Contemporary Mathematics

Curve equations from expansions of 1-forms at a nonrational point

Raymond van Bommel, Edgar Costa, Bjorn Poonen,
and Padmavathi Srinivasan

Abstract. We exhibit an algorithm to compute equations of an algebraic curve over a computable characteristic 0 field from the power series expansions of its regular 1-forms at a *nonrational* point of the curve, extending a 2005 algorithm of Baker, González-Jiménez, González, and Poonen for expansions at a rational point. If the curve is hyperelliptic, the equations present it as an explicit double cover of a smooth plane conic, or as a double cover of the projective line when possible. If the curve is nonhyperelliptic, the equations cut out the canonical model. The algorithm has been used to compute equations over $\mathbb{Q}$ for many hyperelliptic modular curves without a rational cusp in the L-functions and Modular Forms Database.

1. Introduction

A curve X is called nice if it is smooth, projective, and geometrically integral. From now on, X is a nice curve of genus $g \geq 2$ over $\mathbb{Q}$, but all our theorems and algorithms work over any ground field F of characteristic 0 if field operations in F are computable. Our goal is to give an algorithm that takes as input the initial terms of the expansions of 1-forms forming a basis of the $\mathbb{Q}$-vector space $\Gamma(X, \Omega^1_{X/\mathbb{Q}})$ at a *nonrational* point and returns equations for X over $\mathbb{Q}$; such input arises naturally in [Zyw24, Section 5], for instance. (The analogue for expansions at a *rational* point is covered in [BGGP05, Section 2.1].) These equations will cut out the canonical model if X is nonhyperelliptic, and a double cover of a genus 0 curve if X is hyperelliptic; see Theorem 3.1 for more details. Examples of the nonhyperelliptic case (the easier case) were worked out in [Bar14, Section 7] and [MS20, Sections 7 and 8]. So the main new work is in the hyperelliptic case.

The algorithm in [BGGP05, Section 2.1] will produce a model over the field of definition of the nonrational point, but there is no easy way to pass from that to the equation over $\mathbb{Q}$. Also, the presence of the rational point in [BGGP05, Section 2.1] meant that in the hyperelliptic case, the image of the canonical map was $\mathbb{P}^1_{\mathbb{Q}}$, whereas in the present article, it could instead be a pointless genus 0 curve instead of $\mathbb{P}^1_{\mathbb{Q}}$, in which case X will need to be given as a double cover of a plane conic. Moreover, there are additional complications in our article coming from the fact that even the expansion of objects defined over $\mathbb{Q}$ have coefficients in a larger number field.

The motivation for our algorithm is the problem of finding equations of modular curves *that have no rational cusp*. The algorithm has been used so far to calculate equations of over 4700 such hyperelliptic modular curves without a rational cusp for the L-Functions and Modular Forms Database [LMFDB], among which over 1500 are a double cover of a pointless genus 0 curve.

2. Hyperelliptic curves

The curve X is called hyperelliptic if the canonical map $X \to \mathbb{P}^{g-1}$ is not a closed immersion. Equivalently, X is hyperelliptic if there exists a degree 2 morphism π from X to some genus 0 curve C. Suppose that this is the case. Then C and the morphism π are unique up to isomorphism. In fact, C is the image of the canonical map. The curve C need not be isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$, but the anticanonical map for C identifies C with a smooth plane conic in $\mathbb{P}^2 = \operatorname{Proj} \mathbb{Q}[a, b, c]$. For any $d \in \mathbb{Z}_{\geq 0}$, let $\mathbb{Q}[a, b, c]_d$ be the space of degree d homogeneous polynomials in $\mathbb{Q}[a, b, c]$.

3. Main theorem

Now return to the general case, in which X is any nice curve of genus $g \geq 2$ over $\mathbb{Q}$. Let $K \supseteq \mathbb{Q}$ be a finite extension. Let $X_K = X \times_{\mathbb{Q}} K$. Let $P \in X(K)$. Assume that $K = \mathbb{Q}(P)$. Let q be a uniformizer of the completed local ring $\widehat{\mathscr{O}}_{X_K,P}$. Let $\omega_1, \ldots, \omega_g$ be a $\mathbb{Q}$-basis of $\mathrm{H}^0(X, \Omega^1)$. For each $i \in \{1, \ldots, g\}$, the Taylor expansion of ω_i at P is $w_i\, dq$ for some $w_i \in K[[q]]$. For $B \in \mathbb{Z}_{>0}$, let $K[q]_{<B} \simeq K[[q]]/(q^B)$ be the vector space of polynomials of degree $< B$. Let $\bar{w}_i := (w_i \bmod q^B) \in K[q]_{<B}$.

Theorem 3.1. *Let $B = 19g + 48$. There exists an algorithm with*

Input: g, K, and polynomials $\bar{w}_1, \ldots, \bar{w}_g \in K[q]_{<B}$ arising from some nice curve X over $\mathbb{Q}$ and $P \in X(K)$ as above.

