2-group Belyi maps

Michael Musty

July 9, 2019

Dartmouth College

Acknowledgements

- Committee: Dave, Tom, Carl, and John
- Family: Mary, Jim, Matt, and Nicole
- Others: Sam, Jeroen, Edgar, Florian, and Richard

Outline

Motivation

Background

Computing permutation triples

Computing equations

A refined conjecture

Examples

Motivation

Let X be an irreducible, smooth projective algebraic curve of genus $g \ge 1$ over a number field K. Let $G_K := \operatorname{Gal}(K^{\operatorname{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime.

Let X be an irreducible, smooth projective algebraic curve of genus $g \geq 1$ over a number field K. Let $G_K := \operatorname{Gal}(K^{\operatorname{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime. Let $J := \operatorname{Jac}(X)$ be the **Jacobian variety** of X. J is an abelian variety of dimension g.

Let X be an irreducible, smooth projective algebraic curve of genus $g \geq 1$ over a number field K. Let $G_K := \operatorname{Gal}(K^{\operatorname{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime.

Let J := Jac(X) be the **Jacobian variety** of X. J is an abelian variety of dimension g.

 G_K acts on the ℓ -torsion points $J[\ell](K^{al}) \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ of X.

Let X be an irreducible, smooth projective algebraic curve of genus $g \geq 1$ over a number field K. Let $G_K := \operatorname{Gal}(K^{\operatorname{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime.

Let J := Jac(X) be the **Jacobian variety** of X. J is an abelian variety of dimension g.

 G_K acts on the ℓ -torsion points $J[\ell](K^{al}) \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ of X. This action determines a **mod**- ℓ **Galois representation**

$$\rho \colon G_{\mathsf{K}} \to \operatorname{\mathsf{Aut}}(J[\ell]) \cong \operatorname{\mathsf{GL}}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

Let X be an irreducible, smooth projective algebraic curve of genus $g \geq 1$ over a number field K. Let $G_K := \operatorname{Gal}(K^{\operatorname{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime.

Let J := Jac(X) be the **Jacobian variety** of X. J is an abelian variety of dimension g.

 G_K acts on the ℓ -torsion points $J[\ell](K^{al}) \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ of X. This action determines a **mod**- ℓ **Galois representation**

$$\rho \colon G_{\mathcal{K}} \to \operatorname{Aut}(J[\ell]) \cong \operatorname{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

The geometry of X and the arithmetic of ρ are inimately related.

Let X be an irreducible, smooth projective algebraic curve of genus $g \geq 1$ over a number field K. Let $G_K := \operatorname{Gal}(K^{\operatorname{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime.

Let J := Jac(X) be the **Jacobian variety** of X. J is an abelian variety of dimension g.

 G_K acts on the ℓ -torsion points $J[\ell](K^{al}) \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ of X. This action determines a **mod**- ℓ **Galois representation**

$$\rho \colon G_{\mathcal{K}} \to \operatorname{Aut}(J[\ell]) \cong \operatorname{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

The geometry of X and the arithmetic of ρ are inimately related. For example, if X has good reduction at a prime $\mathfrak p$ above $p \neq \ell$, then $\mathfrak p$ will be unramified in the ℓ -torsion field $K(J[\ell])$.

Belyi's theorem

A **Belyi map** is a morphism $\phi \colon X \to \mathbb{P}^1$ of smooth projective algebraic curves over \mathbb{C} that is unramified outside of $\{0,1,\infty\}$.

Belyi's theorem

A **Belyi map** is a morphism $\phi \colon X \to \mathbb{P}^1$ of smooth projective algebraic curves over \mathbb{C} that is unramified outside of $\{0,1,\infty\}$.

Theorem (Belyi 1979)

An algebraic curve (smooth projective) over $\mathbb C$ can be defined over a number field if and only if X admits a Belyi map.

Let $\phi \colon X \to \mathbb{P}^1$ be a Belyi map defined over K.

Let $\phi \colon X \to \mathbb{P}^1$ be a Belyi map defined over K.

The **genus** of ϕ is the genus of the curve X.

Let $\phi \colon X \to \mathbb{P}^1$ be a Belyi map defined over K. The **genus** of ϕ is the genus of the curve X. The **degree** of ϕ is the degree of the field extension

$$K(\mathbb{P}^1) \hookrightarrow K(X)$$
.

Let $\phi \colon X \to \mathbb{P}^1$ be a Belyi map defined over K.

The **genus** of ϕ is the genus of the curve X.

The **degree** of ϕ is the degree of the field extension

$$K(\mathbb{P}^1) \hookrightarrow K(X)$$
.

 ϕ is **geometrically Galois** if $K^{al}(X)$ is a Galois extension.

Let $\phi: X \to \mathbb{P}^1$ be a Belyi map defined over K.

The **genus** of ϕ is the genus of the curve X.

