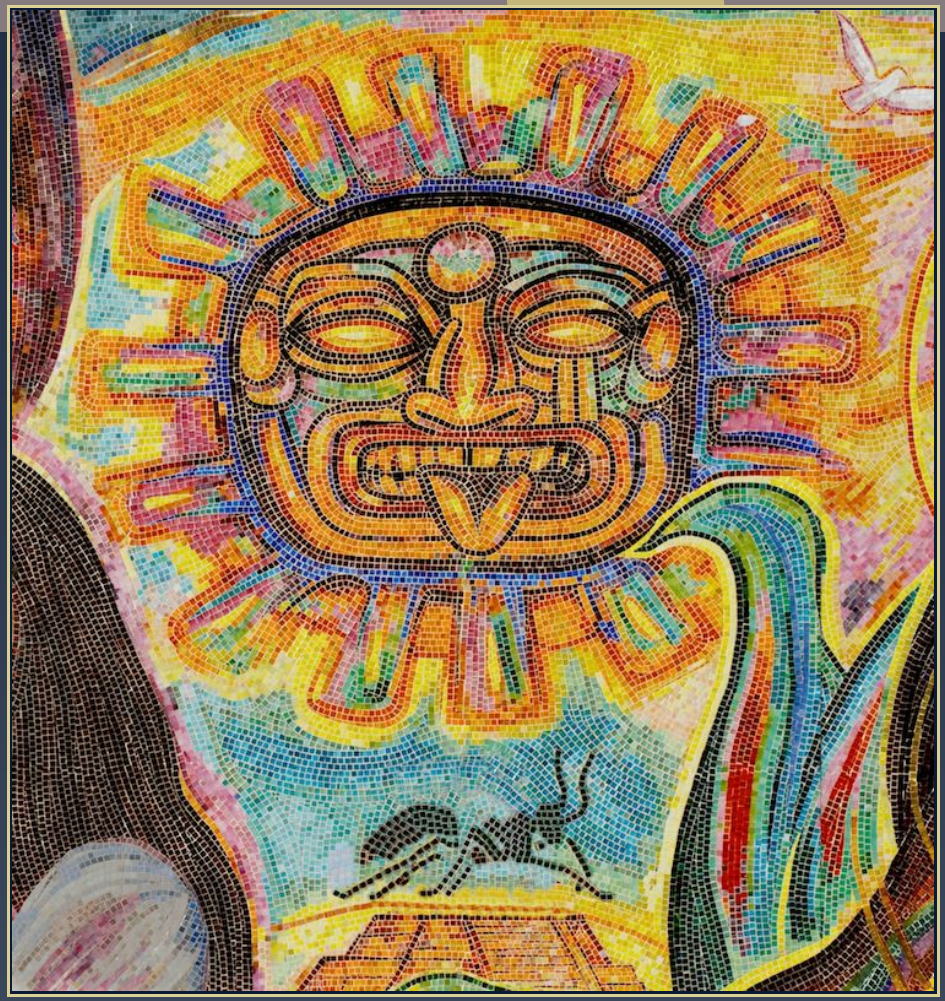
THE OPEN BOOK SERIES 1

# ANTS X
## Proceedings of the Tenth Algorithmic Number Theory Symposium

### Iterated Coleman integration for hyperelliptic curves

Jennifer S. Balakrishnan



msp

THE OPEN BOOK SERIES **1** (2013)
**Tenth Algorithmic Number Theory Symposium**
dx.doi.org/10.2140/obs.2013.1.41

msp

# Iterated Coleman integration for hyperelliptic curves

Jennifer S. Balakrishnan

The Coleman integral is a $p$-adic line integral. Double Coleman integrals on elliptic curves appear in Kim's nonabelian Chabauty method, the first numerical examples of which were given by the author, Kedlaya, and Kim. This paper describes the algorithms used to produce those examples, as well as techniques to compute higher iterated integrals on hyperelliptic curves, building on previous joint work with Bradshaw and Kedlaya.

## 1. Introduction

In a series of papers in the 1980s, Coleman gave a $p$-adic theory of integration on the projective line [8], then on curves and abelian varieties [9; 7]. This integration theory relies on locally defined antiderivatives that are extended analytically by the principle of Frobenius equivariance. In joint work with Bradshaw and Kedlaya [1], we made this construction explicit and gave algorithms to compute single Coleman integrals for hyperelliptic curves.

Having algorithms to compute Coleman integrals allows one to compute $p$-adic regulators in $K$-theory [8; 7], carry out the method of Chabauty-Coleman for finding rational points on higher genus curves [15], and utilize Kim's nonabelian analogue of the Chabauty method [14].

Kim's method, in the case of rank-1 elliptic curves, allows one to find integral points via the computation of double Coleman integrals. Indeed, Coleman's theory of integration is not limited to single integrals; it gives rise to an entire class of

*MSC2010*: primary 11S80; secondary 11Y35, 11Y50.
*Keywords*: Coleman integration, $p$-adic integration, iterated Coleman integration, hyperelliptic curves, nonabelian Chabauty, integral points.

locally analytic functions, the *Coleman functions*, on which antidifferentiation is well-defined. In other words, one can define iterated $p$-adic integrals [4; 8]

$$\int_P^Q \xi_n \cdots \xi_1$$

which behave formally like iterated path integrals

$$\int_0^1 \int_0^{t_1} \cdots \int_0^{t_{n-1}} f_n(t_n) \cdots f_1(t_1)\, dt_n \cdots dt_1.$$

Let us fix some notation. Let $C$ be a genus-$g$ hyperelliptic curve over an unramified extension $K$ of $\mathbb{Q}_p$ having good reduction. Let $k = \mathbb{F}_q$ denote its residue field, where $q = p^m$. We will assume that $C$ is given by a model of the form $y^2 = f(x)$, where $f$ is a monic separable polynomial with $\deg f = 2g + 1$.

Our methods for computing iterated integrals are similar in spirit to those detailed in [1]. We begin with algorithms for tiny iterated integrals, use Frobenius equivariance to write down a linear system yielding the values of integrals between points in different residue disks, and, if needed, use basic properties of integration to correct endpoints. We begin with some basic properties of iterated path integrals.

## 2. Iterated path integrals

We follow the convention of Kim [14] and define our integrals as follows:

$$\int_P^Q \xi_1 \xi_2 \cdots \xi_{n-1} \xi_n := \int_P^Q \xi_1(R_1) \int_P^{R_1} \xi_2(R_2) \cdots \int_P^{R_{n-2}} \xi_{n-1}(R_{n-1}) \int_P^{R_{n-1}} \xi_n,$$

for a collection of dummy parameters $R_1, \ldots, R_{n-1}$ and 1-forms $\xi_1, \ldots, \xi_n$.

We begin by recalling some key formal properties satisfied by iterated path integrals [6].

**Proposition 2.1.** *Let $\xi_1, \ldots, \xi_n$ be 1-forms, holomorphic at points $P, Q$ on $C$. Then*:

(1) $\int_P^P \xi_1 \xi_2 \cdots \xi_n = 0$,

(2) $\sum_{\text{all permutations } \sigma} \int_P^Q \omega_{\sigma(i_1)} \omega_{\sigma(i_2)} \cdots \omega_{\sigma(i_n)} = \prod_{j=1}^n \int_P^Q \omega_{i_j}$,

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

As an easy corollary of Proposition 2.1(2), we have:

**Corollary 2.2.** *For a 1-form $\omega_i$ and points $P, Q$ as before*,

$$\int_P^Q \omega_i\, \omega_i \cdots \omega_i = \frac{1}{n!} \left( \int_P^Q \omega_i \right)^n.$$

When possible, we will use this to write an iterated integral in terms of a single integral.

