ON COMPUTING BELYI MAPS

par

Jeroen Sijsling & John Voight

Résumé. — We survey methods to compute three-point branched covers of the projective line, also known as Belyĭ maps. These methods include a direct approach, involving the solution of a system of polynomial equations, as well as complex analytic methods, modular forms methods, and p-adic methods. Along the way, we pose several questions and provide numerous examples.

Nous donnons un aperçu des méthodes actuelles pour le calcul des revêtements de la droite projective ramifiés sur au plus trois points, aussi appelés les morphismes de Belyĭ. Ces méthodes comprennent une approche directe, qui revient à la solution d'un système d'équations polynomiales, ainsi que des méthodes analytiques complexes, méthodes de formes modulaires, et méthodes p-adiques. En chemin, nous posons quelques questions et donnons de nombreux exemples.

Table des matières

Introduction

Every compact Riemann surface X is an algebraic curve over $\mathbb{C}$, and every meromorphic function on X is an algebraic function. This remarkable fact, generalized in the GAGA principle, links the analytic with the algebraic in a fundamental way. A natural problem is then to link this further with arithmetic; to characterize those Riemann surfaces that can be defined by equations over $\overline{\mathbb{Q}}$ and to study the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on these algebraic curves. To this end, Belyĭ [**12, 13**] proved that a Riemann

surface X over $\mathbb{C}$ can be defined over $\overline{\mathbb{Q}}$ if and only if X admits a Belyĭ map, a map $f : X \to \mathbb{P}^1_{\mathbb{C}}$ that is unramified away from $\{0, 1, \infty\}$. Grothendieck, in his *Esquisse d'un Programme* [**62**], called this result "deep and disconcerting."

Part of Grothendieck's fascination with Belyĭ's theorem was a consequence of the simple combinatorial and topological characterization that follows from it. Given a Belyĭ map $f : X \to \mathbb{P}^1_{\mathbb{C}}$, the preimage $f^{-1}([0, 1])$ of the real interval $[0, 1]$ can be given the structure of a dessin (or dessin d'enfant, "child's drawing"): a connected graph with bicolored vertices (so the two vertices of an edge are colored differently) equipped with a cyclic ordering of the edges around each vertex. Conversely, a dessin determines the corresponding Belyĭ map uniquely up to isomorphism over $\mathbb{C}$ or $\overline{\mathbb{Q}}$. The idea that one can understand the complicated group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by looking at children's pictures casts an alluring spell indeed. As a consequence, hundreds of papers have been written on the subject, several books have appeared, and the topic remains an active area of research with many strands.

In a number of these papers, computation of particular examples plays a key role in understanding phemonena surrounding Belyĭ maps; arguably, part of the richness of the subject lies in the beauty in these examples. Shabat and Voevodsky [**144**, 0.1.1, 0.3] say on this point:

> Here we have no general theory and only give a number of examples. The completeness of our results decrease rapidly with growing genus; we are able to give some complete lists (of non-trivial experimental material) for genus 0, but for genera exceeding 3 we are able to give only some general remarks. [...] The main reasons to publish our results in the present state is our eagerness to invite our colleagues into the world of the divine beauty and simplicity we have been living in since we have been guided by the Esquisse.

In spite of this important role, no survey of computational methods for Belyĭ maps has yet appeared, and in our own calculations we found many techniques, shortcuts, and some tricks that others had also (re)discovered. In this article, we collect these results in one place in the hope that it will be useful to others working in one of the many subjects that touch the theory of Belyĭ maps. We also give many examples; to our knowledge, the larger examples are new, unless mentioned otherwise. We assume that the reader has some familiarity with algebraic curves and with computation, but not necessarily with the theory of Belyĭ maps or dessins; at the same time, we hope that this paper will also be a useful and comprehensive reference, so we will also make some remarks for the experts.

We take as input to our methods the simple group theoretic description of Belyĭ maps: there is a bijection between permutation triples

$$\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3 \text{ that satisfy } \sigma_0\sigma_1\sigma_\infty = 1$$

up to simultaneous conjugation in the symmetric group S_d, and

$$\text{Belyĭ maps } f : X \to \mathbb{P}^1 \text{ of degree } d$$

up to isomorphism over $\overline{\mathbb{Q}}$. In this bijection, the curve X can be disconnected, such as the trivial cover of degree $d > 1$; the cover X is connected if and only if (the dessin is connected if and only if) the corresponding permutation triple σ generates a transitive subgroup of S_d, in which case we call σ transitive. If σ corresponds to f in this bijection, we say that f has monodromy representation σ.

Given the description of a Belyĭ map f in the compressed form of a permutation triple, it has proven difficult in general to determine explicitly an algebraic model for f and the curve X. As a result, many authors have written on this subject of explicit computation

of Belyĭ maps, usually subject to certain constraints or within a certain class of examples. That this is a difficult problem is a common refrain, and the following quote by Magot and Zvonkin [**106**, §1] is typical:

> An explicit computation of a Belyi function corresponding to a given map is reduced to a solution of a system of algebraic equations. It may turn out to be extremely difficult. To give an idea of the level of difficulty, we mention that our attempts to compute Belyi functions for some maps with only six edges took us several months, and the result was achieved only after using some advanced Gröbner bases software and numerous consultations given by its author J.C. Faugère.

The paper is organized as follows. In Section 1, we collect the basic background (including a discussion of fields of definition), and mention some applications and generalizations. In Section 2, we discuss a direct method using Gröbner methods, augmented by the Atkin–Swinnerton-Dyer trick. We then turn to other, more practical methods. We begin in Section 3 with complex analytic methods; in Section 4, we consider methods using modular forms; in Section 5, we consider p-adic methods. In Section 6, we briefly discuss alternative methods for Galois Belyĭ maps. In Section 7, we discuss the delicate subjects of field of moduli and field of definition with an eye to its implications for computation. In Section 8, we treat simplification and verification of Belyĭ maps, and finally in Section 9 we conclude by considering some further topics and generalizations. Along the way, we give explicit examples and pose several questions.

The authors would like to thank Noam Elkies, Ariyan Javanpeykar, Curtis McMullen, John McKay, David Roberts, Steffen Rohde, Sam Schiavone, Matthias Schütt, Marco Streng, Bernd Sturmfels, Mark Watkins and Bruce Westbury for their comments on this work, as well as the referee for his or her many suggestions. The first author was supported by Marie Curie grant IEF-GA-2011-299887, and the second author was supported by an NSF CAREER Award (DMS-1151047).

1. Background and applications

The subject of explicit characterization and computation of ramified covers of Riemann surfaces is almost as old as Riemann himself. Klein [**90**] and Fricke–Klein [**56**] calculated some explicit Belyĭ maps, most notably the icosahedral Galois Belyĭ map $\mathbb{P}^1 \to \mathbb{P}^1$ of degree 60 [**90**, I, 2, §13–14]. These appeared when constructing what we would today call modular functions associated with the triangle groups $\Delta(2,3,5)$ and $\Delta(2,4,5)$ (see Section 4). This in turn allowed them to find a solution to the quintic equation by using analytic functions. Around the same time, Hurwitz [**77**] was the first to consider ramified covers in some generality: besides considering covers of small degree, he was the first to give the classical combinatorical description of covers of the projective line minus a finite number of points, which would later result in Hurwitz spaces being named after him.

Continuing up to the modern day, the existing literature on Belyĭ maps with an explicit flavor is extremely rich: surveys include Birch [**18**], Jones–Singerman [**82, 83**], Schneps [**138**], and Wolfart [**172**]; textbooks include the seminal conference proceedings [**139**], work of Malle–Matzat [**107**], Serre [**142**], and Völklein [**165**], mainly with an eye toward applications to inverse Galois theory, the tome on graphs on surfaces by Lando–Zvonkin [**99**], and the book by Girondo–Gonzalez-Diaz [**58**], which interweaves the subject with an introduction to Riemann surfaces.

We begin this section by reviewing basic definitions; we conclude by mentioning applications and generalizations as motivation for further study. (We postpone some subtle issues concerning fields of moduli and fields of definition until Section 7.)

Definitions, and equivalent categories. — Let K be a field with algebraic closure $\overline{K}$. An (algebraic) curve X over K is a smooth proper separated scheme of finite type over K that is pure of dimension 1.

We now define precisely the main category of this paper whose objects we wish to study. A Belyĭ map over K is a morphism $f : X \to \mathbb{P}^1$ of curves over K that is unramified outside $\{0, 1, \infty\}$. Given two Belyĭ maps $f_1, f_2 : X_1, X_2 \to \mathbb{P}^1$, a morphism of Belyĭ maps from f_1 to f_2 is a morphism $g : X_1 \to X_2$ such that $f_1 = f_2 g$. We thereby obtain a category of Belyĭ maps over K.

A curve X that admits a Belyĭ map is called a Belyĭ curve. Belyĭ [**12, 13**] proved that a curve X over $\mathbb{C}$ can be defined over $\overline{\mathbb{Q}}$ if and only if X is a Belyĭ curve. Consequently, in what follows, we may pass freely between Belyĭ maps over $\overline{\mathbb{Q}}$ and over $\mathbb{C}$: we will simply refer to both categories as the category of Belyĭ maps. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts naturally on (the objects and morphisms in) the category of Belyĭ maps (over $\overline{\mathbb{Q}}$); this action is faithful, as one can see by considering the j-invariant of elliptic curves. We denote the action by a superscript on the right, so the conjugate of a curve X over $\overline{\mathbb{Q}}$ by an automorphism $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is denoted by X^τ, and that of a Belyĭ map f by f^τ.

Let $f : X \to \mathbb{P}^1$ be a Belyĭ map of degree d. The ramification of f above $\{0, 1, \infty\}$ is recorded in its ramification type, the triple consisting of the set of ramification multiplicities above $0, 1, \infty$, respectively. Such a ramification type is therefore given by a triple of partitions of d, or alternatively by a triple of conjugacy classes in the symmetric group S_d.

Part of the beauty of subject of Belyĭ maps is the ability to pass seamlessly between combinatorics, group theory, algebraic geometry, topology, and complex analysis: indeed, one can define categories in these domains that are all equivalent. In the remainder of this subsection, we make these categories and equivalences precise; the main result is Proposition 1.2 below.

To begin, we record the ramification data, or more precisely the monodromy. A permutation triple of degree d is a triple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ such that $\sigma_0\sigma_1\sigma_\infty = 1$. Let $\sigma' = (\sigma'_0, \sigma'_1, \sigma'_\infty)$ be another such triple of degree d'. Then a morphism of permutation triples from σ to σ' is a map $t : \{1, \dots, d\} \to \{1, \dots, d'\}$ such that $t(\sigma_0(x)) = \sigma'_0(t(x))$ for all $x \in S$ and the same for σ_1, σ_∞. In particular, two permutation triples σ, σ' are isomorphic, and we write $\sigma \sim \sigma'$ and say they are simultaneously conjugate, if and only if they have the same degree $d = d'$ and there exists a $\tau \in S_d$ such that

$$\sigma^\tau = \tau^{-1}(\sigma_0, \sigma_1, \sigma_\infty)\tau = (\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau, \tau^{-1}\sigma_\infty\tau) = (\sigma'_0, \sigma'_1, \sigma'_\infty).$$

It is a consequence of the Riemann existence theorem that the category of Belyĭ maps is equivalent to the category of permutation triples. More precisely, let

$$F_2 = \langle x, y, z \mid xyz = 1 \rangle \tag{1.1}$$

be the free group on two generators. Given a group G, a finite G-set is a homomorphism $\alpha : G \to \mathrm{Sym}(S)$ on a finite set S, and a morphism between finite G-sets from α to α' is a map of sets $t : S \to S'$ such that $\alpha'(g)(t(x)) = t(\alpha(g)(x))$ for all $g \in G$ and $x \in S$. We see that giving a permutation triple is the same as giving a finite F_2-set, by mapping

$x, y, z \in F_2$ to $\sigma_0, \sigma_1, \sigma_\infty$, and that two permutation triples are isomorphic if and only if the corresponding F_2-sets are isomorphic.

Returning to covers and topological considerations, we have an isomorphism

$$F_2 \cong \pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\});$$

the generators x, y, z chosen above can be taken to be simple counterclockwise loops around $0, 1, \infty$. We abbreviate $\mathbb{P}^1_* = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. The category of finite topological covers of $\mathbb{P}^1_*$ is equivalent to the category of finite $\pi_1(\mathbb{P}^1_*)$-sets; to a cover, we associate one of its fibers, provided with the structure of $\pi_1(\mathbb{P}^1_*)$-set defined by path lifting. Therefore, a Belyĭ map gives rise to a cover of $\mathbb{P}^1_*$ by restriction, and conversely a finite topological cover of $\mathbb{P}^1_*$ can be given the structure of Riemann surface by lifting the complex analytic structure and thereby yields a map from an algebraic curve to $\mathbb{P}^1$ unramified away from $\{0, 1, \infty\}$.

Let f be a Belyĭ map, corresponding to a permutation triple σ. The corresponding F_2-set $\rho : F_2 \to S_d$ is called the monodromy representation of f, and its image is called the monodromy group of f. The monodromy group, as a subgroup of S_d, is well-defined up to conjugacy and in particular up to isomorphism, and we denote it by $G = \mathrm{Mon}(f)$. By the correspondences above, the automorphism group of a Belyĭ map is the centralizer of its monodromy group (as a subgroup of S_d).

We consider a final category, introduced by Grothendieck [**62**]. A dessin D is a triple (Γ, C, O) where:

(D1) Γ is a finite graph with vertex set V, edge set E, and vertex map $v : E \to V \times V$;
(D2) $C : V \to \{0, 1\}$ is a bicoloring of the vertices such that the two vertices of an edge are colored differently, i.e., $C(v(e)) = \{0, 1\}$ (and not a proper subset) for all edges $e \in E$; and
(D3) O is a cyclic orientation of the edges around every vertex: that is, $O = (O_0, O_1)$ is a pair of permutations in $\mathrm{Sym}(E)$ with the property that two edges e, e' are in the same orbit under O_0 if and only if the vertices $v_0(e), v_0(e')$ of e, e' colored 0 are equal, and the same with the orbit under O_1 for the vertices colored 1.

Concretely, a cycle of O_0 with common vertex v colored 0 describes the result of rotating the edges around v counterclockwise, and the same with O_1. For some examples, see e.g. Couveignes–Granboulan [**33**, p. 15–16]. Note that once the bicoloring C in (D2) is given, the possible orientations $O = (O_0, O_1)$ can be chosen to be any pair of permutations with the property that two edges e, e' are in the same orbit under O_0 (resp. O_1) if and only if the corresponding vertices marked 0 (resp. 1) coincide. A morphism of dessins is a morphism of graphs $\varphi : \Gamma \to \Gamma'$ such that φ takes the bicoloring C to C' (i.e., $C'(\varphi(v)) = C(v)$) and similarly the cyclic orientation O to O'.

The category of dessins is also equivalent to that of Belyĭ maps. Indeed, associated to a Belyĭ map f is the graph given by $f^{-1}([0, 1])$, with the bicoloring on the vertices given by f and with the cyclic ordering induced by the orientation on the Riemann surface. Conversely, given a dessin we can algebraize the topological covering induced by sewing on 2-cells as specified by the ordering O.

Dessins were introduced by Grothendieck [**62**] to study the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on Belyĭ maps through combinatorics. So far, progress has been slow, but we mention one charming result [**138**]; the Galois action is already faithful on the dessins that are trees (as graphs).

We summarize the equivalences obtained in the following proposition and refer to Lenstra [**101**] for further exposition and references.

Proposition 1.2. — *The following categories are equivalent:*

(i) *Belyĭ maps;*
(ii) *permutation triples;*
(iii) *finite F_2-sets; and*
(iv) *dessins.*

In particular, the equivalence in Proposition 1.2 yields the key bijection considered in this paper:

$$\begin{array}{c} \left\{\text{permutation triples } \sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3\right\} / \sim \\ \updownarrow 1{:}1 \\ \left\{\text{Belyĭ maps } f : X \to \mathbb{P}^1 \text{ of degree } d\right\} / \cong_{\overline{\mathbb{Q}}} \end{array} \tag{1.3}$$

where the notions of isomorphism are taken in the appropriate categories. Concretely, under the correspondence (1.3), the cycles of the permutation σ_0 (resp. σ_1, σ_∞) correspond to the points of X above 0 (resp. $1, \infty$) and the length of the cycle corresponds to the ramification index of the corresponding point under the morphism f. Note in particular that because the first set of equivalence classes in (1.3) is evidently finite, there are only finitely many $\overline{\mathbb{Q}}$-isomorphism classes of curves X with a Belyĭ map of given degree.

It is often useful, and certainly more intuitive, to consider the subcategories in Proposition 1.2 that correspond to Belyĭ maps $f : X \to \mathbb{P}^1$ whose source is connected (and accordingly, we say the map is connected). A Belyĭ map is connected if and only if the corresponding permutation triple σ is transitive, i.e., the subgroup $\langle \sigma_0, \sigma_1, \sigma_\infty \rangle$ is a transitive group. Restricting to transitive permutations gives a further equivalent category of finite index subgroups of F_2: the objects are subgroups $H \leq F_2$ of finite index and morphisms $H \to H'$ are restrictions of inner automorphisms of F_2 that map H to H'. The category of finite index subgroups of F_2 is equivalent to that of finite transitive F_2-sets (to a subgroup H of F_2, one associates the F_2-set F_2/H). Proposition 1.2 now becomes the following.

Proposition 1.4. — *The following categories are equivalent:*

(i) *connected Belyĭ maps;*
(ii) *transitive permutation triples;*
(iii) *transitive finite F_2-sets;*
(iii′) *subgroups of F_2 of finite index; and*
(iv) *dessins whose underlying graph is connected.*

Unless stated otherwise (e.g., Section 7), in the rest of this article we will assume without further mention that a Belyĭ map is *connected*; this is no loss of generality, since any disconnected Belyĭ map is the disjoint union of its connected components.

Geometric properties and invariants. — Let $f : X \to \mathbb{P}^1$ be a (connected) Belyĭ map over $\overline{\mathbb{Q}}$. If the cover f is Galois, which is to say that the corresponding extension of function fields $\overline{\mathbb{Q}}(X)/\overline{\mathbb{Q}}(\mathbb{P}^1)$ is Galois, then we call f a Galois Belyĭ map. More geometrically, this property boils down to the demand that a subgroup of $\mathrm{Aut}(X)$ act transitively on the sheets of the cover; and combinatorially, this is nothing but saying that $\mathrm{Mon}(f) \subseteq S_d$ has cardinality $\#\,\mathrm{Mon}(f) = d$. Indeed, the monodromy group of a

Belyĭ map can also be characterized as the Galois group of its Galois closure, which is the smallest Galois cover of which it is a quotient.

The genus of X can be calculated by using the Riemann–Hurwitz formula. If we define the excess $e(\tau)$ of a cycle $\tau \in S_d$ to be its length minus one, and the excess $e(\sigma)$ of a permutation to be the sum of the excesses of its constituent disjoint cycles (also known as the index of the permutation, equal to n minus the number of orbits), then the genus of a Belyĭ map of degree n with monodromy σ is

$$g = 1 - n + \frac{e(\sigma_0) + e(\sigma_1) + e(\sigma_\infty)}{2}. \tag{1.5}$$

In particular, we see that the genus of Belyĭ map is zero if and only if $e(\sigma_0) + e(\sigma_1) + e(\sigma_\infty) = 2n - 2$.

We employ exponential notation to specify both ramification types and conjugacy classes in S_d. So for example, if $d = 10$, then $3^2 2^1 1^2$ denotes both the conjugacy class of the permutation (1 2 3)(4 5)(6 7 8) and the corresponding ramification type; two points of ramification index 3, one of index 2, and two (unramified) of index 1.

The passport of a Belyĭ map $f : X \to \mathbb{P}^1$ is the triple (g, G, C) where g is the genus of X and $G \subseteq S_d$ is the monodromy group of f, and $C = (C_0, C_1, C_\infty)$ is the triple of conjugacy classes of $(\sigma_0, \sigma_1, \sigma_\infty)$ in S_d, respectively [**99**, Definition 1.1.7]. Although the genus of the Belyĭ map is determined by the conjugacy classes by equation (1.5), we still include it in the passport for clarity and ease. The size of a passport (g, G, C) is the number of equivalence classes of triples $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ such that $\langle \sigma \rangle = G$ and $\sigma_i \in C_i$ for $i = 0, 1, \infty$.

We will occasionally need slightly altered notions of passport. The ramification passport of f is the pair (g, C) with conjugacy classes in S_d. Another version of the passport will be considered in Section 7. The passport has the following invariance property [**84**].

Theorem 1.6. — *The passport and the ramification passport of a Belyĭ map are invariant under the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

One can calculate the set of isomorphism classes of permutation triples with given passport using the following lemma with $G = S_d$.

Lemma 1.7. — *Let G be a group and let C_0, C_1 be conjugacy classes in G represented by $\tau_0, \tau_1 \in G$. Then the map*

$$\begin{aligned} C_G(\tau_0) \backslash G / C_G(\tau_1) &\to \{(\sigma_0, \sigma_1) : \sigma_0 \in C_0, \sigma_1 \in C_1\} / \sim_G \\ C_G(\tau_0) g C_G(\tau_1) &\mapsto (\tau_0, g\tau_1 g^{-1}) \end{aligned}$$

is a bijection, where $C_G(\tau)$ denotes the centralizer of τ in G and $\sim_G$ denotes simultaneous conjugation in G.

The virtue of this lemma is that double-coset methods in group theory are quite efficient; by using this bijection and filtering appropriately [**91**, Lemma 1.11], this allows us to enumerate Belyĭ maps with a given passport relatively quickly up to moderate degree d. One can also estimate the size of a passport using character theory; for more on this, see Section 7.

Applications. — Having introduced the basic theory, we now mention some applications of the explicit computation of Belyĭ maps.

We began in the introduction with the motivation to uncover the mysterious nature of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on dessins following Grothendieck's *Esquisse*. Dessins of small degree tend to be determined by their passport in the sense that the set of dessins with given passport forms a full Galois orbit. However, even refined notions of passport do not suffice to distinguish Galois orbits of dessins of high degree in general: a first example was Schneps' flower [**138**, §IV, Example I]. Some further examples of distinguishing features of non-full Galois orbits have been found by Wood [**174**] and Zapponi [**175**], but it remains a challenge to determine the Galois structure for the set of dessins with given passport. Even statistics in small degree are not known yet; an important project remains to construct full libraries of dessins. The original "flipbook" of dessins, due to Bétréma–Péré–Zvonkin [**15**], contained only dessins that were plane trees but was already quite influential, and consequently systematic tabulation promises to be just as inspiring.

Further applications of the explicit study of Belyĭ maps have been found in inverse Galois theory, specifically the regular realization of Galois groups over small number fields: see the tomes of Matzat [**120**], Malle–Matzat [**107**], and Jensen–Ledet–Yui [**80**]. Upon specialization, one obtains Galois number fields with small ramification set: Roberts [**131, 132, 133**], Malle–Roberts [**112**], and Jones–Roberts [**86**] have used the specialization of three-point covers to exhibit number fields with small ramification set or root discriminant. The covering curves obtained are often interesting in their own right, spurring further investigation in the study of low genus curves (e.g., the decomposition of their Jacobian [**127**]). Finally, a Belyĭ map $f : \mathbb{P}^1 \to \mathbb{P}^1$, after precomposing so that $\{0, 1, \infty\} \subseteq f^{-1}(\{0, 1, \infty\})$, is an example of a rigid post-critically finite map, a map of the sphere all of whose critical points have finite orbits. (Zvonkin calls these maps dynamical Belyĭ functions [**176**, §6].) These maps are objects of central study in complex dynamics [**7, 129**]: one may study the associated Fatou and Julia sets.

Belyĭ maps also figure in the study of Hall polynomials, (also called Davenport-Stothers triples) which are those coprime solutions $X(t), Y(t), Z(t) \in \mathbb{C}[t]$ of the equations in polynomials

$$X(t)^3 - Y(t)^2 = Z(t)$$

with $\deg(X(t)) = 2m$, $\deg(Y(t)) = 3m$ and $\deg(Z(t)) = m + 1$. These solutions are extremal in the degree of Z and are analogues of Hall triples, i.e. integers $x, y \in \mathbb{Z}$ for which $|x^3 - y^2| = O(\sqrt{|x|})$. Hall polynomials have been studied by Watkins [**166**] and by Beukers–Stewart [**17**]; Montanus [**124**] uses the link with dessins ($X^3(t)/Y^2(t)$ is a Belyĭ map) to find a formula for the number of Hall polynomials of given degree. Hall polynomials also lead to some good families of classical Hall triples [**50**], as the following example illustrates.

