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, r 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 $8rg+33(g-1)+1$.

The proof is based on Chabauty's method; the new ingredient is an estimate for the number of zeros of an abelian logarithm on 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).

We also show, strengthening a recent result by Poonen and the author, that the lower density of hyperelliptic curves of odd degree over $\mathbb{Q}$ whose only rational point is the point at infinity tends to 1 uniformly over families defined by congruence conditions, as the genus g tends to infinity.

1. Introduction

Since Faltings' proof [Fal83] of Mordell's conjecture, we know that a curve of genus $g\geq 2$ over a number field K can have only finitely many K-rational points. This raises the question whether there might be uniform bounds of some sort on the number of K-rational points. Caporaso, Harris and Mazur [CHM97] have shown that the validity of the weak Lang conjecture on rational points on varieties of general type would imply the existence of a bound depending only on the genus g and the field K. Pacelli [Pac97] has, under the same assumption, shown the existence of a bound depending only on g and the degree of K. (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 K-rational points on the curve with the intersection of the curve and the Mordell-Weil group, one can formulate the following purely geometric statement (Mazur [Maz86, end of Section III.2] asks it as a question):

Conjecture 1.1 (Uniform Mordell-Lang for curves)**.** Given $g\geq 2$ and $r\geq 0$, there is a constant $N(g,r)$ such that for any curve C over $\mathbb{C}$ of genus g with an embedding $i\colon C\to J$ into its Jacobian and for any subgroup $\Gamma\subset J(\mathbb{C})$ of rank r, one has $\#i^{-1}(\Gamma)\leq N(g,r)$.

That this number is finite for each individual curve and subgroup follows from further work by Faltings [Fal94]. Heuristic arguments suggest that such a uniform bound should exist. The existence of such bounds has been shown for k a *function field* of characteristic zero if C is not defined over the algebraic numbers by Buium [Bui93] (and also for function fields

Date: November 25, 2015.

in characteristic p by Buium and Voloch [BV96]). In Section 2 below, we will show that Conjecture 1.1 is implied by (a special case of) the Zilber-Pink conjecture; this implication can be seen as making precise the 'heuristic arguments' alluded to above.

A weaker variant of Conjecture 1.1, turning the geometric statement into an arithmetic one, is the following.

Conjecture 1.2. Given $d \geq 1$, $g \geq 2$ and $r \geq 0$, there is a constant $R(d, g, r)$ such that for any number field K of degree d and any curve C over K of genus g with Jacobian J such that $\operatorname{rank} J(K) = r$, we have $\#C(K) \leq R(d, g, r)$.

This is formulated as a question again by Mazur in [Maz00, page 223] (allowing the constant to depend on K, not just on the degree d).

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. More generally, we can show that on a hyperelliptic curve C of genus g over a number field of degree $\leq d$, there can be at most $R(d, g, r)$ 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 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 9.1 and Corollary 9.4 below. In particular, this proves Conjecture 1.2 for hyperelliptic curves when $r \leq g - 3$.

The proof is based on Chabauty's method [Cha41, Col85, MP12, Sto06], whose 'classical' version we now sketch. 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 3)

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

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 linear 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 parameterize 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'. Such an annulus arises as the set of p-adic points on C reducing to an ordinary double point on the special fiber of a suitable (not necessarily regular) model of the curve, which is obtained by contracting the chain. We can then obtain a bound for the number of points in that subset that is independent of the number of residue disks it contains. Since both the number of such annuli and the number of remaining residue disks are bounded in terms of the genus (and p), see Theorem 4.1, 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 7.3, 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. Our method does in fact generalize to arbitrary curves as demonstrated by recent work of Katz, Rabinoff and Zureick-Brown [KRZB15].

For the convenience of the reader, we give an overview of the proof of the main result, which we state here in simplified form.

Theorem 1.3 (Theorem 8.1)**.** *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 $0 \leq r \leq g-3$. We assume that $p > e+1$.*

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

$$\#\{P \in C(k) : i(P) \in \Gamma\} = O\big((e(r+1)+q)g\big)\,.$$

Applying (a precise version of) this result for $k = \mathbb{Q}_3$ to a curve over $\mathbb{Q}$ and to $\Gamma = J(\mathbb{Q})$ leads to the following bound for the number of rational points.

Theorem 1.4 (Theorem 9.1 for $d = 1$)**.** *Let $g \geq 3$ and $0 \leq r \leq g-3$. Let C be a hyperelliptic curve of genus g over $\mathbb{Q}$ such that the Mordell-Weil rank of its Jacobian is r. Then*

$$\#C(\mathbb{Q}) \leq 33(g-1)+1 \quad \text{if } r = 0 \qquad \text{and} \qquad \#C(\mathbb{Q}) \leq 8rg + 33(g-1) - 1 \quad \text{if } r \geq 1.$$

The proof of Theorem 1.3 proceeds in the following steps.

1. We show that $C(k)$ can be partitioned into $O(qg)$ disks and $O(g)$ annuli (Proposition 5.3).
2. On the union of the disks, $\#i^{-1}(\Gamma)$ can be bounded by $O(qg+er)$ by the usual Chabauty method (Lemma 7.1).
3. We give a bound of the form $O(e(r+1))$ for $\#i^{-1}(\Gamma)$ on an annulus (Proposition 7.7). This is where we need the stronger condition $r \leq g-3$ compared to the usual Chabauty condition $r \leq g-1$. As already mentioned, the reason behind this is that we want to use a different integral that satisfies the Fundamental Theorem of Calculus on annuli to get the bound. We therefore have to compare this integral with the abelian integral used in the Chabauty-Coleman pairing. The result is that both agree when the differential satisfies two extra linear conditions (Proposition 7.3).
4. Finally, we add the bounds for the disks and the annuli.

The paper is organized as follows. In Section 2, we show that a version of the Zilber-Pink Conjecture implies Conjecture 1.1. This is not essential for the main results of the paper, but gives some idea regarding the kind of bound in terms of g and r one might expect to hold. After a short section introducing notation, we proceed in Section 4 with a discussion of the combinatorics of reduction graphs. If one is only interested in the existence of some bound (as long as $r \leq g-3$), then it suffices to use the result of Artin and Winters [AW71] that gives the existence of bounds in terms of g for the number of chains and '$\mathbb{A}^1$-components'. The precise results given by Theorem 4.1 are only needed to obtain the concrete bounds in the statements of Theorems 8.1 and 9.1. Section 5 uses the main result of Section 4 to give bounds in terms of g for the number of disks and annuli needed to cover the set of p-adic points on C. Section 6 gives an explicit description of the annuli on a hyperelliptic curve when the residue characteristic is odd. Section 7 compares the abelian integral on an annulus with the integral satisfying the Fundamental Theorem of Calculus and deduces a bound on the number of common zeros on an annulus of abelian integrals coming from differentials killing a given subgroup of J under the Chabauty-Coleman pairing. The next two Sections 8 and 9 then combine the results of Sections 5 and 7 to state and prove our main result, Theorem 8.1, and its application to bounds for rational points, Theorem 9.1, and for rational torsion packets, Corollary 9.4. The last section, Section 10, uses the generalization of our results on differentials on annuli due to Katz, Rabinoff and Zureick-Brown to deduce a version of the main result of [PS14] that applies uniformly to families of odd degree hyperelliptic curves that are defined by congruence conditions.

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 [PS14]: could we give a family of odd degree hyperelliptic curves C of arbitrarily high 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 size of the image of $C(\mathbb{Q}_2)$ in $\mathbb{P}^{g-1}(\mathbb{F}_2)$ under the 'ρ log' map of [PS14] is bounded by a polynomial in g. This result (with a quadratic bound) is given in Section 10 below. The idea then extended naturally to the original problem. 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 by now been eliminated from the argument, but see Remark 8.3). Dino Lorenzini was very helpful on the question (discussed in Section 4) 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. The idea for proving that Zilber-Pink implies uniform Mordell-Lang for curves germinated upon hearing a talk by Umberto Zannier at the joint ÖMG and DMV meeting in Innsbruck in September 2013 and took shape while reading his book [Zan12] afterwards. Padmavathi Srinivasan asked some questions that helped improve the argument in the proof of Theorem 4.1. Last, but not least, I would like to thank an anonymous referee for spotting a mistake and for making some valuable suggestions that led to improvements in organizing the arguments in Sections 4 and 6.

2. Zilber-Pink implies uniform Mordell-Lang for curves

In [Pin05, Conjecture 6.1], Pink formulates a more general version of the following conjecture. It is a special case of a conjecture on mixed Shimura varieties that belongs to a circle of ideas usually referred to as the 'Zilber-Pink conjecture(s)'.

Conjecture 2.1 (Pink)**.** Let $\pi\colon A \to B$ be an algebraic family of abelian varieties over $\mathbb{C}$. Consider an irreducible subvariety $X \subset A$ of dimension d such that X is not contained in any proper closed subgroup scheme of A. Then the set of points $x \in X$ that are contained in a subgroup of codimension $> d$ of the fiber $A_{\pi(x)}$ above $\pi(x) \in B$ is not Zariski dense in X.

The idea behind this is that based on the dimensions, one would not expect any intersection between X and a subgroup scheme of codimension $> d$, so intersection points are 'unlikely' and should therefore form a 'sparse' subset of X. See Zannier's book [Zan12] for background information on the subject of 'unlikely intersections'.

(Pink's original version is for families of semi-abelian varieties. However, Bertrand [Ber11, Ber13] gave a counterexample to this more general formulation. It turns out that the semi-abelian version needs to be modified to be compatible with the original conjecture on mixed Shimura varieties.)

In this section we show that Conjecture 2.1 implies Conjecture 1.1. The strategy is similar to that employed by Caporaso, Harris, and Mazur in [CHM97]. Namely, we show that Pink's conjecture implies that if a curve has many points whose differences generate a subgroup of bounded rank in the Jacobian, then the points have algebraic dependencies, similar to what is implied by 'correlation' in the sense of [CHM97] under the weak Lang conjecture. In more or less the same way as in that paper, the result then follows.

Let $\pi\colon \mathcal{C} \to B$ be a smooth family of irreducible curves of genus g over $\mathbb{C}$, with B (say, irreducible) of dimension d. We write $\mathcal{J} \to B$ for the induced family of Jacobians. Fix $r \geq 0$. Given $n > r$, consider the n-th fiber power $\mathcal{C}_B^n \to B$. We denote by ϕ the morphism

$$\mathcal{C}_B^n \longrightarrow \mathcal{J}_B^{n-1}, \qquad (b; P_0, P_1, \dots, P_{n-1}) \longmapsto (b; [P_1 - P_0], \dots, [P_{n-1} - P_0])\,.$$

We claim that the image of ϕ is not contained in a proper subgroup scheme of $\mathcal{J}_B^{n-1}$. Consider a point $b \in B$ and fix a basepoint $P_0 \in \mathcal{C}_b$. Since the image of $\mathcal{C}_b$ in $\mathcal{J}_b$ under the embedding

$P \mapsto [P - P_0]$ spans $\mathcal{J}_b$ as a group, it follows that the image of $\mathcal{C}_b^n$ in $\mathcal{J}_b^{n-1}$ spans the latter group. In particular, this image cannot be contained in a proper algebraic subgroup of $\mathcal{J}_b^{n-1}$. Since a proper subgroup scheme of $\mathcal{J}_B^{n-1}$ will meet most fibers in a proper subgroup of the fiber, this shows that $\phi(\mathcal{C}_B^n)$ cannot be contained in a proper subgroup scheme of $\mathcal{J}_B^{n-1}$.