## 3. $p$-adic cohomology

We briefly recall some $p$-adic cohomology from [12], necessary for formulating the integration algorithms.

Let $C'$ be the affine curve obtained by deleting the Weierstrass points from $C$, and let $A = K[x, y, z]/(y^2 - f(x), yz - 1)$ be the coordinate ring of $C'$. Let $A^\dagger$ denote the Monsky-Washnitzer weak completion of $A$; it is the ring consisting of infinite sums of the form

$$\sum_{i=-\infty}^{\infty} \frac{B_i(x)}{y^i}, \quad B_i(x) \in K[x], \quad \deg B_i \leq 2g,$$

further subject to the condition that $v_p(B_i(x))$ grows faster than a linear function of $i$ as $i \to \pm\infty$. We make a ring out of these using the relation $y^2 = f(x)$.

These functions are holomorphic on the space over which we integrate, so we consider odd 1-forms written as

$$\omega = g(x, y)\,\frac{dx}{2y}, \quad g(x, y) \in A^\dagger.$$

Any such differential can be written as

$$\omega = dF + c_0\omega_0 + \cdots + c_{2g-1}\omega_{2g-1}, \tag{1}$$

with $F \in A^\dagger, c_i \in K$, and

$$\omega_i = x^i\,\frac{dx}{2y} \quad (i = 0, \ldots, 2g-1).$$

Namely, the set of differentials $\{\omega_i\}_{i=0}^{2g-1}$ forms a basis of the odd part of the de Rham cohomology of $A^\dagger$, which we denote as $H^1_{dR}(C')^-$.

One computes the $p$-power Frobenius action $\phi^*$ on $H^1_{dR}(C')^-$ as follows:

- Let $\phi_K$ denote the unique automorphism lifting Frobenius from $\mathbb{F}_q$ to $K$. Extend $\phi_K$ to $A^\dagger$ by setting

$$\begin{aligned}
\phi(x) &= x^p, \\
\phi(y) &= y^p\left(1 + \frac{\phi(f)(x^p) - f(x)^p}{f(x)^p}\right)^{\frac{1}{2}} \\
&= y^p \sum_{i=0}^{\infty} \binom{\frac{1}{2}}{i} \frac{(\phi(f)(x^p) - f(x)^p)^i}{y^{2pi}}.
\end{aligned}$$

- Use the relations

$$y^2 = f(x),$$
$$d(x^i y^j) = \left(2ix^{i-1}y^{j+1} + jx^i f'(x)y^{j-1}\right)\frac{dx}{2y}$$

to reduce large powers of $x$ and large (in absolute value) powers of $y$ to write $\phi^*(\omega)$ in the form (1).

This reduction process is known as *Kedlaya's algorithm* [12], and we will repeatedly use this algorithm to reduce iterated integrals involving $\omega \in A^\dagger \frac{dx}{2y}$ to iterated integrals in terms of basis elements $\omega_i$.

## 4. Integrals: lemmas

Recall that we use Kedlaya's algorithm to compute single Coleman integrals as follows:

**Algorithm 4.1** (Coleman integration in non-Weierstrass disks [1]).

*Input*: The basis differentials $(\omega_i)_{i=0}^{2g-1}$, points $P, Q \in C(\mathbb{C}_p)$ in non-Weierstrass residue disks, and a positive integer $m$ such that the residue fields of $P, Q$ are contained in $\mathbb{F}_{p^m}$.

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

1. Calculate the action of the $m$-th power of Frobenius on each basis element (see Remark 4.2):
$$(\phi^m)^*\omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j.$$
2. By a change of variables, we obtain
$$\sum_{j=0}^{2g-1}(M-I)_{ij}\int_P^Q \omega_j = h_i(P) - h_i(Q) - \int_P^{\phi^m(P)} \omega_i - \int_{\phi^m(Q)}^Q \omega_i \qquad (2)$$
(the *fundamental linear system*). Since the eigenvalues of the matrix $M$ are algebraic integers of $\mathbb{C}$-norm $p^{m/2} \neq 1$ (see [12, §2]), the matrix $M - I$ is invertible, and we may solve (2) to obtain the integrals $\int_P^Q \omega_i$.

**Remark 4.2.** To compute the action of $\phi^m$, first carry out Kedlaya's algorithm to write
$$\phi^*\omega_i = dg_i + \sum_{j=0}^{2g-1} B_{ij}\omega_j.$$

If we view $h, g$ as column vectors and $M, B$ as matrices, induction on $m$ shows that

$$h = \phi^{m-1}(g) + B\phi^{m-2}(g) + \cdots + B\phi_K(B)\cdots\phi_K^{m-2}(B)g,$$
$$M = B\phi_K(B)\cdots\phi_K^{m-1}(B).$$

Note, however, that when points $P, Q \in C(\mathbb{C}_p)$ are in the same residue disk, the "tiny" Coleman integral between them can be computed using a local parametrization, just as in the case of a real-valued line integral. This is also true when the integrals are iterated (see Section 5).

However, to compute general iterated integrals, we will need to employ the analogue of "additivity in endpoints" to link integrals between different residue disks. First, let us consider the case where we are breaking up the path by one point.

**Lemma 4.3.** *Let $P, P', Q$ be points on $C$ such that a path is to be taken from $P$ to $Q$ via $P'$. Let $\xi_1, \ldots, \xi_n$ be a collection of 1-forms holomorphic at the points $P, P', Q$. Then*

$$\int_P^Q \xi_1 \cdots \xi_n = \sum_{i=0}^{n} \int_{P'}^{Q} \xi_1 \cdots \xi_i \int_P^{P'} \xi_{i+1} \cdots \xi_n.$$

*Proof.* We proceed by induction. The case $n = 1$ is clear. Let us suppose the statement holds for $n = k$. Then

$$\begin{aligned}\int_P^Q \xi_1 \cdots \xi_{k+1} &= \left(\int_P^Q \xi_1 \cdots \xi_k\right)(R) \int_P^R \xi_{k+1} \\ &= \left(\sum_{i=0}^{k} \int_{P'}^{Q} \xi_1 \cdots \xi_i \int_P^{P'} \xi_{i+1} \cdots \xi_k\right)(R) \int_P^R \xi_{k+1}.\end{aligned}$$

Observe that the summand with $i = k$ can be rewritten as

$$\left(\int_{P'}^Q \xi_1 \cdots \xi_k\right)(R) \int_P^R \xi_{k+1} = \left(\int_{P'}^Q \xi_1 \cdots \xi_k\right)(R) \left(\int_P^{P'} \xi_{k+1} + \int_{P'}^R \xi_{k+1}\right),$$

and that further, the terms with $i < k$ give us

$$\sum_{i=0}^{k-1} \int_{P'}^{Q} \xi_1 \cdots \xi_i \int_P^{P'} \xi_{i+1} \cdots \xi_{k+1}.$$

