THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth
Algorithmic Number Theory Symposium

Fast computation of isomorphisms of hyperelliptic curves and explicit Galois descent

Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling

msp

THE OPEN BOOK SERIES **1** (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.463

Fast computation of isomorphisms of hyperelliptic curves and explicit Galois descent

Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling

We show how to speed up the computation of isomorphisms of hyperelliptic curves by using covariants. We also obtain new theoretical and practical results concerning models of these curves over their field of moduli.

1. Introduction

Let X_1 and X_2 be two curves of genus $g \geq 2$ over a field k. We wish to quickly determine the (possibly empty) set of isomorphisms between them. The standard strategy mainly consists of interpolating the isomorphisms at Weierstrass or small degree places, depending on whether the characteristic of the field is zero or positive [17]. This yields algorithms of complexity at least $O(g^6)$ in general, and at least $O(g^2)$ even in very favorable cases.

In this article we restrict to hyperelliptic curves with equations $X_i : y^2 = f_i(x)$ over a field k of characteristic different from 2. The issue can then be rephrased in terms of isomorphisms of degree $2g+2$ polynomials under the Möbius action of $\mathrm{GL}_2(k)$ (see Section 2E1). Our first contribution is to show how to compute the set of isomorphisms in a much faster way by combining two new ideas. The first one uses the factorization of the Möbius action into a diagonal matrix times a second matrix whose diagonal coefficients are equal to 1. This idea allows us to perform the computation of the isomorphisms with only univariate polynomial calculations (see Section 2B). The second idea relies on a classical generalization of invariants, called *covariants* (see Section 2C). Using covariants, we can reduce our search for an isomorphism between f_1 and f_2 to the search for an isomorphism between polynomials of lower degree. This gives us an algorithm for generic hyperelliptic curves whose complexity is quasilinear in g (see Section 2D). In

MSC2010: primary 13A50; secondary 14Q05, 14H10, 14H25.
Keywords: invariants, covariants, hyperelliptic curves, binary forms, Galois descent, isomorphism, moduli, algorithm.

the genus-2 and genus-3 cases, we analyze the small locus of curves where our strategy fails (see Section 2E2). The use of covariants was inspired by work of van Rijnswou [30], who used covariants, along with a miraculous isomorphism from representation theory, to generically reduce the isomorphism question for ternary quartics to that for binary quartics.

In a related direction, thanks to covariants, we get both theoretical and practical results on Galois descent of hyperelliptic curves over their field of moduli. As the terminology suggests, this issue is related to moduli spaces, namely as follows.

The use of invariants allows the construction of the coarse moduli space of smooth curves admitting a suitable representation (for example, hyperelliptic or planar) as a geometric quotient in the sense of Mumford [28]. Such quotients have been calculated explicitly; for instance, for genus-2 and genus-3 hyperelliptic curves, see [21; 34]. Given a field k, the k-points of these quotients correspond to curves whose field of moduli, in the sense of Definition 3.1, is equal to k (up to a possible purely inseparable extension). This statement is probably well-known, but we could not find it in the literature; therefore, we give the link between these two definitions in Section 3.

A natural question is to determine when a curve descends to its field of moduli, that is, when its field of moduli is also a field of definition (and hence the smallest possible field of definition, under inclusion). Examples of curves that do not so descend were constructed by Shimura [33] and Earle [12], among others. However, curves of genus at most 1 always descend to their field of moduli, and models over the field of moduli can be explicitly constructed. Moreover, in the genus-2 case, although an obstruction to the descent may exist, as is shown in [26] and [7], the question of explicit descent to the field of moduli is solved. One of our aims is to obtain similar results in the general hyperelliptic case.

Many theoretical results for the general case can be found in [18]. In practice, though, computing an explicit model of a given curve over its field of moduli can be a very hard task, as we explain in Section 3B1. Indeed, for a given *finite* Galois extension, Weil's criterion in [35] often leads to a computational answer; the main difficulty in our context is to work out the finite Galois extension over which a descent isomorphism is defined. As far as we know, there is no easy general way to find this extension, except when k is finite or when the geometric automorphism group of the curve is trivial. Moreover, for hyperelliptic curves there is a refinement of the descent question — namely, to ask for a descent to a model of the form $y^2 = f(x)$ — and this introduces additional difficulties.

The "magic" of the covariant method is to reduce the descent problem to lower genus, where a solution may be easier to determine (Theorem 3.8). In the genus-1 case, for example, there is always an explicit model over the field of moduli and we can quickly determine a descent isomorphism to this model, thanks to the first part of our work. It turns out that in suitable cases, this descent induces a descent of the original hyperelliptic curve to its field of moduli.

We illustrate this descent to the field of moduli for genus-3 hyperelliptic curves with automorphism group $(\mathbb{Z}/2\mathbb{Z})^3$, a case which remained unsolved in [25]; see Section 3C1. We also look at the case of genus-3 hyperelliptic curves with automorphism group $(\mathbb{Z}/2\mathbb{Z})^2$; in this case the field of moduli is not always a field of definition, and we prove that we can always find a model over an at most quadratic extension of the field of moduli. Finally, in Section 3D we show that our method can be used to descend families of curves with the example of a 3-dimensional family of genus-5 hyperelliptic curves from [13].

We stress that we are merely beginning to exploit the full strength of these new ideas. An article on nonhyperelliptic curves is in progress. We are also developing a general version of van Rijnswou's algorithms that is much more effective over finite fields and number fields. Finally, we seek to obtain new theoretical and practical descent results by analyzing the influence of twists on covariants.

We have implemented our algorithms in Magma [3]; the resulting programs, together with other useful scripts and output that was too large to include in this paper, may be found at

http://perso.univ-rennes1.fr/christophe.ritzenthaler/programme/hyp-desc.tgz

Notation. In the following, k denotes a field of characteristic p (prime or 0) with algebraic closure K. Hyperelliptic curves are additionally assumed to be smooth, so that when a singular affine model of a curve is given, we actually consider its desingularization. Unless noted otherwise, (iso)morphisms are defined over the base field k. We use the following notation for groups: $\boldsymbol{C}_n = \mathbb{Z}/n\mathbb{Z}$; $\boldsymbol{D}_{2n}$ is the dihedral group with $2n$ elements; $\boldsymbol{U}_6$ is the group with 24 elements defined by $\langle S, T\rangle$ with $S^{12} = T^2 = 1$ and $TST = S^5$; $\boldsymbol{V}_8$ is the group with 32 elements defined by $\langle S, T\rangle$ with $S^4 = T^8 = (ST)^2 = (S^{-1}T)^2 = 1$; $\boldsymbol{S}_n$ is the symmetric group over n symbols. Finally, if f_1 and f_2 are polynomials or matrices or some other such objects over a field k, we will write $f_1 \sim f_2$ if there exists $\lambda \in k^*$ such that $f_1 = \lambda \cdot f_2$.

2. Isomorphisms between forms and hyperelliptic curves

2A. ***Isomorphisms of binary forms.*** Let $n \geq 1$ be an integer, let $V = k^2$ be the k-vector space with basis (x, z), and let $S^n(V)$ be the $(n+1)$-dimensional vector space of homogeneous forms $\sum_{i=0}^{n} a_i x^i z^{n-i}$ of degree n in (x, z). In the sequel, we call an element of $S^n(V)$ a (*binary*) *form*. When $n = 0$, we let $S^0(V) = k$. Let G be a subgroup of $\mathrm{GL}_2(k)$ and let M be an element of G. If f is a form in $S^n(V)$, we define $M.f$ by $(M.f)(x, z) = f(M^{-1}(x, z))$, where the action of a matrix on (x, z) is the standard action on ${}^t(x, z)$.

Definition 2.1. Let f_1, f_2 be forms of degree $n \geq 1$ over a field k. We denote by $\operatorname{Isom}(f_1, f_2) \subset \mathrm{PGL}_2(k)$ the set of matrices M up to scalar equivalence such that $M.f_1 \sim f_2$. Additionally, we write $\operatorname{Aut} f_1$ for $\operatorname{Isom}(f_1, f_1)$.

If $\operatorname{Isom}(f_1, f_2) \neq \varnothing$, this set is a principal homogeneous space over $\operatorname{Aut} f_1$. In particular, $\operatorname{Isom}(f_1, f_2) = M \operatorname{Aut} f_1$ for any $M \in \operatorname{Isom}(f_1, f_2)$.

Let f be a form of degree n over k. Over K, we can write $f = \prod_{i=1}^{s}(\alpha_i x - \beta_i z)^{n_i}$, where $(\alpha_i, \beta_i) \in K^2 \setminus \{(0,0)\}$ and $n_i \in \mathbb{N}$. We associate to such a form its squarefree part $\widetilde{f} = \prod_{i=1}^{s}(\alpha_i x - \beta_i z)$, which is defined up to a multiplicative constant. The action of M on f reflects the classical Möbius action of $\mathrm{PGL}_2(K)$ on the roots $(\alpha_i : \beta_i) \in \mathbb{P}^1_K$ of f. In particular, two forms of the same degree are K-isomorphic if and only if there exists an $M \in \mathrm{GL}_2(K)$ mapping the roots of the first form to the roots of the second form (counting multiplicities). Hence we have:

Lemma 2.2. *The group* $\operatorname{Aut}_K f$ *is finite if and only if* $s \geq 3$, *that is, if and only if* $\deg \widetilde{f} \geq 3$. *Moreover*, $\operatorname{Aut}_K f \subset \operatorname{Aut}_K \widetilde{f}$.

