, then $\sigma(P)$ is in both images.

It is known that the set of curves with $C(\mathbb{Q})_{\text{tors}} \neq \{\infty\}$ has density zero.
So it suffices to show that the lower density of curves such that σ_S is injective and the intersection above is empty tends to 1.

We first show that $\sigma\big(C(\mathbb{Q}_2) \setminus C(\mathbb{Q}_2)_{\text{tors}}\big)$ is usually small and then invoke results of Bhargava and Gross.

The Logarithm

The 2-adic abelian logarithm on J is a homomorphism

$$\log \colon J(\mathbb{Q}_2) \longrightarrow T_0\, J(\mathbb{Q}_2) \cong \mathbb{Q}_2^g$$

that induces the isomorphism

$$\frac{J(\mathbb{Q}_2)}{J(\mathbb{Q}_2)_{\text{tors}}} \xrightarrow{\cong} \mathbb{Z}_2^g\,.$$

We can therefore choose differentials $\omega_1, \dots, \omega_g \in \Omega^1_C(\mathbb{Q}_2) \cong \Omega^1_J(\mathbb{Q}_2)$ such that this isomorphism is given by

$$P \longmapsto \Bigl(\int_0^P \omega_1, \dots, \int_0^P \omega_g\Bigr)\,.$$

For $P \in C(\mathbb{Q}_2) \setminus C(\mathbb{Q}_2)_{\text{tors}}$ we then have

$$\sigma(P) = \mathrm{s\&r}\Bigl(\int_\infty^P \omega_1, \dots, \int_\infty^P \omega_g\Bigr)\,.$$

Logarithms on Residue Disks

Let $\mathcal{C}$ be a (not necessarily minimal) regular model over $\mathbb{Z}_2$ of C. Then every smooth $\mathbb{F}_2$-point $\bar{P}$ on the special fiber of $\mathcal{C}$ gives rise to a parametrized residue disk in $C(\mathbb{Q}_2)$.

On such a residue disk D, the integrals $\int_\infty^P \omega_j$ are given by power series $\ell_j(t)$ that converge for $|t|_2 < 1$.
Let $n_j(D)$ be the order of vanishing of the reduction of ω_j at $\bar{P}$.
We can write such a power series in the form

$$\ell_j(t) = p_j(t) q_j(t)$$

with a polynomial $p_j \in \mathbb{Q}_2[t]$ of degree at most $2n_j(D) + 2$
and a power series q_j whose value for $t \in 2\mathbb{Z}_2$ is always a 2-adic unit.

So $$\sigma\bigl(D \setminus C(\mathbb{Q}_2)_{\mathrm{tors}}\bigr) = \bigl\{ s\&r\bigl(p_1(t), \ldots, p_g(t)\bigr) : t \in 2\mathbb{Z}_2, \exists j : p_j(t) \neq 0 \bigr\}.$$

Values of $s\&r$ on Polynomials

We have to bound the size of

$$\left\{ s\&r\big(p_1(t), \ldots, p_g(t)\big) : t \in 2\mathbb{Z}_2, \exists j : p_j(t) \neq 0 \right\}.$$

Dividing by the gcd of the polynomials,
we can assume that they never all vanish simultaneously.

We will show that

$$\#\left\{ s\&r\big(p_1(t), \ldots, p_g(t)\big) : t \in 2\mathbb{Z}_2 \right\} \leq (2g-1)\left(2\sum_{j=1}^{g} \deg(p_j) - 1\right).$$

Note that for any given $t \in 2\mathbb{Z}_2$, the image is determined by the set

$$I(t) = \left\{ j \in \{1, 2, \ldots, g\} : v_2\big(p_j(t)\big) = \min_i v_2\big(p_i(t)\big) \right\}.$$

Disks in $\bar{\mathbb{Q}}_2$

For $a \in \mathbb{Z}_2$ and $n \geq 0$, define

$$B(a,n) = \{\xi \in \bar{\mathbb{Q}}_2 : v_2(\xi - a) > n\}.$$

Let $\alpha \in \bar{\mathbb{Q}}_2$. If $\alpha \notin B(a,n)$, then $v_2(\xi - \alpha) = v_2(a - \alpha)$ is constant on $B(a,n)$.

Let R be the set of all roots of all the polynomials p_j.

Lemma A.
There are at most $2\#R - 1 \leq 2\sum_j \deg(p_j) - 1$ different sets $B(a,n) \cap R \neq \emptyset$.

Proof. Allowing disks $B(\alpha, r)$ with $\alpha \in \bar{\mathbb{Q}}_2$ and $r \in \mathbb{Q}$,
these sets correspond to the branching nodes and leaves of a tree
whose set of leaves is R.
(The tree can be seen inside the Berkovich projective line over $\mathbb{C}_2$.)

Values of $s\&r$ on Annuli

Lemma B.
Each set $B \cap R$ contributes at most $2g-1$ distinct values under $s\&r$.

