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 23, 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

Abstract ii

Preface iii

1 Introduction **1**

1.1 Belyi maps from a historical perspective 1

1.1.1 Inverse Galois theory 2

1.1.2 Dessins d'enfants 2

2 Background **3**

2.1 What is a Belyi map? 3

2.1.1 Complex manifolds and Riemann surfaces 3

2.1.2 Algebraic curves 3

2.1.3 Branched covering spaces 4

2.1.4 Riemann's existence theorem 4

2.1.5 Belyi's theorem 5

2.1.6 Belyi maps and Galois Belyi maps 6

2.1.7 Permutation triples and passports 8

2.1.8 Triangle groups 10

2.1.9 Background results on Belyi maps 11

2.1.10 Fields of moduli and fields of definition 11
2.2 Group theory 13
2.2.1 Central group extensions and $H^2(G, A)$ 13
2.2.2 Holt's algorithm and `Magma` implementation 13
2.2.3 Results on 2-groups 13

3 A database of 2-group Belyi maps **14**
3.1 Degree 1 Belyi maps 15
3.2 An algorithm to enumerate isomorphism classes of 2-group Belyi maps 15
3.3 An algorithm to compute 2-group Belyi curves and maps 25
3.4 Running time analysis 29
3.5 Explicit computations 29

4 Classifying low genus and hyperelliptic 2-group Belyi maps **30**
4.1 Remarks on Galois Belyi maps 30
4.2 Genus 0 31
4.3 Genus 1 35
4.4 Hyperelliptic 37

5 Fields of definition of 2-group Belyi maps **40**
5.1 Refined passports 40
5.2 A refined conjecture 41

6 Gross's conjecture for $p = 2$ **42**
6.1 Beckmann's theorem 42
6.2 Past results on Gross's conjecture 43

6.3 A nonsolvable Galois number field ramified only at 2 43

References **44**

List of Tables

List of Figures

2.1.1 Belyi map isomorphism 6

2.1.2 Belyi map lax isomorphism 6

2.1.3 G-Galois Belyi map isomorphism 8

3.2.1 $\widetilde{\sigma}$ a lift of σ 15

3.2.2 $\widetilde{G}$ a (central) extension of G 16

3.2.3 The permutation triples $\widetilde{\sigma}$ constructed in Algorithm 3.2.5 correspond to Belyi maps $\widetilde{\phi} : \widetilde{X} \to \mathbb{P}^1$ in the above diagram. 18

3.2.4 Two extensions of G in Example 3.2.7 19

3.2.5 A 2-group Belyi map ϕ as a sequence of degree 2 covers. For $j \in \{1, \dots, i\}$, ϕ factors through a degree 2^j Belyi map denoted ϕ_j. . . . 23

3.3.1 Algorithm 3.3.4 describes how to construct $\widetilde{\phi}$ corresponding to a permutation triple $\widetilde{\sigma}$ from a given 2-group Belyi map ϕ. 26

4.4.1 Galois theory for a hyperelliptic Belyi map 38

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* [5] 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

What is a Belyi map?

2.1.1. Complex manifolds and Riemann surfaces

MM: [enough to define Riemann surfaces]

Definition 2.1.1. A branched cover of Riemann surfaces is a nonconstant holomorphic map $\phi\colon X \to \mathbb{P}^1$ where X is a compact connected Riemann surface.

2.1.2. Algebraic curves

MM: [enough to define good curves and function fields]

Theorem 2.1.2. MM: [correspondence curves and function fields]

Definition 2.1.3. Let $K \subseteq \mathbb{C}$ be a field. A branched cover of algebraic curves over K is a finite map of curves $\phi\colon X \to \mathbb{P}^1$ defined over K.

2.1.3. Branched covering spaces

MM: [monodromy, ramification, Galois cover, etc]

Definition 2.1.4.

2.1.4. Riemann's existence theorem

Riemann surfaces are defined in Section 2.1.1. Algebraic curves are defined in Section 2.1.2. Here in Section 2.1.4 we establish the connection between these objects over the complex numbers.

Let X be an algebraic curve over $\mathbb{C}$. Let $\mathbb{C}(t)$ denote the function field of $\mathbb{P}^1$. By Theorem 2.1.2, X corresponds to a finite extension $L := \mathbb{C}(X)$ over $\mathbb{C}(t)$. Let α be a primitive element of $L/\mathbb{C}(t)$. Then there exists a polynomial

$$f(x,t) = a_0(t) + a_1(t)x + a_2(t)x^2 + \cdots + a_n(t)x^n \in \mathbb{C}(t)[x] \tag{2.1.1}$$

where $f(\alpha, t) = 0$ and (after possibly clearing denominators) $a_i(t) \in \mathbb{C}[t]$. The polynomial f in Equation 2.1.1 defines a Riemann surface X' as a branched cover of $\mathbb{P}^1$ with branch points

$$S := \{t_0 \in \mathbb{C} : f(x, t_0) \text{ has repeated roots }\}.$$

Here x can be viewed as a meromorphic function on X' and we can identify the field of meromorphic functions on X' with L. This explains how we obtain a Riemann surface from an algebraic curve.

Suppose instead we start with a compact Riemann surface X. Can we reverse the above process to construct an algebraic curve? The crucial part of this process is proving that there exists a meromorphic function on X that realizes X as a branched cover of $\mathbb{P}^1$ (see Theorem 2.1.5 below). Given the existence of such a function, the field of meromorphic functions on X is then realized as a finite extension of the meromorphic functions on $\mathbb{P}^1$. Finally, by Theorem 2.1.2, this corresponds to an algebraic curve. The existence of such a function is given by Theorem 2.1.5 (Riemann's existence theorem).

