MATHEMATICS OF COMPUTATION
Volume 85, Number 300, July 2016, Pages 2011–2045
http://dx.doi.org/10.1090/mcom3032
Article electronically published on September 17, 2015

EXPLICIT GALOIS OBSTRUCTION AND DESCENT FOR HYPERELLIPTIC CURVES WITH TAMELY CYCLIC REDUCED AUTOMORPHISM GROUP

REYNALD LERCIER, CHRISTOPHE RITZENTHALER, AND JEROEN SIJSLING

Abstract. This paper is devoted to the study of the Galois descent obstruction for hyperelliptic curves of arbitrary genus whose reduced automorphism groups are cyclic of order coprime to the characteristic of their ground field. We give an explicit and effectively computable description of this obstruction. Along the way, we obtain an arithmetic criterion for the existence of a so-called hyperelliptic descent.

We define homogeneous dihedral invariants for general hyperelliptic curves, and show how the obstruction can be expressed in terms of these invariants. If this obstruction vanishes, then the homogeneous dihedral invariants can also be used to explicitly construct a model over the field of moduli of the curve; if not, then one still obtains a hyperelliptic model over a degree 2 extension of the field of moduli.

Introduction

The classical problem of Galois descent, as first considered by Weil in [19], is the following: Let X be a variety over the algebraic closure K of a perfect base field k. Suppose that X is isomorphic with all its Galois conjugates X^σ under the action of $\mathrm{Gal}(K|k)$, or in other words that k is the *(Galois) field of moduli* of X for the extension $K|k$. Does there then exist a model of X over k?

If such a model exists, then it is called a *descent* of X. Generically, or more precisely, when the geometric automorphism group of X is trivial, there is no obstruction to descent [19], but this partial answer is unsatisfactory, as there are many interesting classes of varieties with nontrivial automorphism group. This paper considers one such class, namely that of hyperelliptic curves. The explicit form of their defining equations makes hyperelliptic curves the simplest class of curves after conics and elliptic curves (for which the answer to the descent question is well known to be affirmative). Due to the presence of the hyperelliptic involution, hyperelliptic curves never have a trivial automorphism group. This makes them a fundamental example in the study of the descent problem.

The problem in fact allows a further refinement for hyperelliptic curves; instead of merely asking for some model over k, one can ask for a model that is again given by

Received by the editor February 20, 2013 and, in revised form, August 10, 2014 and January 6, 2015.

2010 *Mathematics Subject Classification.* Primary 14Q05, 13A50, 14H10, 14H25, 14H37.

Key words and phrases. Hyperelliptic curve, Galois descent, field of definition, field of moduli, invariants, genus 3.

The authors acknowledge support by grant ANR-09-BLAN-0020-01, and by the research programme *Investissements d'avenir* (ANR-11-LABX-0020-01) of the Centre Henri Lebesgue. The third author was additionally supported by a Marie Curie Fellowship IEF-GA-2011-299887.

©2015 American Mathematical Society

a hyperelliptic equation $y^2 = p(x)$. Let us call such a model a *hyperelliptic descent*. Considering the homogenization of p links the study of hyperelliptic descent with the study of homogeneous binary forms. This is a great benefit, since not only was the invariant theory of these forms extensively studied in the nineteenth century, but one can often also apply the *method of covariants*, as in [12].

The answer to the descent question for hyperelliptic curves depends on the *reduced automorphism group* $\overline{G}$ of X, which is the quotient of the automorphism group $G = \mathrm{Aut}(\mathsf{X})$ of X by the hyperelliptic involution. We assume that the characteristic of k does not equal 2 throughout this paper in order to describe hyperelliptic curves as separable covers of a conic over k. Under this running assumption, let us say that $\overline{G}$ is *tamely cyclic* if it is cyclic of order coprime to the characteristic of K. Then Huggins' seminal work [10] shows that if $\overline{G}$ is not tamely cyclic, then the curve X allows a hyperelliptic descent. For tamely cyclic $\overline{G}$, explicit counterexamples for descent were first constructed by Earle [6] and Shimura [16]. More recently, the full classification of the hyperelliptic curves that do not allow a hyperelliptic descent for the extension $\mathbb{C}|\mathbb{R}$ was initiated by Bujalance and Turbek [3] and completed by Huggins [9].

In Section 3, we give a complete answer to the descent problem in the case where X is a hyperelliptic curve with tamely cyclic reduced automorphism group, for any extension $K|k$. The problem is naturally stratified by our notion of the *type* of X, which contains information on the automorphism group and the Weierstrass points of X. We refer to Theorems 3.14 and 3.19 for precise statements, but essentially, once the type is given, then either all the curves of that type descend or the obstruction is classified by the solvability of a certain norm equation.

If the descent obstruction vanishes, then Section 3 also shows how a descent can be effectively constructed if $\overline{G}$ is nontrivial. In Section 3.4, we consider the slightly more involved case when $\overline{G}$ is trivial. In this case, efficient algorithms are constructed by using the covariant method from [12]. Finally, in Section 3.5, we show how to construct essentially all counterexamples to descent, which recovers the aforementioned results on the extension $\mathbb{C}|\mathbb{R}$ as a special case. More precisely, given any quadratic extension of fields $L|k$, Theorem 3.26 gives a completely explicit description of the K-isomorphism classes of the curves which are defined over L and K-isomorphic with their conjugate, but that do not descend to k.

The norm equation mentioned above is in fact determined purely by the *homogeneous dihedral invariants* of the curve X. These invariants, which will be discussed in Section 2, are closely related with and indeed named after the dihedral invariants defined by Gutierrez and Shaska [7]. Like these invariants, they can be calculated quickly once the curve X is given in standard form, a transformation to which can be determined effectively by using the methods in [12, Sec. 2]. However, there are a few important differences between our dihedral invariants and the original ones in [7].

First of all, the models from which we derive our homogeneous dihedral invariants are normalized in a weaker way than in [7]. Second, the homogeneous dihedral invariants give an effective approach to the reconstruction and parametrization of forms with given invariants, also in the nongeneric cases where many of the coefficients in these normal forms are zero. Third, and contrary to what is suggested in Lemma 3.2 and Theorem 4.5 in [7], such nongeneric reconstruction is in fact more involved than that in the generic case. Finally, the claimed reconstruction over the field of moduli k in [7, Thm. 4.5] actually takes place over a quadratic extension of k, as was already pointed out in [11, Rem. 4.17]. In particular, [7, Cor. 4.6] is incorrect, as can also be seen from the results in [10, Sec. 6] and our complete classification of the counterexamples in Theorem 3.14.

To describe our invariants, consider the subgroup D of GL_2 consisting of diagonal and anti-diagonal matrices. Then the homogeneous dihedral invariants are the invariants of binary forms under the action of the group $D \cap \mathrm{SL}_2(K)$ that are, moreover, homogeneous as a function in the defining coefficients of these forms. Alternatively, they are those $D \cap \mathrm{SL}_2(K)$-invariant polynomials in the defining coefficients for which the action by the diagonal subgroup of GL_2 is described by a character. All invariants for $D \cap \mathrm{SL}_2(K)$ (hence in particular the invariants for D itself) can be expressed as a rational function in the homogeneous dihedral invariants.

Before defining the homogeneous dihedral invariants and proving the main theorem, we need a result relating the existence of a general descent with that of a hyperelliptic descent. This theme is explored in Section 1. Building on results by Mestre [13] and Huggins [10], we shall show in Theorem 1.6 that these two variants of the descent problems are in fact equivalent, except possibly when the genus g of X is odd and its reduced automorphism group is tamely cyclic of odd order. In this latter case, Theorem 3.19 shows that a descent always exists. Furthermore, we completely classify the counterexamples to this equivalence in this remaining case in Theorem 3.26.

Even more surprising is that the existence of a hyperelliptic descent of X turns out to allow an arithmetic characterization. To formulate this result, consider the quotient $B = \mathsf{X}/G$ of X by its full automorphism group. The curve B has a canonical descent B_0 to k, and it is well known (see for example [5, Cor. 2.3]) that the presence of a point of B_0 over the field of moduli is a *sufficient* condition for *some* descent of X to exist. In Theorem 1.13, we show that in fact the existence of such a rational point is *equivalent* to the existence of a *hyperelliptic* descent of X. In particular, we see that X always admits a hyperelliptic equation over a degree 2 extension of k.

These results simplify matters from a theoretical point of view. The more general obstruction criterion in [5, Sec. 4] describes the descent obstruction in terms of the triviality of one of *infinitely* many element of H^2-cohomology groups. For hyperelliptic curves, the descent obstruction turns out to be equivalent to the triviality of a single twist (namely B_0) of $\mathbb{P}^1_k$. Alternatively, this amounts to the triviality of a *single* element of an H^1-cohomology group. It is this pleasant surprise that makes the theory of Galois descent for hyperelliptic curves both conceptually simple and effectively computable.

After the proof of Theorems 3.14 and 3.19, we turn to algorithmic considerations and the implementation of our results in Section 4. Our `Magma` [1] functionality is available online[1]. We also discuss how this implementation can be combined with the results of [11]. This concludes the exploration of the arithmetic aspects of the moduli space of hyperelliptic genus 3 curves started in that article; it shows how to reconstruct any given genus 3 curve from its invariants over an extension of the field of moduli of minimal degree (which we now know to be at most 2). This

[1] `http://perso.univ-rennes1.fr/christophe.ritzenthaler/programme/hyp-desc.tgz`

additional functionality has been added to the package `g3twists`[2], and is included in the current versions of `Magma`. Section 5 concludes the paper and briefly discusses the remaining open questions on the descent of hyperelliptic curves.

Table 1 gathers our state of knowledge (we **emphasize** what is proved in the present paper).

TABLE 1. Issues addressed in the present paper.

$\overline{G}$	Condition	Descent ⇔ Hyperelliptic descent	Obstruction to descent	Effective Method
Not tamely cyclic	-	Yes [9]	No [9]	?
Tamely cyclic and $\#\overline{G} > 1$	g odd and $\#\overline{G}$ odd	**No** Ex. 4.6	**No** Thm. 3.19	**Yes** Alg. 3.20
	g even or $\#\overline{G}$ even	**Yes** Thm. 1.6	**Yes** Thm. 3.14	**Yes** Alg. 3.18
$\#\overline{G} > 1$	g odd	No [11]	No [11]	**Generic** if $g \leq 2^7$ Rem. 3.23
	g even	Yes [13]	Yes [13]	**Generic** if $g \leq 2^7$ Rem. 3.23

Notation. We let k be a perfect field of odd characteristic, and we let K denote its algebraic closure. We denote $\Gamma = \mathrm{Gal}(K|k)$. The curves over K and its subfields that are considered in this paper will be smooth, proper and geometrically irreducible throughout. We define a *hyperelliptic curve* over k as in [11, Sec. 1.2]; that is, a curve C over k is hyperelliptic if and only if it admits a degree 2 morphism to $\mathbb{P}^1_K$ over K. In this case, C admits a unique corresponding *hyperelliptic involution* ι for which the quotient C/ι is a conic over k.

In what follows, X denotes a hyperelliptic curve over K of genus g whose field of moduli with respect to the extension $K|k$ equals k. We denote the group $\mathrm{Aut}(\mathsf{X})$ of automorphisms of X defined over K by G. The *reduced automorphism* group $\overline{G} = G/\iota$ is the quotient of G by the central element ι. In the second half of this paper, we will additionally suppose that $\overline{G}$ is *tamely cyclic*, *i.e.*, cyclic of order coprime to the characteristic of K. Finally, given a curve X and a divisor $\mathcal{D}$, we denote the group of automorphisms α of X over K such that the pushforward $\alpha_*(\mathcal{D})$ equals $\mathcal{D}$ by $\mathrm{Aut}(\mathsf{X}, \mathcal{D})$.

We will occasionally construct a model of X over an intermediate field $k \subseteq L \subseteq K$. When considering such curves over intermediate fields, we restrict our consideration of morphisms to those defined over L, unless explicitly specified otherwise. We denote the corresponding automorphism groups by $\mathrm{Aut}_L(\mathsf{X})$, etc.

If $\varphi : \mathsf{X} \to \mathsf{Y}$ is a morphism between algebraic curves, then the *ramification divisor* of φ is the divisor of the points on X that ramify under φ. The *branch divisor* of φ is the image of this divisor under φ_*. Note that we use these divisors without multiplicities throughout.

[2] `http://perso.univ-rennes1.fr/christophe.ritzenthaler/programme/g3twists_v1.1.tgz`

We adopt the usual notation of denoting the Galois action by a superscript, e.g., f^σ for the conjugation on a binary form. We consider this as a left action, which leads to the somewhat counterintuitive equality $f^{\sigma\tau} = (f^\tau)^\sigma$.

We use the notation $\mathbf{C}_n$ (resp. $\mathbf{D}_{2n}$) for the cyclic group with n elements (resp. the dihedral group with $2n$ elements. Given two homogeneous binary forms f_1 and f_2 over a subfield L of K, we say that $f_1 \sim f_2$ if there exists a λ in L^* such that $f_1 = \lambda \cdot f_2$. Given a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ over K, we let $A.f$ be the polynomial given by $(A.f)(x, z) = f(A^{-1}(x, z))$. Finally, given a binary form f over K, we denote by $\mathrm{Aut}(f)$ the group of matrices A up to scalar in $\mathrm{PGL}_2(K)$ such that $A.f \sim f$.

By ζ_n, we denote a fixed choice of n-th roots of unity in K; these roots are chosen in such a way to respect the standard compatibility conditions when raising to powers. The cyclic groups $\mathbf{C}_n = \mathbb{Z}/n\mathbb{Z}$ are always considered as being embedded in $\mathrm{PGL}_2(K)$, by sending the generator 1 of $\mathbf{C}_n$ to the automorphism acting by $(x : z) \mapsto (\zeta_n x : z)$.

Throughout, we usually denote objects that are defined over the ground field k by a zero-subscript, so that, for example, X_0 is typically a hyperelliptic curve over k.

1. Descent and hyperelliptic descent

Consider a perfect field k of odd characteristic, and let K be the algebraic closure of k. Let $\Gamma = \mathrm{Gal}(K|k)$, and let C be a curve over K.

Definition 1.1. The *(Galois) field of moduli* of C with respect to the extension $K|k$ is the fixed field of the group $\{\sigma \in \Gamma : \mathsf{C} \text{ is isomorphic to } \mathsf{C}^\sigma \text{ over } K\}$.

Remark 1.2. For more general extensions $K|k$, one usually defines the field of moduli of C with respect to $K|k$ as the intersection of all fields of definition of C that are contained in K. The Galois field of moduli in the previous definition is then a purely inseparable extension of this more general field of moduli by [14]. We refer to Section 5 for some open questions concerning these matters.

Definition 1.3. Let $L \subset K$ be a subfield of K containing k. A *model* of C over L is a curve C_0 over L such that C is isomorphic to C_0 over K. The field L is then called a *field of definition* for C.

A model of C over its field of moduli is called a *descent* of C. If such a model exists, then C is said to *descend* (to its field of moduli). If not, then we say that there is *descent obstruction* for C.

For hyperelliptic curves, one can ask for a more specific form of descent.

Definition 1.4. Let X be a hyperelliptic curve over K of genus g whose field of moduli for the extension $K|k$ equals k. A *hyperelliptic descent* of X is a model X_0 of X over k that is defined by a homogeneous polynomial $f_0(x, z)$ of degree $2g + 2$ over k without repeated roots. More precisely, this is to say that X_0 is the desingularization of the curve $y^2 = f_0(x, z)$ in the $(1, 1, g + 1)$-weighted projective (x, z, y)-space over k.

Remark 1.5. There is a slight ambiguity to be noted. According to Definition 1.4, any descent X_0 of a hyperelliptic curve X is in fact hyperelliptic as a curve over k. However, such a descent is not always a hyperelliptic descent; this is the case if and only if the quotient Q_0 of X_0 by its hyperelliptic involution ι_0 is isomorphic to $\mathbb{P}^1$ over k.

1.1. **Equivalence between descent and hyperelliptic descent.** A fundamental result of Mestre [13] tells us that if g is even, then the curve X descends if and only if it descends hyperelliptically. However, when $g \geq 3$ is odd, this need not be the case. A counterexample is given in the discussion after [11, Prop. 4.13]. Due to the simpler nature of hyperelliptic descent, we now study in which other cases the equivalence indicated by Mestre continues to hold.

It turns out that the answer to this question depends on the reduced automorphism group $\overline{G} = \mathrm{Aut}(\mathsf{X})/\iota$. To get an idea of the problem, we first consider the case of trivial $\overline{G}$. As in [11, Sec. 4.3], one shows that degree 2 covers of pointless conics over k whose branch locus is Galois stable give rise to curves over K that have trivial reduced automorphism group and nontrivial descent obstruction. Therefore in this case there exist curves that descend but do not descend hyperelliptically. Number fields are an important and naturally occurring class of fields over which such covers of conics exist.

