A polynomial-time solution to the reducibility problem

Ki Hyoung Ko
(Joint with Jang Won Lee)
KAIST

Braid group and lattice structure

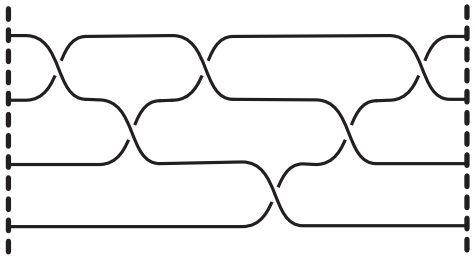
- Artin presentation of the braid groups;

$$B_n = \left\langle \sigma_1, \cdots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_j\sigma_i = \sigma_i\sigma_j & \text{if } |i-j| > 1 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{if } |i-j| = 1 \end{array} \right\rangle$$

- B_n^+ denotes the monoid given by this presentation.
- Partial order on B_n^+: $x \prec y$ if there is $z \in B_n^+$ such that $xz = y$
- Meet on B_n^+: $x \wedge y$ is the maximal braid $z \in B_n^+$ such that $z \prec x$ and $z \prec y$
- Join on B_n^+: $x \vee y$ is the minimal braid $z \in B_n^+$ such that $x \prec z$ and $y \prec z$
- There are also the corresponding right versions $\prec_R, \wedge_R, \vee_R$.

Half twist and permutation braids

- Half-twist braid: $\Delta = (\sigma_1 \cdots \sigma_{n-1})(\sigma_1 \cdots \sigma_{n-2}) \cdots (\sigma_1\sigma_2)\sigma_1$



Half-twist braid in B_4

- $\sigma_i \prec \Delta$ for each $i = 1, \cdots, n-1$
- For any braid $x \in B_n$, $x\Delta = \Delta\tau(x)$
- τ denotes the automorphism of B_n sending σ_i to σ_{n-i}.
- $S_n = \{x \in B_n^+ \mid x \prec \Delta\}$ and an element in S_n is called a permutation braid.

Weighted decomposition

- The right complement of a permutation braid a is a permutation braid a^* such that $aa^* = \Delta$
- A product ab of a permutation braid a and a positive braid b is (left) weighted, written $a \lceil b$, if $a^* \wedge b = e$
- Garside-Thurston's (left) weighted form of a braid x is

$$x = \Delta^u x_1 x_2 \cdots x_k$$

  where x_i are permutation braids and $x_i \lceil x_{i+1}$
- This decomposition is unique and so solve the word problem in $\mathcal{O}(k^2 n \log n)$.
- $\inf(x) = u$, $\sup(x) = u + k$ and $\ell(x) = k$ are called the infimum, the supremum and the canonical length of x, respectively.

Cycling and decycling

Given $x = \Delta^u x_1 x_2 \cdots x_k$ in its weighted form, there are two useful conjugations of x called the cycling $\mathbf{c}(x)$ and the decycling $\mathbf{d}(x)$ defined as follows:

$$\mathbf{c}(x) = \Delta^u x_2 \cdots x_k \tau^u(x_1),$$

$$\mathbf{d}(x) = \Delta^u \tau^u(x_k) x_1 \cdots x_{k-1} = (\mathbf{c}(x^{-1}))^{-1}.$$

- $\inf_c(x)$ and $\sup_c(x)$ denote the maximum of infimums and the minimum of supremums of all braids in the conjugacy class $C(x)$ of x, respectively.
- [Elrifi-Morton, 1994] If $\inf(x) < \inf_c(x)$, then an iterated cycling on x increases the infimum, that is, $\inf(x) < \inf(\mathbf{c}^N(x))$ for some positive integer N.

Invariant subsets of a conjugacy class

- [Garside, 1969] Summit set $SS(x) = \{y \in C(x) \mid \inf(y) = \inf_c(x)\}$
- [Elrifai-Morton, 1994] Super summit set $SSS(x)$
  $= \{y \in C(x) \mid \inf(y) = \inf_c(x) \text{ and } \sup(y) = \sup_c(x)\}$
- [S.Lee, 2000] Reduced super summit set $RSSS(x)$
  $= \{y \in C(x) \mid \mathbf{c}^M(y) = y = \mathbf{d}^N(y) \text{ for positive integers } M, N\}$
- [Gebhardt, 2005] Ultra summit set $USS(x)$
  $= \{y \in SSS(x) \mid \mathbf{c}^M(y) = y \text{ for some positive integer } M\}$
- $RSSS(x) \subset USS(x) \subset SSS(x) \subset SS(x)$
- All of them are finite sets that are invariant under conjugacy and so provide theoretical solutions for the conjugacy problem.

