Applications of Explicit Coleman Integration for Hyperelliptic Curves

Jennifer S. Balakrishnan
Massachusetts Institute of Technology, MIT, Cambridge, MA, USA

Introduction to Coleman Integration

Notation:

- C hyperelliptic curve over an unramified extension k of $\mathbb{Q}_p$ with p a prime of good ordinary reduction
- Points P, Q, R on C
- Differential forms ω, ω' of the second kind on C
- Differential forms $\omega_0, \ldots, \omega_{2g-1}$ a basis for $H^1_{dR}(C)$, where $\omega_i = \frac{x^i dx}{2y}$

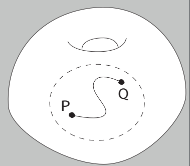
Coleman constructed a definite integral with the following properties:

1. Linearity: $\int_P^Q (\alpha\omega + \beta\omega') = \alpha \int_P^Q \omega + \beta \int_P^Q \omega'$.
2. Additivity: $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$.
3. Change of variables: If C' is another curve and $\phi : C \to C'$ a rigid analytic map between wide opens then $\int_P^Q \phi^*\omega = \int_{\phi(P)}^{\phi(Q)} \omega$.
4. Fundamental theorem of calculus: $\int_P^Q df = f(Q) - f(P)$.

"Tiny" Integrals

Suppose $P, Q \in C(\mathbb{C}_p)$ are in the same residue disc. We compute $\int_P^Q \omega_i$ locally:

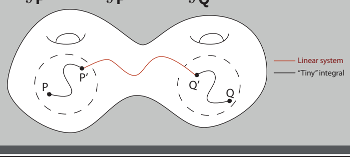
1. Construct an interpolation $x(t), y(t)$ from P to Q.
2. Formally integrate the power series in t: $\int_P^Q \omega_i = \int_P^Q x^i \frac{dx}{2y} = \int_0^1 \frac{x(t)^i}{2y(t)} \frac{dx(t)}{dt} dt$.



Integrals via Kedlaya's algorithm

If P, Q are in different residue discs, we use Frobenius ϕ to construct $\int_P^Q \omega_i$:

1. Find Teichmüller points P', Q' in the discs of P, Q.
2. Compute the tiny integrals $\int_P^{P'} \omega_i, \int_{Q'}^{Q} \omega_i$.
3. Calculate the action of Frobenius on each basis element $\phi^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j$.
4. Change of variables gives $\sum_{j=0}^{2g-1} (M - I)_{ij} \int_{P'}^{Q'} \omega_j = f_i(P') - f_i(Q')$, and solving the linear system gives the integrals $\int_{P'}^{Q'} \omega_i$.
5. Correct endpoints to recover $\int_P^Q \omega_i = \int_P^{P'} \omega_i + \int_{P'}^{Q'} \omega_i + \int_{Q'}^{Q} \omega_i$.



Application: Coleman-Gross height pairing

The Coleman-Gross height pairing is a symmetric bilinear pairing

$$h : \mathrm{Div}^0(C) \times \mathrm{Div}^0(C) \to \mathbb{Q}_p,$$

which can be written as a sum of local height pairings $h = \sum_v h_v$ over all finite places v of the number field K.

Local height above p

Let $D_1, D_2 \in \mathrm{Div}^0(C)$ have disjoint support and ω_{D_1} be a normalized differential associated to D_1. The local height pairing at v above p is given by

$$h_v(D_1, D_2) = \mathrm{tr}_{k/\mathbb{Q}_p}\left(\int_{D_2} \omega_{D_1}\right).$$

To construct ω_{D_1}:

- Choose a differential ω with $\mathrm{Res}(\omega) = D_1$.
- Fix a splitting
$$H^1_{dR}(C/k) = H^{1,0}_{dR}(C/k) \oplus W,$$
where W is the unit root subspace for the action of Frobenius.
- Via the canonical homomorphism $\Psi : T(k)/T_l(k) \longrightarrow H^1_{dR}(C/k)$, compute $\Psi(\omega) = \eta + \Psi(\omega_{D_1})$, for η holomorphic. Then $\omega_{D_1} := \omega - \eta$.

Coleman integration: meromorphic differential

Let ϕ be a p-power lift of Frobenius and set $\alpha := \phi^*\omega - p\omega$. Then for β a differential with residue divisor $D_2 = (R) - (S)$, we compute

$$\int_{D_2} \omega = \int_S^R \omega = \frac{1}{1-p}\left(\Psi(\alpha) \cup \Psi(\beta) + \sum \mathrm{Res}\left(\alpha \int \beta\right)\right) - \frac{1}{1-p}\left(\int_{\phi(S)}^{S} \omega + \int_R^{\phi(R)} \omega\right).$$

Example: global p-adic heights for genus 1

Example: Let C be the elliptic curve $y^2 = x^3 - 5x$, with $Q = (-1, 2), Q' = (-1, -2), R = (5, 10), R' = (5, -10)$, so that $(Q) - (Q') = (R) - (R') = (\frac{9}{4}, -\frac{3}{8}) =: P$.

