COMPOSITIO MATHEMATICA

An effective Chabauty–Kim theorem

Jennifer S. Balakrishnan and Netan Dogra

Compositio Math. **155** (2019), 1057–1075.

doi:10.1112/S0010437X19007243

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

Compositio Math. 155 (2019) 1057–1075
doi:10.1112/S0010437X19007243

An effective Chabauty–Kim theorem

Jennifer S. Balakrishnan and Netan Dogra

Abstract

The Chabauty–Kim method allows one to find rational points on curves under certain technical conditions, generalising Chabauty's proof of the Mordell conjecture for curves with Mordell–Weil rank less than their genus. We show how the Chabauty–Kim method, when these technical conditions are satisfied in depth 2, may be applied to bound the number of rational points on a curve of higher rank. This provides a non-abelian generalisation of Coleman's effective Chabauty theorem.

1. Introduction

Chabauty's method [Cha41] is one of the most powerful tools for studying the Diophantine geometry of curves of genus larger than 1. In its original form, it gives a proof of the Mordell conjecture for curves $X/\mathbb{Q}$ of genus g whose Jacobians have Mordell–Weil rank less than g. The simple idea underlying the proof is to try to prove finiteness of the rational points of a curve X with Jacobian J by bounding the intersection of $X(\mathbb{Q}_p)$ and the p-adic closure of $J(\mathbb{Q})$ inside $J(\mathbb{Q}_p)$.

This paper concerns two subsequent refinements of Chabauty's argument. The first, due to Coleman, is an effective version in the sense of giving a bound on the number of rational points. This amounts to replacing 'soft analysis' (finding, on each residue disk of $X_{\mathbb{Q}_p}$, a non-trivial power series vanishing on $X(\mathbb{Q})$), with 'hard analysis' (giving a bound on the number of zeros of this power series). By bounding the number of zeros of this power series, Coleman produces a bound on the size of $X(\mathbb{Q})$.

The second, due to Kim [Kim05, Kim09], gives a generalisation of Chabauty's method which replaces the Jacobian with a non-abelian cohomology variety with values in (finite-dimensional quotients of) a motivic fundamental group in the sense of Deligne [Del89]. As explained in the next section, Kim's method produces a decreasing sequence of subsets $X(\mathbb{Q}_p) \supset X(\mathbb{Q}_p)_1 \supset X(\mathbb{Q}_p)_2 \supset \cdots \supset X(\mathbb{Q})$. Conjecturally, $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$ for all $n \gg 0$. However, in general it is not known that $X(\mathbb{Q}_p)_n$ is eventually finite. By work of Coates and Kim [CK10], we know unconditionally that $X(\mathbb{Q}_p)_n$ is finite for $n \gg 0$ when X is a curve whose Jacobian has complex multiplication. Recently, Ellenberg and Hast extended this result to give a new proof of Faltings' theorem for solvable covers of $\mathbb{P}^1$ [EH17].

In this paper we only use the set $X(\mathbb{Q}_p)_2$, which is much simpler to describe. In analogy with Coleman's original result, we bound the size of $X(\mathbb{Q})$, under certain technical conditions, by bounding the size of $X(\mathbb{Q}_p)_2$. Just as with the original effective Chabauty results, if one is

Received 11 May 2018, accepted in final form 24 January 2019, published online 14 May 2019.
2010 Mathematics Subject Classification 14G05 (primary), 11D45 (secondary).
Keywords: rational points, curves, effective methods.
Balakrishnan is supported in part by NSF grant DMS-1702196, the Clare Boothe Luce Professorship (Henry Luce Foundation), and Simons Foundation grant #550023.

careful, one can improve the bounds in various ways, but, in the interest of simplicity, here we focus on the problem of finding an explicit bound on $X(\mathbb{Q}_p)_2$ which is polynomial in the genus.

To explain our conditions more precisely, we introduce some notation. Let X be a curve of genus $g > 1$ over $\mathbb{Q}$, with $\operatorname{rk}\operatorname{Jac}(X) = r = g$. Define

$$\rho_f(J) := \dim \mathrm{NS}(\mathrm{Jac}(X_{\mathbb{Q}})) + \dim(\mathrm{NS}(\mathrm{Jac}(X_{\overline{\mathbb{Q}}})^{c=-1})).$$

Our finiteness results will be dependent on one of the following conditions being satisfied.

- Condition A: $r = g$ and $\rho_f(J) > 1$.
- Condition B: $r = g$ and

$$\dim H^1_f(G_T, H^2_{\text{ét}}(X \times X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(1))) = 0.$$

For a generic curve X, the rank $\rho(J)$ of the Néron–Severi group of J will be 1, and hence Condition A will not hold. However, the condition that $\rho_f(J) > 1$ still arises in many examples of interest. For example, if X is a non-trivial cover of a curve of higher genus, or more generally, if J is isogenous to a product of two abelian varieties, then $\rho_f(J) \geqslant \rho(J) \geqslant 2$. By contrast, it is very difficult to give examples when Condition B is satisfied; however, as explained in [BD17, Lemma 2.4], the latter part of Condition B is implied by a conjecture of Bloch and Kato [BK90, Conjecture 5.3(i)].

By [BD17, Proposition 2.2, Lemma 2.6], one may prove the finiteness of $X(\mathbb{Q}_p)_2$ if Condition A or Condition B holds. For v a prime of bad reduction, we define $n_v \in \mathbb{Z}_{>0}$ to be the size of the image of $X(\mathbb{Q}_v)$ under $j_{2,v}$ (see the next section for a precise definition).

Theorem 1.1. *Let $X/\mathbb{Q}$ be a curve of genus $g > 1$ with good reduction at a prime $p \geqslant 3$, satisfying Condition A or Condition B. Let $\kappa_p = 1 + (p-1)/((p-2)\log(p))$. Then:*

(i) $\#X(\mathbb{Q}) < \kappa_p(\prod_{v \in T_0} n_v)\#X(\mathbb{F}_p)(16g^3 + 15g^2 - 16g + 10)$;

(ii) *if X is hyperelliptic and $p \neq 2g+1$, then*

$$\#X(\mathbb{Q}) < \kappa_p\biggl(\prod_{v \in T_0} n_v\biggr)((2g+2)\#X(\mathbb{F}_p) + 2g\#W(\mathbb{F}_p) + 8g^3 + 64g^2 + 20g + 16),$$

where W is the subscheme of Weierstrass points.

As will be explained in the next section, one may obtain bounds on the local constants n_v in terms of the reduction data of the curve X at v. It seems difficult to avoid the bounds obtained by the non-abelian Chabauty method depending on how bad the reduction of X is at bad primes. For this reason, the extent to which this theorem could be used directly to prove uniformity results in the manner of Stoll [Sto19] and Katz, Rabinoff, and Zureick-Brown [KRZ16] is unclear.

However, in special cases, one can control the local factors to provide uniform bounds on the number of rational points of special families of curves. We illustrate this with the following corollary.

Corollary 1.2. *Let $X/\mathbb{Q}$ be a smooth projective hyperelliptic curve of genus g with good reduction at 3 and potential good reduction at all primes. If the curve satisfies Condition A or Condition B, then*

$$\#X(\mathbb{Q}) < 23g^3 + 201g^2 + 122g + 68.$$

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

An example of a hyperelliptic curve satisfying the hypotheses regarding the reduction type is given by

$$X : y^2 = x^n + k,$$

where n is a square-free positive integer prime to 6 and k is an integer prime to 3. If n is composite, then X also satisfies $\rho(J) > 1$, and hence in this case the bound on the number of rational points will hold whenever $r = g$.

The method of proof of Theorem 1.1 may also be used to bound the number of integral points on hyperelliptic curves, answering a question of [BBM16].

Theorem 1.3. *Let X be a smooth projective hyperelliptic curve of genus g with good reduction at $p \geqslant 3$ and Mordell–Weil rank g. Suppose X has a rational Weierstrass point ∞; let $Y := X - \infty$, and let $Y(\mathbb{Z})$ denote the set of integral points of Y with respect to a minimal regular model. Then*

$$\#Y(\mathbb{Z}) < \kappa_p \bigg(\prod_{v \in T_0} m_v\bigg)(8g^3 + 44g^2 - 34g + 9 + (2g+1)\#Y(\mathbb{F}_p) + (2g-1)\#W(\mathbb{F}_p))$$

if $g > 1$ and

$$\#Y(\mathbb{Z}) < 2\kappa_p \bigg(\prod_{v} m_v\bigg) \#Y(\mathbb{F}_p)$$

if $g = 1$, where the m_v are local constants as in [BBM16], and W denotes the scheme of Weierstrass points not equal to ∞.