Nielson-Thurston classification

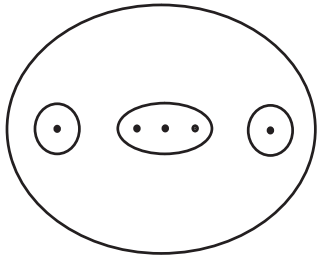
As a homeomorphism of a 2-dimensional disk that preserves n punctures and fixes the boundary of the disk, an n-braid x is isotopic to one of the following three dynamic types:

- periodic if $x^p = \Delta^{2q}$ for some nonnegative integers p, q;
- reducible if x preserves a set of disjointly embedded circles;
- pseudo-Anosov if neither (i) nor (ii).
  A pseudo-Anosov fixes a pair of measured foliations.

The dynamic type of a braid remains the same under taking a conjugation or a power.

Special reduction system for detection

- A set of disjointly embedded essential (i.e. separating punctures) circles preserved by a reducible braid is called a reduction system.



- An essential circle is standard if it intersects the axis containing all punctures exactly twice. A reduction system is standard if each circle in the system is standard.
- Standard reduction systems are especially nice in the sense that they can be recognized in polynomial time.
- Up to conjugacy, every reducible braid has a standard reduction system.

Relevant problems

Concerning Nielson-Thurston classification, we may consider two problems:

- **Reducibility Problem**
  Given a braid, determine its dynamic type.
- **Reduction Problem**
  Given a reducible braid, find a reduction system.

History - Reducibility and Reduction Problem

- [Humphries, 1991] Showed how to recognize split braids.
- [Bestvina-Handel, 1995] Using the "train track" algorithm, they solved both problems for any surface automorphism. But this is a typical exponential algorithm in both word length and braid index (or genus) and an implementation is rather nontrivial.
- [Bernardete-Nitecki-Gutiérrez, 1995] A standard reduction system is preserved by cycling and decycling, so for any reducible braid x, some braid in $SSS(x)$ must have a standard reduction system.
- [E.Lee-S.Lee, 2005] If the outermost component of a reducible braid x is simpler up to conjugacy then every braid in $RSSS(x)$ has a standard reduction system.

Special weighted form for detection

- A weighted form $x = \Delta^u x_1 \cdots x_k$ is (left) rigid if $x_k \lceil \tau^u(x_1)$.
- If x is rigid, then $c^{2\ell(x)}(x) = x = d^{2\ell(x)}(x)$ and so $x \in RSSS(x)$
- If $SSS(x)$ contains at least one rigid braid, then $USS(x) = RSSS(x)$ is the set of all rigid braid conjugate to x.
- For $1 \leq i \leq k$, a weighted form $x = \Delta^u x_1 \cdots x_k$ is (left) i-rigid if the first i factors are identical in the weighted forms of $x_1 \cdots x_k$ and $x_1 \cdots x_k \tau^u(x_1)$.
- A braid x is rigid iff it is $\ell(x)$-rigid.
- We can also consider the corresponding right versions.
- A braid x is tame if $\inf(x^i) = i \inf(x)$ and $\sup(x^i) = i \sup(x)$ for all $i \geq 1$.

Reducibility Algorithm - Input and Output

- Input:
  An n-braid x given as a word in the Artin generators
- Output:
  The dynamical type of x, that is, whether x is periodic, pseudo-Anosov, or reducible.
  Moreover, an orbit of reduction circle when x is reducible and rigid.

Notation: $D = \frac{n(n-1)}{2} = |\Delta|$

Reducibility Algorithm - Tame Power and SSS

Step I. We choose a positive integer $1 \le M \le D^2$ and $y \in SSS(x^M)$ such that x^M is tame via the following loop:

For $1 \le j \le D^2$, we test whether

- $\inf(\mathbf{d}^{D\ell(x)jD}\mathbf{c}^{D\ell(x)jD}(x^{jD})) = D\inf(\mathbf{d}^{D\ell(x)j}\mathbf{c}^{D\ell(x)j}(x^j))$
- $\sup(\mathbf{d}^{D\ell(x)jD}\mathbf{c}^{D\ell(x)jD}(x^{jD})) = D\sup(\mathbf{d}^{D\ell(x)j}\mathbf{c}^{D\ell(x)j}(x^j))$

by computing necessary weighted forms, and then return $M = j$ when the test passes, and set $y = \mathbf{d}^{D\ell(x)M}\mathbf{c}^{D\ell(x)M}(x^M)$.

