2-GROUP BELYI MAPS

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Doctor of Philosophy

in

Mathematics

by

Michael James Musty

DARTMOUTH COLLEGE

Hanover, New Hampshire

March 7, 2019

Examining Committee:

John Voight, Chair

Thomas Shemanske

David Roberts

Carl Pomerance

F. Jon Kull, Ph.D.
Dean of Graduate and Advanced Studies

Abstract

Write your abstract here.

Preface

Preface and Acknowledgments go here!

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Section 1.1

Belyi maps from a historical perspective

In [2], G.V. Belyi proved that a Riemann surface X can be defined over a number field (when viewed as an algebraic curve over $\mathbb{C}$) if and only if there exists a non-constant meromorphic function $\phi : X \to \mathbb{P}^1_{\mathbb{C}}$ unramified outside the set $\{0, 1, \infty\}$. This result came to be known as Belyi's Theorem and the maps ϕ came to be known as Belyi maps (or Belyi functions). Although Belyi's Theorem has an elementary proof, it was a starting point for a great deal of modern research in the area. This work was largely spurred on by Grothendieck's *Esquisse d'un programme* [3] where he was impressed enough to write

> *jamais sans doute un résultat profond et déroutant ne fut démontré en si peu de lignes!*
>
> never, without a doubt, was such a deep and disconcerting result proved in so few lines!

An intriguing aspect of the theory of Belyi maps that arose from Grothendieck's work in the 1980s is the reformulation of these objects in a purely topological way. The preimage $\phi^{-1}([0,1])$ is a graph embedded on X, and Grothendieck developed axioms for embedded graphs in such a way that they coincided exactly with the category of Belyi maps. He called these graphs *dessins d'enfants* or children's drawings.

Even as a standalone theorem, Belyi's Theorem is a remarkable result in the mysterious way that it allows us to distinguish between algebraic and transcendental objects. However, the main interest in Belyi maps arises from Galois theory. The absolute Galois group of $\mathbb{Q}$ acts on the set of Belyi maps via the defining equations. The induced action on the set of dessins

1.1.1. Inverse Galois theory, Hurwitz families, and fields with few ramified primes

Inverse Galois theory.

Hurwitz families.

1.1.2. Grothendieck's theory of dessins d'enfants

Chapter 2

Background

Section 2.1

Belyi maps

2.1.1. Algebraic curves and their function fields

2.1.2. Riemann's existence theorem and covers of $\mathbb{P}^1$

2.1.3. Belyi's theorem

Proposition 2.1.1. MM: [Galois action on Belyi maps]

2.1.4. Belyi maps and G-Belyi maps

Definition 2.1.2. The geometry type of a Belyi map MM: [todo]

(degenerate)

(spherical)

(Euclidean)

(hyperbolic)

Proposition 2.1.3. *Galois correspondence of Belyi maps*

Proof. □

2.1.5. Permutation triples and passports

Definition 2.1.4. MM: [passports and such]

We begin by explaining the combinatorial (or topological) description of Belyi maps and exhibit an efficient method for their enumeration. For general background reading, see [5, §1] and the references therein. Throughout, let $K \subseteq \mathbb{C}$ be a field. A (nice) curve over K is a smooth, projective, geometrically connected (irreducible) scheme of finite type over K that is pure of dimension 1. After extension to $\mathbb{C}$, a curve may be thought of as a compact, connected Riemann surface. A Belyi map over K is a finite morphism $\phi\colon X \to \mathbb{P}^1$ over K that is unramified outside $\{0, 1, \infty\}$; we will sometimes write (X, ϕ) when we want to pay special attention to the source curve X. Two Belyi maps ϕ, ϕ' are isomorphic if there is an isomorphism $\iota\colon X \xrightarrow{\sim} X'$ of curves such that $\phi'\iota = \phi$. Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map over $\overline{\mathbb{Q}}$ of degree $d \in \mathbb{Z}_{\geq 1}$. The monodromy group of ϕ is the Galois group $\mathrm{Mon}(\phi) := \mathrm{Gal}(\mathbb{C}(X) \,|\, \mathbb{C}(\mathbb{P}^1)) \leq S_d$ of the corresponding extension of function fields (understood as the action of the automorphism group of the normal closure); the group $\mathrm{Mon}(\phi)$ may also be obtained by lifting paths around $0, 1, \infty$ to X. A permutation triple of degree $d \in \mathbb{Z}_{\geq 1}$ is a tuple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ such that $\sigma_\infty\sigma_1\sigma_0 = 1$. A permutation triple is transitive if the subgroup $\langle\sigma\rangle \leq S_d$ generated by σ is transitive. We say that two permutation triples

σ, σ' are simultaneously conjugate if there exists $\tau \in S_d$ such that

$$\sigma^\tau := (\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau, \tau^{-1}\sigma_\infty\tau) = (\sigma'_0, \sigma'_1, \sigma'_\infty) = \sigma'. \tag{2.1.1}$$

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

Lemma 2.1.5. *The set of transitive permutation triples of degree d up to simultaneous conjugation is in bijection with the set of Belyi maps of degree d up to isomorphism.*

