UNIFORM BOUNDS FOR THE NUMBER OF RATIONAL POINTS ON HYPERELLIPTIC CURVES OF SMALL MORDELL-WEIL RANK

MICHAEL STOLL

Abstract. We show that there is a bound depending only on g and $[K:\mathbb{Q}]$ for the number of K-rational points on a hyperelliptic curve C of genus g over a number field K such that the Mordell-Weil rank r of its Jacobian is at most $g-3$. If $K=\mathbb{Q}$, an explicit bound is $8(r+4)(g-1)+\max\{1,4r\}\cdot g$.

The proof is based on Chabauty's method; the new ingredient is an estimate for the number of zeros of a logarithm in a p-adic 'annulus' on the curve, which generalizes the standard bound on disks. The key observation is that for a p-adic field k, the set of k-points on C can be covered by a collection of disks and annuli whose number is bounded in terms of g (and k).

1. Introduction

Since Faltings' proof [Fal83] of Mordell's conjecture, we know that a curve of genus $g\geq 2$ can have only finitely many rational points. This raises the question whether there might be uniform bounds of some sort on the number of rational points. Caporaso, Harris, and Mazur have shown [CHM97] that the validity of the Bombieri-Lang conjecture on rational points on varieties of general type would imply the existence of a bound depending only on the genus g. (For function fields like $k=\mathbb{F}_p(t)$, the number of k-points on curves over k of fixed genus is unbounded, however, see for example [CUV12].) On the other hand, considering an embedding of the curve into its Jacobian variety, which identifies the set of rational points on the curve with the intersection of the curve and the Mordell-Weil group, one can ask the following purely geometric question: Given a curve C of genus $g\geq 2$ over a field k of characteristic zero, embedded in its Jacobian J, and a finitely generated subgroup Γ of $J(k)$ of rank $\dim_{\mathbb{Q}}\Gamma\otimes_{\mathbb{Z}}\mathbb{Q}\leq r$, is there a uniform bound in terms of g and r for the number of points in $C\cap\Gamma$? (See Mazur [Maz86, end of Section III.2].) That this number is finite for each individual curve follows from further work by Faltings [Fal94]. Heuristic arguments suggest that such a uniform bound should exist. The existence of such uniform bounds has been shown for k a *function field* if C is not defined over the algebraic numbers by Buium [Bui93] (and also for function fields in characteristic p by Buium and Voloch [BV96]).

However, to our knowledge, so far not even a uniform (and unconditional) bound for the number of *rational torsion points* on curves of some fixed genus $g\geq 2$ has been obtained! In this note, we finally obtain such a bound for hyperelliptic curves of genus at least 3 (but the method should generalize to arbitrary curves). More generally, we can show that on a hyperelliptic curve C of genus g over number field of degree $\leq d$, there can be at most

Date: September 17, 2013.

2010 *Mathematics Subject Classification.* Primary 14G05, 11G20, 11G30; Secondary 14G20, 14G25, 14H25, 14K15, 14K20.

$R(d,g,r)$ rational points mapping into a given subgroup of rank $r \leq g-3$ of the Mordell-Weil group, where $R(d,g,r)$ depends only on d, g and r. This implies uniform bounds in terms of d, g and r only for the number of rational points on such curves as long as the Mordell-Weil rank is at most $g-3$ and also for the number of rational points in a torsion packet when $g \geq 3$, see Theorem 7.1 and Corollary 7.3 below.

The proof is based on Chabauty's method [Cha41, Col85, MP13, Sto06]. If C is a curve over $\mathbb{Q}$, with Jacobian J and minimal regular model $\mathcal{C}$ over $\mathbb{Z}_p$, where the prime p is sufficiently large, and we assume that $r = \operatorname{rank} J(\mathbb{Q}) < g$, then one can bound $\#C(\mathbb{Q})$ by the number of smooth $\mathbb{F}_p$-points on the special fiber of $\mathcal{C}$ plus $2r$, see [KZB13]. This bound is obtained as follows. Consider the Chabauty-Coleman pairing (defined below in Section 2)

$$\Omega^1_J(\mathbb{Q}_p) \times J(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p, \quad (\omega, P) \longmapsto \oint_O^P \omega$$

This pairing is $\mathbb{Q}_p$-linear in ω and additive in P; its kernel on the left is trivial. If $r < g$, then there is a subspace $V \subset \Omega^1_J(\mathbb{Q}_p)$ of dimension at least $g - r \geq 1$ that annihilates the Mordell-Weil group $J(\mathbb{Q}) \subset J(\mathbb{Q}_p)$ under the pairing. Let $P_0 \in C(\mathbb{Q})$ and use P_0 as basepoint for an embedding $i\colon C \to J$. Then for all $P \in C(\mathbb{Q})$ and all $\omega \in V$, we have

$$0 = \oint_O^{i(P)} \omega = \oint_{P_0}^P i^*\omega$$

where $i^*\omega \in \Omega^1_C(\mathbb{Q}_p)$ is a regular differential on C. The integral on the right is defined by this equality. One then shows (see for example [Sto06]) that the number of zeros of the function

$$P \longmapsto \oint_{P_0}^P i^*\omega$$

on a p-adic residue disk of C, which is the set of p-adic points reducing mod p to a given smooth point on the special fiber of $\mathcal{C}$, is at most one plus the number of zeros (counted with multiplicity) of ω on that residue disk. (Here we use that p is large enough, otherwise the bound has to be modified.) Choosing a 'good' $\omega \in V$ for each residue disk leads to the bound

$$\#C(\mathbb{Q}) \leq \#\mathcal{C}(\mathbb{F}_p)^{\text{smooth}} + 2r$$

mentioned earlier.

The problem with this approach is that the bound depends on the complexity of the special fiber of $\mathcal{C}$, which is unbounded — there can be arbitrarily long chains of rational curves in the special fiber, which can lead to an arbitrarily large number of smooth $\mathbb{F}_p$-points. The idea for overcoming this problem is to parametrize the subset of $C(\mathbb{Q}_p)$ corresponding to such a chain not by a union of (an unbounded number of) disks, but by an 'annulus'. We can then obtain a bound for the number of points in that subset that is independent of the number of residue disks. Since both the number of such annuli and the number of remaining residue disks are bounded in terms of the genus (and p), we do obtain a uniform bound. The price we have to pay is that on (at least some of) the annuli, we need to impose additional linear conditions on the differential ω, so that we need the space of differentials annihilating the relevant subgroup of $J(\mathbb{Q}_p)$ to be of dimension at least three. This translates into the rank bound $r \leq g-3$. The key result for our application is Proposition 5.4, which gives a precise comparison of the abelian integral pulled back to an annulus and the p-adic integral of the

pulled-back 1-form. It turns out that the difference between the two is a linear function of the valuation.

We carry out this approach in the case of hyperelliptic curves. We expect that the approach can be generalized to arbitrary curves; we will pursue this in future work.