Theorem 2.1.5. *Let X be a compact Riemann surface. Then there exists a meromorphic function on X that separates points. That is, for any set of distinct points $\{x_1, \dots, x_n\} \subset X$ and any set of distinct points $\{t_1, \dots, t_n\} \subset \mathbb{P}^1$ there exists a meromorphic function f on X such that $f(x_i) = t_i$ for all i.*

MM: [todo: more details...other formulations]

2.1.5. Belyi's theorem

In Sections 2.1.1, 2.1.2, and 2.1.4 we established the equivalence between compact Riemann surfaces and algebraic curves over $\mathbb{C}$. This was done, in part, using branched covers. It turns out that branched covers are the key to descending from the transcendental world to the number-theoretic world in the following sense.

Theorem 2.1.6 (Belyi's theorem [2])**.** *An algebraic curve X over $\mathbb{C}$ can be defined over a number field if and only if there exists a branched cover $\phi\colon X \to \mathbb{P}^1$ unramified outside* $\{0, 1, \infty\}$.

These remarkable covers are the main focus of this work.

2.1.6. Belyi maps and Galois Belyi maps

We now set up the framework to discuss the main mathematical objects of interest in this work.

Definition 2.1.7. A Belyi map is a branched cover of algebraic curves over $\mathbb{C}$ (equivalently of Riemann surfaces) $\phi\colon X \to \mathbb{P}^1$ that is unramified outside $\{0, 1, \infty\}$.

Definition 2.1.8. Two Belyi maps $\phi\colon X \to \mathbb{P}^1$ and $\phi'\colon X' \to \mathbb{P}^1$ are isomorphic if there exists an isomorphism between X and X' such that the diagram in Figure 2.1.1 commutes. If instead we only insist that the isomorphism makes the diagram in Figure 2.1.2 commute, then we say that ϕ and ϕ' are lax isomorphic.

$$\begin{tikzcd}
X \arrow[rr, "\sim"] \arrow[dr, "\phi"'] & & X' \arrow[dl, "\phi'"] \\
& \mathbb{P}^1 &
\end{tikzcd}$$

Figure 2.1.1: Belyi map isomorphism

$$\begin{tikzcd}
X \arrow[r, "\sim"] \arrow[d, "\phi"'] & X' \arrow[d, "\phi'"] \\
\mathbb{P}^1 \arrow[r, "\sim"] & \mathbb{P}^1
\end{tikzcd}$$

Figure 2.1.2: Belyi map lax isomorphism

Definition 2.1.9. A Belyi map $\phi\colon X \to \mathbb{P}^1$ is Galois if it is Galois as a cover (see Definition 2.1.4). A curve X that admits a Galois Belyi map is called a Galois Belyi curve.

Proposition 2.1.10. *Let $\phi\colon X \to \mathbb{P}^1$ be a Galois Belyi map and let $\mathbb{C}(X)$ be the function field of X. Then the field extension $\mathbb{C}(X)/\mathbb{C}(\mathbb{P}^1)$ is Galois.*

Proof. □

Definition 2.1.11. The ramification of a degree d Belyi map ϕ can be encoded with 3 partitions of d denoted $(\lambda_0, \lambda_1, \lambda_\infty)$. We call this triple of partitions the ramification type of ϕ. When ϕ is Galois, according to Lemma 4.1.1, the ramification type of ϕ can more simply be encoded by a triple of integers $(a, b, c) \in \mathbb{Z}^3_{\geq 1}$.

Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map of degree d. Once we label the sheets of the cover and pick a basepoint $\star \notin \{0, 1, \infty\}$, we obtain a homomorphism

$$h\colon \pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, \star) \to S_d \tag{2.1.2}$$

by lifting paths around the branch points of ϕ.

Definition 2.1.12. The image of h in Equation 2.1.2 is the monodromy group of ϕ denoted $\mathrm{Mon}(\phi)$. When ϕ is a Galois Belyi map, we can identify $\mathrm{Mon}(\phi)$ as the Galois group $\mathrm{Gal}(\mathbb{C}(X)/\mathbb{C}(\mathbb{P}^1))$. For this reason, we may also write $\mathrm{Gal}(\phi)$ to denote $\mathrm{Mon}(\phi)$ when ϕ is Galois.

MM: [todo: any propositions about monodromy groups can go here]

Definition 2.1.13. A G-Galois Belyi map is a Galois Belyi map $\phi\colon X \to \mathbb{P}^1$ with monodromy group G equipped with an isomorphism

$$i\colon G \xrightarrow{\sim} \mathrm{Mon}(\phi) \leq \mathrm{Aut}(X).$$

An isomorphism of G-Galois Belyi maps $(\phi\colon X \to \mathbb{P}^1, i\colon G \to \mathrm{Mon}(\phi))$ and $(\phi'\colon X' \to \mathbb{P}^1, i'\colon G \to \mathrm{Mon}(\phi)$ is an isomorphism $h\colon X \xrightarrow{\sim} X'$ such that for all $g \in G$ the diagram in Figure 2.1.3 commutes.

$$\begin{tikzcd}
X \arrow[rr, "h"] \arrow[d, "i(g)"'] & & X' \arrow[d, "i'(g)"] \\
X \arrow[rr, "h"] \arrow[dr, "\phi"'] & & X' \arrow[dl, "\phi'"] \\
& \mathbb{P}^1 &
\end{tikzcd}$$

Figure 2.1.3: G-Galois Belyi map isomorphism

Proposition 2.1.14. MM: [[3, Prop. 3.6 ish]]

2.1.7. Permutation triples and passports

Definition 2.1.15. 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

$$\sigma^\tau := (\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau, \tau^{-1}\sigma_\infty\tau) = (\sigma'_0, \sigma'_1, \sigma'_\infty) = \sigma'. \tag{2.1.3}$$

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 2.1.16. *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 [6, 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 $G_{\mathbb{Q}} := \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ acts on Belyi maps by acting on the coefficients of a set of defining equations; under the bijection of Lemma 2.1.16, 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.

