COMPUTATIONAL TOOLS FOR QUADRATIC CHABAUTY

JENNIFER S. BALAKRISHNAN AND J. STEFFEN MÜLLER

Contents

Date: February 23, 2020.

1. Introduction

The *quadratic Chabauty* method is the first nonabelian step of Kim's program for achieving an algorithmic determination of the set $X(\mathbb{Q})$ of rational points on a nice[1] curve $X/\mathbb{Q}$ of genus g of 2 or more. The quadratic Chabauty set $X(\mathbb{Q}_p)_2 \supset X(\mathbb{Q})$ is a finite subset of $X(\mathbb{Q}_p)$ for those curves with good reduction at p and Jacobian J having Mordell–Weil rank r and Néron–Severi rank $\rho(J)$ satisfying the hypothesis

$$r < g + \rho(J) - 1.$$

In these notes[2], we develop tools for carrying out the quadratic Chabauty method in the case when $r = g$ and $\rho(J) \geq 2$, with a focus on algorithmic and computational[3] aspects. The goal of these notes are two-fold: first, to serve as a user's guide for those interested in getting started with the quadratic Chabauty method, and second, to highlight some interesting problems along the way.

Kim's nonabelian Chabauty program is a vast generalization of the Chabauty–Coleman method. The latter solely uses *abelian* geometric data: the structure of the Jacobian, as well as p-adic abelian integrals. It applies to curves satisfying the hypothesis $r < g$ and relies on the construction of an annihilating differential, which essentially can be computed using p-adic linear algebra.

Since the classical Chabauty–Coleman method motivates some of our framing of the quadratic Chabauty method, we begin our discussion by giving a survey of the tools used to carry out the former method, where there are still a number of tractable computational challenges. The main construction here is how p-adic (Coleman) integrals can be computed using p-adic cohomology. Then when the Chabauty–Coleman hypothesis is satisfied, one can use the calculation of Coleman integrals to compute a finite set of points $X(\mathbb{Q}_p)_1 \supset X(\mathbb{Q})$.

We also describe how n-fold iterated Coleman integrals can be computed, which in the case of $n = 2$, provides input into computations involving p-adic heights. We then survey a few constructions of p-adic heights in various settings, which leads into the quadratic Chabauty method. We briefly describe how this fits into Kim's nonabelian Chabauty program, though a more comprehensive treatment of the theory will be covered in Kim's lecture course. Finally, we combine the algorithms for quadratic Chabauty to carry out an example to determine rational points on the Atkin–Lehner quotient modular curve $X_0(167)^+$, which has genus 2 and rank 2.

Throughout, we illustrate our techniques with examples, and where possible, we include or link to code snippets for carrying out computations in `SageMath` [The20] or `Magma` [BCP97].

[1] Throughout, by a *nice* curve, we mean one that is smooth, projective, and geometrically irreducible.

[2] These are lecture notes for the course "Computational tools for quadratic Chabauty", taught by JB at the 2020 Arizona Winter School on Nonabelian Chabauty. They were originally planned as a combined set of lecture notes for this course and an additional course, "Quadratic Chabauty", taught by SM at the 2020 AWS. SM withdrew his participation after realizing that, in contrast to previous editions, the 2020 edition of the school would be supported by the NSA.

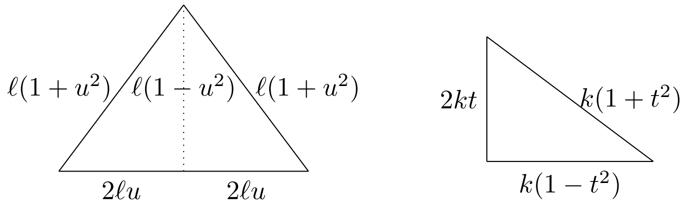
[3] While computations of p-adic objects are usually not exact, one can analyze the precision necessary to produce provably correct results.

1.1. A question about triangles.

We start with a question from Euclidean geometry that leads to an interesting Diophantine problem. We say that a *rational triangle* is one all of whose side lengths are rational.

Question. *Does there exist a rational right triangle and a rational isosceles triangle that have the same area and the same perimeter?*

This would mean that we have a pair of triangles with the following side lengths:



Let us rescale so that we may assume $\ell = 1$. We further suppose that $k, t, u \in \mathbb{Q}$, $0 < t, u < 1$ and $k > 0$. By equating areas and perimeters, we obtain the following system of equations:

$$k^2 t(1-t^2) = 2u(1-u^2)$$

$$k + kt = 1 + 2u + u^2$$

Let $x = 1 + u$. After some algebra, we see that there is $x \in \mathbb{Q} \cap (1, 2)$ such that

$$2xk^2 + (-3x^3 - 2x^2 + 6x - 4)k + x^5 = 0.$$

Then noting that the discriminant of the polynomial in k is a rational square, we have that

$$y^2 = (-3x^5 - 2x^2 + 6x - 4)^2 - 4(2x)x^5,$$

and simplifying, this gives us a genus 2 curve

$$X : y^2 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16.$$

We would like to compute the set of rational points $X(\mathbb{Q})$ on X. Some useful input now is knowing the Mordell–Weil rank of the Jacobian of X: it turns out that the rank is equal to 1. In general, computing the rank of a Jacobian is a difficult problem, but `Magma` has an implementation of 2-descent on Jacobians of hyperelliptic curves that can be used here:

```
> R<x>:=PolynomialRing(RationalField());
> X:=HyperellipticCurve(x^6+12*x^5-32*x^4+52*x^2-48*x+16);
> J:=Jacobian(X);
> RankBounds(J);
1 1
```

The output of `RankBounds` is a lower bound on rank, followed by an upper bound on rank, which are both equal to 1. Consequently, the *Chabauty–Coleman* bound (more on this in a bit; see Theorem 1.4 if you'd like to skip ahead) gives

$$\#X(\mathbb{Q}) \leq 10.$$

Are there rational points on X? After searching in a box, we find

$$\{\infty^{\pm}, (0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3)\} \subseteq X(\mathbb{Q}),$$

and we have found precisely 10 points. So we have determined $X(\mathbb{Q})$, and the rational point $(12/11, 868/11^3)$ gives us a unique pair of triangles.

Theorem 1.1 (Hirakawa–Matsumura [HM19])**.** *Up to similitude, there exists a unique pair of a rational right triangle and a rational isosceles triangle which have the same perimeter and the same area. The unique pair consists of the right triangle with side* $(377, 135, 352)$ *and isosceles triangle with sides* $(366, 366, 132)$.

We begin with some context for these results. It was conjectured by Mordell in 1922 that nice curves of genus 2 or more have only finitely many rational points. This was proved by Faltings:

Theorem 1.2 (Faltings [Fal83])**.** *Let* $X/\mathbb{Q}$ *be a nice curve of genus* ≥ 2*. Then the set* $X(\mathbb{Q})$ *is finite.*

How do we determine the set $X(\mathbb{Q})$? Faltings' proof is not constructive. There is another proof due to Vojta [Voj91] (also revisited by Bombieri [Bom90]), but it is also not effective. We note that the recent proof of Mordell's conjecture by Lawrence and Venkatesh [LV18] gives another approach to finiteness, see also [BBB$^+$19].

One method that allows us to compute the set $X(\mathbb{Q})$ in some cases is due to Coleman [Col85b], who re-interpreted earlier work of Chabauty, who proved Mordell's conjecture in the following special case:

Theorem 1.3 (Chabauty, 1941)**.** *Let* $X/\mathbb{Q}$ *be a nice curve of genus* $g \geq 2$*. Suppose the Mordell-Weil group of* J *has rank* $r < g$*. Then* $X(\mathbb{Q})$ *is finite.*

Coleman gave an effective version of Chabauty's theorem:

Theorem 1.4 (Coleman [Col85a])**.** *Let* $X/\mathbb{Q}$ *be a nice curve of genus at least* 2*. Suppose the Mordell-Weil rank of* $J(\mathbb{Q})$ *is less than* g*. If* $p > 2g$ *is a prime of good reduction for* X*,*

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2.$$

This result comes from bounding the number of zeros of a p-adic (Coleman) integral. We will say a bit more about this later.

Going back to the triangle problem: recall that we have the genus 2 curve

$$X : y^2 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16.$$

The curve X has good reduction at $p = 5$, and we compute the set of $\mathbb{F}_5$-rational points:

$$X(\mathbb{F}_5) = \{\infty^{\pm}, (0, \pm 1), (1, \pm 1), (2, \pm 2)\},$$

so $\#X(\mathbb{F}_5) = 8$. Thus by Coleman's theorem, we have

$$\#X(\mathbb{Q}) \leq 8 + 2 \cdot 2 - 2 = 10.$$

Since the Chabauty–Coleman method involves p-adic integration of certain differentials, we first set some notation on differentials and then discuss p-adic integration. We assume throughout that p is a prime of good reduction for a nice curve X.

Definition 1.5. Let X be a nice curve over a field k. The set of differentials on X over k is a 1-dimensional $k(X)$-vector space $\Omega^1(k)$.

Definition 1.6. Let $0 \neq \omega \in \Omega^1(k)$ and $P \in X(k)$. Let $t \in k(X)$ be a uniformizer at P, and use this to write $\omega = \omega(t)dt$. Then $v_P(\omega) := v_P(\omega(t))$ is the valuation of ω at P.

Definition 1.7. If $v_P(\omega) \geq 0$ (or $\omega = 0$), then ω is regular at P and ω is regular if it is regular at all points $P \in X(\bar{k})$. This is also known as a differential of the first kind. A differential of the second kind is a differential that has residue zero at all points $P \in X(\bar{k})$. A differential of the third kind has at most simple poles at all points.

Example 1.8. Let $X\colon y^2 = f(x)$ be a hyperelliptic curve of genus g over k. Then $H^0(X, \Omega^1)$ has basis

$$\left\{ \frac{dx}{2y}, \frac{xdx}{2y}, ..., \frac{x^{g-1}dx}{2y} \right\}$$

so every regular differential can be uniquely written as $\frac{p(x)dx}{2y}$ with a polynomial p of degree $\deg(p) \leq g-1$.

Now we begin with an introduction to Coleman's theory of p-adic line integration.

Theorem 1.9 (Coleman)**.** *Let $X/\mathbb{Q}_p$ be a nice curve with good reduction at p. Then the p-adic integral*

$$\int_P^Q \omega \in \overline{\mathbb{Q}}_p$$

defined for each pair of points $P, Q \in X(\overline{\mathbb{Q}}_p)$ and regular differential $\omega \in \mathrm{H}^0\left(X, \Omega^1\right)$ satisfies the following properties:

(1) The integral is $\overline{\mathbb{Q}}_p$-linear in ω.

(2) If P, Q reduce to the same point $\bar{P} \in X_{\mathbb{F}_p}\left(\overline{\mathbb{F}}_p\right)$, then we call the integral a tiny integral*. It can be evaluated by writing $\omega = \omega(t)dt$ with t a uniformizer at P reducing to a uniformizer at $\bar{P}$ and ω a power series, then integrating formally and obtaining a power series ℓ such that $d\ell(t) = \omega(t)dt$ and $\ell(0) = 0$ and finally evaluating $\ell(t(Q))$, which converges. This implies*

$$\int_P^P \omega = 0.$$

(3)

$$\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^{Q} \omega.$$

Therefore it makes sense to define $\int_D \omega$ for

$$D = \sum_{j=1}^{n} ((Q_j) - (P_j)) \in \mathrm{Div}_X^0(\overline{\mathbb{Q}}_p)$$

as

$$\int_D \omega = \sum_{j=1}^{n} \int_{Q_j}^{P_j} \omega.$$

(4) If D is principal, then $\int_D \omega = 0$.

(5) The integral is compatible with the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

(6) Fix $P_0 \in X(\overline{\mathbb{Q}}_p)$. If $0 \neq \omega \in H^0\left(X_{\mathbb{Q}_p}, \Omega^1\right)$, then the set of points $P \in X(\overline{\mathbb{Q}}_p)$ reducing to a fixed point on $X(\overline{\mathbb{F}}_p)$ such that $\int_{P_0}^{P} \omega = 0$, is finite.

Remark 1.10. The integral above is known as the *Coleman integral* [Col82, Col85b]. The statement that the curve has good reduction is not necessary but simplifies the statement of (2). The theory of Coleman integration of forms of the second and third kind was developed by Coleman [Col85b] and Coleman–de Shalit [CdS88], respectively.

Remark 1.11. There are a number of closely related approaches to p-adic integration, by Berkovich [Ber07], Zarhin [Zar96] Colmez [Col98], Besser [Bes02], and Vologodsky [Vol03]. See also the excellent survey of Besser [Bes12].

Corollary 1.12. *Given the hypothesis of the previous theorem, let $b \in X(\mathbb{Q}_p)$, let J be the Jacobian of X, and*

$$\begin{aligned} i : X &\to J \\ P &\mapsto [P - b] \end{aligned}$$

be the Abel-Jacobi embedding of X into J. Then there is a map

$$\begin{aligned} J(\mathbb{Q}_p) \times H^0\left(X_{\mathbb{Q}_p}, \Omega^1\right) &\to \mathbb{Q}_p \\ (Q, \omega) \qquad\qquad &\mapsto \langle Q, \omega \rangle \end{aligned}$$

that is additive in Q and $\mathbb{Q}_p$-linear in ω and is given by

$$\langle [D], \omega \rangle = \int_D \omega$$

for $D \in \mathrm{Div}^0_X(\overline{\mathbb{Q}}_p)$. In particular, for $P \in X(\mathbb{Q}_p)$, we have the Abel-Jacobi morphism $\mathrm{AJ_b}$ that takes P to the linear functional

$$\langle i(P), \omega \rangle = \int_b^P \omega =: \mathrm{AJ_b}(P).$$

Remark 1.13. If $P \in J(\mathbb{Q}_p)$ has finite order, then $\langle P, \omega \rangle = 0$ for all $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$. To see this, if $nP = 0$, then $\langle P, \omega \rangle = \frac{1}{n}\langle nP, \omega \rangle = 0$. In fact, one can show that the torsion points are the only points with this property. On the other hand , if ω has the property that $\langle P, \omega \rangle = 0$ for all $P \in J(\mathbb{Q}_p)$, then $\omega = 0$.

In the Chabauty–Coleman method, we will make use of a certain subspace of the space of regular 1-forms. Throughout, we will assume that $b \in X(\mathbb{Q})$ and use it to embed X into J:

Definition 1.14. Let $A = \left\{\omega \in H^0(X, \Omega^1) : \text{ for all } P \in J(\mathbb{Q}),\ \langle P, \omega \rangle = 0\right\}$ be the subspace of *annihilating differentials.*

The embedding i induces an isomorphism of vector spaces $H^0(J_{\mathbb{Q}_p}, \Omega^1) \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1)$ and we likewise have the pairing

$$\begin{aligned} J(\mathbb{Q}_p) \times H^0\left(J_{\mathbb{Q}_p}, \Omega^1\right) &\to \mathbb{Q}_p \\ (Q, \omega_J) \qquad\qquad &\mapsto \int_0^Q \omega_J, \end{aligned}$$

which induces a homomorphism

$$\log : J(\mathbb{Q}_p) \to H^0\left(J_{\mathbb{Q}_p}, \Omega^1\right)^*.$$

We thus have the following diagram:

$$\begin{tikzcd} X(\mathbb{Q}) \arrow[r] \arrow[d] & X(\mathbb{Q}_p) \arrow[d] \arrow[dr, "\mathrm{AJ_b}"] & \\ J(\mathbb{Q}) \arrow[r] & J(\mathbb{Q}_p) \arrow[r, "\log"] & H^0\left(J_{\mathbb{Q}_p}, \Omega^1\right)^* \simeq \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^* \end{tikzcd} \tag{1}$$

Remark 1.15. In general, since we are only considering the case of good reduction, we will identify the p-adic abelian integral on the Jacobian with the abelian integral given by p-adic integration on the curve. In the case of bad reduction (as will be discussed in Zureick-Brown's lecture course), there is a difference in the two integrals, as noted by Stoll [Sto19] and Katz–Rabinoff–Zureick-Brown [KRZB16]. See also the work of Besser–Zerbes [BZ17] for a discussion of Vologodsky integration in the semistable case.

From now on, we will assume basic familiarity with rigid geometry, see for instance [Sch98, FvdP04].

Definition 1.16. Let X^{an} denote the rigid analytic space over $\mathbb{Q}_p$ associated to $X/\mathbb{Q}_p$. There is a specialization map from X^{an} to the reduction of X modulo p. The fibers of this map are called *residue disks*.

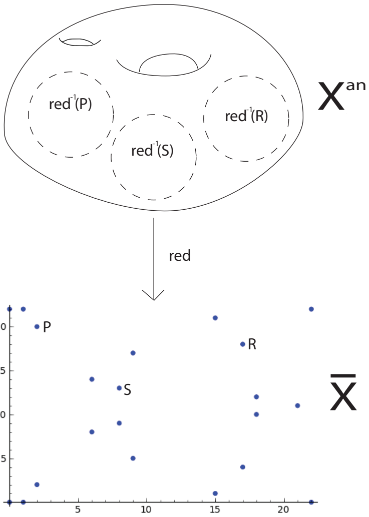


Figure 1. Residue disks in X^{an}

Corollary 1.17. *Let $X/\mathbb{Q}$ be a nice curve of genus g whose Jacobian has Mordell-Weil rank r less than g. Then $\#X(\mathbb{Q})$ is finite.*

Proof. If $X(\mathbb{Q}) = \varnothing$, then the claim is trivially true. Fix a prime p of good reduction for X and fix $b \in X(\mathbb{Q})$ to define $i : X \to J$. Let A be the subspace of annihilating differentials. By additivity of integration pairing in the first argument, this condition is equivalent to requiring $\langle P_j, \omega\rangle = 0$ for a basis $\{P_j\}_{j=1}^r$ of the free part of $J(\mathbb{Q})$. So it leads to at most r linear constraints and $\dim(A) \geq g - r > 0$. Thus there is some $0 \neq \omega \in A$. Since $i(P) \in J(\mathbb{Q})$ for all $P \in X(\mathbb{Q})$ it follows that $\int_b^P \omega = 0$ for all $P \in X(\mathbb{Q})$. By Theorem 1.9 (6), the number of such P is finite in each residue disk of $X(\mathbb{Q}_p)$. Since the number of residue disks (i.e., $\#X(\mathbb{F}_p)$) is finite, the total number of points in $X(\mathbb{Q})$ is finite as well. □

Remark 1.18. By *computing rational points via the Chabauty–Coleman method*, we mean that we compute the finite set of p-adic points

$$X(\mathbb{Q}_p)_1 := \{z \in X(\mathbb{Q}_p) : \int_b^z \omega = 0 \text{ for } \omega \in A\}.$$

By construction, this set contains $X(\mathbb{Q})$. One potential difficulty is that $X(\mathbb{Q}_p)_1$ might be strictly larger than the set of known rational points, so more work must be done to provably extract $X(\mathbb{Q})$; see Section 5.3.3 for one approach to address this, known as the *Mordell–Weil sieve*.

We can use results about the number of zeros of p-adic power series (studied via Newton polygons) to refine the bound in the proof above. Combining this with Riemann–Roch gives Coleman's result, that for X satisfying the hypotheses of Corollary 1.17 and $p > 2g$ a good prime, we have (Theorem 1.4):

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2.$$

Remark 1.19. Here are some related results:

(1) Stoll [Sto06] showed that one can choose the "best" ω for each residue disk, which improves the bound if $r < g$ and $p > 2r + 2$ is a good prime:
$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r.$$
Stoll also showed that one can weaken the assumption that $p > 2r + 2$; if $p > 2$, then
$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r + \left\lfloor \frac{2r}{p-2} \right\rfloor.$$

(2) Katz–Zureick-Brown [KZB13] extended Stoll's result to the case of bad reduction. If $p > 2g$ and $\mathcal{X}$ is the minimal proper regular model for X over $\mathbb{Z}_p$, then
$$\#X(\mathbb{Q}) \leq \#\mathcal{X}_{sm}(\mathbb{F}_p) + 2r$$
where $\mathcal{X}_{sm}(\mathbb{F}_p)$ is the set of smooth $\mathbb{F}_p$-rational points in the special fiber of $\mathcal{X}$.

As will be discussed in Zureick-Brown's lecture course, the Chabauty–Coleman method can be used to prove uniform bounds on the number of rational points on a nice curve. The first result along these lines was given by Stoll, for hyperelliptic curves:

Theorem 1.20 (Stoll [Sto19])**.** *Let $X/\mathbb{Q}$ be a hyperelliptic curve of genus g with Jacobian of Mordell-Weil rank r. If $r \leq g - 3$, then*
$$\#X(\mathbb{Q}) \leq 8rg + 33(g-1) - 1 \quad \textit{if } r \geq 1 \quad \textit{and} \quad \#X(\mathbb{Q}) \leq 33(g-1) + 1 \quad \textit{if } r = 0\,.$$

This was generalized by Katz–Rabinoff–Zureick-Brown to nice curves:

Theorem 1.21 (Katz–Rabinoff–Zureick-Brown [KRZB16])**.** *If $X/\mathbb{Q}$ is a nice curve of genus g with $r \leq g - 3$, then*
$$\#X(\mathbb{Q}) \leq 84g^2 - 98g + 28.$$

1.2. **The Chabauty–Coleman method and explicit Coleman integration.** Here we discuss how to construct an annihilating differential in the Chabauty–Coleman method, using explicit Coleman integration.

Example 1.22. Consider
$$X : y^2 = x^5 - 2x^3 + x + \frac{1}{4},$$
which has LMFDB label 971.a.971.1 [LMF20b]. Here are some facts about this curve:

- Searching for rational points in a box, we find that the set of rational points $X(\mathbb{Q})$ contains $\{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\}$.
- The Jacobian is simple, and its Mordell–Weil group has the structure $J(\mathbb{Q}) \simeq \mathbb{Z}$. The point
$$[(-1, -1/2) - (0, 1/2)] \in J(\mathbb{Q})$$
has infinite order, as can be seen by computing Coleman integrals on regular 1-forms (see below).
- The conductor N is 971, which is prime. So X has good reduction at $p = 3$, and we compute that $\#X(\mathbb{F}_3) = 7$. Using Stoll's refinement of the Chabauty–Coleman bound gives
$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_3) + 2 \cdot 1 + \left\lfloor \frac{2 \cdot 1}{3-2} \right\rfloor = 11,$$
so this bound by itself will not prove[4] that we have all of the $\mathbb{Q}$-points.

[4] Note that we know that we have all of the $\mathbb{Q}$-points, but we suspect we do, and we would like to prove this.

Our strategy will be to use $p = 3$ to construct an annihilating differential. A basis of $\mathrm{H}^0(X_{\mathbb{Q}_3}, \Omega^1)$ is

$$\left\{\omega_i = \frac{x^i dx}{2y}\right\}_{i=0,1}.$$

So the annihilating differential η is a $\mathbb{Q}_3$-linear combination of ω_0 and ω_1. We will use the values of

$$\int_{(0,1/2)}^{(-1,-1/2)} \omega_i$$

to compute η.

We can do this in SageMath as follows:

```
R.<x> = QQ[]
X = HyperellipticCurve(x^5-2*x^3+x+1/4)
p = 3
K = Qp(p,15)
XK = X.change_ring(K)
XK.coleman_integrals_on_basis(XK(0,1/2),XK(-1,-1/2)) #basis is {x^i*dx/(2y)}, i = 0,...,3
(3 + 3^2 + 3^4 + 3^5 + 2*3^6 + 2*3^7 + 2*3^8 + 3^10 + O(3^11),
2 + 2*3 + 2*3^3 + 3^4 + 3^6 + 2*3^8 + 2*3^9 + O(3^10),
2*3^-1 + 2*3 + 2*3^2 + 3^3 + 3^5 + 3^6 + 3^7 + O(3^9),
2*3^-2 + 3^-1 + 2 + 2*3 + 3^2 + 2*3^3 + 3^4 + 2*3^5 + 2*3^6 + 2*3^7 + O(3^8))
```

We find that

$$\alpha := \int_{(0,1/2)}^{(-1,-1/2)} \omega_0 = 3 + 3^2 + 3^4 + 3^5 + 2\cdot 3^6 + 2\cdot 3^7 + 2\cdot 3^8 + 3^{10} + O(3^{11}),$$

$$\beta := \int_{(0,1/2)}^{(-1,-1/2)} \omega_1 = 2 + 2\cdot 3 + 2\cdot 3^3 + 3^4 + 3^6 + 2\cdot 3^8 + 2\cdot 3^9 + O(3^{10}).$$

With a slightly different choice of basis[5], we can also do these computations in Magma (using the package [BTb], available on GitHub) as follows:

```
> load "coleman.m";
> data:=coleman_data(y^2-(x^5-2*x^3+x+1/4),3,10);
> P1:= set_point(0,1/2, data);
> P2:= set_point(-1,-1/2,data);
> coleman_integrals_on_basis(P1,P2,data); //8 times the integrals above
(-7609*3 + O(3^10) 13537 + O(3^10) 77056*3^-1 + O(3^10) -6512*3^-2 + O(3^10))
```

So $\int_{(0,1/2)}^{(-1,-1/2)} \beta\omega_0 - \alpha\omega_1 = 0$, and we take

$$\eta = \beta\omega_0 - \alpha\omega_1$$

as our annihilating differential.

In order to use η to compute $X(\mathbb{Q})$, or more precisely the finite set $X(\mathbb{Q}_3)_1$, that by construction, contains $X(\mathbb{Q})$, we next compute the collection of "indefinite" Coleman integrals

$$\left\{\int_{(0,1/2)}^{P_t} \eta\right\}$$

[5] In this example, the Magma basis is the SageMath basis rescaled by a factor of 8.

where P_t ranges over all residue disks, and solve for all $z \in X(\mathbb{Q}_3)$ such that $\int_{(0,1/2)}^{z} \eta = 0$. Note that to compute these indefinite Coleman integrals, we can take P_0 a lift of an $\mathbb{F}_3$-point in the same residue disk as P_t. Then

$$\int_{(0,1/2)}^{P_t} \eta = \int_{(0,1/2)}^{P_0} \eta + \int_{P_0}^{P_t} \eta$$

where the first is some 3-adic constant, and the latter is a tiny integral computed using a power series. So to compute α, β and $\int_{(0,1/2)}^{P_0} \eta$, we need to compute Coleman integrals between points not in the same residue disk.

Now we explain how to compute these integrals on the curve, using the action of Frobenius on p-adic cohomology.

Remark 1.23. Before we go on, we should note that there is a standard alternative approach to the one presented below for computing Coleman integrals of regular 1-forms between points not in the same residue disk that goes as follows.

Suppose we want to compute the Coleman integral $\int_P^Q \omega$, where $P, Q \in X(\mathbb{Q}_p)$. Letting J denote the Jacobian of X, we first compute an integer k such that the point $k(P-Q)$ is trivial in $J(\mathbb{F}_p)$: for instance, we could take k to be the order of $J(\mathbb{F}_p)$. Then computing $D := [k(P-Q)]$ as an element in the residue disk at 0 of $J(\mathbb{Q}_p)$, we can rewrite the integral as a sum of tiny integrals over D, and then use $\int_{[P-Q]} \omega = \frac{1}{k} \int_D \omega$.

This has worked well in a number of examples in the literature, though there are a few potential limitations. First, implementations of Jacobian arithmetic over $\mathbb{Q}_p$ are currently restricted to very special curves, such as those that are hyperelliptic. Secondly, while the Chabauty–Coleman method only uses integrals of regular 1-forms, there are other applications for which integrals of forms of the second or third kind are useful. Moreover, since this approach uses properties of the Jacobian, it does not have an obvious generalization to iterated integrals. So from the perspective of the nonabelian Chabauty method, where iterated integration is needed, we present the following approach.

We will integrate over a wide open subspace of X^{an}:

Definition 1.24. A wide open subspace of X^{an} is the complement in X^{an} of the union of a finite collection of disjoint closed disks of radius $\lambda_i < 1$.

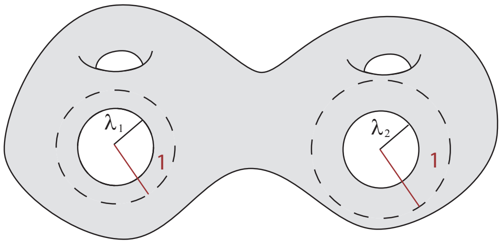


FIGURE 2. A wide open subspace of X^{an}

Here are some further properties of Coleman integrals that we will need:

Theorem 1.25 (Coleman [Col85b]). *Let η and ξ be 1-forms on a wide open subspace V of X^{an}, and $P, Q, R \in V(\overline{\mathbb{Q}}_p)$. Let $a, b \in \overline{\mathbb{Q}}_p$. The definite Coleman integral has the following properties:*

(1) *Linearity:*
$$\int_P^Q (a\eta + b\xi) = a\int_P^Q \eta + b\int_P^Q \xi.$$
(2) *Additivity in endpoints:*
$$\int_P^Q \eta = \int_P^R \eta + \int_R^Q \eta.$$
(3) *Change of variables: if $V' \subset X'$ is a wide open subspace of the rigid analytic space X', ω' a 1-form on V' and $\phi : V \to V'$ a rigid analytic map, then*
$$\int_P^Q \phi^*\omega' = \int_{\phi(P)}^{\phi(Q)} \omega'.$$
(4) *Fundamental Theorem of Calculus:*
$$\int_P^Q df = f(Q) - f(P)$$
for f a rigid analytic function on V.
(5) *Galois compatibility: If $P, Q \in V(\mathbb{Q}_p)$ and ω is defined over $\mathbb{Q}_p$, then $\int_P^Q \omega \in \mathbb{Q}_p$.*

We would first like to integrate $\int_P^Q \omega$ for ω a 1-form of the second kind, where $P, Q \in V(\mathbb{Q}_p)$. We first discuss how to do this in the case when X is a *hyperelliptic* curve and then present a more general construction in Section 1.4. (In our discussion of p-adic heights in Section 2.2, we will also describe how to compute integrals of forms of the third kind.)

The idea is to do the following:

(1) Take ϕ to be a lift of p-power Frobenius from the special fiber.
(2) Compute a basis $\{\omega_i\}$ of 1-forms of the second kind.
(3) Compute $\phi^*\omega_i$ via Kedlaya's zeta function algorithm [Ked01, Ked03] and use properties of Coleman integrals to relate $\int_P^Q \phi^*\omega_i$ to $\int_P^Q \omega_i$ and other terms we can compute.
(4) Use linear algebra to solve for $\int_P^Q \omega_i$.

To do this, we introduce some p-adic cohomology as in Kedlaya's algorithm. For further details, two standard references for rigid analytic geometry are the books by Fresnel and van der Put [FvdP04] and Bosch, Güntzer, and Remmert [BGR84]. See also [Edi] for a nice exposition by Edixhoven of Kedlaya's algorithm.

1.3. **Some p-adic cohomology.**

In [Ked01], Kedlaya gave an algorithm to compute the zeta function of a hyperelliptic curve over a finite field, using Monsky–Washnitzer cohomology. Here is a brief outline of Kedlaya's algorithm:

(1) Work in an affine piece of the hyperelliptic curve, given by deleting Weierstrass points.
(2) Take ϕ to be a lift of p-power Frobenius from the special fiber, sending $x \to x^p$ and Hensel lifting to find the image of y.
(3) Compute the action of Frobenius on a basis of de Rham cohomology (of a lift of the curve) and reduce the pole order of each resulting differential using relations in cohomology.

It turns out that Kedlaya's algorithm produces a few other outputs that can be assembled into an algorithm for Coleman integration on hyperelliptic curves, as given by Balakrishnan–Bradshaw–Kedlaya [BBK10]. In this section, we give an overview of Kedlaya's algorithm and the corresponding Coleman integration algorithm.

For simplicity, we will assume that we start with a genus g hyperelliptic curve $\tilde{X}$ defined over $\mathbb{Q}$, given by $y^2 = \tilde{P}(x)$, where $\tilde{P}(x)$ is a monic polynomial of degree $2g+1$. Let $p \neq 2$ be a prime at which $\tilde{X}$ has good reduction, and consider $\overline{X}/\mathbb{F}_p$, with affine equation $y^2 = P(x)$. Take $X = \overline{X}\backslash\{\infty, y = 0\}$.

Let $A = \mathbb{Z}_p[x, y, y^{-1}]/(y^2 - \tilde{P}(x))$. First, we form the weak completion $A^\dagger$ of A, which can be described as follows. Let v_p denote the p-adic valuation on $\mathbb{Z}_p$, and extend it to polynomials by $v_p(\sum a_i x^i) = \min_i\{v_p(a_i)\}$. The elements of $A^\dagger$ can then be described as the series

$$\sum_{n=-\infty}^{\infty} (S_n(x) + T_n(x)y)y^{2n}$$

where the S_n and T_n are polynomials of degree at most $2g$ such that

$$\liminf_{n\to\infty} \frac{v_p(S_n)}{n}, \qquad \liminf_{n\to\infty} \frac{v_p(S_{-n})}{n}, \qquad \liminf_{n\to\infty} \frac{v_p(T_n)}{n}, \qquad \liminf_{n\to\infty} \frac{v_p(T_{-n})}{n}$$

are all positive.

Monsky–Washnitzer cohomology is a p-adic cohomology theory which takes smooth affine varieties over fields of characteristic $p > 0$ as input, and outputs finite-dimensional $\mathbb{Q}_p$-vector spaces. There is a comparison theorem due to the work of Berthelot [Ber97, Prop. 1.10] (comparing Monsky–Washnitzer and rigid cohomology) and Baldassarri–Chiarellotto [BC94] (comparing rigid cohomology with de Rham cohomology), which relates Monsky–Washnitzer cohomology groups with algebraic de Rham cohomology groups:

Theorem 1.26 (Special case of Baldassarri–Chiarellotto and Berthelot)**.** *Let Y be a smooth affine variety over $\mathbb{F}_p$ and $\widetilde{Y}$ a smooth affine variety over $\mathbb{Q}_p$ that is a lift of Y. Then the Monsky–Washnitzer cohomology of Y coincides with the algebraic de Rham cohomology of $\widetilde{Y}$:*

$$\mathrm{H}^1_{\mathrm{dR}}(\widetilde{Y}) = \mathrm{H}^1_{\mathrm{MW}}(Y).$$

The Monsky–Washnitzer cohomology groups are equipped with an action of Frobenius, hence Theorem 1.26 tells us that we can compute the action of Frobenius on de Rham cohomology.

Proposition 1.27. *The first de Rham cohomology of A splits into two eigenspaces under the hyperelliptic involution*

$$X \to X,\ (x, y) \mapsto (x, -y).$$

The first eigenspace $\mathrm{H}^1(A)^+$ is the positive eigenspace generated by

$$\left\{\frac{x^i dx}{y^2} : i = 0, \cdots, 2g\right\},$$

and the second eigenspace $\mathrm{H}^1(A)^-$ is the negative eigenspace generated by

$$\left\{\frac{x^i dx}{y} : i = 0, \cdots, 2g-1\right\},$$

Moreover, passing to $A^\dagger$ does not change the cohomology, and we compute the action of Frobenius on $\mathrm{H}^1(A^\dagger)^-$. We lift p-power Frobenius to an endomorphism σ of $A^\dagger$ in the following manner: On polynomials in $\mathbb{Z}_p[x]$, we send

$$\sigma : x \mapsto x^p. \tag{2}$$

Since $y^2 = \widetilde{P}(x)$ inside A and $A^\dagger$, we see that the action of σ on y must satisfy the following:

$$(y^\sigma)^2 = (y^2)^\sigma = (\widetilde{P}(x))^\sigma = \widetilde{P}(x)^\sigma \left(\frac{y^2}{\widetilde{P}(x)}\right)^p = \frac{y^{2p}\widetilde{P}(x)^\sigma}{\widetilde{P}(x)^p}.$$

We have

$$\sigma : y \mapsto y^p \left(\frac{\widetilde{P}(x)^\sigma}{\widetilde{P}(x)^p} \right)^{\frac{1}{2}} = y^p \left(1 + \frac{\widetilde{P}(x)^\sigma - \widetilde{P}(x)^p}{\widetilde{P}(x)^p} \right)^{\frac{1}{2}},$$

and by using a Taylor expansion for $(1+\cdot)^{-\frac{1}{2}}$, we get an identity

$$\frac{1}{y^\sigma} = \frac{1}{y^p} \sum_{j=0}^{\infty} \binom{-\frac{1}{2}}{j} \left(\frac{\widetilde{P}(x)^\sigma - \widetilde{P}(x)^p}{\widetilde{P}(x)^p} \right)^j = \frac{1}{y^p} \sum_{j=0}^{\infty} \binom{-\frac{1}{2}}{j} \left(\frac{\widetilde{P}(x)^\sigma - \widetilde{P}(x)^p}{y^{2p}} \right)^j. \tag{3}$$

The reason we write the expansion for $\frac{1}{y^\sigma}$ in this way is to see the p-adic convergence, since $\widetilde{P}(x)^\sigma - \widetilde{P}(x)^p$ is divisible by p, so as $j \to \infty$, the summands go to 0.

This expansion will be used below, and perhaps now it is more clear why we removed Weierstrass points from our curve: given our choice of Frobenius lift, we cannot divide by y.

Finally, we extend the p-power Frobenius action to differentials by sending

$$\sigma^* : dx \mapsto d(x^p) = px^{p-1}dx. \tag{4}$$

In order to prove Proposition 1.27, we will need two key reduction lemmas to compute $(\frac{x^i dx}{y})^\sigma$.

