ON COMPUTING BELYI MAPS

JEROEN SIJSLING AND JOHN VOIGHT

Abstract. In this article, we survey methods to compute three-point branched covers of the projective line $\mathbb{P}^1$.

Contents

Introduction

Every compact Riemann surface X is an algebraic curve over $\mathbb{C}$, and every meromorphic function on X is a rational 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 further link this to arithmetic: to characterize those Riemann surfaces that can be defined over the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and to study the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on them. To this end, Belyĭ [10, 11] proved that a curve X over $\mathbb{C}$ can be defined over $\overline{\mathbb{Q}}$ if and only if X admits a Belyĭ map, a map $f : X \to \mathbb{P}^1_{\mathbb{C}}$ which is unramified away from $\{0, 1, \infty\}$. Grothendieck, in his *Esquisse d'un Programme* [52], 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 d'enfant (or just dessin): a connected graph with bicolored vertices such that two vertices of an edge are colored differently and such that edges around each vertex are given a cyclic ordering. Conversely, a dessin as a graph determines the corresponding Belyĭ map uniquely up to isomorphism. 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,

Date: November 9, 2013.

hundreds of papers have been written on the subject, several books have appeared [48, 88, 121], 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 dessins d'enfants; arguably, part of the richness of the subject lies in the beauty in these examples. Shabat and Voevodsky 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" [126, 0.1.1, 0.3].

However, no survey of these computational methods has yet appeared, and in our own calculations we found many techniques, shortcuts, and some tricks that others had discovered and often rediscovered. So 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 dessins.

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

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

up to simultaneous conjugation in the symmetric group S_n, and

$$\text{Bely\u{\i} maps } f : X \to \mathbb{P}^1 \text{ of degree } n$$

up to isomorphism over $\overline{\mathbb{Q}}$. In this bijection, we allow the curve X to be disconnected, such as in the trivial cover of degree $d \geq 1$; the covering cover X is connected if and only if (the dessin is connected if and only if) the corresponding permutation triple generates a transitive subgroup of S_n, in which case we call it 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 very compact form of a permutation triple, it has proven difficult in general to determine explicitly an algebraic model for f and the surface 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; for example, the following 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 given 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" [93, §1].

The paper is organized as follows. In section 1, we collect the basic background and mention some applications. In section 2, we discuss the "standard technique" using Gröbner methods, the Atkin–Swinnerton-Dyer trick, and methods to verify the correctness of a given cover. 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. Finally, in section 5, we consider p-adic methods. Along the way, we give many explicit examples and pose some questions.

The authors would like to thank Noam Elkies, Curtis McMullen, David Roberts, Steffen Rohde, Bernd Sturmfels, and Mark Watkins for their comments on this work. 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 explicitly characterization and computation of ramified covers of Riemann surfaces is little younger than Riemann himself. Klein [79] and Fricke-Klein [47] constructed some explicit dessins, most notably the icosahedral Galois dessin $\mathbb{P}^1 \to \mathbb{P}^1$ of degree 60. These appeared when constructing what we would today call modular functions associated with the triangle groups $\Delta(2,3,5)$ and $\Delta(2,4,5)$ (for which 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 [64] 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 is extremely rich: surveys include Birch [15], Jones and Singerman [69, 70], Schneps [120], and Wolfart [152]; textbooks include work of Malle and Matzat [94], Serre [124], and Völklein [145], mainly with an eye toward applications to inverse Galois theory. Many other papers are referenced below.

We begin in this section by reviewing basic definitions; we then take some time to deal with some subtle issues concerning fields of moduli and fields of definition, relevant for explicit computation. We conclude by mentioning applications and generalizations as motivation for further study.

Basic definitions. Let K be a field. An (algebraic) curve over K is a smooth projective variety defined over K that is pure of dimension 1, or equivalently, a disjoint union of nonsingular, projective geometrically integral varieties over K of dimension 1.

A Belyĭ map (over $\mathbb{C}$) is a morphism $f : X \to \mathbb{P}^1$ of curves over $\mathbb{C}$ that is unramified outside $\{0,1,\infty\}$; we call the curve X a Belyĭ curve. Two Belyĭ maps $f_1, f_2 : X_1, X_2 \to \mathbb{P}^1$ are isomorphic if there is an isomorphism $i : X_1 \to X_2$ such that $f_1 = f_2 \circ i$. Belyĭ [10, 11] proved that a curve X over $\mathbb{C}$ can be defined over $\overline{\mathbb{Q}}$, an algebraic closure of $\mathbb{Q}$, if and only if X admits a Belyĭ map, so we may just as well work with curves defined over $\overline{\mathbb{Q}}$ as over $\mathbb{C}$.

Let $f : X \to \mathbb{P}^1$ be a Belyĭ map. The ramification above $\{0,1,\infty\}$ is recorded in the ramification type by the multiplicities of the ramified points. It is a consequence of the Riemann existence theorem that there is a bijection between equivalence classes of permutation triples (those triples of permutations whose product is trivial) and isomorphism classes of Belyĭ maps over $\overline{\mathbb{Q}}$:

$$\begin{gathered}\big\{\text{triples } \sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_n^3 \text{ that satisfy } \sigma_0\sigma_1\sigma_\infty = 1\big\} \,/\, \sim \\ \overset{1:1}{\longleftrightarrow} \\ \big\{\text{Belyĭ maps } f : X \to \mathbb{P}^1 \text{ of degree } n\big\} \,/\, \cong_{\overline{\mathbb{Q}}}\end{gathered} \tag{1.1}$$

Here we consider two triples to be equivalent $(\sigma_0, \sigma_1, \sigma_\infty) \sim (\sigma'_0, \sigma'_1, \sigma'_\infty)$ if and only if they are simultaneously conjugate, that is, if and only if there exists a $\tau \in S_n$ such that

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

Equivalently, letting

$$F_2 = \langle x, y, z \mid xyz = 1\rangle$$

by the free group on three generators, this means that the corresponding **monodromy representations** $\sigma, \sigma' : F_2 \to S_n$ of the free group on two generators F_2 (sending $x, y, z \in F_2$ to $\sigma_0, \sigma_1, \sigma_\infty$ resp. $\sigma'_0, \sigma'_1, \sigma'_{infty}$) are conjugate in S_n.

Under the correspondence (1.1), 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 its ramification index under the morphism f. Note in particular that because the left hand side of (1.1) is finite, there are only finitely many $\overline{\mathbb{Q}}$-isomorphism classes of curves X with a Belyĭ map of given bounded degree.

The **automorphism group** of a Belyĭ map is the intersection of the centralizers in S_n of the corresponding permutations, or equivalent of the corresponding monodromy representation.

Let f be a Belyĭ map, corresponding to a triple σ under the correspondence (1.1). We call the subgroup of S_n generated by the elements of σ the **monodromy group** of f. The monodromy group is well-defined up to conjugacy and in particular up to isomorphism, and we denote it by $G = \mathrm{Mon}(f) = \mathrm{Mon}(\sigma)$. The automorphism group of a Belyĭ map is the centralizer of its monodromy group (as a subgroup of S_n).

If the map $f : X \to \mathbb{P}^1$ is **Galois**, which is to say that the corresponding extension of function fields is Galois, then we call f a **Galois Belyĭ map**. More geometrically, this property boils down to the demand that the action of $\mathrm{Aut}(X)$ on the sheets of the cover be transitive; and combinatorially, this is nothing but saying that $\mathrm{Mon}(f) \subseteq S_n$ has cardinality $\#\,\mathrm{Mon}(f) = n$. Indeed, the monodromy group of a Belyĭ map can also be characterized as the Galois group of the smallest Galois cover of which it is a quotient.

The genus of a Belyĭ curve can be calculated by using the Riemann-Hurwitz formula. If we define the **excess** $e(\tau)$ of a cycle $\tau \in S_n$ 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

$$g = 1 - n + \frac{e(\sigma_0) + e(\sigma_1) + e(\sigma_\infty)}{2}. \tag{1.2}$$

In particular, we see that the genus of the 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_n. So for example, if $n = 23$, then $4^4 2^2 1^3$ denotes both the conjugacy class of the permutation (1 20 3 17)(5 9 7 8)(6 10 11 15)(13 14 12 16)(4 18)(19 2) and the corresponding ramification type; four points of ramification index 4, two of index 2, and three of index 1.

The **passport** of a degree n dessin with monodromy group representation σ is the triple (g, G, C), where g is the genus of the dessin, $G \subseteq S_n$ is its monodromy group and $C = (C_0, C_1, C_{infty})$ is the triple of conjugacy classes of $(\sigma_0, \sigma_1, \sigma_\infty)$ in G. The passport of a dessin is invariant under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ [71]). (Although by (1.2) the genus is determined by the conjugacy classes, it is still helpful to include it in the passport.) 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 $\sigma_0 \in C_0, \sigma_1 \in C_1, \sigma_\infty \in C_\infty$.

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 $\{\tau \in \mathrm{Aut}(\overline{\mathbb{Q}}) : X^\tau \cong X\}$ acting on $\overline{\mathbb{Q}}$, where X^τ is the base change of X by the automorphism $\tau \in \mathrm{Aut}(\overline{\mathbb{Q}})$ (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.

