Conjugacy problems in braid groups and other Garside groups

Part II

Juan González-Meneses

Universidad de Sevilla

Problèmes algorithmiques liés aux tresses et à la topologie de basse dimension

GDR Tresses et topologie de basse dimension

Île de Berder, November 15-17, 2006.

Bounding the size of USS

Braid group B_n

In random examples of big canonical length, ***all of them*** satisfy:

$$\#(USS(X)) = 2\,\ell(X)$$

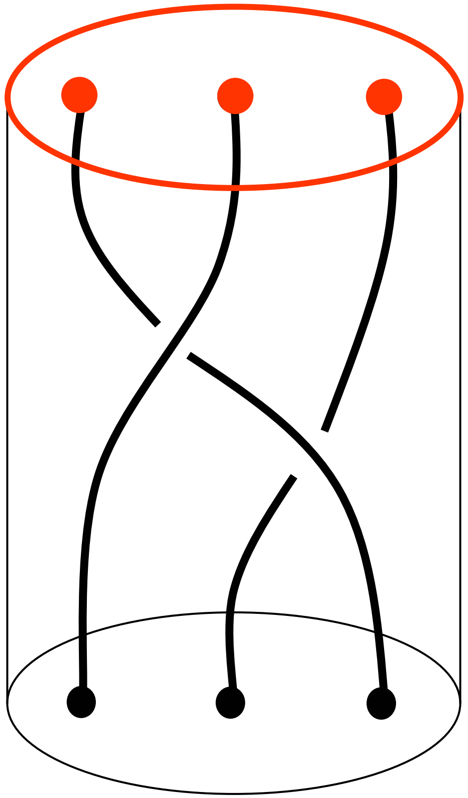
Gebhardt: This happens for n=3,...,8 and $\ell(X) \geq 20$.

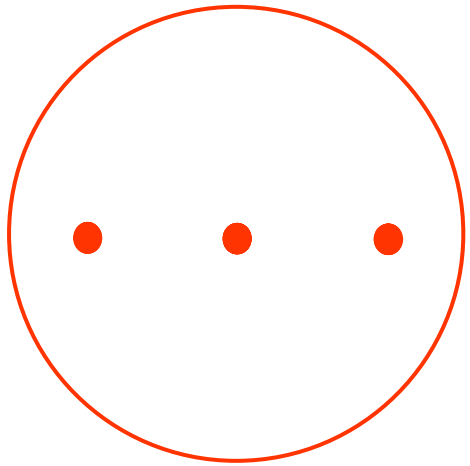
Remark:

All these examples are **pseudo-Anosov** and **rigid.**

Nielsen-Thurston classification

Braids in B_n can be seen as automorphisms of the n-times puncturted disc

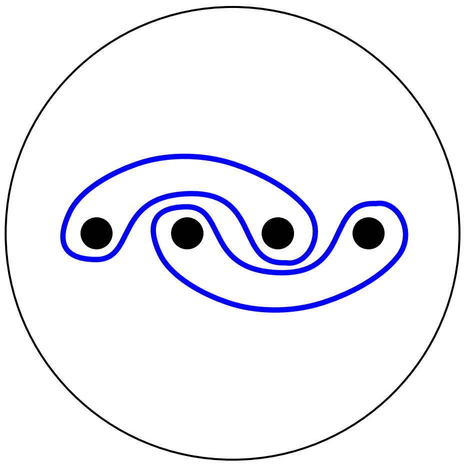




Nielsen-Thurston classification

Periodic Braids **=** Roots of Δ^{2m}, for some $\boldsymbol{m}$ **=** $\{\alpha : \quad \alpha^k = \Delta^{2m}\}$

Reducible Braids **=** Preserve a family of disjoint, closed curves

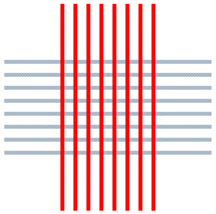


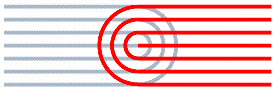
Nielsen-Thurston classification

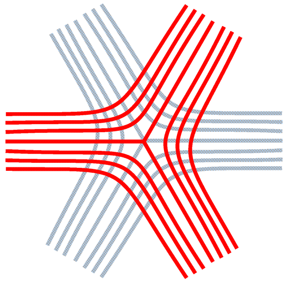
Periodic Braids **=** Roots of Δ^{2m}, for some $\boldsymbol{m}$ **=** $\{\alpha : \quad \alpha^k = \Delta^{2m}\}$

Reducible Braids **=** Preserve a family of disjoint, closed curves

Pseudo-Anosov Braids **=** Preserve two transverse measured foliations…





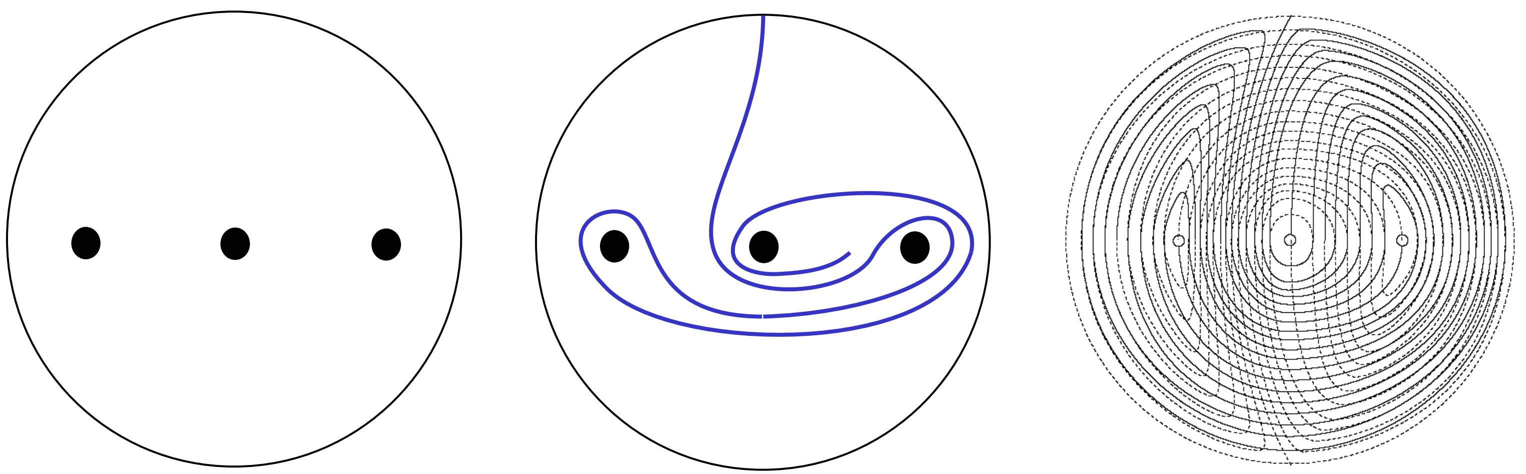


…scaling the measure of $\mathcal{F}^u$ by $\lambda > 1$

and the measure of $\mathcal{F}^s$ by λ^{-1}

Nielsen-Thurston classification

Periodic Braids	=	Roots of Δ^{2m}, for some $\boldsymbol{m}$	=	$\{\alpha : \quad \alpha^k = \Delta^{2m}\}$
Reducible Braids	=	Preserve a family of disjoint, closed curves		
Pseudo-Anosov Braids	=	Preserve two transverse measured foliations…		

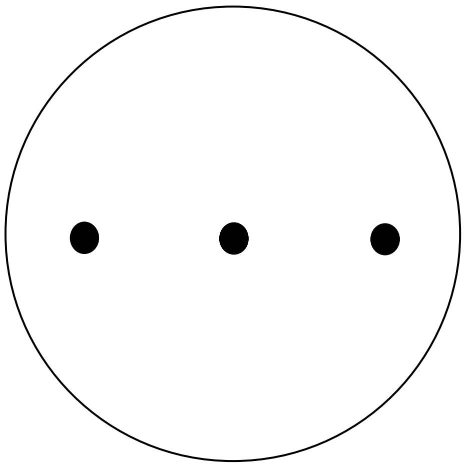


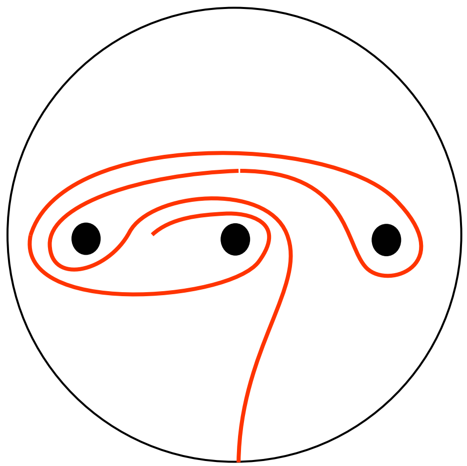
Nielsen-Thurston classification

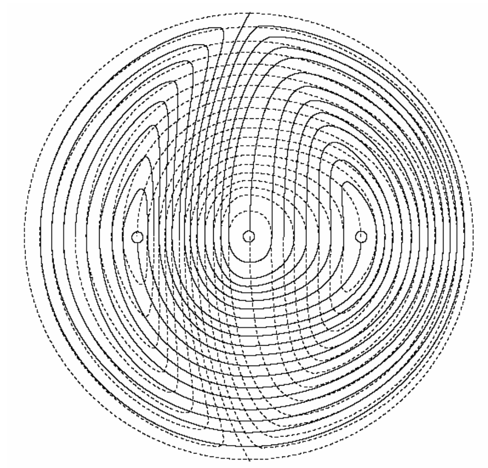
Periodic Braids = Roots of Δ^{2m}, for some $\boldsymbol{m}$ = $\{\alpha : \quad \alpha^k = \Delta^{2m}\}$

Reducible Braids = Preserve a family of disjoint, closed curves

Pseudo-Anosov Braids = Preserve two transverse measured foliations…







Properties of periodic braids

Bestvina (1999)

$$X \in USS(X) \quad \Rightarrow \quad \ell(X) = 1.$$

Birman-Gebhardt-GM (2006)

In general, #(USS(X)) is exponential in n.

Bessis-Digne-Michel (2002)

The centralizer of X is either B_n or the braid group of an annulus.

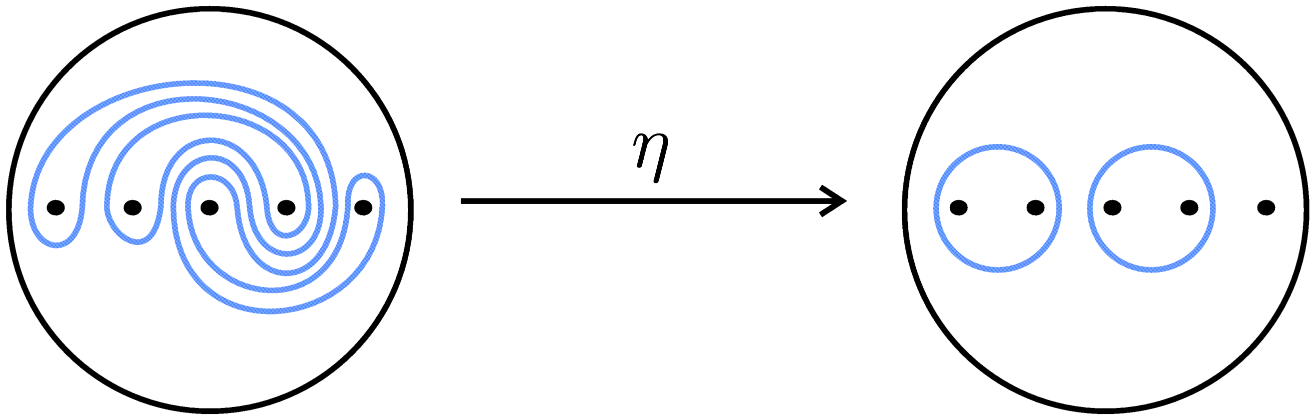
Properties of reducible braids

A reducible braid α preserves a family of curves, called a **reduction system**.

Birman-Lubotzky-McCarthy (1983)

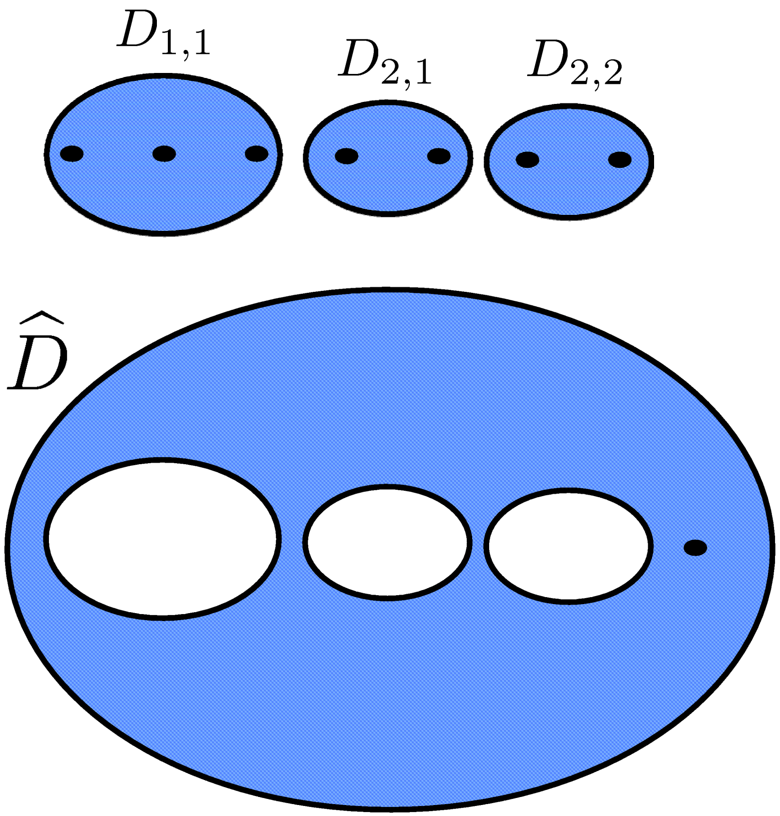
There is a **canonical reduction system** $\mathrm{CRS}(\alpha)$

It can always be simplified by an automorphism η (i.e., by a conjugation).



Properties of reducible braids

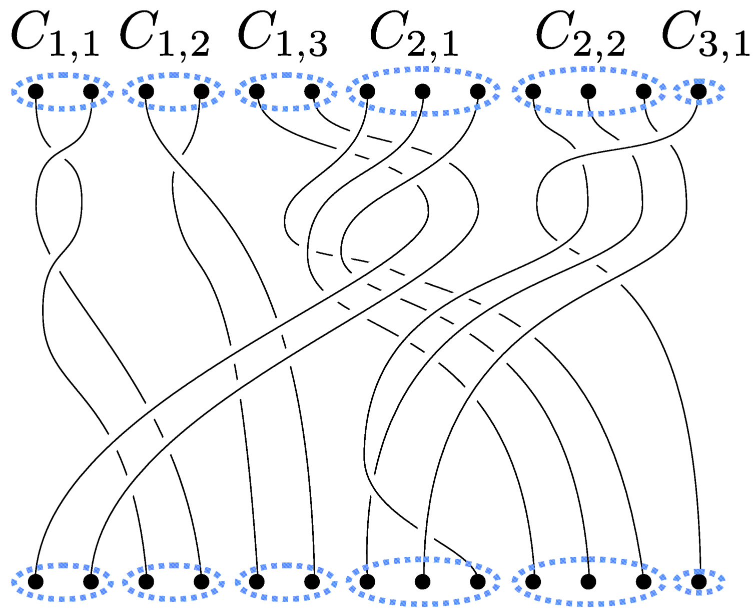
One can then decompose the disc D along $\mathrm{CRS}(\alpha)$.



Properties of reducible braids

Tubular braid: $\widehat{\alpha} \quad = \quad \alpha$ restricted to $\widehat{D}$.

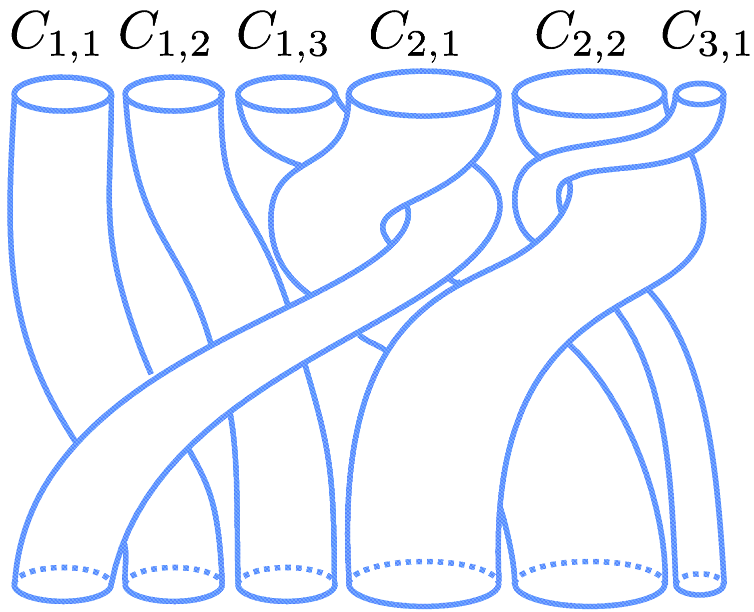
Interior braids: $\alpha_{i,j} \quad = \quad \alpha$ restricted to $D_{i,j}$.



Properties of reducible braids

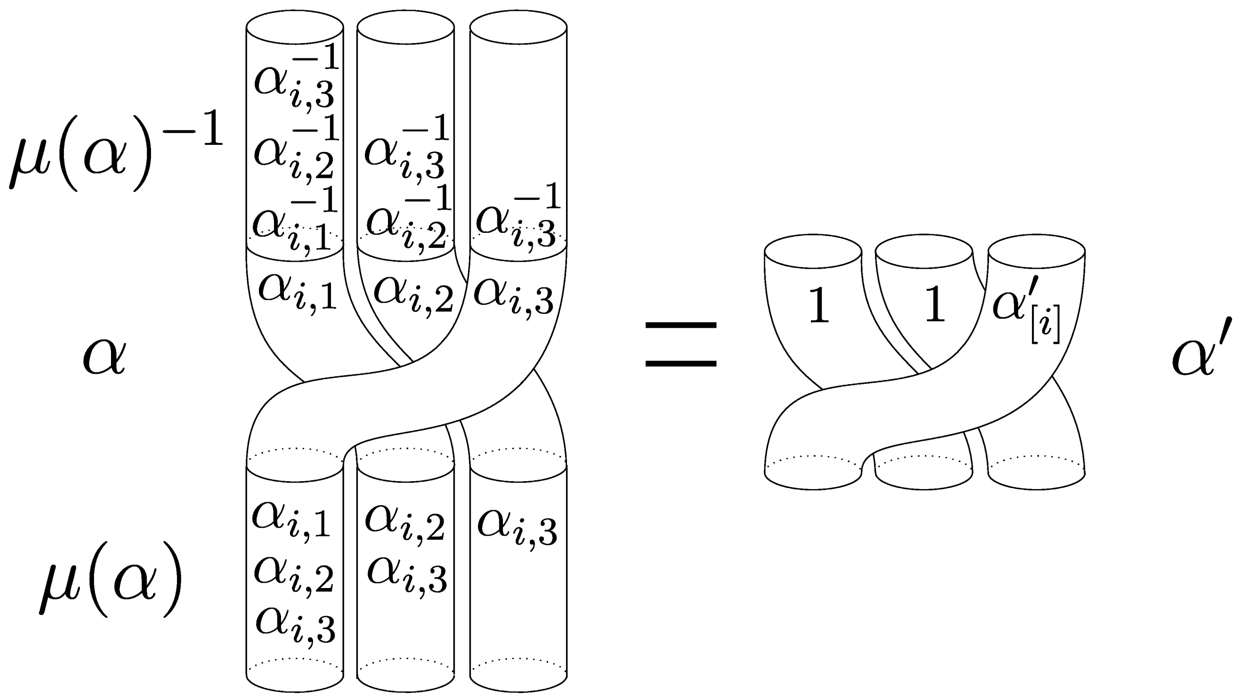
Tubular braid: $\widehat{\alpha} \quad = \quad \alpha$ restricted to $\widehat{D}$.

Interior braids: $\alpha_{i,j} \quad = \quad \alpha$ restricted to $D_{i,j}$.



Properties of reducible braids

We can simplify the interior braids of an orbit of tubes.



Properties of reducible braids

Hence, α can be decomposed into $\widehat{\alpha}$ and $\alpha_{[1]}, \ldots, \alpha_{[m]}$.

GM (2003):

Two reducible braids α and β are **conjugate** if and only if $\widehat{\alpha}$ and $\widehat{\beta}$ are conjugate by some element η such that: η sends the tubes of $\alpha_{[i]}$ to the tubes of $\beta_{[j]}$, which is conjugate to $\alpha_{[i]}$.

GM-Wiest (2004):

The centralizer of α is a semi-direct product determined by:

$$1 \to Z(\alpha_{[1]}) \times \cdots \times Z(\alpha_{[m]}) \to Z(\alpha) \to Z_0(\widehat{\alpha}) \to 1.$$

$Z_0(\widehat{\alpha}) \subset Z(\widehat{\alpha})$

Properties of pseudo-Anosov braids

A **generic** braid is always pseudo-Anosov (Not shown)

GM-Wiest (2004):

Its centralizer is isomorphic to $\mathbb{Z}^2$.

Birman- Gebhardt-GM (2006):

A small power of it is conjugate to a **rigid braid**. **???**

Using powers to detect conjugacy

GM (2003): The m-th root of a braid is unique up to conjugacy.
And if the braid is pseudo-Anosov, the root is unique.

Corollary 1: X and Y are conjugate if and only if so are X^m and Y^m.

We can solve the CDP by using powers.

Corollary 2: If X and Y are pseudo-Anosov, then the **conjugating elements** of (X, Y) and of (X^m, Y^m) coincide.

We can solve the CSP, **in the pseudo-Anosov case**, by using powers.

Rigid elements

In a Garside group:

$$X = \Delta^p X_1 X_2 \cdots X_r \ \text{ in left normal form.}$$

$$\mathbf{c}(X) = \Delta^p X_2 \cdots X_r \tau^{-p}(X_1).$$

X is **rigid** if $X_r \tau^{-p}(X_1)$ is left weighted as written.

$$\varphi(X)\ \iota(X)$$

In this case, cycling (& decycling) is just a cyclic permutation of the factors.

Hence $X \in \text{USS}(X)$, and its orbit under cycling has length either r or $2r$.

Easier combinatorics!

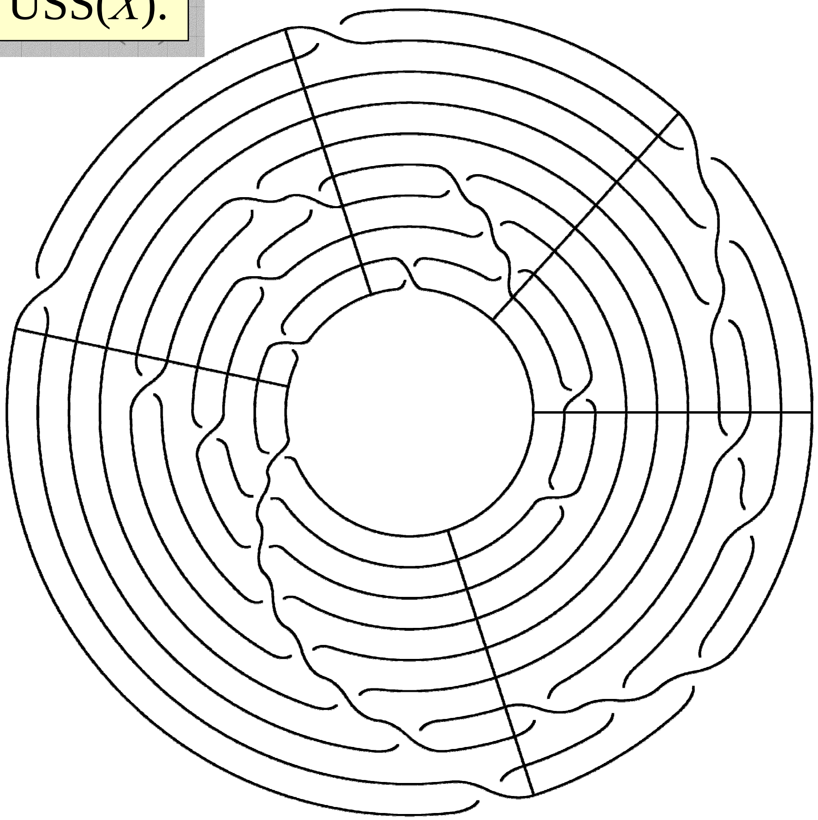
Rigid elements

Birman-Gebhardt-GM (2006): If X is rigid and $\ell(X) > 1$,

then **all elements** in USS(X) are rigid.

One can easily determine if an element is in USS(X).

Orbits under cycling are short.



But how many orbits may appear in a USS?

Open problem.

Rigidity

If an element fails to be rigid, we can measure how far it is from being rigid.

The **rigidity** of $X = \Delta^p X_1 \cdots X_r$ is: $\mathcal{R}(X) = k/r$

$$\text{if the left normal form of} \quad \Delta^p X_1 \cdots X_r \tau^{-p}(X_1)$$

$$\text{is} \quad \Delta^p \underbrace{X_1 \cdots X_k}_{k \text{ factors remain untouched}} Y_1 \cdots Y_t.$$

$$X \text{ is rigid} \;\Leftrightarrow\; \mathcal{R}(X) = 1.$$

Rigidity

Examples:

$$\mathcal{R}(\Delta \cdot \sigma_1\sigma_2 \cdot \sigma_2\sigma_1 \cdot \sigma_1\sigma_2) = 1 \qquad \left(X\ \iota(X) = \Delta \cdot \underbrace{\sigma_1\sigma_2 \cdot \sigma_2\sigma_1 \cdot \sigma_1\sigma_2}_{\text{All factors untouched}} \cdot \sigma_2\sigma_1. \right)$$

$$\mathcal{R}(\sigma_1\sigma_3 \cdot \sigma_1\sigma_3 \cdot \sigma_1) = 2/3 \qquad \left(X\ \iota(X) = \underbrace{\sigma_1\sigma_3 \cdot \sigma_1\sigma_3 \cdot \sigma_1\sigma_3}_{\text{2/3's of the factors untouched}} \cdot \sigma_1. \right)$$

$$\mathcal{R}(\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_4\sigma_3 \cdot \sigma_1\sigma_4\sigma_3) = 0 \qquad \left(X\ \iota(X) = \underbrace{\Delta \cdot \sigma_2\sigma_3\sigma_2\sigma_4\sigma_3\sigma_2\sigma_1}_{\text{No factor is untouched}}. \right)$$

Rigidity

$X \in$ SSS(X).

Rigidity does not decrease by cycling:

$$\mathcal{R}(X) \leq \mathcal{R}(\mathbf{c}^m(X)), \quad \forall m > 0.$$

Example: $X = \sigma_1\sigma_2\sigma_1\sigma_4\sigma_3\sigma_2\sigma_1 \cdot \sigma_3\sigma_2 \cdot \sigma_2\sigma_1\sigma_3\sigma_2\sigma_4.$

$$\{\mathcal{R}(\mathbf{c}^m(X))\}_{m\geq 0} = 1/3,\ 1/3,\ 1/3,\ 2/3,\ 2/3,\ 1,\ 1,\ 1, \ldots$$

Rigidity does not decrease by taking powers:

$$\mathcal{R}(X) \leq \mathcal{R}(X^m), \quad \forall m > 0.$$

Example: $X = \sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1 \cdot \sigma_3\sigma_2\sigma_4\sigma_3.$

$$\{\mathcal{R}(X^m)\}_{m\geq 1} = 0,\ 1/2,\ 0,\ 3/4,\ 0,\ 1,\ 0,\ 6/7,\ 0,\ 8/9,\ 0,\ 1, \ldots$$

Cycling and powers

Iterated cyclings and iterated powers of an element are closely related.

$X \in$ SSS(X).

Iterated cyclings:

$$X \xrightarrow{\iota(X)} \mathbf{c}(X) \xrightarrow{\iota(\mathbf{c}(X))} \mathbf{c}^2(X) \xrightarrow{\iota(\mathbf{c}^2(X))} \mathbf{c}^3(X) \longrightarrow \cdots$$

$$C_i = \iota(\mathbf{c}^{i-1}(X))$$

$$X^{C_1 \cdots C_m} = \mathbf{c}^m(X)$$

Cyclings and powers

Iterated cyclings and iterated powers of an element are closely related

$X \in$ SSS(X).

Iterated cyclings: $$X^{C_1 \cdots C_m} = \mathbf{c}^m(X)$$

Iterated powers:

$$X = \Delta^p \cdot X_1 \cdot X_2 \cdots X_r = \iota(X) \cdot \Delta^p \cdot X_2 \cdots X_r$$
$$= \boxed{C_1 \cdot (\text{Remainder}) \cdot \Delta^p}$$

$$X^2 = (\iota(X) \cdot \underbrace{\Delta^p \cdot X_2 \cdots X_r)(\iota(X)}_{\mathbf{c}(X)} \cdot \Delta^p \cdot X_2 \cdots X_r)$$

$$= \iota(X)\, \overbrace{\iota(\mathbf{c}(X)) \cdot (\text{Remainder}) \cdot \Delta^p}^{\mathbf{c}(X)} \cdot (\text{Remainder}) \cdot \Delta^p$$

$$= \boxed{C_1\, C_2 \cdot (\text{Remainder}) \cdot \Delta^{2p}}$$

Cyclings and powers

Iterated cyclings and iterated powers of an element are closely related

$X \in$ SSS(X).

Iterated cyclings: $$X^{C_1 \cdots C_m} = \mathbf{c}^m(X)$$

Iterated powers: $$X^m = C_1 \cdots C_m \cdot (\text{Remainder}) \cdot \Delta^{mp}$$

Birman-Gebhardt-GM (2006)

The product of the first m factors in the left normal form of $X^m\Delta^{-mp}$ is precisely $C_1 \cdots C_m$.

Cycling and powers

Example:

$$X = \boxed{12132143} \cdot 143 = \boxed{C_1} \cdot R_1$$
$$\mathbf{c}(X) = 121324321 \cdot 14 = C_2 \cdot R_2$$
$$\mathbf{c}^2(X) = 12132432 \cdot 214 = C_3 \cdot R_3$$
$$\mathbf{c}^3(X) = 121343 \cdot 12324 = C_4 \cdot R_4$$
$$\mathbf{c}^4(X) = 12132143 \cdot 143 = C_1 \cdot R_1 = X$$

$$X = \boxed{12132143} \cdot 143$$
$$X^2 = \Delta \cdot 2324321 \cdot 14 \cdot 143$$
$$X^3 = \Delta^2 \cdot 12324 \cdot 214 \cdot 14 \cdot 143$$
$$X^4 = \Delta^2 \cdot 12132143 \cdot 143 \cdot 12324 \cdot 214 \cdot 14 \cdot 143$$
$$X^5 = \Delta^3 \cdot 2324321 \cdot 14 \cdot 143 \cdot 12324 \cdot 214 \cdot 14 \cdot 143$$

Cycling and powers

Example:

$$
\begin{aligned}
X &= 12132143 \cdot 143 = C_1 \cdot R_1 \\
\mathbf{c}(X) &= 121324321 \cdot 14 = C_2 \cdot R_2 \\
\mathbf{c}^2(X) &= 12132432 \cdot 214 = C_3 \cdot R_3 \\
\mathbf{c}^3(X) &= 121343 \cdot 12324 = C_4 \cdot R_4 \\
\mathbf{c}^4(X) &= 12132143 \cdot 143 = C_1 \cdot R_1 = X
\end{aligned}
$$

$$
\begin{aligned}
X &= 12132143 \cdot 143 \\
X^2 &= \Delta \cdot 2324321 \cdot 14 \cdot 143 \\
X^3 &= \Delta^2 \cdot 12324 \cdot 214 \cdot 14 \cdot 143 \\
X^4 &= \Delta^2 \cdot 12132143 \cdot 143 \cdot 12324 \cdot 214 \cdot 14 \cdot 143 \\
X^5 &= \Delta^3 \cdot 2324321 \cdot 14 \cdot 143 \cdot 12324 \cdot 214 \cdot 14 \cdot 143
\end{aligned}
$$

Cycling and powers

Example:

$$\begin{aligned} X &= 12132143 \cdot 143 = C_1 \cdot R_1 \\ \mathbf{c}(X) &= 121324321 \cdot 14 = C_2 \cdot R_2 \\ \mathbf{c}^2(X) &= 12132432 \cdot 214 = C_3 \cdot R_3 \\ \mathbf{c}^3(X) &= 121343 \cdot 12324 = C_4 \cdot R_4 \\ \mathbf{c}^4(X) &= 12132143 \cdot 143 = C_1 \cdot R_1 = X \end{aligned}$$

$$\begin{aligned} X &= 12132143 \cdot 143 \\ X^2 &= \Delta \cdot 2324321 \cdot 14 \cdot 143 \\ X^3 &= \Delta^2 \cdot 12324 \cdot 214 \cdot 14 \cdot 143 \\ X^4 &= \Delta^2 \cdot 12132143 \cdot 143 \cdot 12324 \cdot 214 \cdot 14 \cdot 143 \\ X^5 &= \Delta^3 \cdot 2324321 \cdot 14 \cdot 143 \cdot 12324 \cdot 214 \cdot 14 \cdot 143 \end{aligned}$$

Cyclings and powers

Example:

$$
\begin{aligned}
X &= 12132143 \cdot 143 = C_1 \cdot R_1 \\
\mathbf{c}(X) &= 121324321 \cdot 14 = C_2 \cdot R_2 \\
\mathbf{c}^2(X) &= 12132432 \cdot 214 = C_3 \cdot R_3 \\
\mathbf{c}^3(X) &= 121343 \cdot 12324 = C_4 \cdot R_4 \\
\mathbf{c}^4(X) &= 12132143 \cdot 143 = C_1 \cdot R_1 = X
\end{aligned}
$$

$$
\begin{aligned}
X &= 12132143 \cdot 143 \\
X^2 &= \Delta \cdot 2324321 \cdot 14 \cdot 143 \\
X^3 &= \Delta^2 \cdot 12324 \cdot 214 \cdot 14 \cdot 143 \\
X^4 &= \Delta^2 \cdot 12132143 \cdot 143 \cdot 12324 \cdot 214 \cdot 14 \cdot 143 \\
X^5 &= \Delta^3 \cdot 2324321 \cdot 14 \cdot 143 \cdot 12324 \cdot 214 \cdot 14 \cdot 143
\end{aligned}
$$

Cyclings and powers

Example:

$$\begin{aligned} X &= 12132143 \cdot 143 = C_1 \cdot R_1 \\ \mathbf{c}(X) &= 121324321 \cdot 14 = C_2 \cdot R_2 \\ \mathbf{c}^2(X) &= 12132432 \cdot 214 = C_3 \cdot R_3 \\ \mathbf{c}^3(X) &= 121343 \cdot 12324 = C_4 \cdot R_4 \\ \mathbf{c}^4(X) &= 12132143 \cdot 143 = C_1 \cdot R_1 = X \end{aligned}$$

$$\sup(C_1 \cdots C_m) = m$$

$$\inf(\text{Remainder}) = 0$$

$$\begin{aligned} X &= 12132143 \cdot 143 \\ X^2 &= \Delta \cdot 2324321 \cdot 14 \cdot 143 \\ X^3 &= \Delta^2 \cdot 12324 \cdot 214 \cdot 14 \cdot 143 \\ X^4 &= \Delta^2 \cdot 12132143 \cdot 143 \cdot 12324 \cdot 214 \cdot 14 \cdot 143 \\ X^5 &= \Delta^3 \cdot 2324321 \cdot 14 \cdot 143 \cdot 12324 \cdot 214 \cdot 14 \cdot 143 \end{aligned}$$

Consequences

$X \in$ SSS(X).

$$\iota(X^m) = \iota(C_1 \cdots C_m) \quad \forall m \geq 1$$

$$\inf(C_1 \cdots C_m) \ \leq \ \inf(C_1 \cdots C_{m+1}) \ \leq \ \inf(C_1 \cdots C_m) + 1$$

$$\Downarrow$$

$$\inf(X^m) + p \ \leq \ \inf(X^{m+1}) \ \leq \ \inf(X^m) + p + 1$$

$$\sup(X^m) + p + r - 1 \ \leq \ \sup(X^{m+1}) \ \leq \ \sup(X^m) + p + r$$

Corollary: Translation numbers in G are **positive.**

$$t(X) = \lim_{n \to \infty} \frac{||X^n||}{n}$$

(Shown independently by **Lee & Lee** (2006))

Absolute factors

$X \in \mathrm{USS}(X)$. $\qquad X = \mathbf{c}^N(X)$ for N arbitrarily large.

