The Conjugacy Problem in the Braid Group

Jonathan Boiser

August 13, 2009
Acknowledgements

- Dr. Imre Tuba
- Dr. Michael O’Sullivan
- Dr. Marie Roch
- Dr. Sam Shen
- The students of the 2009 REU.
Outline of Thesis

Title: Computational Problems in the Braid Group

Contents:

▶ A detailed development of the solution to the word and conjugacy problems in $B_n$ from the 1960’s to the present day.
▶ A chapter on implementing software for braids.
▶ Miscellaneous topics: Garside groups, braid group cryptography.

Page count: > 80 pages without appendices.
Focus of this Talk

The conjugacy decision and search problems in the braid group.
Definition: Braid Group

$B_n$, the (Artin) braid group on $n$ strands has the following presentation:

Generators: $\sigma_1, \ldots, \sigma_{n-1}$

Relations:

1. $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $|i - j| > 1$.
2. $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ for $i = 1, \ldots, n-2$. 
Geometric Interpretation of Braids
Geometric Interpretation of Generators

\[ i \quad i + 1 \]
\[ \sigma_i \]

\[ i \quad i + 1 \]
\[ \sigma_i^{-1} \]
Geometric Interpretation of Relations

Simple example:

\[ \sigma_1 \sigma_2 \sigma_1 \sigma_4 = \sigma_4 \sigma_1 \sigma_2 \sigma_1 = \sigma_4 \sigma_2 \sigma_1 \sigma_2 = \sigma_2 \sigma_4 \sigma_1 \sigma_2 = \cdots \]
Definition: Conjugacy Decision Problem

Let \( x, y \in B_n \). \( x \) is said to be *conjugate* to \( y \) if there exists a \( c \in B_n \) such that \( y = c^{-1}xc \).

The *conjugacy decision problem* (CDP) in \( B_n \) asks: given \( x, y \in B_n \), is there a method for determining, in a finite amount of time, whether \( x \) is conjugate to \( y \) (symbolized as \( x \sim y \))?
Definition: Conjugacy Search Problem

The *conjugacy search problem* (CSP) in $B_n$ asks: given $x, y \in B_n$ such that $x \sim y$, is there a method for determining, in a finite amount of time, a $c \in B_n$ such that $c^{-1}xc = y$?

We collectively refer to the conjugacy search and decision problems as the *conjugacy problem*. 

Motivation: Braid Group Cryptography

A number of cryptosystems have been proposed, whose security depends on the intractability of the conjugacy search problem in $B_n$.

For example, in the Anshel-Anshel-Goldfeld key exchange protocol, both parties send their secret key $s$ “hidden” within a number of conjugates.

$$\{s^{-1}a_1s, \ldots, s^{-1}a_ks\}$$

where the $a_i$ are public.

An adversary can only recover the secret key if he can solve the multiple conjugacy search problem for those $k$ conjugates.
Main Problem:

Is there a polynomial-time algorithm for solving the conjugacy problem in $B_n$?

(That is, polynomial in $n$ and some measure of the braids’ complexity).
Decomposition of the Main Problem

Parts:

1. Do solutions to the CDP/CSP exist? (Yes)
2. Are the algorithms required to compute the solution efficient independently of the input? (Yes)
3. Is the CDP/CSP efficiently solvable in some special cases? (Yes)
4. Is the CDP/CSP efficiently solvable in all cases? (Unknown)
Part 1: Does a Solution Exist?

Solution to conjugacy problem is *a priori* unknown.

For a non-identity \( w \in B_n \), the conjugacy class

\[ [w] := \{ c^{-1}wc : c \in B_n \} \]

is infinite, ruling out exhaustive or undirected search.
A Finite, Invariant Subset of $[w]$

Let $w, w' \in B_n$. Suppose there is a set $S^*(w)$ such that

1. $S^*(w)$ is finite.
2. $S^*(w) = S^*(w')$ if and only if $w \sim w'$.

