The Belyi degree of a curve is computable

Ariyan Javanpeykar and John Voight

Abstract. We exhibit an algorithm that, given input a curve X over a number field, computes as output the minimal degree of a Belyĭ map $X \to \mathbb{P}^1$.

1. Introduction

Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Let X be a smooth projective connected curve over $\overline{\mathbb{Q}}$; we call X just a curve. Belyĭ proved [**4, 5**] that there exists a finite morphism $\phi\colon X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ unramified away from $\{0, 1, \infty\}$; we call such a map ϕ a Belyĭ map.

Grothendieck applied Belyĭ's theorem to show that the action of the absolute Galois group of $\mathbb{Q}$ on the set of dessins d'enfants is faithful [**22**, Theorem 4.7.7]. This observation began a flurry of activity [**19**]: for instance, the theory of dessins d'enfants was used to show that the action of the Galois group of $\mathbb{Q}$ on the set of connected components of the coarse moduli space of surfaces of general type is faithful [**2, 10**]. Indeed, the applications of Belyĭ's theorem are vast.

In this paper, we consider Belyĭ maps from the point of view of algorithmic theory. We define the Belyĭ degree of X, denoted by $\operatorname{Beldeg}(X) \in \mathbb{Z}_{\geqslant 1}$, to be the minimal degree of a Belyĭ map $X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$. This integer appears naturally in Arakelov theory, the study of rational points on curves, and computational aspects of algebraic curves [**7, 12, 13, 20**]. The aim of this paper is to show that the Belyĭ degree is an effectively computable invariant of the curve X.

Theorem 1.1. *There exists an algorithm that, given as input a curve X over $\overline{\mathbb{Q}}$, computes as output the Belyĭ degree* $\operatorname{Beldeg}(X)$.

The input curve X is specified by equations in projective space with coefficients in a number field. In fact, the resulting equations need only provide a birational model for X, as one can then effectively compute a smooth projective model birational to the given one.

In the proof of his theorem, Belyĭ provided an algorithm that, given as input a finite set of points $B \subset \mathbb{P}^1(\overline{\mathbb{Q}})$, computes a Belyĭ map $\phi\colon \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ (defined over $\mathbb{Q}$) such that $\phi(B) \subseteq \{0, 1, \infty\}$. Taking B to be the ramification set of any finite map $X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$, it follows that there is an algorithm that, given as input a curve X over

1991 *Mathematics Subject Classification.* 11G32, 11Y40.

Key words and phrases. Belyĭ map, Belyĭ degree, algorithm, effectively computable, Riemann-Roch space, moduli space of curves.

$\overline{\mathbb{Q}}$, computes as output an *upper bound* for $\operatorname{Beldeg}(X)$. Khadjavi [**14**] has given an explicit such upper bound—see Proposition 2.9 for a precise statement. So at least one knows that the Belyĭ degree has a computable upper bound. However, neither of these results give a way to compute the Belyĭ degree: what one needs is the ability to test if a curve X has a Belyĭ map of a given degree d. Exhibiting such a test is the content of this paper, as follows.

A partition triple of d is a triple of partitions $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ of d. The ramification type associates to each isomorphism class of Belyĭ map of degree d a partition triple λ of d.

THEOREM 1.2. *There exists an algorithm that, given as input a curve X over $\overline{\mathbb{Q}}$, an integer $d \geqslant 1$ and a partition triple λ of d, determines if there exists a Belyĭ map $\phi\colon X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ of degree d with ramification type λ; and, if so, gives as output a model for such a map ϕ.*

Theorem 1.2 implies Theorem 1.1: for each $d \geqslant 1$, we loop over partition triples λ of d and we call the algorithm in Theorem 1.2; we terminate and return d when we find a map.

The plan of this paper is as follows. In section 2, we begin to study the Belyĭ degree and gather some of its basic properties. For instance, we observe that, for all odd $d \geqslant 1$, there is a curve of Belyĭ degree d. We also recall Khadjavi's effective version of Belyi's theorem. In section 3, we prove Theorem 1.2 by exhibiting equations for the space of Belyi maps on a curve with given degree and ramification type: see Proposition 3.7. In section 4, we sketch a second proof, which is less instructive but still proves the main result. Finally, in section 5 we conclude with some examples.

Acknowledgements. This note grew out of questions asked to the authors by Yuri Bilu, Javier Fresán, David Holmes, and Jaap Top. The first named author gratefully acknowledges support from SFB Transregio/45. The second named author was supported by an NSF CAREER Award (DMS-1151047).

2. The Belyi degree

In this section, we collect basic properties of the Belyĭ degree. Throughout, a curve X is a smooth projective variety of dimension 1 over $\overline{\mathbb{Q}}$; we denote its genus by $g = g(X)$. We write $\mathbb{P}^n$ and $\mathbb{A}^n$ for the schemes $\mathbb{P}^n_{\overline{\mathbb{Q}}}$ and $\mathbb{A}^n_{\overline{\mathbb{Q}}}$, respectively. A Belyĭ map on X is a finite morphism $X \to \mathbb{P}^1$ unramified away from $\{0, 1, \infty\}$. For $d \geqslant 1$, define $\operatorname{Bel}_d(X)$ to be the set of isomorphism classes of Belyĭ maps of degree d on X, and let $\operatorname{Bel}(X) := \bigcup_d \operatorname{Bel}_d(X)$.

