Algebra & Number Theory

Volume 3

2009

No. 2

Chabauty for symmetric powers of curves

Samir Siksek

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 3:2(2009)

Chabauty for symmetric powers of curves

Samir Siksek

Let C be a smooth projective absolutely irreducible curve of genus $g \geq 2$ over a number field K, and denote its Jacobian by J. Let $d \geq 1$ be an integer and denote the d-th symmetric power of C by $C^{(d)}$. In this paper we adapt the classic Chabauty–Coleman method to study the K-rational points of $C^{(d)}$. Suppose that $J(K)$ has Mordell–Weil rank at most $g - d$. We give an explicit and practical criterion for showing that a given subset $\mathcal{L} \subseteq C^{(d)}(K)$ is in fact equal to $C^{(d)}(K)$.

1. Introduction

Let C be a smooth projective absolutely irreducible curve of genus $g \geq 2$ defined over a number field K, and write J for the Jacobian of C. Suppose that the rank of the Mordell–Weil group $J(K)$ is at most $g-1$. In a pioneering paper, Chabauty [1941] proved the finiteness of the set of K-rational points on C. This has since been superseded by Faltings's proof [1983] of the Mordell conjecture, which gives the finiteness of $C(K)$ without any assumption on the rank of $J(K)$. Chabauty's approach, where applicable, does however have two considerable advantages:

The first is that Chabauty can be refined to give explicit bounds for the cardinality of $C(K)$, as shown by Coleman [1985a]. Coleman's bounds are realistic, and occasionally even sharp; see for example [Grant 1994; Flynn 1995]. Coleman's approach has been adapted to give bounds (assuming some reasonable conditions) for the number of solutions of Thue equations [Lorenzini and Tucker 2002], the number of rational points on Fermat's curves [McCallum 1992; 1994], the number of points on curves of the form $y^2 = x^5 + A$ [Stoll 2006b], and the number of rational points on twists of a given curve [Stoll 2006a].

The second is that the Chabauty–Coleman strategy can often be adapted to compute $C(K)$, as in [Bruin 2002; 2003, Flynn 1997; Flynn and Wetherell 1999; 2001; McCallum and Poonen 2006; Wetherell 1997].

MSC2000: primary 11G30; secondary 11G35, 14K20, 14C20.

Keywords: Chabauty, Coleman, curves, Jacobians, symmetric powers, divisors, differentials, abelian integrals.

The author is supported by an UK EPSRC grant and by a Marie Curie International Reintegration Grant.

One can ask if it is sensible to apply Chabauty to varieties X/K of dimension at least 2, where the Albanese variety $\mathrm{Alb}(X)$ plays the role of the Jacobian. Of course, even when a K-rational degree 1 zero-cycle on X exists, the associated Albanese map $\jmath : X \to \mathrm{Alb}(X)$ is often not injective. Indeed $\mathrm{Alb}(X)$ can have smaller dimension than X. However, if $\jmath$ is injective, or even if $\jmath(X)$ is merely birational to X, there is a hope that Chabauty might enable us to determine the rational points on X. Alas, for a general variety X there are as of yet no algorithms for studying the arithmetic of $\mathrm{Alb}(X)$. A sensible starting point for the investigation of Chabauty in higher dimension is the symmetric powers of curves. Here the Albanese variety is also the Jacobian of the curve.

Suppose d is a positive integer, and denote the d-th symmetric power of C by $C^{(d)}$. The elements of $C^{(d)}(K)$ correspond to effective K-rational divisors on C of degree d. Suppose $C^{(d)}(K)$ is nonempty, and let $\jmath : C^{(d)} \to J$ be the Abel–Jacobi map corresponding to some fixed element of $C^{(d)}(K)$. We shall write γ for the gonality of C; this is defined to be the least possible degree of any nonconstant morphism $C \to \mathbb{P}^1$. If $d < \gamma$, then $C^{(d)}$ is isomorphic to its image in J (denoted by $W^{(d)}$), and if $d \le g$, then $C^{(d)}$ is birational to $W^{(d)}$. Another theorem of Faltings [1991; 1994] states that any proper subvariety of an abelian variety has finitely many K-rational points provided this subvariety does not contain a translate of any nontrivial proper abelian subvariety of J. If $d < \gamma$ and $W^{(d)}$ does not contain the translate of any proper abelian subvariety — this would be the case if J is simple — then it follows from Faltings's theorem that $C^{(d)}(K)$ is finite. This idea is used by Klassen [1993], by Debarre and Klassen [1994], and by Harris and Silverman [1991] to give sufficient conditions for $C^{(d)}(K)$ to be finite in many cases. For example, Harris and Silverman show that if C is neither hyperelliptic nor bielliptic, then the set $C^{(2)}(K)$ is finite. This result fails if C is hyperelliptic or bielliptic.

We are naturally led to the question, if $C^{(d)}(K)$ is finite, can we adapt Chabauty–Coleman to compute it? Klassen makes a first attempt at this question in his PhD thesis [1993]. His main result on Chabauty–Coleman can be summarized as follows. Let $K = \mathbb{Q}$ and $1 < d < \gamma$. Suppose that the rank of $J(\mathbb{Q})$ is at most $g - d$. Let p be an odd prime of good reduction, and let $\mathrm{red} : C^{(d)}(\mathbb{Q}) \to \tilde{C}^{(d)}(\mathbb{F}_p)$ denote the reduction map. Klassen shows the existence of a canonical divisor M on $C^{(d)}$ such that $C^{(d)}(\mathbb{Q}) \setminus \mathrm{red}^{-1}(M(\mathbb{F}_p))$ is finite. In essence he shows that any fibre of the reduction map contains at most one element of $C^{(d)}(\mathbb{Q}) \setminus \mathrm{red}^{-1}(M(\mathbb{F}_p))$.

Our broad objective here is to refine the method of Chabauty–Coleman so that we can compute $C^{(d)}(K)$ in many cases. Our achievements can be summarized as follows:

(I) Let υ be a nonarchimedean prime of the number field K. Inspired by the aforementioned work of Klassen, we give an explicit criterion for an element of $C^{(d)}(K)$ to be the unique K-rational element in its residue class, for a given prime υ (the residue classes are defined to be the fibres of the reduction map $C^{(d)}(K_\upsilon) \to C^{(d)}(k_\upsilon)$). Here, unlike Klassen, we do not assume that $d < \gamma$. Just as in classical Chabauty, we need an assumption on the rank of the Mordell–Weil group: Our criterion requires that rank $J(K) \le g - d$.

(II) We often expect, by applying the criterion of (I), to show that the fibres containing a K-rational element do not contain any other. This criterion however does not tell us anything about fibres that do not seem to contain K-rational elements. Thus, if the reduction map $C^{(d)}(K) \to C^{(d)}(k_\upsilon)$ happens to be surjective, then it might be possible to use (I) to show that the known elements of $C^{(d)}(K)$ are the only ones. But experience suggests that the reduction map is rarely surjective for $d > 1$. To prove that the known elements of $C^{(d)}(K)$ are all its elements, we combine information given by our criterion using several well-chosen primes $\upsilon_1, \dots, \upsilon_t$.

(III) Suppose $\varrho : C \to C'$ is a degree-d morphism defined over K. Then $\varrho^* C'(K)$ is a subset of $C^{(d)}(K)$. If C' has genus 0 or 1, then $C'(K)$ can be infinite, and in this case $\varrho^* C'(K)$ is an infinite subset of $C^{(d)}(K)$, and undoubtedly, the strategy of (I) and (II) fails. In this case we explain how the strategy of (I) and (II) can be suitably modified to compute $C^{(d)}(K) \setminus \varrho^* C'(K)$. Again we need a condition on the ranks of the Mordell–Weil groups; in the obvious notation, we require that rank $J_C(K) -$ rank $J_{C'}(K) \le g_C - g_{C'} - d + 1$.

Although we do not give theoretical bounds for $C^{(d)}(K)$ in the way that Coleman [1985a] does for $C(K)$, we believe that our simplified explicit approach in (I) is a useful first step in this direction.

In the spirit of modern computations on curves of higher genus, we will not require explicit equations for $C^{(d)}$, but rather represent K-rational points on $C^{(d)}$ as effective K-rational divisors of degree d. We suppose we have been supplied with a basis $D_1, \dots, D_r$ for a subgroup of $J(K)$ of full rank and hence finite index — the elements of this basis are represented as degree 0 divisors on C (modulo linear equivalence). Obtaining a basis for a subgroup of full rank is often the happy outcome of a successful descent calculation; see for example [Cassels and Flynn 1996; Flynn 1994; Poonen and Schaefer 1997; Schaefer 1995; Schaefer and Wetherell 2005; Stoll 1998; 2001; 2002]. Obtaining a basis for the full Mordell–Weil group is often time consuming for curves of genus 2 and simply not feasible in the present state of knowledge for curves of higher genus.

We illustrate our method by computing $C^{(2)}(\mathbb{Q})$ for two curves C of genus 3. The first is a hyperelliptic curve, and the second a nonhyperelliptic plane quartic curve. It is noteworthy that in both examples $C^{(2)}$ is a surface of general type, being birational to a Θ-divisor on the Jacobian. Much less is known about the arithmetic of surfaces of general type than that of other surfaces.

Examples of papers that study rational points on symmetric powers of modular curves are [Kamienny 1986a; 1986b; 1992; Merel 1996; Parent 2000; 2003]; some that study rational points on symmetric powers of Fermat curves are [Debarre and Klassen 1994; Gross and Rohrlich 1978; Klassen and Tzermias 1997; Tzermias 1998, 2003; 2004; 2005]. It is our hope that the techniques explained in this paper will lead to useful progress in these directions.

2. Preliminaries

In this section we summarize various results on p-adic integration. The definitions and proofs can be found in [Coleman 1985b; Colmez 1998]. For an introduction to the ideas involved in Chabauty's method we warmly the recommend Wetherell's thesis [1997] and the survey paper of McCallum and Poonen [2006], as well as Coleman's paper [1985a].

Integration. Let p be a rational prime and K_υ be a finite extension of $\mathbb{Q}_p$. Let $\mathbb{O}_\upsilon$ be the ring of integers in K_υ, and let $\mathbb{C}_\upsilon$ be the completion of its algebraic closure. Let $\mathcal{W}$ be a smooth, proper connected scheme of finite type over $\mathbb{O}_\upsilon$, and write W for the generic fibre. Coleman [1985b, Section II] describes how to integrate "differentials of the second kind" on W. We shall however only be concerned with global 1-forms (that is, differentials of the first kind) and so shall restrict our attention to these. Among the properties of integration [loc. cit.] we shall need are

$$\begin{aligned} \int_P^Q \omega &= -\int_Q^P \omega, & \int_Q^P \omega + \int_P^R \omega &= \int_Q^R \omega, \\ \int_Q^P \alpha\omega &= \alpha \int_Q^P \omega, & \int_Q^P \omega + \int_Q^P \omega' &= \int_Q^P \omega+\omega' \end{aligned} \tag{1}$$

for P, Q, $R \in W(\mathbb{C}_\upsilon)$, global 1-forms ω, ω' on $W \times \mathbb{C}_\upsilon$, and $\alpha \in \mathbb{C}_\upsilon$. We shall also need the "change of variables formula" [Coleman 1985b, Theorem 2.7]: If $\mathcal{W}_1$ and $\mathcal{W}_2$ are smooth, proper connected schemes of finite type over $\mathbb{O}_\upsilon$ and $\varrho : W_1 \to W_2$ is a morphism of their generic fibres, then

$$\int_Q^P \varrho^*\omega = \int_{\varrho(Q)}^{\varrho(P)} \omega \tag{2}$$

for all global 1-forms ω on $W_2 \times \mathbb{C}_\upsilon$ and P, $Q \in W_1(\mathbb{C}_\upsilon)$.

Now let A be an abelian variety of dimension g over K_υ, and write Ω_A for the K_υ-space of global 1-forms on A. Consider the pairing

$$\Omega_A \times A(K_\upsilon) \to K_\upsilon, \quad (\omega, P) \mapsto \int_0^P \omega. \tag{3}$$

This pairing is bilinear. It is K_v-linear on the left by the bottom two equalities in (1). That it is also $\mathbb{Z}$-linear on the right is a straightforward consequence of the change of variables formula (2); see [Coleman 1985b, Theorem 2.8]. The kernel on the left is 0 and on the right is the torsion subgroup of $A(K_v)$; see [Bourbaki 1989, III.7.6].

