Conjugacy problems in braid groups and other Garside groups

Part I

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.

Conjugacy Problems

Fix a group G.

Conjugacy decision problem (CDP):

Given two elements $a, b \in G$, determine whether they are conjugate.

Conjugacy search problem (CSP):

Given two conjugate elements $a, b \in G$, find a conjugating element c.

$$c^{-1}ac = b$$

Examples

G = **Abelian group**

CDP = Word problem $(a, b \text{ conjugate} \Leftrightarrow a = b)$

CSP = Trivial $c = 1$

Examples

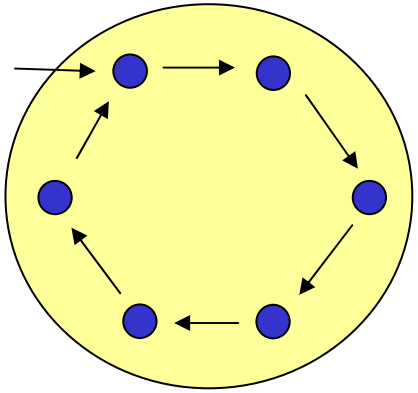
G = **Free group**

Reduce a word: Repeatedly remove all subwords $x_i x_i^{-1}$ or $x_i^{-1} x_i$.

Cycling of a word: Put the first letter at the end, and reduce. (conjugation)

Algorithm to solve CDP & CSP:

$w \xrightarrow{\text{Cycling}} w_1 \xrightarrow{\text{Cycling}} w_2 \xrightarrow{\text{Cycling}} w_3 \cdots \rightarrow$



CRW(*w*): Cyclically Reduced words conjugate to *w*.

CRW(*w*)

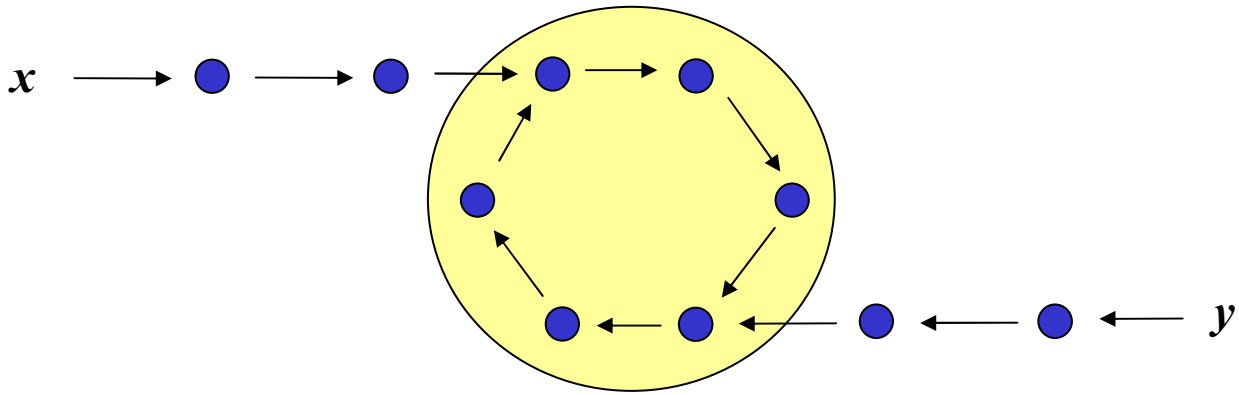
Examples

G = **Free group**

Algorithm to solve CDP & CSP:

CDP: x, y conjugate $\Leftrightarrow CRW(x) = CRW(y)$

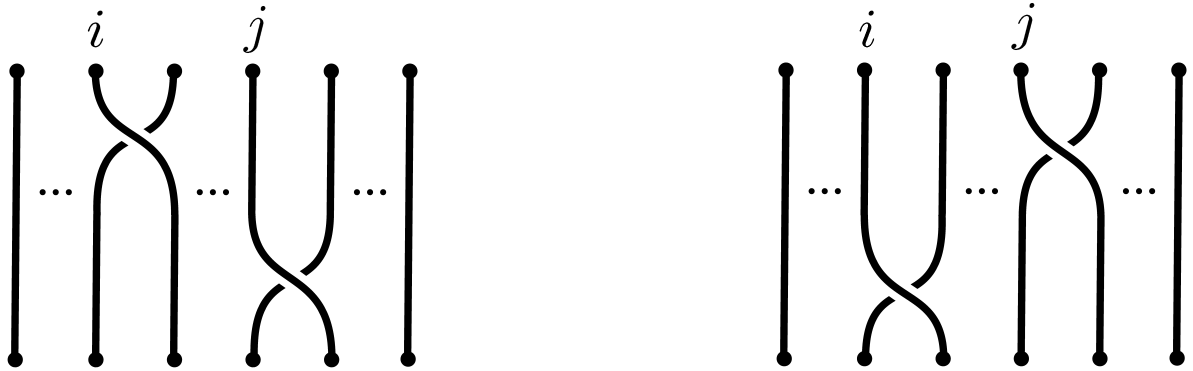
CSP: Each cycling gives a conjugating element.



Braid groups

(E. Artin, 1925)

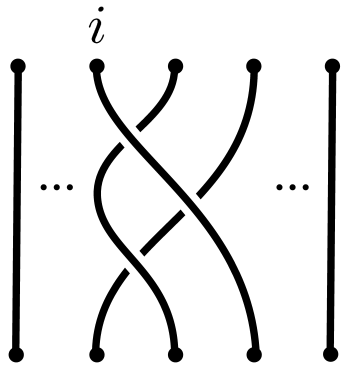
$$B_n = \left\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & (|i-j| \geq 2) \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & (1 \leq i \leq n-2) \end{array} \right\rangle$$

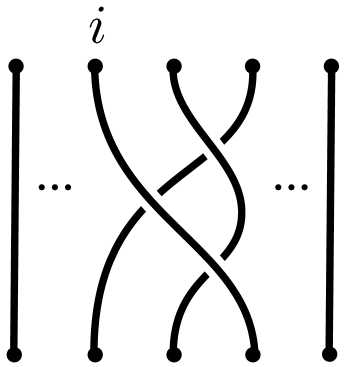


Braid groups

(E. Artin, 1925)

$$B_n = \left\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & (|i-j| \geq 2) \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & (1 \leq i \leq n-2) \end{array} \right\rangle$$