Acknowledgments. The vague idea that one should be able to use Chabauty's method to prove uniform upper bounds for the number of rational points had long been in the author's mind, but was put aside as infeasible because of the apparent problems described above. The new activity leading to the results presented here was prompted by a question Manjul Bhargava asked related to [PS13]: could we give a family of odd degree hyperelliptic curves C of any genus, defined by congruences, such that our method would not work for any curve in the family? The intuition that this should not be possible for large genus led to the idea of using integration on annuli to prove that the image of $C(\mathbb{Q}_2)$ in $\mathbb{P}^{g-1}(\mathbb{F}_2)$ under the '$\rho\log$' map of [PS13] is bounded by a polynomial in g. This result will be presented in a separate paper or in a later version of this article. The idea then extended naturally to the original question. So I would like to thank Manjul for asking the right question. I also wish to thank Amnon Besser for help with questions about p-adic integration and Stefan Wewers for answering my questions on stable models (which have now been eliminated from the argument). Dino Lorenzini was very helpful on the question (discussed in Section 3) of how to bound the number of '$\mathbb{A}^1$-components' in the special fiber of the minimal regular model of a curve. Felipe Voloch provided some pointers to the literature.

2. Notation

Until further notice, we fix the following notation.

Let p be a prime number. As usual, $\mathbb{Q}_p$ denotes the field of p-adic numbers and $\mathbb{C}_p$ the completion of an algebraic closure of $\mathbb{Q}_p$. We let $v\colon \mathbb{C}_p \to \mathbb{Q}\cup\{\infty\}$ denote the valuation on $\mathbb{C}_p$ that is normalized by $v(p)=1$. We also fix an absolute value $|\cdot|$ on $\mathbb{C}_p$. Throughout the paper, $k\subset\mathbb{C}_p$ stands for a finite field extension of $\mathbb{Q}_p$ with ramification index e; we write $\mathcal{O}$ for its ring of integers and κ for the residue field. We set $q:=\#\kappa$; $k^{\mathrm{unr}}\subset\mathbb{C}_p$ is the maximal unramified extension of k.

Let $g\geq 3$ be an integer and let C be a smooth, projective, and geometrically integral curve of genus g over k. The Jacobian variety of C is denoted J; the origin on J is O. We denote the image of the divisor $(P)-(Q)$ on C in J by $[P-Q]$. We denote by $\log_J$ the p-adic abelian logarithm $J(k)\to T_OJ(k)\cong k^g$. On a sufficiently small subgroup neighborhood of O, it is given by evaluating the formal logarithm, and then extended to all of $J(k)$ by linearity. The space $\Omega^1_J(k)$ of global regular 1-forms on J defined over k agrees with the space of invariant (under translations) 1-forms on J and can be identified with the cotangent space $(T_OJ(k))^*$ of J at the origin. This induces a pairing

$$\Omega^1_J(k)\times J(k)\longrightarrow k,\quad (\omega,P)\mapsto\langle\omega,\log_J(P)\rangle =: \int_O^P \omega\,,$$

which we call the *Chabauty-Coleman pairing*. It is k-linear in ω and additive (and $\mathcal{O}$-linear on the kernel of reduction) in P. Its kernel on the left is trivial, and its kernel on the right is the torsion subgroup of $J(k)$.

Let $P_0 \in C(k)$ and let $i\colon C \to J$ be the embedding given by $P \mapsto [P - P_0]$. Then $i^*\colon \Omega^1_J \to \Omega^1_C$ is an isomorphism (which does not depend on P_0). If $\omega \in \Omega^1_C(k)$ is $i^*\omega_J$ for some $\omega_J \in \Omega^1_J(k)$, then we set for points $P, Q \in C(k)$

$$\oint_P^Q \omega := \oint_{i(P)}^{i(Q)} \omega_J = \oint_O^{[Q-P]} \omega_J \,.$$

We use the symbol $\oint$ to distinguish this integral defined via abelian logarithms from the p-adic integral $\int$ given by p-adic integration theory.

Inclusions '$A \subset B$' are meant to be non-strict.

3. Combinatorics of arithmetic graphs

We begin with a study of the combinatorics of the (smooth part of the) special fiber of the minimal regular model $\mathcal{C}$ over $\mathcal{O}$ of a (smooth projective geometrically integral) curve C of genus $g \geq 2$ over k. For the general background, we refer to [Liu02, Section 10.1].

The special fiber $\mathcal{C}_s$ of $\mathcal{C}$ decomposes into irreducible components; we assume for now that the residue field κ is large enough so that the components are geometrically irreducible. Let Γ be one of these components of $\mathcal{C}_s$. If W denotes a relative canonical divisor, then by the adjunction formula we have

$$\Gamma \cdot W = 2p_a(\Gamma) - 2 - \Gamma^2 \,. \tag{3.1}$$

There are two cases: $\Gamma \cdot W > 0$ and $\Gamma \cdot W = 0$. If $m(\Gamma)$ denotes the multiplicity of Γ in $\mathcal{C}_s$, then

$$2g - 2 = \mathcal{C}_s \cdot W = \sum_\Gamma m(\Gamma)(\Gamma \cdot W) \,, \tag{3.2}$$

which implies that there can be at most $2g-2$ components Γ having $\Gamma \cdot W > 0$ (note that W is effective in the situation considered here). On the other hand, $\Gamma \cdot W = 0$ means $p_a(\Gamma) = 0$ and $\Gamma^2 = -2$ or $p_a(\Gamma) = 1$ and $\Gamma^2 = 0$ (the intersection pairing is negative semidefinite, so $\Gamma^2 \leq 0$). $\Gamma^2 = 0$ would imply that Γ is the only component; then $2g - 2 = 0$ and so $g = 1$, which we have excluded. So Γ is isomorphic to $\mathbb{P}^1$ over κ and has self-intersection -2. Such components are called (-2)-curves.

Associated to the special fiber $\mathcal{C}_s$ is a graph G, whose vertices correspond to the components of $\mathcal{C}_s$, with two (distinct) vertices Γ_1 and Γ_2 joined by $\Gamma_1 \cdot \Gamma_2$ edges. The graph G is connected. To each vertex Γ, we associate its multiplicity $m(\Gamma)$ and its arithmetic genus $p_a(\Gamma)$. This data is equivalent to what is called a 'type' in [AW71]. The intersection pairing satisfies

$$\Gamma \cdot \sum_{\Gamma'} m(\Gamma')\Gamma' = \Gamma \cdot \mathcal{C}_s = 0 \,.$$

Using the adjunction formula (3.1), we can write this as

$$\sum_{\Gamma' \neq \Gamma} m(\Gamma')\Gamma \cdot \Gamma' = -m(\Gamma)\Gamma^2 = m(\Gamma)\big(\Gamma \cdot W + 2(1 - p_a(\Gamma))\big) \,.$$

By adding $p_a(\Gamma)$ loops at the vertex Γ, we can assume that $p_a(\Gamma) = 0$ for all Γ, so that

$$m(\Gamma)(\Gamma \cdot W + 2) = \sum_{\Gamma' \neq \Gamma} m(\Gamma')\Gamma \cdot \Gamma' . \tag{3.3}$$

We are interested in the structure of the smooth part $\mathcal{C}_s^{\mathrm{smooth}}$ of the special fiber. It is the union of the components of multiplicity 1 minus their singular points and the points where they meet other components. We have already seen that there can be at most $2g-2$ such components with $\Gamma \cdot W > 0$. The remaining components are (-2)-curves of multiplicity 1, so by (3.3) the total intersection number with other components is 2. There are four cases for such a component Γ.

1) Γ meets two components of multiplicity 1 in two distinct points. Then Γ is part of a maximal *chain* of such components, ending in two components of multiplicity 1 (which can be identical) that are not (-2)-curves.
2) Γ meets a component of multiplicity 2 in one point.
3) Γ meets two components of multiplicity 1 in the same point.
4) Γ meets a component of multiplicity 1 in one point with intersection multiplicity 2.