Proof. The correspondence is via monodromy [4, Lemma 1.1]; in particular, the monodromy group of a Belyi map is (conjugate in S_d to) the group generated by σ. □

The group $\mathrm{Gal}(\overline{\mathbb{Q}}\,|\,\mathbb{Q})$ acts on Belyi maps by acting on the coefficients of a set of defining equations; under the bijection of Lemma 2.1.5, it thereby acts on the set of transitive permutation triples, but this action is rather mysterious. We can cut this action down to size by identifying some basic invariants, as follows. A passport consists of the data $\mathcal{P} = (g, G, \lambda)$ where $g \geq 0$ is an integer, $G \leq S_d$ is a transitive subgroup, and $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ is a tuple of partitions λ_s of d for $s = 0, 1, \infty$. These partitions will be also be thought of as a tuple of conjugacy classes $C = (C_0, C_1, C_\infty)$ by cycle type, so we will also write passports as (g, G, C). The passport of a Belyi map $\phi\colon X \to \mathbb{P}^1$ is $(g(X), \mathrm{Mon}(\phi), (\lambda_0, \lambda_1, \lambda_\infty))$, where $g(X)$ is the genus of X and λ_s is the partition of d obtained by the ramification degrees above $s = 0, 1, \infty$, respectively. Accordingly, the passport of a transitive permutation triple σ is $(g(\sigma), \langle\sigma\rangle, \lambda(\sigma))$, where (by Riemann–Hurwitz)

$$g(\sigma) := 1 - d + (e(\sigma_0) + e(\sigma_1) + e(\sigma_\infty))/2 \tag{2.1.2}$$

and e is the index of a permutation (d minus the number of orbits), and $\lambda(\sigma)$ is the cycle type of σ_s for $s = 0, 1, \infty$. The size of a passport $\mathcal{P}$ is the number of simultaneous conjugacy classes (as in 2.1.1) of (necessarily transitive) permutation triples σ with passport $\mathcal{P}$. The action of $\mathrm{Gal}(\overline{\mathbb{Q}} \,|\, \mathbb{Q})$ on Belyi maps preserves passports. Therefore, after computing equations for all Belyi maps with a given passport, we can try to identify the Galois orbits of this action. We say a passport is irreducible if it has one $\mathrm{Gal}(\overline{\mathbb{Q}} \,|\, \mathbb{Q})$-orbit and reducible otherwise.

Section 2.2

Group theory

2.2.1. Central group extensions and $H^2(G, A)$

Definition 2.2.1.

2.2.2. Holt's algorithm and `Magma` implementation

2.2.3. Results on 2-groups

Lemma 2.2.2. MM: [todo]

Section 2.3

Jacobians of curves

2.3.1. Abel-Jacobi and the construction over $\mathbb{C}$

2.3.2. Algebraic construction

2.3.3. Riemann-Roch

2.3.4. Torsion points and torsion fields

Section 2.4

Galois representations

2.4.1. Representations of Galois groups of number fields

2.4.2. Representations coming from geometry

Chapter 3

A database of 2-group Belyi maps

In this chapter we describe an algorithm to generate 2-group Belyi maps of a given degree. We begin by defining this particular family of Belyi maps in Section 3.1. The algorithm is inductive in the degree. The base case in degree 1 is discussed in Section 3.2. We then move on to describe the inductive step of the algorithm which we describe in two parts. First we discuss the algorithm to enumerate the isomorphism classes using permutation triples in Section 3.3. For a discussion on the relationship between permutation triples and Belyi maps see Section 2.1. Next we discuss the inductive step to produce Belyi curves and maps in Section 3.4. In Section 3.5 we give a detailed description of the running time of the algorithm. Lastly, in Section 3.6, we discuss the implementation and computations that we have carried out explicitly.

Section 3.1

2-group Belyi maps

Recall the definition of a Belyi map in Section 2.1. In this section we define a narrow our focus to a more specific family of Belyi maps which we now describe.

Definition 3.1.1. A degree d Belyi map ϕ with monodromy group G is said to be Galois if $\#G = d$.

Definition 3.1.2. A 2-group Belyi map is a Galois Belyi map with monodromy group a 2-group.

MM: [some exposition]

Section 3.2

Degree 1 Belyi maps

Section 3.3

An algorithm to enumerate isomorphism classes of 2-group Belyi maps

The algorithm we describe here is iterative. The degree 1 case is discussed in Section 3.2. We now set up some notation for the iteration.

Notation 3.3.1. First we suppose that we are given σ a permutation triple corresponding to a 2-group Belyi map $\phi : X \to \mathbb{P}^1$.

Definition 3.3.2. We say that a permutation triple $\widetilde{\sigma}$ is a degree 2 lift (or simply a lift) of a permutation triple σ if there exists a short exact sequence of groups as in Figure 3.3.1 with $\iota(\mathbb{Z}/2\mathbb{Z})$ contained in the center of $\langle\widetilde{\sigma}\rangle$.