Notation. Henceforth we shall be concerned with curves over number fields and their Jacobians. Once and for all, we fix

K	a number field,
C	a smooth projective absolutely irreducible curve defined over K, of genus ≥ 2,
$C^{(d)}$	the d-th symmetric power of C,
J	the Jacobian of C,
v	a nonarchimedean prime of K, of good reduction for C,
K_v	the completion of K at v,
k_v	the residue field of K at v,
$\mathcal{O}_v$	the ring of integers in K_v,
$\mathscr{C}$	a minimal regular proper model for C over $\mathcal{O}_v$,
$\tilde{C}$	the special fibre of $\mathscr{C}$ at v,
Ω_{C/K_v}	the K_v-vector space of global 1-forms on C.

Global 1-forms on curves and Jacobians. For any field extension M/K (not necessarily finite), we shall write $\Omega_{C/M}$ and $\Omega_{J/M}$ for the M-vector spaces of global 1-forms on C/M and J/M, respectively. Corresponding to any $P_0 \in C(\overline{K})$ is the Abel–Jacobi map

$$\jmath : C \hookrightarrow J, \quad P \mapsto [P - P_0].$$

It is well known that the pull-back $\jmath^* : \Omega_{J/\overline{K}} \to \Omega_{C/\overline{K}}$ is an isomorphism; see [Milne 1986, Proposition 2.2]. Moreover any two Abel–Jacobi maps differ by a translation on J. Since 1-forms on J are translation invariant, the map $\jmath^*$ is independent of the choice of P_0; see [Wetherell 1997, Section 1.4]. It is clear that $\jmath^*$ is defined over K if there is some K-rational point P_0 on C. We however do not want to assume the existence of a K-rational point on C. Instead we shall make use of the following (well-known) result, for which we cannot find a reference.

Proposition 2.1. *With notation as above, the pull-back $\jmath^*$ induces an isomorphism $\Omega_{J/K} \to \Omega_{C/K}$.*

Proof. By smoothness there is a rational point on C defined over some finite Galois extension M/K. This induces an isomorphism $\jmath^* : \Omega_{J/M} \to \Omega_{C/M}$. However, by independence of the choice of M-rational point, the isomorphism $\jmath^*$ is equivariant under the action of $\mathrm{Gal}(M/K)$, and hence descends to an isomorphism over the ground field K. $\square$

Integration on curves and Jacobians. Suppose υ is a nonarchimedean place for K of good reduction for C. Let $\jmath$ be the Abel–Jacobi corresponding to any $P_0 \in C(\overline{K})$. Proposition 2.1 asserts that the pull-back induces an isomorphism $\jmath^* : \Omega_{J/K} \to \Omega_{C/K}$ of global 1-forms defined over K (and independent of P_0). This extends to an isomorphism $\Omega_{J/K_\upsilon} \to \Omega_{C/K_\upsilon}$, which we also denote by $\jmath^*$. For any global 1-form $\omega \in \Omega_{J/K_\upsilon}$ and any two points $P, Q \in C(\mathbb{C}_\upsilon)$, we have

$$\int_Q^P \jmath^*\omega = \int_{\jmath Q}^{\jmath P} \omega = \int_0^{[P-Q]} \omega,$$

using the integration properties (1). We shall henceforth use $\jmath^*$ to identify Ω_{C/K_υ} with Ω_{J/K_υ}. With this identification, the pairing (3) with $J = A$ gives the bilinear pairing

$$\Omega_{C/K_\upsilon} \times J(K_\upsilon) \to K_\upsilon, \quad \left(\omega, \left[\sum P_i - \sum Q_i\right]\right) \longmapsto \sum \int_{Q_i}^{P_i} \omega, \tag{4}$$

whose kernel on the right is 0 and on the left is the torsion subgroup of $J(K_\upsilon)$. We ease notation a little by defining, for divisor class $D = \sum P_i - Q_i$ of degree 0, the integral

$$\int_D \omega = \sum \int_{Q_i}^{P_i} \omega.$$

Note that this integral depends on the equivalence class of D and not on the decomposition as $D = \sum P_i - Q_i$. We shall need the following functorial property of integration of curves, for which we are unable to find a reference:

Lemma 2.2. *Suppose $\varrho : C \to C'$ is a nonconstant morphism of curves defined over K, and let υ be a nonarchimedean place of good reduction for both curves. Denote by* Tr *the corresponding trace map $\Omega_{C/K_\upsilon} \to \Omega_{C'/K_\upsilon}$ on global* 1*-forms. If D is a degree* 0 *divisor on C' and $\omega \in \Omega_{C/K_\upsilon}$ then*

$$\int_{\varrho^* D} \omega = \int_D \mathrm{Tr}\,\omega.$$

Proof. First we assume that C/C' is geometrically Galois. Replacing K_υ by a finite extension if necessary, we can assume that $K_\upsilon(C)/K_\upsilon(C')$ is in fact Galois and contains the fields of definition of the points in $\varrho^* D$. Suppose that ϱ has degree d. Then the Galois group of C/C' is some set of automorphisms $\{\sigma_1, \ldots, \sigma_d\}$ where $\sigma_i : C \to C$ is defined over K_υ and commutes with ϱ. The virtue of assuming that C/C' is Galois is that the trace has a very simple formula in terms of the Galois group: $\varrho^* \,\mathrm{Tr}\,\omega = \sum \sigma_i^* \omega$.

Now fix a degree 0 divisor D_0 on C such that $\varrho D_0 = D$. Then $\varrho^* D = \sum \sigma_i D_0$, and

$$\int_{\varrho^* D} \omega = \sum_{i=1}^{d} \int_{\sigma_i D_0} \omega = \sum_{i=1}^{d} \int_{D_0} \sigma_i^* \omega = \int_{D_0} \varrho^* \operatorname{Tr} \omega = \int_D \operatorname{Tr} \omega.$$

where the second and fourth equalities use the change of variables formula (2). This proves the lemma in the geometrically Galois case. For the general case, we will need to work with the (geometric) Galois closure C''/C of C'/C. This is necessarily defined over some finite extension of K_υ, so we again replace K_υ by this finite extension. Consider now the following commutative diagram of curves.

$$\begin{tikzcd} C'' \arrow[r, "\epsilon"] \arrow[dr, "\delta"'] & C \arrow[d, "\varrho"] \\ & C' \end{tikzcd}$$

Both ϵ and δ are geometrically Galois and we may apply the lemma to them. Let D be a degree 0 divisor on C' and ω a global 1-form on C. Applying the lemma to δ, we see

$$\int_{\delta^* D} \epsilon^* \omega = \int_D \operatorname{Tr}_{C''/C'}(\epsilon^* \omega) = \deg(\epsilon) \int_D \operatorname{Tr}_{C/C'} \omega.$$

Likewise, applying the lemma to ϵ, we get

$$\int_{\delta^* D} \epsilon^* \omega = \int_{\epsilon^* \varrho^* D} \epsilon^* \omega = \int_{\varrho^* D} \operatorname{Tr}_{C''/C}(\epsilon^* \omega) = \deg(\epsilon) \int_{\varrho^* D} \omega.$$

Comparing the results of the last two calculations yields the desired conclusion. □

Uniformizers. The usual Chabauty approach when studying rational points in a residue class is to work with a local coordinate (defined shortly) and create power series equations in terms of the local coordinate whose solutions, roughly speaking, contain the rational points. In our situation we find it more convenient to shift the local coordinate so that it becomes a uniformizer at a rational point in the residue class. Fix a nonarchimedean prime υ of good reduction for C, and a minimal regular proper model $\mathscr{C}$ for C over υ. Let $Q \in C(K)$ and let $\tilde{Q}$ be its reduction on the special fibre $\tilde{C}$. Choose a rational function $s_Q \in K(C)$ so that its extension to a rational function on $\mathscr{C}$ is a generator of the maximal ideal in $\mathbb{O}_{\mathscr{C},\tilde{Q}}$; the function s_Q is called in [Lorenzini and Tucker 2002, Section 1] a *local coordinate* at Q. Let $t_Q = s_Q - s_Q(Q)$.

Lemma 2.3. (i) *t_Q is a uniformizer at Q.*

(ii) *$\tilde{t}_Q$ is a uniformizer at $\tilde{Q}$.*

(iii) *Let L_v be a finite extension of K_v with valuation ring $\mathbb{O}_{L_v}$ and uniformizing element π. Then t_Q is regular and injective on $\{P \in C(L_v) : \tilde{P} = \tilde{Q}\}$. Indeed, t_Q defines a bijection between $\{P \in C(L_v) : \tilde{P} = \tilde{Q}\}$ and $\pi\mathbb{O}_{L_v}$, given by $P \mapsto t_Q(P)$.*

Proof. Parts (i) and (ii) are clear from the construction. Part (iii) is standard; see for example [Lorenzini and Tucker 2002, Section 1] or [Wetherell 1997, Sections 1.7 and 1.8]. □

We shall refer to t_Q, constructed as above, as a *well-behaved uniformizer* at Q.

Now let $Q \in C(\overline{K})$ and fix an extension of v to $K(Q)$. By a *well-behaved uniformizer* t_Q at Q, we mean an element $t_Q \in K(Q)(C)$ that is a well-behaved uniformizer for the point Q on the curve $C \times K(Q)$.

Evaluating integrals on curves. Inside Ω_{C/K_v} is the lattice $\Omega_{\mathscr{C}/\mathbb{O}_v}$. Let P and Q belong to $C(K)$ and satisfy $\tilde{P} = \tilde{Q}$. Let $\omega \in \Omega_{\mathscr{C}/\mathbb{O}_v}$. Let $t_Q \in K(C)$ be a well-behaved uniformizer at Q. We can expand ω (after viewing it as an element in $\Omega_{\hat{\mathbb{O}}_Q}$) as a formal power series as

$$\omega = (a_0 + a_1 t_Q + a_2 t_Q^2 + \cdots)\, dt_Q, \tag{5}$$

where the coefficients a_i are all integers in K_v (see for example [Lorenzini and Tucker 2002, Proposition 1.6] or [Wetherell 1997, Sections 1.7 and 1.8]); here we have not used the assumption that $t_Q(Q) = 0$, but instead merely that t_Q is a local coordinate at Q. We can now evaluate the integral (see for example [Lorenzini and Tucker 2002, Proposition 1.3])

$$\int_Q^P \omega = \sum_{i=0}^{\infty} \frac{a_{i+1}}{i+1} t_Q(P)^{i+1},$$

where the infinite series converges since $|t_Q(P)| < 1$ by Lemma 2.3(iii).

3. Chabauty for a single residue class

As an algebraic variety, the d-th symmetric power $C^{(d)}$ is the quotient of the d-th Cartesian power C^d by the action of the d-th symmetric group. We represent points of $C^{(d)}(K)$ as unordered d-tuples $\mathcal{P} = \{P_1, \ldots, P_d\}$ such that $P_i \in C(\overline{K})$ and $\{P_1, \ldots, P_d\}$ is invariant under the action of $\mathrm{Gal}(\overline{K}/K)$. It is often useful to think of $\mathcal{P} = \{P_1, \ldots, P_d\}$ as a positive K-rational divisor on C of degree d. A useful reference on the geometry of symmetric powers of curves is [Milne 1986].

Let $\mathrm{red}_v : C^{(d)}(K_v) \to C^{(d)}(k_v)$ denote the reduction map. The *residue class* of $\mathcal{P}$ in $C^{(d)}(K_v)$ is defined as the fibre of the reduction map containing this d-tuple; in other words, it is the set $\mathrm{red}_v^{-1}(\mathrm{red}_v(\mathcal{P}))$. There are clearly only finitely many residue classes.

