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 $X \to \mathbb{P}^1$. We discuss in detail the example of the Fermat curve of degree 4 and genus 3.

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 [27, Theorem 4.7.7]. This observation began a flurry of activity [24]: 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, 12]. Indeed, the applications of Belyĭ's theorem are vast.

In this paper, we consider Belyĭ maps from the point of view of algorithmic number theory. We define the Belyĭ degree of X, denoted by $\mathrm{Beldeg}(X) \in \mathbb{Z}_{\geqslant 1}$, 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, 14, 15, 25]. It was defined and studied first by Liţcanu [19], whose work suggested that the Belyĭ degree behaves like a height.

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* $\mathrm{Beldeg}(X)$.

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 $\mathbb{Q}$)

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

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

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 $\overline{\mathbb{Q}}$, computes as output an *upper bound* for $\mathrm{Beldeg}(X)$. Khadjavi [**16**] has given an explicit such upper bound—see Proposition 2.10 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 3.16. These equations can be computed in practice, but unfortunately in general it may not be practical to detect if they have a solution over $\overline{\mathbb{Q}}$. In section 4, we sketch a second proof, which is much less practical but still proves the main result. Finally, in section 5 we discuss in detail the example of the Fermat curve $x^4 + y^4 = z^4$ of genus 3.

The theory of Belyĭ maps in characteristic $p > 0$ is quite different, and our main results rely fundamentally on the structure of the fundamental group of $\mathbb{C} \setminus \{0, 1\}$, so we work over $\overline{\mathbb{Q}}$ throughout. However, certain intermediate results, including Lemma 4.1, hold over a general field.

Acknowledgements. This note grew out of questions asked to the authors by Yuri Bilu, Javier Fresán, David Holmes, and Jaap Top, and the authors are grateful for these comments. The authors also wish to thank Jacob Bond, Michael Musty, Sam Schiavone, and the anonymous referee for their feedback. Javanpeykar gratefully acknowledges support from SFB Transregio/45. Voight was supported by an NSF CAREER Award (DMS-1151047) and a Simons Collaboration Grant (550029).

2. The Belyi degree

In this section, we collect basic properties of the Belyĭ degree. Throughout, a curve X is a smooth projective connected 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 $\{0, 1, \infty\}$. Two Belyĭ maps $\phi\colon X \to \mathbb{P}^1$ and $\phi'\colon X' \to \mathbb{P}^1$ are isomorphic if

there exists an isomorphism $i\colon X \xrightarrow{\sim} X'$ such that $\phi' \circ i = \phi$. For $d \geqslant 1$, define $\mathrm{Bel}_d(X)$ to be the set of isomorphism classes of Belyĭ maps of degree d on X, and let $\mathrm{Bel}(X) := \bigcup_d \mathrm{Bel}_d(X)$.

Definition 2.1. The Belyĭ degree of X, denoted $\mathrm{Beldeg}(X) \in \mathbb{Z}_{\geqslant 1}$, 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 $\mathrm{Bel}_d(X)$ is non-empty.

Lemma 2.2. *Let $C \in \mathbb{R}_{\geqslant 1}$. Then the set of isomorphism classes of curves X with $\mathrm{Beldeg}(X) \leqslant C$ is finite.*

For an upper bound on the number of isomorphism classes of curves X with $\mathrm{Beldeg}(X) \leqslant C$ we refer to Lițcanu [19, Théorème 2.1].

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. □

Remark 2.3. One may also restrict to X over a number field $K \subseteq \overline{\mathbb{Q}}$ and ask for the minimal degree of a Belyĭ map defined over K: see Zapponi [29] for a discussion of this notion of relative Belyĭ degree.

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

Example 2.4. 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, as we show now.

Proposition 2.5. *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 $d \geqslant 2g + 1$. □

As an application of Proposition 2.5, we now show that gonal maps on curves of positive genus are not Belyĭ maps.

Corollary 2.6. *Let X be a curve of gonality γ. A finite map $\phi\colon X \to \mathbb{P}^1$ with $\deg \phi = \gamma$ 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 2.5. □

EXAMPLE 2.7. 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 2.5 is sharp for every genus g.