Example 1.8. — Taking $m = 5$ above, one obtains the following Hall polynomials due to Birch:

$$\begin{aligned} X(t) &= \frac{1}{9}(t^{10} + 6t^7 + 15t^4 + 12t), \\ Y(t) &= \frac{1}{54}(2t^{15} + 18t^{12} + 72t^9 + 144t^6 + 135t^3 + 27), \\ Z(t) &= -\frac{1}{108}(3t^6 + 14t^3 + 27). \end{aligned}$$

Choosing $t \equiv 3 \bmod 6$, we get some decent Hall triples, notably

$$|384242766^3 - 7531969451458^2| = 14668$$
$$|390620082^3 - 7720258643465^2| = 14857$$

for $t = \pm 9$; remarkably, in both cases the constant factor $|x^3 - y^2|/\sqrt{|x|}$ is approximately equal to the tiny number 3/4.

Belyĭ maps also give rise to interesting algebraic surfaces. The Belyĭ maps of genus 0 and degree 12 (resp. 24) with ramification indices above $0, 1$ all equal to $3, 2$ correspond to elliptic fibrations of rational (resp. K3) surfaces with only 4 (resp. 6) singular fibers; given such a fibration, the associated Belyĭ map is given by taking its j-invariant. By work of Beauville [**9**] (resp. Miranda and Persson [**122**]), there are 6 (resp. 112) possible fiber types for these families. This result comes down to calculating the number of Belyĭ maps of given degrees with specified conjugacy classes with cycle type $(3, \ldots, 3)$ and $(2, \ldots, 2)$ for σ_0 and σ_1.

Especially in the degree 24 case, the explicit calculation of these Belyĭ maps is quite a challenge. By developing clever methods specific to this case, this calculation was accomplished by Beukers–Montanus [**16**]. They find 191 Belyĭ maps, exceeding the 112 ramification types determined by Miranda and Persson: this is an instance of the phenomenon mentioned above, that the passport may contain more than one Belyĭ map, so that to a given ramification triple there may correspond multiple isomorphism classes of Belyĭ maps.

One can also specialize Belyĭ maps to obtain *abc* triples: this connection is discussed by Elkies [**45**] and Frankenhuysen [**55**] to show that the *abc* conjecture implies the theorem of Faltings, and it is also considered by van Hoeij–Vidunas [**157**, Appendix D].

Modular curves and certain Shimura curves possess a natural Belyĭ map. Indeed, Elkies has computed equations for Shimura curves in many cases using only the extant structure of a Belyĭ map [**46, 47**]. Another such computation was made by Hallouin in [**65**], where a more elaborate argument using Hurwitz spaces of four-point covers is used. Explicit equations are useful in many contexts, ranging from the resolution of Diophantine equations to cryptography [**140**]. Reducing these equations modulo a prime also yields towers of modular curves that are useful in coding theory. Over finite fields of square cardinality q, work of Ihara [**78**] and Tsfasman–Vlăduţ–Zink [**155**] shows that modular curves have enough supersingular points that their total number of rational points is asymptotic with $(\sqrt{q} - 1)g$ as their genus grows; this is asymptotically optimal by work of Drinfeld–Vlăduţ [**163**]. By a construction due to Goppa [**59**], one obtains the asympotically best linear error-correcting codes known over square fields. But to construct and use these codes we need explicit equations for the curves involved. A few of these modular towers were constructed by Elkies [**49**]. There are extensions to other arithmetic triangle towers, using the theory of Shimura curves, which give other results over prime power fields of larger exponent [**41**]. For the cocompact triangle quotients, the modular covers involved are Belyĭ maps, and in fact many congruence towers are unramified (and cyclic) after a certain point, which makes them particularly pleasant to work with.

There are also applications of explicit Belyĭ maps to algebraic solutions of differential equations [**100**]: as we will see in Section 4, subgroups of finite index of triangle groups correspond to certain Belyĭ maps, and the uniformizing differential equations for these

groups (resp. their solutions) can be obtained by pulling back suitable hypergeometric differential equations (resp. hypergeometric functions). Kitaev [**89**] and Vidunas–Kitaev [**162**] consider branched covers at 4 points with all ramification but one occuring above three points ("almost Belyĭ coverings") and apply this to algebraic Painlevé VI functions. Vidunas–Filipuk [**161**] classify coverings yielding transformations relating the classical hypergeometric equation to the Heun differential equation; these were computed by van Hoeij–Vidunas [**157, 158**].

There are applications to areas farther from number theory. Eyral–Oka [**52**] explicitly use dessins (and their generalizations to covers of $\mathbb{P}^1$ branched over more than 3 points) in their classification of the fundamental groups of the complement in the projective plane of certain join-type sextic curves of the form $a\prod_i(X-\alpha_i Z) = b\prod_j(X-\beta_j Z)$. Boston [**20**] showed how three-point branched covers arise in control theory, specifically with regards to a certain controller design equation. Finally, dessins appear in physics in the context of brane tilings [**68**] and there is a moonshine correspondence between genus 0 congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, associated with some special dessins, and certain representations of sporadic groups, with connections to gauge theory [**69, 70, 71**].

2. Gröbner techniques

We now begin our description of techniques for computing Belyĭ maps. We start with the one that is most straightforward and easy to implement, involving the solutions to an explicit set of equations over $\mathbb{Q}$. For Belyĭ maps of small degree, this method works quite well, and considerable technical effort has made it work in moderate degree. However, for more complicated Belyĭ maps, it will be necessary to seek out other methods, which will be described in the sections that follow.

Direct calculation. — The direct method has been used since the first Belyĭ maps were written down, and in small examples (typically with genus 0), this technique works well enough. A large number of authors describe this approach, with some variations relevant to the particular case of interest. Shabat–Voevodsky [**144**] and Atkin–Swinnerton-Dyer [**5**] were among the first. Birch [**18**, Section 4.1] computes a table for covers of small degree and genus. Schneps [**138**, III] discusses the case of clean dessins of genus 0 and trees. Malle [**111**] computed a field of definition for many Belyĭ maps of small degree and genus 0 using Gröbner methods, with an eye toward understanding the field of definition of regular realizations of Galois groups and a remark that such fields of definition also give rise to number fields ramified over only a few very small primes. Malle–Matzat [**107**, §I.9] use a direct method to compute several Belyĭ maps in the context of the inverse Galois problem, as an application of rigidity. Granboulan studied the use of Gröbner bases for genus 0 Belyĭ maps in detail in his Ph.D. thesis [**60**]. Elkies [**46**] used this technique to compute equations for Shimura curves. Other authors who have used this method are Hoshino [**75**] (and Hoshino–Nakamura [**76**]), who computed the non-normal inclusions of triangle groups (related to the Belyĭ-extending maps of Wood [**174**]). Couveignes [**32**, §2] also gives a few introductory examples.

We explain how the method works by example in the simplest nontrivial case.

Example 2.1. — Take the transitive permutation triple $\sigma = ((1\ 2), (2\ 3), (1\ 3\ 2))$ from S_3, with passport $(0, S_3, (2^1 1^1, 2^1 1^1, 3^1))$. Since these permutations generate the full symmetric group S_3, the monodromy group of this Belyĭ map is S_3. The Riemann–Hurwitz

formula (1.5) gives the genus as

$$g = 1 - 3 + \frac{1}{2}(1 + 1 + 2) = 0.$$

So the map $f : X \cong \mathbb{P}^1 \to \mathbb{P}^1$ is given by a rational function $f(t) \in K(t)$ where $K \subset \overline{\mathbb{Q}}$ is a number field. There are two points above 0, of multiplicities $2, 1$, the same holds for 1, and there is a single point above ∞ with multiplicity 3. The point above ∞ is a triple pole of $f(t)$; since it is unique, it is fixed by $\mathrm{Gal}(\overline{K}/K)$; therefore we take this point also to be ∞, which we are free to do up to automorphisms of $\mathbb{P}^1_K$, and hence $f(t) \in K[t]$. Similarly, the ramified points above 0 and 1 are also unique, so we may take them to be 0 and 1, respectively. Therefore, we have

$$f(t) = ct^2(t + a)$$

for some $a, c \in K \setminus \{0\}$ and

$$f(t) - 1 = c(t - 1)^2(t + b)$$

for some $b \in K \setminus \{0, -1\}$. Combining these equations, we get

$$ct^2(t + a) - 1 = c(t^3 + at^2) - 1 = c(t - 1)^2(t + b) = c(t^3 + (b - 2)t^2 + (1 - 2b)t + b)$$

and so by comparing coefficients we obtain $b = 1/2$, $c = -2$, and $a = -3/2$. In particular, we see that the map is defined over $K = \mathbb{Q}$ and is unique up to $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{Q}}) \cong \mathrm{PGL}_2(\mathbb{Q})$. Thus

$$f(t) = -t^2(2t - 3) = -2t^3 + 3t^2, \quad f(t) - 1 = -(t - 1)^2(2t + 1).$$

If we relax the requirement that the ramification set be $\{0, 1, \infty\}$ and instead allow $\{0, r, \infty\}$ for some $r \neq 0, \infty$, then the form of f can be made more pleasing. For example, by taking $f(t) = t^2(t + 3)$ and $r = 4$ we obtain $f(t) - 4 = (t - 1)^2(t + 2)$.

It is hopefully clear from this example (see Schneps [**138**, Definition 8]) how to set up the corresponding system of equations for a Belyĭ map on a curve of genus $g = 0$: with variable coefficients, we equate the two factorizations of a rational map with factorization specified by the cycle types in the permutations triple σ. We illustrate this further in the following example; for a large list of examples of this kind, see Lando–Zvonkin [**99**, Example 2.3.1].

Example 2.2. — To get a small taste of how complicated the equations defining a passport can get, consider the case $G = \mathrm{PGL}_2(\mathbb{F}_7)$ with permutation triple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ given by

$$\sigma_0 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \quad \sigma_\infty = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

The permutation representation of G acting on the set of 8 elements $\mathbb{P}^1(\mathbb{F}_7)$ is given by the elements

$$(1\ 6)(2\ 5)(3\ 4), \quad (0\ \infty\ 1)(2\ 4\ 6), \quad (0\ 1\ 4\ 3\ 2\ 5\ 6\ \infty).$$

The corresponding degree 8 Belyĭ map $f : X \to \mathbb{P}^1$ has passport

$$(0, \mathrm{PGL}_2(\mathbb{F}_7), (2^3 1^2, 3^2 1^2, 8^1)).$$

After putting the totally ramified point at ∞, the map f is given by a polynomial $f(t) \in \overline{\mathbb{Q}}[t]$ such that

$$f(t) = ca(t)^2 b(t) \quad \text{and} \quad f(t) - 1 = cd(t)^3 e(t) \tag{2.3}$$

where $c \in \overline{\mathbb{Q}}^\times$ and $a(t), b(t), d(t), e(t) \in \overline{\mathbb{Q}}[t]$ are monic squarefree polynomials with $\deg a(t) = 3$ and $\deg b(t) = \deg d(t) = \deg e(t) = 2$. We write $a(t) = t^3 + a_2 t^2 + a_1 t + a_0$, etc.

Equating coefficients in (2.3) we obtain the following system of 8 vanishing polynomials in 10 variables:

$$\begin{aligned}
&a_0^2 b_0 c - c d_0^3 e_0,\\
&2a_1 a_0 b_0 c + a_0^2 b_1 c - 3c d_1 d_0^2 e_0 - c d_0^3 e_1,\\
&2a_2 a_0 b_0 c + a_1^2 b_0 c + 2a_1 a_0 b_1 c + a_0^2 c - 3c d_1^2 d_0 e_0 - 3c d_1 d_0^2 e_1 - c d_0^3 - 3c d_0^2 e_0,\\
&2a_2 a_1 b_0 c + 2a_2 a_0 b_1 c + a_1^2 b_1 c + 2a_1 a_0 c + 2a_0 b_0 c - c d_1^3 e_0 - 3c d_1^2 d_0 e_1 - 3c d_1 d_0^2\\
&\qquad - 6c d_1 d_0 e_0 - 3c d_0^2 e_1,\\
&a_2^2 b_0 c + 2a_2 a_1 b_1 c + 2a_2 a_0 c + a_1^2 c + 2a_1 b_0 c + 2a_0 b_1 c - c d_1^3 e_1 - 3c d_1^2 d_0 - 3c d_1^2 e_0\\
&\qquad - 6c d_1 d_0 e_1 - 3c d_0^2 - 3c d_0 e_0,\\
&a_2^2 b_1 c + 2a_2 a_1 c + 2a_2 b_0 c + 2a_1 b_1 c + 2a_0 c - c d_1^3 - 3c d_1^2 e_1 - 6c d_1 d_0 - 3c d_1 e_0 - 3c d_0 e_1,\\
&a_2^2 c + 2a_2 b_1 c + 2a_1 c + b_0 c - 3c d_1^2 - 3c d_1 e_1 - 3c d_0 - c e_0,\\
&2a_2 c + b_1 c - 3c d_1 - c e_1.
\end{aligned}$$

Using a change of variables $t \leftarrow t - r$ with $r \in \overline{\mathbb{Q}}$ we may assume that $b_1 = 0$, so $b_0 \neq 0$. Note that if $f(t) \in K[t]$ is defined over K then we may take $r \in K$, so we do not unnecessarily increase the field of definition of the map. Similarly, if $d_1 \neq 0$, then with $t \leftarrow ut$ and $u \in K^\times$ we may assume $d_1 = b_0$; similarly if $e_1 \neq 0$, then we may take $e_1 = b_0$. If $d_1 = e_1 = 0$, then $f(t) = g(t^2)$ is a polynomial in t^2, whence $a_0 = 0$ so $a_1 \neq 0$, and thus we may take $a_1 = b_0$. This gives a total of three cases: (i) $d_1 = b_0 \neq 0$, (ii) $d_1 = 0$ and $e_1 = b_0 \neq 0$, and (iii) $d_1 = e_1 = 0$ and $a_1 = b_0 \neq 0$. We make these substitutions into the equations above, adding $c \neq 0$ and $b_1 = 0$ in all cases. Note that the equation $c \neq 0$ can be added algebraically by introducing a new variable c' and adding the equation $cc' = 1$.

These equations are complicated enough that they cannot be solved by hand, but not so complicated that they cannot be solved by a Gröbner basis. There are many good references for the theory of Gröbner bases [**1, 34, 35, 64, 97**].

In the degenerate cases (ii) and (iii) we obtain the unit ideal, which does not yield any solutions. In the first case, we find two conjugate solutions defined over $\mathbb{Q}(\sqrt{2})$. After some simplification, the first of the solutions becomes

$$f(t) = \big(2\sqrt{2}t^3 - 2(2\sqrt{2}+1)t^2 + (-4+7\sqrt{2})t + 1\big)^2 \big(14t^2 + 6(\sqrt{2}+4)t - 8\sqrt{2} + 31\big)$$

with

$$f(t) - 432(4\sqrt{2} - 5) = \big(2t^2 - 2\sqrt{2} + 1\big)^3 \big(14t^2 - 8(\sqrt{2}+4)t - 14\sqrt{2} + 63\big).$$

The direct method does not give an obvious way to discriminate among Belyĭ maps by their monodromy groups, let alone to match up which Galois conjugate corresponds to which monodromy triple: all covers with a given ramification type are solutions to the above system of equations.

To set up a similar system of equations in larger genus $g \geq 1$, one can for example write down a general (singular) plane curve of degree equal to $\deg \varphi$ and ask that have sufficiently many nodal singularities so that it has geometric genus g; the Belyĭ map can then be taken as one of the coordinates, and similar techniques apply, though many non-solutions will still be obtained in this way by cancellation of numerator and denominator.

Remark 2.4. — Any explicitly given quasiprojective variety X with a surjective map to the moduli space $\mathcal{M}_g$ of curves of genus g will suffice for this purpose; so for those genera g where the moduli space $\mathcal{M}_g$ has a simpler representation (such as $g \leq 3$), one can use this representation instead. The authors are not aware of any Belyĭ map computed in this way with genus $g \geq 3$.

The direct method can be used to compute the curves X with Belyĭ maps of small degree. The curve $\mathbb{P}^1$ is the only curve with a Belyĭ map of degree 2 (the squaring map), and the only other curve that occurs in degree 3 is the genus 1 curve with j-invariant 0 and equation $y^2 = x^3 + 1$, for which the Belyĭ map is given by projecting onto the y-coordinate. In degree 4, there is the elliptic curve of j-invariant 1728 with equation $y^2 = x^3 - x$ with Belyĭ map given by x^2 and one other given by the the elliptic curve $y^2 = 4(2x + 9)(x^2 + 2x + 9)$ and regular function $y + x^2 + 4x + 18$. Both were described by Birch [**18**].

In the direction of tabulating the simplest dessins in this way, all clean dessins (i.e. those for which all ramification indices above 1 are equal to 2) with at most 8 edges were computed by Adrianov et al. [**2**]. Magot–Zvonkin [**106**] and Couveignes–Granboulan [**33**] computed the genus 0 Belyĭ maps corresponding to the Archimedean solids, including the Platonic solids, using symmetry and Gröbner bases. For a very complete discussion of trees and Shabat polynomials and troves of examples, see Lando–Zvonkin [**99**, §2.2].

In general, we can see that these Gröbner basis techniques will present significant algorithmic challenges. Even moderately-sized examples, including all but the first few of genus 1, do not terminate in a reasonable time. (In the worst case, Gröbner basis methods have running time that is doubly exponential in the input size, though this can be reduced to singly exponential for zero-dimensional ideals; see the surveys of Ayad [**6**] and Mayr [**116**].) One further differentiation trick, which we introduce in the next section, allows us to compute in a larger range. However, even after this modification, another obstacle remains: the set of solutions can have positive-dimensional degenerate components. These components correspond to situations where roots coincide or there is a common factor and are often called parasitic solutions [**95, 96**]. The set of parasitic solutions have been analyzed in some cases by van Hoeij–Vidunas [**158**, §2.1], but they remain a nuisance in general (as can be seen already in Example 2.2 above).

Remark 2.5. — Formulated more intrinsically, the naive equations considered in this section determine a scheme in the coefficient variables that is a naive version of the Hurwitz schemes that will be mentioned in Section 9. Besides containing degenerate components, this naive scheme is usually very non-reduced. We will revisit this issue in Remark 2.10.

When calculating a Belyĭ map $f : \mathbb{P}^1 \to \mathbb{P}^1$, one usually fixes points on the source and the target. As we saw most elaborately when working out equation (2.3), this reduces the problem of calculating a Belyĭ map in genus 0 to finding the points on an affine scheme. The families of solutions in which numerator and denominator cancel give rise to some of the degenerate components mentioned in the previous paragraph.

The ASD differentiation trick. — There is a trick, attributed to Atkin–Swinnerton-Dyer [**5**, §2.4] (also appearing on the Putnam exam in 1956, predating Atkin and Swinnerton-Dyer) that uses the derivative of f to eliminate a large number of the indeterminates ("the number of unknowns c can be cut in half at once by observing that $dj/d\zeta$ has factors $F_3^2F_2$"). Couveignes [**32**] implies that this trick was known to Fricke; it has apparently been rediscovered many times. Hempel [**73**, §3] used differentiation by hand to classify subgroups of $\mathrm{SL}_2(\mathbb{Z})$ of genus 0 with small torsion and many cusps. Couveignes [**29**, §2,§10] used this to compute examples in genus 0 of clean dessins. Schneps [**138**, §III] used this trick to describe a general approach in genus 0. Finally, Vidunas [**160**] applied the trick to differential equations, and Vidunas–Kitaev [**162**] extended this to covers with 4 branch points.

Example 2.6. — Again we illustrate the method by an example. Take

$$\sigma = ((1\ 2), (2\ 4\ 3), (1\ 2\ 3\ 4))$$

with passport $(0, S_4, (2^1 1^2, 3^1 1^1, 4^1))$. Choosing the points 0 and 1 again to be ramified, this time of degrees $2, 3$ above $0, 1$ respectively, and choosing ∞ to be the ramified point above ∞, we can write

$$f(t) = ct^2(t^2 + at + b)$$

and

$$f(t) - 1 = c(t-1)^3(t+d).$$

The trick is now to differentiate these relations, which yields

$$\begin{aligned} f'(t) = ct\left(2(t^2 + at + b) + t(2t + a)\right) &= c(t-1)^2\left((t-1) + 3(t+d)\right) \\ t(4t^2 + 3at + 2b) &= (t-1)^2\left(4t + (3d-1)\right). \end{aligned}$$

By unique factorization, we must have $4t^2 + 3at + 2b = 4(t-1)^2$ and $4t = 4t + (3d-1)$, so we instantly get $a = -8/3$, $b = 2$, and $d = 1/3$. Substituting back we see that $c = 3$, and obtain

$$f(t) = t^2(3t^2 - 8t + 6) = (t-1)^3(3t+1) + 1.$$

More generally, the differentiation trick is an observation on divisors that extends to higher genus, as used by Elkies [**47**] in genus $g = 1$.

Lemma 2.7. — *Let $f : X \to \mathbb{P}^1$ be a Belyĭ map with ramification type σ. Let*

$$\operatorname{div} f = \sum_P e_P P - \sum_R e_R R \quad \textit{and} \quad \operatorname{div}(f-1) = \sum_Q e_Q Q - \sum_R e_R R$$

be the divisors of f and $f-1$. Then the divisor of the differential df is

$$\operatorname{div} df = \sum_P (e_P - 1)P + \sum_Q (e_Q - 1)Q - \sum_R (e_R + 1)R.$$

Démonstration. — Let

$$D = \sum_P (e_P - 1)P + \sum_Q (e_Q - 1)Q - \sum_R (e_R + 1)R.$$

Then $\operatorname{div} df \geq D$ by the Leibniz rule. By Riemann–Hurwitz, we have

$$2g-2 = -2n + \sum_P (e_P - 1) + \sum_Q (e_Q - 1) + \sum_R (e_R - 1)$$

so

$$\deg(D) = 2g - 2 + 2n - 2\sum_R e_R = 2g - 2$$

since $\sum_R e_R = n$. Therefore $\operatorname{div} df$ can have no further zeros. □

Combined with unique factorization, this gives the following general algorithm in genus 0. Write

$$f(t) = \frac{p(t)}{q(t)} = 1 + \frac{r(t)}{q(t)}$$

for polynomials $p(t), q(t), r(t) \in \overline{\mathbb{Q}}[t]$. Consider the derivatives $p'(t), q'(t), r'(t)$ with respect to t and let $p_0(t) = \gcd(p(t), p'(t))$ and similarly $q_0(t), r_0(t)$. Write

$$P(t) = \frac{p(t)}{p_0(t)} \text{ and } \widetilde{P}(t) = \frac{p'(t)}{p_0(t)}$$

and similarly Q, etc. Then by unique factorization, and the fact that P, Q, R have no common divisor, evaluation of the expressions $p(t) - q(t) = r(t)$ and $p'(t) - q'(t) = r'(t)$ yields that $Q(t)\widetilde{R}(t) - \widetilde{Q}(t)R(t)$ is a multiple of $p_0(t)$, and similarly $P(t)\widetilde{R}(t) - \widetilde{P}(t)R(t)$ (resp. $P(t)\widetilde{Q}(t) - \widetilde{P}(t)Q(t)$) is a multiple of $q_0(t)$ (resp. $r_0(t)$).

These statements generalize to higher genus, where they translate to inclusions of divisors; but the usefulness of this for concrete calculations is limited and do not pass to relations of functions, since the coordinate rings of higher genus curves are usually not UFDs. Essentially, one has to be in an especially agreeable situation for a statement on functions to fall out, and usually one only has a relation on the Jacobian (after taking divisors, as in the lemma above). A concrete and important situation where a relation involving functions does occur is considered by Elkies [**47**]. The methods in his example generalize to arbitrary situations where the ramification is uniform (all ramification indices equal) except at one point of the Belyĭ curve: Elkies himself treats the Belyĭ maps with passport $(1, \mathrm{PSL}_2(\mathbb{F}_{27}), (3^9 1^1, 2^{14}, 7^4))$.