Let $f : X \to \mathbb{P}^1$ be a Belyĭ map with monodromy representation $\sigma : F_2 \to G \subseteq S_n$. Let $\mathbb{Q}(\chi(G))$ be the minimal field over which the character table of G is defined. By the Galois invariance of the monodromy group, for $\tau \in \mathrm{Aut}(\overline{\mathbb{Q}})$, we obtain another Belyĭ map $f^\tau : X^\tau \to \mathbb{P}^1$ with monodromy representation $\sigma^\tau : F_2 \to G \subseteq S_n$. If further τ fixes $\mathbb{Q}(\chi(G))$, then the elements σ_s, σ_s^τ are conjugate in G for $s = a, b, c$. This does not imply simultaneous conjugacy (that is, equivalence of the representations σ and σ^τ), but at least the degree of the field of moduli of a Belyĭ map over $\mathbb{Q}(\chi(G))$ is bounded above by the size of its passport.

Exploiting this link with triples of permutations, there are formulas (see e.g. Serre [124, Theorem 7.2.1]) that aid in the calculation the size of a passport and thereby its combinatorial orbit, a set of representative dessins for the passport. More precisely, given $G \subseteq S_n$, there is a formula that yields the total number of dessins with monodromy group contained in G, with the important proviso that a dessin is weighted by the reciprocal of the cardinality of its automorphism group.

These issues are not only interesting from a theoretical point of view; as we will see in our calculations below, it is often necessary to determine equations for dessins by recognizing complex numbers as algebraic numbers, for which LLL [89] is typically used; knowing the degree of the number field involved makes this calculation more efficient. Moreover, the estimate for this degree also gives a sense of how computable a given cover will be—if the estimate for the size is enormous, we are very unlikely to succeed in practice!

Example 1.3. As a concrete example, we give the above-mentioned Serre estimate for the number of genus 0 dessins with passport

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

where $H \leq G = S_{12}$. Calculating directly, we find 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, Serre's formula yields an estimated number of triples $567\frac{1}{4}$, 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). In each of the nontransitive solutions, the associated dessins are disjoint unions of curves of genus 1, such as those corresponding to the products of the genus 1 dessins with ramification types $(2^3, 5\ 1, 6)$ (which always have trivial automorphism group) with those with ramification types $(3^2, 4\ 2, 4\ 2)$ (which have either 1 or 2 automorphisms, depending on the solution).

Example 1.4. Another example is the case $(0, H; (4^4 2^2 1^3, 4^4 2^2 1^3, 5^4 1^3))$ with $H \leq G = M_{23}$. Here 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 an aside, we note that this estimate only gives the number of solutions under a stronger equivalence relation that includes an isomorphism of the monodromy group with M_{23} as part of the data (so-called M_{23}-dessins, also mentioned at the end of the next section); but since M_{23} has trivial normalizer in S_{23}, this coincides with the number of solutions under the usual equivalence relation of simultaneous conjugation.

An explicit (but complicated) formula, using Möbius inversion to deal with the disconnected dessins, was given by Mednykh [106] in much greater generality; in fact it can be used to count covers with specified ramification type of an arbitrary Riemann surface.

The fields of moduli of Belyĭ maps whose monodromy is an arithmetic subgroup of a triangle group were investigated in work of Pete L. Clark and the second author [20]. See also Section 4 for an example of an explicit calculation in this context.

Finally, we mention that in the Galois case, the situation simplifies considerably [22, 72, 132, 133].

Field of moduli versus field of definition. If X is a curve and F is a field of definition for X, then $F \supseteq M(X)$, so if X has a unique minimal field of definition F then in fact $F = M(X)$.

Curves of genus at most 1 over $\overline{\mathbb{Q}}$ are defined over their field of moduli, but this ceases to be the case for curves of larger genus in general. In fact, not all Belyĭ maps are defined over their field of moduli (as a Belyĭ map). This issue is a delicate one, and for more information, we refer to work of Coombes and Harbater [23], Dèbes and Ensalem [33], Dèbes and Douai, [32], and Köck [81]. The obstruction is essentially a lack of rigidification. For example, a curve furnished with an embedding into projective space is trivially defined over its field of moduli. Additionally, marking a point on the source X of a Belyĭ map one can prove that the field of moduli is a field of definition for the pointed Belyĭ curve [15, Theorem 2]. As mentioned before Example 1.3, this implication can then be applied to give an upper bound on the degree of the field of definition of a dessin, an important bit of information needed before applying LLL to recognize coefficients algebraically.

We mention some results that are most useful for generic dessins:

(1) If a curve or a Belyĭ map has trivial automorphism group, then it can be defined over its field of moduli, by Weil's criterion for descent [147].
(2) If the center of the monodromy group of a Belyĭ map is trivial, then it can be defined over its field of moduli by the main result in the article by Dèbes and Douai [32].

Note that for a Belyĭ map $f : X \to \mathbb{P}^1$, the curve X may descend to its field of moduli while the function f does not. 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.

Remark 1.5. Contrary to the vein of these remarks, Couveignes [26] has 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 with all its conjugates.

Additionally, a Belyĭ map may descend to its field of moduli in a weaker sense, namely as a cover of a conic, and not as a cover of $\mathbb{P}^1$ (with three marked points defined over $\mathbb{Q}$). It is this distinction that measures the descent obstruction for hyperelliptic curves, see work of Lercier, Ritzenthaler, and the first author [90]. A deep study of this problem in genus 0 was undertaken by Couveignes; in [24, §§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 $\mathrm{Aut}(\overline{\mathbb{Q}})$ 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.

The practical value of these considerations can be seen in [24, §10], where a dessin is calculated that descend explicitly to $\mathbb{Q}$ in the strong sense, but only as a function on a conic (that, due to the presence of automorphisms, can be twisted). This results in the condensation of equations from half a page to a few lines.

For more on this question, see also [25], and in a similar vein, the exhaustive work of van Hoeij and Vidunas on covers of conics in [139, §§3.3–3.4], [138, §4]. Many of these problems simplify upon passing to the quotient by the full automorphism group, since on this quotient one obtains a Weil cocycle [33]; and we again refer to the fundamental paper [32], that in addition applies to G-dessins, i.e., dessins provided with a rigidification of their monodromy group. As at the end of the previous section, we also briefly mention the situation for Galois dessins; these are defined over their field of moduli even without any rigidification [23].

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 Belyĭ maps 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, there exist passports that do not give rise to full Galois orbits. A first example was Schneps' flower [120, §IV, Example I]. Some further examples of distinguishing features of non-full Galois orbits have been found by Wood [154] and Zapponi [155], but in general 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 because of the non-availability of full libraries of dessins, making it an important project to construct such libraries.

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 [105], Malle and Matzat [94], and Jensen, Ledet, and Yui [67]. Upon specialization, one obtains Galois number fields with small ramification set: Roberts [113, 114] together with Malle [99] and with Jones [73, 74, 75], have used the specialization of three-point covers to exhibit number fields with small ramification set (e.g., ramified only at a subset of $\{2,3,5\}$). 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 [110]). 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 [156, §6].) These maps are objects of central study in complex dynamics [6, 112]: one may study the associated Fatou and Julia sets.

Dessins also figure in the study of Hall polynomials, (also called Davenport-Stothers triples) which are those 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 [146] and by Beukers and Stewart [14]; and Montanus [108] 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 [43].

Example 1.6. 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

$$\begin{aligned}
384242766^3 - 7531969451458^2 &= -14668\\
390620082^3 - 7720258643465^2 &= -14857
\end{aligned}$$

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

Belyĭ maps also give rise to interesting $K3$ surfaces. The Belyĭ maps of genus 0 and degree 12 (resp. 24) with ramification indices above $0, 1$ all equal $3, 2$ correspond to elliptic fibrations of K3 surfaces with only 4 (resp. 6) singular fibers. There are 6 (resp. 191) of these families, and especially in the latter case, their calculation is quite a challenge; by developing clever methods specific to this case, this was accomplished by Beukers and Montanus [13].

One can also specialize Belyĭ maps to obtain *abc* triples: this connection is discussed by Elkies [38], to show that the *abc* conjecture implies the theorem of Faltings, and by van Hoeij and Vidunas [138, 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 structure of this Belyĭ map [39, 40]. Explicit equations are useful in many contexts, ranging from the resolution of Diophantine equations to cryptography [122]. Reducing these equations modulo a prime also yields towers of modular curves that are useful in coding theory. Over finite fields with square q, work of Ihara [65] and Tsfasman, Vlăduţ, and Zink [136] 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 Drinfel'd and Vlăduţ [35]. By a construction due to Goppa [49], 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 [42]. 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 [36]. 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 nice.

There are also applications of explicit Belyĭ maps to algebraic solutions of differential equations: 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 [78] and Vidunas and Kitaev [143] 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 and Filipuk [142] classify coverings yielding transformations relating the classical hypergeometric equation to the Heun differential equation; these were computed by van Hoeij and Vidunas [138, 139].

Finally, there are applications to moonshine and to physics: there is a correspondence between genus zero congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and certain representations of sporadic groups, with connections to gauge theory [56, 57, 58].

Generalizations. Over $\overline{\mathbb{F}}_p$, one can consider the reduction of Belyĭ maps from characteristic 0; this is considered in Section 5 below. 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 $\mathbb{P}^1$ which is ramified only at ∞ by work of Katz [77]. 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 [19]: 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 components of the moduli space of surfaces [37]. Surely some computations in small dimensions and degree will be just as appealing as in the case of Belyĭ maps.

