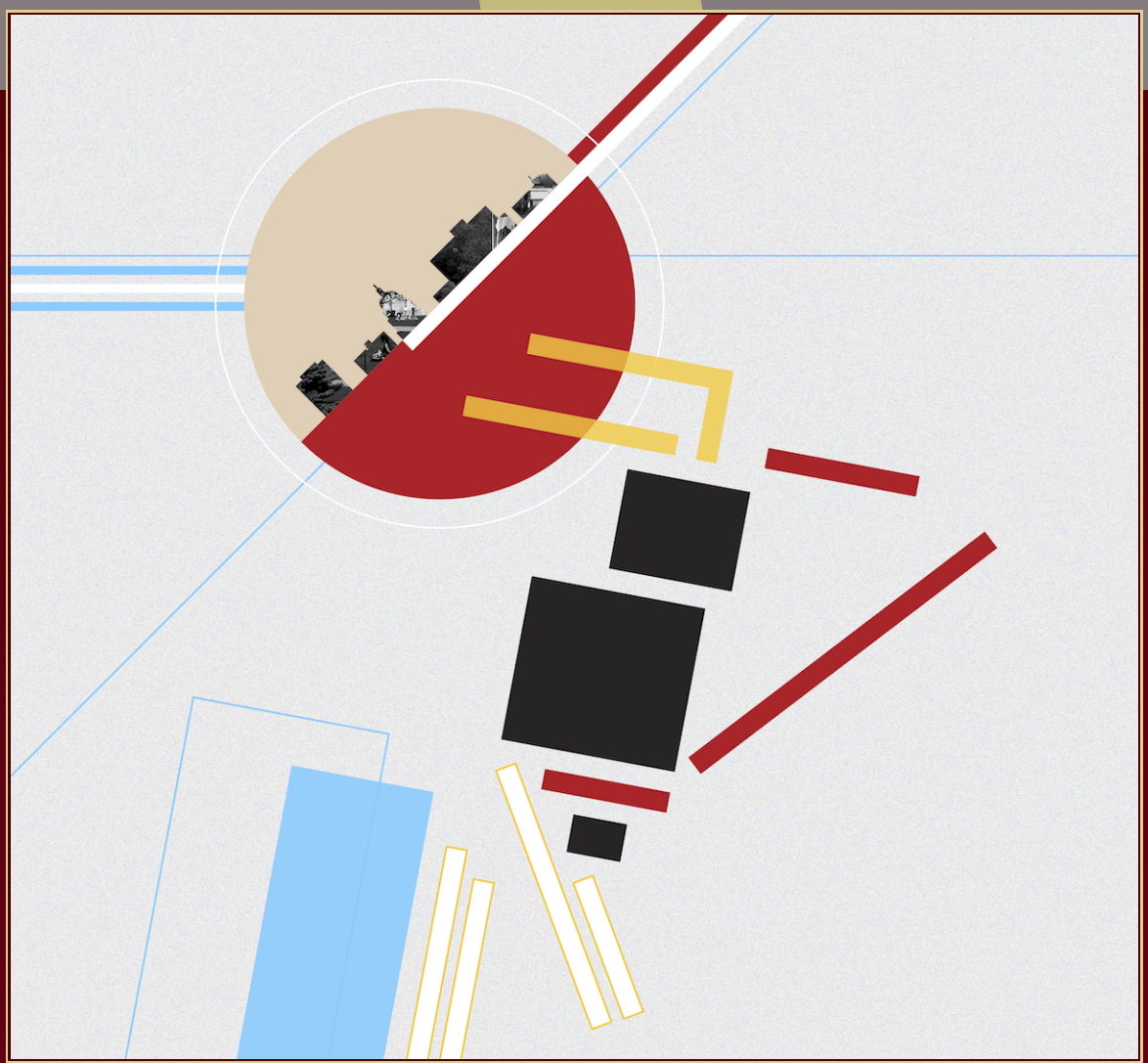
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

A database of Belyi maps

Michael Musty, Sam Schiavone, Jeroen Sijsling, and John Voight



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.375

msp

A database of Belyi maps

Michael Musty, Sam Schiavone, Jeroen Sijsling, and John Voight

We use a numerical method to compute a database of three-point branched covers of the complex projective line of small degree. We report on some interesting features of this data set, including issues of descent.

1. Introduction

1.1. ***Motivation.*** Let X be a smooth, projective curve over $\mathbb{C}$. A *Belyi map* on X is a nonconstant map $\phi : X \to \mathbb{P}^1$ that is unramified away from $\{0, 1, \infty\}$. By a theorem of Belyi [2] and Weil's descent theory [17], X can be defined over the algebraic closure $\mathbb{Q}^{\mathrm{al}}$ of $\mathbb{Q}$ if and only if X admits a Belyi map. This remarkable observation has led to a spurt of activity, with many deep questions still open after forty years. In his study of covers of the projective line minus three points [8], Deligne writes pessimistically:

> A. Grothendieck and his students developed a combinatorial description ("maps") of finite coverings... It has not aided in understanding the Galois action. We have only a few examples of nonsolvable coverings whose Galois conjugates have been computed.

Indeed, although significant mathematical effort has been expended in computing Belyi maps [15], there have been few systematic computations undertaken.

1.2. ***Main result.*** In this article we seek to remedy this state of affairs. We address Deligne's second objection by describing the uniform computation of a large catalog of Belyi maps of small degree. We utilize the numerical method of Klug–Musty–Schiavone–Voight [11] and follow the combinatorial description of Grothendieck. We make some preliminary observations about our data, but leave to future work a more detailed analysis of the Galois action on the maps in our catalog.

A *passport* is the data (g, G, λ) consisting of a nonnegative integer $g \in \mathbb{Z}_{\geq 0}$, a transitive permutation group $G \leq S_d$, and three partitions $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ of d. The *passport* of a Belyi map is given by its genus, its monodromy group, and the ramification degrees of the points above $0, 1, \infty$. There is a natural

MSC2010: primary 11G32; secondary 11G30, 14H57.
Keywords: dessins d'enfants, Belyi maps, triangle groups, hyperelliptic curves.

$d\downarrow \quad g\rightarrow$	0	1	2	3	≥ 4	total
1	1/1	0	0	0	0	1/1
2	1/1	0	0	0	0	1/1
3	2/2	1/1	0	0	0	3/3
4	6/6	2/2	0	0	0	8/8
5	12/12	6/6	2/2	0	0	20/20
6	38/38	29/29	7/7	0	0	74/74
7	89/89	50/50	7/13	2/3	0	148/155
8	243/261	83/217	0/84	0/11	0	326/573
9	410/583	33/427	0/163	0/28	0/6	443/1207
total	802/993	204/732	16/269	2/42	0/6	1024/2042

The number of passports of Belyi maps for each degree d and genus g is shown to the right of the slash; the number of them that we have computed is given to the left of the slash.

permutation action of S_3 on passports, so (without loss of generality) we choose exactly one passport up to this S_3-action. (For more on passports, see Section 2.)

A summary of the scope of our computation so far is given in the table above. Our data is available at https://github.com/michaelmusty/BelyiDB and will hopefully also be available at lmfdb.org in the near future.

1.3. ***Comparison.*** Our database compares to the existing catalogs of Belyi maps that are currently available as follows:

- Birch [4] computed a sampling of Belyi maps of low degree and genus, for a total of 50 passports.
- A *Shabat polynomial* is a Belyi map of genus 0 that is totally ramified at ∞. Bétréma–Péré–Zvonkin [3] computed all *Shabat polynomials* up to degree 8; there are 78 such passports.
- A Belyi map is *clean* if every point above 1 has ramification index 2. (A clean Belyi map has even degree, and if ϕ is an arbitrary Belyi map of degree d then $4\phi(1-\phi)$ is a clean Belyi map of degree $2d$.) Adrianov et al. [1] computed all clean Belyi maps up to degree 8; there are 67 such passports.
- Malle [12] computed fields of definition of some genus-0 passports whose permutation group is primitive, subject to some other restrictions, up to degree 13; there are hundreds of passports.
- Bose–Gundry–He [5] describe a partial catalogue of Belyi maps, inspired by considerations from gauge theory in physics. This database contains many genus-0 maps up to degree 7 and some maps in genus 1 and 2.
- Arsen Elkin also has a database of Belyi maps [9].