Output:

- *If X is nonhyperelliptic, return* `nonhyperelliptic` *and a finite list of homogeneous polynomials over $\mathbb{Q}$ cutting out a curve in $\mathbb{P}^{g-1}$ linearly isomorphic over $\mathbb{Q}$ to the canonical model of X.*
- *If X is hyperelliptic and g is even, return* `hyperelliptic` *and a separable polynomial $f \in \mathbb{Q}[x]$ of degree $2g + 1$ or $2g + 2$ such that X is birational to the curve $y^2 = f(x)$.*
- *If X is hyperelliptic and g is odd, return* `hyperelliptic` *and homogeneous polynomials $Q \in \mathbb{Q}[a, b, c]_2$ and $H \in \mathbb{Q}[a, b, c]_{g+1}$ such that*

$$C \simeq \operatorname{Proj} \frac{\mathbb{Q}[a, b, c]}{(Q)} \subset \mathbb{P}^2 \quad \text{and} \quad X \simeq \operatorname{Proj} \frac{\mathbb{Q}[a, b, c, y]}{(y^2 - H, Q)} \subset \mathbb{P}\left(1, 1, 1, \frac{g+1}{2}\right).$$

  In this case, if a rational point on C is given, find a model $y^2 = f(x)$ as in the even genus hyperelliptic case.

Remark 3.2. In the odd genus hyperelliptic case, we may require the quadratic form Q to be *diagonal*, if desired.

Remark 3.3. By computing Hilbert symbols, one can determine whether a given smooth plane conic C over $\mathbb{Q}$ is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$; this is essentially due to Legendre. (More generally, by the Hasse–Minkowski local–global principle for quadratic forms, this can be done over any number field; see, e.g., [Shi10, Theorem 26.3]. But it

18 Jun 2025 10:53:10 PDT
250124-vanBommel Version 2 - Submitted to LuCaNT

involves more than just field operations, so it is not an algorithm that generalizes to *any* characteristic 0 field.)

4. Theoretical lemmas

Before explaining the algorithm, we prove a few theoretical lemmas. Let $S = \mathbb{Q}[x_1, \dots, x_g]$ be the homogeneous coordinate ring of $\mathbb{P}^{g-1}$ over $\mathbb{Q}$. Let $I \subset S$ be the homogeneous ideal of the canonical image of X. Let $I_d \subset S_d$ be the degree d parts of $I \subset S$.

Lemma 4.1. *Let $f \in S_d$. If $f(w_1, \dots, w_g) \in K[[q]]$ vanishes at $q = 0$ to order $> d(2g-2)/[K : \mathbb{Q}]$, then the corresponding section of $(\Omega^1)^{\otimes d}$ is 0.*

Proof. The section has more than $d(2g-2) = \deg(\Omega^1)^{\otimes d}$ geometric zeros in total (at P and its conjugates), so it is 0. ☐

Corollary 4.2. *If $B > d(2g-2)/[K : \mathbb{Q}]$, then from the input as in Theorem 3.1 one can compute a basis for I_d.*

Proof. By Lemma 4.1, I_d is the kernel of the $\mathbb{Q}$-linear map $S_d \to K[[q]]/(q^B)$ sending each monomial to its truncated expansion. ☐

Lemma 4.3. *The dimension of I_2 is $\binom{g-1}{2}$ if X is hyperelliptic, and $\binom{g-2}{2}$ if not.*

Proof. We may work over $\mathbb{C}$. Let $\mathbb{C}[x]_{\leq n}$ be the space of polynomials of degree at most n. In the hyperelliptic case, X is the smooth projective model of $y^2 = F(x)$ with $\deg F = 2g+1$, and $H^0(X, \Omega^1) = \mathbb{C}[x]_{\leq g-1} \frac{dx}{y}$ (see [ACGH85, p. 11], for example), so I_2 is isomorphic to the kernel of the surjective map $\ker(\mathrm{Sym}^2 \mathbb{C}[x]_{\leq g-1} \to \mathbb{C}[x]_{\leq 2g-2})$, so $\dim I_2 = g(g+1)/2 - (2g-1) = \binom{g-1}{2}$. In the nonhyperelliptic case, this follows from Max Noether's theorem [ACGH85, p. 117]. ☐

Lemma 4.4. *Let X be a hyperelliptic curve over $\mathbb{Q}$. Let L be a finite extension of $\mathbb{Q}$. Let $P' \in X(L)$. Suppose that $\omega'_1, \dots, \omega'_g$ is an L-basis for $\mathrm{H}^0(X_L, \Omega^1)$ such that $\mathrm{ord}_{P'}(\omega'_1) < \ldots < \mathrm{ord}_{P'}(\omega'_g)$. Let $t = \omega'_{g-1}/\omega'_g \in L(X)$. Then $t \in L(C)$ and is of degree 1 (as a rational function on C_L).*

Proof. We may assume that X_L is the smooth projective model of $y^2 = F(x)$ for some $F \in L[x]$, and P' is at infinity. Then for $i = 0, \dots, g-1$, we have $\omega'_{g-i} = J_i(x)\, dx/y$ for some $J_i(x) \in L[x]$ of degree exactly i. Then t is a degree 1 polynomial in $L[x]$. ☐

