2020-01-13

Explicit Coleman integration for curves

EXPLICIT COLEMAN INTEGRATION FOR CURVES

JENNIFER S. BALAKRISHNAN AND JAN TUITMAN

Abstract. The Coleman integral is a p-adic line integral that plays a key role in computing several important invariants in arithmetic geometry. We give an algorithm for explicit Coleman integration on curves, using the algorithms of the second author [Tui16, Tui17] to compute the action of Frobenius on p-adic cohomology. We present a collection of examples computed with our implementation. This includes integrals on a genus 55 curve, where other methods do not currently seem practical.

1. Introduction

In a series of papers in the 1980s, Coleman formulated a p-adic theory of line integration on curves and higher-dimensional varieties with good reduction at p and gave numerous applications in arithmetic geometry. This includes the computation of p-adic polylogarithms [Col82], torsion points on Jacobians of curves [Col85b], rational points on certain curves with small Mordell-Weil rank [Col85a], p-adic heights on curves (joint with Gross) [CG89], and p-adic regulators in K-theory (joint with de Shalit) [CdS88]. In [CdS88], Coleman and de Shalit also introduced a theory of iterated p-adic integration on curves, which plays an important role in Kim's nonabelian Chabauty program [Kim09] to compute rational points on curves.

Besser and de Jeu [BdJ08] gave the first algorithm for explicit computation of these integrals—now known as *Coleman integrals*—in the case of iterated integrals on $\mathbf{P}^1 \setminus \{0, 1, \infty\}$. These integrals compute p-adic polylogarithms, which are conjecturally related to special values of p-adic L-functions. Balakrishnan, Bradshaw and Kedlaya [BBK10] gave an algorithm to compute single Coleman integrals on odd degree models of hyperelliptic curves, which was further generalized to iterated Coleman integrals on arbitrary hyperelliptic curves in [Bal13, Bal15]. These algorithms all rely on an algorithm for computing the action of Frobenius on p-adic cohomology to realize Dwork's principle of *analytic continuation along Frobenius*. In the case of odd degree hyperelliptic curves, this is achieved by Kedlaya's algorithm [Ked01].

Because of all of the applications mentioned above, it is of interest to develop practical algorithms to carry out Coleman integration on *any* smooth curve. In the present work, we do this by building on work of Tuitman [Tui16, Tui17], which generalizes Kedlaya's algorithm to this setting. We give algorithms to compute single Coleman integrals on curves and develop the precision bounds necessary to obtain provably correct results. Moreover, we provide a complete implementation [BT] of our algorithms in the computer algebra system `Magma` [BCP97] and present a selection of examples, including the computation of torsion points on Jacobians and carrying out the Chabauty–Coleman method for finding rational points on curves. We also compare our algorithms to other leading techniques. We present a selection of examples computed using our algorithm, including integrals on a genus 55 curve, where other techniques do not currently seem practical. Our computation

Date: January 14, 2020.
2010 *Mathematics Subject Classification.* 11S80 (primary), 11Y35, 11Y50 (secondary).

shows that the Jacobian of this curve has positive Mordell–Weil rank. The case of iterated Coleman integrals will be discussed in a subsequent paper.

The structure of the paper is as follows: First, in Section 2 we recall what we need from the theory of p-adic cohomology and the algorithms from [Tui16, Tui17]. In Section 3, we present our algorithms for Coleman integration. Next, in Section 4, we discuss the precision bounds necessary to obtain provably correct results. In Section 5, we carry out a complexity analysis of our algorithm and compare it with other approaches. Finally, in Section 6, we conclude with a collection of examples computed with our implementation [BT].

2. p-adic cohomology

Let X be a nonsingular projective geometrically irreducible curve of genus g over $\mathbf{Q}$ given by a (possibly singular) plane model $Q(x, y) = 0$ with $Q(x, y) \in \mathbf{Z}[x, y]$ a polynomial that is irreducible and monic in y. Recall that such a model can easily be obtained from other representations of X, e.g. by computing (a defining equation of) its function field.

Let d_x and d_y denote the degrees of the morphisms x and y, respectively, from X to the projective line. Note that these correspond to the degrees of Q in the variables y and x, respectively. For the performance of our algorithms it will be best to first take d_x as small as possible (ideally equal to the gonality of the curve) and then d_y as small as possible for this value of d_x.

Definition 2.1. *Let $\Delta(x) \in \mathbf{Z}[x]$ denote the discriminant of Q with respect to the variable y. Moreover, define $r(x) \in \mathbf{Z}[x]$ to be the squarefree polynomial with the same zeros as $\Delta(x)$, in other words, $r = \Delta/(\gcd(\Delta, \frac{d\Delta}{dx}))$.*

Definition 2.2. *Let $W^0 \in \mathrm{GL}_{d_x}(\mathbf{Q}[x, 1/r])$ and $W^\infty \in \mathrm{GL}_{d_x}(\mathbf{Q}[x, 1/x, 1/r])$ denote matrices such that, if we denote*

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

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

1. *$[b_0^0, \dots, b_{d_x-1}^0]$ is an integral basis for $\mathbf{Q}(X)$ over $\mathbf{Q}[x]$,*
2. *$[b_0^\infty, \dots, b_{d_x-1}^\infty]$ is an integral basis for $\mathbf{Q}(X)$ over $\mathbf{Q}[1/x]$,*

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

There are good algorithms available to compute such matrices, e.g. [Hes02, Bau16].

Remark 2.3. *We assume that X is a curve over $\mathbf{Q}$ since it is more delicate to compute integral bases in function fields over a p-adic field, both in practice and in theory (to finite precision everything is smooth).*

Example 2.4. *Let $X/\mathbf{Q}$ 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* $\mathbf{Q}[x]$ *and* $\mathbf{Q}[1/x]$*, respectively.*

Definition 2.5. *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 2.6 ([Tui17, Assumption 1])**.**

(1) *The discriminant of* $r(x)$ *is contained in* $\mathbf{Z}_p^\times$*.*
(2) *If we denote* $b_j^0 = \sum_{i=0}^{d_x-1} W^0_{i+1,j+1} y^i$ *and* $b_j^\infty = \sum_{i=0}^{d_x-1} W^\infty_{i+1,j+1} y^i$ *for all* $0 \leq j \leq d_x - 1$*, and if we let* $\mathbf{F}_p(x, y)$ *be the field of fractions of* $\mathbf{F}_p[x, y]/(Q)$*, then:*
   (a) *The reduction modulo* p *of* $[b_0^0, \ldots, b_{d_x-1}^0]$ *is an integral basis for* $\mathbf{F}_p(x, y)$ *over* $\mathbf{F}_p[x]$*.*
   (b) *The reduction modulo* p *of* $[b_0^\infty, \ldots, b_{d_x-1}^\infty]$ *is an integral basis for* $\mathbf{F}_p(x, y)$ *over* $\mathbf{F}_p[1/x]$*.*
(3) $W^0 \in \mathrm{GL}_{d_x}(\mathbf{Z}_p[x, 1/r])$ *and* $W^\infty \in \mathrm{GL}_{d_x}(\mathbf{Z}_p[x, 1/x, 1/r])$*.*
(4) *Denote:*

$$\mathcal{R}^0 = \mathbf{Z}_p[x]b_0^0 \quad + \ldots + \mathbf{Z}_p[x]b_{d_x-1}^0,$$
$$\mathcal{R}^\infty = \mathbf{Z}_p[1/x]b_0^\infty + \ldots + \mathbf{Z}_p[1/x]b_{d_x-1}^\infty.$$

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

Remark 2.7. *These conditions imply that the curve* X *has good reduction at* p *but are stronger. Note that any triple* (Q, W^0, W^∞) *has good reduction at all but finitely many prime numbers* p*.*

From now on, we fix a prime p and a triple (Q, W^0, W^∞) which has good reduction at p. In [Tui17, Proposition 2.3]) it is explained how one can associate to this data a smooth curve $\mathcal{X}$ over $\mathbf{Z}_p$ such that $\mathcal{X} \otimes \mathbf{Q}_p \cong X \otimes \mathbf{Q}_p$. Let X^{an} denote the rigid analytic space over $\mathbf{Q}_p$ which is the generic fibre of $\mathcal{X}$. There is a specialization map from X^{an} to the reduction of X modulo p. The fibres of this map are called *residue disks*. (For further background on rigid analytic geometry, see [FvdP04].)