There are many other papers that compute certain classes of Belyi maps; for further reference, see Sijsling–Voight [15].

1.4. ***Outline.*** The paper is organized as follows. We begin in Section 2 by defining passports and exhibiting an algorithm to enumerate their representative permutation triples up to simultaneous conjugation. In

Section 3, we briefly recall the numerical method employed. In Section 4, we treat the descent issues that arise. In Sections 5–6, we detail steps that are specific to elliptic and hyperelliptic curves, and provide examples of these computations. We conclude in Section 7 with a description of the database, some statistics, and some final observations.

2. Passports

We begin by explaining the combinatorial (or topological) description of Belyi maps and exhibit an efficient method for their enumeration. For general background reading, see Sijsling–Voight [15, §1].

2.1. ***Preliminaries.*** Throughout, let $K \subseteq \mathbb{C}$ be a field. A (*nice*) *curve* over K is a smooth, projective, geometrically connected (irreducible) scheme of finite type over K that is pure of dimension 1. After extension to $\mathbb{C}$, a curve may be thought of as a compact, connected Riemann surface. A *Belyi map* over K is a finite morphism $\phi : X \to \mathbb{P}^1$ over K that is unramified outside $\{0, 1, \infty\}$; we will sometimes write (X, ϕ) when we want to pay special attention to the source curve X. Two Belyi maps ϕ, ϕ' are *isomorphic* if there is an isomorphism $\iota : X \xrightarrow{\sim} X'$ of curves such that $\phi'\iota = \phi$.

Let $\phi : X \to \mathbb{P}^1$ be a Belyi map over $\mathbb{Q}^{\mathrm{al}}$ of degree $d \in \mathbb{Z}_{\geq 1}$. The *monodromy group* of ϕ is the Galois group $\mathrm{Mon}(\phi) := \mathrm{Gal}(\mathbb{C}(X) \mid \mathbb{C}(\mathbb{P}^1)) \leq S_d$ of the corresponding extension of function fields (understood as the action of the automorphism group of the normal closure); the group $\mathrm{Mon}(\phi)$ may also be obtained by lifting paths around $0, 1, \infty$ to X.

A *permutation triple* of degree $d \in \mathbb{Z}_{\geq 1}$ is a tuple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ such that $\sigma_\infty\sigma_1\sigma_0 = 1$. A permutation triple is *transitive* if the subgroup $\langle\sigma\rangle \leq S_d$ generated by σ is transitive. We say that two permutation triples σ, σ' are *simultaneously conjugate* if there exists $\tau \in S_d$ such that

$$\sigma^\tau := (\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau, \tau^{-1}\sigma_\infty\tau) = (\sigma_0', \sigma_1', \sigma_\infty') = \sigma'. \tag{2.1.1}$$

An automorphism of a permutation triple σ is an element of S_d that simultaneously conjugates σ to itself, i.e., $\mathrm{Aut}(\sigma)$ is equal to $Z_{S_d}(\langle\sigma\rangle)$, the centralizer inside S_d.

Lemma 2.1.2. *The set of transitive permutation triples of degree d up to simultaneous conjugation is in bijection with the set of Belyi maps of degree d up to isomorphism.*

Proof. The correspondence is via monodromy [11, Lemma 1.1]; in particular, the monodromy group of a Belyi map is (conjugate in S_d to) the group generated by σ. □

The group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \mid \mathbb{Q})$ acts on Belyi maps by acting on the coefficients of a set of defining equations; under the bijection of Lemma 2.1.2, it thereby acts on the set of transitive permutation triples, but this action is rather mysterious.

We can cut this action down to size by identifying some basic invariants, as follows. A *passport* consists of the data $\mathcal{P} = (g, G, \lambda)$, where $g \geq 0$ is an integer, $G \leq S_d$ is a transitive subgroup, and $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ is a tuple of partitions λ_s of d for $s = 0, 1, \infty$. These partitions will be also be thought of as a tuple of conjugacy classes $C = (C_0, C_1, C_\infty)$ by cycle type, so we will also write passports as

(g, G, C). The *passport* of a Belyi map $\phi : X \to \mathbb{P}^1$ is $(g(X), \mathrm{Mon}(\phi), (\lambda_0, \lambda_1, \lambda_\infty))$, where $g(X)$ is the genus of X and λ_s is the partition of d obtained by the ramification degrees above $s = 0, 1, \infty$, respectively. Accordingly, the *passport* of a transitive permutation triple σ is $(g(\sigma), \langle\sigma\rangle, \lambda(\sigma))$, where (by Riemann–Hurwitz)

$$g(\sigma) := 1 - d + (e(\sigma_0) + e(\sigma_1) + e(\sigma_\infty))/2 \tag{2.1.3}$$

and e is the index of a permutation (d minus the number of orbits), and $\lambda(\sigma)$ is the cycle type of σ_s for $s = 0, 1, \infty$. The *size* of a passport $\mathcal{P}$ is the number of simultaneous conjugacy classes (as in (2.1.1)) of (necessarily transitive) permutation triples σ with passport $\mathcal{P}$.

The action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \mid \mathbb{Q})$ on Belyi maps preserves passports. Therefore, after computing equations for all Belyi maps with a given passport, we can try to identify the Galois orbits of this action. We say a passport is *irreducible* if it has one $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \mid \mathbb{Q})$-orbit and *reducible* otherwise.

2.2. *Passport lemma.* To enumerate passports, we will use the following lemma.

Lemma 2.2.1. *Let S be a group, let $G \leq S$ be a subgroup, let $N := N_S(G)$ be the normalizer of G in S, and let C_0, C_1 be conjugacy classes in N represented by $\tau_0, \tau_1 \in G$. Let $Z_N(g)$ denote the centralizer of g in N. Let*

$$U := \{(\sigma_0, \sigma_1) \in C_0 \times C_1 : \langle\sigma_0, \sigma_1\rangle \subseteq G\}/\sim, \tag{2.2.2}$$

where $\sim$ indicates simultaneous conjugation by elements in S. Then the map

$$\begin{aligned} u : Z_N(\tau_0)\backslash N / Z_N(\tau_1) &\to U, \\ Z_N(\tau_0)\nu Z_N(\tau_1) &\mapsto [(\tau_0, \nu\tau_1\nu^{-1})], \end{aligned} \tag{2.2.3}$$

is surjective, and for all $[(\sigma_0, \sigma_1)] \in U$ such that $\langle\sigma_0, \sigma_1\rangle = G$, there is a unique preimage under u.

Proof. The map (2.2.3) is well-defined, as $\nu \in N$ so $\nu\tau_1\nu^{-1} \in G$ and conjugacy classes are taken in N.

We first show that (2.2.3) is surjective. Let $[(\sigma_0, \sigma_1)] \in U$. Then $g\sigma_0 g^{-1} = \tau_0$ for some $g \in N$, and so $[(\sigma_0, \sigma_1)] = [(\tau_0, g\sigma_1 g^{-1})] \in U$. Similarly, there is $h \in N$ such that $\sigma_1 = h\tau_1 h^{-1}$ so $[(\sigma_0, \sigma_1)] = [(\tau_0, (gh)\tau_1(gh)^{-1})]$, and $gh = \nu \in N$.