Thus we have

$$\begin{aligned}\int_P^Q \xi_1\cdots\xi_{k+1} &= \sum_{i=0}^{k-1}\int_{P'}^{Q}\xi_1\cdots\xi_i\int_P^{P'}\xi_{i+1}\cdots\xi_{k+1}\\ &\qquad + \Big(\int_{P'}^{Q}\xi_1\cdots\xi_k\Big)\Big(\int_P^{P'}\xi_{k+1}\Big) + \int_{P'}^{Q}\xi_1\cdots\xi_{k+1}\\ &= \sum_{i=0}^{k+1}\int_{P'}^{Q}\xi_1\cdots\xi_i\int_P^{P'}\xi_{i+1}\cdots\xi_{k+1},\end{aligned}$$

as desired. □

Applying Lemma 4.3 twice, we obtain a link between different residue disks:

**Lemma 4.4** (Link lemma). *Let points $P, P', Q', Q$ be on $C$ such that a path is to be taken from $P$ to $P'$ to $Q'$ to $Q$. Let $\xi_1,\dots,\xi_n$ be a collection of 1-forms holomorphic at the points $P, P', Q, Q'$. Then*

$$\int_P^Q \xi_1\cdots\xi_n = \sum_{i=0}^{n}\int_{Q'}^{Q}\xi_1\cdots\xi_i\Big(\sum_{j=i}^{n}\int_{P'}^{Q'}\xi_{i+1}\cdots\xi_j\int_P^{P'}\xi_{j+1}\cdots\xi_n\Big).$$

Below we record a specific case of the link lemma, which we shall use throughout this paper.

**Example 4.5** (Link lemma for double integrals). Suppose we have two differentials $\xi_0, \xi_1$. Then

$$\int_P^Q \xi_0\xi_1 = \int_P^{P'}\xi_0\xi_1 + \int_{P'}^{Q'}\xi_0\xi_1 + \int_{Q'}^{Q}\xi_0\xi_1 + \int_P^{P'}\xi_1\int_{P'}^{Q}\xi_0 + \int_{P'}^{Q'}\xi_1\int_{Q'}^{Q}\xi_0.$$

## 5. Tiny iterated integrals

We begin with an algorithm to compute tiny iterated integrals.

**Algorithm 5.1** (Tiny iterated integrals).

*Input*: Points $P, Q \in C(\mathbb{C}_p)$ in the same residue disk (neither equal to the point at infinity) and differentials $\xi_1,\dots,\xi_n$ without poles in the disk of $P$.

*Output*: The integral $\int_P^Q \xi_1\xi_2\cdots\xi_n$.

1. Compute a parametrization $\big(x(t), y(t)\big)$ at $P$ in terms of a local coordinate $t$.
2. For each $k$, write $\xi_k(x, y)$ in terms of $t$: $\xi_k(t) := \xi_k\big(x(t), y(t)\big)$.
3. Let $I_{n+1}(t) := 1$.

4. Compute, for $k = n, \dots, 2$, in descending order,

$$I_k(t) = \int_P^{R_{k-1}} \xi_k I_{k+1} = \int_0^{t(R_{k-1})} \xi_k(u) I_{k+1}(u),$$

with $R_{k-1}$ in the disk of $P$.

5. Upon computing $I_2(t)$, we arrive at the desired integral:

$$\int_P^Q \xi_1 \xi_2 \cdots \xi_n = I_1(t) = \int_0^{t(Q)} \xi_1(u) I_2(u).$$

We show how we carry out Algorithm 5.1 for double integrals on an elliptic curve.

**Example 5.2** (A tiny double integral). Let $C$ be the elliptic curve

$$y^2 = x(x-1)(x+9),$$

let $p = 7$, and consider the points $P = (9, 36)$, $Q = \phi(P)$, and

$$R = \big(a + x(P), \sqrt{f(a + x(P))}\big),$$

so that $R$ is in the same disk as $P$ and $Q$. Furthermore, let $\omega_0 = \frac{dx}{2y}$ and $\omega_1 = \frac{x\,dx}{2y}$. We compute the double integral $\int_P^Q \omega_0 \omega_1$.

First compute the local coordinates at $P$:

$$x(t) = 9 + t + O(t^{20})$$
$$y(t) = 36 + \frac{21}{4}t + \frac{119}{1152}t^2 - \frac{65}{55296}t^3 + \frac{2219}{95551488}t^4 - \frac{7}{509607936}t^5 + O(t^6).$$

Then setting $I_2 := \int x \frac{dx}{2y}$, and making it a definite integral, we have

$$\begin{aligned} I_2|_P^R &= \int_P^R x \frac{dx}{2y} \\ &= \int_0^a x(t) \frac{dx(t)}{2y(t)} \\ &= \frac{1}{8}a - \frac{5}{2304}a^2 + \frac{91}{995328}a^3 - \frac{1121}{191102976}a^4 + \frac{22129}{45864714240}a^5 \\ &\qquad - \frac{360185}{7925422620672}a^6 + \frac{36737231}{7988826001637376}a^7 + O(a^8), \end{aligned}$$

from which we arrive at

$$\begin{aligned} I &= \int_0^{x(Q)-x(P)} I_2(a) \frac{dx(R(a))}{2y(R(a))} \\ &= 4 \cdot 7^2 + 5 \cdot 7^3 + 2 \cdot 7^5 + 4 \cdot 7^6 + 2 \cdot 7^7 + O(7^8). \end{aligned}$$

## 6. Iterated integrals: linear system

As in the case of computing single integrals, to compute general iterated Coleman integrals, we use Kedlaya's algorithm to calculate the action of Frobenius on de Rham cohomology. This gives us a linear system that allows us to solve for all $(2g)^n$ $n$-fold iterated integrals on basis differentials.

**Theorem 6.1.** *Let $P, Q \in C(\mathbb{C}_p)$ be non-Weierstrass points such that the residue fields of $P, Q$ are contained in $\mathbb{F}_{p^m}$. Let $M$ be the matrix of the action of the $m$-th power of Frobenius on the basis differentials $\omega_0, \dots, \omega_{2g-1}$. For constants $c_{i_0,\dots,i_{n-1}}$ computable in terms of $(n-1)$-fold iterated integrals and $n$-fold tiny iterated integrals, the $n$-fold iterated Coleman integrals on basis differentials between $P, Q$ can be computed via a linear system of the form*

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_{i_0} \cdots \omega_{i_{n-1}} \\ \vdots \end{pmatrix} = \left(I_{(2g)^n \times (2g)^n} - (M^t)^{\otimes n}\right)^{-1} \begin{pmatrix} \vdots \\ c_{i_0 \cdots i_{n-1}} \\ \vdots \end{pmatrix}.$$

*Proof.* By the link lemma (Lemma 4.4), we can reduce to the case where both $P$ and $Q$ are Teichmüller points (points fixed by some power of $\phi$). Then we have

$$\begin{aligned} \int_P^Q \omega_{i_i} \cdots \omega_{i_n} &= \int_{\phi^m(P)}^{\phi^m(Q)} \omega_{i_i} \cdots \omega_{i_n} \\ &= \int_P^Q (\phi^m)^*(\omega_{i_i} \cdots \omega_{i_n}) \\ &= \int_P^Q (\phi^m)^*(\omega_{i_i}) \cdots (\phi^m)^*(\omega_{i_n}). \end{aligned} \tag{3}$$

Recall that given $\omega_0, \dots, \omega_{2g-1}$ a basis for $H^1_{dR}(C')^-$, we have

$$(\phi^m)^* \omega_{i_\ell} = df_{i_\ell} + \sum_{j=0}^{2g-1} M_{i_\ell j} \omega_j.$$

Substituting this expression in for each factor of (3) and expanding yields the linear system. □

To illustrate our methods, in the next section, we present a more explicit version of this theorem, accompanied by algorithms, in the case of double integrals. We show how these are used in Kim's nonabelian Chabauty method in Section 8.