Lemma 1.28 (Kedlaya [Ked01, p. 5])**.** *If $R(x) = \widetilde{P}(x)B(X) + \widetilde{P}'(x)C(X)$, then*

$$\frac{R(x)dx}{y^s} = \left(B(x) + \frac{2C'(x)}{s-2} \right) \frac{dx}{y^{s-2}} \tag{5}$$

as elements in $\mathrm{H}^1_{\mathrm{MW}}(X)$.

Also, using $y^2 = \widetilde{P}(x)$, we have $d(y^2) = d\widetilde{P}(x)$, so $2ydy = \widetilde{P}'(x)dx$. This gives us

$$dy = \frac{\widetilde{P}'(x)dx}{2y}. \tag{6}$$

This allows us to compute:

$$\begin{aligned} d(x^i y^j) =& i x^{i-1} y^j dx + x^i j y^{j-1} dy \\ \overset{(6)}{=}& i x^{i-1} y^j dx + j x^i y^{j-1} \frac{\widetilde{P}'(x)dx}{2y} = (2ix^{i-1}y^{j+1} + jx^i \widetilde{P}'(x) y^{j-1}) \frac{dx}{2y} \end{aligned}$$

(So the *highest* monomial of $d(x^i y^j)$ is $x^{i-1}y^{j+1}$ if $1 \le i < 2g+1$ and $x^{2g}y^{j-1}$ if $i = 0$. The *lowest* monomial of $d(x^i y^j)$ is of the form $x^k y^{j-1}$ with $0 \le k < 2g+1$.) As a special case of this computation, we have

$$\begin{aligned} d(2Q(x)y) &= 2Q(x)dy + 2Q'(x)ydx \\ &\overset{(6)}{=} 2Q(x) \frac{\widetilde{P}'(x)dx}{2y} + 2Q'(x)ydx \\ &\overset{y^2 = \widetilde{P}(x)}{=} (Q(x)\widetilde{P}'(x) + 2Q'(x)\widetilde{P}(x)) \frac{dx}{y}, \end{aligned}$$

proving the second reduction lemma:

Lemma 1.29 (Kedlaya [Ked01, p. 5])**.** *If $Q(x) = x^{m-2g}$, then*

$$d(2Q(x)y) = (Q(x)\widetilde{P}'(x) + 2Q'(x)\widetilde{P}(x)) \frac{dx}{y} = 0 \tag{7}$$

as elements in $\mathrm{H}^1_{\mathrm{MW}}(X)$.

To compute $(\frac{x^i dx}{y})^\sigma$, we expand using (2), (3), (4) and reduce using the relations (5) and (7). The reduction process is subtracting appropriate linear combinations of $d(x^i y^j)$ and using the relationship $y^2 = \widetilde{P}(x)$.

The relation

$$\left(\frac{x^i dx}{y}\right)^\sigma = \frac{1}{y^\sigma} x^{pi} p x^{p-1} dx$$

plus (3) gives an infinite sum

$$\left(\frac{x^i dx}{y}\right)^\sigma = \frac{p x^{pi+p-1}}{y^p} \sum_{j=0}^{\infty} \binom{-\frac{1}{2}}{j} \left(\frac{\widetilde{P}(x)^\sigma - \widetilde{P}(x)^p}{y^{2p}}\right)^j dx. \tag{8}$$

To implement the expansion and reduction on a computer, we have to take a truncation of this infinite sum, and thus we need to know how many terms we need to take to get a provably correct result (more on this in a minute). Suppose we have computed this precision and the result in (8) is

$$\sum_{j=-L_1}^{L_2} \frac{R_j(x) dx}{y^{2j+1}}. \tag{9}$$

Here is how we use the reduction relations: we eliminate the $j = L_2$ term, then $j = L_2 - 1$ term. Iterate this procedure until no terms with $j > 0$ remain. Repeat the same thing for $j = -L_1, -(L_1 - 1), \ldots$ terms. At the end of this reduction algorithm, we will be left with

$$\left(\frac{x^i dx}{y}\right)^\sigma = dh_i + \sum_{j=0}^{2g-1} M_{ji} \frac{x^j dx}{y},$$

and as $dh_i \sim 0$ in cohomology, this gives us the matrix of Frobenius M.

Precision is lost when we divide by p in the reduction algorithm. We need to measure the loss of precision at each step to know how many provably correct digits we have. Let $R(x) \in \mathbb{Z}_p[x]$ be a polynomial of degree at most $2g$ and $m \geq 0$.

By (5), the reduction of

$$\omega := R(x) \frac{dx}{y^{2m+1}}$$

is $\omega = B(x) \frac{dx}{y} + df$ for some $B(x) \in \mathbb{Q}_p[x]$ with degree at most $2g - 1$ and $f = \sum_{j=-1}^{m-1} \frac{F_k(x)}{y^{2k+1}}$ with each F_k having degree at most $2g$. The first precision result is:

Lemma 1.30 ([Ked01, Lemma 2], [Edi, §4.3.4])**.** *In the above setting*[6]*, we have*

$$p^{\lfloor \mathrm{Log}_p(2m-1) \rfloor} B(x) \in \mathbb{Z}_p[x].$$

By (7), the reduction of

$$\omega := \frac{R(x) y^{2m} dx}{y}$$

is $\omega = B(x) \frac{dx}{y} + df$ for some $B(x) \in \mathbb{Q}_p[x]$ with degree at most $2g - 1$, and

$$f = C y^{2m+1} + \sum_{k=0}^{m-1} F_k(x) y^{2k+1}$$

[6] In this chapter, Log_p will denote the base p logarithm, to disambiguate from $\log_p$ in subsequent chapters, which will denote the p-adic logarithm.

with $C \in \mathbb{Q}_p$ and each F_k having degree at most $2g$.

Lemma 1.31 ([Ked03])**.** *In the above setting, we have*

$$p^{\lfloor \mathrm{Log}_p((2g+1)(2m+1)) \rfloor} B(x) \in \mathbb{Z}_p[x].$$

Putting Lemmas 1.30 and 1.31 together, one gets the following:

Proposition 1.32 ([Cha16, p. 34])**.** *To get N correct digits in the matrix of Frobenius M, we start with precision*

$$N_1 = N + \max\{\lfloor \mathrm{Log}_p(2N_2 - 3) \rfloor, \lfloor \mathrm{Log}_p(2g+1) \rfloor\} + 1 + \lfloor \mathrm{Log}_p(2g-1) \rfloor,$$

in which N_2 is the smallest integer such that

$$N_2 - \max\{\lfloor \mathrm{Log}_p(2N_2 + 1), \lfloor \mathrm{Log}_p(2g+1) \rfloor\} \geq N.$$

In particular, in (8), we take the truncation

$$\left(\frac{x^i dx}{y}\right)^{\sigma} = \frac{p x^{pi+p-1}}{y^p} \sum_{j=0}^{N_2-1} \binom{-\frac{1}{2}}{j} \left(\frac{\widetilde{P}(x)^{\sigma} - \widetilde{P}(x)^p}{y^{2p}}\right)^j dx.$$

Algorithm 1.33 (Kedlaya's algorithm)**.**

Input:

- The basis of differentials $\{\omega_i = x^i dx/y\}_{i=0}^{2g-1}$ of $H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})$ for a genus g hyperelliptic curve X given by a monic odd degree model, with good reduction at p.
- The desired precision N.

Output: The $2g \times 2g$ matrix M of a p-power lift of Frobenius ϕ, as well as functions $h_i \in A^{\dagger}$ such that $\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M^t_{ij}\omega_j$ to precision $O(p^N)$

(1) Compute the working precision N_1 as in Proposition 1.32, so that all computations will be done mod p^{N_1}.
(2) For each i, compute $F_i := \phi^*(\omega_i)$ and group the resulting terms as $(\sum p^{k+1} c_{i,k,j} y^j) dx/y$, where the $c_{i,k,j} \in \mathbb{Z}_p[x]$ have degree less than or equal to $2g+1$.
(3) Compute a list of differentials $d(x^i y^j)$, where $0 \leq i < 2g+1$ and $j \equiv 1 \pmod 2$.
(4) If F_i has a term $(x^i y^j)dx/y$ with $j < 0$, consider the term $(c_{i,k,j} y^j)dx/y$ where j is minimal. Take the unique linear combination of the $d(x^k y^{1+j})$ such that when this linear combination is subtracted off of F_i and re-initialize this as F_i. Do this until F_i no longer has terms of the form $(x^m y^j)dx/y$ with $j < 0$.
(5) If F_i has terms with $j \geq 0$, let $(x^m y^j)dx/y$ be the term with the highest monomial of F_i. Let $(x^k y^l)dx/y$ be the term such that $d(x^k y^l)$ has highest term $(x^m y^j)dx/y$ and subtract off the appropriate multiple of $d(x^k y^l)$ such that the resulting sum no longer has terms of the form $(x^m y^j)dx/y$ with $j \geq 0$. Re-initialize this as F_i and repeat this process until the resulting F_i is of the form $\left(M_{0i} + M_{1i}x \; + \cdots + M_{2g-1i}x^{2g-1}\right) dx/y$.
(6) For each i, return the expression

$$\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M^t_{ij}\omega_j.$$

Remark 1.34. Analyzing p-adic precision is a delicate task. We illustrate this in one example found by Chan [Cha16] below, where the previously published bounds contained a small inaccuracy. For the remainder of these notes, we do not say much more about p-adic precision analysis of the relevant constructions and instead give relevant pointers to the literature. We encourage the reader to keep the issue of p-adic precision in mind as they work through the algorithms.

Example 1.35 ([Cha16, Remark 13]). Consider the elliptic curve over $\mathbb{Q}$ defined by

$$y^2 = \widetilde{P}(x) = x^3 + x + 1.$$

This curve has good reduction at the prime $p = 5$. We wish to obtain $N = 2$ correct digits of expansion. Proposition 1.32 tells us that taking $N_2 = N_1 = 3$ suffices. Consider the two differentials $\frac{dx}{y}, \frac{xdx}{y}$. We expand (8) and use the equation $y^2 = \widetilde{P}(x)$ as needed to reduce the degree in x in the numerators to produce the following:

$$\begin{aligned}\left(\frac{dx}{y}\right)^{\sigma} &= \left(\frac{25x+50}{y^{15}} + \frac{75x^2+100x+25}{y^{13}} + \frac{50x^2+50x+100}{y^{11}} + \frac{75x+50}{y^9} + \frac{50x^2+50x}{y^7}\right.\\ &\quad \left. + \frac{70x^2+70x+25}{y^5} + \frac{5x}{y^3}\right) dx \pmod{5^3},\\ \left(\frac{xdx}{y}\right)^{\sigma} &= \left(\frac{100x^2+100x+75}{y^{15}} + \frac{25x^2+50x+75}{y^{13}} + \frac{50x^2+100x+100}{y^{11}} + \frac{25x^2+75x+75}{y^9}\right.\\ &\quad \left. + \frac{75x^2+100}{y^7} + \frac{85x^2+90+50}{y^5} + \frac{15x^2+30x+85}{y^3} + \frac{5x^3+65x+65}{y}\right) dx \pmod{5^3}.\end{aligned}$$

Let F_k denote the polynomial in x in the numerator in each of the summands: i.e., writing them as $\frac{F_k(x)dx}{y^{2k+1}}$ modulo 5^3. Compute the sequence S_k for $k = 7, 6, \cdots, 0$ inductively by first setting $S_7 = F_7$, and afterwards, given S_{k+1}, find polynomials B_{k+1}, C_{k+1} such that $S_{k+1} = B_{k+1}\widetilde{P} + C_{k+1}\widetilde{P}'$, and then set $S_k(x) = F_k(x) + B_{k+1}(x) + \frac{2C'_{k+1}(x)}{2k+1}$. Carrying this out, one finds

$$\begin{aligned}\left(\frac{dx}{y}\right)^{\sigma} &= 15x\frac{dx}{y} \pmod{5^2}\\ \left(\frac{xdx}{y}\right)^{\sigma} &= (22x+18)\frac{dx}{y} \pmod{5^2}\end{aligned}$$

This gives us the matrix of the 5-power Frobenius

$$\begin{pmatrix} 0 & 18 \\ 15 & 22 \end{pmatrix} \pmod{5^2},$$

with $N = 2$ correct digits of expansion. Note that taking $N_1 = 3$ is necessary as well, as taking $N_1 = 2$ instead gives the matrix

$$\begin{pmatrix} 15 & 18 \\ 0 & 22 \end{pmatrix} \pmod{5^2}.$$

Now here is the application to Coleman integration, as carried out by Balakrishnan–Bradshaw–Kedlaya [BBK10]. Below we let ϕ denote the lift of p-power Frobenius described earlier.

Algorithm 1.36 (Coleman integration on a hyperelliptic curve [BBK10])**.**
Input:

- A prime $p > 2$ of good reduction for a hyperelliptic curve X
- Points $P, Q \in X(\mathbb{Q}_p)$ not contained in a Weierstrass residue disk
- A 1-form ω of the second kind

Output: The Coleman integral $\int_P^Q \omega$.

(1) Since ω is of the second kind, we may write it as a linear combination of a basis $\{\omega_i\}_{i=0}^{2g-1}$ for $\mathrm{H}^1_{\mathrm{dR}}(X)$ together with an exact form. Use Kedlaya's algorithm to write $\omega = dh + \sum_{i=0}^{2g-1} a_i\omega_i$, which allows us to specialize to the case of Coleman integrals of basis differentials.

(2) Use Kedlaya's algorithm to write, for each basis differential ω_i, the reduced form

$$\phi^*\omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j.$$

(3) Using properties of the Coleman integral, we have

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_j \\ \vdots \end{pmatrix} = (M^t - I)^{-1} \begin{pmatrix} \vdots \\ h_i(P) - h_i(Q) - \int_P^{\phi(P)} \omega_i - \int_{\phi(Q)}^Q \omega_i \\ \vdots \end{pmatrix}. \tag{10}$$

(4) Compute $\int_P^Q \omega = h(Q) - h(P) + \sum_{i=0}^{2g-1} a_i \int_P^Q \omega_i$.

Remark 1.37. We derive (3) above using the following:

$$\begin{aligned}
\int_{\phi(P)}^{\phi(Q)} \omega_i &= \int_P^Q \phi^*\omega_i \\
\text{(by Kedlaya)} &= \int_P^Q dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j \\
&= \int_P^Q dh_i + \sum_{j=0}^{2g-1} M_{ji} \int_P^Q \omega_j \\
&= h_i(Q) - h_i(P) + \sum_{j=0}^{2g-1} M_{ji} \int_P^Q \omega_j.
\end{aligned}$$

By the additivity of the Coleman integral on endpoints, we get

$$\int_P^{\phi(P)} \omega_i + \int_{\phi(P)}^{\phi(Q)} \omega_i + \int_{\phi(Q)}^{Q} \omega_i = \int_P^{\phi(P)} \omega_i + \int_{\phi(Q)}^{Q} \omega_i + h_i(Q) - h_i(P) + \sum_{j=0}^{2g-1} M_{ji} \int_P^Q \omega_j.$$

The left hand side of the equality becomes $\int_P^Q \omega_i$. For the right hand side, P and $\phi(P)$ are in the same residue disk, making $\int_P^{\phi(P)} \omega_i$ a tiny integral and therefore computable via its power series expansion. The same is true for the pair $\phi(Q)$ and Q. The h_i are given to us explicitly from Kedlaya's algorithm, and we can evaluate them on Q and P. Notice that $M^t - 1$ is invertible since, by the Weil conjectures, the eigenvalues of M have norm $\sqrt{p} \neq 1$. Therefore we can compute the left hand side by solving the linear equation.

Remark 1.38. For Weierstrass residue disks, the lift of Frobenius is not defined over the entirety of the disc, but due to overconvergence it is defined near the boundary of the residue disk. So if W is a Weierstrass point and we would like to compute $\int_W^P \omega_i$, we choose a point S close to the boundary of the Weierstrass disk of W and decompose the integral as

$$\int_W^P \omega_i = \int_W^S \omega_i + \int_S^P \omega_i.$$

On the right hand side, the first term is a tiny integral while the second term can be computed using the above method. However, this is computationally expensive, as we have to work over a totally ramified extension of $\mathbb{Q}_p$ to compute the integral.

Remark 1.39. For precision estimates in Algorithm 1.36, see [BBK10, §4.1]. Roughly speaking, there is some loss of precision from truncations of power series giving the necessary tiny integrals, as well as from the valuation of the determinant of the matrix $M^t - 1$.

Remark 1.40. In the case of p-adic integration for a *bad* prime p, Katz and Kaya [KK20] recently gave an algorithm to compute p-adic abelian integrals on hyperelliptic curves. They do this by covering a hyperelliptic curve with bad reduction at p by annuli and basic wide open sets, and then reduce the computation of Berkovich–Coleman integrals to the known algorithms for integration of a 1-form of the second or third kind on a hyperelliptic curve with good reduction [BBK10, BB12] and to integration in annuli.

Remark 1.41. For a genus g hyperelliptic curve over $\mathbb{F}_{p^n}$, Kedlaya's algorithm computes the matrix of p-power Frobenius mod p^N in time $\widetilde{O}(pN^2g^2n)$, where $\widetilde{O}(X)$ denotes $O(X(\log X)^k)$ for some $k \geq 0$. Harvey [Har07] showed that one could interpret the reductions in cohomology in terms of linear recurrences to reduce the dependence on p in the runtime of the algorithm to $\sqrt{p}$. This was later generalized by Minzlaff [Min10] to superelliptic curves. Best showed that similar ideas can be used to improve the runtime of Coleman integration algorithms, first in the case of hyperelliptic curves over $\mathbb{Q}_p$ [Bes19] and superelliptic curves over unramified extensions of $\mathbb{Q}_p$ [Bes20].

Now we return to the Chabauty–Coleman method for a nice curve $X/\mathbb{Q}$.

Example 1.42. Recall the set-up of Example 1.22, with the genus 2 curve

$$X : y^2 = x^5 - 2x^3 + x + \frac{1}{4},$$

with known rational points

$$X(\mathbb{Q})_{\text{known}} = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\}.$$

We computed an annihilating differential

$$\eta = \beta\omega_0 - \alpha\omega_1,$$

where

$$\alpha := \int_{(0,1/2)}^{(-1,-1/2)} \omega_0 = 3 + 3^2 + 3^4 + 3^5 + 2\cdot 3^6 + 2\cdot 3^7 + 2\cdot 3^8 + 3^{10} + O(3^{11}),$$
$$\beta := \int_{(0,1/2)}^{(-1,-1/2)} \omega_1 = 2 + 2\cdot 3 + 2\cdot 3^3 + 3^4 + 3^6 + 2\cdot 3^8 + 2\cdot 3^9 + O(3^{10}),$$

and these values of α and β were produced using Algorithm 1.36.

Now we would like to determine the set

$$X(\mathbb{Q}_3)_1 := \{z \in X(\mathbb{Q}_3) : \int_{(0,1/2)}^{z} \eta = 0\} \supset X(\mathbb{Q}).$$

We begin by enumerating the points in $X(\mathbb{F}_3)$:

$$X(\mathbb{F}_3) = \{\infty, (0, \pm 1), (1, \pm 1), (2, \pm 1)\},$$

which indexes the residue disks. Now we would like to compute the power series expansions of the collection of "indefinite" Coleman integrals $\left\{\int_{(0,1/2)}^{P_t} \eta\right\}$, where P_t ranges over all residue disks, and solve for all $z \in X(\mathbb{Q}_3)$ such that $\int_{(0,1/2)}^{z} \eta = 0$. Note that to compute these indefinite Coleman integrals, we can take P_0 a lift of an $\mathbb{F}_3$-point in the same residue disk as P_t. Then

$$\int_{(0,1/2)}^{P_t} \eta = \int_{(0,1/2)}^{P_0} \eta + \int_{P_0}^{P_t} \eta, \tag{11}$$

where the first integral on the right-hand side of (11) is some 3-adic constant, and the second is a tiny integral computed using a local coordinate at P_0. However, since each residue disk contains one rational point, we may take P_0 to be the rational point in the residue disk. This sets the constant of integration to 0 in each disk, by construction of the annihilating differential. Thus the computation is now purely local. Moreover, using the hyperelliptic involution, we need only to consider the residue disk of P_0 and not the disk of $i(P_0)$ as well.

So we carry out the computation in the residue disks of ∞, (0,1/2), (1,1/2), and $(-1, 1/2)$. For instance, in the residue disk of $(1, 1/2)$, a local coordinate is given by

$$x(t) = 1 + t + O(t^{20})$$

$$y(t) = \frac{1}{2} + 4t^2 + 8t^3 - 11t^4 - 63t^5 + 24t^6 + 680t^7 + 695t^8 - 7210t^9 - 19881t^{10} + 64544t^{11} + 374802t^{12} - 301946t^{13} - 5872722t^{14} - 5265422t^{15} + 78467963t^{16} + 210631116t^{17} - 840861878t^{18} - 4667976084t^{19} + O(t^{20})$$

and the power series for $\int_{(0,1/2)}^{P_t} \eta = \int_{P_0}^{P_t} \eta$ is given by

$$\left(2 + 3 + 2 \cdot 3^2 + 3^3 + 2 \cdot 3^5 + 3^6 + 2 \cdot 3^8 + 3^9 + O(3^{10})\right) t + \left(3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^6 + 3^7 + 3^8 + 3^9 + 2 \cdot 3^{10} + O(3^{12})\right) t^2 + \left(2 \cdot 3 + 3^2 + 3^5 + 3^7 + 3^8 + 3^{10} + O(3^{11})\right) t^3 + \left(3^3 + 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 + 2 \cdot 3^8 + 3^{12} + O(3^{13})\right) t^4 + \left(2 \cdot 3^4 + 2 \cdot 3^7 + 3^8 + 3^9 + 2 \cdot 3^{11} + 2 \cdot 3^{12} + 2 \cdot 3^{13} + O(3^{14})\right) t^5 + \left(3^4 + 2 \cdot 3^5 + 3^6 + 3^7 + 2 \cdot 3^8 + 3^9 + 3^{11} + 3^{12} + O(3^{14})\right) t^6 + \left(2 \cdot 3^6 + 2 \cdot 3^7 + 3^8 + 3^{10} + 2 \cdot 3^{11} + 3^{12} + 2 \cdot 3^{14} + O(3^{16})\right) t^7 + \left(2 \cdot 3^8 + 2 \cdot 3^9 + 3^{11} + 3^{12} + 2 \cdot 3^{14} + 2 \cdot 3^{15} + 2 \cdot 3^{16} + O(3^{18})\right) t^8 + \left(2 \cdot 3^6 + 2 \cdot 3^9 + 2 \cdot 3^{10} + 3^{12} + 2 \cdot 3^{14} + 2 \cdot 3^{15} + O(3^{16})\right) t^9 + \left(2 \cdot 3^9 + 3^{10} + 2 \cdot 3^{11} + 3^{13} + 3^{16} + 3^{17} + O(3^{19})\right) t^{10} + \cdots,$$

which just has a simple zero at $t = 0$, corresponding to $(1, 1/2)$.

Repeating this for each residue disk, we find that each residue disk has a simple zero at the rational point and no others, which gives that

$$X(\mathbb{Q}_3)_1 = X(\mathbb{Q})_{\text{known}} = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\},$$

and proves that

$$X(\mathbb{Q}) = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\}.$$

Here is SageMath code to carry out this computation:

```
R.<x> = QQ[]
X = HyperellipticCurve(x^5-2*x^3+x+1/4)
p = 3
K = Qp(p,15) #some amount of precision loss
XK = X.change_ring(K)
a,b,_,_ = XK.coleman_integrals_on_basis(XK(0,1/2),XK(-1,-1/2))
for P in [X(0,1,0), X(0,1/2), X(-1,1/2), X(1,1/2)]:
    x,y = X.local_coord(P)
    t = x.parent().gen()
    S = K[[t]]
    dx = x.derivative()
    omega0 = dx/(2*y)
    omega1 = x*omega0
    try:
        I = (b*S(omega0)-a*S(omega1)).integral()(p*t)
    except TypeError:
        I = (b*S(omega0.power_series())-a*S(omega1.power_series())).integral()(p*t)
        I = I.power_series()
    coeffval = min(c.valuation() for c in I.list())
    I = I/p^coeffval
    r = (I).truncate(20).roots()
    [rt for rt in r if (rt[0]).valuation() > -1]
```

We note that Magma has an implementation of the Chabauty–Coleman method for genus 2 curves of ranks 0 and 1 (with an additional Mordell–Weil sieve step):

```
> R<x> := PolynomialRing(Rationals());
> X := HyperellipticCurve(x^5-2*x^3+x+1/4);
> C := IntegralModel(X);
> RationalPoints(C:Bound:=1000);
{@ (1 : 0 : 0), (-1 : -1 : 1), (-1 : 1 : 1), (0 : -1 : 1), (0 : 1 : 1), (1 : -1
: 1), (1 : 1 : 1) @}
> J := Jacobian(C);
> P := J!(C![0,1] - C![-1,-1]); //a point of infinite order
> Chabauty(P);
{ (1 : 1 : 1), (0 : -1 : 1), (0 : 1 : 1), (1 : 0 : 0), (-1 : 1 : 1), (1 : -1 :
1), (-1 : -1 : 1) }
{ 11, 19, 41, 43, 83, 179, 211 }
[ 2, 7, 23, 3, 13, 3 ]
```

1.4. More p-adic cohomology.

We saw how Kedlaya's zeta function algorithm played a crucial role in computing Coleman integrals on hyperelliptic curves. It would certainly be useful to compute Coleman integrals on curves beyond those that are hyperelliptic. And indeed, in the years since Kedlaya's algorithm, a number of related zeta function algorithms were given: for superelliptic curves by Gaudry–Gürel [GG01], hyperelliptic curves given by an even degree model by Harrison [Har12], hyperelliptic curves in characteristic 2 by Denef–Vercauteren [DV06b], C_{ab} curves by Denef–Vercauteren [DV06a], and nondegenerate curves by Castryck–Denef–Vercauteren [CDV06]. However, the more general of these algorithms were not obviously practical and were not implemented.

More recently, Tuitman [Tui16, Tui17] gave an efficient algorithm to compute the action of Frobenius on rigid cohomology on smooth curves, by using a plane model with a map to $\mathbb{P}^1$. We give a survey of Tuitman's algorithm and show how it can be turned into an algorithm to compute Coleman integrals on plane curves.

First, we set up Tuitman's algorithm from the point of view of explicit Coleman integration, as done by Balakrishnan–Tuitman [BTa]. Let X be a nice curve over $\mathbb{Q}$ of genus g, birational to

$$Q(x,y) = y^{d_x} + Q_{d_x-1}y^{d_x-1} + \cdots + Q_0 = 0,$$

such that $Q(x,y)$ is irreducible and $Q_i(x) \in \mathbb{Z}[x]$ for $i = 0, \ldots, d_x - 1$. Here is a rough outline of Tuitman's algorithm:

(1) Consider the map: $x : X \to \mathbb{P}^1$ and remove the ramification locus $r(x)$ of x. (This is the analogue of removing the Weierstrass points in Kedlaya's algorithm.)
(2) Choose a lift of Frobenius sending $x \mapsto x^p$ and compute the image of y via Hensel lifting.
(3) Compute the action of Frobenius on differentials and reduce pole orders using relations in cohomology via Lauder's fibration algorithm.

Then for a basis $\{\omega_i\}_{i=0}^{2g-1}$ of $\mathrm{H}^1_{\mathrm{rig}}(X \otimes \mathbb{Q}_p)$, Tuitman's algorithm computes

$$\phi^*\omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j,$$

and, as before, this algorithm for computing the action of Frobenius on cohomology can be used to give an algorithm for Coleman integration.

We let $\Delta(x) \in \mathbb{Z}[x]$ be the discriminant of Q with respect to y, and let $r(x) = \Delta/\gcd(\Delta, d\Delta/dx)$. Note that $r(x)$ is squarefree and divides $\Delta(x)$.

Set

$$\begin{aligned} S &= \mathbb{Z}_p\langle x, 1/r\rangle, & S^\dagger &= \mathbb{Z}_p\langle x, 1/r\rangle^\dagger, \\ R &= \mathbb{Z}_p\langle x, 1/r, y\rangle/(Q), & R^\dagger &= \mathbb{Z}_p\langle x, 1/r, y\rangle^\dagger/(Q), \end{aligned}$$

where $\langle\ \rangle^\dagger$ denotes the ring of overconvergent functions given by weak completion of the corresponding polynomial ring.

Definition 1.43. Let $W^0 \in \mathrm{GL}_{d_x}(\mathbb{Q}[x, 1/r])$ and $W^\infty \in \mathrm{GL}_{d_x}(\mathbb{Q}[x, 1/x, 1/r])$ denote matrices such that, if we denote

$$b^0_j = \sum_{i=0}^{d_x-1} W^0_{i+1,j+1} y^i \quad \text{and} \quad b^\infty_j = \sum_{i=0}^{d_x-1} W^\infty_{i+1,j+1} y^i$$

for all $0 \le j \le d_x - 1$, then

(1) $[b^0_0, \dots, b^0_{d_x-1}]$ is an integral basis for $\mathbb{Q}(X)$ over $\mathbb{Q}[x]$,
(2) $[b^\infty_0, \dots, b^\infty_{d_x-1}]$ is an integral basis for $\mathbb{Q}(X)$ over $\mathbb{Q}[1/x]$,

where $\mathbb{Q}(X)$ denotes the function field of X. Moreover, let $W \in \mathrm{GL}_{d_x}(\mathbb{Q}[x, 1/x])$ denote the change of basis matrix $W = (W^0)^{-1}W^\infty$.

Example 1.44. Let $X/\mathbb{Q}$ be an odd degree monic hyperelliptic curve of genus g given by the plane model

$$Q(x, y) = y^2 - f(x) = 0.$$

We have that

$$r(x) = f(x)$$

and:

$$W^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad W^\infty = \begin{pmatrix} 1 & 0 \\ 0 & 1/x^{g+1} \end{pmatrix}.$$

This means that $b^0 = [1, y]$ and $b^\infty = [1, y/x^{g+1}]$ are integral bases for the function field of X over $\mathbb{Q}[x]$ and $\mathbb{Q}[1/x]$, respectively.

Definition 1.45. We say that the triple (Q, W^0, W^∞) has good reduction at a prime number p if the conditions below (taken from [Tui17, Assumption 1]) are satisfied.

Assumption 1 ([Tui17, Assumption 1])**.**

(1) The discriminant of $r(x)$ is contained in $\mathbb{Z}_p^\times$.

(2) If we let $\mathbb{F}_p(x,y)$ be the field of fractions of $\mathbb{F}_p[x,y]/(Q)$, then:
  (a) The reduction modulo p of $[b^0_0, \dots, b^0_{d_x-1}]$ is an integral basis for $\mathbb{F}_p(x,y)$ over $\mathbb{F}_p[x]$.
  (b) The reduction modulo p of $[b^\infty_0, \dots, b^\infty_{d_x-1}]$ is an integral basis for $\mathbb{F}_p(x,y)$ over $\mathbb{F}_p[1/x]$.

(3) $W^0 \in \mathrm{GL}_{d_x}(\mathbb{Z}_p[x, 1/r])$ and $W^\infty \in \mathrm{GL}_{d_x}(\mathbb{Z}_p[x, 1/x, 1/r])$.

(4) Denote:

$$\begin{aligned}\mathcal{R}^0 &= \mathbb{Z}_p[x]b^0_0 \quad\; + \dots + \mathbb{Z}_p[x]b^0_{d_x-1},\\ \mathcal{R}^\infty &= \mathbb{Z}_p[1/x]b^\infty_0 + \dots + \mathbb{Z}_p[1/x]b^\infty_{d_x-1}.\end{aligned}$$

Then the discriminants of the finite $\mathbb{Z}_p$-algebras $\mathcal{R}^0/(r(x))$ and $\mathcal{R}^\infty/(1/x)$ are contained in $\mathbb{Z}_p^\times$.

Definition 1.46. We say that a point of X^{an} is *very infinite* if its x-coordinate is ∞ and *very bad* if it is either very infinite or its x-coordinate is a zero of $r(x)$.

Definition 1.47. We say that a residue disk (as well as any point inside it) is *infinite* or *bad* if it contains a very infinite or a very bad point, respectively. A point or residue disk is called *finite* if it is not infinite and *good* if it is not bad.

We let U denote the complement of the very bad points in X^{an}.

Definition 1.48. Let $\{\omega_i\}_{i=0,\dots,2g-1}$ be p-adically integral 1-forms on U such that

(1) $\omega_0, \dots, \omega_{g-1}$ form a basis for $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)$,
(2) $\omega_0, \dots, \omega_{2g-1}$ form a basis for $H^1_{\mathrm{rig}}(X \otimes \mathbb{Q}_p)$,
(3) $\mathrm{ord}_P(\omega_i) \geq -1$ for all i at all finite very bad points P,
(4) $\mathrm{ord}_P(\omega_i) \geq -1 + (\mathrm{ord}_0(W) + 1)e_P$ for all i at all very infinite points P.

In [Tui16, Tui17], it is explained how 1-forms satisfying properties (2)-(4) can be computed. Briefly, one computes a basis for $H^1_{\mathrm{rig}}(U)$ and uses the kernel of a residue map to extract those 1-forms of the second kind, to produce a basis for $H^1_{\mathrm{rig}}(X \otimes \mathbb{Q}_p)$. The algorithm can be easily adapted so that (1) is satisfied as well, which is the convention we take.

Definition 1.49. The p-th power Frobenius ϕ acts on $H^1_{\mathrm{rig}}(X \otimes \mathbb{Q}_p)$, so there exist a matrix $M \in M_{2g \times 2g}(\mathbb{Q}_p)$ and functions $h_0, \dots, h_{2g-1} \in R^\dagger \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j$$

for $i = 0, \dots, 2g-1$.

After we compute the action of Frobenius on a 1-form, we need to reduce the pole order using relations in cohomology. Tuitman's algorithm uses Lauder's fibration algorithm, which solves for a cohomologous differential of lower pole order using a linear system. Tuitman applies it first to points not lying over infinity:

Proposition 1.50. *Let r' denote dr/dx for points not over infinity. For all $\ell \in \mathbb{N}$ and every $w \in \mathbb{Q}_p[x]^{\oplus d_x}$, there exist vectors $u, v \in \mathbb{Q}_p[x]^{\oplus d_x}$ such that* $\deg(v) < \deg(r)$ *and*

$$\frac{\sum_{i=0}^{d_x-1} w_i b^0_i}{r^\ell}\frac{dx}{r} = \left(d\frac{\sum_{i=0}^{d_x-1} v_i b^0_i}{r^\ell}\right) + \frac{\sum_{i=0}^{d_x-1} u_i b^0_i}{r^{\ell-1}}\frac{dx}{r}$$

Proof. Since r is separable, r' is invertible in $\mathbb{Q}_p[x]/r$. We check that there is a unique solution v to the $d_x \times d_x$ linear system

$$(M/r' - \ell I)\, v \equiv w/r' \mod r$$

over $\mathbb{Q}_p[r]/(r)$: take

$$u = \frac{w - (M - \ell r' I)v}{r} - \frac{dv}{dx}.$$

□

For reducing pole orders at points over infinity, we have the following proposition:

Proposition 1.51. *For every vector* $w \in \mathbb{Q}_p[x, 1/x]^{\oplus d_x}$ *with* $\operatorname{ord}_\infty(w) \leq -\deg r$*, there exist* $u, v \in \mathbb{Q}_p[x, 1/x]^{\oplus d_x}$ *with* $\operatorname{ord}_\infty(u) > \operatorname{ord}_\infty(w)$ *such that*

$$\left(\sum_{i=0}^{d_x-1} w_i b_i^\infty\right) \frac{dx}{r} = d\left(\sum_{i=0}^{d_x-1} v_i b_i^\infty\right) + \left(\sum_{i=0}^{d_x-1} u_i b_i^\infty\right) \frac{dx}{r}.$$

Here is Tuitman's algorithm for computing the matrix M and the functions $h_0, \ldots, h_{2g-1}$:

Algorithm 1.52 (Tuitman's algorithm [Tui16, Tui17])**.**
Input:

- A prime $p > 2$ of good reduction (in the sense of Definition 1.45) for a nice curve $X/\mathbb{Q}$
- A basis $\{\omega_i\}$ of $H^1_{\text{rig}}(X \otimes \mathbb{Q}_p)$

Output: The matrix $M \in M_{2g\times 2g}(\mathbb{Q}_p)$ and overconvergent functions $h_i \in R^\dagger \otimes \mathbb{Q}_p$ such that $\phi^*\omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j$.

(1) Compute the Frobenius lift: set $\phi(x) = x^p$ and determine the elements $\phi(1/r) \in S^\dagger$ and $\phi(y) \in R^\dagger$ by Hensel lifting.
(2) Finite pole order reduction: For $i = 0, \ldots, 2g-1$, find $h_{i,0} \in R^\dagger \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_{i,0} + G_i \left(\frac{dx}{r(x)}\right),$$

where $G_i \in R \otimes \mathbb{Q}_p$ only has poles at very infinite points.
(3) Infinite pole order reduction. For $i = 0, \ldots, 2g-1$, find $h_{i,\infty} \in R \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_{i,0} + dh_{i,\infty} + H_i \left(\frac{dx}{r(x)}\right),$$

where $H_i \in R \otimes \mathbb{Q}_p$ still only has poles at very infinite points P and satisfies

$$\operatorname{ord}_P(H_i) \geq (\operatorname{ord}_0(W) - \deg(r) + 2)e_P$$

at all these points.
(4) Final reduction: For $i = 0, \ldots, 2g-1$, find $h_{i,end} \in R \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_{i,0} + dh_{i,\infty} + dh_{i,end} + \sum_{j=0}^{2g-1} M_{ji}\omega_j,$$

where $M \in M_{2g\times 2g}(\mathbb{Q}_p)$ is the matrix of ϕ^* on $H^1_{\text{rig}}(U \otimes \mathbb{Q}_p)$ with respect to the basis $\{\omega_i\}_{i=0}^{2g-1}$.