Definition 2.8. *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* $r(x)$*.*

Remark 2.9. *From the fact that* (Q, W^0, W^∞) *has good reduction at* p*, it follows that a residue disk contains at most one very bad point and that this point is defined over an unramified extension of* $\mathbf{Q}_p$*.*

For a very bad point P, we will denote the ramification index of the map x by e_P. We let U denote the complement of the very bad points in X^{an}.

Definition 2.10. *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.*

Remark 2.11. *Note that all infinite points and infinite residue disks are bad.*

Remark 2.12. *If a point is very bad, this can mean one of three things:*

(1) $x(P) = \infty$*,*

(2) *the fiber of X above $x(P)$ contains a ramification point,*
(3) *the fiber of X above $x(P)$ contains a point mapping to a singularity of the plane model $Q(x, y) = 0$.*

We now introduce the main rings over which we work. Let $\langle\rangle^\dagger$ denote the ring of overconvergent functions obtained by weak completion of the corresponding polynomial ring.

Definition 2.13. *We denote*

$$S = \mathbf{Z}_p\langle x, 1/r\rangle, \qquad S^\dagger = \mathbf{Z}_p\langle x, 1/r\rangle^\dagger,$$
$$R = \mathbf{Z}_p\langle x, 1/r, y\rangle/(Q), \qquad R^\dagger = \mathbf{Z}_p\langle x, 1/r, y\rangle^\dagger/(Q).$$

A Frobenius lift $\mathrm{F}_p : R^\dagger \to R^\dagger$ is defined as a continuous ring homomorphism that reduces to the p-th power Frobenius map modulo p.

Theorem 2.14. *There exists a Frobenius lift $\mathrm{F}_p : R^\dagger \to R^\dagger$ for which $\mathrm{F}_p(x) = x^p$.*

Proof. See [Tui17, Thm. 2.6]. □

Definition 2.15. *For a point P on a smooth curve, we let ord_P denote the corresponding discrete valuation on the function field of the curve. In particular, ord_0 and ord_∞ are the discrete valuations on the rational function field $\mathbf{Q}(x)$ corresponding to the points 0 and ∞ on $\mathbf{P}^1_{\mathbf{Q}}$. We extend these definitions to matrices by taking the minimum over their entries.*

From the assumption that (Q, W^0, W^∞) has good reduction at p, it follows that the rigid cohomology spaces $H^1_{\mathrm{rig}}(U \otimes \mathbf{Q}_p)$ and $H^1_{\mathrm{rig}}(X \otimes \mathbf{Q}_p)$ are isomorphic to their algebraic de Rham counterparts [BC94].

Definition 2.16. *Let $[\omega_1, \ldots, \omega_{2g}]$ be p-adically integral 1-forms on U such that*

(1) *$\omega_1, \ldots, \omega_g$ form a basis for $H^0(X, \Omega^1_X)$,*
(2) *$\omega_1, \ldots, \omega_{2g}$ form a basis for $H^1_{rig}(X \otimes \mathbf{Q}_p)$,*
(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. The algorithm can be easily adapted so that (1) is satisfied as well, which is the convention we take.

Definition 2.17. *The p-th power Frobenius F_p acts on $H^1_{rig}(X \otimes \mathbf{Q}_p)$, so there exist a matrix $\Phi \in M_{2g\times 2g}(\mathbf{Q}_p)$ and functions $f_1, \ldots, f_{2g} \in R^\dagger \otimes \mathbf{Q}_p$ such that*

$$\mathrm{F}_p^*(\omega_i) = df_i + \sum_{j=1}^{2g} \Phi_{ij}\omega_j$$

for $i = 1, \ldots, 2g$.

Let us briefly recall from [Tui16, Tui17] how the matrix Φ and the functions $f_1, \ldots, f_{2g}$ are computed.

Algorithm 2.18.

(1) ***Compute the Frobenius lift.*** *Determine F_p as in Theorem 2.14, i.e. set $\mathrm{F}_p(x) = x^p$ and determine the elements $\mathrm{F}_p(1/r) \in S^\dagger$ and $\mathrm{F}_p(y) \in R^\dagger$ by Hensel lifting.*

(2) ***Finite pole order reduction.*** *For $i = 1, \dots, 2g$, find $f_{i,0} \in R^\dagger \otimes \mathbf{Q}_p$ such that*

$$\mathrm{F}_p^*(\omega_i) = df_{i,0} + G_i\left(\frac{dx}{r(x)}\right),$$

where $G_i \in R \otimes \mathbf{Q}_p$ only has poles at very infinite points.

(3) ***Infinite pole order reduction.*** *For $i = 1, \dots, 2g$, find $f_{i,\infty} \in R \otimes \mathbf{Q}_p$ such that*

$$\mathrm{F}_p^*(\omega_i) = df_{i,0} + df_{i,\infty} + H_i\left(\frac{dx}{r(x)}\right),$$

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

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

at all these points.

(4) ***Final reduction.*** *For $i = 1, \dots, 2g$, find $f_{i,end} \in R \otimes \mathbf{Q}_p$ such that*

$$\mathrm{F}_p^*(\omega_i) = df_{i,0} + df_{i,\infty} + df_{i,end} + \sum_{j=1}^{2g} \Phi_{ij}\omega_j,$$

where $\Phi \in M_{2g\times 2g}(\mathbf{Q}_p)$ is the matrix of F_p^* on $H^1_{rig}(U \otimes \mathbf{Q}_p)$ with respect to the basis $[\omega_1, \dots, \omega_{2g}]$.

The matrix Φ and the functions $f_i = f_{i,0} + f_{i,\infty} + f_{i,end}$ are exactly what we need from [Tui16, Tui17] to compute Coleman integrals.

3. Coleman integrals

Let $K/\mathbf{Q}_p$ be a totally ramified extension. Our goal is to compute the Coleman integral $\int_P^Q \omega$ of a 1-form $\omega \in \Omega^1(U \otimes \mathbf{Q}_p)$ of the second kind between points $P, Q \in X(K)$.

The Coleman integral satisfies several key properties, which we will use throughout our integration algorithms:

Theorem 3.1 (Coleman, Coleman–de Shalit)**.** *Let η, ξ be 1-forms on a wide open V of X^{an} and $P, Q, R \in V(K)$. Let $a, b \in K$. 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: $\int_P^Q \xi = \int_P^R \xi + \int_R^Q \xi$.*
(3) *Change of variables: If $V' \subset X'$ is a wide open subspace of a rigid analytic space X' and $\phi : V \to V'$ a rigid analytic map then $\int_P^Q \phi^*\xi = \int_{\phi(P)}^{\phi(Q)} \xi$.*
(4) *Fundamental theorem of calculus: $\int_P^Q df = f(Q) - f(P)$ for f a rigid analytic function on V.*
(5) *Galois equivariance: the integral is compatible with the action of $\mathrm{Gal}(K/\mathbf{Q}_p)$.*

Proof. [Col85b] for 1-forms of the second kind and [CdS88] for general 1-forms. □

Let us first explain how we specify a point P. Note that giving (x, y)-coordinates might not be sufficient even for a finite very bad point, since there may be multiple points on X lying above a singular point (x, y) of the plane model defined by Q. However, a point P is determined uniquely by the value of x ($1/x$ if P is infinite) together with the values of the functions b^0 (b^∞ if P is infinite).