Next, we show (2.2.3) is injective when restricted to generating pairs. Suppose $[(\tau_0, \nu\tau_1\nu^{-1})] = [(\tau_0, \mu\tau_1\mu^{-1})] \in U$ with $\mu, \nu \in N$. Then there exists $\rho \in S$ with

$$\rho(\tau_0, \nu\tau_1\nu^{-1})\rho^{-1} = (\tau_0, \mu\tau_1\mu^{-1}). \tag{2.2.4}$$

Then $\rho\langle\tau_0, \nu\tau_1\nu^{-1}\rangle\rho^{-1} = \rho G\rho^{-1} = \langle\tau_0, \mu\tau_1\mu^{-1}\rangle = G$ under the hypotheses on generation, so we have $\rho \in N$. The equation in the first component reads $\rho\tau_0\rho^{-1} = \tau_0$, so $\rho \in Z_N(\tau_0)$ by definition. The second equation yields

$$\begin{aligned} \rho\nu\tau_1\nu^{-1}\rho^{-1} &= \mu\tau_1\mu^{-1}, \\ (\mu^{-1}\rho\nu)\tau_1(\mu^{-1}\rho\nu)^{-1} &= \tau_1, \end{aligned} \tag{2.2.5}$$

so $\mu^{-1}\rho\nu \in Z_N(\tau_1)$. Writing $\nu = (\rho^{-1})\mu(\mu^{-1}\rho\nu)$, we find that $Z_N(\tau_0)\nu Z_N(\tau_1) = Z_N(\tau_0)\mu Z_N(\tau_1)$, as desired. □

2.3. ***Computing passports.*** We now describe an algorithm to produce all passports for a given degree d and a representative set of permutation triples in each passport up to simultaneous conjugation. We simplify this description by considering the transitive subgroups of S_d one at a time: these are currently available [6] up to degree 47.

There is a natural permutation action of S_3 on passports and on the permutation triples in a passport, corresponding to postcomposition of Belyi maps by an automorphism of the base curve $\mathbb{P}^1$ permuting $\{0, 1, \infty\}$. For the purposes of tabulation, we will choose one passport up to this action of S_3: to do so, we choose a total ordering $\preceq$ on partitions (e.g., refining the dominance partial order).

Algorithm 2.3.1. Let $d \in \mathbb{Z}_{\geq 1}$, let $G \leq S_d$ be a transitive subgroup, and let $N := N_{S_d}(G)$ be the normalizer of G in S_d. This algorithm returns a representative list of passports for G up to the action of S_3; and, for each passport, a representative list of permutation triples (one for each simultaneous conjugacy class).

(1) Compute representatives $\{\tau_1, \ldots, \tau_r\}$ for the conjugacy classes $\{C_1, \ldots, C_r\}$ of G up to conjugation by N.

(2) Out of the r^2 possible pairs of conjugacy class representatives, only consider pairs (τ_i, τ_j) with $\lambda(\tau_i) \preceq \lambda(\tau_j)$.

(3) For each pair (τ_i, τ_j) from Step 2, apply Lemma 2.2.1 to compute the set

$$U_{ij} := \{(\sigma_0, \sigma_1) \in C_i \times C_j : \langle \sigma_0, \sigma_1 \rangle \subseteq G\}/\sim \tag{2.3.2}$$

by computing the double coset $Z_N(\tau_i)\backslash N/Z_N(\tau_j)$ and applying the map u. Complete each pair $(\sigma_0, \sigma_1) \in U_{ij}$ to a permutation triple by setting $\sigma_\infty := (\sigma_1\sigma_0)^{-1}$, and let T_{ij} denote the resulting set of triples obtained from U_{ij}.

(4) Keep only those triples $\sigma \in T_{ij}$ with $\langle \sigma \rangle = G$ and such that $\lambda(\sigma_1) \preceq \lambda(\sigma_\infty)$.

(5) Sort the triples obtained from Step 4 into passports by cycle structure.

Proof of correctness. We compute all possible input pairs (τ_0, τ_1) to Lemma 2.2.1 with $\lambda(\tau_0) \preceq \lambda(\tau_1)$. This accounts for all possible input pairs to Lemma 2.2.1 since every passport is S_3-equivalent to such a passport. We do not have control over the conjugacy class of σ_∞ in this process, but Step 4 insists that every resulting passport representative σ has $\lambda(\sigma_0) \preceq \lambda(\sigma_1) \preceq \lambda(\sigma_\infty)$ thereby ensuring a unique passport up to the action of S_3. □

Using Algorithm 2.3.1 we computed representatives for all passports (without equations) in degree $d \leq 11$; this took about 18 minutes for all degrees $d \leq 9$, about 3.3 hours for $d = 10$, and 2.37 days for $d = 11$.

3. Numerical computation of Belyi maps

With triples and passports in hand, we now briefly review the numerical method used to compute Belyi maps.

3.1. ***Overview.*** The method of Klug–Musty–Schiavone–Voight [11] takes as input a permutation triple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ and produces as output equations for the curve X and Belyi map $\phi : X \to \mathbb{P}^1$ over a number field $K \subseteq \mathbb{C}$ that corresponds to σ (in the monodromy bijection of Lemma 2.1.2).

This method is numerical, so it is not guaranteed to terminate (because of loss of precision or convergence issues), but when it terminates, it gives correct output. The method proceeds in the following steps:

(1) Form the triangle subgroup $\Gamma \leq \Delta(a, b, c)$ associated to σ and compute its coset graph.

(2) Use a reduction algorithm for Γ and numerical linear algebra to compute power series expansions of modular forms $f_i \in S_k(\Gamma)$ for an appropriate weight k.

(3) Use numerical linear algebra (and Riemann–Roch) to find polynomial relations among the series f_i to compute equations for the curve X and similarly to express the map ϕ in this model.

(4) Normalize the equations of X and ϕ so that the coefficients are algebraic; recognize these coefficients as elements of a number field $K \subseteq \mathbb{C}$.

(5) Verify that ϕ has the correct ramification and monodromy.

For the purposes of this article, the reader may treat this method as a black box with two exceptions: in Section 4.4 we describe an improvement to the method in Step 4 for a choice of descent constant, and we discuss a numerical test for hyperellipticity using power series in weight 2 in Section 6.2.

3.2. ***Discussion.*** There are a few key advantages of the above algorithm for our purposes. First, it is uniform, and in particular does not require the permutation triple to have a special form or for the curve to be of any particular genus. Second, it computes one Belyi map at a time, without needing the whole passport, and in particular, there are no *parasitic solutions* (degenerate maps that arise in other computational methods). Third, we obtain the bijection between triples and Belyi maps by the very construction of the equations (and the embedding $K \hookrightarrow \mathbb{C}$).

There is an alternative method due to Monien [13; 14] that uses noncocompact triangle subgroups $\Gamma \leq \Delta(2, 3, \infty) \simeq \mathrm{PSL}_2(\mathbb{Z})$ instead of our cocompact subgroups. This method has been shown to work in genus 0 for maps of very large degree (e.g., a Belyi map with monodromy group isomorphic to the Conway group Co_3 is given in [14]).

4. Descent issues

In this section, we discuss issues of descent for Belyi maps: when can a Belyi map be defined over a minimal field? (The reader eager for Belyi map computations should skip this and proceed to the next section.) A satisfactory answer to this question is crucial for understanding the action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \mid \mathbb{Q})$ on Belyi maps.

4.1. ***Field of moduli and field of definition.*** Let σ be a permutation triple with passport $\mathcal{P}$ and corresponding Belyi map $\phi : X \to \mathbb{P}^1$ over $\mathbb{Q}^{\mathrm{al}}$. The *field of moduli* $M(X, \phi) \subseteq \mathbb{Q}^{\mathrm{al}} \subset \mathbb{C}$ of ϕ is the fixed field

of $\{\tau \in \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) : \tau(\phi) \simeq \phi\}$. The field of moduli is the intersection of all fields over which (X, ϕ) can be defined.

The degree of $M(X, \phi)$ is bounded above by the size of the passport $\mathcal{P}$; this bound is achieved if and only if the passport is irreducible.

Definition 4.1.1. We say that (X, ϕ) *descends* (to its field of moduli) if (X, ϕ) can be defined over its field of moduli $M(X, \phi)$, that is, if there exists a Belyi map $\phi_K : X_K \to \mathbb{P}^1$ over K whose base change to $\overline{\mathbb{Q}}$ is isomorphic to $\phi : X \to \mathbb{P}^1$.