[E.Lee-S.Lee, 2001] For any n-braid β, there is $1 \le M \le D^2$ such that β^M is tame.

[Birman-K-S.Lee, 2001] For any n-braid β,
$$\mathbf{d}^{D\ell(\beta)}\mathbf{c}^{D\ell(\beta)}(\beta) \in SSS(\beta).$$

Reducibility Algorithm - Periodic and 2-Rigid

Step II. If $y = \mathbf{d}^{D\ell(x)M}\mathbf{c}^{D\ell(x)M}(x^M) = \Delta^{2q}$ for some q, then conclude that x is periodic and halt. Otherwise, set

$$z = y^{2D}.$$

Then z is left and right 2-rigid.

Lemma[K-J.LEE] If β is tame and $\beta \in SSS(\beta)$, then β^{iD} is left and right i-rigid.

Reducibility Algorithm - Rigid

Step III. Test whether there exists an integer $0 \leq N \leq n!\ell(z)$ such that $\mathbf{c}^N(z)$ is rigid. If such an N does not exist, then conclude that x is reducible and halt. Or if $\mathbf{c}^N(z)$ is rigid, set $w = \mathbf{c}^N(z)$.

Theorem[K-J.Lee, Birman-González-Gebhardt, 2006]
If a n-braid β is pseudo-Anosov and tame, then every braid in $RSSS(\beta)$ is rigid.
Fact: The centralizer of a pseudo-Anosov braid is a free abelian group generated by a pseudo-Anosov braid and a periodic braid.

Theorem[K-J.LEE] If β is left and right 2-rigid, $\beta \in SSS(\beta)$, and is conjugate to a rigid braid, then $\mathbf{c}^N(\beta)$ is rigid for some $0 \leq N \leq \ell(\beta)n!$.

Reducibility Algorithm - Standard Circle

Step IV. Test whether there exists a permutation braid $t \in S_n$ such that $t^{-1}wt$ is rigid and $t^{-1}wt$ has at least one orbit of standard reduction circles. If such a t exists, conclude that x is reducible. Otherwise, conclude that x is pseudo-Anosov.

Theorem[K-J.LEE] Let β be a reducible, rigid n-braid. Then there exists a permutation n-braid t such that $t^{-1}\beta t$ is rigid and has at least one orbit of standard reduction circles.

[E.Lee-S.Lee, 2006] It takes $\mathcal{O}(\ell(\beta)n^3)$ to check whether a braid β has a standard reduction circle.

Reducibility Algorithm - Complexity

- The complexity in canonical length is dominated by Step I and it is $\mathcal{O}(\ell(x)^3)$.
- The complexity in braid index is dominated by Step III and IV and it is $\mathcal{O}(n!)$.
- The over-all complexity is $\mathcal{O}(\ell(x)^3 n!)$.

Sketchy Proof of Cycling-Bound Theorem

Theorem. If x is left and right 2-rigid, $x \in SSS(x)$, and is conjugate to a rigid braid, then $\mathbf{c}^N(x)$ is rigid for some $0 \leq N \leq \ell(x)n!$.

- Since $USS(x) = RSSS(x)$ contains a rigid braid, iterated cyclings on x must produce a rigid braid. Let $y = \mathbf{c}^N(x)$ be the rigid braid obtained from x by the minimal number of iterated cyclings.

Proof of Cycling-Bound Theorem (cont.)

Theorem. If x is left and right 2-rigid, $x \in SSS(x)$, and is conjugate to a rigid braid, then $\mathbf{c}^N(x)$ is rigid for some $0 \le N \le \ell(x)n!$.

- Assume $\inf y = 0$ for simplicity. Let $y = y_1 y_2 \cdots y_k$ be the weighted form.
- By induction on i, one can prove that for all $1 \le i \le N$

$$\mathbf{c}^{N-i}(x) = a_i y_{[1-i]} z_i$$

for a permutation braid a_i with $y_{[2-k-i]} \cdots y_{[-1-i]} y_{[-i]} \succ_R a_i$ and a positive braid $z_i = y_{[2-k-i]} \cdots y_{[-1-i]} y_{[-i]} a_i^{-1}$ where $[m]$ denotes the integer between 1 and k that equals m mod k.

- $\mathbf{c}^{N-i}(x)$ is completely determined by a nontrivial permutation braid a_i. For each $1 \le i \le \ell(x)$, there are at most $n!$ distinct a_i's. Thus $N \le \ell(x)n!$.