If the subgroup of the Jacobian generated by the point differences has rank at most r, then there are $n-1-r$ independent relations of the form

$$a_{i1}[P_1 - P_0] + a_{i2}[P_2 - P_0] + \ldots + a_{i,n-1}[P_{n-1} - P_0] = 0$$

with integers a_{ij}. For points $(b; Q_1, \ldots, Q_{n-1}) \in \mathcal{J}_B^{n-1}$, the relations

$$a_{i1}Q_1 + a_{i2}Q_2 + \ldots + a_{i,n-1}Q_{n-1} = 0$$

then define a subgroup scheme of $\mathcal{J}_B^{n-1}$ containing $\phi(b; P_0, P_1, \ldots, P_{n-1})$ and of codimension $(n-1-r)g$. The dimension of the image of ϕ is at most $\dim \mathcal{C}_B^n = d+n$. So the codimension is greater than this dimension whenever

$$n > \frac{d+g}{g-1} + \frac{g}{g-1}r\,. \tag{2.1}$$

We conclude:

Lemma 2.2. *Assume Conjecture 2.1. If d, g, r and n satisfy (2.1), then the set of points in $\mathcal{C}_B^n$ such that the differences lie in a subgroup of rank $\leq r$ is not Zariski dense.*

Now we mimic the argument given in [CHM97, Section 1.2]. We first prove the following lemma.

Lemma 2.3. *Assume Conjecture 2.1. Let $\pi\colon \mathcal{C} \to B$ be a smooth family of irreducible curves of genus $g \geq 2$ over $\mathbb{C}$. Fix $r \geq 0$. Then there is a bound $N(\pi, r)$ and a proper closed subvariety B' of B such that for all $b \in B(\mathbb{C}) \setminus B'(\mathbb{C})$, and for any choice of strictly more than $N(\pi, r)$ distinct points on the curve $\mathcal{C}_b$, the differences of these points will generate a subgroup of rank strictly greater than r in the Jacobian $\mathcal{J}_b$.*

Proof. Fix some n satisfying (2.1) for the given values of g, r, and $d = \dim B$. Denote by $Z_n \subset \mathcal{C}_B^n$ the Zariski closure of the set of points $(b; P_0, P_1, \ldots, P_{n-1}) \in \mathcal{C}_B^n$ such that the differences of the P_j generate a subgroup of rank $\leq r$. By Lemma 2.2, Z_n is a proper closed subvariety of $\mathcal{C}_B^n$. Now for $1 \leq j \leq n$, we let $\rho_j\colon \mathcal{C}_B^j \to \mathcal{C}_B^{j-1}$ denote the forgetful morphism that leaves out the last point. For $j = n-1, n-2, \ldots, 0$, define successively Z_j as the (closed) subvariety of $\mathcal{C}_B^j$ of points x such that $\rho_{j+1}^{-1}(x) \subset Z_{j+1}$. Since (inductively) Z_{j+1} is a proper closed subvariety of $\mathcal{C}_B^{j+1}$, Z_j is a proper closed subvariety of $\mathcal{C}_B^j$. We let $B' = Z_0 \subset \mathcal{C}_B^0 = B$.

Arguing as in [CHM97, Proof of Lemma 1.1], there are integers d_j such that $\#\rho_j^{-1}(x) \cap Z_j \leq d_j$ for all $x \in \mathcal{C}_B^{j-1} \setminus Z_{j-1}$. We now show by downward induction the following statement.

Let $0 \leq m \leq n$. Then there is $N_m \geq m$ such that for each $(b; P_0, P_1, \ldots, P_{m-1}) \in \mathcal{C}_B^m \setminus Z_m$, whenever we choose $N_m - m + 1$ distinct additional points $P_m, P_{m+1}, \ldots, P_{N_m} \in \mathcal{C}_b$, then the differences of the P_j generate a subgroup of rank $> r$ in $\mathcal{J}_b$.

For $m = n$ we can take $N_n = n$, by definition of Z_n. Now let $m < n$ and assume the claim is true for $m+1$ in place of m. Let $x = (b; P_0, P_1, \ldots, P_{m-1}) \in \mathcal{C}_B^m \setminus Z_m$, then there are at most d_{m+1} points in Z_{m+1} mapping to x. By the inductive assumption, if we choose

points $P_m, \dots, P_{N_{m+1}}$ with P_m not one of the finitely many possibilities leading to a preimage in Z_{m+1}, then the statement is true. In any case, once we take more than d_{m+1} additional (distinct) points, then at least one of them will lead to a preimage outside Z_{m+1}. Since we can permute the additional points, this brings us back to the previous case. We see that we can take $N_m = \max\{N_{m+1}, m + d_{m+1}\}$.

The final case $m = 0$ then gives the statement of the lemma, with

$$N(\pi, r) = N_0 = \max\{m + d_{m+1} : 0 \le m \le n\}$$

(where $d_{n+1} := 0$). □

Now we are almost done.

Theorem 2.4. *Conjecture 2.1 implies Conjecture 1.1.*

Proof. Assume Conjecture 2.1. Fix $g \ge 2$ and $r \ge 0$ and let $\mathcal{C}_0 \to B_0$ be a universal family of smooth curves of genus g. By Lemma 2.3, there is a proper closed subvariety $B_1 \subset B_0$ and a bound N_0 such that the statement of Conjecture 1.1 holds with this bound for all fibers of $\mathcal{C}_0$ above points not in B_1. If $B_1 \neq \emptyset$, we can apply Lemma 2.3 to the restricted family $\mathcal{C}_1 \to B_1$ and obtain a proper closed subvariety $B_2 \subset B_1$ and a bound N_1 valid for all fibers above points outside B_2. We continue this process, which must stop after finitely many steps since B is noetherian. The statement of Conjecture 1.1 then holds with $N(g, r) = \max_j N_j$. □

Remark 2.5. The same argument shows that there is such a uniform bound for any smooth family of curves inside abelian varieties of dimension at least 2 that are generated fiber-wise by the curves.

Note that we can take $\dim B_j \le \dim B_0 = 3g-3$. Looking at (2.1), this implies that it suffices to take $n = 5 + 2r$. So we would expect that except for points occurring systematically in certain families of curves, there should be a bound of the form $\ll r + 1$ for the number of points on a curve mapping into a subgroup of rank r in the Jacobian. For hyperelliptic curves of genus g, taking a Weierstrass point as basepoint, we always have the $2g + 2$ Weierstrass points mapping to points of order 2 (and no other systematically occurring torsion points, see [PS14, Section 7]). Since any generically chosen additional set of r pairs of 'opposite' points on such a curve will generate a subgroup of rank r, we obtain a lower bound of $2g + 2 + 2r \gg g + r$. In [Sto06] we show that for the family of quadratic twists of a fixed hyperelliptic curve (and over any fixed number field K), there is an upper bound of $2g+2+2r$ for the number of K-rational points whenever $r < g$, with at most finitely many exceptions. In this paper, we prove an upper bound $\ll_{[K:\mathbb{Q}]} (r+1)g$ for the set of K-rational points when the curve is hyperelliptic and $r \le g - 3$. It appears possible that the method can be refined to give a bound of the form $\ll_{[K:\mathbb{Q}]} g + r$. This leads to the following question.

Question 2.6. Can we take $R(d, g, r) \ll_d g + r$ in Conjecture 1.2? Can we perhaps even take $N(g, r) \ll g + r$ in Conjecture 1.1?

3. 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 additive valuation on $\mathbb{C}_p$, normalized by $v(p) = 1$. We also fix the absolute value $|x| = p^{-v(x)}$ 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 map $J(k) \to T_O J(k) \cong k^g$. 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 $(T_O J(k))^*$ of J at the origin. This induces a pairing

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

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 integral $\int$ given by p-adic integration theory. This distinction will be relevant in Section 7.

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

4. Combinatorics of arithmetic graphs

In this section, we study 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, Sections 9 and 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, writing as usual $p_a(\Gamma)$ for the arithmetic genus of Γ,

$$\Gamma \cdot W = 2p_a(\Gamma) - 2 - \Gamma^2 \,. \tag{4.1}$$

By [Liu02, Corollary 9.3.26], $g \geq 2$ implies that $\Gamma \cdot W \geq 0$. So 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

$$2g - 2 = \mathcal{C}_s \cdot W = \sum_{\Gamma} m(\Gamma)(\Gamma \cdot W)\,, \tag{4.2}$$

which implies that there can be at most $2g-2$ components Γ having $\Gamma \cdot W > 0$, with components counted according to multiplicity. 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 $p_a(\Gamma)$. We call G the *arithmetic graph* associated to $\mathcal{C}$. This data is equivalent to what is called a 'type' in [AW71] or [Liu02, Definition 10.1.55]. The intersection pairing satisfies

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

Using the adjunction formula (4.1), we can write this as

$$\sum_{\Gamma' \neq \Gamma} m(\Gamma')\Gamma \cdot \Gamma' = -m(\Gamma)\Gamma^2 = m(\Gamma)(\Gamma \cdot W + 2) - 2m(\Gamma)p_a(\Gamma)\,. \tag{4.3}$$

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 $2g-2$ components Γ of multiplicity 1 and with $\Gamma \cdot W > 0$. The remaining components of $\mathcal{C}_s^{\mathrm{smooth}}$ are (-2)-curves of multiplicity 1, so by (4.3) the total intersection number with other components is 2. We note that not all components of $\mathcal{C}_s$ can be (-2)-curves, since then $2g - 2 = W \cdot \mathcal{C}_s$ would vanish, contradicting the assumption $g \geq 2$. This implies that there cannot be three (-2)-curves of multiplicity 1 meeting in one point or two meeting in one point with intersection multiplicity 2, since in these cases there could be no other components. There are therefore the following possibilities for how a (-2)-curve Γ of multiplicity 1 can meet other components.

(1) Γ meets two components of multiplicity 1 in two distinct points. Then Γ is part of a maximal *chain* of such components that connects 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 Γ', Γ'' of multiplicity 1 in the same point such that
   (3a) either none of Γ', Γ'' is a (-2)-curve, or
   (3b) Γ' is a (-2)-curve, but Γ'' is not.

(4) Γ meets a component of multiplicity 1, which is not a (-2)-curve, in one point with intersection multiplicity 2.

In cases (2) to (4), $\Gamma \cap \mathcal{C}_s^{\mathrm{smooth}}$ is isomorphic to $\mathbb{A}^1$. We will call such components of $\mathcal{C}_s$ simply $\mathbb{A}^1$-*components*.

In general, there can also be chains consisting of (-2)-curves of higher (constant) multiplicity. They do not form part of $\mathcal{C}_s^{\mathrm{smooth}}$, so they are not of interest for our purposes. Artin and Winters [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 of any multiplicity as above. This implies in particular that there must be bounds that depend only on g for the number of (maximal) chains of (-2)-curves of multiplicity 1 and for the number of $\mathbb{A}^1$-components. The following result gives explicit and optimal such bounds.