Lemma 4.5. *Let C be a genus 0 curve over $\mathbb{Q}$. Let $\mathcal{T}$ be the tangent bundle of C. Let $V := \mathrm{H}^0(C, \mathcal{T})$. Let L be a finite extension of $\mathbb{Q}$, with $\mathbb{Q}$-basis $\lambda_1, \dots, \lambda_\ell$. Let t be a degree 1 rational function on C_L.*

(a) *The meromorphic sections $\frac{d}{dt}, t\frac{d}{dt}, t^2\frac{d}{dt}$ of $\mathcal{T}$ form an L-basis of V_L.*
(b) *The elements $\mathrm{Tr}_{L/\mathbb{Q}}(\lambda_j t^i \frac{d}{dt})$ for $0 \leq i \leq 2$ and $1 \leq j \leq \ell$ span V.*

Proof.

(a) Without loss of generality, $C_L = \mathbb{P}^1$ and t is the standard coordinate. Then $\mathcal{T} \simeq \mathscr{O}(2)$, so $\dim V_L = 3$. Also, $\frac{d}{dt}$ has a double zero at ∞, so $\frac{d}{dt}, t\frac{d}{dt}, t^2\frac{d}{dt}$ are independent global sections.
(b) The map $\mathrm{Tr}_{L/\mathbb{Q}} \colon V_L \to V$ is surjective. ☐

18 Jun 2025 10:53:10 PDT
250124-vanBommel Version 2 - Submitted to LuCaNT

Lemma 4.6. *Let C be a smooth plane conic in $\mathbb{P}^2$ over a field k. Let $h \in k(C)$ be a rational function of degree d. Then h is given by a ratio of two homogeneous forms on $\mathbb{P}^2$ of degree $\lceil d/2 \rceil$.*

Proof. Let $L \in \operatorname{Div} C$ be a hyperplane section of $C \subset \mathbb{P}^2$. Write $(h) = (h)_0 - (h)_\infty$, where $(h)_0$ and $(h)_\infty$ are effective and of degree d. Then $\lceil d/2 \rceil L - (h)_\infty$ is of degree ≥ 0, so by Riemann–Roch there exists a section s of $\mathscr{O}_C(\lceil d/2 \rceil)$ vanishing at the poles of h. Then hs is another global section of $\mathscr{O}_C(\lceil d/2 \rceil)$. Both s and hs are restrictions of homogeneous forms on $\mathbb{P}^2$, and h is their ratio. $\square$

Lemma 4.7. *Let $\pi \colon X \to Y$ be a morphism of nice curves over $\mathbb{C}$. Let $P \in X(\mathbb{C})$. Let $Q = \pi(P)$. Let e be the ramification index of π at P. Let s be a nonzero meromorphic section of $(\Omega^1_Y)^{\otimes n}$ for some $n \in \mathbb{Z}$. Then $\operatorname{ord}_P(\pi^* s) = e \operatorname{ord}_Q s + n(e-1)$.*

Proof. Let t be a uniformizer at $\pi(P)$ on Y. For any $f \in \mathbb{Q}(Y)^\times$, we have $\operatorname{ord}_P(\pi^* f) = e \operatorname{ord}_Q(f)$ by definition, and $\operatorname{ord}_P(\pi^* dt) = e - 1$ as in the proof of the Hurwitz formula. Since $s = f\, dt^{\otimes n}$ for some $f \in \mathbb{Q}(Y)^\times$, the formula follows. $\square$

5. Proof of main theorem ignoring precision

We now start the proof of Theorem 3.1. Compute a basis for I_2 using Corollary 4.2 and apply Lemma 4.3 to test if X is hyperelliptic. If X is nonhyperelliptic, compute bases for I_2, I_3, I_4 using Corollary 4.2; these are enough to cut out $X \subset \mathbb{P}^{g-1}$, by Petri's theorem [Pet23]. *Henceforth, we assume that X is hyperelliptic.*

Steps (1)–(2) below require working over a field L such that X has an L-point P', so that there is an isomorphism $C_L \simeq \mathbb{P}^1_L$ such that P' maps to ∞. We choose L to be an isomorphic copy of K, and let $P' \in X(L)$ be the result of applying the isomorphism to $P \in X(K)$. (We will need to consider $(L \otimes K)/K$-traces, so keeping separate names for L and K will help clarify things.) We will need to take $L/\mathbb{Q}$-traces of elements of $\mathrm{H}^0(C_L, \mathcal{T}_L)$ as in Lemma 4.5 to get elements of $\mathrm{H}^0(C, \mathcal{T})$; these will be computed as $(L \otimes K)/K$-traces of their expansions at P (the tensor product is over $\mathbb{Q}$).

We first explain the algorithm as if we had $w_1, \ldots, w_g \in K[[q]]$ to infinite precision, and later in Section 6 explain what modifications are needed when we have only their truncations $\bar{w}_1, \ldots, \bar{w}_g$.

