Coleman integration for even-degree models of hyperelliptic curves

Jennifer S. Balakrishnan

Abstract

The Coleman integral is a p-adic line integral that encapsulates various quantities of number theoretic interest. Building on the work of Harrison [*J. Symbolic Comput.* 47 (2012) no. 1, 89–101], we extend the Coleman integration algorithms in Balakrishnan *et al.* [*Algorithmic number theory*, Lecture Notes in Computer Science 6197 (Springer, 2010) 16–31] and Balakrishnan [*ANTS-X: Proceedings of the Tenth Algorithmic Number Theory Symposium*, Open Book Series 1 (Mathematical Sciences Publishers, 2013) 41–61] to even-degree models of hyperelliptic curves. We illustrate our methods with numerical examples computed in Sage.

1. Introduction

The use of p-adic integration to study rational points on curves was initiated in the 1980s by Coleman [**5**, **7**, **8**]. This theory relies on locally defined antiderivatives that are extended analytically by the principle of *Frobenius equivariance*. Coleman used these techniques to re-interpret the method of Chabauty [**4**], giving an explicit bound on the number of rational points on curves in certain cases [**6**]. In the spirit of this work, together with Besser and Müller [**2**], we gave a 'quadratic' Chabauty method, using p-adic heights re-interpreted as double Coleman integrals to find integral points on hyperelliptic curves with odd-degree models.

All of this relies on explicitly computing various Coleman integrals. In joint work with Bradshaw and Kedlaya [**3**], we gave explicit methods to compute single Coleman integrals for hyperelliptic curves with odd-degree models. The key theoretical input was Kedlaya's algorithm [**12**] to compute the action of Frobenius on Monsky–Washnitzer cohomology, formulated for odd-degree models of hyperelliptic curves. In a similar vein, we also gave algorithms to compute iterated Coleman integrals on hyperelliptic curves with odd-degree models [**1**] and used these algorithms to carry out the quadratic Chabauty method on hyperelliptic curves with odd-degree models [**2**].

Recently, Harrison [**11**] extended Kedlaya's algorithm to even-degree models. Thus, in the current paper, building on Harrison's work, we extend the Coleman integration algorithms in [**3**] and [**1**] to even-degree models of hyperelliptic curves over unramified extensions of $\mathbb{Q}_p$ and discuss what would be needed to carry out quadratic Chabauty for even-degree models.

The main difference between our approach to odd- and even-degree models lies in the dimension of the space of cohomology we compute with, and how the dimension of this space relates to the dimension of the Tate module of the Jacobian of the hyperelliptic curve. In the odd-degree case, the two dimensions coincide. In the even-degree case, they do not. Nevertheless, in the even-degree case, the eigenvalues of Frobenius on the relevant cohomology are easily computable, and one can set up a linear system, as in the odd-degree case, to recover the global p-adic integrals.

The structure of the paper is as follows: in §2, we outline a few essential results of Harrison [11] concerning the relevant background in p-adic cohomology. We use these results to give our Coleman integration algorithms in §3. In §4, we present some numerical examples, computed using our implementation in Sage [13].

2. Some p-adic cohomology

We begin by setting some notation. Let p be an odd prime, let $k = \mathbb{F}_q$ be the finite field of $q = p^m$ elements, and let $W(k)$ be the ring of integers of K, the unique unramified degree-m extension of the local field $\mathbb{Q}_p$. Let $f(x)$ be a polynomial of degree $2g + 2$ with coefficients in $W(k)$ and distinct roots modulo p. The projective normalization $\mathcal{C}$ of the affine curve $C : y^2 = f(x)$ is a smooth hyperelliptic curve of genus g with two points at infinity, ∞^+ and ∞^-. We assume that C has good reduction at p. When necessary, we shall assume that $p > g$.

Let C' be the affine curve obtained by taking C and deleting the Weierstrass points, which are now just the support of the divisor of y. Let $\overline{C}, \overline{C'}$, and $\overline{\mathcal{C}}$ denote the reductions of C, C', and $\mathcal{C}$, respectively. Let $A = W(k)[x, y, z]/(y^2 - f(x), yz - 1)$ denote the coordinate ring of C'. We briefly recall some essential p-adic cohomology from [11, 12].