Weil [17] studied general conditions for descent. For example, if ϕ has trivial automorphism group $\mathrm{Aut}(\phi)$, then ϕ descends — this criterion suffices to deal with a large majority of Belyi maps. More generally, to descend the Belyi map it is necessary and sufficient to construct a *Weil cocycle*, a collection of isomorphisms $f_\sigma : \sigma(X) \to X$, one for every element $\sigma \in \mathrm{Gal}_{M(X,\phi)} := \mathrm{Gal}(\overline{\mathbb{Q}} \mid M(X, \phi))$, such that $f_{\sigma\tau} = f_\sigma \sigma(f_\tau)$ for all $\sigma, \tau \in \mathrm{Gal}_{M(X,\phi)}$. (When $\mathrm{Aut}(\phi)$ is trivial, this condition is satisfied for any collection of isomorphisms f_σ.) This criterion can be made explicit and computable [15, Method 4.1].

4.2. ***Pointed descent.*** There is another way to sidestep descent issues by rigidifying, as follows.

Definition 4.2.1. A *pointed Belyi map* $(X, \phi; P)$ is a Belyi map (X, ϕ) together with a point $P \in \phi^{-1}(\{0, 1, \infty\}) \subseteq X(\overline{\mathbb{Q}})$. An isomorphism of pointed Belyi maps $(X, \phi; P) \xrightarrow{\sim} (X', \phi'; P')$ is an isomorphism of Belyi maps ι such that $\iota(P) = P'$.

Remark 4.2.2. In our computations we choose the point P to be one of the ramification points of ϕ. Any point on X would do, but only the ramification points can be seen from the combinatorial data.

Definition 4.2.3. A *pointed permutation triple* $(\sigma; c)$ is a permutation triple $\sigma \in S_d^3$ together with a distinguished cycle c in one of the permutations σ_s with $s = 0, 1, \infty$; we call s its *base point* and the length of the cycle c its *length*. We call $(\sigma; c)$ a *pointed refinement* of the permutation triple σ.

Two pointed permutation triples $(\sigma; c)$ and $(\sigma'; c')$ are *simultaneously conjugate* if the permutation triples σ, σ' are simultaneously conjugate by an element $\tau \in S_d$ such that $c^\tau = c'$. The automorphism group $\mathrm{Aut}(\sigma; c) \leq \mathrm{Aut}(\sigma)$ is the subgroup of S_d that simultaneously conjugates $(\sigma; c)$ to itself.

Returning to the correspondence of Lemma 2.1.2, we see that pointed permutation triples of degree d up to simultaneous conjugation are in bijection with pointed Belyi maps of degree d up to isomorphism.

Proposition 4.2.4. *The base point, length, and cardinality of the automorphism group of a pointed permutation triple are invariant under simultaneous conjugation and under the action of* $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$.

Proof. The statements for simultaneous conjugation are clear. For the Galois action, we pass back to Belyi maps: the base point, the ramification index, and the automorphism group of a pointed Belyi map are Galois invariant. □

We similarly define the field of moduli $M(X, \phi; P)$ for a pointed Belyi map. The following theorem gives us a widely applicable criterion for descent (even in the presence of automorphisms).

Theorem 4.2.5. *A pointed Belyi map $(X, \phi; P)$ descends; i.e., the curve X, the map ϕ, and the point P can all be defined over $M(X, \phi; P)$.*

Proof. The statement is given by Birch [4, Theorem 2]; for a constructive proof using branches, see Sijsling–Voight [16, Theorem 1.12]. □

4.3. ***Pointed passports.*** Given the simplicity and importance of Theorem 4.2.5, we refine our notion of passport as follows.

Definition 4.3.1. A *pointed passport* is the data $(g, G, \lambda; c)$, where (g, G, λ) is a passport and $c = (s, e, a)$ consists of the data $s \in \{0, 1, \infty\}$, and $e \in \mathbb{Z}_{\geq 1}$ a summand in the partition λ_s, and finally $a \in \mathbb{Z}_{\geq 1}$.

Given a pointed Belyi map $(X, \phi; P)$, we define its *pointed passport* $\mathcal{P}(X, \phi; P)$ to be its passport together with the data $s = \phi(P)$, the ramification degree $e = e_\phi(P)$, and $a = \#\mathrm{Aut}(X, \phi; P)$. Likewise, we define the pointed passport $\mathcal{P}(\sigma; c)$ to be the passport with s its base point, e its length, and a the cardinality of its automorphism group. We define the *size* of a pointed passport $\mathcal{P}$ to be the number of isomorphism classes of pointed Belyi maps (equivalently, number of classes of pointed permutation triples) with pointed passport $\mathcal{P}$.

Corollary 4.3.2. *A pointed Belyi map is defined over a field whose degree is at most the size of its pointed passport.*

Proof. Apply Theorem 4.2.5. □

Proposition 4.3.3. *If the size of $\mathcal{P}(\sigma; c)$ is equal to the size of $\mathcal{P}(\sigma)$, then all Belyi maps with passport $\mathcal{P}(\sigma)$ descend.*

Proof. Any field of definition of a pointed Belyi map is also a field of definition of the underlying Belyi map, so the fields of moduli and pointed moduli coincide by hypothesis. Descent follows by Theorem 4.2.5, since the moduli field of the pointed curve is a field of definition. □

It seems quite common for a permutation triple to have a pointed refinement of size 1. The first example where no such refinement exists occurs in degree 8; see Example 4.5.1 below.

4.4. ***Descent from*** $\mathbb{C}$**.** In Step 4 of our numerical method (see Section 3.1), there is a normalization procedure which we may interpret as an application of pointed descent as follows. In the original method [11, §5], modular forms are expanded as power series centered in a neighborhood of a ramification point of the form $|w| < 1$ in a parameter w, and the coefficients of these power series are renormalized by writing them in terms of Θw for a certain transcendental factor Θ, computed as the ratio of two "consecutive" terms in the power series expansion. In our setting, we instead normalize not the coefficients of the power series but instead coefficients of the Belyi map itself, now setting "consecutive" coefficients equal. In practice, we find that this normalization requires smaller precision to recognize the Belyi map exactly from its numerical approximation.

Remark 4.4.1. In every example we computed, and in both ways of normalizing, we obtained normalized power series expansions that numerically agree with series defined over $M(X, \phi; P)$ with chosen ramification point P. Currently this is only a numerical observation, but it is a sensible expectation, as the method works by computing the pluricanonical image using expansions at the designated point.

Example 4.4.2. Consider the passport $(1, S_5, (5^1, 4^1 1^1, 4^1 1^1))$. The unique representative up to simultaneous conjugation is given by σ with

$$\sigma_0 = (1\ 4\ 2\ 5\ 3), \quad \sigma_1 = (1\ 2\ 3\ 4), \quad \sigma_\infty = (1\ 2\ 3\ 5). \tag{4.4.3}$$

We take $c = (1\ 4\ 2\ 5\ 3)$, which has length 5 and trivial automorphism group. Since the pointed passport also has size 1, the field of moduli of the Belyi map equals $\mathbb{Q}$ by Corollary 4.3.2, and we can descend to this field by Proposition 4.3.3. Computing with 50 digits of precision (here and throughout, we only ever display 5 digits), we find $X : y^2 = x^3 - 27c_4x - 54c_6$ with

$$c_4 \approx 0.01030 + 0.00748i, \quad c_6 \approx -0.00270 + 0.00196i \tag{4.4.4}$$

and Belyi map ϕ with

$$\phi \approx \frac{2.0000}{-1 + (2.21275 + 0.71897i)y + (1.77422i)xy} = \frac{2}{-1 + b_3y + b_5xy} \tag{4.4.5}$$

(where $i^2 = -1$). The indeterminacy in this approximation is by $\lambda \in \mathbb{C}^\times$, acting according to the degree of the pole at ∞, so $(c_4, c_6) \leftarrow (\lambda^{-4}c_4, \lambda^{-6}c_6)$ and $(x, y) \leftarrow (\lambda^{-2}x, \lambda^{-3}y)$. Taking

$$\lambda := \frac{b_5}{b_3^2} \approx -0.19265 - 0.26516i \tag{4.4.6}$$

the rescaled values $b_3' := \lambda^3 b_3 \approx 2^{16}/5^{10}$ and $b_5' := \lambda^5 b_5 \approx -2^8/5^5$ have $(b_3')^2/b_5' = 1$ (and there exists a descent with this ratio, defined over $\mathbb{Q}$). Now all the coefficients $a_0, b_3, b_5, c_4, c_6 \in \mathbb{Q}$ are easily identified. After computing a minimal model and swapping $0, \infty \in \mathbb{P}^1$ for cosmetics, we obtain $X : y^2 = x^3 + 5x + 10$ with map

$$\phi(x, y) = ((x - 5)y + 16)/32. \tag{4.4.7}$$

4.5. ***Examples.*** We now discuss some examples to see the various subtleties that play a role when descending Belyi maps.