Another more general way to look at Belyĭ maps is through the theory of Hurwitz schemes, which give a geometric structure to the set $\mathcal{H}_{n,r}$, whose elements are the degree n morphisms to $\mathbb{P}^1$ ramified above n points. Belyĭś theorem then amounts to saying that by taking the curve associated to a morphism, one obtains a surjective map from the union 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 and Wewers [116] for a more complete account.

2. Gröbner techniques

We now begin our description of techniques for computing Belyĭ maps. We begin with the one that is most straightforward, involving the solutions to an explicit set of equations over $\mathbb{Q}$.

Direct calculation. The direct method has been used since the first Belyĭ maps were written down, and in small examples (typically with genus zero), this technique works well enough. A large number of authors describe this approach, with some variations relevant to the particular case of interest. Shabat and Voevodsky [126] and Atkin and Swinnerton-Dyer [5] were among the first. Birch [15, Section 4.1] computes a table for covers of small degree and genus. Schneps [120, III] discusses the case of clean dessins of genus zero and trees. Malle [98] computed a field of definition for many Belyĭ maps of small degree and genus zero 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 and Matzat [94, §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 zero Belyĭ maps in detail in his Ph.D. thesis [50] (so presumably it was also used in his published work [51]). Elkies [39] used this technique to compute equations for Shimura curves. Other authors who have used this method are Hoshino [62] (and with Nakamura [63]), who computed the non-normal inclusions of triangle groups (related to the Belyĭ-extending maps of Wood [154]). Couveignes [27, §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 monodromy representation $\sigma = ((1\ 2), (2\ 3), (1\ 3\ 2))$ from S_3. Since these permutations generate the full symmetric group S_3, the monodromy group of this dessin is $\mathrm{Mon}(\sigma) = S_3$. The Riemann-Hurwitz formula (1.2) gives the genus as

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

We also compute directly that any permutation triple from these conjugacy classes is simultaneously conjugate to σ. Therefore the Belyĭ map is defined over $\mathbb{Q}(\chi(S_3)) = \mathbb{Q}$. As such, the map $f : X = \mathbb{P}^1 \to \mathbb{P}^1$ is given by a rational function $f(t) \in \mathbb{Q}(t)$. 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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; therefore we take this point also to be ∞, which we are free to do up to automorphisms of $\mathbb{P}^1_{\mathbb{Q}}$, and hence $f(t) \in \mathbb{Q}[t]$. 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 $a, c \in \mathbb{Q} \setminus \{0\}$ and

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

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

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

and so by comparing coefficients we obtain $b = 1/2$, $c = -2$, and $a = -3/2$. In particular, we see that the map is indeed defined over $\mathbb{Q}$. 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 is $\{0, 1, \infty\}$ 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 should be clear from this example (but see Schneps [120, Definition 8]) how to set up the corresponding system of equations for a Belyĭ map on a curve of genus $g = 0$. For a large list of examples of this kind, see Lando and Zvonkin [88, Example 2.3.1].

Example 2.2. To get a sense of how complicated these equations get, consider the case $G = \mathrm{PGL}_2(\mathbb{F}_7)$ with monodromy representation $F_2 \to G$ 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 genus 0. After putting the totally ramified point at ∞, the map f is given by a polynomial $f(t) \in \overline{\mathbb{Q}}[t]$ such that

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

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 $a(t) = t^3 + a_2t^2 + a_1t + a_0$, etc.

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

$$\begin{aligned}
&a_0^2b_0c - cd_0^3e_0, \\
&2a_1a_0b_0c + a_0^2b_1c - 3cd_1d_0^2e_0 - cd_0^3e_1, \\
&2a_2a_0b_0c + a_1^2b_0c + 2a_1a_0b_1c + a_0^2c - 3cd_1^2d_0e_0 - 3cd_1d_0^2e_1 - cd_0^3 - 3cd_0^2e_0, \\
&2a_2a_1b_0c + 2a_2a_0b_1c + a_1^2b_1c + 2a_1a_0c + 2a_0b_0c - cd_1^3e_0 - 3cd_1^2d_0e_1 - 3cd_1d_0^2 \\
&\qquad - 6cd_1d_0e_0 - 3cd_0^2e_1, \\
&a_2^2b_0c + 2a_2a_1b_1c + 2a_2a_0c + a_1^2c + 2a_1b_0c + 2a_0b_1c - cd_1^3e_1 - 3cd_1^2d_0 - 3cd_1^2e_0 \\
&\qquad - 6cd_1d_0e_1 - 3cd_0^2 - 3cd_0e_0, \\
&a_2^2b_1c + 2a_2a_1c + 2a_2b_0c + 2a_1b_1c + 2a_0c - cd_1^3 - 3cd_1^2e_1 - 6cd_1d_0 - 3cd_1e_0 - 3cd_0e_1, \\
&a_2^2c + 2a_2b_1c + 2a_1c + b_0c - 3cd_1^2 - 3cd_1e_1 - 3cd_0 - ce_0, \\
&2a_2c + b_1c - 3cd_1 - ce_1.
\end{aligned}$$

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 $t \leftarrow ut$ with $u \in K^\times$ 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.

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, 29, 30, 54, 86].

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

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

with

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

The direct method does not give an obvious way to discriminate 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 $\deg \phi$ 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. 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, 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 regular function $y + x^2 + 4x + 18$ on the elliptic curve $y^2 = 4(2x+9)(x^2+2x+9)$. Both were described by Birch [15]. In the direction of tabulating the simplest dessins in this way, all clean Belyi dessins with at most 8 edges were computed by Adrianov et al. [2]. Magot and Zvonkin [93] computed the genus zero Belyĭ maps corresponding to the Archimedean solids, including the Platonic solids, using symmetry and Gröbner bases.

For larger examples, 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.) One further differentiation trick, which we introduce in the next section, allows us to compute in a larger range. However, even after this modification, several obstacles to the method remain. The set of solutions can have positive-dimensional degenerate components: these correspond to situations where roots coincide or there is a common factor and are often called parasitic solutions [84, 85]. The set of parasitic solutions have been analyzed in some cases by van Hoeij and Vidunas [139, §2.1], but they remain a nuisance in general.

The ASD differentiation trick. There is a trick, due to Atkin and Swinnerton-Dyer [5, §2.4] to use 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 [27] implies that this trick was known to Fricke; it has apparently been rediscovered many times. Hempel [60, §3] used differentiation by hand to classify subgroups of

$\mathrm{SL}_2(\mathbb{Z})$ of genus zero with small torsion and many cusps. Couveignes [24, §2,§10] used this to compute examples in genus zero of clean dessins (i.e. those for which all ramification indices above 1 are equal to 2). Schneps [120, §III] used this to describe a general approach in genus zero. Finally, Vidunas [141] applied the trick to differential equations, and Vidunas and Kitaev [143] extended this to covers with 4 branch points.

Example 2.4. Again we illustrate the method by an example. Take $\sigma = ((1\,2), (2\,4\,3), (1\,2\,3\,4))$. We again find genus $g = 0$. 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 in 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 noted by Elkies [40].

Lemma 2.5. *Let $f : X \to \mathbb{P}^1$ be a Belyi map with ramification type σ. Let*

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

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

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

Proof. 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 in [40]. The methods in his example generalize to arbitrary situations where the ramification is uniform (all ramification indices equal) except at one point: Elkies [40] treats the case $3^9 1^1, 2^{14}, 7^4$ is exhibited.

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 this not seem to make the ideal grow further than in the first step.

Question 2.6. *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 zero)?*

However, Shabat [125, Theorem 4.4] does derive some further information by considering second-order differentials. Moreover, Dremov [34] obtains an alternative way to calculate dessins by considering the relation $MP(f^{-1}) = -MP(f)/f$ on the quadratic differential

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

which holds for any regular function f. It is not immediately clear from his paper how to apply this in general, though.

Question 2.7. *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 Belyi 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 essential 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.)

Formulated more intrinsically, the naive equations of the previous section determine a scheme in the coefficient variables whose geometric points correspond to those of a closed subscheme of a Hurwitz scheme, but this naive scheme usually is usually very non-reduced. The additional ASD relations partially saturate the corresponding ideal, so that the new equations define 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 2.8. 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 $(2^3, 2^3, 3^2)$, $(2^2 1^2, 3^2, 4\ 2\ )$, $(3^2, 3\ 2\ 1, 3\ 2\ 1)$, $(3\ 1^3, 4\ 2, 4\ 2)$, $(4\ 2, 4\ 1^2, 3\ 2\ 1)$, and $(4\ 2, 3\ 2\ 1, 3\ 2\ 1)$, for which it reduces the multiplicity of the corresponding solutions from $9, 3, 3, 3, 4, 3$ respectively to 1. Note the tendency of dessins with many automorphisms to give rise to highly singular points.

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 7; it corresponds to the ramification triples $(4\ 2\ 1, 3\ 2\ 1^2, 4\ 3)$, 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.

As a more dramatic example, for the ramification triples $(2^4, 3^2 2, 3^2 2)$ and $(2^3 1^2, 4^2, 3^2 2)$, differentiation reduces the multiplicities from 64 to 1 (resp. 64 to 4). In the latter case, these multiplicities are in fact not determined uniquely by the correspond ramification type, and the solutions get split into Galois orbits accordingly.