The previous paragraph can be seen as one of the few exceptions to the main statement of the following theorem, which we will prove in this section, and which we will later use to give an arithmetic criterion for the existence of a hyperelliptic descent in Theorem 1.13.

Theorem 1.6. *Let X be a hyperelliptic curve over K of genus g whose field of moduli for the extension $K|k$ equals k. Let $\overline{G}$ be the reduced automorphism group of X. Then the existence of a descent of X is equivalent to the existence of a hyperelliptic descent, except possibly when g is odd and $\overline{G}$ is tamely cyclic of odd cardinality.*

Remark 1.7. In the remaining case where g and $\#\overline{G}$ are both odd, we refer the reader to Theorem 3.19 for a proof that X always descends. Moreover, in Example 4.6 we will explicitly construct a hyperelliptic curve with nontrivial reduced automorphism group and field of moduli $\mathbb{Q}$ that descends, but does not descend hyperelliptically.

Remark 1.8. An arithmetic criterion for the existence of a hyperelliptic descent is given in Theorem 1.13.

In order to prove Theorem 1.6, we will first need a few technical lemmata to deal with the case where the reduced automorphism group contains an element of order 2. The first such lemma is Lemma 3.1 from [20], there attributed to Poonen and to Witt before him. Here we give a stronger version of this result.

Lemma 1.9. *Let $f : \mathsf{Q}_0 \to \mathsf{B}_0$ be a nonconstant morphism between genus 0 curves over k of degree n.*

(1) If n is even, then B_0 is isomorphic with $\mathbb{P}^1$ over k.
(2) If n is odd, then B_0 is isomorphic with Q_0 over k.

Proof. As in the proof of [20, Lem.3.1], one shows that the class of Q_0 in the Brauer group of k is n times that of B_0. The result then follows from the fact that these classes are 2-torsion elements. □

We will now apply Lemma 1.9 in the situation of interest to us. In what follows, our frequent hypothesis that Q_0 not be isomorphic to $\mathbb{P}^1$ is not always necessary, but we will only need the lemmata in this case. Moreover, our current exposition allows for a more unified treatment of finite and infinite base fields k.

Lemma 1.10. *Let* Q_0 *be a genus* 0 *curve over* k *that is not isomorphic to* $\mathbb{P}^1$ *over* k*, and let* $\alpha_0 \in \mathrm{Aut}_k(\mathsf{Q}_0)$ *be an automorphism of order* 2 *of* Q_0 *that is defined over* k*. Then there exists a* k*-rational divisor* $\mathcal{R}_0$ *of degree* 6 *on* Q_0 *such that* $\mathrm{Aut}_K(\mathsf{Q}_0, \mathcal{R}_0)$ *is generated by* α_0*.*

Proof. Consider the morphism from the affine space $\mathbb{A}^3$ to the moduli space $\mathcal{M}_2$ of genus 2 curves that sends a triple (λ, μ, ν) to the curve $\mathsf{X}_{\lambda,\mu,\nu}$ given by the hyperelliptic equation $y^2 = (x^2 - \lambda)(x^2 - \mu)(x^2 - \nu)$. The results in [4] show that the locus $\mathcal{L}$ of $\mathbb{A}^3$ for which the reduced automorphism group of $\mathsf{X}_{\lambda,\mu,\nu}$ is strictly larger than $\mathbf{C}_2$ is of codimension 1 in $\mathbb{A}^3$.

Now let $\pi_0 : \mathsf{Q}_0 \to \mathsf{Q}_0/\alpha_0$ be the quotient morphism. We choose coordinates over K, that is to say, K-isomorphisms $\varphi : \mathsf{Q}_0 \to \mathbb{P}^1$ and $\psi : \mathsf{Q}_0/\alpha_0 \to \mathbb{P}^1$. Using the three-transitivity of $\mathrm{Aut}_K(\mathbb{P}^1)$, we see that we can do this in such a way that the coordinatization $\psi\pi_0\varphi^{-1}$ of the projection π is given by the degree 2 map $(x : z) \mapsto (x^2 : z^2)$. Let q, r, s be three points on Q_0/α_0 that are not branch points of π_0. Then under our coordinatization, and considering $\mathbb{A}^1$ as a subvariety of $\mathbb{P}^1$ via the coordinate $t = x/z$, the divisor $\mathcal{R} = \pi_0^{-1}(r + s + t)$ on Q_0 is isomorphic over K to the divisor $\psi^*(r) + \psi^*(s) + \psi^*(t)$. Therefore the hyperelliptic curve defined by taking a degree 2 cover of Q_0 ramified over $\mathcal{R}$ is isomorphic to the curve $\mathsf{X}_{\psi(r),\psi(s),\psi(t)}$.

The transformation $\psi^{-1}(\mathcal{L})$ of the exceptional locus $\mathcal{L} \subset \mathbb{A}^3$ is a codimension 1 locus in $(\mathsf{Q}_0/\alpha_0)^3$. Note that k is infinite by the existence of Q_0. This implies that the set of k-rational points is dense in Q_0/α_0, which is isomorphic with $\mathbb{P}^1_k$ by Lemma 1.9(i). Therefore we can find a rational point (r_0, s_0, t_0) of $(\mathsf{Q}_0/\alpha_0)^3$ outside the exceptional locus. By construction, the divisor $\mathcal{R}_0 = \pi^{-1}(r_0 + s_0 + t_0)$ now satisfies our requirements. ∎

Lemma 1.11. *Let* Q_0 *be a genus* 0 *curve over* k *that is not isomorphic with* $\mathbb{P}^1$ *over* k*, and let* α_0 *be an automorphism of order* 2 *of* Q_0 *that is defined over* k*. Then there exists a quadratic extension* L *of* k *and an isomorphism* $\varphi : \mathsf{Q}_0 \to \mathbb{P}^1$ *over* L *such that* $\varphi^\sigma = \varphi\alpha$ *for the generator* σ *of* $\mathrm{Gal}(L|k)$*.*

Proof. Choose $\mathcal{R}_0$ as in Lemma 1.10 and consider the pair $(\mathsf{Q}_0, \mathcal{R}_0)$, which is defined over k. Over K, there exists a degree 2 cover X of Q_0 branched in $\mathcal{R}_0$, which has reduced geometric automorphism group $\mathbf{C}_2$. We emphasize that *a priori* the cover X need not be defined over k, even though $(\mathsf{Q}_0, \mathcal{R}_0)$ is.

Regardless, the field of moduli of X with respect to the extension $K|k$ equals k. Indeed, the configuration $(\mathsf{Q}_0, \mathcal{R}_0)$, which determines the isomorphism class of X over K, is Galois stable. Alternatively, if we choose some K-isomorphism $i : \mathsf{Q}_0 \to \mathbb{P}^1$, then we have $(i_*(\mathcal{R}_0))^\sigma = i_*^\sigma(\mathcal{R}_0^\sigma) = i_*^\sigma(\mathcal{R}_0)$ for $\sigma \in \Gamma$. This shows that $i_*(\mathcal{R}_0)$, which is the branch locus of X, and $(i_*(\mathcal{R}_0))^\sigma$, which is the branch locus of X_0^σ, differ by the K-automorphism $i_*^\sigma i_*^{-1}$ of $\mathbb{P}^1$. We see that the branch loci of X_0 and X_0^σ, considered as degree 2 covers, can be transformed into one another over K. The hyperelliptic curves X_0 and X_0^σ are therefore K-isomorphic.

By [4, Thm. 6], this implies that the genus 2 curve X is hyperelliptically defined over k. The descent morphism $\mathsf{X} \to \mathsf{X}_0$ to a model X_0 over k then yields an isomorphism

$$\varphi : (\mathsf{Q}_0, \mathcal{R}_0) \longrightarrow (\mathbb{P}^1, \mathcal{S}_0)$$

over some Galois extension M of k. Then the map $\mathrm{Gal}(M|k) \to \mathrm{Aut}_K(\mathsf{Q}_0, \mathcal{R}_0) = \langle \alpha \rangle$ that sends τ to $\varphi^{-1}\varphi^{\tau}$ is a homomorphism because $\mathrm{Aut}_K(\mathsf{Q}_0, \mathcal{R}_0) = \mathrm{Aut}_k(\mathsf{Q}_0, \mathcal{R}_0)$. Indeed, we have $\varphi^{-1}\varphi^{\tau_1\tau_2} = \varphi^{-1}\varphi^{\tau_1}(\varphi^{-1})^{\tau_1}\varphi^{\tau_1\tau_2} = \varphi^{-1}\varphi^{\tau_1}\varphi^{-1}\varphi^{\tau_2}$.

The kernel of this homomorphism is not all of $\mathrm{Gal}(M|k)$, because that would imply that Q_0 is isomorphic to $\mathbb{P}^1$ over k. So this kernel cuts out a quadratic extension L of k. By construction, φ is then defined over L, and we have that $\varphi^{\sigma} = \varphi\,\alpha_0$. □

Proposition 1.12. *Let* X_0 *be a hyperelliptic curve over* k. *Suppose that the reduced automorphism group* $\overline{G}$ *of* X *contains an element* α_0 *of order* 2 *that is defined over* k. *Then* X_0, *considered as a curve over* K, *descends hyperelliptically to* k.

Proof. Let ι_0 be the hyperelliptic involution of X_0. Then ι_0 is defined over k, because it is the unique involution of X_0 for which the quotient $\mathsf{Q}_0 = \mathsf{X}_0/\iota_0$ is of genus 0. Consider Q_0 as a curve over k. If Q_0 is isomorphic to $\mathbb{P}^1$ over k, then we are done. So assume the contrary.

Let $\mathcal{R}_0$ be the branch locus of the quotient morphism $\mathsf{X}_0 \to \mathsf{Q}_0$. Let α_0 be the nontrivial geometric automorphism of $(\mathsf{Q}_0, \mathcal{R}_0)$; it is unique by hypothesis. By uniqueness, α_0 is defined over k, as are Q_0 and $\mathcal{R}_0$. Choose L and φ as in Lemma 1.11. The divisor $\mathcal{S}_0 = \varphi_*(\mathcal{R}_0)$ is L-rational, but it is even k-rational since

$$\mathcal{S}_0^{\sigma} = (\varphi_*(\mathcal{R}_0))^{\sigma} = \varphi_*^{\sigma}(\mathcal{R}_0^{\sigma}) = (\varphi\alpha)_*(\mathcal{R}_0) = \varphi_*(\alpha_*(\mathcal{R}_0)) = \varphi_*(\mathcal{R}_0) = \mathcal{S}_0.$$

Now the degree 2 cover of $\mathbb{P}^1$ with branch locus $\mathcal{S}_0$ is K-isomorphic to X. So since X is K-isomorphic to a degree 2 cover of $\mathbb{P}^1$ branching over a k-rational divisor, it admits a hyperelliptic equation over k. □

Proof of Theorem 1.6. The case of even g is due to Mestre in [13], and Huggins proved the result in the case where $\overline{G}$ is not tamely cyclic in [10, Thm. 5.4]. As for the case where $\overline{G}$ is tamely cyclic of even order, this yields a pair $(\mathsf{Q}_0, \mathcal{R}_0)$ as in the proof of Proposition 1.12 whose reduced automorphism group is cyclic of even cardinality. Such a subgroup has a unique element α_0 of order 2, which is then defined over k by uniqueness. It now suffices to invoke Proposition 1.12. □

1.2. **An arithmetic criterion for hyperelliptic descent.** We can now characterize arithmetically whether a hyperelliptic curve X allows a hyperelliptic descent. Denote the quotient X/G by B. By construction, B has a canonical Weil descent datum. Let B_0 be the corresponding model over k; its k-isomorphism class depends only on the K-isomorphism class of X. It is well known (cf. the discussion in [5, Cor. 2.3]) that the existence of a k-rational point on B_0 implies that X descends.

Theorem 1.13. *Let* X *be a hyperelliptic curve over* K *of genus* g *whose field of moduli for the extension* $K|k$ *equals* k. *Let* $\overline{G}$ *be the reduced automorphism group of* X. *Then* X *descends hyperelliptically if and only if the canonical model* B_0 *of the quotient* $\mathsf{B} = \mathsf{X}/G$ *has a* k*-rational point.*

Proof. If X admits a hyperelliptic descent X_0, then B_0 has a rational point. Indeed, the curve B_0 can then be obtained as the quotient of $Q_0 = \mathsf{X}_0/\iota_0 \cong \mathbb{P}^1$ by the reduced automorphism group $\overline{G}_0$ of X_0. Note that $\overline{G}_0$ is defined over k, though its individual elements might not be.

Conversely, if B_0 has a k-rational point, then a descent X_0 of X exists by [5]. In light of Theorem 1.6, it then only remains to consider the case where the reduced automorphism group of X_0 is tamely cyclic of odd order. So again let Q_0 be the quotient of X_0 by its hyperelliptic involution. We get a map $\mathsf{Q}_0 \to \mathsf{B}_0$ of odd degree, so that Lemma 1.9(ii) allows us to conclude that Q_0 is isomorphic to $\mathbb{P}^1$ over k as well. Therefore X_0 is a degree 2 cover of $\mathbb{P}^1$ over k, so that X indeed descends hyperelliptically. □

The next proposition gives a concrete criterion for the presence of a rational point on B_0, which we will use in Section 3. As usual, we define the *twist* of a curve C over k to be a curve C' over k that is isomorphic with C over K; we refer to [15, Ch. III.1] for a correspondence between the set of isomorphism classes of twists of C and the Galois cohomology set $H^1(\mathrm{Gal}(K|k), \mathrm{Aut}_K(\mathsf{C}))$.

Proposition 1.14. *Let L be a quadratic extension of k, and let σ be the non-trivial element of $\mathrm{Gal}(L|k)$. Let $\alpha_0 \in \mathrm{Aut}_k(\mathbb{P}^1)$ be a k-automorphism of $\mathbb{P}^1$ of order two defined over k, represented by an element M_0 of $\mathrm{GL}_2(k)$. Let c_K be the element of $H^1(\mathrm{Gal}(K|k), \mathrm{Aut}_K(\mathbb{P}^1))$ obtained by inflating the cocycle $c_L \in H^1(\mathrm{Gal}(L|k), \mathrm{Aut}_L(\mathbb{P}^1)) = \mathrm{Hom}(\mathrm{Gal}(L|k), \mathrm{Aut}_L(\mathbb{P}^1))$ that sends σ to α_0. Then the twist of $\mathbb{P}^1$ over k determined by c_K is isomorphic to $\mathbb{P}^1$ over k if and only if $-\det(M_0)$ is a norm for the extension $L|k$.*

Proof. Since the characteristic polynomial of M_0 is $x^2 - \nu_0$ for some $\nu \in k$, its Frobenius companion matrix equals $\left(\begin{smallmatrix} 0 & \nu_0 \\ 1 & 0 \end{smallmatrix}\right)$. The twist corresponding to c_K is isomorphic to $\mathbb{P}^1$ over k if and only if c_K is a coboundary. This is the case if and only if there exists an invertible matrix N over L such that we have the equality $N^\sigma M_0 = N$ in $\mathrm{PGL}_2(L)$, or more explicitly, if there exists some scalar $\lambda \in L$ such that

$$N^\sigma = \lambda N \left(\begin{smallmatrix} 0 & \nu_0 \\ 1 & 0 \end{smallmatrix}\right)^{-1} . \tag{1.1}$$

Conjugating N by σ twice and using (1.1), we get that $\lambda \in L$ and $\lambda^\sigma \lambda = \nu_0$, which shows that our condition is necessary. Conversely, if such a λ exists, then we can take

$$N = \left(\begin{smallmatrix} 1 & \lambda^\sigma \\ \beta & \lambda^\sigma \beta^\sigma \end{smallmatrix}\right),$$

where β is any generator of L over k. □

2. Invariants

Let X be a hyperelliptic curve of genus g over K, defined by a homogeneous binary form f over K of degree $2g + 2$. Suppose that the reduced automorphism group $\overline{G}$ of X over K is tamely cyclic of order $n > 1$. In this section we will construct invariants of f that can be used to determine the descent obstruction (general or hyperelliptic) for X, as well as a corresponding descent of X if one of these obstructions vanishes. To this end, we first construct geometric normal forms for f. Modulo a normalization that we do not make, the discussion at the beginning of this section is completely analogous to that in [7, Sec. 2].