Example 4.5.1. The first case of a passport for which Proposition 4.3.3 does not apply occurs in degree 8, given by $(1, V_4^2 : S_3, (3^2 1^2, 4^2, 4^2))$. The passport is size 1 but all pointed passports are size 2. The Belyi map descends because its automorphism group is trivial. A descent is given by $X : y^2 = x^3 + x^2 + 8x + 8$ and

$$\phi(x, y) = \frac{4(7x^4 + 24x^3 + 92x^2 + 320x + 272)y - 16(x + 1)(x^2 + 8)(x^2 + 16x + 24)}{27x^4y}.$$

Because $\mathrm{Aut}(X, \phi)$ is trivial, this is the only model over $\mathbb{Q}$ up to isomorphism. Finally, none of its ramification points is rational, so no descent of a pointed refinement immediately gets us to the field of moduli $\mathbb{Q}$.

Example 4.5.2. The first dessin that does not descend to its field of moduli is of degree 16. Indeed, in lower degree, there are only three passports for which Proposition 4.3.3 does not apply *and* the automorphism group is nontrivial: all occur in degree 12, one with size 1, the other two of size 2. Yet explicit calculation shows that these three examples all descend.

For purposes of illustration, we consider the passport $(4, \text{t12n57}, (6^2, 6^2, 6^2))$ of size 2, where t12n57 denotes the transitive group in S_{12} numbered 57. The passport is irreducible and the curves are nonhyperelliptic: they arise as degree-2 covers branching at the ramification points of the unique Belyi map with passport $(1, A_4(6), (3^2, 3^2, 3^2))$, given by $E : y^2 = x^3 + 6x^2 - 3x$ and Belyi map $\phi(x, y) = (x^2+3)y/(8x^2)$. The ramification points are then exactly the $\mathbb{Q}$-rational points ∞, $(0, 0)$, $(1, \pm 2)$, $(-3, \pm 6)$ on E. To construct the resulting degree-2 cover, we choose a 4-torsion point P_4 on E. Then the sum of the ramification points and $2P_4$ is equivalent to 8∞, so that we get a function whose square root gives rise to the requested cover. The four possible covers thus obtained are all Galois conjugate; we get the same Belyi map, this from the curve

$$X : \begin{array}{l} y^2 = x^3 + 6x^2 - 3x, \\ w^2 = yx^2 + 2yx - 3y + \alpha x^3 + 2\alpha x^2 - 3\alpha x, \end{array} \tag{4.5.3}$$

where $\alpha^4 - 12\alpha^2 + 48 = 0$. The field $\mathbb{Q}(\alpha)$ contains $\mathbb{Q}(\sqrt{-3})$. This unique quadratic subfield is also the field of moduli of the Belyi map from X, since one can show that it is mapped to its $\mathbb{Q}(\sqrt{-3})$-conjugate by the automorphism

$$(x, y, w) \mapsto \left(\frac{-3}{x}, \frac{3y}{x^2}, \frac{3iw}{x^2} \right) \tag{4.5.4}$$

of X. To show that the Belyi map descends, it suffices [7, Corollary 5.4] (or [16, Theorem 3.4.8] with $\mathcal{R} = \varnothing$) to show that the canonical model E_0 of E corresponding to the cocycle defined by the first two entries of (4.5.4) has a rational point. It does; in fact E_0 is isomorphic to E. Still, none of the points on E_0 that correspond to the ramification points of E are rational over $\mathbb{Q}(\sqrt{-3})$. We conclude that there is no choice of *pointed refinement* that will give rise to a descent to $\mathbb{Q}(\sqrt{-3})$ in this case, even though the Belyi map descends.

5. Genus 1

In this section, we discuss some details for Belyi maps of genus 1.

5.1. ***Newton's method.*** Let (X, ϕ) be a Belyi map with X of genus 1 defined by $X : y^2 = f(x) = x^3 - 27c_4x - 54c_6$. In our numerical method (see Section 3.1, or the "Genus 1" subsection of [11, §5]), we compute a numerical Weierstrass X and Belyi map ϕ on X to arbitrary precision.

Klug–Musty–Schiavone–Voight [11, Example 5.28] describe how to use Newton's method in the case of genus 0 to achieve very accurate approximations of the coefficients of the Belyi map, allowing us to quickly pass from tens of digits of precision to tens of thousands. We now explain how Newton's method can be extended to the case of genus-1 Belyi maps, ironing out some wrinkles.

Let $P = (x_P, y_P) \in X(\mathbb{C})$ be an affine point and let $t := x - x_P$ and $s := y - y_P$. Insisting that ϕ have a zero or pole of a given order at P imposes equations that can be determined by working in the completed local ring $\widehat{\mathbb{C}[X]}_P$ as follows.

If P is not a 2-torsion point of X, then t is a uniformizer for $\widehat{\mathbb{C}[X]}_P$. We solve for s in terms of t by substituting $x = t + x_P$ and $y = s + y_P$ into the equation for X, thereby obtaining a quadratic equation in s whose solution is

$$s := -y_P + y_P\sqrt{1 + \frac{t^3 + 3x_P t^2 + (3x_P^2 - 27c_4)t}{y_P^2}}. \tag{5.1.1}$$

If instead P is a 2-torsion point, then s is a uniformizer for $\widehat{\mathbb{C}[X]}_P$; substituting as above, we obtain a cubic equation in s, which we solve via Hensel lifting. In either case, we may express the numerator and denominator of ϕ as power series in the local parameter. Once this has been accomplished, we obtain the equations imposed by a zero or pole at P of order e_P by insisting that the first e_P coefficients of the series for the numerator or denominator, respectively, of ϕ vanish.

Newton's method has proven invaluable in our computations: it has allowed us to compute genus-1 maps that were previously out of reach, and has also sped up our computations considerably.

5.2. ***Example.*** We illustrate the above method with an example.

Example 5.2.1. Consider the passport $(1, S_7, (6^1 1^1, 6^1 1^1, 2^2 3^1))$ of size 13. Its pointed refinement taking the 6-cycle over 0 also has size 13. A representative permutation triple is

$$\sigma_0 = (1\ 2\ 3\ 4\ 5\ 6), \quad \sigma_1 = (2\ 7\ 6\ 3\ 4\ 5), \quad \sigma_\infty = (1\ 7\ 2)(3\ 5)(4\ 6). \tag{5.2.2}$$

This ramification data and a Riemann–Roch calculation implies that ϕ can be written as $\phi = \phi_0/\phi_\infty$ for $\phi_0 \in \mathscr{L}(2\infty)$ and $\phi_\infty \in \mathscr{L}(8\infty)$. (For details, see Section 6.3 below.) Since $1, x$ and $1, x, y, x^2, xy, \ldots, x^4$ are bases for $\mathscr{L}(2\infty)$ and $\mathscr{L}(8\infty)$, respectively, pulling out leading coefficients and changing notation, we write

$$\phi = u\frac{\phi_0}{\phi_\infty} = u\frac{a_0 + x}{b_0 + b_2 x + b_3 y + \cdots + b_7 x^2 y + x^4} \tag{5.2.3}$$

for some $a_0, a_2, b_0, b_2, \ldots, b_7 \in \mathbb{Q}^{\mathrm{al}} \subset \mathbb{C}$. Computing with 40 digits of precision (displaying 5), we find after 20 seconds on a standard CPU the initial approximation for X and ϕ. After normalizing as in Section 4.4 to obtain $b_7 (= b_8) = 1$, we obtain

$$\begin{gathered} c_4, \approx -0.00031, \quad c_6 \approx 0.0000035, \\ \phi \approx 0.0024\frac{-0.18587 + x}{-0.00042 + 0.00112x + \cdots + 0.03839x^3 + x^2 y + x^4}. \end{gathered} \tag{5.2.4}$$