The matrix M and the functions

$$h_i := h_{i,0} + h_{i,\infty} + h_{i,end}$$

are exactly what we need from [Tui16, Tui17] to compute Coleman integrals, giving the necessary input into Algorithm 1.53.

Algorithm 1.53 (Coleman integration on a plane curve [BTa])**.**
Input:

- A prime $p > 2$ of good reduction (in the sense of Definition 1.45) for a nice curve $X/\mathbb{Q}$
- Points $P, Q \in X(\mathbb{Q}_p)$ not contained in very bad residue disks
- A 1-form ω of the second kind

Output: The Coleman integral $\int_P^Q \omega$.

(1) Since ω is of the second kind, we may write it as a linear combination of a basis $\{\omega_i\}_{i=0}^{2g-1}$ for $H^1_{\mathrm{rig}}(X \otimes \mathbb{Q}_p)$ together with an exact form. Use Tuitman's algorithm to write $\omega = dh + \sum_{i=0}^{2g-1} a_i\omega_i$, which allows us to specialize to the case of Coleman integrals of basis differentials.
(2) Compute the action of Frobenius on $H^1_{\mathrm{rig}}(X \otimes \mathbb{Q}_p)$ using Algorithm 1.52 and store M and $h_0, \ldots, h_{2g-1}$.
(3) Compute the integrals $\int_P^{\phi(P)} \omega_i$ and $\int_{\phi(Q)}^Q \omega_i$ for $i = 0, \ldots, 2g-1$ using local coordinates and tiny integrals.
(4) Compute $h_i(P) - h_i(Q)$ for $i = 0, \ldots, 2g-1$ and use the system of equations

$$\sum_{j=0}^{2g-1} (M^t - I)_{ij} \left(\int_P^Q \omega_j \right) = h_i(P) - h_i(Q) - \int_P^{\phi(P)} \omega_i - \int_{\phi(Q)}^Q \omega_i$$

to solve for all $\int_P^Q \omega_i$.

Remark 1.54. As in the case of integrating from a Weierstrass point on a hyperelliptic curve, to integrate from a very bad point B on a plane curve, split up the integral

$$\int_B^Q \omega_i = \int_B^{B'} \omega_i + \int_{B'}^Q \omega_i$$

for B' a point near the boundary of the residue disk of B, then apply Algorithm 1.53 to compute $\int_{B'}^Q \omega_i$ and compute $\int_B^{B'} \omega_i$ using a tiny integral.

Remark 1.55. For precision estimates in Algorithm 1.53, see [BTa, §4].

Example 1.56. We show how the algorithm above can be used to show that a Jacobian of a non-hyperelliptic genus 55 curve has positive rank (for more details, including timing data, see [BTa, §6.4]). We consider the genus 55 curve X with plane model given by $Q(x, y) = 0$ below:

$$\begin{aligned} Q(x,y) = {} & x^{11}y - x^7y^5 - x^6y^6 - x^4y^8 + xy^{11} + y^{12} + x^{11} - x^{10}y + x^8y^3 - x^6y^5 + x^5y^6 + x^3y^8 - x^2y^9 - xy^{10} + \\ & y^{11} + x^{10} + x^9y - x^8y^2 + x^7y^3 + x^6y^4 + x^5y^5 - x^4y^6 + xy^9 + y^{10} - x^9 + x^8y + x^7y^2 + x^6y^3 + x^5y^4 + \\ & x^4y^5 + x^3y^6 - x^2y^7 + y^9 + x^8 - x^7y + x^6y^2 - x^5y^3 + xy^7 + y^8 + x^7 + x^6y + x^5y^2 - x^2y^5 - xy^6 + \\ & y^7 - x^6 - x^4y^2 - x^2y^4 + xy^5 - x^5 + x^3y^2 - x^2y^3 + y^5 - x^4 + x^3y + x^2y^2 + xy^3 + y^4 - x^2y - xy^2 + \\ & y^3 - x^2 - xy + x + y. \end{aligned}$$

Let $p = 7$ and consider $P_1 = (0,0)$ and $P_2 = (1,0)$, which are each good points on X. We compute the Coleman integrals $\left\{\int_{P_1}^{P_2} \omega_i\right\}_{i=1}^{110}$ for the basis $\{\omega_i\}$ of $\mathrm{H}^1_{\mathrm{rig}}(X \otimes \mathbb{Q}_p)$ constructed as in Definition 1.48 with $N = 5$ as our precision. We find that

$$\int_{P_1}^{P_2} \omega_1 = 5 \cdot 7 + O(7^2),$$

and thus the Jacobian of X has positive rank.

The `Magma` code for this example is available at `./examples/g55.m` in [BTb].

Project 1.57 (Coleman integration for curves over number fields)**.** Give an algorithm to compute Coleman integrals on curves over number fields and implement the algorithm. To start, see the Github repository of Balakrishnan–Tuitman [BTb] for plane curves defined over $\mathbb{Q}$. Before implementing, it would be good to think through the current scope of curves and number fields that are practical.

Project 1.58 (A Chabauty–Coleman solver)**.** Use the project above as well as estimates on precision of p-adic power series to give a Chabauty–Coleman solver for curves over number fields that would take as input a genus g curve X defined over a number field K with $r = \operatorname{rk} J(K) < g$, a prime $\mathfrak{p}$ of good reduction, and r generators of the Mordell–Weil group modulo torsion and output the set $X(K_{\mathfrak{p}})_1$. To start, see the Github repositories of Balakrishnan–Tuitman [BTb] and Hashimoto–Morrison [HM].

1.5. **Iterated Coleman integrals.** Let $X/\,\mathbb{Q}$ be a nice curve of genus g with a plane model and let p be a prime of good reduction. In [Col82], Coleman described a construction of iterated p-adic integrals on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ with applications to Beilinson's conjecture. This was extended by Coleman–de Shalit [CdS88] to any curve and by Besser [Bes02] to higher-dimensional varieties. (For the classical theory of iterated integrals, see the work of Chen [Che71].)

By an *iterated Coleman integral* we mean an iterated path integral

$$\int_P^Q \eta_n \dots \eta_1 = \int_0^1 \int_0^{t_1} \cdots \int_0^{t_{n-1}} f_n(t_n) \dots f_1(t_1) dt_n \dots dt_1. \tag{12}$$

We will henceforth use notation on the left hand side of (12) to describe iterated integrals, where the implicit integrations are with respect to a dummy variable: e.g.,

$$\int_P^Q \eta_2\eta_1 := \int_P^Q \eta_2(R) \int_P^R \eta_1 = \int_P^Q \eta_2(R) I(R),$$

where $I(R) = \int_P^R \eta_1$.

The main idea is to apply an algorithm for computing the action of Frobenius on p-adic cohomology (e.g., Kedlaya or Tuitman) to produce the relationship

$$\phi^* \omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j,$$

observe that the eigenvalues of $M^{\otimes n}$, are not 1, and reduce the computation of an n-fold iterated integral to a computation of an $(n-1)$-fold iterated integral. For instance, in writing down a linear system for computing single Coleman integrals, we used the fundamental theorem of calculus to produce the constants

$$\int_P^Q dh_i = h_i(Q) - h_i(P),$$

and now we will apply this idea inductively. As before, iterated integrals between points in the same residue disk can be computed using a local coordinate at one point and (iteratively) integrating power series.

More formally, here is how we compute a tiny iterated integral:

Algorithm 1.59 (Tiny iterated integral on a plane curve X)**.**

Input:

- A prime $p > 2$ of good reduction (in the sense of Definition 1.45) for a plane curve $X/\mathbb{Q}$
- Points $P, Q \in X(\mathbb{Q}_p)$ in same residue disk.

Output: The tiny iterated integral $\int_P^Q \eta_1 \dots \eta_n$

(1) Compute a local coordinate $(x(t), y(t))$ at P.
(2) For each k, write $\eta_k(x, y)$ as $\eta_k(t)dt$.
(3) Let $I_{n+1} = 1$. Compute for $k = n, n-1, \dots, 2$

$$I_k = \int_P^{R_{k-1}} \eta_k I_{k+1} = \int_P^{t(R_{k-1})} \eta_k(t) I_{k+1} dt$$

where $t(R_{k-1})$ is parametrizing points in the residue disk of P.
(4) $\int_P^Q \eta_1 \dots \eta_n = \int_P^{t(Q)} \eta_1(t) I_2(t) dt$.

To compute more general iterated Coleman integrals, we will use the following properties.

Proposition 1.60. *Let $\omega_{i_1}, \dots \omega_{i_n}$ be forms of the second kind, holomorphic at $P, Q \in X(\mathbb{Q}_p)$.*

(1) $\displaystyle\int_P^P \omega_{i_1} \dots \omega_{i_n} = 0$

(2) $\displaystyle\sum_{\text{all permutations } \sigma} \int_P^Q \omega_{\sigma(i_1)} \dots \omega_{\sigma(i_n)} = \prod_{j=1}^n \int_P^Q \omega_{i_j}$

(3) $\displaystyle\int_P^Q \omega_{i_1} \dots \omega_{i_n} = (-1)^n \int_Q^P \omega_{i_n} \dots \omega_{i_1}$

As a corollary, we have

Corollary 1.61. $\displaystyle\int_P^Q \underbrace{\omega_i \dots \omega_i}_{n} = \frac{1}{n!} \left(\int_P^Q \omega_i \right)^n$

The following lemma gives the analogue of additivity in endpoints:

Lemma 1.62. *Let $P, P', Q \in X(\mathbb{Q}_p)$. Then*

$$\int_P^Q \omega_{i_1} \dots \omega_{i_n} = \sum_{j=0}^n \int_{P'}^Q \omega_{i_1} \dots \omega_{i_j} \int_P^{P'} \omega_{i_{j+1}} \dots \omega_{i_n}$$

Now for ease of exposition, we will focus our attention on the case of $n = 2$, the double Coleman integrals [Bal13, Bal15].

Applying Lemma 1.62 twice, we may link double integrals between different residue disks:

$$\int_P^Q \omega_i \omega_k = \int_P^{P'} \omega_i \omega_k + \int_{P'}^{Q'} \omega_i \omega_k + \int_{Q'}^Q \omega_i \omega_k + \int_P^{P'} \omega_k \int_{P'}^Q \omega_i + \int_{P'}^{Q'} \omega_k \int_{Q'}^Q \omega_i.$$

We can directly compute double integrals using a linear system. Indeed, using Lemma 1.62, we take $\phi(P)$ and $\phi(Q)$ to be the points in the disks of P and Q, respectively, which gives

$$\int_P^Q \omega_i\omega_k = \int_P^{\phi(P)} \omega_i\omega_k + \int_{\phi(P)}^{\phi(Q)} \omega_i\omega_k + \int_{\phi(Q)}^{Q} \omega_i\omega_k + \int_P^{\phi(P)} \omega_k \int_{\phi(P)}^{Q} \omega_i + \int_{\phi(P)}^{\phi(Q)} \omega_k \int_{\phi(Q)}^{Q} \omega_i. \tag{13}$$

Then we expand the following

$$\begin{aligned}\int_{\phi(P)}^{\phi(Q)} \omega_i\omega_k = \int_P^Q \phi^*(\omega_i\omega_k) &= \int_P^Q \phi^*(\omega_i)\phi^*(\omega_k) \\ &= \int_P^Q (df_i + \sum_{j=0}^{2g-1} M^t_{ij}\omega_j)(df_k + \sum_{j=0}^{2g-1} M^t_{kj}\omega_j) \\ &= c_{ik} + \int_P^Q \left(\sum_{j=0}^{2g-1} M^t_{ij}\omega_j\right)\left(\sum_{j=0}^{2g-1} M^t_{kj}\omega_j\right),\end{aligned} \tag{14}$$

where

$$\begin{aligned}c_{ik} = \int_P^Q df_i(R)(f_k(R)) - f_k(P)(f_i(Q) - f_i(P)) + \int_P^Q \sum_{j=0}^{2g-1} M^t_{ij}\omega_j(R)(f_k(R) - f_k(P)) \\ + f_i(Q)\int_P^Q \sum_{j=0}^{2g-1} M^t_{kj}\omega_j - \int_P^Q f_i(R)(\sum_{j=0}^{2g-1} M^t_{kj}\omega_j(R)).\end{aligned}$$

Putting together (13) and (14), we get

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i\omega_k \\ \vdots \end{pmatrix} = (I_{4g^2\times 4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} \vdots \\ c_{ik} - \int_{\phi(P)}^{P} \omega_i\omega_k - \left(\int_P^Q \omega_i\right)\left(\int_{\phi(P)}^{P} \omega_k\right) \\ - \left(\int_Q^{\phi(Q)} \omega_i\right)\left(\int_{\phi(P)}^{\phi(Q)} \omega_k\right) + \int_{\phi(Q)}^{Q} \omega_i\omega_k \\ \vdots \end{pmatrix}.$$

Algorithm 1.63 (Double Coleman integrals [Bal13, Bal15])**.**

Input:

- A prime $p > 2$ of good reduction (in the sense of Definition 1.45) for a plane curve $X/\mathbb{Q}$
- Points $P, Q \in X(\mathbb{Q}_p)$ in the region of overconvergence for the lift of p-power Frobenius

Output: The double integrals $\left(\int_P^Q \omega_i\omega_j\right)_{i,j=0}^{2g-1}$.

(1) Use Algorithm 1.53 to compute the single integrals $\int_P^Q \omega_i, \int_{\phi(P)}^{\phi(Q)} \omega_i$ for all i.
(2) Use Algorithm 1.59 to compute $\int_{\phi(P)}^{P} \omega_i\omega_k, \int_{\phi(Q)}^{Q} \omega_i\omega_k$ for all i, k
(3) Compute the constants c_{ik} for all i, k using single integrals.
(4) Recover the double integrals using the linear system

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i\omega_k \\ \vdots \end{pmatrix} = (I_{4g^2\times 4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} \vdots \\ c_{ik} - \int_{\phi(P)}^{P} \omega_i\omega_k - \left(\int_P^Q \omega_i\right)\left(\int_{\phi(P)}^{P} \omega_k\right) \\ - \left(\int_Q^{\phi(Q)} \omega_i\right)\left(\int_{\phi(P)}^{\phi(Q)} \omega_k\right) + \int_{\phi(Q)}^{Q} \omega_i\omega_k \\ \vdots \end{pmatrix}.$$

Remark 1.64. In [Bal13, Bal15], Algorithm 1.63 was described and implemented for hyperelliptic curves, as it used Kedlaya's algorithm (and Harrison's generalization) for the Frobenius step. With Tuitman's algorithm in place of Kedlaya's, one can run the algorithm for (a plane model of) a nice curve.

Example 1.65. Let $X/\mathbb{Q}$ be the genus 2 curve

$$y^2 = x^5 - 2x^4 + 2x^3 - x + 1$$

which is [LMF20a] and has good reduction at $p = 5$.

Using Algorithm 1.63, we compute 5-adic double Coleman integrals between the points $P = (0, 1)$ and $Q = (1, 1)$, where $\omega_i = \frac{x^i}{2y}dx$:

$$\begin{pmatrix} \int_P^Q \omega_0\omega_0 \\ \int_P^Q \omega_0\omega_1 \\ \int_P^Q \omega_0\omega_2 \\ \int_P^Q \omega_0\omega_3 \\ \int_P^Q \omega_1\omega_0 \\ \int_P^Q \omega_1\omega_1 \\ \int_P^Q \omega_1\omega_2 \\ \int_P^Q \omega_1\omega_3 \\ \int_P^Q \omega_2\omega_0 \\ \int_P^Q \omega_2\omega_1 \\ \int_P^Q \omega_2\omega_2 \\ \int_P^Q \omega_2\omega_3 \\ \int_P^Q \omega_3\omega_0 \\ \int_P^Q \omega_3\omega_1 \\ \int_P^Q \omega_3\omega_2 \\ \int_P^Q \omega_3\omega_3 \end{pmatrix} = \begin{pmatrix} 3\cdot 5^2 + 3\cdot 5^3 + 5^4 + 4\cdot 5^5 + 5^6 + O(5^8) \\ 3\cdot 5^2 + 3\cdot 5^3 + 2\cdot 5^4 + 2\cdot 5^5 + 5^6 + 3\cdot 5^7 + O(5^8) \\ 2\cdot 5 + 4\cdot 5^2 + 5^3 + 3\cdot 5^4 + 4\cdot 5^5 + O(5^7) \\ 4\cdot 5 + 5^2 + 4\cdot 5^3 + 5^4 + 3\cdot 5^5 + 2\cdot 5^6 + O(5^7) \\ 5^3 + 3\cdot 5^4 + 2\cdot 5^5 + 4\cdot 5^6 + 5^7 + O(5^8) \\ 2\cdot 5^2 + 5^3 + 4\cdot 5^4 + 5^6 + O(5^8) \\ 2\cdot 5^2 + 4\cdot 5^3 + 5^4 + 3\cdot 5^5 + 5^6 + O(5^7) \\ 1 + 4\cdot 5 + 2\cdot 5^2 + 5^3 + 5^4 + 4\cdot 5^5 + 3\cdot 5^6 + O(5^7) \\ 4\cdot 5^3 + 3\cdot 5^4 + 3\cdot 5^5 + 3\cdot 5^6 + O(5^7) \\ 5 + 2\cdot 5^2 + 4\cdot 5^3 + 4\cdot 5^4 + 5^5 + O(5^7) \\ 2 + 4\cdot 5 + 4\cdot 5^2 + 5^3 + 2\cdot 5^4 + 4\cdot 5^5 + O(5^6) \\ 3 + 2\cdot 5 + 2\cdot 5^2 + 4\cdot 5^3 + 3\cdot 5^4 + 4\cdot 5^5 + O(5^6) \\ 4\cdot 5 + 5^2 + 3\cdot 5^3 + 4\cdot 5^4 + 3\cdot 5^5 + 3\cdot 5^6 + O(5^7) \\ 4 + 4\cdot 5 + 5^2 + 4\cdot 5^3 + 3\cdot 5^5 + 4\cdot 5^6 + O(5^7) \\ 3 + 4\cdot 5 + 4\cdot 5^2 + 2\cdot 5^5 + O(5^6) \\ 2 + 3\cdot 5 + 4\cdot 5^2 + 5^4 + 4\cdot 5^5 + O(5^6) \end{pmatrix}.$$

Using `SageMath` code available on GitHub [Bal], here is how to generate the values of the double integrals above:

```
R.<x> = QQ[]
X = HyperellipticCurve(x^5-2*x^4+2*x^3-x+1)
K = Qp(5,8)
XK = X.change_ring(K)
P = XK(0,1)
Q = XK(1,1)
XK.double_integrals_on_basis(P,Q)
```

Project 1.66. There is a certain amount of redundancy that allows one to express double (or higher iterated) integrals in terms of single integrals. For instance, looking at double integrals in the case of $g = 1$, we have that $\int_P^Q \omega_i\omega_i = \frac{1}{2}\left(\int_P^Q \omega_i\right)^2$ for $i = 0, 1$ and $\int_P^Q \omega_0\omega_1 + \int_P^Q \omega_1\omega_0 = \int_P^Q \omega_0 \int_P^Q \omega_1$. Can these relations be used to give a more efficient algorithm to compute double (or higher iterated) integrals?

1.6. **An application (preview).** Let $\mathcal{E}/\mathbb{Z}$ be the minimal regular model of an elliptic curve. Let $\mathcal{X} = \mathcal{E} \setminus \mathcal{O}$. Let $\omega_0 = \frac{dx}{2y+a_1x+a_3}$, $\omega_1 = x\omega_0$ in Weierstrass coordinates.

Let b be a tangential basepoint at the point at infinity or an integral 2-torsion point. (For more about tangential basepoints, see Deligne [Del89] or Besser [Bes12, §1.5.4]. Roughly, the issue is that ω_1 has a pole at the point at infinity, so to make sense of an integral from the point at infinity, we must normalize with respect to a choice of tangent vector, which essentially means that we are fixing a direction at b.) Let p be a prime of good reduction. Suppose $\mathcal{E}$ has analytic rank 1 and Tamagawa product 1. Consider

$$\log(z) = \int_b^z \omega_0, \qquad\qquad D_2(z) = \int_b^z \omega_0\omega_1.$$

One can think of $\log(z)$ as the Coleman integral extending log on the formal group of $\mathcal{E}/\mathbb{Z}_p$. The function D_2 is labeled as such to suggest a dilogarithm.

Theorem 1.67 ([Kim10, BKK11])**.** *Suppose P is a point of infinite order in $\mathcal{E}(\mathbb{Z})$. Then $\mathcal{X}(\mathbb{Z}) \subseteq \mathcal{E}(\mathbb{Z})$ is in the zero set of*

$$f(z) = (\log(P))^2 D_2(z) - (\log(z))^2 D_2(P),$$

or in other words, $\frac{D_2(z)}{(\log(z))^2}$ is constant on integral points.

We will return to this result and discuss how it is related to p-adic height pairings in the following section.

2. p-adic heights on Jacobians of curves

From a computational point of view, the main idea of quadratic Chabauty is to replace the *linear* relations that make it possible to cut out rational points among p-adic points in the method of Chabauty–Coleman by *bilinear* relations. This can be achieved using the theory of p-adic heights, developed in various degrees of generality by Bernardi [Ber81], Néron [Nér76], Perrin-Riou [PR83], Schneider [Sch82], Mazur–Tate [MT83], Zarhin [Zar90], Iovita–Werner [IW03], Coleman–Gross [CG89], and Nekovář [Nek93].

Most of these constructions are quite similar to constructions of the real valued (or Néron-Tate) height pairing. Recall that this is a symmetric bilinear pairing $A(K) \times A(K) \to \mathbb{R}$, where A is an abelian variety over a global field K, such that the associated quadratic form $\hat{h}\colon A(K) \to \mathbb{R}$ satisfies the Northcott property: for all real numbers B the set of points $P \in A(K)$ such that $\hat{h}(P) < B$ is finite. The latter property has no analogue in the p-adic world, but the bilinearity carries over.

2.1. p-adic heights on elliptic curves.

We begin with a discussion of p-adic heights on elliptic curves defined over the rationals, following the work of Mazur–Stein–Tate [MST06]. In this context already, we can see a hint of some objects that will show up in explicit quadratic Chabauty.

Let $E/\mathbb{Q}$ be an elliptic curve, given by a Weierstrass equation with integral coefficients, and let $\mathcal{O}$ be the point at infinity. let $p \geq 5$ be a prime of good ordinary reduction for E. Let $P \in E(\mathbb{Q})$ be a nonzero point. Write

$$P = (x(P), y(P)) = \left(\frac{a(P)}{d(P)^2}, \frac{b(P)}{d(P)^3}\right),$$

where

$$a(P), b(P), d(P) \in \mathbb{Z}, \quad d(P) \geq 1, \quad \gcd(a(P), d(P)) = 1 = \gcd(b(P), d(P)).$$

We call $d(P)$ the *denominator* of P. Suppose that P satisfies two conditions:

(i) P reduces to $\mathcal{O}$ in $E(\mathbb{F}_p)$;
(ii) P reduces to a nonsingular point of $E(\mathbb{F}_\ell)$ for all bad primes ℓ.

Fix a branch $\log_p \colon \mathbb{Q}_p^* \to \mathbb{Q}_p$ of the p-adic logarithm.

Definition 2.1. The *cyclotomic p-adic height* on such a point $P \in E(\mathbb{Q})$ is

$$h(P) = \frac{1}{p} \log_p \left(\frac{\sigma(P)}{d(P)} \right) \in \mathbb{Q}_p,$$

where $\sigma(P)$ is the p-adic sigma function associated to $E/\mathbb{Z}_p$.

Remark 2.2. More generally, p-adic heights depend on a choice of idèle class character, see Remark 2.11. Over $\mathbb{Q}$, up to scalars, this is uniquely determined and is the *cyclotomic* character.

Mazur and Tate gave 11 different characterizations of the p-adic sigma function [MT91]. We will describe one characterization, which is particularly useful for computations.

Let $x(t) = t^{-2} + \cdots \in \mathbb{Z}_p((t))$ be x in the formal group of $E/\mathbb{Z}_p$; then $y(t) = t^{-3} + \cdots \in \mathbb{Z}_p((t))$.

Theorem 2.3 (Mazur–Tate [MT91])**.** *There is exactly one odd*[7]

$$\sigma(t) = t + \cdots \in t\,\mathbb{Z}[\![t]\!].$$

and constant $c \in \mathbb{Z}_p$ that together satisfy the p-adic differential equation:

$$x(t) + c = -\frac{d}{\omega}\left(\frac{1}{\sigma} \frac{d\sigma}{\omega} \right),$$

where ω is the invariant differential associated to the chosen Weierstrass model for E

$$\omega = \frac{dx}{2y + a_1 x + a_3}, \quad \textit{and } c = \frac{a_1^2 + 4a_2 - \mathbf{E}_2(E, \omega)}{12}.$$

We will return to $\mathbf{E}_2(E,\omega)$ in a bit.

Lemma 2.4. *The height function h extends uniquely to the full Mordell-Weil group $E(\mathbb{Q})$ so that $h(nP) = n^2 h(P)$ for all $n \in \mathbb{Z}$ and $P \in E(\mathbb{Q})$. For $P, Q \in E(\mathbb{Q})$ setting*

$$(P, Q) = h(P) + h(Q) - h(P + Q),$$

we get a symmetric bilinear pairing on $E(\mathbb{Q})$.

To compute $h(Q)$ for arbitrary $Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, let $n_1 = \#E(\mathbb{F}_p)$ and $n_2 = \operatorname{lcm}(\{c_v\})$, where the c_v are the Tamagawa numbers. Let $n = \operatorname{lcm}(n_1, n_2)$. Then $P := nQ$ satisfies (i) and (ii) needed earlier, so we may compute $h(P) = h(nQ)$, and then

$$h(Q) = \frac{1}{n^2} h(nQ) = \frac{1}{n^2} h(P).$$

One reason why the p-adic height is interesting is that, in analogy with canonical height, one can define the p-adic regulator Reg_p of $E/\mathbb{Q}$ as the determinant of the matrix of pairings on $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$. Then the p-adic regulator fits into a p-adic Birch and Swinnerton-Dyer conjecture. The simplest instance of this is as follows:

Conjecture 2.5 (Mazur–Tate–Teitelbaum [MTT86])**.** *Suppose E has good ordinary reduction at p. Let $\mathcal{L}_p(E, T)$ be the p-adic L-function attached to $E/\mathbb{Q}$. Then we have*

(1)

$$\operatorname{ord}_{T=0} \mathcal{L}_p(E, T) = \operatorname{rk} E(\mathbb{Q})$$

[7] By odd, we mean that $\sigma(I(t)) = -\sigma(t)$ where $I(t) = -t - a_1 t^2 + \cdots$ is the formal inverse law.

(2) The leading coefficient $\mathcal{L}_p^*(E,0)$ of the expansion of the p-adic L-function at $T=0$ satisfies the following:

$$\mathcal{L}_p^*(E,0) = \frac{\epsilon_p \prod_v c_v |\text{Ш}(E/\mathbb{Q})| \operatorname{Reg}_p}{(\#E(\mathbb{Q})_{\text{tors}})^2}$$

where $\epsilon_p = (1-\alpha^{-1})^2$, and α is the unit root of $x^2 - a_p x + p = 0$.

Remark 2.6. For numerical methods for the computation of the quantities appearing in the conjecture and applications, see the work of Stein–Wuthrich [SW13].

Remark 2.7. For a precision analysis of computation of p-adic heights on elliptic curves, see the work of Harvey [Har08, Theorem 3].

Example 2.8. Both `SageMath` and `Magma` have implementations of p-adic heights on elliptic curves over $\mathbb{Q}$ for good ordinary primes $p \geq 5$ (with `SageMath` more generally handling semistable reduction). Beware that the normalizations[8] may be slightly different! In `SageMath`, the normalization[9] is chosen for the p-adic Birch–Swinnerton-Dyer conjecture to hold as stated in [MTT86], so differs from [MST06] by a factor of $2p$:

```
sage: E = EllipticCurve([1,1])
sage: p = 5
sage: h = E.padic_height(p,8)
sage: P = E(0,1)
sage: for i in range(1,4):
....:     1/i^2*h(i*P)
....:
2*5 + 4*5^3 + 4*5^4 + 5^6 + 5^7 + O(5^8)
2*5 + 4*5^3 + 4*5^4 + 5^6 + 5^7 + O(5^8)
2*5 + 4*5^3 + 4*5^4 + 5^6 + 5^7 + O(5^8)
```

`Magma`'s normalization[10] is that of [Har08] and is $2p$ (or $-2p$ in some cases) times that in other papers. In this example, it differs from `SageMath` by a sign:

```
> E:=EllipticCurve([1,1]);
> P:=E![0,1];
> pAdicHeight(P,5);
1480998027523*5 + O(5^20)
```

Using the Northcott property, it is easy to see that the canonical height of a point $P \in E(\mathbb{Q})$ vanishes if and only if P is torsion. Similarly, we have

Conjecture 2.9 (Schneider [Sch82])**.** *The cyclotomic p-adic height pairing is nondegenerate. Equivalently,* Reg_p *is nonzero.*

For elliptic curves with complex multiplication, Bertrand [Ber75] proved using p-adic transcendence theory that the p-adic height of a non-torsion point is nonzero, which proves Schneider's conjecture if the curve has rank 1, but this is still all we know.

[8] This is something to be aware of regarding the literature on heights as well.

[9] http://doc.sagemath.org/html/en/reference/curves/sage/schemes/elliptic_curves/ell_rational_field.html

[10] https://magma.maths.usyd.edu.au/magma/handbook/text/1485#16955

Remark 2.10. It is also of interest to study the p-adic height in families of elliptic curves, as initiated by Wuthrich [Wut04], who used this to derive interesting results in view of Schneider's conjecture. Recently, Bianchi [Bia19b] gave an algorithm using p-adic cohomology to compute p-adic heights in families of elliptic curves.

To complete our construction of the p-adic height, we now discuss how to compute the special value $\mathbf{E}_2(E,\omega)$. Katz [Kat73, App. 2] gives an interpretation to $\mathbf{E}_2(E,\omega)$ as the "direction" of the unit root eigenspace W of Frobenius acting on Monsky–Washnitzer cohomology for E. Fix an affine model for $E/\mathbb{Z}_p$ of the form $y^2 = f(x)$ and let ϕ^* be the usual lift of p-power Frobenius from the residue field acting with respect to the basis of $\mathrm{H}^1_{\mathrm{MW}}(E')^-$ given by $\left\{\frac{dx}{y}, \frac{xdx}{y}\right\}$.

Let

$$(\phi^*)^n\left(x\frac{dx}{y}\right) = a_n\frac{dx}{y} + b_n\frac{xdx}{y}.$$

Then we have

$$\mathbf{E}_2(E,\omega) \equiv \frac{-12a_n}{b_n} \pmod{p^n}.$$

What does this have to do with integral points on E? Here is a rough idea. We fix an affine minimal model for $E/\mathbb{Z}_p$ of the form $y^2 = f(x)$ and recall the p-adic differential equation satisfied by the p-adic sigma function:

$$x + c = -\frac{d}{\omega}\left(\frac{1}{\sigma}\frac{d\sigma}{\omega}\right),$$

in the formal group of $E/\mathbb{Z}_p$. Rewriting, we have

$$\omega(x+c) = -d\left(\frac{1}{\sigma}\frac{d\sigma}{\omega}\right),$$

and letting $\omega_0 := \omega$ and $\omega_1 := x\omega$, this implies that

$$\begin{aligned} \int(\omega_1 + c\omega_0) &= -\frac{d\sigma}{\sigma\omega_0}, \\ \omega_0\int(\omega_1 + c\omega_0) &= -\frac{d\sigma}{\sigma} = -d\log\sigma \\ \int(\omega_0\omega_1 + c\omega_0\omega_0) &= -\log\sigma. \end{aligned}$$

Since

$$\int\omega_0\omega_1 = D_2$$

and

$$c\int\omega_0\omega_0 = \frac{c}{2}\left(\int\omega_0\right)^2 = \frac{c}{2}(\log)^2,$$

it follows that

$$D_2 + \frac{c}{2}(\log)^2 = -\log\sigma. \tag{15}$$

Now suppose we may interpret the left hand side of (15) as a Coleman function. Note that the right hand side of (15) is essentially the global p-adic height without a denominator contribution. Then in the case of a rank 1 elliptic curve, if we are able to impose hypotheses (say we restrict to considering integral points and curves with Tamagawa product 1) under which the denominator does not contribute, we have that the right hand side is further equal to $\alpha(\log)^2$ for some computable constant α. Thus we have that

$$\frac{D_2}{(\log)^2}$$

is constant, which would give Theorem 1.67. Of course, one needs to be more careful at various points of this sketch, but this is essentially our first approach toward a fragment of the quadratic Chabauty method (for integral points on rank 1 elliptic curves), as given by Balakrishnan–Besser [BB15]. To say more, we introduce p-adic heights on Jacobians of curves.

2.2. **p-adic heights on Jacobians of curves.** Let $X/\mathbb{Q}$ be a nice curve with genus $g \geq 1$, and p be a prime of good reduction for X. As above, we fix a branch $\log_p\colon \mathbb{Q}_p^* \to \mathbb{Q}_p$. We also fix the following data:

(a) an idèle class character $\chi\colon \mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q}^* \to \mathbb{Q}_p$ (see Remark 2.11 below),
(b) a splitting s of the Hodge filtration on $\mathrm{H}^1_{\mathrm{dR}}(X/\mathbb{Q}_p)$ such that $\ker(s)$ is isotropic with respect to the cup product pairing.

Remark 2.11. Here we mention briefly the role of idèle class characters. More generally, suppose X is a nice curve defined over a number field K. An *idèle class character*

$$\chi = \sum_v \chi_v : \mathbb{A}_K^*/K^* \to \mathbb{Q}_p$$

is a continuous homomorphism that decomposes as a sum of local characters χ_v. Below are some properties:

- For any prime $\mathfrak{q} \nmid p$ we have $\chi_{\mathfrak{q}}(\mathcal{O}_{K_{\mathfrak{q}}}^*) = 0$ because of continuity. So if $\pi_{\mathfrak{q}}$ is a uniformizer in $K_{\mathfrak{q}}$, then $\chi_{\mathfrak{q}}$ is completely determined by $\chi_{\mathfrak{q}}(\pi_{\mathfrak{q}})$.
- For any $\mathfrak{p} \mid p$, there is a $\mathbb{Q}_p$-linear map $t_{\mathfrak{p}}^{\chi}$ such that we can decompose

(16)
$$\begin{tikzcd} \mathcal{O}_{\mathfrak{p}}^* \arrow[rr, "\chi_{\mathfrak{p}}"] \arrow[dr, "\log_{\mathfrak{p}}"'] & & \mathbb{Q}_p, \\ & K_{\mathfrak{p}} \arrow[ur, "t_{\mathfrak{p}}^{\chi}"'] & \end{tikzcd}$$

because $\chi_{\mathfrak{p}}$ takes values in the torsion-free group $(\mathbb{Q}_p, +)$.

If a continuous idèle class character χ is ramified at $\mathfrak{p}$, that is, if the local character $\chi_{\mathfrak{p}}$ does not vanish on $\mathcal{O}_{\mathfrak{p}}^*$, then we can extend $\log_{\mathfrak{p}}$ to

$$\log_{\mathfrak{p}}\colon K_{\mathfrak{p}}^* \to K_{\mathfrak{p}}$$

in such a way that the diagram (16) remains commutative.

Remark 2.12. A splitting of the Hodge filtration on $\mathrm{H}^1_{\mathrm{dR}}(X/\mathbb{Q}_p)$ corresponds to fixing a subspace $W := \ker(s)$ of $\mathrm{H}^1_{\mathrm{dR}}(X/\mathbb{Q}_p)$ complementary to the space of holomorphic forms $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)$, i.e.

$$\mathrm{H}^1_{\mathrm{dR}}(X/\mathbb{Q}_p) = \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1) \oplus W.$$

The isotropy condition on W is necessary in order to obtain a symmetric height pairing below.

In this subsection, we will construct a height pairing h on the Jacobian J of X. Everything can be generalized to number fields K, making choices as above.

Definition 2.13. (Coleman–Gross [CG89]) The (cyclotomic) *p-adic height pairing* is a symmetric bi-additive pairing

$$\operatorname{Div}^0(X) \times \operatorname{Div}^0(X) \to \mathbb{Q}_p,\ (D_1, D_2) \mapsto h(D_1, D_2),$$

for $D_1, D_2 \in \operatorname{Div}^0(X)$ with disjoint support, such that the following holds:

(i) We have

$$\begin{aligned} h(D_1, D_2) &= \sum_{\text{finite primes } v} h_v(D_1, D_2) \\ &= h_p(D_1, D_2) + \sum_{\ell \neq p} h_\ell(D_1, D_2) \\ &= \int_{D_2} \omega_{D_1} + \sum_{\ell \neq p} m_\ell \log_p \ell, \end{aligned}$$

where the integral is a Coleman integral, the sum is finite and $m_v \in \mathbb{Q}$ is an intersection multiplicity.

(ii) For $\beta \in \mathbb{Q}(X)^*$, we have

$$h(D, \operatorname{div}(\beta)) = 0.$$

By (ii), h defines a symmetric bilinear pairing $J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p$.