Since we assumed that the reduced automorphism group of X is tame, we can diagonalize one of its generators α over K. Making the corresponding change of basis if necessary, we may therefore suppose that, using the notation in the introduction,

$$\overline{G} = \mathbf{C}_n = \langle \alpha \rangle . \tag{2.1}$$

The elements of $\overline{G}$ then only have fixed points at $(0 : 1)$ and $(1 : 0)$. Since we know that the binary form f defining X is of even degree without repeated roots, this implies that f has one of the *normal forms* over K figuring in the following definition.

Definition 2.1. Let n, m be positive integers. A binary form f of even degree is said to be *of type* $(0, n, m)$, resp. $(1, n, m)$, resp. $(2, n, m)$, if it is of the form

$$f = a_m x^{mn} + a_{m-1} x^{(m-1)n} z^n + \ldots + a_1 x^n z^{(m-1)n} + a_0 z^{mn}, \quad \text{resp.,} \tag{2.2}$$

$$f = z(a_m x^{mn} + a_{m-1} x^{(m-1)n} z^n + \ldots + a_1 x^n z^{(m-1)n} + a_0 z^{mn}), \quad \text{resp.,} \tag{2.3}$$

$$f = xz(a_m x^{mn} + a_{m-1} x^{(m-1)n} z^n + \ldots + a_1 x^n z^{(m-1)n} + a_0 z^{mn}), \tag{2.4}$$

for some m and n, while also satisfying the following properties:

(i) $\mathrm{Aut}(f)$ coincides with the group $\mathbf{C}_n$ from (2.1), and
(ii) f has no repeated linear factors.

Remark 2.2. We impose condition (ii) in Definition 2.1 to ensure that the forms f under consideration define nonsingular hyperelliptic curves. Condition (i) will hold for generic forms f as in (2.2)–(2.4). It is important that we restrict ourselves to this generic case by imposing (i), since the statement of our Theorem 3.14 essentially depends on the value of m, which in turn depends on that of n once the degree of f is fixed.

As in [7] or [2, Stz. 5.2], a calculation shows the following.

Proposition 2.3. *The automorphism groups* $\mathrm{Aut}(\mathsf{X})$ *of the hyperelliptic curves* $\mathsf{X} : y^2 = f(x, z)$ *defined by the forms in Definition* 2.1 *are as follows.*

(i) If f is of type $(0, n, m)$, then $\mathrm{Aut}(\mathsf{X})$ is isomorphic to the group $\mathbf{C}_2 \times \mathbf{C}_n$, generated by $(x : z : y) \mapsto (\zeta_n x : z : y)$ and $(x : z : y) \mapsto (x : z : -y)$.
(ii) If f is of type $(1, n, m)$, then $\mathrm{Aut}(\mathsf{X})$ is isomorphic to the group $\mathbf{C}_{2n}$, generated by $(x : z : y) \mapsto (\zeta_n x : z : -y)$.
(iii) If f is of type $(2, n, m)$, then $\mathrm{Aut}(\mathsf{X})$ is isomorphic to the group $\mathbf{C}_{2n}$, generated by $(x : z : y) \mapsto (\zeta_n x : z : \zeta_{2n} y)$.

Our methods now diverge from those of [7]; we do not further normalize to suppose $a_m = a_0 = 1$ so as to avoid breaking symmetry. This will make it easy to transform f to a normal form over an at worst quadratic extension of the base field k, as we shall see in Proposition 3.4.

2.1. **Restricting isomorphisms.** We start by determining the possible isomorphisms between two binary forms of type (i, n, m). Let $T \subset \mathrm{GL}_2(K)$ be the subgroup of diagonal matrices and define

$$D = \langle T, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle, \tag{2.5}$$

which is an extension of $\mathbb{Z}/2\mathbb{Z}$ by T.

Proposition 2.4. *Consider two binary forms f, f' of type (i, n, m) with $n > 1$. Suppose that $A \in \mathrm{GL}_2(K)$ is such that $f' \sim A.f$. Then $A \in D$ and, moreover, $A \in T$ if $i = 1$.*

Proof. Under the hypotheses of the proposition, we have that

$$AgA^{-1}f' \sim AgA^{-1}Af \sim Agf \sim Af \sim f'$$

for all $g \in \mathrm{Aut}(f)$ or, in other words, $A\,\mathrm{Aut}(f)A^{-1} \subset \mathrm{Aut}(f')$. Since hypothesis (i) in Definition 2.1 is verified for both f and f', we therefore see that $A\mathbf{C}_n A^{-1} = \mathbf{C}_n$, showing that A is indeed in the normalizer of $\mathbf{C}_n$. The inclusion $A \in D$ then results from the description of this normalizer in [10, Lem. 3.3].

In the case $i = 1$ we can conclude that $A \in T$ because the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ sends z to x, which is impossible since f being of type $(1, n, m)$ implies that the coefficients in (2.3) satisfy $a_m a_0 \neq 0$. □

In the following exposition, we will first focus on the normal form (2.2) with $m = 2\ell$ even. The other cases are discussed in Section 2.4.

2.2. **Homogeneous diagonal invariants.** We want to develop the invariant theory of binary forms of type $(0, n, 2\ell)$ under the action of the group D. We first consider the action of the simpler index 2 subgroup T of D. On the coefficients in (2.2), the action of an element $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ of T is given by

$$(a_m, a_{m-1}, \ldots, a_1, a_0) \longmapsto (\lambda^{mn} a_m, \lambda^{(m-1)n} \mu^n a_{m-1}, \ldots, \lambda^n \mu^{(m-1)n} a_1, \mu^{mn} a_0). \tag{2.6}$$

We now wish to consider the homogeneous invariants under this action, that is, those polynomial expressions that are actually invariant under the action of the proper subgroup $T \cap \mathrm{SL}_2(K)$ of T. The ring of these invariants admits a weight decomposition under the action of the full group T; an element I is of weight w if $A \in T$ sends I to $\det(I)^{w\ell} I$. More intuitively, this simply means that I has degree w as a homogeneous polynomial.

We will construct small systems of invariants that allow us to distinguish the orbits of binary forms of type $(0, n, m)$ under the action of T. First we consider the following homogeneous invariants for the action of T, which will turn out to suffice for distinguishing most of these binary forms:

$$\begin{array}{lrcll}
\text{Degree } 1: & J_1 & = & a_\ell, & \\
\text{Degree } 2: & J_{2,0} & = & a_{2\ell} a_0, & J_{2,1} = a_{2\ell-1} a_1, \ \ldots, \ J_{2,\ell-1} = a_{\ell+1} a_{\ell-1}, \\
\text{Degree } 3: & J_3 & = & a_{\ell+2} a_{\ell-1}^2 & \\
\text{Degree } 4: & J_4 & = & a_{\ell+3} a_{\ell-1}^3 & \\
 & & \vdots & & \\
\text{Degree } \ell+1: & J_{\ell+1} & = & a_{2\ell} a_{\ell-1}^\ell. &
\end{array}$$

The first index for these invariants indicates their homogeneous degree.

Definition 2.5. We call the invariants $J_1, J_{2,0}, \ldots, J_{2,\ell-1}, J_3, \ldots J_{\ell+1}$, defined above, the *generic homogeneous diagonal invariants* (for binary forms of type $(0, n, m)$).

Example 2.6. For forms f of type $(0, n, 4)$ given by $f = a_4 x^{4n} + a_3 x^{3n} z^n + a_2 x^{2n} z^{2n} + a_1 x^n z^{3n} + a_0 z^{4n}$, the generic homogeneous diagonal invariants are given by $J_1 = a_2$, $J_{2,0} = a_4 a_0$, $J_{2,1} = a_3 a_1$ and $J_3 = a_4 a_1^2$. Note that the case $n = 2$ yields a class of hyperelliptic genus 3 curves with extra involutions.

Using the generic homogeneous dihedral invariants already suffices to deal with most binary forms of type $(0, m, n)$:

Proposition 2.7. *Suppose that f and f' are binary forms of type $(0, n, m)$ such that*

$$a_{2\ell}, a_{2\ell-1}, \ldots, a_{\ell+2}, a_{\ell-1} \neq 0$$

and

$$a'_{2\ell}, a'_{2\ell-1}, \ldots, a'_{\ell+2}, a'_{\ell-1} \neq 0.$$

If the generic homogeneous diagonal invariants J and J' of f and f' define the same point in the corresponding weighted projective space, then there exists an $A \in T$ such that $f' \sim A.f$.

Proof. Scaling if necessary, we may suppose that J and J' are equal. Then a suitable modification by a matrix of the form $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ can be used to ensure that $a_{\ell-1} = a'_{\ell-1}$. This does not affect the equality of J and J' since this matrix has trivial determinant. Our result is now clear, since the other a_i can be read off from the values of the generic homogeneous diagonal invariants once $a_{\ell-1} \neq 0$ is known. □

In the nongeneric case (i.e., when one of the conditions of Proposition 2.7 is not satisfied), the construction of the appropriate homogeneous diagonal invariants is slightly more complicated. To proceed in these cases, we first note that the set of indices of the coefficients a_j of f that are nonzero do not change under the action of T, and also that a_0 and $a_{2\ell}$ are never zero. Considering these indices allows us to determine which small set of modified invariants we need to use.

Definition 2.8. Let f be a binary form of type $(0, n, m)$ as in (2.2). Given an integer $r \leq m+1$ and a tuple $S = (s_1, \ldots, s_r)$ of distinct integers in $\{0, \ldots, m\}$, we say that f is *S-admissible* if

(S1) $a_s \neq 0$ for all $s \in S$ and
(S2) if one of a_i, $a_{2\ell-i}$ is nonzero, then exactly one element of $\{i, 2\ell - i\}$ is in S.

Clearly, every binary form f of type $(0, n, m)$ is S-admissible for some S. We now construct the homogeneous invariants of T that are monomials in the $\{a_s : s \in S\}$.

Proposition 2.9. *Under the hypotheses (S1)-(S2), associate with S the single-row matrix $M_S = (s_1 - \ell, \ldots, s_r - \ell)$ over $\mathbb{Q}$. Then the elements of $\ker(M_S) \cap \mathbb{N}^r$ are in one-to-one correspondence with the homogeneous invariants of T for the family of S-admissible binary forms that are monomials in $\{a_s : s \in S\}$, by the association $v \leftrightarrow \prod_{i=1}^r a_{s_i}^{v_i}$.*

Proof. This follows from the transformation behavior of the exponents of the coefficients a_i, which is given in (2.6). □

Generalizing Proposition 2.7, it turns out that together with the invariants $J_1, J_{2,0}, \ldots J_{2,\ell-1}$ these new homogeneous diagonal invariants allow one to reconstruct an S-admissible binary form f, as the following proposition shows.

Proposition 2.10. *Let f and f' be two S-admissible binary forms of type $(0, n, m)$. There exists a finite subset R of the invariants constructed in Proposition 2.9 with the property that there exists an $A \in T$ such that $f' \sim A.f$ if and only if the values of the invariants of f and f' at $R \cup \{J_{2,0}, \ldots J_{2,\ell-1}\}$ determine the same point in the corresponding weighted projective space.*

Proof. We will assume that $\#S > 1$, since the case $S = 1$ is easy. Before starting our construction, we modify S; if M_S consists completely of either only strictly positive or only strictly negative elements, then we change the entry 2ℓ of S to 0 or inversely. Note that f and f' will still be S-admissible after this change since $a_0 a_{2\ell} \neq 0$.

We first construct a $\mathbb{Z}$-basis of the $\mathbb{Z}$-module $K_S = \ker(M_S) \cap \mathbb{Z}^S$ used in Proposition 2.9. The module K_S is torsion-free, since it is a submodule of a torsion-free

$\mathbb{Z}$-module. Furthermore, the quotient $\mathbb{Z}^S/K_S$ is torsion-free as well. Indeed, suppose that $nx \in K_S$ for some $n \in \mathbb{Z}$ and $x \in \mathbb{Z}^S$. Then $M_S(nx) = 0$, so $M_S(x) = 0$ and $x \in \ker(M_S) \cap \mathbb{Z}^S = K_S$. We thus have an exact sequence of finitely generated free $\mathbb{Z}$-modules

$$0 \longrightarrow K_S \longrightarrow \mathbb{Z}^S \longrightarrow \mathbb{Z}^S/K_S \longrightarrow 0. \tag{2.7}$$

Choose a basis $\{v_i\}_{i=1}^{\#S-1}$ of K_S. Then since sequence (2.7) is split, there exists a vector $w \in \mathbb{Z}^S$ such that $\mathbb{Z}^S$ has basis $\{v_i\}_{i=1}^{\#S-1} \cup \{w\}$.

We will now construct an element $v \in K_S$ such that all the entries of v are strictly positive. To accomplish this, we note that not all the entries of M_S have the same sign, since in this case f would have repeated roots. Therefore, given an index i of M_S, we can find another index j such that $(M_S)_i$ and $(M_S)_j$ have the opposite sign. We can now construct an element of K_S whose only nontrivial entries are at i and j, with values $(M_S)_j$ and $-(M_S)_i$. Multiplying by -1 if necessary, we get an element of $\mathbb{N}^S \cap K_S$ that is nontrivial at the index i. Summing over the indices i now gives the requested element v of K_S.

We now claim that there exists a basis $\{v_i\}_{i=1}^{\#S-1} \cup \{w\}$ of $\mathbb{Z}^S$ all of whose elements are in $\mathbb{N}^S$. To see this, consider the element v constructed in the previous paragraph and choose v_1 such that $\mathbb{N}v_1 = \mathbb{Q}v \cap \mathbb{N}^S$. Then v_1 also has all of its entries strictly positive. Moreover, v_1 can again be completed to a basis $\{v_i\}_{i=1}^{\#S-1}$ of K_S because the same argument used to produce the sequence (2.7) shows the existence of a split exact sequence of free $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z}v_1 \longrightarrow K_S \longrightarrow K_S/\mathbb{Z}v_1 \longrightarrow 0.$$

It then only remain to add sufficiently large multiples of v_1 to the other elements of the resulting basis. This yields the requested basis $\{v_i\}_{i=1}^{\#S-1}$ of K_S, which we can augment to a basis $\{v_i\}_{i=1}^{\#S-1} \cup \{w\}$ of $\mathbb{Z}^S$ as before. Moreover, by adding multiples of the v_i to w, we can insure that w is in $\mathbb{N}^S$ as well, which implies our claim.

After these preparations, the proof of the proposition is straightforward. The monomials corresponding to the basis elements v_i under the correspondence in Proposition 2.9 will now play the role of the generic homogeneous diagonal invariants; they will turn out to distinguish the orbits under T of S-admissible binary forms. We let $t = \prod_{i=1}^{\#S} a_{S_i}^{w_i}$ be the monomial corresponding to w. Since w is not in K_S, we can use matrices of the form $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ as in the proof of Proposition 2.7 to suppose that the value of t is the same for f and f' without affecting the value of the invariants corresponding to the v_i; as in that same proof, knowing t and the value of these invariants along with the invariants $J_1, J_{2,0}, \ldots J_{2,\ell-1}$ determines the coefficients of the binary forms involved. Indeed, because $\mathbb{Z}^S$ has basis $\{v_i\}_{i=1}^{\#S-1} \cup \{w\}$, we can reconstruct the nonzero coefficients $\{a_s : s \in S\}$. The invariants $J_{2,0}, \ldots J_{2,\ell-1}$ then determine the other coefficients by property (S2) in Definition 2.8. ☐

Definition 2.11. Given a binary form f of type $(0, n, m)$ and any tuple S for which f is S-admissible, we call any of the finite sets $R \cup \{J_{2,0}, \ldots J_{2,\ell-1}\}$ constructed in Proposition 2.9 the *homogeneous diagonal invariants* of f.

Remark 2.12. It may seem unnatural to modify invariants depending on the vanishing behavior of the coefficients of f, but in practice this is very useful, since the parametrization from Corollary 2.13 is crucial for our reconstruction purposes.

We again emphasize that once an initial binary form f of type $(0, n, m)$ is given, one sees immediately which invariants should be used; indeed, the set S that one can take in Definition 2.8 is purely determined by the vanishing behavior of the coefficients of f.

Corollary 2.13. *The set of S-admissible binary forms with given S-homogeneous diagonal invariants is a rational space of dimension* 1*.*

Proof. This is clear from the proof of Proposition 2.10. Indeed, the given set is parametrized by the monomial corresponding to the complementary vector w. □

Example 2.14. The generic homogeneous diagonal invariants from Definition 2.5 correspond to the case where $S = (2\ell, 2\ell - 1, \ldots, \ell + 2, \ell - 1)$, so $M_S = (\ell, \ell - 1, \ldots, 2, -1)$. The resulting kernel K_S has an ordered basis consisting of the positive elements

$$\begin{gathered} (1, 0, 0, \ldots, 0, 0, \ell), \\ (0, 1, 0, \ldots, 0, 0, \ell - 1), \\ \ldots \\ (0, 0, 0, \ldots, 0, 1, 2) \end{gathered}$$

corresponding to the generic invariants $J_{\ell+1}, J_\ell, \ldots, J_3$, respectively. The complementary element $(0, 0, \ldots, 0, 1)$ corresponds to $a_{\ell-1}$, which can indeed be used to parametrize the corresponding rational spaces, as we have seen in the proof of Proposition 2.7.