This section gives a criterion for a given $\mathcal{Q} \in C^{(d)}(K)$ to be the unique K-rational point in its residue class. Let $V \subset \Omega_{C/K_\upsilon}$ be the annihilator of $J(K) \subset J(K_\upsilon)$ under the pairing (4). Write

$$\mathcal{V} = V \cap \Omega_{\mathscr{C}/\mathbb{O}_\upsilon}.$$

Lemma 3.1. *$\mathcal{V}$ is a free $\mathbb{O}_\upsilon$-module of rank at least $g - \operatorname{rank} J(K)$.*

Proof. This is a standard observation. It suffices to show that $\dim_{K_\upsilon} V \geq g - s$, where s is the rank of $J(K)$. Recall that torsion belongs to the kernel of the pairing (4) on the right. Let $D_1, \ldots, D_s$ be a Mordell–Weil basis for $J(K)$ modulo torsion. Then a global 1-form $\omega \in \Omega_{C/K_\upsilon}$ belongs to V if and only if it annihilates $D_1, \ldots, D_s$. Thus V is a subspace of Ω_{C/K_υ} defined by s (not necessarily independent) K_υ-linear conditions. Since the dimension of Ω_{C/K_υ} is g, the lemma follows. □

Let $\omega \in \Omega_{\mathscr{C}/\mathbb{O}_\upsilon}$. Let $Q \in C(\overline{K})$; fix an extension of υ to $K(Q)$ and denote it also by υ. Let $t_Q \in K(Q)(C)$ be a well-behaved uniformizer at the point Q. Expand ω as in (5), where the coefficients a_i are integers in $K(Q)_\upsilon$. For a positive integer m, define

$$\mathbf{v}(\omega, t_Q, m) = \left(a_0, \tfrac{1}{2}a_1, \tfrac{1}{3}a_2, \ldots, \tfrac{1}{m}a_{m-1}\right). \tag{6}$$

Now let $\omega_1, \ldots, \omega_r$ be an $\mathbb{O}_\upsilon$-basis for $\mathcal{V}$, and let $\mathcal{Q}$ be an element of $C^{(d)}(K)$. The unordered d-tuple $\mathcal{Q}$ may have some repetition in it, and we need to take a careful account of that possibility. At this point it will be convenient to identify $C^{(d)}(K)$ with the set of effective K-rational divisors of degree d. Thus we can write

$$\mathcal{Q} = \sum_{j=1}^{l} d_j Q_j, \tag{7}$$

where $Q_1, Q_2, \ldots, Q_l$ are distinct and $d_j > 0$. We call d_j the *multiplicity* of Q_j in $\mathcal{Q}$. Note that $d = d_1 + d_2 + \cdots + d_l$. Let $L = K(Q_1, \ldots, Q_l)$ and fix an extension of υ to L, which we also denote by υ. Let $\mathcal{A}$ be the $r \times d$ matrix

$$\mathcal{A} = \begin{pmatrix} \mathbf{v}(\omega_1, t_{Q_1}, d_1) & \mathbf{v}(\omega_1, t_{Q_2}, d_2) & \cdots & \mathbf{v}(\omega_1, t_{Q_l}, d_l) \\ \mathbf{v}(\omega_2, t_{Q_1}, d_1) & \mathbf{v}(\omega_2, t_{Q_2}, d_2) & \cdots & \mathbf{v}(\omega_2, t_{Q_l}, d_l) \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}(\omega_r, t_{Q_1}, d_1) & \mathbf{v}(\omega_r, t_{Q_2}, d_2) & \cdots & \mathbf{v}(\omega_r, t_{Q_l}, d_l) \end{pmatrix}. \tag{8}$$

The main objective of this section is to prove the following theorem.

Theorem 3.2. *Suppose C is a smooth projective curve of genus $g \geq 2$ over a number field K, and write J for the Jacobian of C. Let d be a positive integer and $\mathcal{Q}$ an element of $C^{(d)}(K)$. Write $\mathcal{Q}$ as in (7) with $Q_1, Q_2, \ldots, Q_l$ distinct, having positive multiplicities $d_1, d_2, \ldots, d_l$. Let υ be a nonarchimedean prime of K, and let p be the rational prime below υ. Write k_υ for the residue field of υ. Write e for* *the ramification index of υ/p in $K/\mathbb{Q}$. Fix an extension of υ to $K(Q_1, \dots, Q_l)$, which we also denote by υ. Write e_j for the ramification index of υ in $K(Q_j)/K$, and let $f_j := [k_\upsilon(\tilde{Q}_j) : k_\upsilon]$. Let*

$$N = e \cdot \max\bigl\{\mathrm{lcm}(e_j, b) : 1 \le j \le l,\ 1 \le b \le d/f_j\bigr\}. \tag{9}$$

Suppose

(i) *υ is a prime of good reduction for C,*

(ii) *$p > d_1, d_2, \dots, d_l$, and*

(iii) *$\mathrm{ord}_p(d_j + i + 1) \le i/N$ for all $i \ge 0$ and $1 \le j \le l$.*

Let $\omega_1, \dots, \omega_r$ be an $\mathcal{O}_\upsilon$-basis for $\mathcal{V}$ (defined as above), and $\mathcal{A}$ be the $r \times d$ matrix associated with the ω_i and $\mathfrak{Q}$ as in (8). Write $\tilde{\mathcal{A}}$ for the reduction of $\mathcal{A}$ with entries in $\bar{k}_\upsilon$. If $\tilde{\mathcal{A}}$ has rank d, then the point $\mathfrak{Q}$ is the unique element in its residue class belonging to $C^{(d)}(K)$.

Remarks. (a) The matrix $\tilde{\mathcal{A}}$ has dimension $r \times d$, where r is the $\mathcal{O}_\upsilon$-rank of $\mathcal{V}$. It is evident that a necessary condition for the success of the criterion in the theorem is $r \ge d$. Evaluating the precise value of r is difficult, though by Lemma 3.1 we know that $r \ge g - \mathrm{rank}\, J(K)$. Hence it is sensible to apply the theorem when $\mathrm{rank}\, J(K) \le g - d$.

(b) We note the following useful simplification in the case where $d_1 = d_2 = \cdots = d_l = 1$ (that is $\mathfrak{Q} = \{Q_1, Q_2, \dots, Q_d\}$ with the Q_j distinct). Then $\mathcal{A} = (\alpha_{ij})$ is the $r \times d$ matrix with entries given by

$$\alpha_{ij} = \frac{\omega_i}{dt_{Q_j}}\bigg|_{t_{Q_j}=0}.$$

(c) At first glance it seems that hypothesis (iii) of the theorem requires checking an infinite list of inequalities, though this is not the case. To see this, fix $1 \le j \le l$ and let i_0 be the first value of i such that

$$u(i) := \frac{i}{N} - \log_p(d_j + i + 1) \ge 0 \quad \text{and} \quad \upsilon(i) := \frac{1}{N} - \frac{1}{(d_j + i + 1)\log p} \ge 0.$$

But $\upsilon = du/di$; thus u is a nondecreasing function on $i \ge i_0$. So

$$\frac{i}{N} \ge \log_p(d_j + i + 1) \ge \mathrm{ord}_p(d_j + i + 1) \quad \text{for all } i \ge i_0.$$

Hence we need only check the inequality $i/N \ge \mathrm{ord}_p(d_j + i + 1)$ for $0 \le i < i_0$.

(d) Our theorem should be related to [Klassen 1993, Proposition 11]. Klassen assumes that d is strictly less than the gonality, and so he is able to identify $C^{(d)}$ with its image $W^{(d)}$ on the Jacobian. He works with local parameters on $W^{(d)}$ instead of local parameters on the curve as we do. Moreover he phrases his criterion in terms of wedge products of 1-forms. We have not attempted to evaluate the precise overlap between our theorem and Klassen's. We expect that in the case where d is strictly less than the gonality and the multiplicities of $\mathcal{Q}$ are all 1, some variant of our theorem above may be deduced from Klassen's result. We are not at all confident that such a deduction is possible if these restrictions are not assumed.

(e) There is one striking difference between our approach and Klassen's: power series obtained through our method do not contain any mixed terms. Our power series equations are of the form $\sum_{j=1}^{d} f_{i,j}(z_j) = 0$ for $i = 1, \ldots, r$, with $f_{i,j}(z_j)$ being a power series in z_j. By the absence of mixed terms, we mean that our power series do not contain any terms that involve more than one unknown. We believe that these simpler power series should be useful in proving effective bounds for the number of points on $C^{(d)}(K)$, similar to Coleman's bounds [1985a] for $C(K)$.

Proof of Theorem 3.2. We continue with the notation of Theorem 3.2. Suppose that $\mathcal{Q}$ shares its residue class with $\mathcal{P} \in C^{(d)}(K)$. Our objective is to show that the two d-tuples are equal. Let L be the extension of K generated by the supports of the divisors $\mathcal{P}$ and $\mathcal{Q}$. In the statement of the theorem we fixed an extension υ to $K(Q_1, \ldots, Q_l)$, which we denoted also by υ. We now fix a further extension of υ to L (compatible with the earlier extension to $K(Q_1, \ldots, Q_l)$), and also denote it by υ. Let L_υ / K_υ be the corresponding extension of local fields, and write $\mathcal{O}_{L,\upsilon}$ for the integers of L_υ. We normalize $|\cdot|_\upsilon$ in the usual way, requiring $|p|_\upsilon = p^{-1}$. Without loss of generality we can rewrite

$$\mathcal{P} = \sum_{j=1}^{l} \sum_{j'=1}^{d_j} P_{j,j'}, \quad \text{where } \tilde{P}_{j,j'} = \tilde{Q}_j \text{ for } j = 1, \ldots, l.$$

Suppose $\omega \in \mathcal{V}$. Then $\mathcal{P} - \mathcal{Q}$ is a divisor of degree 0 and yields an element of $J(K)$. Since $\mathcal{V}$ is orthogonal to $J(K)$ with respect to the pairing (4), we obtain $\int_{\mathcal{P}-\mathcal{Q}} \omega = 0$. We may rewrite this as

$$\sum_{j=1}^{l} \sum_{j'=1}^{d_j} \int_{Q_j}^{P_{j,j'}} \omega = 0. \tag{10}$$

As before, we choose $t_{Q_j} \in K(Q_j)(C)$ to be well-behaved uniformizers at Q_j. Let $z_{j,j'} = t_{Q_j}(P_{j,j'})$. We note the following:

(a) $|z_{j,j'}|_\upsilon < 1$. This follows from Lemma 2.3(iii) as $P_{j,j'}$ belongs to the residue class of Q_j.

(b) $|z_{j,j'}|_\upsilon \le 1/p^{1/N}$, where N is given by (9). Let $L_{j,j'} = K(Q_j, P_{j,j'})$, which contains $z_{j,j'}$. Since $|z_{j,j'}|_\upsilon < 1$, all we have to show is that υ has ramification index at most N in $L_{j,j'}/\mathbb{Q}$. Recall that the ramification index for υ in $K/\mathbb{Q}$

is e. Hence it is enough to show that the ramification index of υ in $L_{j,j'}/K$ is at most $\operatorname{lcm}(e_j, b)$ for some $1 \le b \le d/f_j$. The ramification index for υ in $L_{j,j'}/K$ is at most the least common multiple of the ramification indices for υ in $K(Q_j)/K$ and $K(P_{j,j'})/K$. The former is denoted by e_j in the theorem. The latter is at most d/f_j since the extension $K(P_{j,j'})/K$ has degree at most d, and the corresponding residue field extension is $k_\upsilon(\tilde{Q}_j)/k_\upsilon$, whose degree was denoted by f_j.

(c) $z_{j,j'} = 0$ if and only if $Q_j = P_{j,j'}$. This again follows from Lemma 2.3(iii).