## 7. Explicit double integrals

**7A.** ***The linear system for double integrals between Teichmüller points.*** In this subsection, we make explicit one aspect of Theorem 6.1: We give an algorithm to compute double integrals between Teichmüller points.

**Algorithm 7.1** (Double Coleman integration between Teichmüller points).

*Input*: The basis differentials $(\omega_i)_{i=0}^{2g-1}$, Teichmüller points $P, Q \in C(\mathbb{C}_p)$ in non-Weierstrass residue disks, and a positive integer $m$ such that the residue fields of $P, Q$ are contained in $\mathbb{F}_{p^m}$.

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

1. Calculate the action of the $m$-th power of Frobenius on each basis element:
$$(\phi^m)^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j.$$
2. Use Algorithm 4.1 to compute the single Coleman integrals $\int_P^Q \omega_j$ on all basis differentials.
3. Use Step 2 and linearity to recover the other single Coleman integrals:
$$\int_P^Q df_i\, f_k, \int_P^Q \sum_{j=0}^{2g-1} M_{ij}\omega_j\, f_k$$
for each $i, k$.
4. Use the results of the above two steps to write down, for each $i, k$, the constant
$$\begin{aligned} c_{ik} = \int_P^Q & df_i(R)(f_k(R)) - f_k(P)\big(f_i(Q) - f_i(P)\big) \\ & + \int_P^Q \sum_{j=0}^{2g-1} M_{ij}\omega_j(R)\big(f_k(R) - f_k(P)\big) \\ & + f_i(Q)\int_P^Q \sum_{j=0}^{2g-1} M_{kj}\omega_j - \int_P^Q f_i(R)\Big(\sum_{j=0}^{2g-1} M_{kj}\omega_j(R)\Big). \end{aligned}$$
5. Recover the double integrals (see Remark 7.2 below) via the linear system
$$\begin{pmatrix} \int_P^Q \omega_0\omega_0 \\ \int_P^Q \omega_0\omega_1 \\ \vdots \\ \int_P^Q \omega_{2g-1}\omega_{2g-1} \end{pmatrix} = (I_{4g^2\times 4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} c_{00} \\ c_{01} \\ \vdots \\ c_{2g-1,2g-1} \end{pmatrix}.$$

**Remark 7.2.** We obtain the linear system in the following manner. Since $P, Q$ are Teichmüller, we have

$$\int_P^Q \omega_i\,\omega_k = \int_{\phi^m(P)}^{\phi^m(Q)} \omega_i\,\omega_k = \int_P^Q (\phi^m)^*(\omega_i\,\omega_k). \tag{4}$$

We begin by expanding the right side of (4).

Recall that given $\omega_0, \ldots, \omega_{2g-1}$ a basis for $H^1_{dR}(C')^-$, we have

$$(\phi^m)^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j.$$

Thus we have

$$\begin{aligned}
&\int_P^Q (\phi^m)^*(\omega_i\,\omega_k)\\
&= \int_P^Q (\phi^m)^*(\omega_i)(\phi^m)^*(\omega_k)\\
&= \int_P^Q \Big(df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j\Big)\Big(df_k + \sum_{j=0}^{2g-1} M_{kj}\omega_j\Big)\\
&= \int_P^Q df_i\,df_k + \Big(\sum_{j=0}^{2g-1} M_{ij}\omega_j\Big)df_k + df_i \sum_{j=0}^{2g-1} M_{kj}\omega_j + \sum_{j=0}^{2g-1} M_{ij}\omega_j \sum_{j=0}^{2g-1} M_{kj}\omega_j.
\end{aligned}$$

We expand the first three quantities separately. First, we have

$$\begin{aligned}
\int_P^Q df_i\,df_k &= \int_P^Q df_i(R) \int_P^R df_k\\
&= \int_P^Q df_i(R)\big(f_k(R) - f_k(P)\big)\\
&= \int_P^Q df_i(R)(f_k(R)) - f_k(P)\int_P^Q df_i(R)\\
&= \int_P^Q df_i(R)(f_k(R)) - f_k(P)\big(f_i(Q) - f_i(P)\big).
\end{aligned}$$

Next, we have

$$\begin{aligned}
\int_P^Q \Big(\sum_{j=0}^{2g-1} M_{ij}\omega_j\Big)df_k &= \int_P^Q \sum_{j=0}^{2g-1} M_{ij}\omega_j(R) \int_P^R df_k\\
&= \int_P^Q \sum_{j=0}^{2g-1} M_{ij}\omega_j(R)\big(f_k(R) - f_k(P)\big).
\end{aligned}$$

The third term (via integration by parts) is

$$\begin{aligned}\int_P^Q df_i\Big(\sum_{j=0}^{2g-1} M_{kj}\omega_j\Big) &= \int_P^Q df_i(R)\int_P^R\Big(\sum_{j=0}^{2g-1} M_{kj}\omega_j\Big)\\ &= f_i(R)\int_P^R\Big(\sum_{j=0}^{2g-1} M_{kj}\omega_j\Big)\Big|_{R=P}^{R=Q} - \int_P^Q f_i(R)\Big(\sum_{j=0}^{2g-1} M_{kj}\omega_j(R)\Big)\\ &= f_i(Q)\int_P^Q \sum_{j=0}^{2g-1} M_{kj}\omega_j - \int_P^Q f_i(R)\Big(\sum_{j=0}^{2g-1} M_{kj}\omega_j(R)\Big).\end{aligned}$$

Denote the sum of these terms by $c_{ik}$; in other words,

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

Then rearranging terms, our linear system reads

$$\begin{pmatrix} \int_P^Q \omega_0\omega_0 \\ \int_P^Q \omega_0\omega_1 \\ \vdots \\ \int_P^Q \omega_{2g-1}\omega_{2g-1}\end{pmatrix} = \big(I_{4g^2\times 4g^2} - (M^t)^{\otimes 2}\big)^{-1}\begin{pmatrix} c_{00} \\ c_{01} \\ \vdots \\ c_{2g-1,2g-1}\end{pmatrix}.$$

**7B.** ***Linking double integrals.*** Let $P'$ and $Q'$ be in the disks of $P$ and $Q$, respectively. Using the link lemma for double integrals (Example 4.5), we may link double integrals between different residue disks:

$$\begin{aligned}\int_P^Q \omega_i\,\omega_k &= \int_P^{P'} \omega_i\,\omega_k + \int_{P'}^{Q'} \omega_i\,\omega_k + \int_{Q'}^{Q} \omega_i\,\omega_k + \int_P^{P'} \omega_k \int_{P'}^{Q} \omega_i + \int_{P'}^{Q'} \omega_k \int_{Q'}^{Q} \omega_i.\end{aligned}$$

**Algorithm 7.3** (Double Coleman integration using intermediary Teichmüller points).

*Input*: The basis differentials $(\omega_i)_{i=0}^{2g-1}$, points $P, Q \in C(\mathbb{C}_p)$ in non-Weierstrass residue disks.