Note that all of these values are p-adically integral. In our implementation, we therefore specify a point P by storing three values (`P‘x,P‘b,P‘inf`):

(1) `P‘x`: the x-coordinate of P ($1/x$ if x is infinite),
(2) `P‘b`: the values of the functions b^0 (b^∞ if P is infinite),
(3) `P‘inf`: true or false, depending on whether the point P is infinite or not.

We will often need power series expansions of functions in terms of a *local coordinate* (i.e., a uniformizing parameter) t at P. This local coordinate should not just be a local coordinate at P on $X \otimes \mathbf{Q}_p$, but on the model $\mathcal{X}$ over $\mathbf{Z}_p$ obtained from the triple (Q, W^0, W^∞) as in [Tui17, Prop. 2.3]. Then it follows that the reduction modulo p of t is a local coordinate at the reduction modulo p of P and that the residue disk at P is given by $|t| < 1$. In a bad residue disk, we will always expand functions at the very bad point. Therefore, in the following proposition, we only consider points that are either good or very bad.

Proposition 3.2. *Let $P \in X(\mathbf{Q}_p)$ be a point. Assume that P is either good or very bad. As a local coordinate at P, we can take*

$$t = \begin{cases} x - x(P) & \text{if } e_P = 1 \text{ (or } t = 1/x \text{ if } P \text{ is infinite)}, \\ b_i^0 - b_i^0(P) \text{ for some } i & \text{otherwise (with } b^0 \text{ replaced by } b^\infty \text{ if } P \text{ is infinite)}. \end{cases}$$

Proof. By definition $e_P = \mathrm{ord}_P(x - x(P))$ (or $e_p = \mathrm{ord}_P(1/x)$ if P is infinite). So if $e_P = 1$ then $t = (x - x(P))$ (or $t = 1/x$ if P is infinite) is a local coordinate at P on $X \otimes \mathbf{Q}_p$. If $e_P \geq 2$, then at least one of the $b_i^0 - b_i^0(P)$ (with b^0 replaced by b^∞ if P is infinite) has to be a local coordinate at P on $X \otimes \mathbf{Q}_p$, since otherwise there would be no functions on $X \otimes \mathbf{Q}_p$ of order 1 at P. In both cases, since (Q, W^0, W^∞) has good reduction at p, the divisor defined by t on $\mathcal{X}$ is smooth over $\mathbf{Z}_p$, so that t is also a local coordinate at P in the stronger sense explained above. □

After choosing a local coordinate t at P, in our implementation we compute `xt,bt` where

(1) `xt` is the power series expansion in t of the function x ($1/x$ if P is infinite),
(2) `bt` is the tuple of power series expansions in t of the functions b^0 (b^∞ if P is infinite).

Note that all of these power series have p-adically integral coefficients. From `xt,bt` we will be able to determine the power series expansion in t of any function which is regular at P.

A 1-form $\omega \in \Omega^1(U \otimes \mathbf{Q}_p)$ is of the form $f dx$ with $f \in R \otimes \mathbf{Q}_p$. We will usually represent it as follows:

$$\omega = \sum_{i=0}^{d_x - 1} \sum_{j \in J} \frac{f_{ij}(x)}{r(x)^j} b_i^0 \frac{dx}{r}$$

with $f_{ij} \in \mathbf{Q}_p[x]$ such that $\deg(f_{ij}) < \deg(r(x))$ for all i, j, since ω needs to be in this form to start the cohomological reduction procedures outlined in Section 2.

We begin by describing the computation of *tiny* integrals.

Definition 3.3. *A tiny integral $\int_P^Q \omega$ is a Coleman integral with endpoints $P, Q \in X(\mathbf{Q}_p)$ that lie in the same residue disk.*

Algorithm 3.4 (Computing the tiny integral $\int_P^Q \omega$)**.**

(1) *If the residue disk of P, Q is bad, then find the very bad point $P' \in X(\mathbf{Q}_p)$, otherwise set $P' = P$.*
(2) *Compute a local coordinate t and the power series expansions* `xt,bt` *at P'.*
(3) *Integrate using t as coordinate:*

$$\int_P^Q \omega = \int_{t(P)}^{t(Q)} \omega(t).$$

The Laurent series expansion $\omega(t)$ can be determined from `xt,bt`*. Note that ω is of the second kind, so the coefficient of $t^{-1}dt$ is zero.*

Remark 3.5. *The calculation of tiny integrals does not require computing the action of Frobenius on the cohomology space $H^1_{rig}(X \otimes \mathbf{Q}_p)$. This can be a useful consistency check for the integration algorithms that follow, which do use the computation of the action of Frobenius.*

Remark 3.6. *Note that Algorithm 3.4 can also be applied for points defined over $\mathbf{Q}_p(p^{1/e})$ for some positive integer e (as long as they are within the same residue disk). This is useful for applications in bad residue disks, as we will see later (Algorithm 3.12).*

When $P, Q \in X(\mathbf{Q}_p)$ do not lie in the same residue disk, this approach breaks down since the Laurent series expansions do not converge anymore. In this case we will compute the Coleman integrals $\int_P^Q \omega_i$ for $i = 1, \dots, 2g$ by solving a linear system imposed by the p-th power Frobenius map F_p. We first assume that the functions $f_1, \dots, f_{2g}$ from Section 2 converge at P, Q. Note that $f_1, \dots, f_{2g}$ converge at all good points, but only at bad points that are not too close to the corresponding very bad point. This will be made more precise in the next section.

Algorithm 3.7 (Compute the $\int_P^Q \omega_i$ assuming $f_1, \dots, f_{2g}$ converge at P, Q)**.**

(1) *Compute the action of Frobenius on $H^1_{rig}(X \otimes \mathbf{Q}_p)$ using Algorithm 2.18 and store Φ and $f_1, \dots, f_{2g}$.*
(2) *Determine the tiny integrals $\int_P^{F_p(P)} \omega_i$ and $\int_{F_p(Q)}^Q \omega_i$ for $i = 1, \dots, 2g$ using Algorithm 3.4.*
(3) *Compute $f_i(P) - f_i(Q)$ for $i = 1, \dots, 2g$ and use the system of equations*

$$\sum_{j=1}^{2g} (\Phi - I)_{ij} \left(\int_P^Q \omega_j \right) = f_i(P) - f_i(Q) - \int_P^{F_p(P)} \omega_i - \int_{F_p(Q)}^Q \omega_i$$

to solve for all $\int_P^Q \omega_i$, as in [BBK10, Algorithm 11].

Remark 3.8. *Note that the matrix $\Phi - I$ is invertible, since the eigenvalues of Φ are algebraic numbers of complex absolute value $p^{1/2}$.*

Remark 3.9. *The algorithm above follows from the first four properties of the Coleman integral in Theorem 3.1, and in particular, change of variables is carried out via Frobenius, which is a rigid analytic map.*

Remark 3.10. *An alternate approach to Algorithm 3.7 that applies outside of the bad residue disks is to compute Teichmüller points (fixed points of the Frobenius map) within the residue disks, solve the resulting linear system between Teichmüller points, then correct endpoints via tiny integrals.*

Remark 3.11. *Note that Algorithm 3.7 can also be applied for points defined over $\mathbf{Q}_p(p^{1/e})$ for some positive integer e. This is useful for applications in bad residue disks, as we will see below in Algorithm 3.12.*

When P or Q are bad points and $f_1, \dots, f_{2g}$ do not converge there, the idea is simply to find points P', Q' in the residue disks of P and Q where these functions do converge, compute the integrals between the new points, and correct for the difference with tiny integrals.