We will show that all $z_{j,j'} = 0$, and then $\mathcal{P} = \mathcal{Q}$ as required. Now fix some j and expand ω in terms of t_{Q_j} to obtain

$$\omega = (a_0 + a_1 t_{Q_j} + a_2 t_{Q_j}^2 + \cdots)\, dt_{Q_j},$$

where the a_i lie in $\mathcal{O}_{L,\upsilon}$ (page 216, middle). Integrating, we obtain

$$\begin{aligned} \int_{Q_j}^{P_{j,j'}} \omega &= \int_0^{z_{j,j'}} (a_0 + a_1 t_{Q_j} + a_2 t_{Q_j}^2 + \cdots)\, dt_{Q_j} = a_0 z_{j,j'} + \tfrac{1}{2} a_1 z_{j,j'}^2 + \cdots \\ &= \mathbf{v}(\omega, t_{Q_j}, d_j) \cdot \begin{pmatrix} z_{j,j'} \\ z_{j,j'}^2 \\ \vdots \\ z_{j,j'}^{d_j} \end{pmatrix} + z_{j,j'}^{d_j+1} \left(\frac{a_{d_j}}{d_j+1} + \frac{a_{d_j+1} z_{j,j'}}{d_j+2} + \cdots . \right). \end{aligned} \tag{11}$$

where $\mathbf{v}(\omega, t_{Q_j}, d_j)$ is as in (6). Note that hypothesis (ii) of the theorem ensures that the entries of $\mathbf{v}(\omega, t_{Q_j}, d_j)$ belong to $\mathcal{O}_{L,\upsilon}$. Moreover, by hypothesis (iii) and observation (b) above, we see that

$$\left(\frac{a_{d_j}}{d_j+1} + \frac{a_{d_j+1} z_{j,j'}}{d_j+2} + \cdots \right) \in \mathcal{O}_{L,\upsilon}.$$

Let π be a uniformizing element of L_υ. Let $\operatorname{ord}_\pi : L_\upsilon \to \mathbb{Z} \cup \{\infty\}$ be the normalized valuation corresponding to π. Write

$$m_j = \min_{j'=1,\ldots,d_j} \operatorname{ord}_\pi(z_{j,j'}) \quad \text{for } j = 1, \ldots, l. \tag{12}$$

Without loss of generality, we may suppose that

$$m_1(d_1+1) \le m_2(d_2+1) \le \cdots \le m_l(d_l+1).$$

We will show that $m_1 = \infty$; thus all $m_j = \infty$ and so all $z_{j,j'} = 0$, completing our proof. Thus suppose that $m_1 < \infty$.

We obtain from (11)

$$\int_{Q_j}^{P_{j,j'}} \omega \equiv \mathbf{v}(\omega, t_{Q_j}, d_j) \cdot \begin{pmatrix} z_{j,j'} \\ z_{j,j'}^2 \\ \vdots \\ z_{j,j'}^{d_j} \end{pmatrix} \pmod{\pi^{m_1(d_1+1)}}, \tag{13}$$

for all j, j'. Write

$$\boldsymbol{z}_j = \begin{pmatrix} z_{j,1} + z_{j,2} + \cdots + z_{j,d_j} \\ z_{j,1}^2 + z_{j,2}^2 + \cdots + z_{j,d_j}^2 \\ \vdots \\ z_{j,1}^{d_j} + z_{j,2}^{d_j} + \cdots + z_{j,d_j}^{d_j} \end{pmatrix} \quad \text{for } j = 1, \ldots, l.$$

From (10) and (13) we deduce that

$$\sum_{j=1}^{l} \mathbf{v}(\omega, t_{Q_j}, d_j) \cdot \boldsymbol{z}_j \equiv 0 \pmod{\pi^{m_1(d_1+1)}}. \tag{14}$$

For $\boldsymbol{z} \in (\mathcal{O}_{L,\upsilon})^d$, write $\boldsymbol{z} = (\boldsymbol{z}_1\ \boldsymbol{z}_2\ \cdots\ \boldsymbol{z}_l)^T$. From (14) we obtain

$$(\mathbf{v}(\omega, t_{Q_1}, d_1), \ldots, \mathbf{v}(\omega, t_{Q_l}, d_l)) \cdot \boldsymbol{z} \equiv 0 \pmod{\pi^{m_1(d_1+1)}}.$$

This is true for $\omega_1, \omega_2, \ldots, \omega_r$ in place of ω. So plainly (from the definition of $\mathcal{A}$ in (8)) we have $\mathcal{A}\boldsymbol{z} \equiv \mathbf{0} \pmod{\pi^{m_1(d_1+1)}}$. However, $\boldsymbol{z} \in (\mathcal{O}_{L,\upsilon})^d$, where $\mathcal{O}_{L,\upsilon}$ are the integers of L_υ. Moreover, we assume in the statement of the theorem that the reduction $\tilde{\mathcal{A}}$ of $\mathcal{A}$ modulo π has rank d. Hence $\boldsymbol{z} \equiv \mathbf{0} \pmod{\pi^{m_1(d_1+1)}}$. From the definition of $\boldsymbol{z}$ we obtain $\boldsymbol{z}_1 \equiv \mathbf{0} \pmod{\pi^{m_1(d_1+1)}}$ or equivalently

$$\begin{aligned} z_{1,1} + z_{1,2} + \cdots + z_{1,d_1} &\equiv 0 \pmod{\pi^{m_1(d_1+1)}}, \\ z_{1,1}^2 + z_{1,2}^2 + \cdots + z_{1,d_1}^2 &\equiv 0 \pmod{\pi^{m_1(d_1+1)}}, \\ &\vdots \\ z_{1,1}^{d_1} + z_{1,2}^{d_1} + \cdots + z_{1,d_1}^{d_1} &\equiv 0 \pmod{\pi^{m_1(d_1+1)}}. \end{aligned}$$

By Lemma 3.4 below, we see that $z_{1,1} \equiv z_{1,2} \equiv \cdots \equiv z_{1,d_1} \equiv 0 \pmod{\pi^{m_1+1}}$; in applying Lemma 3.4 we needed that $p > d_1$, which is given by hypothesis (ii) of the theorem. This contradicts the definition of m_1 in (12). The source of the contradiction is our assumption that $m_1 < \infty$. Thus $m_1 = \infty$. □

Lemma 3.3. *Suppose L_κ is a nonarchimedean local field of characteristic* 0 *with ring of integers $\mathcal{O}_\kappa$ and uniformizing element π. Suppose $\pi \mid p$ for a rational* *prime p. Let $h < p$ be a positive integer, and suppose that $z_1, \dots, z_h \in \mathbb{O}_\kappa$ satisfy*

$$\begin{aligned} z_1 + z_2 + \cdots + z_h &\equiv 0 \pmod{\pi}, \\ z_1^2 + z_2^2 + \cdots + z_h^2 &\equiv 0 \pmod{\pi}, \\ &\vdots \\ z_1^h + z_2^h + \cdots + z_h^h &\equiv 0 \pmod{\pi}. \end{aligned}$$

Then $z_1 \equiv z_2 \equiv \cdots \equiv z_h \equiv 0 \pmod{\pi}$.

Proof. The proof is by easy induction on h. The keys to the proof are Newton's identities [Garling 1986, page 113], which imply that $h z_1 z_2 \dots z_h \equiv 0 \pmod{\pi}$. Since $h < p$ we obtain that $z_j \equiv 0 \pmod{\pi}$ for some j, allowing us to reduce to the $h-1$ case. □

Lemma 3.4. *Suppose L_κ is a nonarchimedean local field of characteristic 0 with ring of integers $\mathbb{O}_\kappa$ and uniformizing element π. Suppose $\pi \mid p$ for a rational prime p. Let $h < p$ be a positive integer, and suppose that $z_1, \dots, z_h \in \mathbb{O}_\kappa$ satisfy*

$$\begin{aligned} z_1 + z_2 + \cdots + z_h &\equiv 0 \pmod{\pi^{m+1}}, \\ z_1^2 + z_2^2 + \cdots + z_h^2 &\equiv 0 \pmod{\pi^{2m+1}}, \\ &\vdots \\ z_1^h + z_2^h + \cdots + z_h^h &\equiv 0 \pmod{\pi^{hm+1}}, \end{aligned}$$

where $m \geq 0$. Then $z_1 \equiv z_2 \equiv \cdots \equiv z_h \equiv 0 \pmod{\pi^{m+1}}$.

Proof. By the previous lemma, $z_1 \equiv z_2 \equiv \cdots \equiv z_h \equiv 0 \pmod{\pi}$. Suppose that $z_1 \equiv z_2 \equiv \cdots \equiv z_h \equiv 0 \pmod{\pi^r}$ where $1 \leq r \leq m$. Let $z_i' = \pi^{-r} z_i$. Then $z_i' \in \mathbb{O}_\kappa$, and the previous lemma again applies with z_i' in place of the z_i. Hence $z_i' \equiv 0 \pmod{\pi}$, giving $z_i \equiv 0 \pmod{\pi^{r+1}}$. □

4. A relative version of Chabauty for covers of curves

Suppose that $\varrho : C \to C'$ is a morphism of curves of degree d defined over a number field K. Then $\varrho^* C'(K)$ is subset of $C^{(d)}(K)$. If $C'(K)$ is infinite, then so is $C^{(d)}(K)$. We know, thanks to Faltings's theorem, that $C'(K)$ can be infinite only if the genus of C' is 0 or 1. If $C'(K)$ is infinite, then some residue classes of $C^{(d)}$ will contain infinitely many K-rational points, and the criterion of Theorem 3.2 is bound to fail for these residue classes. In this situation it is indeed more natural to ask if a given residue class of $C^{(d)}$ contains K-rational points not belonging to $\varrho^* C'(K)$. In this section we give a criterion for a given residue class in $C^{(d)}(K)$ to contain only elements of $\varrho^* C'(K)$.

Let υ be a nonarchimedean prime of good reduction for both C and C'. To ease notation we shall write Ω_C and $\Omega_{C'}$ for the global 1-forms on C/K_υ and C'/K_υ, and let $\mathrm{Tr} : \Omega_C \to \Omega_{C'}$ be the trace map. Write Ω_0 for the kernel of this trace map.

Lemma 4.1. *Ω_0 has dimension $g_C - g_{C'}$, where g_C (respectively $g_{C'}$) is the genus of C (respectively C'). Moreover, $\Omega_C = \varrho^*(\Omega_{C'}) \oplus \Omega_0$.*

Proof. The lemma follows from the fact that the trace map is surjective: if $\omega \in \Omega_{C'}$, then $\mathrm{Tr}\,((1/d)\varrho^*\omega) = \omega$. □

Let $\mathscr{V}$ be as in the previous section, and let $\mathscr{V}_0 = \Omega_0 \cap \mathscr{V}$. Thus the 1-forms belonging to $\mathscr{V}_0$ enjoy two properties; the first is that their trace is 0 with respect to ϱ, and the second is that they are orthogonal to the Mordell–Weil group $J(K)$ with respect to the pairing (4).

Lemma 4.2. *With notation as above, $\mathscr{V}_0$ is a free $\mathbb{O}_\upsilon$-module satisfying*

$$\mathrm{rank}_{\mathbb{O}_\upsilon} \mathscr{V}_0 \geq (g_C - g_{C'}) - (\mathrm{rank}\, J_C(K) - \mathrm{rank}\, J_{C'}(K)).$$

Proof. The pairing (4) restricts to a bilinear pairing $\Omega_0 \times J_C(K_\upsilon) \to K_\upsilon$. Let Ω' be the annihilator of $J_C(K)$ with respect to this pairing. Then $\mathscr{V}_0 = \Omega' \cap \Omega_{\mathscr{C}/\mathbb{O}_\upsilon}$. It is sufficient to show that

$$\dim_{K_\upsilon} \Omega' \geq (g_C - g_{C'}) - (\mathrm{rank}\, J_C(K) - \mathrm{rank}\, J_{C'}(K)).$$

However, by Lemma 2.2 the pairing is trivial on $\varrho^* J_{C'}(K)$. By Lemma 4.1, the K_υ-dimension of Ω_0 is $g_C - g_{C'}$. Thus

$$\dim_{K_\upsilon} \Omega' \geq (g_C - g_{C'}) - \mathrm{rank}(J_C(K)/\varrho^* J_{C'}(K)).$$

The lemma follows at once by observing that the kernel of $\varrho^* : J_{C'} \to J_C$ contains only torsion (since $\varrho_* \circ \varrho^* = \deg(\varrho)$), so that

$$\mathrm{rank}(J_C(K)/\varrho^* J_{C'}(K)) = \mathrm{rank}\, J_C(K) - \mathrm{rank}\, J_{C'}(K). \qquad \square$$

Theorem 4.3. *With notation as above, let $\mathfrak{Q} = \sum_{j=1}^{d} Q_j$ be an element of $\varrho^* C'(K)$. Let υ be a nonarchimedean prime of K, of good reduction for C and C', and let p be the rational prime below υ. Write k_υ for the residue field of υ. Write e for the ramification index of υ/p in $K/\mathbb{Q}$. Fix an extension of υ to $K(Q_1, \ldots, Q_d)$, which we also denote by υ. Write e_j for the ramification index of υ in $K(Q_j)/K$, and let $f_j := [k_\upsilon(\tilde{Q}_j) : k_\upsilon]$. Let*

$$N' = e \cdot \max\left\{\mathrm{lcm}(e_j, b) : 1 \leq j \leq d,\ 1 \leq b \leq d(d-1)/f_j\right\}. \tag{15}$$

Suppose $\mathrm{ord}_p(i+1) < i/N'$ for all $i \geq 0$. Let $t_j \in K(Q_j)(C)$ be a well-behaved uniformizer at Q_j. Let $\omega_1, \omega_2, \ldots, \omega_s$ be a basis for $\mathscr{V}_0$. Let $\mathscr{A} = (\alpha_{i,j})$ be the

$s \times (d-1)$ matrix with entries

$$\alpha_{i,j} = \left.\frac{\omega_i}{dt_j}\right|_{t_j=0}, \quad \textit{for } i = 1, \ldots, s \textit{ and } j = 2, \ldots, d.$$

If the reduced matrix $\tilde{\mathcal{A}}$ with entries in $\bar{k}_v$ has rank $d-1$, then any element of $C^{(d)}(K)$ belonging to the residue class of $\mathcal{Q}$ does in fact belong to $\varrho^* C'(K)$.