Let $A^\dagger$ denote the *Monsky–Washnitzer weak completion* of A; it is the ring consisting of infinite sums of the form

$$\sum_{i=-\infty}^{\infty} \frac{S_i(x)}{y^i}, \quad S_i(x) = \sum_{j=0}^{2g+1} a_j x^j \in W(k)[x],$$

subject to the conditions that $\liminf_{i \to \infty} v_p(S_i)/i > 0$ and $\liminf_{i \to \infty} v_p(S_{-i})/i > 0$, where $v_p(S_i(x)) = \min_i\{v_p(a_i)\}$; when necessary, one uses the relation $y^2 = f(x)$ to convert terms with large powers of x into terms with y^2.

Note that by having deleted the support of y, elements of $A^\dagger$ do not have poles in the space over which we integrate. Since even 1-forms can be integrated directly in terms of x, we focus our attention on odd 1-forms, those negated by the hyperelliptic involution, which we write as

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

Any such differential can be written as

$$\omega = dh + c_0\omega_0 + \ldots + c_{2g}\omega_{2g}, \tag{2.1}$$

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

$$\omega_i = x^i \frac{dx}{2y} \quad (i = 0, \ldots, 2g). \tag{2.2}$$

Namely, Harrison has proved the following result.

LEMMA 2.1. *The set $\{\omega_i\}$ for $i = 0, \ldots, 2g$ forms a basis of the odd part of the de Rham cohomology of $A^\dagger$.*

Proof. See [11, §3.2]. □

We can lift the p-power Frobenius to an endomorphism ϕ of $A^\dagger$ by defining it as the canonical Witt vector Frobenius ϕ_k on $W(k)$, then extending it to $W(k)[x]$ by sending x to x^p and

$$\phi(y) = y^p \left(1 + \frac{\phi(f(x)) - f(x)^p}{f(x)^p}\right)^{1/2}$$

$$= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(\phi(f(x)) - f(x)^p)^i}{y^{2pi}},$$

and using the relations

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

to reduce large powers of x and large (in absolute value) powers of y. By functoriality, ϕ induces a K-linear automorphism ϕ^* on cohomology. Finally, we compute q-power Frobenius by computing the mth power of p-power Frobenius ϕ (see Remark 1).

When C is given by an odd model, the corresponding cohomology has basis $\{x^i (dx/2y)\}_{i=0}^{2g-1}$. By computing the action of Frobenius on each of the $2g$ basis differentials and reducing using the relations above, one knows the action of Frobenius on the entire space. This reduction process was first described by Kedlaya [12] and is now known as *Kedlaya's algorithm*. Harrison [11] showed that the reduction works in essentially the same way when C is given by an even model: one computes the action of Frobenius on each of the $2g + 1$ differentials above and applies the same reduction steps to one extra differential.

To compute Coleman integrals, we must now understand how the eigenvalues of q-power Frobenius change when one introduces this extra differential. To look at this more precisely, let $P_{\overline{C}}(t)$ denote the numerator of the zeta function of $\overline{C}$, with $P_{\overline{C}}(t) = t^{2g} + c_{2g-1}t^{2g-1} + \ldots + c_0$, a monic polynomial over $\mathbb{Z}$. Denote its roots by $(\alpha_i)_{i=1}^{2g}$; recall that $|\alpha_i| = q^{1/2}$. By applying the Lefschetz fixed point formula to $\overline{C'}$ and its image $\mathbb{P}^a$ (where $\mathbb{P}^a = \mathbb{P}_k^1 \backslash S$, with S the set of finite places corresponding to the irreducible factors of $\overline{f}(x) \in k[x]$ and infinity), Harrison obtained the following result.

PROPOSITION 2.2 (Harrison [11], §3.1). *The eigenvalues of q-power Frobenius on H_-^1, the odd part of the de Rham cohomology of $A^\dagger$, are*

$$\{\alpha_1, \ldots, \alpha_{2g}, q\}.$$

Stated in another way, let M denote the matrix of q-power Frobenius with respect to the basis of H_-^1 given by elements of the form (2.2). The characteristic polynomial $P(t)$ of the action of q-power Frobenius on the odd part of the de Rham cohomology of $A^\dagger$ is

$$P(t) = (t - q)P_{\overline{C}}(t).$$

In particular, none of the eigenvalues of M are equal to 1 and $M - I$ is invertible over K.