The differentiation trick does not seem to generalize extraordinarily well to higher derivatives; we can repeat the procedure above and further differentiate $p'(t), q'(t), r'(t)$, but experimentally this not seem to make the ideal grow further than in the first step.

Question 2.8. — *Is the ideal obtained by adding all higher order derivatives equal to the one obtained from just adding equations coming from first order derivatives (in genus 0)?*

However, Shabat [**143**, Theorem 4.4] does derive some further information by considering second-order differentials; and Dremov [**40**] calculates Belyĭ maps using the quadratic differential

$$MP(f) = \frac{df^2}{f(1-f)}$$

for a regular function f and considering the equalities following from the relation

$$MP(f^{-1}) = -MP(f)/f.$$

It is not immediately clear from these paper how to use this strategy in general, though.

Question 2.9. — *How generally does the method of considering second-order differentials apply?*

The additional equations coming from the differentiation trick not only speed up the process of calculating Belyĭ maps, but they also tend to give rise to a Jacobian matrix at a solution that is often of larger rank than the direct system. This is important when trying to Hensel lift a solution obtained over $\mathbb{C}$ or over a finite field, where the non-singularity of the Jacobian involved is essential. (We discuss these methods in sections that follow.)

Remark 2.10. — Phrased in the language of the naive moduli space in Remark 2.5, the additional ASD relations partially saturate the corresponding equation ideal, so that the larger set of equations defines the same set of geometric points, but with smaller multiplicities. (We thank Bernd Sturmfels for this remark.) Reducing this multiplicity all the way to 1 is exactly the same as giving the Jacobian mentioned above full rank.

Example 2.11. — The use of this trick for reducing multiplicities is best illustrated by some small examples.

The first degree d in which the ASD differentiation trick helps to give the Jacobian matrix full rank is $d = 6$; it occurs for the ramification triples $(2^3, 2^3, 3^2)$, $(2^2 1^2, 3^2, 4^1 2^1)$, $(3^2, 3^1 2^1 1, 3^1 2^1 1^1)$, $(3^1 1^3, 4^1 2^1, 4^1 2^1)$, $(4^1 2^1, 4^1 1^2, 3^1 2^1 1^1)$, and $(4^1 2^1, 3^1 2^1 1^1, 3^1 2^1 1^1)$, where it reduces the multiplicity of the corresponding solutions from $9, 3, 3, 3, 4, 3$ respectively to 1. Note the tendency of Belyĭ maps with many automorphisms to give rise to highly singular points, as for curves with many automorphisms in the corresponding moduli spaces.

On the other hand, there are examples where even adding the ASD relations does not lead to a matrix of full rank. Such a case is first found in degree 7; it corresponds to the ramification triples $(4^1 2^1 1^1, 3^1 2^1 1^2, 4^1 3^1)$, and throwing in the ASD relations reduces the multiplicity from 8 to 2. Unfortunately, iterating the trick does not make the ideal grow further in this case.

More dramatically, for the ramification triples $(2^4, 3^2 2^1, 3^2 2^1)$ and $(2^3 1^2, 4^2, 3^2 2^1)$, differentiation reduces some multiplicities from 64 to 1 (resp. 64 to 4). In the latter case, these multiplicities are in fact not determined uniquely by the corresponding ramification type, so that considering these multiplicities gives a way to split the solutions into disjoint Galois orbits.

Question 2.12. — *How close is the ideal obtained from the differentiation trick (combined with the direct method) to being radical? Can one give an upper bound for the multiplicity of isolated points?*

Further extensions. — There can be several reasons why a Gröbner basis calculation fails to terminate. One problem is coefficient blowup while calculating the elimination ideals. This can be dealt by first reducing modulo a suitable prime p, calculating a Gröbner basis for the system modulo p, then lifting the good solutions (or the Gröbner basis itself) p-adically, recognizing the coefficients as rational numbers, and then verifying that the basis over $\mathbb{Q}$ is correct. This was used by Malle [**110, 113**] to compute covers with passports $(0, \mathrm{Hol}(E_8), (4^1 2^1 1^2, 4^1 2^1 1^2, 6^1 2^1))$ and $(0, \mathrm{PGL}(\mathbb{F}_{11}), (2^5 1^2, 4^3, 11^1 1^1))$ and similarly Malle–Matzat [**108**] to compute covers for $(0, \mathrm{PSL}_2(\mathbb{F}_{11}), (2^4 1^3, 6^1 3^1 2^1, 6^1 3^1 2^1))$ and $(0, \mathrm{PSL}_2(\mathbb{F}_{13}), (2^7, 4^3 1^2, 6^2 1^2))$. This idea was also used by Vidunas–Kitaev [**162**, §5].

For further developments on p-adic methods to compute Gröbner bases, see Arnold [**4**] or Winkler [**169**]. One can also lift a solution modulo p directly, and sometimes such solutions can be obtained relatively quickly without also p-adically lifting the Gröbner bases: this is the basic idea presented in Section 5.

In the work of van Hoeij–Vidunas [**157, 158**] mentioned in Section 1, genus 0 Belyĭ functions are computed by using pullbacks of the hypergeometric differential equation and their solutions. This method works well when the order of each ramification point is as large as possible, e.g., when the permutations $\sigma_0, \sigma_1, \sigma_\infty$ contain (almost) solely cycles of order n_0, n_1, n_∞ say, and only a few cycles of smaller order. For example, this occurs when the cover is Galois, or slightly weaker, when it is regular, that is to say, when the permutations $\sigma_0, \sigma_1, \sigma_\infty$ are a product of disjoint cycles of equal cardinality.

The method of van Hoeij–Vidunas to calculate a Belyĭ map $f : X \to \mathbb{P}^1$ is to consider the n exceptional ramification points in X of f whose ramification orders do not equal the usual orders a, b, c. One then equips the base space $\mathbb{P}^1$ with the hypergeometric equation whose local exponents at $0, 1, \infty$ equal a, b, c. Pulling back the hypergeometric equation by f, one obtains a Fuchsian differential equation with singularities exactly in the n exceptional points. The mere fact that this pullback exists implies equations on the undetermined coefficients of f.

For example, when the number of exceptional points is just $n = 3$, the differential equation can be renormalized to a Gaussian hypergeometric differential equation, which completely determines it. When $n = 4$, one obtains a form of Heun's equation [**125, 157**]. Heun's equation depends on the relative position of the fourth ramification point, as well as on an accessory parameter; still, there are only two parameters remaining in the computation.

One shows that for fixed n and genus g (taken as $g = 0$ later), there are only finitely many hyperbolic Belyĭ functions with n exceptional points. For small n, van Hoeij and Vidunas show that this differential method is successful in practice, and they compute all (hyperbolic) examples with $n \leq 4$ (the largest degree of such a Belyĭ map was 60).

Question 2.13. — *Are there other sources of equations (such as those arising from differential equations, algebraic manipulation, etc.) that further simplify the scheme obtained from the direct method?*

3. Complex analytic methods

In this section we consider complex analytic methods for finding equations for Belyĭ maps. These methods are essentially approximative; a high precision solution over $\mathbb{C}$ is determined, from which one reconstructs an exact solution over $\overline{\mathbb{Q}}$.

Newton approximation. — We have seen in the previous section how to write down a system of equations which give rise to the Belyĭ map. These equations can be solved numerically in $\mathbb{C}$ using multidimensional Newton iteration, given an approximate solution that is correct to a sufficient degree of precision and a subset of equations of full rank whose Jacobian has a good condition number (determinant bounded away from zero). Then, given a complex approximation that is correct to high precision, one can then use the LLL lattice-reduction algorithm [**102**] (as well as other methods, such as PSLQ [**53**]) to guess algebraic numbers that represent the exact values. Finally, one can use the

results from Section 8 to verify that the guessed cover is correct; if not, one can go back and iterate to refine the solution.

Remark 3.1. — We may repeat this computation for each representative of the Galois orbit to find the full set of conjugates for each putative algebraic number and then recognize the symmetric functions of these conjugates as rational numbers using continued fractions instead. For example, one can compute each representative in the passport, possibly including several Galois orbits. The use of continued fractions has the potential to significantly reduce the precision required to recognize the Belyĭ map exactly.

Example 3.2. — Consider the permutation triple

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

From the Riemann–Hurwitz formula, we find that the associated Belyĭ curve X has genus $g = 1$. The ramification point of index 7 on X (over ∞) is unique, so we take it to be the origin of the group law on X. Moreover, since there is a unique unramified point above 0, we can use a normal form (due to Tate) of an elliptic curve with a marked point. This is given by an equation

$$y^2 + p_3 y = q(x) = x^3 + p_2 x^2 + p_4 x \tag{3.3}$$

with marked point $(0, 0)$. The equation (3.3) is unique up to scaling the coefficients by $u \neq 0$ according to $(p_2, p_3, p_4) \mapsto (u^2 a_2, u^3 a_3, u^4 a_4)$, showing that the moduli spaces $\mathcal{M}_{1,2}$ of genus 1 curves with two marked points is isomorphic to the weighted projective space $\mathbb{P}(2, 3, 4)$.

Since the origin of the group law of X maps to ∞ and $(0, 0)$ maps to 0, the Belyĭ map $f : X \to \mathbb{P}^1$ of degree 7 is of the form

$$f(x, y) = (a_3 x^3 + a_2 x^2 + a_1 x) + (b_2 x^2 + b_1 x + b_0) y = a(x) + b(x) y.$$

The ramification above $f = 0$ leads to the equation

$$\mathrm{N}_{\mathbb{C}(x,y)/\mathbb{C}(x)}(f(x, y)) = a(x)(a(x) - p_3 b(x)) - b(x)^2 q(x) = -b_2^2 x c(x)^3$$

where $c(x)$ is the monic polynomial $x^2 + c_1 x + c_0$. Consideration of the ramification above 1 yields

$$\mathrm{N}_{\mathbb{C}(x,y)/\mathbb{C}(x)}(f(x, y) - 1) = (a(x) - 1)(a(x) - 1 - p_3 b(x)) - b(x)^2 q(x) = -b_2^2 d(x)^3 e(x)^2$$

where $d(x) = x + d_0$ and $e(x) = x^2 + e_1 x + e_0$.

This yields 13 equations in 14 unknowns. The reason for this is that we are still free to scale the p_i. Here we have to distinguish cases. We first suppose that the point $(0, 0)$ in (3.3) is not 2-torsion, or equivalently, that $p_3 \neq 0$: this is the "generic" case. We can then distinguish two further cases, namely $p_2 \neq 0$ and $p_4 \neq 0$. Accordingly, we may then ensure $p_2 = p_3$ or $p_3 = p_4$ by scaling over the ground field, so that we do not needlessly enlarge the coefficient of the Belyĭ map. In either case, plugging in random choices for the vector of unknowns $(a, b, c, d, e, p) \in \mathbb{C}^{14}$ and applying multivariate Newton iteration fails to yield a solution.

To improve the convergence, we now proceed to remove some degenerate cases from this set of equations. Applying the trick from Example 2.2, we impose that $c_0 d_0 e_0 \neq 0$, as we may since the ramification points are distinct and $(0, 0)$ is a ramification point. (This in fact assumes that none of the other ramification points is $(0, -1)$, which leads to

a subcase that turns out not to yield a solution.) We further insist that c and e do not have a double root, so $(c_1^2 - c_0)(e_1^2 - e_0) \neq 0$. This adds 2 more variables and equations.

Finally, we saturate our equations using the Atkin–Swinnerton-Dyer trick in Lemma 2.7. The differential $dx/(2y + p_3)$ is holomorphic and has no zeros or poles, so denoting derivation with respect to x by $'$, we see that

$$\begin{aligned}\frac{df}{dx/(2y+p_3)} = (2y+p_3)\frac{df}{dx} &= a'(x)(2y+p_3) + b'(x)(2y+p_3)y + b(x)(2y+a_3)y' \\ &= (2b'(x)q(x) + b(x)q'(x) + p_3a'(x)) + (2a'(x) - p_3b'(x))y\end{aligned}$$

satisfies

$$\mathrm{N}(((2y+p_3)(df/dx)) = 49b_2^2c(x)^2d(x)^2e(x).$$

This differentation trick thus yields another 8 equations. But even after adding these and the nondegeneracy conditions, random choices for an initial approximation fail to converge to a solution for the new system of 23 equations in 15 unknowns.

So we are led to consider the case where $p_3 = 0$, so that the unramified point above 0 is 2-torsion. (Here, there is some extra ambiguity, since the moduli space $X_0(2) = X_1(2)$ is not a fine moduli space.) If we write $\mathrm{div}(f) = (0,0) + 3P_1 + 3P_2 - 7\infty$ and $\mathrm{div}(f-1) = 2Q_1 + 2Q_2 + 3Q_3$, then we have

$$\mathrm{div}(df) = 2P_1 + 2P_2 + Q_1 + Q_2 + 2Q_3 - 8\infty$$

and so we obtain the relations

$$Q_1 + Q_2 = 3Q_3 = 0, \quad 3Q_3 = 0, \quad (0,0) + (P_1 + P_2) = -Q_3, \quad 2(0,0) = 0$$

in the group law of X. In particular, $P_1 + P_2$ is a 6-torsion point on X. Relations such as these can be used to find extra equations for X and f by using division polynomials. But again, the new system fails to yield any solutions; perhaps one can prove non-existence of solutions directly.

Here, we look ahead to the methods of this section and Section 4 that allow us to find an approximation to the solution. It turns out that we only need 3 decimal places to get the Newton method converging to a real solution with $p_3 \neq 0$ and $p_2 = p_3$, approximated by the solution

$$\begin{aligned}&(a,b,c,d,e,p) \approx \\ &\quad (182.7513294, 146.8290694, 29.38993410, -308.3482399, -244.0552479 \\ &\qquad - 48.11742858, 0.7992141684, 0.1613326212, 0.1482181605, 0.9764940118, \\ &\qquad 0.2561882114, 1.165925608, 0.4430649844, 163.2364906, 3.003693522)\end{aligned}$$

in $\mathbb{C}^{13}$. The condition number of the system without the additional Atkin–Swinnerton-Dyer relations is approximately $3.3 \cdot 10^7$; but by adding some of these relations, this can be decreased to approximately $1.2 \cdot 10^5$.

Using LLL, we recognize this as a putative solution over $\mathbb{Q}(\alpha)$ with $\alpha^3 - 3\alpha + 12 = 0$; then we verify that the recognized solution is correct using the methods of Section 8. This solution thereby gives rise to two more complex (conjugate) solutions. Since there are only three permutation triples with the given ramification passport, we see that we have found all dessins of the given ramification type, so we need not consider the other cases further.

As mentioned in Remark 3.1, the standard algorithms to recognize algebraic dependency work better after symmetrizing over these conjugate solutions. For the most difficult algebraic number to recognize (which is b_2) using a single solution requires the knowledge of 161 digits, whereas recognition as an algebraic number needs only 76 digits.

If we drop the demand that the unramified point is at $(0,0)$, then we can simplify the solution somewhat, as in Section 8. In Weierstrass form, we can take X to be given by the curve

$$\begin{aligned} y^2 = x^3 &+ (-541809\alpha^2 + 898452\alpha + 2255040)x \\ &+ (-2929526838\alpha^2 + 5759667648\alpha - 11423888784). \end{aligned}$$

and the function $f = a(x) + b(x)y$ by

$$\begin{aligned} 2^{13}3^{14}5^5 a(x) = &(1491\alpha^2 + 6902\alpha + 10360)x^3 \\ &+ (1410885\alpha^2 + 2033262\alpha - 4313736)x^2 \\ &+ (731506545\alpha^2 + 15899218650\alpha + 32119846920)x \\ &- (7127713852353\alpha^2 + 3819943520226\alpha + 62260261739784) \end{aligned}$$

and

$$\begin{aligned} 2^{13}3^{16}5^5 b(x) = &(-197\alpha^2 - 240\alpha + 528)x^2 \\ &+ (906570\alpha^2 - 546840\alpha - 8285760)x \\ &- (715988241\alpha^2 - 2506621464\alpha - 1458270864). \end{aligned}$$

We thank Marco Streng for his help with reducing these solutions. Applying the methods in Section 4 already gives equations that are better than those in the normalized forms (3.3) considered above; at least experimentally, using the modular method also tends to give equations of relatively small height.

As we have seen in the preceding example, in order for this procedure to work, one needs a good starting approximation to the solution. In the non-trivial examples that we have computed so far, it seems that often this approximation must be given to reasonably high precision (at least 30 digits for moderately-sized examples) in order for the convergence to kick in. The required precision seems difficult to estimate from above or below. And indeed the dynamical system arising from Newton's method has quite delicate fractal-like properties and its study is a subject in itself [**128**].

Question 3.4. — *Is there an explicit sequence of Belyĭ maps with the property that the precision required for Newton iteration to converge tends to infinity?*

One way to find a starting approximation to the solution is explained by Couveignes–Granboulan [**29, 60, 33**]. They inductively use the solution obtained from a simpler map: roughly speaking, they replace a point of multiplicity ν with two points of multiplicities ν_1, ν_2 with $\nu_1 + \nu_2 = \nu$. One can use any appropriate base case for the induction, such as a map having simple ramification. Couveignes [**29**] gives a detailed treatment of the case of trees, corresponding to clean Belyĭ polynomials $f(t)$, i.e. those with $f(t) - 1 = g(t)^2$: geometrically, this means that the corresponding dessin can be interpreted as a tree with oriented edges. In this case, after an application of the differentiation trick, one is led to solve a system of equations where many equations are linear. See Granboulan [**60**, Chapter IV] for an example with monodromy group $\mathrm{Aut}(M_{22})$.

Remark 3.5. — There is a misprint in the example of Couveignes [**29**, §3, pg. 8] concerning the discriminant of the field involved, corrected by Granboulan [**60**, p. 64].

So far, it seems that the inductive numerical method has been limited to genus 0 Belyĭ maps with special features. A similar method was employed by Matiyasevich [**119**] for trees: he recursively transforms the initial polynomial $2t^n - 1$ (corresponding to a star tree) into a polynomial representing the desired planar tree.

Question 3.6. — *Can an inductive complex analytic method be employed to compute more complicated Belyĭ maps in practice?*

In particular, the iterative method by Couveignes and Granboulan to find a good starting value seems to rely on intuition involving visual considerations; can these be made algorithmically precise?

Circle packing. — Another complex analytic approach is to use circle packing methods. This technique was extensively developed in work of Bowers–Stephenson [**22**], with a corresponding Java script `CirclePack` available for calculations.

Given a dessin (i.e., the topological data underlying a Belyĭ map), one obtains a triangulation of the underlying surface by taking the inverse image of $\mathbb{P}^1(\mathbb{R}) \subset \mathbb{P}^1(\mathbb{C})$ together with the corresponding cell decomposition. Choosing isomorphisms between these triangle and the standard equilateral triangle in $\mathbb{C}$ and gluing appropriately, one recovers the Riemann surface structure and as a result a meromorphic description of the Belyĭ map.

However, the Riemann surface structure is difficult to determine explicitly, starting from the dessin. As an alternative, one can pass to discrete Belyĭ maps instead. To motivate this construction, note that a Riemann surface structure on a compact surface induces a unique metric of constant curvature $1, 0, -1$ (according as $g = 0, 1, \geq 2$) so that one can then speak meaningfully about circles on such a surface. In particular, it makes sense to ask whether or not there exists a circle packing associated with the triangulation, a pattern of circles centered at the vertices of this triangulation satisfying the tangency condition suggested by the triangulation. Satisfyingly enough, the circle packing theorem, due Koebe–Andreev–Thurston [**93, 114, 154**], states that given a triangulation of a topological surface, there exists a unique structure of Riemann surface that leads to a compatible circle packing. This then realizes the topological map to the Riemann sphere as a smooth function.

In summary, starting with a dessin, one obtains a triangulation and hence a circle packing. The corresponding discrete Belyĭ map will in general *not* be meromorphic for the Riemann surface structure induced by the circle packing; but Bowers and Stephenson prove that it does converge to the correct solution as the triangulation is iteratively hexagonally refined.

The crucial point is now to compute the discrete approximations obtained by circle packing in an explicit and efficient way. Fortunately, this is indeed possible; work by Collins–Stephenson [**26**] and Mohar [**123**] give algorithms for this. The crucial step is to lift the configuration of circles to the universal cover H (which is either the sphere $\mathbb{P}^1(\mathbb{C})$, the plane $\mathbb{C}$, or the upper half-plane $\mathcal{H}$) and perform the calculation in H. In fact, this means that the circle packing method also explicitly solves the uniformization problem for the surface involved; for theoretical aspects, we refer to Beardon–Stephenson [**8**]. Upon passing to H and using the appropriate geometry, one then *first* calculates the radii of

the circles involved from the combinatorics, before fitting the result into H, where it gives rise to a fundamental domain for the corresponding curve as a quotient of H.

An assortment of examples of the circle packing method is given by Bowers–Stephenson [**22**, §5], and numerical approximations are computed to a few digits of accuracy. This includes genus 0 examples of degree up to 18, genus 1 examples of degree up to 24, and genus 2 examples of degree up to 14. For determining the conformal structure, this approach is therefore much more effective indeed than the naive method from Section 2. Even better, one can proceed inductively from simpler dessins by using so-called dessin moves [**22**, §6.1], which makes this approach quite suitable for calculating large tables of conformal realizations of dessins.

On the other hand, there are no theoretical results on the number of refinements needed to obtain given accuracy for the circle packing method [**22**, §7]. In examples, it is possible for the insertion of a new vertex to drastically increase the accuracy needed [**22**, Figure 25] and thereby the number of discrete refinements needed, quite radically increasing the complexity of the calculation [**22**, §8.2]. However, the method is quite effective in practice, particularly in genus 0.

More problematically, it seems difficult to recover equations over $\overline{\mathbb{Q}}$ for the Belyĭ map from the computed fundamental domain if the genus is strictly positive. One can compute the periods of the associated Riemann surface to some accuracy, but one still needs to recover the curve X and transfer the Belyĭ map f on X accordingly. Moreover, is also not clear that the accuracy obtained using this method is enough to jump start Newton iteration and thereby obtain the high accuracy needed to recognize the map over $\overline{\mathbb{Q}}$. In Section 4, we circumvent this problem by starting straightaway with an explicit group Γ of isometries of H so that $\Gamma\backslash H \cong X$ and then finding equations for X by numerically computing modular forms (i.e., differential forms) on X.

Example 3.7. — In Figure 3.8, we give an example from an alternate implementation by Westbury, which is freely available [**168**] for the case of genus 0. In the figure, an outer polygon is inserted instead of a circle to simplify the calculation of the radii. We show the conformal triangulation induced by the second barycentric subdivision of the original triangulation for one of the exactly 2 covers in Example 7.9 that descend to $\mathbb{R}$.

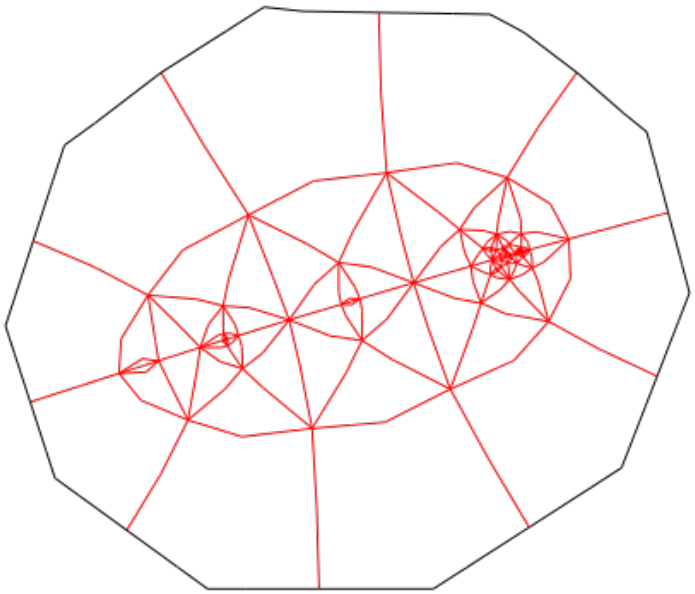


Figure 3.8: A second subdivision for M_{23}

Several more subdivisions would be needed to get the solution close enough to apply Newton's method.