Remark. For the criterion in the theorem to succeed, a necessary condition is $s \geq d-1$, where s is the $\mathcal{O}_v$-rank of $\mathcal{V}_0$. Considering Lemma 4.2, it is sensible to apply the theorem when

$$\operatorname{rank} J_C(K) - \operatorname{rank} J_{C'}(K) \leq g_C - g_{C'} - d + 1.$$

Proof of Theorem 4.3. We are supposing $\mathcal{Q} = \sum_{j=1}^d Q_j$ is some element of $\varrho^* C'(K)$ and $\mathcal{P} = \sum_{j=1}^d P_j$ shares its residue class. We reorder the P_j so that $\tilde{P}_j = \tilde{Q}_j$. Let $\mathcal{P}' = \varrho^* \varrho P_1$ and write $\mathcal{P}' = \sum_{j=1}^d P_j'$, where $P_1' = P_1$ and $\tilde{P}_j' = \tilde{P}_j = \tilde{Q}_j$ for $j = 2, \ldots, d$.

We want to show that $\mathcal{P} \in \varrho^* C'(K)$. We claim it suffices to show that $P_j = P_j'$ for $j = 2, \ldots, d$. Suppose for the moment this holds. Then $\varrho P_j = \varrho P_1$ for $j = 1, \ldots, d$. But the set $\{P_1, \ldots, P_d\}$ is stable under the action of $\mathrm{Gal}(\overline{K}/K)$. Hence ϱP_1 is fixed by the action of Galois and so is in $C'(K)$, establishing our claim.

To show that $P_j = P_j'$ for $j = 2, \ldots, d$, we need to modify the Chabauty strategy used in the proof of Theorem 3.2. Let $\omega \in \mathcal{V}_0$. As before

$$\int_{\mathcal{P}-\mathcal{Q}} \omega = 0, \quad \text{so} \quad 0 = \int_{\mathcal{P}-\mathcal{P}'} \omega + \int_{\mathcal{P}'-\mathcal{Q}} \omega.$$

However,

$$\int_{\mathcal{P}'-\mathcal{Q}} \omega = \int_{\varrho^*(\varrho P_1 - \varrho Q_1)} \omega = \int_{\varrho P_1 - \varrho Q_1} \operatorname{Tr} \omega = 0,$$

where we have used Lemma 2.2 and the fact that $\omega \in \mathcal{V}_0 \subset \Omega_0$, so its trace vanishes. We deduce that

$$0 = \int_{\mathcal{P}-\mathcal{P}'} \omega = \sum_{j=2}^d \int_{P_j'}^{P_j} \omega.$$

Recall that t_j was chosen as a well-behaved uniformizer at Q_j and that P_j and P_j' belong to the residue class at Q_j. Let $z_j = t_j(P_j)$ and $z_j' = t_j(P_j')$. We will show that $z_j = z_j'$ for $j = 2, \ldots, d$. Once this is done, Lemma 2.3 implies that $P_j = P_j'$, as required.

Now we may as before expand $\omega = (\alpha_j + \beta_j t_j + \gamma_j t_j^2 + \cdots)\, dt_j$, where the coefficients are integral. We obtain

$$0 = \sum_{j=2}^d \int_{P_j'}^{P_j} \omega = \sum_{j=2}^d \alpha_j (z_j - z_j') + \tfrac{1}{2}\beta_j (z_j^2 - {z_j'}^2) + \tfrac{1}{3}\gamma_j (z_j^3 - {z_j'}^3) + \cdots,$$

and so

$$\sum_{j=2}^{d} \alpha_j (z_j - z'_j) = \sum_{j=2}^{d} (z'_j - z_j)\big(\tfrac{1}{2}\beta_j (z_j + z'_j) + \tfrac{1}{3}\gamma_j (z_j^2 + z_j z'_j + {z'_j}^2) + \cdots\big). \quad (16)$$

Let L be the finite extension of K generated by the Q_j, P_j and P'_j. In the statement of the theorem, we chose an extension of υ to $K(Q_1, \dots, Q_d)$, which we also denoted by υ. We now extend υ to L in a way that is compatible with the earlier extension to $K(Q_1, \dots, Q_d)$, and we continue to denote it by υ. Let π be a uniformizing element of L_υ. Let

$$m = \min_{j=2,\dots,d} \operatorname{ord}_\pi (z_j - z'_j).$$

We would like to show that $m = \infty$ and so $z_j = z'_j$ for all j. We suppose $m < \infty$, aiming for a contradiction. We will show shortly that

$$|z_j|_\upsilon \le 1/p^{1/N'}, \quad |z'_j|_\upsilon \le 1/p^{1/N'} \quad \text{for } j = 2, \dots, d, \quad (17)$$

where N' is given by (15); let us assume this for the moment. One of the hypotheses of the theorem is that $\operatorname{ord}_p(i+1) < i/N'$ for all $i \ge 0$. Hence

$$|z_j^i/(i+1)|_\upsilon < 1, \quad |{z'_j}^i/(i+1)|_\upsilon < 1 \quad \text{for } i \ge 0 \text{ and } j = 2, \dots, d.$$

Hence $\frac{1}{2}(z_j + z'_j) \equiv \frac{1}{3}(z_j^2 + z_j z'_j + {z'_j}^2) \equiv \cdots \equiv 0 \pmod{\pi}$. Since $z_j \equiv z'_j \pmod{\pi^m}$, Equation (16) shows that

$$\sum_{j=2}^{d} \alpha_j (z_j - z'_j) \equiv 0 \pmod{\pi^{m+1}}.$$

If $\omega = \omega_i$, we see that α_j is precisely what is called $\alpha_{i,j}$ in the statement of the theorem. Hence we obtain

$$\sum_{j=2}^{d} \alpha_{i,j} (z_j - z'_j) \equiv 0 \pmod{\pi^{m+1}} \quad \text{for } i = 1, \dots, s.$$

Let $w_j = (z_j - z'_j)/\pi^m$. Then $w_j \in \mathcal{O}_{L,\upsilon}$. Also $\mathcal{A}(w_2 \ \cdots \ w_d)^T \equiv 0 \pmod{\pi}$. Because $\tilde{\mathcal{A}}$ has rank $d-1$, we see that all the $w_j \equiv 0 \pmod{\pi}$, and therefore $z_j \equiv z'_j \pmod{\pi^{m+1}}$ for all j. This contradicts the definition of m above, and shows that $m = \infty$ as required.

Our proof is complete except for claim (17). Naturally $|z_j|_\upsilon < 1$ and $|z'_j|_\upsilon < 1$. Also, z_j and z'_j are contained in $L_j = K(Q_j, P_j)$ and $L'_j = K(Q_j, P'_j)$. Thus it is sufficient to show that the ramification index in these fields is at most N'. Let us do this for L'_j; the corresponding proof for L_j is easier. The ramification index for υ in $K/\mathbb{Q}$ is e. The ramification index of υ in L'_j/K is the least common multiple of its ramification index in $K(Q_j)/K$ and $K(P'_j)/K$. The former ramification index is denoted by e_j in the statement of the theorem. We will see shortly that the field extension $K(P'_j)/K$ has degree at most $d(d-1)$; we know that the corresponding residue field extension is simply $k_\upsilon(\tilde{Q}_j)/k_\upsilon$, whose degree was denoted by f_j. Hence the ramification index for $K(P'_j)/K$ is at most $d(d-1)/f_j$. Putting this together, it only remains to show that the degree $[K(P'_j):K]$ is at most $d(d-1)$. Now $[K(P_1):K] \le d$ since P_1 belongs to the rational d-tuple $\mathcal{P}$. The P'_j are obtained by solving for P the degree d equation $\varrho P = \varrho P_1$. Clearly any solution must live in some extension of $K(P_1)$ of degree at most $d-1$. □

5. Chabauty using several primes

Let $\mathcal{L}$ be a (known) nonempty subset of $C^{(d)}(K)$. We next give a criterion for showing that $\mathcal{L}$ is equal to $C^{(d)}(K)$. This criterion involves using several well-chosen nonarchimedean primes $\upsilon_1, \dots, \upsilon_t$ of good reduction, applying Theorem 3.2 (and Theorem 4.3 in the case of a cover $C \to C'$) at each prime separately, and finally combining the information so obtained to show that $\mathcal{L}$ is equal to $C^{(d)}(K)$. Our method resembles the Mordell–Weil sieve [Bruin and Elkies 2002], which is often applied to show that a given curve has no rational points [Bruin and Stoll 2008]. We have found the Mordell–Weil sieve to yield very poor information in our situation; not only are we dealing with a variety $C^{(d)}$ which has rational points, we also have many points locally because of the dimension. We improve the situation dramatically by using Chabauty to remove the image under reduction maps of the known rational points, and then merely sieve for unknown rational points. If we obtain a contradiction, then we know there are no unknown rational points and we have provably determined all the rational points.

We shall make some assumptions:

- We know a subset $D_1, \dots, D_n$ of $J(K)$ that generates a subgroup G of finite index in $J(K)$. Such a subset can often be obtained using a descent argument; see for example [Cassels and Flynn 1996; Flynn 1994; Poonen and Schaefer 1997; Schaefer 1995; Schaefer and Wetherell 2005; Stoll 1998; 2001; 2002].
- The orders of the finite groups $J(k_{\upsilon_1}), \dots, J(k_{\upsilon_t})$ are coprime to the index of G in $J(K)$. This assumption can be verified using the standard method of checking p-saturation, as explained in [Flynn and Smart 1997, page 345], [Siksek 1995b, page 1526] and [Siksek 1995a].
- If $\varrho : C \to C'$ is a morphism of degree d, and $C'(K)$ is known, we also suppose $\varrho^* C'(K) \subseteq \mathcal{L}$.