Then, the CDP for $w, w'$ can be solved by computing $S^*(w)$ and one element of $S^*(w')$. If the two sets intersect, then $w \sim w'$. 
Definition: Garside Normal Form

To define this finite, invariant subset, we require the Garside normal form of a braid:

Every $w \in B_n$ has a unique normal form

$$w = \Delta^m p$$

where $\inf w = m \in \mathbb{Z}$ is the \textit{infimum} of $w$, $p$ is a positive braid, and $\Delta$ is the fundamental braid.
Illustration of the Geometric Braid ∆
Lattice Structure of $B_n^+$

The set of positive braids, $B_n^+$ has a partial order $(B_n^+, \leq_L)$, defined by $x \leq_L y$ if there is a $z \in B_n^+$ such that $xz = y$. This is sometimes known as the “prefix order”.

The prefix order is also a lattice in that, for any $x, y \in B_n^+$, the meet $x \wedge_L y$ and join $x \vee_L y$ exist.
Lattice Structure of \( B^+_n \)

The set \( \mathcal{D} := \{ x : e \leq_L x \leq_L \Delta \} \) is an important set in the theory:
Definition: Left-Canonical Form

The left-canonical form of a braid $w$ is the factorization

$$w = \Delta^m p_1 \ldots p_k$$

Where, for all, $i$, $p_i \in D$ and $p_i = p_i \ldots p_k \land L \Delta$.

The supremum of $w$ is given by $\sup w = m + k$ and the canonical length of $w$ is given by $\text{len} w = k$. 
Suppose \( w \in B_n \) and \( \inf w = m \). Define

\[
[w]_m := \{ x \in [w] : \inf x \geq m \}
\]

Theorem: \([w]_m\) is finite.
An Invariant Subset of \([w]\)

Since \([w]_m\) is finite, there exists a subset \(SS(w) \subset [w]_m\) consisting of braids with maximal infimum.

\[
SS(w) := \{ x \in [w]_m : \inf x \text{ maximal} \} \\
= \{ x \in [w] : \inf x \text{ maximal} \}
\]

This solves the CDP, since \(w \sim w'\) iff \([w] = [w']\) iff \(SS(w) = SS(w')\).
Mt. Infimum and the Summit Set

$SS(w)$

w
Improvements to the Summit Set

Summit Set \( SS(w) := \{ x \in [w] : \inf x \ \text{maximal in} \ [w] \} \)

Super Summit Set \( SSS(w) := \{ x \in SS(w) : \sup x \ \text{minimal in} \ SS(w) \} \)

Ultra Summit Set \( USS(w) := \{ x \in SSS(w) : c^N(x) = x \ \text{for some} \ N > 0 \} \)

\([w] \supset SS(w) \supseteq SSS(w) \supseteq USS(w)\)

The operator \( c \) is known as \textit{cycling}, which is a special type of conjugation.
Part 2: Are the Main Computations Efficient?

Primary tasks:

1. Compute normal forms.
2. Find a single element of the super (ultra) summit sets.
3. Derive new super (ultra) summit set elements from a previously-found element.

All of these procedures have algorithms that run in polynomial time. They are the subject of Chapters 3 and 4 in the thesis.
Graphical Overview of Solution
Part 3: Are there Special Cases of the Conjugacy Problem?

Nielsen-Thurston Classification: Every self-homeomorphism of a topological space is either periodic, reducible, or pseudo-Anosov.

Braids have an alternative definition as certain isotopy classes of self-homeomorphisms of the $n$-punctured disk. Therefore, they too can be classified according to the Nielsen-Thurston trichotomy.

As far as the conjugacy problem is concerned, this division has allowed the three classes of braids to be examined independently.
Conjugacy Problem for Periodic Braids

Roughly, a braid $w$ is periodic if there exists an $m > 0$ such that $w^m = \Delta^{2k}$ for some integer $k$. For example, $\sigma_1 \sigma_2 \sigma_3 \in B_4$ is periodic.

It was found by Birman et al. that the CDP/CSP for periodic braids has a polynomial-time solution.
Part 4: Is the Conjugacy Problem Always Efficiently Solvable?

Remaining cases: pseudo-Anosov and reducible braids.
Definition: Rigid pseudo-Anosov Braid

A “randomly” chosen braid is pseudo-Anosov with high probability. That is, PA is the generic case.

A braid is *rigid* if its image under cycling is already in left canonical form. That is, cycling corresponds to a cyclic shift of the braid’s factors:
Definition: Reducible Braid

In braid-specific terms, a braid is reducible, if it can be decomposed into a family of subbraids at different scales:

By the Nielsen-Thurston trichotomy, at some point you only have irreducible braids, which must be periodic or PA.
Four Open Questions

Birman, Gebhart, Gonzales-Meneses: An efficient algorithm to solve the conjugacy problem for $B_n$ can be found if the following open problems are solved in the affirmative:

1. Does there exist a fast algorithm to determine whether a braid is reducible and, if so, find its decomposition into irreducible braids?
2. If $x$ is a rigid braid, is its ultra summit set small?
3. If $y \in SSS(x)$, is there a small power $M$ such that $c^M(y) \in USS(x)$?
4. If $x$ is a pseudo-Anosov, rigid braid, can its centralizer be computed efficiently?
Suppose that the four open problems are solved in the affirmative. Then, if $x, y$ are PA braids,

1. A small power of $x$, $x^K$ is such that $USS(x^K)$ consists entirely of rigid braids (Theorem).
2. $USS(x^K)$ is small (Open Problem 2).
3. A $y' \in USS(y^K)$ can be found quickly (Open Problem 3).
4. For all braids, $x^K \sim y^K$ if and only if $x \sim y$ (Theorem). Thus the CDP is solved.
5. For PA braids, if $c$ conjugates $x^K$ to $y^K$, then $c$ conjugates $x$ to $y$ (Theorem). CSP is solved.
Solution for Reducible Braids

Depends on Open Question 1 which involves finding decompositions, and Open Question 4 for computing centralizers.
Garside Groups

A generalization of the braid groups.

Main characteristics of a Garside group $G$:

- Set of positive elements comprises a monoid with a lattice structure similar to $B_n^+$’s.
- Positive monoid has a *Garside element* $\Delta \in G$ whose properties are similar to $\Delta \in B_n$.

Full definition is more involved.
Example

From Picantin:

$$M_\chi := \langle x, y, z \mid xzxy = yzxx, yzxxz = zxyzx, zxyzx = xzxyz \rangle$$

$$M_\kappa := \langle x, y \mid xyxyxyx = yy \rangle$$
The structure of a Garside group can be gleaned from the lattice structure of its positive monoid $M$.

By the solution to the word problem in Garside groups, this structure can be further condensed to the sublattice of $\Delta$’s factors.
A Geometric Approach

For a Garside group $G$, the geometry of its Cayley graph may provide a means of doing computations in $G$.

For example, the left-canonical form of a word $w \in G$ can be done using the Cayley graph of $\mathcal{D} \subset G$. 
Example

To illustrate this idea: I calculated the LCF of the word $w \in M_\chi$ by hand using the Cayley graph of $\mathcal{D} \subset M_\chi$.

$$w = xxzxyzxxzxyxxyzx$$

$$= (xxzxy)(zxx)(zxyxx)(yzx)$$

$$= \Delta(xx)(zxyxx)(yzx)$$

$$= \Delta(xxz)(xy)(xx)(yzx)$$

$$= \Delta(xxzx)(y)(xx)(yzx)$$

$$= \Delta(xxzxy)(xx)(yzx)$$

This process is not as nice as that for braids, due to the different connectivity properties of this Cayley graph.
How can one do computations in general Garside groups? For example, what data structures, algorithms, etc. can be utilized?

Can the algebraic theory of $B_n$ be recast in a geometric framework? (Geometric group theory)
Thank you!