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\iota} \langle\widetilde{\sigma}\rangle \xrightarrow{\pi} \langle\sigma\rangle \longrightarrow 1$$

Figure 3.3.1: $\widetilde{\sigma}$ a lift of σ

In Algorithm 3.3.5 below we describe how to determine all lifts $\widetilde{\sigma}$ (up to isomorphism) of a given permutation triple σ.

Lemma 3.3.3. *Let σ be a permutation triple corresponding to a 2-group Belyi map $\phi : X \to \mathbb{P}^1$ and $\widetilde{\sigma}$ a lift of σ corresponding to a 2-group Belyi map $\widetilde{\phi} : \widetilde{X} \to \mathbb{P}^1$. Then there exists a permutation triple $\widetilde{\sigma}'$ that is simultaneously conjugate to $\widetilde{\sigma}$ with $\iota(\langle\widetilde{\sigma}'\rangle)$ contained in the center of $\langle\sigma\rangle$.*

Proof. □

Remark 3.3.4. In light of Lemma 3.3.3, we can restrict our attention to central extensions of $\langle\sigma\rangle$ in Definition 3.3.2.

Algorithm 3.3.5. Let the notation be as described above in 3.3.1.

Input: $\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ a permutation triple corresponding to a 2-group Belyi map

Output: all lifts $\widetilde{\sigma}$ of σ up to simultaneous conjugation in S_{2d} sorted by passport

1. Let $G = \langle\sigma\rangle$ and compute all central extensions $\widetilde{G}$ sitting in the exact sequence in Figure 3.3.2 up to isomorphism (see Definition 2.2.1). For more information about the algorithms to do this see Section 2.2.2.

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\iota} \widetilde{G} \xrightarrow{\pi} G \longrightarrow 1$$

Figure 3.3.2: $\widetilde{G}$ a (central) extension of G

2. For each extension $\widetilde{G}$ as in Figure 3.3.2 from the previous step we perform the following:

(a) Consider the set of triples

$$\{\widetilde{\sigma} := (\widetilde{\sigma}_0, \widetilde{\sigma}_1, \widetilde{\sigma}_\infty) : \widetilde{\sigma}_s \in \pi^{-1}(\sigma_s) \text{ for } s \in \{0, 1, \infty\}\} \tag{3.3.1}$$

and let $\text{Lifts}(\sigma)$ denote the set of such $\widetilde{\sigma}$ with the property that $\widetilde{\sigma}_\infty\widetilde{\sigma}_1\widetilde{\sigma}_0 = 1$ and $\langle\widetilde{\sigma}\rangle = \widetilde{G}$.

(b) For each $\widetilde{\sigma} \in \text{Lifts}(\sigma)$ compute $\text{order}(\widetilde{\sigma}) := (\text{order}(\widetilde{\sigma}_0), \text{order}(\widetilde{\sigma}_1), \text{order}(\widetilde{\sigma}_\infty)) \in \mathbb{Z}^3$ and sort $\text{Lifts}(\sigma)$ according to $\text{order}(\widetilde{\sigma})$. Let

$$\text{Lifts}(\sigma, (a, b, c)) := \{\widetilde{\sigma} \in \text{Lifts}(\sigma) : \text{order}(\widetilde{\sigma}) = (a, b, c)\}. \tag{3.3.2}$$

(c) For each set of triples $\text{Lifts}(\sigma, (a, b, c))$ remove simultaneously conjugate triples so that $\text{Lifts}(\sigma, (a, b, c))$ has exactly one representative from each simultaneous conjugacy class. MM: [TODO: reword]

3. Return the union of the sets $\text{Lifts}(\sigma, (a, b, c))$ ranging over all extensions as in Figure 3.3.2 and for each extension ranging over all orders (a, b, c).

Proof of correctness. The algorithms in Step 1 are addressed in Section 2.2.2. Let $\phi : X \to \mathbb{P}^1$ be the 2-group Belyi map corresponding to σ. By Proposition 2.1.3, the groups obtained from Step 1 are precisely the groups that can occur as monodromy groups of degree 2 covers of X. MM: [lemma in section about extensions (or in background about Belyi maps) to prove that two isomorphic extensions cannot produce nonisomorphic Belyi maps and that two nonisomorphic extensions cannot produce isomorphic Belyi maps] In Step 2 we restrict our attention to a single extension of G as in Figure 3.3.2. When we pullback a triple σ under the map π, there are $2^3 = 8$

preimages $\widetilde{\sigma}$. Of these 8 preimages, exactly 4 have the property that $\widetilde{\sigma}_\infty\widetilde{\sigma}_1\widetilde{\sigma}_0 = 1$. Of these 4 triples, we only take those that generate $\widetilde{G}$ and this makes up the set Lifts(σ). In Step 2(b), we are sorting Lifts(σ) by passport. Since 2-group Belyi maps are Galois, the cycle structure of each $\widetilde{\sigma}_s \in \widetilde{\sigma}$ is determined by the order of $\widetilde{\sigma}_s$ so that sorting by order is the same as sorting by cycle structure.

Remark 3.3.6. In fact, even though we do not need this for the algorithm, there are at most 2 different passports that can occur in Lifts(σ). 2 different passports occur when one of $\sigma_s \in \sigma$ is the identity. If σ does not contain an identity element, then all triples in Lifts(σ) have the same passport.