Definition 2.1.17. 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).

Definition 2.1.18. 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.

Definition 2.1.19. The passport of a transitive permutation triple σ is $(g(\sigma), \langle\sigma\rangle, \lambda(\sigma))$, where (by Riemann–Hurwitz)

$$g(\sigma) := 1 - d + (e(\sigma_0) + e(\sigma_1) + e(\sigma_\infty))/2 \tag{2.1.4}$$

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 $s = 0, 1, \infty$.

Definition 2.1.20. The size of a passport $\mathcal{P}$ is the number of simultaneous conjugacy classes (as in 2.1.3) of (necessarily transitive) permutation triples σ with passport $\mathcal{P}$.

The action of $G_{\mathbb{Q}}$ 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.

Definition 2.1.21. We say a passport is irreducible if it has one $G_{\mathbb{Q}}$-orbit and reducible otherwise.

2.1.8. Triangle groups

Definition 2.1.22. Let $(a, b, c) \in \mathbb{Z}^3_{\geq 1}$. If $1 \in (a, b, c)$, then we say the triple is degenerate. Otherwise, we call the triple spherical, Euclidean, or hyperbolic according to whether the value of

$$\chi(a, b, c) = 1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c} \tag{2.1.5}$$

is negative, zero, or positive. We call this the geometry type of the triple. We associate the geometry

$$H = \begin{cases} \mathbb{P}^1 & \chi(a, b, c) < 0 \\ \mathbb{C} & \chi(a, b, c) = 0 \\ \mathfrak{H} & \chi(a, b, c) < 0 \end{cases} \tag{2.1.6}$$

where $\mathfrak{H}$ denotes the complex upper half-plane.

Definition 2.1.23. For each triple (a, b, c) in Definition 2.1.22 we define the triangle group

$$\Delta(a, b, c) = \langle \delta_a, \delta_b, \delta_c | \delta_a^a = \delta_b^b = \delta_c^c = \delta_c \delta_b \delta_a = 1 \rangle \tag{2.1.7}$$

The geometry type of a triangle group $\Delta(a, b, c)$ is the geometry type of the triple (a, b, c).

Definition 2.1.24. The geometry type of a Galois Belyi map with ramification type (a, b, c) is the geometry type of (a, b, c).

Definition 2.1.25. Let $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ be a transitive permutation triple. Let a, b, c

be the orders of $\sigma_0, \sigma_1, \sigma_\infty$ respectively. The geometry type of σ is the geometry type of (a, b, c).

The connection between Belyi maps and triangle groups of various geometry types is explained by Lemma 2.1.26.

Lemma 2.1.26. *The set of isomorphism classes of of degree d Belyi maps with ramification type (a, b, c) is in bijection with the set of index d subgroups $\Gamma \leq \Delta(a, b, c)$ up to isomorphism.*

Proof. See [6] for a detailed discussion. □

2.1.9. Background results on Belyi maps

Theorem 2.1.27. MM: [big bijection]

Proposition 2.1.28. MM: [Galois action on Belyi maps]

Proposition 2.1.29. *Galois correspondence of Belyi maps*

Proof. □

MM: [[10, 1.6, 1.7]]

2.1.10. Fields of moduli and fields of definition

Let $\mathrm{Aut}(\mathbb{C})$ denote the field automorphisms of $\mathbb{C}$.

Definition 2.1.30. Let X be an algebraic curve over $\mathbb{C}$. The field of moduli of X is the fixed field of the field automorphisms

$$\{\tau \in \mathrm{Aut}(\mathbb{C}) : X^\tau \cong X\}$$

where $\tau \in \mathrm{Aut}(\mathbb{C})$ acts on the defining equations of X. Denote this field as $M(X)$.

Definition 2.1.31. Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map. The field of moduli of ϕ is the fixed field of the field automorphisms

$$\{\tau \in \mathrm{Aut}(\mathbb{C}) : \phi^\tau \cong \phi\}$$

where $\tau \in \mathrm{Aut}(\mathbb{C})$ acts on the defining equations of ϕ and isomorphism is determined by Definition 2.1.8. Denote this field as $M(\phi)$.

Definition 2.1.32. Let $\phi\colon X \to \mathbb{P}^1$ be a G-Galois Belyi map. The field of moduli of ϕ is the fixed field of the field automorphisms

$$\{\tau \in \mathrm{Aut}(\mathbb{C}) : \phi^\tau \cong \phi\}$$

where $\tau \in \mathrm{Aut}(\mathbb{C})$ acts on the defining equations of ϕ and isomorphism is determined by Definition 2.1.13. Denote this field as $M(\phi)$.

Theorem 2.1.33. *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. [10] □

Definition 2.1.34. Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map. A number field K is a field of definition for ϕ if ϕ and X can be defined with equations over K. If K is a field of definition for ϕ we say ϕ is defined over K.

Theorem 2.1.35. *A Galois Belyi map is defined over its field of moduli.*

Proof. [3, Lemma 4.1] □

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]

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. The algorithm is inductive in the degree. The base case in degree 1 is discussed in Section 3.1. 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 3.2. 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 3.3. In Section 3.4 we give a detailed description of the running time of the algorithm. Lastly, in Section 3.5, we discuss the implementation and computations that we have carried out explicitly. Recall the definition of a G-Galois Belyi map in Section 2.1. In this section we narrow our focus to G-Galois Belyi maps with $\#G$ a power of 2.