Theorem 4.1. *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 $t + u \leq g - a$, where a denotes the abelian rank of the special fiber of the Néron model of the Jacobian of C, such that*

(i) *The number of components Γ of $\mathcal{C}_s$ with $\Gamma \cdot W > 0$ is $N \leq 2g - 2$.*

(ii) *The number of maximal chains of (-2)-curves of multiplicity 1 in $\mathcal{C}_s$ is at most $N - 1 + t \leq 2g - 3 + t$.*

(iii) *The number of $\mathbb{A}^1$-components in $\mathcal{C}_s$ is at most $3u$.*

Remark 4.2. 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.

Proof. We have $N \leq 2g - 2$ by (4.2).

We note that in terms of the graph G associated to the special fiber $\mathcal{C}_s$, a component as in case (3a) or (4) above is indistinguishable from a chain of length 1, and the two $\mathbb{A}^1$-components involved in case (3b) are indistinguishable from a chain of length 2. (Indeed, after a slight deformation of the special fiber that does not change the intersection multiplicities of the components, the point of intersection breaks up into two or three ordinary double points, and the respective components do form a chain of length 1 or 2.) Write c for the number of maximal chains, $d_{3\mathrm{a}}$, $d_{3\mathrm{b}}$, d_4 for the number of $\mathbb{A}^1$-components as in cases (3a), (3b) and (4) above, and d for the number of remaining $\mathbb{A}^1$-components. We show that there are numbers $t', u' \geq 0$ with $t' + u' \leq g - a$ such that

$$c + d_{3\mathrm{a}} + \frac{1}{2} d_{3\mathrm{b}} + d_4 \leq N - 1 + t' \qquad \text{and} \qquad d \leq 3u' \,. \tag{4.4}$$

Claims (ii) and (iii) follow by taking $t = t' - \delta$ and $u = u' + \delta$ with $\delta = d_{3\mathrm{a}} + \frac{1}{2} d_{3\mathrm{b}} + d_4$ (note that $d_{3\mathrm{b}}$ is even).

We write $\chi(G) = 1 - t'$ for the Euler characteristic of G, where t' denotes the number of independent loops in G.

We now bound the number of chains together with the 'false chains' coming from $\mathbb{A}^1$-components in cases (3a), (3b) or (4), Consider the subgraph G' of G spanned by the N vertices corresponding to components Γ with $\Gamma \cdot W > 0$ and by the vertices corresponding to components in chains (false or otherwise). Contracting each of these chains to an edge,

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

$$\begin{aligned} c + d_{3a} + \frac{1}{2}d_{3b} + d_4 &= \#\{\text{chains}\} + \#\{\text{false chains}\} \\ &\leq \#\{\text{edges of } G''\} = N - \chi(G'') \leq N - \chi(G) = N - 1 + t' \end{aligned}$$

as claimed in the first inequality in (4.4).

To obtain a bound on the number d of the remaining $\mathbb{A}^1$-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. We also write $p_{(m,w)}$ for the sum of $p_a(\Gamma)$ over all (m, w)-vertices Γ.

Taking the sum of (4.3) over all (m, w)-vertices, we obtain

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

or equivalently,

$$v_{(m,w)} = \frac{1}{m(w+2)} \sum_{(m',w')} m' e_{(m,w),(m',w')} + \frac{2}{w+2} p_{(m,w)}\,, \tag{4.5}$$

which allows us to replace $v_{(m,w)}$ by the right hand side. If we use this in (4.2), this gives

$$2g - 2 = \sum_{(m,w)} mw\, v_{(m,w)} = \sum_{(m,w),(m',w')} \frac{wm'}{w+2} e_{(m,w),(m',w')} + \sum_{(m,w)} \frac{2wm}{w+2} p_{(m,w)}\,. \tag{4.6}$$

In addition, remembering that G is connected and that for $(m, w) \neq (m', w')$, the sum $e_{(m,w),(m',w')} + e_{(m',w'),(m,w)}$ counts twice the number of edges between vertices with invariants (m, w) and (m', w'), whereas $e_{(m,w),(m,w)}$ counts twice the number of edges between (m, w)-vertices, 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 (4.5) as

$$\sum_{(m,w),(m',w')} \Big(\frac{2m'}{m(w+2)} - 1\Big) e_{(m,w),(m',w')} + \sum_{(m,w)} \frac{4}{w+2} p_{(m,w)} = 2 - 2t'\,.$$

Adding (4.6) to this, we finally have

$$\begin{aligned} \sum_{(m,w),(m',w')} \Big(\frac{m'(mw+2)}{m(w+2)} - 1\Big) e_{(m,w),(m',w')} &= 2(g - t' - p') - 2\sum_{(m,w)} \frac{w(m-1)}{w+2} p_{(m,w)} \\ &\leq 2(g - t' - p')\,, \end{aligned} \tag{4.7}$$

where we have set

$$p' = \sum_{(m,w)} p_{(m,w)} = \sum_{\Gamma} p_a(\Gamma) \geq \sum_{\Gamma} p_g(\Gamma) = a\,.$$

Here $p_g(\Gamma)$ denotes the geometric genus of Γ. We set $u' = g - t' - p'$; then $t' + u' = g - p' \leq g - a$. Let '$<$' denote the lexicographical ordering of the pairs (m, w). Using the obvious equality $e_{(m,w),(m',w')} = e_{(m',w'),(m,w)}$, we can rewrite (4.7) as

(4.8)
$$\sum_{(m,w)} \frac{(m-1)w}{w+2} e_{(m,w),(m,w)} + \sum_{(m,w)<(m',w')} \Big(\frac{m'(mw+2)}{m(w+2)} + \frac{m(m'w'+2)}{m'(w'+2)} - 2 \Big) e_{(m,w),(m',w')} \leq 2u'\,.$$

We can bound the coefficient of $e_{(m,w),(m',w')}$ in (4.8) from below:

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

So all coefficients on the left hand side of (4.8) 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 (4.8). Then

$$\lambda_{(1,w),(2,0)} = \frac{1}{2} \quad \text{for all } w \geq 0, \qquad \lambda_{(1,0),(2,w')} \geq \frac{2}{3} \quad \text{for all } w' \geq 1,$$
$$\lambda_{(2,0),(2,w')} \geq \frac{1}{3} \quad \text{for all } w' \geq 1, \qquad \lambda_{(2,0),(3,w')} \geq \frac{1}{6} \quad \text{for all } w' \geq 0.$$

Using this in (4.8) we obtain

(4.9)
$$\frac{1}{2} e_{(1,0),(2,0)} + \frac{1}{2} \sum_{w \geq 1} e_{(1,w),(2,0)} + \frac{1}{3} \sum_{w' \geq 1} e_{(2,0),(2,w')} + \frac{1}{6} \sum_{w' \geq 0} e_{(2,0),(3,w')} + \frac{2}{3} \sum_{w' \geq 1} e_{(1,0),(2,w')} \leq 2u'\,.$$

We now claim that

(4.10)
$$3 \sum_{w \geq 1} e_{(1,w),(2,0)} + 2 \sum_{w' \geq 1} e_{(2,0),(2,w')} + \sum_{w' \geq 0} e_{(2,0),(3,w')} \geq e_{(1,0),(2,0)}\,.$$

Assuming this for a moment, we can use (4.10) in (4.9) to obtain

$$\frac{2}{3} \sum_{w' \geq 0} e_{(1,0),(2,w')} \leq 2u' \qquad \text{or equivalently,} \qquad \sum_{w' \geq 0} e_{(1,0),(2,w')} \leq 3u'\,.$$

The left hand side counts exactly the number d of (-2)-curves of multiplicity 1 that meet a component of multiplicity 2, so this finishes the proof of claim (4.4).

It remains to prove (4.10). 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 (4.8). So we can assume without loss of generality that no such edges are present. Equivalently, we can consider chains of $(2,0)$-vertices instead of single $(2,0)$-vertices in the argument below. 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 edge 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. □

Remark 4.3. One can in fact take t and u in Theorem 4.1 to be the toric and unipotent ranks of the special fiber of the Néron model of the Jacobian of C. For claim (ii), this follows from a similar argument as in the proof above, but using the bipartite graph G' whose vertices correspond to the components of the special fiber and the intersection points of components, with edges whenever a point lies on a component. This version of the reduction graph avoids the 'false' chains and satisfies $1-\chi(G') \leq$ the toric rank t, compare [Liu02, Exercise 10.1.19].

For claim (iii), we recall from the proof above that the bound on the number of $\mathbb{A}^1$-components is $3(g-t'+\delta-p')$. We have $t'-\delta+p' \geq t+a = g-u$, where u denotes the unipotent rank, so that $g-t'+\delta-p' \leq u$. Note that $t'-\delta$ is still an upper bound for the part of the toric rank coming from loops in the configuration of components — 'false' chains give rise to 'false' loops — whereas p' is an upper bound for a plus the part of the toric rank coming from individual components.

For our intended application, the version as given in Theorem 4.1 is sufficient, though.

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).

5. 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. Let a, t and u be as in Theorem 4.1; we can assume that $a+t+u = g$. Denoting by $p_g(\Gamma)$ the geometric genus of the component Γ

and writing $\Gamma_1, \dots, \Gamma_{N'}$ 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

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

for the number of smooth κ-points on components having positive intersection with W. 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. For $a + u = g - t$ fixed, the sum of these bounds is maximal when $a = 0$, leading to a bound of

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

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 the sets of k-points of open p-adic disks over k in the following sense.

Definition 5.1. We let $D_{0,k}$ denote the p-adic analytic *open unit disk* over k. Its ring of *analytic regular functions* is the subring of $k[\![z]\!]$ of power series converging whenever $|z| < 1$ (for a power series $f(z) = \sum_{n=0}^{\infty} a_n z^n$, this means that $|a_n| r^n \to 0$ for all $0 < r < 1$). We call any analytic isomorphism $u\colon D_{0,k} \to D_{0,k}$ a *coordinate* on $D_{0,k}$. It can be checked that for any analytic map $h\colon D_{0,k} \to D_{0,k}$, the map u given by $u(z) = z(1 + h(z))$ is a coordinate on $D_{0,k}$.

For $k \subset K \subset \mathbb{C}_p$ a field extension, we set $D_0(K) = \{\xi \in K : |\xi| < 1\}$.

An *(open) disk in C* is an injective analytic map $\varphi\colon D_{0,k} \to C$ (i.e., given by coordinates that are analytic regular functions on $D_{0,k}$).

Now consider a maximal chain of (-2)-curves of multiplicity 1 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 an ordinary 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 the k-points of an open annulus over k in the sense of Definition 5.2 below. The number of such annuli equals the number of chains (defined over κ) and so is bounded according to Theorem 4.1 by $2g - 3 + t$.