2B. *The direct approach.* The classical method to compute isomorphisms between two binary forms f_1, f_2 of degree n over a field k is to find a $\mathrm{PGL}_2(k)$-transformation of $\mathbb{P}^1$ which maps the roots of the first form to the root of the second form. The most time-consuming task is to compute an isomorphism between the splitting fields of f_1 and f_2. Even in the most favorable case, where k is a finite field, the fastest algorithms need at least $O(n^{2,5+o(1)})$ operations in k (see [22]).

We show here that it is actually possible to get rid of this cumbersome ring isomorphism computation, and describe an algorithm of time complexity only quasilinear in n. This algorithm takes as input binary forms $f_1 = \sum_i A_i x^i z^{n-i}$ and $f_2 = \sum_i B_i x^i z^{n-i}$ of equal degree $n \geq 3$, each having at least three distinct roots. It returns matrices representing the elements of $\operatorname{Isom}(f_1, f_2)$.

First, we suppose that the coefficient A_{n-1} is equal to zero. Note that this is typically not a big restriction, since we may apply linear transformations to f_1. A notable exception is when p divides n. We therefore assume that p is prime to n.

Second, we note that determining $\operatorname{Isom}(f_1, f_2)$ is equivalent to determining the matrices $M = (m_{i,j}) \in \mathrm{GL}_2(k)$ such that

$$f_2(m_{11}x + m_{12}z, m_{21}x + m_{22}z) = \lambda f_1(x, z) \quad \text{for some } \lambda \in k^*. \tag{1}$$

Third, because of homogeneity, we may suppose that the λ in (1) equals 1, after enlarging k by a radical extension if necessary. Note that though this radical extension is *a priori* unknown, the details of the algorithm below will show how it can be determined.

Finally, we may suppose that the M in (1) are of the form

$$M = \begin{bmatrix} 1/\alpha & \beta/\delta \\ \gamma/\alpha & 1/\delta \end{bmatrix}.$$

Of course this may not be true, because a zero may occur on the diagonal of one of these M. However, one can fix this situation by applying a suitable change of variables to f_2.

The equation $f_2(m_{11}x + m_{12}z, m_{21}x + m_{22}z) = f_1(x, z)$ now becomes

$$f_2(x + \beta z, \gamma x + z) = f_1(\alpha x, \delta z).$$

Equating the coefficients of x^n in both sides of this equation yields $A_n \alpha^n = f_2(1, \gamma)$, and we can write α^n in terms of γ. Similarly, the equality of the coefficients of $x^{n-1}z$,

$$\beta \frac{\partial f_2}{\partial x}(1, \gamma) + \frac{\partial f_2}{\partial z}(1, \gamma) = 0,$$

enables us to write β in term of γ too. More generally, equating the coefficients of $x^{n-i}z^i$ for $i = 2, \dots, n$, where we substitute α^n and β in term of γ, yields $n - 1$ equations of the form

$$A_n \left(\sum_{j=0}^{i} \binom{i}{j} \left(-\frac{\partial f_2}{\partial z} \right)^j \left(\frac{\partial f_2}{\partial x} \right)^{i-j} \frac{\partial^i f_2}{\partial x^j \partial z^{i-j}} \right)(1, \gamma) \\ = i! \left(\frac{\partial f_2}{\partial x}(1, \gamma) \right)^i \left(\frac{\delta}{\alpha} \right)^i f_2(1, \gamma). \quad (2)$$

Note that the left-hand side of (2) is actually a polynomial multiple of $f_2(x, z)$, and we can divide both sides by $f_2(1, \gamma)$ — see [16, Chapter 1, §§15–16] for an elegant explanation. This yields equations of degree $i(n-2)$ in γ for the left side and of degree $i(n-1)$ in γ and degree i in δ/α on the right side.

Now, dividing the square of (2) specialized at $i = 3$ by the cube of (2) specialized at $i = 2$ allows to eliminate, up to some constant, the right-hand side of these equations, in particular the unknown δ/α. We end up with an equation of degree $6(n-2)$ in γ. Similarly, when $n > 3$, dividing (2) specialized at $i = 4$ by the square of (2) specialized at $i = 2$ yields an equation of degree $4(n-2)$ in γ. Taking the gcd, we obtain a polynomial of low degree with root γ. Generically, this gcd is of degree 1.

Under the assumptions made, the algorithm is therefore straightforward. For each possible γ, we compute α, β and δ and check whether the resulting matrix is in $\mathrm{Isom}(f_1, f_2)$.

The computations involved in this algorithm (taking gcds of polynomials of degree $O(n)$, taking n-th roots, and so forth) are all of time complexity quasilinear in n.

We have implemented the algorithm in Magma (version 2.18-2) and have timed the resulting procedure, `IsGL2EquivFast`, on a laptop (based on an Intel Core i7 M620 2.67GHz processor) for irreducible forms of increasing degree, the most

	Computations over $\mathbb{F}_{10007}$			Computations over $\mathbb{Q}$		
Genus	Old	Section 2B	Section 2D	Old	Section 2B	Section 2D
1	0.0	0.0	0.0	0.0	0.0	0.0
2	0.0	0.0	0.0	0.0	0.0	0.0
4	0.0	0.0	0.0	0.4	0.0	0.0
8	0.0	0.0	0.0	15	0.0	0.0
16	0.1	0.0	0.0	1150	0.1	0.0
32	0.2	0.0	0.0	—	0.2	0.0
64	0.9	0.1	0.0	—	0.6	0.0
128	6.5	0.6	0.0	—	3	0.2
256	39	3.7	0.1	—	30	0.6
512	242	25	0.5	—	382	3.4
1024	1560	165	2.5	—	5850	7

Table 1. Timings (in seconds) for isomorphisms between forms of degree $2g+2$, over $\mathbb{F}_{10007}$ and over $\mathbb{Q}$. The columns labeled "Old" give timings for Magma's built-in function `IsGL2Equivalent`; the columns labeled "Section 2B" give timings for the function `IsGL2EquivFast` described in Section 2B; and the columns labeled "Section 2D" give timings for the function `IsGL2EquivCovariant` described in Section 2D. Entries of "—" indicate computations that were aborted after an hour.

favorable case for the native Magma routine `IsGL2Equivalent`. We compare with `IsGL2Equivalent`, which implements the classical method, first over the finite field $\mathbb{F}_{10007}$, then over the rationals with coefficients bounded by ±2. The results are in Table 1. (See Section 2D for the definition of `IsGL2EquivCovariant`.)

As concluding remarks, we note first of all that this algorithm is equally suitable for determining K-isomorphisms. Moreover, in the special case of binary quartics, it is just as efficient as the algorithm given in [8].

2C. *The covariant approach.*

Let k be an infinite field of characteristic p and let $n > 1$ be an integer.

Definition 2.3. Let $r \geq 0$ be an integer. A homogeneous polynomial function $C : S^n(V) \to S^r(V)$ of degree d is a *covariant* if there exists $\omega \in \mathbb{Z}$ such that, for all $M \in G$ and all $f \in S^n(V)$, we have

$$C(M.f) = (\det M)^{-\omega} \cdot M.C(f).$$

When $r = 0$, such a C is called a (relative) *invariant* and is denoted by I.

The integer r is called the *order* of the covariant. If $nd - r$ is odd, the covariant is necessarily zero. Otherwise the integer ω is unique, and is called the *weight* of the covariant. It is equal to $(nd - r)/2$. In the sequel, we often identify C

with $C(f)$ for a general form $f \in F(a_0, \ldots, a_n)[x, z]$, where F is the prime field of k. For instance, the identity function $S^n(V) \to S^n(V)$ is a covariant of degree 1 and order n that we identify with f itself.

Remark 2.4. The determinant factor prevents the addition of covariants of different weights when $G = \mathrm{GL}_2(K)$. Hence one generally studies the graded algebra $\mathscr{C}_n$ of covariants and $\mathscr{I}_n$ of invariants under the action of $\mathrm{SL}_2(K)$. It is easy to see that the homogeneous elements of $\mathscr{C}_n$ and $\mathscr{I}_n$ are actually all the covariants or invariants under the action of $\mathrm{GL}_2(K)$. Despite this ambiguity, in the rest of the article we work with $G = \mathrm{GL}_2(K)$ instead of $\mathrm{SL}_2(K)$ because, in practice, this choice often allows us to avoid a quadratic extension of k when looking for an isomorphism M between two forms.

There is a large literature on how to generate invariants and covariants starting from f. Gordan's algorithm [15] allows to find a set of generators for the algebras $\mathscr{C}_n$ and $\mathscr{I}_n$ thanks to the use of certain differential operators, called *h-transvectants* and defined as follows. Given two covariants C_1, C_2 of degree d_1, d_2 and of order r_1, r_2, and given an integer $h \geq 1$, we can create a new covariant denoted $(C_1, C_2)_h$ and usually defined as [29, p. 88]

$$\frac{(r_1-h)!(r_2-h)!}{r_1!r_2!} \sum_{i=0}^{h} (-1)^i \binom{h}{i} \frac{\partial^h C_1}{\partial x^{h-i} \partial z^i} \frac{\partial^h C_2}{\partial x^i \partial z^{h-i}}.$$

In practice, we use the univariate counterpart. Looking at C_1, C_2 as univariate polynomials in x/z, we get [29, Theorem 5.6]

$$h! \frac{(r_1-h)!(r_2-h)!}{r_1!r_2!} \sum_{i=0}^{h} (-1)^i \binom{r_1-i}{h-i} \binom{r_2-h+i}{i} \frac{d^{h-i} C_1}{dx^{h-i}} \frac{d^i C_2}{dx^i}. \tag{3}$$

Effective methods for computing sets of generators when $K = \mathbb{C}$ have been worked out for n up to 10 (see [11; 14; 10; 2; 34; 9; 5; 4]). It has been shown that, if $\mathbb{C}$ is replaced by an algebraically closed field K of characteristic p, these computations are still valid for $g = 2$ if $p \neq 2, 3, 5$ [24] and for $g = 3$ if $p \neq 2, 3, 5, 7$ [25].