An Alternative to Standard-Circle Theorem

Theorem. Let x be a reducible, rigid n-braid. Then there exists a permutation n-braid t such that $t^{-1}xt$ is rigid and has at least one orbit of standard reduction circles.

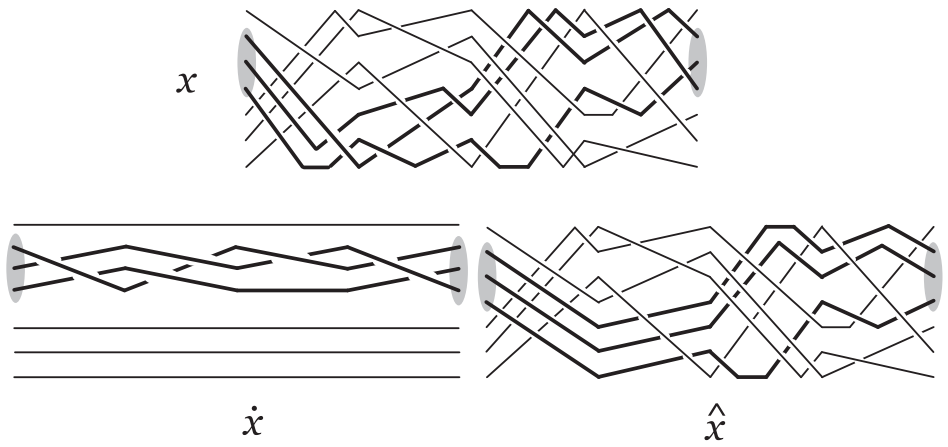
In $RSSS(x)$ of a reducible, rigid braid x, every braid has a braid with standard reduction circle near by (i.e. conjugation by a permutation braid). From the view point of a reducible, rigid braid with standard circle, an equivalent statement is:

Theorem′. Suppose that a reducible n-braid x is rigid and has an orbit of standard circles starting with a standard circle C. If β is a positive n-braid such that $\beta^{-1}x\beta$ is rigid and $\alpha(C)$ is not standard for any $e \precneqq \alpha \prec \beta$ such that $\alpha^{-1}x\alpha$ is rigid, then $\ell(\beta) \leq 1$.

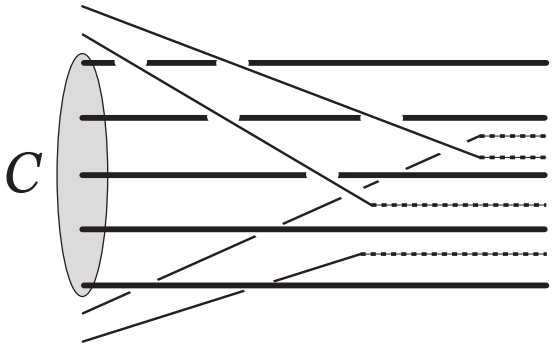
Decomposition of reducible braids

If a reducible n-braid x has an orbit of standard reduction circles, then x^j has a standard reduction circle for some $1 \leq j \leq n$.

Assume x preserves a standard circle. Then C uniquely determines a decomposition $x = \dot{x}\hat{x} = \hat{x}\dot{x}$.



Ingredients for Standard-Circle Theorem′



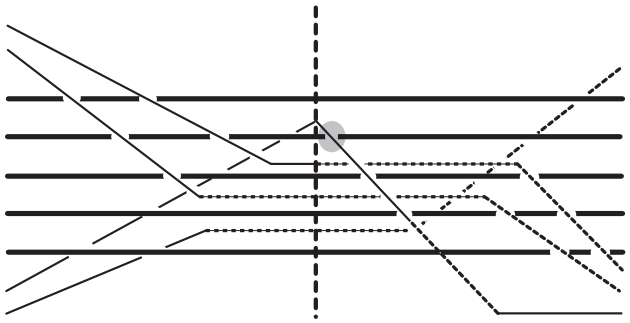
For a standard circle C, a permutation n-braid β is called a destroyer of C if $\alpha(C)$ is not standard for all $e \precneqq \alpha \prec \beta$.

Destroyer Lemma. Suppose that a reducible n-braid x is rigid and has a standard circle C. If β is a permutation n-braid such that $\beta^{-1}x\beta$ is rigid and $\alpha(C)$ is not standard for any $e \precneqq \alpha \prec \beta$ such that $\alpha^{-1}x\alpha$ is rigid, then β is a destroyer of C.