Algorithm 3.12 (Computing the $\int_P^Q \omega_i$ in general)**.**

(1) *Determine P', Q' in the residue disks of P, Q at which all functions $f_1, \dots, f_{2g}$ converge. (See Remark 4.4.)*
(2) *Compute the tiny integrals $\int_P^{P'} \omega_i$ and $\int_{Q'}^{Q} \omega_i$ for $i = 1, \dots, 2g$ using Algorithm 3.4.*
(3) *Determine $\int_{P'}^{Q'} \omega_i$ for $i = 1, \dots, 2g$ using Algorithm 3.7.*
(4) *Compute*

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

In general, we have to take the points P', Q' to be defined over some (totally ramified) extension K of $\mathbf{Q}_p$ to get far enough away from the very bad point in the bad residue disk; see Remark 4.4. We will always take this extension to be of the form $\mathbf{Q}_p(p^{1/e})$ for some positive integer e. Recall that Algorithms 3.4 and 3.7 can still be applied in this case and that we may take $P' \in X(\mathbf{Q}_p)$ in Algorithm 3.4. Since computing in extensions is more expensive, integrals involving bad points are usually the hardest to compute.

For more general 1-forms of the second kind $\omega \in \Omega^1(U \otimes \mathbf{Q}_p)$, we can now compute the Coleman integrals $\int_P^Q \omega$ as follows from the output of Algorithms 3.7 and 3.12.

Algorithm 3.13 (Computing $\int_P^Q \omega$)**.**

(1) *Use Steps (2),(3) and (4) of Algorithm 2.18 to find $f \in R$ and $c_i \in \mathbf{Q}_p$ for $i = 1, \dots, 2g$ such that*

$$\omega = df + \sum_{i=1}^{2g} c_i \omega_i.$$

(2) *Compute $f(Q) - f(P)$ and determine*

$$\int_P^Q \omega = f(Q) - f(P) + \sum_{i=1}^{2g} c_i \int_P^Q \omega_i.$$

Remark 3.14. *Note that we are only considering points P, Q defined over a totally ramified extension K of $\mathbf{Q}_p$ because we want the residue field to be $\mathbf{F}_p$ so that we work with a lift of p-power Frobenius. It would be of interest to extend our work to points defined over arbitrary finite extensions of $\mathbf{Q}_p$ as discussed in* [BBK10, Remark 12] *and more generally work with a lift of q-power Frobenius.*

4. Precision bounds

So far we have not paid any attention to the fact that we can only compute to finite p-adic and t-adic precision in our algorithms. By *precision* we will always mean *absolute* p-adic precision, i.e., the valuation of the error term. We extend the p-adic valuation and the notion of precision to all finite extensions of $\mathbf{Q}_p$, where they will take non-integer values in general.

Let us start with tiny integrals.

Proposition 4.1. *Let e be a positive integer and $P, Q \in X(\mathbf{Q}_p(p^{1/e}))$ two points in the same residue disk accurate to precision N. Let t be a local coordinate (in the sense of Proposition 3.2) at the point P' from Algorithm 3.4. Suppose that $\omega = g(t)dt$ is a differential of the second kind with*

$$g(t) = a_{-k}t^{-k} + a_{-k+1}t^{-k+1} + \ldots \in \mathbf{Z}_p[[t]][t^{-1}]$$

for some positive integer k. If g is accurate to p-adic precision N and truncated modulo t^l, then the tiny integral $\int_P^Q \omega$ computed as in Algorithm 3.4 is correct to precision $\min\{\nu_1, \nu_2, \nu_3\}$ where:

$$\begin{aligned}
\nu_1 &= 1/e + \min_{i \geq l}\{i/e - \lfloor \log_p(i+1) \rfloor\}, \\
\nu_2 &= N + \min_{0 \leq i \leq l-1}\{i/e - \lfloor \log_p(i+1) \rfloor\}, \\
\nu_3 &= N - k\max\{\mathrm{ord}_p(t(P)), \mathrm{ord}_p(t(Q))\} - \lfloor \log_p(k-1) \rfloor.
\end{aligned}$$

Proof. Recall from Algorithm 3.4 that

$$\int_P^Q \omega = \int_{t(P)}^{t(Q)} \omega(t) = \sum_{i=-k}^{\infty} \frac{a_i}{i+1}\left(t(Q)^{i+1} - t(P)^{i+1}\right).$$

where $a_{-1} = 0$ since ω is of the second kind. Since P, Q both lie in the residue disk given by $|t| < 1$, we have that $\mathrm{ord}_p(t(P)), \mathrm{ord}_p(t(Q)) \geq 1/e$.

First, we bound the error introduced by omitting the terms with $i \geq l$. Note that

$$\mathrm{ord}_p(t(P)^{i+1}), \mathrm{ord}_p(t(Q)^{i+1}) \geq (i+1)/e$$

and

$$\mathrm{ord}_p(i+1) \leq \lfloor \log_p(i+1) \rfloor.$$

Therefore, the valuation of this error is at least ν_1.

Next, we consider the error coming from terms with $0 \leq i \leq l-1$. Since $t(P), t(Q)$ are accurate to precision N and have valuation at least $1/e$, we have that $t(P)^{i+1}, t(Q)^{i+1}$ are correct to precision $N + i/e$. Therefore, the valuation of this error is at least ν_2.

Finally, we bound the error coming from terms with $-k \leq i \leq -2$. This time $t(P)^{i+1}, t(Q)^{i+1}$ are correct to precision at least $N + i\,\mathrm{ord}_p(t(P)), N + i\,\mathrm{ord}_p(t(Q))$, respectively (since the loss of precision of an inversion is 2 times the valuation). Therefore, the valuation of the error is at least ν_3 this time. □

Remark 4.2. *Since we always have that $\nu_2 \leq N$, there is no point in increasing the t-adic precision l further if $\nu_1 \geq N$ already. Therefore, in our implementation we take l to be minimal such that $\nu_1 \geq N$.*

To compute integrals that are not tiny, in Algorithm 3.7 we have to evaluate the functions

$$f_i = f_{i,0} + f_{i,\infty} + f_{i,end}$$

from Section 2 at the endpoints for $i = 1, \ldots, 2g$. Evaluating an element of $R^\dagger \otimes \mathbf{Q}_p$ at a bad point leads to problems with convergence and loss of precision. We first recall from [Tui16, Tui17] what we know about the poles of the functions $f_{i,0}, f_{i,\infty}, f_{i,end} \in R^\dagger \otimes \mathbf{Q}_p$.

The only poles of infinite order are those of the $f_{i,0}$ at the finite very bad points. It follows from [Tui17, Prop. 2.12, Prop. 3.3, Prop. 3.7] that

$$f_{i,0} = \sum_{j=0}^{d_x-1} \sum_{k=1}^{\infty} \frac{c_{ijk}(x)}{r(x)^k} b_j^0, \tag{1}$$

for all i, where the c_{ijk} are elements of $\mathbf{Q}_p[x]$ of degree smaller than $\deg(r)$ that satisfy

$$\mathrm{ord}_p(c_{ijk}) \geq \lfloor k/p \rfloor + 1 - \lfloor \log_p(ke_0) \rfloor \tag{2}$$

with $e_0 = \max\{e_P \colon P \text{ finite very bad point}\}$.

Similarly, it follows from [Tui17, Prop. 2.12, Prop. 3.4, Thm. 3.6] that

$$f_{i,\infty} = \sum_{j=0}^{d_x-1} \sum_{k=0}^{\kappa_1} c_{ijk} x^k b_j^0 = \sum_{j=0}^{d_x-1} \sum_{k=\kappa_2}^{\kappa_3} d_{ijk} x^k b_j^\infty \tag{3}$$

for all i, where the c_{ijk}, d_{ijk} are elements of $\mathbf{Q}_p$ and

$$\kappa_3 \leq -\min\{p(\mathrm{ord}_0(W)+1), (\mathrm{ord}_\infty(W^{-1})+1)\},$$

where $W = (W^0)^{-1}W^\infty$. This determines bounds on κ_1, κ_2 as well.

Finally, it follows from [Tui17, Thm. 3.6] that

$$f_{i,end} = \sum_{j=0}^{d_x-1} \sum_{k=0}^{\lambda_1} c_{ijk} x^k b_j^0 = \sum_{j=0}^{d_x-1} \sum_{k=\lambda_2}^{\lambda_3} d_{ijk} x^k b_j^\infty \tag{4}$$

for all i, where the c_{ijk}, d_{ijk} are elements of $\mathbf{Q}_p$ and

$$\lambda_3 \leq -(\mathrm{ord}_0(W)+1).$$

Note that this determines bounds on λ_1, λ_2 as well.