Our second idea to compute isomorphisms between forms of a given degree is to reduce the question to smaller degree by using covariants. Indeed, the following observation is a simple consequence of the definition itself.

Proposition 2.5. *Let f_1, f_2 be forms of even degree n over a field k. Let C be a covariant of order r for binary forms of degree n, defined over the prime field of k, and let $c_i = C(f_i) \in S^r(V)$. Then* $\mathrm{Isom}(f_1, f_2) \subset \mathrm{Isom}(c_1, c_2)$. □

We illustrate this idea and study its limitations with the computation of isomorphisms for forms and hyperelliptic curves in Sections 2D and 2E. As we want the covariants c_i to have the smallest degree possible and $\mathrm{Isom}(c_1, c_2)$ to be finite, we want that $\deg \widetilde{c}_i \geq 3$. Actually, in what follows we mostly deal with forms of even degree, so nonzero covariants will be of even order, and the smallest degree meeting our restriction is then 4.

Consider a binary quartic $q = a_4x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4$ over k with $p \neq 2, 3$. We define

$$\begin{aligned} I &= I(q) = 12a_4a_0 - 3a_3a_1 + a_2^2, \\ J &= J(q) = 72a_4a_2a_0 + 9a_3a_2a_1 - 27a_4a_1^2 - 27a_0a_3^2 - 2a_2^3 \end{aligned}$$

as in [8]. The form q has distinct roots if and only if $\Delta = 4I^3 - J^2 \neq 0$. Given $I, J \in K$ such that $\Delta \neq 0$, one can easily reconstruct a form with at least three distinct roots which is K-isomorphic to q. We can take

$$q = \begin{cases} x^3z - 27(I^3/J^2)xz^3 - 27(I^3/J^2)z^4 & \text{if } J \neq 0, \\ x^3z + xz^3 & \text{otherwise.} \end{cases} \tag{4}$$

Concerning the geometric automorphisms of binary quartics, we have the following easy result, for which we could not find a reference.

Proposition 2.6. *Let q be a binary quartic form over K, with invariants I and J. Suppose that $\Delta \neq 0$. Then*

$$\operatorname{Aut} q \cong \begin{cases} \boldsymbol{A}_4 & \textit{if } I = 0, \\ \boldsymbol{D}_8 & \textit{if } J = 0, \\ \boldsymbol{D}_4 & \textit{otherwise.} \end{cases} \tag{5}$$

Proof. Let $\Lambda \subset \mathbb{P}^1(K)$ be the set of four roots of q. Using the 3-transitivity of the action of $\mathrm{PGL}_2(K)$ on $\mathbb{P}^1(K)$, we may assume that $\Lambda = \{0, 1, \infty, \lambda\}$ for some $\lambda \in K \setminus \{0, 1\}$. Then the transformation $x \mapsto \lambda/x$ induces the permutation $(0\infty)(1\lambda)$ of Λ. By symmetry, we see that $\operatorname{Stab} \Lambda \subset \operatorname{Sym} \Lambda$ contains the Vierergruppe $\boldsymbol{D}_4 \subset \operatorname{Sym} \Lambda$.

We are reduced to analyzing the case when $\operatorname{Stab} \Lambda$ properly contains $\boldsymbol{D}_4$. Since the extension $1 \to \boldsymbol{D}_4 \to \boldsymbol{S}_4 \to \boldsymbol{S}_3 \to 1$ is split and all subgroups of $\boldsymbol{S}_3$ of equal order are conjugate, this is in turn equivalent to determining when $\operatorname{Stab} \Lambda$ contains an additional given 2- or 3-cycle. These cases give rise to the exceptional groups in (5) of order 8 and 12.

First let us see for which λ the permutation (1λ) is in $\operatorname{Stab} \Lambda$. In this case, the fractional linear transformation fixes 0 and ∞ and is therefore of the form $x \mapsto cx$. This only gives a new automorphism if $c = -1$, so $\lambda = -1$ and $J = 0$.

In the case where the permutation (01λ) is in $\operatorname{Stab} \Lambda$, a slightly more involved calculation gives that $\lambda = \zeta_3 + 1$ for a primitive third root of unity ζ_3, and in that case $I = 0$. □

We will also need in the sequel the following result.

Proposition 2.7. *Let q be a binary quartic form defined over k with distinct roots, and let $\mathfrak{q}$ be the form defined by* (4). *Assume that $I(q) \neq 0$ and $J(q) \neq 0$. Then a K-isomorphism between q and $\mathfrak{q} = z(x^3 + b_1 xz^2 + b_0 z^3)$ is defined over any extension of k where q has a root.*

Proof. Let k' be an extension of k where q has a root. By a change of variable defined over k', we can map this root to infinity and hence q onto $q' = zr$, where $r = x^3 + a_1 xz^2 + a_0 z^3 \in k'[x, z]$. Now, since

$$I(q') = -a_1/4, \qquad I(\mathfrak{q}) = -b_1/4,$$
$$J(q') = -a_0/16, \quad J(\mathfrak{q}) = -b_0/16,$$

we get the relation $a_1^3/a_0^2 = b_1^3/b_0^2$. Hence if we define $\lambda \in k'$ by

$$\lambda = \frac{J(q')I(\mathfrak{q})}{J(\mathfrak{q})I(q')},$$

the k'-isomorphism $M : (x, z) \mapsto (\lambda x, z)$ maps q' onto $\mathfrak{q}$. □

2D. ***Generic forms of even degree.*** We now describe an algorithm, based on the ideas of Sections 2B and 2C, to compute the isomorphisms between two generic binary forms f_1 and f_2. Our notation is as in Section 2B.

Algorithm 2.8 (`IsGL2EquivCovariant`).

```
Input:  Two forms $f_1$ and $f_2$ of the same degree $n \geq 3$ over $k$, and integer
        parameters $B_{\text{order}} \geq 3$, $B_{\text{degree}} \geq 2$, and $B_{\text{singular}} \geq 0$.
Output: The matrices $M = (m_{i,j})_{i,j}$ in $\mathrm{PGL}_2(k)$ such that $M.f_1 \sim f_2$.

1. Order loop. For $o$ increasing from 3 to $B_{\text{order}}$ do:
   (a) Degree loop. For $d$ increasing from 2 to $B_{\text{degree}}$ do:
       i.   Compute a random covariant $C$ of order $o$ and degree $d$ using transvectants.
       ii.  If $\widetilde{C}(f_1)$ is of degree at least 3, then compute $\mathrm{Isom}(\widetilde{C}(f_1), \widetilde{C}(f_2))$ and
            return the elements which induce isomorphisms between $f_1$ and $f_2$.
       iii. Otherwise, repeat the following procedure $B_{\text{singular}}$ times:
            – Compute a new random covariant $C'$ of order $o$ and degree $d$ using
              transvectants, and replace $C$ by the covariant $C + \kappa C'$ for some
              random $\kappa$ in the field $k$.
            – If $\widetilde{C}(f_1)$ is of degree at least 3, compute $\mathrm{Isom}(\widetilde{C}(f_1), \widetilde{C}(f_2))$ and
              return the elements that induce isomorphisms between $f_1$ and $f_2$.
2. Failure. Return the result of IsGL2EquivFast($f_1$, $f_2$).
```

For the purpose of computing random covariants, we follow Gordan [15]. Given an order o and a degree d, we construct recursively a covariant $C = \left(\prod C_{d',o'}, f\right)_h$ as a transvectant of some level h of the form f and a product of covariants of intermediate orders o' and degrees d', under the two constraints $d = \sum d'$ and $o = n + \sum o' - 2h$.

When n is even, the transvectant of smallest order and degree is $C_{2,4} = (f, f)_{n-2}$. The next simplest transvectant is $C_{3,4} = ((f, f)_{n/2}, f)_{n-2}$, of order 4 and degree 3. For large orders and degrees, covariants must be computed "on the fly", specialized for f_1 and f_2, since expressions are far too large to be precomputed.