Question 2.9. *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 [97, 100] to compute covers with passports $(0; \mathrm{Hol}(E_8); (4\ 2\ 1^2, 4\ 2\ 1^2, 6\ 2))$ and $(0; \mathrm{PGL}(\mathbb{F}_{11}); (2^5 1^2, 4^3, 11\ 1))$ and similarly Malle and Matzat [95] to compute covers for the passports $(0; \mathrm{PSL}_2(\mathbb{F}_{11}); (2^4 1^3, 6\ 3\ 2, 6\ 3\ 2))$ 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 and Kitaev [143, §5]. For further developments on p-adic methods to compute Gröbner bases, see Arnold [4] or Winkler [149]. One can also simplify lift a solution modulo p directly, and sometimes such solutions can be obtained relatively quickly without also p-adically lifting the Gröbner bases: see Section 5 below.

For a very complete discussion of trees and Shabat polynomials and troves of examples, see Lando and Zvonkin [88, §2.2].

In the work of van Hoeij and Vidunas [138, 139] mentioned in Section 1, genus zero Belyi 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 and 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 [138]. 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 2.10. *Are there other sources of equations (such as those arising from differential equations, algebraic manipulation, or other sources) 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.

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 [89] (and other variants, such as PSLQ [45]) to guess algebraic numbers which represent the exact values. Finally, one can use the results from Section 7 to verify that the guessed cover is correct; if not, one can go back and iterate to refine the solution.

Remark 3.1. In the situation where the complete Galois orbit of the triple is contained in the passport, 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. When applicable, this drastically reduces the precision required to recognize the Belyĭ map exactly.

In order for this procedure to work, one needs a good starting approximation to the solution. In the examples that have been computed, 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;

indeed, the dynamical system arising from Newton's method has quite delicate fractal-like properties and its study is a subject in itself [111].

Question 3.2. *Is there a 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 and Granboulan [24, 50, 28]. 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 [24] gives a detailed treatment of the case of trees, corresponding to clean Belyĭ polynomials $f(t)$ 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 in unknown variables. See Granboulan [50, Chapter IV] for an example with monodromy group $\mathrm{Aut}(M_{22})$.

Remark 3.3. There is a misprint in the example of Couveignes [24, §3, pg. 8], corrected by Granboulan [50, p. 64].

So far, it seems that this method has been limited to genus zero Belyĭ maps with special features. A similar method was employed by Matiyasevich [104] 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 3.4. *Can an inductive 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 and Stephenson [18], 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 or 1, 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, and Thurston [82, 101, 135], states that given a triangulation of a 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 and Stephenson [21] and Mohar [107] 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 and Stephenson [7]. 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 and Stephenson [18, §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 [18, §6.1], which makes this approach quite suitable for calculating large bases 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 [18, §7]. In examples, it is possible for the insertion of a new vertex to drastically increase the accuracy needed [18, Figure 25] and thereby the number of discrete refinements needed, quite radically increasing the complexity of the calculation [18, §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 we find equations for X by numerically computing modular forms on X.

Example 3.5. In Figure 3.6, we give an example from an alternate implementation by Bruce Westbury which is freely available [148] for the case of genus 0, where 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 1.4 that descend to $\mathbb{R}$.

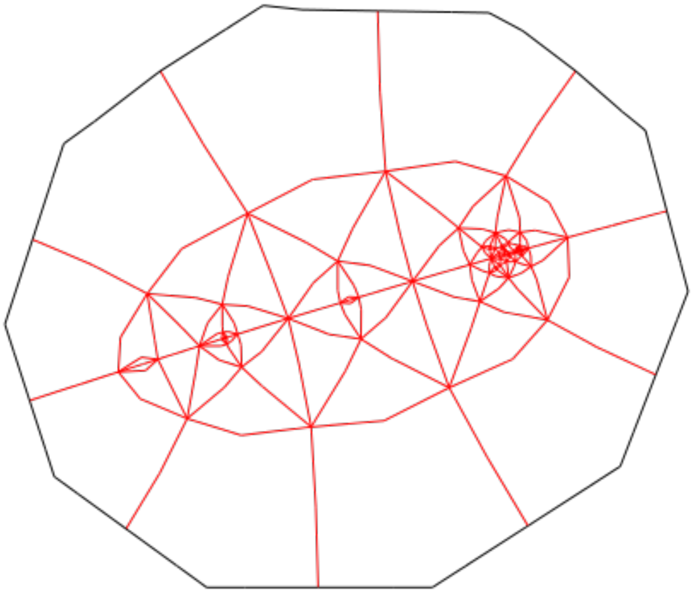


Figure 3.6: A second subdivision for M_{23}

Several more subdivisions are needed to get the solution close enough to apply Newton-Raphson.

Puiseux series. Couveignes and Granboulan [28, §6] have 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 which converges in a neighborhood of P. Similarly, at a ramification point P, there is an expansion for f which 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 [28, §7].

Question 3.7. *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 [8, 140], 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 combined into a refined technique.

Question 3.8. *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 [27, §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. It is an extension of the zipper method due to Marshall and Rohde [103]. The zipper method finds a numerical approximation of the conformal map of the unit disk onto any Jordan region [102]. In its extension, this amount to solving the Dirichlet problem with boundary for the domain of the exterior of the desired dessin, which can be done quite simply for trees even with thousands of branches. For example, Rohde has computed the dessins associated to the 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).

Question 3.9. *Does the zipper method extend to more complicated genus zero dessins and to higher genus?*

In the latter extension, one would need to consider not only the convergence of the dessin but also the associated Belyĭ curve X, so one will have to do more than simply solve the Dirichlet problem.

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 [52]: "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 Belyi announced exactly that result."

Classical modular forms. Let F_2 be the free group on two generators x, y, and let $z = (xy)^{-1}$. Then the map which considers the permutation action of x, y, z on the cosets of a subgroup yields a bijection

$$\begin{gathered} \left\{\text{permutation triples } \sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_n^3\right\} / \sim \\ \overset{1:1}{\longleftrightarrow} \\ \{\text{subgroups of } F_2 \text{ of index } n\} / \sim; \end{gathered} \tag{4.1}$$

here the equivalence relation on triples is again uniform conjugation, and the equivalence relation on subgroups is conjugation in F_2. By equation (1.1) in Section 1, this means that the isomorphism classes of Belyĭ maps are also 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, acting faithfully on the complex upper half plane. Indeed, consider the group

$$\mathrm{SL}_2(\mathbb{Z}) = \{\gamma \in \mathrm{M}_2(\mathbb{Z}) : \det(\gamma) = 1\}$$

of 2-by-2 matrices with integer coefficients with determinant 1. Then 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 zero by uniformizing map $j : X(1) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C})$ (often called the modular elliptic j-function),

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

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

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

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

The quotient $X(2) = \Gamma(2)\backslash\mathcal{H}^*$ is again a Riemann surface of genus zero, and we obtain another uniformizing map $\lambda : X(2) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C})$. As for the set of cusps for $\Gamma(2)$, its action on $\mathbb{P}^1(\mathbb{Q})$ has three orbits, with representatives $0, 1, \infty \in \mathbb{P}^1(\mathbb{Q})$. Note that the cusps -1 and 1 are equivalent. The function λ has an expansion

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

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

As a uniformizer for a congruence subgroup of $\mathrm{PSL}_2(\mathbb{Z})$, the function $\lambda(z)$ has a modular interpretation. Since we do not divide by the full group $\mathrm{PSL}_2(\mathbb{Z})$, the family of elliptic curves living over $X(2)$ inherits extra structure from the family with rigidified torsion on $\mathcal{H}$. Algebraically, this structure is as follows. 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 which forgets this additional torsion structure on a Legendre curve and remembers its 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 quotient $j : X(2) \to X(1)$ is a Belyĭ map of degree 6 with monodromy S_3 ramified over $0, 1728, \infty$, given explicitly by (4.2).

The cusp ∞ places 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

$$\begin{gathered} \left\{ \begin{array}{c} \text{triples } \sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_n^3 \text{ that satisfy } \sigma_0\sigma_1\sigma_\infty = 1 \\ \text{with a marked cycle of } \sigma_\infty \end{array} \right\} /\!\sim \\ \overset{1:1}{\longleftrightarrow} \\ \{\text{subgroups of } \Gamma_2 \text{ of index } n\} /\!\sim \end{gathered} \tag{4.3}$$

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 $(\sigma_0, \sigma_1, \sigma_\infty)$ and $(\sigma_0', \sigma_1', \sigma_\infty')$ in S_n^3 along with marked cycles c, c' in $\sigma_\infty, \sigma_\infty'$ are equivalent if and only if there exists a τ in S_n such that $\tau\sigma_s\tau^{-1} = \sigma_s'$ for $s \in \{0, 1, \infty\}$ and additionally $\tau c \tau^{-1} = c'$.

It is a marvelous consequence of this bijection, 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 $\mathcal{H}^*/\Gamma \xrightarrow{\sim} X(\mathbb{C})$. This is the meaning of Grothendieck's comment: the rigidification here corresponding to the subgroup Γ. In general, the group Γ is noncongruence, meaning that it does not contain a subgroup $\Gamma(N)$ (and thereby membership in the group can be determined by congruences on the coordinate entries of the matrices). The perspective of modular forms is taken by Atkin and Swinnerton-Dyer [5] and Birch [15, 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, and Yang [91] 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 $\Gamma(2) \to S_n$ given by $x, y, z \mapsto \sigma_0, \sigma_1, \sigma_\infty$ as in (4.3). A fundamental domain for Γ be given by Farey symbols [87], 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 [119] (in a package for *arithmetic subgroups defined by permutations*, by Kurth, Loeffler, and Monien) and Magma [16] (by Verill).

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

$$\lambda : X \to X(2),$$

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 $\mathcal{H}$ which are invariant under Γ.