To explain the method of proof, we briefly recall Coleman's proof of effective Chabauty [Col85]. There, he gave a bound for the number of zeros of $G := \int \omega$ in a residue disk $]\,\overline{z}\,[$ for ω a global differential. This bound is derived from understanding some piece of the Newton polygon of G: specifically, from bounding the length of the slope -1 segment of the Newton polygon. By *length* of a segment, we take the usual convention: the length of the projection of the segment onto the x-axis. We recall the following classical result.

Proposition 1.4. *Suppose the slope $\leqslant -1$ segment of the Newton polygon has endpoint (M, N). Then G has at most M zeros in $B(0, |p|)$.*

Proof. See, for example, [Kob84, IV.4]. □

In particular, Coleman related the Newton polygon of G to the zeros of ω mod p, which can be bounded by elementary algebraic geometry.

The idea of the proof in the depth 2 case is similar. We want to bound the number of zeros of a non-algebraic power series G (from depth 2 Chabauty–Kim; see Proposition 2.3) in a residue disk $]\,\overline{z}\,[$, or equivalently, understand the slopes of its Newton polygon. We would like to reduce this to a question about the slopes of something algebraic, but as G involves double integrals, we have to replace simply taking the derivative by applying a more complicated differential operator $\mathcal{D}$. We show in § 3 that for suitable 'nice' differential operators, we can relate the Newton polygon of G to the zeros of $\mathcal{D}(G)$. We then want to find a $\mathcal{D}$ that sends our power series G to some algebraic function whose zeros we can bound mod p. We give constructions of $\mathcal{D}$ in the general case, hyperelliptic case, and hyperelliptic and integral points case in the three subsequent sections.

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

2. Explicit Chabauty–Kim at depth 2

We begin with a brief review of a few essential results from the Chabauty–Kim method [Kim05, Kim09]. Associated to a pointed curve (X, b) over $\mathbb{Q}$, with good reduction outside a finite set T_0, and a prime p of good reduction, we have a map

$$j_n : X(\mathbb{Q}) \to H^1(G_T, U_n),$$

where $T := T_0 \cup \{p\}$, G_T is the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside T, and U_n is the maximal n-unipotent quotient of the $\mathbb{Q}_p$ pro-unipotent completion of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)$. We also have local maps

$$j_{n,v} : X(\mathbb{Q}_v) \to H^1(G_{\mathbb{Q}_v}, U_n)$$

for v in T_0 and

$$j_{n,p} : X(\mathbb{Q}_p) \to H^1(G_{\mathbb{Q}_p}, U_n)$$

(for the definition of $H^1_f(G_{\mathbb{Q}_p}, U_n)$ see [Kim05]). We define

$$X(\mathbb{Q}_p)_n := j_{n,p}^{-1}\biggl(\mathrm{loc}_p\biggl(\bigcap_{v \in T_0} \mathrm{loc}_v^{-1}(X(\mathbb{Q}_v))\biggr)\biggr) \subset X(\mathbb{Q}_p),$$

where loc_v is the localisation map from $H^1(G_T, U_n)$ to $H^1(G_v, U_n)$. By construction, the set of rational points $X(\mathbb{Q})$ is a subset of $X(\mathbb{Q}_p)_n$ for all n.

The behaviour of the maps $j_{n,v}$ is fundamentally different depending on whether or not $v = p$. In the $v \neq p$ case, we have the following theorem, due to Kim and Tamagawa [KT08, Corollary 0.2].

Theorem 2.1 (Kim and Tamagawa). *Let v be a prime not equal to p. Then for all n, $\mathrm{im}(j_{v,n})$ is finite.*

In fact, one can bound the image of $j_{n,v}$ in terms of the reduction data of the curve as follows. Let L be a finite extension of $\mathbb{Q}_v$ over which X_L acquires stable reduction. Let $\mathcal{X}/\mathcal{O}_L$ be a regular semistable model, and let $V(\mathcal{X}_{k_L})$ denote the set of irreducible components of the special fibre. Since the model is regular, specialisation induces a well-defined map

$$r_v : X(\mathbb{Q}_v) \to V(\mathcal{X}_{k_L}).$$

For v a prime of bad reduction, we define $n_v \in \mathbb{Z}_{>0}$ to be the size of the image of $X(\mathbb{Q}_v)$ under $j_{2,v}$ in $H^1(G_v, U_2)$.

Lemma 2.2. *With notation as above,*

$$n_v \leqslant \mathrm{im}(r_v).$$

A detailed proof of this lemma will appear in forthcoming work of the second named author and Alex Betts. However, for the sake of completeness, we briefly indicate the method of proof. First, if $L|\mathbb{Q}_v$ is a finite extension, then it is easy to show that $H^1(G_{\mathbb{Q}_v}, U_n) \to H^1(G_L, U_n)$ is injective, hence one reduces to the case where X has stable reduction. In this case, one can use the description of the action of G_L on $\pi_1^{\text{ét},(v')}(X_{\overline{\mathbb{Q}}_v}, b)$ (the maximal prime-to-v quotient of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}_v}, b)$) in terms of the dual graph of a regular

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

semistable model given in [Oda95] to deduce that if points b_1 and b_2 lie on a common irreducible component of $V(\mathcal{X}_{k_L})$, then the class of $[\pi_1^{\text{ét},(v')}(X_{\overline{\mathbb{Q}}_v}; b_1, b_2)]$ in $H^1(G_L, \pi_1^{\text{ét},(v')}(X_{\overline{\mathbb{Q}}_v}, b_1))$ is trivial. This straightforwardly implies the lemma.

The finiteness of the maps $j_{n,v}$ allows us to partition the set $X(\mathbb{Q}_p)_n$ as follows. We refer to a tuple $\alpha = (\alpha_v)_v$ in $\prod_{v\in T_0} \operatorname{im}(j_{n,v})$ as a collection of *local conditions*, and define

$$X(\mathbb{Q}_p)_\alpha := j_{n,p}^{-1}\biggl(\operatorname{loc}_p\biggl(\bigcap_{v\in T_0} \operatorname{loc}_v^{-1}(\alpha_v)\biggr)\biggr) \subset X(\mathbb{Q}_p).$$

By construction, $X(\mathbb{Q}_p)_n$ is the disjoint union of the $X(\mathbb{Q}_p)_\alpha$ for α a collection of local conditions. The bound in Theorem 1.1 comes from a bound on $\#X(\mathbb{Q}_p)_\alpha$ in the case of $n = 2$, together with a bound on the number of local conditions, that is, on the size of $\prod_{v\in T_0} j_{2,v}X(\mathbb{Q}_v)$.

2.1 Local structure at p

The power series G in the introduction is from the following result of [BD17].

Proposition 2.3 [BD17, Proposition 6.4]. *Let $X/\mathbb{Q}$ be a curve of genus $g > 1$. Suppose X satisfies Condition A or Condition B. Let $\omega_0, \dots, \omega_{2g-1} \in H^0(X, \Omega(D))$ be differentials of the second kind forming a basis of $H^1_{\mathrm{dR}}(X)$, where D is an effective divisor. Then, for all local conditions α, there are constants a_{ij} and a_i, a differential of the third kind η, and a function $h \in H^0(X, \mathcal{O}(2D))$ such that*

$$X(\mathbb{Q}_p)_\alpha \subset \{z \in X(\mathbb{Q}_p) : G(z) = 0\},$$

where

$$G(z) := \sum_{0\leqslant i,j<2g} a_{ij} \int_b^z \omega_i\omega_j + \sum_{0\leqslant i<2g} a_i \int_b^z \omega_i + \int_b^z \eta + h(z).$$

2.2 Proof of Corollary 1.2

In this subsection we prove that Theorem 1.1 implies Corollary 1.2.

Lemma 2.4. *Let $v \neq p$ be a prime of potential good reduction. Then, for all n, the map*

$$j_{n,v} : X(\mathbb{Q}_v) \to H^1(G_v, U_n)$$

is trivial.