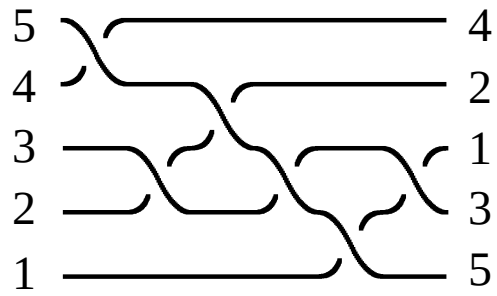




Positive and simple elements

Positive elements: Braids in which every crossing is positive

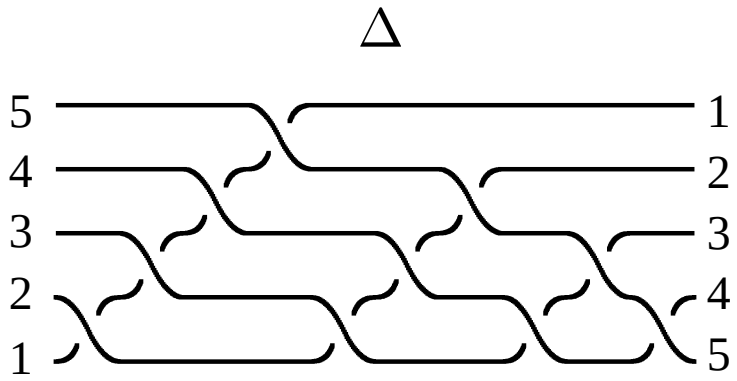
Simple elements: Positive elements in which every pair of strands cross at most once.



Simple elements of B_n $\longleftrightarrow$ (Bij.) Permutations of Σ_n

Garside element

There is a special simple element, called **half twist** or **Garside's Delta.**



Center of $B_n = \langle \Delta^2 \rangle$.

Garside group

A group G is said to be a **Garside group** if

A. G admits a **lattice order**, invariant under left-multiplication. $(G, \preceq, \vee, \wedge)$

$$a \preceq b \;\Rightarrow\; ca \preceq cb \qquad \forall c \in G$$

Unique lcm $s \vee t$

Unique gcd $s \wedge t$

Positive cone $P = \{p \in G;\ 1 \preceq p\}$

P and $\preceq$ determine each other: $\quad a \preceq b \quad \Leftrightarrow \quad a^{-1}b \in P.$

Garside group

A group G is said to be a **Garside group** if

A. G admits a **lattice order**, invariant under left-multiplication. $(G, \preceq, \vee, \wedge)$

B. There exists a **Garside element** $\Delta \in P$, satisfying:

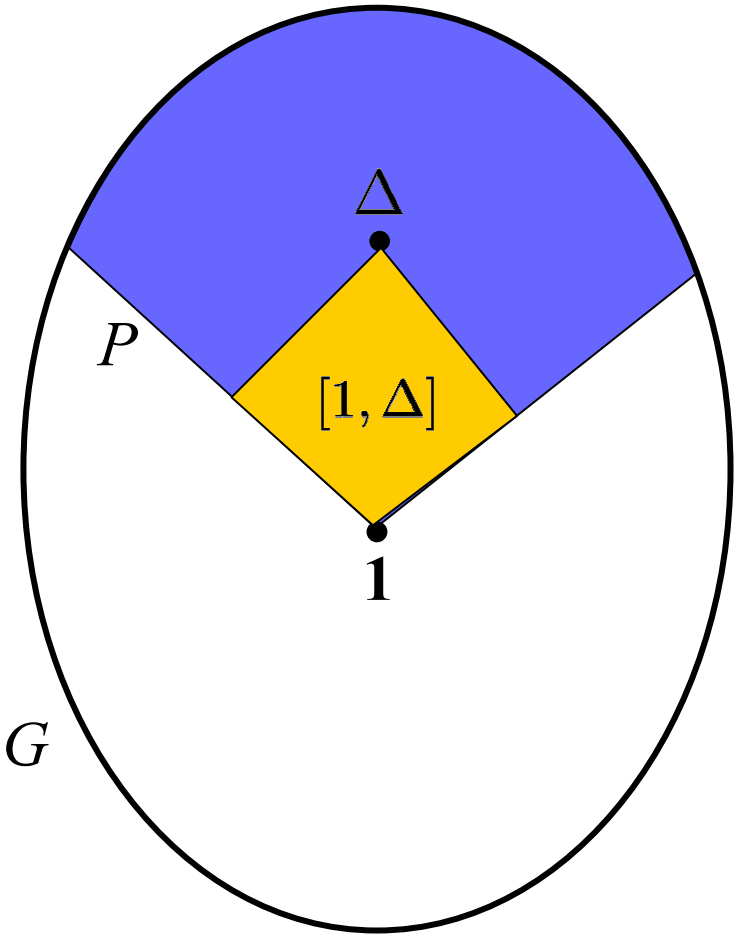
1. The interval $[1, \Delta] = \{s \in G;\ 1 \preceq s \preceq \Delta\}$ generates G.
2. The conjugation by Δ preserves the order: $\Delta^{-1} P \Delta = P$.