Fix υ to be one of these primes of good reduction $\upsilon_1, \dots, \upsilon_t$. Let $N_{i,\upsilon}$ be the order of the reduction of $\tilde{D}_i$ in $J(k_\upsilon)$. Fix once and for all an element $\mathcal{Q}_0 \in \mathcal{L}$, and denote by $\jmath : C^{(d)}(K) \to J(K)$ the Abel–Jacobi map corresponding to $\mathcal{Q}_0$. We also lazily denote by $\jmath$ the Abel–Jacobi map $\jmath : C^{(d)}(k_\upsilon) \to J(k_\upsilon)$ corresponding to $\tilde{\mathcal{Q}}_0$. Let

$$\phi : \mathbb{Z}^n \to J(K), \quad (b_1, \dots, b_n) \mapsto \sum b_i D_i.$$

This induces a well-defined map

$$\tilde{\phi} : \prod_{i=1}^{n} \mathbb{Z}/N_{i,\upsilon}\mathbb{Z} \to J(k_\upsilon), \quad (\tilde{b}_1, \dots, \tilde{b}_n) \mapsto \sum b_i \tilde{D}_i.$$

These maps fit together in the commutative diagram

$$\begin{tikzcd}
\mathcal{L} \arrow[r, hook] \arrow[dr, "\mathrm{red}"'] & C^{(d)}(K) \arrow[r, "\jmath"] \arrow[d, "\mathrm{red}"] & J(K) \arrow[d, "\mathrm{red}"] & \mathbb{Z}^n \arrow[l, "\phi"'] \arrow[d] \\
 & C^{(d)}(k_\upsilon) \arrow[r, "\jmath"] & J(k_\upsilon) & \prod_{i=1}^n \mathbb{Z}/N_{i,\upsilon}\mathbb{Z}. \arrow[l, "\tilde{\phi}"']
\end{tikzcd}$$

We immediately notice that $\mathrm{red}(C^{(d)}(K)) \subseteq \jmath^{-1}\,\mathrm{red}(J(K))$. By assumption, the order of $J(k_\upsilon)$ is coprime to the index $[J(K) : G]$. Thus $\mathrm{red}(J(K)) = \mathrm{red}(G)$. We deduce that $\mathrm{red}(C^{(d)}(K)) \subset \jmath^{-1}\,\mathrm{im}\,\tilde{\phi}$. The set $\jmath^{-1}\,\mathrm{im}\,\tilde{\phi}$ is finite and computable. Recall that our objective is to show, somehow, that $C^{(d)}(K) = \mathcal{L}$. Assume the existence of some element $\mathcal{P} = \{P_1, \dots, P_d\}$ of $C^{(d)}(K)$ that *does not* belong to $\mathcal{L}$. We would like to say something about the reduction $\tilde{\mathcal{P}}$ in $C^{(d)}(k_\upsilon)$. Suppose now that $\mathcal{Q} = \{Q_1, \dots, Q_d\} \in \mathcal{L}$ satisfies the criterion of Theorem 3.2. Then $\mathcal{Q}$ is the only element in its residue class. Hence $\tilde{\mathcal{P}} \neq \tilde{\mathcal{Q}}$. Likewise in the case of a morphism $\varrho : C \to C'$ of degree d, if $\mathcal{Q}$ belongs to $\varrho^* C'(K) \subseteq \mathcal{L}$ and satisfies the criterion of Theorem 4.3, then $\tilde{\mathcal{P}} \neq \tilde{\mathcal{Q}}$. Now let $\mathcal{M}_\upsilon$ be the subset of those $\tilde{\mathcal{R}}$ in $\jmath^{-1}\,\mathrm{im}\,\tilde{\phi}$ satisfying either

- $\tilde{\mathcal{R}} \notin \mathrm{red}(\mathcal{L})$, or
- $\tilde{\mathcal{R}} = \tilde{\mathcal{Q}}$ for some $\mathcal{Q} \in \mathcal{L}$ that *does not* satisfy the criterion of Theorem 3.2, or
- we are in the case of a degree d cover $\varrho : C \to C'$ and $\tilde{\mathcal{R}} = \tilde{\mathcal{Q}}$ for some $\mathcal{Q} \in \varrho^* C'(K)$ that *does not* satisfy the criterion of Theorem 4.3.

It is plain that the reduction $\tilde{\mathcal{P}}$ of our hypothetical point $\mathcal{P} \in C^{(d)}(K) \setminus \mathcal{L}$ belongs to $\mathcal{M}_\upsilon$. Define

$$\mathcal{N}_\upsilon = \tilde{\phi}^{-1} \jmath(\mathcal{M}_\upsilon) \subseteq \prod_{i=1}^{n} \mathbb{Z}/N_{i,\upsilon}\mathbb{Z}.$$

The set $\mathcal{N}_\upsilon$ carries some information about the hypothetical point $\mathcal{P}$. This information was obtained by considering only one nonarchimedean prime υ. We would like to combine the information coming from each of our chosen primes $\upsilon_1, \dots, \upsilon_t$. We let

$$N_i = \mathrm{lcm}(N_{i,\upsilon_1}, N_{i,\upsilon_2}, \dots, N_{i,\upsilon_t}) \quad \text{for } i = 1, \dots, n.$$

For each $\upsilon = \upsilon_1, \dots, \upsilon_t$, there is a natural projection

$$\sigma_\upsilon : \prod_{i=1}^{n} \mathbb{Z}/N_i\mathbb{Z} \to \prod_{i=1}^{n} \mathbb{Z}/N_{i,\upsilon}\mathbb{Z}.$$

We are now ready to state our main result of this section.

Theorem 5.1. *Under the hypotheses above, suppose that*

$$\bigcap_{\upsilon=\upsilon_1}^{\upsilon_t} \sigma_\upsilon^{-1}\mathcal{N}_\upsilon = \varnothing.$$

Then $C^{(d)}(K) = \mathcal{L}$.

Proof. Suppose $\mathcal{P} \in C^{(d)}(K) \setminus \mathcal{L}$. From the discussion above, we know that

$$\tilde{\mathcal{P}} \in \mathcal{M}_\upsilon \quad \text{for } \upsilon = \upsilon_1, \dots, \upsilon_t.$$

Now $\jmath\mathcal{P} \in J(K)$ and $D_1, \dots, D_n$ generate a subgroup G of $J(K)$ of finite index $m = [J(K) : G]$. Thus

$$m \cdot \jmath\mathcal{P} = a_1 D_1 + a_2 D_2 + \cdots + a_n D_n \quad \text{for some } a_1, \dots, a_n \in \mathbb{Z}.$$

The index m is coprime to $\#J(k_\upsilon)$ for $\upsilon = \upsilon_1, \dots, \upsilon_t$. Hence there is some $m^* \in \mathbb{Z}$ such that

$$m^* m \equiv 1 \mod \operatorname{lcm}\{\#J(k_\upsilon) : \upsilon = \upsilon_1, \dots, \upsilon_t\}.$$

The equality $m^*m \cdot \jmath\mathcal{P} = (m^*a_1)D_1 + (m^*a_2)D_2 + \cdots + (m^*a_n)D_n$ takes place in $J(K)$, with the coefficients m^*a_i belonging to $\mathbb{Z}$. Applying $\operatorname{red}_\upsilon : J(K) \to J(k_\upsilon)$, and recalling that $m^*m \equiv 1 \mod \#J(k_\upsilon)$, we get

$$\jmath\tilde{\mathcal{P}} = (m^*a_1)\tilde{D}_1 + (m^*a_2)\tilde{D}_2 + \cdots + (m^*a_n)\tilde{D}_n.$$

Recall our observation at the beginning of the proof that $\tilde{\mathcal{P}} \in \mathcal{M}_\upsilon$. Hence the image of $(m^*a_1, \dots, m^*a_n) \in \mathbb{Z}^n$ in $\prod_{i=1}^n \mathbb{Z}/N_{i,\upsilon}\mathbb{Z}$ belongs to $\mathcal{N}_\upsilon = \tilde{\phi}^{-1}\jmath\mathcal{M}_\upsilon$. Thus the image of $(m^*a_1, \dots, m^*a_n) \in \mathbb{Z}^n$ in $\prod_{i=1}^n \mathbb{Z}/N_i\mathbb{Z}$ belongs to $\bigcap \sigma_\upsilon^{-1}\mathcal{N}_\upsilon$. This contradicts the assumption that $\bigcap \sigma_\upsilon^{-1}\mathcal{N}_\upsilon = \varnothing$ and completes our proof. □

6. Examples

In this section we use our method to compute $C^{(2)}(\mathbb{Q})$ for two genus 3 curves, both with Jacobians having rank 1. The first example is hyperelliptic and the second is a nonsingular plane quartic. All computations are done using the `MAGMA` package [Bosma et al. 1997; MAGMA 2009].

A hyperelliptic example. Let C be the smooth projective curve over $\mathbb{Q}$ with affine chart

$$C : y^2 = x(x^2+2)(x^2+43)(x^2+8x-6), \tag{18}$$

and write f for the polynomial on the right. Being hyperelliptic, C is of course a double cover of the projective line. In our earlier notation, the map $\varrho : C \to C'$ is just the map

$$C \to \mathbb{P}^1, \quad (x, y) \mapsto x, \ \infty \mapsto \infty.$$

Thus

$$\varrho^*\mathbb{P}^1(\mathbb{Q}) = \left\{\{(x, \sqrt{f(x)}), (x, -\sqrt{f(x)})\} : x \in \mathbb{Q}\right\} \cup \{\{\infty, \infty\}\}.$$

Note that the hyperelliptic involution $\imath : C \to C$ extends to an involution on $C^{(2)}$, which we will also denote by $\imath$. Thus

$$\imath : C^{(2)} \to C^{(2)}, \quad \{(x_1, y_1), (x_2, y_2)\} \mapsto \{(x_1, -y_1), (x_2, -y_2)\}.$$

Let

$$\mathscr{L} = \varrho^*\mathbb{P}^1(\mathbb{Q}) \cup \{\mathfrak{Q}_i : i = 1, \dots, 10\} \subseteq C^{(2)}(\mathbb{Q})$$

where

$$\begin{aligned}
\mathfrak{Q}_1 &= \{(\sqrt{6}, 56\sqrt{6}), (-\sqrt{6}, -56\sqrt{6})\},\\
\mathfrak{Q}_2 &= \{(0, 0), \infty\},\\
\mathfrak{Q}_3 &= \{(\sqrt{-2}, 0), (-\sqrt{-2}, 0)\},\\
\mathfrak{Q}_4 &= \{(\sqrt{-43}, 0), (-\sqrt{-43}, 0)\},\\
\mathfrak{Q}_5 &= \{(-4+\sqrt{22}, 0), (-4-\sqrt{22}, 0)\},\\
\mathfrak{Q}_6 &= \left\{\left(\frac{41+\sqrt{1509}}{2}, -222999-5740\sqrt{1509}\right), \text{ conjugate}\right\}\\
\mathfrak{Q}_7 &= \left\{\left(\frac{-164+\sqrt{22094}}{49}, \frac{257704352-1648200\sqrt{22094}}{823543}\right), \text{ conjugate}\right\},\\
\mathfrak{Q}_8 &= \imath\mathfrak{Q}_1,\\
\mathfrak{Q}_9 &= \imath\mathfrak{Q}_6,\\
\mathfrak{Q}_{10} &= \imath\mathfrak{Q}_7.
\end{aligned}$$

We want to show that $C^{(2)}(\mathbb{Q}) = \mathscr{L}$. First we need some information about the Mordell–Weil group $J(\mathbb{Q})$, where J is the Jacobian of C. Using the `MAGMA` routine for 2-descent on Jacobians of hyperelliptic curves, we find $J(\mathbb{Q})$ has Mordell–Weil rank 1; this routine is an implementation of the algorithm in [Stoll 2001].

Write $\jmath : C^{(2)} \to J$ for the Abel–Jacobi map given by $\mathscr{P} \mapsto \mathscr{P} - 2\infty$. Write $D_i = \jmath\mathfrak{Q}_i$, where $i = 1, \dots, 10$. Then D_1 has infinite order, and D_2, D_3, D_4 are a basis for the 2-torsion. We note the relations

$$D_5 = D_2 + D_3 + D_4, \quad D_6 = D_1 + D_2 + D_3, \quad D_7 = D_1 + D_2 + D_4,$$
$$D_8 = -D_1, \quad D_9 = -D_7, \quad D_{10} = -D_8.$$

We believe that D_1, D_2, D_3, D_4 is a Mordell–Weil basis for $J(\mathbb{Q})$, although we are unable to prove this. However, D_1, D_2, D_3, D_4 generates a subgroup G of full rank and hence finite index. Using our implementation of the p-saturation method (from [Flynn and Smart 1997, page 345], [Siksek 1995b, page 1526] and [Siksek 1995a]) we verified that this index is not divisible by any prime $l \le 100$; this verification took just a few seconds.

The primes of bad reduction for C are 2, 3, 11, 41, 43, 5153. We shall work with primes $p = 5$, 7, 13 of good reduction. Note that

$$\#J(\mathbb{F}_5) = 2^6 \times 3, \qquad \#J(\mathbb{F}_7) = 2^5 \times 5, \qquad \#J(\mathbb{F}_{13}) = 2^{10}.$$

It follows that the index of G in $J(\mathbb{Q})$ is coprime to the orders of these groups. To use our theorems we must, for each of our chosen primes p, compute a $\mathbb{Z}_p$-basis for the global 1-forms $\mathcal{V}$ that kill off $J(\mathbb{Q})$. Of course $\mathcal{V}$ is a submodule of the $\mathbb{Z}_p$-module spanned by the basis for global 1-forms: dx/y, $x\,dx/y$, x^2dx/y.