Example 2.15. Let $\ell = 6$ and take $S = (12, 8, 3, 1)$. A basis for K_S in $\mathbb{N}^4$ is given by $\{(3, 0, 1, 3), (3, 1, 0, 4), (5, 0, 0, 6)\}$, and a complementary element w is furnished by $(1, 0, 0, 1)$. This shows that for binary forms f of type $(0, n, m)$ such that

$$a_{10} = a_7 = a_5 = a_2 = 0$$

and $a_8, a_3, a_1 \neq 0$, a set of S-homogeneous diagonal invariants is furnished by

$$\begin{aligned} J_1 &= a_6, \\ J_{2,0} &= a_{12} a_0, \\ J_{2,1} &= a_{11} a_1, \\ J_{2,3} &= a_9 a_3, \\ J_{2,4} &= a_8 a_4, \\ J_7 &= a_{12}^3 a_3 a_1^3, \\ J_8 &= a_{12}^3 a_8 a_1^4, \\ J_{11} &= a_{12}^5 a_1^6. \end{aligned}$$

Moreover, we can use $w = a_{12} a_1$ to parametrize the corresponding rational spaces of binary forms with given S-homogeneous invariants.

Remark 2.16. A uniform approach to the problem is also available, namely by constructing the full invariant algebra of the action of T on the general binary form (2.2) in Definition 2.1. This can be done by writing down the invariant monomials of given weight, adding the result to the set of generator if it is not an expression in the monomials already found. By a result of Wehlau [18], this process always terminates at degree $m-1$. A script to generate this invariant algebra is available online[1]. For the case $m=8$, it is generated by the expressions

$$
\begin{array}{lll}
\text{Degree } 1: & a_4, & \\
\text{Degree } 2: & a_7a_1,\ a_6a_2, & a_5a_3,\ a_8a_0, \\
\text{Degree } 3: & a_8a_3a_1,\ a_7a_5a_0, & a_7a_3a_2,\ a_6a_5a_1, \\
 & a_8a_2^2,\ a_6^2a_0, & a_6a_3^2,\ a_5^2a_2, \\
\text{Degree } 4: & a_8a_6a_1^2,\ a_7^2a_2a_0, & a_8a_5a_2a_1,\ a_7a_6a_3a_0, \\
 & a_7a_5a_2^2,\ a_6^2a_3a_1, & a_7a_3^3,\ a_5^3a_1, \\
 & a_8a_3^2a_2,\ a_6a_5^2a_0, & \\
\text{Degree } 5: & a_8^2a_2a_1^2,\ a_7^2a_6a_0^2, & a_8a_5^2a_1^2,\ a_7^2a_3^2a_0, \\
 & a_7^2a_2^3,\ a_6^3a_1^2, & a_8a_3^4,\ a_5^4a_0, \\
\text{Degree } 6: & a_8^2a_5a_1^3,\ a_7^3a_3a_0^2, & \\
\text{Degree } 7: & a_8^3a_1^4,\ a_7^4a_0^3\,. &
\end{array}
$$

The nongeneric invariants constructed in Proposition 2.9 are of course expressions in these monomials. Theoretically, this uniform approach is much more satisfying, but the results get unwieldy for bigger m; the number of invariants runs into the hundreds for $m \geq 12$, whereas by contrast, the number of homogeneous invariants constructed above is always at most $\ell+1$, no matter which subset S of coefficients is considered.

2.3. **Homogeneous dihedral invariants.** We resume the main thread of our argument. Now that we have determined useful small sets of invariants for the action of the normal subgroup $T \subset D$ of index 2, we can construct the invariants for D itself by a symmetrization. Before starting, we need an elementary result.

Lemma 2.17. *Let $n \geq 1$, and let X be the affine space with coordinates $(s_1,\dots,s_n, t_1,\dots t_n)$. Define an action of the cyclic group $\mathbf{C}_2$ on X by $s_i \leftrightarrow t_i$. Consider the invariants $\{s_i+t_i\}_{i=1}^n \cup \{s_it_j+s_jt_i\}_{i,j=1}^n$ of this action. Then the orbit under the action of $\mathbf{C}_2$ of a point $x \in X$ is determined by these invariants.*

Proof. Certainly the subset of invariants $\{s_i+t_i\}_{i=1}^n \cup \{2s_it_i\}_{i=1}^n$ determines $x = (s_1,\dots,s_n,t_1,\dots t_n)$ up to some sequence of exchanges $s_i \leftrightarrow t_i$. We have to show that the additional invariants suffice to distinguish a sequence of such exchanges, except when either none or all of the s_i and t_i are exchanged. So suppose that we have two indices i and j where $s_i \neq t_i$ and $s_j \neq t_j$, and we exchange s_i and t_i while leaving the coordinates with index j fixed. Then equality of the invariants yields $s_it_j+s_jt_i = t_it_j+s_js_i$, hence $(s_i-t_i)(s_j-t_j)=0$, a contradiction to our hypothesis. □

By using Lemma 2.17, we can now find small sets of homogeneous invariants that can be used to distinguish orbits of binary forms f of type $(0,n,m)$. First we consider the generic case. Let J_i' denote the transformation of the invariant J_i under the involution $a_i \mapsto a_{m-i}$ on the coefficients, and let

$$
\begin{array}{ll}
I_1 = J_1, & \\
I_{2,0} = J_{2,0},\ I_{2,1} = J_{2,1},\ \dots, & I_{2,\ell-1} = J_{2,\ell-1}, \\
I_{3,3,1} = J_3 + J_3', & I_{3,3,2} = J_3J_3', \\
\vdots & \vdots
\end{array}
$$

$$I_{\ell+1,\ell+1,1} = J_{\ell+1} + J'_{\ell+1}, \qquad I_{\ell+1,\ell+1,2} = J_{\ell+1}J'_{\ell+1},$$
$$I_{3,4} = J_3J'_4 + J'_3J_4, \qquad I_{3,5} = J_3J'_5 + J'_3J_5,\ \dots,$$
$$I_{3,\ell+1} = J_3J'_{\ell+1} + J'_3J_{\ell+1},$$
$$I_{4,5} = J_4J'_5 + J'_4J_5, \qquad I_{4,6} = J_4J'_6 + J'_4J_6, \dots,$$
$$I_{4,\ell+1} = J_4J'_{\ell+1} + J'_4J_{\ell+1},$$
$$\vdots$$
$$I_{\ell,\ell+1} = J_\ell J'_{\ell+1} + J'_\ell J_{\ell+1}.$$

These expressions are homogeneous invariants under the action of D. Though D is not a dihedral group, we still employ the following terminology, which was introduced in [7].

Definition 2.18. We call the symmetrized invariants I, defined above by the *generic homogeneous dihedral invariants* (for binary forms of type $(0, n, m)$).

Example 2.19. For the forms f of type $(0, n, 4)$ considered in Example 2.19, the generic homogeneous diagonal invariants are given by $I_1 = J_1 = a_2, I_{2,0} = J_{2,0} = a_4a_0, I_{2,1} = J_{2,1} = a_3a_1, I_{3,3,1} = J_3 + J'_3 = a_4a_1^2 + a_3^2a_0$ and $I_3 = J_3J'_3 = a_4a_3^2a_1^2a_0$.

Remark 2.20. As long as $J_3 \neq J'_3$ the invertible linear systems in J_i and J'_i given by considering two of the invariants $I_{i,i,1} = J_i + J'_i$ and $I_{3,i} = J_3J'_i + J'_3J'_i$ are invertible. Therefore, we can usually even get by with a further subset of these generic homogeneous dihedral invariants in our calculations, namely $I_1, I_{2,0} \dots, I_{2,\ell+1}, I_{3,3,1}, \dots, I_{\ell+1,\ell+1,1}, I_{3,3,2}, I_{3,4}, \dots, I_{3,\ell+1}$. In Example 4.1, we take this approach.

The symmetrization process is similarly straightforward for the S-homogeneous diagonal invariants, so we can also construct homogeneous dihedral invariants in the nongeneric cases.

Definition 2.21. Given a binary form f of type $(0, n, m)$ with $m = 2\ell$ even and any tuple S for which f is S-admissible, we call the symmetrization of any of the finite sets $R \cup \{J_{2,0}, \dots J_{2,\ell-1}\}$ constructed in Proposition 2.9 the *homogeneous dihedral invariants* of f.

Proposition 2.22. *Let $T = (0, n, m)$ be a type with $m = 2\ell$ even.*

(1) Suppose that f and f' in (2.2) *of type T are such that*
  - *(i) either $a_{2\ell}, a_{2\ell-1}, \dots, a_{\ell+1}, a_{\ell-1} \neq 0$ or $a_{\ell+1}, a_{\ell-1}, \dots, a_1, a_0 \neq 0$ and*
  - *(ii) either $a'_{2\ell}, a'_{2\ell-1}, \dots, a'_{\ell+1}, a'_{\ell-1} \neq 0$ or $a'_{\ell+1}, a'_{\ell-1}, \dots, a'_1, a'_0 \neq 0$.*

  If the generic homogeneous dihedral invariants I and I' of f and f' define the same point in the corresponding weighted projective space, then there exists an $A \in D$ such that $f' \sim A.f$.

(2) For general S-admissible f and f' whose invariants define the same point in the corresponding weighted projective space, the same conclusion holds.

Proof. Note that the conditions of part (i) of the proposition are indeed invariant under the action of D. Using Lemma 2.17, we see that replacing f' by its transformation by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ if necessary, we may assume that f and f' have the same homogeneous diagonal invariants. Then the parametrization by $a_{\ell-1}$ in Proposition 2.7 allows us to conclude.

For general forms, the argument is essentially the same, replacing the parametrizing element $a_{\ell-1}$ by the monomial corresponding to w in Proposition 2.10. Note that forms in the same D-orbit are indeed S-admissible for the same S, so that the same set of homogeneous dihedral invariants can be used. □

The construction of general homogeneous dihedral invariants is perhaps best illustrated by an example.

Example 2.23. Consider the binary forms f of type $(0, n, 12)$ such that both $a_2 = a_5 = a_7 = a_{10} = 0$ and either $a_{11}, a_9, a_4 \neq 0$ or $a_8, a_3, a_1 \neq 0$. The symmetrization of the invariants in Example 2.23 yields the following S-homogeneous dihedral invariants for this family:

$$I_1 = a_6,$$

$$I_{2,0} = a_{12}a_0,\ I_{2,1} = a_{11}a_1, \qquad I_{2,3} = a_9a_3,\ I_{2,4} = a_8a_4,$$

$$I_{7,7,1} = a_{11}^6a_0^5 + a_{12}^5a_1^6, \qquad I_{7,7,2} = a_{12}^5a_{11}^6a_1^6a_{12}^5,$$

$$I_{8,8,1} = a_{11}^3a_9a_0^3 + a_{12}^3a_3a_1^3, \qquad I_{8,8,2} = a_{12}^3a_{11}^3a_9a_3a_1^3a_0^3,$$

$$I_{11,11,1} = a_{11}^4a_4a_0^3 + a_{12}^3a_8a_1^4, \qquad I_{11,11,2} = a_{12}^3a_{11}^4a_8a_4a_1^4a_0^3,$$

$$I_{7,8} = a_{12}^3a_{11}^6a_3a_1^3a_0^5 + a_{12}^5a_{11}^3a_9a_1^6a_0^3, \qquad I_{7,11} = a_{12}^3a_{11}^6a_8a_1^4a_0^5 + a_{12}^5a_{11}^4a_4a_1^6a_0^3,$$

$$I_{8,11} = a_{12}^3a_{11}^3a_9a_8a_1^4a_0^3 + a_{12}^3a_{11}^4a_4a_3a_1^3a_0^3.$$

Remark 2.24. The homogeneous dihedral invariants of a general binary octavic form

$$f = a_8x^8 + a_7x^7z + \ldots + a_1xz^7 + a_0z^8$$

are the following:

Degree 1 : $i_1 = a_4,$

Degree 2 : $i_2 = a_0\, a_8,\ j_2 = a_1\, a_7,\ k_2 = a_2\, a_6,\ l_{2,} = a_3\, a_5,$

Degree 3 : $i_3 = a_0\, a_5\, a_7 + a_1\, a_3\, a_8,\ j_3 = a_0\, {a_6}^2 + {a_2}^2 a_8,$
$k_3 = a_1\, a_5\, a_6 + a_2\, a_3\, a_7,\ l_3 = a_2\, {a_5}^2 + {a_3}^2 a_6,$

Degree 4 : $i_4 = a_0\, {a_5}^2 a_6 + a_2\, {a_3}^2 a_8,\ j_4 = a_0\, a_3\, a_6\, a_7 + a_1\, a_2\, a_5\, a_8,$
$k_4 = a_0\, a_2\, {a_7}^2 + {a_1}^2 a_6\, a_8,\ l_4 = a_1\, {a_5}^3 + {a_3}^3 a_7,$
$m_4 = a_1\, a_3\, {a_6}^2 + {a_2}^2 a_5\, a_7,$

Degree 5 : $i_5 = {a_0}^2 a_6\, {a_7}^2 + {a_1}^2 a_2\, {a_8}^2,\ j_5 = a_0\, {a_5}^4 + {a_3}^4 a_8,$
$k_5 = a_0\, {a_3}^2 {a_7}^2 + {a_1}^2 {a_5}^2 a_8,\ l_5 = {a_1}^2 {a_6}^3 + {a_2}^3 {a_7}^2,$

Degree 6 : $i_6 = {a_0}^2 a_3\, {a_7}^3 + {a_1}^3 a_5\, {a_8}^2,$

Degree 7 : $i_7 = {a_0}^3 {a_7}^4 + {a_1}^4 {a_8}^3.$

Since there is an inclusion of invariant rings

$$k[a_0, a_1, \ldots, a_8]^{\mathrm{SL}_2(K)} \subset k[a_0, a_1, \ldots, a_8]^{D\cap \mathrm{SL}_2(K)},$$

the Shioda invariants [17] can be expressed as polynomials in the generic homogeneous dihedral invariants. For example, the degree 2 Shioda invariant can be written as

$$\frac{1}{70}\, {i_1}^2 + 2\, i_2 - \frac{1}{4}\, j_2 + \frac{1}{14}\, k_2 - \frac{1}{28}\, l_2,$$

whereas the degree 3 invariant equals

$$\frac{9}{34300}\, {i_1}^3 + \frac{3}{35}\, i_1\, i_2 + \frac{9}{560}\, i_1\, j_2 - \frac{33}{13720}\, i_1\, k_2 - \frac{27}{27440}\, i_1\, l_2 - \frac{3}{56}\, i_3 + \frac{9}{392}\, j_3 - \frac{3}{784}\, k_3 + \frac{9}{5488}\, l_3.$$

These formulas, as well as formulas expressing the dihedral invariants in terms of the Shioda invariants, are available online [1].

2.4. **Homogeneous dihedral invariants in the remaining cases.** We now discuss the invariants that have to be used in the remaining cases. First we treat binary forms of type $(0,n,m)$ for odd m (recall that in the previous subsections we assumed m to be even). Only small modifications are needed; the generic homogeneous diagonal invariants are given by

$$\begin{array}{rcl} J_{2,0} & = & a_{2\ell-1}a_0, \\ J_{2,1} & = & a_{2\ell-2}a_1, \ \ldots, \ J_{2,\ell-1} = a_\ell a_{\ell-1}, \\ J_4 & = & a_{\ell+1}a_{\ell-1}^3, \\ & \vdots & \\ J_{2\ell} & = & a_{2\ell-1}a_{\ell-1}^{2\ell-1}. \end{array}$$

These invariants suffice as long as $a_{2\ell-1}, a_{2\ell-2}, \ldots, a_{\ell+1}, a_{\ell-1} \neq 0$. Symmetrizing with respect to the involution $a_i \leftrightarrow a_{m-i}$, one again obtains the generic homogeneous dihedral invariants for odd m. Homogeneous invariants for the nongeneric cases can be also constructed as for even m as well; the only difference is that the matrix M_S is now given by $(2(s_1-\ell)+1,\ldots,2(s_r-\ell)+1)$.