C. The monoid P is **atomic**:

For $x \in P$, there is an upper bound on the length of chains

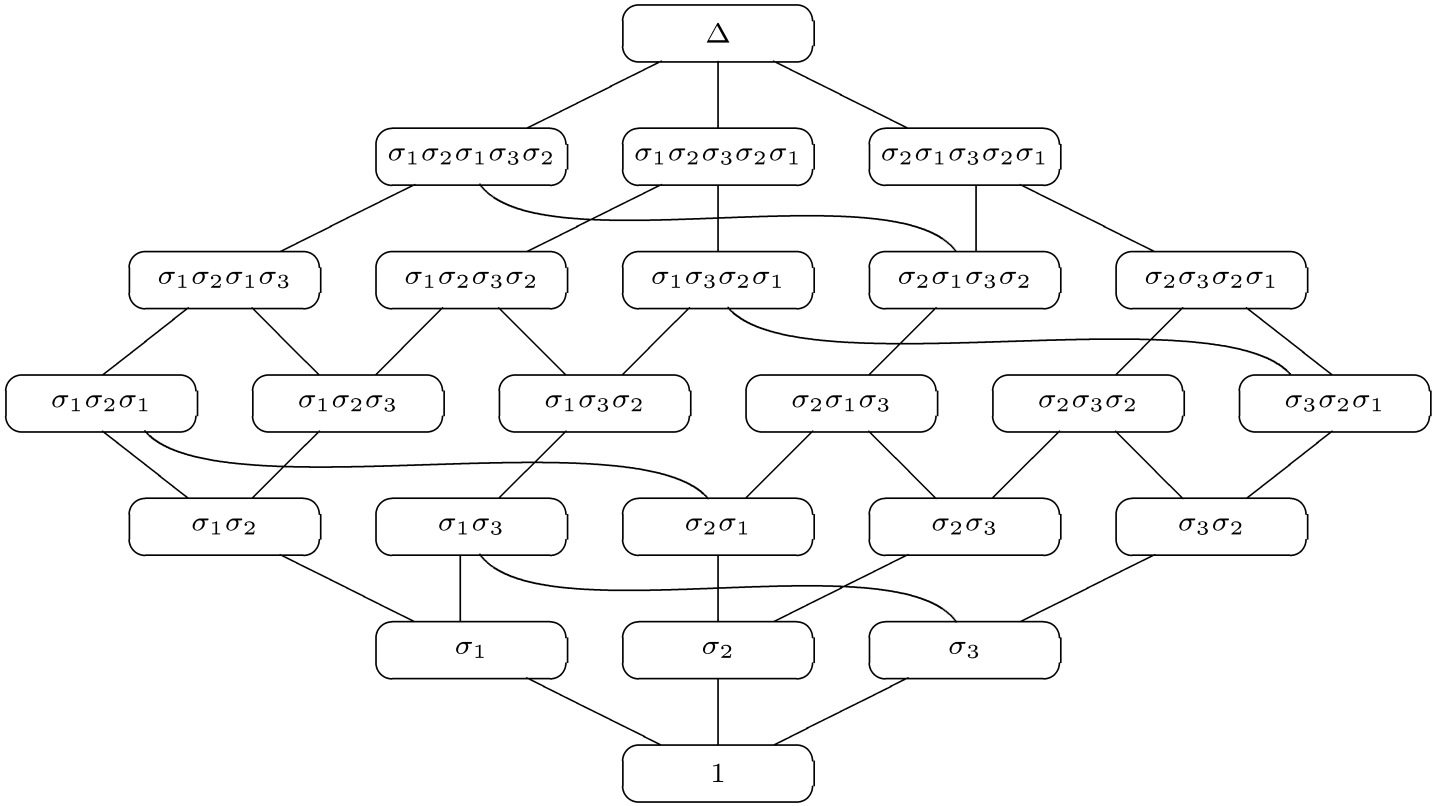
$$1 \prec x_1 \prec \cdots \prec x_n = x.$$

Garside group



A Garside group has **finite type** if the set $[1, \Delta]$ is finite.

Simple elements



Lattice of simple elements in the braid group B_4.

Word Problem

Garside: (1969) Every element can be written as $\Delta^p X$

where $p \in \mathbb{Z}$ and X is a positive element.

Since every positive element is a product of simple elements,
every element can be written as

$$\Delta^p X_1 \cdots X_r$$

where every factor is simple.

Want *r* as small as possible.

Word Problem

Garside (1969), Deligne (1972), Adyan (1984), Thurston (1992), Elrifai-Morton (1994).

An element X is said to be in **left normal form** if it is written as:

$$\Delta^p X_1 \cdots X_r$$

where p is maximal,

& X_i is the biggest simple prefix of $X_i \cdots X_r$. $\Big\}$ $\Rightarrow$ r is minimal.

Infimum:	$\inf(X) = p$
Supremum:	$\sup(X) = p + r$
Canonical length:	$\ell(X) = r$

Initial and final factors

Let $\tau(\alpha) = \Delta^{-1}\alpha\,\Delta$.

If X is written in left normal form, $\Delta^p X_1 \cdots X_r$, we define:

Initial factor: $\iota(X) = \tau^{-p}(X_1)$.

Final factor: $\varphi(X) = X_r$.

Remark: The left normal form of X^{-1} is: $\Delta^{-p-r} Y_r \cdots Y_1$,

where $X_i\,\tau^{p+i}(Y_i) = \Delta$.

$$\inf(X^{-1}) = -\sup(X)$$
$$\sup(X^{-1}) = -\inf(X)$$
$$\ell(X^{-1}) = \ell(X)$$

$$\varphi(X)\iota(X^{-1}) = \Delta$$
$$\varphi(X^{-1})\iota(X) = \Delta$$

Conjugacy Problem

In a **Garside group**:

Garside,	**Elrifai-Morton,**	**Birman-Ko-Lee,**	**Franco-GM,**	**Gebhardt, ...**
(1969)	(1994)	(1998)	(2003)	(2005)

Charney: Artin groups of spherical type are biautomatic.
(1992)

Fiedler-Kurlin: CDP in braid groups.
(2006)

Cyclings and decyclings

Cycling of X: Put the initial factor at the end.

$$\text{Si } X = \Delta^p X_1 \cdots X_r,$$

$$\mathbf{c}(X) = \widetilde{X}_1 \, \Delta^p \, X_2 \cdots X_r \qquad \text{(not necessarily in left normal form)}$$

$$\widetilde{X}_1 = \iota(X)$$

Deycling of X: Put the final factor at the beginning.

$$\mathbf{d}(X) = X_r \, \Delta^p X_1 \cdots X_{r-1}$$

Summit Set

Garside (1969):

SS(X) (Summit Set of X): Conjugates of X of maximal inf.

It is an invariant of the conjugacy class, hence:

X and Y are conjugate iff SS(X)=SS(Y)

How to compute it?

Summit Set

ElRifai-Morton (1994): If the infimum of X can be increased by a conjugation, **repeated cycling** will do it.