*Output*: The double integrals

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

1. Compute Teichmüller points $P', Q'$ in the disks of $P, Q$, respectively.
2. Use Algorithm 4.1 to compute the single integrals $\int_P^Q \omega_i, \int_{P'}^P \omega_i, \int_Q^{Q'} \omega_i$ for all $i$.
3. Use Algorithm 5.1 to compute the tiny double integrals $\int_{P'}^P \omega_i\,\omega_k, \int_{Q'}^Q \omega_i\,\omega_k$.
4. Use Algorithm 7.1 to compute the double integrals $\left\{\int_{P'}^{Q'} \omega_i\,\omega_j\right\}_{i,j=0}^{2g-1}$.
5. Correct endpoints using

$$\begin{aligned}\int_P^Q \omega_i\,\omega_k &= \int_P^{P'} \omega_i\,\omega_k + \int_{P'}^{Q'} \omega_i\,\omega_k + \int_{Q'}^{Q} \omega_i\,\omega_k + \int_P^{P'} \omega_k \int_{P'}^{Q} \omega_i + \int_{P'}^{Q'} \omega_k \int_{Q'}^{Q} \omega_i.\end{aligned}$$

**7C.*Without Teichmüller points.*** Alternatively, instead of finding Teichmüller points and correcting endpoints, we can directly compute double integrals using a slightly different linear system. Indeed, using the link lemma for double integrals, we take $\phi(P)$ and $\phi(Q)$ to be the points in the disks of $P$ and $Q$, respectively, which gives

$$\begin{aligned}\int_P^Q \omega_i\,\omega_k = \int_P^{\phi(P)} \omega_i\,\omega_k + \int_{\phi(P)}^{\phi(Q)} \omega_i\,\omega_k + \int_{\phi(Q)}^{Q} \omega_i\,\omega_k \\ + \int_P^{\phi(P)} \omega_k \int_{\phi(P)}^{Q} \omega_i + \int_{\phi(P)}^{\phi(Q)} \omega_k \int_{\phi(Q)}^{Q} \omega_i. \quad (5)\end{aligned}$$

To write down a linear system without Teichmüller points, we begin as before, with

$$\int_{\phi(P)}^{\phi(Q)} \omega_i\,\omega_k = \int_P^Q \phi^*(\omega_i\,\omega_k) = c_{ik} + \int_P^Q \left(\sum_{j=0}^{2g-1} A_{ij}\omega_j\right)\left(\sum_{j=0}^{2g-1} A_{kj}\omega_j\right). \quad (6)$$

Putting together (5) and (6), we get

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i\,\omega_k \\ \vdots \end{pmatrix} = \left(I_{4g^2\times 4g^2} - (M^t)^{\otimes 2}\right)^{-1} \cdot \begin{pmatrix} \vdots \\ c_{ik} - \int_{\phi(P)}^P \omega_i\,\omega_k - \left(\int_P^Q \omega_i\right)\left(\int_{\phi(P)}^P \omega_k\right) \\ \quad - \left(\int_Q^{\phi(Q)} \omega_i\right)\left(\int_{\phi(P)}^{\phi(Q)} \omega_k\right) + \int_{\phi(Q)}^Q \omega_i\,\omega_k \\ \vdots \end{pmatrix}. \quad (7)$$

This gives us the following alternative to Algorithm 7.1.

**Algorithm 7.4** (Double Coleman integration).

*Input*: The basis differentials $(\omega_i)_{i=0}^{2g-1}$, points $P, Q \in C(\mathbb{Q}_p)$ in non-Weierstrass residue disks or in Weierstrass disks in the region of convergence.

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

1. Use Algorithm 4.1 to compute the single integrals $\int_P^Q \omega_i, \int_{\phi(P)}^{\phi(Q)} \omega_i$ for all $i$.
2. Use Algorithm 5.1 to compute $\int_{\phi(P)}^P \omega_i\,\omega_k, \int_{\phi(Q)}^Q \omega_i\,\omega_k$ for all $i, k$
3. As in Step 4 of Algorithm 7.1, compute the constants $c_{ik}$ for all $i, k$.
4. Recover the double integrals using the linear system (7).

**Example 7.5.** Let $C$ be the genus-2 curve $y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1$ and let $P = (1, -1)$, $Q = (-1, -1)$ and $p = 7$. We compute double integrals on basis differentials:

$$\begin{aligned}
\textstyle\int_P^Q \omega_0\omega_0 &= 2\cdot 7^2 + 7^3 + 4\cdot 7^4 + O(7^5),\\
\textstyle\int_P^Q \omega_0\omega_1 &= 7^2 + 5\cdot 7^3 + 3\cdot 7^4 + O(7^5),\\
\textstyle\int_P^Q \omega_0\omega_2 &= 4\cdot 7 + 5\cdot 7^2 + 7^3 + O(7^4),\\
\textstyle\int_P^Q \omega_0\omega_3 &= 7 + 5\cdot 7^2 + 3\cdot 7^4 + O(7^5),\\
\textstyle\int_P^Q \omega_1\omega_0 &= 7^2 + 6\cdot 7^3 + 5\cdot 7^4 + O(7^5),\\
\textstyle\int_P^Q \omega_1\omega_1 &= 4\cdot 7^2 + 3\cdot 7^3 + O(7^5),\\
\textstyle\int_P^Q \omega_1\omega_2 &= 5\cdot 7 + 6\cdot 7^2 + 2\cdot 7^3 + 4\cdot 7^4 + O(7^5),\\
\textstyle\int_P^Q \omega_1\omega_3 &= 2 + 3\cdot 7 + 7^2 + 4\cdot 7^3 + O(7^4),\\
\textstyle\int_P^Q \omega_2\omega_0 &= 7^2 + 4\cdot 7^3 + O(7^4),\\
\textstyle\int_P^Q \omega_2\omega_1 &= 4\cdot 7 + 6\cdot 7^2 + 4\cdot 7^3 + 5\cdot 7^4 + O(7^5),\\
\textstyle\int_P^Q \omega_2\omega_2 &= 2 + 5\cdot 7 + 3\cdot 7^2 + O(7^3),
\end{aligned}$$

$$\int_P^Q \omega_2\omega_3 = 5 + 2\cdot 7 + 3\cdot 7^2 + O(7^3),$$
$$\int_P^Q \omega_3\omega_0 = 3\cdot 7 + 2\cdot 7^2 + 5\cdot 7^3 + 5\cdot 7^4 + O(7^5),$$
$$\int_P^Q \omega_3\omega_1 = 5 + 5\cdot 7 + 7^2 + 6\cdot 7^3 + O(7^4),$$
$$\int_P^Q \omega_3\omega_2 = 6 + 7 + 5\cdot 7^2 + O(7^3),$$
$$\int_P^Q \omega_3\omega_3 = 2 + 6\cdot 7 + 5\cdot 7^2 + O(7^3).$$

**Example 7.6.** Using the previous example, we verify the Fubini identity

$$\int_P^Q \omega_j\,\omega_i + \int_P^Q \omega_i\,\omega_j = \left(\int_P^Q \omega_i\right)\left(\int_P^Q \omega_j\right).$$