Puiseux series. — Couveignes–Granboulan [**33**, §6] proposed an alternative method using Puiseux series expansions to get a good complex approximation to the solution so that again multidimensional Newton iteration can kick off.

At every regular point P in the curve X, the Belyĭ map has an analytic expansion as a power series in a uniformizer z at P that converges in a neighborhood of P. Similarly, at a ramification point P, there is an expansion for f that is a Puiseux series in the uniformizer z; more specifically, it is a power series in $z^{1/e} = \exp(2\pi i \log(z)/e)$ where e is the ramification index of P and log is taken to be the principal logarithm. Now, these series expansions must agree whenever they overlap, and these relations between the various expansions give conditions on their coefficients. More precisely, one chooses tangential base points, called standards, and the implied symbolic relations are then integrated with respect to a measure with compact support. Collecting the relations, one obtains a block matrix, the positioning of whose blocks reflects the topology of the overlaps of the cover used.

Unfortunately, Couveignes and Granboulan do not give an example of this method in practice, and the most detail they give concerns iterative ad hoc methods [**33**, §7].

Question 3.9. — *How effective is the method of Puiseux series in finding a good starting approximation? Can one prove rigorously that this method gives a correct answer to a desired precision?*

Homotopy methods. — One idea that has yet to be explored (to the authors' knowledge) is the use of techniques from numerical algebraic geometry, such as polyhedral homotopy methods [**10, 159**], to compute Belyĭ maps. The success of homotopy methods in solving extremely large systems of equations, including those with positive-dimensional components, has been dramatic. In broad stroke, one deforms the solution of an easier

system to the desired ones and carefully analyzes the behavior of the transition matrix (Jacobian) to ensure convergence of the final solution. Because these methods are similar in spirit to the ones above, but applied for a more general purpose, it is natural to wonder if these ideas can be specialized and then combined into a refined technique tailored for Belyĭ maps.

Question 3.10. — *Can the techniques of numerical algebraic geometry be used to compute Belyĭ maps efficiently?*

A potential place to start in deforming is suggested by the work above and by Couveignes [**32**, §6]: begin with a stable curve (separating the branch points) and degenerate by bringing together the genus 0 components. The difficulty then becomes understanding the combinatorial geometry of this stable curve, which is an active area of research.

Zipper method. — Complex analytic techniques can also be brought to bear on Belyĭ maps of extremely large degree, at least for the case of trees, using an extension of the zipper method due to Marshall–Rohde [**117, 118**]. The zipper method finds a numerical approximation of the conformal map of the unit disk onto any Jordan region [**115**]. In its extension, this amounts to constructing the conformal map onto the domain of the exterior of the desired dessin, which can be done quite simply for trees even with thousands of branches. For example, Marshall and Rohde have computed the dessins associated to the Belyĭ maps $f^n(z)$ where $f(z) = (3z^3 - 9z - 2)/4$, giving a sequence of Belyĭ trees (under the preimage of $[-2, 1]$), and by extension one can obtain complex approximation to Belyĭ maps of extremely large degree: trees with tens of thousands of edges, far beyond the reach of other methods.

Question 3.11. — *Does the zipper method extend to higher genus?*

In the latter extension, one would need to consider not only the convergence of the Belyĭ map but also the associated Belyĭ curve X, so it appears one will have to do more than simply solve the Dirichlet problem. See also work by Larusson and Sadykov [**100**], where the connection with the classical Riemann-Hilbert problem is discussed in the context of trees.

4. Modular forms

In this section we continue with the general strategy of using complex analytic methods but shift our focus in the direction of geometry and consideration of the uniformization theorem; we work explicitly with quotients of the upper half-plane by Fuchsian groups and recast Belyĭ maps in this language. This point of view is already suggested by Grothendieck [**62**]:

> In more erudite terms, could it be true that every projective non-singular algebraic curve defined over a number field occurs as a possible "modular curve" parametrising elliptic curves equipped with a suitable rigidification? ... [T]he Soviet mathematician Belyĭ announced exactly that result.

As in the last section, the method here uses numerical approximations; however, the use of modular functions adds considerable more number-theoretic flavor to the analytic techniques in the previous section.

Classical modular forms. — Let F_2 be the free group on two generators as in (1.1). Recall that the map that considers the permutation action of x, y, z on the cosets of a subgroup yields a bijection

$$\begin{array}{c} \left\{\text{transitive permutation triples } \sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3\right\} / \sim \\ \updownarrow \text{1:1} \\ \{\text{subgroups of } F_2 \text{ of index } d\} / \sim ; \end{array} \tag{4.1}$$

here the equivalence relation on triples is again uniform conjugation, and the equivalence relation on subgroups is conjugation in F_2. In particular, by Proposition 1.4, isomorphism classes of (connected) Belyĭ maps are in bijection with the conjugacy classes of subgroups F_2 of finite index.

The key observation is now that F_2 can be realized as an arithmetic group, as follows. The group $\Gamma(1) = \mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$ acts on the completed upper half-plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ by linear fractional transformations

$$z \mapsto \frac{az+b}{cz+d}, \quad \text{for } \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}).$$

The quotient $X(1) = \Gamma(1)\backslash\mathcal{H}^*$ can be given the structure of a Riemann surface of genus 0 by the uniformizing map $j : X(1) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C})$ (often called the modular elliptic j-function),

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots$$

where $q = \exp(2\pi i z)$.

For an integer N, we define the normal subgroup $\Gamma(N)$ as the kernel of the reduction map $\mathrm{PSL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$. We will be particularly interested in the subgroup

$$\Gamma(2) = \left\{ \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) : b \equiv c \equiv 0 \pmod 2 \right\}$$

of index 6, with quotient isomorphic to $\Gamma(1)/\Gamma(2) \cong \mathrm{PSL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$. The group $\Gamma(2)$ is in fact isomorphic to the free group $F_2 \cong \Gamma(2)$: it is freely generated by $\pm \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, which act on $\mathcal{H}$ by $z \mapsto z+2$ and $z \mapsto z/(2z+1)$, respectively; the corresponding action on the upper half plane is free as well.

The quotient $X(2) = \Gamma(2)\backslash\mathcal{H}^*$ is again a Riemann surface of genus 0; the action of $\Gamma(2)$ on $\mathbb{P}^1(\mathbb{Q})$ has three orbits, with representatives $0, 1, \infty \in \mathbb{P}^1(\mathbb{Q})$. We obtain another uniformizing map $\lambda : X(2) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C})$ with expansion

$$\lambda(z) = 16q^{1/2} - 128q + 704q^{3/2} - 3072q^2 + 11488q^{5/2} - 38400q^3 + \dots.$$

As a uniformizer for a congruence subgroup of $\mathrm{PSL}_2(\mathbb{Z})$, the function $\lambda(z)$ has a modular interpretation: there is a family of elliptic curves over $X(2)$ equipped with extra structure. Specifically, given $\lambda \in \mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$, the corresponding elliptic curve with extra structure is given by the Legendre curve

$$E : y^2 = x(x-1)(x-\lambda),$$

equipped with the isomorphism $(\mathbb{Z}/2\mathbb{Z})^2 \xrightarrow{\sim} E[2]$ determined by sending the standard generators to the 2-torsion points $(0,0)$ and $(1,0)$.

There is a forgetful map that forgets this additional torsion structure on a Legendre curve and remembers only isomorphism class; on the algebraic level, this corresponds to an expression of j in terms of λ, which is given by

$$j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}; \tag{4.2}$$

indeed, the map $X(2) \to X(1)$ given by $j/1728$ is a Galois Belyĭ map of degree 6 with monodromy group S_3, given explicitly by (4.2). This map is the Galois closure of the map computed in Example 2.1.

The cusp ∞ plays a special role in the theory of modular forms, and marking it in our correspondence will allow a suitable rigidification. With this modification, the correspondence (4.1) becomes a bijection

$$\begin{array}{c} \left\{ \begin{array}{c} \text{transitive permutation triples } \sigma \in S_d \\ \text{with a marked cycle of } \sigma_\infty \end{array} \right\} / \sim \\ \updownarrow 1{:}1 \\ \{\text{subgroups of } F_2 \cong \Gamma(2) \text{ of index } d\} / \sim \end{array} \tag{4.3}$$

with equivalence relations as follows: given $\Gamma, \Gamma' \leq \Gamma(2)$, we have $\Gamma \sim \Gamma'$ if and only if $g\Gamma g^{-1} = \Gamma'$ for g an element of the subgroups of translations generated by $z \mapsto z+2$; and two triples $\sigma, \sigma' \in S_d^3$ with marked cycles c, c' in $\sigma_\infty, \sigma'_\infty$ are equivalent if and only if they are simultaneously conjugate by an element τ with $\tau c \tau^{-1} = c'$.

It is a marvelous consequence of either of the bijections (4.1) and (4.3), combined with Belyĭ's theorem, that any curve X defined over a number field is uniformized by a subgroup $\Gamma \leq \Gamma(2) < \mathrm{PSL}_2(\mathbb{Z})$, so that there is a uniformizing map $\Gamma\backslash\mathcal{H}^* \xrightarrow{\sim} X(\mathbb{C})$. This is the meaning of Grothendieck's comment: the rigidification here corresponds to the subgroup Γ. In general, the group Γ is noncongruence, meaning that it does not contain a subgroup $\Gamma(N)$, so membership in the group cannot be determined by congruences on the coordinate entries of the matrices. This perspective of modular forms is taken by Atkin–Swinnerton-Dyer [**5**] and Birch [**18**, Theorem 1] in their exposition of this subject: they discuss the relationship between modular forms, the Atkin–Swinnerton-Dyer congruences for noncongruence modular forms, and Galois representations in the context of Belyĭ maps. For more on the arithmetic aspects of this subject, we refer to the survey by Li–Long–Yang [**104**] and the references therein.

The description (4.3) means that one can work quite explicitly with the Riemann surface associated to a permutation triple. Given a triple σ, the uniformizing group Γ is given as the stabilizer of 1 in the permutation representation $\Gamma(2) \to S_d$ given by $x, y, z \mapsto \sigma_0, \sigma_1, \sigma_\infty$ as in (4.3). A fundamental domain for Γ is given by Farey symbols [**98**], including a reduction algorithm to this domain and a presentation for the group Γ together with a solution to the word problem in Γ. These algorithms have been implemented in the computer algebra systems `Sage` [**137**] (in a package for *arithmetic subgroups defined by permutations*, by Kurth, Loeffler, and Monien) and `Magma` [**19**] (by Verrill).

Once the group Γ has been computed, and the curve $X = \Gamma\backslash\mathcal{H}^*$ is thereby described, the Belyĭ map is then simply given by the function

$$\lambda : X \to X(2) \cong \mathbb{P}^1,$$

so one immediately obtains an analytic description of Belyĭ map. In order to obtain explicit equations, one needs meromorphic functions on X, which is to say, meromorphic functions on $\mathcal{H}$ that are invariant under Γ.

We are led to the following definition. Let $\Gamma \leq \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index. A modular form for $\Gamma \leq \mathrm{PSL}_2(\mathbb{Z})$ of weight $k \in 2\mathbb{Z}$ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

$$f(\gamma z) = (cz+d)^k f(z) \quad \text{for all } \gamma = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \tag{4.4}$$

and such that the limit $\lim_{z\to c} f(z) = f(c)$ exists for all cusps $c \in \mathbb{Q} \cup \{\infty\} = \mathbb{P}^1(\mathbb{Q})$ (with the further technical condition that as $z \to \infty$, we take only those paths that remain in a bounded vertical strip). A cusp form is a modular form where $f(c) = 0$ for each cusp c. The space $S_k(\Gamma)$ of cusp forms for Γ of weight k is a finite-dimensional $\mathbb{C}$-vector space. If Γ is torsion-free or $k = 2$, then there is an isomorphism

$$\begin{aligned} S_k(\Gamma) &\xrightarrow{\sim} \Omega^{k/2}(X) \\ f(z) &\mapsto f(z)\,(dz)^{\otimes k/2} \end{aligned} \tag{4.5}$$

where $\Omega^{k/2}(X)$ is the space of holomorphic differential $(k/2)$-forms on X. In any case, evaluation on a basis for $S_k(\Gamma)$ defines a holomorphic map $\varphi : X \to \mathbb{P}^{r-1}$ where $r = \dim_{\mathbb{C}} S_k(\Gamma)$, whenever $r \geq 1$. Classical theory of curves yields a complete description of the map φ; for example, for generic X of genus $g \geq 3$, taking $k = 2$ (i.e., a basis of holomorphic 1-forms) gives a canonical embedding of X as an algebraic curve of degree $2g-2$ in $\mathbb{P}^{g-1}$, by the theorem of Max Noether.

Selander–Strömbergsson [**141**] use this analytic method of modular forms to compute Belyĭ maps; this idea was already present in the original work of Atkin–Swinnerton-Dyer [**5**] and was developed further by Hejhal [**72**] in the context of Maass forms. Starting with the analytic description of a subgroup $\Gamma \leq \Gamma(2)$, they compute a hyperelliptic model of a curve of genus 2 from the knowledge of the space $S_2(\Gamma)$ of holomorphic cusp forms of weight 2 for Γ. These cusp forms are approximated to a given precision by truncated q-expansions

$$f(z) = \sum_{n=0}^{N} a_n q^n, \tag{4.6}$$

one for each equivalence class of cusp c and corresponding local parameter q under the action of Γ. These expansions (4.6) have undetermined coefficients $a_n \in \mathbb{C}$, and the equation (4.4) implies an approximate *linear* condition on these coefficients for any pair of Γ-equivalent points z, z'. These linear equations can then be solved using the methods of numerical linear algebra. This seems to work well in practice, and once complex approximations for the cusp forms are known, the approximate algebraic equations that they satisfy can be computed, so that after a further Newton iteration and then lattice reduction one obtains an exact solution. Atkin–Swinnerton-Dyer say of this method [**5**, p. 8]:

> From the viewpoint of numerical analysis, these equations are of course very ill-conditioned. The power series converge so rapidly that one must be careful not to take too many terms, and the equality conditions at adjacent points in a subdivision of the sides are nearly equivalent. However, by judicious choice of the number of terms in the power series and the number of subdivision points,

for which we can give no universal prescription, we have been able to determine the first 8 or so coefficients [...] with 7 significant figures in many cases.

Question 4.7. — *Does this method give rise to an* algorithm *to compute Belyĭ maps? In particular, is there an explicit estimate on the numerical stability of this method?*

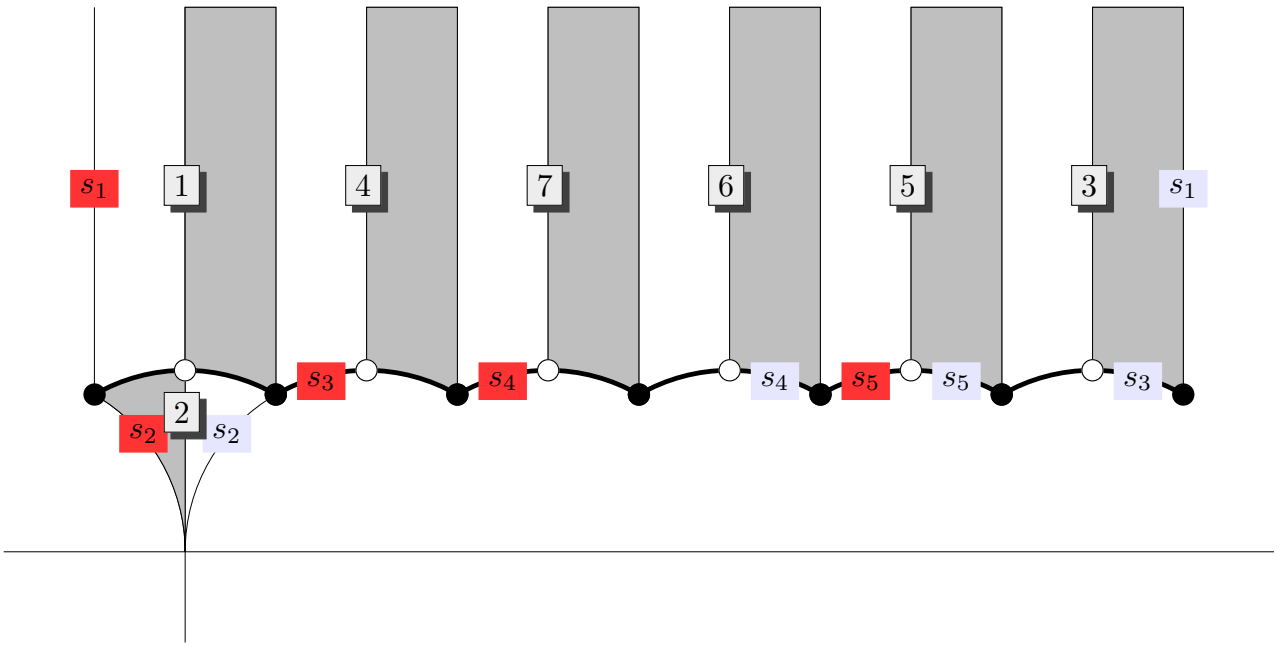
For Belyĭ maps such that the corresponding subgroup Γ is congruence, methods of modular symbols [**36, 149**] can be used to determine the q-expansions of modular forms using exact methods. The Galois groups of congruence covers are all subgroups of $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$ for some integer N, though conversely not all such covers arise in this way; as we will see in the next subsection, since $\mathrm{PSL}_2(\mathbb{Z})$ has elliptic points of order 2 and 3, a compatibility on the orders of the ramification types is required. Indeed, "most" subgroups of finite index in $\mathrm{PSL}_2(\mathbb{Z})$ (in a precise sense) are noncongruence [**81**].

Example 4.8. — To give a simple example, we consider one of the two (conjugacy classes of) noncongruence subgroups of index 7 of $\mathrm{PSL}_2(\mathbb{Z})$, the smallest possible index for a noncongruence subgroup by Wohlfarht [**170**]. The cusp widths of this subgroup are 1 and 6. The information on the cusps tells us that the ramification type of the Belyĭ map above ∞ is given by $(6,1)$, whereas the indices above 0 (resp. 1) have to divide 3 (resp. 2). This forces the genus of the dessin to equal 0, with ramification triple $(6^1 1^1, 3^2 1^1, 2^3 1^1)$.

There are exactly two transitive covers with this ramification type, both with passport $(0, G, (2^3 1^1, 3^2 1^1, 6^1 1^1))$. Here the monodromy group G is the Frobenius group of order 42; the two covers correspond to two choices of conjugacy classes of order 6 in G. For one such choice, we obtain the following unique solution up to conjugacy:

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

A fundamental domain for the action of $\Gamma = \Gamma_7$ is as follows.



Label	Coset Representative
1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
2	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
3	$\begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix}$
4	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
5	$\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$
6	$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$
7	$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$

Label	Side Pairing Element
s_1	$\begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$
s_2	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$
s_3	$\begin{pmatrix} 5 & -6 \\ 1 & -1 \end{pmatrix}$
s_4	$\begin{pmatrix} 3 & -7 \\ 1 & -2 \end{pmatrix}$
s_5	$\begin{pmatrix} 4 & -17 \\ 1 & -4 \end{pmatrix}$

Figure 4.9: A fundamental domain and side pairing for $\Gamma_7 \leq \Gamma(1)$ of index 7

We put the cusp of $\Gamma(1)$ at $t = \infty$ and the elliptic point of order 3 (resp. 2) at $t = 0$ (resp.z $t = 1$). After this normalization, the q-expansion for the Hauptmodul t for Γ is given by

$$t(q) = \frac{1}{\zeta} + 0 + \frac{9 + \sqrt{-3}}{2^1 3^4}\zeta + \frac{-3 - 5\sqrt{-3}}{2^2 3^5}\zeta^2 + \frac{1 - 3\sqrt{-3}}{2^1 3^7}\zeta^3 + \dots$$

where $\zeta = \eta q^{1/6}$ and

$$\eta^6 = \frac{3^{10}}{7^7}(-1494 + 3526\sqrt{-3}).$$

From this, we compute using linear algebra the algebraic relationship between $t(q)$ and $j(q)$, expressing $j(q)$ as a rational function in $t(q)$ of degree 7:

$$j = -\frac{2^6(1 + \sqrt{-3})}{(5 - \sqrt{-3})^7} \frac{(54\sqrt{-3}t^2 + 18\sqrt{-3}t + (5 - 3\sqrt{-3}))^3(6\sqrt{-3}t - (1 + 3\sqrt{-3}))}{(6\sqrt{-3}t - (1 + 3\sqrt{-3}))}.$$

We will compute this example again using p-adic methods in the next section (Example 5.5).

Modular forms on subgroups of triangle groups. — There is related method that works with a *cocompact* discrete group $\Gamma \leq \mathrm{PSL}_2(\mathbb{R})$, reflecting different features of Belyĭ maps. Instead of taking the free group on two generators, corresponding to the fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, we instead consider orbifold covers arising from triangle groups, a subject of classical interest (see e.g. Magnus [**105**]). For an introduction to triangle groups, including their relationship to Belyĭ maps and dessins, see the surveys of Wolfart [**172, 173**].

Let $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. We define the triangle group

$$\Delta(a, b, c) = \langle \delta_0, \delta_1, \delta_\infty \mid \delta_0^a = \delta_1^b = \delta_\infty^c = \delta_0\delta_1\delta_\infty = 1 \rangle$$

where infinite exponents a, b, c are ignored in the relations. Let $\chi(a, b, c) = 1/a + 1/b + 1/c - 1 \in \mathbb{Q}$. For example, we have $\Delta(2, 3, \infty) \cong \mathrm{PSL}_2(\mathbb{Z})$ and $\Delta(\infty, \infty, \infty) \cong F_2 \cong \Gamma(2)$,

so this construction generalizes the previous section. The triangle group $\Delta(a,b,c)$ is the index 2 orientation-preserving subgroup of the group generated by the reflections in the sides of a triangle $T(a,b,c)$ with angles $\pi/a, \pi/b, \pi/c$ drawn in the geometry H, where $H = \mathbb{P}^1, \mathbb{C}, \mathcal{H}$ according as $\chi(a,b,c)$ is positive, zero, or negative.

Associated to a transitive permutation triple σ from S_d is a homomorphism

$$\begin{aligned} \Delta(a,b,c) &\to S_d \\ \delta_0, \delta_1, \delta_\infty &\mapsto \sigma_0, \sigma_1, \sigma_\infty \end{aligned}$$

where $a, b, c \in \mathbb{Z}_{\geq 2}$ are the orders of $\sigma_0, \sigma_1, \sigma_\infty$, respectively. (Here we have no index ∞, so $\Delta(a,b,c)$ is cocompact, which is where this method diverges from that using classical modular forms.) The stabilizer of a point $\Gamma \leq \Delta(a,b,c)$ has index d, and the above homomorphism is recovered by the action of Δ on the cosets of Γ. The quotient map

$$\varphi : X = \Gamma\backslash H \to \Delta\backslash H$$

then realizes the Belyĭ map with monodromy σ, so from this description we have a way of constructing the Belyĭ map associated to σ. More precisely, as in (4.1), the bijection (1.3) generalizes to

$$\begin{gathered} \left\{ \begin{array}{c} \text{permutation triples } \sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3 \\ \text{such that } a, b, c \text{ are multiples of the orders of } \sigma_0, \sigma_1, \sigma_\infty \end{array} \right\} / \sim \\ \xleftrightarrow{1:1} \\ \{\text{subgroups of } \Delta(a,b,c) \text{ of index } n\} / \sim, \end{gathered} \tag{4.10}$$

where the equivalences are as usual: conjugacy in the group $\Delta(a,b,c)$ and simultaneous conjugacy of triples $(\sigma_0, \sigma_1, \sigma_\infty)$. (In particular, these triples are not marked, as by contrast they are in (4.3), though certainly our construction could be modified in this way if so desired.)

Explicitly, one obtains the Riemann surfaces corresponding to a subgroup $\Gamma < \Delta(a,b,c)$ under the bijection (4.10) by gluing together triangles $T(a,b,c)$ and making identifications. This gives a conformally correct way to draw dessins and a method for computing the covers themselves numerically.