At this point, we have constructed the sets Lifts($\sigma, (a, b, c)$). In light of Remark 3.3.6, there are only 2 possibilities:

- There is only one such set Lifts($\sigma, (a, b, c)$) consisting of at most 4 triples.
- There are 2 sets Lifts($\sigma, (a, b, c)$) and Lifts($\sigma, (a', b', c')$) each consisting of at most 2 triples.

Step 2(c) is to eliminate simultaneous conjugation in each set Lifts($\sigma, (a, b, c)$). After Step 2(c) is complete, the sets Lifts($\sigma, (a, b, c)$) contain exactly one permutation triple for each isomorphism class of 2-group Belyi map with passport determined by (a, b, c) and monodromy group $\widetilde{G}$ such that the diagram in Figure 3.3.3 commutes. In Step 3 we collect together all sets Lifts($\sigma, (a, b, c)$) as we range over all possible extensions in Step 1, and by the discussion for Step 2 yields the desired output. □

We now illustrate Algorithm 3.3.5 with the following example.

Example 3.3.7. In this example we carry out Algorithm 3.3.5 for the degree 2 permutation triple $\sigma = ((1\,2), (1)(2), (1\,2))$. Here $G = \langle\sigma\rangle \cong \mathbb{Z}/2\mathbb{Z}$. In Step 1, we obtain

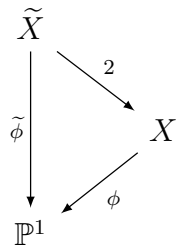

Figure 3.3.3: The permutation triples $\widetilde{\sigma}$ constructed in Algorithm 3.3.5 correspond to Belyi maps $\widetilde{\phi} : \widetilde{X} \to \mathbb{P}^1$ in the above diagram.

two group extensions $\widetilde{G}_1 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\widetilde{G}_2 \cong \mathbb{Z}/4\mathbb{Z}$: We will consider the two

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\iota_1} \widetilde{G}_1 \xrightarrow{\pi_1} G \longrightarrow 1$$

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\iota_2} \widetilde{G}_2 \xrightarrow{\pi_2} G \longrightarrow 1$$

Figure 3.3.4: Two extensions of G in Example 3.3.7

extensions separately:

- For $\widetilde{G}_1$, we have

$$\begin{aligned}\text{Lifts}(\sigma) = \Big\{&((1\,2)(3\,4), (1)(2)(3)(4), (1\,2)(3\,4)), ((1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)),\\ &((1\,4)(2\,3), (1)(2)(3)(4), (1\,4)(2\,3)), ((1\,4)(2\,3), (1\,3)(2\,4), (1\,2)(3\,4))\Big\}\end{aligned}$$

  Before we continue with the algorithm, let us take a moment to explain this more closely in the following remark.

  Remark 3.3.8. First, note that the image of ι_1 is an order 2 subgroup of $\widetilde{G}_1$. Let $\tau \in \widetilde{G}_1$ denote the generator of this image. From the perspective of branched covers, τ is identifying 4 sheets in a degree 4 cover down to 2 sheets in a degree 2 cover. Elements $\widetilde{\sigma}$ of $\text{Lifts}(\sigma)$ must induce a well-defined action on the identified

sheets and this action must be compatible with σ. In this example $\tau = (1\,3)(2\,4)$ meaning that τ identifies the sheets labeled 1 and 3 into a single sheet and τ identifies the sheets labeled 2 and 4 into a single sheet. Another way of saying that $\widetilde{\sigma}$ induces a well-defined action is that $\widetilde{\sigma}$ acts on the blocks $\Big\{\boxed{1\,3}, \boxed{2\,4}\Big\}$. Saying that this action is compatible with σ means that for each $s \in \{0, 1, \infty\}$ the induced action of $\widetilde{\sigma}_s$ on blocks is the same as σ_s. For

$$\widetilde{\sigma} = ((1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,4))$$

we have $\widetilde{\sigma}_0\boxed{1\,3} = \boxed{2\,4}$ and $\widetilde{\sigma}_0\boxed{2\,4} = \boxed{1\,3}$ so that the induced permutation of blocks is

$$\Big(\boxed{1\,3}, \boxed{2\,4}\Big)$$

which is the same as the permutation $\sigma_0 = (1\,2)$ (as long as we identity $\boxed{1\,3}$ with 1 and $\boxed{2\,4}$ with 2).

To finish Step 2(a) we only take triples in Lifts(σ) that generate $\widetilde{G}_1$, so at the end of Step 2(a) for this extension we have

$$\text{Lifts}(\sigma) = \Big\{((1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)), ((1\,4)(2\,3), (1\,3)(2\,4), (1\,2)(3\,4))\Big\}.$$

In Step 2(b) we sort Lifts(σ) into passports as determined by orders of elements. Here, all $\widetilde{\sigma} \in$ Lifts(σ) have the same orders (and hence belong to the same passport). Thus we get a single set Lifts($\sigma, (2, 2, 2)$) = Lifts(σ). Lastly, in Step 2(c) we see that that the two triples in Lifts($\sigma, (2, 2, 2)$) are simultaneously conjugate (by the permutation $(2\,4)$) and hence we remove one of the triples

from $\mathrm{Lifts}(\sigma, (2,2,2))$.