Note that we compute M from an expression involving the matrix of p-power Frobenius, which we will denote by B; see Remark 1 and (3.3) for the computation producing M from B. When p is small relative to the genus of the curve g (in particular, when $p \leqslant g$), then B is not necessarily p-adically integral, that is, the integral lattice generated by the basis is not necessarily stable under Frobenius. This is undesirable because repeated multiplications involving a non-integral B (in particular, the computation in Remark 1) could result in problems with p-adic precision. To this end, we recall that Harrison also proved a lemma on integrality of the matrix of Frobenius B: namely, if $p > g$, the matrix B of the action of p-power Frobenius with respect to the basis in Lemma 2.1 is p-adically integral. Consequently, so is the matrix of q-power Frobenius M. Thus, for computational purposes, we will assume that $p > g$.

We will use the above in §3 to compute a linear system involving the Frobenius action on these differentials as in [3] and recover Coleman integrals.

3. *Coleman integration on even-degree models*

We now give algorithms to compute Coleman integrals on even-degree models of hyperelliptic curves. As in the odd-model case, local coordinates allow us to compute Coleman integrals

between two points in the same residue disk. In particular, we will distinguish between finite *non-Weierstrass* and *Weierstrass residue disks*. A point $P = (a, b) \in C(K)$ is in a finite non-Weierstrass disk if $a \in W(k)$ and $b \in W(k)^\times$; a point $P = (a, b) \in C(K)$ is in a Weierstrass disk if $a \in W(k)$ and $b \in W(k) \backslash W(k)^\times$.

3.1. *Local coordinates*

ALGORITHM 1 (Local coordinate at a point in a finite non-Weierstrass disk).
Input: A point $P = (a, b) \in C(K)$ in a finite non-Weierstrass disk and precision n.
Output: A parametrization $(x(t), y(t))$ at P in terms of a local coordinate.
  (i) Let $x(t) = t + a$, where t is a local coordinate.
  (ii) Solve for $y(t) = \sqrt{f(x(t))}$ by Newton's method: take $y_0(t) = b$, then set

$$y_i(t) = \frac{1}{2}\left(y_{i-1}(t) + \frac{f(x(t))}{y_{i-1}(t)} \right), \quad i \geqslant 1$$

  with $y_i(t) \to y(t)$. The number of iterates i to be taken depends on the necessary power series precision; for precision $O(t^n)$, one can take i to be $\lceil \log_2 n \rceil$.

ALGORITHM 2 (Local coordinate at a point in a Weierstrass disk).
Input: A point $P = (a, b)$ in $C(K)$ in a Weierstrass disk and precision n.
Output: A parametrization $(x(t), y(t))$ at P in terms of a local coordinate.
  (i) Let $y(t) = t + b$, where t is a local coordinate.
  (ii) Iteratively solve for $x(t)$ as follows: take $x_0(t) = a$; then Newton's method yields

$$x_i(t) = x_{i-1}(t) - \frac{f(x_{i-1}(t)) - y(t)^2}{f'(x_{i-1}(t))}, \quad i \geqslant 1$$

  with $x_i(t) \to x(t)$. The number of iterates i to be taken depends on the necessary power series precision; for precision $O(t^n)$, one can take i to be $\lceil \log_2 n \rceil$.

3.2. *Integrals*

We use the local coordinates above to compute 'tiny' Coleman integrals, those integrals between points in the same residue disk. Note that when one of the end points of integration is above infinity, one can change coordinates to work with finite non-Weierstrass points.