Proof. Let $L|\mathbb{Q}_v$ be an extension over which X acquires good reduction. Then the map

$$j_{n,L} : X(L) \to H^1(G_L, U_n)$$

has trivial image. Recall from [Ser97, I.5.8] that, given a profinite group G, closed normal subgroup H, and G-group A, we get an exact sequence of pointed sets

$$H^1(G/H, A^H) \to H^1(G, A) \xrightarrow{\text{Res}} H^1(H, A).$$

We apply this when $G = G_v$, $H = G_L$. We claim $U_n^{G_L} = 1$. To see this, note that it is enough to show that the graded pieces $U_n[i]$ of U_n with respect to the central series filtration satisfy $U_n[i]^{G_w} = 1$, which follows from the fact that $U_n[i]$ is an unramified representation of G_L of weight $-i$.

Hence we deduce that the restriction map

$$H^1(G_v, U_n) \xrightarrow{\text{Res}} H^1(G_L, U_n)$$

is injective. The lemma thus follows from commutativity of the following diagram.

$$\begin{tikzcd} X(\mathbb{Q}_v) \arrow[r, "j_{n,v}"] \arrow[d] & H^1(G_v, U_n) \arrow[d, "\text{Res}"] \\ X(L) \arrow[r, "j_{n,w}"] & H^1(G_L, U_n) \end{tikzcd}$$

□

Now let X be as in Corollary 1.2. Then all the n_v are 1. Taking $p = 3$ and using the Hasse–Weil estimate $\#X(\mathbb{F}_3) \leqslant 4 + 2g\sqrt{3}$ and the trivial bound $\#W(\mathbb{F}_3) \leqslant 4$, we deduce

$$\#X(\mathbb{Q}) \leqslant (8g^3 + (64 + 4\sqrt{3})g^2 + (64 + 4\sqrt{3})g + 24)\kappa_3,$$

from which the corollary follows.

3. Bounding the number of zeros via a differential operator

In this section, we explain how to bound the zeros of a power series G by finding a bound on $\mathcal{D}(G)$ for a suitably 'nice' (in a way we will make precise shortly) differential operator $\mathcal{D}$. The construction of a nice differential operator in the case when G is the Coleman function from Proposition 2.3 will be given in the next section.

We begin by fixing notation. We denote by v the p-adic valuation homomorphism $\mathbb{Q}_p^\times \to \mathbb{Z}$. We fix a point b and a rational function x which is a uniformising parameter at b. We let $]\,b\,[$ denote the tube (or *residue disk*) of b, that is, the set of points reducing to b mod p (we also denote this set as $]\,\overline{b}\,[$, where $\overline{b}$ is the mod p reduction of b). Given an analytic function F on $]\,b\,[$, we let $N_b(F)$ denote the number of $\mathbb{C}_p$-valued zeros of F in $]\,b\,[$, counted with multiplicity.

Let C_i denote the function $\mathbb{Q}_p[\![x]\!] \to \mathbb{Q}_p$ sending a power series to its x^i coefficient. By a differential operator we will simply mean an element of the non-commutative ring $\mathbb{Q}_p[\![x]\!][d/dx]$. By an algebraic differential operator we will mean a differential operator in the image of $\mathbb{Q}_p(X)[d/dx]$, where $\mathbb{Q}_p(X)$ denotes the function field of X over $\mathbb{Q}_p$. The *order* of a differential operator will refer to its degree as a polynomial in d/dx, when given in the form $\sum_{i=0}^N a_i(d/dx)^i$, for $a_i \in \mathbb{Q}_p[\![x]\!]$.

Definition 3.1. A differential operator $\mathcal{D} = \sum_{i=0}^N g_i(d^i/dx^i) \in \mathbb{Q}_p[\![x]\!][d/dx]$ is *nice* if all the g_i are in $\mathbb{Z}_p[\![x]\!]$, and g_N is in $\mathbb{Z}_p[\![x]\!]^\times$.

The main result of this section is the following proposition, which shows that one may use nice differential operators to bound the zeros of power series, in analogy with Coleman's use of differentiation.

Proposition 3.2. *Let G be a power series in $\mathbb{Q}_p[\![x]\!]$. Let $\mathcal{D}$ be a nice differential operator of order N. Suppose $\mathcal{D}(G)$ is an algebraic function with no poles on $]\,b\,[$. Then the number of zeros of G in $]\,b\,[$ is at most $\kappa_p(N_b(\mathcal{D}(G)) + N)$.*

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

The proof of this proposition will occupy the remainder of the section. Before giving the proof, we remark on how it is applied in the proof of Theorem 1.1. To deduce part (i) of the theorem, it will be enough to deduce (under the assumptions of the theorem) that, for each $b \in X(\mathbb{F}_p)$ and each set of local conditions α, we may choose a non-zero effective divisor D disjoint from $]\,b\,[$, and differentials $\omega_0, \ldots, \omega_{2g-1}$ and a nice differential operator $\mathcal{D}$ of degree N, such that

$$N_b(\mathcal{D}(G)) + N \leqslant 16g^3 + 15g^2 - 16g + 10,$$

where G is the function from Proposition 2.3. In practice, we bound the number of zeros of $\mathcal{D}(G)$ in $]\,b\,[$ by the degree of $\mathcal{D}(G)$. In the hyperelliptic case, we choose D, ω_i, and G in a more uniform way (more precisely, they are the same for all points in $X - W$), and for this reason, we get an improved bound

$$\sum_{x \in (X-W)(\mathbb{F}_p)} N_b(\mathcal{D}(G)) + N \leqslant \deg(\mathcal{D}(G)) + N\#(X - W)(\mathbb{F}_p).$$

Lemma 3.3. *Let $F \in \mathbb{Q}_p[\![x]\!]$ come from a non-zero element of $\mathbb{Q}_p(X)$ without poles in $]\,b\,[$. Then $\{v(C_i(F)) : i \geqslant 0\}$ is bounded below, and the least i such that $v(C_i(F))$ attains this bound is less than or equal to $N_b(F)$.*

Proof. There is some λ in $\mathbb{Q}_p$ such that λF reduces to a non-zero rational function on $X_{\mathbb{F}_p}$. Since F has no poles in $]\,b\,[$, the reduction mod p of λF is the $\mathrm{red}_p(x)$-adic expansion of λF thought of as a rational section of $X_{\mathbb{F}_p}$, hence the least i such that the minimum of $v(C_i(F))$ is attained is just the order of $\mathrm{red}_p(\lambda F)$. □

Now let G be a power series in $\mathbb{Q}_p[\![x]\!]$, with $\mathcal{D}(G) \in H^0(X, \mathcal{O}(D))$, with D an effective divisor (in our intended application, G will be the power series in Proposition 2.3). Let M denote the length of the slope $\leqslant -1$ part of the Newton polygon. Write $\mathcal{D}$ as $\sum_{i=1}^N g_i(d/dx)^i$, where $g_N \in \mathbb{Z}_p[\![x]\!]^\times$. Recall the following well-known lemma.

Lemma 3.4. *For any $n_1 \leqslant n_2$,*

$$v\left(\frac{n_2!}{n_1!}\right) \leqslant \log_p(n_1) + \frac{n_2 - n_1}{p-1}.$$

Proof. Using Legendre's formula $v(n!) = (n - s(n))/(p-1)$, where $s(n)$ is the sum of digits in base p, it follows that

$$\begin{aligned} v\left(\frac{n_2!}{n_1!}\right) = \frac{n_2 - n_1}{p-1} + \frac{s(n_1) - s(n_2)}{p-1} &\leqslant \frac{n_2 - n_1}{p-1} + \frac{s(n_1)}{p-1} \\ &\leqslant \frac{n_2 - n_1}{p-1} + \frac{(p-1)\log_p(n_1)}{p-1} \\ &= \frac{n_2 - n_1}{p-1} + \log_p(n_1). \end{aligned}$$ □

Lemma 3.5. *Let M be the length of the slope $\leqslant -1$ part of the Newton polygon of G. Suppose that $M > 1$, and $i \leqslant M$ satisfies*

$$v(C_i(G)) \leqslant v(C_M(G)) + v(M!/i!).$$

Then $i \geqslant \kappa_p^{-1} M$.