- For $\widetilde{G}_2$, we have

$$\mathrm{Lifts}(\sigma) = \Big\{((1\,4\,3\,2),(1)(2)(3)(4),(1\,2\,3\,4)),((1\,2\,3\,4),(1\,3)(2\,4),(1\,2\,3\,4)),$$
$$((1\,2\,3\,4),(1)(2)(3)(4),(1\,4\,3\,2)),((1\,4\,3\,2),(1\,3)(2\,4),(1\,4\,3\,2))\Big\}$$

  All 4 of the above triples in $\mathrm{Lifts}(\sigma)$ generate $\widetilde{G}_2$, so we continue to Step 2(b) with $\#\,\mathrm{Lifts}(\sigma) = 4$. In Step 2(b), we sort $\mathrm{Lifts}(\sigma)$ into two sets $\mathrm{Lifts}(\sigma, (4,1,4))$ and $\mathrm{Lifts}(\sigma, (4,2,4))$ each containing 2 triples. In Step 2(c), we find that the 2 triples in $\mathrm{Lifts}(\sigma, (4,1,4))$ are simultaneously conjugate (by the permutation $(2\,4)$) and the 2 triples in $\mathrm{Lifts}(\sigma, (4,2,4))$ are simultaneously conjugate (also by the permutation $(2\,4)$), so we remove one permutation triple from each of these sets so that $\mathrm{Lifts}(\sigma, (4,1,4))$ and $\mathrm{Lifts}(\sigma, (4,2,4))$ both have cardinality 1.

In Step 3, we return

$$\mathrm{Lifts}(\sigma, (2,2,2)) \cup \mathrm{Lifts}(\sigma, (4,1,4)) \cup \mathrm{Lifts}(\sigma, (4,2,4))$$

which is a set of 3 permutation triples each corresponding to an isomorphism class of 2-group Belyi map as in Figure 3.3.3.

Now that we have an algorithm to find all lifts of a single permutation triple, the next step is to describe how to use this to organize all isomorpism classes of 2-group Belyi maps of a given degree.

Algorithm 3.3.9. Let the notation be as described above in 3.3.1.

Input: $d = 2^m$ for some positive integer m

Output: a sequence of bipartite graphs $\mathscr{G}_2, \mathscr{G}_4, \ldots, \mathscr{G}_{2^m}$ where the two sets of nodes of $\mathscr{G}_{2^i}$ are

- $\mathscr{G}_{2^i}^{\text{above}}$: the set of isomorphism classes of 2-group Belyi maps of degree 2^i indexed by permutation triples $\widetilde{\sigma}$
- $\mathscr{G}_{2^i}^{\text{below}}$: the set of isomorphism classes of 2-group Belyi maps of degree 2^{i-1} indexed by permutation triples σ

and there is an edge between $\widetilde{\sigma}$ and σ if and only if $\widetilde{\sigma}$ is a lift (as in Definition 3.3.2) of σ. This algorithm is iterative. For each $i = 1, \ldots, m$, we use $\mathscr{G}_{2^i}^{\text{below}}$ to compute $\mathscr{G}_{2^i}^{\text{above}}$ and then we define

$$\mathscr{G}_{2^{i+1}}^{\text{below}} := \mathscr{G}_{2^i}^{\text{above}}$$

and continue the process.

1. To begin the iteration we let $\mathscr{G}_2^{\text{below}} = \{\sigma\}$ where $\sigma = ((1),(1),(1)) \in S_1^3$ corresponds to the degree 1 Belyi map.
2. Now suppose we have computed $\mathscr{G}_{2^i}^{\text{below}}$. We compute $\mathscr{G}_{2^i}^{\text{above}}$ as follows:
   (a) Apply Algorithm 3.3.5 to every $\sigma \in \mathscr{G}_{2^i}^{\text{below}}$ to obtain $\#\mathscr{G}_{2^i}^{\text{below}}$ sets Lifts(σ). As a word of caution, the notation Lifts(σ) has a different meaning here than in Algorithm 3.3.5. Here Lifts(σ) is the set of lifts of σ up to simultaneous conjugation. Let

$$\mathscr{G}_{2^i}^{\text{above}} := \bigcup_{\sigma \in \mathscr{G}_{2^i}^{\text{below}}} \text{Lifts}(\sigma)$$

and place an edge of $\mathscr{G}_{2^i}$ between $\widetilde{\sigma} \in \mathscr{G}_{2^i}^{\text{above}}$ and $\sigma \in \mathscr{G}_{2^i}^{\text{below}}$ if and only if $\widetilde{\sigma} \in \text{Lifts}(\sigma)$.