ALGORITHM 3 (Tiny Coleman integrals).
Input: Points $P, Q \in C(\mathbb{C}_p)$ in the same residue disk (neither equal to ∞^+, ∞^-) and a basis differential ω_i.
Output: The integral $\int_P^Q \omega_i$.
  (i) Using Algorithm 1 or 2, compute a parametrization $(x(t), y(t))$ at P in terms of a local coordinate t.
  (ii) Formally integrate the power series in t:

$$\int_P^Q \omega_i = \int_P^Q x^i \frac{dx}{2y} = \int_0^{t(Q)} \frac{x(t)^i}{2y(t)} \frac{dx(t)}{dt} dt.$$

Now we consider the case when the points $P, Q \in C(\mathbb{C}_p)$ are in different residue disks. As noted earlier, an odd differential ω on C can be represented as a linear combination

$$\omega = dh + c_0 \omega_0 + \ldots + c_{2g} \omega_{2g}.$$

The computation of $\int_P^Q \omega$ thus can be reduced to the computation of Coleman integrals on $(\omega_i)_{i=0}^{2g}$, and we have the following algorithms.

ALGORITHM 4 (Coleman integration between finite non-Weierstrass disks).

Input: The differentials $(\omega_i)_{i=0}^{2g}$, points $P, Q \in C(\mathbb{C}_p)$ in finite 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 $(\int_P^Q \omega_i)_{i=0}^{2g}$.

(i) Calculate the action of the mth power of p-power Frobenius ϕ on each basis element (see Remark 1 below):

$$(\phi^m)^* \omega_i = dh_i + \sum_{j=0}^{2g} M_{ij}^t \omega_j. \tag{3.1}$$

(ii) By change of variables (see Remark 2), we obtain

$$\sum_{j=0}^{2g} (M^t - I)_{ij} \int_P^Q \omega_j = h_i(P) - h_i(Q) - \int_P^{\phi^m(P)} \omega_i - \int_{\phi^m(Q)}^Q \omega_i \tag{3.2}$$

(the *fundamental linear system*). As the eigenvalues of the matrix M are algebraic integers of norm not equal to 1 (see Proposition 2.2), the matrix $M^t - I$ is invertible, and we may solve (3.2) to obtain the integrals $\int_P^Q \omega_i$.

REMARK 1. To compute the action of ϕ^m, we carry out the following strategy. Let B be the matrix of p-power Frobenius ϕ with respect to the standard basis $\{\omega_i\}$, so that

$$\phi^* \omega_i = dg_i + \sum_{j=0}^{2g} B_{ij}^t \omega_j,$$

where B^t denotes the transpose of B. We compute the action of ϕ^m by iteratively computing the action of ϕ, using the vector of functions $\mathbf{g} = (g_i)$ and the matrix B above to write

$$(\phi^m)^* \omega_i = dh_i + \sum_{j=0}^{2g} M_{ij}^t \omega_j,$$

where

$$\mathbf{h} = \phi^{m-1}(\mathbf{g}) + \sum_{i=1}^{m-1} \phi_k^{m-1}(B^t) \dots \phi_k^i(B^t) \phi^{i-1}(\mathbf{g}),$$

$$M^t = \phi_k^{m-1}(B^t) \dots \phi_k(B^t) B^t. \tag{3.3}$$

REMARK 2. We obtain (3.2) as follows. By change of variables,

$$\int_{\phi^m(P)}^{\phi^m(Q)} \omega_i = \int_P^Q (\phi^m)^* \omega_i$$

$$= \int_P^Q \left(dh_i + \sum_{j=0}^{2g} M_{ij}^t \omega_j \right)$$

$$= h_i(Q) - h_i(P) + \sum_{j=0}^{2g} M_{ij}^t \int_P^Q \omega_j.$$

Adding $\int_P^{\phi^m(P)} \omega_i + \int_{\phi^m(Q)}^Q \omega_i$ to both sides of this equation yields

$$\int_P^Q \omega_i = \int_P^{\phi^m(P)} \omega_i + \int_{\phi^m(Q)}^Q \omega_i + h_i(Q) - h_i(P) + \sum_{j=0}^{2g} M_{ij}^t \int_P^Q \omega_j,$$

which is equivalent to (3.2).

In Algorithm 4, note that the function h_i belongs to $A^\dagger$ and need not converge at a Weierstrass point P. It is for this reason that Algorithm 4 cannot be directly applied to the situation where P or Q is a Weierstrass point.