In the latter three cases, the corresponding component of $\mathcal{C}_s^{\mathrm{smooth}}$ is isomorphic to $\mathbb{A}^1$. We will call such components of $\mathcal{C}$ simply $\mathbb{A}^1$-*components*.

Artin and Winters in [AW71, Theorem 1.6] show that there are only finitely many different 'types' of fixed genus up to an equivalence that ignores the lengths of chains (also of higher multiplicity) as above. This implies that there must be bounds that depend only on g for the number of (maximal) chains and for the number of $\mathbb{A}^1$-components. The following result gives explicit and optimal such bounds.

Theorem 3.4. *Let $\mathcal{C}_s$ be the special fiber of the minimal proper regular model of a smooth projective geometrically integral curve C of genus $g \geq 2$ over a p-adic field k. Then there are numbers $t, u \geq 0$ with $t + u \leq g$ such that*

i) *The number of components Γ with $\Gamma \cdot W > 0$ is $N \leq 2g-2$.*
ii) *The number of chains is $\leq N - 1 + t \leq 2g - 3 + t$.*
iii) *The number of (-2)-curves of multiplicity 1 outside of chains is $\leq 3u$.*

Remark 3.5. It is not very hard to construct an arithmetic graph of genus g with $2g-2$ components Γ such that $\Gamma \cdot W > 0$ and having $2g-3+t$ chains and $3(g-t)$ $\mathbb{A}^1$-components, for every $t = 0, 1, \ldots, g$. We leave this as an exercise for the interested reader. This shows that the bounds given in the theorem above are optimal.

Remark 3.6. It is easy to see that the numbers t and u in the statement of the theorem can be taken to be the toric and unipotent ranks of the special fiber of the Néron model of the Jacobian of C.

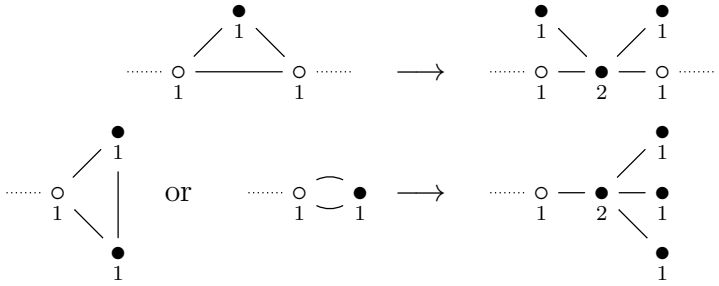
Proof. We first bound the number of chains. As in the statement of the theorem, let N denote the number of components Γ such that $\Gamma \cdot W > 0$. Then $N \leq 2g-2$ by (3.2). Consider the subgraph G' of G spanned by the N corresponding vertices and the vertices corresponding to components in chains. Contracting each chain to an edge, we obtain a

graph G'' whose Euler characteristic equals that of G', which cannot be smaller than that of G (since G is connected). So we find that

$$\#\{\text{chains}\} \leq \#\{\text{edges of } G''\} = N - \chi(G'') \leq N - \chi(G) = N - (1-t)$$

as claimed.

In the last two cases in the enumeration preceding the theorem, we can modify $\mathcal{C}_s$ locally to obtain a situation with normal crossings, but with a larger number of $\mathbb{A}^1$-components. Below, a vertex corresponding to a (-2)-curve is represented as $\bullet$, whereas a vertex corresponding to a component Γ with $\Gamma \cdot W > 0$ is represented as $\circ$. The numbers near the symbols are the multiplicities.



So we can assume that all the $\mathbb{A}^1$-components meet a component of multiplicity 2.

To obtain a bound on the number of $\mathbb{A}^1$-components, we classify the vertices Γ of G according to the pair $(m(\Gamma), \Gamma \cdot W) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{\geq 0}$ of invariants. Given $m \geq 1$ and $w \geq 0$, we call a vertex Γ of G with $m(\Gamma) = m$ and $\Gamma \cdot W = w$ an (m,w)-*vertex*. We denote by $v_{(m,w)}$ the number of (m,w)-vertices. We consider each edge of G as an oriented edge with both possible choices of orientation. We then denote by $e_{(m,w),(m',w')}$ the number of oriented edges leading from an (m,w)-vertex to an (m',w')-vertex.

Taking the sum of (3.3) over all (m,w)-vertices, we obtain

$$m(w+2)v_{(m,w)} = \sum_{(m',w')} m' e_{(m,w),(m',w')}\,,$$

or equivalently,

$$v_{(m,w)} = \frac{1}{m(w+2)} \sum_{(m',w')} m' e_{(m,w),(m',w')}\,, \tag{3.7}$$

which allows us to replace $v_{(m,w)}$ by the right hand side. If we use this in (3.2), this gives

$$\sum_{(m,w),(m',w')} \frac{wm'}{w+2} e_{(m,w),(m',w')} = \sum_{(m,w)} mw\, v_{(m,w)} = 2g-2\,. \tag{3.8}$$

In addition, denoting by t the number of independent loops in G (also known as the first Betti number of G) and remembering that G is connected and that $e_{(m,w),(m',w')} + e_{(m',w'),(m,w)}$ counts twice the edges between vertices with invariants (m,w) and (m',w'), we have the relation

$$2\sum_{(m,w)} v_{(m,w)} - 2 + 2t = \sum_{(m,w),(m',w')} e_{(m,w),(m',w')}\,,$$

which we rewrite using (3.7) as

$$\sum_{(m,w),(m',w')} \Big(\frac{2m'}{m(w+2)} - 1\Big) e_{(m,w),(m',w')} = 2 - 2t\,.$$

Adding (3.8) to this, we finally have

$$\sum_{(m,w),(m',w')} \Big(\frac{m'(mw+2)}{m(w+2)} - 1\Big) e_{(m,w),(m',w')} = 2(g-t)\,. \tag{3.9}$$

Let $\le$ denote the lexicographical ordering of the pairs (m,w). Since $e_{(m,w),(m',w')} = e_{(m',w'),(m,w)}$, we can rewrite (3.9) as

$$\sum_{(m,w)} \frac{(m-1)w}{w+2} e_{(m,w),(m,w)} + \sum_{(m,w)<(m',w')} \Big(\frac{m'(mw+2)}{m(w+2)} + \frac{m(m'w'+2)}{m'(w'+2)} - 2\Big) e_{(m,w),(m',w')} = 2(g-t). \tag{3.10}$$

We can bound the coefficient of $e_{(m,w),(m',w')}$ in (3.10) from below:

$$\begin{aligned}\frac{m'(mw+2)}{m(w+2)} + \frac{m(m'w'+2)}{m'(w'+2)} - 2 &= m' - 2\frac{m'(m-1)}{m(w+2)} + m - 2\frac{m(m'-1)}{m'(w'+2)} - 2 \\ &\overset{w\ge 0}{\ge} m' - \frac{m'(m-1)}{m} + m - \frac{m(m'-1)}{m'} - 2 \\ &= \frac{m'}{m} + \frac{m}{m'} - 2 \ge 0\,.\end{aligned}$$

So all coefficients on the left hand side of (3.10) are nonnegative; the coefficient of $e_{(m,w),(m,w)}$ vanishes if and only if $w = 0$ or $m = 1$, and the coefficient of $e_{(m,w),(m',w')}$ vanishes if and only if we have equality everywhere in the above, which is equivalent to $m = m' = 1$ (or $m = m'$ and $w = w' = 0$, but then $(m,w) = (m',w')$).