This construction of the p-adic height is similar to the Arakelov-theoretic description of the canonical height due to Faltings and Hriljac.

2.2.1. *Local heights at p.* We will now provide more detail on the local height pairings h_v, beginning with the case $v = p$, as described by Coleman–Gross [CG89] and computed by Balakrishnan–Besser in the case of hyperelliptic curves [BB12, BB19].

We first discuss the construction of the differential ω_{D_1} in (i). Let $\{\omega_0, \cdots, \omega_{2g-1}\}$ be a basis for $\mathrm{H}^1_{\mathrm{dR}}(X)$ with $\{\omega_0, \cdots, \omega_{g-1}\} \in \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)$. Fix a lift ϕ of Frobenius.

Let $T(\mathbb{Q}_p)$ be the group of differentials of the third kind on X. In this section, we take this to mean something stronger than in the previous section: that they have at most simple poles and *integer* residues.

We have a residue divisor homomorphism

$$\operatorname{Res} : T(\mathbb{Q}_p) \to \operatorname{Div}^0(X),\ \omega \mapsto \operatorname{Res}(w) = \sum_P (\operatorname{Res}_P \omega) P,$$

which induces a short exact sequence

$$0 \to \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1) \to T(\mathbb{Q}_p) \overset{\operatorname{Res}}{\to} \operatorname{Div}^0(X) \to 0. \tag{17}$$

The differential ω_{D_1} will be a differential of the third kind with $\operatorname{Res}(\omega_{D_1}) = D_1$. Here is an example:

Example 2.14. Suppose that X is a hyperelliptic curve with affine model $y^2 = f(x)$, and D_1 is the divisor $(P) - (Q)$ with non-Weierstrass points $P, Q \in X(\mathbb{Q})$. We want to write down a differential ω having simple poles with residues $+1$ at P and -1 at Q respectively, and no other poles. For example,

$$\omega = \frac{dx}{2y}\left(\frac{y + y(P)}{x - x(P)} - \frac{y + y(Q)}{x - x(Q)}\right) \tag{18}$$

has residue divisor equal to D_1, as desired. However, adding any holomorphic differential η to ω, and taking the residue divisor map of $\eta + \omega$ will again give us D_1, as we can see by (17). So we must make some choice, which we do below.

We can fix a normalized differential with a given residue divisor using the complementary subspace W mentioned above. For this, let $T_l(\mathbb{Q}_p)$ denote the group of logarithmic differentials $\frac{df}{f}$ with $f \in \mathbb{Q}_p(X)^*$. Since

$$T_l(\mathbb{Q}_p) \cap \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1) = 0$$

and $\mathrm{Res}\frac{df}{f} = \mathrm{div} f$, from the short exact sequence (17) we get a new short exact sequence

$$0 \to \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1) \to T(\mathbb{Q}_p)/T_l(\mathbb{Q}_p) \to J(\mathbb{Q}_p) \to 0.$$

Proposition 2.15. *There is a canonical homomorphism*

$$\Psi : T(\mathbb{Q}_p)/T_l(\mathbb{Q}_p) \to \mathrm{H}^1_{\mathrm{dR}}(X)$$

with the following properties:

(1) Ψ is the identity on differentials of the first kind;
(2) Ψ sends third kind differentials to second kind modulo exact differentials.

Proof. See [CG89, §2]. □

Definition 2.16. Let $D \in \mathrm{Div}^0(X)$. Then we define ω_D to be the unique differential of the third kind with $\mathrm{Res}(\omega_D) = D$ and $\Psi(\omega_D) \in W$.

In fact, Ψ can be extended to general meromorphic (and even rigid analytic) forms. Having fixed our normalized differential ω_D, we can now define:

Definition 2.17. The local height at p of $D_1, D_2 \in \mathrm{Div}^0(X)$ with disjoint support is

$$h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}$$

As in Section 2.1, we can take W to be the unit root subspace if p is ordinary. It can be computed as follows:

Proposition 2.18. *If ϕ is a lift of Frobenius, then $\{(\phi^*)^n\omega_g, \cdots, (\phi^*)^n\omega_{2g-1}\}$ is a basis for the unit root subspace modulo p^n.*

For the following algorithm, recall that $\mathrm{H}^1_{\mathrm{dR}}(X/\mathbb{Q}_p)$ is equipped with the cup product: a canonical, alternating, non-degenerate bilinear form, which we compute using Serre's formula:

$$\begin{aligned} \mathrm{H}^1_{\mathrm{dR}}(X/\mathbb{Q}_p) \times \mathrm{H}^1_{\mathrm{dR}}(X/\mathbb{Q}_p) &\to \mathbb{Q}_p \\ ([\mu_1], [\mu_2]) &\mapsto [\mu_1 \cup \mu_2] = \sum_{Q \in X(\mathbb{C}_p)} \mathrm{Res}_Q\left(\mu_2 \int \mu_1\right). \end{aligned}$$

Remark 2.19. Note that since μ_2 is of the second kind, it has residue zero everywhere, and so the result above does not depend on a choice of constant of integration for $\int \mu_1$.

Algorithm 2.20 (Coleman integral of differentials of the third kind [BB12])**.**
Input:

- A differential ω with $\mathrm{Res}(\omega) = (P) - (Q)$ such that $P, Q \in X(\mathbb{Q}_p)$ are non-Weierstrass points.
- Points $R, S \in X(\mathbb{Q}_p)$ such that R, S do not lie in residue disk of P, Q.

Output: The integral $\int_S^R \omega$.

(1) Compute $\Psi(\omega) \in \mathrm{H}^1_{\mathrm{dR}}(X)$: suppose $\Psi(\omega) = \sum_{i=0}^{2g-1} b_i[\omega_i]$. Then by taking the cup products $\Psi(\omega)\cup[\omega_j]$ for all j, one can solve for the coefficients b_i by computing residues. Let $\alpha := \phi^*\omega - p\omega$. Use Frobenius equivariance to get

$$\Psi(\alpha) = \phi^*\Psi(\omega) - p\Psi(\omega).$$

(2) Let β be a 1-form with $\mathrm{Res}(\beta) = (R) - (S)$. Compute $\Psi(\beta)$.
(3) Compute $\Psi(\alpha)\cup\Psi(\beta)$. (This is easy, since both are elements in $\mathrm{H}^1_{\mathrm{dR}}(X)$ that we have computed.)
(4) Compute $\int_{\phi(S)}^{S} \omega$ and $\int_{R}^{\phi(R)} \omega$. (These are tiny integrals.)
(5) Compute $\sum_{A\in X(\mathbb{C}_p)} \mathrm{Res}_A\left(\alpha \int \beta\right)$. (This is more involved since there are more poles that are not defined over $\mathbb{Q}_p$.)
(6) Finally, we get

$$\int_S^R \omega = \frac{1}{1-p}(\Psi(\alpha)\cup\Psi(\beta) + \sum_{A\in X(\mathbb{C}_p)} \mathrm{Res}_A\left(\alpha\int\beta\right) - \int_{\phi(S)}^{S}\omega - \int_{R}^{\phi(R)}\omega).$$

Remark 2.21. We introduce this auxiliary differential α in Step (1) above, because α is almost of the second kind, meaning that the sum of residues of α in each annulus in 0.

Algorithm 2.22 (The local height at p of the global p-adic height, $h_p(D_1, D_2)$ [BB12]).

(1) Let ω be a differential in $T(\mathbb{Q}_p)$ with $\mathrm{Res}(\omega) = D_1$.
(2) Compute $\Psi(\omega) = \sum_{i=0}^{2g-1} a_i\omega_i \in \mathrm{H}^1_{\mathrm{dR}}(X)$. Then $\Psi(\omega) - \sum_{i=0}^{g-1} a_i\omega_i \in W$. Let

$$\omega_{D_1} = \omega - \sum_{i=0}^{g-1} a_i\omega_i.$$

(3) Compute using Algorithm 2.20

$$h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}.$$

Remark 2.23. For the precision needed in Algorithm 2.22, see [BB12, §6.2].

Example 2.24 ([BBM17, Example 9.2]). Consider the genus 3 curve

$$X : y^2 = (x^3 + x + 1)(x^4 + 2x^3 - 3x^2 + 4x + 4).$$

This is a new modular curve C^J_{496} studied by Baker–González-Jiménez–González–Poonen [BGJGP05]. For this curve, $J(\mathbb{Q}) \simeq \mathbb{Z}^3 \oplus \mathbb{Z}/2$. Let $P = (-1, 2), Q = (0, 2), R = (-2, 12), S = (3, 62)$ and let w denote the hyperelliptic involution.

We take $p = 7$ and use Algorithm 2.22 to compute the local height $h_7(D_2, D_3)$ where $D_2 = (S) - (w(Q))$ and $D_3 = (w(S)) - (R)$. Let ω be the differential (18) constructed in Example 2.14 using residue divisor D_2. Using Algorithm 2.20, we find

$$\int_{D_3} \omega = 7 + 4\cdot 7^2 + 6\cdot 7^3 + 7^4 + 3\cdot 7^5 + 3\cdot 7^6 + 3\cdot 7^7 + O(7^{10}).$$

Let $\eta := \sum_{i=0}^{2} a_i\omega_i$ where $\Psi(\omega) = \sum_{i=0}^{5} a_i\omega_i$. We calculate that

$$\begin{aligned}\eta = {} & (4 + 5\cdot 7 + 2\cdot 7^2 + 2\cdot 7^3 + 5\cdot 7^4 + 5\cdot 7^5 + 2\cdot 7^8 + 7^9 + O(7^{10}))\omega_0 + \\ & (1 + 4\cdot 7 + 6\cdot 7^2 + 7^3 + 6\cdot 7^4 + 5\cdot 7^6 + 5\cdot 7^7 + 3\cdot 7^8 + 7^9 + O(7^{10}))\omega_1 + \\ & (5 + 7 + 2\cdot 7^2 + 6\cdot 7^3 + 7^4 + 4\cdot 7^6 + 2\cdot 7^7 + 3\cdot 7^8 + 5\cdot 7^9 + O(7^{10}))\omega_2,\end{aligned}$$

and using Algorithm 1.36, we find

$$\int_{D_3} \omega_0 = 2\cdot 7 + 4\cdot 7^2 + 7^3 + 6\cdot 7^4 + 7^5 + 5\cdot 7^6 + 7^7 + 5\cdot 7^8 + 4\cdot 7^9 + O(7^{10})$$
$$\int_{D_3} \omega_1 = 4\cdot 7 + 4\cdot 7^2 + 3\cdot 7^3 + 2\cdot 7^4 + 6\cdot 7^5 + 4\cdot 7^6 + 2\cdot 7^7 + 5\cdot 7^8 + O(7^{10})$$
$$\int_{D_3} \omega_2 = 7^2 + 3\cdot 7^3 + 3\cdot 7^4 + 3\cdot 7^5 + 5\cdot 7^6 + 3\cdot 7^7 + 7^8 + 4\cdot 7^9 + O(7^{10}),$$

so we have

$$\int_{D_3} \eta = 5\cdot 7 + 3\cdot 7^2 + 3\cdot 7^3 + 4\cdot 7^4 + 6\cdot 7^5 + 7^6 + 7^7 + 6\cdot 7^8 + 4\cdot 7^9 + O(7^{10}).$$

Putting this together, we have

$$h_7(D_2, D_3) = \int_{D_3} \omega - \int_{D_3} \eta = 3\cdot 7 + 3\cdot 7^3 + 4\cdot 7^4 + 3\cdot 7^5 + 7^6 + 2\cdot 7^7 + 7^8 + 4\cdot 7^9 + O(7^{10}).$$

Likewise we may compute $h_7(D_3, D_2) = \int_{D_2} \omega_{D_3}$ and numerically verify that $h_7(D_2, D_3) = h_7(D_3, D_2)$.

Using SageMath code available on GitHub [Bal], here is how to compute the above values:

```
R.<x> = QQ[]
X = HyperellipticCurve((x^3+x+1)*(x^4 +2*x^3-3*x^2+4*x+4))
p = 7
K = Qp(p,10)
XK = X.change_ring(K)
S = XK(3,62)
iS = XK(3,-62)
iQ = XK(0,-2)
R = XK(-2,12)
XK.height([(1,S),(-1,iQ)],[(1,iS),(-1,R)])
XK.height([(1,iS),(-1,R)],[(1,S),(-1,iQ)])
```

Remark 2.25. Forthcoming work of Gajović will give an extension of Algorithm 2.22 to more general nice curves, based on Tuitman's algorithm. The main issue is the computation of the normalized differential ω_D.

Remark 2.26. The construction of Coleman–Gross local heights can be extended to curves with bad reduction, replacing Coleman integration with Vologodsky integration; see for instance [Bes17]. Kaya is currently working on an extension of Algorithm 2.22 to hyperelliptic curves with semistable reduction.

Since the global p-adic height respects linear equivalence, it can be extended to pairs of divisors with common support. The local height pairings can also be extended in a non-canonical way. We first discuss this for the pairing at p. This uses the following idea of Gross [Gro86]. At each point x in the common support of our divisors, choose a basis $t := t_x$ of the tangent space. Let $z := z_x$ be a uniformizing parameter at x with $\partial_t z = 1$. Any rational function f on $X_{\mathbb{Q}_p}$ then has a well-defined value at x,

$$f[x] = \frac{f}{z^m}(x),$$

where m is the order of f at x. This depends only on t, but not on z.

For an odd degree hyperelliptic curve, we will let ω_i be $\frac{x^i dx}{2y}$ and we let $\overline{\omega}_i$ denote the dual of ω_i with respect to the cup product pairing.

Proposition 2.27 ([BB15])**.** *Let $X/\mathbb{Q}$ be a hyperelliptic curve given by a monic odd degree model. Then there is a natural choice of tangent vectors such that the local height $h_p(P-\infty, P-\infty)$ can be written as a double integral*

$$h_p(P-\infty, P-\infty) = -2\sum_{i=0}^{g-1}\int_b^P \omega_i\overline{\omega}_i,$$

where b is a tangential base point at ∞.

The proof uses p-adic Arakelov theory, as developed by Besser [Bes05]. In this theory, the local height is given by a p-adic Green function. One shows equality in the proposition by first computing the curvature of this p-adic Green function, then proving that the two values are the same up to a constant which one can then show to be 0.

As a consequence, we have that

$$\theta(z) := h_p((z)-(\infty),(z)-(\infty))$$

extends to a locally analytic function on $X(\overline{\mathbb{Q}}_p)\setminus\{\infty\}$, where we fix the choice of tangent vectors as in Proposition 2.27.

2.3. An application to integral points.

For certain curves, we can use p-adic heights to study integral points.

Theorem 2.28 (Quadratic Chabauty for integral points on hyperelliptic curves [BBM16, Theorem 3.1])**.** *Let $f(x)\in\mathbb{Z}[x]$ be a monic separable polynomial of degree $2g+1\geq 3$. Let $\mathscr{U} = \operatorname{Spec}(\mathbb{Z}[x,y]/(y^2-f(x))$ and let X be the normalization of the projective closure of the generic fiber of $\mathscr{U}$. Let J be the Jacobian of X and assume that $\operatorname{rk} J(\mathbb{Q}) = g$. Choose a prime p of good reduction and suppose that $\log\colon J(\mathbb{Q})\otimes\mathbb{Q}_p \to \mathrm{H}^0(X_{\mathbb{Q}_p},\Omega^1)^*$ is an isomorphism*[11]*. Then there exist explicitly computable constants $\alpha_{ij}\in\mathbb{Q}_p$ such that the function*

$$\rho(z) = \theta(z) - \sum_{0\leq i\leq j\leq g-1}\alpha_{ij}\int_\infty^z\omega_i\int_\infty^z\omega_j$$

takes values in an explicitly computable finite set $S\subset\mathbb{Q}_p$ for all z in $\mathscr{U}(\mathbb{Z}[\frac{1}{p}])$.

Proof. The key idea is that the global height $h((P)-(\infty),(P)-(\infty))$ can be decomposed in two ways:

(i) Because of the assumption on log, and since the global height h is a symmetric bilinear pairing we can find $\alpha_{ij}\in\mathbb{Q}_p$ such that for all $P\in X(\mathbb{Q})$ we have

$$h((P)-(\infty),(P)-(\infty)) = \sum\alpha_{ij}\int_\infty^P\omega_i\int_\infty^P\omega_j,$$

and this extends to a locally analytic function on $X(\bar{\mathbb{Q}}_p)$ away from the residue disk at infinity.

(ii) We have

$$h((P)-(\infty),(P)-(\infty)) = \theta(P) + \sum_{\ell\neq p}h_\ell(P-\infty,P-\infty).$$

[11] If this fails, we can simply use Chabauty–Coleman to compute the rational points.

Hence we deduce

$$\rho(P) = \sum_{\ell \neq p} h_\ell(P - \infty, P - \infty)$$

for all $P \in X(\mathbb{Q})$. The proof of the theorem now follows from

Proposition 2.29 ([BBM16, Proposition 3.3])**.** *Let $\ell \neq p$ be prime. There is a proper regular model $\mathcal{X}$ of $X \otimes \mathbb{Q}_\ell$ over $\mathbb{Z}_\ell$ such that if $z \in X(\mathbb{Q}_\ell)$ is integral then $h_\ell((z) - (\infty), (z) - (\infty))$ depends solely on the component of the special fiber $\mathcal{X}_\ell$ that the section in $\mathcal{X}(\mathbb{Z}_\ell)$ corresponding to z intersects, and is explicitly computable. If the sections corresponding to z and ∞ intersect the same component, then the local height is 0.*

We will not prove this here, but see Section 2.3.1 below. □

As a special case of Theorem 2.28, we have the following extension of Theorem 1.67.

Corollary 2.30. *Let f, p, $\mathscr{U}$ and X satisfy the conditions of Theorem 2.28. Suppose that there exists a regular model $\mathcal{X}\,/\,\mathbb{Z}$ of X such that, for every bad prime ℓ, all $\mathbb{Q}_\ell$-rational points on X reduce to the same irreducible component of the special fiber of $\mathcal{X} \times \mathbb{Z}_\ell$. Then there exists explicitly computable constants $\alpha_{ij} \in \mathbb{Q}_p$ such that the function*

$$\rho(z) = \theta(z) - \sum_{0 \leq i \leq j \leq g-1} \alpha_{ij} \int_\infty^z \omega_i \int_\infty^z \omega_j$$

vanishes on $\mathscr{U}(\mathbb{Z}[\frac{1}{p}])$.

We can use Theorem 2.28 to compute the integral points on a curve X satisfying the conditions in practice. We give some more computational details here; for more, see [BBM17]. For an extension to number fields, see [BBBM19]. For $P \in J(\mathbb{Q}_p)$ and $i \in \{0, \dots, g-1\}$, we set $f_i(P) := \int_0^P \omega_i$; then $f_0, \dots, f_{g-1}$ restrict to linearly independent functionals on $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ by assumption.

Algorithm 2.31 (The set of integral points on a curve $X/\mathbb{Q}$ satisfying the assumptions of Theorem 2.28)**.**

(1) Let $D_1, \dots, D_g \in \mathrm{Div}^0(X)$ be representatives of a basis for $J(\mathbb{Q}) \otimes \mathbb{Q}$. Then compute the global height pairings $h(D_i, D_j)$. A basis for the space of bilinear forms on $J(\mathbb{Q}) \otimes \mathbb{Q}$ is given by $1/2(f_k f_\ell + f_\ell f_k)$ so compute $1/2(f_k(D_i)f_\ell(D_j) + f_\ell(D_i)f_k(D_j))$ and do linear algebra to compute $\alpha_{k\ell}$:

$$h(D_i, D_j) = \sum_{k,\ell < g-1} \alpha_{k\ell}(1/2(f_k(D_i)f_\ell(D_j) + f_\ell(D_i)f_k(D_j))).$$

(2) In order to compute $\{\overline{\omega}_i\}$ for $0 \leq i \leq g-1$ such that $[\overline{\omega}_i] \cup [\omega_j] = \delta_{ij}$ we proceed as follows:
   (i) Compute a splitting of $H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p}) = \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1) \oplus W$, isotropic with respect to the cup product. For instance, when p is ordinary we can take W to be the unit root eigenspace of Frobenius. In this case, modulo p^n, we have a basis for W is given by $\{(\phi^*)^n \omega_g, \dots, (\phi^*)^n \omega_{2g-1}\}$.
   (ii) For $j = 0, \dots, g-1$, let $\widetilde{\omega_j}$ be a projection on W along $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)$, i.e., $\widetilde{\omega_j} = \omega_j - \sum_{i=0}^{g-1} a_i \omega_i$ for some $a_i \in \mathbb{Q}_p$.
   (iii) Use the cup product matrix to compute

$$\overline{\omega}_j = \sum_{i=g}^{2g-1} b_{ji} \widetilde{\omega_i}$$

for $j = 0$ to $g-1$.

(3) Expand $\theta(z) := -2\sum_{i=0}^{g-1}\int \omega_i\overline{\omega}_i$ into a power series in each residue disk D not containing ∞, compute a $\mathbb{Z}_p$-point $P \in D$, the value $\theta(P)$, and a local coordinate z_P at P. Then
$$\theta(z) = -2\sum_{i=0}^{g-1}\int_b^{g-1} \omega_i\overline{\omega}_i = -2\left(\sum_{i=0}^{g-1}\int_b^{P} \omega_i\overline{\omega}_i + \sum_{i=0}^{g-1}\int_P^{z_P} \omega_i\overline{\omega}_i + \sum_{i=0}^{g-1}\int_P^{z_P} \omega_i \int_b^{P} \overline{\omega}_i\right)$$
which is equal to
$$\theta(P) - 2\left(\sum_{i=0}^{g-1}\int_P^{z_P} \omega_i\overline{\omega}_i + \sum_{i=0}^{g-1}\int_P^{z_P} \omega_i \int_b^{P} \overline{\omega}_i\right),$$
where b is a tangential basepoint at infinity.

(4) Use intersection theory to compute the finite set S_ℓ of possible values of $h_\ell((z)-(\infty),(z)-(\infty))$ for bad primes ℓ and integral $X(\mathbb{Q}_\ell)$. Obtain a finite set $S \subset \mathbb{Q}_p$ such that $\sum_{\ell\neq p} h_\ell(P-\infty, P-\infty) \in S$ for $P \in \mathscr{U}(\mathbb{Z}[\frac{1}{p}])$.

(5) Now proceed similar to the classical Chabauty–Coleman method: We can expand ρ in each disk, set it equal to each value in S, solve for all $z \in \mathscr{U}(\mathbb{Z}_p)$ such that $\rho(z) \in S$. Take the collection of all such points, we will call that solution set $\mathcal{Z}$.

(6) If $\mathcal{Z}$ is strictly larger than the known points in $\mathscr{U}(\mathbb{Z})$, we can run the Mordell-Weil sieve [BS10] (see also Section 5.3.3), possibly after re-running steps (1)-(4) on a collection of good primes p.

2.3.1. *Local heights away from p.* We say a few more words about the local heights at $\ell \neq p$. Given divisors $D_1, D_2 \in \mathrm{Div}^0(X)$ with disjoint support, we can express $h_\ell(D_1, D_2)$ as an intersection multiplicity
$$h_\ell(D_1, D_2) = (\mathcal{D}_1 \cdot \mathcal{D}_2)\chi_\ell(\ell),$$
where $\chi_\ell(\ell) = \log_p(\ell)$, see the beginning of the present subsection. Here $\mathcal{D}_i$ is an extension of D_i to a regular model $\mathcal{X}$ of $X_{\mathbb{Q}_\ell}$ such that $\mathcal{D}_i$ has trivial intersection with all vertical divisors. For instance, we can pick a regular model that dominates the Zariski closure of X. We can extend the local height pairing to divisors with common support via tangent vectors as above. Then we find that for $z \in X(\mathbb{Q}_\ell)$, $h_\ell(z-\infty, z-\infty)$ decomposes into

- terms which only depend on the irreducible component of the special $\mathcal{X}_\ell$ that the section $z_{\mathcal{X}} \in \mathcal{X}(\mathbb{Z}_\ell)$ corresponding to z intersects,
- the intersection multiplicity between $z_{\mathcal{X}}$ and $\infty_{\mathcal{X}}$.

The latter term vanishes if z is integral. In general, it is determined by the denominator of $x(P)$, which is why it's not obvious how to go beyond integral points using this construction.

Example 2.32. In the case of elliptic curves, we have the Mazur–Stein–Tate p-adic height
$$h(P) = \frac{1}{p}\log_p(\sigma(P)) - \frac{1}{p}\log_p(D(P))$$
on a certain finite index subgroup of the Mordell–Weil group, as well as the Coleman–Gross p-adic height
$$h(P-\infty) = h_p(P-\infty) + \sum_{v\neq p}(P-\infty).$$
Extending appropriately, we have $\frac{1}{p}\log(\sigma(P)) = h_p(P-\infty)$ and $-\frac{1}{p}\log_p(D(P)) = \sum_{v\neq p}(P-\infty)$.

To compute local heights h_ℓ for $\ell \neq p$, we need to compute regular models (implemented in `Magma` by Donnelly, see also recent work of Dokchitser [Dok18]) and Gröbner bases of ideals of divisors. For more details, see [Hol12, Mül14, VBHM20].

Example 2.33 ([BBM17, Example 9.2]). Let $X : y^2 = (x^3 + x + 1)(x^4 + 2x^3 - 3x^2 + 4x + 4)$ be the new modular curve C^J_{496} discussed in Example 2.24. Recall that the Mordell–Weil group of the Jacobian is

$$J(\mathbb{Q}) \simeq \mathbb{Z}^3 \oplus \mathbb{Z}/2.$$

Let $P = (-1, 2), Q = (0, 2), R = (-2, 12), S = (3, 62)$. We want to show that up to the hyperelliptic involution w, these are the only integral points. Generators for $J(\mathbb{Q}) \otimes \mathbb{Q}$ are given by $\{P_1 = [P - \infty], P_2 = [S - w(Q)], P_3 = [w(S) - R]\}$. Then the set S in Theorem 2.28 is

$$S = \{a \log_p 2 + b \log_p 31 : a \in \{0, 15/4, 7/4\}, b \in \{0, 1/2\}\}.$$

We can carry out quadratic Chabauty for $p = 7, 17$, and 37 and apply the Mordell-Weil sieve (see Section 5.3.3) to conclude the desired result.

3. Nekovář's p-adic heights

The quadratic Chabauty method uses p-adic heights to cut out rational points on certain nice curves $X/\mathbb{Q}$ using bilinear relations. We showed in Section 2.3 that the construction of Coleman and Gross leads to an algorithm to compute the integral points on certain hyperelliptic curves, and we mentioned why this approach does not extend easily to rational points.

As explained below in Section 4, we will in fact cut out a subset $X(\mathbb{Q}_p)_U \supseteq X(\mathbb{Q})$ of $X(\mathbb{Q}_p)$, depending on a certain non-abelian unipotent quotient U of the $\mathbb{Q}_p$-étale fundamental group of $X_{\overline{\mathbb{Q}}}$. The set $X(\mathbb{Q}_p)_U$ is defined using a non-abelian generalization of Chabauty's method due to Kim, which we briefly summarize in Section 4.1. Kim's philosophy suggests that our construction should not use the geometry of the Jacobian, but rather a "motivic" version (but see Remark 5.5 below). In this section, we recall such a motivic construction of p-adic heights, due to Nekovář [Nek93].

3.1. p-adic Hodge theory.

We begin by briefly recalling some notions from p-adic Hodge theory. A good reference for most of what we need in this section is [Bel09], but [Nek93, §1] recalls the relevant background in a concise way. See [Ber04, And03, BC09] for other accounts of p-adic Hodge theory. In Section 4.1 we will also use results from Olsson's non-abelian p-adic Hodge theory [Ols11].

Fix a prime p. For any prime v, let G_v denote the absolute Galois group of $\mathbb{Q}_v$. Let V be a p-adic Galois representation, by which we mean a finite dimensional $\mathbb{Q}_p$-vector space with a continuous action of G_p. Fontaine defined p-adic period rings $B_{\mathrm{cris}} \subset B_{\mathrm{dR}}$ and functors $D_{\mathrm{cris}}, D_{\mathrm{dR}}$:

$$D_{\mathrm{cris}}(V) = (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)^{G_p}, \quad D_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_p}.$$

We always have

$$\dim_{\mathbb{Q}_p} D_{\mathrm{cris}}(V) \leq \dim_{\mathbb{Q}_p}(V).$$

If equality holds, then we say that V is *crystalline*. Similarly, V is called *de Rham* if

$$\dim_{\mathbb{Q}_p} D_{\mathrm{dR}}(V) = \dim_{\mathbb{Q}_p}(V).$$

If V is crystalline, then it is also de Rham. Note that V is crystalline if it is unramified; in fact the p-adic notion *unramified* is too strong to be useful; the "right" p-adic analogue of the ℓ-adic notion *unramified* turns out to be *crystalline*.

An element $\xi \in \mathrm{H}^1(G_p, V)$ corresponds to an isomorphism class of extension of $\mathbb{Q}_p$ by V

$$0 \to V \to E \to \mathbb{Q}_p \to 0;$$

here ξ is the image of the neutral element of $\mathrm{H}^0(G_p, \mathbb{Q}_p)$ under the connecting homomorphism $\mathrm{H}^0(G_p, \mathbb{Q}_p) \to \mathrm{H}^1(G_p, V)$. We call ξ *crystalline*, provided that the Galois representation E is.

Definition 3.1. The *local Bloch–Kato Selmer group* $\mathrm{H}^1_f(G_p, V)$ be the set of crystalline classes in $\mathrm{H}^1(G_p, V)$. The (global) *Bloch–Kato Selmer group* $\mathrm{H}^1_f(G_{\mathbb{Q}}, V)$ is the group of $\xi \in \mathrm{H}^1(G_{\mathbb{Q}}, V)$ whose image $\mathrm{loc}_v(V) \in \mathrm{H}^1(G_v, V)$ is crystalline for $v = p$ and unramified for all $v \neq p$.

Example 3.2. Suppose that K is a finite extension of $\mathbb{Q}_p$. Then Kummer theory gives an isomorphism

$$\kappa\colon \widehat{K^*} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\simeq} \mathrm{H}^1(G_K, \mathbb{Q}_p(1)),$$

where $\widehat{K^*} = \varprojlim K^* \otimes \mathbb{Z}/p^n\mathbb{Z}$ is the p-adic completion. According to [Bel09, Proposition 2.9], this isomorphism identifies $\mathscr{O}_K^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ with $\mathrm{H}^1_f(G_p, \mathbb{Q}_p(1))$.

Example 3.3. Let K be a number field. Then, by [Bel09, Proposition 2.12] we have

$$\mathrm{H}^1_f(G_K, \mathbb{Q}_p(1)) \simeq \mathscr{O}_K^* \otimes_{\mathbb{Z}} \mathbb{Q}_p\,.$$

Remark 3.4. More generally, when G is a topological group and V, W are finite-dimensional continuous $\mathbb{Q}_p$-representations of G, we can identify $\mathrm{H}^1(G, V^* \otimes W)$ with the group $\mathrm{Ext}^1(V, W)$, and we can define and identify $\mathrm{H}^1_f(G, V^* \otimes W)$ and $\mathrm{Ext}^1_f(V, W)$, where the former contains crystalline torsors and the latter crystalline extensions.

Nekovář's approach is inspired by a motivic construction due to Scholl [Sch94] of archimedean local height pairings arising in Beilinson's extension of canonical heights to Chow groups based on mixed Hodge structures.

3.2. **Nekovář's construction of p-adic heights.** Fix a prime p and a finite set of primes T_0. Let $T := T_0 \cup \{p\}$. For "good"[12] p-adic Galois representations V, Nekovář constructs a bilinear p-adic height pairing on Bloch–Kato Selmer groups

$$h\colon\ \mathrm{H}^1_f(G_{\mathbb{Q}}, V) \times \mathrm{H}^1_f(G_{\mathbb{Q}}, V^*(1)) \to \mathbb{Q}_p\,.$$

This global p-adic height depends only on

(a) the choice of an idèle class character $\chi\colon \mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \to \mathbb{Q}_p$,
(b) a splitting s of the Hodge filtration on $V_{\mathrm{dR}} := D_{\mathrm{cris}}(V)$.

For everything that follows, we let $X/\mathbb{Q}$ denote a nice curve of genus $g \geq 2$ such that X has good reduction at p and such that T_0 contains the set of primes of bad reduction for X. We set $V = \mathrm{H}^1_{\text{ét}}(X_{\overline{\mathbb{Q}}})^*$, This V is "good" in the sense of Nekovář; in particular V is crystalline and $V_{\mathrm{dR}} = \mathrm{H}^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})^*$ by a theorem of Faltings [Fal89]. Note that the choices (a) and (b) are exactly the choices required in the construction of Coleman and Gross.

In [Nek93, Section 2], Nekovář presents a global construction of the height pairing h. We will not discuss it here, but rather focus on a construction of local heights h_v, so that we have

$$h = h_p + \sum_{v \neq p} h_v.$$

See [Nek93, §4] for more details. See also [BDM$^+$19, §3], [BD18a, §4.2] for similar treatments, and a reformulation in terms of non-abelian cohomology. A generalization of Nekovář's construction is discussed in [BD18b].

[12] The conditions for being "good" are spelled out in [Nek93, 2.1.2]. In particular, we want V to be crystalline at p and unramified outside T.

Recall that, starting with two points in $J(\mathbb{Q})$, the local Coleman–Gross heights are defined by first choosing divisors of degree 0 representing these points. The local heights then depend on these choices, whereas the global height does not. In our present setting, the idea is to interpret classes $e_1 \in \mathrm{H}^1_f(G_\mathbb{Q}, V)$ and $e_2 \in \mathrm{H}^1_f(G_\mathbb{Q}, V^*(1))$ as extensions

$$0 \to V \to E_1 \to \mathbb{Q}_p \to 0$$
$$0 \to \mathbb{Q}_p(1) \to E_2 \to V \to 0,$$

where we identify $\mathrm{H}^1_f(G_\mathbb{Q}, V)$ with crystalline extensions of V by $\mathbb{Q}_p$ with a continuous $G_\mathbb{Q}$-action. Nekovář shows [Nek93, Proposition 4.4] that one can lift these extensions to form a *mixed extension* E of E_1 and E_2, i.e. a p-adic $G_\mathbb{Q}$-representation with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$, sitting in a commutative diagram

(19)
$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathbb{Q}_p(1) \arrow[r] \arrow[d, "="] & E_2 \arrow[r] \arrow[d] & V \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{Q}_p(1) \arrow[r] & E \arrow[r] \arrow[d] & E_1 \arrow[r] \arrow[d] & 0 \\
 & & \mathbb{Q}_p \arrow[r, "="] \arrow[d] & \mathbb{Q}_p \arrow[d] & \\
 & & 0 & 0 & .
\end{tikzcd}$$

and having a weight filtration by $G_\mathbb{Q}$-subrepresentations

$$0 = W_{-3}E \subseteq W_{-2}E \subseteq W_{-1}E \subseteq W_0E = E\,,$$

so that $W_{-1}E \simeq E_2$ and $W_0E/W_{-2}E \simeq E_1$. In other words, the mixed extension E has a block matrix representation

$$\begin{pmatrix} 1 & 0 & 0 \\ * & \rho_V & 0 \\ * & * & \chi_p \end{pmatrix}$$

where the representation ρ_V corresponds to V and χ_p is the p-adic cyclotomic character.

Given any mixed extension E of $G_\mathbb{Q}$-representations with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$, we can define projections

$$\pi_1(E) := [W_0E/W_{-2}E] \in \mathrm{H}^1(G_\mathbb{Q}, V), \quad \pi_2(E) := [W_{-1}E] \in \mathrm{H}^1(G_\mathbb{Q}, V^*(1))\,. \tag{20}$$

For a mixed extension E of E_1 and E_2 as above, we then have $\pi_i(E) = e_i$.

For every prime v, we can define local mixed extension of G_v-representations with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$ in an analogous way. We say a global mixed extension E is *crystalline* if $\mathrm{loc}_p(E)$ is crystalline. If E is crystalline, the projections $\pi_i(E)$ are crystalline as well.

Nekovář defines a local height h_v on mixed extension of G_v-representations with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$. We will assume it is of the form $\mathrm{loc}_v(E)$ for a global mixed extension E. The local height is not well-defined on $\mathrm{H}^1_f(G_\mathbb{Q}, V) \times \mathrm{H}^1_f(G_\mathbb{Q}, V^*(1))$, it depends on the chosen mixed extension (in fact on its equivalence class). Such mixed extensions can be added via the Baer sum; the local heights are then bi-additive in the sense of [BD18a, Definition 4.4]. By [Nek93, Theorem 4.11],

$$h(e_1, e_2) = \sum_v h_v(\mathrm{loc}_v(E)) \tag{21}$$

is independent of the choice of E and defines a bilinear pairing

$$h\colon \mathrm{H}^1_f(G_{\mathbb{Q}}, V) \times \mathrm{H}^1_f(G_{\mathbb{Q}}, V^*(1)) \to \mathbb{Q}_p\ .$$

By Poincaré duality, we have $V \simeq V^*(1)$, so we in fact get a bilinear pairing

$$h\colon \mathrm{H}^1_f(G_{\mathbb{Q}}, V) \times \mathrm{H}^1_f(G_{\mathbb{Q}}, V) \to \mathbb{Q}_p\ .$$

Remark 3.5. If $\ker(s)$ is isotropic with respect to the dual of the cup product, then this pairing is symmetric by [Nek93, Theorem 4.11 (4)].