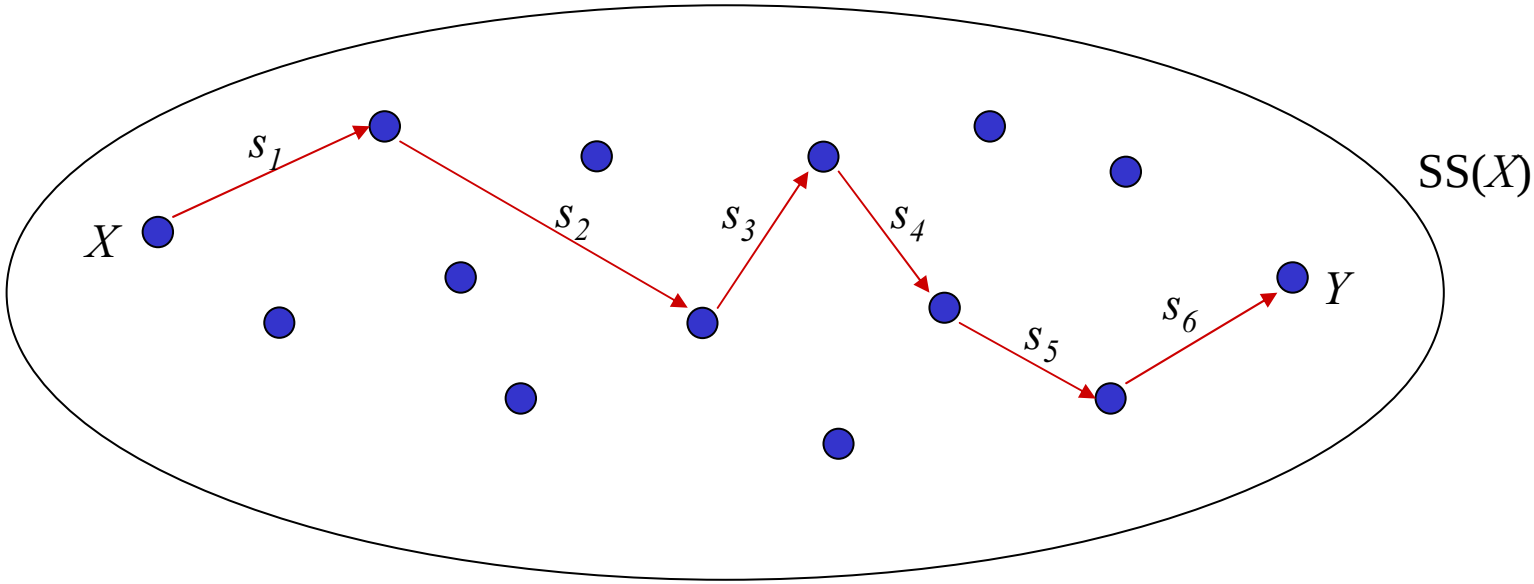
Birman-Ko-Lee (2001): The number of times one needs to cycle to increase inf is bounded by $|\Delta|$.

$$\ell(X) = m \;\Rightarrow\; \mathbf{c}^{m|\Delta|}(X) \in SS(X).$$

This procedure finds **one element** in SS(X).

Summit Set

ElRifai-Morton (1994): Two elements in SS(X) are always conjugate through a sequence of conjugations by simple elements.

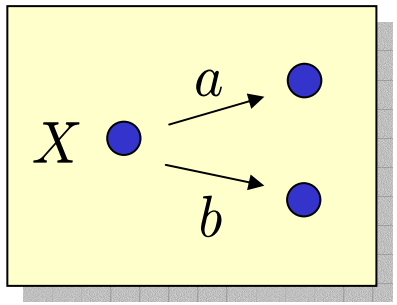


Summit Set

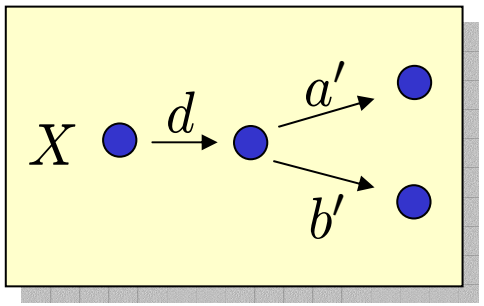
ElRifai-Morton (1994): Two elements in SS(X) are always conjugate through a sequence of conjugations by simple elements.

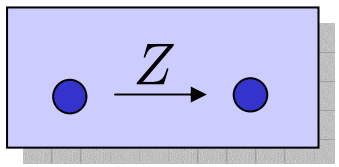
Alternative proof:

Franco-GM (2003): $X, X^a, X^b \in SS(X) \;\Rightarrow\; X^{a\wedge b} \in SS(X).$



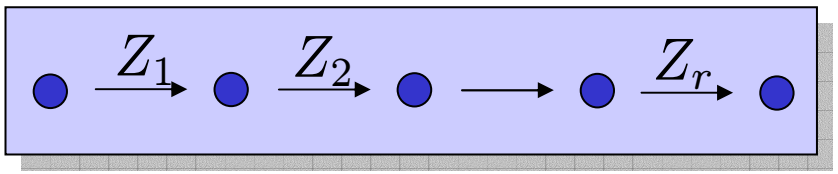
$d = a \wedge b$





$Z = Z_1 \cdots Z_r$

$(Z \wedge \Delta^i = Z_1 \cdots Z_i)$



Summit Set

Algorithm to compute SS(X):

1. Find one element in SS(X) by iterated cycling.
2. Conjugate each known element in SS(X) by **all simple elements**.
3. Repeat 2 until no new elements appear.

This terminates since SS(X) and the set of simple elements are **finite.**

But both sets are, in general, huge!

Super Summit Set

ElRifai-Morton (1994)

SSS (Super Summit Set): Conjugates of X of minimal length.

Iterated cycling sends X to Y in SS(X).

Iterated decycling sends Y to Z in SSS(X).

Analogous construction and results.

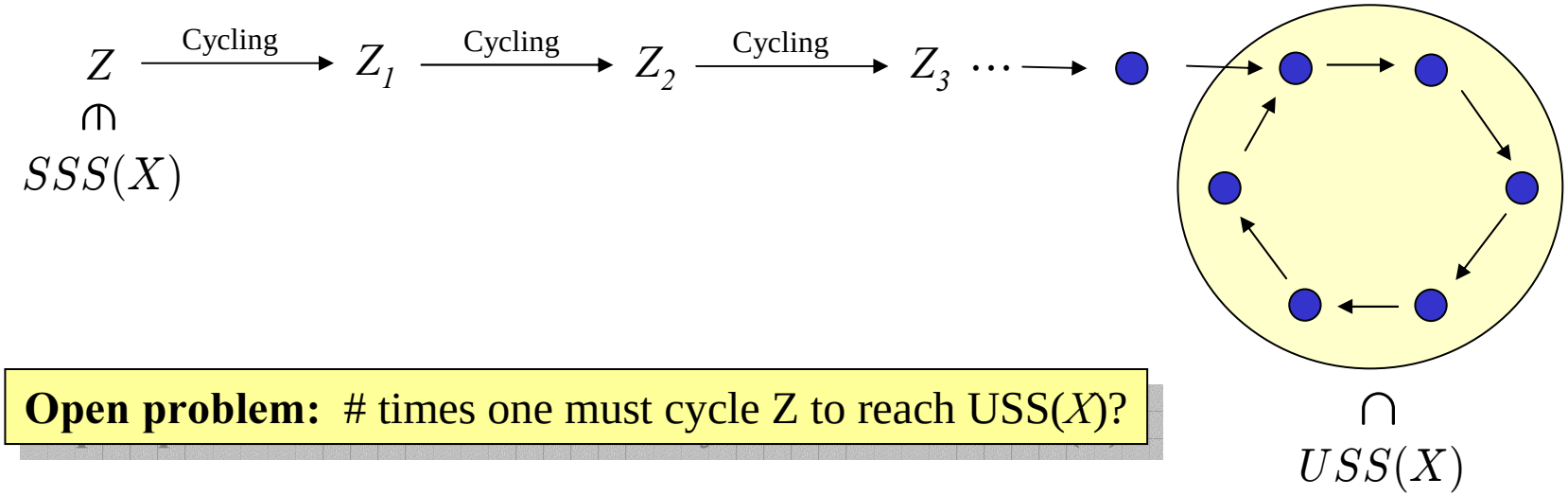
SSS(X) is much smaller than SS(X)

Ultra Summit Set

Gebhardt (2005)

USS (Ultra Summit Set):

Elements Y in SSS(X) s. t. $\mathbf{c}^k(Y) = Y$ for some $k > 0$.