Definition 3.0.1. A 2-group Belyi map is a Galois Belyi map with monodromy group a 2-group.

Section 3.1

Degree 1 Belyi maps

Section 3.2

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 3.1. We now set up some notation for the iteration.

Notation 3.2.1. 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 3.2.2. 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 3.2.1 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 3.2.1: $\widetilde{\sigma}$ a lift of σ

In Algorithm 3.2.5 below we describe how to determine all lifts $\widetilde{\sigma}$ (up to isomorphism) of a given permutation triple σ.

Lemma 3.2.3. *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 3.2.4. In light of Lemma 3.2.3, we can restrict our attention to central extensions of $\langle\sigma\rangle$ in Definition 3.2.2.

Algorithm 3.2.5. Let the notation be as described above in 3.2.1.

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}

1. Let $G = \langle\sigma\rangle$ and compute all central extensions $\widetilde{G}$ sitting in the exact sequence in Figure 3.2.2 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 3.2.2: $\widetilde{G}$ a (central) extension of G

2. For each extension $\widetilde{G}$ as in Figure 3.2.2 from the previous step we perform the following:

   (a) Consider the set of triples

$$\{\widetilde{\sigma} := (\widetilde{\sigma}_0, \widetilde{\sigma}_1, \widetilde{\sigma}_\infty) : \widetilde{\sigma}_s \in \pi^{-1}(\sigma_s) \text{ for } s \in \{0, 1, \infty\}\} \tag{3.2.1}$$

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

$$\mathrm{Lifts}(\sigma, (a,b,c)) := \{\widetilde{\sigma} \in \mathrm{Lifts}(\sigma) : \mathrm{order}(\widetilde{\sigma}) = (a,b,c)\}. \tag{3.2.2}$$

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

3. Return the union of the sets $\mathrm{Lifts}(\sigma, (a,b,c))$ ranging over all extensions as in Figure 3.2.2 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 2.1.29, 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 3.2.2. 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 $\mathrm{Lifts}(\sigma)$. In Step 2(b), we are sorting $\mathrm{Lifts}(\sigma)$ 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 3.2.6. In fact, even though we do not need this for the algorithm, there are at most 2 different passports that can occur in $\mathrm{Lifts}(\sigma)$. 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 $\mathrm{Lifts}(\sigma)$ have the same passport.

At this point, we have constructed the sets $\mathrm{Lifts}(\sigma, (a, b, c))$. In light of Remark 3.2.6, there are only 2 possibilities:

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

Step 2(c) is to eliminate simultaneous conjugation in each set $\mathrm{Lifts}(\sigma, (a, b, c))$. After Step 2(c) is complete, the sets $\mathrm{Lifts}(\sigma, (a, b, c))$ 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 3.2.3 commutes. In Step

$$\begin{tikzcd}
\widetilde{X} \arrow[dr, "2"] \arrow[dd, "\widetilde{\phi}"'] & \\
& X \arrow[dl, "\phi"] \\
\mathbb{P}^1 &
\end{tikzcd}$$

Figure 3.2.3: The permutation triples $\widetilde{\sigma}$ constructed in Algorithm 3.2.5 correspond to Belyi maps $\widetilde{\phi} : \widetilde{X} \to \mathbb{P}^1$ in the above diagram.

3 we collect together all sets $\mathrm{Lifts}(\sigma, (a, b, c))$ as we range over all possible extensions in Step 1, and by the discussion for Step 2 yields the desired output. $\square$

We now illustrate Algorithm 3.2.5 with the following example.

Example 3.2.7. In this example we carry out Algorithm 3.2.5 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 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 3.2.4: Two extensions of G in Example 3.2.7

extensions separately:

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

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

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

  Remark 3.2.8. 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 $\mathrm{Lifts}(\sigma)$ 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 $\left\{\boxed{1\,3}, \boxed{2\,4}\right\}$. 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

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

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 $\mathrm{Lifts}(\sigma)$ that generate $\widetilde{G}_1$, so at the end of Step 2(a) for this extension we have

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

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

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

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 3.2.3.

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 3.2.9. Let the notation be as described above in 3.2.1.

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

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

- $\mathscr{G}_{2^i}^{\mathrm{above}}$: the set of isomorphism classes of 2-group Belyi maps of degree 2^i indexed by permutation triples $\widetilde{\sigma}$
- $\mathscr{G}_{2^i}^{\mathrm{below}}$: 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 3.2.2) of σ. This algorithm is iterative. For each $i = 1, \dots, m$, 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 3.2.5 to every $\sigma \in \mathscr{G}_{2^i}^{\text{below}}$ to obtain $\#\mathscr{G}_{2^i}^{\text{below}}$ sets $\text{Lifts}(\sigma)$. As a word of caution, the notation $\text{Lifts}(\sigma)$ has a different meaning here than in Algorithm 3.2.5. Here $\text{Lifts}(\sigma)$ 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 $\mathscr{G}_2, \mathscr{G}_4, \dots, \mathscr{G}_{2^m}$.