We are led to the following definition. A modular form for a finite index subgroup $\Gamma \leq \mathrm{PSL}_2(\mathbb{Z})$ 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: 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. Consequently, evaluation on a basis for $S_k(\Gamma)$ defines a holomorphic map $\phi : X \to \mathbb{P}^{d-1}$ where $d = \dim_{\mathbb{C}} S_k(\Gamma)$. Classical theory of curves yields a complete description of the map ϕ; for example, for generic X of genus $g \geq 3$, already taking $k = 2$ (i.e., a basis of holomorphic 1-forms) gives a canonical embedding of X as an algebraic curve in projective space, by the theorem of Max Noether.

Selander and Strömbergsson [123] use this analytic method of modular forms to compute Belyĭ maps, an idea already implicit in the original work of Atkin and Swinnerton-Dyer [5] and developed earlier by Hejhal [59] 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 6 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 a 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. However, it seems to work well in practice, and once complex approximations for the cusp forms are known, they compute approximate algebraic equations that they satisfy, and finally turn to Newton iteration and get the exact solution by lattice reduction. Atkin and 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 of ζ in powers of ξ 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?*

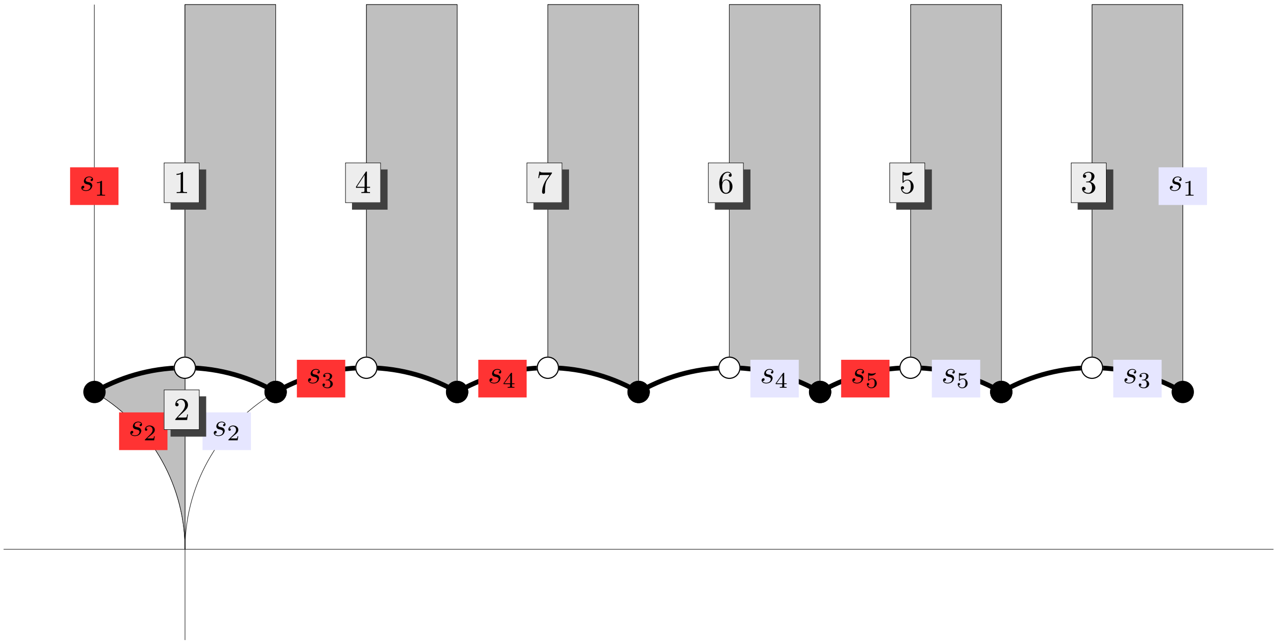
For Belyĭ maps for which the corresponding subgroup Γ is congruence, and contains $\Gamma(N)$ for some $N \in \mathbb{Z}_{>0}$ (and so membership in the group is defined by congruence conditions on the entries of the matrix), methods of modular symbols [130] can be used to determine the q-expansions of modular forms using exact methods. The Galois groups of congruence covers are all contained in a quotient 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 [68].

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 [150]. The cusp widths of this subgroup are 1 and 6. The information on the cusps tells us that the ramification type of the dessin is given by $(6, 1)$, whereas the indices above 0 (resp. 1) have to be divisible by 3 (resp. 2). This forces the genus of the dessin to equal 0, with ramification triple $(6\ 1, 3^2 1, 2^3 1)$.

There are exactly two transitive covers with this ramification type, both of genus 0. The monodromy group G of these dessins are both isomorphic with the same Frobenius group of order 42; they correspond to two choices of conjugacy classes of cyclic subgroups of G of order 6. 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 points of order 3 at $t = 0$ and order 2 at $t = 1$. In this case, the q-expansion for the Hauptmodul for Γ is given by

$$x(q) = \frac{1}{\eta q^{1/6}} + 0 + \frac{9+\sqrt{-3}}{2^1 3^4}\eta q^{1/6} + \frac{-3-5\sqrt{-3}}{2^2 3^5}(\eta q^{1/6})^2 + \frac{1-3\sqrt{-3}}{2^1 3^7}(\eta q^{1/6})^3 + \dots$$

where

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

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

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

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

Modular forms on subgroups of triangle groups. There is related method to the use of classical modular forms which 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 [92]). For an introduction to triangle groups, including their relationship to Belyĭ maps and dessins d'enfants, see the surveys of Wolfart [152, 153].

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

$$\Delta(a, b, c) = \langle \delta_a, \delta_b, \delta_c \mid \delta_a^a = \delta_b^b = \delta_c^c = \delta_a\delta_b\delta_c = 1\rangle$$

where exponents with $s = \infty$ are ignored and the quantity $\chi(a, b, c) = 1 - 1/a - 1/b - 1/c \in \mathbb{Q}$. 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 orientation-preserving subgroup of the group generated by the reflections in the sides of a triangle with angles $\pi/a, \pi/b, \pi/c$ drawn in the geometry H, where H is the sphere, Euclidean plane, or hyperbolic plane, according as $\chi(a,b,c)$ is negative, zero, or positive.

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

$$\begin{aligned} \Delta(a,b,c) &\to S_n \\ \delta_a, \delta_b, \delta_c &\mapsto \sigma_0, \sigma_1, \sigma_\infty \end{aligned}$$

where $a,b,c \in \mathbb{Z}_{\geq 2}$ are the orders of $\sigma_0, \sigma_1, \sigma_\infty$, respectively. The stabilizer of a point $\Gamma \leq \Delta(a,b,c)$ has index n, and the above homomorphism is recovered by the action of Δ on the cosets of Γ. The quotient map

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

then realizes the Belyĭ map with monodromy σ, so from this description we have a way of constructing the Belyĭ map associated to σ. In other words, as in (4.1), the bijection (1.1) generalizes to

$$\begin{gathered} \left\{ \begin{array}{c} \text{triples } \sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_n^3 \text{ that satisfy } \sigma_0\sigma_1\sigma_\infty = 1 \\ \text{and } a,b,c \text{ are the orders of } \sigma_0, \sigma_1, \sigma_\infty \end{array} \right\} \Big/ \sim \\ \overset{1:1}{\longleftrightarrow} \\ \{\text{subgroups of } \Delta(a,b,c) \text{ of index } n\} \, / \sim, \end{gathered} \tag{4.10}$$

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, the triples are not marked, as in the previous subsection.)

Explicitly, one obtains the Riemann surfaces corresponding to a subgroup $\Gamma < \Delta(a,b,c)$ under the bijections (4.10) and (1.1) by gluing together triangles of the right sizes and making identifications. This gives a conformally correct way to draw dessins and a method for computing the covers themselves numerically.

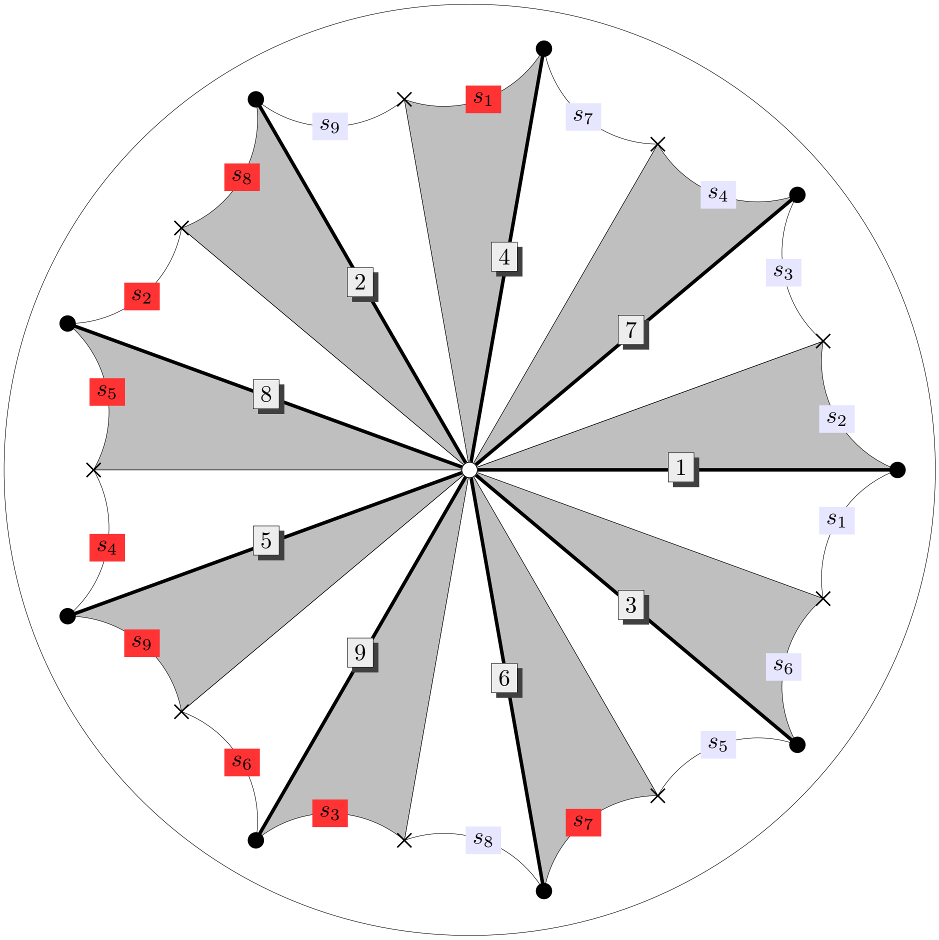
This method has been developed in recent work of Klug, Musty, Schiavone, and the second author [80]. Algorithms are provided for working with the corresponding triangle group Δ, determining explicitly the associated finite index subgroup Γ, and then drawing the dessin on H together with the gluing relations which 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 the second author and Willis [144]. This method works quite well in practice; as an application, a Belyĭ map of degree 50 of genus zero regularly realizing the group $\mathrm{PSU}_3(\mathbb{F}_5)$ is computed.