This method has been developed in recent work of Klug–Musty–Schiavone–Voight [**91**]. Algorithms are provided for working with the corresponding triangle group Δ, determining explicitly the associated finite index subgroup Γ, and then drawing the dessin on H together with the gluing relations that define the quotient $X = \Gamma\backslash H$. From this explicit description of the Riemann surface (or more precisely, Riemann 2-orbifold) X one obtains equations for the Belyĭ map f numerically. The main algorithmic tool for this purpose is a generalization of Hejhal's method replacing q-expansions with power series expansions, due to Voight–Willis [**164**]. This method works quite well in practice; as an application, a Belyĭ map of degree 50 of genus 0 regularly realizing the group $\mathrm{PSU}_3(\mathbb{F}_5)$ over $\mathbb{Q}(\sqrt{-7})$ is computed.

Example 4.11. — Consider the permutation triple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$, where

$$\begin{aligned} \sigma_0 &= (1\ 7\ 4\ 2\ 8\ 5\ 9\ 6\ 3) \\ \sigma_1 &= (1\ 4\ 6\ 2\ 5\ 7\ 9\ 3\ 8) \\ \sigma_\infty &= (1\ 9\ 2)(3\ 4\ 5)(6\ 7\ 8). \end{aligned}$$

Then $\sigma_0\sigma_1\sigma_\infty = 1$ and these permutations generate a transitive subgroup

$$G \cong \mathbb{Z}/3\mathbb{Z} \wr \mathbb{Z}/3\mathbb{Z} \leq S_9$$

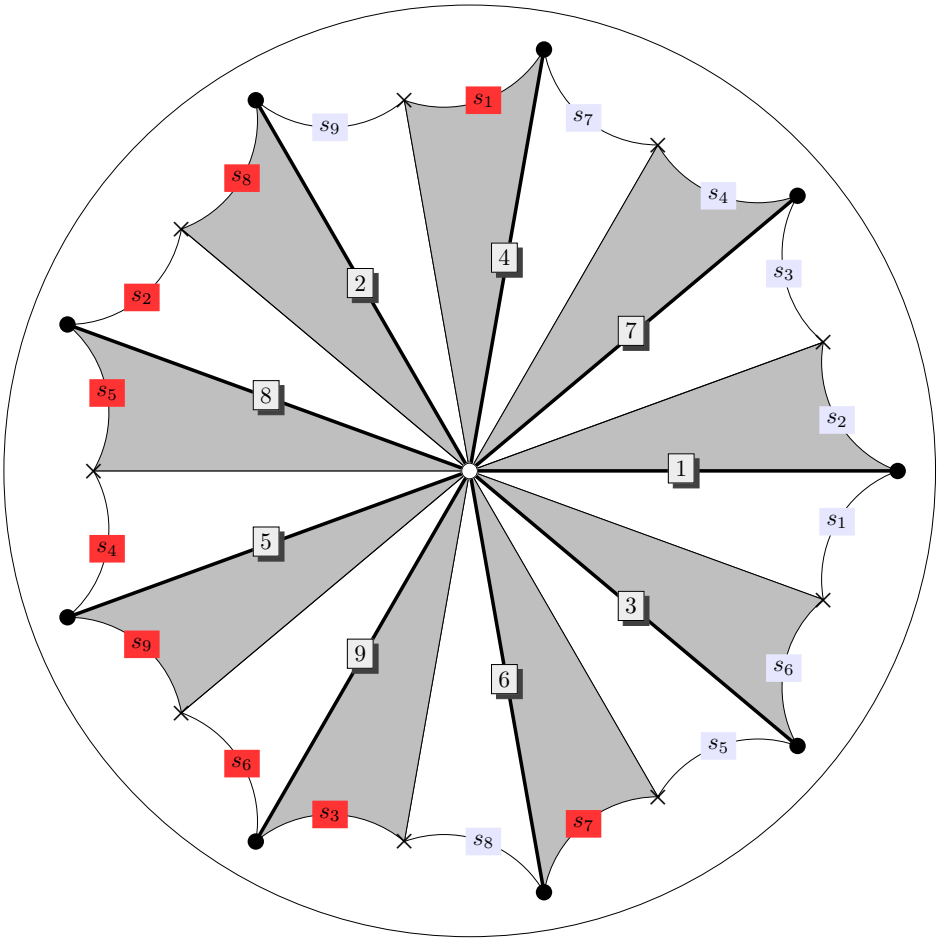
of order 81 and give rise to a Belyĭ map with passport $(0, G, (9^1, 9^1, 3^3))$. The corresponding group $\Gamma \leq \Delta(9,9,3) = \Delta$ of index 9 arising from (4.10) has signature $(3;-)$, i.e., the quotient $\Gamma\backslash\mathcal{H}$ is a (compact) Riemann surface of genus 3. The map $X(\Gamma) = \Gamma\backslash\mathcal{H} \to X(\Delta) = \Delta\backslash\mathcal{H} \cong \mathbb{P}^1$ gives a Belyĭ map of degree 9, which we now compute.

First, we compute a coset graph, the quotient of the Cayley graph for Δ on the generators $\delta_0^\pm, \delta_1^\pm$ by Γ with vertices labelled with coset representatives $\Gamma\alpha_i$ for $\Gamma\backslash\Delta$. Given a choice of fundamental domain D_Δ for Δ (a fundamental triangle and its mirror, as above), such a coset graph yields a fundamental domain $D_\Gamma = \bigcup_{i=1}^n \alpha_i D_\Delta$ equipped with a side pairing, indicating how the resulting Riemann orbifold is to be glued. We consider this setup in the unit disc $\mathcal{D}$, identifying $\mathcal{H}$ conformally with $\mathcal{D}$ taking a vertex to the center $w = 0$; the result is Figure 4.12. We obtain in this way a reduction algorithm that takes a point in $z \in \mathcal{H}$ (or $\mathcal{D}$) and produces a representative $z' \in D_\Gamma$ and $\gamma \in \Gamma$ such that $z' = \gamma z$.

We consider the space $S_2(\Gamma)$ of cusp forms of weight 2 for Γ, defined as in (4.4) (but note that since no cusps are present we can omit the corresponding extra conditions). As in (4.5), we have an isomorphism $S_2(\Gamma) \cong \Omega^1(X)$ of $\mathbb{C}$-vector spaces with the space of holomorphic 1-forms on X. Since X has genus 3, we have $\dim_{\mathbb{C}} S_2(\Gamma) = 3$. We compute a basis of forms by considering power series expansions

$$f(w) = (1-w)^2 \sum_{n=0}^{\infty} b_n w^n$$

for $f \in S_2(\Gamma)$ around $w = 0$ in the unit disc $\mathcal{D}$. (The presence of the factor $(1-w)^2$ makes for nicer expansions, as below.) We compute with precision $\epsilon = 10^{-30}$, and so $f(w) \approx (1-w)^2 \sum_{n=0}^{N} b_n w^n$ with $N = 815$. We use the Cauchy integral formula to isolate each coefficient b_n, integrating around a circle of radius $\rho = 0.918711$ encircling the fundamental domain. This integral is approximated by summing the evaluations at $O(N)$ points on this circle, which can be explictly represented by elements in the fundamental domain D_Γ after using the reduction algorithm.



Label	Coset Representative
1	1
2	δ_0^3
3	δ_0^{-1}
4	δ_0^2
5	δ_0^{-4}
6	δ_0^{-2}
7	δ_0
8	δ_0^4
9	δ_0^{-3}

Label	Side Pairing Element
s_1	$\delta_1\delta_0^{-2}$
s_2	$\delta_1^{-1}\delta_0^{-4}$
s_3	$\delta_0\delta_1\delta_0^3$
s_4	$\delta_0\delta_1^{-1}\delta_0^4$
s_5	$\delta_0^{-1}\delta_1\delta_0^{-4}$
s_6	$\delta_0^{-1}\delta_1^{-1}\delta_0^3$
s_7	$\delta_0^2\delta_1\delta_0^2$
s_8	$\delta_0^{-2}\delta_1\delta_0^{-3}$
s_9	$\delta_0^3\delta_1\delta_0^4$

Figure 4.12: A fundamental domain and side pairing for $\Gamma \leq \Delta(9,9,3)$ of index 9

We find the echelonized basis

$$x(w) = (1-w)^2\left(1 - \frac{40}{6!}(\Theta w)^6 + \frac{3080}{9!}(\Theta w)^9 - \frac{1848000}{12!}(\Theta w)^{12} + O(w^{15})\right)$$
$$y(w) = (1-w)^2\left((\Theta w) + \frac{4}{4!}(\Theta w)^4 + \frac{280}{7!}(\Theta w)^7 - \frac{19880}{10!}(\Theta w)^{10} + O(w^{13})\right)$$
$$z(w) = (1-w)^2\left((\Theta w)^3 - \frac{120}{6!}(\Theta w)^6 - \frac{10080}{9!}(\Theta w)^9 - \frac{2698080}{12!}(\Theta w)^{12} + O(w^{15})\right)$$

where $\Theta = 1.73179\ldots + 0.6303208\ldots\sqrt{-1}$. The algebraicity and near integrality of these coefficients are conjectural [**91**], so this expansion is only numerically correct, to the computed precision.

We now compute the image of the canonical map

$$X(\Gamma) = \Gamma\backslash\mathcal{H} \to \mathbb{P}^2$$
$$w \mapsto (x(w) : y(w) : z(w));$$

we find a unique quartic relation

$$216x^3z - 216xy^3 + 36xz^3 + 144y^3z - 7z^4 = 0$$

so at least numerically the curve X is nonhyperelliptic. Evaluating these power series at the ramification points, we find that the unique point above $f = 0$ is $(1 : 0 : 0)$, the point above $f = 1$ is $(1/6 : 0 : 1)$, and the three points above $f = \infty$ are $(0 : 1 : 0)$ and $((-1 \pm 3\sqrt{-3})/12 : 0 : 1)$.

The uniformizing map $f : X(\Gamma) \to X(\Delta) \cong \mathbb{P}^1$ is given by the reversion of an explicit ratio of hypergeometric functions:

$$f(w) = -\frac{1}{8}(\Theta w)^9 - \frac{11}{1280}(\Theta w)^{18} - \frac{29543}{66150400}(\Theta w)^{27} + O(w^{36}).$$

Using linear algebra, we find the expression for f in terms of x, y, z:

$$f(w) = \frac{-27z^3}{216x^3 - 108x^2z + 18xz^2 - 28z^3}.$$

Having performed this numerical calculation, we then verify on the curve $X(\Gamma)$ that this rational function defines a three-point cover with the above ramification points, as in Section 8.

An important feature of methods using modular forms is that it allows a much more direct algebraic approach to determining the algebraic structure on the target Riemann surface. There are no "parasitic" solutions to discard, just as when using the more advanced analytic method of Section 3. Moreover, the equation for the source surface are much easier to find than with the analytic method, where one typically needs to compute period matrices to high precision.

Question 4.13. — *What are the advantages of the* noncocompact *(q-expansions) and* cocompact *(power series expansions) approaches relative to one another? How far (degree, genus) can these methods be pushed? Can either of these methods be made rigorous?*

5. p-adic methods

As an alternative to complex analytic methods, we can use p-adic methods to find a solution; in this section we survey this method, and give a rather elaborate example of how this works in practice. It is simply the p-adic version of the complex analytic method, with the big distinction that finding a suitable approximation and then Hensel lifting can be much easier; usually finding a solution over a finite field suffices to guarantee convergence of Newton approximation.

Basic idea. — The p-adic method begins by finding a solution in a finite field of small cardinality, typically by exhaustive methods, and then lifts this solution using p-adic Newton iteration. Again, lattice methods can be then employed to recognize the solution over $\overline{\mathbb{Q}}$. *Turning the 'p-adic crank'*, as it is called, has been a popular method, rediscovered many times and employed in a number of contexts. Malle [**109**] used this method to compute polynomials with Galois groups M_{22}, $\mathrm{Aut}(M_{22})$, and $\mathrm{PSL}_3(\mathbb{F}_4) : 2$ over $\mathbb{Q}$. Elkies [**47**] computed a degree 28 cover $f : X \to \mathbb{P}^1$ with group $G = \mathrm{PSL}_2(\mathbb{F}_{27})$ via its action on $\mathbb{P}^1(\mathbb{F}_{27})$ modulo 29, and other work of Elkies [**48**], Watkins [**166**] and Elkies–Watkins [**50**] have also successfully used p-adic methods to compute Belyĭ maps. Elkin–Siksek [**51**] used this method and tabulated Belyĭ maps of small degree. Van Hoeij–Vidunas [**157**] used this approach to compute a list of examples whose branching is nearly regular, before extending the direct method [**158**] as explained in Section 2. More recently, Bartholdi–Buff–von Bothmer–Kröker [**7**] computed a Belyĭ map in genus 0 that is of degree 13 and which arises in a problem of Cui in dynamical systems; they give a relatively complete description of each of the steps involved.

A foundational result by Beckmann indicates which primes are primes of good reduction for the Belyĭ map; which primes, therefore, can be used in the procedure above.

Theorem 5.1 **(Beckmann [11])**. — *Let $f : X \to \mathbb{P}^1$ be a Belyĭ map and let G be the monodromy group of f. Suppose that $p \nmid \#G$. Then there exists a number field L such that p is unramified in L and f is defined over L with good reduction at all primes $\mathfrak{p}$ of L lying over p.*

Remark 5.2. — In fact, Beckmann proves as a consequence that under the hypotheses of the theorem, the prime p is unramified in the field of moduli K of f. (For the definition of the field of moduli, see Section 7.)

If one works with a pointed cover instead, then the statement of Beckmann's theorem is simpler [**18**, Theorem 3]. In the notation of this theorem, if p divides the order of one of the permutations σ then f has bad reduction at $\mathfrak{p}$ [**18**, Theorem 4]. But for those p that divide $\#G$ but not any of the ramification indices, it is much harder to find methods (beyond explicit calculation) to decide whether or not a model of f with good reduction over $\mathfrak{p}$ exists. Important work in this direction is due to Raynaud [**130**] and Obus [**126**].

Question 5.3. — *Can one perform a similar lifting procedure by determining solutions modulo primes where f has bad reduction?*

As the matrix of derivatives of the equations used is almost always of full rank (see Section 2), the most time-consuming part is usually the search for a solution over a finite field. In order for this method to be efficient, one must do better than simply running over the potential solutions over $\mathbb{F}_q$. Bartholdi–Buff–van Bothmer–Kröker describe [**7**,

Algorithm 4.7] a more careful method for genus 0, working directly with univariate polynomials (and rational functions) with coefficients in $\mathbb{F}_q$. In the example below, we show an approach that is similar in spirit to theirs and that works for hyperelliptic curves as well.

When the field of definition is "generic" in some sense, then there is often a split prime of small norm, so this method is often efficient in practice. The following question still merits closer investigation.

Question 5.4. — *How efficiently can a Belyĭ map be computed modulo a prime p? How far can one reduce the dimension of the affine space employed in the enumeration?*

In particular, can a "partial projection" (partial Gröbner basis) be computed efficiently to reduce the number of looping variables?

Example 5.5. — We return to the Belyĭ maps with ramification type $(6^1 1^1, 3^2 1^1, 2^3 1^1)$ considered in Example 4.8.

Theorem 5.1 suggests to reduce modulo 5 first. We put the ramification type $(6, 1)$ over ∞ and the corresponding points at ∞ and 0; we can do this without risking an extension of the field of definition since these points are unique. In the same way, we put the type $(3^2, 1)$ over 0 and the single point in this fiber at 1. This defines a reasonably small system over $\mathbb{F}_5$ of dimension 7, which could even be checked by enumeration. We get the solutions

$$f(t) = \frac{\alpha^8 (t-2)^3 (t+\alpha)^3 (t-1)}{t}$$

and its conjugate, where α is a root of the Conway polynomial defining $\mathbb{F}_{5^2}$ over $\mathbb{F}_5$, i.e., $\alpha^2 - \alpha + 2 = 0$. At the prime 13, we get two solutions defined over $\mathbb{F}_{13}$:

$$f(t) = \frac{-3(t^2+3t+8)^3 (t-1)}{t}, \quad f(t) = \frac{2(t^2+6)^3 (t-1)}{t}.$$

In both cases, the derivative matrices of the equations (with or without ASD) are non-singular, so we can lift to the corresponding unramified p-adic fields. After a few iterations of the second pair of solutions, we get the 13-adic approximations

$$\begin{aligned} f(t) &= (-3 - 5\cdot 13 - 13^2 + \dots)(t-1)t^{-1} \\ &\qquad \cdot (t^2 + (3 + 8\cdot 13 - 2\cdot 13^2 + \dots)t + (8 - 3\cdot 13 - 6\cdot 13^2 + \dots))^3 \\ f(t) &= (2 - 3\cdot 13 + 3\cdot 13^2 + \dots)(t-1)t^{-1} \\ &\qquad \cdot (t^2 + (-4\cdot 13 + 6\cdot 13^2 + \dots)t + (6 - 3\cdot 13^2 + \dots))^3. \end{aligned}$$

We continue, with quadratically growing accuracy, in order to use LLL in the end. This suggests a pair of solutions over $\mathbb{Q}(\sqrt{-3})$ given by

$$f(t) = \frac{-1+\sqrt{-3}}{4\sqrt{-3}^3 (\sqrt{-3}+2)^7} \frac{(162t^2 + 18(-\sqrt{-3}-6)t + (\sqrt{-3}+3))^3 (t-1)}{t}$$

and its conjugate. One verifies as in Section 8 that this yields a solution over $\mathbb{Q}(\sqrt{-3})$ to the given equations and that they are the requested Belyĭ maps. Though we stop here, one could further simplify the equation even further by suitable scalar multiplications in t, or even better, the general methods described in Section 8.

Example 5.6. — We now illustrate the complexities involved in employing the above method in an example. It arose during a study of Galois Belyĭ maps with monodromy group $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$, undertaken by Clark–Voight [**25**].

Consider the passport with uniform ramification orders $3, 5, 6$ and monodromy group $G = \mathrm{PSL}_2(\mathbb{F}_{11}) \leq S_{11}$. Here the embedding of G in S_{11} results from its conjugation action on the cosets of its exceptional subgroup A_5 (and indeed $\#G/\#A_5 = 660/60 = 11$).

Let $f : E \to \mathbb{P}^1$ be the degree 11 Belyĭ map defined by the above data, and let $\varphi : X \to \mathbb{P}^1$ be its Galois closure, with Galois group G. We anticipate [**25**] that φ with its Galois action is defined over an at most quadratic extension of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, in which case by the Galois correspondence the quotient map f will be defined over the same field. We confirm this by direct computation.

Using the representation of G above, we find that f has passport

$$(1, \mathrm{PSL}_2(\mathbb{F}_{11}), (3^3 1^2, 5^2 1^1, 6^1 3^1 2^1));$$

in accordance with the construction above, the ramification orders are divisors of $3, 5, 6$, and E has genus 1.

We distinguish the point of ramification degree 6 above ∞ and obtain a corresponding group law on E. We fix two more points by taking the other points above ∞ (with ramification 3 and 2, respectively) to be $(0, 1)$ and $(1, y_1)$. We write the equation

$$y^2 = \pi_3 x^3 + \pi_2 x^2 + (y_1^2 - \pi_3 - \pi_2 - 1)x + 1 = \pi(x)$$

for the curve E. The Belyĭ function f has the form

$$f(x, y) = \frac{q(x) + r(x)y}{(x-1)^2 x^3}$$

where $q(x) = q_8 x^8 + \cdots + q_0$ and $r(x) = r_6 x^6 + \cdots + r_0$ have degree $8, 6$ respectively and the numerator $f_{\mathrm{num}}(x, y) = q(x) + r(x)y$ vanishes to degree 3 at $(0, -1)$ and 2 at $(0, -y_1)$.

By the ramification description above 0, we must have

$$\begin{aligned} \mathrm{N}_{\overline{\mathbb{Q}}(x,y)/\overline{\mathbb{Q}}(x)}(f_{\mathrm{num}}(x, y)) &= q(x)^2 - r(x)^2 \pi(x) \\ &= q_8^2 x^3 (x-1)^2 s(x)^3 t(x) \end{aligned} \tag{5.7}$$

where $s(x) = x^3 + s_2 x^2 + s_1 x + s_0$ and $t(x) = x^2 + t_1 x + t_0$, and similarly above 1 we should have

$$\begin{aligned} \mathrm{N}_{\overline{\mathbb{Q}}(x,y)/\overline{\mathbb{Q}}(x)}((f(x, y) - 1)_{\mathrm{num}}) &= (q(x) - (x-1)^2 x^3)^2 - r(x)^2 \pi(x) \\ &= q_8^2 x^3 (x-1)^2 u(x) v(x) \end{aligned} \tag{5.8}$$

where $u(x) = x^2 + u_1 x + u_0$ and $v(x) = x + v_0$.

An approach using Gröbner basis techniques utterly fails here, given the number of variables involved. This calculation is also made more difficult by the possibility that other Belyĭ covers will intervene: the Mathieu group $M_{11} \hookrightarrow S_{11}$ also has a $(3, 5, 6)$ triple of genus 1, and it is a priori conceivable that S_{11} occurs as well. Discarding these parasitic solutions is a nontrivial task until one has already computed all of them along with the correct ones, just as in Section 2.

As explained above, we search for a solution in a finite field $\mathbb{F}_q$, lift such a solution using Hensel's lemma (if it applies), and then attempt to recognize the solution p-adically as an algebraic number using the LLL lattice reduction algorithm. The primes of smallest norm in the field $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ that are relatively prime to $\#\,\mathrm{PSL}_2(\mathbb{F}_{11})$ have norm $q = 49, 59$, so

there is no hope of simply running over all the $\mathbb{F}_q$-rational values in the affine space in $y_1, \pi, q, r, s, t, u, v$, which is 28-dimensional.

We speed up the search with a few tricks. Subtracting the two equations (5.7)–(5.8), we have

$$q_8^2 s(x)^3 t(x) - 2q(x) + (x-1)^2 x^3 = r_8^2 u(x)^5 v(x).$$

Comparing coefficients on both sides, by degree we see that the coefficients of x^9 and x^{10} of $s(x)^3 t(x)$ and $u(x)^5 v(x)$ must agree. So we precompute a table of the possible polynomials of the form $u(x)^5 v(x)$; there are $O(q^3)$ such, and we sort them for easy table lookup. Then, for each of the possible polynomials of the form $s(x)^3 t(x)$, of which there are $O(q^5)$, we match the above coefficients. Typically there are few matches. Then for each $q_8^2 \in \mathbb{F}_q^{\times 2}$, we compute $q(x)$ as

$$q(x) = \frac{1}{2}\left(q_8^2 s(x)^3 t(x) - q_8^2 u(x)^5 v(x) - (x-1)^2 x^3\right).$$

From equation (5.7) we have

$$q(x)^2 - q_8^2 (x-1)^2 x^3 s(x)^3 t(x) = \pi(x) r(x)^2,$$

so we compute the polynomial on the right and factor it into squarefree parts. If the corresponding $\pi(x)$ has degree 3, then we find $r(x)$ as well, whence also our solution.