So, let us suppose that P is a Weierstrass point. Here is how we adapt Algorithm 4. Note that h_i converges at any point R near the boundary of the residue disk containing P: in particular, Algorithm 4 can be applied using R as one of the end points. So, we first find an auxiliary point R near the boundary of the disk of P. Next, to compute the integral between P and any other finite non-Weierstrass point Q, we use a tiny integral (between P and R) and the fundamental linear system in Algorithm 4 (between R and Q) to recover the desired integral: $\int_P^Q \omega_i = \int_P^R \omega_i + \int_R^Q \omega_i$.

Thus, to compute integrals in a Weierstrass disk, we first compute an auxiliary point.

ALGORITHM 5 (Finding a near-boundary point in a Weierstrass disk).
Input: A Weierstrass point P and a positive integer d.
Output: A point $R = (x(p^{1/d}), y(p^{1/d}))$ in the disk of P, near the boundary of the disk.
  (i) Using Algorithm 2, compute a parametrization $(x(t), y(t))$ at P in terms of the local coordinate t.
 (ii) Evaluate the parametrization at $t = p^{1/d}$. This is R.

ALGORITHM 6 (Coleman integration between a Weierstrass disk and a finite non-Weierstrass disk).
Input: A point P in a Weierstrass disk, a positive integer d, a point Q in a finite non-Weierstrass disk, and a basis differential ω_i.
Output: The integral $\int_P^Q \omega_i$.
  (i) Use Algorithm 5 to find R.
 (ii) Compute $\int_P^R \omega_i$ as a tiny integral.
(iii) Use the fundamental linear system in Algorithm 4 to compute $\int_R^Q \omega_i$.
 (iv) Use additivity in end points to recover $\int_P^Q \omega_i = \int_P^R \omega_i + \int_R^Q \omega_i$.

REMARK 3. In practice, we choose d in Algorithms 5 and 6 by starting with an initial guess based on p, g, and precision n. If the resulting value of the integral produced by Algorithm 6 is not in K (up to $O(p^n)$) but is rather in $K(p^{1/d})$, the value of d is subsequently increased and the computation of the integral repeated until one sees the value of the integral converge to an element of K (up to $O(p^n)$).

One can see, then, that the algorithms for single Coleman integrals do not depend on the model of the hyperelliptic curve in an essential way. Indeed, the algorithms for odd- and even-degree models are essentially the same.

With this observation in hand, we now state the generalization of our method to iterated integrals on hyperelliptic curves of even-degree model and refer the interested reader to [1] for the details in the odd-model case, which carry over directly to the even-model case.

An *iterated* Coleman integral
$$\int_P^Q \xi_n \ldots \xi_1$$
of 1-forms $\xi_1, \ldots, \xi_n$ formally behaves like an iterated path integral
$$\int_0^1 \int_0^{t_1} \ldots \int_0^{t_{n-1}} f_n(t_n) \ldots f_1(t_1) \, dt_n \ldots dt_1.$$

Within a single residue disk, we may use a local coordinate to parametrize the path between

points and iteratively integrate. Between two different residue disks, we think of the integral

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

using a collection of dummy parameters $R_1,\ldots,R_{n-1}$ and repeatedly compute the action of Frobenius on differentials to yield a linear system giving the values of integrals between points in different residue disks. Thus, for C/K a hyperelliptic curve given by an even-degree model, we also have the following result.

THEOREM 3.1. *Let $P, Q \in C(\mathbb{C}_p)$ be finite 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 mth power of p-power Frobenius on the basis differentials $\omega_0,\ldots,\omega_{2g}$. For constants $c_{i_0,\ldots,i_{n-1}}$ 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*

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

For details turning this theorem into an algorithm in the odd-degree case, see [1, §§ 4–7]. The only differences between the odd- and the even-degree cases are in the dimensions of the tensor powers of the relevant matrix of Frobenius.

4. Applications

4.1. *Computing single integrals and carrying out the Chabauty method*

Consider the genus-2 curve X given by $y^2 = (x^2+1)(x^2+2)(x^2+2x+2)$, whose Jacobian J has rank 1, as computed by Flynn [9, Example 3.1]. The rational points $X(\mathbb{Q})$ were computed by Flynn [10, Example 3.1] by computing appropriate elements in the kernel of the reduction map from $J(\mathbb{Q}_3)$ to $J(\mathbb{F}_3)$.