DEFINITION 2.1. The Belyĭ degree of X, denoted $\operatorname{Beldeg}(X) \in \mathbb{Z}_{\geqslant 1}$, is the minimal degree of a Belyĭ map on X.

In our notation, the Belyĭ degree of X is the smallest positive integer d such that $\operatorname{Bel}_d(X)$ is non-empty.

LEMMA 2.2. *The set of isomorphism classes of curves X with $\operatorname{Beldeg}(X) \leqslant C$ is finite for all $C \in \mathbb{R}_{\geqslant 1}$.*

PROOF. The monodromy representation provides a bijection between isomorphism classes of Belyĭ maps of degree d and permutation triples from S_d up to simultaneous conjugation; and there are only finitely many of the latter for each

d. Said another way: the (topological) fundamental group of $\mathbb{P}^1(\mathbb{C}) \smallsetminus \{0, 1, \infty\}$ is finitely generated, and so there are only finitely many conjugacy classes of subgroups of bounded index. $\square$

Classical modular curves have their Belyĭ degree bounded above by the index of the corresponding modular group, as follows.

EXAMPLE 2.3. Let $\Gamma \leqslant \mathrm{PSL}_2(\mathbb{Z})$ be a finite index subgroup, and let $X(\Gamma) := \Gamma\backslash\mathbf{H}^{2*}$ where $\mathbf{H}^{2*}$ denotes the completed upper half-plane. Then $\mathrm{Beldeg}(X(\Gamma)) \leqslant [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma]$, because the natural map $X(\Gamma) \to X(1) = \mathrm{PSL}_2(\mathbb{Z})\backslash\mathbf{H}^{2*} \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{C}}$ descends to $\overline{\mathbb{Q}}$ and defines a Belyĭ map, where the latter isomorphism is the normalized modular j-invariant $j/1728$.

A lower bound on the Belyĭ degree may be given in terms of the genus.

PROPOSITION 2.4. *For every curve X, the inequality* $\mathrm{Beldeg}(X) \geqslant 2g(X) + 1$ *holds.*

PROOF. By the Riemann–Hurwitz theorem, the degree of a map is minimized when its ramification is total, so for a Belyĭ map of degree d on X we have

$$2g + 2 \leqslant -2d + 3(d-1) = d - 3$$

and therefore $d \geqslant 2g + 1$. $\square$

COROLLARY 2.5. *A map of minimal degree $\phi\colon X \to \mathbb{P}^1$ is a Belyĭ map only if ϕ is an isomorphism.*

PROOF. If $g(X) = 0$, then the result is clear. On the other hand, the gonality of X is bounded above by $\lceil g(X)/2 \rceil + 1$ by Brill–Noether theory [**1**, Chapter V], and the strict inequality $2g(X) + 1 > g(X)/2 + 1$ holds unless $g(X) = 0$, so the result follows from Proposition 2.4. $\square$

EXAMPLE 2.6. Let $d = 2g + 1 \geqslant 1$ be odd, and let X be the curve defined by $y^2 - y = x^d$. Then X has genus g, and we verify that the map $y\colon X \to \mathbb{P}^1$ is a Belyĭ map of degree d. Therefore, the lower bound in Proposition 2.4 is sharp for every g.

REMARK 2.7. The bound in Proposition 2.4 gives a "topological" lower bound for the Belyĭ degree of X. One can also give "arithmetic" lower bounds as follows. Let p be a prime number, and let X be the elliptic curve given by $y^2 = x(x-1)(x-p)$ over $\mathbb{Q}$. Then X has (bad) multiplicative reduction at p and this bad reduction persists over any extension field. It follows from work of Beckmann [**3**] that $\mathrm{Beldeg}(X) \geqslant p$: if $\phi\colon X \to \mathbb{P}^1$ is a Belyĭ map of degree $d < p$, then the monodromy group G of ϕ has $p \nmid \#G$, and so ϕ and therefore X has potentially good reduction (obtained over an extension of $\mathbb{Q}$ unramified at p), a contradiction.

EXAMPLE 2.8. For every $n \geqslant 1$, the Belyĭ degree of the Fermat curve $X\colon x^n + y^n = z^n$ in $\mathbb{P}^2$ is at most n^2, because there is a Belyĭ map $(x : y : z) \mapsto (x^n : z^n)$ of degree n^2.

For $n = 1, 2$, we have $X \simeq \mathbb{P}^1$ so $\mathrm{Beldeg}(X) = 1$. For $n = 3$, the curve X is a genus 1 curve with j-invariant 0, so isomorphic to $y^2 - y = x^3$, and $\mathrm{Beldeg}(X) = 3$ by Example 2.6.

For $n = 4$, the curve X is genus 3 curve, so $\mathrm{Beldeg}(X) \geqslant 7$ by Proposition 2.4. On the other hand, X maps to the genus 1 curve with affine model $z^2 = x^4 + 1$

and j-invariant 1728, and this latter curve has a Belyĭ map of degree 4 (taking the quotient by its automorphism group of order 4 as an elliptic curve, equipped with a point at infinity). Composing the two, we obtain a Belyĭ map of degree 8 on X defined by $(x:y:z) \mapsto x^2+z^2$; therefore $\operatorname{Beldeg}(X) \leqslant 8$.