Example 4.11. Consider the following triple of permutations:

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

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. 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.

We follow the method of Klug, Musty, Schiavone, and the second author [80]. First, we compute a coset graph, the quotient of the Cayley graph for Δ on the generators $\delta_a^{\pm}, \delta_b^{\pm}$ 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 $z' = \gamma z$.



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

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

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

We consider the space $S_2(\Gamma)$ of cusp forms of weight 2 for Γ, defined as in (4.4) but with no conditions on the cusps. 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; we approximate this integral by evaluation at $O(N)$ points taken up to automorphy as points in the fundamental domain D_Γ using the reduction algorithm.

We find the echelonized basis

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

where $\Theta = 1.73179\ldots + 0.6303208\ldots\sqrt{-1}$. The algebraicity and near integrality of these coefficients are conjectural [80], so this expansion is only correct numerically to the precision computed.

We now compute the image of the canonical map $X \to \mathbb{P}^2$ given by $w \mapsto (x(w) : y(w) : z(w))$; we find a unique quartic relation

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

so 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:

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

We can then verify on the curve $X(\Gamma)$ that this rational function defines a three-point cover with the above ramification points.

An important feature of methods using modular forms is that it works directly on the target Riemann surface, and hence there are no "parasitic" solutions to discard.

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

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.

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 [96] used this method to compute polynomials with Galois groups M_{22}, $\mathrm{Aut}(M_{22})$, and $\mathrm{PSL}_3(\mathbb{F}_4) \cdot 2$ over $\mathbb{Q}$. Elkies [40] 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 [41], Watkins [146] and Elkies and Watkins [43]) has also successfully used p-adic methods to compute Belyĭ maps. Elkin and Siksek [44] have used this method and tabulated Belyĭ maps of small degree. Van Hoeij and Vidunas [138] used this approach to compute a list of examples whose branching is nearly regular, before extending the direct method in [139] as explained in Section 2. More recently, Bartholdi, Buff, von Bothmer, and Kröker [6] computed a Belyĭ map in genus 0 which 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 modulo which primes one can reduce in the initial step (finding Belyĭ maps over finite field) of the procedure above.

Theorem 5.1 (Beckmann [9]). *Let $f : X \to \mathbb{P}^1$ be a Belyĭ map defined over its moduli field K, and let G be the monodromy group of f. Suppose that $\mathfrak{p}$ is a prime ideal of K lying above the rational prime p and that $p \nmid \#G$. Then p is unramified in K and f has a model defined over K with good reduction modulo $\mathfrak{p}$.*

In the notation of this theorem, if p divides the order of one of the permutations σ then f has bad reduction at $\mathfrak{p}$ [15, 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 Obus [109].

Question 5.2. *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, and Kröker describe [6, Algorithm 4.7] a more careful method for genus 0, working directly with univariate polynomials (and rational functions) with coefficients in $\mathbb{F}_q$. We show in the example below an approach that is similar in spirit to their approach and that works for hyperelliptic curves as well.

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

Question 5.3. *How efficiently can a Belyĭ map be computed modulo a prime p? How far can one reduce the affine space required for the enumeration?*

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

Example 5.4. We consider again the dessins with ramification type $((6,1),(3^2,1),(2^3,1))$ 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., $\alpha^2+4\alpha+2=0$. 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 nonsingular, 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 merrily 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 that this yields a solution over $\mathbb{Q}(\sqrt{-3})$ to the given equations and that they are the requested Belyĭ maps. Though we content ourselves with this representation, one can simplify the equation even further by suitable scalar multiplications in t, or even better, the general methods described in Section 7.

Example. 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 Pete L. Clark and the second author [20].

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

Let $f : E \to \mathbb{P}^1$ be the degree 11 map defined by the above data, and let $\phi : X \to \mathbb{P}^1$ be the corresponding Wolfart curve, i.e. the smallest Galois cover of f, whose automorphism group is isomorphic with M. Then X has genus 100, and by [20, Theorem A] the field of moduli $M(X)$ of the curve X is equal to its minimal field of definition. Moreover, $M(X)$ is an extension of degree at most 2 of $\mathbb{Q}(\sqrt{5})$ that is contained in the ray class field of $\mathbb{Q}(\sqrt{3},\sqrt{5})$ of conductor 11∞. The field of moduli $M(X,G)$ of the Belyĭ map ϕ together with its Galois group G (which is the monodromy group of f) is contained in the same ray class field and is an extension of $M(X)$ of degree at most two, and is again a field of definition of these data. As a consequence of the calculations that follow, we will see that $M(X)$ is a proper extension of degree 2 of $\mathbb{Q}(\sqrt{5})$ and that a further degree 2 extension is in fact needed to obtain the Galois action.

The ramification above the points $0, 1, \infty$ (which in accordance with the construction above are divisors of $3, 5, 6$) are given by $3^3 1^2, 5^2 1, 6\ 3\ 2$, and one computes that 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 Belyi function f has the form

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

where $q(x) = q_8 x^8 + \dots + q_0$ and $r(x) = r_6 x^6 + \dots + r_0$ 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

$$\begin{aligned} \mathrm{N}_{\mathbb{C}(x,y)/\mathbb{C}(x)}(f_{\mathrm{num}}(x,y)) &= q(x)^2 - r(x)^2\pi(x) \\ &= q_8^2 x^3 (x-1)^2 s(x)^3 t(x) \end{aligned} \tag{5.5}$$

where $s(x) = x^3 + s_2x^2 + s_1x + s_0$ and $t(x) = x^2 + t_1x + t_0$, and similarly above 1 we should have

$$\begin{aligned}(5.6)\qquad \mathrm{N}_{\mathbb{C}(x,y)/\mathbb{C}(x)}((f(x,y)-1)_{\mathrm{num}}) &= (q(x)-(x-1)^2x^3)^2 - r(x)^2\pi(x)\\ &= q_8^2x^3(x-1)^2u(x)v(x)\end{aligned}$$

where $u(x) = x^2 + u_1x + u_0$ 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 Matthieu 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} also occurs. Discarding these parasitic solutions is a nontrivial task until one has already computed all of them along with the correct ones.

As explained above, we search for a solution in a finite field $\mathbb{F}_\ell$, lift such a solution using Hensel's lemma (if it applies), and then attempt to recognize the solution ℓ-adically as an algebraic number using the LLL-lattice reduction algorithm. This curve will be defined over $M(X,G)$ and more precisely that this field is a quadratic extension of $\mathbb{Q}(\sqrt{3},\sqrt{5})$ ramified only at 11 [20]. 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 $\ell = 49, 59$, so there is no hope of simply running over the solution 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 (5.5)–(5.6), we have

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

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

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

From equation (5.5) we have

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

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 (the Vermont Advanced Computing Center) using Magma [16], after a few days we have our answer. We find some solutions in $\mathbb{F}_{49}$ but only one solution lifts ℓ-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 7), 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 but 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

$$b = 4\sqrt{3} + \frac{1}{2}(11+\sqrt{5});$$

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:

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

The j-invariant of E generates the field $\mathbb{Q}(\sqrt{3},\sqrt{5},\beta)$, so this is its field of definition. This also shows that $M(X,G) = \mathbb{Q}(\sqrt{3},\sqrt{5},\beta)$, since $M(X,G)$ is an extension of degree at most 2 of $\mathbb{Q}(\sqrt{3},\sqrt{5})$ [20]. Indeed, in the case of equality, the curve E would be defined over $\mathbb{Q}(\sqrt{3},\sqrt{5})$ by the Galois correspondence for covers applied to the subgroup $A_5 \subset \mathrm{PSL}_2(\mathbb{F}_{11})$.

The results on the field of moduli in [20] were obtained by weak rigidity. We see that even in this case, where the fields of moduli are proper extensions of what they could minimally be, we still get partial information that allows one to capture information about its field of moduli by computational methods.