Let $\lambda_{(m,w),(m',w')}$ denote the coefficient of $e_{(m,w),(m',w')}$ in (3.10). Then

$$\begin{aligned}\lambda_{(1,w),(2,0)} &= \frac{1}{2} \quad \text{for all } w \ge 0, \\ \lambda_{(1,0),(2,w')} &\ge \frac{2}{3} \quad \text{for all } w' \ge 1, \\ \lambda_{(2,0),(2,w')} &\ge \frac{1}{3} \quad \text{for all } w' \ge 1, \\ \lambda_{(2,0),(3,w')} &\ge \frac{1}{6} \quad \text{for all } w' \ge 0.\end{aligned}$$

Using this in (3.10) we obtain

$$\frac{1}{2} e_{(1,0),(2,0)} + \frac{1}{2}\sum_{w\ge 1} e_{(1,w),(2,0)} + \frac{1}{3}\sum_{w'\ge 1} e_{(2,0),(2,w')} + \frac{1}{6}\sum_{w'\ge 0} e_{(2,0),(3,w')} + \frac{2}{3}\sum_{w'\ge 1} e_{(1,0),(2,w')} \le 2(g-t)\,. \tag{3.11}$$

We now claim that

$$3\sum_{w\ge 1} e_{(1,w),(2,0)} + 2\sum_{w'\ge 1} e_{(2,0),(2,w')} + \sum_{w'\ge 0} e_{(2,0),(3,w')} \ge e_{(1,0),(2,0)}\,. \tag{3.12}$$

Assuming this for a moment, we can use (3.12) in (3.11) to obtain

$$\frac{2}{3}\sum_{w'\geq 0} e_{(1,0),(2,w')} \leq 2(g-t) \qquad \text{or equivalently,} \qquad \sum_{w'\geq 0} e_{(1,0),(2,w')} \leq 3(g-t)\,.$$

The left hand side counts exactly the (-2)-curves of multiplicity 1 that meet a component of multiplicity 2. Since we have seen that after possibly a local modification of the graph this is an upper bound for the $\mathbb{A}^1$-components we want to count, this shows the last assertion in Theorem 3.4.

It remains to prove (3.12). We first observe that contracting an edge between two $(2,0)$-vertices does not change the genus or the topological properties of G and also does not affect (3.10). So we can assume without loss of generality that no such edges are present. We now consider those $(2,0)$-vertices that contribute to $e_{(1,0),(2,0)}$, i.e., that have an edge to a $(1,0)$-vertex. Let a_j $(1 \leq j \leq 3)$ denote the number of such vertices Γ such that the highest multiplicity of a vertex connected to Γ is j. Since $g \geq 2$, there cannot be a $(2,0)$-vertex connected only to $(1,0)$-vertices, as this would give rise to a connected component of genus 1, contradicting the fact that G is connected. This implies that a vertex counted by a_j can have at most $(4-j)$ edges to $(1,0)$-vertices; it also has at least one egde to a vertex with multiplicity j that is not a $(1,0)$-vertex. So

$$\sum_{w\geq 1} e_{(1,w),(2,0)} \geq a_1, \quad \sum_{w'\geq 1} e_{(2,0),(2,w')} \geq a_2, \quad \sum_{w'\geq 0} e_{(2,0),(3,w')} \geq a_3$$

and therefore

$$e_{(1,0),(2,0)} \leq 3a_1 + 2a_2 + a_3 \leq 3\sum_{w\geq 1} e_{(1,w),(2,0)} + 2\sum_{w'\geq 1} e_{(2,0),(2,w')} + \sum_{w'\geq 0} e_{(2,0),(3,w')}$$

as claimed. □

In general, some of the components of $\mathcal{C}_s$ may not be defined over κ. If a chain contains a component defined over κ, then either all components of the chain are defined over κ, or else the chain contains an odd number of components of which only the middle one is defined over κ (and the action of Frobenius reverses the orientation of the chain).

4. Partition into disks and annuli

We keep the notation introduced so far. Let $P \in C(k)$ be a point. Then P reduces to a point $\bar{P} \in \mathcal{C}_s^{\mathrm{smooth}}(\kappa)$, and so $\bar{P}$ is either on a component Γ with $\Gamma \cdot W > 0$ (and multiplicity 1), or on an $\mathbb{A}^1$-component, or on a component belonging to a chain. We bound the number of smooth κ-points occurring in the first two cases. Denoting by $p_g(\Gamma)$ the geometric genus of the component Γ and writing $\Gamma_1, \ldots, \Gamma_{N'}$ for the components occurring in the first case (with $N' \leq N$, since we only consider components defined over κ and with multiplicity 1), we obtain the bound

$$\sum_{j=1}^{N'} \big(q + 1 + 2p_g(\Gamma_j)\sqrt{q}\big) \leq (2g-2)(q+1) + 2a\sqrt{q}$$

for the number of smooth κ-points on components having positive intersection with W. Here a denotes the abelian rank of the special fiber of the Néron model of the Jacobian of C. For

the number of smooth κ-points on $\mathbb{A}^1$-components, we have the bound $3uq$, since each $\mathbb{A}^1$-component defined over κ has q smooth κ-points. Fixing $a+u=g-t$, the sum of these bounds is maximal when $a=0$, leading to a bound of

$$(2g-2)(q+1)+3(g-t)q=(5g-2)q-3tq+2g-2$$

for the number of smooth κ-points outside components belonging to chains. Each such point P gives rise to a *residue disk*, which is the subset of $C(k)$ of points reducing to P; these subsets are analytically isomorphic to open p-adic disks in k.

Now consider a chain in the special fiber $\mathcal{C}_s$. Its two ends each meet some other component of multiplicity 1 transversally. Contracting the components in the chain, we obtain another model $\mathcal{C}'$ of C such that the image of the chain in $\mathcal{C}'_s$ is a simple double point Q. (We consider only chains containing a component defined over κ. If the action of Frobenius reverses the orientation of the chain, we replace k by its unramified extension of degree 2, so that the Frobenius action is trivial. Since the bound we will obtain for the number of relevant points in the residue annulus of Q does not depend on q and so is valid even for k^{unr}-points, we do not lose anything in this way.) By [BL85, Proposition 2.3], the preimage of Q in $C(k)$ under the reduction map is analytically isomorphic to an open annulus of the form $\{x:\alpha<|x|<1\}$ with $\alpha=|\xi|$ for some $\xi\in k$. The number of such annuli equals the number of chains (defined over κ) and so is bounded according to Theorem 3.4 by $2g-3+t$.

Summarizing the discussion above, we have shown:

Proposition 4.1. *Let C be a smooth projective geometrically integral curve over k of genus g. Then there is a number $0\le t\le g$ such that $C(k)$ can be written as a disjoint union of at most $(5g-2)q-3tq+2g-2$ open (residue) disks and at most $2g-3+t$ open (residue) annuli.*

Let $C_D(k)$ be the union of the disks and $C_A(k)$ the union of the annuli in this partition.