Definition 5.2. Let $0 < \alpha < 1$ be such that $\alpha = |\xi|$ for some $\xi \in k$. We let $A_{\alpha,k}$ denote the standard p-adic *open annulus* over k of height α. Its ring of *analytic regular functions* is the ring of (infinite in both directions) Laurent series in z converging whenever $\alpha < |z| < 1$ (for $f(z) = \sum_{n=-\infty}^{\infty} a_n z^n$, this means that $\lim_{n\to\pm\infty} |a_n| r^n = 0$ for all $\alpha < r < 1$). We call any analytic isomorphism $u\colon A_{\alpha,k} \to A_{\alpha,k}$ a *coordinate* on $A_{\alpha,k}$. It can be checked that for any analytic map $h\colon A_{\alpha,k} \to D_{0,k}$, the map u given by $u(z) = z(1 + h(z))$ is a coordinate

on $A_{\alpha,k}$ (see for example [BGR84, Lemma 9.7.1/1 and Proposition 9.7.1/2], applied to all closed annuli in $A_{\alpha,K}$ for $k \subset K \subset \mathbb{C}_p$).

For $k \subset K \subset \mathbb{C}_p$ a field extension, we set $A_\alpha(K) = \{\xi \in K : \alpha < |\xi| < 1\}$.

An *(open) annulus in C* is an injective analytic map $\varphi\colon A_{\alpha,k} \to C$ (i.e., given by coordinates that are analytic regular functions on $A_{\alpha,k}$), for some α as above.

Summarizing the discussion above, we have shown:

Proposition 5.3. *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 the sets of k-points of at most $(5q+2)(g-1)-3q(t-1)$ open disks and at most $2(g-1)+(t-1)$ open annuli in C.*

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

6. Annuli in hyperelliptic curves

In this section we give an explicit description of the annuli on a hyperelliptic curve. This is used in Section 7 below to obtain bounds for the number of points on an annulus that map into a given subgroup of the Jacobian. We do this for a p-adic field k when p is *odd*. We proceed in three steps, as follows.

1. We construct disks and annuli in C from disks and annuli in $\mathbb{P}^1$.
2. We give a classification of analytic involutions on disks and annuli.
3. We use Step 2 to show that all annuli in C arise as in Step 1.

We then use this explicit description to describe the restriction of the global regular differentials on C to these annuli.

We begin with the construction of disks and annuli in the hyperelliptic curve C. We write $\iota\colon C \to C$ for the hyperelliptic involution, $\pi\colon C \to \mathbb{P}^1$ for the hyperelliptic double cover and $\Theta \subset \mathbb{P}^1$ for its set of branch points; note that $\#\Theta = 2g+2$ is even. We can assume that $\infty \notin \Theta$; then an equation for C is given by

$$y^2 = f(x) = c\prod_{\theta\in\Theta}(x-\theta)$$

with some $c \in k^\times$. For $0 \ne \theta \in \Theta$ we set

$$f_\theta^+(x) = \left(1-\frac{\theta}{x}\right)^{1/2} \in k[\![x^{-1}]\!] \qquad \text{and} \qquad f_\theta^-(x) = \left(1-\frac{x}{\theta}\right)^{1/2} \in k[\![x]\!]\,.$$

Note that $f_\theta^+(x)$ converges for $|x| > |\theta|$ and that $f_\theta^-(x)$ converges for $|x| < |\theta|$ (here we use that p is odd). We then have

$$x-\theta = x f_\theta^+(x)^2 \qquad \text{and} \qquad x-\theta = -\theta f_\theta^-(x)^2$$

for x in the respective domain of convergence.

Lemma 6.1. *Let $\varphi\colon D_{0,k} \xrightarrow{\sim} D \subset \mathbb{P}^1_k$ be an open disk.*

(1) *If $D(\mathbb{C}_p)\cap\Theta=\emptyset$, then let $\xi\in D(k)$. If $f(\xi)$ is not a square in k, then $\pi^{-1}(D)\cap C(k)$ is empty. Otherwise $\pi^{-1}(D)$ is the union of two disjoint open disks in C, each isomorphic to D via π.*

(2) *If $D(\mathbb{C}_p)\cap\Theta=\{\theta_1\}$, then $\theta_1\in k$. We assume that the radius r of D (in terms of a coordinate on $\mathbb{P}^1$ such that $\infty\notin D$) satisfies $r|f'(\theta_1)|=|\xi|^2$ for some $\xi\in k$. Then $D'=\pi^{-1}(D)$ is a disk in C. In terms of suitable coordinates on D' and D, $\pi\colon D'\to D$ is given by $z\mapsto z^2$. The hyperelliptic involution acts on D' as $z\mapsto -z$.*

(3) *If $D(\mathbb{C}_p)\cap\Theta=\{\theta_1,\theta_2\}$ has two elements, then $(x-\theta_1)(x-\theta_2)$ has coefficients in k. The set $\pi^{-1}(D)\cap C(k)$ is either contained in the preimage of the smallest closed disk containing θ_1 and θ_2, or else $\pi^{-1}(D)$ is an annulus A in C such that in terms of suitable coordinates on A and D, $\pi\colon A\to D$ is given by $z\mapsto z+\beta/z$ with some $\beta\in k^\times$. The hyperelliptic involution acts on A as $z\mapsto\beta/z$.*

Proof. We can (after possibly a coordinate change on $\mathbb{P}^1$) assume that $\varphi=\mathrm{id}$ and $D=D_0$. Then in case (1), we can take $\xi=0$, and we have $|\theta|\geq 1$ for all $\theta\in\Theta$. So on D we can write the equation of C as

$$y^2=c\prod_{\theta\in\Theta}\theta\cdot\Big(\prod_{\theta\in\Theta}f_\theta^-(x)\Big)^2=c'h(x)^2\,,$$

where $c'=c\prod_{\theta\in\Theta}\theta=f(0)$ and $h(x)=\prod_{\theta\in\Theta}f_\theta^-(x)$. If c' is not a square in k, then this equation has no solution in k and so $\pi^{-1}(D)$ does not contain k-points of C. Otherwise write $c'=\gamma^2$ for some $\gamma\in k^\times$. Then $\pi^{-1}(D)$ is the disjoint union of

$$D^+=\big\{(\xi,\gamma h(\xi)):\xi\in D\big\}\qquad\text{and}\qquad D^-=\big\{(\xi,-\gamma h(\xi)):\xi\in D\big\}\,,$$

and the projection to the first coordinate $\pi\colon D^\pm\to D$ is an analytic isomorphism.

In case (2), we first observe that θ_1 must be fixed under the action of the absolute Galois group of k, since D and Θ are; it follows that $\theta_1\in k$. We can then in addition assume that $\theta_1=0$. Since we assume that $D=D_0$, we have $r=1$. Similarly as in case (1) we write the equation of C on D as

$$y^2=-c\prod_{0\neq\theta}\theta\cdot x\Big(\prod_{0\neq\theta\in\Theta}f_\theta^-(x)\Big)^2=c'xh(x)^2\,,$$

where $c'=-c\prod_{0\neq\theta\in\Theta}\theta=f'(\theta_1)$ and $h(x)=\prod_{0\neq\theta\in\Theta}f_\theta^-(x)$. Choosing $\gamma\in k$ and $u\in\mathcal{O}^\times$ such that $\gamma^2=uc'$, we can now parameterize $D_{0,k}\xrightarrow{\sim}D'=\pi^{-1}(D)$ via

$$z\longmapsto\big(uz^2,\gamma zh(uz^2)\big)\,.$$

If we use $u^{-1}x$ as the coordinate on D, then $\pi\colon D'\to D$ is given by $z\mapsto z^2$. It is clear that the hyperelliptic involution is given in terms of z by $z\mapsto -z$. We remark that the condition '$r|f'(\theta_1)|=|\xi|^2$ for some $\xi\in k$' is invariant under coordinate transformations.

In case (3), we see in the same way as before that the set $\{\theta_1,\theta_2\}$ is fixed by the action of the absolute Galois group of k, which implies that the coefficients of $(x-\theta_1)(x-\theta_2)$ are in k. We can then change coordinates so that $\theta_1+\theta_2=0$ (and D is still the open unit disk).

Let $\theta_1\theta_2 = a \in k^\times$ (θ_1 and θ_2 must be nonzero, since f does not have multiple roots). Set $\Theta' = \Theta \setminus \{\theta_1, \theta_2\}$; then the equation of C on D can be written as

$$y^2 = c \prod_{\theta\in\Theta'} \theta \cdot (x^2 - a)\Big(\prod_{\theta\in\Theta'} f_\theta^-(x)\Big)^2 = c'(x^2 - a)h(x)^2\,,$$

where $c' = c\prod_{\theta\in\Theta'}\theta$ and $h(x) = \prod_{\theta\in\Theta'} f_\theta^-(x)$. If c' is not a square in k, then there are no solutions when $|x| > |\theta_1| = |\theta_2|$, and $\pi^{-1}(D) \cap C(k)$ is contained in the preimage of $\{\xi : |\xi| \le |\theta_1|\}$. Otherwise, write $c' = \gamma^2$ with some $\gamma \in k^\times$. Taking

$$z = \frac{1}{2}\Big(x + \frac{y}{\gamma h(x)}\Big)\,,$$

we can parameterize $\pi^{-1}(D)$ via

$$z \longmapsto \Big(z + \frac{a}{4z}, \gamma \cdot \Big(z - \frac{a}{4z}\Big)h\Big(z + \frac{a}{4z}\Big)\Big)\,.$$

The condition $|z + a/(4z)| < 1$ translates into $|a| < |z| < 1$, which defines the annulus A. The covering map to D is given by $z \mapsto z + (a/4)/z$. The involution $z \mapsto a/(4z)$ fixes the x-coordinate and changes the sign of the y-coordinate, so it is the hyperelliptic involution on A. □

Lemma 6.2. *Let $\varphi\colon A_{\alpha,k} \xrightarrow{\simeq} A \subset \mathbb{P}^1_k$ be an open annulus with $A(\mathbb{C}_p) \cap \Theta = \emptyset$ and $A(k) \neq \emptyset$. The complement of A in $\mathbb{P}^1_k$ is a disjoint union of two closed disks, which partitions Θ into two disjoint subsets Θ_0 and Θ_∞. This induces a factorization $f(x) = cf_0(x)f_\infty(x)$ with f_0 and f_∞ monic such that the roots of f_0 are the elements of Θ_0 and the roots of f_∞ are the elements of Θ_∞.*

(1) *If $\#\Theta_0$ and $\#\Theta_\infty$ are odd, we assume in addition that $\alpha = |\beta_1|^2$ for some $\beta_1 \in k$ and that $r|cf_\infty(\xi)| = |\beta_2|^2$ for some $\xi \in k$ in the closed disk defining Θ_0 and some $\beta_2 \in k$, where r is the outer (or inner) radius of A in terms of some coordinate on $\mathbb{P}^1$ such that $0, \infty \notin A$. Then $\pi^{-1}(A)$ is an annulus A' in C. In terms of suitable coordinates on A' and A, $\pi\colon A' \to A$ is given by $z \mapsto z^2$ and the hyperelliptic involution on A' is $z \mapsto -z$.*

(2) *If $\#\Theta_0$ and $\#\Theta_\infty$ are even, then let $\xi \in A(k)$. If $cf_\infty(\xi)$ is not a square in k, then $\pi^{-1}(A) \cap C(k)$ is empty. Otherwise $\pi^{-1}(A)$ is a disjoint union of two annuli in C, each isomorphic to A via π.*

Proof. We can assume that $\varphi = \mathrm{id}$ and $A = A_{\alpha,k}$ and that $0 \notin \Theta$. We fix notations by setting $\Theta_0 = \{\theta \in \Theta : |\theta| \le \alpha\}$ and $\Theta_\infty = \{\theta \in \Theta : |\theta| \ge 1\}$. Note that, in a similar way as in the proof of Lemma 6.1, the sets Θ_0 and Θ_∞ are each fixed by the action of the absolute Galois group of k. In particular, the product $\prod_{\theta\in\Theta_\infty}(-\theta)$ is in k. We can then write the equation of C on A as

$$y^2 = c \prod_{\theta\in\Theta_\infty} (-\theta) \cdot x^{\#\Theta_0}\Big(\prod_{\theta\in\Theta_\infty} f_\theta^-(x) \prod_{\theta\in\Theta_0} f_\theta^+(x)\Big)^2 = c'x^{\#\Theta_0}h(x)^2\,,$$

where $c' = c\prod_{\theta\in\Theta_\infty}(-\theta) = (-1)^{\#\Theta_\infty}cf_\infty(0)$ and $h(x) = \prod_{\theta\in\Theta_\infty} f_\theta^-(x)\prod_{\theta\in\Theta_0} f_\theta^+(x)$.