6. Galois dessins

In this short section, we sketch some approaches for calculating Galois dessins, corresponding to Belyĭ maps $f : X \to \mathbb{P}^1$ whose extension of function fields is Galois. The flavor of these computations is completely different from those in the other sections, and the action of the group is used heavily. In a sense, all dessins are known once the Galois dessins are known; however, the growth in degree between the dessin and its Galois closure makes it very difficult in general to carry this out in practice.

Galois dessins in genus 0 are given by Couveignes and Granboulan [28], and correspond to the regular solids. The most difficult case, that of the icosahedron, was calculated first by Klein [79]. The Galois dessins 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 and Syddall [128].

So it remains to consider the higher genus case, where dessins are linked with triangle groups (see Section 4). In genus ≥ 2, Wolfart [153] has shown that Galois dessins 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 $\mathcal{M}_g$. Wolfart [151] compares these dessins 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 these curves are essentially known; they come from Fermat curves [151, §4].

A fundamental technique for proving these theorems is to determine the representation of the automorphism group on the space of differentials; this is elaborated by Berry and Tretkoff [12] and Streit [131]. 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 under a linear action. In other words, determining the 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 6.1. We illustrate the invariant theory involved by giving an example of a calculation of a quotient map $C \to C/\operatorname{Aut}(C)$ that turns out to be a Belyĭ map; the example was suggested by Elkies.

Consider the curve C defined by the following variant of the Bring equations:

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

There is an obvious action by S_5 on this curve by permutation of coordinates. To find coordinates on the quotient C/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 C. 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 $f = (p_3^5 : p_5^6)$ as a morphism from $f : C \to \mathbb{P}^1$.

The intersection of the hyperplanes defined by $p_3 = 0$ and $p_5 = 0$ with C are finite; indeed, this is obvious since the corresponding functions do not vanish indentically on C. By Bézout's theorem, these zero loci are of degree 24 resp. 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 $C/\operatorname{Aut}(C)$ is uniformized by the upper half plane $\mathcal{H}$ since the genus 9 curve C is, so $C/\operatorname{Aut}(C)$ 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 C; this point turns out to be $-(15/2)^2$. So the map $f : C \to \mathbb{P}^1$ defined by

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

realizes the quotient $C \to C/S_5$.

In fact we have an isomorphism $\mathrm{Aut}(C) \cong S_5$ since $\mathrm{Aut}(C)$ cannot be bigger than S_5; this is because such a proper inclusion would give rise to a Fuchsian group properly containing the triangle group $\Delta(2,5,6)$. But this group is maximal (by work of Takeuchi [134], or more generally see Singerman [127] or Greenberg [53, 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. From the exceptional isomorphism $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$, we also have found a Galois cover realizing a projective linear group.

Remark 6.2. Since $\Delta(3,5,5) \leq \Delta(2,5,6)$ lies with 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 originals. An equation for this cover (and dessin) 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 originals $\pm 15/2$ of the point of order 5 to 0 and 1, respectively.

Alternatively, we can calculate as follows. It is known that the full ring of invariant homogeneous polynomials for S_5 is generated by the power sums $p_1, \dots, p_5$ 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

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

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

$$Q : y^2 = \frac{4}{45}xz + 5z^2$$

and g is given by

$$g(v,w,x,y,z) = (s_3^5 : as_5 : s_5^3).$$

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 Q satisfy $(x : z) = (0 : 1)$. But the corresponding points are only defined over $\mathbb{Q}(\sqrt{5})$, so this is a descent only in the weak sense. We explain why this happens at the group-theoretical level.

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 $\mathbb{Z}/2\mathbb{Z}$.

In particular, this means that the Galois orbit of these covers consists of a single isomorphism class, as their monodromy group upon composition differ [154]. A Galois cover, considered as a mere cover, is defined over its field of moduli [32], so our equations above can be twisted to a dessin over $\mathbb{Q}$, that is, with ramification at three rational points.

However, the methods of Dèbes and Douai [32] also show that the Galois cover does *not* descend as a Galois cover unramified outside $\{0, 1, \infty\}$. This is essentially due to the action of the outer automorphism induced by the inclusion $A_5 < S_5$. 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 omit this calculation and content ourselves with the symmetric form above.

To conclude, we note that this means that we have found a Galois cover realizing $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$ over its minimal field of definition as a Galois cover.

7. Simplification and verification

Once a potential model for a Belyĭ map has been computed, it often remains to simply the model as much as possible and to verify its correctness (independently of the method used to compute it).

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 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 and Vidunas [139, §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 and Stoll in [31], using results from Julia [76] to find a binary quadratic covariant, to which classical reduction algorithms are then applied. The resulting algorithms substiantially reduce the height of the coefficients of the binary form in practice. A generalization to, and implementation for, totally real fields is given in Bouyer and Streng [17].

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 Belyĭ map. That the resulting binary form may have double roots is no problem; see the discussion by Cremona and Stoll [31, 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 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 and Streng [17, §3.3].

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

Question 7.1. *Are there general methods to simplifying equations of curves defined over a number field in practice?*

For the case of plane curves, at least, the results for binary forms are relevant, considering the decomposition of SL_2-representations

$$\mathrm{Sym}^d(\mathrm{Sym}^2 \mathbb{C}^2) = \bigoplus_{i=0}^{\lfloor d/2 \rfloor} \mathrm{Sym}^{2d-4i} \mathbb{C}^2,$$

which gives a link between ternary forms of degree d and suitable tuples of binary forms.

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 corresponding to a given monodromy group G and dessin D. To show this, we have to verify that

(i) f is indeed a Belyĭ map;
(ii) f has monodromy group G;
(iii) The pullback under f of the closed interval $[0, 1]$ is isomorphic (as a dessin) to D.

Even when using the direct method of Section 2, this step is needed, since not all solutions of the corresponding system of equations are even dessins (recall the parasitic solutions from Section 2), let alone dessins with correct monodromy group or pullback.

Point (i) can be computationally expensive, but it can be accomplished using methods of computational algebraic geometry (computing the discriminant locus). Not even this point is 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 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 is included in the monodromy group G by an elementary specialization argument.

So suppose that we are given a finite number of covers, only one of which has the desired monodromy group G. To eliminate a cover in the given list, it suffices to show that specializing this cover gives a set of cycle type in H, considered as a subgroup of S_n, that is not contained in the given monodromy group $G \subseteq S_n$. 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 [46]. This method proceeds by computing the maximal subgroups of S_n 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_n. Working a little bit harder, this allows one to compute the monodromy group of f instead of merely giving a necessary criterion. Indeed, by the theorem of Beckmann [9], one may work modulo a prime $\mathfrak{p}$ of good reduction, which we may take to be any prime of the ring of integers of K that is coprime with the cardinality $\#G$ of the monodromy group.

Second, one can compute the monodromy by using numerical approximation. This has been implemented directly by van Hoeij [137], though one must be very careful to do this with rigorous error bounds. This idea was used by Granboulan [51] in the computation of a cover with Galois group M_{24}, first realized (without explicit equation) by Malle and Matzat [94, III.7.5]. In particular, Schneps [120, §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, and Kröker [6], who lift a Delaunay triangulation numerically and read off the permutations by traversing the sequence of edges counterclockwise around a basepoint. As mentioned less precisely in point (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; the above numerical method allows us to do this.

A third and final method is due to Elkies, 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_n.

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

Question 7.2. *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 input size?*

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 [66] 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 of a number field.

8. Further generalizations

8.1. **Origamis.** One generalization of dessins 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 and Schmithüsen [61]; dessins can be obtained from origamis by a degeneration process [61, §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 that in the case of dessins. 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 and 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 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 at all clear how to achieve this.

Question 8.1. *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 [117], [118]. 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 [117], 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 dessins, and therefore we ask the following question.

Question 8.2. *Which extension of the field of moduli is needed to define similar covers totally ramified above a singular point for general curves?*

8.2. **Specialization.** Hurwitz spaces 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: König [83] computes a family of polynomials with Galois group $\mathrm{PSL}_5(\mathbb{F}_2)$ over $\mathbb{Q}(t)$ with four branch points by reversing this approach: a "degenerate" three-point branched cover is obtained by p-adic methods and then the four-point branched cover is obtained by complex approximation (using Puiseux expansions).

Roberts and Venkatesh [115] use fields of moduli of branched covers with specified branching and monodromy to give significant evidence that in many cases there are infinitely many number fields with symmetric or alternating Galois group that are unramified away from a fixed set of primes. Also, as mentioned in Section 3, Couveignes [27] 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, and this question should be in reach of the techniques of numerical algebraic geometry.

References

[1] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner bases*, 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 denfants with* $\leq$ *4 edges*, `arXiv:0710.2658v1`.

[3] Ane S. I. Anema, Jaap Top, *Explicit algebraic coverings of a pointed torus*, Arithmetic and geometry of K3 surfaces and Calabi-Yau threefolds, Fields Inst. Comm., vol. 67, 2013, 143–152.

[4] E. 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*, Combinatorics (Proc. Sympos. Pure Math., vol. XIX, Univ. California, Los Angeles), Amer. Math. Soc., Providence, 1968, 1–25.

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

[7] A. F. Beardon and K. Stephenson, The uniformization theorem for circle packings, Indiana Univ. Math. J. **39** (1990), no. 4, 1383–1425. MR1087197 (92b:52038)

[8] 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`.