Here we take another approach, constructing an annihilating differential ω on the curve by computing Coleman integrals between different residue disks. Consider $P = (0, 2)$ and $\iota(P) = (0, -2)$, its image under the hyperelliptic involution ι. Then we have

$$a := \int_P^{\iota(P)} \omega_0 = 2\cdot3^2 + 2\cdot3^3 + 3^5 + O(3^8),$$

$$b := \int_P^{\iota(P)} \omega_1 = 2\cdot3^2 + 2\cdot3^3 + 2\cdot3^4 + 2\cdot3^6 + O(3^8),$$

and thus the integral of

$$\omega := b\omega_0 - a\omega_1$$

computed from the base point P can be used to find the other rational points on X. In particular, X has the following rational points:

$$\{(0, \pm2), (-\tfrac{1}{2}, \pm\tfrac{15}{8}), \infty^+, \infty^-\}.$$

4.2. *Quadratic Chabauty for even-degree models of hyperelliptic curves*

By Theorem 3.1, we can compute double integrals on even-degree models of hyperelliptic curves, which is a crucial step in carrying out quadratic Chabauty for even-degree models of hyperelliptic curves. Nevertheless, one must also explicitly compute the local component of the p-adic height pairing above p for even-degree models of hyperelliptic curves. We plan to address this in future work with Besser and Müller.

References

1. J. S. BALAKRISHNAN, 'Iterated Coleman integration for hyperelliptic curves', *ANTS-X: Proceedings of the Tenth Algorithmic Number Theory Symposium*, Open Book Series 1 (eds E. W. Howe and K. S. Kedlaya; Mathematical Sciences Publishers, 2013) 41–61.
2. J. S. BALAKRISHNAN, A. BESSER and J. S. MÜLLER, 'Quadratic Chabauty: p-adic height pairings and integral points on hyperelliptic curves', *J. reine angew. Math.*, to appear.
3. J. S. BALAKRISHNAN, R. W. BRADSHAW and K. S. KEDLAYA, 'Explicit Coleman integration for hyperelliptic curves', *Algorithmic number theory*, Lecture Notes in Computer Science 6197 (eds G. Hanrot, F. Morain and E. Thomé; Springer, 2010) 16–31.
4. C. CHABAUTY, 'Sur les points rationnels des courbes algébriques à l'unité', *C. R. Acad. Sci. Paris* 212 (1941) 882–885.
5. R. F. COLEMAN, 'Dilogarithms, regulators and p-adic L-functions', *Invent. Math.* 69 (1982) no. 2, 171–208.
6. R. F. COLEMAN, 'Effective Chabauty', *Duke Math. J.* 52 (1985) no. 3, 765–770.
7. R. F. COLEMAN, 'Torsion points on curves and p-adic abelian integrals', *Ann. of Math.* (2) 121 (1985) no. 1, 111–168.
8. 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.
9. E. V. FLYNN, 'Descent via isogeny in dimension 2', *Acta Arith.* 66 (1994) no. 1, 23–43.
10. E. V. FLYNN, 'A flexible method for applying Chabauty's theorem', *Compos. Math.* 105 (1997) no. 1, 79–94.
11. M. C. HARRISON, 'An extension of Kedlaya's algorithm for hyperelliptic curves', *J. Symbolic Comput.* 47 (2012) no. 1, 89–101.
12. K. S. KEDLAYA, 'Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology', *J. Ramanujan Math. Soc.* 16 (2001) 323–338; erratum *J. Ramanujan Math. Soc.* 18 (2003) 417–418.
13. W. A. STEIN *et al.*, 'Sage mathematics software, version 6.2' (The Sage Development Team, 2014) http://www.sagemath.org.

Jennifer S. Balakrishnan
Mathematical Institute
Radcliffe Observatory Quarter
Woodstock Road
Oxford OX2 6GG
United Kingdom

balakrishnan@maths.ox.ac.uk