The degree of ϕ is the degree of the field extension

$$K(\mathbb{P}^1) \hookrightarrow K(X).$$

 ϕ is **geometrically Galois** if $K^{al}(X)$ is a Galois extension.

The **monodromy group of** ϕ , $Mon(\phi)$, is the image of the map

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

obtained by path lifting.

Let $\phi: X \to \mathbb{P}^1$ be a Belyi map defined over K.

The **genus** of ϕ is the genus of the curve X.

The **degree** of ϕ is the degree of the field extension

$$K(\mathbb{P}^1) \hookrightarrow K(X)$$
.

 ϕ is **geometrically Galois** if $K^{al}(X)$ is a Galois extension.

The **monodromy group of** ϕ , Mon (ϕ) , is the image of the map

$$\pi_1(\mathbb{P}^1\setminus\{0,1,\infty\},\star) o \mathcal{S}_d$$

obtained by path lifting.

When ϕ is Galois we can identify $\mathsf{Mon}(\phi)$ with $\mathsf{Gal}(K^{\mathsf{al}}(X) | K^{\mathsf{al}}(\mathbb{P}^1))$.

Let $\phi \colon X \to \mathbb{P}^1$ be a Belyi map defined over K.

The **genus** of ϕ is the genus of the curve X.

The **degree** of ϕ is the degree of the field extension

$$K(\mathbb{P}^1) \hookrightarrow K(X)$$
.

 ϕ is **geometrically Galois** if $K^{al}(X)$ is a Galois extension.

The **monodromy group of** ϕ , $Mon(\phi)$, is the image of the map

$$\pi_1(\mathbb{P}^1\setminus\{0,1,\infty\},\star) o \mathcal{S}_d$$

obtained by path lifting.

When ϕ is Galois we can identify $\mathsf{Mon}(\phi)$ with $\mathsf{Gal}(K^{\mathsf{al}}(X) \mid K^{\mathsf{al}}(\mathbb{P}^1))$.

We can now state Beckmann's theorem.

Beckmann's theorem

Theorem (Beckmann 1989)

Let $\phi \colon X \to \mathbb{P}^1$ be a Galois Belyi map with monodromy group G. Let p be a prime not dividing #G.

Beckmann's theorem

Theorem (Beckmann 1989)

Let $\phi \colon X \to \mathbb{P}^1$ be a Galois Belyi map with monodromy group G. Let p be a prime not dividing #G.

Then there exists a number field M satisfying the following properties.

Beckmann's theorem

Theorem (Beckmann 1989)

Let $\phi: X \to \mathbb{P}^1$ be a Galois Belyi map with monodromy group G. Let p be a prime not dividing #G.

Then there exists a number field M satisfying the following properties.

- p is unramified in M
- φ is defined over M
- X is defined over M
- X has good reduction at all primes p of M above p

Conjecture (Gross 1998)

For every prime p, there exists a nonsolvable Galois number field ramified only at p.

Conjecture (Gross 1998)

For every prime p, there exists a nonsolvable Galois number field ramified only at p.

```
p \ge 11: existence (Serre), explicit (Edixhoven, Mascot)
```

```
p = 7: existence (Dieulefait)
```

```
p=5: existence (Dembélé, Greenberg, Voight), explicit (Roberts)
```

```
p = 3: existence (Dembélé, Greenberg, Voight)
```

p=2: existence (Dembélé)

Conjecture (Gross 1998)

For every prime p, there exists a nonsolvable Galois number field ramified only at p.

```
p \ge 11: existence (Serre), explicit (Edixhoven, Mascot)
```

p = 7: existence (Dieulefait)

p = 5: existence (Dembélé, Greenberg, Voight), explicit (Roberts)

p = 3: existence (Dembélé, Greenberg, Voight)

p = 2: existence (Dembélé)

The hope is that an explicit nonsolvable field ramified only at 2 can be obtained as K(Jac(X)[2]) where X is the domain of a Galois Belyi map with monodromy group a 2-group.

Conjecture (Gross 1998)

For every prime p, there exists a nonsolvable Galois number field ramified only at p.

```
p \ge 11: existence (Serre), explicit (Edixhoven, Mascot)
```

p = 7: existence (Dieulefait)

p = 5: existence (Dembélé, Greenberg, Voight), explicit (Roberts)

p = 3: existence (Dembélé, Greenberg, Voight)

p = 2: existence (Dembélé)

The hope is that an explicit nonsolvable field ramified only at 2 can be obtained as K(Jac(X)[2]) where X is the domain of a Galois Belyi map with monodromy group a 2-group.

We call these Belyi maps 2-group Belyi maps.

Motivated by the applications of 2-group Belyi maps to arithmetic geometry, we now state the main results.

 implementation of an algorithm to enumerate isomorphism classes of 2-group Belyi maps

- implementation of an algorithm to enumerate isomorphism classes of 2-group Belyi maps
- implementation of an algorithm to compute equations for 2-group Belyi maps over finite fields

- implementation of an algorithm to enumerate isomorphism classes of 2-group Belyi maps
- implementation of an algorithm to compute equations for 2-group Belyi maps over finite fields
- implementation of a method to compute equations for 2-group Belyi maps over number fields

- implementation of an algorithm to enumerate isomorphism classes of 2-group Belyi maps
- implementation of an algorithm to compute equations for 2-group Belyi maps over finite fields
- implementation of a method to compute equations for 2-group Belyi maps over number fields
- computational and theoretical evidence supporting a conjecture that every 2-group Belyi map is defined over an abelian extension of the rationals

Background

Isomorphism of Belyi maps

Let $\phi: X \to \mathbb{P}^1$ and $\phi': X' \to \mathbb{P}^1$ be Belyi maps of degree d.

Isomorphism of Belyi maps

Let $\phi \colon X \to \mathbb{P}^1$ and $\phi' \colon X' \to \mathbb{P}^1$ be Belyi maps of degree d. ϕ and ϕ' are **isomorphic** (respectively **lax isomorphic**) if the diagrams



commute where $\beta(\{0,1,\infty\}) = \{0,1,\infty\}.$

Permutation Triples

A transitive permutation triple of degree d is a triple

$$\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$$

such that

- $\sigma_{\infty}\sigma_{1}\sigma_{0}=1$
- σ generates a transitive subgroup of S_d

Permutation Triples

A transitive permutation triple of degree d is a triple

$$\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$$

such that

- $\sigma_{\infty}\sigma_{1}\sigma_{0}=1$
- lacksquare σ generates a transitive subgroup of S_d

The set of degree d Belyi maps up to isomorphism is in bijection with the set of degree d transitive permutation triples up to **simultaneous conjugation** and the group $\langle \sigma \rangle$ is the monodromy group of ϕ .

Passports

A passport \mathcal{P} consists of the data (g, G, λ) 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 triple of partitions of d.

Passports

A **passport** \mathcal{P} consists of the data (g, G, λ) 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 triple of partitions of d.

The passport of a Belyi map $\phi: X \to \mathbb{P}^1$ is $(g(X), \mathsf{Mon}(\phi), (\lambda_0, \lambda_1, \lambda_\infty))$ with g(X) the genus of X, $\mathsf{Mon}(\phi)$ the monodromy group of ϕ , and the partitions specified by ramification.

Passports

A **passport** \mathcal{P} consists of the data (g, G, λ) 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 triple of partitions of d.

The passport of a Belyi map $\phi: X \to \mathbb{P}^1$ is $(g(X), \operatorname{Mon}(\phi), (\lambda_0, \lambda_1, \lambda_\infty))$ with g(X) the genus of X, $\operatorname{Mon}(\phi)$ the monodromy group of ϕ , and the partitions specified by ramification.

The passport of a permutation triple σ is $(g(\sigma), \langle \sigma \rangle, \lambda(\sigma))$ where

$$g(\sigma) = 1 - d + (e(\sigma_0) - e(\sigma_1) - e(\sigma_\infty))/2$$

with

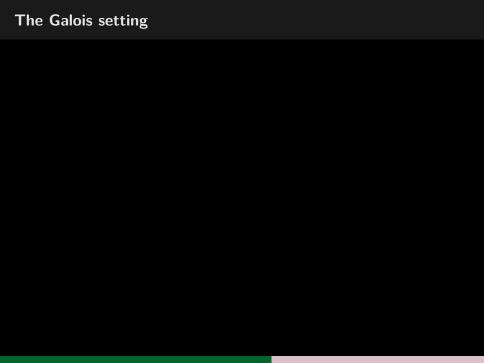
$$e(\tau) = d - \#$$
cycles of τ ,

and $\lambda(\sigma)$ is specified by cycle structures.

Function fields

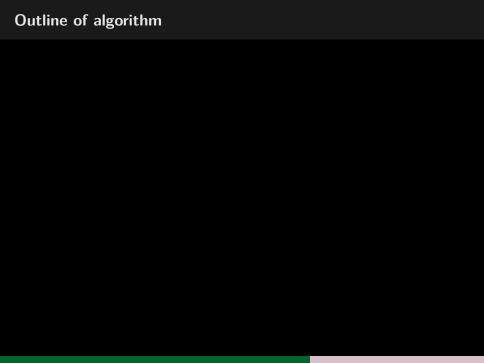
Let $\phi \colon X \to \mathbb{P}^1$ be a Belyi map







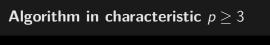
General idea



Results

Computing equations







Results

A refined conjecture





Examples

Notation

4T1-4,1,4-g0

An

4T1-4,1,4-g0

Backup slides