We have

$$\int_P^Q \omega_0 = 5\cdot 7 + 2\cdot 7^2 + 5\cdot 7^3 + 7^4 + 4\cdot 7^5 + O(7^6),$$
$$\int_P^Q \omega_1 = 6\cdot 7 + 6\cdot 7^2 + 2\cdot 7^3 + 4\cdot 7^4 + 3\cdot 7^5 + O(7^6),$$
$$\int_P^Q \omega_2 = 5 + 5\cdot 7^3 + 6\cdot 7^4 + 2\cdot 7^5 + O(7^6),$$
$$\int_P^Q \omega_3 = 5 + 3\cdot 7 + 4\cdot 7^2 + 3\cdot 7^3 + 6\cdot 7^4 + 2\cdot 7^5 + O(7^6).$$

We see, for example, that

$$\int_P^Q \omega_0\omega_1 + \int_P^Q \omega_1\omega_0 = 2\cdot 7^2 + 4\cdot 7^3 + 2\cdot 7^4 + O(7^5) = \left(\int_P^Q \omega_0\right)\left(\int_P^Q \omega_1\right)$$
$$\int_P^Q \omega_2\omega_3 + \int_P^Q \omega_3\omega_2 = \qquad 4 + 4\cdot 7 + 7^2 + O(7^3) = \left(\int_P^Q \omega_2\right)\left(\int_P^Q \omega_3\right).$$

**7D.** ***Weierstrass points.*** Suppose one of $P$ or $Q$ is a finite Weierstrass point. Then directly using the linear system as above fails, since the $f_i$ have essential singularities at finite Weierstrass points. We remedy this as follows:

**Proposition 7.7.** *Let $Q$ be a non-Weierstrass point, $P$ a finite Weierstrass point, and $S$ be a point in the residue disk of $P$, near the boundary. Then the integral from $P$ to $Q$ can be computed as a sum of integrals*:

$$\int_P^Q \omega_i\,\omega_k = \int_P^S \omega_i\,\omega_k + \int_S^Q \omega_i\,\omega_k + \int_P^S \omega_k \int_S^Q \omega_i\,.$$

*Proof.* This follows from Lemma 4.3 in the case of $n = 2$, where $P' = S$. □

To compute tiny iterated integrals in a Weierstrass disk, we modify Algorithm 5.1 slightly:

**Algorithm 7.8** (Tiny iterated integral in a Weierstrass disk).

*Input*: A Weierstrass point $P$, the degree $d$ of a totally ramified extension, and basis differentials $\omega_i, \omega_j$.

*Output*: The integral

$$\int_P^S \omega_i \omega_j = \int_P^S \omega_i(R) \int_P^R \omega_j = \int_{t=0}^{t=1} \omega_i(R) \int_{u=0}^{u=t} \omega_j.$$

1. Compute local coordinates $(x(u), u)$ at $P$.
2. Let $a = p^{1/d}$. Rescale coordinates so that $y := au, x := x(au)$.
3. Compute $I_2(u) = \int x^j \frac{dx}{2y}$ as a power series in $u$.
4. Compute the appropriate definite integral using the step above:

$$\int_R^S x^j \frac{dx}{2y} = \int_0^t x(au) \frac{a\, du}{u} = I_2(t)$$

   (where $R = (x(t), t)$). Call this definite integral (now a power series in $t$) $I_2$.
5. Now since $R = (x(t), t)$, we have $\int_P^S \omega_i \omega_j = \int_0^1 x(t)^i I_2 \frac{dx(t)}{2t}$.

Suppose $P$ is a finite Weierstrass point. While one could compute the integral $\int_P^Q \omega_i \omega_j$ directly using Algorithm 7.4 for all of the tiny double integrals (and Algorithm 7.8 for the other double integrals), in practice, that approach is expensive, as it requires the computation of several intermediate integrals with Frobenius of points that are defined over ramified extensions. This, in turn, makes the requisite degree $d$ extension for convergence quite large.

Instead, the key idea is to compute a local parametrization at the finite Weierstrass point $P$ and to use this to compute the indefinite integral $\int_P^* \omega_i$. Then to compute integrals involving "boundary points," one can simply evaluate this indefinite integral at the appropriate points, instead of directly computing parametrizations, and thus integrals, over a totally ramified extension of $\mathbb{Q}_p$. This idea is also used to evaluate double integrals involving boundary points.

**Algorithm 7.9** (Intermediary integrals for double integrals with a Weierstrass endpoint).

*Input*: A finite Weierstrass point $P$, a non-Weierstrass point $Q$, the degree $d$ of a totally ramified extension, the desired precision $n$ of $\mathbb{Q}_p$, and basis differentials $\omega_i, \omega_j$.

*Output*: Necessary things for the eventual computation of $\int_P^Q \omega_i \omega_j$.

1. Compute $(x(t), t)$ local coordinates at $P$ to precision $nd$.
2. Let $S = (x(a), a)$, where $a = p^{1/d}$.
3. Compute as a power series in $t$, $I_2(t) = \int x(t)^i \frac{dx(t)}{y(t)}$.

4. Compute the definite integral $\int_P^S \omega_i = I_2(a)$.
5. For all $i < j$, compute the definite integral $\int_P^S \omega_i \omega_j$ via Algorithm 5.1. Keep the intermediary indefinite integral.
6. For all $i = j$, use the fact that $\int_P^S \omega_i \omega_j = \frac{1}{2}\left(\int_P^S \omega_i\right)^2$ to compute the double integral in terms of the single integral.
7. For all $i > j$, use the fact that $\int_P^S \omega_i \omega_j = -\int_P^S \omega_j \omega_i + \int_P^S \omega_i \int_P^S \omega_j$ to compute $\int_P^S \omega_i \omega_j$ (instead of directly computing it as a double integral).
8. Compute $\int_S^{\phi(S)} \omega_i = \int_P^{\phi(S)} \omega_i - \int_P^S \omega_i$ by the indefinite integral in Step 3. Use this to deduce $\int_S^{\phi(S)} \omega_i \omega_j$ for $i = j$.
9. Use the indefinite integral in Step 5 to get $\int_S^{\phi(S)} \omega_i \omega_j$ for $i < j$.
10. Repeat the trick in Step 7 to get $\int_S^{\phi(S)} \omega_i \omega_j$ for $i > j$.
11. Compute $\int_Q^{\phi(Q)} \omega_i$ and use it to deduce $\int_Q^{\phi(Q)} \omega_i \omega_j$ for $i = j$.
12. Compute $\int_Q^{\phi(Q)} \omega_i \omega_j$ for $i < j$.
13. Repeat the trick in Step 7 to get $\int_Q^{\phi(Q)} \omega_i \omega_j$ for $i < j$.
14. Use $\int_S^Q \omega_i = \int_P^Q \omega_i - \int_P^S \omega_i$ to get $\int_S^Q \omega_i$.

**Algorithm 7.10** (Double integrals from a Weierstrass endpoint).

*Input*: A finite Weierstrass point $P$, a non-Weierstrass point $Q$, and basis differentials $\omega_i, \omega_j$.

*Output*: The double integrals $\int_P^Q \omega_i \omega_j$.

1. Compute all of the integrals as in Algorithm 7.9.
2. Compute double integrals $\int_S^Q \omega_i \omega_j$ using the terms in Step 1 as appropriate in Algorithm 7.4. (See Remark 7.11 for an additional improvement to this step.)
3. Recover the double integrals $\int_P^Q \omega_i \omega_j = \int_P^S \omega_i \omega_j + \int_S^Q \omega_i \omega_j + \int_P^S \omega_j \int_S^Q \omega_i$ by using additivity.