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

Proof. Since $i \leqslant M$ and M is the length of the slope $\leqslant -1$ part of the Newton polygon, we have

$$M - i \leqslant v(C_i(G)) - v(C_M(G)) \leqslant v(M!/i!).$$

This implies $\log_p(i) + (M-i)/(p-1) \geqslant M - i$, by the previous lemma. Using the inequality $\log_p(i) \leqslant i/\log(p)$, we get

$$\kappa_p i \geqslant M. \qquad \square$$

Given a power series F, let $S(F) = \{i \geqslant 0 : v(C_i(F)) = \min\{v(C_j(F)) : j \geqslant 0\}\}$ if this minimum exists, and take S to be empty otherwise.

We now prove a key lemma which gives a quantitative relation between the Newton polygon of G and the Newton polygon of $\mathcal{D}(G)$, when $\mathcal{D}$ is a nice differential operator. The idea of the proof is as follows. Let s denote the least i such that $v(C_i(\mathcal{D}(G)))$ attains its minimum. We would like to say that if the valuation of $C_M(G)$ is smaller than the valuation of $C_i(G)$ for all $i < M$, then the valuation of $C_{M-N}(\mathcal{D}(G))$ is smaller than that of $C_i(\mathcal{D}(G))$ for all $i < M - N$ (and hence $s \geqslant M - N$).

This is not quite true, because when we apply $(d/dx)^N$ to $C_M(G)x^M$, we increase the valuation by $v(M!/(M-N)!)$, so it may happen that there is some cancellation. However, for such cancellation to occur, there must be an $M_1 < M$ for which $v(C_{M_1}(G))$ is within $v(M!/(M-N)!)$ of $v(C_M(G))$. Similarly, if $v(C_{M_1-N}(\mathcal{D}(G)))$ is not smaller than $v(C_i(\mathcal{D}(G)))$ for all $i < M_1 - N$, then there must be some $M_2 < M_1$ such that $v(C_{M_2}(G))$ is close to $v(C_{M_1}(G))$, and so on, giving a sequence $M, M_1, \ldots$ until we get to $M_n \leqslant s + N$. By construction, the $v(C_{M_i}(G))$ are 'close together', but since M is the endpoint of the slope $\leqslant -1$ part of the Newton polygon they are also 'far apart', and comparing these two conditions gives the lemma.

Note that, without any additional conditions on $\mathcal{D}$ or G, to prove a result of the form '$\mathcal{D}(G)$ has small slopes implies G has small slopes', it is necessary to assume $p > 2$ (consider, for example, the case $\mathcal{D} = (d/dx) - 1$ and $G = \exp(x) + 1$). Note that, by Lemma 3.3, if F is algebraic without poles on $]\,b\,[$, then $\min S(F) \leqslant \operatorname{ord}_{\overline{b}}(\operatorname{red}_p(F))$. Hence the following lemma implies Proposition 3.2.

Lemma 3.6. *Let $p > 2$, and let M be the length of the slope $\leqslant -1$ part of the Newton polygon of G. Suppose $S(\mathcal{D}(G))$ is non-empty. Then*

$$M < \kappa_p(N + \min S(\mathcal{D}(G))).$$

Proof. For integers $i \leqslant j$, let

$$q(i,j) := \begin{cases} v(i!/(j-N)!), & \text{if } i \geqslant j - N, \\ 0, & \text{otherwise.} \end{cases}$$

For $k \geqslant 0$, let

$$T(k) = \{0 \leqslant i \leqslant k : v(C_i(G)) + q(i,k) \leqslant v(C_k(G)) + q(k,k)\}.$$

Clearly, for all k, we have $k \in T(k)$. Suppose $N \leqslant k \leqslant M$, and $T(k) = \{k\}$. It follows that

$$v(C_{k-N}(\mathcal{D}(G))) = v(C_k(G)) + q(k,k). \tag{1}$$

Indeed, writing $\mathcal{D} = \sum g_i(d^i/dx^i)$, we have that

$$C_{k-N}(\mathcal{D}(G)) = \sum_{i,j,m \in \{0,\ldots,N\} \times \mathbb{Z}^2_{\geqslant 0} : j+m-i = k-N} \frac{m!}{(m-i)!} C_m(G) C_j(g_i). \tag{2}$$

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

Note that $v((k!/(k-N)!)C_k(G)C_0(g_N)) = q(k,k)+v(C_k(G))$ by assumption. For i in $\{0,\dots,N\}$ and j,m in $\{0,\dots k\}$ such that $j+m-i=k-N$, by our assumption on $T(k)$ we have

$$\begin{aligned} v\left(\frac{m!}{(m-i)!}C_m(G)C_j(g_i)\right) &\geqslant v(C_m(G))+v(m!)-v((m-i)!) \geqslant v(C_m(G))+q(m,k) \\ &\geqslant v(C_k(G))+q(k,k), \end{aligned}$$

with simultaneous equalities if and only if $(i,j,m)=(N,0,k)$.

For all $0 \leqslant a < k-N$, by expanding out $\mathcal{D}(G)$ as in (2), we have

$$\begin{aligned} v(C_a(\mathcal{D}(G))) &\geqslant \min\{v(C_i(G))+q(i,N+i-j) : 0 \leqslant i,j,i+j \leqslant a\} \\ &\geqslant \min\{v(C_i(G))+q(i,k) : 0 \leqslant i \leqslant a\}, \end{aligned}$$

since $i-j \leqslant k-N$ implies $q(i,k) \leqslant q(i,N+i-j)$. Hence by our assumption on $T(k)$, we have

$$v(C_a(\mathcal{D}(G))) > v(C_k(G))+q(k,k).$$

We deduce that if k is less than or equal to M and satisfies $T(k)=\{k\}$, then

$$\min(S(\mathcal{D}(G)))+N \geqslant k. \tag{3}$$

In particular, if $T(M)=\{M\}$, then the lemma follows.

Now suppose that $T(M)$ has cardinality larger than 1. We define a decreasing sequence $M_0,\dots,M_n$ of positive integers as follows. Let $M_0 := M$, and define $M_1 = \min T(M_0)$. If $T(M_1)=\{M_1\}$, this is the end of the sequence, otherwise we define M_2 as the minimum, and so on. Let M_n be the last term in the sequence. Since $T(M_n)=\{M_n\}$, by (3) we have

$$\min(S(\mathcal{D}(G)))+N \geqslant M_n.$$

Note that for each i, we have

$$v(C_{M_{i+1}}(G))+q(M_{i+1},M_i) \leqslant v(C_{M_i}(G))+q(M_i,M_i).$$

Hence

$$v(C_{M_n}(G))-v(C_{M_0}(G)) \leqslant \sum_i (q(M_i,M_i)-q(M_{i+1},M_i)) \leqslant v(M_0!/M_n!).$$

Since they lie in the slope $\leqslant -1$ part of the Newton polygon, this implies that M_n and $M=M_0$ satisfy the inequality $M-M_n \leqslant v(M!/M_n!)$, which by Lemma 3.4 is less than or equal to $\log_p(M_n)+(M-M_n)/(p-1)$. Thus we deduce

$$\min(S(\mathcal{D}(G)))+N \geqslant M_n \geqslant M-\frac{p-1}{p-2}\log_p(M_n).$$

The lemma then follows from the elementary estimate

$$\log_p(M_n) < M_n/\log(p). \qquad \square$$

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

3.1 Example: integral points on elliptic curves

Before describing a general method for constructing suitable nice differential operators, we illustrate how Proposition 3.2 can be used to prove effective versions of known finiteness results in the quadratic Chabauty method by considering the simplest possible case: that of integral points on a rank 1 elliptic curve. By work of Kim [Kim10], we know that integral points on rank 1 elliptic curves are contained in the zeros of

$$G(z) = \int_t^z \omega_0\omega_1 + a\int_t^z \omega_0\omega_0 + b_i$$

for some constants $a, b_i \in \mathbb{Q}_p$, where the number of b_i is determined by the Tamagawa numbers at bad primes. In this case, finding a differential operator is quite simple: if we take $\mathcal{D} = (d/\omega_0)^2$, then

$$\mathcal{D}(G) = x + a.$$

Hence, in the notation of Proposition 3.2, we may take $N = 2$, and $\sum_{b\in(E-O)(\mathbb{F}_p)} N_b(\mathcal{D}(G)) = 2$, giving the bound

$$\#X(\mathbb{Z}_p)_2 < 2\kappa_p \#E(\mathbb{F}_p)\bigg(\prod_v m_v\bigg).$$

4. Differential operators for rational points: general case

To use Proposition 3.2 to bound $X(\mathbb{Q}_p)_2$, it remains to give a construction of a nice differential operator $\mathcal{D}$ such that $\mathcal{D}(G)$ is an algebraic function whose divisor can be controlled when G is the iterated integral function from Proposition 2.3. The construction of the operator $\mathcal{D}$ is elementary. First we make some preliminary notes about calculating the divisor of $\mathcal{D}(F)$ when F and $\mathcal{D}$ are algebraic.