REMARK 2.8. The bound in Proposition 2.5 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 the equation $y^2 = x(x-1)(x-p)$ 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 $\mathrm{Beldeg}(X) \geqslant p$ (see also Zapponi [29, Theorem 1.3]): 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 at p (in fact, obtained over an extension of $\mathbb{Q}$ unramified at p), a contradiction.

EXAMPLE 2.9. For every $n \geqslant 1$, the Belyĭ degree of the Fermat curve

$$X_n\colon x^n + y^n = z^n \subset \mathbb{P}^2$$

is bounded above by $\mathrm{Beldeg}(X_n) \leqslant n^2$, because there is a Belyĭ map

$$X_n \to \mathbb{P}^1$$
$$(x : y : z) \mapsto (x^n : z^n)$$

of degree n^2. On the other hand, we have $\mathrm{Beldeg}(X_n) \geqslant (n-1)(n-2) + 1 = n^2 - 3n + 3$ by Proposition 2.5.

For $n = 1, 2$, we have $X_n \simeq \mathbb{P}^1$ so $\mathrm{Beldeg}(X_1) = \mathrm{Beldeg}(X_2) = 1$. As observed by Zapponi [29, Example 1.2], for $n = 3$, the curve X_3 is a genus 1 curve with j-invariant 0, so isomorphic to $y^2 - y = x^3$, and $\mathrm{Beldeg}(X_3) = 3$ by Example 2.7.

We consider the case $n = 4$ in section 5, and show that $\mathrm{Beldeg}(X_4) = 8$ in Proposition 5.1.

We finish this section with an effective version of Belyĭ's theorem, due to Khadjavi [16]. (An effective version was also proven independently by Lițcanu [19, Théorème 4.3], with a weaker bound.) 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 $H(a) := (\prod_v \max(1, \|\alpha\|_v))^{1/[K:\mathbb{Q}]}$, where the product runs over the set of absolute values indexed by the places v of K normalized so that the product formula holds [16, 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 2.10 (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 [16, Theorem 1.1.c]. □

COROLLARY 2.11. *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 2.10 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 $I \subseteq \overline{\mathbb{Q}}[x_1, \dots, x_N]$ such that the zero locus of I is the variety obtained by removing all the diagonals from X^t/S_t.*

PROOF. Let $X = \operatorname{Spec} \overline{\mathbb{Q}}[x_1, \dots, x_n]/I$. By (classical) invariant theory (see Sturmfels [26]), there is an algorithm to compute the coordinate ring of invariants $\left(\overline{\mathbb{Q}}[x_1, \dots, x_n]/I\right)^{S_t}$. In other words, there is an algorithm which computes

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

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

REMARK 3.2. We will use Lemma 3.1 below to parametrize extra ramification points, write equations in terms of these parameters, and check whether the system of equations has a solution over $\overline{\mathbb{Q}}$. For this purpose, we need not take the quotient by the symmetric group S_t, as the system of equations with unordered parameters has a solution over $\overline{\mathbb{Q}}$ if and only if the one with ordered parameters does.

Next, we show how to represent rational functions on X explicitly in terms of a Riemann–Roch basis.

LEMMA 3.3. *Let X be a curve over K of genus g, let $\mathscr{L}$ be an ample sheaf on X, and let d be a positive integer. Let*

$$t := \left\lceil \frac{d+g}{\deg \mathscr{L}} \right\rceil. \tag{3.4}$$

Then, for all $f \in \overline{\mathbb{Q}}(X)$ of degree d, there exist $a, b \in \mathrm{H}^0(X_{\overline{\mathbb{Q}}}, \mathscr{L}^{\otimes t})$ with $b \neq 0$ such that $f = a/b$.