Open problem: # times one must cycle Z to reach USS(X)?

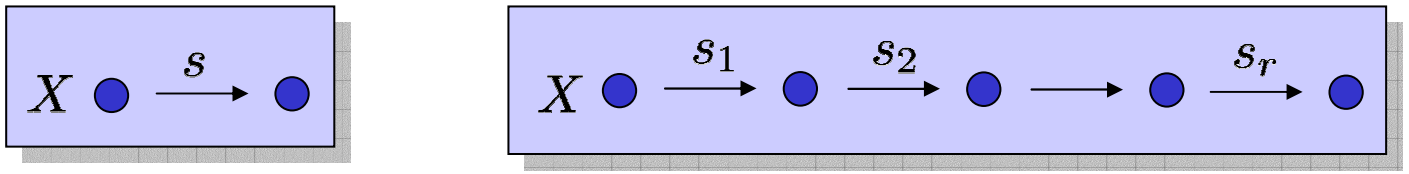
Open problem: Find a bound on the size of USS(X).

Improvement

With the bove method, one still needs to conjugate every element in USS(X)

by all simple elements.

But if s is a simple element that can be decomposed...



... then one does not need to use s to go from X to X^s.

It suffices to use simple elements that cannot be decomposed.

Minimal simple elements

Franco-GM (2003)

Every two elements in USS(X) are **connected** by **minimal simple elements**.

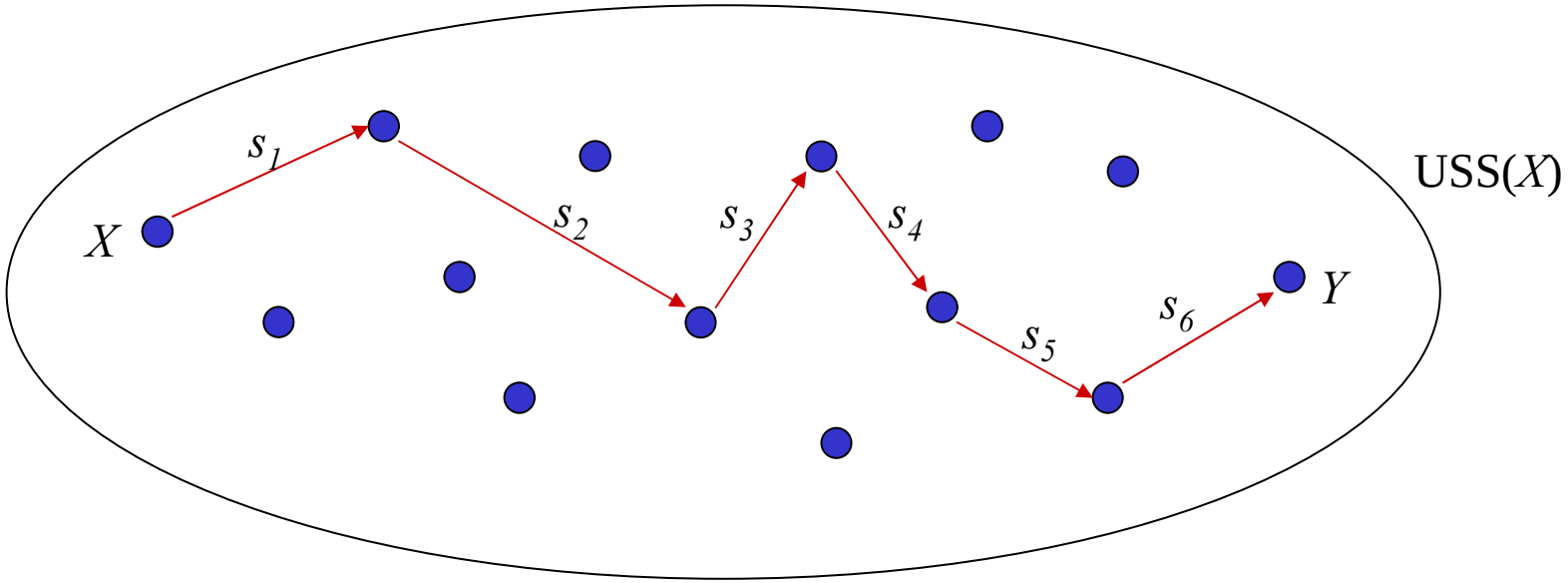
Given X in USS(X), s is a **minimal simple element** for X if:

- s is **simple**.
- $X^s \in \mathrm{USS}(X)$.
- No prefix of s satisfies the above property.

Minimal simple elements

Franco-GM (2003)

Every two elements in USS(X) are **connected** by **minimal simple elements**.



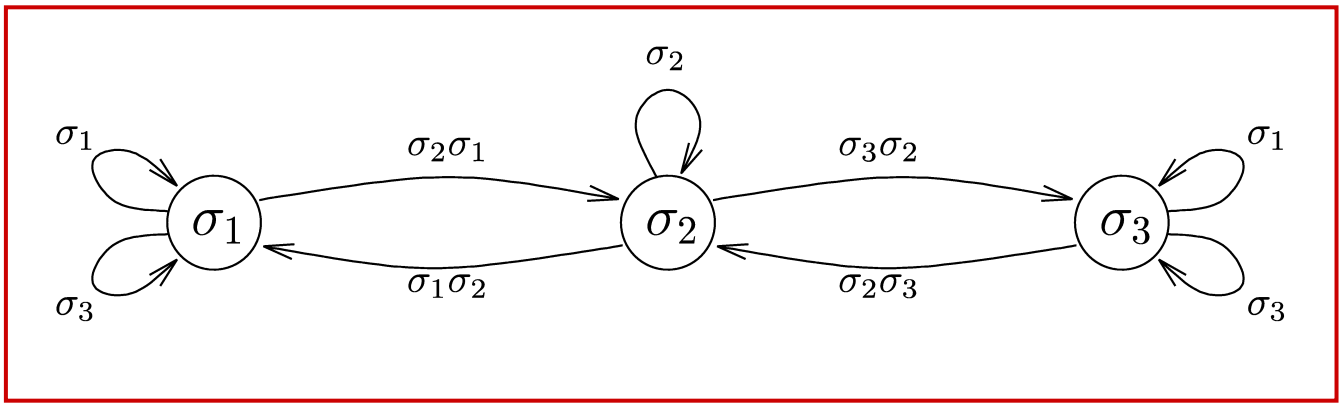
Minimal simple elements

Franco-GM (2003)

Every two elements in USS(X) are **connected** by **minimal simple elements**.