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

$$G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_i \tag{3.2.3}$$

where $G_0 = \{1\}$, $G_i = G$, and each consecutive quotient is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. By the Galois correspondence, Proposition 2.1.29, this normal tower of groups corresponds to the diagram in Figure 3.2.5. Let σ_j be the permutation triple corresponding

$$\begin{tikzcd}
X_i = X \arrow[d, "2"'] \arrow[ddddr, bend left, "\phi_i = \phi"] \\
\vdots \arrow[d, "2"'] \\
X_2 \arrow[d, "2"'] \arrow[ddr, bend left, "\phi_2"] \\
X_1 \arrow[dr, "\phi_1", "2"'] \\
& X_0 = \mathbb{P}^1
\end{tikzcd}$$

Figure 3.2.5: A 2-group Belyi map ϕ as a sequence of degree 2 covers. For $j \in \{1, \dots, i\}$, ϕ factors through a degree 2^j Belyi map denoted ϕ_j.

to ϕ_j in Figure 3.2.5. Applying Algorithm 3.2.5 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 3.2.5 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 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 3.2.10. *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 3.2.9. MM: [maybe go up to 512 or 1024 and include source code link to implementation] □

Algorithm 3.2.11. We use Algorithm 3.2.9 to count the number of Passports of 2-group Belyi maps of a given degree. MM: [todo]

Theorem 3.2.12. *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 3.2.11. □

Section 3.3

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 3.1. We now set up some notation for the iteration.

Notation 3.3.1. First 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 3.2.5 applied to the input σ

Algorithm 3.3.4 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 3.3).

$$\begin{tikzcd}
\widetilde{X} \arrow[dd, "\widetilde{\phi}"'] \arrow[dr, "\psi"] & \\
& X \arrow[dl, "\phi"] \\
\mathbb{P}^1 &
\end{tikzcd}$$

Figure 3.3.1: Algorithm 3.3.4 describes how to construct $\widetilde{\phi}$ corresponding to a permutation triple $\widetilde{\sigma}$ from a given 2-group Belyi map ϕ.

Lemma 3.3.2. *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, $f/g \in K^\times$. $\square$

Definition 3.3.3. Let $\phi\colon X \to \mathbb{P}^1$ be a 2-group Belyi map. Let $\operatorname{div} \phi = D_0 - D_\infty$ and $\operatorname{div}(\phi - 1) = D_1 - D'_\infty$ with $D_0, D_1, D_\infty, D'_\infty$ effective. For $s \in \{0, 1, \infty\}$ let

$$R_s \subseteq \operatorname{supp} D_s$$

and $R := R_0 + R_1 + R_\infty$. Let K be a number field containing the coordinates of all ramification points in $\operatorname{supp} R$ and let

$$M = (R + 2\mathbb{Z}R) \cap \operatorname{Div}^0(X), \tag{3.3.1}$$

and consider the map $M \to \operatorname{Pic}^0(X)(K)$. If this map has nontrivial kernel we say that ϕ is fully ramified for the ramification divisor R.

Algorithm 3.3.4. Let the notation be as described above in 3.3.1.

Input:

- $\phi : X \to \mathbb{P}^1$ a 2-group Belyi map
- $\widetilde{\sigma}$ a permutation triple which is a lift of σ a permutation triple corresponding to ϕ
- Suppose ϕ is fully ramified for R in Step 1

Output: A model over a number field K for the Belyi map $\widetilde{\phi} : \widetilde{X} \to \mathbb{P}^1$ 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 K be a number field containing all coordinates of points in R (a subset of the ramification points of ϕ).
3. Let $M = (R + 2\mathbb{Z}R) \cap \operatorname{Div}^0(X)$.
4. For each $D \in M$ do the following:
   - Compute the Riemann-Roch space $\mathscr{L}(D)$.
   - If $\dim \mathscr{L}(D) = 1$, then compute $f \in K(X)^\times$ corresponding to a generator of $\mathscr{L}(D)$ exit the loop and go to Step 5.

- If $\dim \mathscr{L}(D) = 0$, then continue this loop with another choice of D.

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

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

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

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

7. 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 3.2.5, 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 3.3). Now that we have the ramification points, we can construct the new Belyi map and curve by extracting a square root in the function field. More precisely, again by Algorithm 3.2.5, there exists $\widetilde{X}$ and a number field K with $K(\widetilde{X}) = K(X, \sqrt{f})$ where $f \in K(X)^\times / K(X)^{\times 2}$ and

$$\operatorname{div} f = \sum_{Q_{s,\tau} \in R} Q_{s,\tau} + 2D_\epsilon \in \frac{\mathrm{Div}^0(X)}{2\,\mathrm{Div}^0(X)} \tag{3.3.2}$$

Since ϕ is fully ramified for R, there is a $D \in M$ such that $f \in \mathscr{L}(D)$ will be obtained in Step 4. In Step 5 we start with the ideal of X and add a new equation (using an extra variable) corresponding to extracting the square root of f. This is our candidate ideal for $\widetilde{X}$, but this process may introduce extra components. To eliminate these components, we saturate the ideal in Step 6. By construction, the projection map to the first (affine) coordinate is the desired Belyi map with Belyi curve $\widetilde{X}$. □

Remark 3.3.5. The condition that ϕ is fully ramified is required to avoid a potentially infinite loop in Step 4. Testing this condition is only implemented over a finite field, so in practice we simply search for candidate divisors in M without testing if ϕ is fully ramified. This appears to work well in practice, and has been used to carry out the explicit computations in Section 3.5.

Remark 3.3.6. Another important aspect of this process is the choice of K. In Algorithm 3.3.4, we try to keep the degree of K as small as possible. Adjoining all coordinates of ramification points can lead to high degree extensions which are not feasible in practice. We choose to obtain the Belyi curve over a subfield when possible.

Section 3.4

Running time analysis

Section 3.5

Explicit computations

MM: [link to database, code, and some tables]

Chapter 4

Classifying low genus and hyperelliptic 2-group Belyi maps

In this chapter we organize some results on 2-group Belyi maps with low genus. 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 these special cases.