PROOF. By definition, we have

$$t \deg \mathscr{L} - d + 1 - g \geqslant 1. \tag{3.5}$$

Let $\operatorname{div}_\infty f \geqslant 0$ be the divisor of poles of f. By Riemann–Roch,

$$\dim_{\overline{\mathbb{Q}}} \mathrm{H}^0(X_{\overline{\mathbb{Q}}}, \mathscr{L}^{\otimes t}(-\operatorname{div}_\infty f)) \geqslant t \deg \mathscr{L} - d + 1 - g \geqslant 1. \tag{3.6}$$

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. Then $fb \in \mathrm{H}^0(X_{\overline{\mathbb{Q}}}, \mathscr{L}^{\otimes t})$. (In effect, we have "cancelled the poles" of f by the zeros of b, at the expense of possibly introducing new poles

supported within $\mathscr{L}$.) Letting $fb = a \in \mathrm{H}^0(X, \mathscr{L}^{\otimes t})$ we have written $f = a/b$ as claimed. □

The quantities in Lemma 3.3 can be effectively computed, as follows. Recall that a curve X over K is specified in bits by a set of defining equations in projective space with coefficients in K. (Starting with any birational model for X, we can effectively compute a smooth projective model.)

LEMMA 3.7. *Let $X \subset \mathbb{P}^n_K$ be a curve over K. Then the following quantities are effectively computable:*

(i) *The genus $g = g(X)$;*
(ii) *An effective divisor D on X over K and its degree.*
(iii) *Given a divisor D over K, a basis for the K-vector space $\mathrm{H}^0(X, \mathscr{O}_X(D))$.*

PROOF. For (a), to compute the genus 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. For (b), intersecting X with a hyperplane, we obtain an effective divisor D on X over K, and its degree is the leading term of the Hilbert polynomial computed in (a). For (c), it suffices to note that Riemann–Roch calculations can be done effectively: see e.g. Coates [9] or Hess [13]. □

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 $\mathrm{Bel}_{d,\lambda}(X) \subseteq \mathrm{Bel}_d(X)$ be the subset of Belyĭ maps of degree d on X with ramification type λ. For the ramification type λ and $* \in \{0, 1, \infty\}$, let $\lambda_{*,1}, \ldots, \lambda_{*,r_*}$ be the parts of λ (and r_* the number of parts), so

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

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

$$\begin{aligned} 2g - 2 &= -2d + \sum_{i=1}^{r_0} (\lambda_{0,i} - 1) + \sum_{i=1}^{r_1} (\lambda_{1,i} - 1) + \sum_{i=1}^{r_\infty} (\lambda_{\infty,i} - 1) \\ &= d - r_0 - r_1 - r_\infty. \end{aligned} \tag{3.8}$$

To prove our main theorem, we will show that one can compute equations whose vanishing locus over $\overline{\mathbb{Q}}$ is precisely the set $\mathrm{Bel}_{d,\lambda}(X)$ (see Proposition 3.16): we call such equations a model for $\mathrm{Bel}_{d,\lambda}(X)$.

On our way to prove Proposition 3.16, we first characterize Belyĭ maps of degree d with ramification type λ among rational functions on a curve written in terms of a Riemann–Roch basis. This characterization is technical but we will soon see that it is quite suitable for our algorithmic application.

PROPOSITION 3.9. *Let $d \geqslant 1$ be an integer and let $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ be a ramification type for d with r_0, r_1, r_∞ parts, respectively. Let X be a curve over a number field K. Let g be the genus of X, and suppose that*

$$2g - 2 = d - r_0 - r_1 - r_\infty. \tag{3.10}$$

Let D_0 be an effective divisor of degree d_0, and let $\mathscr{L} = \mathscr{O}_X(D_0)$. Let $t \geqslant 1$ be the smallest positive integer such that $t \deg \mathscr{L} - d + 1 - g \geqslant 1$. Let $g_1, \ldots, g_n \in K(X)$

be a basis for the K-vector space $\mathrm{H}^0(X, \mathscr{L}^{\otimes t})$. Let $0 \leqslant k, l \leqslant n$ be integers. Let m be minimal so that $g_k, g_l \in \mathrm{H}^0(X_{\overline{\mathbb{Q}}}, \mathscr{L}^{\otimes m}) \subseteq \mathrm{H}^0(X_{\overline{\mathbb{Q}}}, \mathscr{L}^{\otimes t})$. Let

$$\phi := \frac{a}{b} = \frac{a_1 g_1 + \ldots + a_k g_k}{b_1 g_1 + \ldots + b_l g_l}$$

be a nonconstant rational function with $a_1, \ldots, b_l \in \overline{\mathbb{Q}}$.