So to show $\operatorname{Beldeg}(X) = 8$, it suffices to rule out the existence of a Belyĭ map of degree 7: we do this in Example 5.2, following (and motivating) the algorithm of this paper. The only partition triple of 7 that gives rise to a Belyĭ map $\phi\colon X \to \mathbb{P}^1$ with X of genus 3 is $(7,7,7)$. It is classical that $\operatorname{Aut}(X) \simeq S_3 \rtimes (\mathbb{Z}/4\mathbb{Z})^2$, so $\#\operatorname{Aut}(X) = 96$. We compute directly from the permutations that the Belyĭ maps of degree 7 and genus 3 have three possible monodromy groups: cyclic of order 7, the simple group $\mathrm{GL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$ of order 168, or the alternating group A_7. The first cyclic case is the map in Example 2.6 above: the curve $y^2 - y = x^7$ has an automorphism of order 7, and X does not. The second was computed by Klug–Musty–Schiavone–Voight [**15**, Example 5.27]: it is minimally defined over $\mathbb{Q}(\sqrt{-7})$, whereas X is defined over $\mathbb{Q}$. We can apply the same argument in the third case, appealing to the exhaustive computation of Belyĭ maps of small degree by Musty–Schiavone–Voight [**17**].

But here is a self-contained argument for the two noncyclic cases. Computing the centralizers of the $2+23=25$ permutation triples up to simultaneous conjugation, we conclude that the Belyĭ maps in the noncyclic case have no automorphisms. An automorphism $\alpha \in \operatorname{Aut}(X)$ of order coprime to 7 cannot commute with a Belyĭ map of prime degree 7 because the quotient by α would be an intermediate curve. So if X had a Belyĭ map of degree 7, there would be 96 nonisomorphic such Belyĭ maps, but that is impossible.

We finish this section with an effective version of Belyĭ's theorem, due to Khadjavi [**14**]. To give her result, we need the height of a finite subset of $\mathbb{P}^1(\overline{\mathbb{Q}})$. For K a number field and $a \in K$, we define the **(exponential) height** to be $H(a) := \left(\prod_v \max(1, \|\alpha\|_v)\right)^{1/[K:\mathbb{Q}]}$, where the product runs over the set of absolute values indexed by the places v of K normalized so that the product formula holds [**14**, Section 2]. For a finite subset $B \subset \mathbb{P}^1(\overline{\mathbb{Q}})$, and K a number field over which the points B are defined, we define its **(exponential) height** by $H_B := \max\{H(\alpha) : \alpha \in B\}$, and we let N_B be the cardinality of the Galois orbit of B.

Proposition 2.9 (Effective version of Belyĭ's theorem). *Let $B \subset \mathbb{P}^1(\overline{\mathbb{Q}})$ be a finite set. Write $N = N_B$. Then there exists a Belyĭ map $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ such that $\phi(B) \subseteq \{0,1,\infty\}$ and*

$$\deg \phi \leqslant (4NH_B)^{9N^3 2^{N-2} N!}.$$

Proof. See Khadjavi [**14**, Theorem 1.1.c]. □

Corollary 2.10. *Let X be a curve, and let $\pi\colon X \to \mathbb{P}^1$ be a finite morphism with branch locus $B \subset \mathbb{P}^1(\overline{\mathbb{Q}})$. Write $N = N_B$. Then*

$$\operatorname{Beldeg}(X) \leqslant (4NH_B)^{9N^3 2^{N-2} N!} \deg \pi.$$

Proof. Choose ϕ as in Proposition 2.9 and consider the composed morphism $\phi \circ \pi$. □

3. First proof of Theorem 1.2

Throughout this section, let K be a number field. We begin with two preliminary lemmas.

LEMMA 3.1. *There exists an algorithm that, given as input an affine variety $X \subset \mathbb{A}^n$ and $t \geqslant 1$, computes as output $N \geqslant 1$ and generators for an ideal $I \subseteq \overline{\mathbb{Q}}[x_1, \ldots, x_N]$ such that the zero locus of I is the variety obtained by removing all the diagonals from X^t/S_t.*

PROOF. Let $X = \operatorname{Spec} \overline{\mathbb{Q}}[x_1, \ldots, x_n]/I$. By (classical) invariant theory (see Sturmfels [**21**]), there is an algorithm to compute the coordinate ring of invariants $\left(\overline{\mathbb{Q}}[x_1, \ldots, x_n]/I\right)^{S_t}$. In other words, there is an algorithm which computes

$$X^t/S_t = \operatorname{Spec}\left(\left(\overline{\mathbb{Q}}[x_1, \ldots, x_n]/I\right)^{S_t}\right).$$

To conclude the proof, note that the complement of a divisor $D = Z(f)$ is again an affine variety, adding a coordinate z satisfying $zf - 1$. □

Next, we show how to represent rational functions on X explicitly.