**Remark 7.11.** In the case of $g = 1$, the linear system only yields *one* double integral not obtainable through single integrals. Indeed, for $0 \le i, j \le 1$, we have

$$\int_S^Q \omega_i \omega_i = \frac{1}{2}\left(\int_S^Q \omega_i\right)^2 \quad \text{and} \quad \int_S^Q \omega_i \omega_j = -\int_S^Q \omega_j \omega_i + \int_S^Q \omega_i \int_S^Q \omega_j.$$

So it suffices to compute $\int_S^Q \omega_0 \omega_1$. Thus, rather than computing all of the constants $c_{00}, c_{01}, c_{10}, c_{11}$ and their correction factors (see (7)), if we precompute the two double integrals that are expressible in terms of single integrals, as well as the product of single integrals that relates $\int_S^Q \omega_1 \omega_0$ to $\int_S^Q \omega_0 \omega_1$, it suffices to compute $c_{01}$ (and its correction factor) to solve for the other three constants and $\int_S^Q \omega_0 \omega_1$.

In other words, the linear system in Algorithm 7.4 tells us that

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

which we write as

$$A\begin{pmatrix}i_{00}\\ v_{01}\\ s_{01}-v_{01}\\ i_{11}\end{pmatrix}=\begin{pmatrix}x_{00}\\ \ell_{01}\\ x_{10}\\ x_{11}\end{pmatrix},$$

where the vector on the left consists of integrals (with $i_{00}=\int_S^Q \omega_0\,\omega_0$, $i_{11}=\int_S^Q \omega_1\,\omega_1$, $s_{01}=\int_S^Q \omega_0\int_S^Q \omega_1$ all computed), and the vector on the right consists of constants (with $\ell_{01}$ computed). So we solve for $v_{01}:=\int_S^Q \omega_0\,\omega_1, x_{00}, x_{10}, x_{11}$, since knowing $v_{01}$ gives us the complete set of double integrals on basis differentials. While this only gives a constant speedup in terms of complexity, in practice, this helps when $S$ is defined over a highly ramified extension of $\mathbb{Q}_p$.

As numerical checks, one may use the following corollaries of Proposition 7.7.

**Corollary 7.12.** *For $P, Q$ Weierstrass points and $S$ a third point, we have additivity in endpoints*: $\int_P^Q \omega_i\,\omega_j+\int_Q^S \omega_i\,\omega_j=\int_P^S \omega_i\,\omega_j$.

**Corollary 7.13.** *For $P, Q$ Weierstrass points, we have*

$$\int_P^Q \omega_i\,\omega_j+\int_P^Q \omega_j\,\omega_i=0.$$

It is worth noting that in general, unlike in the case of a single Coleman integral, for $P$ and $Q$ both Weierstrass points, unless $i=k$, the double Coleman integral $\int_P^Q \omega_i\,\omega_k$ is not necessarily 0. However, in the case of $i=k$, the integral can be computed as $\int_P^Q \omega_i\,\omega_i=\frac{1}{2}\left(\int_P^Q \omega_i\right)^2=0$.

**Example 7.14.** Consider the curve $y^2=x(x-1)(x+9)$, over $\mathbb{Q}_7$, and the points $P_1=(1,0)$, $P_2=(0,0)$, and $Q=(-1,4)$. We have

$$\begin{pmatrix}\int_{P_1}^Q \omega_0\,\omega_0\\ \int_{P_1}^Q \omega_0\,\omega_1\\ \int_{P_1}^Q \omega_1\,\omega_0\\ \int_{P_1}^Q \omega_1\,\omega_1\end{pmatrix}=\begin{pmatrix}2\cdot 7^2+5\cdot 7^3+4\cdot 7^4+3\cdot 7^5+O(7^6)\\ 6\cdot 7+5\cdot 7^2+4\cdot 7^3+6\cdot 7^4+O(7^6)\\ 2\cdot 7^2+3\cdot 7^3+3\cdot 7^4+7^5+O(7^6)\\ 1+5\cdot 7+5\cdot 7^3+4\cdot 7^4+4\cdot 7^5+O(7^6)\end{pmatrix}$$

and

$$\begin{pmatrix} \int_{P_2}^{Q} \omega_0\omega_0 \\ \int_{P_2}^{Q} \omega_0\omega_1 \\ \int_{P_2}^{Q} \omega_1\omega_0 \\ \int_{P_2}^{Q} \omega_1\omega_1 \end{pmatrix} = \begin{pmatrix} 2\cdot 7^2 + 5\cdot 7^3 + 4\cdot 7^4 + 3\cdot 7^5 + O(7^6) \\ 2\cdot 7^2 + 7^3 + 6\cdot 7^4 + 5\cdot 7^5 + O(7^6) \\ 6\cdot 7 + 5\cdot 7^2 + 6\cdot 7^3 + 3\cdot 7^4 + 3\cdot 7^5 + O(7^6) \\ 1 + 5\cdot 7 + 5\cdot 7^3 + 4\cdot 7^4 + 4\cdot 7^5 + O(7^6) \end{pmatrix},$$

from which we see that $\int_{P_1}^{P_2} \omega_0\omega_1 \neq 0$ and likewise $\int_{P_1}^{P_2} \omega_1\omega_0 \neq 0$.

## 8. Kim's nonabelian Chabauty method

We now present the motivation for all of the algorithms thus far. Let $\mathscr{C}/\mathbb{Z}$ be the minimal regular model of an elliptic curve $C/\mathbb{Q}$ of analytic rank 1 with Tamagawa numbers all 1. Let $\mathscr{X} = \mathscr{C} - \{\infty\}$ and $\omega_0 = \frac{dx}{2y}, \omega_1 = \frac{x\,dx}{2y}$. Taking a tangential basepoint $b$ at $\infty$ (or letting $b$ be an integral 2-torsion point), we have the analytic functions

$$\log_{\omega_0}(z) = \int_b^z \omega_0, \quad D_2(z) = \int_b^z \omega_0\omega_1.$$

With this setup, we have:

**Theorem 8.1** [2; 14]. *Suppose $P$ is a point of infinite order in $\mathscr{C}(\mathbb{Z})$. Then $\mathscr{X}(\mathbb{Z}) \subset \mathscr{C}(\mathbb{Z}_p)$ is in the zero set of*

$$f(z) := \big(\log_{\omega_0}(P)\big)^2 D_2(z) - \big(\log_{\omega_0}(z)\big)^2 D_2(P).$$

**Corollary 8.2** [2; 14]. *The expression*

$$\frac{D_2(P)}{\big(\log_{\omega_0}(P)\big)^2} \tag{8}$$

*is independent of the point $P$ of infinite order in $\mathscr{C}(\mathbb{Z})$.*