Then the rational function ϕ 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 $md_0 - d$, distinct points

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

and distinct points

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

allowing these two sets of points to meet, such that

$$\begin{aligned} \operatorname{div}(a) &= \sum_{i=1}^{r_0} \lambda_{0,i}[P_i] + \sum_{i=1}^{s} \mu_i[Y_i] - mD_0 \\ \operatorname{div}(a-b) &= \sum_{i=1}^{r_1} \lambda_{1,i}[Q_i] + \sum_{i=1}^{s} \mu_i[Y_i] - mD_0 \\ \operatorname{div}(b) &= \sum_{i=1}^{r_\infty} \lambda_{\infty,i}[R_i] + \sum_{i=1}^{s} \mu_i[Y_i] - mD_0. \end{aligned} \tag{3.11}$$

Proof. We first prove the implication ($\Leftarrow$) of the proposition. Suppose ϕ satisfies the equations (3.11). Then

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

since the set of points $\{P_1, \ldots, P_{r_0}\}$ is disjoint from $\{R_1, \ldots, R_{r_\infty}\}$, we have $\deg \phi = d$. We see some ramification in $\phi\colon X \to \mathbb{P}^1$ above the points $0, 1, \infty$ according to the ramification type λ, specified by the equations (3.11); let ρ be the degree of the remaining ramification locus. We claim there can be no further ramification. Indeed, the Riemann–Hurwitz formula gives

$$\begin{aligned} 2g - 2 &= -2d + \sum_{i=0}^{r_0} (\lambda_{0,i} - 1) + \sum_{i=0}^{r_1} (\lambda_{1,i} - 1) + \sum_{i=0}^{r_\infty} (\lambda_{\infty,i} - 1) + \rho \\ &= d - r_0 - r_1 - r_\infty + \rho. \end{aligned} \tag{3.12}$$

On the other hand, we are given the equality 3.10, so $\rho = 0$. Therefore $\phi \in \mathrm{Bel}_{d,\lambda}(\overline{\mathbb{Q}})$.

We now prove the other implication ($\Rightarrow$). Suppose $\phi \in \mathrm{Bel}_{d,\lambda}(\overline{\mathbb{Q}})$. We have

$$\operatorname{div}(\phi) = \operatorname{div}(a) - \operatorname{div}(b) = \sum_{i=1}^{r_0} \lambda_{0,i}[P_i] - \sum_{i=1}^{r_\infty} \lambda_{\infty,i}[R_i] \tag{3.13}$$

and

$$\operatorname{div}(\phi - 1) = \operatorname{div}(a - b) - \operatorname{div}(b) = \sum_{i=1}^{r_1} \lambda_{1,i}[Q_i] - \sum_{i=1}^{r_\infty} \lambda_{\infty,i}[R_i] \tag{3.14}$$

for distinct points $P_1, \dots, P_{r_0}, Q_1, \dots, Q_{r_1}, R_1, \dots, R_{r_\infty} \in X(\overline{\mathbb{Q}})$. Moreover, 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 (3.13) 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 (3.11) hold. □

Remark 3.15. $\mathrm{Bel}_{d,\lambda}(X)$ is a (non-positive dimensional) Hurwitz space: see for instance Bertin–Romagny [**6**, Section 6.6] (but also Mochizuki [**20**] and Romagny–Wewers [**23**]). Indeed, for a scheme S over $\overline{\mathbb{Q}}$, let $\underline{\mathrm{Bel}}_{d,\lambda,X}(S)$ be the groupoid whose objects are tuples $(\phi\colon Y \to \mathbb{P}^1_S,\ g\colon Y \to X_S)$, where Y is a smooth proper geometrically connected curve over S, the map $\phi\colon Y \to \mathbb{P}^1_S$ 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) separated finite type Deligne–Mumford 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 $\mathrm{Bel}_{d,\lambda,X}$.

We now prove the following key ingredient to our main result.

Proposition 3.16. *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 a field of definition of X (containing the coefficients of the input model). Applying the algorithm in Lemma 3.7 to X over K, we compute the genus g of X.

Recall the Riemann–Hurwitz formula (3.8) for a Belyĭ map. If the Riemann–Hurwitz formula is not satisfied for d and the ramification type λ, 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. So we may suppose that (3.8) holds.