We compute the 13-adic height of P:

- Above 13, the local height $h_{13}((Q) - (Q'), (R) - (R'))$ is $2 \cdot 13 + 6 \cdot 13^2 + 13^3 + 5 \cdot 13^4 + O(13^5)$.
- Away from 13, the only nontrivial contribution is $2 \log 3$ (by work of Müller).
- So the global 13-adic height is $12 \cdot 13 + 4 \cdot 13^2 + 10 \cdot 13^3 + 9 \cdot 13^4 + O(13^5)$.

We compare this to Harvey's implementation of Mazur-Stein-Tate in Sage:

```
sage:  C = EllipticCurve([-5,0])
sage:  f = C.padic_height(13)
sage:  f(C(9/4,-3/8)) + O(13^5)
12*13 + 4*13^2 + 10*13^3 + 9*13^4 + O(13^5)
```

Application: Kim's nonabelian Chabauty method

Kim's nonabelian Chabauty method allows us to recover integral points on elliptic curves:

Theorem:
Let $\mathcal{C}/\mathbb{Z}$ be the minimal regular model of an elliptic curve $C/\mathbb{Q}$ of analytic rank 1 with Tamagawa numbers all 1. Let $\mathcal{X} = \mathcal{C} - \{\infty\}$ and $\omega_0 = \frac{dx}{2y}, \omega_1 = \frac{xdx}{2y}$. Taking a tangential base point b at ∞, let $\log_{\omega_0}(z) = \int_b^z \omega_0, D_2(z) = \int_b^z \omega_0\omega_1$. Suppose y is a point of infinite order in $\mathcal{C}(\mathbb{Z})$. Then $\mathcal{X}(\mathbb{Z}) \subset \mathcal{C}(\mathbb{Z}_p)$ is in the zero set of

$$f(z) := \log^2_{\omega_0}(y) D_2(z) - \log^2_{\omega_0}(z) D_2(y).$$

Computing $D_2(z)$: Double Coleman integrals

We take as our normalization $\int_P^Q \omega_i\omega_j := \int_P^Q \omega_i(R) \int_P^R \omega_j$.

A straightforward generalization of single Coleman integration yields the following techniques:

- "Tiny" double integration (points P, Q in the same residue disc)
  - Compute local coordinates $x(t), y(t)$ at P, and let $R = (a + x(Q), \sqrt{f(a + x(Q))})$.
  - Write $\int_P^Q \omega_i\omega_j = \int_0^{x(Q)-x(P)} \left(\int_0^a \frac{x(t)^j dx(t)}{2y(t)}\right) \frac{x(R(a))^i}{2y(R(a))} \frac{dx(R(a))}{da}$.
- Linking integrals between non-Weierstrass points via Frobenius:
  - Compute Teichmüller points P', Q' in the discs of P, Q.
  - Use Frobenius to calculate $\int_{P'}^{Q'} \omega_i\omega_k$.
  - Recover the double integral: $\int_P^Q \omega_i\omega_k = \int_{P'}^{Q'} \omega_i\omega_k - \int_{P'}^{P} \omega_i\omega_k - \left(\int_P^Q \omega_i\right)\left(\int_{P'}^{P} \omega_k\right) - \left(\int_Q^{Q'} \omega_i\right)\left(\int_{P'}^{Q'} \omega_k\right) + \int_{Q'}^{Q} \omega_i\omega_k$.

Example: integral points

Let $E : y^2 = x^3 - 16x + 16$ (which has minimal model 37a1). Given two integral points x, y of infinite order, a third point z occurs in the zero set of the function

$$\left(\left(\int_b^z \omega_0\right)^2 - \left(\int_b^x \omega_0\right)^2\right) \frac{\int_x^y \omega_0\omega_1 + \int_x^y \omega_0 \int_b^x \omega_1}{(\int_b^y \omega_0)^2 - (\int_b^x \omega_0)^2} - \left(\int_x^z \omega_0\omega_1 + \int_x^z \omega_0 \int_b^x \omega_1\right).$$

Indeed, fixing $x = (0, 4), y = (4, 4)$ on E, we may recover $z = (-4, -4), (8, -20), (24, 116)$.

Acknowledgments

This work was carried out as part of the author's PhD thesis with Kiran Kedlaya, thanks to the support of the National Defense Science and Engineering Fellowship and the National Science Foundation Graduate Fellowship Program. We would also like to thank Robert Bradshaw, Minhyong Kim, and Steffen Müller for many helpful conversations, as well as William Stein and NSF Grant No. DMS-0821725 for use of sage.math.washington.edu.

jen@math.mit.edu