Proposition 4.3. *On a finite bad residue disk, the functions $f_{i,0}$ converge outside of the closed disk defined by $\mathrm{ord}_p(r(x)) \geq 1/p$.*

Proof. This is clear from (1) and (2). □

Remark 4.4. *Let t denote a local coordinate at the very bad point of a finite bad residue disk. Then we have that $\mathrm{ord}_p(r(x)) < 1/p$ is equivalent to the condition $\mathrm{ord}_p(t) < \frac{1}{pe_P}$. Consequently, for the functions $f_{i,0}$ to converge at a point $P' \in X(\mathbf{Q}_p(p^{1/e}))$ in the residue disk of P, we need to take $e > pe_P$.*

When $f_1, \ldots, f_{2g}$ do converge at a point P, their computed values at this point will suffer some loss of p-adic precision in general. In the next three propositions we quantify this precision loss for good, finite bad, and infinite points, respectively.

Proposition 4.5. *Suppose that the functions $f_{i,0}, f_{i,\infty}, f_{i,end}$ are accurate to precision N. Moreover, let e be a positive integer and let $P \in X(\mathbf{Q}_p(p^{1/e}))$ be a good point that is accurate to precision N. Then the computed values $f_i(P)$ are correct to precision N as well.*

Proof. Note that a good point is always finite. Since we have that $\mathrm{ord}_p(x(P)) \geq 0$ and $\mathrm{ord}_p(r(x(P))) = 0$, there is no loss of precision in evaluating (1) and the expressions in the middle of (3) and (4). □

Proposition 4.6. *Suppose that the functions $f_{i,0}, f_{i,\infty}, f_{i,end}$ are accurate to precision N. Moreover, let e be a positive integer and let $P \in X(\mathbf{Q}_p(p^{1/e}))$ be a finite bad point that is accurate to precision N. Let $\epsilon = \mathrm{ord}_p(r(P))$ and suppose that $\epsilon < 1/p$. Define a function π on positive integers by*

$$\pi(k) = \max\{N, \lfloor k/p \rfloor + 1 - \lfloor \log_p(ke_0) \rfloor\},$$

where $e_0 = \max\{e_P \colon P \text{ finite bad point }\}$. Then the computed values $f_i(P)$ are correct to precision

$$\min_{k \in \mathbf{N}} \{\pi(k) - k\epsilon\}.$$

Proof. In this case $\mathrm{ord}_p(x(P)) \geq 0$, but $\mathrm{ord}_p(r(x(P))) = \epsilon$ with $0 < \epsilon < 1/p$. Clearly there is still no loss of precision in evaluating the expressions in the middle of (3) and (4). However for the $f_{i,0}$ there will be loss of precision. After dropping the terms with valuation greater than or equal to N in (1), the coefficient c_{ijk} will be correct to precision $\pi(k)$ for all k. Dividing by $r(x(P))^k$ leads to the loss of $k\epsilon$ digits of precision, so the terms corresponding to k will be correct to precision $\pi(k) - k\epsilon$. Taking the minimum over k, we obtain the result. □

Proposition 4.7. *Suppose that the functions $f_{i,0}, f_{i,\infty}, f_{i,end}$ are accurate to precision N. Moreover, let e be a positive integer and let $P \in X(\mathbf{Q}_p(p^{1/e}))$ be an infinite point that is accurate to precision N. Let $\epsilon = \mathrm{ord}_p(1/x(P))$. Then the computed values $f_i(P)$ are correct to precision*

$$N + \epsilon \min\{\mathrm{ord}_\infty(W^{-1}) + 1), p(\mathrm{ord}_0(W) + 1)\}.$$

Proof. In this case $\mathrm{ord}_p(x(P)) = -\epsilon < 0$ and $\mathrm{ord}_p(r(x(P))) = -\deg(r)\epsilon$. Let us first consider the $f_{i,0}$. Determining the $b_j^0(P)$ from the $b_j^\infty(P)$ in (1) leads to a precision loss of $-\mathrm{ord}_\infty(W^{-1})\epsilon$. However, since $\deg(c_{ijk}) < \deg(r)$, we have that

$$\mathrm{ord}_p\left(\frac{c_{ijk}(x(P))}{r(x(P))^k}\right) \geq \epsilon$$

for all $k \geq 1$. Therefore, we recover precision ϵ and the loss of precision will be at most $-(\mathrm{ord}_\infty(W^{-1}) + 1)\epsilon$. Evaluating the expressions on the right of (3) and (4) leads to precision loss at most

$$-\min\{p(\mathrm{ord}_0(W) + 1), (\mathrm{ord}_\infty(W^{-1}) + 1)\}\epsilon$$

and

$$-(\mathrm{ord}_0(W) + 1)\epsilon,$$

respectively. The result follows easily from this. □

Now all that is left to analyze in Algorithm 3.7 is the precision loss from solving the linear system, i.e. computing the matrix $(\Phi - I)^{-1}$ and multiplying by it.

Proposition 4.8. *Suppose that the matrix Φ is p-adically integral and accurate to precision N. Moreover, let e be a positive integer and let $P, Q \in X(\mathbf{Q}_p(p^{1/e}))$ be points accurate to precision N. Suppose that the right hand side of (3) in Algorithm 3.7 is accurate to precision $N' \leq N$ according to Propositions 4.1, 4.5, 4.6, and 4.7. Then the integrals $\int_P^Q \omega_i$ as computed in Algorithm 3.7 are correct to precision*

$$N' - \mathrm{ord}_p(\det(\Phi - I)).$$

Proof. This follows since $(\Phi - I)^{-1}$ has valuation at least $-\mathrm{ord}_p(\det(\Phi - I))$ and is correct to precision $N - \mathrm{ord}_p(\det(\Phi - I))$. □

Remark 4.9. *If we do not assume that Φ is p-adically integral, then we can show that the integrals $\int_P^Q \omega_i$ as computed in Algorithm 3.7 are correct to precision*

$$N' - \mathrm{ord}_p(\det(\Phi - I)) - \delta$$

with δ defined as in [Tui17, Definition 4.4].

Remark 4.10. *To analyze the loss of precision in Algorithm 3.13, we proceed as follows. First, we use* [Tui17, Prop. 3.7, Prop. 3.8] *to determine the precision to which f and the c_i are correct. Then we proceed as in Propositions 4.5, 4.6, and 4.7 to determine the precision of the computed values of $f(P)$, $f(Q)$ and $\int_P^Q \omega_i$ for $i = 1, \ldots, 2g$. Finally, we determine the precision to which $\int_P^Q \omega$ is correct, taking into account the valuations of the c_i as well.*

5. Complexity analysis and comparison with other algorithms

In this section, we discuss the complexity of our algorithm and compare it to other approaches. We use the $\widetilde{O}(-)$ notation that ignores logarithmic factors, i.e. $\widetilde{O}(f)$ denotes the class of functions that lie in $O(f \log^k(f))$ for some $k \in \mathbf{N}$. To be able to apply the complexity analysis from [Tui17] we will need one more assumption from that paper:

Assumption 5.1 ([Tui17, Assumption 2]). *Both $-\operatorname{ord}_P(W^0)$ and $-\operatorname{ord}_P(W^\infty)$ are contained in $O(d_x d_y)$ for all $P \in \mathbf{P}^1(\overline{\mathbf{Q}})$.*

In [Tui17], it is explained why this is a reasonable assumption: for instance, standard algorithms for computing integrals bases of function fields will yield matrices W^0, W^∞ satisfying this condition.