Let $P = (x_P, y_P)$ be the point corresponding to the 3-cycle in σ_∞. Since $P \in X(\mathbb{C})$, our first equation is $y_P^2 = x_P^3 - 27c_4 x_P - 54c_6$. Computing s as in (5.1.1), we find

$$s = \frac{\frac{3}{2}x_P^2 - \frac{27}{2}c_4}{y_P}t + \frac{-\frac{9}{8}x_P^4 + \frac{81}{4}c_4x_P^2 + \frac{3}{2}x_Py_P^2 - \frac{729}{8}c_4^2}{y_P^3}t^2 + \frac{\frac{27}{16}x_P^6 - \frac{729}{16}c_4x_P^4 + \cdots + \frac{81}{4}c_4x_Py_P^2 + \frac{1}{2}y_P^4 - \frac{19683}{16}c_4^3}{y_P^5}t^3 + O(t^4). \quad (5.2.5)$$

Substituting $x = t + x_P$ and $y = s + y_P$ into the above expression for ϕ_∞ yields

$$\begin{aligned}\phi_\infty = {} & x_P^4 + x_P^3b_6 + x_P^2y_Pb_7 + x_P^2b_4 + x_Py_Pb_5 + x_Pb_2 + y_Pb_3 + b_0 \\ & + \left(\tfrac{3}{2}x_P^4b_7 + 4x_P^3y_P + \tfrac{3}{2}x_P^3 + \cdots + b_5 + y_Pb_2 - \tfrac{27}{2}c_4b_3\right)\frac{t}{y_P} \\ & + \left(-\tfrac{9}{8}x_P^6b_7 - \tfrac{9}{8}x_P^5b_5 + \cdots + \tfrac{729}{8}c_4^2b_3\right)\frac{t^2}{y_P^3} + O(t^3). \end{aligned} \quad (5.2.6)$$

To impose the condition that ϕ has a pole of order 3 at P, we set the first three coefficients of ϕ_∞ equal to 0, giving three relations.

Proceeding similarly with the other ramification points, we obtain 22 polynomial equations in the 23 variables $u, c_4, c_6, a_0, b_0, \ldots, b_7$ and x_P, y_P for each of the ramification points, other than the point corresponding to the cycle containing 1 in σ_0. (The point corresponding to this cycle is ∞, and we have already imposed the condition that ϕ vanishes to order 6 at ∞ by taking $\phi_0 \in \mathscr{L}(2\infty)$ and $\phi_\infty \in \mathscr{L}(8\infty)$.) This system is underdetermined, so in order to apply Newton's method, we must find at least one more equation. We observe that although ϕ is a degree-7 map, ϕ_∞ has degree 8, so there must be a common zero of ϕ_0 and ϕ_∞. Calling this point $P_s = (x_s, y_s)$, we obtain three more equations

$$\begin{aligned} y_s^2 &= x_s^3 - (27c_4x_s - 54c_6), \\ 0 &= \phi_0(P_s) = a_0 + x_s, \\ 0 &= \phi_\infty(P_s) = b_0 + b_2x_s + b_3y_s + \cdots + b_7x_s^2y_s + x_s^4. \end{aligned} \quad (5.2.7)$$

We have adjoined two more variables x_s, y_s and produced three more equations to ensure nondegeneracy. This produces a system of 25 equations in 25 variables. Applying Newton's method to this system, in 16.20 seconds we obtain approximations of coefficients with 2000 digits of precision, which allows us to recognize the coefficients of ϕ as algebraic numbers. After a change of variables to reduce the size of the output, we find the elliptic curve

$$X : y^2 = x^3 - (24\nu + 75)x + \tfrac{1}{2}(-657\nu^2 - 1014\nu + 3278) \quad (5.2.8)$$

and Belyi map $\phi = u\phi_0/\phi_\infty$, where $u = 1/(2^93^2)$ and

$$\begin{aligned}\phi_0 &= (-419\nu^2 - 358\nu + 2947) + 49x, \\ \phi_\infty &= (-806361\nu^2 - 724014\nu + 5449304) + (-3150\nu^2 - 15652\nu + 84560)x \\ &\quad + (-11310\nu^2 + 17940\nu + 118656)y + (-33180\nu^2 + 74760\nu - 55104)x^2 \\ &\quad + (59556\nu^2 - 189336\nu + 233856)xy + (5166\nu^2 - 16380\nu + 20720)x^3 \\ &\quad + (-59022\nu^2 + 184980\nu - 225792)x^2y + (25557\nu^2 - 80122\nu + 97832)x^4 \end{aligned}$$

over the number field $\mathbb{Q}(\nu)$ where $\nu^3 - 6\nu + 12 = 0$. It turns out that this passport decomposes into two Galois orbits, one of size 3 as shown above, and the other of size 10. The coefficients of the Belyi map for the size-10 orbit are too large for us to display here, but it is defined over the number field $\mathbb{Q}(\mu)$ where

$$\mu^{10} - 2\mu^9 + 15\mu^8 - 78\mu^7 + 90\mu^6 + 48\mu^5 + 90\mu^4 - 78\mu^3 + 15\mu^2 - 2\mu + 1 = 0. \tag{5.2.9}$$

Remark 5.2.10. The "extra zero" phenomenon in (5.2.7) is typical; it can be avoided in the special case when 0 is totally ramified (i.e., when σ_0 is a d-cycle).

6. Hyperelliptic curves

We now discuss some issues and improvements for hyperelliptic curves.

6.1. ***Setup.*** Recall that a hyperelliptic curve of genus $g \geq 2$ over K has a model

$$X : y^2 + u(x)y = v(x), \tag{6.1.1}$$

where $\deg(u) \leq g+1$ and $\deg(v) \leq 2g+2$. Letting $f(x) := u(x)^2 + 4v(x)$, we have $f(x)$ separable with $\deg f(x) = 2g+1$ or $2g+2$; we refer to the model as *even* or *odd* according to the parity of $\deg f(x)$. Note that an odd model has the single point $\infty = (1:1:0)$ at infinity, while an even model has two, $\infty' = (1 : \sqrt{f_0} : 0)$ and $\infty = (1 : -\sqrt{f_0} : 0)$, where f_0 is the leading coefficient of $f(x)$ (i.e., the point ∞ is a Weierstrass point if and only if the model is odd.) In constructing the Belyi map, in both cases we take ∞ to be the marked point (around which we expand series), and by convention it corresponds to the cycle containing 1 in σ_0.

6.2. ***Numerical test for hyperellipticity.*** Let Γ be a triangle subgroup with $X = X(\Gamma)$ of genus $g \geq 2$. We test if X is numerically hyperelliptic (in the sense the curve appears to be hyperelliptic to the precision computed) as follows. First, we compute power series expansions of an *echelonized* basis $f_1, f_2, \ldots, f_g$ of $S_2(X(\Gamma))$. We have an isomorphism $S_2(X(\Gamma)) \cong \Omega(X(\Gamma))$ given by $f(z) \mapsto f(z)\,\mathrm{d}z$, where $\Omega(X(\Gamma))$ is the $\mathbb{C}$-vector space of holomorphic differential 1-forms on $X(\Gamma)$. If X is hyperelliptic with model as in (6.1.1), since $f_1, \ldots, f_g$ is an echelonized basis we have the further isomorphism

$$\begin{aligned} \Omega(X(\Gamma)) &\xrightarrow{\sim} \Omega(X), \\ f_i(z)\,\mathrm{d}z &\mapsto x^{g-i}\,\frac{\mathrm{d}x}{y}, \end{aligned} \tag{6.2.1}$$

for $i = 1, \ldots, g$. Thus, to recover x, y defined on $X(\Gamma)$, we can take

$$x := f_1/f_2, \quad y := x'/f_g, \tag{6.2.2}$$

where x' denotes the derivative of x with respect to w (the coordinate in the hyperbolic disc). If the model is odd, then $\operatorname{ord}_\infty x = -2$ and $\operatorname{ord}_\infty y = -(2g+1)$; if the model is even, then $\operatorname{ord}_\infty x = -1$ and $\operatorname{ord}_\infty y = -(g+1)$.