The homogeneous dihedral (and diagonal) invariants for binary forms of type $(2,n,m)$ are exactly the same as expressions in the a_i as for those of type $(0,n,m)$. Finally, for the binary forms of type $(1,n,m)$, such, we only need to consider the action of T when constructing our invariants in light of the second part of Proposition 2.4. But we know that the (identical) homogeneous diagonal invariants considered for the types $(0,n,m)$ and $(2,n,m)$ already suffice to distinguish the orbits under this group. So we also know how to construct a finite (and small) set of invariants for these curves.

3. Explicit obstruction and descent

In this section, we will use the homogeneous dihedral invariants from Section 2 to obtain an explicit arithmetic description of the descent obstruction for hyperelliptic curves with tamely cyclic reduced automorphism group. If this obstruction vanishes, then we also indicate how an explicit descent can be obtained. To phrase our results in a concise way, we first define the *type* of a hyperelliptic curve with tamely cyclic reduced automorphism group.

Definition 3.1. Let X be a hyperelliptic curve over K. If X is isomorphic to a hyperelliptic curve associated with a binary form of type (i,n,m) over K (as in Definition 2.1), then X will be said to be of *type* (i,n,m).

Remark 3.2. Let X be a hyperelliptic curve of type (i,n,m), Then i equals the number of Weierstrass points fixed by $G = \mathrm{Aut}(\mathsf{X})$. The quantity n equals the cardinality of the reduced automorphism group of X, since as in [11, Sec. 1.2], one can use the fact that the hyperelliptic involution is central to prove that the group $\overline{G}$ is canonically isomorphic to $\mathrm{Aut}(f)$. Finally, if $n>1$, then m equals the cardinality of the divisor of branch points of $\mathsf{X} \to \mathsf{X}/G$ of order 2. Conversely, any binary form of type (i,n,m) determines a hyperelliptic curve with these geometric properties.

Note that the genus g of a hyperelliptic curve X of type (i,n,m) is determined by the equality $2g+2 = mn+i$.

In what follows, we let X denote a hyperelliptic curve over K of type (i, n, m) whose field of moduli for the extension $K|k$ equals k. In Theorem 1.6, we have proved that the existence of a descent implies the existence of a hyperelliptic descent except possibly if both n and g are odd. We now divide the issue of explicit descent into three cases.

(i) In the case where $n > 1$, Section 3.1 shows how to express the hyperelliptic descent obstruction in terms of the homogeneous dihedral invariants. Moreover, we discuss in Section 3.2 how to calculate a hyperelliptic descent explicitly if this obstruction vanishes.
(ii) In the case where n and g are both odd, Section 3.3 shows that the curve always descends, though perhaps not hyperelliptically. Moreover, we discuss how to calculate such a descent explicitly.
(iii) In the case where $n = 1$, Section 3.4 gives a generic method to calculate the (hyperelliptic) descent obstruction, and a corresponding descent if this obstruction vanishes. Its main approach is based on the covariant method developed in [12].

To conclude these considerations, we show in Section 3.5 how essentially all counterexamples to (hyperelliptic) descent can be constructed.

3.1. **Explicit hyperelliptic descent obstruction.** In what follows, we will let f be a binary form of type (i, n, m) with $n > 1$. We denote homogeneous diagonal (resp. dihedral) invariants of f by $J(f)$ (resp. $I(f)$). We will often consider these tuples $J(f)$, $I(f)$ invariants as points in the corresponding weighted projective spaces. As in [11, Sec. 1.3], one can associate a unique representative with such a point p, which we shall here call a *normalized representative.* This normalized representative is a tuple of coordinates that represents p whose entries are defined over the same field as the point p when the latter is considered as an element of a weighted projective space.

Example 3.3. Let $p = (3 : 6\sqrt{3})$, considered as a point in the weighted projective $(2, 3)$-space. Then p is defined over $\mathbb{Q}$, since its conjugate $(3 : -6\sqrt{3})$ can be obtained from p by multiplying with the scalar -1. While the tuple $(3, 6\sqrt{3})$ representing p is not defined over $\mathbb{Q}$, its normalized representative from [11, Sec. 1.3] is; this representative is given by $(\frac{1}{4}, \frac{1}{4})$.

Conversely, note that once a curve X over K with tamely cyclic reduced automorphism group is given explicitly, it is possible to quickly determine a binary form of the corresponding type (as in (2.2)), (2.3) or (2.4)) that defines X over K by using the methods from [12, Sec. 2]. Indeed, using the methods in *loc. cit.* one diagonalizes the cyclic reduced automorphism group $\mathbf{C}_n$ of X into our standard embedding of the group $\mathbf{C}_n$.

Proposition 3.4. *(i) The normalized representative of the homogeneous dihedral invariants $I(f)$ of f is defined over k.*
(ii) The normalized representative of the homogeneous diagonal invariants $J(f)$ of f is defined over a quadratic extension $L = k(\sqrt{d})$ of k.
(iii) The binary form f is isomorphic over K to a binary form f_L of the same type that is defined over L.

Proof. (i) By Proposition 2.4 the homogeneous dihedral invariants of f and its conjugates all define the same point in the corresponding weighted projective space, since by construction these invariants transform by suitable powers of a scalar under the action of D. It therefore suffices to invoke the uniqueness of the canonical representative from [11, Sec. 1.4].

(ii) By Lemma 2.17, given a tuple of homogeneous dihedral invariants, there are at most 2 tuples of homogeneous diagonal invariants of which these can be the symmetrization. As such, the Galois group fixing these tuples defines an, at worst, quadratic extension of k.

(iii) One uses the rational parametrization in Corollary 2.13. □

Definition 3.5. We call the field extension L of k in Proposition 3.4 the *invariant extension* defined by f.

Corollary 3.6. *The curve* X *defined by* f *descends to the at most quadratic invariant extension* L *of* k.

Proposition 3.7. *Generically, the invariant extension* L *is given by* $k(\sqrt{d})$, *where* $d = I_{3,3,1}^2 - 4I_{3,3,2}$ *if* m *is even and* $d = I_{4,4,1}^2 - 4I_{4,4,2}$ *if* m *is odd.*

Proof. This follows because when m is even (resp. odd) the field extension $L|k$ is already incurred when reconstructing the first pair of nondihedral diagonal invariants J_3, J_3' from $I_{3,3,1}, I_{3,3,2}$ (resp. J_4, J_4' from $I_{4,4,1}, I_{4,4,2}$). □

We now consider some examples in order to get an idea of what the extension $L|k$ looks like.

Example 3.8. Consider the binary forms

$$f = a_4x^8 + a_3x^6z^2 + a_2x^4z^4 + a_1x^2z^6 + a_0$$

of type $(0, 2, 4)$. Then the generic homogeneous dihedral invariants are symmetrizations of the generic diagonal invariants $J_1 = a_2$, $J_{2,0} = a_4a_0$, $J_{2,1} = a_3a_1$ and $J_3 = a_4a_1^2$.

In this case the only new dihedral invariants obtained by symmetrizing the diagonal invariants are $I_{3,3,1} = J_3 + J_3'$ and $I_{3,3,2} = J_3J_3'$. For the generic forms f in Proposition 2.7 of type $(0, 2, 4)$, the quadratic extension L is therefore *always* the one incurred by passing from $J_3 + J_3'$ and J_3J_3' to J_3, J_3'. As we have seen, this means that $L = k(\sqrt{d})$, where $d = I_{3,3,1}^2 - 4I_{3,3,2}$.

Example 3.9. Consider the binary forms

$$f = a_5x^{10} + a_4x^8z^2 + a_3x^6z^4 + a_2x^4z^6 + a_1x^2z^8 + a_0z^{10}$$

of type $(0, 2, 5)$. Then the generic homogeneous dihedral invariants are symmetrizations of $J_{2,0} = a_6a_0$, $J_{2,1} = a_5a_1$, $J_{2,2} = a_4a_2$, $J_4 = a_5a_2^3$ and $J_6 = a_6a_2^5$.

This time the quadratic extension L is a bit more complicated to determine. Indeed, we get two pairs of new dihedral invariants, namely $I_{4,4,1}, I_{4,4,2}$ and $I_{6,6,1}$, $I_{6,6,2}$. Generically, the extension L is already incurred by passing from $I_{4,4,1}, I_{4,4,2}$ to J_4, J_4', which gives $L = k(\sqrt{d})$ where $d = I_{4,4,1}^2 - 4I_{4,4,2}$. But it is possible that this does not give an extension of the ground field, while passing from $I_{6,6,1}, I_{6,6,2}$ to J_6, J_6' does. In the latter case we have $L = k(\sqrt{d})$ with $d = I_{6,6,1}^2 - 4I_{6,6,2}$ instead.

Now let L be the invariant extension defined by f, and let f_L be the partial descent from Proposition 3.4. We may suppose that X is defined by f_L. As at the beginning of Section 1.2, the isomorphisms between X and its conjugates induce a canonical descent datum on the quotient $\mathsf{B} = \mathsf{X}/\operatorname{Aut}(\mathsf{X})$, which yields a model B_0

of B over k. Now Theorem 1.13 shows that X descends hyperelliptically if and only if B_0 has a k-rational point.

To study the twist B_0, we construct the corresponding Weil cocycle c. Let σ be the generator $\mathrm{Gal}(L|k)$. By our running hypotheses, f_L^σ has the same homogeneous dihedral invariants as f_L. Let S be the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Then either

$$f_L^\sigma \sim D.f_L \tag{3.1}$$

or

$$f_L^\sigma \sim DS.f_L \tag{3.2}$$

for some $D = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right) \in T$. Note that by Proposition 2.4, the latter case does not occur if f_L has type $(1, n, m)$. Regardless, we now either have

$$(a_m^\sigma, a_{m-1}^\sigma, \dots, a_1^\sigma, a_0^\sigma) \longmapsto (\lambda^{mn} a_m, \lambda^{(m-1)n} \mu^n a_{m-1}, \dots, \lambda^n \mu^{(m-1)n} a_1, \mu^{mn} a_0) \tag{3.3}$$

or

$$(a_m^\sigma, a_{m-1}^\sigma, \dots, a_1^\sigma, a_0^\sigma) \longmapsto (\lambda^{mn} a_0, \lambda^{(m-1)n} \mu^n a_1, \dots, \lambda^n \mu^{(m-1)n} a_{m-1}, \mu^{mn} a_m). \tag{3.4}$$

depending on whether (3.1) or (3.2) holds.

Lemma 3.10. *Choose isomorphisms $g_\sigma : \mathsf{X} \to \mathsf{X}^\sigma$ for all $\sigma \in \Gamma$. Then the induced Weil cocycle c on B given by $\sigma \mapsto h_\sigma : \mathsf{B} \to \mathsf{B}^\sigma$ is trivial on the index 2 subgroup of Γ that fixes the invariant extension L of k.*

Proof. Indeed, since we divide out by the automorphisms of X, the induced maps h_σ are independent of the choice of the g_σ. Since X is defined over L, we may just take g_σ to be the identity if σ fixed L. The result follows. □

Using the inflation-restriction exact sequence, Lemma 3.10 implies that $c \in H^1(\mathrm{Gal}(K|k), \mathrm{PGL}_2(K))$ is the inflation of a Weil cocycle

$$c_L \in H^1(\mathrm{Gal}(L|k), \mathrm{PGL}_2(L)).$$

In the case (3.1), the cocycle c_L is given by

$$\sigma \longmapsto \left(\begin{smallmatrix} \lambda^n & 0 \\ 0 & \mu^n \end{smallmatrix}\right) \tag{3.5}$$

and in the case (3.2) by

$$\sigma \longmapsto \left(\begin{smallmatrix} 0 & \mu^n \\ \lambda^n & 0 \end{smallmatrix}\right) . \tag{3.6}$$

Suppose that c_L is given by (3.5). Then by dividing by the scalar λ^n, we can normalize c_L to

$$\sigma \longmapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & r \end{smallmatrix}\right) . \tag{3.7}$$

The Weil cocycle condition translates into the equality $r^\sigma r = 1$, so by Hilbert's 90 the cocycle (3.7) is a coboundary. More precisely, the descent morphism is then given by a diagonal matrix, so there exists a hyperelliptic descent defined by a binary form f_k of the same type as f_L. But in that case the normalized representative of $I(f_L)$ would be defined over k already; so L was already the trivial extension of k. Since we are always in the case (3.5) if f_L is of type $(1, n, m)$, we get the following result.

Lemma 3.11. *If X is of type $(1, n, m)$, then X can be defined over k by a binary form f of the given type.*

In the second case where c_L is given by (3.6), let $r = \mu^n/\lambda^n$. Now c_L normalizes to

$$\sigma \longmapsto \left(\begin{smallmatrix} 0 & r \\ 1 & 0 \end{smallmatrix}\right) . \tag{3.8}$$

The fact that (3.6) indeed defines a cocycle shows that $r^\sigma = r$, so $r \in k$.

Definition 3.12. We call the image of r in the quotient group $k^*/\operatorname{Nm}_{L|k}(L^*)$ the *norm obstruction* for X.

Lemma 3.13. *Let f_L be a form of type $(0, n, m)$ or $(2, n, m)$.*

(i) If $m = 2\ell$ is even, then if we suppose additionally that f_L is generic, then the norm obstruction for X is trivial if and only if the generic homogeneous dihedral invariant $I_{2,\ell-1}(f)$ is a norm from L.

(ii) If m is odd, then the norm obstruction is always trivial.

Proof. (i) If $a_{\ell-1}$, a_ℓ and $a_{\ell+1}$ are all nonzero, the transformation formula (3.4) shows that we have

$$r = (a_\ell^\sigma a_{\ell-1})/(a_{\ell+1}^\sigma a_\ell) = a_{\ell-1}/a_{\ell+1}^\sigma$$

(note that $a_\ell = a_\ell^\sigma$ by the k-rationality of the homogeneous dihedral invariants). The demand that this be a norm is satisfied if and only if $a_{\ell+1}a_{\ell-1} = I_{2,\ell-1}$ is a norm.

(ii) Let $m = 2\ell - 1$ be odd. We first suppose that a_ℓ and $a_{\ell+1}$ are nonzero. Then $r = (a_{\ell+1}^\sigma a_{\ell+1})/(a_\ell^\sigma a_\ell)$ is a norm. In the general case, the same argument shows that r^{2i-1} is a norm for all i such that $a_{\ell+i}$ (and hence $a_{\ell+1-i}$, since we are in case (3.6)) is nonzero. The set of exponents of r thus obtained has greatest common divisor equal to one, since one observes that otherwise the binary form f that we started with would have more automorphisms than $\mathbf{C}_n$ and would therefore not be of the given type. ☐

We can now prove our main theorem of this section.

Theorem 3.14. *Let X denote a hyperelliptic curve over K of genus g and type (i, n, m) with $n > 1$ whose field of moduli for the extension $K|k$ equals k, represented by a binary form f over K of the given type. Let $L|k$ be the invariant extension defined by f. Then the hyperelliptic descent obstruction is as follows, depending on the type of X.*

- *If X is of type $(0, n, m)$ or $(2, n, m)$, then a hyperelliptic descent always exists if m is odd. If m is even, then X descends hyperelliptically if and only if its norm obstruction is trivial. In either of the two cases, X always admits a hyperelliptic model of the given type over the at most quadratic extension L of k.*
- *If X is of type $(1, n, m)$, then a hyperelliptic descent always exists. Moreover, this descent can be defined by a hyperelliptic model of the given type over k.*

Proof. By Proposition 3.4(ii), we can always construct a hyperelliptic model of X over the quadratic extension L of k. By Lemma 3.11, this extension L in fact coincides with k if f is of type $(1, n, m)$, which proves the theorem for this case.

It remains to see when the descent obstruction to k vanishes in the other cases. By Theorem 1.13, this is the case if and only if the canonical descent B_0 of $\mathsf{B} = \mathsf{X}/\operatorname{Aut}(\mathsf{X})$ admits a point over k. The twist B_0 of the projective line B is determined by the cocycle σ in (3.8). Proposition 1.14 now shows that B_0 is isomorphic to $\mathbb{P}^1$ if and only if the norm obstruction for X vanishes. It now suffices to invoke Lemma 3.13(ii) to show that the extension $L|k$ is always trivial if m is odd. □

Remark 3.15. The existence of a descent can sometimes also be proved by using [2] and a signature argument as in [11, Prop. 4.3] to show that B_0 has a k-rational point. That there exist a hyperelliptic descent then follows from Theorem 1.13. However, our explicit construction of f_0 in the following section uses the homogeneous diagonal invariants and the parametrization from Corollary 2.13 in an essential way.

3.2. **Explicit hyperelliptic descent.** We will now show how to construct a descent of X to k if the obstruction in Theorem 3.14 vanishes. For this, we first prove the following proposition.