Lemma 4.1. *Let $D = \sum n_i P_i$ be an effective divisor and let $F(x)$ be a function in $H^0(X, \mathcal{O}(D))$. Suppose dx is an algebraic differential with divisor $W - W'$, with W, W' effective, and $W = \sum m_i Q_i$. Define $D_0 := \sum P_i$ and $W_0 := \sum Q_i$. Then, for all $j > 0$,*

$$\frac{d^j F}{dx^j} \in H^0(X, \mathcal{O}(jW + (j-1)W_0 + D + jD_0)).$$

In particular, $d^j F/dx^j \in H^0(X, \mathcal{O}((2j-1)W + (j+1)D))$.

Proof. When $j = 1$, this follows from the fact that the differential dF has poles only in the support of D and has a pole of order $n_i + 1$ at P_i. The differential dx only has zeros at W, each of order 1. The general case follows by induction. □

We now restrict to our specific case of interest. Fix a point $\overline{z}$ in $X(\mathbb{F}_p)$. Let D be an effective divisor on X whose support is disjoint from $]\,\overline{z}\,[$. Let $\omega_0, \ldots, \omega_{2g-1} \in H^0(X, \Omega^1(D))$ be a set of differentials of the second kind forming a basis of $H^1_{\mathrm{dR}}(X)$. Let $x \in \mathbb{Q}_p[\![t]\!]$ be a formal parameter at some point $z_0 \in\,]\,\overline{z}\,[$, such that dx is algebraic with divisor $D_1 - D_0$ (where D_1 and D_0 are effective). Let $f_i := \omega_i/dx \in H^0(X, \mathcal{O}(D + D_1))$. Finally, let η be a differential in $H^0(X, \Omega^1(D))$, and let

$$G(z) := \sum a_{ij}\int_b^z \omega_i\omega_j + \sum a_i \int_b^z \omega_i + \int_b^z \eta + h(z)$$

be the Coleman function from Proposition 2.3.

The first step in constructing a differential operator satisfying the hypotheses of Proposition 3.2 is to reduce to constructing a nice differential operator which kills all the f_i.

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

Lemma 4.2. *Suppose $\mathcal{D}_1 = \sum_{i=0}^{N} g_i(d/dx)^i$ is a nice differential operator of degree N, with coefficients in $H^0(X,\mathcal{O}(E))$, for an effective divisor E such that*

$$\mathcal{D}_1(f_i) = 0$$

for all i. Then $\mathcal{D} := \mathcal{D}_1(d/dx)$ is a nice differential operator with

$$\mathcal{D}(G) \in \begin{cases} H^0(X,\mathcal{O}(E+3(N-1)D_1+(N+3)D)), & N \geqslant 4 \\ H^0(X,\mathcal{O}(E+(2N+1)D_1+(N+3)D)), & N = 2,3. \end{cases}$$

Proof. The operator $\mathcal{D}$ is nice because its leading coefficient is the same as that of $\mathcal{D}_1$. We deal with the $\int \omega_i, \int \eta, h$ and $\int \omega_i\omega_j$ terms of G separately. First, we have

$$\mathcal{D}\left(\int \omega_i\right) = \mathcal{D}_1(f_i) = 0.$$

For $\int \eta$, note that $(d/dx)(\int \eta) = \eta/dx \in H^0(X,\mathcal{O}(D+D_1))$. Thus by Lemma 4.1,

$$\mathcal{D}\left(\int \eta\right) \in H^0(X,\mathcal{O}(E+(2N+1)D_1+(N+1)D)). \tag{4}$$

For h, by Lemma 4.1 we have, for all $k > 0$,

$$\frac{d^k h}{dx^k} \in H^0(X,\mathcal{O}((2k-1)D_1+(k+2)D)),$$

hence

$$\mathcal{D}(h) \in H^0(X,\mathcal{O}((2N+1)D_1+(N+3)D+E)). \tag{5}$$

Finally,

$$\begin{aligned}\mathcal{D}\left(\int \omega_i\omega_j\right) &= \mathcal{D}_1\left(f_i\int \omega_j\right) \\ &= \sum_{k\leqslant N} g_k\left(\frac{d}{dx}\right)^k\left(f_i\int\omega_j\right) \\ &= \sum_{k\leqslant N} g_k \sum_{0\leqslant m\leqslant k}\binom{k}{m}\left(\frac{d}{dx}\right)^m(f_i)\left(\frac{d}{dx}\right)^{k-m}\left(\int\omega_j\right) \\ &= \mathcal{D}_1(f_i)\int\omega_j + \sum_{k\leqslant N} g_k \sum_{0\leqslant m<k}\binom{k}{m}\left(\frac{d}{dx}\right)^m(f_i)\left(\frac{d}{dx}\right)^{k-m-1}(f_j) \\ &= \sum_{k\leqslant N} g_k \sum_{0\leqslant m<k}\binom{k}{m}\left(\frac{d}{dx}\right)^m(f_i)\left(\frac{d}{dx}\right)^{k-m-1}(f_j)\end{aligned}$$

since $\mathcal{D}(f_1) = 0$. By Lemma 4.1, for all $k \leqslant N$, and all $m < k$,

$$\left(\frac{d}{dx}\right)^m(f_i)\left(\frac{d}{dx}\right)^{k-m-1}(f_j) \in H^0(X,\mathcal{O}((2k-4)D_1+(k+1)D_2)),$$

where $D_2 := D_1 + D$. Hence

$$\mathcal{D}\left(\int\omega_i\omega_j\right) \in H^0(X,\mathcal{O}(3(N-1)D_1+(N+1)D+E)). \tag{6}$$

Putting (4), (5) and (6) together, we find

$$\mathcal{D}(G) \in H^0(X,\mathcal{O}(E+(N+3)D+\max\{3(N-1),2N+1\}D_1)). \qquad \square$$

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

4.1 Finding $\mathcal{D}_1$: the general case

By the previous lemma, to get a bound on the number of zeros of G, we need to construct a nice differential operator (with algebraic coefficients we can control) which annihilates all the $f_i := \omega_i/dx$. In general, given m functions $F_1, \ldots, F_m$, it is an elementary exercise to construct a non-trivial differential operator of order at most m which annihilates all the F_i. Hence the non-trivial question is how to find a *nice* differential operator.

First we introduce some notation. Let $F_1, \ldots, F_{2g}$ be elements of a formal power series algebra $\mathbb{Q}_p[\![x]\!]$. Let S be subset of $\mathbb{Z}_{\geqslant 0}$ of size $2g+1$. Write $S = \{n_1, \ldots, n_{2g+1}\}$ with $n_i < n_{i+1}$. Let $A(S, F_1, \ldots, F_{2g})$ denote the $2g \times (2g+1)$ matrix with entries in $\mathbb{Q}_p[\![x]\!]$ whose (i,j)th entry is $(1/n_j!)(d^{n_j}/dx^{n_j})(F_i)$. Let $A^{(j)}(S, F_1, \ldots, F_{2g})$ denote the $2g \times 2g$ matrix obtained by deleting the jth column. Let $\mathcal{D} = \mathcal{D}_{S,F_1,\ldots,F_{2g}} \in \mathbb{Q}_p[\![x]\!][d/dx]$ denote the differential operator

$$\mathcal{D}_{S,F_1,\ldots,F_{2g}} := \sum_{i=1}^{2g+1} (-1)^{i+1} \frac{n_{2g+1}!}{n_i!} \det(A^{(i)}) \frac{d^{n_i}}{dx^{n_i}}.$$

We first note that $\mathcal{D}$ is always a differential operator which annihilates the F_i, and then show that the set S can be chosen so that $\mathcal{D}$ is nice.