To completely specify the algorithm, we have to be more precise about how to compute covariants and how to choose the loop bounds B_{order}, B_{degree} and B_{singular}. A straightforward choice for the loop bounds is $B_{\text{order}} = 4$, $B_{\text{degree}} = 2$, and $B_{\text{singular}} = 0$. With this choice, only the covariant $C_{2,4} = (f, f)_{n-2}$ is tested for n even, and when it turns out that the discriminant of this covariant vanishes, we go back to the method `IsGL2EquivFast`. First note that the covariant $(f, f)_{n-2}$ can be easily computed. Using (3), we find that we can write

$$\frac{(n!)^2}{(n-2)!}(f, f)_{n-2} = c_4x^4 + c_3x^3z + c_2x^2z^2 + c_1xz^3 + c_0z^4, \tag{6}$$

where the coefficients c_i are given by

$$\begin{aligned}
c_0 &= \sum_{k=0}^{n-2} (-1)^k (n-k)!(k+2)!\, a_{n-2-k}a_k,\\
c_1 &= \sum_{k=0}^{n-2} (-1)^k (n-k)!(k+2)!\big((n-1-k)a_{n-1-k}a_k + (k+1)a_{n-2-k}a_{k+1}\big),\\
c_2 &= \frac{1}{2}\sum_{k=0}^{n-2} (-1)^k (n-k)!(k+2)!\big((k+2)(k+1)a_{k+2}a_{n-2-k}\\
&\qquad\qquad + 2(n-1-k)(k+1)a_{k+1}a_{n-1-k} + (n-k)(n-1-k)a_k a_{n-k}\big),\\
c_3 &= \sum_{k=0}^{n-2} (-1)^k (n-k)!(k+2)!\big((n-1-k)a_{n-k}a_{k+1} + (k+1)a_{n-1-k}a_{k+2}\big),\\
c_4 &= \sum_{k=0}^{n-2} (-1)^k (n-k)!(k+2)!\, a_{n-k}a_{k+2}.
\end{aligned}$$

Moreover, this setting is a good option for generic forms, as the following proposition shows.

Proposition 2.9. *Let $n \geq 6$ be an even integer and $p \neq 2, 3$. Let f be a generic binary form of degree n over k. Then the discriminant of $C_{2,4}(f)$ is nonzero.*

Proof. It is enough to find a single form f of degree n for which $C_{2,4}(f)$ has nonzero discriminant. First let us suppose that p is coprime to

$$n(n-2)(n-3)(n^2+3n+6).$$

We then take $f = x^n + x^{n-1}z - xz^{n-1} - z^n$. Note that this form is in fact nonsingular because $f = (x+z)(x^{n-1} - z^{n-1})$. We have that

$$-C_{2,4}(f) = \frac{4}{n}x^3z + \frac{2(n^2-n+6)}{n^2}x^2z + \frac{4}{n}xz^2.$$

This form has discriminant equal to $64(n-3)(n-2)(n^2+3n+6)/n^6$, which is nonzero by hypothesis.

One calculates similarly that for the other values of $p \neq 2, 3, 5$, one can use the form $x^n + x^{n-1}z + xz^{n-1} - z^n$ instead. Indeed, under these hypotheses on p the numerator $n^4 + 2n^3 + 5n^2 - 12n + 36$ of the resulting discriminant is coprime to the previous numerator. To finish the proof, $p = 5$ can be excluded using the form $x^n + x^{n-1}z + xz^{n-1} + 2z^n$. □

For nonrandom forms, especially forms of small degree with nontrivial automorphism group, it may be interesting to test other covariants than merely $C_{4,2}$. We then propose the following settings:

$$B_{\text{order}} = \min(8, n), \quad B_{\text{degree}} = 10, \quad \text{and} \quad B_{\text{singular}} = 10.$$

These bounds are constant in order to keep the total time complexity quasilinear in n. More precisely, the bound B_{order} is chosen to be at most 8 so as to take advantage of the classification work of [25], the bound B_{degree} is chosen to cover all the possible fundamental covariants of degree 8 and with order between 4 and 8 (see [25, Table 1, p. 607]), and the bound B_{singular} is chosen so as to increase the probability that our covariants, if singular, have distinct points of singularity (so that a linear combination may be nonsingular).

Remark 2.10. We may enter the last loop of the algorithm even if the form f has no geometric automorphisms. For example, this happens with the degree-8 form

$$x^7z + 7x^6z^2 + 7x^5z^3 + 8x^4z^4 + 2x^3z^5 + 10x^2z^6 + 9xz^7$$

over $k = \mathbb{F}_{11}$.

We have programmed Algorithm 2.8 in Magma (version 2.18-2), using the first setting of the parameters. In particular, we have implemented the covariant $C_{4,2}$ using (6), and we have measured the timings of the resulting procedure, `IsGL2EquivCovariant`, in the same experiments as in Section 2B. The results are presented in Table 1. As expected, computing isomorphisms is much faster with the help of covariants, even if the forms are split over k.

2E. *Application to isomorphisms of hyperelliptic curves.*

2E1. *Isomorphisms of forms and of hyperelliptic curves.* A curve X of genus $g \geq 1$ defined over k will be called *hyperelliptic* if X/K has a separable degree-2 map to $\mathbb{P}^1_K$. If $g > 1$, the curve X then has a unique involution ι, called the *hyperelliptic involution*, such that $Q = X/\langle\iota\rangle$ is of genus 0. This involution is in the center of $\mathrm{Aut}_K X$. We call $\overline{\mathrm{Aut}}_K X = (\mathrm{Aut}_K X)/\langle\iota\rangle$ the *reduced automorphism group* of X.

Let us assume from now on that $p \neq 2$. Then if Q has a rational point, X is birationally equivalent to an affine curve of the form $y^2 = f(x)$ for a separable polynomial f of degree $2g+1$ or $2g+2$. We say that f is a *hyperelliptic polynomial* and that X has a *hyperelliptic equation* if a curve in its isomorphism class (over k) can be written in the form above. We denote by X_f the curve associated to a hyperelliptic polynomial f. A hyperelliptic curve automatically has a hyperelliptic equation when k is algebraically closed or a finite field. However, for more general fields and curves of odd genus, this is not necessarily the case (see [25]).

By homogenizing to weighted projective coordinates of weight $(1, g+1, 1)$, we obtain an equation $y^2 = f(x, z)$. Here f is seen as a form of degree $2g+2$, taking into account a "root" at infinity when $\deg f = 2g+1$. With this convention, the roots of f are the ramification points of the cover X/Q. We will use these conventions for the roots and degree in the sequel when we speak about a hyperelliptic polynomial or the associated form.

If f_1 and f_2 are hyperelliptic polynomials of even degree $2g+2 \geq 6$, then isomorphisms between the hyperelliptic curves $y^2 = f_i(x, z)$ are represented by pairs (M, e) with

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(k)$$

and $e \in k^*$. To such a couple, one associates the isomorphism

$$(x, z, y) \mapsto (ax + bz, cx + dz, ey).$$

The representation is unique up to the equivalence $(M, e) \equiv (\lambda M, \lambda^{g+1} e)$ for $\lambda \in k^*$. Hence, if $M.f_1 = \mu \cdot f_2$ then the map

$$\mathrm{Isom}(f_1, f_2) \to (\mathrm{GL}_2(k) \times K^*)/\equiv, \quad M \mapsto (M, \pm\sqrt{\mu})$$

is well-defined up to the choice of a sign. It surjects onto $\mathrm{Isom}(X_{f_1}, X_{f_2})$, so knowing $\mathrm{Isom}(f_1, f_2)$ is enough to determine $\mathrm{Isom}(X_{f_1}, X_{f_2})$ "up to the hyperelliptic involution".

2E2. *Hyperelliptic curves of genus* 2 *and* 3. The covariant approach requires a covariant with at least three distinct roots, and hence it may fail in special cases, which we can specify for small genera. We give some details on the more difficult of the two cases: the genus-3 case. This problem is naturally stratified by the

$\mathrm{Aut}_K X_f$	$\overline{\mathrm{Aut}}_K X_f$	Normal models $X_f : y^2 = f$
$\boldsymbol{C}_2$	$\{1\}$	$f = x(x-1)(x^5+ax^4+bx^3+cx^2+dx+e)$
$\boldsymbol{D}_4$	$\boldsymbol{C}_2$	$f = x^8+ax^6+bx^4+cx^2+1$ or $f = (x^2-1)(x^6+ax^4+bx^2+c)$
$\boldsymbol{C}_4$	$\boldsymbol{C}_2$	$f = x(x^2-1)(x^4+ax^2+b)$
$\boldsymbol{C}_2^3$	$\boldsymbol{D}_4$	$f = (x^4+ax^2+1)(x^4+bx^2+1)$
$\boldsymbol{C}_2 \times \boldsymbol{C}_4$	$\boldsymbol{D}_4$	$f = (x^4-1)(x^4+ax^2+1)$ or $f = x(x^2-1)(x^4+ax^2+1)$
$\boldsymbol{D}_{12}$	$\boldsymbol{D}_6$	$f = x(x^6+ax^3+1)$
$\boldsymbol{C}_2 \times \boldsymbol{D}_8$	$\boldsymbol{D}_8$	$f = x^8+ax^4+1$
$\boldsymbol{C}_{14}$	$\boldsymbol{C}_7$	$f = x^7-1$
$\boldsymbol{U}_6$	$\boldsymbol{D}_{12}$	$f = x(x^6-1)$
$\boldsymbol{V}_8$	$\boldsymbol{D}_{16}$	$f = x^8-1$
$\boldsymbol{C}_2 \times \boldsymbol{S}_4$	$\boldsymbol{S}_4$	$f = x^8+14x^4+1$

Table 2. Automorphism groups of genus-3 hyperelliptic curves. For each automorphism group, we list the associated reduced automorphism group, together with normal model(s) for the generic hyperelliptic curve with that automorphism group. The notation for the groups is given at the end of the Introduction.

possible automorphism groups of the curve; we list these automorphism groups, together with normal models and inclusion relations between the strata, in Table 2 and Figure 1. We assume here that $p = 0$ or $p > 7$.