Proposition 3.16. *Let $\mathcal{D}_0$ be a k-rational effective divisor of degree 2 on $\mathbb{P}^1$. Then for every $n > 1$ prime to the characteristic of k there exists a tamely cyclic cover $\mathbb{P}^1 \to \mathbb{P}^1$ of degree n that is defined over k and whose branch divisor has support in $\mathcal{D}_0$.*

Proof. The case where $\mathcal{D}_0 = [p_1] + [p_2]$ with $p_1, p_2 \in k$ is trivial. In the case where p_1 and p_2 are Galois conjugate, we can change coordinates in $\mathbb{P}^1$ to suppose that $\mathcal{D}_0 = [\sqrt{d}] + [-\sqrt{d}]$, where d is nonsquare in k. In that case, consider the expansion of the expression $(x + \sqrt{d}z)^n$ as $p + q\sqrt{d}$, with $p, q \in k[x, z]$. Then we claim that we can take $(x : z) \mapsto (p : q)$ as our cover.

To see this, first note that p and q do not contain a common factor. Indeed, this would be a factor of $(x + \sqrt{d}z)^n$ as well, hence it would equal $(x + \sqrt{d}z)$. But because p and q are defined over k, they would then both be divisible by $(x^2 - dz^2)$. Hence the same would be true for $(x + \sqrt{d}z)^n$, which is absurd. So $(p : q)$ does indeed define a degree n cover of $\mathbb{P}^1$ over k.

To see that $(p : q)$ is (tamely) cyclic, note that by construction, the equation $p(t, 1)/q(t, 1) = -\sqrt{d}$ has $t = -\sqrt{d}$ as an n-fold solution. Therefore $(-\sqrt{d} : 1)$ is in the branch locus of $(p : q)$, and hence $\sqrt{d}$ as well since $(p : q)$ is defined over k. The Riemann-Hurwitz formula excludes the possibility of other points occurring in the branch locus of $(p : q)$, which is therefore indeed given by $\mathcal{D}_0$. □

We consider the first case of Theorem 3.14. In order to descend effectively, we first construct some special divisors on the canonical model B_0 of $\mathsf{B} = X/\operatorname{Aut}(X)$.

We let $\mathcal{R}$ be the support of the branch divisor of the quotient map $\pi : \mathsf{X} \to \mathsf{B}$. Given $\sigma \in \operatorname{Gal}(K|k)$, the divisor $\mathcal{R}$ is mapped to its conjugate $\mathcal{R}^\sigma$ under the well-determined isomorphisms $\mathsf{B} \to \mathsf{B}^\sigma$ induced by a choice of isomorphism $\mathsf{X} \to \mathsf{X}^\sigma$. We let $\mathcal{R}_0$ be the image of $\mathcal{R}$ under the canonical descent morphism $\varphi : \mathsf{B} \to \mathsf{B}_0$.

The branch divisor $\mathcal{R}$ naturally admits a decomposition $\mathcal{R} = \mathcal{S} + \mathcal{T}$ into effective subdivisors, $\mathcal{S}$ and $\mathcal{T}$. Here $\mathcal{T}$ is the branch divisor of the tamely cyclic cover $q : \mathsf{Q} = \mathsf{X}/\iota \to \mathsf{B}$, and $\mathcal{S}$ is contained in the image of the branch divisor of the quotient morphism $\pi_\iota : \mathsf{X} \to \mathsf{Q}$ under q. We let $\mathcal{S}_0$ (resp. $\mathcal{T}_0$) be the image of $\mathcal{S}$ (resp. $\mathcal{T}$) under φ.

We summarize the situation, as well as indicate some additional divisors which we will obtain later in our argument, in the diagram below:

$$\begin{array}{ccccc} & & \mathcal{D} & & \mathcal{R} = \mathcal{S} + \mathcal{T} \\ & & \cap & & \cap \\ \mathsf{X} & \xrightarrow{\pi_\iota} & \mathsf{Q} = \mathsf{X}/\iota & \xrightarrow{q} & \mathsf{B} = \mathsf{X}/\operatorname{Aut}(\mathsf{X}) \\ & & \downarrow & & \downarrow \\ & & \mathsf{Q}_0 & \xrightarrow{q_0} & \mathsf{B}_0 \\ & & \cup & & \cup \\ & & \mathcal{D}_0 & & \mathcal{R}_0 = \mathcal{S}_0 + \mathcal{T}_0 \end{array}$$

Proposition 3.17. *(i) The divisors $\mathcal{R}_0$, $\mathcal{S}_0$ and $\mathcal{T}_0$ are defined over k.*
(ii) The support of $\mathcal{T}_0$ is of degree 2.

Proof. (i) This follows because the action of an element $\sigma \in \Gamma$ transforms the branch divisor of $\pi : \mathsf{X} \to \mathsf{B}$ (resp. $q : \mathsf{X}/\iota_{\mathsf{X}} \to \mathsf{B}$) into the branch divisor of $\pi^\sigma : \mathsf{X}^\sigma \to \mathsf{B}^\sigma$ (resp. $q^\sigma : \mathsf{X}^\sigma/\iota_{\mathsf{X}}^\sigma \to \mathsf{B}^\sigma$). Note that for $\mathsf{X}/\iota \to \mathsf{B}$ this uses the fact that the involution ι is canonical to obtain the equality $\iota_{\mathsf{X}}^\sigma = \iota_{\mathsf{X}^\sigma}$.

(ii) Taking a normal form (2.2)–(2.4) over the algebraic closure K transforms the quotient map q into the map $(x : z) \mapsto (x^n, z^n)$, for which $\mathcal{T}$ becomes the divisor $(n-1)[0] + (n-1)[\infty]$. □

We first consider the curves X defined by a form f of type $(0, n, m)$ or $(2, n, m)$. The quotient B has natural coordinates $(s : t) = (x^n : z^n)$, in terms of which $\mathcal{T}$ is given by the zero locus of $a_m s^m + a_{m-1} s^{m-1} t + \ldots + a_1 s t^{m-1} + a_0 t^m$. If the hyperelliptic descent obstruction vanishes, then B_0 is isomorphic with $\mathbb{P}^1$ over k, and we can apply the explicit matrix N from the proof of Proposition 1.14 to $\mathcal{T}$ to get the k-rational divisor $\mathcal{T}_0$ on $\mathsf{B}_0 \cong \mathbb{P}^1$. The divisor $\mathcal{S}$, which corresponds to $(n-1)[(1:0)] + (n-1)[(0:1)]$ in our normalization, is transformed under N to the k-rational divisor $\mathcal{S}_0 = (n-1)[(1:\beta)] + (n-1)[(1:\beta^\sigma)]$. We can now apply Proposition 3.16 with $\mathcal{D}$ equal to the support $\mathcal{U}_0$ of $\mathcal{T}_0$ to get a model $q_0 : \mathsf{Q}_0 := \mathbb{P}^1 \to \mathbb{P}^1 = \mathsf{B}_0$ defined over k of the quotient map q. We now distinguish three cases:

(1) If X has type $(0, n, m)$, then the branch divisor $\mathcal{D}$ of π_ι equals the pullback $q^*(\mathcal{S})$. Pulling back $\mathcal{S}_0$ by q_0, we therefore get a k-rational model $\mathcal{D}_0 = q_0^*(\mathcal{S}_0)$ on $\mathsf{Q}_0 \cong \mathbb{P}^1$ of this branch divisor. We can then construct a model X_0 of X over k by taking the degree 2 cover of $\mathsf{Q}_0 \cong \mathbb{P}^1$ ramified over $\mathcal{D}_0$.
(2) If X has type $(2, n, m)$, the pullback $q^*(\mathcal{S})$ is properly contained in $\mathcal{D}$; we have to add the two points $(1:0)$ and $(0:1)$ in the ramification locus of q that constitute the support $\mathcal{U}$ of $\mathcal{T}$. This support transforms into the ramification divisor $\mathcal{U}_0 = [(1:\beta)] + [(1:\beta^\sigma)]$ of q_0, which is k-rational. So by ramifying over $\mathcal{D}_0 = q_0^*(\mathcal{S}_0) + \mathcal{U}_0$ instead, we again get a hyperelliptic descent.
(3) If X has type $(1, n, m)$, then Lemma 3.11 shows that the construction of the binary form f_L from the normalized diagonal invariants of X in fact automatically gives rise to a form $f_0 = f_L$ defined over k.

Combining these three cases, we get the following algorithm to construct a hyperelliptic descent if the obstruction vanishes.

Algorithm 3.18. *Let* X *denote a hyperelliptic curve over* K *of genus* g *and type* (i, n, m) *with* $n > 1$ *whose field of moduli for the extension* $K|k$ *equals* k*. Suppose that the hyperelliptic descent obstruction vanishes for* X*. Then a binary form* f_0 *defined over* k *that gives a hyperelliptic descent* $\mathsf{X}_0 : y^2 = f_0$ *of* X *can be constructed as follows.*

(i) *Using the methods in* [12, Sec. 2], *construct a binary form* f *of type* (i, n, m) *that represents* X.
(ii) *Compute the normalized homogeneous dihedral invariants* $I(f)$.
(iii) *Construct a descent* f_L *to the invariant extension* L *of* k *defined by* f *by using Corollary* 2.13.
(iv) *If* $i = 1$, *then set* $f_0 = f_L$ *and terminate.*
(v) *Determine the quantity* r *in* (3.8) *for* f_L, *either by using Lemma* 3.13 *in the generic case, or alternatively by using the methods in* [12, Sec. 2].
(vi) *Determine a coboundary matrix* $N = \begin{pmatrix} 1 & \lambda^\sigma \\ \beta & \lambda^\sigma \beta^\sigma \end{pmatrix}$ *as in Proposition* 1.14.
(vii) *Let* $\mathcal{U}_0 = [(1 : \beta)] + [(1 : \beta^\sigma)]$. *Construct the* k*-rational morphism* $q : \mathbb{P}^1 \to \mathbb{P}^1$ *ramifying over* $\mathcal{U}_0$ *as in Proposition* 3.16.
(viii) *Let* $\mathcal{D}_0 = q_0^*(\mathcal{T}_0)$ *(resp.* $\mathcal{D}_0 = q_0^*(\mathcal{S}_0) + \mathcal{U}_0$*) if* $i = 0$ *(resp.* $i = 2$*).*
(ix) *Let* f_0 *be the monic polynomial in* $k[x]$ *whose zero divisor equals* $\mathcal{D}_0$*. Return* f_0 *and terminate.*

We refer to Example 4.5 for a concrete calculation with this algorithm.

3.3. **Explicit nonhyperelliptic descent.** In the case where asking for a hyperelliptic descent and a general descent is not equivalent, it turns out that one can always descend.

Theorem 3.19. *Let* X *denote a hyperelliptic curve over* K *of genus* g *and type* (i, n, m) *with* $n > 1$ *whose field of moduli for the extension* $K|k$ *equals* k*. If* n *and* g *are odd, then* X *descends.*

Proof. Let f be a binary form representing X of the given type. As in Proposition 3.4, we first construct a descent f_L of f to the invariant extension L of k, and once more, as in Section 3.1 the study of the cocycle $c_L \in H^1(\mathrm{Gal}(L|k), \mathrm{PGL}_2(L))$ given by (3.8) will be crucial.

Let us first explicitly construct a conic Q corresponding to the cocycle c_L. We take Q to be given by the equation $x^2 + \lambda y^2 + \mu z^2 = 0$, where $\lambda = -1/r$ and where $\mu \in k$ is such that $L = k(\sqrt{-\mu})$. Consider the L-rational morphism $\varphi : \mathbb{P}^1 \to \mathsf{Q}$ given by the rational parametrization from the point $(\sqrt{-\mu} : 0 : 1) \in \mathsf{Q}(L)$. Then one verifies that $\varphi^\sigma = \varphi\alpha$ for the automorphism $\alpha : x \mapsto r/x$ of $\mathbb{P}^1$ corresponding to (3.8).

So Q is isomorphic to the canonical model B_0 of $\mathsf{B} = \mathsf{X}/\mathrm{Aut}(\mathsf{X})$ over k. Moreover, φ can be used as a descent morphism $\mathsf{B} \to \mathsf{B}_0$. This morphism transforms the branch divisor $\mathcal{T} = [(1 : 0)] + [(0 : 1)]$ of the quotient morphism $q : \mathsf{Q} = \mathsf{X}/\iota \to \mathsf{X}/\mathrm{Aut}(\mathsf{X}) = \mathsf{B}$ into a k-rational divisor $\mathcal{T}_0$. Indeed, we have

$$\mathcal{T}_0^\sigma = (\varphi_*([0] + [\infty]))^\sigma = \varphi_*^\sigma([0] + [\infty]) = \varphi_*(\alpha_*([0] + [\infty])) = \varphi_*([\infty] + [0]) = \mathcal{T}_0.$$

This allows us to once again construct a cyclic cover $q_0 : \mathsf{Q} \to \mathsf{Q}$ ramifying over $\mathcal{T}_0$ that is a k-rational model of the cyclic cover $q : \mathsf{Q} \to \mathsf{B}$ ramifying over $\mathcal{T}$. Indeed, let $f : \mathbb{P}^1 \to \mathbb{P}^1$ be the K-rational morphism given by $x \to x^n/r^{(n-1)/2}$, and let $f_0 = \varphi f \varphi^{-1}$. One verifies that $f = \alpha f \alpha^{-1}$, which implies that $f_0 = \varphi f \varphi^{-1} = \varphi \alpha f \alpha^{-1} \varphi^{-1} = \varphi^\sigma f (\varphi^\sigma)^{-1} = f_0^\sigma$. Therefore we can take $q_0 = f_0$.

If X has type $(0, n, m)$, then we once again get a k-rational model $\mathcal{D}_0 = q_0^*(\mathcal{S}_0)$ of the branch divisor $\mathcal{D}$ of π_ι, this time on the conic Q, which is not necessarily isomorphic to $\mathbb{P}^1$ over k. If X has type $(2, n, m)$, then we again have to throw in the ramification divisor $\mathcal{U}_0$ of q_0 with $q_0^*(\mathcal{S}_0)$ to get $\mathcal{D}_0$. Note that this ramification divisor is again k-rational; in fact, it is given by the zero divisor $(y)_0$ of the function y on Q.

Regardless, one can now construct a k-rational degree 2 cover X_0 of Q that ramifies over $\mathcal{D}_0$ as in the proof [11, Prop. 4.13], since g is odd. This X_0 is the desired descent. ☐

In this case, the algorithm to obtain a descent is as follows.

Algorithm 3.20. *Let X denote a hyperelliptic curve over K of genus g and type (i, n, m) with $n > 1$ whose field of moduli for the extension $K|k$ equals k. Suppose that n and g are both odd. Then a descent X_0 of X can be constructed as follows.*

- *(i) Using the methods in* [12, Sec. 2]*, construct a binary form f of type (i, n, m) that represents X.*
- *(ii) Compute the normalized homogeneous dihedral invariants $I(f)$.*
- *(iii) Construct a descent f_L to the invariant extension L of k defined by f by using Corollary* 2.13.
- *(iv) If $i = 1$, then set $f_0 = f_L$ and terminate.*
- *(v) Determine the quantity r in* (3.8) *for f_L, either by using Lemma* 3.13 *in the generic case, or alternatively by using the methods in* [12, Sec. 2].
- *(vi) Let $\lambda = -1/r$ and let $\mu \in k$ be such that $L = k(\sqrt{\mu})$. Construct the conic $\mathsf{Q} : x^2 + \lambda y^2 + \mu z^2 = 0$ over k, and let $\varphi : \mathbb{P}^1 \to \mathsf{Q}$ be the rational parametrization from the point $(\sqrt{-\mu} : 0 : 1) \in \mathsf{Q}(L)$.*
- *(vii) Let $f : \mathbb{P}^1 \to \mathbb{P}^1$ be the K-rational morphism given by $x \to x^n/r^{(n-1)/2}$, and let $f_0 = \varphi f \varphi^{-1}$.*
- *(viii) Let $\mathcal{D}_0 = f_0^*(\mathcal{S}_0)$ (resp. $\mathcal{D}_0 = f_0^*(\mathcal{S}_0) + (y)_0$) if $i = 0$ (resp. $i = 2$).*
- *(ix) As in* [11, Prop. 4.13]*, let X_0 be the k-rational degree 2 cover of Q ramifying in $\mathcal{D}_0$.*

A calculation involving this algorithm can be found in Example 4.6.

3.4. **The case of trivial reduced automorphism group.** We conclude our discussion of explicit descent by considering the case where the hyperelliptic curve X over K is of type $(i, 1, m)$, or more straightforwardly expressed, the reduced automorphism group X is trivial. Our descent obstruction results in the previous sections generalize to this case. If g is even, then our Theorem 1.6 recovers a classical result by Mestre [13] which states that in even genus a curve X with trivial reduced automorphism group descends if and only if it descends hyperelliptically [13]. On the other hand, if g is odd, then [11, Prop. 4.13] shows that a descent always exists, completely in line with our Theorem 3.19.