5. The pull-back of an abelian logarithm to an annulus

We fix a basepoint $P_0\in C(k)$; this gives rise to the k-defined embedding $i\colon C\to J$, $P\mapsto[P-P_0]$. Let ω be a regular differential on C and denote by ω_J the corresponding regular and invariant 1-form on J (so that $\omega=i^*\omega_J$). We write for $P\in C(k)$

$$\lambda_\omega(P)=\oint_{P_0}^{P}\omega=\oint_{O}^{[P-P_0]}\omega_J=\langle\omega_J,\log[P-P_0]\rangle\,.$$

Let $D_0=\{\xi:|\xi|<1\}$ be the unit disk. If $\varphi\colon D_0\to C$ parametrizes a residue disk, then

$$\varphi^*\omega=w(z)\,dz$$

with a power series $w(z)$ converging on D_0. Let ℓ be a power series whose derivative is w. Then it is well-known that for $\xi_0,\xi_1\in D_0(k)$ we have

$$\oint_{\varphi(\xi_0)}^{\varphi(\xi_1)}\omega=\int_{\xi_0}^{\xi_1}w(z)\,dz=\ell(\xi_1)-\ell(\xi_0)\,.$$

Using Newton polygons, one then shows (see for example [Sto06, Section 6]) that the number of zeros of λ_ω on $\varphi(D_0(k))$ (or even $\varphi(D_0(k^{\mathrm{unr}}))$) is bounded by 1 plus the number n of zeros

of ω (counted with multiplicity) on $\varphi(D_0)$ plus a term (denoted by $\delta(v,n)$ in [Sto06]) that depends only on n, p and the ramification index e of k. We write $\Delta_k(s,r)$ for what is denoted $\Delta_v(s,r)$ in [Sto06], namely

$$\Delta_k(s,r) = \max\Big\{\sum_{j=1}^{s} \delta(v,m_j) : m_j \geq 0, \sum_{j=1}^{s} m_j \leq r\Big\}.$$

Then we have the following bound.

Lemma 5.1. *Let $V \neq 0$ be a linear subspace of the space of regular differentials on C of codimension r and let N_D denote the number of residue disks whose union is $C_D(k)$. Then the functions λ_ω for $\omega \in V$ have at most*

$$N_D + 2r + \Delta_k(N_D, 2r)$$

common zeros in $C_D(k)$. If $p > e+1$, then we can take the bound to be

$$N_D + 2r + e\Big\lfloor \frac{2r}{p-e-1} \Big\rfloor \leq (5g-2)q - 3tq + 2g - 2 + 2r + e\Big\lfloor \frac{2r}{p-e-1} \Big\rfloor .$$

Proof. This is essentially [Sto06, Theorem 6.6]. The bound for Δ_k is [Sto06, Lemma 6.2], and the bound for N_D comes from Proposition 4.1. □

Now we consider the situation for an annulus $A = \{\xi : \rho_1 < v(\xi) < \rho_2\}$ parametrizing the preimage under reduction of a chain in $\mathcal{C}_s$. Let $\varphi\colon A \to C$ be the parametrization. Pulling back ω, we obtain, using z as the coordinate on A,

$$\varphi^*\omega = w(z)\,dz = d\ell(z) + c(\omega)\frac{dz}{z}$$

for Laurent series w and ℓ converging on A and some constant $c(\omega) \in k$. Let Log_0 denote the branch of the p-adic logarithm that takes the value 0 at p. Then, given this choice, there is a unique global integral on A that in our is case given by

$$\int_{\xi_0}^{\xi_1} \varphi^*\omega = \big(\ell(\xi_1) + c(\omega)\,\mathrm{Log}_0(\xi_1)\big) - \big(\ell(\xi_0) + c(\omega)\,\mathrm{Log}_0(\xi_0)\big).$$

We want to compare this with

$$\oint_{\varphi(\xi_0)}^{\varphi(\xi_1)} \omega\,.$$

Perhaps surprisingly, these two integrals can differ.

The following result is crucial. It was first suggested by numerical computations and appears to be new. When we asked Amnon Besser about this, we learned that a related result also is part of current work of his with Sarah Zerbes. To make this paper independent of (so far) unpublished work, a (different) proof is presented here.

Proposition 5.2. *Let ω, A and $\varphi\colon A \to C$ be as above, and write*

$$\varphi^*\omega = d\ell(z) + c(\omega)\frac{dz}{z}\,.$$

Then there is a constant $a(\omega)$ depending linearly on ω such that for $\xi_0, \xi_1 \in A(k)$ we have

$$\oint_{\varphi(\xi_0)}^{\varphi(\xi_1)} \omega = \big(\ell(\xi_1) + c(\omega)\operatorname{Log}_0(\xi_1) + a(\omega)v(\xi_1)\big) - \big(\ell(\xi_0) + c(\omega)\operatorname{Log}_0(\xi_0) + a(\omega)v(\xi_0)\big)$$
$$= \int_{\xi_0}^{\xi_1} \varphi^*\omega + a(\omega)\big(v(\xi_1) - v(\xi_0)\big)\,.$$

Proof. We assume without loss of generality that $1 \in A$. Let $i\colon C \to J$ be the embedding sending $\varphi(1)$ to O.

According to [BL84, Proposition 6.3], the analytic map $i \circ \varphi\colon A \to J$ can be written uniquely as

$$i(\varphi(\xi)) = \psi_1(j(\xi)) + \psi_2(\xi)$$

where $j\colon A \to \mathbb{G}_{\mathrm{m}}$ is the natural inclusion, $\psi_1\colon \mathbb{G}_{\mathrm{m}} \to J$ is an analytic group homomorphism and $\psi_2\colon A \to U$ is an analytic map, where U denotes the formal fiber of the origin on J (so that $U(k)$ is the subgroup of points reducing to the origin). We write ω_J for the 1-form on J such that $i^*\omega_J = \omega$; ω_J is translation invariant. On U, ω_J is exact, so $\omega_J = d\lambda$ for some analytic function λ on U; we can assume $\lambda(0) = 0$. The pull-back $\psi_1^*\omega_J$ is a translation invariant differential on $\mathbb{G}_{\mathrm{m}}$, so it has the form $c\,dz/z$ for some $c \in k$. The pull-back $\psi_2^*\omega_J$ is $\psi_2^* d\lambda = d(\lambda \circ \psi_2)$. Since

$$\varphi^*\omega = \varphi^* i^*\omega_J = \psi_1^*\omega_J + \psi_2^*\omega_J = c\frac{dz}{z} + d\lambda\big(\psi_2(z)\big)\,,$$

we see that $\ell(z) = \lambda(\psi_2(z))$ (up to a constant) and $c = c(\omega)$. Fix $\xi \in A(k)$. We obtain on the one side that

$$\oint_{\varphi(1)}^{\varphi(\xi)} \omega = \oint_O^{i(\varphi(\xi))} \omega_J = \oint_O^{\psi_1(\xi)+\psi_2(\xi)} \omega_J = \oint_O^{\psi_1(\xi)} \omega_J + \oint_O^{\psi_2(\xi)} d\lambda = \oint_O^{\psi_1(\xi)} \omega_J + \lambda\big(\psi_2(\xi)\big)$$

and on the other side that

$$\int_1^{\xi} \varphi^*\omega = \int_1^{\xi} \Big(d\ell(z) + c\frac{dz}{z}\Big) = \ell(\xi) - \ell(1) + c\operatorname{Log}_0(\xi) = \lambda\big(\psi_2(\xi)\big) + c\operatorname{Log}_0(\xi)\,.$$

So the difference is

$$\delta(\xi) = \oint_{\varphi(1)}^{\varphi(\xi)} \omega - \int_1^{\xi} \varphi^*\omega = \oint_O^{\psi_1(\xi)} \omega_J - c\operatorname{Log}_0(\xi)\,.$$

Since ψ_1 is a group homomorphism, the first term in the last difference is a homomorphism $k^\times \to k$; the same is true for the second term. Both terms agree on the residue disk U_1 of 1, since they are given by the same formal integral on U_1. Since $\mathcal{O}^\times/U_1$ is torsion and the target group k is torsion-free, we have $\delta = 0$ on $\mathcal{O}^\times$. This implies that $\delta(\xi)$ is a linear function of the valuation $v(\xi)$, so there is $a = a(\omega) \in k$ such that $\delta(\xi) = av(\xi)$. This gives the claim for $(\xi_0, \xi_1) = (1, \xi)$; by taking differences the more general statement follows.