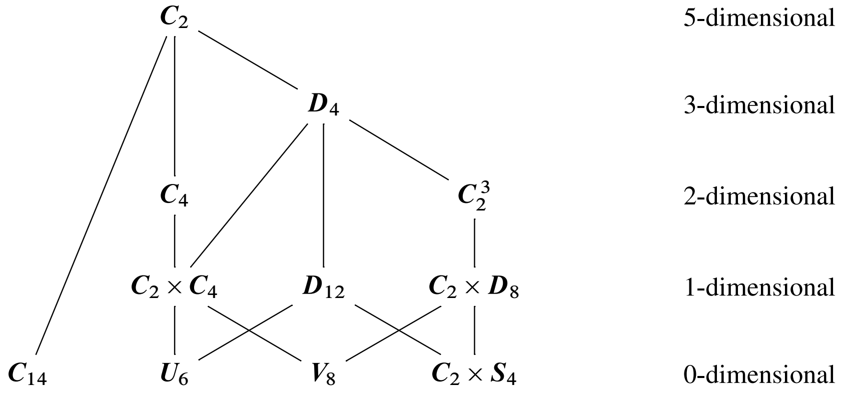

Figure 1. Dimensions and containment relationships among the moduli spaces of genus-3 hyperelliptic curves with given automorphism groups.

The moduli space of hyperelliptic curves of genus 3 is 5-dimensional, and can be explicitly described using the Shioda invariants $J_2, J_3, \dots, J_{10}$ constructed in [34]. These invariants were used to speed up the calculations leading to the proof of the following proposition, which shows that the locus where the covariant method fails is of codimension 4 in the full moduli space. (The Magma parts of this proof, and of other proofs in this section, may be found at the URL listed in the Introduction.)

Proposition 2.11. *Let $X_f/K : y^2 = f(x)$ be a genus-3 hyperelliptic curve such that the form f cancels the discriminants of all its quartic covariants. Then* $\operatorname{Aut} X_f$ *contains either $\boldsymbol{D}_{12}$, $\boldsymbol{C}_2 \times \boldsymbol{D}_8$, or $\boldsymbol{C}_{14}$.*

Proof. Construct

$$C(f) \pm \kappa \cdot I(f) \cdot C'(f)$$

such that $\deg C = \deg I + \deg C'$, where C and C' run through the 14 fundamental quartic covariants given in [25, Table 1], where $I(f)$ equals either 1 or a Shioda invariant $J_i(f)$, and where κ runs through the integers between 0 and 10. We rewrite the discriminants of these covariants in terms of Shioda invariants and add to them the five Shioda relations [34, Theorem 3, p. 1042]. Using Magma, we have been able to compute a Gröbner basis of this polynomial system, over $\mathbb{Q}$, for the graded reverse lexicographical (grevlex) order $J_2 < J_3 < \cdots < J_{10}$ with weights 2, 3, …, 10. Upon removing multiplicities, we obtain a basis with 22 polynomials, of total degree between 8 and 20. One then checks, using the stratum formulas from [25], that the irreducible components of the corresponding subscheme of the moduli space either correspond to families of forms with discriminant zero or to strata of curves X_f such that $\operatorname{Aut} X_f$ contain $\boldsymbol{D}_{12}$, $\boldsymbol{C}_2 \times \boldsymbol{D}_8$, or $\boldsymbol{C}_{14}$. □

We see from this that curves with automorphism group $\boldsymbol{D}_{12}$, $\boldsymbol{C}_2 \times \boldsymbol{D}_8$, or $\boldsymbol{C}_{14}$ cannot have separable quartic covariants. In these cases, using Proposition 2.5 and the normal models from Table 2, one can show:

- if $\operatorname{Aut} X$ is equal to $\boldsymbol{D}_{12}$ or $\boldsymbol{U}_6$ then the sextic covariant $C_{3,6} = ((f, f)_4, f)_5$ has nonzero discriminant;
- if $\operatorname{Aut} X$ contains $\boldsymbol{C}_2 \times \boldsymbol{D}_8$ or is equal to $\boldsymbol{C}_{14}$ then there is no order-4 or order-6 covariant with three distinct roots.

The number of covariants considered in the proof of Proposition 2.11 — namely, 1253 — is not minimal, but the redundancy helped Magma during the Gröbner basis computations. Nevertheless, similar computations show that we can easily reduce this number for curves with automorphism group larger than $\boldsymbol{C}_2$ (and also impose conditions on the automorphism groups of the covariants; see Sections 3B2 and 3C2). For example, consider the following five quartic covariants:

$$\begin{aligned} C_{2,4} &= (f, f)_6, & C_{4,4} &= (((f, f)_4, f)_6, f)_4, \\ C_{3,4} &= ((f, f)_4, f)_6, & C'_{4,4} &= (((f, f)_4, f)_4, f)_6, \\ & & C_{5,4} &= ((((f, f)_4, f)_6, f)_1, f)_7. \end{aligned}$$

If X_f/K is a genus-3 hyperelliptic curve, we find that:

- If $\operatorname{Aut} X_f \cong \boldsymbol{D}_4$, one of the five covariants above has nonzero discriminant.
- If $\operatorname{Aut} X_f \cong \boldsymbol{C}_4$, one of $C_{2,4}$, $C_{3,4}$, $C_{4,4}$, and $C'_{4,4}$ has nonzero discriminant.
- If $\operatorname{Aut} X_f \cong \boldsymbol{C}_2^3$, one of $C_{2,4}$, $C_{3,4}$, and $C_{4,4}$ has nonzero discriminant.
- If $\operatorname{Aut} X_f \cong \boldsymbol{C}_2 \times \boldsymbol{C}_4$, the covariant $C_{3,4}$ has nonzero discriminant.

Remark 2.12. Similar conclusions hold for genus 2. Specifically, there is no quartic covariant with nonzero discriminant for the curves X_f/K such that $\boldsymbol{D}_{12} \subset \operatorname{Aut} X_f$ or $\operatorname{Aut} X_f \simeq \boldsymbol{C}_{10}$. Moreover, when $\operatorname{Aut} X_f \simeq \boldsymbol{D}_8$ then $(f, f)_4$ has nonzero discriminant, and when $\operatorname{Aut} X_f \simeq \boldsymbol{D}_4$ then at least one of $(f, f)_4$, $(((f, f)_2, f)_4, f)_4$, and $((((f, f)_2, f)_3, f)_2, f)_6$ has nonzero discriminant.

3. Explicit descent for hyperelliptic curves

3A. ***Field of moduli and fields of definition.*** Let X be a curve defined over K of genus $g \geq 1$, let k be a subfield of K, and let F be the prime field of K.

Definition 3.1. The *field of moduli* of X, denoted $\boldsymbol{M}_X$, is the subfield of K fixed by $\{\sigma \in \operatorname{Aut} K \mid X \simeq X^\sigma\}$.

We now restrict to hyperelliptic curves and we assume that $p \neq 2$. Let $X = X_f$ be a hyperelliptic curve over K given by a hyperelliptic polynomial f of even degree n. Our first task is to show that we can get information on $\boldsymbol{M}_X$ through the invariants.

Lemma 3.2. *Let I_1, I_2 be two invariants of the same degree for binary forms of degree n. Assume that I_1, I_2 are defined over F and that $I_2(f) \neq 0$. Then $\iota = I_1(f)/I_2(f)$ is an element of $\boldsymbol{M}_{X_f}$.*

Proof. It is enough to prove that $\iota^\sigma = \iota$ for all $\sigma \in \operatorname{Gal}(K/\boldsymbol{M}_X)$. By the definition of $\boldsymbol{M}_X$, there exists an isomorphism between X and X^σ. We have seen that such an isomorphism induces an element $M \in \operatorname{Isom}(f, f^\sigma)$. Therefore

$$\iota^\sigma = \frac{I_1(f^\sigma)}{I_2(f^\sigma)} = \frac{I_1(\lambda \cdot M.f)}{I_2(\lambda \cdot M.f)} = \iota. \qquad \square$$

It is not always practical to work with a fixed quotient of invariants as above, since $I_2(f)$ may be zero. As shown in [25], it is better to work inside a weighted projective space, for elements of which one can define a canonical representative as follows. Let $(I_1 : \cdots : I_m)$ be an m-tuple of degree-d_i invariants of degree-n binary forms, where $m \geq 2$, and suppose each I_i is defined over F. Let f be a binary form of degree n. Let d be the gcd of the degrees d_i of the invariants I_i whose values at f are nonzero. Then there exist $c_i \in \mathbb{Z}$, with $c_i = 0$ if $I_i(f) = 0$, such that $\sum c_i d_i = d$. We then define $I = \prod_i I_i^{c_i}$. The *canonical representative* of $(I_1(f) : \cdots : I_m(f))$ is

$$(\mathfrak{I}_1(f), \dots, \mathfrak{I}_m(f)) = \left(\frac{I_1(f)}{I(f)^{d_1/d}}, \dots, \frac{I_m(f)}{I(f)^{d_m/d}} \right) \in \boldsymbol{M}_X^m.$$

Proposition 3.3. *Let $(I_1 : \cdots : I_m)$ be a set of generators for $\mathcal{I}_n$ defined over F. Then*

$$\boldsymbol{M}_X = F(\mathfrak{I}_1(f), \dots, \mathfrak{I}_m(f)).$$

Proof. Let $\sigma \in \operatorname{Gal}(K/F(\mathfrak{I}_1(f), \dots, \mathfrak{I}_m(f)))$. Since

$$(\mathfrak{I}_1(f^\sigma), \dots, \mathfrak{I}_m(f^\sigma)) = (\mathfrak{I}_1(f), \dots, \mathfrak{I}_m(f)),$$

and since $\mathcal{I}_n$ separates the orbits of separable forms [28, p. 78], there exists a matrix $M \in \mathrm{GL}_2(K)$ such that $M.f \sim f^\sigma$, hence an isomorphism between X_f and X_f^σ. □

With our current knowledge of invariants, we are then able to compute $\boldsymbol{M}_{X_f}$ for $n = 6, 8, 10$. However, in the following applications to descent we will see that we often do not need a complete set of invariants.