LEMMA 3.2. *There exists an algorithm that, given as input a curve X defined over K and a positive integer d, computes as output K-linearly independent elements $g_1, \ldots, g_n \in K(X)$ with the following property: for all $f \in \overline{\mathbb{Q}}(X)$ of degree d, there exist $a, b \in \operatorname{span}_{\overline{\mathbb{Q}}}(\{g_1, \ldots, g_n\})$ with $f = a/b$.*

PROOF. First, we compute the genus $g = g(X)$: we compute a Gröbner basis for the defining ideal I of X, compute its Hilbert polynomial, and recover the (arithmetic equals geometric) genus from the constant term. Next, intersecting X with a hyperplane, we obtain an effective divisor D_0 on X over K. Let $\mathscr{L} = \mathscr{O}_X(D_0) = \mathscr{O}_{\mathbb{P}^N}(1)|_X$; then $\mathscr{L}$ is ample on X. For the purposes of this lemma, any ample divisor D_0 on X will do.

We compute $t \geqslant 1$ as the smallest positive integer such that

$$t \deg \mathscr{L} - d + 1 - g \geqslant 1. \tag{3.3}$$

We then (compute a positive integer n and) output

$$g_1, \ldots, g_n \text{ a basis for the } K\text{-vector space } \mathrm{H}^0(X, \mathscr{L}^{\otimes t}). \tag{3.4}$$

This Riemann–Roch calculation can be done effectively, see e.g. Hess [**11**].

We now prove that this output is correct. Let $\operatorname{div}_\infty f \geqslant 0$ be the divisor of poles of f. By Riemann–Roch,

$$\dim_{\overline{\mathbb{Q}}} \mathrm{H}^0(X_{\overline{\mathbb{Q}}}, \mathscr{L}^{\otimes t}(-\operatorname{div}_\infty f)) \geqslant t \deg \mathscr{L} - d + 1 - g \geqslant 1. \tag{3.5}$$

Let

$$b \in \mathrm{H}^0(X_{\overline{\mathbb{Q}}}, \mathscr{L}^{\otimes t}(-\operatorname{div}_\infty f)) \subseteq \mathrm{H}^0(X_{\overline{\mathbb{Q}}}, \mathscr{L}^{\otimes t})$$

be a nonzero element, so $b \in \operatorname{span}_{\overline{\mathbb{Q}}}(\{g_1, \ldots, g_n\})$. Then $fb \in \mathrm{H}^0(X_{\overline{\mathbb{Q}}}, \mathscr{L}^{\otimes t})$: we have cancelled the poles of f by the zeros of b, at the expense of possibly introducing new poles supported within D_0. Letting $fb = a \in \mathrm{H}^0(X, \mathscr{L}^{\otimes t})$ we have written $f = a/b$ as claimed. □

A **ramification type** for a positive integer d is a triple $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ of partitions of d. For X a curve, d an integer, and λ a ramification type, let $\operatorname{Bel}_{d,\lambda}(X) \subseteq \operatorname{Bel}_d(X)$ be the subset of Belyĭ maps of degree d on X with ramification type λ. To prove our main theorem, we will show that one can compute equations whose vanishing locus over $\overline{\mathbb{Q}}$ is precisely the set $\operatorname{Bel}_{d,\lambda}(X)$ (see Proposition 3.7): we call such equations a **model** for $\operatorname{Bel}_{d,\lambda}(X)$.

REMARK 3.6. $\mathrm{Bel}_{d,\lambda}(X)$ is a (non-positive dimensional) Hurwitz space: see for instance Bertin–Romagny [**6**, Section 6.6] (but also Mochizuki [**16**] and Romagny–Wewers [**18**]). Indeed, for a scheme S over $\overline{\mathbb{Q}}$, let $\underline{\mathrm{Bel}}_{d,\lambda,X}(S)$ be the groupoid whose objects are tuples $(f\colon Y \to \mathbb{P}^1_S,\, g\colon Y \to X_S)$, where Y is a smooth proper geometrically connected curve over S, the map $f\colon Y \to \mathbb{P}^1_S$ is a finite flat finitely-presented morphism of degree d ramified only over $0, 1, \infty$ with ramification type λ, and g is an isomorphism of S-schemes. This defines a (possibly empty) finite étale Deligne-Mumford separated algebraic stack $\underline{\mathrm{Bel}}_{d,\lambda,X}$ over $\overline{\mathbb{Q}}$ which is usually referred to as a *Hurwitz stack*. Its coarse space, denoted by $\mathrm{Bel}_{d,\lambda,X}$, is usually referred to as a *Hurwitz space*. Since the set of $\overline{\mathbb{Q}}$-points $\mathrm{Bel}_{d,\lambda,X}(\overline{\mathbb{Q}})$ of its coarse space $\mathrm{Bel}_{d,\lambda,X}$ is naturally in bijection with $\mathrm{Bel}_{d,\lambda}(X)$, one could say that the following proposition says that there is an algorithm to compute a model for the Hurwitz space $\mathrm{Bel}_{d,\lambda,X}$.

PROPOSITION 3.7. *There exists an algorithm that, given as input a curve X over $\overline{\mathbb{Q}}$, an integer d, and a ramification type λ of d, computes a model for* $\mathrm{Bel}_{d,\lambda}(X)$.