Next, we compute an effective divisor D_0 on X with $\mathscr{L} := \mathscr{O}_X(D_0)$ and its degree $d_0 := \deg D_0$. Let

$$t := \left\lceil \frac{d+g}{\deg \mathscr{L}} \right\rceil$$

as in (3.4). By Lemma 3.7, we may compute a K-basis $g_1, \dots, g_n$ of $\mathrm{H}^0(X, \mathscr{L}^{\otimes t})$. Then by Lemma 3.3, if $\phi \in \overline{\mathbb{Q}}(X)$ 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 $\phi = a/b$.

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

$$\phi = \frac{a}{b} = \frac{a_1 g_1 + \cdots + a_{k-1} g_{k-1} + a_k g_k}{b_1 g_1 + \cdots + b_{\ell-1} g_{\ell-1} + g_\ell} \tag{3.17}$$

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

Note that Proposition 3.9 characterizes precisely when a rational function of the form (3.17) lies in $\mathrm{Bel}_{d,\lambda}(X)(\overline{\mathbb{Q}})$. Thus, by Proposition 3.9, we may finish by noting that the equations (3.11) 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 $D_0 = \sum_i \rho_i [D_{0i}]$ 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 D_{0i} or they are all distinct from D_{0i}. 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 (3.11) hold for any solution to this large system of equations. □

Example 3.18. We specialize Proposition 3.16 to the case $X = \mathbb{P}^1$. (The Belyĭ degree of $\mathbb{P}^1$ is 1, but it is still instructive to see what the equations (3.11) look like in this case.) Let $X = \mathbb{P}^1$ with coordinate x, defined by $\mathrm{ord}_\infty x = -1$. We take $D_0 = (\infty)$. Then the basis of functions g_i is just $1, \ldots, x^d$, 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 3.16 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 using Gröbner techniques [**25**, §2].

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 3.19. *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 [**11**, 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. □

Corollary 3.20. *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 3.19 and the definition of a model for a set S as being given by equations. □

We are now ready to give the first proof of the main result of this note.

First proof of Theorem 1.2. Let X be a curve over $\overline{\mathbb{Q}}$. Let $d \geqslant 1$ be an integer, and let λ be a ramification type of d. To prove the theorem, it suffices to show that there is an algorithm which computes whether the set $\mathrm{Bel}_{d,\lambda}(X)$ of Belyĭ

maps of degree d with ramification type λ is empty. We explain how to use the above results to do this.

By Proposition 3.16, we may (and do) compute a model for the set $\mathrm{Bel}_{d,\lambda}(X)$. By Corollary 3.20, we can check algorithmically whether this set is empty or not (by using the model we computed). This means that we can algorithmically check whether X has a Belyĭ map of degree d with ramification type λ. □

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 Belyĭ maps and effectively compute equations to check for isomorphism between curves. We saw this method already at work in Example 2.9.

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 [**10**, 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, given 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 3.3): 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 [**13**] 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 $h\colon Y \to \mathbb{P}^1$ 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.

As remarked by Ngo–Nguyen–van der Put–Top [**22**, Appendix], the existence of an algorithm which decides whether two curves are isomorphic over an algebraically closed field is well-known. We include the following proof for the sake of completeness.

Proof of Corollary 4.2. 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 $h = \alpha \circ f$.

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 3.3. 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 Corollary 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. The Fermat curve of degree four

In this section we prove the following proposition, promised in Example 2.9.

Proposition 5.1. *The Belyĭ degree of the curve* $X\colon x^4 + y^4 = z^4$ *is equal to* 8.

Proof. The curve X is a canonically embedded curve of genus 3. By Proposition 2.5, we have $\mathrm{Beldeg}(X) \geqslant 7$. 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 $\mathrm{Beldeg}(X) \leqslant 8$. So to show $\mathrm{Beldeg}(X) = 8$, it suffices to rule out the existence of a Belyĭ map of degree 7.

By enumeration of partitions and the Riemann–Hurwitz formula, we see that 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 $(7, 7, 7)$. By enumeration of permutation triples up to simultaneous

conjugation, we compute 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. We rule these out by consideration of automorphism groups.