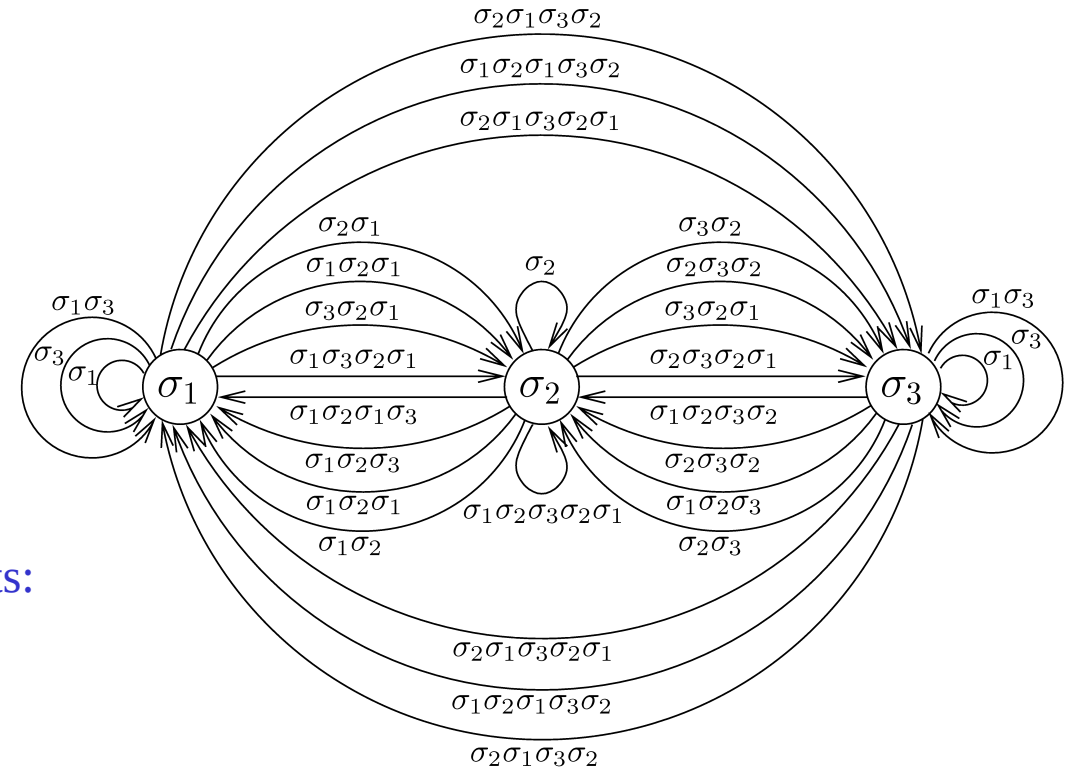
One can compute a **directed graph**:

- **Vertices:** Elements in USS(X).
- **Arrows:** minimal simple elements.



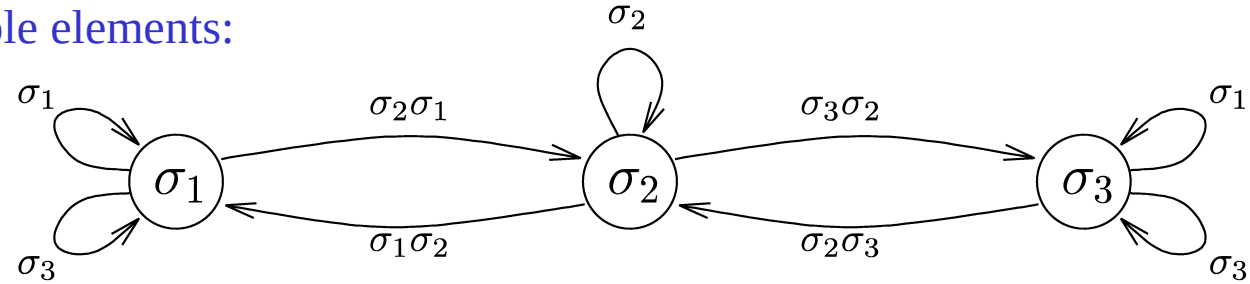
USS(σ_1) in B_4

USS(σ_1) in B_4



With all simple elements:

With minimal simple elements:



Properties of minimal simple elements

Franco-GM (2003)

Given X, #(minimal simple elements for X) $\leq$ #(atoms)

(In B_n, the atoms are $\sigma_1, \ldots, \sigma_{n-1}$.)

Proof: Every atom a is a prefix of at most one minimal simple element.

Otherwise:

$$\left.\begin{array}{l} a \preceq s_1 \\ a \preceq s_2 \end{array}\right\} \Rightarrow\ a \preceq (s_1 \wedge s_2).$$

$\downarrow$

Contradicts the minimality of s_1 and s_2. $\square$

For each X, one needs n-1 conjugations, instead of n!

Properties of minimal simple elements

Birman-Gebhardt-GM (2006)

Given X, if s is a minimal simple element for X, then

$$\text{either} \quad s \preceq \iota(X) \quad \text{or} \quad s \preceq \iota(X^{-1}).$$

Proof: Left normal form $X = \Delta^p X_1 \cdots X_r$.

$\iota(X^{-1}) = (X^{-1}\Delta^{p+r}) \wedge \Delta$ conjugates X to USS(X).

Since s is minimal:

1) $s \wedge \iota(X^{-1}) = s \longrightarrow s \preceq \iota(X^{-1}).$

2) $s \wedge \underbrace{\iota(X^{-1})}_{\text{Complement of } X_r} = 1 \longrightarrow$ $\Delta^p X_1 \cdots X_r s$ is in left normal form.
$s^{-1}\Delta^p X_1 \cdots X_r s \in USS(X)$

$\downarrow$

$s \preceq \tau^{-p}(X_1) \longrightarrow s \preceq \iota(X).$ □

Partial cycling

Birman-Gebhardt-GM (2006)

Given X, if s is a minimal simple element for X, then

$$\text{either} \quad s \preceq \iota(X) \quad \text{or} \quad s \preceq \iota(X^{-1}).$$

Conjugation by a prefix of $\iota(X)$ corresponds to a **partial cycling** of X.

(For $p = 0$) **Cycling:** $X_2 \cdots X_r \, X_1$

Partial cycling: $t \, X_2 \cdots X_r \, s \qquad (X_1 = s \, t)$

Partial cycling

Birman-Gebhardt-GM (2006)

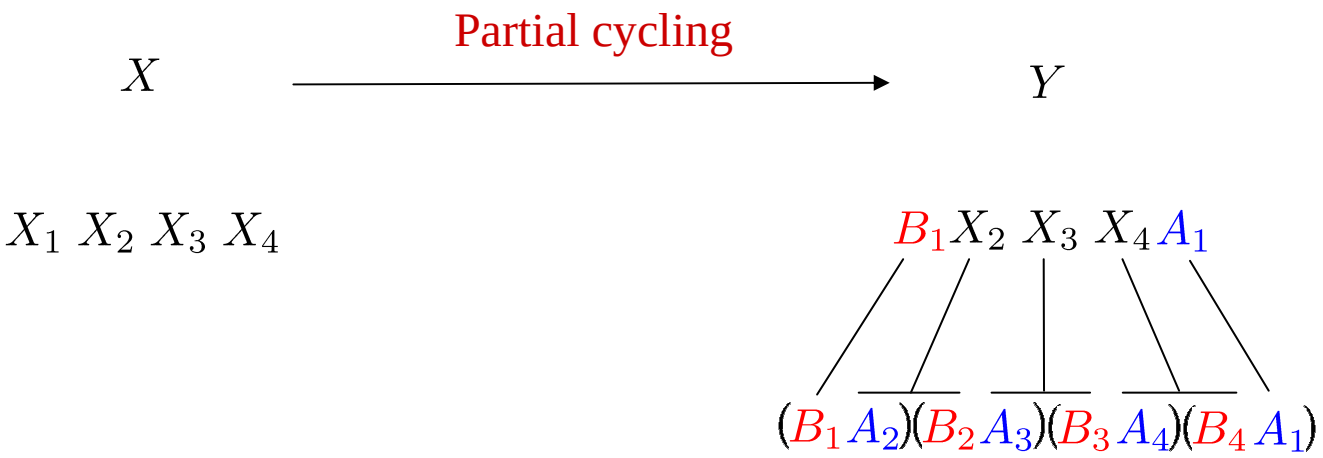
Given X, if s is a minimal simple element for X, then

$$\text{either} \quad s \preceq \iota(X) \quad \text{or} \quad s \preceq \iota(X^{-1}).$$

Conjugation by a prefix of $\iota(X)$ corresponds to a **partial cycling** of X.

Conjugation by a prefix of $\iota(X^{-1})$ corresponds to a **partial cycling** of X^{-1}.

Partial cycling



Partial cycling

$X_1\ X_2\ X_3\ X_4$ $\qquad$ $B_1 X_2\ X_3\ X_4 A_1$

$$(A_1\,B_1)(A_2\,B_2)(A_3\,B_3)(A_4\,B_4) \longrightarrow (B_1\,A_2)(B_2\,A_3)(B_3\,A_4)(B_4\,A_1)$$

Black and red arrows

The graph of USS(X) has **two kinds of arrows:**

- **Partial cyclings.** Black arrows →
- **Partial cyclings of the inverse.** Red arrows →

In general, two elements in USS(X) are **not** connected by **black** (resp. **red**) arrows.

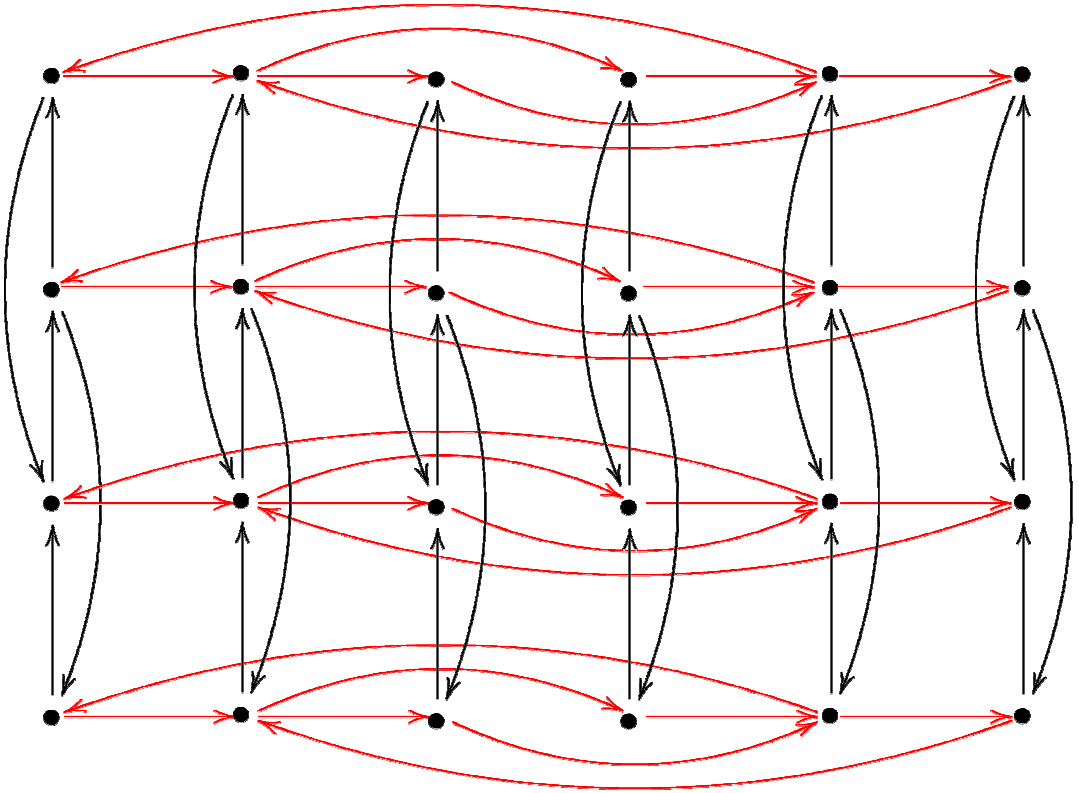
There are several **black components.**

There are several **red components.**

Example

USS of the braid in B_{10} :

$$(\sigma_1\sigma_3\sigma_2\sigma_1\sigma_4\sigma_5\sigma_7\sigma_8\sigma_9\sigma_8)\ (\sigma_2\sigma_1\sigma_3\sigma_5\sigma_4\sigma_3\sigma_6\sigma_7\sigma_8\sigma_7\sigma_9)\ (\sigma_1\sigma_3\sigma_4\sigma_3\sigma_7\sigma_6\sigma_8\sigma_7\sigma_9)$$