(b) Consider all pairs $(\widetilde{\sigma}, \widetilde{\sigma}') \in \mathscr{G}_{2^i}^{\text{above}}$ and for each pair test if $\widetilde{\sigma}$ is simultaneously conjugate to $\widetilde{\sigma}'$ in S_{2^i}. If the pair is simultaneously conjugate, then combine the nodes $\widetilde{\sigma}$ and $\widetilde{\sigma}'$ into a single node (take either triple) and combine the edge sets of $\widetilde{\sigma}$ and $\widetilde{\sigma}'$ to be the edge set of the new node.

(c) Return the resulting bipartite graph as $\mathscr{G}_{2^i}$.

(d) If $i < m$, then let $\mathscr{G}_{2^{i+1}}^{\text{below}} := \mathscr{G}_{2^i}^{\text{above}}$ and repeat Step 2 with $i+1$. If $i = m$, then return the sequence of bipartite graphs $\mathscr{G}_2, \mathscr{G}_4, \ldots, \mathscr{G}_{2^m}$.

Proof of correctness. We first address the claim that every 2-group Belyi map $\phi : X \to \mathbb{P}^1$ of degree 2^i is represented by a permutation triple in $\mathcal{G}_{2^i}^{\text{above}}$. Let G be the monodromy group of ϕ. Since $\#G = 2^i$, by Lemma 2.2.2, there exists a normal tower of groups

$$G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_i \tag{3.3.3}$$

where $G_0 = \{1\}$, $G_i = G$, and each consecutive quotient is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. By the Galois correspondence, Proposition 2.1.3, this normal tower of groups corresponds to the diagram in Figure 3.3.5. Let σ_j be the permutation triple corresponding to ϕ_j in Figure 3.3.5. Applying Algorithm 3.3.5 to σ_j we obtain σ_{j+1} as a lift of σ_j so that the permutation triple corresponding to ϕ appears in $\mathscr{G}_{2^i}^{\text{above}}$. This shows that every 2-group Belyi map of degree 2^i is represented by at least one node in $\mathscr{G}_{2^i}$. We now claim that every 2-group Belyi map of degree 2^i is represented by exactly one node in $\mathscr{G}_{2^i}$. Since we are applying Algorithm 3.3.5 to every permutation triple in $\mathscr{G}_{2^i}^{\text{below}}$, it is possible that in Step 2(a), the set of permutation triples in $\mathscr{G}_{2^i}^{\text{above}}$ has

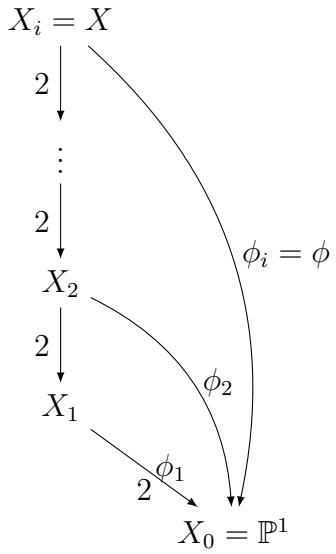

Figure 3.3.5: A 2-group Belyi map ϕ as a sequence of degree 2 covers. For $j \in \{1, \ldots, i\}$, ϕ factors through a degree 2^j Belyi map denoted ϕ_j.

simultaneously conjugate triples which arise when a degree 2^i Belyi map is a degree 2 cover of more than one nonisomorphic Belyi map of degree 2^{i-1}. In Step 2(b), we combine permutation triples in $\mathscr{G}_{2^i}^{\text{above}}$ that are simultaneously conjugate by taking a single permutation triple to represent this isomorphism class of 2-group Belyi map. Note that in Step 2(b) we never remove any edges in the graph $\mathscr{G}_{2^i}$. It follows from Step 2(b) that $\mathscr{G}_{2^i}^{\text{above}}$ has at most one node for each 2-group Belyi map isomorphism class of degree 2^i. □

Theorem 3.3.10. *The following table lists the number of isomorphism classes of 2-group Belyi maps of degree d for d up to 256.*

d	2	4	8	16	32	64	128	256
#								

Proof. Apply Algorithm 3.3.9. □

Algorithm 3.3.11. We use Algorithm 3.3.9 to count the number of Passports of 2-group Belyi maps of a given degree. MM: [todo]

Theorem 3.3.12. *The following table lists the number of passports of 2-group Belyi maps of degree d for d up to 256.*

d	2	4	8	16	32	64	128	256
# *passports*	3	7	16	41	96	267	834	2893

Proof. Apply Algorithm 3.3.11. □

Section 3.4

An algorithm to compute 2-group Belyi curves and maps

The algorithm we describe here is iterative. The degree 1 case is discussed in Section 3.2. We now set up some notation for the iteration.