Section 4.1

Remarks on Galois Belyi maps

We summarize some of the results on Galois Belyi maps that we use for 2-group Belyi maps. A great deal is known about Galois Belyi maps (regular dessins) in general (see MM: [TODO: sources]).

Lemma 4.1.1. *Let σ be a degree d permutation triple corresponding to $\phi\colon X \to \mathbb{P}^1$ a Galois Belyi map with monodromy group G and m_s be the order of σ_s for $s \in$*

$\{0, 1, \infty\}$. *Then* σ_s *consists of* d/m_s *many* m_s*-cycles. In particular, for a* 2*-group Belyi map,* m_s *and* $\#G$ *are powers of* 2*.*

Proof. □

In light of Lemma 4.1.1, we get a refined version of Riemann-Hurwitz for Galois Belyi maps.

Proposition 4.1.2. *Let* σ *be a degree* d *permutation triple corresponding to* $\phi\colon X \to \mathbb{P}^1$ *a Galois Belyi map with monodromy group* G*. Let* a, b, c *be the orders of* $\sigma_0, \sigma_1, \sigma_\infty$ *respectively. Then*

$$g(X) = 1 + \frac{\#G}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right). \tag{4.1.1}$$

Proof. □

Section 4.2

Genus 0

Let $\phi : X \to \mathbb{P}^1$ be a 2-group Belyi map where X has genus 0. Proposition 4.1.2 immediately restricts the possibilities for ramification indices.

Proposition 4.2.1. *A* 2*-group Belyi map of genus* 0 *with monodromy group* G *has the following possibilities for ramification indices:*

- *degenerate:* $(1, \#G, \#G)$, $(\#G, 1, \#G)$, $(\#G, \#G, 1)$
- *dihedral:* $\left(\frac{\#G}{2}, 2, 2\right)$, $\left(2, \frac{\#G}{2}, 2\right)$, $\left(2, 2, \frac{\#G}{2}\right)$

Proof. Let a, b, c be the ramification indices of the Belyi map. Then by Lemma 4.1.1, $a, b, c, \#G$ are all positive powers of 2. Without loss of generality we may assume

$a \leq b \leq c$. The proof is by cases. For $g(X) = 0$, Proposition 4.1.2 yields

$$\frac{\#G}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right) = -1. \tag{4.2.1}$$

$\underline{a = 1}$: If $a = 1$, then Equation 4.2.1 becomes $\frac{1}{b} + \frac{1}{c} = \frac{2}{\#G}$.

$\underline{b = 1}$: If $a = b = 1$, then Equation 4.2.1 implies $a = b = c = \#G = 1$.

$\underline{b \geq 2}$: If $a = 1$ and $b \geq 2$, then we can let $b = 2^m$ and $c = 2^n$ with $m \leq n$. In this case Equation 4.2.1 becomes

$$\frac{1}{2^m} + \frac{1}{2^n} = \frac{2}{\#G} \implies \#G\left(2^{n-m} + 1\right) = 2^{n+1}.$$

Since $\#G$ is a power of 2, we must have $2^{n-m} + 1 \in \{1, 2\}$ which only occurs when $m = n$. Therefore $m = n$ which implies $b = c = \#G$.

$\underline{a = 2}$: If $a = 2$, then Equation 4.2.1 becomes

$$\frac{2}{\#G} = \frac{1}{b} + \frac{1}{c} - \frac{1}{2}.$$

$\underline{b = 2}$: If $a = 2$ and $b = 2$, then Equation 4.2.1 implies $c = \frac{\#G}{2}$.

$\underline{b \geq 4}$: If $a = 2$ and $b, c \geq 4$, then Equation 4.2.1 implies

$$\frac{2}{\#G} = \frac{1}{b} + \frac{1}{c} - \frac{1}{2} \implies \frac{2}{\#G} \leq 0$$

which cannot occur.

$\underline{a \geq 4}$: If $a, b, c \geq 4$, then Equation 4.2.1 becomes

$$\frac{2}{\#G} = \frac{1}{b} + \frac{1}{c} - \left(1 - \frac{1}{a}\right).$$

But $\left(1 - \frac{1}{a}\right) \geq \frac{3}{4}$ and $\frac{1}{b} + \frac{1}{c} \leq \frac{1}{2}$ imply that $\frac{2}{\#G} < 0$ which cannot occur.

In summary there are 2 possibilities:

- $a = 1$ and $b = c = \#G$
- $a = 2$, $b = 2$, and $c = \frac{\#G}{2}$

By reordering the ramification indices we obtain the possibilities in Proposition 4.2.1.

□

In particular, from Proposition 4.2.1 we see that all genus 0 2-group Belyi maps are degenerate or spherical dihedral. The explicit maps in these cases are well understood MM: [TODO: cite][7]. We summarize with Proposition 4.2.2.