In case (1), writing $uc' = \gamma^2$ with $\gamma \in k$ and $u \in \mathcal{O}^\times$, we obtain the parameterization

$$A_{\sqrt{\alpha},k} \xrightarrow{\simeq} A' = \pi^{-1}(A), \qquad z \longmapsto \big(uz^2, \gamma u^{(\#\Theta_0-1)/2} z^{\#\Theta_0} h(uz^2)\big)\,,$$

in a similar way as in case (2) of Lemma 6.1. The statements on π and on the hyperelliptic involution follow in the same way as there. We remark that the condition '$r|cf_\infty(\xi)| = |\beta_2|^2$ for some $\beta_2 \in k$' is (assuming that $\alpha = |\beta_1|^2$ for some $\beta_1 \in k$) invariant under coordinate transformations.

In case (2) we have $x^{\#\Theta_0}h(x)^2 = \left(x^{\#\Theta_0/2}h(x)\right)^2$. This case is similar to case (1) of Lemma 6.1: there are no solutions in k unless $c' = \gamma^2$ is a square, and in the latter case, we have $\pi^{-1}(A) = A^+ \cup A^-$ with

$$A^\pm = \left\{(\xi, \pm\gamma\xi^{\#\Theta_0/2}h(\xi)) : \xi \in A\right\}. \qquad \square$$

We state some results on involutions of disks and annuli. An *analytic involution* on $D_{0.k}$ or $A_{\alpha,k}$ is an analytic automorphism ι of order two. Recall that we assume the residue characteristic p to be odd. We do not claim that the results below are original, but we were unable to find a suitable reference.

Lemma 6.3. *Let $0 < \alpha < 1$ be of the form $\alpha = |\xi|$ for some $\xi \in k$.*

(1) *Let $\iota\colon D_{0,k} \to D_{0,k}$ be an analytic involution. Then ι has a unique fixed point in $D_0(\mathbb{C}_p)$, which is in fact in $D_0(k)$, and in terms of a suitable coordinate u on $D_{0,k}$, ι is given by $u \mapsto -u$.*

(2) *Let $\iota\colon A_{\alpha,k} \to A_{\alpha,k}$ be an analytic involution such that $|\iota(\xi)| = |\xi|$ for all $\xi \in A_\alpha(\mathbb{C}_p)$. Then ι is given in terms of a suitable coordinate u on $A_{\alpha,k}$ by $u \mapsto -u$. In particular, ι has no fixed points, and $A_\alpha/\langle\iota\rangle \simeq A_{\alpha^2}$ is an annulus.*

(3) *Let $\iota\colon A_{\alpha,k} \to A_{\alpha,k}$ be an analytic involution such that $|\iota(\xi)| = \alpha/|\xi|$ for all $\xi \in A_\alpha(\mathbb{C}_p)$. Then ι is given in terms of a suitable coordinate u on $A_{\alpha,k}$ by $u \mapsto a/u$ for some $a \in k$ with $|a| = \alpha$. In particular, ι has exactly two fixed points $u = \pm\sqrt{a}$ in $A_\alpha(\mathbb{C}_p)$, $A_{\alpha,k}/\langle\iota\rangle \simeq D_{0,k}$ is a disk, and the covering $A_{\alpha,k} \to D_{0,k}$ is branched above two points.*

Proof.

(1) We first show that we can assume that 0 is a fixed point of ι, possibly after a coordinate change. So assume otherwise. ι is then given by a power series $\sum_{n=0}^\infty a_n z^n \in \mathcal{O}[\![z]\!]$ whose constant term satisfies $0 < |a_0| < 1$. Since ι is an involution, we have $\iota(a_0) = 0$, which implies that $|a_0 + a_1a_0| \le |a_0|^2$, so $|a_1 + 1| \le |a_0|$. This in turn implies that $z \mapsto (\iota(z) + z)/2$ is contracting on every sufficiently large closed disk contained in $D_0(k)$ and so has a fixed point in $D_0(k)$ by the Banach fixed point theorem. We can then shift the coordinate so that the fixed point is at the origin; we denote this coordinate by z again.

We now have $\iota(0) = 0$. Then $\iota(z) = a_1z + a_2z^2 + \ldots$, and $\iota \circ \iota = \mathrm{id}$ implies that $a_1^2 = 1$. If $a_1 = 1$, then it follows that $\iota = \mathrm{id}$, which is excluded: assume otherwise, then $\iota(z) = z + \beta z^n + \ldots$ with $n > 1$ and $\beta \neq 0$, which leads to the contradiction

$$z = \iota(\iota(z)) = z + 2\beta z^n + \ldots .$$

So $a_1 = -1$ and $\iota(z) = -z(1 + h(z))$ with $h\colon D_{0,k} \to D_{0,k}$. Write $h_1(z) = 1 + h(z)$. The relation $\iota(\iota(z)) = z$ implies that $h_1(z)h_1(\iota(z)) = 1$. We set $u(z) = z(1 + h_1(z))/2$; then

u is a coordinate on $D_{0,k}$, and

$$u(\iota(z)) = \iota(z)\frac{1+h_1(\iota(z))}{2} = -z\frac{h_1(z)+h_1(z)h(\iota(z))}{2} = -z\frac{h_1(z)+1}{2} = -u(z)\,,$$

so in terms of u, ι acts as $u \mapsto -u$. In particular, 0 is the only fixed point of ι on $D_0(\mathbb{C}_p)$.

(2) Since $|\iota(\xi)| = |\xi|$, ι is given by a Laurent series $zf_1(z)$ where $|f_1(\xi)| = 1$ for all $\xi \in A_\alpha(\mathbb{C}_p)$. Let a_0 be the constant term of $f_1(z)$; then $|a_0| = 1$ and $|f_1(\xi) - a_0| < 1$ for all $\xi \in A_\alpha(\mathbb{C}_p)$. Writing $\lambda = a_0$ and $h(z) = f_1(z)/\lambda - 1$, we have $\iota(z) = \lambda z(1+h(z))$ with $h\colon A_{\alpha,k} \to D_{0,k}$. Since ι is an involution, we find that $|\lambda^2 - 1| < 1$. If λ were close to 1, then $|f(\xi) - \xi| < |\xi|$, so ι would induce an involution of the open disk $\{|z-\xi| < |\xi|\} \subset A_\alpha$, for each $\xi \in A_\alpha(\mathbb{C}_p)$. By part (1), ι would have a fixed point in each of these disks, which is impossible, since there are infinitely many of them (even with fixed $|\xi|$) and ι is not the identity. It follows that $|\lambda + 1| < 1$. This already implies that ι has no fixed points.

Write $h_1(z) = 1 + h(z)$. Note that $\iota(\iota(z)) = z$ implies that $h_1(z)h_1(\iota(z)) = \lambda^{-2}$. Similarly as in part (1) we set $u(z) = z(1 - \lambda h_1(z))/(1-\lambda)$; this is a coordinate on $A_{\alpha,k}$. We check that

$$u(\iota(z)) = \iota(z)\frac{1-\lambda h_1(\iota(z))}{1-\lambda} = \lambda z\frac{h_1(z) - \lambda h_1(z)h_1(\iota(z))}{1-\lambda} = z\frac{\lambda h_1(z) - 1}{1-\lambda} = -u(z)$$

as before. The last claim is then clear.

(3) Here we have $\iota(z) = \frac{a}{z}(1 + h(z))$ for some $a \in k$ with $|a| = \alpha$ and some analytic map $h\colon A_{\alpha,k} \to D_{0,k}$. Write $h_1(z) = 1 + h(z)$ The fact that ι is an involution implies this time that $h_1(\iota(z)) = h_1(z)$. Set $u(z) = zh_1(z)^{-1/2}$. Then

$$u(\iota(z)) = \iota(z)h_1(\iota(z))^{-1/2} = \frac{a}{z}h_1(z)h_1(z)^{-1/2} = \frac{a}{zh_1(z)^{-1/2}} = \frac{a}{u(z)}\,,$$

so u is a suitable coordinate. The fixed points are where $u^2 = a$; the map $A_{\alpha,k} \to D_{0,k}$, $u \mapsto u + a/u$, realizes the quotient by $\langle\iota\rangle$. □

Now we show that every (maximal) annulus in C arises as in Lemmas 6.1 and 6.2. A *maximal annulus* in C is an annulus that is not contained in a disk or in a strictly larger annulus in C.

Proposition 6.4. *Let $\varphi\colon A_{\alpha,k} \xrightarrow{\sim} A \subset C$ be a maximal annulus such that $A(k) \neq \emptyset$. Then A is obtained from a disk or an annulus in $\mathbb{P}^1_k$ as in Lemma 6.1, (3), or Lemma 6.2, (1) or (2). In the latter two cases, the two sets Θ_0 and Θ_∞ both have at least three elements.*

Proof. We consider the action of the hyperelliptic involution ι on A and its pullback $\varphi^*\iota$ to $A_{\alpha,k}$. There are three possibilities.

(1) $A \cap \iota(A) = \emptyset$.

Then clearly $\pi(A)$ is analytically isomorphic to A, hence is an annulus in $\mathbb{P}^1_k$ that does not contain any branch points of π. We must then be in case (2) of Lemma 6.2, since the preimage of $\pi(A)$ splits into the two annuli A and $\iota(A)$. If Θ_0 or Θ_∞ had zero or two elements, then we could 'fill in' the annulus $\pi(A)$ to obtain a disk containing zero or two branch points. Then A would be contained in a disk or in a larger annulus by Lemma 6.1, (1) or (3), a contradiction.

(2) $\iota(A) = A$ and ι preserves the orientation of the chain corresponding to A.