Proof.
Let $S = B \cap R$ and $A_S = \{a \in 2\mathbb{Z}_2 : v_2(a-\rho)$ is minimal exactly for $\rho \in S\}$.
(This is some kind of 2-adic annulus.)
Then there is $\alpha \in \bar{\mathbb{Q}}_2$ such that $v_2\big(p_j(t)\big) = m_j v_2(t-\alpha) + m_j'$ for $t \in A_S$.
Given the linear functions $l_j : x \mapsto m_j x + a_j'$ on $\mathbb{R}$,
there are at most $2g-1$ possibilities for $\{j : l_j(x) = \min_i l_i(x)\}$.

Lemmas A and B imply the result:

$$\#\big\{s\&r\big(p_1(t),\dots,p_g(t)\big) : t \in 2\mathbb{Z}_2\big\} \le (2g-1)(2\#R-1) \le (2g-1)\left(2\sum_{j=1}^{g} \deg(p_j)-1\right).$$

Bounding the Number of Residue Disks

Let Δ be the discriminant and R_f the set of all roots of f.

Lemma C.
$C(\mathbb{Q}_2)$ can be covered with at most $2v_2(\Delta) + 17$ residue disks.

Proof (Sketch).
The disks $B(a, n)$ are the nodes of two infinite binary trees
(rooted at $B(0, 0)$ and $B(1, 0)$).
The subset of disks B with $\#(B \cap R_f) \geq 2$ is a union T of two finite subtrees
with less than $v_2(\Delta)/2$ edges in total.
$\mathbb{Z}_2$ is partitioned into sets $B \cap \mathbb{Z}_2$ where $B \notin T$ is a child of a node in T;
the points in $C(\mathbb{Q}_2)$ with x-coordinate in B fall into ≤ 4 residue disks.
The number of B's is the number of edges plus 4; add a disk for ∞.

Bounding the Discriminant

Lemma D.
The density of the set of curves in $\mathcal{F}_g$ such that $v_2(\Delta) \geq n$ exists and is $\leq 2g\, 2^{-n/(2g)}$.

Remark.
We think that it should actually be $\leq 2^{-n/2}$.
Does anybody know results in this direction?

Corollary.
For a set of curves in $\mathcal{F}_g$ of lower density $\geq 1 - 2g\, 2^{-g}$,
we have $\#\sigma\big(C(\mathbb{Q}_2) \setminus C(\mathbb{Q}_2)_{\mathrm{tors}}\big) \ll g^4$.

Proof. There are $\ll g^2$ residue disks with $\ll g^4$ distinct values in total.
This uses $\sum_D n_j(D) \leq 2g - 2$ for all j.

Bhargava-Gross

Manjul Bhargava and Dick Gross have recently proved the following.

Theorem.
The average of $\#\,\mathrm{Sel}(J)$ exists in $\mathcal{F}_g$ and equals 3.
This is still true for subfamilies defined by congruence conditions.

If in such a subfamily $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = G$ is constant,
then each element of G has on average $\frac{2}{\#G}$ nontrivial preimages in $\mathrm{Sel}(J)$.

This implies that on 2-adically small subsets of $\mathcal{F}_g$,
an element of $\mathbb{F}_2^g \setminus \{0\}$ is in the image of σ_S with density $\leq 2^{1-g}$
and that σ_S is not injective on a set of density $\leq 2^{1-g}$.

Conclusion

Excluding a set of density $\leq 2g\,2^{-g}$, we have

$$\#\sigma\big(C(\mathbb{Q}_2) \setminus C(\mathbb{Q}_2)_{\mathrm{tors}}\big) \ll g^4 .$$

Excluding a further set of density $\leq 2 \cdot 2^{-g}$, we have that σ_S is injective.

Excluding a further set of density $\ll g^4 2^{-g}$,
we have that the image of σ_S misses $\sigma\big(C(\mathbb{Q}_2) \setminus C(\mathbb{Q}_2)_{\mathrm{tors}}\big)$.

Conclusion.
The set $\mathcal{C}_g$ of curves C in $\mathcal{F}_g$ with $C(\mathbb{Q}) = \{\infty\}$
has lower density $1 - O(g^4 2^{-g})$.

Small Genus

We can also use this approach to show that
$\mathcal{C}_g$ has positive lower density for all $g \geq 3$.

For this, it is sufficient to exhibit one curve $C_0 \in \mathcal{F}_g$
such that $\#\sigma\big(C_0(\mathbb{Q}_2) \setminus C_0(\mathbb{Q}_2)_{\mathrm{tors}}\big) = 1$.
This will remain true for curves C 2-adically sufficiently close to C_0,
so on a subfamily of positive density.
Let $\sigma\big(C_0(\mathbb{Q}_2) \setminus C_0(\mathbb{Q}_2)_{\mathrm{tors}}\big) = \{w\} \subset \mathbb{F}_2^g \setminus \{0\}$.

Apply Bhargava-Gross to this subfamily to obtain positive density of

$$\sigma_S \text{ injective} \qquad \text{and} \qquad w \notin \sigma_S\big(\mathrm{Sel}(J)\big)\,.$$

(For $g = 2$ the equidistribution result of Bhargava-Gross
is not strong enough for this last step.)