That $a(\omega)$ is linear in ω is clear, since ℓ (if we set $\ell_0 = 0$), $c(\omega)$ and the left-hand side are. □

Remark 5.3. The numerical example mentioned above shows that it is possible to have $a(\omega) \neq 0$ and $c(\omega) = 0$, so that the appearance of $a(\omega)$ cannot in all cases be avoided by choosing a suitable branch of the p-adic logarithm.

In this situation we have $\psi_1^*\omega_J = 0$ and the difference term above is given by $\oint_O^{\psi_1(\xi)} \omega_J$. Even though the pull-back of ω_J along ψ_1 vanishes, it does not follow that the abelian integral vanishes on the image of ψ_1. Consider for example $\xi = p$ and $P = \psi_1(p) \in J(k)$. There is a positive integer n such that $nP \in U$; then

$$\oint_O^{\psi_1(p)} \omega_J = \frac{1}{n} \oint_O^{nP} \omega_J = \frac{1}{n} \lambda(nP)\,.$$

There is no reason to assume that $\log_J(nP)$ is parallel to the derivative of ψ_1 at 1, so $\psi_1^*\omega_J = 0$ does not in general imply that $\lambda(nP)$ vanishes.

We say that ω is *good* for the subset of $C(k)$ parametrized by A if both $c(\omega)$ and $a(\omega)$ in Proposition 5.2 vanish. This is a linear condition on ω of codimension at most two.

Recall that we fix some $P_0 \in C(k)$ and set

$$\lambda_\omega \colon C(k) \longrightarrow k, \qquad P \longmapsto \oint_{P_0}^{P} \omega\,.$$

Proposition 5.4. *In the situation of Proposition 5.2 assume that $V \neq 0$ is a linear subspace of the space of regular differentials on C of codimension $r \geq 1$ and such that all elements of V are good. Assume further that C is hyperelliptic and that p is odd. Then the number of zeros of λ_ω on $\varphi(A(k^{\mathrm{unr}}))$ is bounded by a number $B_A(p,e,r)$ that depends only on r, p and the ramification index e of k. If $p > e+1$, then we can take $B_A(p,e,r) = 2r + e\lfloor 2r/(p-e-1)\rfloor$.*

Proof. We first indicate how to show the claim under the following additional assumption. Write $\varphi^*\omega = w(z)\,dz$, which by assumption has no z^{-1} term. Then $w(z) = u(z)h(z)$ with a Laurent polynomial u and a Laurent series h such that $|h(\xi) - 1| < 1$ for all $\xi \in A$. We assume that for some $0 \neq \omega \in V$ the terms in u have exponents between n_1 and n_2 such that $n_1 < -1 < n_2$ and $n_2 - n_1 \leq 2r$. Given this, the proof can be carried out using Newton polygons in essentially the same way as for power series.

Now one can check by an explicit computation that this condition is satisfied when C is a hyperelliptic curve and p is odd. A proof is given in Lemma 8.1 below (where $m = g-r$). □

Corollary 5.5. *Let V be a linear subspace of the space of regular differentials on C of codimension $r \leq g-3$, where C is as in Proposition 5.4. Then the number of common zeros of all λ_ω for $\omega \in V$ in $C_A(k)$ is bounded by*

$$(2g - 3 + t)B_A(p, e, r+2)\,,$$

which for $p > e+1$ is at most

$$(2g - 3 + t)\big(2(r+2) + e\Big\lfloor \frac{2(r+2)}{p-e-1} \Big\rfloor\big)\,.$$

Proof. For each annulus A occurring in $C_A(k)$, we let V_A be the subspace of V consisting of differentials that are good for A. Then V_A has codimension at most $r+2 < g$, and by Proposition 5.4 the number of common zeros of λ_ω on A for $\omega \in V_A$ is at most $B_A(p,e,r+2)$. We multiply by the bound $2g-3+t$ for the number of annuli from Proposition 4.1 to obtain the result. □

6. Bounding the number of points mapping into a subgroup of small rank

In this section we state and prove our main result.

Theorem 6.1. *Let k be a p-adic field with p odd and write e for the ramification index of k and q for the size of its residue field. Let $g \geq 3$ and $0 \leq r \leq g-3$. Then there is a bound $N(k,g,r)$ depending only on k, g and r such that the following holds.*

Let $C\colon y^2 = f(x)$ be a hyperelliptic curve of genus g over k. We denote by J the Jacobian variety of C. Let $\Gamma \subset J(k)$ be a subgroup of rank r. Let $i\colon C \to J$ be an embedding given by choosing some basepoint $P_0 \in C(k)$. Then

$$\#\{P \in C(k) : i(P) \in \Gamma\} \leq N(k,g,r)\,.$$

If $p > e+1$, then we can take

$$\begin{aligned} N(k,g,r) &= (5g-2)q + 2g - 2 + 2r + e\Big\lfloor \frac{2r}{p-e-1}\Big\rfloor + (2g-3)\Big(2r+4+e\Big\lfloor\frac{2(r+2)}{p-e-1}\Big\rfloor\Big) \\ &\qquad + g\max\Big\{0, 2r+4+e\Big\lfloor\frac{2(r+2)}{p-e-1}\Big\rfloor - 3q\Big\} \\ &\ll g\big(q + e(r+1)\big)\,. \end{aligned}$$

Proof. The rank condition implies that there is a k-vector space V of regular differentials on C of codimension $\leq r \leq g-3$ and such that each $\omega \in V$ annihilates Γ under the Chabauty-Coleman pairing. This means that (taking P_0 to be the basepoint for λ_ω) the set of points in question is contained in the common zero set of all λ_ω for $\omega \in V$. We can then use Lemma 5.1 and Corollary 5.5 to bound the number of points in $C_D(k)$ and in $C_A(k)$, respectively, that map to Γ. Adding these bounds and maximizing over $0 \leq t \leq g$ gives the result. □

Remark 6.2. It is conceivable that a more careful analysis of the functions λ_ω on annuli will result in a bound for the number of zeros that applies to differentials ω that do not necessarily satisfy the conditions that $c(\omega)$ and/or $a(\omega)$ (in the notation of Proposition 5.2) vanish. If this is indeed the case, then the condition $r \leq g-3$ can be relaxed to $r \leq g-2$ or even $r \leq g-1$. This will be the subject of future work.

7. A uniform bound on the number of rational points

We can apply the result of the previous section to obtain bounds for the number of rational points on hyperelliptic curves with small Mordell-Weil rank relative to the genus.