Let $\xi \in A_\alpha(\mathbb{C}_p)$. There is a finite extension K of k such that $|\xi| = |\beta|$ for some $\beta \in K$. Since the minimal regular model $\mathcal{C}$ of C is semistable near the reduction of A, the special fiber of the minimal regular model of C over $\mathcal{O}_K$ contains a chain corresponding to A_K obtained by successive blow-ups of intersection points of components of the chain in $\mathcal{C}_s$ with other components (within or outside the chain). There is one such component that corresponds to the points $\xi' \in A_\alpha(K)$ with $|\xi'| = |\beta| = |\xi|$. Since ι preserves the orientation of the chain, it fixes every component; it follows that $|\varphi^*\iota(\xi)| = |\xi|$. By Lemma 6.3, (2), $\pi(A)$ is an annulus of height α^2 in $\mathbb{P}^1_k$ that does not contain any branch points. We must then be in case (1) of Lemma 6.2, since $A \to \pi(A)$ is an unramified double cover. (The condition $r|cf_\infty(\xi)| = |\beta_2|^2$ is automatically satisfied, since A is an annulus over k.) If Θ_0 or Θ_∞ had only one element, then we could again 'fill in' the annulus $\pi(A)$ to obtain a disk containing exactly one branch point, so that A would be contained in a disk in C by Lemma 6.1, (2).

(3) $\iota(A) = A$ and ι reverses the orientation of the chain corresponding to A.

By a similar argument as in the preceding case, we see that $|\varphi^*\iota(\xi)| = \alpha/|\xi|$. By Lemma 6.3, (3), $\pi(A)$ is a disk in $\mathbb{P}^1_k$ that contains exactly two branch points. We must then be in case (3) of Lemma 6.1. □

We give names to the three possible kinds of annuli.

Definition 6.5. Let A be a maximal annulus in C. We call A

(1) a *branch annulus*, if A is obtained as in Lemma 6.1, (3);
(2) an *odd annulus*, if A is obtained as in Lemma 6.2, (1) (with $\#\Theta_0, \#\Theta_\infty \geq 3$);
(3) an *even annulus*, if A is obtained as in Lemma 6.2, (2) (with $\#\Theta_0, \#\Theta_\infty \geq 4$).

Now we describe what the regular differentials of C look like on the various types of annuli.

Proposition 6.6. *Let $\varphi\colon A_{\alpha,k} \to C$ be an annulus in C, in terms of a coordinate z as in the proofs of Lemma 6.1, (3) and Lemma 6.2. Then there is an analytic function $h\colon A_{\alpha,k} \to D_{0,k}$ such that a basis of $\varphi^*\Omega^1_C(k)$ is given by*

$$\left(z + \frac{a}{4z}\right)^\nu (1 + h(z))\,\frac{dz}{z}, \qquad z^{2\nu+2-\#\Theta_0}(1 + h(z))\,\frac{dz}{z}, \qquad z^{\nu+1-\#\Theta_0/2}(1 + h(z))\,\frac{dz}{z},$$

for $\nu = 0, 1, 2, \ldots, g-1$, when A is a branch, odd, or even annulus, respectively.

Proof. This is an easy consequence of the parameterizations and the fact that $\Omega^1_C(k)$ is spanned by $x^\nu\,dx/y$ for $\nu = 0, 1, 2, \ldots, g-1$. □

Corollary 6.7. *Let $\varphi\colon A_{\alpha,k} \to C$ be an annulus as before. There are numbers $n_1 < 0 < n_2$ with $n_2 - n_1 \leq 2g - 2$ and an analytic map $h\colon A_{\alpha,k} \to D_{0,k}$ such that for every differential $\omega \in \Omega^1_C(k)$, we have*

$$\varphi^*\omega = u(z)(1 + h(z))\,\frac{dz}{z}$$

where $u(z) \in k[z, z^{-1}]$ is a Laurent polynomial all of whose terms have exponents between n_1 and n_2, inclusive.

Proof. In Proposition 6.6, we can take $n_1 = -(g-1)$, $n_2 = g-1$ in the branch case, $n_1 = 2 - \#\Theta_0$, $n_2 = 2g - \#\Theta_0$ in the odd case, and $n_1 = 1 - \#\Theta_0/2$, $n_2 = g - \#\Theta_0/2$ in the even case. Note that $3 \leq \#\Theta_0 \leq 2g-1$, which implies that $n_1 < 0 < n_2$. □

A bound like this for the 'relevant' exponents is important to obtain uniform bounds. We note that Katz, Rabinoff and Zureick-Brown [KRZB15, Lemma 4.15] prove the following statement that applies to arbitrary curves, but has a weaker conclusion. It is this extension that allows them to generalize our results from hyperelliptic to arbitrary curves.

Proposition 6.8 (Katz, Rabinoff, Zureick-Brown)**.** *Let k be a p-adic field ($p = 2$ is allowed here). Let C be a curve over k of genus $g \geq 2$ and let $\varphi\colon A_{\alpha,k} \to C$ be an annulus. Then for every differential $\omega \in \Omega^1_C(k)$, we have*

$$\varphi^*\omega = u(z)(1+h(z))\,\frac{dz}{z}$$

where $h\colon A_{\alpha,k} \to D_{0,k}$ and $u(z) \in k[z,z^{-1}]$ is a Laurent polynomial all of whose terms have exponents between $-(2g-2)$ and $2g-2$, inclusive.

It would be interesting to see whether the conclusion can be strengthened as in Corollary 6.7.

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

We fix a basepoint $P_0 \in C(k)$; this gives rise to the embedding $i\colon C \to J$, $P \mapsto [P - P_0]$, defined over k. 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 $P \in C(k)$

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

If $\varphi\colon D_0 \to C$ is an open disk in C, then

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

with an analytic regular function $w(z)$ 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 $\varphi(D_0(\bar{k}))$ 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

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

Recall that e denotes the ramification index of k. If $p > e+1$, then we set

$$\mu = 1 + \frac{e}{p-e-1} = \frac{p-1}{p-e-1}\,;$$

note that $1 < \mu \le e+1$. By [Sto06, Lemma 6.2], we have $\Delta_k(s,n) \le e\lfloor n/(p-e-1)\rfloor$ in this case, so that $n + \Delta_k(s,n) \le \mu n$. We have the following bound.

Lemma 7.1. *Let $V \neq 0$ be a linear subspace of codimension r of the space of regular differentials on C and let N_D denote the number of 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

$$N_D + 2\mu r \le (5q+2)(g-1) - 3q(t-1) + 2\mu r\,.$$

Proof. This is essentially [Sto06, Theorem 6.6], using [KZB13, Theorem 4.4] in the case of bad reduction. In the case $p > e+1$ we use the bound stated above; the bound for N_D comes from Proposition 5.3. □

Now we consider the situation for an annulus $\varphi\colon A_{\alpha,k} \xrightarrow{\sim} A \subset C$. Pulling back ω, we obtain

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

for analytic regular functions w and ℓ on $A_{\alpha,k}$ 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, we can define a p-adic integral on A_α by

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

We want to compare this with

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

Perhaps surprisingly, these two integrals can differ.

Remark 7.2. There is in fact a unique p-adic integration theory in a suitable sense that is functorial and satisfies $\int_1^\xi dz/z = \mathrm{Log}_0(\xi)$ on any annulus containing 1 and ξ [Ber07]. It is called the *Berkovich-Coleman integral* in [KRZB15] to distinguish it from the *Abelian integral* that we denote $\oint$ in this paper.

The following result is crucial. It was first suggested by numerical computations and appears to be new. Recall that $v\colon k^\times \to \mathbb{Q}$ denotes the valuation on k, normalized so that $v(p) = 1$.

Proposition 7.3. *Let ω and $\varphi\colon A_{\alpha,k} \to C$ be as above, and write*

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

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

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

Proof. Let $\xi_0 \in A_\alpha(k)$. Let $i\colon C \to J$ be the embedding sending $\varphi(\xi_0)$ to O. According to [BL84, Proposition 6.3], the analytic map $i \circ \varphi\colon A_{\alpha,k} \to J$ can be written uniquely as

$$i(\varphi(z)) = \psi_1(\xi_0^{-1} j(z)) + \psi_2(z)\,,$$

where $j\colon A_{\alpha,k} \to \mathbb{G}_{\mathrm{m},k}$ is the natural inclusion, $\psi_1\colon \mathbb{G}_{\mathrm{m},k} \to J$ is an analytic group homomorphism and $\psi_2\colon A_{\alpha,k} \to U$ 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 regular 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 $\lambda(O) = 0$. The pull-back $\psi_1^*\omega_J$ is a translation invariant differential on $\mathbb{G}_{\mathrm{m},k}$, so it has the form $c\,dz/z$ for some $c \in k$; the (multiplicative) translation by ξ_0^{-1} does not change it. The pull-back $\psi_2^*\omega_J$ is $\psi_2^* d\lambda = d(\lambda \circ \psi_2)$. Since

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

we see that $\ell(z) = \lambda(\psi_2(z))$ (up to an additive constant) and $c = c(\omega)$. Let $\xi_1 \in A_\alpha(k)$. We obtain on the one side that

$$\begin{aligned}\oint_{\varphi(\xi_0)}^{\varphi(\xi_1)} \omega = \oint_O^{i(\varphi(\xi_1))} \omega_J &= \oint_O^{\psi_1(\xi_0^{-1}\xi_1)+\psi_2(\xi_1)} \omega_J \\ &= \oint_O^{\psi_1(\xi_0^{-1}\xi_1)} \omega_J + \oint_O^{\psi_2(\xi_1)} d\lambda = \oint_O^{\psi_1(\xi_1/\xi_0)} \omega_J + \lambda\big(\psi_2(\xi_1)\big)\end{aligned}$$

and on the other side that

$$\begin{aligned}\int_{\xi_0}^{\xi_1} \varphi^*\omega = \int_{\xi_0}^{\xi_1} \Big(d\ell(z) + c\frac{dz}{z}\Big) &= \ell(\xi_1) - \ell(\xi_0) + c\big(\mathrm{Log}_0(\xi_1) - \mathrm{Log}_0(\xi_0)\big) \\ &= \lambda\big(\psi_2(\xi_1)\big) + c\,\mathrm{Log}_0(\xi_1/\xi_0)\,.\end{aligned}$$

Here we use that $\lambda(\psi_2(\xi_0)) = \lambda(O) = 0$. So the difference is

$$\delta(\xi_1/\xi_0) := \oint_{\varphi(\xi_0)}^{\varphi(\xi_1)} \omega - \int_{\xi_0}^{\xi_1} \varphi^*\omega = \oint_O^{\psi_1(\xi_1/\xi_0)} \omega_J - c\,\mathrm{Log}_0(\xi_1/\xi_0)\,.$$

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 in the first difference 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 $\delta(\xi) = a v(\xi)$.

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 7.4. 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 $\oint_O^{\psi_1(\xi_1/\xi_0)} \omega_J$. 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 $\xi_1/\xi_0 = p$ and $P = \psi_1(p) \in J(k)$. There is a positive integer n such that $nP \in U$; then

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

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 $\lambda_{\omega_J}(nP)$ vanishes.

Remark 7.5. Katz, Rabinoff and Zureick-Brown [KRZB15] generalize Proposition 7.3 to a comparison of the abelian integral and the Berkovich-Coleman integral on more general 'wide open' subsets of (the Berkovich analytic space associated to) C.

We say that ω is *good* for the annulus $\varphi\colon A_{\alpha,k} \to C$ if both $c(\omega)$ and $a(\omega)$ in Proposition 7.3 vanish. This is a linear condition on ω of codimension at most two.