PROOF. Let K be the field of definition of X (containing the coefficients of the input model). Applying the algorithm in Lemma 3.2 over $\overline{\mathbb{Q}}$ with ample line bundle $\mathscr{L} = \mathscr{O}_X(D_0)$ (and D_0 an effective divisor) in its proof, we compute $g_1, \dots, g_n \in K(X)$ such that if $f \in \overline{\mathbb{Q}}(X)$ is a degree d rational function on X, then there exist $a_1, \dots, a_n, b_1, \dots, b_n \in \overline{\mathbb{Q}}$ such that $a = \sum_{i=1}^n a_i g_i$ and $b = \sum_{i=1}^n b_i g_i$ satisfy $f = a/b$. We recall from (3.4) that $g_1, \dots, g_n$ are a K-basis for $H^0(X, \mathscr{L}^{\otimes t})$, where t satisfies (3.3). Let $d_0 = \deg D_0$.

We now give algebraic conditions on the coefficients a_i, b_j that characterize the subset $\mathrm{Bel}_{d,\lambda}(X)$. There is a rescaling redundancy in the ratio a/b so we work affinely as follows. We loop over pairs $0 \leqslant k, \ell \leqslant n$ and consider functions

$$f = \frac{a}{b} = \frac{a_1 g_1 + \cdots + a_{k-1} g_{k-1} + a_k g_k}{b_1 g_1 + \cdots + b_{\ell-1} g_{\ell-1} + g_\ell} \tag{3.8}$$

with $a_k \neq 0$. Every function $f = a/b$ arises for a unique such k, ℓ. Let m be minimal so that $g_k, g_\ell \in \mathrm{H}^0(X_{\overline{\mathbb{Q}}}, \mathscr{L}^{\otimes m}) \subseteq \mathrm{H}^0(X_{\overline{\mathbb{Q}}}, \mathscr{L}^{\otimes t})$.

For the ramification type $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ and $* \in \{0, 1, \infty\}$, let $\lambda_{*,1}, \dots, \lambda_{*,r_*}$ be the parts of λ (and r_* the number of parts), so

$$d = \lambda_{*,1} + \cdots + \lambda_{*,r_*}.$$

If $f\colon X \to \mathbb{P}^1$ is a Belyĭ map of degree d with ramification type λ, then the Riemann–Hurwitz formula is satisfied:

$$2g - 2 = -2d + \sum_{i=0}^{r_0} (\lambda_{0,i} - 1) + \sum_{i=0}^{r_1} (\lambda_{1,i} - 1) + \sum_{i=0}^{r_\infty} (\lambda_{\infty,i} - 1)\,. \tag{3.9}$$

If the Riemann–Hurwitz formula is not satisfied, there is no Belyĭ map of degree d with ramification type λ on X (indeed, on any curve of genus g), and the algorithm gives trivial output.

We claim that a rational function of the form (3.8) lies in $\mathrm{Bel}_{d,\lambda}(X)(\overline{\mathbb{Q}})$ if and only if there exists a partition $\mu = \mu_1 + \cdots + \mu_s$ of $md_0 - d$, and distinct points

$$P_1, \dots, P_{r_0},\, Q_1, \dots, Q_{r_1},\, R_1, \dots, R_{r_\infty} \in X(\overline{\mathbb{Q}})$$

and distinct points

$$Y_1, \dots, Y_s \in X(\overline{\mathbb{Q}})$$

(allowing these two sets of points to meet) such that

$$\begin{aligned} \operatorname{div}(a) &= \sum_{i=1}^{r_0} \lambda_{0,i}[P_i] + \sum_{i=1}^{s} \mu_i [Y_i] - mD_0 \\ \operatorname{div}(a-b) &= \sum_{i=1}^{r_1} \lambda_{1,i}[Q_i] + \sum_{i=1}^{s} \mu_i [Y_i] - mD_0 \\ \operatorname{div}(b) &= \sum_{i=1}^{r_\infty} \lambda_{\infty,i}[R_i] + \sum_{i=1}^{s} \mu_i [Y_i] - mD_0. \end{aligned} \tag{3.10}$$

We first prove the implication ($\Leftarrow$) of the claim. Suppose $f = a/b$ satisfies the equations (3.10). Then

$$\operatorname{div} f = \operatorname{div}(a) - \operatorname{div}(b) = \sum_{i=1}^{r_0} \lambda_{0,i}[P_i] - \sum_{i=1}^{r_\infty} \lambda_{\infty,i}[R_i]$$

so in particular $\deg f = d$. But then the map $f \colon X \to \mathbb{P}^1$ cannot be any further ramified by the Riemann–Hurwitz formula. Indeed, we have at least the ramification specified by the equations (3.10); let ρ be the degree of the remaining ramification locus. Then the Riemann–Hurwitz formula gives

$$2g - 2 = -2d + \sum_{i=0}^{r_0} (\lambda_{0,i} - 1) + \sum_{i=0}^{r_1} (\lambda_{1,i} - 1) + \sum_{i=0}^{r_\infty} (\lambda_{\infty,i} - 1) + \rho. \tag{3.11}$$

On the other hand, the equality (3.9) holds, so we must have $\rho = 0$.