Notation 3.4.1. First we suppose we are given the following data:

- $X \subset \mathbb{P}^n_K$ defined over a number field K with coordinates $x_0, \ldots, x_n$ cut out by the equations $\{h_i = 0\}_i$ with $h_i \in K[x_0, \ldots, x_n]$
- $\phi : X \to \mathbb{P}^1$ a 2-group Belyi map of degree $d = 2^n$ given by $\phi([x_0 : \cdots : x_n]) = [x_0 : x_1]$ with monodromy group $G = \langle \sigma \rangle$ (necessarily a 2-group) with σ a permutation triple corresponding to ϕ

- For $s \in \{0, 1, \infty\}$ and τ a cycle of $\sigma_s \in \sigma$, denote the ramification point above s corresponding to τ by $Q_{s,\tau}$
- $Y \subset \mathbb{A}^n_K$ the affine patch of X with $x_0 \neq 0$ with coordinates $(y_1, \ldots, y_n)$ where $y_i = x_i/x_0$ cut out by the equations $\{g_i = 0\}_i$ with $g_i \in K[y_1, \ldots, y_n]$ so that $\phi : Y \to \mathbb{A}^1$ is given by $\phi(y_1, \ldots, y_n) = y_1$
- $\widetilde{\sigma}$ as in the output of Algorithm 3.3.5 applied to the input σ

Algorithm 3.4.3 below describes how to lift the degree d Belyi map ϕ to a degree $2d$ Belyi map $\widetilde{\phi}$ with ramification prescribed by $\widetilde{\sigma}$ (also see Figure 3.4).

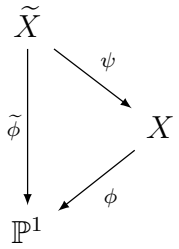

Figure 3.4.1: Algorithm 3.4.3 describes how to construct $\widetilde{\phi}$ corresponding to a permutation triple $\widetilde{\sigma}$ from a given 2-group Belyi map ϕ.

Lemma 3.4.2. *Let D be a degree 0 divisor on X. Then* $\dim \mathscr{L}(D) \leq 1$.

Proof. Suppose $\deg D = 0$, and Let $f, g \in \mathscr{L}(D) \setminus \{0\}$. Write $D = D_0 - D_\infty$ with $D_0, D_\infty \geq 0$. Since $f, g \in \mathscr{L}(D)$, we have $\operatorname{div} f, \operatorname{div} g \geq D_0 - D_\infty$. In particular, $f/g \in K^\times$. □

Algorithm 3.4.3. Let the notation be as described above in 3.4.1.

Input: A 2-group Belyi map $\phi : X \to \mathbb{P}^1_K$ and a permutation triple $\widetilde{\sigma}$

Output: A model (over $\mathbb{Q}^{\mathrm{al}}$) for the Belyi map $\widetilde{\phi} : \widetilde{X} \to \mathbb{P}^1_K$ with monodromy $\widetilde{\sigma}$

1. Let R be the empty set of points on X. For each $s \in \{0, 1, \infty\}$, If the order of σ_s is strictly less than the order of $\widetilde{\sigma}_s$, then append the ramification points $\{Q_{s,\tau}\}_{\tau \in \sigma_s}$ (the ramification points on X above s corresponding to the cycles of σ_s) to R.

2. Let $D = \sum_P n_P P$ be a degree 0 divisor on X with n_P odd for every $P \in R$ and $n_P = 0$ for $P \notin R$. MM: [class group and base field]

3. Compute $f \in \overline{K}(X)^\times$ corresponding to a generator of the Riemann-Roch space $\mathscr{L}(D)$.

4. Write $f = a/b$ with $a, b \in \overline{K}[y_1, \ldots, y_n]$ and construct the ideal

$$\widetilde{I} := \langle g_1, \ldots, g_k, by_{n+1}^2 - a \rangle$$

   in $\overline{K}[y_1, \ldots, y_n, y_{n+1}]$.

5. Saturate $\widetilde{I}$ at $\langle b \rangle$ and denote this ideal by $\mathrm{sat}(\widetilde{I})$.

6. Let $\widetilde{X}$ be the curve corresponding to $\mathrm{sat}(\widetilde{I})$ and $\widetilde{\phi}$ the map $(y_1, \ldots, y_{n+1}) \mapsto y_1$.

Proof of correctness. By Algorithm 3.3.5, there exists a 2-group Belyi map $\widetilde{\phi} : \widetilde{X} \to \mathbb{P}^1$ with ramification according to $\widetilde{\sigma}$. Since $\widetilde{\phi}$ is Galois, the ramification behavior above each $s \in \{0, 1, \infty\}$ is constant (i.e. for a fixed s, all $Q_{s,\tau}$ are either unramified or ramified to order 2). This ensures that the set R constructed in Step 1 is precisely the set of ramification values of ψ (in Figure 3.4). Now that we have the ramification values, we can construct the new Belyi map and curve. We do this by extracting a square root in the function field. More precisely, again by Algorithm 3.3.5, there

exists $\widetilde{X}$ with $\overline{K}(\widetilde{X}) = \overline{K}(X, \sqrt{f})$ where $f \in \overline{K}(X)^\times / \overline{K}(X)^{\times 2}$ and

$$\operatorname{div} f = \sum_{Q_{s,\tau} \in R} Q_{s,\tau} + 2D_\epsilon \in \frac{\operatorname{Div}^0(X)}{2\operatorname{Div}^0(X)} \tag{3.4.1}$$

□

Example 3.4.4.