Consider the rational map $X(\Gamma) \to \mathbb{A}^2_{\mathbb{C}}$ with coordinates x, y. Using numerical linear algebra, we test if there is an approximate linear relation among

$$1, x, \dots, x^{2g+2}, y, xy, \dots, x^{g+1}y, y^2 \in \mathbb{C}[\![w]\!]. \tag{6.2.3}$$

If there is such a relation, we obtain a rational map from X to a hyperelliptic curve $X' \subseteq \mathbb{A}^2$. If $g(X') = g(X)$, then the Riemann–Hurwitz formula implies that this map is birational; hence X' is a model of X as in (6.1.1). If no such relation exists, then we conclude that X is not numerically hyperelliptic.

6.3. ***Computing a hyperelliptic Belyi map.*** Suppose now that X is hyperelliptic with model as in (6.1.1). We compute the expression of the Belyi map ϕ as a rational function in x and y roughly as follows. (1) Determine an appropriate Riemann–Roch space $\mathscr{L}(D)$. (2) Compute a basis of $\mathscr{L}(D)$ in terms of x and y. (3) Using numerical linear algebra, express ϕ as a linear combination of functions in this basis.

We make this precise as follows, following Javanpeykar–Voight [10, Lemma 3.2]. Let $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ be a transitive permutation triple of degree d with corresponding hyperelliptic Belyi map (X, ϕ), and let g be the genus of X. Let s be the length of the cycle containing 1 in σ_0 and let $k_1, \dots, k_r$ be the lengths of the remaining cycles in σ_0. Then the divisor of poles of $1/\phi$ is $\operatorname{div}_\infty(1/\phi) = s\infty + \sum_{i=1}^r k_i P_i$ for some points $P_1, \dots, P_r \in X(\mathbb{C})$. Since we do not have control over the points $P_1, \dots, P_r$, we "cancel" these poles by multiplying ϕ by a suitable function ϕ_0 that has zeroes at $P_1, \dots, P_r$ and has poles only at ∞. Such a ϕ_0 will belong to the space $\mathscr{L}(D) \subseteq \mathscr{L}(t\infty)$, where

$$D := -\sum_{i=1}^r k_i P_i + t\infty \tag{6.3.1}$$

for some (as of yet undetermined) $t \in \mathbb{Z}_{\geq 0}$. Once we have obtained ϕ_0, then $\phi_0/\phi \in \mathscr{L}((s+t)\infty)$. As we will describe in the next step, we can write down a basis for Riemann–Roch spaces for divisors of the form $m\infty$. This allows us to compute ϕ_0 and $\phi_\infty := \phi_0/\phi \in \mathscr{L}((s+t)\infty)$ with respect to this basis. Thus we have $\phi = \phi_0/\phi_\infty$ for some $\phi_0 \in \mathscr{L}(t\infty)$ and $\phi_\infty \in \mathscr{L}((s+t)\infty)$.

It remains to determine a value of t so that such a ϕ_0 exists. To do this, we apply Riemann–Roch to the divisor D. Since $\sum_{i=1}^r k_i = d - s$, this yields

$$\ell(D) - \ell(K_X - D) = 1 - g + \deg(D) = 1 - g + (s - d + t), \tag{6.3.2}$$

where K_X is a canonical divisor of X. To ensure the existence of a nonzero ϕ_0 as above, we must have $\ell(D) \geq 1$. By (6.3.2), this holds if $1 - g + s - d + t \geq 1$, i.e., if $t \geq d - s + g$. Thus we may take $t = d - s + g$. (This conclusion actually does not require X to be hyperelliptic.)

Next, we explain how to compute bases for $\mathscr{L}(t\infty)$ and $\mathscr{L}((s+t)\infty)$ as in Step 2. In the case of an odd model, this basis is particularly simple: x and y have poles at ∞ of orders 2 and $2g+1$, respectively, so

$$1, x, x^2, \dots, x^{\lfloor m/2 \rfloor}, y, xy, \dots, x^{\lfloor (m-(2g+1))/2 \rfloor} y \tag{6.3.3}$$

is a basis for $\mathscr{L}(m\infty)$. In the case of an even model the situation is more complicated. Now $x, y \notin \mathscr{L}(m\infty)$ because they have poles at ∞'. We compute a basis for $\mathscr{L}(m\infty)$ as follows. Since x has a

simple pole at ∞' we know $t = 1/x$ has a simple zero, and hence is a uniformizing parameter at ∞'. Working in the completed local ring $\widehat{\mathcal{O}}_{X,\infty'} \simeq \mathbb{C}[\![t]\!]$, we can express y as a Laurent series in t via

$$y = \tfrac{1}{2}\big(-u(1/t) \pm \sqrt{u(1/t)^2 + 4v(1/t)}\big). \tag{6.3.4}$$

We use the series expansions $x(w), y(w)$ at ∞ to match the correct sign in (6.3.4). For each $j \in \{0, \dots, m - (g+1)\}$ we compute the Laurent tail $P_j \in \mathbb{C}[1/t] = \mathbb{C}[x]$ of $x^j y$, so that $x^j y - P_j$ is holomorphic at ∞'. In this way we obtain the basis

$$1,\ y - P_0,\ xy - P_1,\ \dots,\ x^{m-(g+1)}y - P_{m-(g+1)} \tag{6.3.5}$$

for $\mathscr{L}(m\infty)$.

Example 6.3.6. We now illustrate the above procedure. Consider the passport $(2, G, (6^1, 6^1, 3^2))$, where $G := 2A_4(6) \simeq A_4 \times C_2$. The passport (and pointed passport) are size 1, with representative triple

$$\sigma_0 = (1\ 6\ 2\ 4\ 3\ 5), \quad \sigma_1 = (1\ 3\ 5\ 4\ 6\ 2), \quad \sigma_\infty = (1\ 3\ 5)(2\ 4\ 6). \tag{6.3.7}$$

Computing the coordinate functions x, y as in (6.2.2) to 50 digits (displaying 5), we find approximate series

$$\begin{aligned} x &\approx 0.99999w^{-1} - 0.79370w - 0.31498w^3 + O(w^4), \\ y &\approx -0.99999w^{-3} - 0.79370w^{-1} - 0.94494w - 0.02142w^3 + O(w^4). \end{aligned} \tag{6.3.8}$$

Since the series for y has a pole of order $3 = g + 1$, we are in the case of an even model. Forming the matrix of coefficients of the monomials

$$1, x, x^2, x^3, x^4, x^5, x^6, y, xy, x^3y, y^2, \tag{6.3.9}$$

we find a hyperelliptic equation as in (6.1.1) with $u = 0$ and

$$v \approx 1.00000x^6 + 6.34960x^4 + 15.11905x^2 + 11.99999. \tag{6.3.10}$$

This gives the local expansion

$$\begin{aligned} y = \sqrt{v(1/t)} &= \sqrt{1.00000t^{-6} + 6.34960t^{-4} + 15.11905t^{-2} + 11.99999} \\ &= 1.00000t^{-3} + 3.17480t^{-1} + 2.51984t - 1.99999t^3 + O(t^4). \end{aligned} \tag{6.3.11}$$

Thus the Laurent tail of y is $1.00000x^3 + 3.17480x$, and the first nonconstant element of our basis for $\mathscr{L}(m\infty)$ for $m \geq 3$ is

$$y - (1.00000x^3 + 3.17480x) \approx -2.00000w^{-3} - 1.58740w^{-1} + 0.62996w - 0.04285w^3 + O(w^4) \tag{6.3.12}$$

and we can compute the remaining elements of the basis similarly. Proceeding as explained above, we obtain the Belyi map

$$\phi(x, y) = \frac{x^4 + 2x^2 + xy + 1}{2(x^2+1)^2} \tag{6.3.13}$$

defined on the hyperelliptic curve $X : y^2 = x^6 + 4x^4 + 6x^2 + 3$.

passport	size	precision (Newton)	CPU time
$(0, A_9, (5^1 2^2, 3^3, 4^1 2^1 1^3))$	2	20 (1000)	7 s
$(0, S_9, (7^1 2^1, 4^1 2^1 1^3, 4^1 2^2 1^1))$	23	20 (16000)	2 m 46 s
$(1, A_7, (7^1, 3^1 2^2, 3^1 2^2))$	2	30 (1000)	23 s
$(1, S_7, (5^1 2^1, 5^1 2^1, 3^1 2^2))$	4	40 (1500)	2 m 48 s
$(1, A_7, (7^1, 4^1 2^1 1^1, 4^1 2^1 1^1))$	22	20 (1500)	10 s
$(2, \mathrm{GL}_3(\mathbb{F}_2), (7^1, 7^1, 3^2 1^1))$	4	20	4 m 59 s

Approximate CPU time for computing one Belyi map in the listed passport.