We studied the **final factors** of:

$$\varphi(C_N) = F_1$$
$$\curlyvee|$$
$$\varphi(C_{N-1}C_N) = F_2$$
$$\curlyvee|$$
$$\varphi(C_{N-2}C_{N-1}C_N) = F_3$$
$$\curlyvee|$$
$$\varphi(C_{N-3}C_{N-2}C_{N-1}C_N) = F_4$$
$$\curlyvee|$$
$$\vdots$$
$$\varphi(C_{N-m+1}\cdots C_{N-3}C_{N-2}C_{N-1}C_N) = F_m \longrightarrow$$

$F(X)$ Absolute final factor

The chain stabilizes for $m \leq |\Delta|$.

Looking at initial factors of suitable remainders (ascending chain that stabilizes) $\longrightarrow$ $I(X)$ Absolute initial factor

Absolute factors

$X \in$ USS(X).

$F(X)\, I(X)$ is always left-weighted.

Absolute factors are related to powers:

For every $m \geq 1$ such that $X^m \in$ SSS(X^m),

(For every m, if X belongs to the stable USS)

$$F(X) \succeq \varphi(X^m)$$

$$I(X) \preceq \iota(X^m)$$

If X^m is rigid, the equalities hold.

Elements having a rigid power

Suppose that $X \in \mathrm{USS}(X)$ has a rigid power.

If an element has non-zero rigidity, its powers have the same inital factor.

Hence:

$$\text{If } \mathcal{R}(X^t) > 0, \text{ then } \iota(X^t) = I(X).$$

$$\text{If } \mathcal{R}(X^{-t}) > 0, \text{ then } \varphi(X^t) = F(X).$$

We need to know how many powers of X may have 0 rigidity.

Elements having a rigid power

We compare $\iota(X^m)$ for all m.

If $X \in \text{Stable} - USS(X)$, then for every $s, t > 0$
either $\iota(X^s) \preceq \iota(X^t)$ or $\iota(X^t) \preceq \iota(X^s)$.

The set $\{\iota(X), \iota(X^2), \dots, \iota(X^{|\Delta|})\}$ is **totally ordered** by $\preceq$.

Example: $X = \Delta \cdot 1213214 \cdot 23$

$\iota(X) = 34321\ 34$

$\iota(X^2) = 34321\ 34\ 23$

$\iota(X^3) = 34321$

$\vdots$

$\iota(X^3) \preceq \iota(X) \preceq \iota(X^2)$

Elements having a rigid power

The set $\{\iota(X), \iota(X^2), \ldots, \iota(X^{|\Delta|})\}$ is **totally ordered** by $\preceq$.

In this set there is a **repetition:** $\iota(X^a) = \iota(X^b)$, with $1 \leq a \leq b \leq |\Delta|$.

Then the sequence $\iota(X^a), \iota(X^{a+1}), \iota(X^{a+2}), \ldots$ is periodic.

Then $\iota(X^s) = \iota(X^{2s})$, with $a \leq s < b$. $\longrightarrow$ $\mathcal{R}(X^s) > 0$

$(s < |\Delta|)$

In the same way: $\longrightarrow$ $\mathcal{R}(X^{-t}) > 0$

$(t < |\Delta|)$

Elements having a rigid power

$$\mathcal{R}(X^s) > 0 \qquad \mathcal{R}(X^{-t}) > 0$$

$$(s < |\Delta|) \qquad (t < |\Delta|)$$

Taking $m = \mathrm{lcm}(s,t)$,

$$\left.\begin{array}{lcl} \mathcal{R}(X^m) > 0 & \Rightarrow & \iota(X^m) = I(X) \\ \mathcal{R}(X^{-m}) > 0 & \Rightarrow & \varphi(X^m) = F(X) \end{array}\right\} \qquad X^m \text{ is rigid}$$

$$(m < |\Delta|^2)$$

But which elements have a rigid power?

pseudo-Anosov braids

Birman-Gebhardt-GM (2006)

$X \in USS(X)$ has a rigid power $\quad \Leftrightarrow \quad C_1 \cdots C_M = \Delta^k X^t$

for some M, k, t.

McCarthy (1982), **GM-Wiest** (2004)

If X is **pseudo-Anosov**, every element in its **centralizer** has a common power with X, up to powers of Δ.

If N is the orbit length of X, $\quad C_1 \cdots C_N \in Z(X)$.

Hence $\quad (C_1 \cdots C_N)^d = \boxed{C_1 \cdots C_{Nd} = \Delta^k X^t.}$

Every pseudo-Anosov braid in its USS has a **small** power which is **rigid**