

Computational properties of braid groups

Three computational problems for groups:

Let S be a set of generators for a group G .

1) The Word Problem:

if $s_i, s_i' \in S$ $\forall i$ and

$g_1 = s_1 \dots s_m$, $g_2 = s_1' \dots s_n'$, does $g_1 = g_2$?

2) The Conjugacy Problem:

Given two words w_1, w_2 , is w_1 conjugate as a group elt to w_2 ?

3) The Conjugator Search Problem

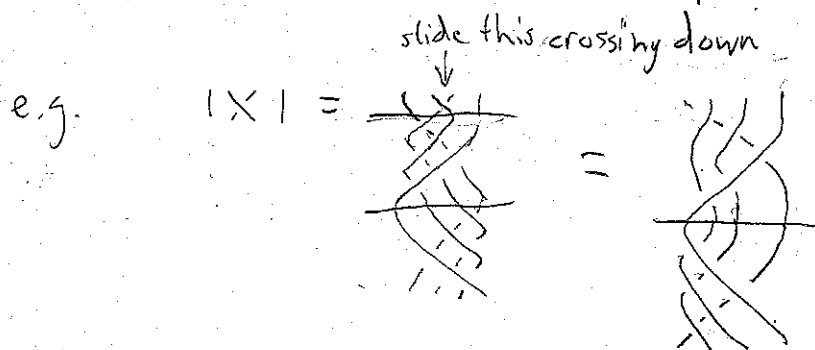
Given two words w_1, w_2 which represent conjugate group elements, find a word a such that $w_1 = aw_2a^{-1}$.

- The word problem is undecidable in general.
- The conjugacy problem contains the word problem as a special case (i.e. is $w_2^{-1}w_1 \neq e$).
- Conjugator search is decidable, but exponential in the length of w_1, w_2 in general (as far as we know)

Braid groups are examples of automatic groups. This gives them a quadratic time word problem and a normal form for each group element.

Prop: Any braid $b \in B_n$ can be expressed in the form $\Delta_n^k b^+$, where $k \in \mathbb{Z}$ and $b^+ \in B_n^+$

Pf: Any σ_i^{-1} appearing in a braid word expressing b can be rewritten as $\Delta_n^{-1} \Delta_n \sigma_i^{-1}$. Sliding σ_i^{-1} into Δ_n allows it to cancel with one of the crossings in Δ_n . The result is a positive braid expression of $\Delta_n \sigma_i^{-1}$



Using the commutativity property of Δ_n , one can slide all Δ_n^{-1} to the left side of the word. This gives a word of the form $\Delta_n^{-i} b^+$ for some $i \in \mathbb{N}$. \square

There will be many ways to produce a word of the form $\Delta_n^k b^+$ equivalent to b , however,

Prop: Let $b \in B_n$. Then b has a canonical expression of the form $\Delta_n^k b^+$

Pf: For a given braid b , let $c(b) = \# \text{ positive crossings} - \# \text{ negative crossings}$. $c(b)$ is a homomorphism $c: B_n \rightarrow \mathbb{Z}$ (check!).

This result isn't really necessary for the proof, but makes the situation a little clearer.

Since Δ_n has $\frac{n(n-1)}{2}$ positive crossings, we have

$$c(b) = \left(\frac{n(n-1)}{2}\right) \cdot k + (\# \text{ crossings in } b^+).$$

Thus, there is some representative with maximal k .

Given a braid word b^+ , one may attempt to slide a crossing left to σ_i as follows:

(we'll write the braids sideways so that left in words agrees with left in pictures)

In class

I presented an incorrect algorithm for sliding a crossing to the left of a positive braid using only R-III moves. The algorithm incorrectly gives up when a slide is possible. This algorithm was the basis of the rest of my proof.

There is a linear time algorithm for sliding a crossing when it is possible, so the proof in these notes can be made to work.

However, once you see what that algorithm does it becomes apparent that sliding crossings in the order specified in this proof is not the most efficient or conceptually simple way to proceed. Therefore I have rewritten the proof (see the next section of notes).

The exact braid that results depends on which Reidemeister III moves we chose to apply; but any two such braids differ only by R-III moves which do not involve the leftmost crossing.

* Note that applying an R-III move to an element of b^+ does not change whether it is possible to slide a crossing left to σ_i or not. (check!)

Observation: Δ_n can be written as follows

$$\Delta_n^W \sigma_{n-1} \sigma_{n-2} \dots \sigma_1 \sigma_{n-1} \sigma_{n-2} \dots \sigma_2 \dots \sigma_{n-1} \sigma_{n-2} \sigma_{n-1}$$

The procedure for finding the canonical form of b is as follows:

Begin by ^{computing} $b = \Delta_n^W b^+$ (as in the above proposition)
let b' be the empty word.

This gives a maximal collection of slid crossings such that no strand crosses itself twice.

Repeat the following until b^+ is the empty word:
For each letter σ_i in Δ_n^W , slide a crossing to the left of σ_i , provided a) it is possible, and b) we have not previously slid a crossing that crossed the same two strands at this step. If we succeed, getting $\sigma_i \hat{b}$, set $b' := b' \sigma_i$, $b^+ := \hat{b}$.

b' may now begin with some copies of Δ_n . The canonical form \bar{b} is given by $\Delta_n^k b'$ with copies of $\Delta_n \Delta_n$ cancelled out.