5.1. Complexity analysis.

Proposition 5.2. *Let notation and assumptions be as introduced in Section 2. The matrix Φ and the functions $f_1, \dots, f_{2g}$ from Definition 2.17 can be computed to p-adic precision N using Algorithm 2.18 in time $\widetilde{O}(p d_x^4 d_y^2 (N^2 + d_x d_y N))$.*

Proof. Take the maximum over the four steps in [Tui17, Section 4], leaving N instead of replacing it with $O(d_x d_y)$. Note that technically, here we have to replace N by the working precision of the algorithm from [Tui17], necessary to obtain the matrix Φ to precision N. However, by the argument from [Tui17, Proposition 4.9], this working precision can be chosen to be $N + O(\log(d_x d_y))$, yielding the same expression for the complexity since $\log(d_x)$ and $\log(d_y)$ are absorbed by the $\widetilde{O}$ symbol. □

In what follows, we will restrict to the (generic) case of integrals between good points, only making a few remarks about integrals between bad points. First, we consider tiny integrals between good points.

Proposition 5.3. *Let $P, Q \in X(\mathbf{Q}_p)$ be good points that lie in the same residue disk and ω an element of our basis $[\omega_1, \dots, \omega_{2g}]$. Then Algorithm 3.4 will compute $\int_P^Q \omega$ to p-adic precision N in time $\widetilde{O}(\log(p) d_x^2 d_y N^2)$.*

Proof. Since P is a good point, it can be written as $P = (x_0, y_0)$ with $x_0, y_0 \in \mathbf{Z}_p$, and we can take the local coordinate at P to be $t = x - x_0$. Suppose that we use t-adic precision l in our computations, where l will be determined later. We need to expand ω as a power series in t using t-adic Hensel lifting in the ring $A = (\mathbf{Z}/p^N\mathbf{Z})[t]/(t^l)$. Note that a single operation in A takes time $\widetilde{O}(\log(p) N l)$.

From the equation $Q(t + x_0, y(t)) = 0$, which can be computed in $O(d_x d_y)$ operations in A and has degree d_x in y, we can compute $y(t)$ by Hensel lifting the solution y_0 modulo t in $O(d_x \log(l))$ operations in A. Computing the power series expansion of $1/r(x)$ in t is similar but easier. By [Tui17, Section 4.1], we have that

$$\omega = g(x, y) \frac{dx}{r(x)}$$

where $g(x, y) \in \mathbf{Z}_p[x, y]$ is of degree at most $d_x - 1$ in y and degree $O(d_x d_y)$ in x. Therefore, $\omega(t)$ can be computed in $O(d_x^2 d_y \log(l))$ operations in A, i.e. in time $\widetilde{O}(d_x^2 d_y N l)$.

The actual integration and evaluation at the endpoints can be done naively in time $\widetilde{O}(\log(p) N l)$.

Finally, by Remark 4.2, we should take l minimal such that

$$l + 1 - \lfloor \log_p(l+1) \rfloor \geq N.$$

Therefore l is $O(N)$ and the proposition follows. □

Now we consider general integrals between good points.

Proposition 5.4. *Let $P, Q \in X(\mathbf{Q}_p)$ be good points and ω an element of our basis $[\omega_1, \ldots, \omega_{2g}]$. Suppose that Φ is p-adically integral and $\mathrm{ord}_p(\det(\Phi - I)) = m$. Then Algorithm 3.7 will compute $\int_P^Q \omega$ to p-adic precision $N - m$ in time $\widetilde{O}(p d_x^4 d_y^2 (N^2 + d_x d_y N))$.*

Proof. By Proposition 5.2, the matrix Φ and the functions $f_1, \ldots, f_{2g}$ can be computed to p-adic precision N in time $\widetilde{O}(p d_x^4 d_y^2 (N^2 + d_x d_y N))$.

Since P is a good point, it can be written as $P = (x_0, y_0)$ with $x_0, y_0 \in \mathbf{Z}_p$. Note that $\mathrm{F}_p(P) = (x_0^p, y_p)$, where $y_p \in \mathbf{Z}_p$ can be obtained by Hensel lifting the solution y_0^p modulo p to the equation $Q(x_0^p, y) = 0$. This can be done in $O(d_x d_y \log(N))$ operations in $\mathbf{Z}_p$, i.e. in time $\widetilde{O}(\log(p) d_x d_y \log^2(N))$. The complexity of computing $\mathrm{F}_p(Q)$ is the same.

The tiny integrals $\int_P^{\mathrm{F}_p(P)} \omega_i$ and $\int_{\mathrm{F}_p(Q)}^Q \omega_i$ can be computed in time $\widetilde{O}(\log(p) d_x^2 d_y N^2)$ for a single value of i by Proposition 5.3. Since g is $O(d_x d_y)$ by [Tui17, Proposition 4.1], we can do this for all $1 \leq i \leq 2g$ in time $\widetilde{O}(\log(p) d_x^3 d_y^2 N^2)$.

The functions f_i have $\widetilde{O}(p d_x d_y N)$ terms, so can be evaluated at the points P and Q for all $1 \leq i \leq 2g$ in time $\widetilde{O}(p d_x^2 d_y^2 N^2)$.

Finally, the $2g \times 2g$ linear system can be solved (naively) in time $\widetilde{O}(\log(p) d_x^3 d_y^3 N)$ and the proposition follows. □

The input size of our algorithm is naturally determined by d_x, d_y, N and $\log(p)$. Note that the complexity bounds above are polynomial in d_x, d_y and N, but exponential in $\log(p)$. This is a typical feature of algorithms using p-adic cohomology, so should not come as a surprise. Actually, for integrals involving a finite bad point, the dependence of the complexity on p will even get a bit worse. By Remark 4.4, we will have to compute in an extension of $\mathbf{Q}_p$ of degree at least p, which will worsen the dependence of the complexity on p from (quasi)linear to (quasi)quadratic. (Note that this does not happen at infinite points, so it might be useful to transform the curve so that a bad point of interest is moved to infinity, but we have not yet tried this.)

5.2. **Comparison with other algorithms.**

Another approach that has often been used to compute $\int_P^Q \omega$ is as follows. Let J denote the Jacobian of X. First find some integer k such that (the reduction mod p of) the point $k(P - Q)$ is trivial in $J(\mathbf{F}_p)$. Note that for this k, one would usually take the order of $J(\mathbf{F}_p)$. After computing $k(P - Q)$ as an element (in the residue disk at 0) of $J(\mathbf{Q}_p)$, one is reduced to computing a tiny integral over this divisor and dividing by k. Here we discuss how this approach compares to ours.

Currently, implementations of algorithms to compute in $J(\mathbf{Q}_p)$ are restricted to very special curves, e.g. hyperelliptic ones. Indeed, for non-hyperelliptic curves of genus 4 or larger, there does not seem to be a readily available implementation of divisor arithmetic over $\mathbf{Q}_p$. In some cases,

this can be circumvented by computing in $J(\mathbf{Q})$ instead, which then suffers from coefficient swell. However, even if the Jacobian arithmetic over $\mathbf{Q}_p$ is not a problem, in general one has to compute the order of $J(\mathbf{F}_p)$ first. Suppose that p, N are small but d_x or d_y are large. The fastest known way to compute the order of $J(\mathbf{F}_p)$ is then to compute the zeta function of $X \otimes \mathbf{F}_p$ using the algorithm from [Tui17] and evaluate its numerator at 1. However, the complexity of that algorithm is that of our current algorithm with N of the order $\widetilde{O}(d_x d_y)$. In other words, for p, N fixed our algorithm computes Coleman integrals in time $\widetilde{O}(d_x^5 d_y^3)$, while the best known algorithm for computing the order of $J(\mathbf{F}_p)$ already takes time $\widetilde{O}(d_x^6 d_y^4)$. In Section 6.4, we consider an example with large d_x and d_y and present some timings.

As we will illustrate in the next section, the main strength of our algorithm is the range of examples it can routinely handle.