Remark 3.6. One can associate a mixed extension as above to a pair of divisors $D_1, D_2 \in \mathrm{Div}^0(X)$ with disjoint support via an étale Abel-Jacobi map, see [Nek93, Section 5]. Besser [Bes04] shows that for our choice of V, the local Coleman–Gross and Nekovář heights (with respect to these choices) are equivalent.

3.3. **Local heights.** The construction of the local heights h_v is not particularly intuitive. The rough idea is to construct a class $c \in \mathrm{H}^1(G_v, \mathbb{Q}_p(1))$ (crystalline when $v = p$) from a local mixed extension E_v. One can then use the Kummer isomorphism

$$\kappa_v\colon \widehat{\mathbb{Q}_v^*} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\simeq} \mathrm{H}^1(G_v, \mathbb{Q}_p(1))$$

to define a p-adic number

$$h_v(E_v) := \chi_v(c) \in \mathbb{Q}_p, \tag{22}$$

where χ_v is the map

$$\chi_v\colon \mathrm{H}^1(G_v, \mathbb{Q}_p(1)) \to \widehat{\mathbb{Q}_v^*} \otimes \mathbb{Q}_p \to \mathbb{Q}_p \tag{23}$$

induced by the local component $\chi_v\colon \mathbb{Q}_v^* \to \mathbb{Q}_p$ of our chosen idèle class character and by κ_v^{-1}. Our exposition follows [BDM+19, §3] closely.

3.3.1. *Local heights away from p.* First consider a prime $\ell \neq p$. Our main focus will be on algorithms for h_p, so we will only discuss this case briefly. Not that $\chi_\ell(\mathbb{Z}_\ell^*) = 0$ because of continuity, hence the second map in (23) factors through the valuation $\mathrm{ord}_\ell\colon \mathbb{Q}_\ell^* \to \mathbb{Z}$ for $v = \ell$.

It is explained in [BDM+19, §3.2] that we have $\mathrm{H}^1(G_\ell, V) = \mathrm{H}^1(G_\ell, V^*(1)) = 0$, essentially since (by the weight-monodromy conjecture for curves) $\mathrm{H}^0(G_\ell, V) = \mathrm{H}^0(G_\ell, V^*(1))^* = 0$. Hence, if E_ℓ is a mixed extension of G_ℓ-representations with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$, then, from the local version of the diagram (19), we obtain a splitting $E_\ell \simeq V \oplus N$, where N is an extension

$$0 \to \mathbb{Q}_p(1) \to N \to \mathbb{Q}_p \to 0\,,$$

so the class $c := [N]$ lies in $\mathrm{H}^1(G_\ell, \mathbb{Q}_p(1))$, and we define $h_\ell(E_\ell)$ as in (22). See [Nek93, §4.6] and [BDM+19, §3.2]. If E_ℓ is unramified, then $h_\ell(E_\ell) = 0$, so the sum in (21) is finite. More generally, a simple argument shows:

Remark 3.7. Suppose that E_ℓ is potentially unramified. Then $h_\ell(E_\ell)$ is trivial by [BDM+19, Lemma 3.2]. This implies that the local heights at ℓ of interest to us are trivial when X has potentially good reduction at ℓ.

3.3.2. *Local heights at p.* We now describe the main object we will need to compute in order to apply quadratic Chabauty for rational points: the local height $h_p(E_p)$, where E_p is a crystalline mixed extension E_p of G_p-extensions with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$. The construction is in terms of p-adic Hodge theory. More precisely, the local height $h_p(E_p)$ is defined in terms of $D_{\mathrm{cris}}(E_p)$, which turns out to be a mixed extension of filtered ϕ-module, defined below. For the mixed extensions of interest to us, we will show later that we can construct $D_{\mathrm{cris}}(E_p)$ explicitly, by solving differential equations and applying linear algebra.

The definition of $h_p(E_p)$ is similar to the construction of local heights away from p, but the construction of the class $c \in \mathrm{H}^1_f(G_p, \mathbb{Q}_p(1))$ is more involved, because we do not have $\mathrm{H}^1(G_p, V) = \mathrm{H}^1(G_p, V^*(1)) = 0$. We will end this section by making the construction rather explicit, in terms of splittings of filtered ϕ-modules.

Definition 3.8. A filtered ϕ-module (over $\mathbb{Q}_p$) is a finite dimensional $\mathbb{Q}_p$-vector space W, equipped with an exhaustive and separated decreasing filtration Fil^i and an automorphism ϕ. Recall

- exhaustive means $W = \cup_i \mathrm{Fil}^i$,
- separated means $\cap_i \mathrm{Fil}^i = 0$,
- decreasing means $\mathrm{Fil}^{i+1} \subseteq \mathrm{Fil}^i$.

Example 3.9. Here are some examples of filtered ϕ-modules:

(1) $\mathbb{Q}_p$ with $\mathrm{Fil}^0 = \mathbb{Q}_p$, $\mathrm{Fil}^n = 0$ for all $n > 0$, and $\phi = id$.
(2) $\mathbb{Q}_p(1) = D_{\mathrm{cris}}(\mathbb{Q}_p(1))$ with $\mathrm{Fil}^{-1} = \mathbb{Q}_p$, $\mathrm{Fil}^n = 0$ for all $n > -1$, and $\phi = 1/p$.
(3) By Faltings' comparison theorem [Fal89], we have $H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p}) = D_{\mathrm{cris}}(\mathrm{H}^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p))$ and $\mathrm{H}^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ is crystalline. Frobenius ϕ on crystalline cohomology and the Hodge filtration endow $H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})$ with the structure of a filtered ϕ-module.
(4) $V_{\mathrm{dR}} := H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})^* = D_{\mathrm{cris}}(V)$ with the dual filtration and action.
(5) The direct sum of $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$ has the structure of a filtered ϕ-module as well.

In general, we think of the filtration as a Hodge filtration and of the automorphism as a Frobenius action coming from comparison theorems.

Remark 3.10. To be precise, all filtered ϕ-modules below are *admissible* (i.e. they come from p-adic Galois representations), but we drop the adjective for simplicity.

The following construction will be used several times, so we state it as a

Lemma 3.11. *For any filtered ϕ-module W for which*

$$W^{\phi=1} = 0$$

we have an isomorphism

$$\mathrm{Ext}^1_{\mathrm{Fil},\phi}(\mathbb{Q}_p, W) \simeq W/\mathrm{Fil}^0 .$$

Proof. Given an extension of $\mathbb{Q}_p$ by W in the category of filtered ϕ-modules

$$0 \to W \to E \to \mathbb{Q}_p \to 0$$

choose a splitting $s^\phi \colon \mathbb{Q}_p \to E$ which is ϕ-equivariant. Furthermore, choose a splitting $s^{\mathrm{Fil}} \colon \mathbb{Q}_p \to E$ which respects the filtration. Then, since $W^{\phi=1} = 0$, s^ϕ is unique, while s^{Fil} is only determined up to an element of $\mathrm{Fil}^0 W$, so

$$s^\phi - s^{\mathrm{Fil}} + \mathrm{Fil}^0 W \in W/\mathrm{Fil}^0 W$$

is independent of choices.

The inverse of this map is the Bloch–Kato exponential. See [Nek93, Theorem 1.15] and [BK90, §3.8]. □

The condition $W^{\phi=1} = 0$ will be satisfied by most filtered ϕ-modules we encounter. For instance, it holds trivially for $W = \mathbb{Q}_p(1)$, and the Weil conjectures imply that it holds for $W = V_{\mathrm{dR}}$.

The filtered ϕ-module $\mathbb{Q}_p \oplus V \oplus \mathbb{Q}_p(1)$ has a weight filtration, just like the mixed extensions of Galois representations we encountered above. We call such objects *mixed extensions of filtered ϕ-modules with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$*.

Now let E_p be a crystalline mixed extension of G_p-representations with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$. Then $E_{\mathrm{dR}} := D_{\mathrm{cris}}(E_p)$ is a mixed extension of filtered ϕ-modules with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$. In analogy with the case of Galois-representations, we can define crystalline extensions

$$E_1 := E_{\mathrm{dR}}/\,\mathbb{Q}_p(1)$$

and

$$E_2 := \ker(E_{\mathrm{dR}} \to \mathbb{Q}_p).$$

of filtered ϕ-modules:

$$0 \to V_{\mathrm{dR}} \to E_1 \to \mathbb{Q}_p \to 0$$
$$0 \to \mathbb{Q}_p(1) \to E_2 \to V_{\mathrm{dR}} \to 0,$$

fitting into a commutative diagram (19) of filtered ϕ-modules.

By Lemma 3.11, we have

$$\mathrm{Ext}^1_{\mathrm{Fil},\phi}(\mathbb{Q}_p, E_2) \simeq E_2/\operatorname{Fil}^0.$$

Hence we can map the extension E_{dR} of $\mathbb{Q}_p$ by E_2 into $V_{\mathrm{dR}}/\operatorname{Fil}^0$ via the exact sequence

$$0 \to \mathbb{Q}_p(1) \to E_2/\operatorname{Fil}^0 \to V_{\mathrm{dR}}/\operatorname{Fil}^0 \to 0, \tag{24}$$

and the image of E_{dR} is $[E_1]$.

Let $\gamma\colon V_{\mathrm{dR}} \to E_2$ be the unique Frobenius equivariant splitting of

$$0 \to \mathbb{Q}_p(1) \to E_2 \to V_{\mathrm{dR}} \to 0.$$

We define

$$\delta\colon V_{\mathrm{dR}}/\operatorname{Fil}^0 \xrightarrow{s} V_{\mathrm{dR}} \xrightarrow{\gamma} E_2 \to E_2/\operatorname{Fil}^0.$$

Then $[E_{\mathrm{dR}}]$ and $\delta([E_1])$ have the same image in $V_{\mathrm{dR}}/\operatorname{Fil}^0$; hence $[E_{\mathrm{dR}}]-\delta([E_1]) \in \mathbb{Q}_p(1)$ by (24). Recall that our goal was to construct a class in $\mathrm{H}^1_f(G_p, \mathbb{Q}_p(1))$. But since

$$\mathbb{Q}_p(1) \simeq \mathrm{Ext}^1_{\mathrm{Fil},\phi}(\mathbb{Q}_p, \mathbb{Q}_p(1)) \simeq \mathrm{H}^1_f(G_p, \mathbb{Q}_p(1))$$

by Lemma 3.11, we can think of this difference as a class

$$c := [E_{\mathrm{dR}}] - \delta([E_1]) \in \mathrm{H}^1_f(G_p, \mathbb{Q}_p(1)).$$

As above, we define the height of E_p by

$$h_p(E_p) := \chi_p(c). \tag{25}$$

In order to apply quadratic Chabauty in practice, it will be crucial to compute (25). To this end, we now give a more explicit version, based on splittings of E_{dR}. Namely, suppose that we are given a vector space splitting

$$s_0\colon\ \mathbb{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbb{Q}_p(1) \xrightarrow{\sim} E_{\mathrm{dR}}.$$

We choose two further splittings

$$s^{\phi}\colon\ \mathbb{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbb{Q}_p(1) \xrightarrow{\sim} E_{\mathrm{dR}}$$

$$s^{\mathrm{Fil}}\colon\ \mathbb{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbb{Q}_p(1) \xrightarrow{\sim} E_{\mathrm{dR}},$$

where s^{ϕ} is Frobenius-equivariant and s^{Fil} respects the filtrations. As in the proof of Lemma 3.11, we have that s^{ϕ} is unique and s^{Fil} is not.

Now choose bases for $\mathbb{Q}_p, V_{\mathrm{dR}}, \mathbb{Q}_p(1)$ such that with respect to these bases we have

$$s_0^{-1} \circ s^{\phi} = \begin{pmatrix} 1 & 0 & 0 \\ \alpha_{\phi} & 1 & 0 \\ \gamma_{\phi} & \beta_{\phi}^{\mathrm{T}} & 1 \end{pmatrix}$$

$$s_0^{-1} \circ s^{\mathrm{Fil}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \gamma_{\mathrm{Fil}} & \beta_{\mathrm{Fil}}^{\mathrm{T}} & 1 \end{pmatrix}$$

(the point is to make the "α_{Fil}-term" in $s_0^{-1} \circ s^{\mathrm{Fil}}$ zero).

Finally, the splitting s of the Hodge filtration defines idempotents

$$s_1,\ s_2\colon V_{\mathrm{dR}} \to V_{\mathrm{dR}}$$

projecting onto

$$s(V_{\mathrm{dR}}/\,\mathrm{Fil}^0) \text{ and } \mathrm{Fil}^0$$

components, respectively. A computation shows

Proposition 3.12. *We have*

$$h_p(E_p) = \chi_p(\gamma_{\phi} - \gamma_{\mathrm{Fil}} - \beta_{\phi}^{\mathrm{T}} s_1(\alpha_{\phi}) - \beta_{\mathrm{Fil}}^{\mathrm{T}} s_2(\alpha_{\phi})).$$

4. Quadratic Chabauty: theory

In this section we discuss the theoretical justification for the quadratic Chabauty method. Since we focus on computational methods in this course and the foundations of non-abelian Chabauty, of which quadratic Chabauty is a special case, are covered in Kim's lectures, we will be brief. Kim's approach relies on choosing a unipotent quotient U of the $\mathbb{Q}_p$-étale fundamental group of a curve and defining a subset of p-adic points containing the rational points using local conditions. The hope is that this set can be proved to be finite and can be computed explicitly.

Our main situation of interest is when the Chabauty condition is not satisfied, but the curve satisfies the quadratic Chabauty condition (29). In particular, this condition holds when the Mordell-Weil rank is equal to the genus and the Picard number is greater than 1, a situation frequently encountered for modular curves, as shown by Siksek [Sik17]. In this case, we can construct a non-abelian quotient U such that the corresponding set of p-adic points is finite and, we can indeed compute it. In the present section, we show finiteness.

4.1. **Chabauty–Kim theory.** Let X be a nice curve over $\mathbb{Q}$ of genus $g > 1$, and let J be its Jacobian. Assume $X(\mathbb{Q}) \neq \varnothing$ and fix $b \in X(\mathbb{Q})$. We fix a prime p of good reduction, we let T_0 denote the set of bad primes for X, and we set $T := T_0 \cup \{p\}$.

We begin by reformulating classical Chabauty in terms of p-adic Hodge theory, see also [Cor19] and Zureick-Brown's lectures. As in the previous section, we let $V := \mathrm{H}^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)^*$, and $V_{\mathrm{dR}} := \mathrm{H}^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})^*$, viewed as a filtered vector space with the dual filtration to the Hodge filtration, so that there is an isomorphism $V_{\mathrm{dR}}/\operatorname{Fil}^0 \simeq \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$. Let G_T be the maximal quotient of $G_{\mathbb{Q}}$ unramified outside T. The étale formulation of classical Chabauty can be summarized in the following commutative diagram:

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d] & X(\mathbb{Q}_p) \arrow[d] \arrow[dr, "\mathrm{AJ_b}"] & \\
J(\mathbb{Q}) \arrow[r] \arrow[d] & J(\mathbb{Q}_p) \arrow[r, "\log"] \arrow[d] & \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^* \arrow[d, "\simeq"] \\
\mathrm{H}^1_f(G_T, V) \arrow[r] & \mathrm{H}^1_f(G_p, V) \arrow[r, "\simeq"] & \mathrm{H}_1^{\mathrm{dR}}(X_{\mathbb{Q}_p})/F^0
\end{tikzcd} \; . \tag{26}$$

We give a very brief summary of Kim's generalization, referring to [Kim09] and Kim's lectures for more details. Choose a Galois-stable unipotent quotient U of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}})_{\mathbb{Q}_p}$, the unipotent $\mathbb{Q}_p$-étale fundamental group of $X_{\overline{\mathbb{Q}}}$ with base point b. The latter is the $\mathbb{Q}_p$-pro-unipotent completion of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}})$. We also want U to be motivic, in the sense that it also has a de Rham realization. In fact we will assume that U is a quotient of the maximal n-unipotent (i.e. having unipotency index $\leq n$) quotient of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}})_{\mathbb{Q}_p}$, which we denote by U_n.

There is a commutative diagram

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d, "j_U"'] & \prod_{v \in T} X(\mathbb{Q}_v) \arrow[d, "\prod j_{U,v}"] \\
\mathrm{H}^1(G_T, U) \arrow[r, "\prod \mathrm{loc}_v"] & \prod_{v \in T} \mathrm{H}^1(G_v, U).
\end{tikzcd}$$

where j_U and $j_{U,v}$ denote the global, respectively local, unipotent Kummer maps defined in [Kim05, Kim09]. It is a highly nontrivial result due to Kim [Kim05, Kim09] that the nonabelian pointed continuous cohomology sets $\mathrm{H}^1(G_T, U)$ and $\mathrm{H}^1(G_v, U)$ are affine algebraic varieties over $\mathbb{Q}_p$. Kim also shows that the localization maps are variety morphisms and that the crystalline torsors have the structure of (the $\mathbb{Q}_p$-points on) a subvariety.

In analogy with the classical theory of Selmer groups, we can cut down $\mathrm{H}^1(G_T, U)$ by local conditions to find a pointed set containing the images of the rational points, which we hope to be able to compute.

Definition 4.1 ([BD18a, Definition 2.2])**.** We define the *Selmer variety* $\operatorname{Sel}(U)$ to be the reduced scheme associated to the subscheme of $\mathrm{H}^1(G_T, U)$ containing those classes c such that

- $\mathrm{loc}_p(c)$ is crystalline,
- $\mathrm{loc}_\ell(c) \in j_{U,\ell}(X(\mathbb{Q}_\ell))$ for all $\ell \neq p$,
- the projection of c to $\mathrm{H}^1(G_T, V)$ comes from an element of $J(\mathbb{Q}) \otimes \mathbb{Q}_p$.

See Kim [Kim09] for a proof that $\mathrm{H}^1_f(G_p, U)$ is a subvariety of $\mathrm{H}^1_f(G_p, U)$; it also follows from loc. cit. and [KT08] that $\operatorname{Sel}(U)$ is a subvariety of $\mathrm{H}^1(G_T, U)$ (see [Kim12]) for an explanation why the conditions above might not produce a reduced scheme). The relation between our (slightly non-standard) definition of the Selmer variety and other definitions in the literature is discussed in [BD18a, Remark 2.3]. Our version has the convenient feature that our results will not depend on finiteness of the p-primary part of the Shafarevich-Tate group of J.

Since $j_{U,p}(X(\mathbb{Q}_p)) \subset \mathrm{H}^1_f(G_p, U)$ by Olsson's comparison theorem [Ols11, Theorem 1.4] in non-abelian p-adic Hodge theory, we obtain another commutative diagram

$$\begin{tikzcd} X(\mathbb{Q}) \arrow[r] \arrow[d, "j_U"'] & X(\mathbb{Q}_p) \arrow[d, "j_{U,p}"] \\ \mathrm{Sel}(U) \arrow[r, "\mathrm{loc}_p"] & \mathrm{H}^1_f(G_p, U). \end{tikzcd} \tag{27}$$

Remark 4.2. Note that under our definitions, $\mathrm{Sel}(U)$ need not be contained in $\mathrm{H}^1_f(G_T, U)$, because $j_{U,\ell}(z)$ need not be unramified for all $\ell \neq p$ and $z \in X(\mathbb{Q}_\ell)$. In contrast to Bloch–Kato's foundational paper [BK90] and much of the subsequent literature, many papers in non-abelian Chabauty do not require unramified away from p in their definition of the global H^1_f. Following [BD18b], we will try to avoid confusion by writing $\mathrm{H}^1_{f,S}(G_T, U)$ to mean those classes that are crystalline at p and unramified at all primes ℓ that are not in S, where we will always choose S to be a subset of T_0. In this notation, we have $\mathrm{H}^1_{f,\varnothing}(G_T, U) = \mathrm{H}^1_f(G_T, U)$ and $\mathrm{Sel}(U) \subset \mathrm{H}^1_{f,T_0}(G_T, U)$ (but see Remark 4.4 below).

Although the image of $j_{U,\ell}$ can be unramified, we have the following result about its image.

Theorem 4.3 (Kim–Tamagawa [KT08])**.** *Suppose that $\ell \neq p$. Then the image $j_{U,\ell}(X(\mathbb{Q}_\ell))$ is finite. For a prime ℓ of good reduction for X, the image is trivial.*

This crucial result will enable us to control certain local heights away from p in a manner somewhat similar to Proposition 2.29. In fact we will use the following generalization of the second statement.

Remark 4.4 ([BD18a, Lemma 5.4]). If X has potentially good reduction at ℓ, then $j_{U,\ell}(X(\mathbb{Q}_\ell))$ is trivial. Hence

$$\mathrm{Sel}(U) \subset \mathrm{H}^1_{f,T_0'}(G_T, U),$$

where T_0' is the set of bad primes of X where X has potentially good reduction.

We define

$$X(\mathbb{Q}_p)_U := j_p^{-1}\left(\mathrm{loc}_p \, \mathrm{Sel}(U)\right) \subset X(\mathbb{Q}_p).$$

By commutativity of the diagram (27), we have that $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)_U$. Since U is a quotient of the maximal n-step unipotent quotient U_n of the $\mathbb{Q}_p$-étale fundamental group of $X_{\overline{\mathbb{Q}}}$ with base point b, we obtain

$$X(\mathbb{Q}) \subset X(\mathbb{Q}_p)_n := X(\mathbb{Q}_p)_{U_n} \subset X(\mathbb{Q}_p)_U\,. \tag{28}$$

Of course this is only useful for the purpose of computing rational points if $X(\mathbb{Q}_p)_U$ is finite and can be computed in practice. Kim conjectured that the first condition is eventually satisfied:

Conjecture 4.5 (Kim [Kim09])**.** *For $n \gg 0$, $X(\mathbb{Q}_p)_n$ is finite.*

There is very strong evidence for this conjecture, as shown in [Kim09, Section 3]. It is implied by a special case of the conjecture of Bloch–Kato (and other standard conjectures on motives).

For computational purposes this is sufficient, once we can compute $X(\mathbb{Q}_p)_n$ as in Conjecture 4.5. The reasons is that the Mordell–Weil sieve, discussed in Section 5.3.3 can often be used to show that given p-adic points do not come from a rational point. However, one of the most exciting potential applications of Kim's ideas would be an effective version of the Mordell conjecture. But while heuristics imply that the Mordell-Weil sieve should always work eventually [Poo06], it is not effective. The following stronger conjecture circumvents this issue.

Conjecture 4.6 (Kim [BDCKW18]). *For $n \gg 0$, $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$.*

The n in Conjecture 4.6 may not be the n of Conjecture 4.5. They can differ already for the Chabauty–Coleman case $n = 1$. See recent work of Bianchi [Bia19a] along these lines in the case of punctured elliptic curves.

Project 4.7 (Quadratic Chabauty and Kim's conjecture). When $X/\mathbb{Q}$ is a genus g curve with $r = \operatorname{rk} J(\mathbb{Q}) = g - 1$, then typically the set of p-adic points $X(\mathbb{Q}_p)_1$ cut out by the Chabauty–Coleman method strictly contains $X(\mathbb{Q})$. In this project, we will first give an algorithm to compute the quadratic Chabauty set $X(\mathbb{Q}_p)_2$ under these hypotheses. Then we will investigate whether the quadratic Chabauty set, which satisfies

$$X(\mathbb{Q}) \subset X(\mathbb{Q}_p)_2 \subset X(\mathbb{Q}_p)_1 \subset X(\mathbb{Q}_p),$$

is equal to $X(\mathbb{Q})$. (See [Bia19a] for the case of integral points on punctured elliptic curves.) If $X(\mathbb{Q}) \neq X(\mathbb{Q}_p)_2$, we would like to characterize the points in $X(\mathbb{Q}_p)_2 \setminus X(\mathbb{Q})$. This project could be carried out on a database of genus 2 and 3 curves [The19].

Generalizing the étale formulation of classical Chabauty, Kim's approach is to show finiteness of $X(\mathbb{Q}_p)_U$ using p-adic Hodge theory. He obtains the following amendment of diagram (27):

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d, "j_U"'] & X(\mathbb{Q}_p) \arrow[d, "j_{U,p}"'] \arrow[dr, "j_U^{\mathrm{dR}}"] & \\
\mathrm{Sel}(U) \arrow[r, "\mathrm{loc}_{U,p}"] & \mathrm{H}^1_f(G_p, U) \arrow[r, "\simeq"] & U^{\mathrm{dR}}/\mathrm{Fil}^0
\end{tikzcd}$$

We refer to [Kim09] and Kim's lectures for the definitions of $U^{\mathrm{dR}} := D_{\mathrm{cris}}(U)$ (a quotient of Deligne's de Rham fundamental group $\pi_1^{\mathrm{dR}}(X_{\mathbb{Q}_p}, b)$), the isomorphism $\mathrm{H}^1_f(G_p, U) \to U^{\mathrm{dR}}/\mathrm{Fil}^0$ (coming from Olsson's comparison theorem [Ols11, Theorem 1.4]), and the locally analytic maps j_U^{dR} (these are iterated Coleman integrals).

Note that this diagram specializes to Diagram (26) for $U = V$.

The analogue of the analytic properties of $\mathrm{AJ_b}$ (specifically that if there exists a nonzero functional we can construct that vanishes on $\overline{J(\mathbb{Q})}$ with Zariski dense image, given by a convergent p-adic power series then there are finitely many zeros on each residue disk of $X(\mathbb{Q}_p)$) is as follows:

Theorem 4.8 (Kim [Kim09]). *The map j_U^{dR} has Zariski dense image and is given by convergent p-adic power series on every residue disk.*

The analogue of the Chabauty–Coleman hypothesis of $r < g$ is the non-density of $\mathrm{loc}_{U,p}$.

Theorem 4.9 (Kim [Kim09]). *Suppose $\mathrm{loc}_{U,p}$ is non-dominant. Then $X(\mathbb{Q}_p)_U$ is finite.*

All known finiteness results come from bounding the dimension of $\mathrm{Sel}(U)$. For instance, Coates and Kim used Iwasawa theory to obtain dimension bounds in the following setting:

Theorem 4.10 (Coates–Kim [CK10]). *Let $X/\mathbb{Q}$ be a nice curve of genus $g \geq 2$ and suppose that J is isogenous over $\overline{\mathbb{Q}}$ to a product $\prod A_i$ of abelian varieties, with A_i having CM by a number field K_i of degree $2 \dim A_i$. Then $X(\mathbb{Q}_p)_n$ is finite for $n \gg 0$.*

Example 4.11. Theorem 4.10 shows eventual finiteness in many nontrivial settings. For instance, Ellenberg and Hast use it to prove finiteness of rational points on solvable covers of $\mathbb{P}^1$ over $\mathbb{Q}$, see [EH17].

4.2. Quadratic Chabauty.

Suppose that the set $X(\mathbb{Q}_p)_1$ cut out by classical Chabauty–Coleman is infinite. The goal of the quadratic Chabauty method is to

(a) show that $X(\mathbb{Q}_p)_2$ is finite
(b) construct explicit functions on $X(\mathbb{Q}_p)$ cutting out (a finite set containing) $X(\mathbb{Q}_p)_2$.

In this section, we tackle (a), using Theorem 4.9. We will focus on (b) in Section 5.

Let $\rho(J)$ denote the *Picard number* of J, that is, the rank of $\mathrm{NS}(J)$, the Néron-Severi group of J (as a variety over $\mathbb{Q}$). In this section, we will prove the following fundamental result.

Theorem 4.12 ([BD18a, Lemma 3.2]). *Suppose that*

$$\mathrm{rk}(J(\mathbb{Q})) < g + \rho(J) - 1\,. \tag{29}$$

Then $X(\mathbb{Q}_p)_2$ is finite.

We call (29) the *quadratic Chabauty condition.* The rough idea of the proof is to show that, assuming (29), there exists a Galois-stable quotient U of U_2 such that $\dim \mathrm{Sel}(U) < \dim \mathrm{H}^1_f(G_p, U)$. The result then follows from (28) and Theorem 4.9.

In fact, we will first prove a simpler, but important special case.

Proposition 4.13. *Suppose that X has potentially good reduction everywhere. If $\mathrm{rk}(J(\mathbb{Q})) = g$ and $\rho(J) > 1$, then $X(\mathbb{Q}_p)_2$ is finite.*

For instance, this suffices to prove finiteness of $X(\mathbb{Q}_p)_2$ for the split (or non-split) Cartan modular curve at level 13 [BDM$^+$19].

4.3. Dimension counts.

From now on, suppose that U is a Galois-stable quotient of U_2 which sits in a Galois-equivariant short exact sequence

$$1 \to [U, U] \to U \to V \to 1\,, \tag{30}$$

where $V = \mathrm{H}^1_{\text{ét}}(\bar{X}, \mathbb{Q}_p)$. We want to choose U so that $X(\mathbb{Q}_p)_U$ is finite. Of course we cannot take $U = V$, since that would only recover Chabauty's result. The idea is to choose U only "slightly non-abelian". In order to do so, we first compute $\dim \mathrm{H}^1_f(G_p, U)$ and bound $\dim \mathrm{Sel}(U)$ in terms of data depending only on $[U, U]$; this will then suggest find a quotient U such that $[U, U] \simeq \mathbb{Q}_p(1)$ (or a direct sum thereof).

We start with the local computation.

Lemma 4.14. *We have*

$$\dim \mathrm{H}^1_f(G_p, U) = \dim \mathrm{H}^1_f(G_p, [U, U]) + g.$$

Proof. Note that all representations in (30) are de Rham. Hence, we obtain a short exact sequence

$$1 \to D_{\mathrm{dR}}([U, U])/F^0 \to D_{\mathrm{dR}}(U)/F^0 \to D_{\mathrm{dR}}(V)/F^0 \to 1\,. \tag{31}$$

Now we have an isomorphism of schemes (algebraic by [Kim05, Section 1])

$$\mathrm{H}^1_f(G_p, W) \simeq D_{\mathrm{dR}}(W)/F^0$$

for $W \in \{[U, U], V, U\}$ (since $\phi = 1$ on these; compare Lemma 3.11) and therefore we deduce

$$\dim \mathrm{H}^1_f(G_p, U) = \dim \mathrm{H}^1_f(G_p, [U, U]) + \dim \mathrm{H}^1_f(G_p, V) \tag{32}$$

from (31). But $\mathrm{H}^1_f(G_p, V) \simeq \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)$, so the result follows. □

We now turn to the dimension of $\mathrm{Sel}(U)$. We have that $\mathrm{H}^0(G_T, W) = 0$, for all terms in (30), so the corresponding six-term exact sequence of non-abelian Galois cohomology (see Proposition A.2) induces an exact sequence

$$\mathrm{H}^1(G_T, [U,U]) \to \mathrm{H}^1(G_T, U) \to \mathrm{H}^1(G_T, V)\,.$$

It is shown in [Kim05] that this is an exact sequence of pointed varieties, inducing another exact sequence

$$\mathrm{H}^1_f(G_T, [U,U]) \to \mathrm{H}^1_f(G_T, U) \to \mathrm{H}^1_f(G_T, V) \tag{33}$$

of pointed varieties (note that this is in general weaker than the local version leading to (32)).

For now let's assume that X has potentially good reduction everywhere. This implies that a class $c \in \mathrm{Sel}(U)$ satisfies $\mathrm{loc}_\ell(c) = 0$ (and, in particular, is unramified) for all $\ell \neq p$; hence

$$\mathrm{Sel}(U) \subset \mathrm{H}^1_{f,\varnothing}(G_T, U) = \mathrm{H}^1_f(G_T, U). \tag{34}$$

This is where we use the third requirement in Definition 4.1: we may now conclude

$$\dim \mathrm{Sel}(U) \le \mathrm{rk}(J(\mathbb{Q})) + \dim \mathrm{H}^1_f(G_T, [U,U]) \tag{35}$$

from (33) and (34) without any finiteness assumptions on the Shafarevich-Tate group.

To prove non-density of the localization map, we want $\mathrm{H}^1_{f,\varnothing}(G_T, U)$ (or $\mathrm{H}^1_{f,T_0'}(G_T, U)$ if we don't have potentially good reduction) to be small, and $\mathrm{H}^1_f(G_p, U)$ to be large. Hence it is natural to look for quotients U such that $[U,U] \simeq \mathbb{Q}_p(1)$, since in this case Example 3.2, Example 3.3, Lemma 4.14 and (35) imply:

Lemma 4.15. *Suppose that X has potentially good reduction everywhere. If $\mathrm{rk}(J(\mathbb{Q})) \le g$ and $[U,U] \simeq \mathbb{Q}_p(1)$, then $X(\mathbb{Q}_p)_U$ is finite.*

We will generalize Lemma 4.15 below. For now, let us note:

Corollary 4.16. *Suppose that X has potentially good reduction everywhere and that $\mathrm{rk}(J(\mathbb{Q})) \le g$. If there exists a Galois stable quotient U of U_2 such that $[U,U] \simeq \mathbb{Q}_p(1)$, then $X(\mathbb{Q}_p)_2$ is finite.*

4.4. **Constructing a $\mathbb{Q}_p(1)$-quotient of U_2.** We will now show that a quotient of U_2 as in Corollary 4.16 exists when the Picard number of J is strictly greater than 1.

Lemma 4.17. *Suppose that $\rho(J) > 1$. Then there exists a Galois-stable quotient U of U_2 surjecting onto V such that $[U,U] = \mathbb{Q}_p(1)$.*

Combining Corollary 4.16 and Lemma 4.17, we deduce Proposition 4.13.

All known methods to construct such a quotient U use a geometric approach. We will follow [BDM+19] in phrasing the construction in terms of a correspondence $Z \subset X \times X$. See [Smi05, Chapter 3] for background on correspondences and [Mil80, Chapter VI.9] for background on cycle classes. Applying the Künneth projector to the cycle class in $H^2(\bar{X} \times \bar{X})$ of Z, we obtain

$$\xi_Z \in \mathrm{H}^1(\bar{X}, \mathbb{Q}_p) \otimes \mathrm{H}^1(\bar{X}, \mathbb{Q}_p)(1) \simeq \mathrm{End}\,\mathrm{H}^1(\bar{X}, \mathbb{Q}_p).$$

Definition 4.18. A nontrivial correspondence $Z \subset X \times X$ is nice if

(i) there are $c_1, c_2 \in \mathrm{Pic}(X)$ such that the pushforward of the class $[Z] \in \mathrm{Pic}(X \times X)$ under the canonical involution $(x,y) \mapsto (y,x)$ is $[Z] + \pi_1^* c_1 + \pi_2^* c_2$ where π_1, π_2 are the canonical projections,
(ii) the class ξ_Z, viewed as an endomorphism of $\mathrm{H}^1(\bar{X}, \mathbb{Q}_p)$, has trace zero.

Note that a correspondence satisfying (i) induces an endomorphism of J fixed by the Rosati involution, i.e. a nontrivial element of $\mathrm{NS}(J)$. This proves the first part of the following result. The second part follows from (ii), since the trace factors through the cup product.

Lemma 4.19 ([BDM+19, Lemma 2.4])**.** *Suppose J is absolutely simple, and let $Z \subset (X \times X)$ be a correspondence satisfying (i) above. Then ξ_Z lies in the subspace*

$$\bigwedge^2 \mathrm{H}^1(\bar{X}, \mathbb{Q}_p)(1) \subseteq \mathrm{H}^1(\bar{X}, \mathbb{Q}_p) \otimes \mathrm{H}^1(\bar{X}, \mathbb{Q}_p)(1).$$

Moreover Z is nice if and only if the image of ξ_Z in $H^2(\bar{X}, \mathbb{Q}_p)(1)$ under the cup product is zero.

Composing the cycle class map with the Künneth projector, we therefore get a morphism

$$c_Z\colon\ \mathbb{Q}_p(-1) \to \ker\left(\bigwedge^2 \mathrm{H}^1(\bar{X}, \mathbb{Q}_p) \xrightarrow{\cup} H^2(\bar{X}, \mathbb{Q}_p)\right) \tag{36}$$

for every nice correspondence Z.

Proof of Lemma 4.17. Let $U[2] := \ker(U_2 \to U_1 = V)$, so that we have an exact sequence

$$1 \to U[2] \to U_2 \to V \to 1.$$

A Galois-stable quotient of U_2 surjecting onto V is therefore of the form U_2/W, where W is a Galois-stable subrepresentation of $U[2]$. So if we have a Galois-equivariant morphism $\gamma\colon U[2] \to \mathbb{Q}_p(1)$, then we can form a suitable quotient $U := U_2/\ker\gamma$ of U_2 via pushout:

$$\begin{tikzcd}
1 \arrow[r] & U[2] \arrow[r] \arrow[d, "\gamma"'] & U_2 \arrow[r] \arrow[d] & V \arrow[r] \arrow[d, "="'] & 1 \\
1 \arrow[r] & \mathbb{Q}_p(1) \arrow[r] & U \arrow[r] & V \arrow[r] & 1
\end{tikzcd}$$

To describe the representation $U[2]$, note that there is an anti-symmetric pairing

$$V \times V = U_1 \times U_1 \to U[2]$$

induced by the commutator map. It is surjective with kernel equal to the image of $H^2_{\text{ét}}(\bar{X}, \mathbb{Q}_p)$ inside $\wedge^2 V$ under the dual of the cup product $\cup\colon\ \wedge^2 \mathrm{H}^1(\bar{X}, \mathbb{Q}_p) \to H^2_{\text{ét}}(\bar{X}, \mathbb{Q}_p)^*$, so the Galois representation $U[2]$ can be described via an exact sequence

$$1 \to H^2_{\text{ét}}(\bar{X}, \mathbb{Q}_p) \xrightarrow{\cup^*} \wedge^2 V \to U[2] \to 1.$$

Hence we want a morphism

$$\gamma\colon\ \mathrm{Coker}(\cup^*\colon H^2_{\text{ét}}(\bar{X}, \mathbb{Q}_p) \to \wedge^2 V) \to \mathbb{Q}_p(1).$$

By Lemma 4.19, if Z is a nice correspondence, then we can take $\gamma := c(Z)^*(1)$, where c_Z^* is the dual of the map in (36). Then $U := U_2/\ker c(Z)^*(1)$ has the desired properties. Lemma 4.19 also implies that the subspace of $\mathrm{Pic}(X \times X) \otimes \mathbb{Q}$ consisting of 0 and the classes of nice correspondences has dimension $\rho(J) - 1$, completing the proof. □

In the following, we will denote the quotient $U_2/\ker c(Z)^*(1)$ associated to a nice correspondence Z by U_Z.