Theorem 7.1. *Let $g \geq 3$, $d \geq 1$ and $0 \leq r \leq g-3$. Then there is a bound $R(d,g,r)$ depending only on d, g and r such that for any hyperelliptic curve C of genus g over a number field K of degree at most d such that the Mordell-Weil rank of its Jacobian is r, we have $\#C(K) \leq R(d,g,r)$.*

For $d = 1$ (hence $K = \mathbb{Q}$), we can take

$$R(1,g,r) = 8(r+4)(g-1) + \max\{1, 4r\}\cdot g\,.$$

Proof. Fix some odd prime p. Then there are only finitely many possible completions k at places above p of number fields of degree $\le d$. We take $R(d,g,r)$ to be the maximum of the bounds $N(k,g,r)$ of Theorem 6.1 over all these k.

Let C be a curve as in the statement. If $C(K) = \emptyset$, there is nothing to prove. So we can assume that there is some $P_0 \in C(K)$, which we use as basepoint for an embedding $i\colon C \to J$. We can then apply Theorem 6.1 to C base-changed to a completion k of K at a place above p and to $\Gamma = J(K) \subset J(k)$.

To obtain the bound for $d = 1$, we take $k = \mathbb{Q}_3$ (with $p = 3 > 2 = e+1$ and $q = p = 3$). □

Remark 7.2. Using the bound in Theorem 6.1 when $p > e+1$, we obtain the estimate

$$R(d,g,r) \ll g\big(p^d + d(r+1)\big) \ll g\big((2d)^d + d(r+1)\big)$$

where p is the smallest prime $> d+1$. (The worst case is when K is totally ramified at all primes $\le d+1$ and inert at all reasonably small primes $> d+1$.)

Taking $r = 0$, we obtain the following.

Corollary 7.3. *Let C be a hyperelliptic curve of genus $g \ge 3$ over $\mathbb{Q}$. Then any torsion packet on C can contain at most $33g - 32$ rational points.*

If we write $T(g)$ for the maximal number of rational points in a torsion packet on a hyperelliptic curve of genus g over $\mathbb{Q}$, then this gives

$$2 \le \liminf_{g\to\infty} \frac{T(g)}{g} \le \limsup_{g\to\infty} \frac{T(g)}{g} \le 33$$

(the leftmost inequality is obtained by considering curves with all $2g+2$ Weierstrass points rational). So we know that the growth rate of $T(g)$ is linear!

8. Explicit results for hyperelliptic curves

In this section, we show that the assumption we needed for the proof of Proposition 5.4 holds in the case of hyperelliptic curves over a p-adic field with p odd.

Lemma 8.1. *Let k be a p-adic field with p odd, and let C be a hyperelliptic curve over k of genus g. Consider a maximal chain in the special fiber of the minimal regular model $\mathcal{C}$ of C over $\mathcal{O}$. Then there is a k-defined annulus $A = \{\xi : \rho_1 < |\xi| < \rho_2\}$ and an analytic embedding $\varphi\colon A \to C$ (possibly defined over the unramified quadratic extension of k) such that the following holds.*

Let $V \subset \Omega^1_C$ be a linear subspace of dimension $m \ge 1$ of the space of regular differentials on C such that $c(\omega) = a(\omega) = 0$ for all $\omega \in V$ in the notation of Proposition 5.2. Then there is some $0 \ne \omega \in V$ such that $\varphi^*\omega = u(z)h(z)\,dz$ with a Laurent series h satisfying $|h(\xi) - 1| < 1$ on A and a Laurent polynomial u with the property that all its terms have exponents between n_1 and n_2 where $n_1 < -1 < n_2$ and $n_2 - n_1 \le \max\{2(g-m), 2\}$.

Proof. We write $\pi\colon C \to \mathbb{P}^1$ for the hyperelliptic double cover. We already know that there is a k-defined annulus A parametrizing the preimage of the chain under reduction. We want to give an explicit construction of A and the map φ. To this end, we consider the action

of the hyperelliptic involution ι of C on A and on the corresponding chain in $\mathcal{C}_s$. There are three possibilities:

a) The *odd case.* ι fixes the chain component-wise. Then ι acts on A preserving the valuation (which is determined by the component of the chain the point under consideration maps to). Then the image $A' = \pi(\varphi(A))$ in $\mathbb{P}^1$ is an annulus not containing any branch points of π; this annulus separates the set of branch points into two subsets of odd cardinality ≥ 3.
b) The *even case.* ι interchanges the chain with another (disjoint) chain. Then the image $A' = \pi(\varphi(A))$ in $\mathbb{P}^1$ is an annulus isomorphic to A that does not contain any branch points of π and separates the branch points into two subsets of even cardinality ≥ 4.
c) The *Weierstrass case.* ι fixes the chain but reverses its orientation. Then ι acts on A interchanging the 'inner' and 'outer' boundaries. The image $A' = \pi(\varphi(A))$ in $\mathbb{P}^1$ is a disk containing exactly two branch points of π.

Note that if one of the subsets of branch points in the odd or even cases would have at most one element, then the annulus in $\mathbb{P}^1$ would be contained in a k-defined disk containing at most one branch point, which would give rise to either one (Weierstrass) point (odd case) or a pair of points (even case) in $\mathcal{C}_s^{\mathrm{smooth}}(\kappa)$, contradicting the assumption that the annulus comes from a chain. In the even case with two branch points in the 'interior' of A' (say), 'filling in' the annulus A' would result in a disk containing two branch points. This would correspond to a chain of type c) containing the chain considered, contradicting its maximality.

We write $\Theta \subset \mathbb{P}^1$ for the set of branch points. In the odd and even cases, we can assume without loss of generality that $0, \infty \notin A'$ and $\infty \notin \Theta$. Then

$$A' = \{\xi : \rho_1' < |\xi| < \rho_2'\} \subset \mathbb{A}^1 \subset \mathbb{P}^1 .$$

We write Θ_0 and Θ_∞ for the two subsets of Θ defined by A', where Θ_0 contains the branch points in the 'interior' of A' (i.e., such that $|\theta| \leq \rho_1'$) and Θ_∞ those in the 'exterior' of A' (such that $|\theta| \geq \rho_2'$).

We assume that C is given by the affine equation $y^2 = f(x)$ (with $f \in k[x]$ squqarefree of degree $2g+2$, since $\infty \notin \Theta$). Let c be the leading coefficient of f, so that

$$f(x) = c \prod_{\theta \in \Theta} (x - \theta) .$$

We can then write

$$\begin{aligned} f(x) &= c \prod_{\theta \in \Theta_\infty} (x - \theta) \prod_{\theta \in \Theta_0} (x - \theta) \\ &= c \prod_{\theta \in \Theta_\infty} (-\theta) \cdot x^{\#\Theta_0} \prod_{\theta \in \Theta_\infty} \left(1 - \frac{x}{\theta}\right) \prod_{\theta \in \Theta_0} \left(1 - \frac{\theta}{x}\right) . \end{aligned}$$

Each factor $1 - \theta/x$ or $1 - x/\theta$ can be written as the square of a Laurent series that converges on A', so that

$$f(x) = \gamma x^{\#\Theta_0} \tilde{h}(x)^2$$

for some Laurent series $\tilde{h}$ converging on A', where $\gamma = c \prod_{\theta \in \Theta_\infty} (-\theta) \in k^\times$ and $|\tilde{h}(\xi) - 1| < 1$ for all $\xi \in A'$.