As in Lemma 4.1 but instead using the canonical embedding as K_X is already ample, we have $\mathrm{Aut}(X) \leqslant \mathrm{Aut}(\mathbb{P}^2) = \mathrm{PGL}_3(\overline{\mathbb{Q}})$, and a direct calculation yields that $\mathrm{Aut}(X) \simeq S_3 \rtimes (\mathbb{Z}/4\mathbb{Z})^2$ and $\#\,\mathrm{Aut}(X) = 96$. (For the automorphism group of the general Fermat curve X_n of degree $n \geqslant 4$, see Leopoldt [18] or Tzermias [28]: they prove that $\mathrm{Aut}(X_n) \simeq S_3 \rtimes (\mathbb{Z}/n\mathbb{Z})^2$.)

The cyclic case is a geometrically Galois map, but X does not have an automorphism of order 7, impossible. For the two noncyclic cases, computing the centralizers of the $2 + 23 = 25$ permutation triples up to simultaneous conjugation, we conclude that these Belyĭ maps have no automorphisms. An automorphism $\alpha \in \mathrm{Aut}(X)$ 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 too many. □

Remark 5.2. The above self-contained proof works because of the large automorphism group on the Fermat curve, and it seems difficult to make this strategy work for an arbitrary curve.

To illustrate how our algorithms work, we now show how they can be used to give two further proofs of Proposition 5.1.

Example 5.3. We begin with the first algorithm exhibited in Proposition 3.16. We show that X has no Belyĭ map of degree 7 with explicit equations to illustrate our method; we finish the proof as above.

We take the divisor $D_0 = [D_{01}]$ where $D_{01} = (1:0:1) \in X(\mathbb{Q})$ and $\deg D_0 = d_0 = 1$. 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 (3.5), taking $\mathscr{L} = \mathscr{O}_X(D_0)$ we need $t - 7 + 1 - 3 \geqslant 1$, so we take $t = 10$. By a computation in Magma [8], the space $\mathrm{H}^0(X, \mathscr{L}^{\otimes 10})$ has dimension $n = 8$ and basis

$$
\begin{aligned}
g_1 &= 1 \\
g_2 &= \frac{x^3 + x^2 + x + 1}{y^3} \\
g_3 &= g_2/y \\
g_4 &= \frac{4(x^3 + x^2 + x + 1) - x^2y^4 - 2xy^4 - 3y^4}{4y^6} \\
g_5 &= g_5/y \\
g_6 &= g_6/y \\
g_7 &= \frac{16(x^3 + x^2 + x + 1) - 6x^3y^4 - 10x^2y^4 + xy^8 - 14xy^4 + 3y^8 - 18y^4}{6y^9} \\
g_8 &= \frac{32(x^3 + x^2 + x + 1) - 3x^2y^8 - 8x^2y^4 - 4xy^8 - 16xy^4 - 3y^8 - 24y^4}{32y^{10}}
\end{aligned}
\tag{5.4}
$$

We compute that $\mathrm{ord}_{D_0} g_i = 0, -3, -4, -6, -7, -8, -9, -10$.

The general case is where $a_8 b_8 \neq 0$, for which $k = \ell = 8$ and we may take

$$\phi = \frac{a}{b} = \frac{\sum_{i=1}^{8} a_i g_i}{\sum_{i=1}^{8} b_i g_i}$$

so we let $b_8 = 1$ and $m = t = 10$. As we already saw in Example 2.9, the only ramification type possible is $\lambda = (7,7,7)$, with $r_0 = r_1 = r_\infty = 1$ and $\lambda_0 = \lambda_1 = \lambda_\infty = 7$.

We have $md_0 - d = 10 - 7 = 3$, so we consider the partitions of 3. We start with the trivial partition $\mu = \mu_1 = 3$ with $s = 1$. Then the equations (3.11) read, dropping subscripts: we want distinct points $P, Q, R \in X(\overline{\mathbb{Q}})$ such that $\operatorname{div}(a) \geqslant 7[P] + 3[Y]$ and $\operatorname{div}(a-b) \geqslant 7[Q] + 3[Y]$ and $\operatorname{div}(b) \geqslant 7[R] + 3[Y]$.