Remark 4.20. By the above, we can think of U as coming from a nontrivial cycle $Z \in \ker(\widetilde{\mathrm{AJ}}^*)$, where

$$\widetilde{\mathrm{AJ}}^*\colon\ \mathrm{NS}(J) \to \mathrm{NS}(X \times X) \to \mathrm{NS}(X)$$

is as in [DF19, Section 2].

Remark 4.21. Another construction of U_Z is described in [BBB$^+$19, §4.2]. It closely resembles the approach of Edixhoven–Lido [EL19]. Roughly speaking, we start with a cycle $Z \in \ker \widetilde{\mathrm{AJ}}^*$ as above, lift it to a line bundle L_Z on J whose restriction to X is trivial and we let U_Z denote the $\mathbb{Q}_p$-étale fundamental group of the $\mathbb{G}_m$-torsor L_Z^*. This yields the same U_Z as the one in the proof above, and probably (after taking a multiple and extending to the Néron model) the same $\mathbb{G}_m$-torsor $\mathcal{L}_Z$ as in Edixhoven-Lido. Betts [Bet] constructs local p-adic heights on $\mathcal{L}_Z(\mathbb{Q}_p)$, factoring through $\mathrm{H}^1_f(G_p, U_Z)$; his results could be used as an alternative way to our approach for computing local p-adic heights on $\mathrm{H}^1_f(G_p, U_Z)$ discussed below.

4.5. **Beyond potentially good reduction: the twisting construction.** To finish the proof of Theorem 4.12, we need to generalize Lemma 4.15 by

- allowing $[U, U] \simeq \mathbb{Q}_p(1)^{\oplus n}$, where $0 < n < \rho(J)$, rather than requiring $[U, U] \simeq \mathbb{Q}_p(1)$;
- removing the condition that X has potentially good reduction everywhere.

The first of these is trivial, since we have

$$\dim \mathrm{H}^1_f(G_p, \mathbb{Q}_p(1)^{\oplus n}) = n$$

by Example 3.2 and

$$\dim \mathrm{H}^1_f(G_T, \mathbb{Q}_p(1)^{\oplus n}) = 0$$

by Example 3.3. Moreover, the proof of Lemma 4.17 can be amended easily to show that we can always construct a suitable quotient $[U, U] \simeq \mathbb{Q}_p(1)^{\oplus \rho(J)-1}$. Hence the proof of Theorem 4.12 is complete once we show the following result:

Lemma 4.22. *Let U be a Galois-stable quotient of U_2 which sits in a Galois-equivariant short exact sequence* (30). *Then we have*

$$\dim \mathrm{Sel}(U) \le \mathrm{rk}(J(\mathbb{Q})) + \dim \mathrm{H}^1_f(G_T, [U, U]). \tag{37}$$

Proof. Note that (37) is a generalization of (35). Recall that to prove (35), we used that $\mathrm{Sel}(U) \subset \mathrm{H}^1_f(G_T, U)$, which might not hold in general, see Remark 4.2. To remedy this, suppose that $\alpha = (\alpha_\ell)_\ell \in \prod_{\ell \in T_0} j_\ell(X(\mathbb{Q}_\ell))$ is a set of *local conditions* such that $\alpha_\ell \in j_\ell(X(\mathbb{Q}_\ell))$ is ramified for some ℓ. Let $\mathrm{Sel}(U)_\alpha$ denote the preimage of α under $\prod_{\ell \in T_0} \mathrm{loc}_\ell$ and let $\beta \in \mathrm{Sel}(U)_\alpha$. The idea is to to use the twisting construction in non-abelian cohomology (see Appendix A) to show that $\mathrm{Sel}(U)_\alpha$ is isomorphic to a subvariety $\mathrm{H}^1_f(G_T, U^{(\beta)})'$ of $\mathrm{H}^1_f(G_T, U^{(\beta)})$. There is an analogue of the exact sequence (33) for $U^{(\beta)}$, leading to an upper bound

$$\dim \mathrm{H}^1_f(G_T, U^{(\beta)})' \le \dim \mathrm{H}^1_f(G_T, U^{(\beta)}) \le \dim \mathrm{H}^1_f(G_T, V) + \dim \mathrm{H}^1_f(G_T, [U, U]) \tag{38}$$

and hence

$$\dim \mathrm{Sel}(U)_\alpha \le \mathrm{rk}(J(\mathbb{Q})) + \dim \mathrm{H}^1_f(G_T, [U, U]).$$

Since $\mathrm{Sel}(U)$ is the disjoint union of finitely many $\mathrm{Sel}(U)_\alpha$ by Theorem 4.3, this proves the lemma.

We give a bit more detail. Letting U act on itself by conjugation, we form the twist $U^{(\beta)}$ of U by the U-torsor β. Let

$$f\colon\ \mathrm{H}^1(G_T, U) \to \mathrm{H}^1(G_T, U^{(\beta)})$$

denote the bijection from Proposition A.3, sending β to the trivial class. Then f maps crystalline classes to crystalline classes and preimages of $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ to preimages of $J(\mathbb{Q}) \otimes \mathbb{Q}_p$, see the proof of [BD18a, Lemma 2.6]. We define $\mathrm{H}^1_f(G_T, U^{(\beta)})'$ to be the reduced subscheme of $\mathrm{H}^1(G_T, U^{(\beta)})$ representing classes c such that

- $\mathrm{loc}_p(c)$ is crystalline

- $\mathrm{loc}_\ell(c) = 0$ for all $\ell \neq p$
- the projection of c to $\mathrm{H}^1(G_T, V)$ comes from an element of $J(\mathbb{Q}) \otimes \mathbb{Q}_p$

(compare with Definition 4.1). By the first two items, we have $\mathrm{H}^1_f(G_T, U^{(\beta)})' \subset \mathrm{H}^1_f(G_T, U^{(\beta)})$, and the discussion above shows that $f(\mathrm{Sel}(U)_\alpha) \subset \mathrm{H}^1_f(G_T, U^{(\beta)})'$. [13]

Now consider the twists $[U, U]^{(\beta)}$ and $V^{(\beta)}$, where, as above, U acts by conjugation. Since this action is unipotent, the two twisting morphisms are Galois-equivariant group isomorphisms. Hence the twisting construction turns (33) into a Galois-equivariant exact sequence

$$1 \to [U, U] \to U^{(\beta)} \to V \to 1,$$

resulting, via Kim's arguments in [Kim05] as in the discussion following Lemma 4.14, in an exact sequence of pointed varieties

$$\mathrm{H}^1(G_T, [U, U]) \to \mathrm{H}^1(G_T, U^{(\beta)}) \to \mathrm{H}^1(G_T, V)$$

and, via [Kim09], in another exact sequence of pointed varieties

$$\mathrm{H}^1_f(G_T, [U, U]) \to \mathrm{H}^1_f(G_T, U^{(\beta)}) \to \mathrm{H}^1_f(G_T, V)\,. \tag{39}$$

In the above, we are using by Remark A.4 the twisting morphism f is an isomorphism of schemes, since $\mathrm{H}^1(G_T, W)$ and $\mathrm{H}^1(G_T, W^{(\beta)})$ are affine schemes for $W \in \{[U, U], U, V\}$ by [Kim09]. Finally, (38) follows from (39) just like (35). □

4.6. **Extending the quadratic Chabauty Lemma.** Theorem 4.12 has been extended in several ways. First, there is an obvious extension to curves over imaginary quadratic fields, and in fact [BD18a, Lemma 3.2] already includes this case. One needs to restrict to such fields because of the crucial use of Example 3.3.

In [DF19], Dogra and Le Fourn extend Theorem 4.12 for Jacobians admitting an isogeny $J \to A \times B$ defined over $\mathbb{Q}$ such that $\mathrm{Hom}(A, B) = 0$ and satisfying a condition similar to the quadratic Chabauty condition, but phrased in terms of A and B. See [DF19, Proposition 1.6] for the precise statement. They use this result to show that $X(\mathbb{Q}_p)_2$ is finite for the nonsplit Cartan modular curve at prime level $N \neq p$, whenever this curve has genus at least 2 and at least one rational point.

In [BD18b], Balakrishnan and Dogra weaken the rank condition by replacing $\rho(J)$ by $\rho(J) + \mathrm{rk}(\mathrm{NS}(J_{\bar{\mathbb{Q}}})^{c=-1})$, where c denotes complex conjugation. In this setting, one needs to allow more general $[U, U]$. This essentially exhausts the Artin-Tate part of $[U_2, U_2]$, so new ideas are needed to prove finiteness of $X(\mathbb{Q}_p)_2$ for more general curves.

We expect that $X(\mathbb{Q}_p)_2$ is finite for $\mathrm{rk}(J(\mathbb{Q})) < g^2$, independently of $\mathrm{NS}(J_{\mathbb{Q}})$. In fact Balakrishnan–Dogra show in [BD18b, Lemma 2.6] that this would follow from a special case of the Bloch–Kato conjecture [BK90, Conjecture 5.3(i)], applied to $X \times X$. In the proof, they work directly with U_2, rather than a quotient.

5. Computing with quadratic Chabauty

Let $X/\mathbb{Q}$ be a nice curve of genus $g \geq 2$. In the previous section, we showed that when X satisfies the quadratic Chabauty condition (29), then there is a Galois-stable quotient $U = U_Z$ of U_2, depending on a nice correspondence Z, such that $X(\mathbb{Q}_p)_U$ is finite (and hence $X(\mathbb{Q}_p)_2$ is finite as well). We now discuss how to compute $X(\mathbb{Q}_p)_U$ in practice.

[13] It can be shown that f is indeed an isomorphism, but we don't need this in our argument.

Recall the situation discussed in Section 2.3, in particular Corollary[14] 2.30: When X is hyperelliptic and satisfies some additional conditions, then we use the Coleman–Gross construction of the p-adic height pairing

$$h(P-\infty,P-\infty)=h_p(P-\infty,P-\infty)+\sum_{\ell\neq p}h_\ell(P-\infty,P-\infty)$$

for $P\in X(\mathbb{Q})$. We showed that

(i) the function $P\mapsto h_p(P-\infty,P-\infty)$ extends to a locally analytic function $\theta\colon X(\mathbb{Q}_p)\to\mathbb{Q}_p$;
(ii) $h_\ell(z-\infty,z-\infty)=0$ for *integral*[15] points $z\in X(\mathbb{Q}_\ell)$;
(iii) h is a symmetric bilinear pairing on $J(\mathbb{Q})\otimes\mathbb{Q}_p$, and hence can be written as a linear combination of a basis of such pairings.

More precisely, the local height h_p had an interpretation as a sum of double Coleman integrals, which can be thought of as a solution to a p-adic differential equation. Since we assumed in Corollary 2.30 that log restricts to an isomorphism $J(\mathbb{Q})\otimes\mathbb{Q}_p\to\mathrm{H}^0(X_{\mathbb{Q}_p},\Omega^1)^*$, we can construct a basis in (iii) via products of single integrals. These are restrictions of locally analytic functions, so we get a function $\rho\colon X(\mathbb{Q}_p)\to\mathbb{Q}_p$ from (i) and (iii) with finitely many zeros which vanishes on integral points $P\in X(\mathbb{Q})$ (ii).

Remark 5.1. The presence of double Coleman integrals suggest that we have found some part of $X(\mathbb{Z}_p)_2$, the "quadratic" or depth 2 part of Kim's nonabelian Chabauty, since $X(\mathbb{Q}_p)_n$ or $X(\mathbb{Z}_p)_n$ are cut out by n-fold iterated integrals [Kim09, BDCKW18].

The difficulty in extending this construction to *rational points* is that we do not have a good way to control $\sum_{\ell\neq p}h_\ell(P-\infty,P-\infty)$ (or a similar local height in the non-hyperelliptic case) for general $P\in X(\mathbb{Q})$. This is where we use Chabauty–Kim: Recall that for $\ell\neq p$, the image $j_{U,\ell}(X(\mathbb{Q}_\ell))$ inside $\mathrm{H}^1(G_\ell,U)$ is finite by Theorem 4.3, and is trivial if X has potentially good reduction at ℓ by Remark 4.4. Therefore we want (local and global) p-adic heights which factor through Kim's unipotent Kummer maps $j_{U,v}$. It turns out that Nekovář's construction of p-adic heights discussed in Section 3, based on p-adic Hodge theory, makes this possible, via the twisting construction in non-abelian cohomology.

Recall that for a prime v the local Nekovář-height h_v is defined on mixed extensions of p-adic G_v-representations with graded pieces $\mathbb{Q}_p,V$ and $\mathbb{Q}_p(1)$. We will see below that we can take a torsor $P\in\mathrm{H}^1(G_v,U)$ and produce such a mixed extension $\tau_v(P)$ (depending on Z). In fact, the same construction produces a global mixed extension $\tau(P)$ for $P\in\mathrm{H}^1(G_T,U)$. We deduce that the function

$$\mathrm{Sel}(U)\to\mathbb{Q}_p\,;\quad P\mapsto h_\ell(\tau_\ell(\mathrm{loc}_\ell(P))) \tag{40}$$

has finite image, and if X has potentially good reduction at ℓ, then the image of the map (40) is trivial.

To ease notation, we write

$$A(x):=\tau(j_{U,p}(x))$$

for $x\in X(\mathbb{Q}_v)$. This assigns a mixed extension of G_v-representations with graded pieces $\mathbb{Q}_p,V$ and $\mathbb{Q}_p(1)$ to a $\mathbb{Q}_p$-rational point on X.

We now use this to give an analogue of Theorem 2.28 in the simplest situation covered by Theorem 4.12, namely

(i) $r=g>1$,
(ii) $\log\colon J(\mathbb{Q})\otimes\mathbb{Q}_p\to\mathrm{H}^0(X_{\mathbb{Q}_p},\Omega^1)^*$ is an isomorphism[16], and

[14] More generally, see Theorem 2.28.
[15] See Proposition 2.29 for a more general statement.
[16] If this fails, we can simply use Chabauty–Coleman to compute the rational points.

(iii) $\rho(J) > 1$.

Under these assumptions,

$$\mathrm{H}^1_f(G_{\mathbb{Q}}, V) \xrightarrow{\mathrm{loc}_p} \mathrm{H}^1_f(G_p, V) \xrightarrow{\log} \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$$

is an isomorphism, so by Poincaré duality we may view the global height h as a bilinear pairing

$$h\colon\ \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^* \times \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^* \to \mathbb{Q}_p\ .$$

By abuse of notation, we may replace the target of the projection maps π_1, π_2 introduced in (20) by $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$.

As in Section 3.2, we fix

(a) an idèle class character $\chi\colon \mathbb{A}^*_{\mathbb{Q}}/\,\mathbb{Q}^* \to \mathbb{Q}_p$,
(b) a splitting s of the Hodge filtration on V_{dR} such that $\ker(s)$ is isotropic with respect to the dual of the cup product pairing.

Recall from Remark 3.5 that the isotropicity condition implies that h is symmetric. The following result sums up the theoretical foundation for our approach to computing rational points via p-adic heights:

Theorem 5.2 (Quadratic Chabauty for rational points [BD18a, Proposition 5.5])**.** *Let $X/\,\mathbb{Q}$ be a nice curve, let J be the Jacobian of X, assume that* $\operatorname{rk} J(\mathbb{Q}) = g > 1$, *and that $\rho(J) > 1$. Choose a prime p of good reduction for X such that* $\log\colon J(\mathbb{Q}) \otimes \mathbb{Q}_p \to \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ *is an isomorphism. Choose a nice correspondence Z on X and let $U = U_Z$. Finally, fix a basis $\psi_1, \dots, \psi_N$ of $(\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^* \otimes \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*)^*$.*

Then there exist computable constants $\alpha_i \in \mathbb{Q}_p$ such that the function $X(\mathbb{Q}_p) \to \mathbb{Q}_p$ defined by

$$\rho(x) := h_p(A(x)) - \sum_{i=1}^{N} \alpha_i \psi_i \circ (\pi_1, \pi_2)(A(x))$$

has finitely many zeros and takes values in a finite set $S \subset \mathbb{Q}_p$ on $X(\mathbb{Q}_p)_U$.

If X has everywhere potentially good reduction, then this holds for $S = \{0\}$.

Proof. By the above, $\rho(X(\mathbb{Q}_p)_U)$ is contained in the finite subset of $\mathbb{Q}_p$ coming from the possible values of the functions in (40). To show that ρ only has finitely many zeros, we use that by [BD18b, Lemma 3.7],

$$(\pi_*,\ h_p \circ \tau_p)\ :\ \mathrm{H}^1_f(G_p, U) \longrightarrow \mathrm{H}^1_f(G_p, V) \times \mathbb{Q}_p$$

is an isomorphism of schemes. Because $j_{U,p}$ has Zariski dense image [Kim09], the result follows. □

To fill in the gaps in the discussion above, we will construct τ (and τ_p) in the next subsection. This will be done by first constructing a mixed extension A_Z as a quotient of the universal enveloping algebra of the Lie algebra of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}})_{\mathbb{Q}_p}$, following the construction of U itself. Then we define τ via the twisting construction in non-abelian cohomology.

In Section 5.2, we discuss how to compute $\pi_1(A(x))$, $\pi_2(A(x))$ and $h_p(A(x))$ for $x \in X(\mathbb{Q}_p)$. Further computational issues are addressed in Section 5.3; there, we also give an algorithmic version of Theorem 5.2 (Algorithm 5.27), and we describe how the set S can be computed and how the coefficients α_i can be derived for a suitable basis $\{\psi_i\}$. In particular, this will show:

Corollary 5.3. *In the situation of Theorem 5.2, the function ρ and the set S are explicitly computable.*

Finally, we give a worked example, determining rational points on the modular curve $X_0(167)/w_{67}$ in Section 5.4, and we discuss some possible future directions in Section 5.5.

Remark 5.4. In Theorem 5.2, the dependence on Z is hidden by our notation. In fact, both the mixed extensions $A(x)$ (and thus the function ρ) and the set S depend on Z. Due to our crucial use of local heights, ρ depends on the choices of χ and s, and S depends on χ.

Remark 5.5. In [BD18a, Section 6], Balakrishnan and Dogra show that for $z \in X(\mathbb{Q}_v)$, the mixed extension $A(x)$ can be expressed geometrically, as the mixed extension associated to the divisors $z - b$ and $D_Z(b, z)$ on X of degree 0 as in [Nek93, Section 5]. They use this to compute the rational points on a bielliptic genus 2 curve over $\mathbb{Q}$ and the $\mathbb{Q}(i)$-rational points on the bielliptic genus 2 curve $X_0(37)$, answering a question of Daniels and Lozano-Robledo. Here

$$D_Z(b, z) = \Delta^*(Z) - i_{1,b}^*(Z) - i_{2,z}^*(Z)\,,$$

where $i_{1,b}(x) = (x, b) \in X \times X$, $i_{2,z}(x) = (z, x)$ and $\Delta\colon X \to X \times X$ is the diagonal embedding. One needs that Z does not intersect $(\Delta - X \times x_1 - x_2 \times X)$ for any pair $(x_1, x_2) \in X \times X$. In particular, this approach requires that we have explicit equations for Z as a divisor on $X \times X$. When X is a bielliptic curve of genus 2, then Z is a sum of sections, and the heights can be computed on the corresponding elliptic curves.

In work in progress of Besser, Müller, and Srinivasan, a version of Theorem 5.2 is proved by applying the construction of Coleman–Gross and p-adic Arakelov theory [Bes05] directly to the divisors $z - P$ and $D_Z(b, P)$ without relying on fundamental groups or p-adic Hodge theory. This also leads to an alternative way to compute the function ρ and the set S.

Remark 5.6. What if we have two nice correspondences Z, Z'? Under our assumptions, the corresponding sets $X(\mathbb{Q}_p)_{U_Z}$ and $X(\mathbb{Q}_p)_{U_{Z'}}$ are the same if and only if Z and Z' are dependent[17], see [BD18a, Remark 5.7].

Remark 5.7. In the remainder of these notes, we discuss how Theorem 5.2 can be turned into a method for *computing* the rational points for a given curve X. However, it is also possible to *bound* $\#X(\mathbb{Q})$ for curves X satisfying our assumptions; see [BD19a]. See also [DF19] for an extension.

5.1. **Twisting and mixed extensions.**

In this section, we first construct a mixed extension A_Z of Galois representations with graded pieces $\mathbb{Q}_p$, V and $\mathbb{Q}_p(1)$, depending on a nice correspondence Z on X, which we fix. The idea is to mimic the construction of U_Z, but on the Lie algebra side. For more details, see [BD18a, Section 5], and see [BD18b, Sections 3,4] for a generalization.

Recall that U_Z is a unipotent quotient of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}$, the unipotent $\mathbb{Q}_p$-étale fundamental group of $X_{\overline{\mathbb{Q}}}$. We first define

$$\mathbb{Z}_p[[\pi_1^{\text{ét},(p)}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}]] := \varprojlim \mathbb{Z}_p[\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)]/N$$

where the limit is over all group algebras of finite quotients of p-power order [Qui69, Appendix A].

Letting I denote the augmentation ideal of $\mathbb{Q}_p \otimes \mathbb{Z}_p[[\pi_1^{\text{ét},(p)}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}]]$, we define the algebra

$$A_n := A_n(b) := \mathbb{Q}_p \otimes \mathbb{Z}_p[[\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}]]/I^{n+1}.$$

Then A_n is a quotient of the enveloping algebra of U_n; in fact the limit of the A_n is (isomorphic to) the pro-universal enveloping algebra of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}$, see [CK10, §2]. Moreover, there is an action of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)_{\mathbb{Q}_p}$ on A_n which factors through U_n.

For $n = 1, 2$, we can describe A_n as follows:

$$1 \to V \to A_1 \to \mathbb{Q}_p \to 1,$$

[17] as elements of the space of nice correspondences (together with 0); i.e. as elements of $\ker(\mathrm{NS}(J) \to \mathrm{NS}(X))$

and, similar to the situation[18] considered in Section 4.4, there is an exact sequence

$$1 \to \operatorname{coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} V^{\otimes 2}) \to A_2 \to A_1 \to 1, \tag{41}$$

coming from the isomorphism $I^2/I^3 \cong \operatorname{coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} V^{\otimes 2})$. Following the argument in Lemma 4.17, we can define a quotient of A_2 using Z as follows.

Definition 5.8. The representation $A_Z := A_Z(b)$ is the pushout of A_2 by

$$\mathrm{cl}_Z^*\colon \operatorname{coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} V^{\otimes 2}) \to \mathbb{Q}_p(1).$$

Note that U_Z acts faithfully on A_Z on the left; the action is unipotent with respect to the I-adic filtration. In fact we have:

Lemma 5.9. *The I-adic filtration gives A_Z the structure of a crystalline mixed extension of G_T-representations with graded pieces $\mathbb{Q}_p, V, \mathbb{Q}_p(1)$.*

To show that A_Z is crystalline, one first proves that A_2 is crystalline using [Ols11, Theorem 1.4].

Recall that we want to construct a mixed extension with graded pieces $\mathbb{Q}_p, V, \mathbb{Q}_p(1)$ from a given torsor $P \in \mathrm{Sel}(U_Z)$. Via the action of U_Z on A_Z, this can now be achieved by twisting A_Z (see Appendix A).

Definition 5.10. For $P \in \mathrm{H}^1(G_T, U)$ we define

$$\tau(P) := P \times_{U_Z} A_Z.$$

When $x \in X(\mathbb{Q})$ and P is the path torsor $P(b,x) := \pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b, x)$, then we define $A(x) := \tau(P)$.

The most important features of the twisting map τ are summarized in the following lemma. Since we want to focus on computational methods, we refer to [BD18a, §5.1] and [BD18b, §3.3] for proofs of these assertions.

Lemma 5.11. *Let $P \in \mathrm{H}^1(G_T, U)$. Then we have the following:*

(i) $\tau(P)$ is a mixed extension of G_T-representations with graded pieces $\mathbb{Q}_p, V, \mathbb{Q}_p(1)$.
(ii) The map τ is injective.
(iii) If P is crystalline at p, then $\tau(P)$ is crystalline at p as well.
(iv) We have $\pi_1(\tau(P)) = P \times_{U_Z} A_1$ and $\pi_2(\tau(P)) = P \times_{U_Z} IA_Z$.

Remark 5.12. Similarly, we can construct a mixed extension $\tau_v(P)$ of G_v-representations from a local torsor $P \in \mathrm{H}^1(G_v, U)$, with the special case $A(x)$ for $x \in X(\mathbb{Q}_v)$. The analogue of Lemma 5.11 remains valid for τ_v.

For our algorithm, we need to describe $\pi_i(A(x))$ explicitly for $i = 1, 2$ and $x \in X(\mathbb{Q})$. See [BD18a, § 5.2] and [BD18b, Lemma 3.5] for more details. We find that on $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$, we have

$$\pi_1(A(x)) = \log([x-b])$$

(similar to Section 2.3), but $\pi_2(A(x))$ is more difficult to describe, since it depends on Z. In $\mathrm{Ext}^1(V, \mathbb{Q}_p(1))$ we have

$$[P(b,x) \times_{U_Z} IA_Z] = E_Z(\pi_1(A(x))) + [IA_Z],$$

[18] Note that $\operatorname{coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} V^{\otimes 2}) \cong \operatorname{coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} \wedge^2 V) \oplus \mathrm{Sym}^2 V$; in Section 4.4 there was no $\mathrm{Sym}^2 V$ summand.

where E_Z is the endomorphism of $\mathrm{H}^1_f(G_T, V)$ induced by Z. So let $c_Z \in \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ be the constant functional corresponding to $[IA_Z]$. This is a p-adic logarithm of the Chow-Heegner point associated to Z, see [BDM+19, Remarks 3.11 and 5.6] and [DRS12]. Then, in $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$, we find

$$\pi_2(A(x)) = E_Z(\log([x-b])) + c_Z\,, \tag{42}$$

where, by abuse of notation, E_Z denotes the endomorphism of $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ induced by Z.

In practice, we can read off $\pi_i(A(x))$ directly from our explicit description of $A(x)$, see (48) below.

5.2. **Algorithms for the local height at p.** To compute $X(\mathbb{Q}_p)_U$, we need to compute $h_p(A(x))$, so we need to choose a nice correspondence Z and write the locally analytic function

$$\theta\colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$$
$$x \mapsto h_p(A(x))$$

as a power series on every residue disk of $X(\mathbb{Q}_p)$. In this section, we follow [BDM+19] closely.

By Proposition 3.12 we have the formula

$$h_p(A(x)) = \chi_p(\gamma_\phi - \gamma_{\mathrm{Fil}} - \beta_\phi^{\mathrm{T}} \cdot s_1(\alpha_\phi) - \beta_{\mathrm{Fil}}^{\mathrm{T}} s_2(\alpha_\phi)), \tag{43}$$

for the local height of the mixed extension $A(x)$. The quantities on the right hand side only depend on the filtered ϕ-module $D_{\mathrm{cris}}(A(x))$, so it suffices to compute an explicit description of this. In particular, we do not need to construct the representation $A(x)$ at all.

We will utilize the de Rham realization of A_Z: this is a filtered connection $\mathcal{A}_Z$ with Frobenius structure (more precisely, a unipotent isocrystal), and Olsson's comparison theorem [Ols11, Theorem 1.4] then implies the following isomorphism of filtered ϕ-modules:

Lemma 5.13 ([BDM+19, Lemma 5.4])**.** *We have*

$$x^*\mathcal{A}_Z = D_{\mathrm{cris}}(A(x)), \quad \text{for all } x \in X(\mathbb{Q}_p).$$

Hence it suffices to construct the Hodge filtration and Frobenius structure of $\mathcal{A}_Z$. We will construct the filtered connection $\mathcal{A}_Z$ as a quotient of a universal connection $\mathcal{A}_2^{\mathrm{dR}}$ via push-out, similar to the construction of U_Z and A_Z. The universal properties of A_2^{dR} then allow us to determine the Hodge filtration and Frobenius structure of $\mathcal{A}_Z$ uniquely. The Hodge filtration is determined by the Hodge filtration on its graded pieces, as well as its global nature: that starting with an affine piece Y, it extends nicely to X, by work of Hadian. The Frobenius structure is determined by its action on the unit vector [BDM+19, Lemma 5.2], which is essentially an initial condition for our p-adic differential equation that we can extend via parallel transport.

Definition 5.14. A filtered connection (V, ∇) is a connection on X together with an exhaustive, descending filtration

$$\cdots \supseteq \mathrm{Fil}^i V \supseteq \mathrm{Fil}^{i+1} V \supseteq \cdots$$

satisfying Griffiths transversality

$$\nabla(\mathrm{Fil}^i V) \subseteq \mathrm{Fil}^{i-1} V \otimes \Omega^1.$$

We use the Tannakian formalism, see [Del90, DM82]. Let $\mathcal{C}^{\mathrm{dR}}(X)$ be the category of unipotent vector bundles[19] with connection on X. The fiber functor b^* at the base point $b \in X(\mathbb{Q})$ gives $\mathcal{C}^{\mathrm{dR}}(X)$ the structure of a neutral Tannakian category. Its fundamental group $\pi_1^{\mathrm{dR}}(X, b)$ is pro-unipotent (it is the direct limit of its n-step unipotent quotients $U_n^{\mathrm{dR}}(b)$), so we obtain a unipotent Tannakian category.

[19] In general, one would also require flatness, but this is automatic for curves.

For $n \neq 1$, we define

$$A_n^{\mathrm{dR}}(b) := A(\mathcal{C}^{\mathrm{dR}}(X, b^*))/I^{n+1},$$

where $A(\mathcal{C}^{\mathrm{dR}}(X, b^*))$ is the pro-universal enveloping algebra with augmentation ideal I. For $x \in X(\mathbb{Q}_p)$, we have associated path torsors

$$A_n^{\mathrm{dR}}(b, x) := A_n^{\mathrm{dR}}(b) \times_{\pi_1^{\mathrm{dR}}(X,b)} \pi_1^{\mathrm{dR}}(X; b, x).$$

The theory of universal objects in unipotent Tannakian categories (see [BDM+19, Appendix A.1] and [BD18b, Appendix A]) shows that there is a universal n-step unipotent object (see [BDM+19, Definition A.2, Lemma A.3])

$$\mathcal{A}_n^{\mathrm{dR}} := \mathcal{A}_n^{\mathrm{dR}}(b)$$

associated to the $\pi_1^{\mathrm{dR}}(X, b)$-representation $A_n^{\mathrm{dR}}(b)$. In other words, if $\mathcal{V}$ is an n-step unipotent connection on X and $v \in b^*\mathcal{V}$, then there is a unique morphism of connections $f\colon \mathcal{A}_n^{\mathrm{dR}} \to \mathcal{V}$ such that $b^*(f)(e_n) = v$ (e_n being the unit element). As discussed in [Kim09], $\mathcal{A}_n^{\mathrm{dR}}$ carries a Hodge filtration $\mathrm{Fil}^\bullet$ satisfying the following universal property.

Theorem 5.15 (Hadian [Had11])**.** *For all $n > 0$ the Hodge filtration $\mathrm{Fil}^\bullet$ on $\mathcal{A}_n^{\mathrm{dR}}(b)$ is the* unique *filtration such that*

(1) $\mathrm{Fil}^\bullet$ makes $(\mathcal{A}_n^{\mathrm{dR}}(b), \nabla)$ into a filtered connection.
(2) The natural maps induce a sequence of filtered connections:

$$V_{\mathrm{dR}}^{\otimes n} \otimes \mathcal{O}_X \to \mathcal{A}_n^{\mathrm{dR}}(b) \to \mathcal{A}_{n-1}^{\mathrm{dR}}(b) \to 0.$$

(3) The identity element of $A_n^{\mathrm{dR}}(b)$ lies in $\mathrm{Fil}^0 A_n^{\mathrm{dR}}(b)$.

In analogy with (41), we obtain an exact sequence of filtered vector bundles

$$0 \to \operatorname{coker}(\mathrm{H}^2_{\mathrm{dR}}(X)^* \xrightarrow{\cup^*} V_{\mathrm{dR}}^{\otimes 2}) \otimes \mathcal{O}(X) \to \mathcal{A}_2^{\mathrm{dR}} \to \mathcal{A}_1^{\mathrm{dR}} \to 0.$$

Recall the discussion of nice correspondences in Section 4.4; the statements there have natural de Rham analogues. We will denote the Tate class in $\mathrm{H}^1_{\mathrm{dR}}(X/\mathbb{Q}) \otimes \mathrm{H}^1_{\mathrm{dR}}(X/\mathbb{Q})$ induced by a nice correspondence Z (and its matrix representation with respect to the basis $\{\omega_i\}$) also by Z; in analogy with (36), Z induces a map

$$\operatorname{coker}(\mathrm{H}^2_{\mathrm{dR}}(X)^* \xrightarrow{\cup^*} V_{\mathrm{dR}}^{\otimes 2}) \to \mathbb{Q}_p(1). \tag{44}$$

As before, we can now form a quotient by push-out, noting that it carries the structure of a filtered connection.

Definition 5.16. The filtered connection $\mathcal{A}_Z := \mathcal{A}_Z(b)$ is the pushout of $\mathcal{A}_2^{\mathrm{dR}}$ by the map (44).

Remark 5.17. The important part of Theorem 5.15 is the *uniqueness*. Below, the sub-bundle Fil^0 of the quotient $\mathcal{A}_Z$ of $\mathcal{A}_2^{\mathrm{dR}}$ is determined in an explicit trivialization on Y, by writing down a general form for a basis, solving for the coefficients using the fact that it extends uniquely to X and satisfies the three conditions.

Remark 5.18. In our setting, Griffiths transversality is actually an empty condition, since $\mathrm{Fil}^1 \mathcal{A}_Z = 0$ and $\mathrm{Fil}^{-1} \mathcal{A}_Z = \mathcal{A}_Z$.

5.2.1. *Computing the Hodge filtration.* The Hodge filtration on $\mathcal{A}_Z$ is determined by the Hodge filtration on its graded pieces, via the universal property in Hadian's theorem.

We first determine it on an affine open $Y \subseteq X$. This is easier than working directly on X, since unipotent vector bundles on Y are trivial. Let $b \in Y(\mathbb{Q})$ and suppose

$$\#(X \smallsetminus Y)(\overline{\mathbb{Q}}) = d$$

and let $L/\mathbb{Q}$ be a finite extension over which all points of $D = X \smallsetminus Y$ are defined.

Choose differentials $\omega_0, \dots, \omega_{2g+d-2} \in \mathrm{H}^0(Y_{\overline{\mathbb{Q}}}, \Omega^1)$ such that

(1) The differentials $\omega_0, \dots, \omega_{2g-1}$ are of the second kind on X and form a symplectic basis of $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbb{Q}})$ with respect to the cup product pairing.
(2) The differentials
$$\omega_{2g}, \dots, \omega_{2g+d-2}$$
are of the third kind on X, by which we mean that all poles are simple; in this section, we do not require integer residues.

The connection $\mathcal{A}_n^{\mathrm{dR}}(X)|_Y$ can be obtained as a quotient of a connection $\mathcal{A}_n^{\mathrm{dR}}(Y)$ having similar universal properties, but on Y. More precisely $\mathcal{A}_n^{\mathrm{dR}}(X)|_Y$ is the maximal quotient of $\mathcal{A}_n^{\mathrm{dR}}(Y)$ which extends to a holomorphic connection on X. The connection $\mathcal{A}_n^{\mathrm{dR}}(Y)$ can be computed explicitly via a universal property due to Kim (see [BDM+19, Section 4.2]). It follows from this and from [BDM+19, Remark 4.9] that we may choose a trivialization

$$s_0(b, \cdot) \colon (\mathbb{Q} \oplus V_{\mathrm{dR}} \oplus \mathbb{Q}(1)) \otimes \mathcal{O}_Y \xrightarrow{\sim} \mathcal{A}_Z|_Y$$

such that the connection ∇ on $\mathcal{A}_Z$ via this trivialization is given by

$$s_0^{-1} \nabla s_0 = \mathrm{d} + \Lambda,$$

where

$$\Lambda = -\begin{pmatrix} 0 & 0 & 0 \\ \vec{\omega} & 0 & 0 \\ \eta & \vec{\omega}^{\mathrm{T}} Z & 0 \end{pmatrix}$$

for some η of the third kind on X, and where

$$\vec{\omega} = \{\omega_0, \dots, \omega_{2g-1}\}.$$

This is to be understood with respect to a basis

$$\{1, T_0, \dots, T_{2g-1}, S\}$$

of the 2-step unipotent filtration, where $T_0, \dots, T_{2g+d-2}$ is the basis of $V_{\mathrm{dR}}(Y) = \mathrm{H}^1_{\mathrm{dR}}(Y)^*$ dual to $\omega_0, \dots, \omega_{2g+d-2}$.