Work first with $p = 5$. Now $D = 3D_1 + D_3 + D_4$ is in the kernel of reduction. We compute (see [McCallum and Poonen 2006] and [Wetherell 1997] for hints on computing p-adic integrals):

$$\int_D \frac{dx}{y} \equiv 5 \times 1471729 \pmod{5^{10}},$$
$$\int_D \frac{x\,dx}{y} \equiv 5 \times 1174134 \pmod{5^{10}},$$
$$\int_D \frac{x^2dx}{y} \equiv 5 \times 1135401 \pmod{5^{10}}.$$

We can take

$$\omega_1 = \frac{dx}{y} + \epsilon\frac{x^2dx}{y} \quad \text{and} \quad \omega_2 = \frac{x\,dx}{y} + \delta\frac{x^2dx}{y}$$

as a $\mathbb{Z}_5$-basis for $\mathcal{V}$, where

$$\epsilon \equiv 510496 \pmod{5^9} \quad \text{and} \quad \delta \equiv 395091 \pmod{5^9}.$$

Since $\mathbb{P}^1$ has genus 0, Lemma 4.1 shows that $\boldsymbol{\Omega}_0 = \boldsymbol{\Omega}$ (in the notation of Section 4) and hence $\mathcal{V}_0 = \mathcal{V}$.

Although we programmed our criteria for Theorems 3.2, 4.3 and 5.1 in `MAGMA`, we will however carry out some of the calculations explicitly to give the reader a taste for these. Consider for example $\mathcal{Q}_0 = \{(0,0), (0,0)\} \in \varrho^*\mathbb{P}^1(\mathbb{Q})$. Let us show that $\mathcal{Q}_0$ does not share its residue class with any element of $C^{(2)}(\mathbb{Q})$ not belonging to $\varrho^*\mathbb{P}^1(\mathbb{Q})$. We apply the criterion of Theorem 4.3. We take y as the uniformizer at the point $(0,0)$. From $y^2 = f(x)$, we see that $2y dy = f'(x) dx$. Hence

$$\left(\frac{1}{y}\frac{dx}{dy}\right)\Big|_{y=0} = \frac{2}{f'(x)}\Big|_{y=0} = \frac{2}{f'(0)} = \frac{-1}{258}.$$

Hence

$$\frac{\omega_1}{dy}\Big|_{y=0} \equiv 3 \pmod 5$$

and so by Theorem 4.3, $\mathcal{Q}_0$ does not share its residue class with any element of $C^{(2)}(\mathbb{Q})$ not belonging to $\varrho^*\mathbb{P}^1(\mathbb{Q})$. The reader may care to repeat this calculation with $\{\infty, \infty\}$, and $\{(a, \sqrt{f(a)}), (a, -\sqrt{f(a)})\}$ for $a = 1, \ldots, 4$. The outcome of such a calculation is that no element in $\varrho^*\mathbb{P}^1(\mathbb{Q})$ shares its residue class with an element of $C^{(2)}(\mathbb{Q})$ not belonging to $\varrho^*\mathbb{P}^1(\mathbb{Q})$.

We now apply Theorem 3.2 to $\mathcal{Q}_1$. We can take $t_1 = x - \sqrt{6}$ as a uniformizer at $(\sqrt{6}, 56\sqrt{6})$. Note that $dt_1 = dx$. Thus

$$\frac{x^i}{y}\frac{dx}{dt_1}\Big|_{t_1=0} = \frac{\sqrt{6}^{\,i}}{56\sqrt{6}}.$$

We see that

$$\frac{\omega_1}{dt_1}\Big|_{t_1=0} = \frac{1+6\epsilon}{56\sqrt{6}} \quad \text{and} \quad \frac{\omega_2}{dt_1}\Big|_{t_1=0} = \frac{\sqrt{6}+6\delta}{56\sqrt{6}}.$$

For $(-\sqrt{6}, -56\sqrt{6})$, we take $t_2 = x + \sqrt{6}$ as a uniformizer. We get

$$\frac{\omega_1}{dt_2}\Big|_{t_2=0} = \frac{1+6\epsilon}{-56\sqrt{6}} \quad \text{and} \quad \frac{\omega_2}{dt_2}\Big|_{t_2=0} = \frac{-\sqrt{6}+6\delta}{-56\sqrt{6}}.$$

We compute the determinant

$$\begin{vmatrix} \dfrac{1+6\epsilon}{56\sqrt{6}} & \dfrac{\sqrt{6}+6\delta}{56\sqrt{6}} \\ \dfrac{1+6\epsilon}{-56\sqrt{6}} & \dfrac{-\sqrt{6}+6\delta}{-56\sqrt{6}} \end{vmatrix} = \frac{2(1+6\epsilon)}{56^2\sqrt{6}} \equiv 4 \pmod 5,$$

where in the last step we chose $\sqrt{6} = 1 + 3\times 5 + 4\times 5^3 + \cdots$. By Theorem 3.2, $\mathcal{Q}_1$ does not share its residue class with any other element of $C^{(2)}(\mathbb{Q})$. By similar arguments, the same is true of $\mathcal{Q}_i$ for $i = 2, \ldots, 10$.

Suppose now that $\mathcal{P} \in C^{(2)}(\mathbb{Q}) \setminus \mathcal{L}$. We would like to deduce a contradiction. The argument at the end of the proof of Theorem 5.1 shows that there are integers n_1, n_2, n_3, n_4 such that simultaneously in each of $J(\mathbb{F}_p)$ with $p = 5, 7, 13$ we have

$$\jmath\tilde{\mathcal{P}} = n_1\tilde{D}_1 + n_2\tilde{D}_2 + n_3\tilde{D}_3 + n_4\tilde{D}_4.$$

In $J(\mathbb{F}_5)$, the order of $\tilde{D}_1$ is 6 while $\tilde{D}_2$, $\tilde{D}_3$, $\tilde{D}_4$ are of order 2. Consider the maps

$$C^{(2)}(\mathbb{F}_5) \xrightarrow{\jmath} J(\mathbb{F}_5) \xleftarrow{\tilde{\phi}} \mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3.$$

We see that (n_1, n_2, n_3, n_4) mod $(6, 2, 2, 2)$ belongs to $\tilde{\phi}^{-1}(\jmath C^{(2)}(\mathbb{F}_5))$. Using our `MAGMA` program, we wrote down the set $\tilde{\phi}^{-1}(\jmath C^{(2)}(\mathbb{F}_5))$ and found that it has 22 elements. In the notation of Section 5, we want to write down the set $\mathcal{N}_5$. This is the subset of $\tilde{\phi}^{-1}(\jmath C^{(2)}(\mathbb{F}_5))$ containing all quadruples that, on the basis of our Chabauty calculations above, cannot be (n_1, n_2, n_3, n_4) mod $(6, 2, 2, 2)$. For example, the quadruple $(0, 0, 0, 0)$ is in $\tilde{\phi}^{-1}(\jmath C^{(2)}(\mathbb{F}_5))$. However, if $(n_1, n_2, n_3, n_4) \equiv (0, 0, 0, 0)$ mod $(6, 2, 2, 2)$, then $\mathcal{P}$ shares its residue class with some element of $\jmath^{-1}\mathbb{P}^1(\mathbb{Q})$, contradicting our computations above. Therefore $(0, 0, 0, 0) \notin \mathcal{N}_5$. Similarly we can exclude another 10 elements corresponding to $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_{10}$. This leaves us with 11 elements in $\mathcal{N}_5$:

$$\begin{aligned}\mathcal{N}_5 = \{&(2,0,1,1),\ (2,1,0,1),\ (2,1,1,0),\ (3,0,0,1),\ (3,0,1,0),\ (3,0,1,1),\\ &(3,1,0,0),\ (3,1,1,1),\ (4,0,1,1),\ (4,1,0,1),\ (4,1,1,0)\}\\ &\subset \mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3.\end{aligned}$$

We know that (n_1, n_2, n_3, n_4) is equivalent modulo $(6, 2, 2, 2)$ to one of these 11 elements of $\mathcal{N}_5$.

Next we repeat the calculation with $p = 7$. Our Chabauty arguments, Theorems 3.2 and 4.3, succeed for $\jmath^{-1}\mathbb{P}^1(\mathbb{Q})$ and $\mathfrak{Q}_3$ and fail for all other $\mathfrak{Q}_i$. There are good reasons for these failures. It turns out that $\mathfrak{Q}_1$, $\mathfrak{Q}_4$ and $\mathfrak{Q}_8$ share the same residue class, likewise for $\mathfrak{Q}_5$, $\mathfrak{Q}_6$ and $\mathfrak{Q}_9$, and for $\mathfrak{Q}_2$, $\mathfrak{Q}_7$ and $\mathfrak{Q}_{10}$. Despite this, the information given by $p = 7$ is still useful, this time because the set $\tilde{\phi}^{-1}(\jmath C^{(2)}(\mathbb{F}_7))$ is small, having only 10 elements. We have excluded two of them, those corresponding to $\jmath^{-1}\mathbb{P}^1(\mathbb{Q})$ and $\mathfrak{Q}_3$. We are left with

$$\begin{aligned}\mathcal{N}_7 = \{&(0,0,0,1), (0,1,0,0),\ (0,1,1,1),\ (1,0,0,0),\\ &(1,0,0,1),\ (1,0,1,1),\ (1,1,0,1),\ (1,1,1,0)\} \subset (\mathbb{Z}/2\mathbb{Z})^4.\end{aligned}$$

We know that (n_1, n_2, n_3, n_4) is equivalent modulo $(2, 2, 2, 2)$ to one of these eight elements of $\mathcal{N}_7$. Combining the information from $\mathcal{N}_5$ and $\mathcal{N}_7$, we see that

$$(n_1, n_2, n_3, n_4) \equiv (3, 0, 0, 1) \quad \text{or} \quad (3, 0, 1, 1) \qquad \text{mod}\ (6, 2, 2, 2). \tag{19}$$

We still have not obtained a contradiction. Finally we let $p = 13$. This time we find

$$\begin{aligned}\mathcal{N}_{13} = \{&(3,1,0,1),\ (8,0,1,0), (8,0,1,1),\ (8,1,0,0),\ (8,1,0,1),\ (13,1,0,1)\}\\ &\subset \mathbb{Z}/16\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3.\end{aligned}$$

Again we know that (n_1, n_2, n_3, n_4) is equivalent modulo $(16, 2, 2, 2)$ to one of these six elements of $\mathcal{N}_{13}$. This contradicts the congruences in (19). We deduce that $C^{(2)}(\mathbb{Q}) = \mathcal{L}$ as required.

A plane quartic example. Let C be the smooth plane quartic (genus 3) curve with affine equation

$$C: \quad x^4 + (y^2+1)(x+y) = 0,$$

and let J be its Jacobian. Schaefer and Wetherell [2005] observe that it has a trivial automorphism group, and that its J is absolutely simple and not modular. Using a deep descent argument, they show that $J(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. They apply Chabauty to conclude that $C(\mathbb{Q}) = \{(0,0), (-1,0), \infty\}$.

Using our method we showed that $C^{(2)}(\mathbb{Q}) = \{\mathfrak{Q}_1, \dots, \mathfrak{Q}_{10}\}$, where

$$\begin{aligned}
\mathfrak{Q}_1 &= \bigl\{(-17+\sqrt{259}, -48+3\sqrt{259}),\ (-17-\sqrt{259}, -48-3\sqrt{259})\bigr\},\\
\mathfrak{Q}_2 &= \bigl\{\bigl(-1, \tfrac{1}{2}(1+\sqrt{-3})\bigr),\ \bigl(-1, \tfrac{1}{2}(1-\sqrt{-3})\bigr)\bigr\},\\
\mathfrak{Q}_3 &= \bigl\{\bigl(\tfrac{1}{2}(1+\sqrt{-3}), 0\bigr),\ \bigl(\tfrac{1}{2}(1-\sqrt{-3}), 0\bigr)\bigr\},\\
\mathfrak{Q}_4 &= \{(0,0), \infty\},\\
\mathfrak{Q}_5 &= \{(0,0), (0,0)\},\\
\mathfrak{Q}_6 &= \{(0,i), (0,-i)\},\\
\mathfrak{Q}_7 &= \{(-1,0), \infty\},\\
\mathfrak{Q}_8 &= \{(-1,0), (0,0)\},\\
\mathfrak{Q}_9 &= \{(-1,0), (-1,0)\},\\
\mathfrak{Q}_{10} &= \{\infty, \infty\}.
\end{aligned}$$

Acknowledgments

We thank the referees for carefully reading the manuscript and suggesting many improvements and corrections. We are indebted to Nils Bruin, Bjorn Poonen, Michael Stoll and Joseph Wetherell for helpful conversations about Chabauty, and to Miles Reid for useful algebraic geometry discussions. In particular, we are aware of some earlier Chabauty computations on symmetric squares of hyperelliptic genus 3 curves by Wetherell, although no details of such computations have been published.