Lemma 4.3. *For any choice of S, and all i,*

$$\mathcal{D}(F_i) = 0.$$

Proof. For any power series f,

$$\mathcal{D}_{S,F_1,\ldots,F_{2g}}(f) = n_{2g+1}! \det \begin{pmatrix} \frac{1}{n_1!}\frac{d^{n_1}}{dx^{n_1}}(F_1) & \cdots & \frac{1}{n_{2g+1}!}\frac{d^{n_{2g+1}}}{dx^{n_{2g+1}}}(F_1) \\ \vdots & \ddots & \vdots \\ \frac{1}{n_1!}\frac{d^{n_1}}{dx^{n_1}}(F_{2g}) & \cdots & \frac{1}{n_{2g+1}!}\frac{d^{n_{2g+1}}}{dx^{n_{2g+1}}}(F_{2g}) \\ \frac{1}{n_1!}\frac{d^{n_1}}{dx^{n_1}}(f) & \cdots & \frac{1}{n_{2g+1}!}\frac{d^{n_{2g+1}}}{dx^{n_{2g+1}}}(f) \end{pmatrix}.$$

When $f = F_i$, the matrix does not have full rank. □

We now apply this construction in our case of interest. Let $D, D_0, D_1, \omega_i, f_i$ be as defined earlier in this section.

Lemma 4.4. *There exists an $S \in \mathbb{Z}_{\geqslant 0}^{2g+1}$ with $\max S \leqslant \deg(D) + 2g - 1$ such that $\mathcal{D}_{S,f_0,\ldots,f_{2g-1}}$ is nice.*

Proof. By construction, for any choice of S, the differential operator $\mathcal{D}_{S,f_0,\ldots,f_{2g-1}}$ lies in $\mathbb{Z}_p[\![x]\!][d/dx]$, hence the only non-trivial condition is that the leading coefficient is in $\mathbb{Z}_p^\times$. Note that

$$\frac{1}{n_i!}\frac{d^{n_i}}{dx^{n_i}} f|_{x=0} = C_{n_i}(f),$$

hence requiring that the leading coefficient is in $\mathbb{Z}_p^\times$ is equivalent to requiring that

$$\det(C_i(f_j))_{1 \leqslant i \leqslant 2g, 0 \leqslant j \leqslant 2g-1} \in \mathbb{Z}_p^\times.$$

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

Therefore, by definition, the least N such that there exists a subset S with $\max S \leqslant N+1$ for which $\mathcal{D}_{S,f_0,\dots,f_{2g-1}}$ is nice is exactly the least N such that the f_i remain $\mathbb{F}_p$-linearly independent after reduction mod (p,x^N). Suppose that for all subsets S of $\{0,\dots,N\}$ of size $2g+1$, $\mathcal{D}_{S,f_0,\dots,f_{2g-1}}$ is not nice. Then there is a non-trivial $\mathbb{F}_p$-linear combination of $\operatorname{red}_p \omega_0,\dots,$ $\operatorname{red}_p \omega_{2g-1}$ which has a zero of order N. This gives an element of $H^0(X_{\mathbb{F}_p},\Omega^1(D))$ with a zero of order N, which completes the proof. □

Proof of Theorem 1.1 part (i). To complete the proof of Theorem 1.1, it remains to estimate the degree of the coefficients of a nice $\mathcal{D} := \mathcal{D}_{S,f_0,\dots,f_{2g-1}}$. We follow the construction of basis differentials in [DDLR15, § 4.2]. Let P be a non-Weierstrass point of $X(\mathbb{Q}_p)$ whose mod p reduction is different from b, and let $h \in \mathbb{Q}_p(X)$ be a non-constant function in $H^0(X,\mathcal{O}((g+1)P))$. Let $\omega_0,\dots,\omega_{g-1}$ be a basis of $H^0(X,\Omega^1)$. Define $\omega_{i+g} = h\omega_i$ for $0 \leqslant i \leqslant g-1$. Then $(\omega_i)_{0\leqslant i\leqslant 2g-1}$ gives a basis of $H^1_{\mathrm{dR}}(X)$.

Let $\omega \in H^0(X,\Omega^1)$ be a differential which does not vanish mod p. Let x denote the formal parameter on $]\,z\,[$ obtained by integrating ω. Let $D_1 = (\omega)$. As above, define $f_i = \omega_i/dx \in H^0(X,\mathcal{O}(D_1+(g+1)P))$.

Since $D=(g+1)P$ above, we have an $S=\{n_1,\dots,n_{2g+1}\}$ such that $\mathcal{D}_1 = \mathcal{D}_{S,f_0,\dots,f_{2g-1}}$ is nice and $\max S \leqslant 3g$. Hence the differential operator $\mathcal{D} := \mathcal{D}_1(d/\omega)$ has order at most $3g+1$. To apply Lemma 4.2, it remains to estimate the degrees of the coefficients of $\mathcal{D}_{S,f_0,\dots,f_{2g-1}}$. By Lemma 4.1, we have, for all $k \geqslant 0$,

$$\left(\frac{d^k}{dx^k}\right) f_i \in H^0(X,\mathcal{O}(2kD_1+(g+k+1)P)).$$

The kth coefficient of $\mathcal{D}$ is hence a sum of functions in

$$H^0\Bigg(X,\mathcal{O}\Bigg(\sum_{1\leqslant i\leqslant 2g+1, i\neq k}(2n_iD_1+(g+n_i+1)P)\Bigg)\Bigg).$$

Note that

$$\sum_{i\neq k} n_i \leqslant \sum_{i=g+1}^{3g} i = 4g^2+g.$$

Hence the coefficients of $\mathcal{D}_1$ are in

$$H^0(X,\mathcal{O}((8g^2+2g)D_1+3g(2g+1)P)).$$

Applying Lemma 4.2 with $g \geqslant 2$, $N=3g$, $E=(8g^2+2g)D_1+3g(2g+1)P$, and $D=(g+1)P$, we find that

$$\begin{aligned}\mathcal{D}(G) &\in H^0(X,\mathcal{O}((8g^2+2g)D_1+3g(2g+1)P+3(3g-1)D_1+3(g+1)^2P))\\ &= H^0(X,\mathcal{O}((8g^2+11g-3)D_1+3(3g^2+3g+1)P)).\end{aligned}$$

Hence $\mathcal{D}(G)$ has degree at most

$$(8g^2+11g-3)(2g-2)+3(3g^2+3g+1) = 16g^3+15g^2-19g+9.$$

Applying Proposition 3.2, we deduce that on each residue disk, $X(\mathbb{Q}_p)_\alpha$ has at most

$$\kappa_p(16g^3+15g^2-16g+10)$$

points. □

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

5. Differential operators for rational points: hyperelliptic case

5.1 The hyperelliptic case: non-Weierstrass disks

In this subsection we prove the second part of Theorem 1.1. Let X be a hyperelliptic curve of genus g with good reduction at $p \neq 2g+1$ and Mordell–Weil rank g. The assumptions on p imply that X has a smooth model over $\mathbb{Z}_p$ of the form

$$y^2 = f(x) = x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_0.$$

Let W denote the subscheme of Weierstrass points.

As mentioned below Proposition 3.2, our strategy for applying Proposition 3.2 is slightly different from the previous section, in that we choose one set of basis differentials and one differential operator $\mathcal{D}$ for the whole of $X - W$. This means we get a bound of the form

$$\#(X(\mathbb{Q}_p)_\alpha \cap](X-W)_{\mathbb{F}_p}[) < \kappa_p(\deg(\mathcal{D}(G)) + N\#(X-W)_{\mathbb{F}_p}),$$

and similarly for the Weierstrass disks.

Let ω_i be the differential $x^i dx/y$. We take as a basis of $H^1_{\mathrm{dR}}(X)$ a subset of the $\mathbb{Q}$-span of the differentials $\omega_i := x^i dx/y$, $0 \leqslant i \leqslant 2g$. Hence, changing notation somewhat, we may write G in the form

$$G(z) = \sum_{0 \leqslant i,j \leqslant 2g} a_{ij} \int_b^z \omega_i\omega_j + \sum_{0 \leqslant i \leqslant 2g} a_i \int_b^z \omega_i + h(z).$$

Let $\infty := \infty^+ + \infty^-$ denote the degree 2 divisor of the two points ∞^+, ∞^- above infinity. Since all the ω_i are in $H^0(X, \Omega^1((g+1)\infty))$, h lies in $H^0(X, \mathcal{O}(2(g+1)\infty))$.