We now prove the other implication ($\Rightarrow$) of the claim. Suppose $f \in \mathrm{Bel}_{d,\lambda}(X)(\overline{\mathbb{Q}})$ is of the form (3.8). Then

$$\operatorname{div}(f) = \operatorname{div}(a) - \operatorname{div}(b) = \sum_{i=1}^{r_0} \lambda_{0,i}[P_i] - \sum_{i=1}^{r_\infty} \lambda_{\infty,i}[R_i] \tag{3.12}$$

and

$$\operatorname{div}(f-1) = \operatorname{div}(a-b) - \operatorname{div}(b) = \sum_{i=1}^{r_1} \lambda_{1,i}[Q_i] - \sum_{i=1}^{r_\infty} \lambda_{\infty,i}[R_i] \tag{3.13}$$

for distinct points $P_i, Q_i, R_i \in X(\overline{\mathbb{Q}})$. Since $a \in \mathrm{H}^0(X, \mathscr{L}^{\otimes t})$, we have

$$\operatorname{div}(a) = \sum_{i=1}^{r_0} \lambda_{0,i}[P_i] + E - mD_0$$

for some effective divisor E (not necessarily disjoint from D_0) with $\deg E = md_0 - d$; from (3.12) we obtain

$$\operatorname{div}(b) = \sum_{i=1}^{r_\infty} \lambda_{\infty,i}[R_i] + E - mD_0.$$

Writing out $E = \sum_{i=1}^{s} \mu_i[Y_i]$ with Y_i distinct as an effective divisor and arguing similarly for $\operatorname{div}(a-b)$, we conclude that the equations (3.10) hold.

With the claim in hand, we finish by noting that the equations (3.10) can be written explicitly. To this end, we loop over the partitions μ and consider the configuration space of $r_0 + r_1 + r_\infty$ and s distinct points (but allowing the two sets to meet), which can be effectively computed by Lemma 3.1. Next, we write $D_0 = \sum_i \rho_i S_i$ and loop over the possible cases where one of the points P_i, Q_i, R_i, Y_i is equal to one of the points S_i or they are all distinct from S_i. In each case, cancelling terms when they coincide, we impose the vanishing conditions on $a, a-b, b$ with multiple order vanishing defined by higher derivatives, in the usual way. For each such function, we have imposed that the divisor of zeros is at least as large in degree as the function itself, so there can be no further zeros, and therefore the equations (3.10) hold for any solution to this large system of equations. $\square$

Given equations for the algebraic set $\mathrm{Bel}_{d,\lambda}(X)$, we now prove that there is an algorithm to check whether this set is empty or not.

Lemma 3.14. *There exists an algorithm that, given as input an affine variety X over $\overline{\mathbb{Q}}$, computes as output whether $X(\overline{\mathbb{Q}})$ is empty or not.*

Proof. Let I be an ideal defining the affine variety X (in some polynomial ring over $\overline{\mathbb{Q}}$). One can effectively compute a Gröbner basis for I [**9**, Chapter 15]. With a Gröbner basis at hand one can easily check whether 1 is in the ideal or not, and conclude by Hilbert's Nullstellensatz accordingly if $X(\overline{\mathbb{Q}})$ is empty or not. $\square$

Corollary 3.15. *There exists an algorithm that, given as input a set S with a model computes as output whether S is empty or not.*

Proof. Immediate from Lemma 3.14 and the definition of a model for a set S as being given by equations. $\square$

We are now ready to prove the main result of this note.

Proof of Theorem 1.2. Combine Proposition 3.7 and Corollary 3.15. $\square$

4. Second proof of Theorem 1.2

In this section, we sketch a second proof of Theorem 1.2. Instead of writing down equations for the Hurwitz space $\mathrm{Bel}_d(X)$, we enumerate all Belyǐ maps and effectively compute equations to check for isomorphism between curves. We saw this method already at work in Example 2.8.

Let X, Y be curves over $\overline{\mathbb{Q}}$. The functor $S \mapsto \mathrm{Isom}_S(X_S, Y_S)$ from the (opposite) category of schemes over $\overline{\mathbb{Q}}$ to the category of sets is representable [**8**, Theorem 1.11] by a finite étale $\overline{\mathbb{Q}}$-scheme $\underline{\mathrm{Isom}}(X, Y)$. Our next result shows that one can effectively compute a model for the (finite) set $\mathrm{Isom}(X, Y) = \underline{\mathrm{Isom}}(X, Y)(\overline{\mathbb{Q}})$ of isomorphisms from X to Y. Equivalently, one can effectively compute equations for the finite étale $\overline{\mathbb{Q}}$-scheme $\underline{\mathrm{Isom}}(X, Y)$.