7. Database

7.1. ***Technical description.*** Our database is organized by passports as computed in Algorithm 2.3.1. For each passport we store basic information such as degree, genus, ramification indices, and the monodromy group. We also store the automorphism group and passport representatives, as well as their pointed counterparts. After computing equations for every Belyi map in a passport, we store the Belyi maps, curves, the fields over which they are defined, and the associated complex embedding. We then partition the pointed passport representatives into Galois orbits obtained from this information. Lastly, the numerical power series and information to recover the normalization in Section 3.1 Step 4 are also saved.

7.2. ***Running time.*** Since our numerical method for computing equations sometimes requires a workaround for corner cases, we do not have detailed information about the total running time. To give a rough idea of the running time, we consider some examples. In the table above we list the approximate CPU time to compute *one* Belyi map in the listed passport, with power series computed to the specified number of decimal digits of precision and then precision obtained in Newton iteration.

The current database of Belyi maps consists of approximately 240MB of text files.

7.3. ***Observations.*** Having completed a large scale computation of Belyi maps, it remains to analyze our data.

- The largest passport sizes in each degree are:

degree	≤ 4	5	6	7	8	9	10	11
passport size	1	3	8	38	177	1260	8820	72572

(7.3.1)

- The largest degree number field arising as a field of definition of a Belyi map in our database occurs for the passport $(1, S_7, (6^1 1^1, 6^1 1^1, 4^1 2^1 1^1))$, which is irreducible of size 32. This degree-32 number field has discriminant $2^{68} 3^{27} 5^9 7^{15}$ and Galois group $\mathbb{Z}/2\mathbb{Z} \wr S_{16}$.

- The passport $(2, A_7, (7^1, 7^1, 5^1 1^1 1^1))$ provides an example of a highly reducible passport: it has size 24 and decomposes into six Galois orbits of sizes 1, 2, 3, 4, 6, and 8. The associated number fields are $\mathbb{Q}$,

and those with defining polynomials

$$x^2 - x - 5, \quad x^3 + 2x - 2, \quad x^4 - 2x^3 - 2x^2 + 3x - 3, \quad x^6 - 2x^4 - 5x^3 - 2x^2 + 1,$$
$$\text{and} \quad x^8 - 4x^7 + 14x^5 - 35x^4 + 42x^3 - 126x^2 + 108x + 135.$$

• There are 262 passports with degree $d \leq 7$. We have computed equations for all Belyi maps in 255 of these passports and found that 37 are reducible. For a passport $\mathcal{P}$ of size l, the Galois action determines a partition of l with parts $l_1, \ldots, l_r$. To measure the irreducibility of $\mathcal{P}$, define

$$\mathrm{w}(\mathcal{P}) := \begin{cases} 1 & \text{if } l = 1, \\ (l-1)^{-2} \sum_{i=1}^{r} (l_i - 1)^2 & \text{if } l \geq 2. \end{cases} \tag{7.3.2}$$

Let $\mathscr{P}_d$ be the set of passports with degree no larger than d and define

$$\beta(d) := (\#\mathscr{P}_d)^{-1} \sum_{\mathcal{P} \in \mathscr{P}_d} \mathrm{w}(\mathcal{P}). \tag{7.3.3}$$

From the database we find that $\beta(d) = 1$ for $d \leq 4$, $\beta(5) \approx 0.9393$, $\beta(6) \approx 0.9444$, and $0.8779 < \beta(7) < 0.9046$.

Acknowledgements

The authors would like to thank Hartmut Monien and Greg Warrington for useful conversations; Mauricio Esquivel Rogel for his implementation of some numerical linear algebra routines, supported by a James O. Freedman Presidential Scholarship; and Joshua Perlmutter for help in verification. Thanks also to Maarten Derickx, Noam Elkies, and David P. Roberts for comments. Our calculations are performed in the computer algebra system Magma [6]. Voight was supported by an NSF CAREER Award (DMS-1151047) and a Simons Collaboration Grant (550029).

References

[1] N. M. Adrianov, N. Y. Amburg, V. A. Dremov, Y. Y. Kochetkov, E. M. Kreines, Y. A. Levitskaya, V. F. Nasretdinova, and G. B. Shabat, *Catalog of dessins d'enfants with no more than* 4 *edges*, J. Math. Sci. **158** (2009), no. 1, 22–80.

[2] G. V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Math. USSR-Izv. **14** (1980), 247–256.

[3] J. Bétréma, D. Péré, and A. Zvonkin, *Plane trees and their Shabat polynomials*, catalog 92-75, Lab. Bordelais Recherche Informatique, 1992.

[4] Bryan Birch, *Noncongruence subgroups, covers and drawings*, The Grothendieck theory of dessins d'enfants (Luminy, 1993), London Math. Soc. Lecture Note Ser., no. 200, Cambridge Univ. Press, 1994, pp. 25–46. MR 1305392

[5] Sownak Bose, James Gundry, and Yang-Hui He, *Gauge theories and dessins d'enfants: beyond the torus*, J. High Energy Phys. **2015** (2015), no. 1, art. id. 135.

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

[7] Pierre Dèbes and Michel Emsalem, *On fields of moduli of curves*, J. Algebra **211** (1999), no. 1, 42–56. MR 1656571

[8] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, Galois groups over $\mathbb{Q}$ (Berkeley, 1987), Math. Sci. Res. Inst. Publ., no. 16, Springer, 1989, pp. 79–297. MR 1012168

[9] A. Elkin, *Beyli-Maps*, github repository, https://github.com/arsenelkin/Belyi-Maps.

[10] Ariyan Javanpeykar and John Voight, *The Belyi degree is computable*, preprint, 2017. arXiv 1711.00125

[11] 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** (2014), no. 1, 379–430. MR 3356040

[12] Gunter Malle, *Fields of definition of some three point ramified field extensions*, The Grothendieck theory of dessins d'enfants (Luminy, 1993), London Math. Soc. Lecture Note Ser., no. 200, Cambridge Univ. Press, 1994, pp. 147–168. MR 1305396

[13] Hartmut Monien, *The sporadic group J_2, Hauptmodul and Belyĭ map*, preprint, 2017. arXiv 1703.05200

[14] ———, *The sporadic group* Co_3*, Hauptmodul and Belyĭ map*, preprint, 2018. arXiv 1802.06923

[15] J. Sijsling and J. Voight, *On computing Belyi maps*, Publ. Math. Besançon **2014** (2014), no. 1, 73–131. MR 3362631

[16] Jeroen Sijsling and John Voight, *On explicit descent of marked curves and maps*, Res. Number Theory **2** (2016), art. id. 27. MR 3582054

[17] André Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524. MR 0082726

Received 28 Feb 2018. Revised 20 Sep 2018.

MICHAEL MUSTY: michaelmusty@gmail.com
Department of Mathematics, Dartmouth College, Hanover, NH, United States

SAM SCHIAVONE: sam.schiavone@gmail.com
Department of Mathematics, Dartmouth College, Hanover, NH, United States

JEROEN SIJSLING: jeroen.sijsling@uni-ulm.de
Universität Ulm, Institut für Reine Mathematik, Ulm, Germany

JOHN VOIGHT: jvoight@gmail.com
Department of Mathematics, Dartmouth College, Hanover, NH, United States

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

The cover image is based on a design by Linh Chi Bui.

The contents of this work are copyrighted by MSP or the respective authors. All rights reserved.

Electronic copies can be obtained free of charge from http://msp.org/obs/2 and printed copies can be ordered from MSP (contact@msp.org).

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

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

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine