Toroidal Belyĭ Pairs and Their Monodromy Groups

Ivan Gonzalez[1] Dionel Jaime[2] Caitlin Lienkaemper[3]
Gabriel Ngwe[4] Baiming Qiao[5]

Florida International University [1], University of Rochester [2], Harvey Mudd College [3], Williams College [4], Purdue University [5],
Purdue Research in Mathematics Experience 2016

July 31, 2016

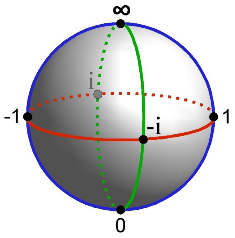
Motivation for Project

- Throughout the entire summer, our overall goal was to study the embeddings of particular graphs on the torus
- We split into two projects:
- Project 1: Find Belyĭ pairs and create a database of them
- Project 2: Investigate the monodromy groups of Belyĭ pairs

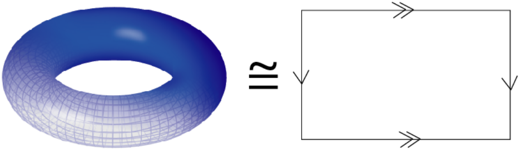
Spaces

The Riemann Sphere $\mathbb{P}^1(\mathbb{C})$.

$\mathbb{C} \cup \{\infty\}$

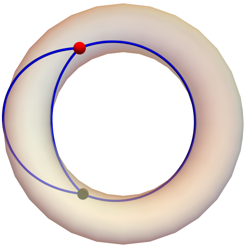


The Torus



Toroidal Graphs

- Planar graphs are those that can be drawn on the plane without edge crossings
- Toroidal graphs are those that can be drawn on the torus without edge crossings.
- It turns out that there do exists non-planar graphs that can be drawn on the Torus without crossings.



Example

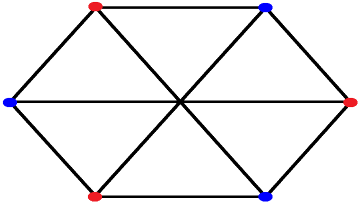


Figure: $K_{3,3}$

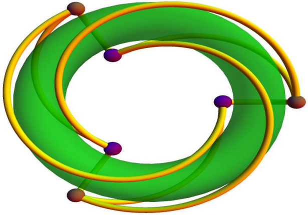


Figure: $K_{3,3}$ embedded on a torus

Elliptic Curves

- Assuming each $a_i \in \mathbb{C}$, consider a curve of the form
$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$
- A linear change of variables allows us to get this curve in the form
$$y^2 = x^3 + Ax + B.$$

Elliptic Curves

- Assuming each $a_i \in \mathbb{C}$, consider a curve of the form

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6.$$

- A linear change of variables allows us to get this curve in the form

$$y^2 = x^3 + Ax + B.$$

- This curve is said to be non-singular if

$$4A^3 + 27B^2 \neq 0.$$

Elliptic Curves

- Assuming each $a_i \in \mathbb{C}$, consider a curve of the form
$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$
- A linear change of variables allows us to get this curve in the form
$$y^2 = x^3 + Ax + B.$$
- This curve is said to be non-singular if
$$4A^3 + 27B^2 \neq 0.$$
- A non-singular curve of this form can be shown to have existing tangent lines at all points.

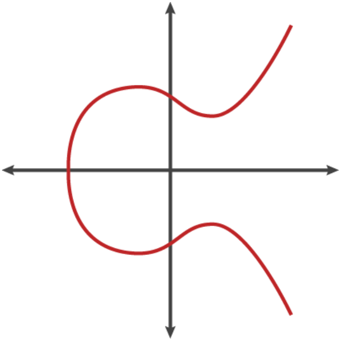
Elliptic Curves

Definition. *An elliptic curve is a non-singular, cubic curve of the form*

$$y^2 = x^3 + Ax + B$$

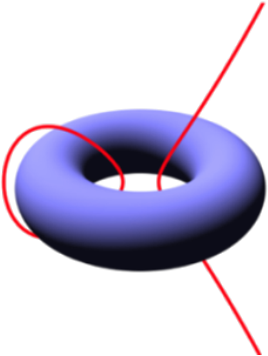
with a j-invariant

$$j(E) = \frac{6912A^3}{4A^3 + 27B^2}.$$



Elliptic Curves and the Torus

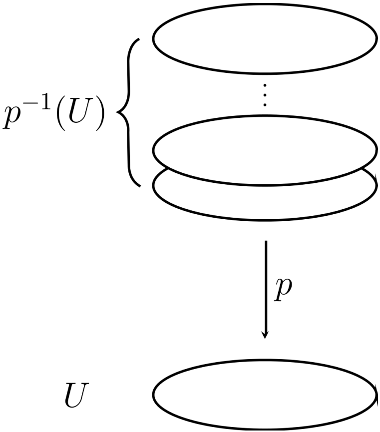
- Theorem: There exists a bijection between the points on an elliptic curve and the set of points on a torus.
- This is a classic result and can be seen via elliptic logarithms.



Covering Spaces

Definition (covering space)

Let X be a topological space. A covering space of X consists of a topological space $\tilde{X}$ and a map $p : \tilde{X} \to X$ such that for each $x \in X$, there exists an open neighborhood U of x such that $p^{-1}(U)$ is the disjoint union of open sets, each of which is mapped homeomorphically onto U by p.



Notions of Degree

Definition. *The degree d of a covering $p : X \to Y$ is the number of points in X in the preimage of a point in Y, that is, $d = |p^{-1}(y)|$. It turns out that this is the same for all points.*

Notions of Degree

Definition. *The degree d of a covering $p : X \to Y$ is the number of points in X in the preimage of a point in Y, that is, $d = |p^{-1}(y)|$. It turns out that this is the same for all points.*

Definition. *If $p(x, y)$ is a rational function on an elliptic curve, that is, a quotient of two relatively prime bivariate polynomials, $p(x, y) = \frac{r(x,y)}{q(x,y)}$, we say $deg(p) = N$ if $|p^{-1}(\omega)| = N$ for all but finitely many ω.*

- This means that if $p : X \to Y$ is both a covering map and a rational map, where $X = E(\mathbb{C}) \setminus A$ (where A is finite), its degree as a rational map and as a cover coincide.

Belyĭ Maps

Definition. *Given a rational function* $f(x, y)$ *with degree* N*, we say that* ω *is a critical value if* $|f^{-1}(\omega)| < N$.

Belyĭ Maps

Definition. *Given a rational function* $f(x, y)$ *with degree* N, *we say that* ω *is a critical value if* $|f^{-1}(\omega)| < N$.

Definition. *A rational function* $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ *is called a Belyĭ map if there are no critical values other than* $0, 1,$ *and* ∞.

Belyĭ Maps

Definition. *Given a rational function $f(x, y)$ with degree N, we say that ω is a critical value if $|f^{-1}(\omega)| < N$.*

Definition. *A rational function $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is called a Belyĭ map if there are no critical values other than $0, 1,$ and ∞.*

Theorem. *Given an elliptic curve E defined over the algebraic numbers, there exists a Belyĭ map $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$.*

- β acts as a cover on $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$
- A Belyĭ map associated with its particular elliptic curve is called a Belyĭ pair.

Example of a Belyĭ Pair

An example of a Belyĭ pair is

$$y^2 = x^3 + 1, \quad \beta(x, y) = -x^3.$$

Example of a Belyĭ Pair

An example of a Belyĭ pair is

$$y^2 = x^3 + 1, \quad \beta(x, y) = -x^3.$$

- $\beta^{-1}(-1) = \{(\zeta_3, \pm\sqrt{2}), (\zeta_3^2, \pm\sqrt{2}), (1, \pm\sqrt{2})\}$.
- β has degree 6.

Example of a Belyĭ Pair

An example of a Belyĭ pair is

$$y^2 = x^3 + 1, \quad \beta(x,y) = -x^3.$$

- $\beta^{-1}(-1) = \{(\zeta_3, \pm\sqrt{2}), (\zeta_3^2, \pm\sqrt{2}), (1, \pm\sqrt{2})\}$.
- β has degree 6.
- $\beta^{-1}(0) = \{(0,1), (0,-1)\}$.

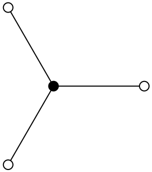
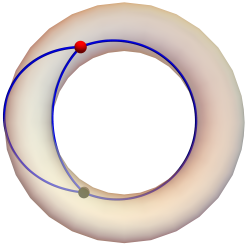
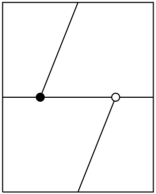
Example of a Belyĭ Pair

An example of a Belyĭ pair is

$$y^2 = x^3 + 1, \quad \beta(x, y) = -x^3.$$

- $\beta^{-1}(-1) = \{(\zeta_3, \pm\sqrt{2}), (\zeta_3^2, \pm\sqrt{2}), (1, \pm\sqrt{2})\}$.
- β has degree 6.
- $\beta^{-1}(0) = \{(0, 1), (0, -1)\}$.
- $\beta^{-1}(1) = \{(-\zeta_3, 0), (-\zeta_3^2, 0), (-1, 0)\}$ where $\zeta_3 \neq 1$ is a $3rd$ root of unity.

Dessins d'Enfants

- A Dessin d'Enfant is a connected bipartite graph Γ embedded in an oriented compact surface X, such that $X \setminus \Gamma$ is a disjoint union of 2-dimensional cells. Those cells are called faces. We adopt the convention of representing the bipartite structure by black and white colorings.
-   
- Dessins can also be seen as arising from Belyĭ maps

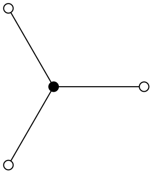
Dessins From Belyĭ Maps

Belyĭ maps give rise to Dessins d'Enfants

- Let $\beta^{-1}(0) =$ Black Vertices
- Let $\beta^{-1}(1) =$ White Vertices
- Let $\beta^{-1}([0, 1]) =$ Edges
- Let $\beta^{-1}(\infty) =$ Midpoints of Faces

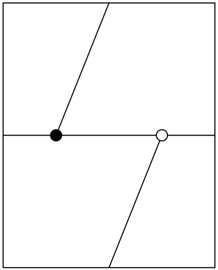
Example 1

- $\beta : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C}), \quad \beta(x) = x^3$
- $\beta^{-1}(0) = \{0\}$, $\beta^{-1}(1) = \{1, \zeta_3, \zeta_3^2\}$, $\beta^{-1}(\infty) = \{\infty\}$.
- The corresponding Dessin d'Enfant is



Example 2

- $E : y^2 = x^3 + 1$ and $\beta(x, y) = \frac{y+1}{2}$
- Its Dessin d'Enfant is given by

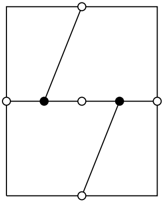


Degree Sequences of a Dessin

- Let Γ be a dessin. Its degree sequence $\mathcal{D}$ is defined to be the multiset $\{B, W, F\}$, where B, W and F are sets of numbers, defined as follows:
  - B $= \{e_b |$b is a black vertex, and e_b is the number of edges adjacent to it$\}$
  - W $= \{e_w |$w is a white vertex, and e_w is the number of edges adjacent to it$\}$
  - F $= \{e_f |$f is a face, and e_f is the number of white vertices adjacent to it$\}$
- The degree sequence of the Belyĭ map is defined to be the degree sequence of the associated dessin.
- The degree sequence can also be defined purely in terms of the Belyĭ map.

Example

- Consider the Belyĭ pair, $E : y^2 = x^3 + 1$ and $\beta(x, y) = -x^3$.
- The corresponding dessin is



- We have that
  - $\beta^{-1}(0) = \{(0, 1), (0, -1)\}$.
  - $\beta^{-1}(1) = \{(-\zeta_3, 0), (-\zeta_3^2, 0), (-1, 0)\}$ where $\zeta_3 \neq 1$ is a $3rd$ root of unity.
- Its degree sequence is $\mathcal{D} = \{\{3, 3\}, \{2, 2, 2\}, \{6\}\}$.

Degree Sequences

- The degree sequence of a Belyĭ map always satisfies

$$\sum_{b \in B} e_b = \sum_{w \in W} e_w = \sum_{f \in F} e_f = |B| + |W| + |F| = deg(\beta)$$

Degree Sequences

- The degree sequence of a Belyĭ map always satisfies

$$\sum_{b\in B} e_b = \sum_{w\in W} e_w = \sum_{f\in F} e_f = |B| + |W| + |F| = deg(\beta)$$

- Note that $\sum_{b\in B} e_b = \sum_{w\in W} e_w = \sum_{f\in F} e_f = deg(\beta)$ is a direct consequence of the degree sum formula or the Fundamental Theorem of Algebra.

Degree Sequences

- The degree sequence of a Belyĭ map always satisfies

$$\sum_{b\in B} e_b = \sum_{w\in W} e_w = \sum_{f\in F} e_f = |B| + |W| + |F| = deg(\beta)$$

- Note that $\sum_{b\in B} e_b = \sum_{w\in W} e_w = \sum_{f\in F} e_f = deg(\beta)$ is a direct consequence of the degree sum formula or the Fundamental Theorem of Algebra.
- $|B| + |W| + |F| = deg(\beta)$ follows from the fact that Euler characteristic of torus is 0:

$$2\,g_E - 2 = \deg\beta\,\left(2g_{\mathbb{P}^1} - 2\right) + \sum_{P\in E(\mathbb{C})} \left(e_P - 1\right)$$

Degree Sequences

Question. For any given $N \in \mathbb{N}$, suppose we have sets $\mathcal{D} = \left\{B, W, F\right\}$ satisfying

$$\sum_{b \in B} b = \sum_{w \in W} w = \sum_{f \in F} f = |B| + |W| + |F| = N.$$

When is $\mathcal{D}$ the degree sequence of a Belyĭ pair with Belyĭ map having degree N?

Degree Sequences

Answer (Hurwitz, 1891). The precise conditions for when this occurs are given as follows:

1. There exist $\sigma_0, \sigma_1, \sigma_\infty \in S_N$ with cycle types B, W, and F respectively for which $\sigma_0 \circ \sigma_1 \circ \sigma_\infty = 1$.
2. The group $G = \langle \sigma_0, \sigma_1, \sigma_\infty \rangle$ is a transitive subgroup of S_N.

Thus, for any $N \in \mathbb{N}$, to find Belyĭ maps of degree N, we use the above theorem to find all possible degree sequences.

Example

Consider the degree sequence $\mathcal{D} = \{\{3\},\{3\},\{3\}\}$. This corresponds to some Belyĭ pair (E, β) because, by choosing

$$\sigma_0 = (123)$$
$$\sigma_1 = (123)$$
$$\sigma_\infty = (123)$$

we obtain $\sigma_0 \circ \sigma_1 \circ \sigma_\infty = 1$. Moreover, $G = \langle \sigma_0, \sigma_1, \sigma_\infty \rangle$ is the cyclic group of order 3, which is a transitive subgroup of S_3.

Motivation for Monodromy Groups

Recall Hurwitz's Theorem:

Theorem (Hurwitz, 1891). Fix $N \in \mathbb{N}$. Given a degree sequence $\mathcal{D} = \{B, W, F\}$ satisfying

$$\sum_{b \in B} b = \sum_{w \in W} w = \sum_{f \in F} f = |B| + |W| + |F| = N.$$

Then $\mathcal{D}$ is the degree sequence of some dessin on torus if and only if there exist three elements σ_0,σ_1, and σ_∞ in S_N, such that σ_0 has cycle type B, σ_1 has cycle type W, and σ_∞ has cycle type F, and they generate a transitive subgroup of S_N

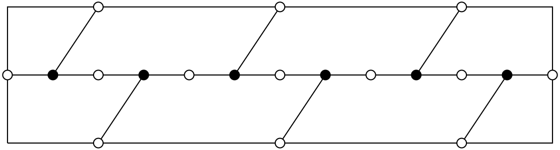
Infinite Families of Regular Dessins

- A Dessin d'Enfant is regular if the degree for all black (or, respectively, white) vertices are the same, and the degree for all faces are the same.
- The degree sequence of a regular dessin on the torus is always one of the following three types:

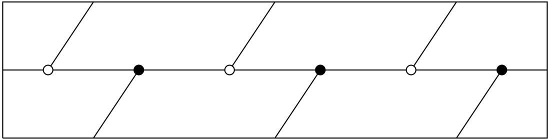
$$\mathcal{D}_{3,2,6}(n) = \{\{3, \underset{2n}{\ldots}, 3\}, \{2, \underset{3n}{\ldots}, 2\}, \{6, \underset{n}{\ldots}, 6\}\}$$
$$\mathcal{D}_{4,2,4}(n) = \{\{4, \underset{n}{\ldots}, 4\}, \{2, \underset{2n}{\ldots}, 2\}, \{4, \underset{n}{\ldots}, 4\}\}$$
$$\mathcal{D}_{3,3,3}(n) = \{\{3, \underset{n}{\ldots}, 3\}, \{3, \underset{n}{\ldots}, 3\}, \{3, \underset{n}{\ldots}, 3\}\}$$

Infinite Families of Regular Dessins

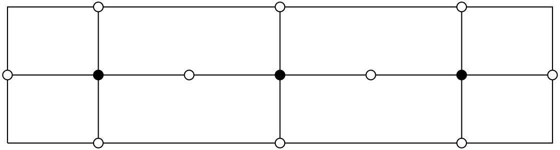
$\mathcal{D}_{2,3,6}(3)$:



$\mathcal{D}_{3,3,3}(3)$:



$\mathcal{D}_{4,2,4}(3)$:



Monodromy Group of a covering space

- Let $p : X \to Y$ be a covering map of degree d. Fixing a point $y \in Y$, we can define an action of $\pi_1(Y, y)$ on the set $p^{-1}(y)$ as follows:

Monodromy Group of a covering space

- Let $p : X \to Y$ be a covering map of degree d. Fixing a point $y \in Y$, we can define an action of $\pi_1(Y, y)$ on the set $p^{-1}(y)$ as follows:
- Let $x_1, x_2, \dots x_d$ be points above y and $\gamma \in \pi_1(Y, y)$ be a loop. By the unique lifting property of covering space, there is a unique path γ_i starts at each x_i that lifts γ. Let $x_{\sigma(i)}$ be the end point of γ_i. It must be a point above y. Then $i \to \sigma(i)$ is a permutation of the $x_i's$. This gives an action of $\pi_1(Y, y)$ on the points of the preimage of y.

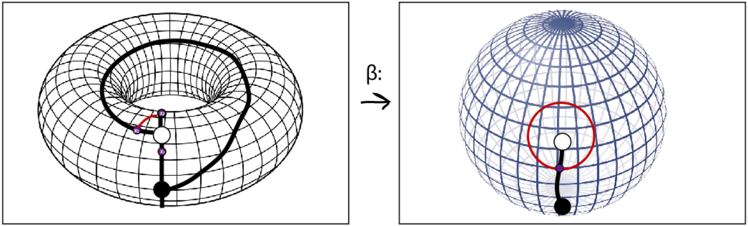
Monodromy Group of a covering space

- Let $p : X \to Y$ be a covering map of degree d. Fixing a point $y \in Y$, we can define an action of $\pi_1(Y, y)$ on the set $p^{-1}(y)$ as follows:
- Let $x_1, x_2, \dots x_d$ be points above y and $\gamma \in \pi_1(Y, y)$ be a loop. By the unique lifting property of covering space, there is a unique path γ_i starts at each x_i that lifts γ. Let $x_{\sigma(i)}$ be the end point of γ_i. It must be a point above y. Then $i \to \sigma(i)$ is a permutation of the $x_i's$. This gives an action of $\pi_1(Y, y)$ on the points of the preimage of y.
- This action is called monodromy action. This action is equivalent to a group homomorphism $\alpha : \pi_1(Y, y) \to S_d$. The image of α is called monodromy group.

Monodromy Group of a covering space

- Let $p : X \to Y$ be a covering map of degree d. Fixing a point $y \in Y$, we can define an action of $\pi_1(Y, y)$ on the set $p^{-1}(y)$ as follows:
- Let $x_1, x_2, \dots x_d$ be points above y and $\gamma \in \pi_1(Y, y)$ be a loop. By the unique lifting property of covering space, there is a unique path γ_i starts at each x_i that lifts γ. Let $x_{\sigma(i)}$ be the end point of γ_i. It must be a point above y. Then $i \to \sigma(i)$ is a permutation of the $x_i's$. This gives an action of $\pi_1(Y, y)$ on the points of the preimage of y.
- This action is called monodromy action. This action is equivalent to a group homomorphism $\alpha : \pi_1(Y, y) \to S_d$. The image of α is called monodromy group.
- $\operatorname{im} \alpha$ is a transitive subgroup of S_d

Here, the torus is a acting as a covering space of $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ under the covering map β, with $\beta(x_1) = \beta(x_2) = \beta(x_3) = y$.



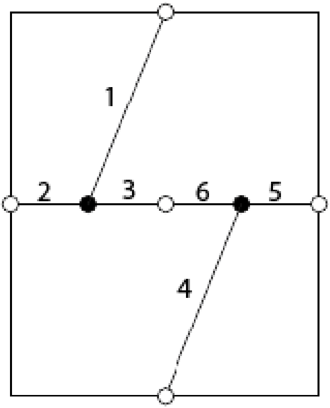
The monodromy group of this covering is $Z_3 \subset S_3$.

Monodromy groups and dessins

- Belyĭ maps are covering maps of $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$
- The fundamental group $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\})$ is generated by σ_0, a small loop goes around 0, and σ_1, a small loop that goes around 1, with no other relations. Let σ_∞ be the elements satisfies $\sigma_0\sigma_1\sigma_\infty = 1$.
- Let $\mathcal{D} = \{B, W, F\}$ be a degree sequence associated with some dessin D on an elliptic curve E.
- Let $\alpha : \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}) \to S_n$ be the monodromy map, then $\alpha(\sigma_0)$,$\alpha(\sigma_1)$ and $\alpha(\sigma_\infty)$ will have cycle type B,W and F respectively.

Computing Monodromy groups

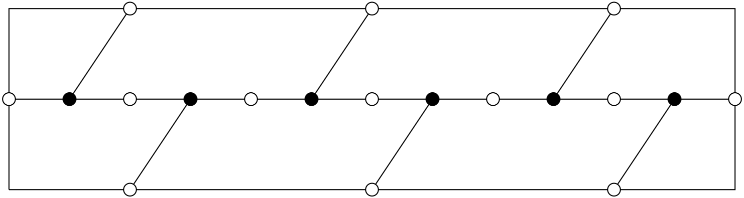
- $\alpha(\sigma_0)$ is the product of cycles given by listing the edges we meet in a counterclockwise loop around the black vertices
- Likewise, $\alpha(\sigma_1)$ comes from counterclockwise loops around the white vertices
- The degree sequence $\mathcal{D} = \{\{3,3\},\{2,2,2\},\{6\}\}$
- $\alpha(\sigma_0) = (123)(645)$
  $\alpha(\sigma_1) = (25)(14)(36)$
  $\alpha(\sigma_\infty) = (162435)$



Theorem

The dessin in our infinite family with degree sequence $\mathcal{D}_{2,3,6}(n)$ has monodromy group $G_n \cong (Z_n \times Z_n) \rtimes Z_6$

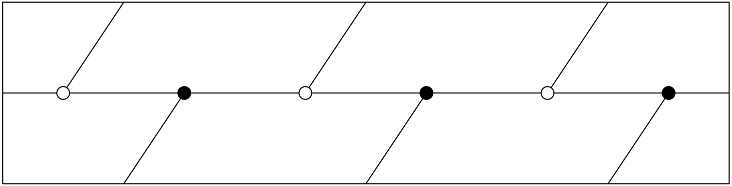
- $\mathcal{D}_{2,3,6}(n) = \{\{\underbrace{3,\ldots,3}_{2n}\}, \{\underbrace{2,\ldots,2}_{3n}\}, \{\underbrace{6,\ldots,6}_{n}\}\}$



Theorem

The dessin in our infinite family with degree sequence $\mathcal{D}_{3,3,3}(n)$ has monodromy group $G_n \cong (Z_n \times Z_n) \rtimes Z_3$

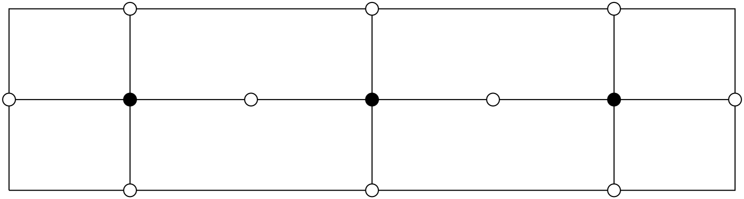
- $\mathcal{D}_{3,3,3}(n) = \{\{\underbrace{3, \ldots, 3}_{n}\}, \{\underbrace{3, \ldots, 3}_{n}\}, \{\underbrace{3, \ldots, 3}_{n}\}\}$



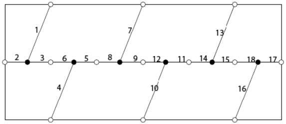
Theorem

The dessin in our infinite family with degree sequence $\mathcal{D}_{4,2,4}(n)$ has monodromy group $G_n \cong (Z_n \times Z_n) \rtimes Z_4$

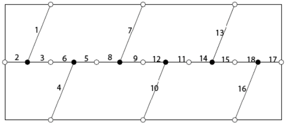
- $\mathcal{D}_{4,2,4}(n) = \{\underbrace{\{4, \ldots, 4\}}_{n}, \underbrace{\{2, \ldots, 2\}}_{2n}, \underbrace{\{4, \ldots, 4\}}_{n}\}$



Proof in $D_{(2,3,6)}(n)$ case:

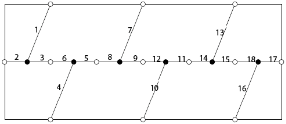
- For any n, we can algorithmically write down σ_0, σ_1, and σ_∞.
- 

Proof in $D_{(2,3,6)}(n)$ case:

- For any n, we can algorithmically write down σ_0, σ_1, and σ_∞.
- 

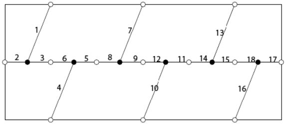
- Let c_i be the cycle permuting the elements of $\{1, \ldots, 6n\}$ which are equivalent to i mod 6. For instance, $c_2 = (2, 8, \ldots, 6n+2)$.

Proof in $D_{(2,3,6)}(n)$ case:

- For any n, we can algorithmically write down σ_0, σ_1, and σ_∞.
- 

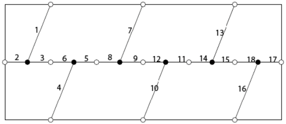
- Let c_i be the cycle permuting the elements of $\{1, \ldots, 6n\}$ which are equivalent to i mod 6. For instance, $c_2 = (2, 8, \ldots, 6n + 2)$.
- $\beta = \sigma_\infty = \sigma_1^{-1}\sigma_0^{-1}$, $|\beta| = 6$

Proof in $D_{(2,3,6)}(n)$ case:

- For any n, we can algorithmically write down σ_0, σ_1, and σ_∞.
- 

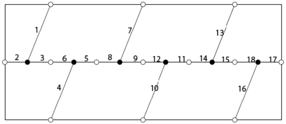
- Let c_i be the cycle permuting the elements of $\{1, \ldots, 6n\}$ which are equivalent to i mod 6. For instance, $c_2 = (2, 8, \ldots, 6n + 2)$.
- $\beta = \sigma_\infty = \sigma_1^{-1}\sigma_0^{-1}$, $|\beta| = 6$
- $\gamma = \sigma_1\sigma_0\sigma_1^{-1}\sigma_0^{-1} = c_2c_3^{-1}c_5^{-1}c_6$, $|\gamma| = n$

Proof in $D_{(2,3,6)}(n)$ case:

- For any n, we can algorithmically write down σ_0, σ_1, and σ_∞.
- 

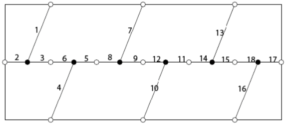
- Let c_i be the cycle permuting the elements of $\{1, \ldots, 6n\}$ which are equivalent to i mod 6. For instance, $c_2 = (2, 8, \ldots, 6n+2)$.
- $\beta = \sigma_\infty = \sigma_1^{-1}\sigma_0^{-1}, \ |\beta| = 6$
- $\gamma = \sigma_1\sigma_0\sigma_1^{-1}\sigma_0^{-1} = c_2c_3^{-1}c_5^{-1}c_6, \ |\gamma| = n$
- $\delta = \sigma_0^{-1}\sigma_1^{-1}\sigma_0\sigma_1 = c_1c_2^{-1}c_4^{-1}c_5, \ |\delta| = n.$

Proof in $D_{(2,3,6)}(n)$ case:

- For any n, we can algorithmically write down σ_0, σ_1, and σ_∞.
- 

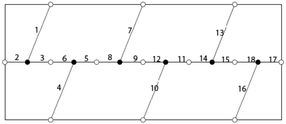
- Let c_i be the cycle permuting the elements of $\{1, \ldots, 6n\}$ which are equivalent to i mod 6. For instance, $c_2 = (2, 8, \ldots, 6n + 2)$.
- $\beta = \sigma_\infty = \sigma_1^{-1}\sigma_0^{-1}$, $|\beta| = 6$
- $\gamma = \sigma_1\sigma_0\sigma_1^{-1}\sigma_0^{-1} = c_2 c_3^{-1} c_5^{-1} c_6$, $|\gamma| = n$
- $\delta = \sigma_0^{-1}\sigma_1^{-1}\sigma_0\sigma_1 = c_1 c_2^{-1} c_4^{-1} c_5$, $|\delta| = n$.
- γ and δ commute, thus $\langle\gamma, \delta\rangle = \langle\gamma\rangle \times \langle\delta\rangle$.

Proof in $D_{(2,3,6)}(n)$ case:

- For any n, we can algorithmically write down σ_0, σ_1, and σ_∞.
- 

- Let c_i be the cycle permuting the elements of $\{1, \ldots, 6n\}$ which are equivalent to i mod 6. For instance, $c_2 = (2, 8, \ldots, 6n+2)$.
- $\beta = \sigma_\infty = \sigma_1^{-1}\sigma_0^{-1}$, $|\beta| = 6$
- $\gamma = \sigma_1\sigma_0\sigma_1^{-1}\sigma_0^{-1} = c_2 c_3^{-1} c_5^{-1} c_6$, $|\gamma| = n$
- $\delta = \sigma_0^{-1}\sigma_1^{-1}\sigma_0\sigma_1 = c_1 c_2^{-1} c_4^{-1} c_5$, $|\delta| = n$.
- γ and δ commute, thus $\langle\gamma, \delta\rangle = \langle\gamma\rangle \times \langle\delta\rangle$.
- $\langle\gamma, \delta\rangle \lhd \langle\beta, \gamma, \delta\rangle$

Proof in $D_{(2,3,6)}(n)$ case:

- For any n, we can algorithmically write down σ_0, σ_1, and σ_∞.
- 

- Let c_i be the cycle permuting the elements of $\{1, \ldots, 6n\}$ which are equivalent to i mod 6. For instance, $c_2 = (2, 8, \ldots, 6n + 2)$.
- $\beta = \sigma_\infty = \sigma_1^{-1}\sigma_0^{-1}$, $|\beta| = 6$
- $\gamma = \sigma_1\sigma_0\sigma_1^{-1}\sigma_0^{-1} = c_2 c_3^{-1} c_5^{-1} c_6$, $|\gamma| = n$
- $\delta = \sigma_0^{-1}\sigma_1^{-1}\sigma_0\sigma_1 = c_1 c_2^{-1} c_4^{-1} c_5$, $|\delta| = n$.
- γ and δ commute, thus $\langle\gamma, \delta\rangle = \langle\gamma\rangle \times \langle\delta\rangle$.
- $\langle\gamma, \delta\rangle \triangleleft \langle\beta, \gamma, \delta\rangle$
- $\langle\gamma, \delta, \beta\rangle = G_n$, since $\sigma_0, \sigma_1 \in \langle\gamma, \delta, \beta\rangle$.

Database of Belyĭ Pairs and Monodromy Groups

Having defined all the necessary terminology, the database of Belyĭ pairs will consist of

- Natural numbers $N \in \mathbb{N}$.
- All Belyĭ pairs of degree N.
- For each Belyĭ pair, its corresponding Dessin d'Enfant, degree sequence, and monodromy group.

Why should such a database exist?

Theorem (Zapponi, 2009). Fix $N \in \mathbb{N}$. Then there are finitely many j-invariants such that there exists a Belyĭ pair (E, β) with $\deg(\beta) \leq N$.

Corollary. For a given $N \in \mathbb{N}$, there exists only finitely many Belyĭ pairs (E, β) with $\deg(\beta) = N$, up to automorphism of the elliptic curve.

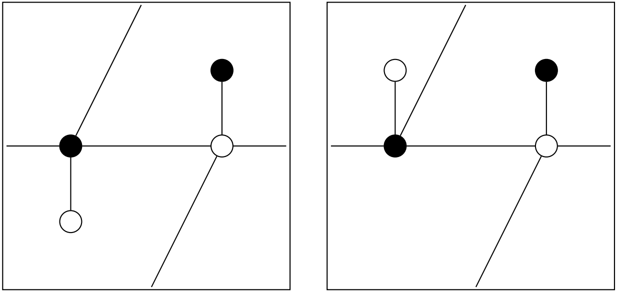
Compiling the Database

- We begin with a positive integer N.
- We find all degree sequences for degree N.
- For each degree sequence, we set up a system of polynomial equations to find Belyĭ pairs which will have the corresponding degree sequence.

Current State of Database

- We have all Belyĭ pairs up to degree 4, as well as the majority of degree 5 Belyĭ pairs.
- There are no Belyĭ pairs of degree ≤ 2.
- There is one Belyĭ pair of degree 3, two of degree 4, and 5 Belyĭ pairs of degree 5.
- We have all degree sequences and their monodromy groups up to degree 8.

Dessins of With Degree Sequence $\{\{4,1\},\{4,1\},\{5\}\}$.



The dessin to the left has monodromy group S_5, the dessin to the right has the holomorph of $\mathbb{Z}_5$ as its monodromy group.

What's next?

- Find all degree 6 Belyĭ pairs.
- We expect there to be no fewer than 30 Belyĭ pairs of degree 6.
- Find an efficient method of obtaining Belyĭ pairs.
- Compute monodromy groups from Belyĭ pairs

Acknowledgments

We would like to thank:

- National Science Foundation
- Purdue University - College of Science
- Dr. Edray Goins
- Mark Pengitore

Questions?