(1) (Find the expansion of a rational function $t \colon X_L \to C_L \simeq \mathbb{P}^1_L$.) Let $W \subset K[[q]]$ be the $\mathbb{Q}$-span of $w_1, \ldots, w_g$, and let $W_K \subset K[[q]]$ be their K-span. Run Gaussian elimination over K to find a new K-basis $w'_1, \ldots, w'_g$ of W_K such that $\operatorname{ord}_P(w'_1) < \cdots < \operatorname{ord}_P(w'_g)$. Let $M \in \mathrm{GL}_g(K)$ be the change-of-basis matrix sending $w_1, \ldots, w_g$ to $w'_1, \ldots, w'_g$. Applying the isomorphism $K \to L$ yields a matrix $M_L \in \mathrm{GL}_g(L)$. Then M_L sends $\omega_1, \ldots, \omega_g$ to an L-basis $\omega'_1, \ldots, \omega'_g$ of $\mathrm{H}^0(X_L, \Omega^1)$ as in Lemma 4.4. Computing the same L-linear combinations of $w_1, \ldots, w_g \in K[[q]]$ produces elements $w''_1, \ldots, w''_g \in L \otimes W \subset (L \otimes K)[[q]]$ representing the expansions at P of the ω'_i, which have increasing order of vanishing at P'.

Let $t = \omega'_{g-1}/\omega'_g \in L(X)$, as in Lemma 4.4, so t is the "x-coordinate" on a hyperelliptic model. Its expansion at P is in $(L \otimes K)((q))$.

(2) (Find expansions of a $\mathbb{Q}$-basis of $\mathrm{H}^0(C,\mathcal{T})$.) Let $\lambda_1,\dots,\lambda_\ell$ be a $\mathbb{Q}$-basis of L. The $L/\mathbb{Q}$-traces in Lemma 4.5(b) span $V := \mathrm{H}^0(C,\mathcal{T})$, so three of them form a $\mathbb{Q}$-basis of C. To calculate with them, we start with the expansions of $\lambda_j t^i \frac{d}{dt}$ in $(L\otimes K)((q))$ for $i=0,1,2$ and $j=1,\dots,\ell$, calculate $(L\otimes K)/K$-traces (traces are compatible with base change), and find three of them that are K-linearly independent and hence $\mathbb{Q}$-linearly dependent; call them $\partial_0,\partial_1,\partial_2 \in K((q))\frac{d}{dq}$; these are the expansions of a basis of global sections of $\mathcal{T}$ pulled back to X.

(3) (Find the equation $Q=0$ of the conic C.) There is a unique $Q\in\mathbb{Q}[a,b,c]_2$ up to scalar such that $Q(\partial_0,\partial_1,\partial_2)=0$ in $K((q))\left(\frac{d}{dq}\right)^2$. Then $Q=0$ is the anticanonical model of C in $\mathbb{P}^2$. We find Q by linear algebra.

(4) (Find the expansion of $h\in\mathbb{Q}(C)$ such that $\mathbb{Q}(X)=\mathbb{Q}(C)(\sqrt{h})$.) In this step, we compute $h\in\mathbb{Q}(C)$ such that $\mathbb{Q}(X)=\mathbb{Q}(C)(\sqrt{h})$. Let $f:=a/b$, viewed as a rational function on C; its expansion is ∂_0/∂_1. Let $y=df/\omega_1\in\mathbb{Q}(x)$ and $h=y^2$. The hyperelliptic involution fixes df and acts as -1 on $H^0(X,\Omega^1)$, so it negates y and fixes h; that is, $h\in\mathbb{Q}(C)$. Then $\mathbb{Q}(X)=\mathbb{Q}(C)(y)=\mathbb{Q}(C)(\sqrt{h})$.

(5) (Write h as a ratio of homogeneous forms.) We now show how to write h explicitly as F/G for some $F,G\in\mathbb{Q}[a,b,c]_{g+3}$. Since f is a rational function of degree 2 on C, it has at most 2 poles with multiplicity, so df on C has at most 4 poles with multiplicity (the worst case being when f has two simple poles), so its pullback to X has at most 8 poles. On the other hand, ω_1 has at most $2g-2$ zeros on X, so y has at most $2g+6$ poles on X. Then h has at most $2(2g+6)$ poles on X, so its degree on C is at most $2g+6$. By Lemma 4.6, there exist homogeneous forms $F,G\in\mathbb{Q}[a,b,c]_{g+3}$ such that $F/G=h$. To find the coefficients of possible F and G, we solve the linear system $F=hG$ in these unknown coefficients, using expansions of $\partial_0,\partial_1,\partial_2$ and h.