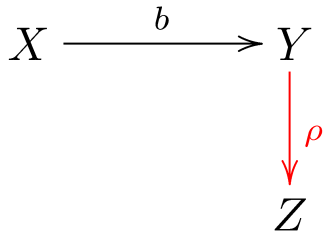
24 orbits.

72 Elements.

Black and red components

Every **black component** intersects every **red component**.

Proof: Suppose we have



$$\left.\begin{array}{l} X = \Delta^p X_1 \cdots X_r \\ b \text{ is a black arrow} \end{array}\right\} \Rightarrow X_r\, b \quad \text{left weighted (not simple)} \quad \Rightarrow \quad X_r\, b\, \rho \quad \text{not simple.}$$

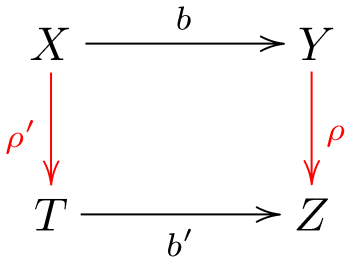
Normal form of $X_r\, b\, \rho \longrightarrow (X_r\, \rho')\, b'$

- ρ' is a red arrow
- b' is a black arrow
- $b\, \rho = \rho'\, b'$

Black and red components

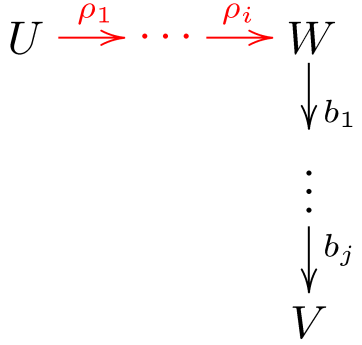
Every **black component** intersects every **red component**.

Proof:



Every $U, V \in \mathrm{USS}(X)$ are joined by a path.

Every path in USS(X) (made of **black** and **red** arrows) can be replaced by a **red path** followed by a **black path**.



$\Rightarrow$ The **red component** of U intersects the **black component** of V. Q.E.D.

Algorithm

To determine if two elements X and Y are conjugate:

Compute $U \in \mathrm{USS}(X)$.

Compute the **red component** of U.

Compute $V \in \mathrm{USS}(Y)$.

Compute the **black component** of V.

X and Y are conjugate $\Leftrightarrow$ these two components are not disjoint.

By construction, this also computes the **conjugating element**.

Some conclusions

- The **black component** of X is analogous to the set of CRW's in a free group.

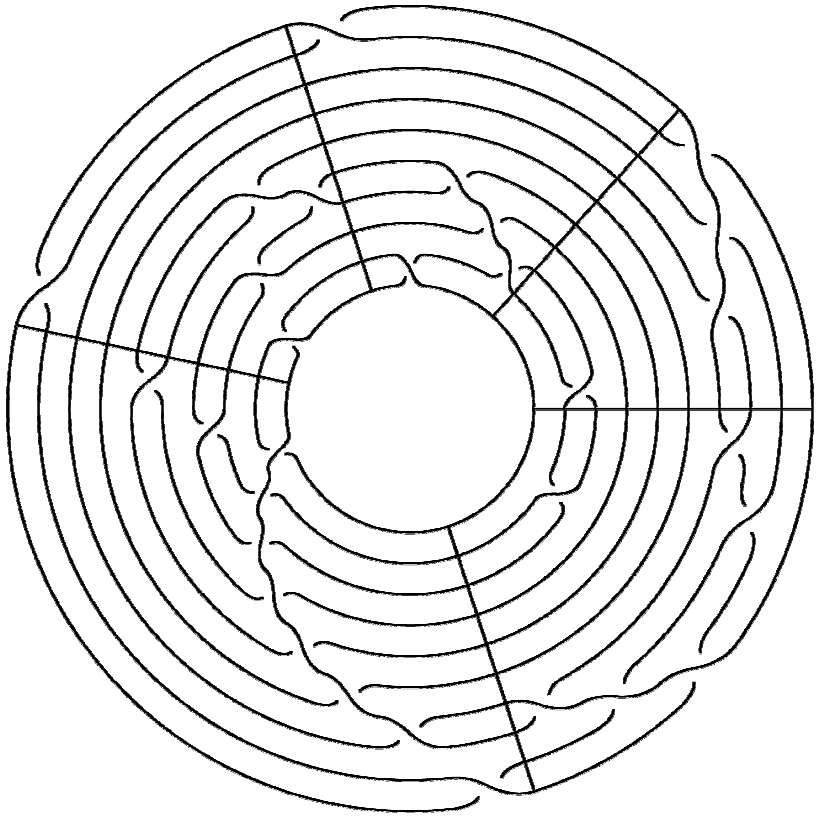
- Given X, one can generate its black component using only partial cyclings.

- For elements of a given canonical length:

  If every every black component has #(vertices) $\leq$ N

  then #(USS) $\leq$ N^2.

$X \in USS(X)$



All elements in the **black component** are obtained from this one by:

1) Applying semigroup relations: $\sigma_i\sigma_j = \sigma_j\sigma_i, \quad \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$.

2) Rotating.

ways to reorganize the above crossings, to obtain an element in USS(X)?

Other sets smaller than USS

Lee-Lee (2006)

$$\text{Stable SSS} = \{X \in SSS(X) : \ X^m \in SSS(X^m), \ \forall m\}.$$

Birman-Gebhardt-GM (2006)

$$\text{Stable USS} = \{X \in USS(X) : \ X^m \in USS(X^m), \ \forall m\}.$$

Zheng (2006)

***q*-cycling of X :** $\mathbf{c}_q(X)$ Move the first q factors to the end.

$$\text{C*(X)} = \{X \in G : \quad \mathbf{c}_q^{N_q}(X) = X, \ \forall q\}.$$

All these sets are **non-empty**, **finite** and **invariants** of the conjugacy class.