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

February 27, 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 [1], 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* [2] 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

2.1.4. Belyi maps and G-Belyi maps

Proposition 2.1.1. *Galois correspondence of Belyi maps*

Proof. □

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

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 Chapter **??**. 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 Lifts$(\sigma,(a,b,c))$ has exactly one representative from each simultaneous conjugacy class. MM: [TODO: reword]

3. Return the union of the sets 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 2.1.1, 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 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 $\text{Lifts}(\sigma, (a, b, c))$ and $\text{Lifts}(\sigma, (a', b', c'))$ each consisting of at most 2 triples.

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

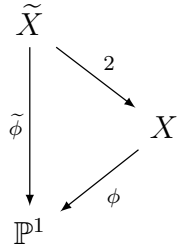

Figure 3.3.3: The permutation triples $\widetilde{\sigma}$ constructed in Algorithm 3.3.5 correspond to Belyi maps $\widetilde{\phi} : \widetilde{X} \to \mathbb{P}^1$ in the above diagram.

3 we collect together all sets $\text{Lifts}(\sigma, (a, b, c))$ 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 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 Lifts$(\sigma, (2,2,2))$.

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

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

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

In Step 3, we return

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

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 bipartite graph

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).

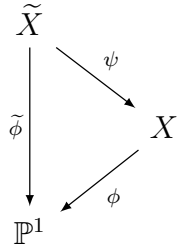

Figure 3.4.1: Algorithm 3.4.3 describes how to construct $\widetilde{\phi}$ corresponding to a permutation triple $\widetilde{\sigma}$ from a given 2-group Belyi map ϕ.

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

Bibliography

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

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