This form is called the greedy normal form

To prove that this form is actually canonical one needs to show the following:

- 1) If $b \rightarrow c$ via a R-III move, $\bar{b} = \bar{c}$
- 2) If $b \rightarrow c$ via inserting $\sigma; \sigma^{-1}$, $\bar{b} = \bar{c}$.

We're essentially done (1) already: If b and c differ by an R3 move, so do $\Delta_n^k b^+$ and $\Delta_n^{k'} c^+$ (and $k=k'$).

If b and c differ by an R-II move ($\sigma; \sigma^{-1} = \text{Id}$)

Then (WLOG) we have

$\Delta_n^k b^+$ and $\Delta_n^{k-1} c^+$, where c^+ is b^+ with a copy of Δ_n inserted somewhere.

Since this copy of Δ_n can be pulled back to the left using only R-III moves, the greedy normal form \bar{c} for c must be

$$\Delta_n^{k-1} \hat{c}^+ = \Delta_n^{k-1} \Delta_n \hat{b}^+ = \Delta_n^k \hat{b}^+ = \bar{b}.$$

Aside:

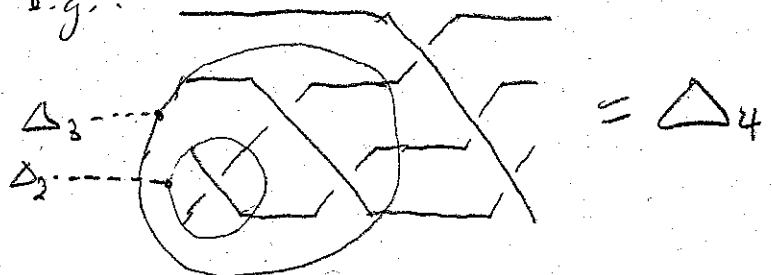
A note about Δ_n :

- We often appeal to the pictures in this argument.
 If one wants to work more algebraically, the following formula is helpful:

$$\Delta_n = i(\Delta_{n-1}) \sigma_1 \sigma_2 \dots \sigma_{n-1}$$

where $i: \mathcal{B}_{n-1} \rightarrow \mathcal{B}_n$ is the inclusion given by adding a strand on the left.

e.g.:



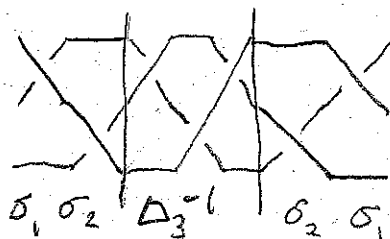
Greedy Normal Form by example

Start with a braid word b :

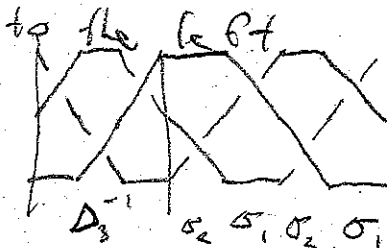
$$\sigma_1 \sigma_2 \sigma_2^{-1}$$

Replace each σ_i^{-1} with $\Delta_n^{-1} \cdot b^+$, with $b^+ \in \mathcal{B}_n^+$.

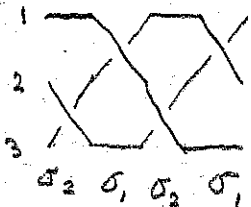
$$\sigma_2^{-1} = \Delta_3^{-1} \Delta_3 \sigma_2^{-1} = \Delta_3^{-1} \sigma_2 \sigma_1 \sigma_2 \sigma_2^{-1} = \Delta_3^{-1} \sigma_2 \sigma_1$$



Use the commutation relation for Δ_n^{-1} to slide each Δ_n^{-1} to the left.

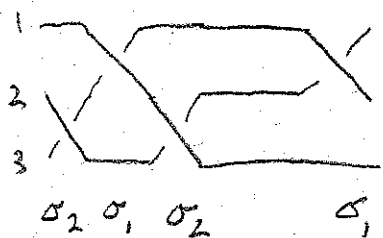


This gives $\Delta_n^{-k} b^+$ for some (new) $b^+ \in \mathcal{B}_n^+$, $k \in \mathbb{N}$
 Set Δ_n^{-k} aside. Number the strands in increasing
 order:



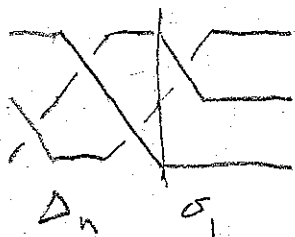
Associate with each crossing the pair of strand
 numbers which cross ^{largest first}. These pairs have a lexicographic
 order, e.g. $(6, 2) > (6, 1) > (5, 4)$

Slide over a maximal set of crossings such
 that no pair of strand numbers repeats, choosing
 larger pairs before smaller



Here: $(3, 2), (3, 1), (1, 2)$ is greedy and maximal.

Repeat until every crossing has been slid over



Glue Δ_n^{-k} back on and cancel with copies
 of Δ_n at the beginning of b^+ : $\underline{\Delta_n^{-k} b^+}$