Definition 3.4. We say that k is a *field of definition* of X if there exists a curve $\mathcal{X}/k$ such that $\mathcal{X}$ is K-isomorphic to X. The curve $\mathcal{X}/k$ is a model of X over k and we call a geometric isomorphism between the two curves a *descent isomorphism*.

A classical problem is to determine the smallest field of definition of a curve. Assuming for simplicity that every subfield of K is perfect, if $\boldsymbol{M}_X$ is a field of definition then it is the smallest possible field of definition, because it is the intersection of all the fields of definition (see [23] or [19, Theorem 1.5.8]). There might be an obstruction for $\boldsymbol{M}_X$ being a field of definition, but if there is none we will denote by $\mathcal{X}$ a model of X over $\boldsymbol{M}_X$. In the case of hyperelliptic curves of odd genus, there is a subtlety: The curve $\mathcal{X}$ does not necessarily admit a hyperelliptic equation. However, if it does, we will say that X can be *hyperelliptically defined over* $\boldsymbol{M}_X$, and we denote by $\mathfrak{f} \in \boldsymbol{M}_X[x]$ a hyperelliptic polynomial associated to this model.

One can find in the literature several sufficient conditions for a curve to be hyperelliptically defined over $\boldsymbol{M}_X$. For instance, it is always the case when K is the algebraic closure of a finite field (see [18, Corollary 2.11]). Over an arbitrary algebraically closed field K, the work of Huggins [18] shows that if the reduced automorphism group is noncyclic then the curve can be hyperelliptically defined over its field of moduli. For $g = 2$, it has been proved that if the reduced automorphism group is nontrivial, then the curve can be hyperelliptically defined over its field of moduli [7]. This is also the case for $g = 3$, except for curves with automorphism group isomorphic to $\boldsymbol{D}_4$ (see [25] and Section 3C2).

3B. ***Explicit hyperelliptic descent.*** Now let X_f be a hyperelliptic curve over K that can be hyperelliptically defined over $\boldsymbol{M}_X$. We want to find $\mathfrak{f} \in \boldsymbol{M}_X[x]$ and $A \in \mathrm{GL}_2(K)$ such that $\mathfrak{f} \sim A.f$. The first task is of course to compute $\boldsymbol{M}_X$. As we have seen, this can be done if we have a set of generators for the invariants of the form f. However, if we do not have a full set of generators, and instead have only some invariants $(I_1, \ldots, I_m)$ over F with $m \geq 2$, we can always try to hyperelliptically descend X_f over the field k generated by $(\mathfrak{I}_1(f), \ldots, \mathfrak{I}_m(f))$. Since $k \subset \boldsymbol{M}_X$, if this can be achieved, we are done.

3B1. *The cocycle approach.* The direct approach relies on the following slightly modified version of Weil's cocycle relations (see [25]).

Lemma 3.5. *The curve X_f can be hyperelliptically defined over k if and only if there exists a finite extension k'/k such that for all $\sigma \in \mathrm{Gal}(K/k)$, there exists $M_\sigma \in \mathrm{GL}_2(k')$ such that $M_\sigma \in \mathrm{Isom}_{k'}(f, f^\sigma)$ and such that for all $\sigma, \tau \in \mathrm{Gal}(K/k)$, we have $M_{\sigma\tau} = M_\sigma^\tau M_\tau$.*

Assume that X_f can be hyperelliptically defined over k and let $\phi : X_f \to X_{\mathfrak{f}}$ be a descent isomorphism. It induces a matrix $\widetilde{A} \in \mathrm{Isom}_K(f, \mathfrak{f}) \subset \mathrm{PGL}_2(K)$. If we choose a representative $A \in GL_2(K)$ of $\widetilde{A}$, we can define $M_\sigma = (A^{-1})^\sigma A$ for all $\sigma \in \mathrm{Gal}(K/k)$. It is easy to check that this choice of M_σ satisfies all the hypotheses of the lemma. Moreover, if A is defined over a Galois extension L/k then $k' \subset L$, and we have $M_\sigma = \mathrm{id}$ for all $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma_{|L} = \mathrm{id}$. Conversely, the crucial step to construct such an A is to identify a Galois extension L/k satisfying this property, since in this case one can use an explicit version of Hilbert 90 as in [31, Proposition 3, p. 159]: For a general matrix $P \in \mathrm{GL}_2(k')$ the matrix

$$A = \sum_{\tau \in \mathrm{Gal}(L/k)} P^\tau M_\tau \tag{7}$$

gives a descent morphism.

Lemma 3.6. *Assume that f is defined over an extension k' of k. If $\mathrm{Aut}_K f = \{\mathrm{id}\}$ then we can take L to be the Galois closure of k'/k.*

Proof. We have to prove that A can be defined over such an L. Let A' be induced by a descent morphism. Since $A' \in \mathrm{Isom}_K(f, \mathfrak{f})$, we have

$$((A')^{-1})^{\sigma} A' \in \mathrm{Isom}_K(f, f^{\sigma}) = \mathrm{Aut}_K f$$

for all $\sigma \in \mathrm{Gal}(K/L)$; hence there exists $\lambda_\sigma \in K^*$ such that $(A')^{\sigma} = \lambda_\sigma \cdot A'$. One can easily check that the λ_σ satisfy a cocycle relation, so there exists $e \in K^*$ such that $\lambda_\sigma = e/e^{\sigma}$ for all σ. We then define $A = e \cdot A'$, and we are done. □

As far as we know, there is no easy way to determine such an L when the automorphism group is nontrivial (but see [25] for the case when k is a finite field). Naïvely, one would expect to be able to construct the cocycle over the field L_0 over which all isomorphisms between f and its conjugates are defined. Typically, what then happens is the following: Let $\sigma \in \mathrm{Gal}(L_0/k)$ be an element of order n. Then usually no M_σ exists over L_0 such that the cocycle condition $1 = M_{\sigma^n} = M^{\sigma^{n-1}} \cdots M^{\sigma} \cdot M$ is satisfied. We have to work with matrices of the form λM_σ, where λ belongs to a quadratic extension L of L_0. This enlarges the field and the Galois group, which may in turn give rise to more problems of the same type. Even if this problem can be resolved, the computation of (7) is time-consuming and limited to extensions of small degree (less than 50) in practice. In the next section, we present a new idea that works extremely well to get around these difficulties in certain cases.

Remark 3.7. In the odd genus case, it turns out that if we only want X_f to have a model over k, instead of a hyperelliptic model, then the cocycle condition is replaced by the condition $M_{\sigma\tau} \sim M_\sigma^\tau M_\tau$. However, even in this case we do not know a general method to address the problem effectively.

3B2. *The covariant approach.* Using covariants, we can sometimes reduce the problem of descent for X_f to a descent problem for a curve of lower genus.

Theorem 3.8. *Assume that there exists a covariant C of order $r \geq 4$ such that $c = C(f)$ is a hyperelliptic polynomial, and let $X_c : y^2 = c(x)$ be the associated curve. Then $\boldsymbol{M}_{X_c} \subset \boldsymbol{M}_{X_f}$.*

Moreover, if X_c is hyperelliptically defined over $\boldsymbol{M}_{X_c}$, then X_f is hyperelliptically defined over an extension of $\boldsymbol{M}_{X_f}$ of degree at most $[\mathrm{Aut}_K c : \mathrm{Aut}_K f]$.

In particular, if $\mathrm{Aut}_K c = \mathrm{Aut}_K f$ *and X_c is hyperelliptically defined over $\boldsymbol{M}_{X_c}$, then X_f is hyperelliptically defined over $\boldsymbol{M}_{X_f}$.*

Proof. Let σ be an element of the group $\Gamma = \mathrm{Gal}(K/\boldsymbol{M}_{X_f})$. Then there exists a K-isomorphism between X_f and X_f^σ which induces a matrix $M \in \mathrm{Isom}_K(f, f^\sigma)$. Since we have the inclusion $\mathrm{Isom}_K(f, f^\sigma) \subset \mathrm{Isom}_K(c, c^\sigma)$ by Proposition 2.5, we get a K-isomorphism between X_c and X_c^σ, so $\boldsymbol{M}_{X_c} \subset \boldsymbol{M}_{X_f}$.