Lemma 4.1. *There exists an algorithm that, gives as input curves X, Y over $\overline{\mathbb{Q}}$ with at least one of X or Y of genus at least 2, computes a model for the set $\mathrm{Isom}(X, Y)$.*

Proof. We first compute the genera of X, Y (as in the proof of Lemma 3.2): if these are not equal, then we correctly return the empty set. Otherwise, we compute a canonical divisor K_X on X by a Riemann–Roch calculation [**11**] and the image of the pluricanonical map $\varphi \colon X \hookrightarrow \mathbb{P}^N$ associated to the complete linear series on the very ample divisor $3K_X$ via Gröbner bases. We repeat this with Y. An isomorphism $\mathrm{Isom}(X, Y)$ induces via its action on canonical divisors an element of $\mathrm{PGL}_{N-1}(\overline{\mathbb{Q}})$ mapping the canonically embedded curve X to Y, and vice versa, and so a model is provided by the equations that insist that a linear change of variables in $\mathbb{P}^N$ maps the ideal of X into the ideal of Y, which can again be achieved by Gröbner bases. □

COROLLARY 4.2. *There exists an algorithm that, given as input maps of curves $f\colon X \to \mathbb{P}^1$ and $g\colon Y \to \mathbb{P}^1$ over $\overline{\mathbb{Q}}$, computes as output whether there exists an isomorphism $\alpha\colon X \xrightarrow{\sim} Y$ such that $g = \alpha \circ f$ or not.*

Similarly, there exists an algorithm that, given as input curves X, Y over $\overline{\mathbb{Q}}$, computes as output whether $X \simeq Y$ or not.

PROOF. We compute the genera of X, Y and again if these are different we correctly return as output *no*. Otherwise, let g be the common genus.

If $g = 0$, we parametrize X and Y to get $X \simeq Y \simeq \mathbb{P}^1$ and then ask for $\alpha \in \mathrm{PGL}_2(\overline{\mathbb{Q}})$ to map f to g in a manner analogous to the proof of Lemma 4.1.

If $g = 1$, we loop over the preimages of $0 \in \mathbb{P}^1$ in X and Y as origins, we compute Weierstrass equations via Riemann–Roch, and return *no* if the j-invariants of X, Y are unequal. Otherwise, these j-invariants are equal and we compute an isomorphism $X \simeq Y$ of Weierstrass equations. The remaining isomorphisms are twists, and we conclude by checking if there is a twist α of the common Weierstrass equation that maps f to g.

If $g \geqslant 2$, we call the algorithm in Lemma 4.1: we obtain a finite set of isomorphisms, and for each $\alpha \in \mathrm{Isom}(X, Y)$ we check if $g = \alpha \circ f$.

The second statement is proven similarly (ignoring the map). □

We now give a second proof of our main result.

SECOND PROOF OF THEOREM 1.2. We first loop over integers $d \geqslant 1$ and all ramification types λ of d. For each λ, we count the number of permutation triples up to simultaneous conjugation with ramification type λ.

We then compute the set of Belyĭ maps of degree d with ramification type λ over $\overline{\mathbb{Q}}$ as follows. There are countably many number fields K, and they may be enumerated by a minimal polynomial of a primitive element. For each number field K, there are countably many curves X over K up to isomorphism over $\overline{\mathbb{Q}}$, and this set is computable: for $g = 0$ we have only $\mathbb{P}^1_K$, for $g = 1$ we can enumerate j-invariants, and for $g \geqslant 2$ we can enumerate candidate pluricanonical ideals (by Petri's theorem). Finally, for each curve X over K, there are countably many maps $f\colon X \to \mathbb{P}^1$, and these can be enumerated using Lemma 3.2. Diagonalizing, we can enumerate the entire countable set of such maps. For each such map f, using Gröbner bases we can compute the degree and ramification type of f, and in particular detect if f is a Belyĭ map of degree d with ramification type λ. Along the way in this (ghastly) enumeration, we can detect if two correctly identified Belyĭ maps are isomorphic using 4.2. Having counted the number of isomorphism classes of such maps, we know when to stop with the complete set of such maps.

Now, to see whether $\mathrm{Bel}_{d,\lambda}(X)$ is nonempty, we just check using Corollary 4.2 whether X is isomorphic to one of the source curves in the set of all Belyĭ maps of degree d and ramification type λ. □

5. Examples

Here we show explicitly what the equations provided by Proposition (3.7) look like in some examples.

Example 5.1. The Belyĭ degree of $\mathbb{P}^1$ is 1, but it is still instructive to see what Proposition 3.7 and the equations (3.10) look like in this case. Let $X = \mathbb{P}^1$ with coordinate x, defined by $\operatorname{ord}_\infty x = -1$. We take $D_0 = (\infty)$. Then the basis of functions g_i is just $1, \dots, x^d$, and $f = a/b$ is a ratio of two polynomials of degree $\leqslant d$, at least one of which is degree exactly d. Having hit the degree on the nose, the "cancelling" divisor $E = \sum_{i=1}^s \mu_i[Y_i] = 0$ in the proof of Proposition 3.7 does not arise, and the equations for $a, b, a-b$ impose the required factorization properties of f. This method is sometimes called the *direct method* and has been frequently used (and adapted) in the computation of Belyĭ maps [**20**, §2] using Gröbner techniques.

Example 5.2. Consider the Fermat quartic $X\colon x^4+y^4 = z^4$ in $\mathbb{P}^2$: by Example 2.8, we know $\operatorname{Beldeg}(X) \leqslant 8$. In this example, we will show that X has no Belyĭ map of degree 7 with explicit equations to illustrate our method.