(6) (For even g, find an equation $y^2=f(x)$ for X.) Suppose that g is even. In this case, $C\simeq\mathbb{P}^1$, and we will describe a method to find a rational parametrization of C, following the strategy of Lemma 4.6. The 1-form ω_1 corresponds to a linear form on $\mathbb{P}^{g-1}$, which cuts out a divisor D of odd degree $g-1$ on C. Let $\mathcal{S}$ be the space of $S\in\mathbb{Q}[a,b,c]_{g/2}$ that vanish along D. By the Riemann–Roch theorem, $\dim\mathcal{S}=2$; we next seek an explicit basis of $\mathcal{S}$, which will define an isomorphism $C\to\mathbb{P}^1$. For each $S\in\mathcal{S}$ and for $j=2,\dots,g$, the element $R_j:=S\omega_j/\omega_1\in\mathbb{Q}(a,b,c)$ lies in $\mathbb{Q}[a,b,c]_{g/2}$ since S vanishes along D. Thus $\mathcal{S}$ is the projection on the last coordinate of the space $\mathcal{R}$ of g-tuples $(R_2,\dots,R_g,S)$ of polynomials in $\mathbb{Q}[a,b,c]_{g/2}$ such that

$$\omega_1 R_j = S\omega_j$$

for all $j=2,\dots,g$. Using the expansions of $a,b,c,\omega_1,\dots,\omega_g$ at P, we compute $\mathcal{R}$ by linear algebra. Thus we obtain an isomorphism $C\simeq\mathbb{P}^1$.

Under $C\simeq\mathbb{P}^1$, the function h corresponds to some $f\in\mathbb{Q}(x)^\times$. Now X is birational to the curve $y^2=f(x)$. Multiply f by a square to make it a polynomial. Remove square factors (by computing $\gcd(f,f')$, etc.) to make f separable. By Riemann–Hurwitz, $\deg f$ is $2g+1$ or $2g+2$.

(7) (For odd g, find H.) Now assume that g is odd. Let F, G be as in Step 5. We seek $H \in \mathbb{Q}[a,b,c]_{g+1}$ separable and $J \in \mathbb{Q}[a,b,c]_{(g+5)/2}$ such that $FG \equiv HJ^2 \pmod{Q}$; then the rational function $h = F/G$ equals HJ^2/G^2 on $C\colon Q = 0$, so the function field of the smooth projective curve $X' := \operatorname{Proj} \frac{\mathbb{Q}[a,b,c,y]}{(y^2-H,Q)}$ equals $\mathbb{Q}(C)(\sqrt{HJ^2/G^2}) = \mathbb{Q}(C)(\sqrt{h})$, so $X' \simeq X$; that is, H is as in the statement of the theorem. We cannot simply factor FG to find H and J, since $\mathbb{Q}[a,b,c]/(Q)$ is not a UFD. Instead we will decompose the zero locus $D := Z_C(FG) \in \operatorname{Div} C$ as $U + 2V$ with U, V effective divisors on C and U reduced. First, choose $p \in \mathbb{P}^2(\mathbb{Q})$ not on any line connecting geometric points in D and not on any line tangent to a geometric point in D; then the projection from p restricts to a morphism $\nu\colon C \to \mathbb{P}^1$ that is injective on the geometric points in D and unramified at those points. Write $\nu_* D = U' + 2V'$ with U', V' effective divisors on $\mathbb{P}^1$ and U' reduced, using factorization in the homogeneous coordinate ring of $\mathbb{P}^1$. Let $U = \nu^* U' \cap D$ and $V = \nu^* V' \cap D$; then $D = U + 2V$ by choice of ν. We have $\deg U = \deg U' = 2g+2$, so $\deg V = \deg V' = g+5$. By Riemann–Roch on C, an effective divisor of even degree $2d$ is the zero locus of a form in $\mathbb{Q}[a,b,c]_d$, unique up to scalar and modulo multiples of Q; in particular, there exist $H \in \mathbb{Q}[a,b,c]_{g+1}$ and $J \in \mathbb{Q}[a,b,c]_{(g+5)/2}$ with $Z_C(H) = U$ and $Z_C(J) = V$; we find explicit H and J by linear algebra. Then $FG \equiv \alpha HJ^2 \pmod{Q}$ for some $\alpha \in \mathbb{Q}^\times$. Evaluate F, G, H, J at some zero of Q in $\overline{\mathbb{Q}}^3$ to find α, and replace H by αH to get $FG \equiv HJ^2 \pmod{Q}$.

If a rational point on C is given, projection from it defines an isomorphism $C \to \mathbb{P}^1$. Find an equation $y^2 = f(x)$ for X as in the last paragraph of (6).