Assume now that X_c can be hyperelliptically defined over $\boldsymbol{M}_{X_c}$ as $X_{\mathfrak{c}}$ for some form $\mathfrak{c} \in \boldsymbol{M}_{X_c}[x]$. There exists $A \in \operatorname{Isom}_K(c, \mathfrak{c})$. Let us consider $h = A.f$, which we can assume to be monic. We want to prove that h is defined over an extension of $\boldsymbol{M}_{X_f} = \boldsymbol{M}_{X_h}$ of degree at most

$$\ell = \#(\operatorname{Aut}_K c/\operatorname{Aut}_K f) = \#(\operatorname{Aut}_K \mathfrak{c}/\operatorname{Aut}_K h).$$

First note that $C(h) \sim A.C(f) \sim \mathfrak{c}$. Let $H \subset \Gamma$ be the subgroup consisting of the automorphisms σ such that $h \sim h^\sigma$. Since we have assumed that h is monic, we even have $h = h^\sigma$. We must show that $\#\Gamma/H \leq \ell$. To this end, we note that $\mathfrak{c}^\sigma = \mathfrak{c}$ for all $\sigma \in \Gamma$. Hence we can associate to each $\sigma \in \Gamma$ a matrix $M \in \operatorname{Isom}_K(h, h^\sigma) \subset \operatorname{Aut}_K \mathfrak{c}$. In fact, this association gives rise to a well-defined class of $\operatorname{Aut}_K \mathfrak{c}/\operatorname{Aut}_K h$, so we have defined a map ρ from Γ to $\operatorname{Aut}_K \mathfrak{c}/\operatorname{Aut}_K h$. If $\rho(\sigma) = \rho(\sigma')$ then we have $h^\sigma \sim h^{\sigma'}$, and hence $\sigma^{-1}\sigma' \in H$. Therefore ρ induces an injective map from Γ/H to $\operatorname{Aut}_K \mathfrak{c}/\operatorname{Aut}_K h$, and we get our result. □

To use the theorem in a constructive way, we need a covariant that has a finite automorphism group and for which we know how to find a hyperelliptic model over its field of moduli. We give some examples in Sections 3C and 3D.

Remark 3.9. The fields of moduli of X_f and X_c may be different, even when the automorphism groups of the forms are the same. For instance, let r be a root of $t^2 + 2t + 16/9 = 0$ and let f be the form

$$f = (x^4 + rx^2z^2 + z^4)(x^4 - 3rx^2z^2 + z^4);$$

then the field of moduli of f is $\mathbb{Q}(r)$, while the field of moduli of

$$c = (f, f)_6 = (16/49)x^4 + (992/441)x^2 + (16/49)$$

is $\mathbb{Q}$. Using the programs of [25], one sees that $\operatorname{Aut}_K f = \operatorname{Aut}_K c \simeq \boldsymbol{D}_4$.

3C. ***Application to genus-3 hyperelliptic curves.*** In [25], the two first authors give algorithms for reconstructing genus-3 hyperelliptic models from given invariants. These models are defined over the field of moduli, with the notable exception of the 2-dimensional stratum $\boldsymbol{C}_2^3$ and the 3-dimensional stratum $\boldsymbol{D}_4$. As an illustration of our strategy, we see how our method applies in these remaining cases.

3C1. *Descent of curves with automorphism group $\boldsymbol{C}_2^3$.* Let $X/K : y^2 = f(x)$ be a genus-3 hyperelliptic curve with automorphism group isomorphic to $\boldsymbol{C}_2^3$. Since the reduced automorphism group is not cyclic, [18] shows that X can be hyperelliptically defined over its field of moduli. In [25], we showed how to construct a hyperelliptic equation for a model over an extension of the field of moduli of degree at most 3. Using covariants, we can now give a method to get an equation over the field of moduli itself.

In Section 2E2, we checked that at least one of the quartic covariants in the list $\{C_{2,4}(f), C_{3,4}(f), C_{4,4}(f)\}$ has nonzero discriminant. Moreover, we see by Proposition 2.6 that the automorphism group of such a quartic is equal to $\boldsymbol{D}_4$ if the quartic invariants I and J are both nonzero. Using some formal computations (see the Magma scripts available at the URL listed in the Introduction), we checked that it is always the case that at least one of the three covariants has nonzero discriminant and I and J nonzero. Since $\mathrm{Aut}_K(f) \simeq \boldsymbol{D}_4$ we can use the approach of Theorem 3.8 to find a hyperelliptic equation $y^2 = \mathfrak{f}(x)$ over the field of moduli. The procedure can actually be applied to a generic element of the family, but the result is too large to be written down here; instead, we present an example.

Example 3.10. When we evaluate the parametrization formulas given in [25] for the stratum $\boldsymbol{C}_2^3$ at $t = 0$ and $u = 1$, we find the rational point

$$(j_2 : j_3 : \cdots : j_{10}) \\ = \left(0 : 0 : -\frac{25}{98} : -\frac{25}{98} : -\frac{225}{2744} : -\frac{25}{1372} : -\frac{225}{134456} : \frac{1125}{76832} : \frac{15125}{3764768}\right)$$

in the moduli space. This gives rise to the curve $X : y^2 = f$ with

$$f = (-32\alpha^2 + 420\alpha - 2275)x^8/160 + (-12\alpha^2 + 140\alpha - 700)x^6/25 \\ + \alpha x^4 + x^2 + (16\alpha^2 + 280\alpha - 2275)/12250$$

over $\mathbb{Q}(\alpha)$, with $\alpha^3 - (35/2)\alpha^2 + (1925/16)\alpha - (18375/64) = 0$. By Proposition 3.3, we have $\boldsymbol{M}_X = \mathbb{Q}$.

Let c be the covariant $(f, f)_6$. We find

$$c = \frac{-16\alpha^2 + 180\alpha - 875}{280}x^4 + \frac{24\alpha^2 - 630\alpha + 3150}{1225}x^2z^2 + \frac{4\alpha + 35}{490}z^4,$$

so that $I = -75/49$ and $J = -2025/343$. Then $\mathfrak{c} = x^3z + (25/9)xz^3 + (25/9)z^4$ is $\mathrm{GL}_2(\overline{\mathbb{Q}})$-equivalent to c, is defined over $\boldsymbol{M}_X = \mathbb{Q}$, and satisfies $\mathrm{Aut}_{\overline{\mathbb{Q}}}\, \mathfrak{c} \simeq \boldsymbol{D}_4$. The direct approach of Section 2B explicitly finds a $\overline{\mathbb{Q}}$-isomorphism M between c and $\mathfrak{c}$. Its inverse M^{-1} is equal to $(m_{i,j})_{i,j}$, where

$$m_{11} = 110250,$$

$$m_{12} = (3360\alpha^2 - 58800\alpha + 147000)\beta^2 - 16800\alpha^2 + 147000\alpha - 18375,$$

$$m_{21} = (-2064\alpha^2 + 24780\alpha - 60900)\beta^3 + (-3120\alpha^2 + 67200\alpha - 375375)\beta,$$

$$m_{22} = (-5840\alpha^2 + 74900\alpha - 280000)\beta^3 + (16880\alpha^2 - 173600\alpha + 487375)\beta.$$

Here β satisfies

$$\beta^4 + \frac{32\alpha^2 - 280\alpha + 350}{175}\beta^2 - \frac{176\alpha^2 - 1820\alpha + 7350}{175} = 0.$$

We compute the monic form $\mathfrak{f} \sim M.f$:

$$\mathfrak{f} = x^8 + 160x^7 - 560x^6 - 2800x^5 + 64750x^4 - 91000x^3 + 3010000x^2 - 2225000x - 9696875.$$

So $y^2 = \mathfrak{f}(x)$ is a model of X over $\boldsymbol{M}_X = \mathbb{Q}$.

3C2. *Descent of curves with automorphism group $\boldsymbol{D}_4$.* It is proved in [19, Chapter 5] that there may be an obstruction for a genus-3 hyperelliptic curve over K with automorphism group isomorphic to $\boldsymbol{D}_4$ to have a model over its field of moduli. In [25], we were able to construct a model of such curves over an extension of the field of moduli of degree at most 8. Using Theorem 3.8, we find:

Proposition 3.11. *Let X_f be a genus-3 hyperelliptic curve over K with automorphism group isomorphic to $\boldsymbol{D}_4$. Then there exists an explicit model of X over an at most quadratic extension of $\boldsymbol{M}_X$.*

Proof. Applying the methods of Proposition 2.11 to the stratum $\boldsymbol{D}_4$ shows that at least one of the five binary covariants $C_{2,4}(f)$, $C_{3,4}(f)$, $C_{4,4}(f)$, $C'_{4,4}(f)$, $C_{5,4}(f)$ has not only a discriminant different from 0, but also $I(f) \neq 0$, $J(f) \neq 0$. (The computations can be found in the Magma scripts available at the URL given in the Introduction.) One then combines Proposition 2.6 and Theorem 3.8. □

We plan to investigate how to apply the theory of twists to the binary quartics used in the application of Theorem 3.8 to give a precise characterization of the obstruction to the descent on the field of moduli.

3D. ***Application to a family of Fuertes-González-Diez in genus 5.*** Let k be the degree-3 Galois extension of $\mathbb{Q}$ defined by the irreducible polynomial $t^3 - 3t + 1$. Let r_1, r_2, r_3 be the roots of this polynomial in k. Then, as in [13], we can consider the family

$$y^2 = \prod_{i=4}^{6} \left(x^4 - 2\left(1 - 2\,\frac{r_3 - r_1}{r_3 - r_2}\,\frac{q_i - r_2}{q_4 - r_1}\right)x^2 + 1 \right) \tag{8}$$

of genus-5 hyperelliptic curves, with q_4, q_5, q_6 in $\mathbb{Q}$. It was proved in [13] that the members of this family have field of moduli equal to $\mathbb{Q}$ and automorphism group isomorphic to $\boldsymbol{C}_2^3$. Moreover, it was claimed in [13] that these curves cannot be hyperelliptically defined over $\mathbb{Q}$, in contradiction with [18]. However, the proof turns out to contain a subtle error. Still, the explicit descent of any of the member of the family was extremely hard.