Proposition 4.2.2. *Every possible ramification type in Proposition 4.2.1 corresponds to exactly one Belyi map up to isomorphism. Moreover, the equations for these maps have simple formulas given below. In the formulas below, we use the notation from Proposition 4.2.1 for ramification types and write a Belyi map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ with monodromy G as a rational function in the coordinate x on an affine patch of the domain of ϕ.*

- $(1, 1, 1)$

$$\phi(x) = x$$

- $(1, \#G, \#G)$, $\#G \geq 2$

$$\phi(x) = 1 - x^{\#G}$$

- $(\#G, 1, \#G),\ \#G \geq 2$

$$\phi(x) = x^{\#G}$$

- $(\#G, \#G, 1),\ \#G \geq 2$

$$\phi(x) = \frac{x^{\#G}}{x^{\#G} - 1}$$

- $(2, 2, 2),\ \#G = 2$

$$\phi(x) = -\left(\frac{x(x-1)}{x - \frac{1}{2}}\right)^2$$

- $(2, 2, \frac{\#G}{2}),\ \#G \geq 4$

$$\phi(x) = -\frac{1}{4}\left(x^{\#G/2} + \frac{1}{x^{\#G/2}}\right) + \frac{1}{2}$$

- $(2, \frac{\#G}{2}, 2),\ \#G \geq 4$

$$\phi(x) = 1 - \frac{1}{1 - \left(-\frac{1}{4}\left(x^{\#G/2} + \frac{1}{x^{\#G/2}}\right) + \frac{1}{2}\right)}$$

- $(\frac{\#G}{2}, 2, 2),\ \#G \geq 4$

$$\phi(x) = \frac{1}{-\frac{1}{4}\left(x^{\#G/2} + \frac{1}{x^{\#G/2}}\right) + \frac{1}{2}}$$

Proof. We first address the correctness of the equations. For the ramification triples containing 1, the equations are all lax isomorphic to one of the form

$$\phi(x) = x^{\#G} \tag{4.2.2}$$

for the ramification triple $(\#G, 1, \#G)$. The rational function ϕ in Equation 4.2.2 has a root of multiplicity $\#G$ at 0, a pole of multiplicity $\#G$ at ∞, and $\#G$ unique preimages above 1. The Belyi maps for ramification triples $(1, \#G, \#G)$ and $(\#G, \#G, 1)$ are lax isomorphic to ϕ in Equation 4.2.2 and similarly have the correct ramification of this degenerate Belyi map.

For the other ramification triples, we focus on the triple $(2, 2, \frac{\#G}{2})$. The equation for this map is a modification (pointed out to me by Sam Schiavone) of the dihedral Belyi map

$$\phi(x) = x^d + \frac{1}{x^d} \tag{4.2.3}$$

in [7, Example 5.1.2]. The other dihedral maps are then lax isomorphic to (the modification of) the map in Equation 4.2.3.

To show that there is at most one Belyi map in each of the above cases, we refer to Algorithm 3.2.5. MM: [todo] □

Section 4.3

Genus 1

Let $\phi\colon X \to \mathbb{P}^1$ be a 2-group Belyi map where X has genus 1. Let (a, b, c) be the ramification indices of ϕ with $a \leq b \leq c$. From Proposition 4.1.2, we have that

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 0. \tag{4.3.1}$$

Since a, b, c are powers of 2, the only solution to Equation 4.3.1 is $a = 2$ and $b = c = 4$. We summarize this discussion in Proposition 4.3.1.

Proposition 4.3.1. *The only possible ramification indices for a 2-group Belyi map of genus 1 are $(2, 4, 4)$, $(4, 2, 4)$, or $(4, 4, 2)$.*

As was the case in genus 0, all ramification triples in Proposition 4.3.1 have corresponding Belyi maps. However, as we see in Proposition 4.3.2, these genus 1 Belyi maps occur in infinite families.

Proposition 4.3.2. *Let (a, b, c) be a ramification triple in Proposition 4.3.1 and let $d = 2^m$ for $m \in \mathbb{Z}_{\geq 2}$. Then there exists exactly one degree d 2-group Belyi map up to isomorpism with ramification (a, b, c). Moreover, the equations for these maps have simple formulas which are described below. In these equations let E be the elliptic curve with j-invariant 1728 given by the Weierstrass equation*

$$E\colon y^2 = x^3 + x.$$

Every degree 4 Belyi map below is of the form $\phi\colon E \to \mathbb{P}^1$ where ϕ (written as an element of the function field of E) is one of the following:

$$\begin{aligned} \phi_{(2,4,4)} &= \frac{x^2+1}{x^2} \\ \phi_{(4,2,4)} &= \phi_{(2,4,4)} - 1 = -\frac{1}{x^2} \\ \phi_{(4,4,2)} &= \frac{1}{\phi_{(2,4,4)}} = \frac{x^2}{x^2+1} \end{aligned} \tag{4.3.2}$$

Every degree d Belyi map for $d \geq 8$ is of the form

$$E \xrightarrow{\psi} E \xrightarrow{\phi} \mathbb{P}^1$$

where ϕ is a degree 4 genus 1 Belyi map and ψ is degree $d/4$ isogeny of E. Moreover, *if we let $\alpha\colon E \to E$ be defined by*

$$(x, y) \mapsto \left((1+\sqrt{-1})^{-2}\left(x+\frac{1}{x}\right), (1+\sqrt{-1})^{-3}y\left(1-\frac{1}{x^2}\right)\right) \tag{4.3.3}$$

then ψ is the map α composed with itself $d/8$ times.

Proof. For a proof that these are the only such 2-group Belyi maps we used [3, Lemma 3.5]. This can also be seen from Algorithm 3.2.9. The degree 4 Belyi maps are all lax isomorphic to the degree 4 genus 1 Belyi map with ramification indices $(4, 4, 2)$ in [8]. For degree d with $d \geq 8$ let ϕ be one of the degree 4 maps in Equation 4.3.2. We then precompose ϕ with $\alpha \cdots \alpha$ ($d/8$ times) where α is the degree 2 endomorphism of E found in [12, Proposition 2.3.1]. Since isogenies are unramified in characteristic 0 (see [11, Chapter III, Theorem 4.10]) the composition $\phi\alpha^{d/8}$ is a degree d Belyi map with the same ramification type as ϕ. □

Section 4.4

Hyperelliptic

Definition 4.4.1. Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map of genus ≥ 2. We say a Belyi map ϕ is hyperelliptic if X is a hyperelliptic curve. A hyperelliptic curve X over $\mathbb{C}$ is defined by having an element $\iota \in \mathrm{Aut}(X)$ such that the quotient map $X \to X/\langle\iota\rangle$ is a degree 2 map to $\mathbb{P}^1$. This element ι is known as the hyperelliptic involution.