6. Precision analysis

Object	Space	ord_P	Absolute error	Relative error
ω_j	$\mathrm{H}^0(X, \Omega^1)$	$[0, 2g-2]$	$+O(q^B)\,dq$	$\cdot(1 + O(q^{B-2g+2}))$
ω'_j	$\mathrm{H}^0(X_L, \Omega^1)$	$[0, 2g-2]$	$+O(q^B)\,dq$	$\cdot(1 + O(q^{B-2g+2}))$
t	$L(C)$	$[-2, 2]$	$+O(q^{B-2g})$	$\cdot(1 + O(q^{B-2g+2}))$
dt	$(\Omega^1_{C_L})_{\eta_{C_L}}$	$[-3, 1]$	$+O(q^{B-2g-1})\,dq$	$\cdot(1 + O(q^{B-2g-2}))$
$t^i \frac{d}{dt}$	$\mathrm{H}^0(C_L, \mathcal{T})$	$[-1, 3]$	$+O(q^{B-2g-3})\,\frac{d}{dq}$	$\cdot(1 + O(q^{B-2g-2}))$
∂_i	$\mathrm{H}^0(C, \mathcal{T})$	$[-1, 3]$	$+O(q^{B-2g-3})\,\frac{d}{dq}$	$\cdot(1 + O(q^{B-2g-6}))$
$M(\partial_0, \partial_1, \partial_2)$	$\mathrm{H}^0(C, \mathcal{T}^d)$	$[-d, 3d]$	$+O(q^{B-2g-d-2})\,\left(\frac{d}{dq}\right)^d$	$\cdot(1 + O(q^{B-2g-4d-2}))$
f	$\mathbb{Q}(C)$	$[-4, 4]$	$+O(q^{B-2g-10})$	$\cdot(1 + O(q^{B-2g-6}))$
df	$(\Omega^1_C)_{\eta_C}$	$[-5, 5]$	$+O(q^{B-2g-11})\,dq$	$\cdot(1 + O(q^{B-2g-16}))$
y	$\mathbb{Q}(X)$	$[-2g-3, 5]$	$+O(q^{B-4g-19})$	$\cdot(1 + O(q^{B-2g-16}))$
h	$\mathbb{Q}(C)$	$[-4g-6, 10]$	$+O(q^{B-6g-22})$	$\cdot(1 + O(q^{B-2g-16}))$
hG	$\mathcal{T}^{g+3}_{\eta_C}$	$[-5g-9, 3g+19]$	$+O(q^{B-11g-23})\,\left(\frac{d}{dq}\right)^{g+3}$	$\cdot(1 + O(q^{B-6g-14}))$
$F - hG$	$\mathcal{T}^{g+3}_{\eta_C}$		$+O(q^{B-11g-23})\,\left(\frac{d}{dq}\right)^{g+3}$	
$\omega_1 R_j,\ S\omega_j$	$\mathrm{H}^0(X, \Omega^1_X \otimes \pi^* \mathcal{T}^{\frac{g}{2}})$	$[-g/2, 7g/2-2]$	$+O(q^{B-9g/2-2})\,\left(\frac{d}{dq}\right)^{\frac{g}{2}-1}$	$\cdot(1 + O(q^{B-4g-2}))$

TABLE 1. Tracking q-adic precision of objects in the proof of the main theorem.

In Section 5, we assumed that $w_1, \dots, w_g \in K[[q]]$ were given to infinite precision. Now, in Table 1, we track how much precision we have in the steps if we start only with $w_1, \dots, w_g$ up to addition of $O(q^B)$. For each Laurent series, we bound both absolute error (addition of $O(q^n)$ for some n) and relative error (multiplication by $1 + O(q^n)$ for some n); we can pass between them if the valuation of a power series is controlled; these valuations lie in the range given in the ord_P column of Table 1. For series with coefficients in the étale algebra $L \otimes K$, the bounds apply when projected onto any field factor of $L \otimes K$. Let η_C be the generic point of C, so the stalk $(\Omega^1_C)_{\eta_C}$ is the space of meromorphic 1-forms on C. Define η_{C_L} similarly.

Lemma 6.1. *Table 1 is correct.*

Proof. Each ω_j is regular and has $2g-2$ zeros in total, so $\operatorname{ord}_P(\omega_j) \in [0, 2g-2]$. It is given to absolute error $O(q^B)\,dq$. The ω'_j are L-linear combinations of the ω_j, so they have the same absolute error. Since each ω_j and ω'_j vanishes at P to order at most $2g-2$, their relative error is $1 + O(q^{B-2g+2})$ (as usual, big-O notation allows for the possibility that the error could be smaller than specified).

Now $t = \omega'_{g-1}/\omega'_g$, so its relative error is again $1 + O(q^{B-2g+2})$. On the other hand, t is the "x-coordinate" of a hyperelliptic model of X, so $\operatorname{ord}_P(t) \in [-2, 2]$. Since $\operatorname{ord}_P t \geq -2$, the absolute error of t is $O(q^{B-2g})$.

The absolute error of dt is then $O(q^{B-2g-1})\,dq$. Again since t is the "x-coordinate" of a hyperelliptic model of X, we have $\operatorname{ord}_P(dt) \in [-3, 1]$. Since $\operatorname{ord}_P(dt) \leq 1$, the relative error of dt is $1 + O(q^{B-2g-2})$.

Fix $i \in \{0, 1, 2\}$. The relative error of $t^i \frac{d}{dt}$ is the worse of the relative errors of t and dt, which is $1 + O(q^{B-2g-2})$. The section $t^i \frac{d}{dt}$ is regular on C, with 2 zeros, so $\operatorname{ord}_{\pi(P)}(t^i \frac{d}{dt}) \in [0, 2]$, so $\operatorname{ord}_P(t^i \frac{d}{dt})$ is in $[0, 2]$ or $-1 + 2[0, 2] = [-1, 3]$ according to whether π is unramified or ramified at P, by Lemma 4.7 applied with $n = -1$. Since $\operatorname{ord}_P(t^i \frac{d}{dt}) \geq -1$, the absolute error of $t^i \frac{d}{dt}$ is $O(q^{B-2g-3})\,\frac{d}{dq}$.