a) In the odd case with $\#\Theta_0 = 2\nu + 1$, say (with $1 \le \nu \le g-1$), we can take

$$A = \{\tau : \gamma\tau^2 \in A'\};$$

and

$$\varphi\colon A \longrightarrow C, \quad \tau \longmapsto \big(\gamma\tau^2, \gamma^{\nu+1}\tau^{2\nu+1}\tilde{h}(\gamma\tau^2)\big);$$

note that φ is equivariant with respect to $\tau \mapsto -\tau$ on the left and ι on the right.

b) In the even case we write $\#\Theta_0 = 2\nu$ (with $2 \le \nu \le g-1$) and we let $\alpha \in k^\times$ denote a suitable square root of γ. (Note that γ must be a square in this case.) Taking $A = A'$, we have

$$\varphi\colon A \longrightarrow C, \quad \tau \longmapsto \big(\tau, \alpha\tau^\nu\tilde{h}(\tau)\big).$$

c) In the Weierstrass case, write $A' \cap \Theta = \{\theta_1, \theta_2\}$. Without loss of generality, we can assume that $A' = \{\xi : |\xi| < 1\}$. In a similar way as above, we can write

$$f(x) = \gamma\tilde{h}(x)^2(x-\theta_1)(x-\theta_2)$$

with a power series $\tilde{h}$ converging on A' such that $|\tilde{h}(\xi) - 1| < 1$ for $\xi \in A'$. We can in addition assume that $\theta_2 = -\theta_1$, so that $(x-\theta_1)(x-\theta_2) = x^2 - a$ for some $a \in k^\times$. One can check that the valuation of γ must be even if the situation comes from a chain in $\mathcal{C}_s$ (otherwise the relevant part of $\mathcal{C}_s$ consists of a sequence of (-2)-curves of multiplicity 2, with two $\mathbb{A}^1$-components attached to the last of these). Let $k' = k(\sqrt{\gamma})$ and let $\alpha \in k'$ be a square root of γ; then k' is a (possibly trivial) unramified extension of k. Setting $y = \alpha\tilde{h}(x)\tilde{y}$, the equation of C becomes $\tilde{y}^2 = x^2 - a$. This can be parametrized by setting $t = x + \tilde{y}$, so that

$$x = \frac{1}{2}\Big(t + \frac{a}{t}\Big) \quad \text{and} \quad \tilde{y} = \frac{1}{2}\Big(t - \frac{a}{t}\Big), \quad \text{so} \quad y = \frac{\alpha}{2}\Big(t - \frac{a}{t}\Big)\tilde{h}\Big(\frac{1}{2}\Big(t + \frac{a}{t}\Big)\Big).$$

Taking $A = \{\tau : |a| < |\tau| < 1\}$ (this is an annulus defined over k), the map $\tau \mapsto \frac{1}{2}(\tau + a/\tau)$ gives a double cover $A \to A'$ branched at θ_1 and θ_2. This implies that $\tilde{h}\big(\frac{1}{2}(t + a/t)\big)$ converges on A with values close to 1; we obtain an analytic embedding $\varphi\colon A \to C$. We note that $t \mapsto a/t$ fixes x and changes the sign of y, so it corresponds to the hyperelliptic involution on the image of φ.

Now we consider a regular differential ω on C. It can be written in the form

$$\omega = \tilde{u}(x)\,\frac{dx}{2y}$$

with a polynomial $\tilde{u}$ of degree at most $g-1$. This leads to $\varphi^*\omega = u(t)h(t)\,dt$ with a Laurent series $h(t)$ such that $|h(\tau) - 1| < 1$ on A and a Laurent polynomial u given by

$$\text{a)}\ \frac{\tilde{u}(\gamma t^2)}{(\gamma t^2)^\nu}, \qquad \text{b)}\ \frac{\tilde{u}(t)}{2\alpha t^\nu}, \qquad \text{or} \qquad \text{c)}\ \frac{\tilde{u}(t + at^{-1})}{2\alpha t}.$$

Since we are free to impose up to $m-1$ linear conditions on ω, we can arrange for the terms in $\tilde{u}$ to have exponents in any interval of length $g-m$ containing ν in cases a) and b), or in the interval $[0, g-m]$ in case c). Writing ν_1 and ν_2 for the minimal and maximal degree of a term in u, we can therefore arrange in all cases to have $\nu_1 \ge n_1$, $\nu_2 \le n_2$ such that $n_2 - n_1 = \max\{2(g-m), 2\}$ and $n_1 < -1 < n_2$. This proves the claim. □

References

[AW71] M. Artin and G. Winters, *Degenerate fibres and stable reduction of curves*, Topology **10** (1971), 373–383. MR0476756 (57 #16313) ↑3, 3

[Bos80] Siegfried Bosch, *Formelle Standardmodelle hyperelliptischer Kurven*, Math. Ann. **251** (1980), no. 1, 19–42, DOI 10.1007/BF01420278 (German). MR583822 (82b:14018) ↑

[BL85] Siegfried Bosch and Werner Lütkebohmert, *Stable reduction and uniformization of abelian varieties. I*, Math. Ann. **270** (1985), no. 3, 349–379, DOI 10.1007/BF01473432. MR774362 (86j:14040a) ↑4

[BL84] ———, *Stable reduction and uniformization of abelian varieties. II*, Invent. Math. **78** (1984), no. 2, 257–297, DOI 10.1007/BF01388596. MR767194 (86j:14040b) ↑5

[Bui93] Alexandru Buium, *Effective bound for the geometric Lang conjecture*, Duke Math. J. **71** (1993), no. 2, 475–499, DOI 10.1215/S0012-7094-93-07120-7. MR1233446 (95c:14055) ↑1

[BV96] Alexandru Buium and José Felipe Voloch, *Lang's conjecture in characteristic p: an explicit bound*, Compositio Math. **103** (1996), no. 1, 1–6. MR1404995 (98a:14038) ↑1

[CHM97] Lucia Caporaso, Joe Harris, and Barry Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35, DOI 10.1090/S0894-0347-97-00195-1. MR1325796 (97d:14033) ↑1

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885 (French). MR0004484 (3,14d) ↑1

[Col85] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. MR808103 (87f:11043) ↑1

[CUV12] Ricardo Conceição, Douglas Ulmer, and José Felipe Voloch, *Unboundedness of the number of rational points on curves over function fields*, New York J. Math. **18** (2012), 291–293. MR2928577 ↑1

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366 (German). Erratum in: Invent. Math. **75** (1984), 381. MR718935 (85g:11026a) ↑1

[Fal94] Gerd Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 175–182. MR1307396 (95m:11061) ↑1

[KZB13] Eric Katz and David Zureick-Brown, *The Chabauty–Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions*, January 25, 2013. Preprint, `arXiv:1204.3335v3`. ↑1

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné; Oxford Science Publications. MR1917232 (2003g:14001) ↑3

[Maz86] Barry Mazur, *Arithmetic on curves*, Bull. Amer. Math. Soc. (N.S.) **14** (1986), no. 2, 207–259, DOI 10.1090/S0273-0979-1986-15430-3. MR828821 (88e:11050) ↑1

[MP13] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Panoramas et Synthèses, vol. 36, Société Math. de France, 2013. ↑1

[PS13] Bjorn Poonen and Michael Stoll, *Most odd degree hyperelliptic curves have only one rational point*, May 21, 2013. Preprint, `arXiv:1302.0061v2`. ↑1

[Sto06] Michael Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR2264661 ↑1, 5, 5

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

E-mail address: `Michael.Stoll@uni-bayreuth.de`

URL: `http://www.computeralgebra.uni-bayreuth.de`