The curve X has genus 3 and so is already canonically embedded as a plane quartic, so $\omega_X = \mathscr{O}_X(1)$. We take $\mathscr{L} = \mathscr{O}_X(1) = \mathscr{O}_X(D_0)$ with D_0 the intersection of X with the line at infinity, and $d_0 = \deg D_0 = 3$. We write rational functions on X as ratios of polynomials in $\mathbb{Q}[x, y]$, writing x, y instead of $x/z, y/z$.

According to (3.3), we need $4m - 7 + 1 - 3 \geqslant 1$, so $m \geqslant 10/4$ and we may take $m = 3$. The space $\mathrm{H}^0(X, \mathscr{L}^{\otimes 3})$ has basis

$$1,\ x, y,\ x^2, xy, y^2,\ x^3, x^2y, xy^2, y^3.$$

We consider several affine cases, the first of which is

$$f = \frac{a}{b} = \frac{a_{00} + a_{10}x + a_{01}y + \cdots + a_{03}y^3}{b_{00} + \cdots + y^3}$$

and $a_{03} \neq 0$. Then $md_0 - d = 9 - 7 = 2$, so we consider the partitions of 2, and we exhibit the case of the partition $2 = 1 + 1$. As we already saw in Example 2.8, the only ramification type possible is $\lambda = (7, 7, 7)$. So we want distinct points $P, Q, R \in X(\overline{\mathbb{Q}})$ such that $\operatorname{div}(a) \geqslant 7[P]$ and $\operatorname{div}(a - b) \geqslant 7[Q]$ and $\operatorname{div}(b) \geqslant 7[R]$, and there are distinct points Y_1, Y_2 such that $a(Y_i) = b(Y_i) = 0$ for $i = 1, 2$.

References

[1] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I*, volume 267 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1985.

[2] Ingrid Bauer, Fabrizio Catanese, and Fritz Grunewald. Faithful actions of the absolute Galois group on connected components of moduli spaces. *Invent. Math.*, 199(3):859–888, 2015.

[3] Sybilla Beckmann. Ramified primes in the field of moduli of branched coverings of curves. *J. Algebra*, 125(1):236–255, 1989.

[4] G. V. Belyĭ. Galois extensions of a maximal cyclotomic field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(2):267–276, 479, 1979.

[5] G. V. Belyĭ. Another proof of the three-point theorem. *Mat. Sb.*, 193(3):21–24, 2002.

[6] José Bertin and Matthieu Romagny. Champs de Hurwitz. *Mém. Soc. Math. Fr. (N.S.)*, (125-126):219, 2011.

[7] Y. F. Bilu and M. Strambi. Quantitative Riemann existence theorem over a number field. *Acta Arith.*, 145(4):319–339, 2010.

[8] P. Deligne and D. Mumford. The irreducibility of the space of curves of given genus. *Inst. Hautes Études Sci. Publ. Math.*, (36):75–109, 1969.

[9] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[10] G. González-Diez and D. Torres-Teigell. Non-homeomorphic Galois conjugate Beauville structures on $\mathrm{PSL}(2, p)$. *Adv. Math.*, 229(6):3096–3122, 2012.

[11] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4):425–445, 2002.

[12] Ariyan Javanpeykar. Polynomial bounds for Arakelov invariants of Belyi curves. *Algebra Number Theory*, 8(1):89–140, 2014. With an appendix by Peter Bruin.

[13] Ariyan Javanpeykar and Rafael von Känel. Szpiro's small points conjecture for cyclic covers. *Doc. Math.*, 19:1085–1103, 2014.

[14] L.S. Khadjavi. An effective version of Belyi's theorem. *J. Number Theory*, 96(1):22–47, 2002.

[15] Michael Klug, Michael Musty, Sam Schiavone, and John Voight. Numerical calculation of three-point branched covers of the projective line. *LMS J. Comput. Math.*, 17(1):379–430, 2014.

[16] Shinichi Mochizuki. The geometry of the compactification of the Hurwitz scheme. *Publ. Res. Inst. Math. Sci.*, 31(3):355–441, 1995.

[17] Michael Musty, Sam Schiavone, and John Voight. Computing a database of Belyi maps. preprint.

[18] Matthieu Romagny and Stefan Wewers. Hurwitz spaces. In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Sémin. Congr.*, pages 313–341. Soc. Math. France, Paris, 2006.

[19] Leila Schneps, editor. *The Grothendieck theory of dessins d'enfants*, volume 200 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1994. Papers from the Conference on Dessins d'Enfant held in Luminy, April 19–24, 1993.

[20] J. Sijsling and J. Voight. On computing Belyi maps. In *Numéro consacré au trimestre "Méthodes arithmétiques et applications", automne 2013*, volume 2014/1 of *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 73–131. Presses Univ. Franche-Comté, Besançon, 2014.

[21] Bernd Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. SpringerWienNewYork, Vienna, second edition, 2008.

[22] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2009.

Mathematical Institute, Johannes-Gutenberg University, Mainz, Germany
E-mail address: peykar@uni-mainz.de

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA
E-mail address: jvoight@gmail.com