References

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I, The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR 1484478 Zbl 0898.68039

[Bourbaki 1989] N. Bourbaki, *Lie groups and Lie algebras, Chapters 1–3*, Springer, Berlin, 1989. MR 89k:17001 Zbl 0672.22001

[Bruin 2002] N. R. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract **133**, Centrum voor Wiskunde en Informatica, Amsterdam, 2002. MR 2003i:11042 Zbl 1043.11029

[Bruin 2003] N. Bruin, "Chabauty methods using elliptic curves", *J. Reine Angew. Math.* **562** (2003), 27–49. MR 2004j:11051 Zbl 1135.11320

[Bruin and Elkies 2002] N. Bruin and N. D. Elkies, "Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with Galois groups of order 168 and $8 \cdot 168$", pp. 172–188 in *Algorithmic number theory* (Sydney, 2002), edited by C. Fieker and D. R. Kohel, Lecture Notes in Comput. Sci. **2369**, Springer, Berlin, 2002. MR 2005d:11094 Zbl 1058.11044

[Bruin and Stoll 2008] N. Bruin and M. Stoll, "Deciding existence of rational points on curves: An experiment", *Experiment. Math.* **17**:2 (2008), 181–189. MR 2433884

[Cassels and Flynn 1996] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series **230**, Cambridge University Press, 1996. MR 97i:11071 Zbl 0857.14018

[Chabauty 1941] C. Chabauty, "Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension", *C. R. Acad. Sci. Paris* **212** (1941), 1022–1024. MR 6,102e Zbl 0025.24903

[Coleman 1985a] R. F. Coleman, "Effective Chabauty", *Duke Mathematical J.* **52**:3 (1985), 765–770. MR 87f:11043 Zbl 0588.14015

[Coleman 1985b] R. F. Coleman, "Torsion points on curves and p-adic abelian integrals", *Ann. of Math.* (2) **121**:1 (1985), 111–168. MR 86j:14014 Zbl 0578.14038

[Colmez 1998] P. Colmez, *Intégration sur les variétés p-adiques*, Astérisque **248**, Société Mathématique de France, Paris, 1998. MR 2000e:14026 Zbl 0930.14013

[Debarre and Klassen 1994] O. Debarre and M. J. Klassen, "Points of low degree on smooth plane curves", *J. Reine Angew. Math.* **446** (1994), 81–87. MR 95f:14052 Zbl 0784.14014

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. MR 85g:11026a Zbl 0588.14026

[Faltings 1991] G. Faltings, "Diophantine approximation on abelian varieties", *Ann. of Math.* (2) **133**:3 (1991), 549–576. MR 93d:11066 Zbl 0734.14007

[Faltings 1994] G. Faltings, "The general case of S. Lang's conjecture", pp. 175–182 in *Barsotti Symposium in Algebraic Geometry* (Abano Terme, 1991), edited by V. Cristante and W. Messing, Perspect. Math. **15**, Academic Press, San Diego, CA, 1994. MR 95m:11061 Zbl 0823.14009

[Flynn 1994] E. V. Flynn, "Descent via isogeny in dimension 2", *Acta Arith.* **66**:1 (1994), 23–43. MR 95g:11057 Zbl 0835.14009

[Flynn 1995] E. V. Flynn, "On a theorem of Coleman", *Manuscripta Math.* **88**:4 (1995), 447–456. MR 97b:11082 Zbl 0865.14012

[Flynn 1997] E. V. Flynn, "A flexible method for applying Chabauty's theorem", *Compositio Math.* **105**:1 (1997), 79–94. MR 97m:11083 Zbl 0882.14009

[Flynn and Smart 1997] E. V. Flynn and N. P. Smart, "Canonical heights on the Jacobians of curves of genus 2 and the infinite descent", *Acta Arith.* **79**:4 (1997), 333–352. MR 98f:11066 Zbl 0895.11026

[Flynn and Wetherell 1999] E. V. Flynn and J. L. Wetherell, "Finding rational points on bielliptic genus 2 curves", *Manuscripta Math.* **100**:4 (1999), 519–533. MR 2001g:11098 Zbl 1029.11024

[Flynn and Wetherell 2001] E. V. Flynn and J. L. Wetherell, "Covering collections and a challenge problem of Serre", *Acta Arith.* **98**:2 (2001), 197–205. MR 2002b:11088 Zbl 1049.11066

[Garling 1986] D. J. H. Garling, *A course in Galois theory*, Cambridge University Press, 1986. MR 88d:12007 Zbl 0608.12025

[Grant 1994] D. Grant, "A curve for which Coleman's effective Chabauty bound is sharp", *Proc. Amer. Math. Soc.* **122**:1 (1994), 317–319. MR 94k:14019 Zbl 0834.14015

[Gross and Rohrlich 1978] B. H. Gross and D. E. Rohrlich, "Some results on the Mordell–Weil group of the Jacobian of the Fermat curve", *Invent. Math.* **44**:3 (1978), 201–224. MR 58 #10911 Zbl 0369.14011

[Harris and Silverman 1991] J. Harris and J. Silverman, "Bielliptic curves and symmetric products", *Proc. Amer. Math. Soc.* **112**:2 (1991), 347–356. MR 91i:11067 Zbl 0727.11023

[Kamienny 1986a] S. Kamienny, "Torsion points on elliptic curves over all quadratic fields", *Duke Mathematical J.* **53**:1 (1986), 157–162. MR 87g:11068 Zbl 0599.14029

[Kamienny 1986b] S. Kamienny, "Torsion points on elliptic curves over all quadratic fields, II", *Bull. Soc. Math. France* **114**:1 (1986), 119–122. MR 87j:11051 Zbl 0599.14030

[Kamienny 1992] S. Kamienny, "Torsion points on elliptic curves and q-coefficients of modular forms", *Invent. Math.* **109**:2 (1992), 221–229. MR 93h:11054 Zbl 0773.14016

[Klassen 1993] M. J. Klassen, *Algebraic points of low degree on curves of low rank*, thesis, University of Arizona, 1993.

[Klassen and Tzermias 1997] M. Klassen and P. Tzermias, "Algebraic points of low degree on the Fermat quintic", *Acta Arith.* **82**:4 (1997), 393–401. MR 98k:11086 Zbl 0917.11022

[Lorenzini and Tucker 2002] D. Lorenzini and T. J. Tucker, "Thue equations and the method of Chabauty–Coleman", *Invent. Math.* **148**:1 (2002), 47–77. MR 2003d:11088 Zbl 1048.11023

[MAGMA 2009] "MAGMA Computational Algebra System", web site, University of Sydney, 2009, Available at http://magma.maths.usyd.edu.au/magma/.

[McCallum 1992] W. G. McCallum, "The arithmetic of Fermat curves", *Math. Ann.* **294**:3 (1992), 503–511. MR 93j:11037 Zbl 0766.14013

[McCallum 1994] W. G. McCallum, "On the method of Coleman and Chabauty", *Math. Ann.* **299**:3 (1994), 565–596. MR 95c:11079 Zbl 0824.14017

[McCallum and Poonen 2006] W. McCallum and B. Poonen, "The method of Chabauty and Coleman", preprint, 2006, Available at http://math.arizona.edu/~wmc/Research/Chabauty.pdf.

[Merel 1996] L. Merel, "Bornes pour la torsion des courbes elliptiques sur les corps de nombres", *Invent. Math.* **124**:1-3 (1996), 437–449. MR 96i:11057 Zbl 0936.11037

[Milne 1986] J. S. Milne, "Jacobian varieties", pp. 167–212 in *Arithmetic geometry* (Storrs, CT, 1984), edited by G. Cornell and J. H. Silverman, Springer, New York, 1986. MR 861976 Zbl 0604.14018

[Parent 2000] P. Parent, "Torsion des courbes elliptiques sur les corps cubiques", *Ann. Inst. Fourier* (*Grenoble*) **50**:3 (2000), 723–749. MR 2001i:11067 Zbl 0971.11030

[Parent 2003] P. Parent, "No 17-torsion on elliptic curves over cubic number fields", *J. Théor. Nombres Bordeaux* **15**:3 (2003), 831–838. MR 2006a:11071 Zbl 1072.11037

[Poonen and Schaefer 1997] B. Poonen and E. F. Schaefer, "Explicit descent for Jacobians of cyclic covers of the projective line", *J. Reine Angew. Math.* **488** (1997), 141–188. MR 98k:11087 Zbl 0888.11023

[Schaefer 1995] E. F. Schaefer, "2-descent on the Jacobians of hyperelliptic curves", *J. Number Theory* **51**:2 (1995), 219–232. MR 96c:11066 Zbl 0832.14016

[Schaefer and Wetherell 2005] E. F. Schaefer and J. L. Wetherell, "Computing the Selmer group of an isogeny between abelian varieties using a further isogeny to a Jacobian", *J. Number Theory* **115**:1 (2005), 158–175. MR 2006g:11116 Zbl 1095.11033

[Siksek 1995a] S. Siksek, *Descents on curves of genus* 1, thesis, University of Exeter, 1995.

[Siksek 1995b] S. Siksek, "Infinite descent on elliptic curves", *Rocky Mountain J. Math.* **25**:4 (1995), 1501–1538. MR 97g:11053 Zbl 0852.11028

[Stoll 1998] M. Stoll, "On the arithmetic of the curves $y^2 = x^l + A$ and their Jacobians", *J. Reine Angew. Math.* **501** (1998), 171–189. MR 99h:11069 Zbl 0902.11024

[Stoll 2001] M. Stoll, "Implementing 2-descent for Jacobians of hyperelliptic curves", *Acta Arith.* **98**:3 (2001), 245–277. MR 2002b:11089 Zbl 0972.11058

[Stoll 2002] M. Stoll, "On the arithmetic of the curves $y^2 = x^l + A$, II", *J. Number Theory* **93**:2 (2002), 183–206. MR 2003d:11090 Zbl 1004.11038

[Stoll 2006a] M. Stoll, "Independence of rational points on twists of a given curve", *Compos. Math.* **142**:5 (2006), 1201–1214. MR 2007m:14025 Zbl 1128.11033

[Stoll 2006b] M. Stoll, "On the number of rational squares at fixed distance from a fifth power", *Acta Arith.* **125**:1 (2006), 79–88. MR 2007g:11039

[Tzermias 1998] P. Tzermias, "Algebraic points of low degree on the Fermat curve of degree seven", *Manuscripta Math.* **97**:4 (1998), 483–488. MR 99j:11075 Zbl 0952.11017

[Tzermias 2003] P. Tzermias, "Parametrization of low-degree points on a Fermat curve", *Acta Arith.* **108**:1 (2003), 25–35. MR 2004b:11091 Zbl 1056.11040

[Tzermias 2004] P. Tzermias, "Low-degree points on Hurwitz-Klein curves", *Trans. Amer. Math. Soc.* **356**:3 (2004), 939–951. MR 2004j:11061 Zbl 1116.14017

[Tzermias 2005] P. Tzermias, "Improved bounds on the number of low-degree points on certain curves", *Acta Arith.* **117**:3 (2005), 277–282. MR 2006m:11093 Zbl 1079.11032

[Wetherell 1997] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, thesis, University of California at Berkeley, 1997.

Communicated by Bjorn Poonen
Received 2008-04-02 Revised 2009-01-20 Accepted 2009-02-17

s.siksek@warwick.ac.uk *Institute of Mathematics, University of Warwick, Coventry CV4 7AL, United Kingdom*
http://www.warwick.ac.uk/~maseap/