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

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

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

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

[13] F. Beukers and H. Montanus, Explicit calculation of elliptic fibrations of $K3$-surfaces and their Belyi-maps, in *Number theory and polynomials*, 33–51, London Math. Soc. Lecture Note Ser., 352 Cambridge Univ. Press, Cambridge. MR2428514 (2009j:14011)

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

[15] Bryan Birch, *Noncongruence subgroups, covers and drawings*, The Grothendieck theory of dessins d'enfants (Luminy, 1993), London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, 25–46.

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

[17] F. Bouyer and M. Streng, *Examples of CM curves of genus two defined over the reflex field*, `arxiv:1307.0486v1`

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

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

[20] Pete L. Clark and John Voight, *Algebraic curves uniformized by congruence subgroups of triangle groups*, preprint.

[21] C. R. Collins and K. Stephenson, A circle packing algorithm, Comput. Geom. **25** (2003), no. 3, 233–256. MR1975216 (2004c:52035)

[22] M. D. E. Conder et al., Galois actions on regular dessins of small genera, Rev. Mat. Iberoam. **29** (2013), no. 1, 163–181.

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

[24] 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.

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

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

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

[28] Jean-Marc Couveignes and Granboulan, *Dessins from a geometric point of view*, The Grothendieck theory of dessins d'enfants (Luminy, 1993), London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994.

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

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

[31] M. Stoll and J. E. Cremona, On the reduction theory of binary forms, J. Reine Angew. Math. **565** (2003), 79–99. MR2024647 (2005e:11091)

[32] P. Dèbes and J.-C. Douai, Algebraic covers: field of moduli versus field of definition, Ann. Sci. École Norm. Sup. (4) **30** (1997), no. 3, 303–338. MR1443489 (98k:11081)

[33] Debes and Emsalem, *On fields of moduli of curves*, J. Algebra **211** (1999), no. 1, 42–56.

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

[35] 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. MR0695100 (85b:14028)

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

[37] 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.

[38] Noam Elkies, *ABC* implies Mordell, Internat. Math. Res. Notices **1991**, no. 7, 99–109. MR1141316 (93d:11064)

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

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

[41] Noam Elkies, *The complex polynomials* $P(x)$ *with* $\mathrm{Gal}(P(x)-t)=M_{23}$, to appear in ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, Everett Howe and Kiran Kedlaya, eds., Mathematical Science Publishers, 2013.

[42] Noam D. Elkies, *Explicit modular towers*, 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`.

[43] Noam 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`.

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

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

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

[47] R. Fricke and F. 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. MR0183872 (32 #1348)

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

[49] V. D. Goppa, Codes that are associated with divisors, Problemy Peredači Informacii **13** (1977), no. 1, 33–39. MR0497293 (58 #15672)

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

[51] L. Granboulan, *Construction dune extension régulière de $\mathbb{Q}(T)$ de groupe de Galois M_{24}*, Experimental Math. **5** (1996), 3-14.

[52] Alexandre Grothendieck, *Sketch of a programme (translation into English)*, Geometric Galois Actions. 1. Around Grothendieck's Esquisse d'un Programme, eds. Leila Schneps and Pierre Lochak, London Math. Soc. Lect. Note Series, vol. 242, Cambridge University Press, Cambridge, 1997, 243–283.

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

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

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

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

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

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

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

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

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

[62] 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.

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

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

[65] Y. 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). MR0656048 (84c:14016)

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

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

[68] 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.

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

[70] Gareth Jones and David Singerman, *Maps, hypermaps, and triangle groups*, The Grothendieck theory of dessins d'enfants (Luminy, 1993), London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, 115–145.

[71] G. A. Jones and M. Streit, Galois groups, monodromy groups and cartographic groups, in *Geometric Galois actions, 2*, 25–65, London Math. Soc. Lecture Note Ser., 243 Cambridge Univ. Press, Cambridge. MR1653008 (2000d:14028)

[72] G. A. Jones, M. 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.

[73] John W. Jones and David P. Roberts, *Sextic number fields with discriminant* $-^j 2^a 3^b$, Number Theory (Ottawa, 1996), CRM Proc. Lecture Notes, vol. 19, eds. R. Gupta and K. Williams, Amer. Math. Soc., Providence, RI, 1999, 141–172.

[74] John W. Jones and David P. Roberts, *Septic number fields with discriminant* $\pm 2^a 3^b$, Math. Comp. **72** (2003), 1975–1985.

[75] John W. Jones and David P. Roberts, *Number fields ramified at one prime*, Algorithmic Number Theory, Lecture Notes in Comp. Sci., vol. 5011, eds. ?, Springer, Berlin, 2008, 226–239.

[76] G. Julia, *Étude sur les formes binaires non quadratiques à indéterminées réelles ou complexes*, Mémoires de lAcadémie des Sciences de lInstitut de France 55, 1296 (1917).

[77] N. Katz, *Travaux de Laumon*, Séminaire Bourbaki **691** (1987–1988), 105–132.

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

[79] F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, reprint of the 1884 original, Birkhäuser, Basel, 1993. MR1315530 (96g:01046)

[80] Michael Klug, Michael Musty, Sam Schiavone, and John Voight, *Numerical computation of three-point branched covers of the projective line*, preprint.

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

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

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

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

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

[86] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 1*, Springer-Verlag, New York, 2000.

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

[88] Segei 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.

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

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

[91] 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.

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

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

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

[95] 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.

[96] 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.

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

[98] Gunter Malle, *Fields of definition of some three point ramified field extensions*, The Grothendieck theory of dessins d'enfants (Luminy, 1993), London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, 147–168.

[99] 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.

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

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

[102] Donald Marshall, *Numerical conformal mapping software: zipper*, `http://www.math.washington.edu/~marshall/zipper.html`.

[103] Donald E. Marshall and Steen Rohde, *Convergence of a variant of the zipper algorithm for conformal mapping*, SIAM J. Numer. Anal. **45** (2007), no. 6, 2577–2609.

[104] Yu. V. Matiyasevich, *Computer evaluation of generalized Chebyshev polynomials*, Moscow Univ. Math. Bull. **51** (1996), no. 6, 39–40.

[105] B. Heinrich Matzat, *Konstructive Galoistheorie*, Lect. Notes in Math., vol. 1284, Springer, Berlin, 1987.

[106] A. D. Mednykh, *Nonequivalent coverings of Riemann surfaces with a prescribed ramification type*, Siberian Math. J. **25** (1984), 606–625.

[107] B. Mohar, A polynomial time circle packing algorithm, Discrete Math. **117** (1993), no. 1-3, 257–263. MR1226147 (94h:52038)

[108] H. Montanus, Hall triples and dessins d'enfant, Nieuw Arch. Wiskd. (5) **7** (2006), no. 3, 172–176. MR2260081 (2007e:11035)

[109] Andrew Obus, *Ramification of primes in fields of moduli of three-point covers*, Ph.D. thesis, University of Pennsylvania, 2009.

[110] J. Paulhus, *Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups*, to appear in ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, Everett Howe and Kiran Kedlaya, eds., Mathematical Science Publishers, 2013.

[111] Heinz-Otto Peitgen (ed.), *Newton's method and dynamical systems*, Kluwer Academic, Dordrecht, 1989.

[112] Kevin Pilgrim, *Dessins d'enfants and Hubbard trees*, Ann. Sci. École Norm. Sup. (4) **33** (2000), no. 5, 671–693.

[113] David P. Roberts, *Nonsolvable polynomials with field discriminant* 5^A, Int. J. Number Theory **7** (2011), no. 2, 289–322.

[114] David P. Roberts, *An ABC construction of number fields*, Number theory, CRM Proc. Lecture Notes, vol. 36, Amer. Math. Soc., Providence, 2004, 237–267.

[115] David P. Roberts and Akshay Venkatesh, *Hurwitz number fields*, preprint.

[116] M. Romagny and S. Wewers, Hurwitz spaces, in *Groupes de Galois arithmétiques et différentiels*, 313–341, Sémin. Congr., 13 Soc. Math. France, Paris. MR2316356 (2008e:14040)

[117] Simon Rubinstein-Salzedo, *Totally ramified branched covers of elliptic curves*, preprint.

[118] Simon Rubinstein-Salzedo, *Period computations for covers of elliptic curves*, preprint.

[119] William Stein, *SAGE Mathematics Software* (version 4.3), The SAGE Group, 2013, `http://www.sagemath.org/`.

[120] Leila Schneps, *Dessins d'enfants on the Riemann sphere*, The Grothendieck theory of dessins d'enfants, Lecture Notes in Math., vol. 200, Cambridge University Press, 1994, 47–77.

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

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

[123] Björn Selander and Andreas Strömbergsson, *Sextic coverings of genus two which are branched at three points*, preprint.

[124] J.-P. Serre, *Topics in Galois theory*, Research Notes in Mathematics 1, Jones and Bartlett, 1992.

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

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

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

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

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

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

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

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

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

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

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

[136] 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. MR0705893 (85i:11108)

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

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

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

[140] 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`.

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

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

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

[144] John Voight and John Willis, *Computing power series expansions of modular forms*, accepted to "Computations with modular forms".

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

[146] 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.

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

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

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

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

[151] Jürgen Wolfart, *Triangle groups and Jacobians of CM type*, preprint.

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

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

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

[155] L. Zapponi, Fleurs, arbres et cellules: un invariant galoisien pour une famille d'arbres, Compositio Math. **122** (2000), no. 2, 113–133. MR1775414 (2001g:14050)

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

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

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 address: `jvoight@gmail.com`