6. Examples

6.1. An example from the work of Bruin–Poonen–Stoll.

Let $X/\mathbf{Q}$ be the genus 3 curve given by the following plane model:

$$Q(x, y) = y^3 + (-x^2 - 1)y^2 - x^3 y + x^3 + 2x^2 + x = 0.$$

Bruin, Poonen, and Stoll [BPS16, Prop. 12.17] show that, under the assumption of the Generalized Riemann Hypothesis, the Jacobian of X has Mordell-Weil rank 1 over $\mathbf{Q}$. (Note that our working plane model is given by taking the equation in [BPS16, §12.9.2], provided by D. Simon, and setting $x := 1, z := x$.)

We have $W^0 = I$, which means that $b^0 = [1, y, y^2]$ is an integral basis for the function field of X over $\mathbf{Q}[x]$. Moreover, we have

$$W^\infty = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/x^2 & 0 \\ 0 & -1/x, & 1/x^3 \end{pmatrix},$$

so that $b^\infty = [1, y/x^2, -y/x + y^2/x^3]$ is an integral basis for the function field of X over $\mathbf{Q}[1/x]$.

We consider the following points on X : $P_1 = (0, 0), P_2 = (0, 1), P_3 = (-3, 4), P_4 = (-1, 0), P_5 = (-1, 1)$, as well as three very infinite points: P_6 with b^∞-values $[1, 0, 1]$, P_7 with b^∞-values $[1, 1, 1]$, and P_8 with b^∞-values $[1, 0, 0]$.

In [BPS16, Prop. 12.17], the authors compute $X(\mathbf{Q})$ by using the fact that $[(P_3) - (P_2)]$ is of infinite order in $J(\mathbf{Q})$ and running a 3-adic Chabauty–Coleman argument. In particular, by computing 3-adic tiny integrals between P_2 and P_3, they produce a two-dimensional subspace of regular 1-forms annihilating rational points on X and use the Coleman integrals of these differentials to show that these eight points are all of the rational points on X.

Here we show how to produce a basis for the two-dimensional space of annihilating 1-forms without immediately appealing to tiny integrals. While it is desirable to use tiny integrals whenever possible, some curves do not readily admit points of infinite order in $J(\mathbf{Q})$ that are given as small integral combinations of known rational points that allow a tiny integral computation. Consequently, in such a scenario, some arithmetic in the Jacobian would be needed to reduce the necessary Coleman integral computation to a tiny integral computation, as discussed in Section 5.2. The computation below shows how one might bypass the Jacobian arithmetic by using Coleman integrals that are not necessarily tiny integrals.

We have $r = x(x+1)(x^8+7x^7+21x^6+31x^5+3x^4-51x^3-69x^2-23x+4)$. Taking $p=3$ makes all eight points various types of bad:

Point P	$r(x(P))$	Type of point
$P_1 = (0,0)$	0	finite very bad
$P_2 = (0,1)$	0	finite very bad
$P_3 = (-3,4)$	-600	finite bad
$P_4 = (-1,0)$	0	finite very bad
$P_5 = (-1,1)$	0	finite very bad
$1/x(P_6) = 0, b^\infty = [1,0,1]$	∞	very infinite
$1/x(P_7) = 0, b^\infty = [1,1,1]$	∞	very infinite
$1/x(P_8) = 0, b^\infty = [1,0,0]$	∞	very infinite

We compute the 3-adic Coleman integrals on a basis of $H^1_{\mathrm{rig}}(X \otimes \mathbf{Q}_p)$, in particular, the regular 1-forms are given by

$$\begin{aligned}
\omega_1 = (b^0 \cdot (&-8x^8 - 8x^7 + 86x^6 + 192x^5 + 118x^4 + 12x,\\
&-31x^7 - 98x^6 - 75x^5 + 70x^4 + 183x^3 + 234x^2 + 83x - 12,\\
&31x^5 + 60x^4 - 52x^3 - 246x^2 - 119x + 12))\frac{dx}{r},\\
\omega_2 = (b^0 \cdot (&2x^8 - 4x^7 - 56x^6 - 120x^5 - 76x^4 + 6x^2,\\
&13x^7 + 44x^6 + 45x^5 - 22x^4 - 81x^3 - 144x^2 - 77x + 12,\\
&-13x^5 - 24x^4 + 28x^3 + 138x^2 + 77x - 12))\frac{dx}{r},\\
\omega_3 = (b^0 \cdot (&4x^7 + 22x^6 + 44x^5 + 30x^4 + 4x^3,\\
&-3x^7 - 10x^6 - 11x^5 + 6x^4 + 19x^3 + 42x^2 + 27x - 4,\\
&3x^5 + 4x^4 - 12x^3 - 46x^2 - 27x + 4))\frac{dx}{r},
\end{aligned}$$

producing the following values:

$$\begin{aligned}
\int_{P_1}^{P_2} \omega_1 &= 2\cdot 3^2 + 3^3 + 2\cdot 3^5 + 3^6 + 2\cdot 3^7 + 3^8 + O(3^9),\\
\int_{P_1}^{P_2} \omega_2 &= 3^3 + 3^4 + 2\cdot 3^5 + 2\cdot 3^6 + 3^7 + O(3^9),\\
\int_{P_1}^{P_2} \omega_3 &= 3 + 2\cdot 3^2 + 3^3 + 3^4 + 3^5 + O(3^9).
\end{aligned}$$

We use the values of these three integrals (i.e., by computing the kernel of the associated 3×1 matrix) to compute that the two differentials

$$\begin{aligned}
\xi_1 &= (1+O(3^9))\omega_1 + O(3^9)\omega_2 + (430\cdot 3 + O(3^9))\omega_3\\
\xi_2 &= O(3^9)\omega_1 + (1+O(3^9))\omega_2 + (569\cdot 3^2 + O(3^9))\omega_3
\end{aligned}$$

give a basis for the regular 1-forms annihilating rational points. Indeed, we can numerically see that the values of the two integrals $\int_{P_1}^{P}\xi_1, \int_{P_1}^{P}\xi_2$ vanish for all $P = P_3, P_4, \ldots, P_8$. The code for this example can be found in the file `./examples/bps.m` in [BT].

6.2. **The modular curve $X_0(44)$.**

We consider the genus 4 curve $X = X_0(44)$. We work with the plane model found by Yang [Yan06]:

$$Q(x, y) = y^5 + 12x^2y^3 - 14x^2y^2 + (13x^4 + 6x^2)y - (11x^6 + 6x^4 + x^2) = 0.$$

We have

$$W^0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{x} & 0 \\ \frac{-10x^3}{x^4+6x^2+1} & \frac{-6x^3-13x}{x^4+6x^2+1} & \frac{x^3+12x}{x^4+6x^2+1} & \frac{-x}{x^4+6x^2+1} & \frac{1}{x^5+6x^3+x} \end{bmatrix}.$$

Indeed, this plane model is singular, as we see $W^0 \neq I$. We have

$$r = x(x^4 + 6x^2 + 1)(45753125x^8 + 8440476x^6 + 1340814x^4 + 69756x^2 + 3125)$$

and

$$b^0 = \left[1, y, y^2, \frac{y^3}{x}, \frac{-10x^4 - (6x^4 - 13x^2)y + (x^4 + 12x^2)y^2 - x^2y^3 + 1}{x^5 + 6x^3 + x}\right].$$

We have that (Q, W^0, W^∞) has good reduction at $p = 7$. Let P_1 be the (good) point $(1, 1)$ and consider the unique point P_2 on the smooth model which lies over the singularity $x = 0, y = 0$ of the plane model. At it turns out, at P_2 we have that y^3/x is a local coordinate and the values of the b^0 are $[1, 0, 0, 0, 0]$. Computing 7-adic integrals gives

$$\left(\int_{P_1}^{P_2} \omega_1, \int_{P_1}^{P_2} \omega_2, \int_{P_1}^{P_2} \omega_3, \int_{P_1}^{P_2} \omega_4\right) = (O(7^9), O(7^9), O(7^9), O(7^9)),$$

which seems to suggest that $[(P_2) - (P_1)]$ is a torsion point in the Jacobian of X. A computation in Magma verifies that $15[(P_2) - (P_1)] = 0$. The code for this example can be found in the file `./examples/X0_44.m` in [BT].