Putting this on a cluster at the Vermont Advanced Computing Center (VACC) using Magma [**19**], after a few days we have our answer. We find several solutions in $\mathbb{F}_{49}$ but only one solution lifts p-adically without additional effort; it turns out the Jacobian of the corresponding system of equations is not of full rank. After some effort (see also Section 8), we recognize this cover as an M_{11}-cover with ramification $(3, 5, 6)$, defined over the number field $\mathbb{Q}(\alpha)$ where

$$\alpha^7 - \alpha^6 - 8\alpha^5 + 21\alpha^4 + 6\alpha^3 - 90\alpha^2 + 60\alpha + 60 = 0.$$

We find 62 solutions in $\mathbb{F}_{59}$. Note that the M_{11}-covers above do not reappear since there is no prime of norm 59 in $\mathbb{Q}(\alpha)$. Only 8 of these solutions yield covers with the correct ramification data; our above conditions are necessary, but not sufficient, as we have only considered the x-coordinates and not the y-coordinates. These 8 covers lift to a single Galois orbit of curves defined over the field $\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{b})$ where

$$b = 4\sqrt{3} + \frac{11 + \sqrt{5}}{2};$$

with $N(b) = 11^2$; more elegantly, the extension of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ is given by a root β of the equation

$$T^2 - \frac{1 + \sqrt{5}}{2} T - (\sqrt{3} + 1) = 0.$$

The elliptic curve E has minimal model

$$\begin{aligned}
y^2 &+ ((\tfrac{1}{2}(13\sqrt{5}+33)\sqrt{3}+\tfrac{1}{2}(25\sqrt{5}+65))\beta + (\tfrac{1}{2}(15\sqrt{5}+37)\sqrt{3}+(12\sqrt{5}+30)))xy \\
&+ (((8\sqrt{5}+15)\sqrt{3}+\tfrac{1}{2}(31\sqrt{5}+59))\beta + (\tfrac{1}{2}(13\sqrt{5}+47)\sqrt{3}+\tfrac{1}{2}(21\sqrt{5}+77)))y \\
&= x^3 + ((\tfrac{1}{2}(5\sqrt{5}+7)\sqrt{3}+\tfrac{1}{2}(11\sqrt{5}+19))\beta + (\tfrac{1}{2}(3\sqrt{5}+17)\sqrt{3}+(2\sqrt{5}+15)))x^2 \\
&+ ((\tfrac{1}{2}(20828483\sqrt{5}+46584927)\sqrt{3}+\tfrac{1}{2}(36075985\sqrt{5}+80687449))\beta \\
&\quad + (\tfrac{1}{2}(21480319\sqrt{5}+48017585)\sqrt{3}+\tfrac{1}{2}(37205009\sqrt{5}+83168909)))x \\
&+ (((43904530993\sqrt{5}+98173054995)\sqrt{3}+\tfrac{1}{2}(152089756713\sqrt{5}+340081438345))\beta \\
&\quad + ((45275857298\sqrt{5}+101240533364)\sqrt{3}+(78420085205\sqrt{5}+175353747591))).
\end{aligned}$$

The j-invariant of E generates the field $\mathbb{Q}(\sqrt{3},\sqrt{5},\beta)$, so this is its minimal field of definition. This confirms that $\varphi : X \to \mathbb{P}^1$ as a G-cover is defined over an at most quadratic extension of $\mathbb{Q}(\sqrt{3},\sqrt{5})$ contained in the ray class field of conductor 11∞, as predicted by the results of Clark–Voight [**25**].

6. Galois Belyĭ maps

In this short section we sketch some approaches for calculating Galois Belyĭ maps, i.e., those Belyĭ maps $f : X \to \mathbb{P}^1$ corresponding to Galois extensions of function fields. The flavor of these computations is completely different from those in the other sections, as the representation-theoretic properties of the Galois group involved are used heavily. In light of the Galois correspondence, all Belyĭ maps are essentially known once the Galois Belyĭ maps are known; however, the growth in degree between the degree of the Belyĭ map and that of its Galois closure makes it very difficult in general to make this remark a feasible approach to computing general Belyĭ maps. We therefore consider the subject only in itself, and even here we limit ourselves to the general idea: exploiting representations and finding invariant functions.

The Galois Belyĭ maps in genus 0 correspond to the regular solids, and can be computed using the direct method (see the end of Section 2). The most difficult case, that of the icosahedron, was calculated first by Klein [**90**]. The Galois Belyĭ maps in genus 1 only occur on curves with CM by either $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-1})$, and can therefore be calculated by using explicit formulas for isogenies; see work of Singerman–Syddall [**147**].

So it remains to consider the case of genus ≥ 2, where Belyĭ maps are related with hyperbolic triangle groups (see Section 4). In genus ≥ 2, Wolfart [**173**] has shown that Galois Belyĭ maps can be identified with quotient maps of curves with many automorphisms, that is, those curves that do not allow nontrivial deformations that leave the automorphism group intact and whose automorphism group therefore defines a zero-dimensional subscheme of the moduli space of curves $\mathcal{M}_g$ of genus $g \geq 2$. Wolfart [**171**] compares these Belyĭ maps with the related phenomenon of Jacobians of CM type, which define zero-dimensional subschemes of the moduli space of principally polarized abelian varieties $\mathcal{A}_g$. In particular, the CM factors of the Jacobians of the Galois Belyĭ curves that arise from one-dimensional subrepresentations of the automorphism group are essentially known; they come from Fermat curves [**171**, §4]. (Wolfart [**171**, §6.5] exhibits Hurwitz curves that are not of CM type and that therefore cannot come from Fermat curves.)

A fundamental technique for proving these theorems is to determine the representation of the automorphism group on the space of differentials, first considered by Chevalley and Weil [**24**]; this is elaborated by Berry–Tretkoff [**14**] and Streit [**150**]. Once this is done, one typically recovers the curve by determining the shape of its canonical embedding, often an intersection of quadrics. (When the canonical embedding is not injective, the situation is even simpler; since the hyperelliptic involution is central in the automorphism group, this reduce to the calculations in genus 0 mentioned above.) The particular form of the equations is then determined by being fixed under the action of the automorphism group, which acts by linear transformations.

Question 6.1. — *Can the representation of the automorphism group G on the space of differentials be used to give a rigorous algorithm for the computation of G-Galois Belyĭ maps (with a bound on the running time)?*

Put another way, computing a Galois Belyĭ map amounts to determining G-invariant polynomials of a given degree; in some cases, there is a unique such polynomial with given degree and number of variables, and so it can be found without any computation.

Example 6.2. — We illustrate the invariant theory involved by giving an example of a calculation of a quotient map $X \to X/\operatorname{Aut}(X) \cong \mathbb{P}^1$ that turns out to be a Belyĭ map; the example was suggested to us by Elkies.

Consider the genus 9 curve X defined by the following variant of the Bring equations:

$$\begin{aligned} v + w + x + y + z &= 0, \\ v^2 + w^2 + x^2 + y^2 + z^2 &= 0, \\ v^4 + w^4 + x^4 + y^4 + z^4 &= 0. \end{aligned}$$

This curve is known as Fricke's octavic curve, and it was studied extensively by Edge [**44**]. There is an obvious linear action by S_5 on this curve by permutation of coordinates. To find coordinates on the quotient X/S_5 it therefore suffices to look at the symmetric functions in the variables v, w, x, y, z. We see that the power sums with exponents $1, 2, 4$ vanish on X. Since the ring of invariants function for S_5 is generated by the power sums of degree at most 5, this suggests that we cook up a function from the power sums p_3 and p_5 of degree 3 and 5. These functions do not have the same (homogeneous) degree; to get a well-defined function, we consider their quotient $f = (p_3^5 : p_5^3)$ as a morphism from $f : X \to \mathbb{P}^1$.

The intersection of the hyperplanes defined by $p_3 = 0$ and $p_5 = 0$ with X are finite; indeed, this is obvious since the corresponding functions do not vanish indentically on X. By Bézout's theorem, these zero loci are of degrees $24, 40$. But whereas in the former case one indeed obtains 24 distinct geometric points in the intersection, one obtains only 20 geometric points in the latter case. This shows that the ramification indices over 0 and ∞ of the degree 120 morphism f are 6 and 5.

This is in fact already enough to conclude that there is only one other branch point for q. Indeed, the orbifold $X/\operatorname{Aut}(X)$ is uniformized by the upper half plane $\mathcal{H}$ since the genus 9 curve X is, so $X/\operatorname{Aut}(X)$ is a projective line with at least 3 branch points for the quotient by the action of S_5. On the other hand, the Riemann–Hurwitz formula shows that adding a single minimal contribution of 2 outside the contributions 5 and 6 already known from ∞ and 0 already makes the genus grow to 9, so additional ramification is

impossible. The additional branch point of f can be found by considering the divisor of df on X; this point turns out to be $-(15/2)^2$. So the morphism $f : X \to \mathbb{P}^1$ defined by

$$f(v,w,x,y,z) = \frac{-2^2 p_3^5}{15^2 p_5^3} = -\left(\frac{2}{15}\right)^2 \frac{(v^3+w^3+x^3+y^3+z^3)^5}{(v^5+w^5+x^5+y^5+z^5)^3}$$

realizes the quotient $X \to X/S_5$ as a Belyĭ map. Moreover, we see that the Galois action is defined over $\mathbb{Q}$, since it is given by permuting the given coordinate functions on X.

In fact we have an isomorphism $\mathrm{Aut}(X) \cong S_5$ since $\mathrm{Aut}(X)$ cannot be bigger than S_5; such a proper inclusion would give rise to a Fuchsian group properly containing the triangle group $\Delta(2,5,6)$, whereas on the other hand this group is maximal (by work of Takeuchi [**153**], or more generally see Singerman [**146**] or Greenberg [**63**, Theorem 3B]).

We therefore have found a Galois cover realizing S_5 with ramification indices $2, 5, 6$. It turns out that this is the only such cover up to isomorphism. Considering the exceptional isomorphism $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$, we see that our calculation also yields a Galois cover realizing a projective linear group.

7. Field of moduli and field of definition

Considering Grothendieck's original motivation for studying dessins, it is important to consider the rather delicate issue of fields of definition of Belyĭ maps. In fact this is not only an engaging question on a theoretic level, but it is also interesting from a practical point of view. Indeed, as we have seen in our calculations above, it is often necessary to determine equations for Belyĭ maps by recognizing complex numbers as algebraic numbers. A bound on the degree K is an important part of the input to the LLL algorithm that is typically used for this. Moreover, having an estimate for the degree of K is a good indication of how computable a given cover will be—if the estimate for the size is enormous, we are very unlikely to succeed in practice!

Field of moduli. — For a curve X defined over $\overline{\mathbb{Q}}$, the field of moduli $M(X)$ of X is the fixed field of the group $\{\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) : X^\tau \cong X\}$ on $\overline{\mathbb{Q}}$, where as before X^τ is the base change of X by the automorphism $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (obtained by applying the automorphism τ to the defining equations of an algebraic model of X over $\overline{\mathbb{Q}}$). One similarly defines the field of moduli of a Belyĭ map: $M(f)$ is the fixed field of $\{\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) : f^\tau \cong f\}$ with isomorphisms as defined in Section 1.

Now let $f : X \to \mathbb{P}^1$ be a Belyĭ map with monodromy representation $\sigma : F_2 \to S_d$ and monodromy group G. By Theorem 1.6, the monodromy group G of f, considered as a conjugacy class of subgroups of S_d, is invariant under the Galois action. Therefore, given $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the conjugated morphism $f^\tau : X^\tau \to \mathbb{P}^1$ is a Belyĭ map, and its monodromy representation $\sigma^\tau : F_2 \to S_d$, which is well-defined up to conjugation, can be taken to have image G. Because the Galois action preserves the monodromy group up to conjugation and the ramification indices [**84**], the Belyĭ map f^τ has the same passport P as f. We therefore get an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set S of Belyĭ maps with passport P. Since the stabilizer of an element of S under this action has index at most $\#S$ in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we get the following result.

Proposition 7.1. — *Let f be a Belyĭ map with passport P and field of moduli K. Then the degree $[K : \mathbb{Q}]$ is bounded above by the size of P.*

As mentioned at the end of Section 1, finding better bounds than in Proposition 7.1 is far from trivial and a subject of ongoing research. Experimentally, the bound is often an equality for generic (non-Galois) Belyĭ maps.

Rigidified categories. — Working with Galois Belyĭ maps and the additional structure coming from their automorphism group naturally leads one to consider a new, more rigidified category [**38**]. A G-Belyĭ map is a pair (f, i), where $f : X \to \mathbb{P}^1$ is a Galois Belyĭ map and $i : G \xrightarrow{\sim} \mathrm{Mon}(f)$ is an isomorphism of the monodromy group of f with G. A morphism of G-Belyĭ maps from (f, i) to (f', i') is an isomorphism of Belyĭ maps $h : X \xrightarrow{\sim} X'$ that identifies i with i', i.e., such that

$$h(i(g)x) = i'(g)h(x) \text{ for all } g \in G \text{ and } x \in X. \tag{7.2}$$

A G-permutation triple is a triple of permutations $(\sigma_0, \sigma_1, \sigma_\infty)$ in G such that $\sigma_0\sigma_1\sigma_\infty = 1$ and such that $\sigma_0, \sigma_1, \sigma_\infty$ generate G. A morphism of G-permutation triples is an isomorphism of permutation triples induced by simultaneous conjugation by an element in G. The main equivalence is now as follows.

Proposition 7.3. — *The following categories are equivalent:*

(i) *G-Belyĭ maps;*
(ii) *G-permutation triples;*
(iii) *surjective homomorphisms $F_2 \to G$.*

We leave it to the reader to similarly rigidify the notion of dessins; it will not be needed in what follows.

We will need a slight weakening of this notion in the following section. A weak G-Belyĭ map is a pair (f, i), where $f : X \to \mathbb{P}^1$ is a Galois Belyĭ map and $i : H \hookrightarrow \mathrm{Mon}(f)$ is an isomorphism of the monodromy group of f with a subgroup H of G. A morphism of weak G-Belyĭ maps from (f, i) to (f', i') is an isomorphism of Belyĭ maps $h : X \xrightarrow{\sim} X'$ such that (7.2) holds up to conjugation, i.e., such that there exists a $t \in G$ such that $h(i(g)x) = i'(tgt^{-1})h(x)$ for all $g \in G$ and $x \in X$.

A weak G-permutation triple is a triple of permutations $(\sigma_0, \sigma_1, \sigma_\infty)$ in G such that $\sigma_0\sigma_1\sigma_\infty = 1$. A morphism of weak G-permutation triples is an isomorphism of permutation triples induced by simultaneous conjugation by an element in G. The equivalence of Proposition 7.3 now generalizes to the following result.

Proposition 7.4. — *The following categories are equivalent:*

(i) *weak G-Belyĭ maps;*
(ii) *weak G-permutation triples;*
(iii) *homomorphisms $F_2 \to G$.*

The set of Belyĭ maps of degree d can be identified with the set of weak S_d-Belyĭ maps. In particular, whereas G-Belyĭ maps are always connected, weak G-Belyĭ maps need not be. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of (weak) G-Belyĭ maps, so we can again define the field of moduli of these rigidified Belyĭ maps.

Having introduced weak G-Belyĭ maps, it makes sense to consider passports up to the action of the monodromy group $G \subset S_d$ instead of the full group S_d. We accordingly define the refined passport of a (not necessarily Galois) Belyĭ map $f : X \to \mathbb{P}^1$ to be the triple (g, G, C), where g is the genus of X, the group G is the monodromy group of f,

and $C = (C_0, C_1, C_\infty)$ are the conjugacy classes of $\sigma_0, \sigma_1, \sigma_\infty$ in G, not the conjugacy classes in S_d included in the (usual) passport.

Fried [**57**] shows how the conjugacy classes C_i change under the Galois action. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, let $n = \#G$, and let $\zeta_n \in \overline{\mathbb{Q}}$ be a primitive n-th root of unity. Then σ sends ζ_n to ζ_n^a for some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. We obtain new conjugacy classes C_i^a by raising a representative of C_i to the ath power. Then for any character χ of G we have

$$\sigma(\chi(C_i)) = \chi(C_i^a). \tag{7.5}$$

Let $\mathbb{Q}(\chi(C_i))$ be the field generated by the character values of the conjugacy classes C_i. We have $\mathbb{Q}(\chi(C_i)) = \mathbb{Q}$ if and only if all conjugacy classes of G are rational, as for instance in the case $G = S_d$.

Proposition 7.6. — *Let (f, i) be a weak G-Belyĭ map with refined passport R and field of moduli K as a weak G-Belyĭ map. Then the degree $[K : \mathbb{Q}(\chi(C_i))]$ is bounded above by the size of R.*

Calculating in the category of weak G-Belyĭ maps can be useful even when considering Belyĭ maps without this additional structure. More precisely, this is useful when using formulas that approximate the size of a passport. To this end, let G be a finite group and let C_0, C_1, C_∞ be conjugacy classes in G. Let S be the set of isomorphism classes of weak G-Belyĭ maps $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ with the property that $\sigma_i \in C_i$ for $i \in \{0, 1, \infty\}$. Then a formula that goes back to Frobenius (see Serre [**142**, Theorem 7.2.1]) shows that

$$\sum_{(f,i)\in S} \frac{1}{\mathrm{Aut}_G(f, i)} = \frac{\#C_0 \#C_1 \#C_\infty}{(\#G)^2} \sum_\chi \frac{\chi(C_0)\chi(C_1)\chi(C_\infty)}{\chi(1)}. \tag{7.7}$$

Here the automorphism group $\mathrm{Aut}_G(f, i)$ is the group of automorphisms of (f, i) as a weak G-Belyĭ map. The sum on the left of (7.7) runs over all weak Belyĭ maps with the aforementioned property; in particular, one often obtains non-transitive solutions that one does not care about in practice.

When working with mere Belyĭ maps (without rigidification as a weak G-Belyĭ map), it can still be useful to consider the estimate (7.7) when the monodromy group of the Belyĭ map is question is included in G. We illustrate this by a few concrete examples.

Example 7.8. — We start by taking G to be a full symmetric group and give the above-mentioned estimate for the number of genus 0 Belyĭ maps with ramification passport

$$(0, (3^2 2^3, 5^1 4^1 2^1 1^1, 6^1 4^1 2^1)),$$

Before giving it, we calculate the possible permutation triples up to conjugacy directly using Lemma 1.7. This shows that the number of solutions is 583, of which 560 are transitive. The transitive solutions all have monodromy group S_{23} and hence trivial automorphism group. On the other hand, the Serre estimate (7.7) equals $567\frac{1}{4}$, which more precisely decomposes as

$$567\frac{1}{4} = \frac{560}{1} + \frac{1}{1} + \frac{3}{2} + \frac{19}{4};$$

of the 23 nontransitive solutions, there is only one with trivial automorphism group, whereas there are 3 (resp. 19) with automorphism group of cardinality 2 (resp. 4). For each of the nontransitive solutions, the associated Belyĭ maps are disjoint unions of curves of genus 1, such as those corresponding to the products of the genus 1 Belyĭ maps with ramification types $(2^3, 5^1 1^1, 6^1)$ (which always have trivial automorphism group) with

those with ramification types $(3^2, 4^1 2^1, 4^1 2^1)$ (which have either 1 or 2 automorphisms, depending on the solution).

Example 7.9. — Another example is the case $(0, H, (4^4 2^2 1^3, 4^4 2^2 1^3, 5^4 1^3))$ with $H \leq M_{23}$. We can identify M_{23}-conjugacy classes with S_{23}-conjugacy classes for these groups, as the conjugacy classes of S_{23} do not split upon passing to M_{23}.

The calculations are much more rapid working with M_{23} than for the full group S_{23}. We obtain the estimate 909, which fortunately enough equals the exact number of solutions because the corresponding subgroups of M_{23} all have trivial centralizer; this is not the case when they are considered as subgroups of S_{23}. Of these many solutions, it turns out that only 104 are transitive.

As mentioned before, this estimate only gives the number of weak M_{23}-Belyĭ maps; accordingly, permutation triples are only considered isomorphic if they are conjugated by an element of M_{23} rather than S_{23}. However, since M_{23} coincides with its own normalizer in S_{23}, this coincides with the number of solutions under the usual equivalence. Directly working with the group M_{23} indeed saves a great deal of computational overhead in this case.

An explicit (but complicated) formula, using Möbius inversion to deal with the disconnected Belyĭ maps, was given by Mednykh [**121**] this vein; in fact, his formula can be used to count covers with specified ramification type of an arbitrary Riemann surface.

Finally, we mention that in the Galois case, the situation sometimes simplifies: there are criteria [**27, 85**] for Galois Belyĭ maps to have cyclotomic fields of moduli, in which case the Galois action is described by a simple powering process known as Wilson's operations. Additionally, Streit–Wolfart [**152**] have calculated the field of moduli of an infinite family of Belyĭ maps whose Galois group is a semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ of cyclic groups of prime order.

Field of moduli versus field of definition. — We have seen that in all the categories of objects over $\overline{\mathbb{Q}}$ considered so far (curves, Belyĭ maps, etc.) there is a field of moduli for the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Given an object Y of such a category with field of moduli M, it is reasonable to ask whether Y is defined over M, i.e., if there exists an object Y_M in the appropriate category over M that is isomorphic with Y over $\overline{\mathbb{Q}}$, in which case M is said to be a field of definition of Y. For example, if $Y = (X, f)$ is a Belyĭ map over $\overline{\mathbb{Q}}$, this means that there should exist a curve X_M over M and a Belyĭ map $f_M : X_M \to \mathbb{P}^1_M$ such that (X, f) can be obtained from (X_M, f_M) by extending scalars to $\overline{\mathbb{Q}}$.

We first consider the case of curves. Curves of genus at most 1 are defined over their field of moduli. But this ceases to be the case for curves of larger genus in general, as was already observed by Earle [**42**] and Shimura [**145**]. The same is true for Belyĭ maps and G-Belyĭ maps. This issue is a delicate one, and for more information, we refer to work of Coombes–Harbater [**28**], Dèbes–Ensalem [**39**], Dèbes–Douai, [**38**], and Köck [**92**].

The obstruction can be characterized as a lack of rigidification. For example, a curve furnished with an embedding into projective space is trivially defined over its field of moduli (as a projectively embedded curve). Additionally, marking a point on the source X of a Belyĭ map and passing to the appropriate category, [**18**, Theorem 2] states that the field of moduli is a field of definition for the pointed Belyĭ curve [**18**, Theorem 2]; however, this issue seems quite subtle, and in [**92**] only auxiliary points with trivial stabilizer in $\mathrm{Aut}(X)$ are used. Note that the more inclusive version of this rigidification (with possibly

non-trivial stabilizer) was considered in Section 4 (see e.g. (4.3)). As mentioned at the beginning of the previous subsection, this implication can then be applied to give an upper bound on the degree of the field of definition of a Belyĭ map, an important bit of information needed when for example applying LLL to recognize coefficients algebraically.

Note that for a Belyĭ map $f : X \to \mathbb{P}^1$, the curve X may descend to its field of moduli in the category of curves while f does not descend to this same field of moduli in the category of Belyĭ maps. Indeed, this can be seen already for the example $X = \mathbb{P}^1$, as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of genus 0 dessins. In general, the problem requires careful consideration of obstructions that lie in certain Galois cohomology groups [**38**].

Remark 7.10. — Although in general we will have to contend with arbitrarily delicate automorphism groups, Couveignes [**31**] proved that every curve defined over a number field K admits a Belyĭ map without automorphisms defined over K. This map will then necessarily not be isomorphic to any of its proper conjugates.

On top of all this, a Belyĭ map may descend to its field of moduli in the weak sense, i.e., as a cover of a possibly non-trivial conic ramified above a Galois-stable set of three points, rather than in the strong sense, as a cover of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ (i.e., in the category of Belyĭ maps over the field of moduli). This distinction also measures the descent obstruction for hyperelliptic curves, as in work of Lercier–Ritzenthaler–Sijsling [**103**]. For Belyĭ maps, a deep study of this problem in genus 0, beyond the general theory, was undertaken by Couveignes [**29**, §§4–7]: he shows that for the clean trees, those Belyĭ maps with a single point over ∞ and only ramification index 2 over 1, on the set of which $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts faithfully, the field of moduli is always a field of definition in the strong sense. Moreover, he shows that in genus 0, the field of moduli is always a field of definition in the weak sense as long as the automorphism group of the Belyĭ map is not cyclic of even order, and in the strong sense as long as the automorphism group is not cyclic.

These considerations have practical value in the context of computations. For example, Couveignes [**29**, §10] first exhibits a genus 0 Belyĭ map that descends explicitly to $\mathbb{Q}$ in the strong sense. Then, due to the presence of non-trivial automorphisms of this Belyĭ map, one can realize it as a morphism $f : C \to \mathbb{P}^1$ for infinitely many mutually non-isomorphic conics C over $\mathbb{Q}$. And by choosing C appropriately (not isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$), Couveignes manages to condense his equations from half a page to a few lines. Further simplification techniques will be considered in the next section.

We mention some results on the field of moduli as a field of definition that are most useful for generic (G-)Belyĭ maps.

1. If a curve or (G-)Belyĭ map has trivial automorphism group, then it can be defined over its field of moduli, by Weil's criterion for descent [**167**].
2. If the center of the monodromy group of a Galois Belyĭ map is trivial, then it can be defined over its field of moduli by the main result in the article by Dèbes–Douai [**38**].
3. A G-Belyĭ map, when considered in the category of Belyĭ maps (without extra structure) is defined over its field of moduli as a Belyĭ map [**28**].