Lemma 7.6. *In the situation of Proposition 7.3 assume that C is hyperelliptic and p is odd. Let $V \neq 0$ be a linear subspace of codimension $r \geq 1$ of the space of regular differentials on C. Then there exists $0 \neq \omega \in V$ such that $\varphi^*\omega = u(z)(1 + h(z))\, dz/z$ with an analytic map $h\colon A_{\alpha,k} \to D_{0,k}$ and a Laurent polynomial u such that the terms in u have exponents between n_1 and n_2 (inclusive), where $n_1 \leq 0 \leq n_2$ and $n_2 - n_1 \leq 2r$ if the annulus is branch or odd, and $n_2 - n_1 \leq r$ if the annulus is even.*

Proof. This follows from Proposition 6.6.

In the branch case,

$$\varphi^*\omega = \sum_{\nu=0}^{g-1} a_\nu \Big(z + \frac{a}{4z}\Big)^\nu (1 + h(z))\, \frac{dz}{z}\,.$$

Since V has codimension r, we can impose $g - 1 - r$ linear conditions, which we can take to be the vanishing of the coefficients $a_{r+1}, a_{r+2}, \ldots, a_{g-1}$. Then the claim holds with $n_1 = -r$, $n_2 = r$.

In the odd case,

$$\varphi^*\omega = \sum_{\nu=0}^{g-1} a_\nu z^{2\nu+2-\#\Theta_0} (1 + h(z))\, \frac{dz}{z}\,.$$

Here we impose the vanishing of $g - 1 - r$ coefficients a_ν with ν small and/or large, so that the remaining coefficients form a contiguous sequence of odd integers containing negative as well as positive numbers. The difference of the largest and the smallest remaining exponent is then $2r$.

In the even case,

$$\varphi^*\omega = \sum_{\nu=0}^{g-1} a_\nu z^{\nu+1-\#\Theta_0/2} (1 + h(z))\, \frac{dz}{z}\,.$$

We proceed in the same way as in the odd case, leaving a contiguous range of exponents containing 0 and of length r. □

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

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

Proposition 7.7. *In the situation of Proposition 7.3 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 common zeros on $\varphi(A_\alpha(k^{\mathrm{unr}}))$ of the λ_ω for all $\omega \in V$ 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 $B_A(p,e,r) = 2\mu r$. If the annulus is even and $r \geq 2$, we can replace this by μr, so that we get the bound $2\mu r$ for the union of the annulus and its image under the hyperelliptic involution.

Proof. By Lemma 7.6, there is $0 \neq \omega \in V$ such that $\varphi^*\omega = u(z)(1+h(z))\,dz/z$ with an analytic map $h\colon A_{\alpha,k} \to D_{0,k}$ and a Laurent polynomial u having exponents between n_1 and n_2 with $n_1 \leq 0 \leq n_2$ and $n_2 - n_1 \leq 2r$ ($\leq r$ if the annulus is even). Since $r \geq 1$ (or $r \geq 2$ in the even case), we can in fact assume that $n_1 < 0 < n_2$. Given this, the proof can be carried out using Newton polygons in essentially the same way as for power series. One possibility for this is to consider the 'positive' and the 'negative' part of the formal integral separately. To the positive part, we can directly apply the corresponding result for power series; for the negative part, we substitute $z \leftarrow z^{-1}$. The bound we obtain for the length of the relevant interval of exponents (belonging to segments of the Newton polygon corresponding to zeros of absolute values in the largest k-defined closed annulus contained in A_α) is then $n_2 - n_1 + \Delta_k(2, n_2 - n_1)$, which for $p > e+1$ can be bounded as stated. □

Note that in contrast to the corresponding result for disks, the '$1+$' term that causes the non-uniformity of the 'classical' Chabauty-Coleman bound does not show up here. This is because the constant of integration affects a coefficient whose exponent lies within the relevant part of the Newton polygon of the formal integral, whereas in the power series case, it can increase the length of the relevant range of exponents by 1.

Corollary 7.8. *Let V be a linear subspace of codimension $r \leq g-3$ of the space of regular differentials on C, where C is as in Proposition 7.7. Let t be as in Proposition 5.3. Then the number of common zeros in $C_A(k)$ of all λ_ω for $\omega \in V$ is bounded by*

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

If $p > e+1$, then we have the bound

$$\min\{2g-1, 2g-3+t\} \cdot 2\mu(r+2)\,.$$

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 7.7 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 5.3 to obtain the result.

Now assume that $p > e+1$; then $B_A(p,e,r+2)$ is bounded by the second factor in the last formula. By the last statement in Proposition 7.7, we can replace $2g-3+t$ by a bound for

the number of orbits of annuli under the hyperelliptic involution, which can be obtained as follows. The image of a minimal skeleton of the p-adic Berkovich analytic space associated to C in the Berkovich projective line is a tree with at most $2g$ nodes (it is obtained from the convex hull of the branch points, which is a tree with $2g+2$ leaves, by removing the leaves and the edges connected to them) and hence at most $2g-1$ edges. The edges correspond to the orbits of annuli under ι, so there are at most $2g-1$ such orbits. (These are the orbits we see when C has split semistable reduction. Since annuli persist under finite extensions of the p-adic base field, this gives an upper bound for the orbits of annuli that are relevant to us here.) □

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

In this section we state and prove our main result.

Theorem 8.1. *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

$$\begin{aligned} N(k,g,r) &= \big(2+5q+4\mu(r+2)\big)(g-1) + \max\{3q-4\mu, 4\mu(r+1)-3q\} \\ &\leq \big(2+5q+4\mu(r+2)\big)g\,, \end{aligned}$$

where $\mu = (p-1)/(p-e-1) \leq e+1$.

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 7.1 and Corollary 7.8 to bound the number of points in $C_D(k)$ and in $C_A(k)$, respectively, that map to Γ. Adding these bounds gives the first result.

In the case $p > e+1$, adding the corresponding explicit bounds and maximizing over $0 \leq t \leq g$ gives the bound

$$\begin{aligned} &(5q+2)(g-1) + 3q + 2\mu r + (2g-3)2\mu(r+2) + 2\max\{0, 2\mu(r+2)-3q\} \\ &\qquad = \big(2+5q+4\mu(r+2)\big)(g-1) + \max\{3q-4\mu, 4\mu(r+1)-3q\}\,. \end{aligned}$$ □

Remark 8.2. 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 7.3) vanish. If this is indeed the case, then the condition $r \leq g-3$ can be relaxed to $r \leq g-2$ or even $r \leq g-1$. However, in view of the facts that $\mathrm{Log}_0(z) = 0$ has infinitely many solutions in $\mathbb{Q}_p$ and that the number of solutions to $z^{-1} + av(z) + z = 0$ is unbounded when

the valuation of a can be arbitrarily negative, it is very likely that more subtle arguments will be necessary to obtain uniform bounds under these less restrictive assumptions.

Remark 8.3. We sketch two variants of the approach taken here.

(i) One possibility is to prove a result like Theorem 8.1 above for *semi-stable* curves. Since a curve of genus g over a p-adic field k acquires semi-stable reduction over an extension of k of degree bounded in terms of g only, this implies the general result. The advantage of this approach is that the structure of the special fiber of the minimal regular model is much easier to understand, so the discussion of the combinatorics of arithmetic graphs as in Section 4 can be bypassed. The disadvantage is that the explicit bounds one obtains are much worse, since one is effectively working over much larger fields.

(ii) Another possibility is to prove directly that for a given hyperelliptic curve C of genus g over k, one can partition $\mathbb{P}^1(k)$ into $\ll qg$ disks containing at most one branch point and $\ll g$ disks containing exactly two branch points and annuli containing no branch points of the hyperelliptic covering map $\pi\colon C \to \mathbb{P}^1$ as in Lemmas 6.1 and 6.2. Since each of the former gives rise to zero, one or two residue disks on C (when p is odd) and each of the latter gives rise to zero, one or two annuli, one obtains a result similar to Proposition 5.3. The advantage is again that one circumvents the discussion of arithmetic graphs, which, however, has to be replaced by a discussion of partitions of $\mathbb{P}^1(k)$ as above. A disadvantage of this approach is that it is restricted to hyperelliptic curves from the start. Another advantage is that with some modifications it also works for $p = 2$.

No matter which approach is taken, Proposition 7.7 remains the crucial ingredient of the proof.

9. 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 9.1. *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 $\#C(K) \leq R(d,g,r)$.*

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

$$R(1,g,0) = 33(g-1)+1 \qquad \text{and} \qquad R(1,g,r) = 8rg + 33(g-1) - 1 \quad \text{for } r \geq 1.$$

Proof. Fix some odd prime p. Then there are only finitely many possible completions k at places above p of number fields of degree $\leq d$. We take $R(d,g,r)$ to be the maximum of the bounds $N(k,g,r)$ of Theorem 8.1 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 8.1 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 $q = p = 3$). $\square$

Remark 9.2. We note that by choosing $p \approx \sqrt{r}$ for large r instead of $p = 3$, one obtains a bound with leading term $(4r + O(\sqrt{r}))g$.

Remark 9.3. Using the bound in Theorem 8.1 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 $\leq d + 1$ and inert at all reasonably small primes $> d + 1$.)

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

Corollary 9.4. *Let C be a hyperelliptic curve of genus $g \geq 3$ over $\mathbb{Q}$. Then any torsion packet on C can contain at most $33(g - 1) + 1$ rational points.*

Recall that a *torsion packet* on C is a subset of C such that the difference of any two points in the set is a torsion point on the Jacobian.

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

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

(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! An analogous statement holds for the size of a set of rational points mapping into a subgroup of rank $\leq r$.

10. A uniform version of the Poonen-Stoll result

Let C be a curve of genus g over the p-adic field k. We fix a k-basis $\underline{\omega} = (\omega_1, \ldots, \omega_g)$ of the space of regular differentials on C defined over k. We also fix a point $P_0 \in C(k)$. As in [PS14], we write ρ for the partially defined composition

$$k^g \dashrightarrow k^g \setminus \{0\} \longrightarrow \mathbb{P}^{g-1}(k) \longrightarrow \mathbb{P}^{g-1}(\kappa)$$

(recall that κ denotes the residue field of k). We define the map

$$\log_{\underline{\omega}} \colon C(k) \longrightarrow k^g, \quad P \longmapsto \oint_{P_0}^{P} \underline{\omega}\,;$$

then we have the partially (away from the finitely many points mapping to torsion under the embedding of C into J given by the base-point P_0) defined composition

$$\rho \log_{\underline{\omega}} \colon C(k) \dashrightarrow \mathbb{P}^{g-1}(\kappa)\,.$$

For a subset X of $C(k)$, we write $\rho \log_{\underline{\omega}}(X)$ for the image of the subset of X consisting of elements on which $\rho \log_{\underline{\omega}}$ is defined.

We now specialize to $k = \mathbb{Q}_2$.