6.3. **A superelliptic genus 4 curve.**

We consider the superelliptic genus 4 curve $X/\mathbf{Q}$ given by the plane model

$$Q(x, y) = y^3 - (x^5 - 2x^4 - 2x^3 - 2x^2 - 3x) = 0.$$

Using the `Magma` intrinsic `RankBounds`, which is based on [PS97] and implemented by Creutz, we find that the Mordell-Weil rank of its Jacobian is 1. A search yields the rational points

$$P_1 = (1, -2), P_2 = (0, 0), P_3 = (-1, 0), P_4 = (3, 0), P_5 = \infty.$$

We have $b^0 = [1, y, y^2]$ and $r = x^5 - 2x^4 - 2x^3 - 2x^2 - 3x$. A basis for the regular 1-forms on X is given by

$$\omega_1 = \frac{ydx}{r}, \quad \omega_2 = \frac{xydx}{r}, \quad \omega_3 = \frac{x^2ydx}{r}, \quad \omega_4 = \frac{y^2dx}{r}.$$

Now we take $p = 7$ and compute

$$\int_{P_1}^{P_2} \omega_1 = 12586493 \cdot 7 + O(7^{10}).$$

Since this integral does not vanish, $[(P_2) - (P_1)]$ is non-torsion in the Jacobian.

The space of annihilating regular 1-forms is 3-dimensional, and a basis is given by

$$\begin{aligned}\xi_1 &= (1+O(7^{10}))\omega_1 + O(7^{10})\omega_2 + O(7^{10})\omega_3 - (139167240 + O(7^{10}))\omega_4\\ \xi_2 &= O(7^{10})\omega_1 + (1+O(7^{10}))\omega_2 + O(7^{10})\omega_3 + (93159229 + O(7^{10}))\omega_4\\ \xi_3 &= O(7^{10})\omega_1 + O(7^{10})\omega_2 + (1+O(7^{10}))\omega_3 + (8834289 + O(7^{10}))\omega_4.\end{aligned}$$

Indeed, we can numerically see that the values of the 3 integrals $\int_{P_1}^{P}\xi_1, \int_{P_1}^{P}\xi_2, \int_{P_1}^{P}\xi_3$ vanish for $P = P_3, P_4, P_5$. The code for this example can be found in the file `./examples/C35.m` in [BT].

6.4. **A curve of genus 55.** As discussed in Section 5.2, to compute Coleman integrals using the other leading approach, there are challenges to working in the Jacobian of the curve in the case of large genus. Here we present some timings indicating the feasibility of our algorithm. The computations in this subsection were carried out on a single core of a 28-core 2.2 GHz Intel Xeon server with 256GB RAM.

Here we consider the genus 55 curve X with plane model given by $Q(x, y) = 0$ below:

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

This example was constructed using the `Magma` intrinsic `RandomPlaneCurve`, with the call

```
> P<x,y,z>:=ProjectiveSpace(Rationals(),2);
> RandomPlaneCurve(12,[0],P:RandomBound:=1);
```

producing a smooth plane curve of degree 12 and coefficients randomly selected from $\{-1, 0, 1\}$. We generated a number of such curves and considered a selection that had at least 3 rational points. We present one illustrative example here.

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 $H^1_{\mathrm{rig}}(X \otimes \mathbf{Q}_p)$ constructed as in Definition 2.16 with $N = 5$ as our precision. We find that

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

and we deduce that the Jacobian of X has positive rank.

The computation of `coleman_data` took 79685 s, after which the call to `coleman_integrals_on_basis` took 39 s.

The code for this example can be found in the file `./examples/g55.m` in [BT].

Further examples illustrating how to call and use the code are available in the file `examples.pdf` in [BT].

Acknowledgements

We would like to thank Amnon Besser, Netan Dogra, Alan Lauder and Steffen Müller for helpful discussions, as well as the anonymous referees for their valuable comments on an earlier version of of this manuscript. Balakrishnan is supported in part by NSF grant DMS-1702196, the Clare Boothe Luce Professorship (Henry Luce Foundation), and Simons Foundation grant #550023. Tuitman is a Postdoctoral Researcher of the Fund for Scientific Research FWO - Vlaanderen.

References

[Bal13] J. S. Balakrishnan, *Iterated Coleman integration for hyperelliptic curves*, ANTS-X: Proceedings of the Tenth Algorithmic Number Theory Symposium (E. W. Howe and K. S. Kedlaya, eds.), Open Book Series, vol. 1, Mathematical Sciences Publishers, 2013, pp. 41–61. ↑1.

[Bal15] ———, *Coleman integration for even-degree models of hyperelliptic curves*, LMS J. Comput. Math. **18** (2015), no. 1, 258–265. MR 3349319 ↑1.

[Bau16] Jens-Dietrich Bauch, *Computation of integral bases*, J. Number Theory **165** (2016), 382–407. ↑2.

[BBK10] J. S. Balakrishnan, R. W. Bradshaw, and K. S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic Number Theory (G. Hanrot, F. Morain, and E. Thomé, eds.), Lecture Notes in Computer Science, vol. 6197, Springer, 2010, pp. 16–31. ↑1, 7, 8.

[BC94] Francesco Baldassarri and Bruno Chiarellotto, *Algebraic versus rigid cohomology with logarithmic coefficients*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 11–50. MR 1307391 (96f:14024) ↑4.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1 484 478 ↑1.

[BdJ08] A. Besser and R. de Jeu, $\mathrm{Li}^{(p)}$*-service? An algorithm for computing p-adic polylogarithms*, Math. Comp. **77** (2008), no. 262, 1105–1134. ↑1.

[BPS16] N. Bruin, B. Poonen, and M. Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum Math. Sigma **4** (2016), e6, 80. ↑14.

[BT] J. S. Balakrishnan and J. Tuitman, *Magma code*, https://github.com/jtuitman/Coleman. ↑1, 2, 15, 16, 17.

[CdS88] R. F. Coleman and E. de Shalit, *p-adic regulators on curves and special values of p-adic L-functions*, Invent. Math. **93** (1988), no. 2, 239–266. ↑1, 5.

[CG89] R. F. Coleman and B. H. Gross, *p-adic heights on curves*, Algebraic Number Theory – in honor of K. Iwasawa, Advanced Studies in Pure Mathematics, vol. 17, 1989, pp. 73–81. ↑1.

[Col82] R. F. Coleman, *Dilogarithms, regulators and p-adic L-functions*, Invent. Math. **69** (1982), no. 2, 171–208. ↑1.

[Col85a] ———, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. ↑1.

[Col85b] ———, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168. ↑1, 5.

[FvdP04] J. Fresnel and M. van der Put, *Rigid analytic geometry and its applications*, Progress in Mathematics, vol. 218, Birkhäuser Boston Inc., Boston, MA, 2004. ↑3.

[Hes02] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445. ↑2.

[Ked01] K. S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), 323–338, erratum *ibid.* **18** (2003), 417–418. ↑1.

[Kim09] M. Kim, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), no. 1, 89–133. ↑1.

[PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. ↑16.

[Tui16] Jan Tuitman, *Counting points on curves using a map to* $\mathbf{P}^1$, Math. Comp. **85** (2016), no. 298, 961–981. ↑1, 2, 4, 5, 9.

[Tui17] J. Tuitman, *Counting points on curves using a map to* $\mathbf{P}^1$*, II*, Finite Fields Appl. **45** (2017), 301–322. ↑1, 2, 3, 4, 5, 6, 9, 10, 11, 12, 13, 14.

[Yan06] Y. Yang, *Defining equations of modular curves*, Adv. Math. **204** (2006), no. 2, 481–508. ↑16.

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

E-mail address: jbala@bu.edu

Jan Tuitman, KU Leuven, Departement Wiskunde, Celestijnenlaan 200B, 3001 Leuven, Belgium

E-mail address: jan.tuitman@kuleuven.be