First let $\mathcal{D}_0$ be the differential operator d/ω_0. Then define $G_1 := \mathcal{D}_0 G$. Hence

$$G_1 = \sum a_{ij}x^i \int \omega_j + \sum a_i x^i + h_1,$$

where $h_1 := y(d/dx)h$. Define $\mathcal{D}_1 = (d/dx)^{2g+1}$ and $\mathcal{D} = \mathcal{D}_1\mathcal{D}_0$.

Lemma 5.1. *Let W denote the degree $2g+2$ divisor of Weierstrass points. Then the power series $\mathcal{D}(G)$ lies in $H^0(X, \mathcal{O}((g+1)\infty + (4g+1)W))$.*

Proof. We have $\mathcal{D}(\int \omega_i) = 0$ for all i, so it will be enough to prove this for h and for $\int \omega_i\omega_j$. Note that we have $\mathrm{div}(dx) = W - 2\infty$, $\mathrm{div}(y) = W - (g+1)\infty$, and so $\mathrm{div}(\omega_0) = (g-1)\infty$. For h, we use Lemma 4.1 to deduce

$$\mathcal{D}_0(h) \in H^0(X, \mathcal{O}((3g+2)\infty)).$$

Since dx has divisor $W - 2\infty$, if $F \in H^0(X, \mathcal{O}(n\infty + mW))$, a direct computation gives

$$\frac{dF}{dx} \in \begin{cases} H^0(X, \mathcal{O}((n-1)\infty + (m+2)W)), & m > 0, \\ H^0(X, \mathcal{O}((n-1)\infty + W)), & m = 0. \end{cases}$$

Hence $\mathcal{D}(h) \in H^0(X, \mathcal{O}((g+1)\infty + (4g+1)W))$.

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

For $\int \omega_i\omega_j$, we have

$$\begin{aligned}\mathcal{D}\left(\int \omega_i\omega_j\right) &= \mathcal{D}_1\left(x^i \int \omega_j\right)\\ &= \sum_{k=0}^{i} \binom{2g+1}{k} \frac{i!}{(i-k)!} x^{i-k} \left(\frac{d}{dx}\right)^{2g-k+1} \int (\omega_j)\\ &= \sum_{k=0}^{i} \binom{2g+1}{k} \frac{i!}{(i-k)!} x^{i-k} \left(\frac{d}{dx}\right)^{2g-k} \left(\frac{x^j}{y}\right). \end{aligned} \tag{7}$$

Now we have

$$\frac{x^j}{y} \in H^0(X, \mathcal{O}((j-g-1)\infty + W)),$$

so

$$\left(\frac{d}{dx}\right)^{(2g-k)} \left(\frac{x^j}{y}\right) \in H^0(X, \mathcal{O}((j-3g+k-1)\infty + (4g-2k+1)W)),$$

which gives that

$$x^{i-k}\left(\frac{d}{dx}\right)^{(2g-k)} \left(\frac{x^j}{y}\right) \in H^0(X, \mathcal{O}((i+j-1-3g)\infty + (4g-2k+1)W)),$$

and thus each summand of (7) is an element of $H^0(X, \mathcal{O}((g-1)\infty + (4g+1)W))$. □

Since the degree of $(g+1)\infty + (4g+1)W$ is $2g+2+(4g+1)(2g+2) = 8g^2+12g+4$, applying Proposition 3.2, and summing over all non-Weierstrass residue disks, we find that the number of points of $X(\mathbb{Q}_p)_\alpha$ which reduce to non-Weierstrass points away from infinity is at most

$$\kappa_p((8g^2+12g+4) + (2g+2)\#(X - W - \infty)(\mathbb{F}_p)).$$

For the two points at infinity, we may apply the same analysis with the equation at infinity

$$y^2 = a_0x^{2g+2} + a_1x^{2g+1} + \cdots + 1.$$

We deduce that the number of points of $X(\mathbb{Q}_p)_\alpha$ which reduce to non-Weierstrass points is at most

$$\kappa_p((16g^2+24g+8) + (2g+2)\#(X - W)(\mathbb{F}_p)).$$

5.2 The hyperelliptic case: Weierstrass points

The computation at Weierstrass disks is carried out in a manner similar to the method developed in § 4. The essential difference is that, instead of trying to find a new nice differential operator $\mathcal{D}_1$ annihilating the $2g$ functions $\{f_0, \ldots, f_{2g-1}\}$ for each residue disk $]\,b\,[$, we find a differential operator $\mathcal{D}_1$ which annihilates the $2g+1$ functions ω_i/ω_0 $(0 \leqslant i \leqslant 2g)$ at all Weierstrass disks. The price paid for this is that the degree is slightly larger. Let $B \in M_{2g+1}(\mathbb{Q}_p(X))$ denote the matrix

$$B = \left(\frac{1}{(2i)!}\left(\frac{d}{\omega_0}\right)^{2i} x^j\right)_{0\leqslant i,j\leqslant 2g}.$$

Lemma 5.2. *For all Weierstrass points $z = (\alpha, 0) \in X(\mathbb{F}_p)$, $\det(B) \in \mathcal{O}^\times_{\mathcal{X},z}$.*

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

Proof. Clearly $\det(B)$ is defined at z, so it is sufficient to prove it is non-zero at z. First note that, since $x-\alpha$ has a zero of order 2 at z, a linear combination of $1, x, \ldots, x^{2g}$ can have a zero of order at most $4g$. Hence the $(2g+1)\times(4g+1)$ matrix $((d^i/\omega_0^i)x^j|_z)_{0\leqslant i\leqslant 4g, 0\leqslant j\leqslant 2g}$ has rank at least $2g+1$. On the other hand, for all odd j, $(d^j/\omega_0^j)x^i$ is an odd function with respect to the hyperelliptic involution, and hence vanishes at z. Hence $B|_z$ is invertible in $M_{2g+1}(\mathbb{F}_p)$. □

Proof of Theorem 1.1 part (ii). We deduce that we can apply the construction of § 4.1 with A taken to be the $(2g+1)\times(2g+2)$ matrix

$$\left(\left(\frac{d}{\omega_0}\right)^i x^j\right)_{0\leqslant j\leqslant 2g, i=0,2,4,\ldots,4g,4g+1}.$$

The function $(d/\omega_0)^i x^j$ lies in $H^0(X, \mathcal{O}((gi+j)\infty))$, hence the differential operator

$$\mathcal{D}_1 = \mathcal{D}_{S,\omega_0/\omega_0,\omega_1/\omega_0,\ldots,\omega_{2g}/\omega_0}$$

has coefficients in

$$H^0\left(X, \mathcal{O}\left(\left(g\sum_{i=1}^{2g} 2i\right) + g(4g+1) + \sum_{j=0}^{2g} j\right)\right) = H^0(X, \mathcal{O}((4g^3+8g^2+2g)\infty)).$$

Define $\mathcal{D} := \mathcal{D}_1\mathcal{D}_0$, where $\mathcal{D}_0 := (d/\omega_0)$. Applying Lemma 4.2 with $E = (4g^3+8g^2+2g)\infty$, $N = 4g+1$, $D_1 = (g-1)\infty$, $D = (g+1)\infty$, we deduce

$$\mathcal{D}(G) \in H^0(X, \mathcal{O}((4g^3+24g^2-2g+4)\infty)).$$

The number of points of $X(\mathbb{Q}_p)_\alpha$ on all Weierstrass disks is hence, by Proposition 3.2, at most

$$\kappa_p((4g+2)\#W(\mathbb{F}_p) + 2(4g^3+24g^2-2g+4)).$$

Combining with the bounds from the non-Weierstrass residue disks in the previous subsection, we find that

$$\#X(\mathbb{Q}_p)_\alpha \leqslant \kappa_p((2g+2)\#X(\mathbb{F}_p) + 2g\#W(\mathbb{F}_p) + 8g^3 + 64g^2 + 20g + 16). \quad □$$