Lemma 10.1. *Let $\varphi\colon A_{\alpha,\mathbb{Q}_2} \to C$ be an annulus. Then with the notation introduced above, we have*

$$\#\rho\log_{\underline{\omega}}(\varphi(A_\alpha(\mathbb{Q}_2))) \le 96(g-1)+31\,.$$

Proof. We first need a version of [PS14, Proposition 3.8] for Laurent series. So let $\underline{\ell}$ and $\underline{w}$ be tuples of Laurent series with coefficients in $\mathbb{Q}_2$, converging on A_α and with $d\underline{\ell}(z)/dz = \underline{w}(z)$. By Proposition 6.8, a linear combination $\sum b_j w_j(z)$, with (b_j) a $\mathbb{Z}_2$-basis of the ring of integers of a suitable unramified extension of $\mathbb{Q}_2$, can be written in the form $u(z)h(z)$, where $|h(\xi)-1|<1$ for all $\xi \in A_\alpha(\mathbb{C}_2)$ and u is a Laurent polynomial with exponents contained in $[-2g+1, 2g-3]$. Then

$$\#\rho(\underline{\ell}(A_\alpha(\mathbb{Q}_2))) \le 12(g-1)+3\,. \tag{10.1}$$

This can be proved in the same way as [PS14, Proposition 3.8]; the point is that the relevant range of exponents of $\underline{\ell}$ is contained in $[-2g+2-\delta(v,2g-3), 2g-2+\delta(v,2g-3)]$. We also use $\delta(v,n) \le 1+n/2$. (This is also analogous to the proof of Proposition 7.7.)

Write $\varphi^*\underline{\omega} = d\underline{\ell}(z) + \underline{c}\frac{dz}{z}$ with $\underline{c} \in \mathbb{Q}_2^g$; we can assume that the constant term in $\underline{\ell}(z)$ is zero. Let $\underline{a} = (a_1,\dots,a_g)$ with $a_j = a(\omega_j)$ be the constants arising in Proposition 7.3. Then, by the same proposition, we have

$$\log_{\underline{\omega}}(\varphi(\xi)) = \underline{\ell}(\xi) + \underline{c}\,\mathrm{Log}_0(\xi) + \underline{a}v(\xi) + \underline{b}$$

with a constant vector $\underline{b}$. Let $r\colon \mathbb{Q}_2^g\setminus\{0\} \to \mathbb{F}_2^g\setminus\{0\}$ be the map that first scales its argument by a power of 2 so that its entries are coprime elements of $\mathbb{Z}_2$ and then reduces it mod 2 (so that ρ is r followed by the canonical map $\mathbb{F}_2^g\setminus\{0\} \to \mathbb{P}^{g-1}(\mathbb{F}_2)$). Since the size of $\#\rho\log_{\underline{\omega}}(\varphi(A_\alpha(\mathbb{Q}_2)))$ depends only on the $\mathbb{Z}_2$-module generated by $\underline{\omega}$, we are free to replace $\underline{\omega}$ by any other $\mathbb{Z}_2$-basis of this module. We can choose a basis such that all of $\underline{a}$, $\underline{b}$ and $\underline{c}$ are of the form $(*,*,*,0,\dots,0)$. We assume in the following that $\underline{a}$, $\underline{b}$ and $\underline{c}$ are linearly independent. (If the dimension of their span is strictly less than 3, an argument similar to that carried out below results in a better bound.) For any given $\xi \in A_\alpha(\mathbb{Q}_2)$ such that $\rho\log_{\underline{\omega}}(\varphi(\xi))$ is defined, we then have that $r(\log_{\underline{\omega}}(\varphi(\xi)))$ is of the form $(\beta_1,\beta_2,\beta_3,0,\dots,0)$ with $(\beta_1,\beta_2,\beta_3) \in \mathbb{F}_2^3\setminus\{(0,0,0)\}$ or $(\beta_1,\beta_2,\beta_3,\lambda_4,\dots,\lambda_g)$ with $(\beta_1,\beta_2,\beta_3) \in \mathbb{F}_2^3$, where $(0,0,0,\lambda_4,\dots,\lambda_g) = r(0,0,0,\ell_4(\xi),\dots,\ell_g(\xi))$. This shows that

$$\#\rho\log_{\underline{\omega}}(\varphi(A_\alpha(\mathbb{Q}_2))) \le 8\#\{r(0,0,0,\ell_4(\xi),\dots,\ell_g(\xi)) : \xi \in A_\alpha(\mathbb{Q}_2), (\ell_4,\dots,\ell_g)(\xi)\ne 0\}+7\,. \tag{10.2}$$

Now (10.1), applied to $(\ell_4,\dots,\ell_g)$, gives

$$\#\{r(0,0,0,\ell_4(\xi),\dots,\ell_g(\xi)) : \xi \in A_\alpha(\mathbb{Q}_2), (\ell_4,\dots,\ell_g)(\xi)\ne 0\} \le 12(g-1)+3\,.$$

Using this in (10.2) gives the bound in the statement of the lemma. □

This now implies a uniform bound on $\#\rho\log_{\underline{\omega}}(C(\mathbb{Q}_2))$.

Proposition 10.2. *Let C be a curve of genus g over $\mathbb{Q}_2$. Then*

$$\#\rho\log_{\underline{\omega}}(C(\mathbb{Q}_2)) \le 288(g-1)^2+129(g-1)\,.$$

In particular, $\#\rho\log(C(\mathbb{Q}_2)) \le 288(g-1)^2+129(g-1)$, where $\rho\log$ is as in [PS14].

Proof. We partition $C(\mathbb{Q}_2)$ into residue disks and annuli according to Proposition 5.3. Write $C_D(\mathbb{Q}_2)$ for the union of disks and $C_A(\mathbb{Q}_2)$ for the union of annuli. By [PS14, Proposition 5.4] (with $p = 2$), we have $\#\rho\log_{\underline{\omega}}(C_D(\mathbb{Q}_2)) \leq 5d + 6g - 6$ where d is the number of disks. By Proposition 5.3, $d \leq 12(g-1) - 6(t-1)$ and there are at most $2g - 3 + t$ annuli, for some $0 \leq t \leq g$. This leads to the bound

$$\begin{aligned}\#\rho\log_{\underline{\omega}}(C(\mathbb{Q}_2)) &\leq \#\rho\log_{\underline{\omega}}(C_D(\mathbb{Q}_2)) + \#\rho\log_{\underline{\omega}}(C_A(\mathbb{Q}_2)) \\ &\leq \max_{0\leq t\leq g}\big\{66(g-1) - 30(t-1) + (2(g-1)+(t-1))(96(g-1)+31)\big\} \\ &= 288(g-1)^2 + 129(g-1)\end{aligned}$$

as claimed. The $\rho\log$ map from [PS14] is $\rho\log_{\underline{\omega}}$ for a specific choice of $\underline{\omega}$. □

We remark that this bound can be improved somewhat with a bit more work for hyperelliptic curves C. For example, one can use the approach of Section 6 to get a partition of $C(\mathbb{Q}_2)$ into disks and (not necessarily maximal) annuli such that on the annuli the statement of Corollary 6.7 holds. This gives an improvement of roughly a factor 2, so that the conclusion of Corollary 10.3 below already holds for $g = 17$. However, it appears that our method will not produce a bound better than linear in g for the size of the image of an annulus under $\rho\log$, and so the final bound for $\#\rho\log(C(\mathbb{Q}_2))$ will stay quadratic in g.

We finally obtain a uniformity result for the density of odd degree hyperelliptic curves with only one rational point in any family defined by congruence conditions, assuming the genus is sufficiently large.

Corollary 10.3. *Let $g \geq 18$ and consider any subfamily $\mathcal{F}$ of odd degree hyperelliptic curves of genus g over $\mathbb{Q}$ defined by finitely many congruence conditions and ordered by height as in* [PS14]. *Then the lower density of curves in $\mathcal{F}$ whose only rational point is the point at infinity is at least $1 - \big(576(g-1)^2 + 258(g-1) + 2\big)2^{-g} > 0$.*

Proof. This follows from Proposition 8.13 of [PS14] (with $p = 2$), since we know from Proposition 10.2 that (in the notation of [PS14]) $\#I \leq 288(g-1)^2 + 129(g-1)$. □

The lower bound on the density tends to 1 quickly as $g \to \infty$, so we can phrase this result as 'most odd degree hyperelliptic curves in any congruence family have only one rational point.'

References

[AW71] M. Artin and G. Winters, *Degenerate fibres and stable reduction of curves*, Topology **10** (1971), 373–383. MR0476756 (57 #16313) ↑1, 4, 4

[Ber07] Vladimir G. Berkovich, *Integration of one-forms on p-adic analytic spaces*, Annals of Mathematics Studies, vol. 162, Princeton University Press, Princeton, NJ, 2007. MR2263704 (2008a:14035) ↑7.2

[Ber11] Daniel Bertrand, *Special points and Poincaré bi-extensions*, 2011. Preprint, `arXiv:1104.5178`, with an appendix by Bas Edixhoven. ↑2

[Ber13] D. Bertrand, *Unlikely intersections in Poincaré biextensions over elliptic schemes*, Notre Dame J. Form. Log. **54** (2013), no. 3-4, 365–375, DOI 10.1215/00294527-2143907. MR3091662 ↑2

[BGR84] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 261, Springer-Verlag, Berlin, 1984. A systematic approach to rigid analytic geometry. MR746961 (86b:32031) ↑5.2

[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) ↑5

[BL84] ———, *Stable reduction and uniformization of abelian varieties. II*, Invent. Math. **78** (1984), no. 2, 257–297, DOI 10.1007/BF01388596. MR767194 (86j:14040b) ↑7

[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, 2, 2, 2

[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*, Compos. Math. **149** (2013), no. 11, 1818–1838, DOI 10.1112/S0010437X13007410. MR3133294 ↑1, 7

[KRZB15] Eric Katz, Joseph Rabinoff, and David Zureick-Brown, *Uniform bounds for the number of rational points on curves of small Mordell-Weil rank*, April 25, 2015. Preprint, `arXiv:1504.00694v2 [math.NT]`. ↑1, 6, 7.2, 7.5

[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) ↑4, 4, 4, 4.3

[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

[Maz00] ———, *Abelian varieties and the Mordell-Lang conjecture*, Model theory, algebra, and geometry, Math. Sci. Res. Inst. Publ., vol. 39, Cambridge Univ. Press, Cambridge, 2000, pp. 199–227. MR1773708 (2001e:11061) ↑1

[MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit methods in number theory, Panor. Synthèses, vol. 36, Soc. Math. France, Paris, 2012, pp. 99–117 (English, with English and French summaries). MR3098132 ↑1

[Pac97] Patricia L. Pacelli, *Uniform boundedness for rational points*, Duke Math. J. **88** (1997), no. 1, 77–102, DOI 10.1215/S0012-7094-97-08803-7. MR1448017 (98b:14020) ↑1

[Pin05] Richard Pink, *A Common Generalization of the Conjectures of André-Oort, Manin-Mumford, and Mordell-Lang*, 2005. Preprint, `http://www.math.ethz.ch/~pink/ftp/AOMMML.pdf`. ↑2

[PS14] Bjorn Poonen and Michael Stoll, *Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) **180** (2014), no. 3, 1137–1166, DOI 10.4007/annals.2014.180.3.7. MR3245014 ↑1, 1, 2, 10, 10, 10, 10.2, 10, 10.3, 10

[Sto06] Michael Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR2264661 ↑1, 2, 7, 7

[Zan12] Umberto Zannier, *Some problems of unlikely intersections in arithmetic and geometry*, Annals of Mathematics Studies, vol. 181, Princeton University Press, Princeton, NJ, 2012. With appendixes by David Masser. ↑1, 2

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

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

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