**Example 8.3.** We revisit Example 1 in [2]. Let $E$ be the rank-1 elliptic curve $y^2 = x^3 - 1323x + 3942$, with minimal model $\mathscr{E}$ having Cremona label 65a1. Consider the following points on $E$ which are integral on $\mathscr{E}$: $b = (3, 0)$, $P = (39, 108)$, $Q = (-33, -108)$, $R = (147, 1728)$. Using Algorithm 7.10, we compute the integrals

$$\int_b^P \omega_0\omega_1 = 4\cdot 11 + 4\cdot 11^2 + 7\cdot 11^3 + 9\cdot 11^4 + 5\cdot 11^6 + O(11^7),$$
$$\int_b^P \omega_0 = 4\cdot 11 + 7\cdot 11^2 + 9\cdot 11^3 + 3\cdot 11^4 + 5\cdot 11^5 + 7\cdot 11^6 + O(11^7),$$

$$\int_b^Q \omega_0\omega_1 = 4\cdot 11 + 4\cdot 11^2 + 7\cdot 11^3 + 9\cdot 11^4 + 5\cdot 11^6 + O(11^7),$$
$$\int_b^Q \omega_0 = 7\cdot 11 + 3\cdot 11^2 + 11^3 + 7\cdot 11^4 + 5\cdot 11^5 + 3\cdot 11^6 + O(11^7),$$
$$\int_b^R \omega_0\omega_1 = 5\cdot 11 + 6\cdot 11^2 + 7\cdot 11^3 + 5\cdot 11^4 + 3\cdot 11^5 + 9\cdot 11^6 + O(11^7),$$
$$\int_b^R \omega_0 = 3\cdot 11 + 7\cdot 11^2 + 2\cdot 11^3 + 3\cdot 11^4 + 7\cdot 11^6 + O(11^7),$$

and we see that the ratio in Corollary 8.2 is constant on integral points:

$$\frac{D_2(P)}{\big(\log_{\omega_0}(P)\big)^2} = \frac{D_2(Q)}{\big(\log_{\omega_0}(Q)\big)^2} = \frac{D_2(R)}{\big(\log_{\omega_0}(R)\big)^2},$$
$$= 3\cdot 11^{-1} + 6 + 2\cdot 11 + 10\cdot 11^2 + 3\cdot 11^3 + 5\cdot 11^4 + O(11^5).$$

However, for $S = (103, 980)$, which is not integral on $\mathscr{C}$, we see that

$$\int_b^S \omega_0\omega_1 = 3\cdot 11 + 10\cdot 11^2 + 4\cdot 11^3 + 10\cdot 11^4 + 7\cdot 11^5 + 10\cdot 11^6 + O(11^7)$$
$$\int_b^S \omega_0 = 11 + 7\cdot 11^3 + 5\cdot 11^5 + O(11^7)$$
$$\frac{D_2(S)}{\big(\log_{\omega_0}(S)\big)^2} = 3\cdot 11^{-1} + 10 + 6\cdot 11 + 9\cdot 11^2 + 8\cdot 11^3 + 6\cdot 11^4 + O(11^5).$$

**Example 8.4.** We give a variation on Example 4 in [2]. Let $E$ be the rank-1 elliptic curve $y^2 = x^3 - 16x + 16$, with minimal model $\mathscr{C}$ having Cremona label 37a1. Letting $P, Q$ be two fixed integral points on $E$, we can use the link lemma to rewrite Theorem 8.1 so that the relevant double integral is no longer from a tangential basepoint. Indeed, integral points $z$ occur in the zero set of

$$\left(\left(\int_b^z \omega_0\right)^2 - \left(\int_b^P \omega_0\right)^2\right)\frac{\int_P^Q \omega_0\omega_1 + \int_P^Q \omega_0 \int_b^P \omega_1}{\left(\int_b^Q \omega_0\right)^2 - \left(\int_b^P \omega_0\right)^2} - \left(\int_P^z \omega_0\omega_1 + \int_P^z \omega_0 \int_b^P \omega_1\right).$$

Slightly modifying Algorithm 7.4 to take as endpoint a parameter $z$ (see [3, §7.2.2] for more details), we can recover the integral points

$$\big\{(0, \pm 4), (4, \pm 4), (-4, \pm 4), (8, \pm 20), (24, \pm 116)\big\}.$$

**Remark 8.5.** Note that in the classical Chabauty method, one can use the Jacobian of the curve $J$ to find the global constant of integration (see [5; 10]). In particular,

the points on $J$ form a $\mathbb{Z}$-module and we have multiplication-by-$n$ morphisms $[n]\colon J(\mathbb{Q}_p) \to J(\mathbb{Q}_p)$, which gives $n\int_P^Q \omega = \int_{[n](P)}^{[n](Q)} \omega$. By choosing $n$ carefully, we can ensure that $[n]P$ and $[n]Q$ both lie in the residue disk of the identity, and pulling back to the curve, all integrals can be computed by tiny integrals. For iterated integrals, we do not have appropriate endomorphisms available.

## Acknowledgments

The author thanks Kiran Kedlaya and Nils Bruin for several helpful conversations, William Stein for access to the computer `sage.math.washington.edu`, and the referees for useful suggestions. This work was done as part of the author's doctoral thesis at MIT, during which she was supported by an NSF Graduate Fellowship and an NDSEG Fellowship. This paper was prepared for submission while the author was supported by NSF grant DMS-1103831.

## References

[1] Jennifer S. Balakrishnan, Robert W. Bradshaw, and Kiran S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, in Hanrot et al. [11], 2010, pp. 16–31. MR 2012b:14048

[2] 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** (2011), no. 1, 281–291. MR 2011m:11108

[3] Jennifer Sayaka Balakrishnan, *Coleman integration for hyperelliptic curves: algorithms and applications*, Ph.D. thesis, Department of Mathematics, Massachusetts Institute of Technology, 2011. http://hdl.handle.net/1721.1/67785

[4] Amnon Besser, *Coleman integration using the Tannakian formalism*, Math. Ann. **322** (2002), no. 1, 19–48. MR 2003d:11176

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

[6] Kuo-tsai Chen, *Algebras of iterated path integrals and fundamental groups*, Trans. Amer. Math. Soc. **156** (1971), 359–379. MR 43 #1069

[7] Robert Coleman and Ehud de Shalit, *p-adic regulators on curves and special values of p-adic L-functions*, Invent. Math. **93** (1988), no. 2, 239–266. MR 89k:11041

[8] Robert F. Coleman, *Dilogarithms, regulators and p-adic L-functions*, Invent. Math. **69** (1982), no. 2, 171–208. MR 84a:12021

[9] ———, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168. MR 86j:14014

[10] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-2 curve*, Duke Math. J. **90** (1997), no. 3, 435–463. MR 98j:11048

[11] Guillaume Hanrot, François Morain, and Emmanuel Thomé (eds.), *Algorithmic number theory: Proceedings of the 9th Biennial International Symposium (ANTS-IX) held in Nancy, July 19–23, 2010*, Lecture Notes in Computer Science, no. 6197, Berlin, Springer, 2010. MR 2011g:11002

[12] Kiran S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338, errata: [13]. MR 2002m:14019

[13] ———, *Errata for*: *"Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology"*, J. Ramanujan Math. Soc. **18** (2003), no. 4, 417–418. MR 2005c:14027

[14] Minhyong Kim, *Massey products for elliptic curves of rank* 1, J. Amer. Math. Soc. **23** (2010), no. 3, 725–747. MR 2012b:11091

[15] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, preprint, 2010. http://math.mit.edu/~poonen/papers/chabauty.pdf

JENNIFER S. BALAKRISHNAN: jen@math.harvard.edu
*Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138, USA*

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

---



ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

---

**MATHEMATICAL SCIENCES PUBLISHERS**
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

# THE OPEN BOOK SERIES 1

# Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

## TABLE OF CONTENTS