Lemma 5.19 ([BDM+19, Lemma 4.10]). *The differential η in Λ is the unique differential satisfying the following two conditions:*

(1) η is in the span of
$$\{\omega_{2g}, \dots, \omega_{2g+d-2}\}.$$
(2) The connection ∇ extends to a holomorphic connection on the whole of X.

The proof uses a unipotent gauge transformation C_x at all $x \in D = X \setminus Y$, which we now introduce. In a formal neighborhood of a point $x \in X \setminus Y$ with local coordinate t_x, we can find a trivialization of $\mathcal{A}_Z$

$$s_x \colon ((\mathbb{Q} \oplus V_{\mathrm{dR}} \oplus \mathbb{Q}(1)) \otimes L[[t_x]], \mathrm{d}) \xrightarrow{\sim} (\mathcal{A}_Z|_{L[[t_x]]}, \nabla)$$

since $\mathcal{A}_Z$ is unipotent and any unipotent connection on a formal disk is trivial and we define

$$C_x = s_x^{-1} s_0 = \begin{pmatrix} 1 & 0 & 0 \\ \Omega_x & 1 & 0 \\ g_x & \Omega_x^{\mathrm{T}} Z & 1 \end{pmatrix},$$

where

$$\mathrm{d}\Omega_x = -\vec{\omega} \qquad \mathrm{d}g_x = \Omega_x^{\mathrm{T}} Z \,\mathrm{d}\Omega_x - \eta.$$

We now describe the Hodge filtration on $\mathcal{A}_Z$ with respect to s_0, i.e. we give an explicit isomorphism

$$s^{\mathrm{Fil}} \colon ((\mathbb{Q} \oplus V_{\mathrm{dR}} \oplus \mathbb{Q}(1)) \otimes \mathcal{O}_Y) \xrightarrow{\sim} \mathcal{A}_Z \tag{45}$$

that respects the Hodge filtration on both sides.

It suffices to describe $\mathrm{Fil}^0 \mathcal{A}_Z$; define

$$\gamma_{\mathrm{Fil}} \in \mathcal{O}_Y, \qquad b_{\mathrm{Fil}} = (b_g, \dots, b_{2g-1})^{\mathrm{T}} \in \mathbb{Q}^g$$

by the requirement that

$$\gamma_{\mathrm{Fil}}(b) = 0$$

and for all $x \in D$:

$$g_x + \gamma_{\mathrm{Fil}} - b_{\mathrm{Fil}}^{\mathrm{T}} N^{\mathrm{T}} \Omega_x - \Omega_x^{\mathrm{T}} Z N N^{\mathrm{T}} \Omega_x \in L[[t_x]]$$

where

$$N = (0_g, 1_g)^{\mathrm{T}} \in M_{2g \times g}(\mathbb{Q}).$$

Theorem 5.20 ([BDM+19, Theorem 4.11])**.** *We can choose s^{Fil} in (45) such that the restriction of $s_0^{-1} s^{\mathrm{Fil}}$ to $(\mathbb{Q} \oplus \mathrm{Fil}^0 V_{\mathrm{dR}}) \otimes \mathcal{O}_Y$ is given by the $(2g+2) \times (g+1)$ matrix*

$$\begin{pmatrix} 1 & 0 \\ 0 & N \\ \gamma_{\mathrm{Fil}} & b_{\mathrm{Fil}}^{\mathrm{T}} \end{pmatrix}.$$

From this result, we obtain the following algorithm for computing γ_{Fil} and b_{Fil}, as desired for (43).

Algorithm 5.21 (The Hodge filtration on $\mathcal{A}_Z$)**.**

(1) Compute local coordinates t_x at each $x \in D$.
(2) For each $x \in D$ compute Laurent series expansions of the elements in $\vec{\omega}$ at x to large enough precision, which is at least mod $t_x^{d_x}$, where d_x is the order of the largest pole occurring.
(3) Compute the vector Ω_x, defined by
$$d\Omega_x = -\vec{\omega}_x.$$
(4) Solve for η as the unique linear combination of $\omega_{2g}, \dots, \omega_{2g+d-2}$ such that $d\Omega_x^{\mathrm{T}} Z \Omega_x - \eta$ has residue zero at all $x \in D$.
(5) Solve the system of equations for g_x such that $dg_x = \Omega_x^{\mathrm{T}} Z d\Omega_x - \eta$.
(6) Compute the vector of constants $b_{\mathrm{Fil}} = (b_g, \dots, b_{2g-1}) \in \mathbb{Q}^g$ and the function γ_{Fil} characterized by $\gamma_{\mathrm{Fil}}(b) = 0$ and
$$g_x + \gamma_{\mathrm{Fil}} - b_{\mathrm{Fil}}^{\mathrm{T}} N^{\mathrm{T}} \Omega_x - \Omega_x^{\mathrm{T}} Z N N^{\mathrm{T}} \Omega_x \in L[[t_x]],$$
where $N = (0_g, 1_g)^{\mathrm{T}} \in M_{2g \times g}(\mathbb{Q})$. Set $\beta_{\mathrm{Fil}} = (0, \dots, 0, b_g, \dots, b_{2g-1})^{\mathrm{T}}$.

Remark 5.22. If X is hyperelliptic, then we have that $\eta = 0$ and $\beta_{\mathrm{Fil}} = (0, \dots, 0)^{\intercal}$ by [BD18b, Lemma 6.5].

5.2.2. *Computing the Frobenius structure.* The importance of the filtered connection discussed above is that we can base change $\mathcal{A}_Z$ to $\mathbb{Q}_p$. This base change has a Frobenius structure and we get an isomorphism of filtered ϕ-modules

$$x^* \mathcal{A}_Z = D_{\mathrm{cris}}(A(x))$$

for all $x \in X(\mathbb{Q}_p)$. We will describe the Frobenius structure on the isocrystal $\mathcal{A}_Z^{\mathrm{rig}}(\overline{b})$.

For now, we will focus on the affine story. For details on the rigid structure, see the appendix of [BDM+19]. Let A be an affinoid algebra over K, a complete discrete valuation field of characteristic 0, and let $A^\dagger$ be its weak completion. Let $\overline{A} = A^\dagger/\pi$ where π is a uniformizer of R, the ring of integers of K.

The main idea behind isocrystals and their relation to iterated Coleman integrals is that the integrals can be seen as solutions to certain p-adic differential equations. For instance, the iterated Coleman integral

$$\int \omega_n \dots \omega_1$$

is the y_n-coordinate of a solution to the following system of p-adic differential equations:

$$dy_0 = 0, dy_1 = \omega_1 y_0, \dots, dy_n = \omega_n y_{n-1},$$

or equivalently,

$$d\vec{y} = \Omega\vec{y}, \text{ where } \Omega := \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ \omega_1 & 0 & \cdots & 0 & 0 \\ 0 & \omega_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \omega_n & 0 \end{pmatrix},$$

with $y_0 = 1$. This is a unipotent differential equation.

Definition 5.23. A unipotent isocrystal on $\overline{A}$ is an $A^\dagger$-module M together with an (integrable) connection

$$\nabla : M \to M \otimes_{A^\dagger} \Omega^1(\otimes K)$$

that is an iterated extension of trivial connections, where the trivial connection is $\mathbb{1} = (A^\dagger, d)$.

A morphism of unipotent isocrystals is a map of $A^\dagger$-modules that is horizontal (i.e. commutes with connection).

There is an analogous category of unipotent isocrystals via rigid triples (see [BDM+19, Appendix A]). Let $\mathcal{C}^{\mathrm{rig}}(X_{\mathbb{F}_p})$ be the category of (rigid) unipotent isocrystals on the special fiber of X. This has an action of Frobenius on path torsors $\pi_1^{\mathrm{rig}}(X_{\mathbb{F}_p}, \overline{b}, \overline{x})$ of π_1^{rig}, and hence on the n-step unipotent quotients:

$$\phi_n : A_n(\overline{b}, \overline{x}) \to A_n(\overline{b}, \overline{x}).$$

There is a Frobenius structure on $\mathcal{A}_n^{\mathrm{rig}}(\overline{b})$, the universal n-step object. The Frobenius structure is an isomorphism

$$\Phi_n : \phi^* \mathcal{A}_n^{\mathrm{rig}}(\overline{b}) \xrightarrow{\sim} \mathcal{A}_n^{\mathrm{rig}}(\overline{b})$$

of overconvergent unipotent isocrystals, where ϕ is a lift of Frobenius from the special fiber.

There is a corresponding de Rham realization pullback Frobenius on $X_{\mathbb{F}_p}$, which gives a Frobenius action on $\pi_1^{\mathrm{dR}}(X_{\mathbb{Q}_p}, b, x)$ and a Frobenius operator on the n-step unipotent quotients

$$\phi_n(b, x) : A_n^{\mathrm{dR}}(b, x) \to A_n^{\mathrm{dR}}(b, x).$$

Theorem 5.24 (Chiarelletto-Le Strum [CLS99])**.** *There is an equivalence of categories*

$$\mathcal{C}^{\mathrm{dR}}(X_{\mathbb{Q}_p}) \xrightarrow{\sim} \mathcal{C}^{\mathrm{rig}}(X_{\mathbb{F}_p})$$

given by the analytification functor $(\cdot)^{an}$.

For any $x \in X(\mathbb{Q}_p)$ with reduction $\overline{x}$, we have a canonical isomorphism of fiber functors

$$i_x : \overline{x}^* \circ (\cdot)^{an} \equiv x^*$$

such that if $x, y \in X(\mathbb{Q}_p)$ belong to the same residue disk, the canonical isomorphism $i_x \circ i_y^{-1}$ is given by parallel transport $T_{x,y}$ along the connection.

Let b_0 and x_0 be Teichmüller representatives of b and x, respectively. We relate the Frobenius operator $\phi_n(\cdot)$ to the isocrystal $\mathcal{A}_n^{\mathrm{rig}}(\bar{b})$ by defining

$$\phi_n(b,x) = \tau_{b,x} \circ \phi_n(b_0,x_0) \circ \tau_{b,x}^{-1}$$

where $\tau_{b,x}$ is the canonical isomorphism from Theorem 5.24, given by

$$\begin{aligned} \tau_{b,x} : \mathrm{Hom}(b_0^*, x_0^*) &\xrightarrow{\sim} \mathrm{Hom}(b^*, x^*) \\ g &\mapsto T_{x,x_0} \circ g \circ T_{b_0,b}. \end{aligned}$$

We can describe $\tau_{b,x}$ on $A_n^{\mathrm{dR}}(b,x)$ via formal integration on residue disks. Since $A_n^{\mathrm{dR}}(b,x)$ is a quotient of $A_n^{\mathrm{dR}}(Y)(b,x)$, it suffices to describe the parallel transport here.

Recall that we've fixed s_0 where

$$s_0(b,x) : \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i} \xrightarrow{\sim} A_n^{\mathrm{dR}}(b,x).$$

For any $x_1, x_2 \in X(\mathbb{Q}_p)$ that lie in the same residue disk, we define $I(x_1,x_2) \in \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i}$ as

$$I(x_1,x_2) = 1 + \sum_w \int_{x_1}^{x_2} w(\omega_0, \ldots, \omega_{2g+d-2})$$

where the sum is over all words w in $\{T_0, \ldots, T_{2g+d-2}\}$ of length at most n, making substitution of T_i with ω_i. Here, the integrals are given by formally integrating power series.

This gives $\tau_{b,x}$, when considered on $A_n^{\mathrm{dR}}(Y)$ via s_0 as

$$\begin{aligned} \tau_{b,x} : \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i} &\xrightarrow{\sim} \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i} \\ v &\mapsto I(x_0,x) v I(b,b_0). \end{aligned} \tag{46}$$

By Besser's theory of Coleman integration on unipotent connections [Bes02], we have that for any points $b, b_0, x, x_0 \in Y(\mathbb{Q}_p)$, the map (46) describes the unique Frobenius-equivariant isomorphism $A_n^{\mathrm{dR}}(b_0,x_0) \xrightarrow{\sim} A_n^{\mathrm{dR}}(b,x)$ if $I(\cdot,\cdot)$ is interpreted using Coleman integration.

By taking quotients of the various $\mathcal{A}_Z^*$ by our nice correspondence Z, we get Frobenius operators

$$\phi_Z(b,x) : A_Z^{\mathrm{dR}}(b,x) \to A_Z^{\mathrm{dR}}(b,x)$$

and a quotient $\mathcal{A}_Z^{\mathrm{rig}}(\bar{b})$ of the universal 2-step object.

Moreover, Theorem 5.24 gives us an isomorphism

$$\Phi_Z : \phi^* \mathcal{A}_Z^{\mathrm{rig}}(\bar{b}) \xrightarrow{\sim} \mathcal{A}_Z^{\mathrm{rig}}(\bar{b}).$$

We have the following equations:

$$\begin{aligned} \phi_Z(b_0, x_0) &= x_0^* \Phi_Z \\ \phi_Z(b, x) &= \tau_{b,x} \circ \phi_Z(b_0, x_0) \circ \tau_{b,x}^{-1} \end{aligned}$$

which is how we compute $\phi_Z(b, x)$.

The connections on $\phi^* \mathcal{A}_Z^{\mathrm{dR}}(b) \mid_Y$ are described with respect to s_0 and are equal to $d + \Lambda$ (as before) and $d + \Lambda_\phi$ where

$$\Lambda_\phi := - \begin{pmatrix} 0 & 0 & 0 \\ \phi^* \vec{\omega} & 0 & 0 \\ \phi^* \eta & \phi^* \vec{\omega}^T Z & 0 \end{pmatrix}.$$

So to make the Frobenius structure explicit, we need to compute G (which is equal to Φ_Z^{-1}, the inverse of the Frobenius structure) such that $\Lambda_\phi G + dG = G\Lambda$.

Proposition 5.25. *We can take G as follows:*

$$G = \begin{pmatrix} 1 & 0 & 0 \\ \vec{f} & F & 0 \\ h & \vec{g}^T & p \end{pmatrix},$$

where we have

$$\begin{aligned} \phi^* \vec{\omega} &= F\vec{\omega} + d\vec{f} \quad (\textit{with } \vec{f}(b_0) = 0) \\ d\vec{g}^T &= d\vec{f}^T Z F \\ dh &= \vec{\omega}^T Z \vec{f} + d\vec{f}^T Z \vec{f} - \vec{g}\omega + \phi^* \eta - \eta \quad (\textit{with } h(b_0) = 0). \end{aligned}$$

Algorithm 5.26 (The Frobenius structure on $\mathcal{A}_Z$)**.**

(1) Use Tuitman's algorithm (Algorithm 1.52) to compute the matrix[20] of Frobenius F and the overconvergent function f such that $\phi^* \vec{\omega} = F\vec{\omega} + d\vec{f}$.

(2) Compute the matrix $L = I(x, x_0)^+ I(b_0, b)^-$, where we define for any pair $x_1, x_2 \in X(\mathbb{Q}_p)$ the following parallel transport matrices:

$$I^{\pm}(x_1, x_2) = \begin{pmatrix} 1 & 0 & 0 \\ \int_{x_1}^{x_2} \vec{\omega} & 1 & 0 \\ \int_{x_1}^{x_2} \eta + \int_{x_1}^{x_2} \vec{\omega} + Z\vec{\omega} & \pm \int_{x_1}^{x_2} \vec{\omega}^T Z & 1 \end{pmatrix}.$$

(3) Solve the p-adic differential equation of Proposition 5.25, then compute

$$M(b_0, x_0) = \begin{pmatrix} 1 & 0 & 0 \\ (I - F)^{-1} \vec{f} & 1 & 0 \\ \frac{1}{1-p}(g^T (I - F)^{-1} \vec{f} + h) & g^T (F - p)^{-1} & 1 \end{pmatrix} (x_0)$$

(using the same notation as in Proposition 5.25).

(4) Compute the matrix

$$\begin{aligned} s_0^{-1}(b, x) \circ s^\phi(b, x) &= L \cdot M(b_0, x_0) \\ &= \begin{pmatrix} 1 & 0 & 0 \\ \vec{\alpha}_\phi(b, x) & 1 & 0 \\ \gamma(b, x) & \vec{\beta}_\phi(b, x) & 1 \end{pmatrix}. \end{aligned}$$

[20] In Section 1, this was denoted by M, but we rename it here to F to avoid the clash in notation; likewise f was previously denoted as h.

To summarize, we have described algorithms to compute matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \gamma_{\mathrm{Fil}}(b,x) & \boldsymbol{\beta}^{\mathsf{T}}_{\mathrm{Fil}}(b) & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_{\phi}(b,x) & 1 & 0 \\ \gamma_{\phi}(b,x) & \boldsymbol{\beta}^{\mathsf{T}}_{\phi}(b,x) & 1 \end{pmatrix},$$

and the entries are exactly the ingredients for our formula (43) for the local height $h_p(A(x))$.

5.3. **Algorithms for quadratic Chabauty.** Theorem 5.2 suggests the following method for computing $X(\mathbb{Q}_p)_U$, where $U = U_Z$ is associated to a nice correspondence Z as above.

Algorithm 5.27 (Quadratic Chabauty for rational points)**.**

(1) Write the function $x \mapsto h_p(A(x))$ as a convergent power series on every residue disk in $X(\mathbb{Q}_p)$.
(2) Compute the finite set S of possible values of ρ.
(3) Compute the constants α_i.
(4) Write the function $x \mapsto \psi_i \circ (\pi_1, \pi_2)(A(x))$ as a convergent power series on every residue disk in $X(\mathbb{Q}_p)$ and solve for its zero set $X(\mathbb{Q}_p)_U$.
(5) Show that $X(\mathbb{Q}_p)_U \setminus X(\mathbb{Q})_{\mathrm{known}} = \varnothing$.

We have already discussed the first step of Algorithm 5.27. In this section we describe algorithms for the other steps.

Note that we might have to repeat this for several affine patches Y covering X (but see Section 5.4 for a worked example, where we get away with only one affine patch Y). Moreover, we cannot use the algorithm directly for a residue disk D in which Tuitman's lift of Frobenius is not defined. If there are no small rational points in such a disk, then we can try to show that there are none at all using the Mordell-Weil sieve, see Section 5.3.3. Otherwise, we can pick an affine patch such that Frobenius is defined in this disk or we can use a trick described in [BDM+19, §5.5], essentially reducing the computation of $h_p(A(x))$ for $x \in D(\mathbb{Q}_p)$ to the computation of Coleman integrals $\int_b^P \omega_i$, where $P \in D(\mathbb{Q})$.

If $\rho(J) > 2$, then we can run the algorithm above for several independent nice correspondences, and we expect that this suffices to prove $X(\mathbb{Q})_{\mathrm{known}} = X(\mathbb{Q})$ (provided this is indeed the case, of course).

Remark 5.28. As suggested by the notation, the set of points cut out by the condition $\rho(x) \in S$ in Theorem 5.2 does not depend on the choices of s or χ (note that we are working over $\mathbb{Q}$, so χ is well-defined up to a scalar multiple). See [BDM+19, Remark 3.12].

5.3.1. *Local heights away from p.* Let $\ell \neq p$ be prime. We already know that by Theorem 4.3 the function

$$\mathrm{Sel}(U) \to \mathbb{Q}_p\,; \quad P \mapsto h_\ell(\tau_\ell(\mathrm{loc}_\ell(P))) \tag{47}$$

takes values in a finite set S_ℓ, and that S_ℓ is trivial when X has potentially good reduction at ℓ. For our intended application, we need to be able to compute S_ℓ. This problem was solved recently by Betts and Dogra.

Lemma 5.29 (Betts–Dogra [BD19b])**.**

(1) The functions $j_{U,\ell}$ and (47) are constant on preimages of components of a regular semistable model of $X/\mathbb{Q}_\ell$.
(2) The function (47) and the set S_ℓ can be computed explicitly [BD19b, §12.1].

Betts and Dogra express (47) in terms of harmonic analysis on the reduction graph of X at ℓ in the sense of Zhang [Zha93]. To make this explicit, it is necessary to compute the endomorphism induced by Z on the reduction graph. For interesting examples, such as nice correspondences on modular curves derived from Hecke correspondences, this is often known. An algorithmic version of Lemma 5.29 will appear in [BDM$^+$].

The lemma implies, in particular, that S_ℓ is often trivial, even when X does not have potentially good reduction at ℓ. For instance, if $X\colon y^2 = f(x)$ is hyperelliptic, $\ell > 2$ and the discriminant $\Delta(X)$ satisfies $\mathrm{ord}_\ell(\Delta(X)) = 1$, then this holds.

We give a slightly more elaborate example. This was used in [BBB$^+$19, Section 6]; a proof will appear in [BDM$^+$].

Example 5.30. Let $N > 2$ be prime and let w_N be the Atkin–Lehner involution on $X_0(N)$. Then the curve $X_0(N)^+ = X_0(N)/w_N$ has good reduction away from N. At N, there is a regular semistable model (over an extension) whose special fiber is a projective line intersecting itself $g(X_0(N)^+)$ times. Therefore the local heights at N are all trivial on $\mathrm{Sel}(U)$, although $X_0(N)^+$ does not have potentially good reduction at N.

5.3.2. *Fitting the height pairing.* The third step of Algorithm 5.27 consists of writing the height pairing in terms of a given basis $\{\psi_i\}$ of the space $(\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^* \otimes \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*)^*$ of bilinear pairings on $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$. This is similar to the computation of an annihilating differential in the classical method of Chabauty–Coleman. In order to do so, we need to pick a basis $\{\psi_i\}$ and we need to evaluate ψ_i and the height pairing on sufficiently many elements to determine it. Since the height pairing is symmetric by construction, we can restrict to symmetric bilinear pairings.

One source of elements of $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^* \otimes \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ comes from representations $A(x)$ for rational points $x \in X(\mathbb{Q})$. The advantage is that we already know how to compute $h(A(x))$ for these. So if we have sufficiently many $x \in X(\mathbb{Q})$ so that we can generate $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^* \otimes \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ using the elements

$$\pi_1(A(x)) \otimes \pi_2(A(x)) = \log([x-b]) \otimes (E_Z(\log([x-b])) + c_Z)\,,$$

(see (42) and the discussion preceding it) then we can compute the coefficients of h in terms of the dual basis $\{\psi_i\}$. Computationally, we can read off $\pi_i(A(x))$ from our explicit description of the Hodge filtration and Frobenius structure on $A(x)$. Namely, for $x \in Y(\mathbb{Q})$, we have

$$\pi_1(A(x)) \otimes \pi_2(A(x)) = \alpha_\phi(b,x)^\intercal \cdot \left(\frac{I_g}{0_g}\right) \otimes \beta_\phi^\intercal(b,x) - \beta_{\mathrm{Fil}}^\intercal(b)) \cdot \left(\frac{0_g}{I_g}\right). \tag{48}$$

The required number of rational points can be decreased by working with $\mathrm{End}_0(J)$-equivariant heights. If the splitting s of the Hodge filtration on V_{dR} commutes with the endomorphisms on J, then h is $\mathrm{End}_0(J)$-equivariant. Hence we determine h in terms of a basis of

$$(\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^* \otimes_{\mathrm{End}_0(J)\otimes\mathbb{Q}_p} \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*)^*.$$

We still need (at least) $g + 1$ rational points on X.

Example 5.31. Let $X = X_{S_4}(13)$ be the modular curve associated to the pullback of $S_4 \subset \mathrm{PGL}_2(\mathbb{F}_{13})$ to $\mathrm{GL}_2(\mathbb{F}_{13})$, as studied by Banwait–Cremona [BC14]. Then $g = r = \rho(J) = 3$, and there are 4 obvious rational points on X. In [BDM$^+$] we apply the method just discussed and a nice correspondence constructed from the action of the Hecke operator T_{23} on $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbb{Q}_{23}})$ to determine the equivariant 23-adic height pairing using

$$\log([x-b]) \otimes E_Z(\log([x-b])) + c_Z$$

for the known rational points $x \in X(\mathbb{Q})$. Applying Algorithm 5.27, we prove that indeed $\#X(\mathbb{Q}) = 4$.

Remark 5.32. If p is ordinary and s is the unit root splitting, then the height is equivariant.

However, even if we use equivariant heights, it is often the case that we do not have enough rational points on X for this approach. Instead, we can use the fact that the construction of Coleman–Gross and Nekovář result in the same height, see Remark 3.6. We can then determine the height pairing in terms of a basis of bilinear pairings on $J(\mathbb{Q}) \otimes \mathbb{Q}_p \simeq \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ given by products of single integrals as in Section 2.3. In other words, we use the approach already employed in the first step of Algorithm 2.31, computing the heights of pairs of divisors on X of degree 0 with disjoint support via the Coleman–Gross construction as discussed there. This approach is currently restricted to hyperelliptic curves having an odd degree model at p.

5.3.3. *The Mordell-Weil sieve.* We briefly review the Mordell-Weil sieve. The original idea is due to Scharaschkin [Sch99], see [BS10] for an implementation-oriented account. Let $M > 1$ be an integer, let S be a finite set of primes of good reduction for X and consider the commutative diagram

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d] & J(\mathbb{Q})/MJ(\mathbb{Q}) \arrow[d, "\alpha_S"] \\
\prod_{v\in S} X(\mathbb{F}_v) \arrow[r, "\beta_S"'] & \prod_{v\in S} J(\mathbb{F}_v)/MJ(\mathbb{F}_v) .
\end{tikzcd}$$

Commutativity gives us a way to exclude the existence of rational points satisfying certain local conditions, by choosing the set S and the integer M carefully. When $X(\mathbb{Q})$ is empty, heuristics due to Poonen [Poo06] predict that there should always be a choice of S and M so that the images of α_S and β_S do not intersect.

We can use the Mordell-Weil sieve to show that for a fixed prime p, a given residue class in $X(\mathbb{Q}_p)$ does not contain a rational point. For this application we choose $M = M' \cdot p$ for some auxiliary integer M' and we choose S to be a set containing the prime divisors q of pM', and additional primes ℓ so that $\gcd(\#J(\mathbb{F}_\ell), \#J(\mathbb{F}_q))$ is large for some of these q.

In our setting, we can also apply this method as follows: Suppose we have a point $P \in X(\mathbb{Q}_p)_U$, computed to finite precision p^N, and we want to show that it does not come from a rational point. Assume that it does, so there are integers $a_1, \dots, a_g$ such that

$$[P - b] = a_1 P_1 + \ldots + a_g P_g,$$

where $P_1, \dots, P_g$ generate $J(\mathbb{Q}) \otimes \mathbb{Q}$. We can compute (for instance using linearity of single Coleman integrals), $(\tilde{a}_1, \dots, \tilde{a}_g) \in \mathbb{Z}/p^N\mathbb{Z}$ so that $a_i \equiv \tilde{a}_i \pmod{p^N}$ for all $i \in \{1, \dots, g\}$. We can then use the Mordell-Weil sieve to show that the corresponding coset of $p^N J(\mathbb{Q})$ does not contain the image of a rational point on X. We can also apply quadratic Chabauty with several primes p or choose $M = p^n M'$, where M' is a small auxiliary integers as above. For more details on the combination of quadratic Chabauty and the Mordell-Weil sieve see [BBM17] and [BBB$^+$19, §6.7].

5.4. **An example.** Let N be a positive integer and consider the Atkin–Lehner involution w_N. Then the quotient

$$X_0(N)^+ := X_0(N)/w_N$$

is a nice curve whose non-cuspidal points classify unordered pairs $\{E_1, E_2\}$ of elliptic curves admitting an N-isogeny between them.

In this section we illustrate the quadratic Chabauty method by computing the rational points on $X := X_0(167)^+$. It was shown by Galbraith [Gal96] that X has genus 2 and that

$$y^2 = x^6 - 4x^5 + 2x^4 - 2x^3 - 3x^2 + 2x - 3$$

is a model for X. There are four small rational points on X, namely the two points at infinity and $(1, \pm 1)$. For reasons explained below, we prefer a model without rational points at infinity, so we instead use the model

$$X\colon y^2 = -3x^6 + 2x^5 - 3x^4 - 2x^3 + 2x^2 - 4x + 1 \tag{49}$$

with small rational points $(0, \pm 1)$ and $(-1, \pm 1)$. The Jacobian $J = J_0(167)^+$ of X is geometrically irreducible. It has real multiplication, so the Picard number is 2. Using `Magma`, we compute that the rank of $J(\mathbb{Q})$ is also 2. We can do this in two different ways:

- via a 2-descent on J;
- by computing that analytic rank of the unique (up to conjugation) newform of level 167 and weight 2 invariant under w_{167} is equal to 1; we may conclude $\operatorname{rk}(J(\mathbb{Q})) = 2$ by the work of Gross–Zagier and Kolyvagin–Logachev.

We fix the prime $p = 7$ of good ordinary reduction. Then the logarithm gives an isomorphism $J(\mathbb{Q}) \otimes \mathbb{Q}_7 \to \mathrm{H}^0(X_{\mathbb{Q}_7}, \Omega_1))^*$. According to Theorem 5.2, all requirements for quadratic Chabauty are satisfied, and we may follow Algorithm 5.27 to compute a finite set of 7-adic points containing $X(\mathbb{Q})$.

5.4.1. *Step (1): Expand $h_7(A(x))$.* The most involved step is the computation (and expansion) of the local height $h_7(A(x))$ for a nice correspondence Z via the explicit formula (43). See [BBB+19, Section 6] for a more detailed description of the analogous computation for $X_0(67)^+$. We fix the unit root splitting s of the Hodge filtration and the standard idèle class character χ having $\chi_7 = \log_7$, the Iwasawa branch of the 7-adic log.

We first find a symplectic basis of $\mathrm{H}^1_{\mathrm{dR}}(X/\,\mathbb{Q}_7)$, given by

$$\omega_0 = -\frac{dx}{y}, \quad \omega_1 = (-1-x)\frac{dx}{y}, \quad \omega_2 = \frac{1}{6}x^2(1-x+2x^2)\frac{dx}{y}, \quad \omega_3 = \frac{1}{18}(-1-x^2+4x^3)\frac{dx}{y},$$

constructed so that the cup product is the standard symplectic form with respect to $(\omega_0, \ldots, \omega_3)$. Our subsequent computations will be in terms of this basis. Via Tuitman's algorithm (Algorithm 1.52), we determine the matrix Φ_7 of Frobenius on $\mathrm{H}^1_{\mathrm{dR}}(X/\,\mathbb{Q}_7)$. Eichler–Shimura [21] then allows us to compute the matrix representing the Hecke operator on $\mathrm{H}^1_{\mathrm{dR}}(X/\,\mathbb{Q}_7)$:

$$T_7 = \Phi_7^{\intercal} + 7 \cdot (\Phi_7^{\intercal})^{-1} = \begin{pmatrix} -1 & 1/2 & 0 & -1/12 \\ 1/2 & -3/2 & 1/12 & 0 \\ 0 & 0 & -1 & 1/2 \\ 0 & 0 & 1/2 & -3/2 \end{pmatrix}.$$

From this we obtain the following matrix representing the endomorphism on $\mathrm{H}^1_{\mathrm{dR}}(X/\,\mathbb{Q}_7)$ corresponding to a nice correspondence

$$Z = (\operatorname{Tr}(T_7) \cdot I_4 - 4T_7)C^{-1} = \begin{pmatrix} 0 & -1/3 & -1 & -2 \\ 1/3 & 0 & -2 & 1 \\ 1 & 2 & 0 & 0 \\ 2 & -1 & 0 & 0 \end{pmatrix},$$

where C is the matrix of the cup product on our basis $\{\omega_i\}$.

[21] There are of course other methods for the computation of Hecke operators, but we have to compute Φ_7 anyway, so we might as well use it.

The next step is the computation of the Hodge filtration (see Section 5.2.1). We use the base point $b = (-1, -1)$ and the affine patch Y cut out by our defining equation (49), so we only need a single differential ω_4 of the third kind, having a pole of order 1 at the two points at infinity. Since X is hyperelliptic, we have that η and β_{Fil} are trivial by Remark 5.22. Applying Algorithm 5.21, we find $\gamma_{\mathrm{Fil}} = 2x + 2$.

We compute the Frobenius structure based on the matrix Φ_7 as discussed in 5.2.2. Equation (43) then allows us to expand the function $x \mapsto h_7(A(x))$ into a 7-adic power series on those residue disks of $X(\mathbb{Q}_7)$ where our lift of Frobenius is defined.

5.4.2. *Step (2): Find the possible values of* ρ. This step requires us to find the possible values of $h_\ell(A(x))$ for $\ell \neq 7$ and $x \in X(\mathbb{Q}_\ell)$. Fortunately these are all trivial by Example 5.30.

5.4.3. *Step (3): Determine the height pairing as a bilinear pairing.* Since $X(\mathbb{Q})$ consists of two pairs of points swapped by the hyperelliptic involution, we do not have enough rational points on X to determine the height pairing as a bilinear pairing using only 7-adic heights of the form $h(A(x))$ for $x \in X(\mathbb{Q})$, even taking $\mathrm{End}_0(J)$-equivariance into account. Instead we determine the height pairing between points in $J(\mathbb{Q})$ via the Coleman–Gross construction.

A basis of $J(\mathbb{Q})$ is given by the points with Mumford representation $P = (x^2 - x + 1, x - 1)$ and $Q = (x^2, -2x + 1)$; this can be computed using the methods[22] of [Sto02, MS16].

For our computations, we use the following representatives

$$D_1 = D_0 - \mathrm{div}_0(x-4), \quad D_1' = \mathrm{div}_0(x-6) - D_0'$$
$$D_2 = 2(0,1) - \mathrm{div}_0(x-6), D_2' = \mathrm{div}_0(x-4) - 2(0,-1),$$

where D_0 (resp. D_0') is the divisor cut out by $x^2 + x + 1$ and $y - (x-1)$ (resp. $y - (1-x)$). Then we can compute the local height pairings $h_v(D_1, D_2)$ and $h_v(D_i, D_i')$ for $i = 1, 2$, noting that their base changes to $X(\mathbb{Q}_7)$ split as sums of $\mathbb{Q}_7$-rational points.

The model (49) is regular outside 2. While the curve X has good reduction at 2, the model (49) does not (the reduction modulo 2 is not reduced), but a regular model can be found easily. Using `Magma`, we find

$$\sum_{\ell \neq p} h_\ell(D_1, D_1') = 2\log 2 - \log 13 - \log 31,$$
$$\sum_{\ell \neq p} h_\ell(D_1, D_2) = 2\log 2 - \log 31,$$
$$\sum_{\ell \neq p} h_\ell(D_2, D_2') = -4\log 2 - 2\log 3.$$

In order to compute the local height pairings at 7, we move the unique Weierstrass point in $X(\mathbb{Q}_7)$ to infinity and work with the corresponding odd degree model of X over $\mathbb{Q}_7$ as required by our current `Sage`-implementation. Algorithm 2.22 gives

$$h_7(D_1, D_1') = 3 \cdot 7 + 6 \cdot 7^2 + 7^4 + 6 \cdot 7^5 + 5 \cdot 7^6 + 3 \cdot 7^7 + 3 \cdot 7^8 + 2 \cdot 7^9 + O(7^{10})$$
$$h_7(D_1, D_2) = 4 \cdot 7 + 6 \cdot 7^2 + 4 \cdot 7^3 + 5 \cdot 7^4 + 5 \cdot 7^5 + 7^6 + 5 \cdot 7^7 + 2 \cdot 7^8 + 3 \cdot 7^9 + O(7^{10})$$
$$h_7(D_2, D_2') = 2 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + 5 \cdot 7^4 + 5 \cdot 7^5 + 4 \cdot 7^6 + 4 \cdot 7^7 + 7^8 + 5 \cdot 7^9 + O(7^{10}).$$

[22] Strictly speaking, a basis of a finite index subgroup is enough, as long as we can show that a given prime does not divide the index.