Still, to construct an explicit descent X_0 of X in these cases is actually more complicated, due to the absence of homogeneous dihedral invariants. We briefly discuss two ways to get around this problem.

3.4.1. *The covariant method.* The first and most effective way is to use the *covariant method* [12]. We now apply it to the case under consideration.

Proposition 3.21. *Let* X *be a hyperelliptic curve with trivial reduced automorphism group, defined by a binary form* f. *Let* c *be a covariant of* f *with single roots whose automorphism group is trivial as well, and let* $\mathsf{Y} : y^2 = c$ *be the hyperelliptic curve defined by* c.

(i) The field of moduli of the curve Y *with respect to the extension* $K|k$ *again equals* k.

(ii) X *admits an hyperelliptic descent if and only if* Y *does. Moreover, if* Y *does not allow a hyperelliptic descent, then neither does* X *allow a general descent if the genus of* X *is even.*

(iii) Suppose that Y *admits a hyperelliptic descent* Y_0 *defined by a homogeneous polynomial* c_0. *Then if* $A \in \mathrm{GL}_2(K)$ *transforms* c *into* c_0, *the transformation* $A.f$ *of* f *also yields a descent of* f *(after possibly dividing out a scalar).*

(iv) Suppose that the genus of X *is odd. Let* $\mathsf{R} = \mathsf{Y}/\iota_{\mathsf{Y}} = \mathsf{Y}/\operatorname{Aut}(\mathsf{Y})$, *and let* R_0 *be the canonical model of* R. *Let* $\varphi : \mathsf{R} \to \mathsf{R}_0$ *be the canonical descent morphism. Let* $\mathcal{D}$ *be the branch locus of* $\pi : \mathsf{X} \to \mathsf{X}/\iota_{\mathsf{X}} = \mathsf{X}/\operatorname{Aut}(\mathsf{X})$. *Then the image* $\mathcal{D}_0 = \varphi(\mathcal{D})$ *is a* k*-rational divisor on* B_0. *There exists a degree* 2 *cover* X_0 *of* R_0 *over* k *whose branch locus equals* $\mathcal{D}_0$. *The curve* X_0 *is then a descent of* X.

Proof. (i) By definition of covariance, the isomorphisms $\mathsf{X} \to \mathsf{X}^\sigma$ give rise to isomorphisms $\mathsf{Y} \to \mathsf{Y}^\sigma$.

(ii) The first part follows from [12, Thm. 3.8], and the second part from [13].

(iii) This again follows from [12, Thm. 3.8].

(iv) The canonical descent datum on the quotient R gives rise to the conic R_0, which is a k-rational model for both $\mathsf{Y}/\iota_{\mathsf{Y}}$ and $\mathsf{X}/\iota_{\mathsf{X}}$. By covariance, the morphism φ is also the Weil coboundary $(\mathsf{X}/\iota_{\mathsf{X}}, \mathcal{D}) \to (\mathsf{R}_0, \mathcal{D}_0)$ for the pair $(\mathsf{X}/\iota_{\mathsf{X}}, \mathcal{D})$. Therefore the image $\mathcal{D}_0$ is indeed k-rational. One then again invokes [11, Prop. 4.13]. □

Remark 3.22. Proposition 3.21 is especially useful for sextic and octavic covariants c, since for these, the results from [13] and [12, Sec. 2] allow us to test effectively whether it has trivial automorphism group. Moreover, in these cases effective methods to determine the descent obstruction are available, as well as methods to determine an explicit descent if this obstruction vanishes.

Remark 3.23. At least in characteristic 0 and genus $g \leq 2^7$, a covariant c with the properties in Proposition 3.21 exists. More precisely, if we let f be a generic binary form defining X, then the covariant form $c = (f, f)_{2g-2}$ is a nonsingular binary octavic with trivial automorphism group.

Given a genus g, this statement is easy to verify with a computer algebra package; by the proof of [12, Prop. 2.9], it suffices to produce a single example of such an f. Usually the first randomly chosen f already works, in line with our expectations that a covariant c should generically always exist. On the other hand, to prove the existence of such a covariant in the generic case for arbitrary genus, let alone for all hyperelliptic curves with trivial reduced automorphism group, seems to be more involved.

3.4.2. *Explicit cocycle construction.* We mention a second approach, which could be used in the unlikely event that no suitable covariant is available. If X is defined by a binary form f over a finite Galois extension M of k, then one can construct a suitable cocycle for $\mathsf{B} = \mathsf{X}/\operatorname{Aut}(\mathsf{X}) = \mathsf{X}/\iota$ over M by using the fast methods from [12, Sec. 2]. One then calculates canonical model B_0 of B along with the descent morphism $\mathsf{B} \to \mathsf{B}_0$ as in [8]. If the descent obstruction is trivial, then one proceeds as before; one constructs a descent X_0 of X by ramifying over the image of the branch locus of $\mathsf{X} \to \mathsf{B}$ under the morphism $\mathsf{B} \to \mathsf{B}_0$.

3.5. **Counterexamples.** To finish this section, we will show how to obtain explicit counterexamples to descent. We first treat some classical counterexamples to hyperelliptic descent, where $K = \mathbb{C}$ and $k = \mathbb{R}$. In this case, the classification of the curves that do not descend is known. These curves were essentially first constructed by [3], but the final correct statement is due to Huggins in [9]. The following proposition is a slight improvement of their results.

Proposition 3.24. *Let* Q_0 *be the pointless conic over* $\mathbb{R}$ *defined by the homogeneous equation* $x^2 + y^2 + z^2 = 0$. *Let* $(\mathbb{P}^1, \mathcal{R})$ *be one of the divisors over* $\mathbb{C}$ *defined in* [9, Prop. 5.0.5]. *Consider the* $\mathbb{C}$*-morphism* $\varphi : \mathbb{P}^1 \to \mathsf{Q}_0$ *given by*

$$(s : t) \to (i(s^2 + t^2) : s^2 - t^2 : 2st).$$

Then $\mathcal{R}_0 = \varphi_*(\mathcal{R})$ *is an* $\mathbb{R}$*-rational divisor on* Q_0 *that defines a hyperelliptic curve* X *over* $\mathbb{C}$ *whose field of moduli for the extension* $\mathbb{C}|\mathbb{R}$ *is* $\mathbb{R}$ *but which does not descend hyperelliptically.*

Up to isomorphism over $\mathbb{C}$*, all counterexamples to hyperelliptic descent from* $\mathbb{C}$ *to* $\mathbb{R}$ *are of the form* X *considered above. Such a curve* X *still descends to* $\mathbb{R}$ *if and only if its genus and the cardinality of its reduced automorphism group* $\overline{G}$ *of* X *are both odd.*

Proof. Let σ be the generator of $\operatorname{Gal}(\mathbb{C}|\mathbb{R})$. Then $\mathcal{R}^\sigma = \alpha_*(\mathcal{R})$, where $\alpha : \mathbb{P}^1 \to \mathbb{P}^1$ is the $\mathbb{R}$-rational morphism given by $(s : t) \to (-t : s)$. Now we have $\varphi^\sigma = \varphi\alpha$. Therefore

$$\mathcal{R}_0^\sigma = \varphi_*^\sigma(\mathcal{R}^\sigma) = (\varphi\alpha)_*(\mathcal{R}) = \varphi_*(\alpha_*(\mathcal{R})) = \varphi_*(\mathcal{R}) = \mathcal{R}_0$$

and hence $\mathcal{R}_0$ is indeed $\mathbb{R}$-rational. All is now clear from [9, Prop. 5.0.5], except for our sharpening of the result (the final line of the proposition). But this follows from Theorem 3.19. ☐

Remark 3.25. A signature argument as in [11, Prop. 4.3] can also be used to prove Proposition 3.24, except if $\overline{G} \cong \mathbf{C}_n$ with n odd and either g/n is odd or $(g+1)/n$ is even. Theorem 3.19 shows that in these cases, a descent is always possible, and Algorithm 3.20 shows how this descent can be obtained explicitly.

Having precisely analyzed the obstruction to descent in the previous subsections, it is now straightforward to give a complete classification of those hyperelliptic curves with tamely cyclic and nontrivial reduced automorphism group whose field of moduli is not a field of definition.

Theorem 3.26. *Let* $L = k(\sqrt{d_1})$ *be a quadratic extension of* k *defined by an element* d_1 *of* k*, and choose* $d_2 \in k$ *such that* d_2 *is not a norm from* L. *Let* $u \in L$ *be such that* $\operatorname{Nm}_k^L(u) = 1$. *Let* $m = 2\ell$ *be an even number, and choose* $a_m, \dots, a_0$ *in* L *such that*

$$a_\ell^\sigma = ua_\ell,\ a_{\ell-1} = ud_2 a_{\ell+1}^\sigma, \dots,\ a_0 = ud_2^\ell a_m^\sigma$$

for the nontrivial element σ *of* $\operatorname{Gal}(L|k)$. *Consider the binary forms*

$$f = a_m x^{mn} + a_{m-1} x^{(m-1)n} z^n + \dots + a_1 x^n z^{(m-1)n} + a_0 z^{mn},$$
$$g = xzf.$$

Suppose that f is of type $(0, n, m)$, so that g is of type $(2, n, m)$, and that the geometric automorphism group $\mathrm{Aut}_K(f)$ is generated by $(x, z) \mapsto (\zeta_n x, z)$. Then the curves corresponding to f and g have field of moduli k for the extension $K|k$ and do not descend hyperelliptically to k.

Up to isomorphism over K, all counterexamples to hyperelliptic descent from K to k are of the form X considered above. Such a curve X still descends to k if and only if its genus and n are both odd.

Proof. The forms under consideration are already in normal form. Therefore their invariant extension equals the quadratic extension L itself. This makes it straightforward to calculate the matrix (3.8) for these examples, which is simply given by $\left(\begin{smallmatrix} 0 & d_2 \\ 1 & 0 \end{smallmatrix}\right)$. Combining Theorem 1.13 with Proposition 1.14 then shows that we indeed get counterexamples.

The universality statement needs a bit more work. Note first that indeed any counterexample is determined by a normal form (2.2)–(2.4) in light of Proposition 3.4(ii). We only have to cull those normal forms for which the element r in the matrix (3.8) is not a norm from $L = k(\sqrt{d_1})$. We can do this by inverting the procedure in Section 3; one chooses $d_2 = r$ not to be a norm, constructs the matrix $A = \left(\begin{smallmatrix} 0 & d_2 \\ 1 & 0 \end{smallmatrix}\right)$, and finally determines those forms f over L for which there exists a scalar u such that $Af = uf^\sigma$. This gives the requested forms, with the demand that $\mathrm{Nm}_k^L(u) = 1$ coming from the compatibility condition $(f^\sigma)^\sigma = f$.

The final statement of the theorem is again a consequence of Theorem 3.19. □

Remark 3.27. Phrased differently, we have shown that the curves constructed in Theorem 3.26 descend if and only if the quaternion algebra defined by d_1 and d_2 splits. This gives some unexpected symmetry properties for the obstruction since, for example, exchanging d_1 and d_2 yields the same quaternion algebra.

Remark 3.28. For genus 3, the explicit stratum equations in [11, Sec. 3] can be used to quickly determine whether a given curve X is of a given type (i, n, m). For general genus, it is usually easy to verify this once the coefficients of the polynomial f defining X are given, by using the methods of [12, Sec. 2].

This construction gives counterexamples for many more quadratic field extensions than the usual $\mathbb{C}|\mathbb{R}$. Moreover, the cases where d_2 *is* a norm from L yield a host of examples for which it is anything but obvious that the resulting curves descend, and which we will consider in the next section.

4. Implementation and examples

We have used the generic homogeneous dihedral invariants of Proposition 2.7 in `Magma` to give an implementation of Algorithms 3.18 and 3.20 for the curves for which these invariants suffice. Our code is available online[1].

The implementation is straightforward considering the constructive methods that were used. First one determines a generator α_0 of the reduced automorphism group, which can be done effectively by using the methods in [12, Sec. 2]. Subsequently, one diagonalizes α_0 over an at most quadratic extension of the base field of K. The remaining steps in Algorithms 3.18 and 3.20 (determining and normalizing the homogeneous invariants, parametrizing to determine a partial descent, solving a norm equation and if necessary constructing the necessary cover to define X over k) are effective and efficient for 'natural' fields such as number fields and finite fields.

We now give some examples of these computations. Throughout, we will have $k = \mathbb{Q}$ and $K = \overline{\mathbb{Q}}$. To begin with, we mention that we usually do not need the full set of generic homogeneous dihedral invariants in our computations, and our algorithms take this into account. The following example of a hyperelliptic curve of type $(0, 2, 6)$ illustrates this.

Example 4.1. In Theorem 3.14, let $d_1 = 2, d_2 = 3$, let σ be an automorphism of K restricting to a generator of $k(\sqrt{d_1})$, and take

$$\begin{aligned} a_6 &= 7 + \sqrt{d_1}, a_5 = 3 - 2\sqrt{d_1}, a_4 = (1 + \sqrt{d_1}), a_3 = 12\sqrt{d_1}, \\ a_2 &= -d_2 a_4^\sigma = -d_2(1 - \sqrt{d_1}), a_1 = -d_2^2 a_5^\sigma = -d_2^2(3 + 2\sqrt{d_1}), \\ a_0 &= -d_2^3 a_6^\sigma = -d_2^3(7 - \sqrt{d_1}). \end{aligned}$$

Let

$$f = a_6 x^{12} + a_5 x^{10} z^2 + a_4 x^8 z^4 + a_3 x^6 z^6 + a_2 x^4 z^8 + a_1 x^2 z^{10} + a_0 z^{12}.$$

As in Remark 2.20, the corresponding hyperelliptic curve is determined by the following subset of the homogeneous dihedral invariants:

$$(I_1, I_{2,0}, I_{2,1}, I_{2,2}, I_{3,3,1}, I_{3,3,2}, I_{3,4}).$$

Indeed, one shows by direct calculation that $J_3 \neq J_3'$ for f, hence also for all its transformations. Having chosen the ordering of the roots J_3 and J_3' of the corresponding quadratic equation, the linear system

$$\begin{aligned} J_i + J_i' &= I_{i,i,1}, \\ J_3' J_i + J_3 J_i' &= I_{3,i} \end{aligned}$$

is always invertible for $i > 3$, determining J_i and J_i' in terms of the choice of the order of J_3 and J_3' and the invariants $(I_1, I_{2,0}, I_{2,1}, I_{2,2}, I_{3,3,1}, I_{3,3,2}, I_{3,4})$. In particular, we need only normalize these latter invariants to determine the field of moduli of our curve. This normalization is

$$\left(1, \frac{-3 \cdot 47}{2^5}, \frac{-1}{2^5}, \frac{1}{2^5 \cdot 3}, \frac{-1}{2^4}, \frac{-1}{2^{15} \cdot 3^2}, \frac{-1}{2^{13} \cdot 3^2}\right),$$

so the field of moduli is indeed the rational field k. Calculating the norm obstruction r and $L = \mathbb{Q}(\sqrt{d_1})$ in Theorem 3.14 and using the norm criterion now shows that the curve corresponding to f does not descend to k. This is as expected, because this example was constructed by using Theorem 3.26.

Now we will consider a hyperelliptic curve of type $(2, 2, 3)$.

Example 4.2. Consider the genus 3 hyperelliptic curve X over K corresponding to the binary form

$$\begin{aligned} &(20456\sqrt{5} + 43640)x^8 + (-17772\sqrt{5} - 56716)x^7 z \\ &\quad + (28984\sqrt{5} + 3584)x^6 z^2 + (25862\sqrt{5} - 95522)x^5 z^3 \\ &\quad + (67320\sqrt{5} - 136740)x^4 z^4 + (84995\sqrt{5} - 193217)x^3 z^5 \\ &\quad + (75097\sqrt{5} - 167611)x^2 z^6 + (38764\sqrt{5} - 86676)x z^7 + (7942\sqrt{5} - 17762)z^8 \end{aligned}$$

over $L = \mathbb{Q}(\sqrt{5}) \subset K$. This curve has an automorphism of order 2, and it allows a normal form (2.4) over L given by

$$xz((11270829\sqrt{5} - 25242007)x^6 + (1408299\sqrt{5} - 5284449)x^4z^2 + (-5642070\sqrt{5} - 12929374)x^2z^4 + (-204992252\sqrt{5} - 458411532)z^6).$$

The normalized homogeneous dihedral invariants of this form now generate the field of moduli k. They are given by

$$(I_{2,0}, I_{2,1}, I_{4,4,1}, I_{4,4,2}) = \left(\frac{2}{3}, 1, \frac{29}{3^2}, \frac{2}{3}\right).$$

Lemma 3.13 shows that the norm obstruction is trivial because $m = 3$ is odd. In this particular case, this reflects itself in the fact that the homogeneous diagonal invariants are themselves already rational. They are given by

$$(J_{2,0}, J_{2,1}, J_4) = \left(\frac{2}{3}, 1, 3\right).$$

Reconstructing as in Corollary 2.13, we get the descent

$$y^2 = xz\left(3x^6 + x^4z^2 + x^2z^4 + \frac{2}{9}z^6\right).$$

Finally, we descend a hyperelliptic curve of type $(1, 3, 3)$.