To give an impression of the subtleties involved, we further elaborate on Example 6.2 from the previous section. Along the way, we will illustrate some of the subtleties that arise when considering fields of moduli. As we will see, these subtleties correspond with very natural questions on the level of computation.

Example 7.11. — Since $\Delta(3,5,5)$ is a subgroup of $\Delta(2,5,6)$ of index 2, we also obtain from this example a Belyĭ map with indices $3,5,5$ for the group A_5 by taking the corresponding quotient. Indeed, ramification can only occur over the points of order 2 and 6, which means that in fact the cover is a cyclic degree 2 map of conics ramifying of order 2 over these points and under which the point of order 5 has two preimages. An equation for this cover (which is a Belyĭ map) can now be found by drawing an appropriate square root of the function $(s_3^5/s_5^3) + (15/2)^2$ (which indeed ramifies of order 6 over ∞ and of order 2 over 0) and sending the resulting preimages $\pm 15/2$ of the point of order 5 to 0 and 1, respectively.

Alternatively, we can calculate as follows. The full ring of invariant homogeneous polynomials for A_5 (acting linearly by permutation of coordinates) is generated by the power sums $p_1, \ldots, p_5$ and the Vandermonde polynomial

$$a = (v-w)(v-x)(v-y)(v-z)(w-x)(w-y)(w-z)(x-y)(x-z)(y-z).$$

One easily determines the expression for a^2 in terms of the p_i; setting $p_1 = p_2 = p_4 = 0$, we get the relation

$$a^2 = \frac{4}{45} s_3^5 s_5 + 5 s_5^3.$$

This suggests that to get a function realizing the quotient $X \to X/A_5$, we take the map $g : X \to C$, where C is the conic

$$C : 45y^2 = 4xz + 225z^2$$

and g is given by

$$g(v,w,x,y,z) = (s_3^5 : a s_5 : s_5^3).$$

Note that Q admits the rational point $(1:0:0)$.

This result is not as strong as one would like. As we have seen when calculating the full quotient f, the branch points of g of order 5 on C satisfy $(x:z) = (0:1)$. But the corresponding points are only defined over $\mathbb{Q}(\sqrt{5})$, so this is a descent of a Belyĭ map in the weak sense. We explain at the group-theoretical level what other kinds of descent can be expected.

There are actually two Galois covers with ramification indices $(3,5,5)$ for A_5 up to isomorphism. The other cover is not found as a subcover of f; when composing with the same quadratic map, we instead get a Galois Belyĭ map whose Galois group is the direct product of A_5 and $\mathbb{Z}/2\mathbb{Z}$. The corresponding curve is given by taking the hyperelliptic cover ramified over the vertices of an icosahedron, leading to the equation

$$t^2 = s^{20} + 228 s^{15} + 494 s^{10} - 228 s^5 + 1.$$

In particular, this means that the Galois orbit of these covers consists of a single isomorphism class, as their monodromy groups upon composition differ [**174**]. As mentioned above, an A_5-Belyĭ map, considered as a mere Belyĭ map, is defined over its field of moduli as a Belyĭ map, so our equations above can be twisted to a Belyĭ map over $\mathbb{Q}$, that is, with ramification at three rational points.

However, the Galois cover does *not* descend as an A_5-Belyĭ map (so in the strong sense, as a Galois cover unramified outside $\{0,1,\infty\}$). Indeed, the character table of A_5 is only defined over $\mathbb{Q}(\sqrt{5})$. Twisting may therefore give a cover defined over $\mathbb{Q}$, but the Galois action will then only be defined over $\mathbb{Q}(\sqrt{5})$ and be accordingly more complicated. We therefore forgo this calculation and content ourselves with the symmetric form above.

For more on the questions considered in this section, see also further work by Couveignes [**30**], and in a similar vein, the work of van Hoeij–Vidunas on covers of conics [**158**, §§3.3–3.4], [**157**, §4]. We again refer to the fundamental paper of Dèbes–Douai [**38**], in which strong results are given for both Belyĭ maps and G-Belyĭ maps that suffice in many concrete situations. Admittedly, this subject is a delicate one, and we hope that computations will help to further clarify these nuances.

8. Simplification and verification

Once a potential model for a Belyĭ map has been computed, it often remains to simplify the model as much as possible and to verify its correctness (independently of the method used to compute it). The former problem is still open in general; the latter has been solved to a satisfactory extent.

Simplification. — By simplifying a Belyĭ map $f : X \to \mathbb{P}^1$, we mean to reduce the total (bit) size of the model. Lacking a general method for doing this, we focus on the following:

1. If X is of genus 0, we mean to find a coordinate on X that decreases the (bit) size of the defining coefficients of f.
2. If X is of strictly positive genus, we mean to simplify the defining equations for X. (In practice, this will also lead to simpler coefficients of the Belyĭ map f.)

Problem (1) was considered by van Hoeij–Vidunas [**158**, §4.2] under the hypotheses that one of the ramification points has a minimal polynomial of degree at most 4; one tries to find a smaller polynomial defining the associated number field and changes the coordinate accordingly, which typically yields one a simpler expression of the Belyĭ map.

Problem (1) is directly related with Problem (2) for hyperelliptic curves, since simplifying the equations for hyperelliptic curves over a field K boils down to finding a small representative of the $\mathrm{GL}_2(K)$-orbit of a binary form. Typically one also requires the defining equation to have integral coefficients. For the case $K = \mathbb{Q}$, this leads one to consider the problem of finding simpler representations for binary forms under the action of the group of integral matrices $\mathrm{SL}_2(\mathbb{Z})$. This is considered by Cremona–Stoll [**37**], using results from Julia [**87**] to find a binary quadratic covariant, to which classical reduction algorithms are then applied. The resulting algorithms substantially reduce the height of the coefficients of the binary form in practice, typically at least halving the bit size of already good approximations in the applications [**37**]. A generalization to, and implementation for, totally real fields is given in Bouyer–Streng [**21**].

In fact, corresponding results for the simplification of Belyĭ maps can be obtained by taking the binary form to be the product of the numerator and denominator of the hyperelliptic Belyĭ map. That the resulting binary form may have double roots and hence may not correspond to hyperelliptic curves is no problem; see the discussion by Cremona–Stoll [**37**, after Proposition 4.5].

This problem of reduction is intimately related with the problem of finding a good model of a Belyĭ map or hyperelliptic curve over $\mathbb{Z}$. Note that even for the case $K = \mathbb{Q}$ we have not yet used the full group $\mathrm{GL}_2(\mathbb{Q})$; the transformations in $\mathrm{SL}_2(\mathbb{Z})$ considered by Cremona and Stoll preserve the discriminant, but it could be possible that a suitable rational transformation decreases this quantity while still preserving integrality of the binary form. An approach to this problem is given by Bouyer–Streng [**21**, §3.3].

In general, Problem (2) is much harder, if only because curves of high genus become more difficult to write down.

Question 8.1. — *Are there general methods to simplifying equations of curves defined over a number field in practice?*

Verification. — Let $f : X \to \mathbb{P}^1$ be a map defined over a number field K of degree d that we suspect to be a Belyĭ map of monodromy group G, or more precisely to correspond to a given permutation triple σ or a given dessin D. To show that this is in fact the case, we have to verify that

(i) f is indeed a Belyĭ map;
(ii) f has monodromy group G; and
(iii) f (or its monodromy representation) corresponds to the permutation triple σ; or
(iii)' the pullback under f of the closed interval $[0, 1]$ is isomorphic (as a dessin) to D.

This verification step is necessary for all known methods, and especially when using the direct method from Section 2; the presence of parasitic solutions means that not even all solutions of the corresponding system of equations will be Belyĭ maps, let alone Belyĭ maps with correct monodromy group or pullback.

Point (i) can be computationally expensive, but it can be accomplished, by using the methods of computational algebraic geometry. Not even if $X = \mathbb{P}^1$ is this point trivial, since although verifying that a Belyĭ map is returned is easy for dessins of small degree, we need better methods than direct factorization of the polynomials involved as the degree mounts.

As for point (ii), one simple sanity check is to take a field of definition K for f and then to substitute different K-rational values of $t \notin \{0, 1, \infty\}$. One obtains an algebra that is again an extension of K of degree d and whose Galois group H must be a subgroup of the monodromy group G by an elementary specialization argument. So if we are given a finite number of covers, only one of which has the desired monodromy group G, then to eliminate a cover in the given list it suffices to show that specializing this cover gives a set of cycle type in H that is not contained in the given monodromy group G when considered as a subgroup of S_d. Such cycle types can be obtained by factoring the polynomial modulo a small prime of K.

There are many methods to compute Galois groups effectively in this way; a general method is given by Fieker–Klüners [**54**]. This method proceeds by computing the maximal subgroups of S_d and checking if the Galois group lies in one of these subgroups by evaluating explicit invariants. This method works well if G has small index in S_d. Iterating, this allows on to compute the monodromy group of a Belyĭ map explicitly instead of merely giving the maximal groups in which is it included. To this end, one may work modulo a prime $\mathfrak{p}$ of good reduction, and in light of Beckmann's Theorem, we may still reasonably expect a small prime of the ring of integers of K that is coprime with the cardinality $\#G$ of the monodromy group to do the job.

Second, one can compute the monodromy by using numerical approximation. This has been implemented by van Hoeij [**156**], though one must be very careful to do this with rigorous error bounds. This idea was used by Granboulan [**61**] in the computation of a cover with Galois group M_{24}, first realized (without explicit equation) by Malle–Matzat [**107**, III.7.5]. In particular, Schneps [**138**, §III.1] describes a numerical method to draw the dessin itself, from which one can read off the mondromy. This method is further developed by Bartholdi–Buff–von Bothmer–Kröker [**7**], who lift a Delaunay

triangulation numerically and read off the permutations by traversing the sequence of edges counterclockwise around a basepoint. In particular this solves (iii): if we express each of the complex solutions obtained by embedding $K \hookrightarrow \mathbb{C}$, we may also want to know which cover corresponds to which permutation triple up to conjugation.

A third and final method is due to Elkies [**48**], who uses an effective version (due to Weil's proof of the Riemann hypothesis for curves over finite fields) of the Chebotarev density theorem in the function field setting. This was applied to distinguish whether the Galois group of a given cover was equal to M_{23} or A_{23}. More precisely, one relies on reduction modulo a prime whose residue field is prime of sufficiently large characteristic (in his case, $> 10^9$) and uses the resulting distribution of cycle structures to deduce that the cover was actually M_{23}. This method has the advantage of using exact arithmetic and seems particularly well-suited to verify monodromy of large index in S_d.

9. Further topics and generalizations

This section discuss some subjects that are generalizations of or otherwise closely related with Belyĭ maps. At the end, we briefly discuss the theoretical complexity of calculating Belyĭ maps.

Generalizations. — Over $\overline{\mathbb{F}}_p$, one can consider the reduction of Belyĭ maps from characteristic 0; this is considered in Section 5 above. Switching instead to global function fields might be interesting, especially if one restricts to tame ramification and compares with the situation in characteristic 0. As a generalization of Belyĭ's theorem, over a perfect field of characteristic $p > 0$, every curve X has a map to $\mathbb{P}^1$ that is ramified only at ∞ by work of Katz [**88**]. But this map is necessarily wildly ramified at ∞ if $g(X) > 0$, so the corresponding theory will differ essentially from that of Belyĭ maps over $\overline{\mathbb{Q}}$.

If we view Belyĭ's theorem as the assertion that every curve over a number field is an étale cover of $\mathbb{P}^1 \setminus \{0, 1, \infty\} \cong \mathcal{M}_{0,4}$, the moduli space of genus 0 curves with 4 marked points, then Belyĭ's result generalizes to a question by Braungardt [**23**]: is every connected, quasi-projective variety X over $\overline{\mathbb{Q}}$ birational to a finite étale cover of some moduli space of curves $\mathcal{M}_{g,n}$? Easton and Vakil also have proven that the absolute Galois group acts faithfully on the irreducible components of the moduli space of surfaces [**43**]. Surely some computations in small dimensions and degree will be just as appealing as in the case of Belyĭ maps.

As mentioned on a naive level in Remarks 2.5 and 2.10, another more general way to look at Belyĭ maps is through the theory of Hurwitz schemes, which give a geometric structure to the set $\mathcal{H}_{n,r}(\overline{\mathbb{Q}})$ parametrizing degree n morphisms to $\mathbb{P}^1$ over $\mathbb{Q}$ that are ramified above r points. The theorem of Belyĭ then amounts to saying that by taking the curve associated to a morphism, one obtains a surjective map from the union of the $\overline{\mathbb{Q}}$-rational points of the spaces $\mathcal{H}_{n,3}$ to the union of the $\overline{\mathbb{Q}}$-rational points of the moduli spaces of curves $\mathcal{M}_g$ of genus g. We refer to work of Romagny–Wewers [**134**] for a more complete account.

Origamis. — One generalization of Belyĭ maps is given by covers called origamis: covers of elliptic curves that are unramified away from the origin. For a more complete account on origamis, see Herrlich–Schmithüsen [**74**]; Belyĭ maps can be obtained from origamis by a degeneration process [**74**, §8].

The reasons for considering origamis are many. First, the fundamental group of an elliptic curve minus a point is analogous to that of the Riemann sphere, in that it is again free on two generators. The ramification type above the origin is now given by the image of the commutator of these two generators. The local information at this single point of ramification reflects less information about the cover than in the case of Belyĭ maps. Additionally, the base curve can be varied, which makes the subject more subtle, as Teichmüller theory makes its appearance.

An exciting family of special origamis was considered by Anema–Top [**3**]: they consider the elliptic curve $E : y^2 = x^3 + ax + b$ over the scheme $B : 4a^3 + 27b^2 = 1$ defined by the constant non-vanishing discriminant 1 of E. Considering the torsion subschemes $E[n]$ over B, one obtains a family of covers over the base elliptic curve B of j-invariant 0 that is only ramified above the point at infinity and whose Galois groups are subgroups of special linear groups. It would be very interesting to deform this family to treat the case of arbitrary base curves, though it is not clear how to achieve this.

Question 9.1. — *How does one explicitly deform special origamis to families with arbitrary base curves?*

Explicit examples of actual families of origamis were found by Rubinstein-Salzedo [**135, 136**]. In particular, by using a deformation argument starting from a nodal cubic, he obtains a family of hyperelliptic origamis that are totally ramified at the origin. For the case of degree 3, this gives a unique cover of genus 2. More precisely, starting with an elliptic curve E with full 2-torsion in Legendre form

$$y^2 = x(x-1)(x-\lambda),$$

the hyperelliptic curve

$$y^2 = \frac{1}{2}\left(-4x^5 + 7x^3 - (2\lambda - 1)x^2 - 3x + (2\lambda - 1)\right)$$

admits a morphism to E given by

$$(x, y) \longmapsto \left(\frac{1}{2}\left(-4x^3 + 3x + 1\right), \frac{y}{2}\left(-4x^2 + 1\right)\right)$$

that is only ramified at the points at infinity of these curves.

It is important to note here that the field of moduli of these covers is an extension of the field of moduli of the base elliptic curve; more precisely, as suggested by the formulas above, this field of moduli is exactly the field obtained by adjoint the 2-torsion of the curve. This is a variation on a result in Rubinstein-Salzedo [**135**], where simpler expressions for similar covers are found in every degree. Amusingly enough, adjoining the full 2-torsion of the base curves always suffices to define these covers. This result is appealing and quite different from the corresponding situation for Belyĭ maps, and therefore we ask the following question.

Question 9.2. — *Which extension of the field of moduli is needed to define similar covers totally ramified above a single point for general curves?*

Specialization. — Covering maps of the projective line with more than 3 ramification points specialize to Belyĭ maps by having the ramification points coincide. In many cases, the covers in the original spaces are easier to compute, and this limiting process will then lead to some non-trivial Belyĭ maps. This also works in reverse, and provides

another application of computing Belyĭ maps. Hallouin–Riboulet-Deyris [**66**] explicitly computed polynomials with Galois group A_n and S_n over $\mathbb{Q}(t)$ with four branch points for small values of n; starting from a relatively simple "degenerate" three-point branched cover, the four-point branched cover is obtained by complex approximation (using Puiseux expansions). These methods were considerably augmented by Hallouin in [**67**] to find another such family with group $\mathrm{PSL}_2(\mathbb{F}_8)$. More recently, König [**94**] similarly computed such an extension of $\mathbb{Q}(t)$ with Galois group $\mathrm{PSL}_5(\mathbb{F}_2)$, using a p-adic approximation to calculate the initial three-point degeneration. In all aforementioned cases, the resulting covers can be specialized to find explicit solution to the inverse Galois problem for the groups involved, and as mentioned at the end of Section 1, the results from [**67**] have also found an application in the determination of equations for Shimura curves [**65**].

As mentioned in Section 3, Couveignes [**32**] has used a patching method to describe more generally the computation of families of ramified branch covers, using a degeneration to the situation of three-point covers. More extensive algorithmic methods to deal with this question should therefore be in reach of the techniques of numerical algebraic geometry.

Complexity. — In this article, we have been primarily concerned with practical methods for computing Belyĭ maps; but we conclude this section by posing a question concerning the theoretical complexity of this task.

Question 9.3. — *Is there an algorithm that takes as input a permutation triple and produces as output a model for the corresponding Belyĭ map over $\overline{\mathbb{Q}}$ that runs in time doubly exponential in the degree n?*

There is an algorithm (without a bound on the running time) to accomplish this task, but it is one that no one would ever implement: there are only countably many Belyĭ maps, so one can enumerate them one at a time in some order and use any one of the methods to check if the cover has the desired monodromy. It seems feasible that the Gröbner method would provide an answer to the above problem, but this remains an open question. Javanpeykar [**79**] has given explicit bounds on the Faltings height of a curve in terms of the degree of a Belyĭ map; in principle, this could be used to compute the needed precision to recover the equations over a number field.

Références

[1] William W. Adams and Philippe Loustaunau, *An introduction to Gröbner bases*, Grad. Studies in Math., 3, Amer. Math. Soc., Providence, RI, 1994.

[2] N. M. Adrianov, N. Ya. Amburg, V. A. Dremov, Yu. A. Levitskaya, E. M. Kreines, Yu. Yu. Kochetkov, V. F. Nasretdinova, and G. B. Shabat, *Catalog of dessins d'enfants with* ≤ 4 *edges*, `arXiv:0710.2658v1`, 2007.

[3] Ane S. I. Anema and Jaap Top, *Explicit algebraic coverings of a pointed torus*, in *Arithmetic and geometry of K3 surfaces and Calabi-Yau threefolds*, Fields Inst. Commun., vol. 67, Springer, New York, 143–152.

[4] Elizabeth A. Arnold, *Modular algorithms for computing Gröbner bases*, J. Symbolic Comput. **35** (2003), no. 4, 403–419.

[5] A. O. L. Atkin, H. P. F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups*, in *Combinatorics*, (Proc. Sympos. Pure Math., vol. XIX, Univ. California, Los Angeles), Amer. Math. Soc., Providence, 1968, 1–25.

[6] Ali Ayad, *A survey on the complexity of solving algebraic systems*, International Math. Forum **5** (2010), no. 7, 333–353.

[7] Laurent Bartholdi, Xavier Buff, Hans-Christian Graf von Bothmer, and Jakob Kröker, *Algorithmic construction of Hurwitz maps*, `arXiv:1303.1579v1`, 2013.

[8] Alan F. Beardon and Kenneth Stephenson, *The uniformization theorem for circle packings*, Indiana Univ. Math. J. **39** (1990), no. 4, 1383–1425.

[9] Arnaud Beauville, *Les familles stables de courbes elliptiques sur* $\mathbf{P}^1$ *admettant quatre fibres singulières*, C. R. Acad. Sci. Paris Sér. I Math. **294** (1982), no. 19, 657–660.

[10] Daniel J. Bates, Jonathan D. Hauenstein, Andrew J Sommese, and Charles W. Wampler, *Bertini: Software for numerical algebraic geometry*, available at `bertini.nd.edu` with permanent doi: `dx.doi.org/10.7274/R0H41PB5`.

[11] Sybilla Beckmann, *Ramified primes in the field of moduli of branched coverings of curves*, J. Algebra **125** (1989), no. 1, 236–255.

[12] G.V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Math. USSR-Izv. **14** (1980), no. 2, 247–256.

[13] G.V. Belyĭ, *A new proof of the three-point theorem*, translation in Sb. Math. **193** (2002), no. 3–4, 329–332.

[14] Kevin Berry and Marvin Tretkoff, *The period matrix of Macbeath's curve of genus seven*, in *Curves, Jacobians, and abelian varieties*, Amherst, MA, 1990, Providence, RI: Contemp. Math., vol. 136, Amer. Math. Soc., 31–40.

[15] Jean Bétréma, Danielle Péré, and Alexander Zvonkin, *Plane trees and their Shabat polynomials*, Laboratoire Bordelais de Recherche en Informatique, Université Bordeaux I, 1992.

[16] Frits Beukers and Hans Montanus, *Explicit calculation of elliptic fibrations of* $K3$*-surfaces and their Belyi-maps*, in *Number theory and polynomials*, London Math. Soc. Lecture Note Ser., vol. 352, Cambridge Univ. Press, Cambridge, 33–51.

[17] F. Beukers and C. L. Stewart, *Neighboring powers*, J. Number Theory **130** (2010), 660-679.

[18] Bryan Birch, *Noncongruence subgroups, covers and drawings*, in *The Grothendieck theory of dessins d'enfants*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge University Press, 1994, 25–46.

[19] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (3–4), 1997, 235–265.

[20] Nigel Boston, *On the Belgian chocolate problem and output feedback stabilization: Efficacy of algebraic methods*, 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton) 2012, October 2012, 869–873.

[21] Florian Bouyer and Marco Streng, *Examples of CM curves of genus two defined over the reflex field*, `arxiv:1307.0486v1`, 2013.

[22] Philip L. Bowers and Kenneth Stephenson, *Uniformizing dessins and Belyĭ maps via circle packing*, Mem. Amer. Math. Soc. **170** (2004), no. 805.

[23] V. Braungardt, *Covers of moduli surfaces*, Compositio Math. **140** (2004), no. 4, 1033–1036.

[24] C. Chevalley, A. Weil and E. Hecke, *Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers*, Abh. Math. Sem. Univ. Hamburg **10** (1934), no. 1, 358–361.

[25] Pete L. Clark and John Voight, *Algebraic curves uniformized by congruence subgroups of triangle groups*, preprint at `http://www.math.dartmouth.edu/~jvoight/articles/triangle-072011.pdf`.

[26] Charles R. Collins and Kenneth Stephenson, *A circle packing algorithm*, Comput. Geom. **25** (2003), no. 3, 233–256.

[27] Marston D. E. Conder, Gareth A. Jones, Manfred Streit and Jürgen Wolfart, *Galois actions on regular dessins of small genera*, Rev. Mat. Iberoam. **29** (2013), no. 1, 163–181.

[28] Kevin Coombes and David Harbater, *Hurwitz families and arithmetic Galois groups*, Duke Math. J. **52** (1985), no. 4, 821–839.

[29] Jean-Marc Couveignes, *Calcul et rationalité de fonctions de Belyi en genre 0*, Annales de l'Institut Fourier (Grenoble) **44** (1994), no. 1, 1–38.

[30] Jean-Marc Couveignes, *Quelques revêtements definis sur* $\mathbb{Q}$, Manuscripta Math. **92** (1997), no. 4, 409-445.

[31] Jean-Marc Couveignes, *A propos du théorème de Belyi*, J. Théor. Nombres Bordeaux **8** (1996), no. 1, 93–99.

[32] Jean-Marc Couveignes, *Tools for the computation of families of coverings*, in *Aspects of Galois theory*, London Math. Soc. Lecture Notes Ser., vol. 256, Cambridge Univ. Press, Cambridge, 1999, 38–65.

[33] Jean-Marc Couveignes and Granboulan, *Dessins from a geometric point of view*, in *The Grothendieck theory of dessins d'enfants*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge University Press, 1994, 79–113.

[34] David A. Cox, John B. Little, Donal O'Shea, *Ideals, varieties, and algorithms*, 2nd ed., Springer-Verlag, New York, 1996.

[35] David A. Cox, John B. Little, Donal O'Shea, *Using algebraic geometry*, Springer-Verlag, New York, 2005.

[36] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997.