Let $\phi\colon X \to \mathbb{P}^1$ be a hyperelliptic 2-group Belyi map with monodromy group $H \leq G := \mathrm{Aut}(X)$, and hyperelliptic involution $\iota \in \mathrm{Aut}(X)$.

Lemma 4.4.2. $\langle\iota\rangle \trianglelefteq \mathrm{Aut}(X)$

Proof. □

Definition 4.4.3. The reduced automorphism group of X is the quotient group $G_{\text{red}} := G/\langle\iota\rangle$.

From Lemma 4.4.2 and the Galois condition on ϕ, we obtain the diagram in Figure 4.4.1.

$$\begin{tikzcd}
& X \arrow[dl, Rightarrow, "\phi"'] \arrow[dr, Rightarrow, "\langle\iota\rangle"] \arrow[dd, Rightarrow, "\psi"] & \\
\mathbb{P}^1 \simeq X/H \arrow[dr] & & \mathbb{P}^1 \simeq X/\langle\iota\rangle \arrow[dl, Rightarrow, "G/\langle\iota\rangle"] \\
& \mathbb{P}^1 \simeq X/G &
\end{tikzcd}$$

Figure 4.4.1: Galois theory for a hyperelliptic Belyi map

Proposition 4.4.4. *Let ϕ and ψ be the maps shown in Figure 4.4.1. If ϕ is a Belyi map, then ψ is a Belyi map.*

Proof. By Theorem 2.1.27, ϕ corresponds to a normal inclusion of triangle groups $\Delta_1 \trianglelefteq \Delta_H$ and the map $X/H \to X/G$ corresponds to an inclusion of Fuchsian groups

$$\Delta_H \leq \Gamma. \tag{4.4.1}$$

By a result in [13, Page 36], the inclusion of a triangle group Δ_H in a Fuchsian group Γ as in Equation 4.4.1 implies that Γ is a triangle group which we denote Δ_G. Now we have the (normal by Lemma 4.4.2) inclusion $\Delta_1 \trianglelefteq \Delta_G$ which (again by Theorem 2.1.27) implies that ψ is a Belyi map. □

Proposition 4.4.4 reduces the classification of these hyperelliptic 2-group Belyi maps to the situation on the right side of the diagram in Figure 4.4.1. The possibilities for G_{red} in this setting are known (see [4, §1.1]). Moreover, since G is a 2-group (MM: [G only contains a 2-group. . .]), the only possibilities for G_{red} are cyclic or dihedral of order $\#G/2$. G is then an extension of G_{red} by ι (an element of order 2 generating a normal subgroup of G). Such groups are classified in [9] which we summarize in the following theorem.

Theorem 4.4.5. *Let G be the full automorphism group of a 2-group Belyi curve. Let $\#G_{\mathrm{red}} = 2^n$. Then G is isomorphic to one of the following groups:*

- $\mathbb{Z}/2^{n+1}\mathbb{Z}$
- $\mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $D_{2^{n+1}}$
- $D_{2^n} \times \mathbb{Z}/2\mathbb{Z}$

where D_m denotes the dihedral group of order m.

Proof. [9, Theorem 2.1]. □

MM: [you get a genus zero phi0 : Belyi map PP1 $\to$ PP1 and the degree 2 map on top must be ramified, corresponding to the hyperelliptic involution, can only be ramified along the preimages of ramification points of phi0, and in a group-invariant way, so that should really give you the equations as well.]

MM: [maybe write down explicit maps for g=2,3]

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. Recall Section 2.1.10 on fields of moduli and fields of definition and Recall Section 2.1.7 on passports.

Section 5.1

Refined passports

Definition 5.1.1. 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 5.2

A refined conjecture

Conjecture 5.2.1. *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. MM: [computational evidence, true in easy cases] □

Corollary 5.2.2. *Every 2-group Belyi map is defined over a cyclotomic field $\mathbb{Q}(\zeta_{2^m})$ for some m.*

Proof. MM: [The group $\mathrm{Gal}(\mathbb{Q}^{\mathsf{al}}/\mathbb{Q}^{\mathsf{ab}})$ acts on the refined passport] □

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] Pete L Clark and John Voight, *Algebraic curves uniformized by congruence subgroups of triangle groups*, arXiv preprint arXiv:1506.01371 (2015).

[4] I Dolgachev, *Mckay correspondence. winter 2006/07*, Lecture notes (2009).

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

[6] 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.

[7] Cemile Kürkoğlu, *Exceptional belyi coverings*, Ph.D. thesis, bilkent university, 2015.

[8] Michael Musty, Sam Schiavone, Jeroen Sijsling, and John Voight, *A database of belyi maps*, arXiv preprint arXiv:1805.07751 (2018).

[9] Tanush Shaska, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 248–254.

[10] 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.

[11] Joseph H Silverman, *The arithmetic of elliptic curves*, vol. 106, Springer Science & Business Media, 2009.

[12] ———, *Advanced topics in the arithmetic of elliptic curves*, vol. 151, Springer Science & Business Media, 2013.

[13] David Singerman, *Finitely maximal fuchsian groups*, Journal of the London Mathematical Society **2** (1972), no. 1, 29–38.