The ∂_i are linear combinations of the $t^i \frac{d}{dt}$, so they have the same absolute error $O(q^{B-2g-3})\,\frac{d}{dq}$. As for $t^i \frac{d}{dt}$, we have $\operatorname{ord}_P(\partial_i) \in [-1, 3]$. Since $\operatorname{ord}_P(\partial_i) \leq 3$, the relative error of ∂_i is $1 + O(q^{B-2g-6})$.

We will need to analyze the error in $M(\partial_0, \partial_1, \partial_2)$ for various nonzero forms $M \in \mathrm{H}^0(\mathbb{P}^2, \mathscr{O}(d)) = \mathbb{Q}[a, b, c]_d$, for various $d \geq 1$, so we do a calculation for all of these at once, and later specialize to the particular M we need. Its order of vanishing at $\pi(P)$ is in $[0, 2d]$, since C is a curve of degree 2 in $\mathbb{P}^2$. Then its order of vanishing at P is in $[0, 2d]$ or $-d + 2[0, 2d] = [-d, 3d]$, according to whether π is unramified or ramified at P, by Lemma 4.7 applied with $n = -d$. If M is a monomial, then the absolute error of $M(\partial_0, \partial_1, \partial_2)$ is at worst that of one ∂_i minus $d - 1$ (because all the ∂_j in the monomial have at worst a simple pole), hence at worst $O(q^{B-2g-d-2})\left(\frac{d}{dq}\right)^d$. Since $\operatorname{ord}_P(M(\partial_0, \partial_1, \partial_2)) \leq 3d$, the relative error is at worst $1 + O(q^{B-2g-4d-2})$.

The rational function $f := a/b$ is of degree 2 on C, and the ramification index of π at P is at most 2, so $\operatorname{ord}_P(f) \in [-4, 4]$. Its relative error is the same as that of $a = \partial_0$ and $b = \partial_1$, which is $1 + O(q^{B-2g-6})$. Since $\operatorname{ord}_P(f) \geq -4$, its absolute error is $O(q^{B-2g-10})$.

Then $\operatorname{ord}_P(df) \geq \operatorname{ord}_P(f) - 1 \geq -5$. Since f on C has at most 2 poles with multiplicity, df on C has at most 4 poles with multiplicity, but the divisor of df on C has degree -2, so df has at most 2 zeros on C, so $\operatorname{ord}_P(df) \leq 2 \cdot 2 + 1 = 5$, the worst case being if π is ramified at P. The absolute error of df is $O(q^{B-2g-11})$, so the relative error is $1+O(q^{B-2g-16})$.

Since $\operatorname{ord}_P(df) \in [-5,5]$ and $\operatorname{ord}_P(\omega_1) \in [0, 2g-2]$, we have $\operatorname{ord}_P(y) = \operatorname{ord}_P(df/\omega_1) \in [-2g-3, 5]$. The relative error of y is the worse of the relative errors of df and ω_1, which is $1+O(q^{B-2g-16})$. Then the absolute error of y is $O(q^{B-4g-19})$.

Squaring gives $\operatorname{ord}_P(h) \in 2[-2g-3,5] = [-4g-6, 10]$, and h has relative error $1+O(q^{B-2g-16})$ and absolute error $1+O(q^{B-6g-22})$.

For hG, we compute ord_P and the relative error from the corresponding numbers for h and $M := G$ of degree $d = g+3$. Since $\operatorname{ord}_P(hG) \geq -5g-9$, the absolute error is then $O(q^{(B-6g-14)+(-5g-9)}) \left(\frac{d}{dq}\right)^{g+3} = O(q^{B-11g-23}) \left(\frac{d}{dq}\right)^{g+3}$. The absolute error for F, from the $M(\partial_0, \partial_1, \partial_2)$ row with $d = g+3$, is $O(q^{B-2g-(g+3)-2}) \left(\frac{d}{dq}\right)^{g+3}$. Combining these gives $F - hG$ with absolute error $O(q^{B-11g-23}) \left(\frac{d}{dq}\right)^{g+3}$. (We do not need the ord_P and relative error of $F - hG$.)

The calculations for $\omega_1 R_j$ and $S\omega_j$ are analogous to those for hG. $\square$

Lemma 6.2. *If $B \geq 19g+48$, then we can perform Steps 1–6 in the proof of Theorem 3.1.* (*Step 7 does not involve expansions; it is carried out exactly.*)

Proof. In Step 3, Q is determined by $Q(\partial_0, \partial_1, \partial_2) \bmod q^7$ because when $M \in \mathrm{H}^0(\mathbb{P}^2, \mathscr{O}(2))$, we have $\operatorname{ord}_P M(\partial_0, \partial_1, \partial_2) \leq 6$. We computed $Q(\partial_0, \partial_1, \partial_2)$ to absolute error $O(q^{B-2g-d-2}) \left(\frac{d}{dq}\right)^{d}$ with $d = 2$, which is good enough since $B - 2g - 2 - 2 \geq 7$.