As described in step (1) of Algorithm 2.31, we can now express the height h in terms of products of single integrals with coefficients

$$\begin{aligned}
\alpha_{00} &= 5 \cdot 7^{-1} + 4 + 4 \cdot 7 + 4 \cdot 7^2 + 2 \cdot 7^4 + 2 \cdot 7^5 + 7^6 + 2 \cdot 7^7 + 3 \cdot 7^9 + O(7^{10}) \\
\alpha_{01} &= 5 \cdot 7^{-1} + 5 + 6 \cdot 7 + 2 \cdot 7^2 + 4 \cdot 7^3 + 6 \cdot 7^4 + 4 \cdot 7^5 + 4 \cdot 7^6 + 5 \cdot 7^7 + 2 \cdot 7^8 + 6 \cdot 7^9 + O(7^{10}) \\
\alpha_{11} &= 6 \cdot 7^{-1} + 1 + 7 + 3 \cdot 7^2 + 5 \cdot 7^3 + 5 \cdot 7^4 + 6 \cdot 7^5 + 5 \cdot 7^6 + 2 \cdot 7^7 + 2 \cdot 7^8 + 3 \cdot 7^9 + O(7^{10}).
\end{aligned}$$

Hence we obtain our desired function

$$\rho \colon X(\mathbb{Q}_7) \to \mathbb{Q}_7$$

as in Theorem 5.2. We find that it indeed vanishes on the four known rational points; we also see that it has the additional zeros

$$\begin{aligned}
&(2 \cdot 7 + 6 \cdot 7^2 + 7^3 + 7^4 + 2 \cdot 7^5 + O(7^6), \pm(1 + 3 \cdot 7 + 4 \cdot 7^2 + 3 \cdot 7^3 + 5 \cdot 7^4 + 4 \cdot 7^5 + O(7^6))) \\
&(6 + 6 \cdot 7 + 2 \cdot 7^2 + 3 \cdot 7^3 + 3 \cdot 7^4 + 7^5 + O(7^6), \pm(6 + 6 \cdot 7 + 2 \cdot 7^2 + 4 \cdot 7^3 + 2 \cdot 7^4 + 2 \cdot 7^5 + O(7^6))) \\
&(5 + 2 \cdot 7 + 4 \cdot 7^2 + 6 \cdot 7^3 + 7^5 + O(7^6)), \pm(4 + 2 \cdot 7 + 6 \cdot 7^2 + 7^3 + 2 \cdot 7^4 + 2 \cdot 7^5 + O(7^6))) \\
&(5 + 4 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + 3 \cdot 7^4 + 7^5 + O(7^6), \pm(4 + 5 \cdot 7 + 2 \cdot 7^2 + 4 \cdot 7^3 + 2 \cdot 7^5 + O(7^6))).
\end{aligned}$$

This means that we have computed $X(\mathbb{Q}_7)_U \cap Y(\mathbb{Q}_7) \setminus D_{\text{bad}}$, where D_{bad} is the residue disk of the unique Weierstrass point $(1, 0) \in X(\mathbb{F}_7)$ (where our Frobenius lift is not defined). Since the Picard number is 2, we cannot show that these do not come from a rational point using an additional nice correspondence, see Remark 5.6. Instead we apply the Mordell-Weil sieve with the auxiliary integer 95 and the primes $v \in \{3, 5, 19, 31\}$, noting that

$$\#J(\mathbb{F}_3) = 19, \quad \#J(\mathbb{F}_5) = 7^2, \quad \#J(\mathbb{F}_{19}) = 2^2 \cdot 5 \cdot 19, \quad \#J(\mathbb{F}_{31}) = 2^2 \cdot 11 \cdot 19.$$

So now we have shown that $X_0(167)^+$ consists only of the four known rational points – almost. We still have to deal with the disks at infinity and the disk D_{bad}. But since we do not expect any rational points in these disks, we can use the Mordell-Weil sieve to prove this. Since $J(\mathbb{F}_7) \cong \mathbb{Z}/109\,\mathbb{Z}$, we need primes v such that $109 \mid \#J(\mathbb{F}_v)$, which does not happen too often and makes the computation quite involved [23]. But using the auxiliary integer 60, we finally succeed in proving that none of these disks contain a rational point. Comparing with [Gal96, Table 7], we obtain the following:

Theorem 5.33. *There are exactly four rational points on $X_0(167)^+$, and they are all cusps or CM-points.*

For $N = 67, 73, 103$ the rational points on $X_0(N)^+$ were computed in [BBB+19]; these all have genus 2. In [BDM+] we compute the rational points for all other prime values of N such that $X_0(N)^+$ has genus 2 or 3. See [BGX19] for recent results on the rational points on $X_0(N)^+$ for several composite squarefree values of N such that $X_0(N)^+$ has genus 2, based on a combination of elliptic curve Chabauty with covering techniques.

Project 5.34 (Quadratic Chabauty on modular curves $X_0(N)^+$)**.** Galbraith [Gal96, Gal99, Gal02] has constructed models for all modular curves $X_0(N)^+ = X_0(N)/w_N$ of genus ≤ 5 (with the exception of $N = 263$) and has conjectured that he has found all exceptional points on these curves. This project will use quadratic Chabauty to prove as much as possible about Galbraith's conjecture. Another goal is to investigate whether we can use p-adic Gross-Zagier to carry out quadratic Chabauty for $X_0(N)^+$, starting with the case of such curves of genus 2.

[23] We end up using 5-digit primes.

5.5. **Future directions.** So far, all curves whose rational points have been computed using quadratic Chabauty are either bielliptic of genus 2 ([BD18a, BD18b, EL19]) or modular [BDM$^+$19, BBB$^+$19, BDM$^+$]. For instance, in joint work [BDM$^+$19] with Dogra, Tuitman and Vonk we use quadratic Chabauty to compute the rational points on the non-split Cartan modular curve $X^+_{\mathrm{ns}}(13)$ (or the split Cartan curve of the same level, which is isomorphic to it).

It would be interesting to extend the practical scope of the method. As a first step, one could consider (modular) curves satisfying $r = g$ whose Jacobians have complex multiplication. Possible examples include twisted Fermat curves $ax^m + by^m + cz^m$ or van Wamelen's list of genus 2 curves whose Jacobians have CM and are simple [vW99].

Also note that [BD18a] contains a general recipe for quadratic Chabauty when the quadratic Chabauty condition is satisfied, but $r > g$. This has not been used in practice yet. More generally, the Bloch–Kato conjecture predicts that quadratic Chabauty should be applicable when $r < g^2$, without any assumptions on ρ (see [BD18b]), and it would be very interesting to make this explicit.

Acknowledgements. We are very grateful to Francesca Bianchi, Stephanie Chan, Netan Dogra, and Enis Kaya for detailed feedback on an earlier draft of these notes. Additionally, special thanks are due to the participants of the Boston University fall 2019 course MA 841: Oana Adascalitei, Alex Best, María Inés de Frutos Fernández, Stevan Gajović, Sachi Hashimoto, Aashraya Jha, Wanlin Li, Ricky Magner, Angus McAndrew, John Sim, Yifan Wu, and Susan Ye. JB was partially supported by NSF grant DMS-1702196, the Clare Boothe Luce Professorship (Henry Luce Foundation), Simons Foundation grant #550023, and a Sloan Research Fellowship. SM was supported by an NWO VIDI grant.

Appendix A. Some nonabelian cohomology

We collect some results on nonabelian cohomology, closely following Serre [Ser02, §I.5].

Let G be a profinite group. Consider the category of G-sets: an object E in this category is a discrete topological space on which G acts continuously, and a morphism between G-sets E_1 and E_2 is a map $f : E_1 \to E_2$ that commutes with the action of G. If $s \in G$ and $x \in E$, the image of x under s will be denoted by ${}^s x$. A G-group A is a group in the category of G-sets. This means that A is a G-set, with a group structure that is invariant under G, so that ${}^s(xy) = {}^s x\, {}^s y$. (Note that when A is commutative, one gets a G-module.)

If E is a G-set, we let

$$\mathrm{H}^0(G, E) = E^G,$$

the set of elements of E fixed by G. If E is a G-group, $\mathrm{H}^0(G, E)$ is a group. If A is a G-group, a 1-cocycle of G in A is a map $s \mapsto a_s$ of G to A that is continuous and such that $a_{st} = a_s\, {}^s a_t$ for $s, t \in G$. We denote the set of these cycles as $Z^1(G, A)$. Two cocycles a and a' are cohomologous if there exists $b \in A$ such that $a'_s = b^{-1} a_s\, {}^s b$. This is an equivalence relation $\sim$ in $Z^1(G, A)$, and the quotient set is denoted as

$$\mathrm{H}^1(G, A) = Z^1(G, A)/\sim .$$

We now give another useful interpretation of $\mathrm{H}^1(G, A)$ for a G-group A. We say that A acts on the left on a G-set E if it acts on E in the usual way and if ${}^s(a \cdot x) = {}^s a \cdot {}^s x$ for $a \in A, x \in E$. An action on the right is defined analogously. A G-equivariant (left[24]) A-torsor is a non-empty G-set P, on which A acts on the left, so that for each pair $x, y \in P$, there exists a unique $a \in A$ such that $y = a \cdot x$. We have the following:

[24] Right A-torsors are defined analogously.

Proposition A.1 ([Ser02, Prop. 33])**.** *Let A be a G-group. There is a bijection between the equivalence classes of G-equivariant A-torsors and the set* $\mathrm{H}^1(G,A)$.

Note that while $\mathrm{H}^0(G,A)$ is a group, $\mathrm{H}^1(G,A)$ is merely a *pointed set* when G is non-abelian: it has no group structure, but a distinguished element, given by the class of the unit cocycle. Moreover, the association $A \mapsto \mathrm{H}^i(G,A)$ is functorial for $i = 0, 1$. We can talk about exact sequences of pointed sets (where the image of a map is the inverse image of the neutral element). For instance, we get the following important result:

Proposition A.2 (Six-term exact sequence in non-abelian cohomology [Ser02, Prop. 38])**.** *Let*

$$1 \to A \to B \to C \to 1$$

be a short exact sequence of G-groups. The following sequence of pointed sets:

$$1 \to \mathrm{H}^0(G,A) \to \mathrm{H}^0(G,B) \to \mathrm{H}^0(G,C) \to \mathrm{H}^1(G,A) \to \mathrm{H}^1(G,B) \to \mathrm{H}^1(G,C)$$

is exact.

However, some desirable features are lacking: for instance, injectivity does not follow from having a trivial kernel. More generally, we would like to determine fibers of maps between pointed sets $\mathrm{H}^1(G,A) \to \mathrm{H}^1(G,B)$. Serre's twisting construction, motivated by the theory of fiber bundles, and described below, makes it possible to turn fibers into kernels.

There are analogous constructions when G and A are topological groups, and G acts continuously on A. Considering continuous cocycles and continuous G-equivariant A-torsors yields the continuous cohomology set $\mathrm{H}^1(G,A)$, and the results of [Ser02, §I.5.3] remain valid. Henceforth, we shall assume that we are in this setting, and we shall mostly omit the word "continuous".

A.1. **The twisting construction.** Let G be a topological group, let A be a topological group with a continuous G-action, and let P be a continuous G-equivariant A-torsor. Let F be a G-set on which A acts on the right. We form the twist of F by P as follows: consider the equivalence relation that identifies an element (f,p) with $(a\cdot p, fa^{-1})$, for $a \in A$. This relation is compatible with the action of G, and the quotient $F \times_A P$ is a G-set. An element of $F \times_A P$ can be written as $f \cdot p$ for $p \in P, f \in F$, and one has $f(ap) = (fa)p$. Note that for all $p \in P$, the map $f \mapsto f \cdot p$ is a bijection of F onto $F \times_A P$ For this reason, one says that $F \times_A P$ is obtained from F by twisting it using P. This construction gives P the structure of a G-equivariant $F \times_A P$-torsor. We write $A^{(P)} := A \times_A P$, where A acts on itself by conjugation. This construction is easily seen to be functorial in A.

Proposition A.3 ([Ser02, Prop. 35])**.** *Let P be a G-equivariant A-torsor. Then there is a bijection* $\mathrm{H}^1(G,A) \to \mathrm{H}^1(G,A^{(P)})$*, mapping the class of P in* $\mathrm{H}^1(G,A)$ *to the neutral element of* $\mathrm{H}^1(G,A^{(P)})$.

So if we have a map $\mathrm{H}^1(G,A) \to \mathrm{H}^1(G,B)$ of pointed sets, coming from a G-group homomorphism $A \to B$, and we want to determine the fiber above the image of some G-equivariant A-torsor P, then we can do this using the induced diagram

$$\begin{tikzcd}
\mathrm{H}^1(G,A) \arrow[r] \arrow[d] & \mathrm{H}^1(G,A^{(P)}) \arrow[d] \\
\mathrm{H}^1(G,B) \arrow[r] & \mathrm{H}^1(G,B^{(P\times_A B)})
\end{tikzcd}$$

which commutes due to functoriality of the twisting construction [Ser02, §5.4]. This approach is used in [Ser02, §I.5.5] to determine information about images and fibers of the maps in the six-term exact sequence in Proposition A.2.

Remark A.4. We record some additional useful properties of the twisting construction:

(1) Alternatively, the twisting construction can also be described in terms of cocycles, see [Ser02, §I.5.3] and [Bet, §4.0.1].
(2) If $H^1(G, A)$ and $H^1(G, A^{(P)})$ are representable by schemes, then the twisting bijection in Proposition A.3 is an isomorphism of schemes.
(3) If v is a prime and $U/\mathbb{Q}_v$ is the representation of the absolute Galois group G_p of $\mathbb{Q}_p$ on a finitely generated pro-unipotent group in the sense of [Bet, Section 4], then we can describe $\mathrm{H}^1(G_p, U(Q_v))$ via finite-dimensional G_p-equivariant quotients: Writing $U = \varprojlim U_n$ as an inverse limit of such quotients, we have a natural bijection
$$\mathrm{H}^1(G_p, U(\mathbb{Q}_v)) = \varprojlim \mathrm{H}^1(G_p, U_n(\mathbb{Q}_v)).$$
In particular, this includes pro-unipotent fundamental groups, such as the ones considered by Kim.

References

[And03] Yves André. Period mappings and differential equations. *From* **C** *to* $\mathbf{C}_p$*, MSJ Memoirs*, 12, 2003. ↑3.1.

[Bal] J. S. Balakrishnan. Sage code. https://github.com/jbalakrishnan/AWS. ↑1.65, 2.24.

[Bal13] J. S. Balakrishnan. Iterated Coleman integration for hyperelliptic curves. In E. W. Howe and K. S. Kedlaya, editors, *ANTS-X: Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Series*, pages 41–61. Mathematical Sciences Publishers, 2013. ↑1.5, 1.63, 1.64.

[Bal15] J. S. Balakrishnan. Coleman integration for even-degree models of hyperelliptic curves. *LMS J. Comput. Math.*, 18(1):258–265, 2015. ↑1.5, 1.63, 1.64.

[BB12] J. S. Balakrishnan and A. Besser. Computing local p-adic height pairings on hyperelliptic curves. *IMRN*, 2012(11):2405–2444, 2012. ↑1.40, 2.2.1, 2.20, 2.22, 2.23.

[BB15] Jennifer S. Balakrishnan and Amnon Besser. Coleman–Gross height pairings and the p-adic sigma function. *Journal für die reine und angewandte Mathematik (Crelle's Journal)*, 2015(698):89–104, 2015. ↑2.1, 2.27.

[BB19] J. S. Balakrishnan and A. Besser. Errata for "Computing local p-adic height pairings on hyperelliptic curves". http://math.bu.edu/people/jbala/cg_heights_errata.pdf, 2019. ↑2.2.1.

[BBB$^+$19] Jennifer S. Balakrishnan, Alex J. Best, Francesca Bianchi, Brian Lawrence, J. Steffen Müller, Nicholas Triantafillou, and Jan Vonk. Two recent p-adic approaches towards the (effective) Mordell conjecture. https://arxiv.org/abs/1910.12755, 2019. ↑1.1, 4.21, 5.3.1, 5.3.3, 5.4.1, 5.4.3, 5.5.

[BBBM19] Jennifer S. Balakrishnan, Francesca Bianchi, Amnon Besser, and J. Steffen Müller. Explicit quadratic Chabauty over number fields. https://arxiv.org/abs/1910.04653, 2019. ↑2.3.

[BBK10] J. S. Balakrishnan, R. W. Bradshaw, and K. Kedlaya. Explicit Coleman integration for hyperelliptic curves. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 16–31. Springer, Berlin, 2010. ↑1.3, 1.3, 1.36, 1.39, 1.40.

[BBM16] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller. Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves. *Journal für die reine und angewandte Mathematik (Crelle's Journal)*, 2016(720):51–79, 2016. ↑2.28, 2.29.

[BBM17] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller. Computing integral points on hyperelliptic curves using quadratic Chabauty. *Math. Comp.*, 86:1403–1434, 2017. ↑2.24, 2.3, 2.33, 5.3.3.

[BC94] Francesco Baldassarri and Bruno Chiarellotto. Algebraic versus rigid cohomology with logarithmic coefficients. In *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, volume 15 of *Perspect. Math.*, pages 11–50. Academic Press, San Diego, CA, 1994. ↑1.3.

[BC09] O. Brinon and B. Conrad. CMI summer school notes on p-adic Hodge theory. 2009. ↑3.1.

[BC14] Barinder S. Banwait and John E. Cremona. Tetrahedral elliptic curves and the local-global principle for isogenies. *Algebra Number Theory*, 8(5):1201–1229, 2014. ↑5.31.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp*, 24(3-4):235–265, 1997. ↑1.

[BD18a] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. ↑3.2, 3.2, 4.1, 4.4, 4.12, 4.5, 4.6, 5.2, 5.5, 5.6, 5.1, 5.1, 5.1, 5.5.

[BD18b] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *IMRN, to appear*, 2018. https://arxiv.org/abs/1705.00401. ↑3.2, 4.2, 4.6, 5, 5.1, 5.1, 5.1, 5.2, 5.22, 5.5.

[BD19a] Jennifer S. Balakrishnan and Netan Dogra. An effective Chabauty-Kim theorem. *Compos. Math.*, 155(6):1057–1075, 2019. ↑5.7.

[BD19b] L. Alexander Betts and Netan Dogra. Ramification of étale path torsors and harmonic analysis on graphs, Sep 2019. https://arxiv.org/abs/1909.05734. ↑5.29, 2.

[BDCKW18] J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers. A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves. *Math. Ann.*, 372(1-2):369–428, 2018. ↑4.6, 5.1.

[BDM$^+$] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Quadratic Chabauty for modular curves: Algorithms and examples. in progress. ↑5.3.1, 5.31, 5.4.3, 5.5.

[BDM$^+$19] J.S. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3), 2019. ↑3.2, 3.3, 3.3.1, 3.7, 4.2, 4.4, 4.19, 5.1, 5.2, 5.13, 5.2, 5.2, 5.2.1, 5.19, 5.20, 5.2.2, 5.2.2, 5.3, 5.28, 5.5.

[Bel09] J. Bellaïche. CMI summer school notes on an introduction to the conjecture of Bloch-Kato. 2009. ↑3.1, 3.2, 3.3.

[Ber75] Daniel Bertrand. Valeurs algébriques de fonctions méromorphes. In *Séminaire Delange-Pisot-Poitou, 15e année (1973/74), Théorie des nombres, Fasc. 1, Exp. No. 21*, page 6. 1975. ↑2.1.

[Ber81] Dominique Bernardi. Hauteur p-adique sur les courbes elliptiques. In *Seminar on Number Theory, Paris 1979–80*, volume 12 of *Progr. Math.*, pages 1–14. Birkhäuser, Boston, Mass., 1981. ↑2.

[Ber97] Pierre Berthelot. Finitude et pureté cohomologique en cohomologie rigide. *Invent. Math.*, 128(2):329–377, 1997. With an appendix in English by Aise Johan de Jong. ↑1.3.

[Ber04] Laurent Berger. An introduction to the theory of p-adic representations. *Geometric aspects of Dwork theory*, 1:255–292, 2004. ↑3.1.

[Ber07] Vladimir G. Berkovich. *Integration of one-forms on p-adic analytic spaces*, volume 162 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2007. ↑1.11.

[Bes02] Amnon Besser. Coleman integration using the Tannakian formalism. *Math. Ann.*, 322(1):19–48, 2002. ↑1.11, 1.5, 5.2.2.

[Bes04] Amnon Besser. The p-adic height pairings of Coleman-Gross and of Nekovář. In *Number theory*, volume 36 of *CRM Proc. Lecture Notes*, pages 13–25. Amer. Math. Soc., Providence, RI, 2004. ↑3.6.

[Bes05] Amnon Besser. p-adic Arakelov theory. *J. Number Theory*, 111(2):318–371, 2005. ↑2.2.1, 5.5.

[Bes12] Amnon Besser. Heidelberg lectures on Coleman integration. In J. Stix, editor, *The arithmetic of fundamental groups—PIA 2010*, volume 2 of *Contrib. Math. Comput. Sci.*, pages 3–52. Springer, Heidelberg, 2012. ↑1.11, 1.6.

[Bes17] Amnon Besser. p-adic heights and Vologodsky integration. https://arxiv.org/abs/1711.06957, 2017. ↑2.26.

[Bes19] Alex J. Best. Explicit Coleman integration in larger characteristic. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Ser.*, pages 85–102. Math. Sci. Publ., Berkeley, CA, 2019. ↑1.41.

[Bes20] Alex J. Best. Square root time Coleman integration on superelliptic curves. https://alexjbest.github.io/papers/coleman-superelliptic.pdf, 2020. ↑1.41.

[Bet] L. Alexander Betts. The motivic anabelian geometry of local heights on abelian varieties. https://arxiv.org/abs/1706.04850. ↑4.21, 1, 3.

[BGJGP05] Matthew H Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen. Finiteness results for modular curves of genus at least 2. *American Journal of Mathematics*, 127(6):1325–1387, 2005. ↑2.24.

[BGR84] S. Bosch, U. Güntzer, and R. Remmert. *Non-Archimedean analysis*, volume 261 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1984. A systematic approach to rigid analytic geometry. ↑1.2.

[BGX19] Francesc Bars, Josep González, and Xavier Xarles. Hyperelliptic parametrizations of $\mathbb{Q}$-curves. 2019. https://arxiv.org/abs/1910.10545. ↑5.4.3.

[Bia19a] Francesca Bianchi. Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture. arXiv:1904.04622, 2019. ↑4.1, 4.7.

[Bia19b] Francesca Bianchi. Topics in the theory of p-adic heights on elliptic curves. *Oxford DPhil thesis*, 2019. ↑2.10.

[BK90] Spencer Bloch and Kazuya Kato. L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990. ↑3.3.2, 4.2, 4.6.

[BKK11] Jennifer S. Balakrishnan, Kiran S. Kedlaya, and Minhyong Kim. Appendix and erratum to "Massey products for elliptic curves of rank 1". *J. Amer. Math. Soc.*, 24(1):281–291, 2011. ↑1.67.

[Bom90] Enrico Bombieri. The Mordell conjecture revisited. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 17(4):615–640, 1990. ↑1.1.

[BS10] Nils Bruin and Michael Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010. ↑6, 5.3.3.

[BTa] Jennifer S. Balakrishnan and Jan Tuitman. Explicit Coleman integration for curves. https://arxiv.org/abs/1710.01673. ↑1.4, 1.53, 1.55, 1.56.

[BTb] J. S. Balakrishnan and J. Tuitman. Magma code. https://github.com/jtuitman/Coleman. ↑1.22, 1.56, 1.57, 1.58.

[BZ17] Amnon Besser and Sarah Livia Zerbes. Vologodsky integration on curves with semi-stable reduction, 2017. https://arxiv.org/abs/1711.06950. ↑1.15.

[CdS88] Robert Coleman and Ehud de Shalit. p-adic regulators on curves and special values of p-adic L-functions. *Invent. Math.*, 93(2):239–266, 1988. ↑1.10, 1.5.

[CDV06] W. Castryck, J. Denef, and F. Vercauteren. Computing zeta functions of nondegenerate curves. *IMRP Int. Math. Res. Pap.*, pages Art. ID 72017, 57, 2006. ↑1.4.

[CG89] Robert F. Coleman and Benedict H. Gross. p-adic heights on curves. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 73–81. Academic Press, Boston, MA, 1989. ↑2, 2.13, 2.2.1, 2.2.1.

[Cha16] S. Chan. Topics in the theory of zeta functions of curves. *Oxford MMath thesis*, 2016. https://www.ucl.ac.uk/~ucahytc/chan_dissertation.pdf. ↑1.32, 1.34, 1.35.

[Che71] Kuo-tsai Chen. Algebras of iterated path integrals and fundamental groups. *Trans. Amer. Math. Soc.*, 156:359–379, 1971. ↑1.5.

[CK10] John Coates and Minhyong Kim. Selmer varieties for curves with CM Jacobians. *Kyoto J. Math.*, 50(4):827–852, 2010. ↑4.10, 5.1.

[CLS99] Bruno Chiarellotto and Bernard Le Stum. F-isocristaux unipotents. *Compositio Math.*, 116(1):81–110, 1999. ↑5.24.

[Col82] R. F. Coleman. Dilogarithms, regulators and p-adic L-functions. *Invent. Math.*, 69(2):171–208, 1982. ↑1.10, 1.5.

[Col85a] Robert F. Coleman. Effective Chabauty. *Duke Mathematical Journal*, 52(3):765–770, 1985. ↑1.4.

[Col85b] Robert F. Coleman. Torsion points on curves and p-adic abelian integrals. *Ann. of Math. (2)*, 121(1):111–168, 1985. ↑1.1, 1.10, 1.25.

[Col98] Pierre Colmez. Intégration sur les variétés p-adiques. *Astérisque*, (248):viii+155, 1998. ↑1.11.

[Cor19] David Corwin. From Chabauty's method to Kim's non-abelian Chabauty's method. 2019. https://math.berkeley.edu/~dcorwin/files/ChabautytoKim.pdf. ↑4.1.

[Del89] P. Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois groups over* $\mathbf{Q}$ *(Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 79–297. Springer, New York, 1989. ↑1.6.

[Del90] P. Deligne. Catégories tannakiennes. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 111–195. Birkhäuser Boston, Boston, MA, 1990. ↑5.2.

[DF19] Netan Dogra and Samuel Le Fourn. Quadratic Chaubauty for modular curves and modular forms of rank one, June 2019. https://arxiv.org/abs/1906.08751v3. ↑4.20, 4.6, 5.7.

[DM82] P. Deligne and J. S. Milne. *Tannakian Categories*, pages 101–228. Springer Berlin Heidelberg, Berlin, Heidelberg, 1982. ↑5.2.

[Dok18] T. Dokchitser. Models of curves over DVRs. 2018. https://arxiv.org/abs/1807.00025. ↑2.3.1.

[DRS12] H. Darmon, V. Rotger, and I. Sols. Iterated integrals, diagonal cycles, and rational points on elliptic curves. *Publ. Math. de Besançon*, 2:19–46, 2012. ↑5.1.

[DV06a] Jan Denef and Frederik Vercauteren. Counting points on C_{ab} curves using Monsky-Washnitzer cohomology. *Finite Fields Appl.*, 12(1):78–102, 2006. ↑1.4.

[DV06b] Jan Denef and Frederik Vercauteren. An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. *J. Cryptology*, 19(1):1–25, 2006. ↑1.4.

[Edi] B. Edixhoven. Point counting after Kedlaya, EIDMA-Stieltjes graduate course, Leiden, September 22-26,2003. http://www.math.leidenuniv.nl/~edix/oww/mathofcrypt/carls_edixhoven/kedlaya.pdf. ↑1.2, 1.30.

[EH17] Jordan S. Ellenberg and Daniel Rayor Hast. Rational points on solvable curves over $\mathbb{Q}$ via non-abelian chabauty. *ArXiv preprint*, 2017. ↑4.11.

[EL19] Bas Edixhoven and Guido Lido. Geometric quadratic Chaubauty, Oct 2019. https://arxiv.org/abs/1910.10752. ↑4.21, 5.5.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983. ↑1.2.

[Fal89] Gerd Faltings. Crystalline cohomology and p-adic Galois-representations. In *Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988)*, pages 25–80. Johns Hopkins Univ. Press, Baltimore, MD, 1989. ↑3.2, 3.

[FvdP04] Jean Fresnel and Marius van der Put. *Rigid analytic geometry and its applications*, volume 218 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 2004. ↑1.1, 1.2.

[Gal96] S. D. Galbraith. Equations for modular curves. *Oxford DPhil thesis*, 1996. ↑5.4, 5.4.3, 5.34.

[Gal99] Steven D. Galbraith. Rational points on $X_0^+(p)$. *Experiment. Math.*, 8(4):311–318, 1999. ↑5.34.

[Gal02] Steven D. Galbraith. Rational points on $X_0^+(N)$ and quadratic $\mathbb{Q}$-curves. *J. Théor. Nombres Bordeaux*, 14(1):205–219, 2002. ↑5.34.

[GG01] Pierrick Gaudry and Nicolas Gürel. An extension of Kedlaya's point-counting algorithm to superelliptic curves. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 480–494. Springer, Berlin, 2001. ↑1.4.

[Gro86] Benedict H Gross. Local heights on curves. In *Arithmetic geometry*, pages 327–339. Springer, 1986. ↑2.2.1.

[Had11] M. Hadian. Motivic fundamental groups and integral points. *Duke Math. J.*, 160(3):503–565, 2011. ↑5.15.

[Har07] D. Harvey. Kedlaya's algorithm in larger characteristic. *Int Math Res Notices*, 2007(rnm095):rnm095–29, 2007. ↑1.41.

[Har08] D. Harvey. Efficient computation of p-adic heights. *LMS J. Comput. Math.*, 11:40–59, 2008. ↑2.7, 2.8.

[Har12] M. C. Harrison. An extension of Kedlaya's algorithm for hyperelliptic curves. *J. Symb. Comp.*, 47(1):89 – 101, 2012. ↑1.4.

[HM] S. Hashimoto and T. Morrison. Magma code. https://github.com/travismo/Coleman. ↑1.58.

[HM19] Yoshinosuke Hirakawa and Hideki Matsumura. A unique pair of triangles. *Journal of Number Theory*, 194:297–302, 2019. ↑1.1.

[Hol12] David Holmes. Computing Néron-Tate heights of points on hyperelliptic Jacobians. *J. Number Theory*, 132(6):1295–1305, 2012. ↑2.3.1.

[IW03] Adrian Iovita and Annette Werner. p-adic height pairings on abelian varieties with semistable ordinary reduction. *J. Reine Angew. Math.*, 564:181–203, 2003. ↑2.

[Kat73] N. Katz. p-Adic properties of modular schemes and modular forms. In P. Deligne and W. Kuyk, editors, *Modular forms in one variable III*, volume 350 of *LNM*, pages 69–190. Springer-Verlag, 1973. ↑2.1.

[Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001. ↑3, 1.3, 1.28, 1.29, 1.30.

[Ked03] Kiran S. Kedlaya. Errata for: "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology" [J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338; mr1877805]. volume 18, pages 417–418. 2003. Dedicated to Professor K. S. Padmanabhan. ↑3, 1.31.

[Kim05] Minhyong Kim. The motivic fundamental group of $\mathbf{P}^1 - \{0, 1, \infty\}$ and the theorem of Siegel. *Inventiones mathematicae*, 161(3):629–656, 2005. ↑4.1, 4.3, 4.3, 4.5.

[Kim09] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS*, 45:89–133, 2009. ↑4.1, 4.1, 4.5, 4.1, 4.1, 4.8, 4.9, 4.5, 4.5, 5.1, 5, 5.2.

[Kim10] M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23(3):725–747, 2010. ↑1.67.

[Kim12] Minhyong Kim. Tangential localization for Selmer varieties. *Duke Math. J.*, 161(2):173–199, 2012. ↑4.1.

[KK20] Eric Katz and Enis Kaya. p-adic integration on bad reduction hyperelliptic curves. preprint, 2020. ↑1.40.

[KRZB16] Eric Katz, Joseph Rabinoff, and David Zureick-Brown. Uniform bounds for the number of rational points on curves of small Mordell–Weil rank. *Duke Mathematical Journal*, 165(16):3189–3240, 2016. ↑1.15, 1.21.

[KT08] M. Kim and A. Tamagawa. The l-component of the unipotent Albanese map. *Math. Ann.*, 340(1):223–235, 2008. ↑4.1, 4.3.

[KZB13] Eric Katz and David Zureick-Brown. The Chabauty-Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions. *Compos. Math.*, 149(11):1818–1838, 2013. ↑2.

[LMF20a] The LMFDB Collaboration. The L-functions and modular forms database, home page of the genus 2 curve 8832.a.17664.1. https://www.lmfdb.org/Genus2Curve/Q/8832/a/17664/1, 2020. [Online; accessed 7 February 2020]. ↑1.65.

[LMF20b] The LMFDB Collaboration. The L-functions and modular forms database, home page of the genus 2 curve 971.a.971.1. https://www.lmfdb.org/Genus2Curve/Q/971/a/971/1, 2020. [Online; accessed 30 January 2020]. ↑1.22.

[LV18] B. Lawrence and A. Venkatesh. Diophantine problems and p-adic period mappings. 2018. https://arxiv.org/abs/1807.02721. ↑1.1.

[Mil80] J. Milne. *Étale cohomology*. Princeton University Press, 1980. ↑4.4.

[Min10] Moritz Minzlaff. Computing zeta functions of superelliptic curves in larger characteristic. *Mathematics in Computer Science*, 3(2):209–224, 2010. ↑1.41.

[MS16] Jan Steffen Müller and Michael Stoll. Canonical heights on genus-2 Jacobians. *Algebra Number Theory*, 10(10):2153–2234, 2016. ↑5.4.3.

[MST06] Barry Mazur, William Stein, and John Tate. Computation of p-adic heights and log convergence. *Doc. Math*, pages 577–614, 2006. ↑2.1, 2.8.

[MT83] B. Mazur and J. Tate. Canonical height pairings via biextensions. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 195–237. Birkhäuser Boston, Boston, MA, 1983. ↑2.

[MT91] Barry Mazur and John Tate. The p-adic sigma function. *Duke Mathematical Journal*, 62(3):663–688, 1991. ↑2.1, 2.3.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.*, 84(1):1–48, 1986. ↑2.5, 2.8.

[Mül14] J. Steffen Müller. Computing canonical heights using arithmetic intersection theory. *Mathematics of Computation*, 83(285):311–336, 2014. ↑2.3.1.

[Nek93] J. Nekovar. On p-adic height pairings. In *Séminaire de Théorie des Nombres, Paris 1990-1991*, pages 127–202. Birkhäuser, 1993. ↑2, 3, 3.1, 3.2, 12, 3.2, 3.5, 3.6, 3.3.1, 3.3.2, 5.5.

[Nér76] André Néron. Hauteurs et fonctions thêta. *Rend. Sem. Mat. Fis. Milano*, 46:111–135 (1978), 1976. ↑2.

[Ols11] M. Olsson. Towards non-abelian p-adic Hodge theory in the good reduction case. *Memoirs of the AMS*, (990), 2011. ↑3.1, 4.1, 4.1, 5.1, 5.2.

[Poo06] Bjorn Poonen. Heuristics for the Brauer-Manin obstruction for curves. *Experiment. Math.*, 15(4):415–420, 2006. ↑4.1, 5.3.3.

[PR83] Bernadette Perrin-Riou. Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe. *Invent. Math.*, 70(3):369–398, 1982/83. ↑2.

[Qui69] Daniel Quillen. Rational homotopy theory. *Ann. of Math. (2)*, 90:205–295, 1969. ↑5.1.

[Sch82] Peter Schneider. p-adic height pairings. I. *Invent. Math.*, 69(3):401–409, 1982. ↑2, 2.9.

[Sch94] A. J. Scholl. Height pairings and special values of L-functions. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 571–598. Amer. Math. Soc., Providence, RI, 1994. ↑3.1.

[Sch98] Peter Schneider. Basic notions of rigid analytic geometry. In *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, volume 254 of *London Math. Soc. Lecture Note Ser.*, pages 369–378. Cambridge Univ. Press, Cambridge, 1998. ↑1.1.

[Sch99] Victor Scharaschkin. *Local-global problems and the Brauer-Manin obstruction*. ProQuest LLC, Ann Arbor, MI, 1999. Thesis (Ph.D.)–University of Michigan. ↑5.3.3.

[Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, English edition, 2002. ↑A, A.1, A.2, A, A.3, A.1, 1.

[Sik17] S. Siksek. Quadratic Chabauty for modular curves. *preprint*, 2017. ↑4.

[Smi05] B. Smith. *Explicit endomorphisms and correspondences*. PhD thesis, University of Sydney, 2005. ↑4.4.

[Sto02] Michael Stoll. On the height constant for curves of genus two. II. *Acta Arith.*, 104(2):165–182, 2002. ↑5.4.3.

[Sto06] Michael Stoll. Independence of rational points on twists of a given curve. *Compos. Math.*, 142(5):1201–1214, 2006. ↑1.

[Sto19] Michael Stoll. Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank. *J. Eur. Math. Soc. (JEMS)*, 21(3):923–956, 2019. ↑1.15, 1.20.

[SW13] William Stein and Christian Wuthrich. Algorithms for the arithmetic of elliptic curves using Iwasawa theory. *Mathematics of Computation*, 82(283):1757–1792, 2013. ↑2.6.

[The19] The LMFDB Collaboration. The L-functions and Modular Forms Database. http://www.lmfdb.org, 2019. [Online; accessed 1 July 2019]. ↑4.7.

[The20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. `https://www.sagemath.org`. ↑1.

[Tui16] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$. *Math. Comp.*, 85(298):961–981, 2016. ↑1.4, 1.4, 1.52, 1.4.

[Tui17] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields Appl.*, 45:301–322, 2017. ↑1.4, 1.45, 1, 1.4, 1.52, 1.4.

[VBHM20] Raymond Van Bommel, David Holmes, and J. Steffen Müller. Explicit arithmetic intersection theory and computation of Néron-Tate heights. *Mathematics of Computation*, 89(321):395–410, 2020. ↑2.3.1.

[Voj91] Paul Vojta. Siegel's theorem in the compact case. *Ann. of Math. (2)*, 133(3):509–548, 1991. ↑1.1.

[Vol03] Vadim Vologodsky. Hodge structure on the fundamental group and its application to p-adic integration. *Mosc. Math. J.*, 3(1):205–247, 260, 2003. ↑1.11.

[vW99] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225):307–320, 1999. ↑5.5.

[Wut04] Christian Wuthrich. On p-adic heights in families of elliptic curves. *J. London Math. Soc. (2)*, 70(1):23–40, 2004. ↑2.10.

[Zar90] Yuri G. Zarhin. p-adic heights on abelian varieties. In *Séminaire de Théorie des Nombres, Paris 1987–88*, volume 81 of *Progr. Math.*, pages 317–341. Birkhäuser Boston, Boston, MA, 1990. ↑2.

[Zar96] Yu. G. Zarhin. p-adic abelian integrals and commutative Lie groups. volume 81, pages 2744–2750. 1996. Algebraic geometry, 4. ↑1.11.

[Zha93] Shouwu Zhang. Admissible pairing on a curve. *Invent. Math.*, 112(1):171–193, 1993. ↑5.3.1.

J. S. Balakrishnan, Department of Mathematics and Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA

Email address: `jbala@bu.edu`

J. S. Müller, Bernoulli Institute, University of Groningen, Nijenborgh 9, 9747 AG Groningen, The Netherlands

Email address: `steffen.muller@rug.nl`