Example 4.3. Consider the genus 4 hyperelliptic curve X corresponding to the binary form

$$\begin{aligned}(138076\sqrt{5} + 291100)x^{10} &+ (-120728\sqrt{5} - 370816)x^9z \\ &+ (243042\sqrt{5} + 208878)x^8z^2 + (48987\sqrt{5} - 760529)x^7z^3 \\ &+ (515947\sqrt{5} - 751581)x^6z^4 + (754227\sqrt{5} - 1880505)x^5z^5 \\ &+ (1243617\sqrt{5} - 2713183)x^4z^6 + (1462433\sqrt{5} - 3287139)x^3z^7 \\ &+ (1243263\sqrt{5} - 2777109)x^2z^8 + (625402\sqrt{5} - 1398734)xz^9 \\ &+ (124654\sqrt{5} - 278722)z^{10}.\end{aligned}$$

over $L = \mathbb{Q}(\sqrt{5})$. This curve has an automorphism of order 3, and it allows a normal form (2.3) over the ground field given by

$$\begin{aligned}z((91955817\sqrt{5} - 213442907)x^9 &+ (268416746\sqrt{5} + 589172042)x^6z^3 \\ &+ (-30323641593\sqrt{5} - 67805941509)x^3z^6 \\ &+ (3073332514916\sqrt{5} + 6872180416996)z^9).\end{aligned}$$

Lemma 3.11 shows that the normalized homogeneous diagonal invariants for this case will generate the field of moduli $k = \mathbb{Q}$. In this case, these invariants are up to scalar given by

$$(J_{2,0}, J_{2,1}, J_4) = \left(\frac{2}{3}, 1, \frac{8}{3^2}\right).$$

Using the parametrization of Corollary 2.13 for the generic case, we obtain the following hyperelliptic descent of X:

$$y^2 = z\left(\frac{8}{3^2}x^9 + x^6z^3 + x^3z^6 + \frac{3}{4}z^9\right).$$

As Lemma 3.11 predicts, this normal form is already defined over the field of moduli k itself (rather than over a quadratic extension).

We now discuss some examples of curves of genus 3. Indeed, this was our initial motivation for this paper, the cases of genus 2 having been completely resolved already in [13] and [4].

The invariant theory of binary octavics was completely determined by Shioda in [17], and can be applied to solve the descent problem for genus 3 hyperelliptic curves with great efficiency. The steps for this are as follows.

- Using the stratum equations from [11, Sec. 3], determine the geometric automorphism group G of X from its Shioda invariants.
- If $G \not\cong \mathbf{D}_4$, then use either the parametrizations or reconstruction methods from [11, Sec. 3] or (in the case $G \cong \mathbf{C}_2^3$) the covariant descent method in [12, Sec. 3B2].
- If $G \cong \mathbf{D}_4$, then determine the homogeneous dihedral invariants of f, directly or from its Shioda invariants [2], and apply the methods of this paper.

Example 4.4. As in Example 4.1, let $d_1 = 2, d_2 = 3$. This time, take

$$a_4 = 7 + \sqrt{d_1}, a_3 = 3 - 2\sqrt{d_1}, a_2 = 12\sqrt{d_1},$$
$$a_1 = -d_2 a_3^\sigma = -d_2(3 + 2\sqrt{d_1}), a_0 = -d_2^2 a_4^\sigma = -d_2^2(7 - \sqrt{d_1}).$$

Construct the binary octavic

$$f = a_4 x^8 + a_3 x^6 z^2 + a_2 x^4 z^4 + a_1 x^2 z^6 + a_0 z^8.$$

The normalized Shioda invariants of this octavic (and of its transformations under $\mathrm{GL}_2(K)$) are given by

$$\begin{gathered}
-5 \cdot 7 \cdot 401^3/(3^3 \cdot 13^2 \cdot 23^2 \cdot 1667^2),\\
-5 \cdot 7 \cdot 401^3/(3^3 \cdot 13^2 \cdot 23^2 \cdot 1667^2),\\
2^4 \cdot 5^4 \cdot 7^{13} \cdot 401^4 \cdot 3435911/(3^7 \cdot 13^4 \cdot 23^4 \cdot 1667^4),\\
2^3 \cdot 5^4 \cdot 7^{16} \cdot 401^5 \cdot 1663 \cdot 29947/(3^7 \cdot 13^5 \cdot 23^5 \cdot 1667^5),\\
2^3 \cdot 5^7 \cdot 7^{18} \cdot 47 \cdot 59 \cdot 401^6 \cdot 3271 \cdot 14653/(3^{11} \cdot 13^6 \cdot 23^6 \cdot 1667^6),\\
2^3 \cdot 5^7 \cdot 7^{22} \cdot 401^7 \cdot 166150639393/(3^{11} \cdot 13^7 \cdot 23^7 \cdot 1667^7),\\
-2 \cdot 5^7 \cdot 7^{25} \cdot 401^8 \cdot 25309 \cdot 148913 \cdot 395201/(3^{13} \cdot 13^8 \cdot 23^8 \cdot 1667^8),\\
2^6 \cdot 5^8 \cdot 7^{27} \cdot 17 \cdot 401^9 \cdot 4278649 \cdot 127546933/(3^{15} \cdot 13^9 \cdot 23^9 \cdot 1667^9),\\
-2^2 \cdot 5^8 \cdot 7^{30} \cdot 11 \cdot 61 \cdot 401^{10} \cdot 537787278082528849/(3^{17} \cdot 13^{10} \cdot 23^{10} \cdot 1667^{10}).
\end{gathered}$$

This gives the normalized homogeneous dihedral invariants

$$(I_1, I_{2,0}, I_{2,1}, I_{3,3,1}, I_{3,3,2}) = \left(1, \frac{-47}{2^5}, \frac{-1}{2^5 \cdot 3}, \frac{101}{2^6 \cdot 3}, \frac{-47}{2^{15} \cdot 3^2}\right),$$

which are somewhat simpler. We have $I_{3,3,1}^2 - 4I_{3,3,2} = 11^2 13^2/2^{13}3^2$. This defines the quadratic extension $L = \mathbb{Q}(\sqrt{2})$ of the rational field, which therefore equals the invariant field of f over the field of moduli $k = \mathbb{Q}$. The invariant $I_{2,1}$ is not a norm from this extension, so we see by Lemma 3.13 that no hyperelliptic descent exists, and hence no descent at all by Theorem 1.6.

We can still use the normalized homogeneous diagonal invariants to get a hyperelliptic descent over invariant extension L. Up to switching J_3 and J_3' we have

$$(J_1, J_{2,0}, J_{2,1}, J_3) = \left(1, \frac{-47}{32}, \frac{-1}{96}, \frac{-143\sqrt{2} + 202}{768}\right).$$

Using Corollary 2.13 in the generic case where the parameter is a_1, we get the following hyperelliptic descent over L:

$$y^2 = (-143/768\sqrt{2} + 101/384)x^8 - 1/96x^6z^2 + x^4z^4 + x^2z^6 + (1716\sqrt{2} + 2424)z^8.$$

Example 4.5. Modifying $d_1 = 3, d_2 = 13$ in Example 4.4 so that the obstruction vanishes, we do get a descent to the rationals. Explicitly, this descent can be constructed as follows, using Algorithm 3.18. This time the norm obstruction r in (3.8) equals 144/13. We then apply Proposition 1.14, taking $\lambda = (-60-24\sqrt{3})/13$ and $\beta = 1/\sqrt{3}$ in the proof. Transforming the quotient $B = \mathsf{X}/G \cong \mathbb{P}^1_K$ into $B_0 \cong \mathbb{P}^1_k$ by the N from Proposition 1.14, the ramification divisor $\mathcal{T}$ of $q : Q \to B$ transforms to $\mathcal{T}_0 = [(\sqrt{3} : 1)] + [(-\sqrt{3} : 1)]$. Using Proposition 3.16, we get the k-rational cover $q_0 : Q_0 = \mathbb{P}^1 \to \mathbb{P}^1 = B_0$ given by

$$(x : z) \longmapsto (x^2 + 3z^2 : 2xz).$$

Under N, the divisor $\mathcal{S}$ on B, that is, the image on B of branch divisor of $\pi_\iota : X \to Q$ is mapped from the zero locus of

$$1/5184(10309\sqrt{3} + 17745)x^4 + 13/144x^3z + x^2z^2 + xz^3 + (-244\sqrt{3} + 420)z^4$$

into that of

$$38x^4 + 320x^3z + 657x^2z^2 + 924xz^3 + 387z^4$$

on the canonical model $B_0 = \mathbb{P}^1_k$ of B. Taking a suitable k-rational binary form vanishing on the pullback of this divisor by q_0, we obtain the hyperelliptic descent

$$\begin{aligned} y^2 = {} & 19x^8 + 320x^7z + 1542x^6z^2 + 6576x^5z^3 + 12006x^4z^4 \\ & +19728x^3z^5 + 13878x^2z^6 + 8640xz^7 + 1539z^8. \end{aligned}$$

Example 4.6. Finally, by modifying Example 4.4 to

$$f = a_4x^{12} + a_3x^9z^3 + a_2x^6z^6 + a_1x^3z^9 + a_0z^{12}$$

we get a curve that does not descend hyperelliptically but which does descend as the cover of a conic. Our implementation of Algorithm 3.20 returns a divisor on the conic $X^2 - 2Y^2 + 96Z^2 = 0$ over which we have to branch. The result, whose expression is slightly unwieldy, can be found online[1] too; here we just mention that over the finite field with 43 elements, where the hyperelliptic descent obstruction vanishes (as over all finite fields by Theorem 1.13), we obtain the descended equation

$$\begin{aligned} y^2 = {} & x^{12} + 25x^{11}z + 6x^{10}z^2 + 30x^9z^3 + 21x^8z^4 + 9x^7z^5 + 21x^6z^6 + \\ & + 37x^5z^7 + 42x^4z^8 + 22x^3z^9 + 5x^2z^{10} + 37xz^{11} + 3z^{12}. \end{aligned}$$

5. Conclusions and remaining questions

In [11] and [12], effective parametrizations of the automorphism strata in genus 3 were determined, which return a model over the field of moduli as long as the reduced automorphism group is not $\mathbf{C}_2$. These methods can also be used to obtain equations for the curves with reduced automorphism group $\mathbf{C}_2$. However, these equations can be of degree up to 8 over the field of moduli, which is far from optimal. The present work shows how one calculates whether such a curve admits a (hyperelliptic) descent to the field of moduli, and how such a descent can be determined explicitly if it exists. Even if the curve does not descend all the way to the field of moduli, a model over the quadratic invariant extension of this field can still be constructed efficiently.

This concludes our explicit arithmetic exploration of the moduli space of hyperelliptic genus 3 curves, at least when the characteristic of the ground field is 0 or bigger than 7. Given any tuple of Shioda invariants of a genus 3 curve, one can now determine

- the automorphism group of the curve,
- whether or not the curve descends to the field of moduli, and
- a model of the curve over its field of moduli, if it exists.

When the characteristic of the ground field is positive and less than or equal to 7, a nontrivial effort is already needed to find the appropriate analogues of the Shioda invariants.

There are some open questions remaining. First of all, though we have given a complete set of effective methods for determining when the field of moduli is a field of definition, it remains to descend effectively if the reduced automorphism group is either not tamely cyclic or trivial. Second, our methods should apply to the *superelliptic* curves $y^n = f(x, z)$ as well. Third, it seems likely that the case of hyperelliptic curves in characteristic 2 will require completely new methods altogether.

Finally, and most intriguingly, while our perfectness hypothesis on k enables us to resolve the descent problem for most interesting ground fields (such as number fields and finite fields), it remain to deal with imperfect base fields k, as mentioned in Remark 1.2. Dealing with general ground fields by further studying the inseparable extension in [14] seems to merit a study of its own, not least towards studying the geometric nature of this extension, which we hope to undertake in the future. Here we merely remark that by [9, Th. 1.6.9], our methods can at least be used to determine whether or not a descent *exists* in these more general cases, while a method to explicitly determine a descent still seems to be out of reach.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[2] R. Brandt and H. Stichtenoth, *Die Automorphismengruppen hyperelliptischer Kurven*, Manuscripta Math. **55** (1986), no. 1, 83–92, DOI 10.1007/BF01168614. MR828412 (87m:14033)

[3] E. Bujalance and P. Turbek, *Asymmetric and pseudo-symmetric hyperelliptic surfaces*, Manuscripta Math. **108** (2002), no. 1, 1–11, DOI 10.1007/s002290200261. MR1912944 (2003h:30056)

[4] G. Cardona and J. Quer, *Field of moduli and field of definition for curves of genus 2*, Computational Aspects of Algebraic Curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 71–83, DOI 10.1142/9789812701640_0006. MR2181874 (2006h:14036)

[5] P. Dèbes and M. Emsalem, *On fields of moduli of curves*, J. Algebra **211** (1999), no. 1, 42–56, DOI 10.1006/jabr.1998.7586. MR1656571 (99k:14044)

[6] C. J. Earle, *On the moduli of closed Riemann surfaces with symmetries*, Advances in The Theory of Riemann Surfaces (Proc. Conf., Stony Brook, N.Y., 1969), Princeton Univ. Press, Princeton, N.J., 1971, pp. 119–130. Ann. of Math. Studies, No. 66. MR0296282 (45 #5343)

[7] J. Gutierrez and T. Shaska, *Hyperelliptic curves with extra involutions*, LMS J. Comput. Math. **8** (2005), 102–115, DOI 10.1112/S1461157000000917. MR2135032 (2006b:14049)

[8] R. A. Hidalgo and S. Reyes, *A constructive proof of Weil's Galois descent theorem*. Preprint at `http://arxiv.org/abs/1203.6294`.

[9] B. S. Huggins, *Fields of Moduli and Fields of Definition of Curves*, ProQuest LLC, Ann Arbor, MI, 2005. Thesis (Ph.D.)–University of California, Berkeley. MR2708514

[10] B. Huggins, *Fields of moduli of hyperelliptic curves*, Math. Res. Lett. **14** (2007), no. 2, 249–262, DOI 10.4310/MRL.2007.v14.n2.a8. MR2318623 (2009a:14040)

[11] R. Lercier and C. Ritzenthaler, *Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects*, J. Algebra **372** (2012), 595–636, DOI 10.1016/j.jalgebra.2012.07.054. MR2990029

[12] R. Lercier, C. Ritzenthaler, and J. Sijsling, *Fast computation of isomorphisms of hyperelliptic curves and explicit descent*, ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, pages 463–486. Mathematical Science Publishers, 2013.

[13] J.-F. Mestre, *Construction de courbes de genre 2 à partir de leurs modules* (French), Effective Methods in Algebraic Geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334. MR1106431 (92g:14022)

[14] T. Sekiguchi, *On the fields of rationality for curves and for their Jacobian varieties*, Nagoya Math. J. **88** (1982), 197–212. MR683250 (85a:14021)

[15] J.-P. Serre, *Cohomologie Galoisienne* (French), 5th ed., Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin, 1994. MR1324577 (96b:12010)

[16] G. Shimura, *On the field of rationality for an abelian variety*, Nagoya Math. J. **45** (1972), 167–178. MR0306215 (46 #5342)

[17] T. Shioda, *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89** (1967), 1022–1046. MR0220738 (36 #3790)

[18] D. L. Wehlau, *Constructive invariant theory for tori*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 1055–1066. MR1252937 (95c:14068)

[19] A. Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524. MR0082726 (18,601a)

[20] X. Xarles, *Trivial points on towers of curves*, J. Théor. Nombres Bordeaux **25** (2013), no. 2, 477–498. MR3228317

DGA MI La Roche Marguerite, 35174 Bruz, France

IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes, France
E-mail address: reynald.lercier@m4x.org

IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes, France
E-mail address: ritzenth@iml.univ-mrs.fr

Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL, United Kingdom
E-mail address: sijsling@gmail.com