As in Example 3.10, we can use Theorem 3.8 to construct an explicit descent for the curves in this family. For this particular family, the descent can even be performed uniformly to yield a general expression in q_4, q_5, q_6. Let $F = k(q_4, q_5, q_6)$

be the rational function field over k in three indeterminates, and define the binary quartic form $f \in F[x, z]$ as the homogenization of the right-hand side of (8). Let c be the transvectant $(f, f)_{10}$. Then c is a covariant of order 4 with nonzero discriminant and nonzero $I(c)$ and $J(c)$, and hence has automorphism group $\boldsymbol{D}_4$. The field of moduli of X_c is contained in the field of moduli of X_f, which is a subfield of $\mathbb{Q}(q_4, q_5, q_6)$; therefore the quartic $\mathfrak{c}$ as in (4) is defined over $\mathbb{Q}(q_4, q_5, q_6)$ and is $\mathrm{GL}_2(\overline{F})$-equivalent to c.

Now let L be the degree-4 extension of F defined by the dehomogenization of c. From Proposition 2.7, we can explicitly construct an L-isomorphism between c and $\mathfrak{c}$. This transformation gives a descent of the curve corresponding to c, which by Theorem 3.8 also yields a descent of the curve corresponding to f. The resulting expression, though indeed defined over the rationals, is huge and impossible to give here. (The computations above, their final result, and the program to compute the descent of any given specialization are available at the URL listed in the Introduction.) However, we can give an example for a specialization.

Example 3.12. Take $q_4 = 1$, $q_5 = 2$, $q_6 = 3$. The hyperelliptic equation over $\mathbb{Q}$ is

$$\begin{aligned} y^2 = {} & 199950247575x^{12} - 296949924611352x^{11} - 6665981624581275 0x^{10} \\ & - 154219754955073606 56x^9 + 2005635519424553708745x^8 \\ & + 1307920888647724194612 00x^7 + 44148454149188354317253820x^6 \\ & - 971884708390869364980395 9136x^5 \\ & + 9374947292703631283942405 4441x^4 \\ & + 86331359417888600607650948443656x^3 \\ & - 742391208066318251304593820516 1326x^2 \\ & + 2495111976411684049395109460415 15184x \\ & - 30066561438584723177639735809842606 81. \end{aligned}$$

Acknowledgment

The authors acknowledge support by grant ANR-09-BLAN-0020-01.

References

[1] Lars V. Ahlfors, Lipman Bers, Hershel M. Farkas, Robert C. Gunning, Irwin Kra, and Harry E. Rauch (eds.), *Advances in the theory of Riemann surfaces*: *Proceedings of the* 1969 *Stony Brook Conference*, Annals of Mathematics Studies, no. 66, Princeton University Press, 1971. MR 43 #5023

[2] Leonid Bedratyuk, *On complete system of invariants for the binary form of degree 7*, J. Symbolic Comput. **42** (2007), no. 10, 935–947. MR 2008h:13009

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system, I: The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265. MR 1484478

[4] Andries E. Brouwer and Mihaela Popoviciu, *The invariants of the binary decimic*, J. Symbolic Comput. **45** (2010), no. 8, 837–843. MR 2011f:13007

[5] ———, *The invariants of the binary nonic*, J. Symbolic Comput. **45** (2010), no. 6, 709–720. MR 2011e:13012

[6] Duncan Buell (ed.), *Algorithmic number theory: Proceedings of the 6th International Symposium (ANTS-VI) held at the University of Vermont, Burlington, VT, June 13–18, 2004*, Lecture Notes in Computer Science, no. 3076, Berlin, Springer, 2004. MR 2005m:11002

[7] Gabriel Cardona and Jordi Quer, *Field of moduli and field of definition for curves of genus 2*, in Shaska [32], 2005, pp. 71–83. MR 2006h:14036

[8] J. E. Cremona and T. A. Fisher, *On the equivalence of binary quartics*, J. Symbolic Comput. **44** (2009), no. 6, 673–682. MR 2010c:11049

[9] H. Cröni, *Zur Berechnung von Kovarianten von Quantiken*, Ph.D. thesis, Universität des Saarlandes, 2002.

[10] J. Dixmier and D. Lazard, *Le nombre minimum d'invariants fondamentaux pour les formes binaires de degré* 7, Portugal. Math. **43** (1985/86), no. 3, 377–392. MR 88f:15045

[11] Jacques Dixmier, *Quelques aspects de la théorie des invariants*, Gaz. Math. (1990), no. 43, 39–64. MR 90m:15047

[12] Clifford J. Earle, *On the moduli of closed Riemann surfaces with symmetries*, in Ahlfors et al. [1], 1971, pp. 119–130. MR 45 #5343

[13] Y. Fuertes and G. González-Diez, *Fields of moduli and definition of hyperelliptic covers*, Arch. Math. (Basel) **86** (2006), no. 5, 398–408. MR 2007f:14028

[14] August Freiherr von Gall, *Das vollständige Formensystem der binären Form 7^{ter} Ordnung*, Math. Ann. **31** (1888), no. 3, 318–336. MR 1510486

[15] Paul Gordan, *Beweis, dass jede Covariante und Invatiante einer binären Form eine ganze Function mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist*, J. Reine Angew. Math. **69** (1868), 323–354.

[16] J. H. Grace and A. Young, *The algebra of invariants*, Cambridge University Press, 1903.

[17] F. Hess, *An algorithm for computing isomorphisms of algebraic function fields*, in Buell [6], 2004, pp. 263–271. MR 2006d:11141

[18] Bonnie Huggins, *Fields of moduli of hyperelliptic curves*, Math. Res. Lett. **14** (2007), no. 2, 249–262. MR 2009a:14040

[19] Bonnie Sakura Huggins, *Fields of moduli and fields of definition of curves*, Ph.D. thesis, University of California, Berkeley, 2005. arXiv math/0610247 [math.NT]

[20] IEEE (ed.), *49th IEEE Symposium on Foundations of Computer Science (FOCS 2008), held in Philadelphia, October 25–28, 2008*, Los Alamitos, CA, Institute of Electrical and Electronics Engineers, IEEE Computer Society, 2008.

[21] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR 22 #5637

[22] Kiran S. Kedlaya and Christopher Umans, *Fast modular composition in any characteristic*, in IEEE [20], 2008, pp. 146–155.

[23] Shoji Koizumi, *The fields of moduli for polarized abelian varieties and for curves*, Nagoya Math. J. **48** (1972), 37–55. MR 50 #4582

[24] Reynald Lercier and Christophe Ritzenthaler, *Invariants and reconstructions for genus 2 curves in any characteristic*, available in MAGMA 2.15 [3] and later.

[25] ______, *Hyperelliptic curves and their invariants: Geometric, arithmetic and algorithmic aspects*, J. Algebra **372** (2012), 595–636. MR 2990029

[26] Jean-François Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, in Mora and Traverso [27], 1991, pp. 313–334. MR 92g:14022

[27] Teo Mora and Carlo Traverso (eds.), *Effective methods in algebraic geometry: Papers from the symposium (MEGA-90) held in Castiglioncello, April 17–21, 1990*, Progress in Mathematics, no. 94, Birkhäuser, Boston, 1991. MR 91m:14003

[28] David Mumford and John Fogarty, *Geometric invariant theory*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete, no. 34, Springer, Berlin, 1982. MR 86a:14006

[29] Peter J. Olver, *Classical invariant theory*, London Mathematical Society Student Texts, no. 44, Cambridge University Press, 1999. MR 2001g:13009

[30] Sander Matthijs van Rijnswou, *Testing the equivalence of planar curves*, Ph.D. thesis, Technische Universiteit Eindhoven, 2001. http://repository.tue.nl/543172

[31] Jean-Pierre Serre, *Corps locaux*, 2nd ed., Publications de l'Université de Nancago, no. VIII, Hermann, Paris, 1968. MR 50 #7096

[32] Tanush Shaska (ed.), *Computational aspects of algebraic curves*: *Papers from the conference held at the University of Idaho*, *Moscow*, *ID*, *May* 26–28, 2005, Lecture Notes Series on Computing, no. 13, World Sci. Publ., Hackensack, NJ, 2005. MR 2006e:14003

[33] Goro Shimura, *On the field of rationality for an abelian variety*, Nagoya Math. J. **45** (1972), 167–178. MR 46 #5342

[34] Tetsuji Shioda, *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89** (1967), 1022–1046. MR 36 #3790

[35] André Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524. MR 18,601a

REYNALD LERCIER: `reynald.lercier@m4x.org`
DGA MI, La Roche Marguerite, 35174 Bruz, France

and

Laboratoire IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes, France

CHRISTOPHE RITZENTHALER: `christophe.ritzenthaler@univ-rennes1.fr`
Institut de Mathématiques de Luminy, UMR 6206 du CNRS, Luminy, Case 907, 13288 Marseille, France
Current address: *Laboratoire IRMAR, UMR CNRS 6625, Campus de Beaulieu, 35042 Rennes, France*

JEROEN SIJSLING: `sijsling@gmail.com`
Laboratoire IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes, France
Current address: *Mathematics Institute, Zeeman Building, University of Warwick,*
Coventry CV4 7AL, United Kingdom

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

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

Electronic copies can be obtained free of charge from http://msp.org/obs/1 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

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

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

First published 2013.

msp

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