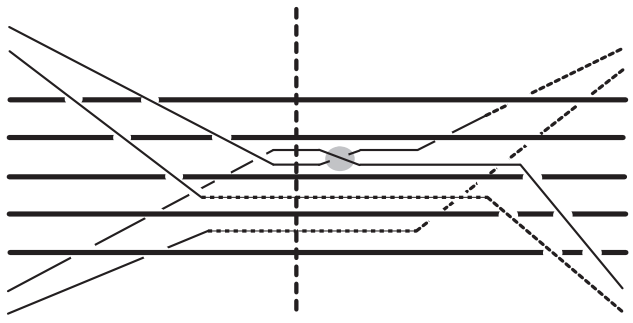
Subword Lemma. Suppose that an n-braid x is rigid and $\ell(x) \geq 2$. If γ is a positive n-braid such that $\gamma^{-1}x\gamma$ is rigid and $\ell(\gamma) \geq 2$ then there is a positive braid β such that $\beta^{-1}x\beta$ is also rigid, $\ell(\beta) \geq 2$, and moreover β is a left subword of either $\gamma \wedge x^i$ or $\gamma \wedge x^{-i}$ for some $i \geq 1$, where assuming $\inf(x) = 0$ for simplicity.

Sketchy proof of Standard-Circle Theorem′

- We assume that $\inf(x) = 0$ and $x(C) = C$ for simplicity.
- Suppose $\ell(\gamma) \geq 2$. By Subword Lemma, we may assume that $\gamma \prec x^i$ for some $i \geq 1$. The case $\gamma \prec (x^{-1})^i$ is similar since $x^i(C) = C = (x^{-1})^i(C)$.
- Let $\gamma_1\gamma_2$ be the first two factors in the weighted form of γ. By Destroyer Lemma, γ_1 must be a destroyer of C.
- Since $\gamma_1\gamma_2$ is left weighted, γ_2 must start with one of two types of crossings given in Figure Type I and Type II.



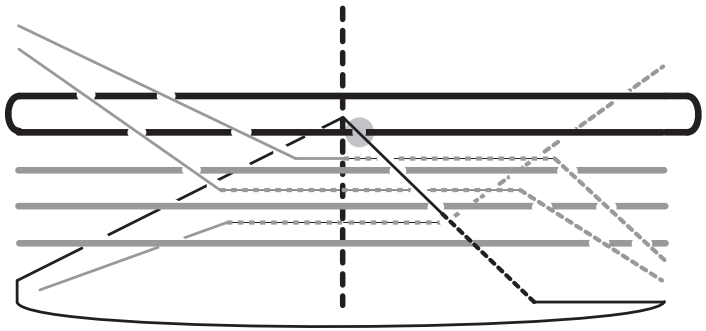
TypeI



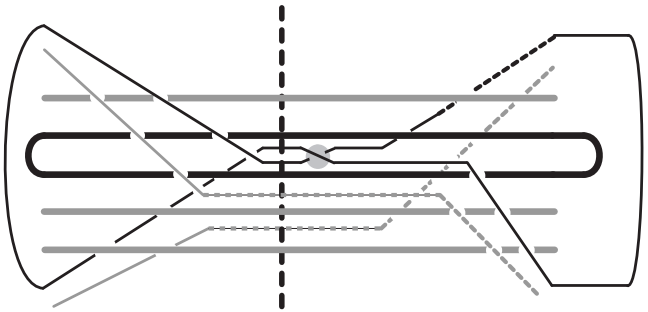
TypeII

Proof of Standard-Circle Theorem′ (cont.)

- Two components of the link obtained from $\gamma_1\gamma_2$ of type I via the plat closing for two inner strands and Markov closing for an outer stand has the linking number 1.
- Two components of the link obtained from $\gamma_1\gamma_2$ of type II via plat closings for two pairs of inner and outer strands has the linking number 2.
- This is a contradiction since a positive braid x^i preserve the circle C and the two component links must split.



Type I



Type II

Two Smmarizing Theorems

The results that were needed for our reducibility algorithm can be summarized as two theorems:

Theorem. Every pseudo-Anosov braid is "virtually" rigid, that is, it is rigid up to taking powers, iterated cycling and decycling. Furthermore powers and numbers of iterations have upper bounds prescribed by canonical length and braid index.

Theorem. Every reducible, rigid braid is at most one conjugation by a permutation braid away from another reducible, rigid braid with an orbit of standard circles.

Comment on Reduction Problem

- Rigidity is inherited to $\dot{x}$ or $\hat{x}$.
- By inductively applying Step 4 of our algorithm to $\dot{x}$ or $\hat{x}$, one can find a whole reduction system for a reducible braid that is virtually rigid.