Section 3.5

Running time analysis

Section 3.6

Explicit computations

Chapter 4

Classifying 2-group Belyi maps

In this chapter we discuss some results on 2-group Belyi maps obtained, in part, from the data in Chapter 3. The conditions that need to be satisfied for a general Belyi map to be a 2-group Belyi map are quite stringent. This allows us to give a clear picture of the story in the low genus cases.

Section 4.1

Genus 0

Section 4.2

Genus 1

Section 4.3

Genus 2

Section 4.4

Genus 3

Section 4.5

Hyperelliptic

Chapter 5

Fields of definition of 2-group Belyi maps

Using data from Chapter 3, we formulate a conjecture about the possible fields of definition of 2-group Belyi maps.

Section 5.1

Fields of moduli

Recall the action of $G_{\mathbb{Q}}$ on the set of Belyi maps described in Proposition 2.1.1. For a fixed Belyi map, we can simplify matters as described in the following definition.

Definition 5.1.1. The field of moduli of a Belyi map $\phi : X \to \mathbb{P}^1$ is the fixed field

$$\{\tau \in G_{\mathbb{Q}} : \phi^\tau \cong \phi\}.$$

Definition 5.1.1 allows us to study a more manageable finite extension. Moreover, passports (recall Definition 2.1.4) allow us to bound the degree of the field of moduli.

Theorem 5.1.2. *Let $\phi : X \to \mathbb{P}^1$ be a Belyi map with passport $\mathcal{P}$. Then the degree of the field of moduli of ϕ is bounded by the size of $\mathcal{P}$.*

Proof. □

Section 5.2

Refined passports

Definition 5.2.1. A refined passport $\mathcal{P}$ consists of the data (g, G, C) where $g \geq 0$ is an integer, $G \leq S_d$ is a transitive subgroup, and $C = (C_0, C_1, C_\infty)$ is a triple of conjugacy classes of G.

MM: [some exposition about refined passports] For a refined passport $\mathcal{P}$ consider the set

$$\Sigma_{\mathcal{P}} = \{(\sigma_0, \sigma_1, \sigma_\infty) \in C_0 \times C_1 \times C_\infty : \sigma_\infty \sigma_1 \sigma_0 = 1, \text{ and } \langle \sigma \rangle = G\}/\sim$$

where $(\sigma_0, \sigma_1, \sigma_\infty) \sim (\sigma_0', \sigma_1', \sigma_\infty')$ if and only if there exists $\alpha \in \mathrm{Aut}(G)$ with $\alpha(\sigma_s) = \sigma_s'$ for $s \in \{0, 1, \infty\}$.

Section 5.3

A refined conjecture

Conjecture 5.3.1. *Let $\mathcal{P} = (g, G, C)$ be a refined passport with $G = \mathrm{Mon}(\phi)$ for some 2-group Belyi map ϕ. Then $\#\Sigma_{\mathcal{P}} = 0$ or 1.*

Proof. □

Corollary 5.3.2. *Every 2-group Belyi map is defined over a cyclotomic field* $\mathbb{Q}(\zeta_{2^m})$ *for some* m.

Proof. □

Chapter 6

Gross's conjecture for $p = 2$

We begin this chapter with Theorem 6.1.1 which provides the arithmetic motivation to study 2-group Belyi maps. We then detail past results on Gross's conjecture in Section 6.2 and finish with some discussion on 2-group Belyi maps in relation to the $p = 2$ case of Gross's conjecture.

Section 6.1

Beckmann's theorem

In this Section we state Beckmann's theorem for Belyi maps over $\mathbb{C}$ from 1989 which can be found in [1]. We then adapt Theorem 6.1.1 to our particular situation in Corollary 6.1.2.

Theorem 6.1.1. *Let $\phi : X \to \mathbb{P}^1$ be a Belyi map with monodromy group G and suppose p does not divide $\#G$. Then there exists a number field M with the following properties:*

- *p is unramified in M*

- *the Belyi map ϕ is defined over M*
- *the Belyi curve X is defined over M*
- *X has good reduction at all primes $\mathfrak{p}$ of M above p*

Proof. [1] □

Corollary 6.1.2. *Let $\phi : X \to \mathbb{P}^1$ be a 2-group Belyi map. Then there exists a smooth projective model for X with good reduction away from $p = 2$.*

Proof. □

Section 6.2

Past results on Gross's conjecture

Section 6.3

A nonsolvable Galois number field ramified only at 2

Bibliography

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

[2] Gennadii Vladimirovich Belyi, *On galois extensions of a maximal cyclotomic field*, Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya **43** (1979), no. 2, 267–276.

[3] Alexandre Grothendieck, *Esquisse d'un programme*, London Mathematical Society Lecture Note Series (1997), 5–48.

[4] Michael Klug, Michael Musty, Sam Schiavone, and John Voight, *Numerical calculation of three-point branched covers of the projective line*, LMS Journal of Computation and Mathematics **17** (2014), no. 01, 379–430.

[5] Jeroen Sijsling and John Voight, *On computing belyi maps, numéro consacré au trimestre "méthodes arithmétiques et applications", automne 2013*, Publ. Math. Besançon Algèbre Théorie Nr **2014/1** (2014), 73–131.