Let $(h)_\infty$ be the polar part of the divisor of h, which has degree at most $2g+6$ as explained in Step 5. For any $F, G \in \mathbb{Q}[a,b,c]_{g+3}$, the expression $F - hG$ is a global section of $\mathcal{T}^{g+3} \otimes \mathscr{O}_C((h)_\infty)$, which is a line bundle of degree at most $2(g+3) + (2g+6) = 4g+12$. The pullback of this bundle to X has degree at most $2(4g+12) = 8g+24$. Thus, if $\operatorname{ord}_P(F - hG) > 8g+24$, then $F - hG = 0$. In other words, it suffices to do the linear algebra in Step 5 to absolute precision $+O(q^{8g+25}) \left(\frac{d}{dq}\right)^{g+3}$. By Table 1, we have this precision if $B - 11g - 23 \geq 8g + 25$, or, equivalently, $B \geq 19g + 48$.

The degree of $\Omega^1_X \otimes \pi^* \mathcal{T}^{g/2}$ on X is $2g-2+2\cdot 2(g/2) = 4g-2$, so if $\operatorname{ord}_P(\omega_1 R_j - S\omega_j) > 4g-2$, then $\omega_1 R_j - S\omega_j = 0$. In other words, it suffices to do the linear algebra in Step 6 to absolute precision $+O(q^{4g-1}) \left(\frac{d}{dq}\right)^{g/2-1}$. By Table 1, we have this precision if $B - 9g/2 - 2 \geq 4g - 1$, or, equivalently, $B \geq 17g/2 + 1$. $\square$

Remark 6.3. In each of the models found, we have the expansions at P of the new coordinate functions, as Laurent series in q, so we can find the coordinates of P in the new model. Similarly, by linear algebra we can express $\omega_1, \ldots, \omega_g$ in terms of the new coordinates, if desired.

Remark 6.4. The genus of a modular curve with geometric gonality 2 is at most 17 [BGGP05, Remark 4.5]. So, in running the algorithm of Theorem 3.1 on hyperelliptic modular curves, we always have $g \leq 17$.

Acknowledgments

We thank David Roe for his comments on early versions of the algorithm of this article. His computations using our algorithm were essential in helping us debug and improve it. We thank the anonymous referees for corrections and suggestions.

Van Bommel, Costa, and Poonen were supported by Simons Foundation grant 550033. Van Bommel was additionally supported by Céline Maistret's Royal Society Dorothy Hodgkin Fellowship. Costa was additionally supported by Simons Foundation grant SFI-MPS-Infrastructure-00008651. Poonen was partially supported also by National Science Foundation grant DMS-2101040 and Simons Foundation grant 402472. Srinivasan was supported by National Science Foundation grant DMS-2401547 and Simons Foundation grant 546235.

References

[ACGH85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. "Geometry of algebraic curves. Vol. I". Vol. 267. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, New York, 1985, pp. xvi+386 (↑ 3).

[BGGP05] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen. "Finiteness results for modular curves of genus at least 2". In: *Amer. J. Math.* 127.6 (2005), pp. 1325–1387 (↑ 1, 8).

[Bar14] Burcu Baran. "An exceptional isomorphism between modular curves of level 13". In: *J. Number Theory* 145 (2014), pp. 273–300 (↑ 1).

[LMFDB] The LMFDB Collaboration. "The L-functions and modular forms database". `https://www.lmfdb.org`. [Online; accessed 23 January 2025]. 2025 (↑ 2).

[MS20] Pietro Mercuri and René Schoof. "Modular forms invariant under non-split Cartan subgroups". In: *Math. Comp.* 89.324 (2020), pp. 1969–1991 (↑ 1).

[Pet23] K. Petri. "Über die invariante Darstellung algebraischer Funktionen einer Veränderlichen". In: *Math. Ann.* 88.3-4 (1923), pp. 242–289 (↑ 4).

[Shi10] Goro Shimura. "Arithmetic of quadratic forms". Springer Monographs in Mathematics. Springer, New York, 2010, pp. xii+237 (↑ 2).

[Zyw24] David Zywina. "Explicit open images for elliptic curves over $\mathbb{Q}$". In: *preprint* (2024). `arXiv:2206.14959` (↑ 1).

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

School of Mathematics, University of Bristol, Fry Building, Woodland Road, Bristol, BS8 1UG, UK
Email address: r.vanbommel@bristol.ac.uk
URL: https://raymondvanbommel.nl/

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
Email address: edgarc@mit.edu
URL: https://edgarcosta.org

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
Email address: poonen@math.mit.edu
URL: https://math.mit.edu/~poonen/

Boston University, 665 Commonwealth Avenue, Boston, MA 02215, USA
Email address: padmask@bu.edu
URL: https://padmask.github.io/