6. Integral points for hyperelliptic curves

The proof of the $g>1$ case of Theorem 1.3 follows a similar strategy to the previous section. Let X be a hyperelliptic curve of genus $g>1$ with equation

$$y^2 = f(x) = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_0$$

and suppose the rank of the Jacobian of X is equal to g. Then the set $X(\mathbb{Z}_p)_2$ is partitioned into a disjoint union of sets $X(\mathbb{Z}_p)_\alpha$. Each set $X(\mathbb{Z}_p)_\alpha$ is contained in the set of zeros of a Coleman function of the form

$$G(z) = \sum_{0\leqslant i,j<2g} a_{ij}\int_b^z \omega_i\omega_j + \sum_{0\leqslant i<2g} a_i \int_b^z \omega_i + h(z),$$

where $h \in H^0(X, \mathcal{O}(4g\infty))$, with ∞ now denoting the divisor of degree 1 consisting of the unique point at infinity. Let W denote the degree $2g+1$ divisor of Weierstrass points away from infinity and define $\mathcal{D}_0 := d/\omega_0$. For non-Weierstrass points, we take the differential operator to be

$$\mathcal{D} = \left(\frac{d}{dx}\right)^{2g} \mathcal{D}_0.$$

Since ω_0 has a zero of order $(2g-2)$ at ∞, we have

$$\frac{dh}{\omega_0} \in H^0(X, \mathcal{O}((6g-1)\infty)).$$

Similar to the case of an even degree model, since dx has divisor $W - 3\infty$, if F is in $H^0(X, \mathcal{O}(nW + m\infty))$ then

$$\frac{dF}{dx} \in \begin{cases} H^0(X, \mathcal{O}((n+2)W + (m-2)\infty)), & n > 0, \\ H^0(X, \mathcal{O}(W + (m-2)\infty)), & n = 0. \end{cases}$$

Hence $\mathcal{D}(h)$ is in $H^0(X, \mathcal{O}((2g-1)\infty + (4g-1)W))$.

For the remaining term, note that

$$\left(\frac{d}{dx}\right)^k \left(\frac{x^j}{y}\right) \in H^0(X, \mathcal{O}((2k+1)W + (2j-2k-2g-1)\infty)). \tag{8}$$

Since

$$\begin{aligned} \mathcal{D}\left(\int \omega_i \omega_j\right) &= \left(\frac{d}{dx}\right)^{2g} \left(x^i \int \omega_j\right) \\ &= \sum_{0 \leqslant k < 2g} \binom{2g}{k} \frac{i!}{(i-k)!} x^{i-k} \left(\frac{d}{dx}\right)^{2g-k-1} \left(\frac{x^j}{y}\right), \end{aligned}$$

equation (8) implies

$$x^{i-k} \left(\frac{d}{dx}\right)^{2g-k-1} \left(\frac{x^j}{y}\right) \in H^0(X, \mathcal{O}((4g-2k-1)W + (2j+2i-6g+1)\infty)).$$

Hence $\mathcal{D}(\int \omega_i \omega_j)$ lies in $H^0(X, \mathcal{O}((4g-1)W + (2g-3)\infty))$. Arguing as in § 5.1, we deduce that the number of integral points of X which reduce to non-Weierstrass points mod p is bounded by

$$\kappa_p \left(\prod_{v \in T_0} m_v\right) (8g^2 + 4g - 4 + (2g+1)\#(Y - W)(\mathbb{F}_p)).$$

6.1 Differential operators at Weierstrass points

Let $B \in M_{2g}(\mathbb{Q}_p(X))$ be the matrix

$$\left(\frac{1}{(2i)!} \left(\frac{d}{\omega_0}\right)^{2i} x^j\right)_{0 \leqslant i,j < 2g}.$$

As in § 5.2, we may show $\det(B)$ is a unit at all points in W, and hence construct a differential operator $\mathcal{D}_1$ from the matrix

$$A = \left(\frac{1}{i!} \left(\frac{d}{\omega_0}\right)^{i} x^j\right)_{0 \leqslant j < 2g, i = 0, 2, \ldots, 4g-2, 4g-1}.$$

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

Since ω_0 has a zero of order $(2g-2)$ at ∞, we find that

$$\left(\frac{d}{\omega_0}\right)^i x^j \in H^0(X, \mathcal{O}((i(2g-1)+2j)\infty)).$$

We deduce that the coefficients of $\mathcal{D}_1$ lie in $H^0(X, \mathcal{O}(8g^3+4g^2-6g+1)\infty)$. Define $\mathcal{D} := \mathcal{D}_1\mathcal{D}_0$, where $\mathcal{D}_0 := (d/\omega_0)$. Applying Lemma 4.2 with $E = (8g^3+4g^2-6g+1)\infty$, $D_1 = 2(g-1)\infty$, $D = 2g\infty$ and $N = 4g-1$, we deduce that $\mathcal{D}(G)$ lies in $H^0(X, \mathcal{O}((8g^3+36g^2-38g+13)\infty))$, hence by Proposition 3.2, we find that the number of integral points reducing to Weierstrass points is bounded by

$$\left(\prod_v m_v\right)\kappa_p(8g^3+36g^2-38g+13+4g\#W(\mathbb{F}_p)).$$

We deduce a bound for the total number of integral points of

$$\kappa_p\left(\prod_{v\in T_0} m_v\right)(8g^3+44g^2-34g+9+(2g+1)\#Y(\mathbb{F}_p)+(2g-1)\#W(\mathbb{F}_p)).$$

Acknowledgements

We thank the anonymous referee for pointing out how to improve the bound in Corollary 1.2, and several other corrections, and thank Kevin Buzzard, Minhyong Kim and Jan Vonk for helpful suggestions.

References

BBM16 J. S. Balakrishnan, A. Besser and J. S. Müller, *Quadratic Chabauty: p-adic height pairings and integral points on hyperelliptic curves*, J. Reine Angew. Math. **720** (2016), 51–79.

BD17 J. S. Balakrishnan and N. Dogra, *Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties*, Preprint (2017), arXiv:arXiv:1705.00401.

BK90 S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, in *The Grothendieck Festschrift, Vol. I* (Birkhäuser, Boston, 1990).

Cha41 C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.

CK10 J. Coates and M. Kim, *Selmer varieties for curves with CM Jacobians*, Kyoto J. Math. **50** (2010), 827–852.

Col85 R. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), 765–770.

Del89 P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, in *Galois groups over* $\mathbb{Q}$, Mathematical Sciences Research Institute Publications, vol. 16, eds Y. Ihara, K. Ribet and J.-P. Serre (Springer, New York, 1989).

DDLR15 H. Darmon, M. Daub, S. Lichtenstein and V. Rotger, *Algorithms for Chow–Heegner points via iterated integrals*, Math. Comput. **84** (2015), 2505–2547.

EH17 J. S. Ellenberg and D. R. Hast, *Rational points on solvable curves over* $\mathbb{Q}$ *via non-abelian Chabauty*, Preprint, 2017, arXiv:1706.00525.

KRZ16 E. Katz, J. Rabinoff and D. Zureick-Brown, *Uniform bounds for the number of rational points on curves of small Mordell–Weil rank*, Duke. Math. J. **165** (2016), 3189–3240.

Kim05 M. Kim, *The motivic fundamental group of* $\mathbb{P}^1 - \{0,1,\infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), 629–656.

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press

Kim09 M. Kim, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), 89–133.

Kim10 M. Kim, *Massey products for elliptic curves of rank 1*, J. Amer. Math. Soc. **23** (2010), 725–747.

KT08 M. Kim and A. Tamagawa, *The l-component of the unipotent Albanese map*, Math. Ann. **340** (2008), 223–235.

Kob84 N. Koblitz, *p-adic Numbers, p-adic analysis and zeta-functions*, Graduate Texts in Mathematics, vol. 58 (Springer, New York, 1984).

Oda95 T. Oda, *A note on the ramification of the Galois representation on the fundamental group of an algebraic curve, II*, J. Number Theory **53** (1995), 342–355.

Ser97 J.-P. Serre, *Galois cohomology* (Springer, Berlin, 1997).

Sto19 M. Stoll, *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell–Weil rank*, J. Eur. Math. Soc. (JEMS) **21** (2019), 923–956.

Jennifer S. Balakrishnan jbala@bu.edu
Department of Mathematics and Statistics, Boston University,
111 Cummington Mall, Boston, MA 02215, USA

Netan Dogra dogra@maths.ox.ac.uk
Mathematical Institute, University of Oxford,
Radcliffe Observatory Quarter, Woodstock Road,
Oxford OX2 6GG, UK

https://doi.org/10.1112/S0010437X19007243 Published online by Cambridge University Press