[37] Michael Stoll and John E. Cremona, *On the reduction theory of binary forms*, J. Reine Angew. Math. **565** (2003), 79–99.

[38] Pierre Dèbes and Jean-Claude Douai, *Algebraic covers: field of moduli versus field of definition*, Ann. Sci. École Norm. Sup. (4) **30** (1997), no. 3, 303–338.

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

[40] V. A. Dremov, *Computation of two Belyi pairs of degree 8*, Russian Math. Surveys **64** (2009), no. 3, 570–572.

[41] Virgile Ducet, *Cnstruction of algebraic curves with many rational points over finite fields*, Ph.D. thesis, Université d'Aix-Marseille, 2013.

[42] Clifford J. Earle, *On the moduli of closed Riemann surfaces with symmetries*, in *Advances in the theory of riemann surfaces (Proc. Conf., Stony Brook, N.Y., 1969)*, Ann. of Math. Studies, vol. 66, Princeton Univ. Press, Princeton, 119–130.

[43] Robert W. Easton and Ravi Vakil, *Absolute Galois acts faithfully on the components of the moduli space of surfaces: A Belyi-type theorem in higher dimension*, Int. Math. Res. Notices **2007**, no. 20, Art. ID rnm080.

[44] W. L. Edge, *Fricke's octavic curve*, Proc. Edinburgh Math. Soc. **27** (1984), 91–101.

[45] Noam D. Elkies, *ABC implies Mordell*, Internat. Math. Res. Notices **1991**, no. 7, 99–109.

[46] Noam D. Elkies, *Shimura curve computations*, Algorithmic number theory (Portland, OR, 1998), Lecture notes in Comput. Sci., vol. 1423, 1–47.

[47] Noam D. Elkies, *Shimura curves for level-3 subgroups of the* $(2, 3, 7)$ *triangle group, and some other examples*, in *Algorithmic number theory*, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, 302–316.

[48] Noam D. Elkies, *The complex polynomials* $P(x)$ *with* $\mathrm{Gal}(P(x) - t) = M_{23}$, in *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium*, eds. Everett Howe and Kiran Kedlaya, Open Book Series 1, Math. Science Publishers, 2013, 359–367.

[49] Noam D. Elkies, *Explicit modular towers*, in *Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing (1997)*, eds. T. Basar and A. Vardy, Univ. of Illinois at Urbana-Champaign, 1998, 23-32, `arXiv:math.NT/0103107`.

[50] Noam D. Elkies and Mark Watkins, *Polynomial and Fermat-Pell families that attain the Davenport-Mason bound*, preprint at `http://magma.maths.usyd.edu.au/~watkins/papers/hall.ps`.

[51] Arsen Elkin, *Belyi Maps*, `http://homepages.warwick.ac.uk/~masjaf/belyi/`.

[52] Christophe Eyral and Mutsuo Oka, *Fundmental groups of join-type sextics via dessins d'enfants*, Proc. London Math. Soc. (3) 107 (2013), 76–120.

[53] Helaman R. P. Ferguson, David H. Bailey, and Steve Arno, *Analysis of PSLQ, an integer relation finding algorithm*, Math. Comp. **68** (1999), 351–369.

[54] Claus Fieker and Jürgen Klüners, *Computation of Galois groups of rational polynomials*, Galois group, `arxiv:1211.3588v2`, 2012.

[55] Machiel van Frankenhuysen, *The ABC conjecture implies Vojta's height inequality for curves*, J. Number Theory **95** (2002), 289–302.

[56] Robert Fricke and Felix Klein, *Vorlesungen über die Theorie der automorphen Funktionen. Band 1: Die gruppentheoretischen Grundlagen. Band II*, Bibliotheca Mathematica Teubneriana, Bände 3, 4 Johnson, New York, 1965.

[57] M. Fried, *Fields of definition of function fields and Hurwitz families—groups as Galois groups*, Comm. Algebra **5** (1977), no. 1, 17–82.

[58] Ernesto Girondo and Gabino González-Diez, *Introduction to compact Riemann surfaces and dessins d'enfants*, Cambridge University Press, Cambridge, 2012.

[59] V. D. Goppa, *Codes that are associated with divisors*, Problemy Peredači Informacii **13** (1977), no. 1, 33–39.

[60] Louis Granboulan, *Calcul d'objets géométriques à l'aide de méthodes algébriques et numériques: dessins d'enfants*, Ph.D. thesis, Université Paris 7, 1997.

[61] L. Granboulan, *Construction d'une extension régulière de $\mathbb{Q}(T)$ de groupe de Galois M_{24}*, Experimental Math. **5** (1996), 3–14.

[62] Alexandre Grothendieck, *Sketch of a programme (translation into English)*, in *Geometric Galois actions 1*, eds. Leila Schneps and Pierre Lochak, London Math. Soc. Lect. Note Series, vol. 242, Cambridge University Press, Cambridge, 1997, 243–283.

[63] Leon Greenberg, *Maximal Fuchsian groups*, Bull. Amer. Math. Soc. **69** (1963), 569–573.

[64] Gert-Martin Greuel and Gerhard Pfister, *A Singular introduction to commutative algebra*, Springer, Berlin, 2002.

[65] Emmanuel Hallouin, *Computation of a cover of Shimura curves using a Hurwitz space*, J. of Algebra **321** (2009), no. 2, 558–566.

[66] Emmanuel Hallouin and Emmanuel Riboulet-Deyris, *Computation of some moduli spaces of covers and explicit $\mathcal{S}_n$ and $\mathcal{A}_n$ regular $\mathbb{Q}(T)$-extensions with totally real fibers*, Pacific J. Math. **211** (2003), no. 1, 81–99.

[67] Emmanuel Hallouin, *Study and computation of a Hurwitz space and totally real $\mathrm{PSL}_2(\mathbb{F}_8)$-extensions of $\mathbb{Q}$*, J. Algebra **292** (2005), no. 1, 259–281.

[68] Amihay Hanany, Yang-Hui He, Vishnu Jejjala, Jurgis Pasukonis, Sanjaye Ramgoolam, and Diego Rodriguez-Gomez, *The beta ansatz: a tale of two complex structures*, J. High Energy Physics **6** (2011), `arXiv:1104.5490`.

[69] Yang-Hui He and John McKay, *$\mathcal{N} = 2$ gauge theories: congruence subgroups, coset graphs and modular surfaces*,
`arXiv:1201.3633v1`, 2012.

[70] Yang-Hui He and John McKay, *Eta products, BPS states and K3 surfaces*,
`arXiv:1308.5233v1`, 2013.

[71] Yang-Hui He, John McKay, and James Read, *Modular subgroups, dessins d'enfants and elliptic K3 surfaces*, `arXiv:1211.1931v1`, 2012.

[72] Dennis A. Hejhal, *On eigenfunctions of the Laplacian for Hecke triangle groups*, Emerging Applications of Number Theory, eds. D. Hejhal, J. Friedman, M. Gutzwiller and A. Odlyzko, IMA Series No. 109, Springer-Verlag, 1999, 291-315.

[73] Joachim A. Hempel, *Existence conditions for a class of modular subgroups of genus zero*, Bull. Austral. Math. Soc. **66** (2002), 517–525.

[74] Frank Herrlich and Gabriela Schmithüsen, *Dessins d'enfants and origami curves*, in *Handbook of Teichmüller theory, Vol. II*, IRMA Lect. Math. Theor. Phys., 13, Eur. Math. Soc., Zürich, 2009, 767–809.

[75] Kenji Hoshino, *The Belyi functions and dessin d'enfants corresponding to the non-normal inclusions of triangle groups*, Math. J. Okayama Univ. **52** (2010), 45–60.

[76] Kenji Hoshino and Hiroaki Nakamura, *Belyi function on $X_0(49)$ of degree 7*, Math. J. Okayama Univ. **52** (2010), 61–63.

[77] A. Hurwitz, *Über Riemannsche Flächen mit gegebenen Verzweigungspunkten*, Math. Ann. **39** (1891), 1–61.

[78] Yasutaka Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 721–724 (1982).

[79] Ariyan Javanpeykar, *Polynomial bounds for Arakelov invariants of Belyi curves*, with an appendix by Peter Bruin, Ph.D. thesis, Universiteit Leiden, 2013.

[80] Christian U. Jensen, Arne Ledet, and Noriko Yui, *Generic polynomials: Constructive aspects of the inverse Galois problem*, Cambridge University Press, Cambridge, 2002.

[81] Gareth A. Jones, *Congruence and noncongruence subgroups of the modular group: a survey*, Proceedings of groups–St. Andrews 1985, London Math. Soc. Lecture Note Ser., vol. 121, Cambridge, 1986, 223–234.

[82] Gareth Jones and David Singerman, *Belyĭ functions, hypermaps and Galois groups*, Bull. London Math. Soc. **28** (1996), no. 6, 561–590.

[83] Gareth Jones and David Singerman, *Maps, hypermaps, and triangle groups*, in *The Grothendieck theory of dessins d'enfants*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge University Press, 1994, 115–145.

[84] Gareth A. Jones and Manfred Streit, *Galois groups, monodromy groups and cartographic groups*, in *Geometric Galois actions 2.*, eds. Leila Schneps and Pierre Lochak, London Math. Soc. Lect. Note Series, vol. 243, Cambridge University Press, Cambridge, 1997, 25–65

[85] Gareth A. Jones, Manfred Streit and J. Wolfart, *Wilson's map operations on regular dessins and cyclotomic fields of definition*, Proc. Lond. Math. Soc. (3) **100** (2010), no. 2, 510–532.

[86] John W. Jones and David P. Roberts, *Galois number fields with small root discriminant*, J. Number Theory **122** (2007), 379–407.

[87] Gaston Julia, *Étude sur les formes binaires non quadratiques à indéterminées réelles ou complexes*, Mémoires de l'Académie des Sciences de l'Institut de France 55, 1296 (1917).

[88] Nicholas M. Katz, *Travaux de Laumon*, Séminaire Bourbaki **691** (1987–1988), 105–132.

[89] A. V. Kitaev, *Dessins d'enfants, their deformations and algebraic the sixth Painlevé and Gauss hypergeometric functions*, `arXiv:nlin/0309078v3`, 2003.

[90] Felix Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, reprint of the 1884 original, Birkhäuser, Basel, 1993.

[91] Michael Klug, Michael Musty, Sam Schiavone, and John Voight, *Numerical computation of three-point branched covers of the projective line*, `arxiv:1311.2081`, 2014.

[92] Bernhard Köck, *Belyĭ's theorem revisited*, Beiträge Algebra Geom. **45** (2004), no. 1, 253–265.

[93] Paul Koebe, *Kontaktprobleme der konformen Abbildung*, Ber. Sächs. Akad. Wiss. Leizig, Math.-Phys. Kl. **88** (1936), 141–164.

[94] Joachim König, *A family of polynomials with Galois group* $\mathrm{PSL}_5(2)$ *over* $\mathbb{Q}(t)$, `arXiv:1308.1566v1`, 2013.

[95] E. M. Kreĭnes, *On families of geometric parasitic solutions for Belyi systems of genus zero*, Fundamentalnaya i Priklandaya Matematika **9** (2003), no. 1, 103-111.

[96] E. M. Kreĭnes, *Equations determining Belyi pairs, with applications to anti-Vandermonde systems*, Fundamentalnaya i Priklandaya Matematika **13** (2007), no. 4, 95–112.

[97] Martin Kreuzer and Lorenzo Robbiano, *Computational commutative algebra 1*, Springer-Verlag, New York, 2000.

[98] Chris A. Kurth and Ling Long, *Computations with finite index subgroups of* $\mathrm{PSL}_2(\mathbb{Z})$ *using Farey symbols*, `arXiv:0710.1835`, 2007.

[99] Sergei K. Lando and Alexander K. Zvonkin, *Graphs on surfaces and their applications*, with an appendix by D. Zagier, Encyclopaedia of Mathematical Sciences, Low-Dimensional Topology, II, Springer-Verlag, Berlin, 2004.

[100] Finnur Larusson and Timur Sadykov, *Dessins d'enfants and differential equations*, `arXiv:math/0607773`, 2006.

[101] H.W. Lenstra, *Galois theory for schemes*, online notes at `http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf`.

[102] A.K. Lenstra, H.W. Lenstra and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 513–534.

[103] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling, *Explicit Galois obstruction and descent for hyperelliptic curves with tamely cyclic reduced automorphism group*, `arXiv:1301.0695`, 2013.

[104] Wen-Ching Winnie Li, Ling Long, and Zifeng Yang, *Modular forms for noncongruence subgroups*, Q. J. Pure Appl. Math. **1** (2005), no. 1, 205–221.

[105] Wilhelm Magnus, *Noneuclidean tesselations and their groups*, Pure and Applied Mathematics, vol. 61, Academic Press, New York, 1974.

[106] Nicolas Magot and Alexander Zvonkin, *Belyi functions for Archimedean solids*, Discrete Math. **217** (2000), no. 1–3, 249–271.

[107] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer, Berlin, 1999.

[108] G. Malle and B. H. Matzat, *Realisierung von Gruppen* $\mathrm{PSL}_2(\mathbb{F}_p)$ *als Galoisgruppen über* $\mathbb{Q}$, Math. Ann. **272** (1985), 549–565.

[109] Gunter Malle, *Polynomials with Galois groups* $\mathrm{Aut}(M_{22})$, M_22, *and* $\mathrm{PSL}_3(\mathbb{F}_4)\cdot 2$ *over* $\mathbb{Q}$, Math. Comp. **51** (1988), 761–768.

[110] Gunter Malle, *Polynomials for primitive nonsolvable permutation groups of degree* $d \leq 15$, J. Symbolic Comput. **4** (1987), no. 1, 83–92.

[111] Gunter Malle, *Fields of definition of some three point ramified field extensions*, in *The Grothendieck theory of dessins d'enfants*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge University Press, 1994, 147–168.

[112] Gunter Malle and David P. Roberts, *Number fields with discriminant* $\pm 2^a 3^b$ *and Galois group* A_n *or* S_n, LMS J. Comput. Math. **8** (2005), 1–22.

[113] G. Malle and W. Trinks, *Zur Behandlung algebraischer Gleichungssysteme mit dem Computer*, Mathematisches Institut, Universität Karlsruhe, 1984, unpublished manuscript.

[114] Al Marden and Burt Rodin, *On Thurston's formulation and proof of Andreev's theorem*, Lecture Notes in Math., vol. 1435, Springer, 1989, 103–164.

[115] Donald E. Marshall, *Numerical conformal mapping software: zipper*, `http://www.math.washington.edu/~marshall/zipper.html`.
[116] Ernst W. Mayr, *Some complexity results for polynomial ideals*, J. Complexity **13** (1997), no. 3, 303–325.
[117] Donald E. Marshall and Steffen Rohde, *The zipper algorithm for conformal maps and the computation of Shabat polynomials and dessins*, in preparation.
[118] Donald E. Marshall and Steffen Rohde, *Convergence of a variant of the zipper algorithm for conformal mapping*, SIAM J. Numer. Anal. **45** (2007), no. 6, 2577–2609.
[119] Yu. V. Matiyasevich, *Computer evaluation of generalized Chebyshev polynomials*, Moscow Univ. Math. Bull. **51** (1996), no. 6, 39–40.
[120] B. Heinrich Matzat, *Konstructive Galoistheorie*, Lect. Notes in Math., vol. 1284, Springer, Berlin, 1987.
[121] A. D. Mednykh, *Nonequivalent coverings of Riemann surfaces with a prescribed ramification type*, Siberian Math. J. **25** (1984), 606–625.
[122] Rick Miranda and Ulf Persson, *Configurations of* I_n *fibers on elliptic* $K3$ *surfaces*, Math. Z. **201** (1989), no. 3, 339–361.
[123] Bojan Mohar, *A polynomial time circle packing algorithm*, Discrete Math. **117** (1993), no. 1-3, 257–263.
[124] Hans Montanus, *Hall triples and dessins d'enfant*, Nieuw Arch. Wiskd. (5) **7** (2006), no. 3, 172–176.
[125] Hossein Movasati and Stefan Reiter, *Heun equations coming from geometry*, Bull. Braz. Math. Soc. (N.S.) **43** (2012), no. 3, 423–442.
[126] Andrew Obus, *Good reduction of three-point Galois covers*, `arXiv:1208.3909`, 2012.
[127] Jennifer Paulhus, *Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups*, in *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium*, eds. Everett Howe and Kiran Kedlaya, the Open Book Series 1, Mathematical Science Publishers, 2013, 487–505.
[128] Heinz-Otto Peitgen (ed.), *Newton's method and dynamical systems*, Kluwer Academic, Dordrecht, 1989.
[129] Kevin Pilgrim, *Dessins d'enfants and Hubbard trees*, Ann. Sci. École Norm. Sup. (4) **33** (2000), no. 5, 671–693.
[130] Michel Raynaud, *Spécialisation des revêtements en charactéristique* $p > 0$, Ann. Sci. École Norm. Sup. (4) **32** (1999), no. 1, 87–126.
[131] David P. Roberts, *Nonsolvable polynomials with field discriminant* 5^A, Int. J. Number Theory **7** (2011), no. 2, 289–322.
[132] David P. Roberts, *An ABC construction of number fields*, in *Number theory*, CRM Proc. Lecture Notes, vol. 36, Amer. Math. Soc., Providence, 2004, 237–267.
[133] David P. Roberts, *Lightly ramified number fields with Galois group* $S.M12.A$, preprint at `http://cda.morris.umn.edu/~roberts/research/m12.pdf`.
[134] Matthieu Romagny and Stefan Wewers, *Hurwitz spaces*, in *Groupes de Galois arithmétiques et différentiels*, Sémin. Congr., vol. 13, Soc. Math. France, Paris, 313–341.
[135] Simon Rubinstein-Salzedo, *Totally ramified branched covers of elliptic curves*, `arxiv:1210.3195`, 2012.
[136] Simon Rubinstein-Salzedo, *Period computations for covers of elliptic curves*, `arxiv:1210.4721`, 2012.
[137] William Stein, *SAGE Mathematics Software* (version 4.3), The SAGE Group, 2013, `http://www.sagemath.org/`.
[138] Leila Schneps, *Dessins d'enfants on the Riemann sphere*, in *The Grothendieck theory of dessins d'enfants*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge University Press, 1994, 47–77.

[139] Leila Schneps, ed. *The Grothendieck theory of dessins d'enfants*, London Mathematical Society Lecture Note Series, vol. 200, Cambridge University Press, Cambridge, 1994.

[140] René Schoof, *Counting points on elliptic curves over finite fields*, J. Théorie Nombres Bordeaux **7** (1995), 219–254.

[141] Björn Selander and Andreas Strömbergsson, *Sextic coverings of genus two which are branched at three points*, preprint at `http://www2.math.uu.se/~astrombe/papers/g2.ps`.

[142] Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics 1, Jones and Bartlett, 1992.

[143] G. Shabat, *On a class of families of Belyi functions*, in *Formal power series and algebraic combinatorics*, eds. D. Krob, A. A. Mikhalev and A. V. Mikhalev, Springer-Verlag, Berlin, 2000, 575–581.

[144] G.B. Shabat and V. Voevodsky, *Drawing curves over number fields*, in *The Grothendieck Festschrift, vol. III*, Birkhauser, Boston, 1990, 199–227.

[145] Gorō Shimura, *On the field of rationality for an abelian variety*, Nagoya Math. J. **45** (1972), 167–178.

[146] David Singerman, *Finitely maximal Fuchsian groups*, J. London Math. Soc. (2) **6** (1972), 29–38.

[147] D. Singerman and R.I. Syddall, *Belyĭ uniformization of elliptic curves*, Bull. London Math. Soc. **139** (1997), 443–451.

[148] Andrew J. Sommese, Charles W. Wampler II, *The numerical solution of systems of polynomials arising in engineering and science*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.

[149] William Stein, *Modular forms: a computational approach*, Grad. Studies in Math., vol. 79, American Mathematical Society, Providence, RI, 2007.

[150] Manfred Streit, *Homology, Belyĭ functions and canonical curves*, Manuscripta Math. **90** (1996), 489–509.

[151] Manfred Streit, *Field of definition and Galois orbits for the Macbeath-Hurwitz curves*, Arch. Math. (Basel) **74** (2000), no. 5, 342–349.

[152] Manfred Streit and Jürgen Wolfart, *Characters and Galois invariants of regular dessins*, Rev. Mat. Complut. **13** (2000), no. 1, 49–81.

[153] Kisao Takeuchi, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 24 (1977), 201-212.

[154] W. Thurston, *The geometry and topology of* 3*-manifolds*, Princeton University Notes, Princeton, 1982.

[155] M. A. Tsfasman, S. G. Vlăduţ and Th. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28.

[156] Mark van Hoeij, *algcurves package*, available at `http://www.math.fsu.edu/~hoeij/maple.html`.

[157] Mark van Hoeij and Raimundas Vidunas, *Belyi functions for hyperbolic hypergeometric-to-Heun transformations*, `arxiv:1212.3803v2`, 2013.

[158] Mark van Hoeij and Raimundas Vidunas, *Algorithms and differential relations for Belyi functions*, `arxiv:1305.7218v1`, 2013.

[159] Jan Verschelde, *Algorithm 795: PHCpack: A General-Purpose Solver for Polynomial Systems by Homotopy Continuation*, ACM Trans. Math. Softw. **25** (1999), no. 2, 251–276, `http://www.math.uic.edu/~jan/PHCpack/phcpack.html`.

[160] Raimundas Vidunas, *Transformations of some Gauss hypergeometric functions*, J. Comp. Appl. Math. **178** (2005), 473–487.

[161] Raimundas Vidunas and Galina Filipuk, *A classification of coverings yielding Heun-to-hypergeometric reductions*, `arXiv:1204.2730v1`, 2012.

[162] Raimundas Vidunas and Alexander V. Kitaev, *Computation of highly ramified coverings*, `arxiv:0705.3134v1`, 2007.

[163] S. G. Vlăduţ and V. G. Drinfel'd, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** (1983), no. 1, 68–69.

[164] John Voight and John Willis, *Computing power series expansions of modular forms*, in *Computations with modular forms*, eds. Gebhard Boeckle and Gabor Wiese, Contrib. Math. Comput. Sci., vol. 6, Springer, Berlin, 2014, 331–361.

[165] Helmut Völklein, *Groups as Galois groups. An introduction*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996.

[166] Mark Watkins, *A note on integral points on elliptic curves*, with an appendix by N. D. Elkies, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 707-719.

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

[168] Bruce Westbury, *Circle packing*, available at `https://github.com/BruceWestbury/Circle-Packing`, 2013.

[169] Franz Winkler, *A p-adic approach to the computation of Gröbner bases*, J. Symb. Comp. **6** (1988), no. 2–3, 287–304.

[170] Klaus Wohlfahrt, *An extension of F. Klein's level concept*, Illinois J. Math. **8** (1964), 529–535.

[171] Jürgen Wolfart, *Triangle groups and Jacobians of CM type*, preprint at `http://www.math.uni-frankfurt.de/~wolfart/Artikel/jac.pdf`.

[172] Jürgen Wolfart, *ABC for polynomials, dessins d'enfants, and uniformization – a survey*, in *Elementare und analytische Zahlentheorie*, Schr. Wiss. Ges. Johann Wolfgang Goethe Univ. Frankfurt am Main, 20, Franz Steiner Verlag Stuttgart, Stuttgart, 2006, 313–345.

[173] Jürgen Wolfart, *The "obvious" part of Belyi's theorem and Riemann surfaces with many automorphisms*, *Geometric Galois actions 1*, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 97–112.

[174] Melanie Wood, *Belyi-extending maps and the Galois action on dessins d'enfants*, Publ. RIMS, Kyoto Univ. **42** (2006), 721–737.

[175] Leonardo Zapponi, *Fleurs, arbres et cellules: un invariant galoisien pour une famille d'arbres*, Compositio Math. **122** (2000), no. 2, 113–133.

[176] Alexander Zvonkin, *Belyi functions: examples, properties, and applications*, `http://www.labri.fr/perso/zvonkin/Research/belyi.pdf`.

May 9, 2019

Jeroen Sijsling, Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL, UK • *E-mail :* `sijsling@gmail.com`

John Voight, Department of Mathematics and Statistics, University of Vermont, 16 Colchester Ave, Burlington, VT 05401, USA; Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA • *E-mail :* `jvoight@gmail.com`