Continuing in the general case, the points P, Q, R, Y, D_0 are all distinct, each such point belongs to the affine open with $z \neq 0$, and furthermore $x - x(Z)$ is a uniformizer at Z for each point $Z = P, \ldots, D_0$.

The conditions for the point P we write as follows: letting $P = (x_P : y_P : 1)$ with unknowns x_P, y_P, we add the equation $x_P^4 + y_P^4 = 1$ so that P lies on the curve X, and then (by Taylor expansion) to ensure $\operatorname{ord}_P a \geqslant 7$ we add the equations

$$\frac{\partial^j a}{\partial x^j}(x_P, y_P) = \sum_{i=1}^{8} a_i \frac{\partial^j g_i}{\partial x^j}(x_P, y_P) = 0 \tag{5.5}$$

for $j = 0, \ldots, 6$, and using implicit differentiation on the defining equation of X to obtain $\dfrac{\mathrm{d}y}{\mathrm{d}x} = -\dfrac{x^3}{y^3}$. For example, the case $j = 1$ (asserting that a vanishes to order at least 2 at P, assuming that $a(P) = 0$) is

$$\begin{aligned}
&(3x_P^6y_P^7 + 3x_P^5y_P^7 + 3x_P^4y_P^7 + 3x_P^3y_P^7 + 3x_P^2y_P^{13} + 2x_Py_P^{13} + y_P^{13})a_2 \\
&+ (4x_P^6y_P^6 + 4x_P^5y_P^6 + 4x_P^4y_P^6 + 4x_P^3y_P^6 + 3x_P^2y_P^{12} + 2x_Py_P^{12} + y_P^{12})a_3 \\
&+ (6x_P^6y_P^4 - \tfrac{11}{2}x_P^5y_P^8 + 6x_P^5y_P^4 - 7x_P^4y_P^8 + 6x_P^4y_P^4 \\
&\qquad - \tfrac{17}{2}x_P^3y_P^8 + 6x_P^3y_P^4 + 3x_P^2y_P^{10} + 4x_Py_P^{10} + 2y_P^{10})a_4 \\
&+ (7x_P^6y_P^3 - \tfrac{23}{4}x_P^5y_P^7 + 7x_P^5y_P^3 - \tfrac{15}{2}x_P^4y_P^7 + 7x_P^4y_P^3 \\
&\qquad - \tfrac{37}{4}x_P^3y_P^7 + 7x_P^3y_P^3 + 3x_P^2y_P^9 + 4x_Py_P^9 + 2y_P^9)a_5 \\
&+ (8x_P^6y_P^2 - 6x_P^5y_P^6 + 8x_P^5y_P^2 - 8x_P^4y_P^6 + 8x_P^4y_P^2 \\
&\qquad - 10x_P^3y_P^6 + 8x_P^3y_P^2 + 3x_P^2y_P^8 + 4x_Py_P^8 + 2y_P^8)a_6 \\
&+ (5x_P^6y_P^5 - 24x_P^6y_P + 11x_P^5y_P^5 - 24x_P^5y_P - \tfrac{19}{2}x_P^4y_P^9 + 17x_P^4y_P^5 - 24x_P^4y_P \\
&\qquad - \tfrac{25}{2}x_P^3y_P^9 + 23x_P^3y_P^5 - 24x_P^3y_P + 6x_P^2y_P^7 + 4x_Py_P^7 + 3y_P^7)a_7 \\
&+ (10x_P^6 - \tfrac{143}{16}x_P^5y_P^8 - \tfrac{13}{2}x_P^5y_P^4 + 10x_P^5 - \tfrac{37}{4}x_P^4y_P^8 - 9x_P^4y_P^4 + 10x_P^4 \\
&\qquad - \tfrac{143}{16}x_P^3y_P^8 - \tfrac{23}{2}x_P^3y_P^4 + 10x_P^3 + 3x_P^2y_P^6 + 6x_Py_P^6 + 3y_P^6)a_8 \\
&= 0.
\end{aligned} \tag{5.6}$$

The equations for the points Q, R are the same, with $a - b$ and b in place of a, and again for Y but with a *and* b in place of a. We must also impose the conditions that the points are distinct and that $a_8 \neq 0$: for example, to say $P \neq Q$ we introduce the variable z_{PQ} and the equation

$$((x_P - x_Q)z_{PQ} - 1)((y_P - y_Q)z_{PQ} - 1) = 0. \tag{5.7}$$

In this general case, we end up with $8+7+2\cdot 4+10=33$ variables

$$a_1,\dots,a_8,b_1,\dots,b_7,x_{P_1},y_{P_1},x_{Q_1},y_{Q_1},x_{R_1},y_{R_1},x_{Y_1},y_{Y_1},z_{PQ},\dots,z_{RD_0} \tag{5.8}$$

and $8\cdot 3+7+10=41$ equations.

Moving on from the general case, we consider also the case where x does not yield a uniformizer for one of the points; that one of the points lies along the line $z=0$; or that some of the points coincide. After this, we have completed the case $k=\ell=8$, and consider more degenerate cases (k,ℓ).

Finally, we repeat the entire process again with the partitions $\mu=2+1$ and $\mu=1+1+1$.

We conclude by a version of the second proof of our main result, explained in section 4.

EXAMPLE 5.9. We compute each Belyĭ map of degree 7 and genus 3 and show that no source curve is isomorphic to X.

As above, there are three cases to consider. The first cyclic case is the map in Example 2.7 above, followed by its post-composition by automorphisms of $\mathbb{P}^1$ permuting $\{0,1,\infty\}$. But the curve $y^2-y=x^7$ has an automorphism of order 7, and X does not.

The genus 3 Belyĭ maps of degree 7 in the noncyclic case with 2 permutation triples up to conjugation was computed by Klug–Musty–Schiavone–Voight [**17**, Example 5.27]: using the algorithm in Lemma 4.1 we find that X is not isomorphic to either source curve. Alternatively, these two curves are minimally defined over $\mathbb{Q}(\sqrt{-7})$ (and are conjugate under $\mathrm{Gal}(\mathbb{Q}(\sqrt{-7})\,|\,\mathbb{Q})$), whereas X can be defined over $\mathbb{Q}$.

In the third case, we apply the same argument, appealing to the exhaustive computation of Belyĭ maps of small degree by Musty–Schiavone–Voight [**21**] and again checking for isomorphism.

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] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[9] J. Coates. Construction of rational functions on a curve. *Proc. Cambridge Philos. Soc.*, 68:105–123, 1970.

[10] 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.

[11] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.
[12] 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.
[13] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4):425–445, 2002.
[14] Ariyan Javanpeykar. Polynomial bounds for Arakelov invariants of Belyi curves. *Algebra Number Theory*, 8(1):89–140, 2014. With an appendix by Peter Bruin.
[15] Ariyan Javanpeykar and Rafael von Känel. Szpiro's small points conjecture for cyclic covers. *Doc. Math.*, 19:1085–1103, 2014.
[16] L.S. Khadjavi. An effective version of Belyi's theorem. *J. Number Theory*, 96(1):22–47, 2002.
[17] 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.
[18] Heinrich-Wolfgang Leopoldt. über die Automorphismengruppe des Fermatkörpers. *J. Number Theory*, 56(2):256–282, 1996.
[19] R. Liţcanu. Propriétés du degré des morphismes de Belyi. *Monatsh. Math.*, 142(4):327–340, 2004.
[20] Shinichi Mochizuki. The geometry of the compactification of the Hurwitz scheme. *Publ. Res. Inst. Math. Sci.*, 31(3):355–441, 1995.
[21] Michael Musty, Sam Schiavone, and John Voight. Computing a database of Belyi maps. preprint.
[22] L. X. Chau Ngo, K. A. Nguyen, M. van der Put, and J. Top. Equivalence of differential equations of order one. *J. Symbolic Comput.*, 71:47–59, 2015.
[23] 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.
[24] 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.
[25] 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.
[26] Bernd Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. Springer, second edition, 2008.
[27] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2009.
[28] Pavlos Tzermias. The group of automorphisms of the Fermat curve. *J. Number Theory*, 53(1):173–178, 1995.
[29] Leonardo Zapponi. On the Belyi degree(s) of a curve defined over a number field. `arXiv:0904.0967`, 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`