# Pure Braid Group

Hannah Lewis

At the center of a crypto system is a mathematical trapdoor, that is, a computational problem that is easy to do in one direction (encryption) but hard to do in reverse (decryption). Mathematicians search for trapdoors that involve computations in non-commutative structures that provide more security in crypto systems. One such problem is the conjugacy problem in group theory. I have been studying the conjugacy problem in the pure braid group.

There are two ways to look at the braid group $B_n$

- Geometrically
- Algebraically

# Definition

Geometrically, an n-braid is a collection of n disjoint strings where the endpoints are fixed.

# Definition

Geometrically, an n-braid is a collection of n disjoint strings where the endpoints are fixed.

In $B_n$ the endpoints can be permuted.
In $P_n$ the endpoints are not permuted.
So $P_n$ is the kernel in the homomorphism $g : B_n \to S_n$
that sends a braid to the appropriate permutation of the endpoints. In particular, $P_n$ is a normal subgroup of $B_n$ of index $n!$.

# Definition

Geometrically, an n-braid is a collection of n disjoint strings where the endpoints are fixed.

In $B_n$ the endpoints can be permuted.
In $P_n$ the endpoints are not permuted.
So $P_n$ is the kernel in the homomorphism $g : B_n \to S_n$
that sends a braid to the appropriate permutation of the endpoints. In particular, $P_n$ is a normal subgroup of $B_n$ of index $n!$.

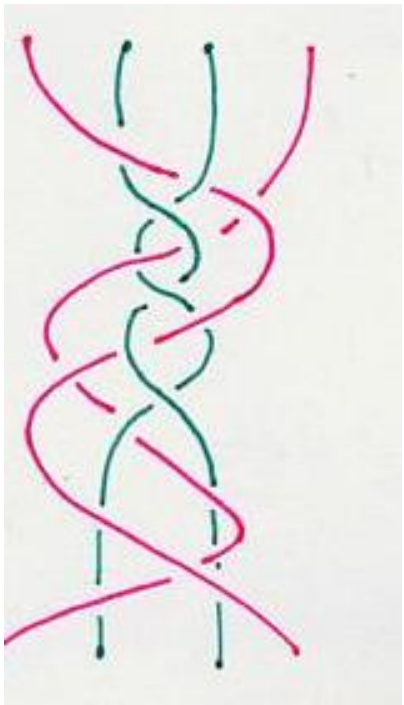


Figure 1: Braid

# Definition

Geometrically an n-braid is a collection of n disjoint strings where the endpoints are fixed.

In $B_n$ the endpoints can be permuted.
In $P_n$ the endpoints are not permuted.
So $P_n$ is the kernel in the homomorphism $g : B_n \to S_n$ that sends a braid to the appropriate permutation of the endpoints. In particular, $P_n$ is a normal subgroup of $B_n$ of index $n!$.

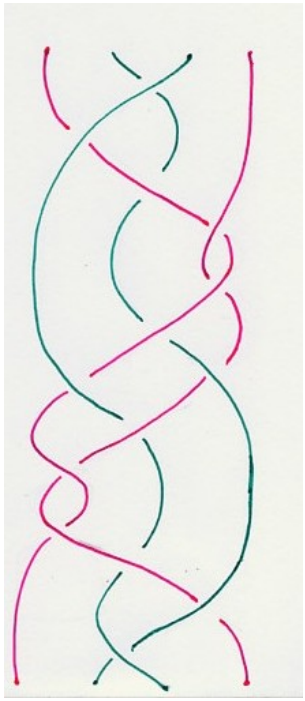
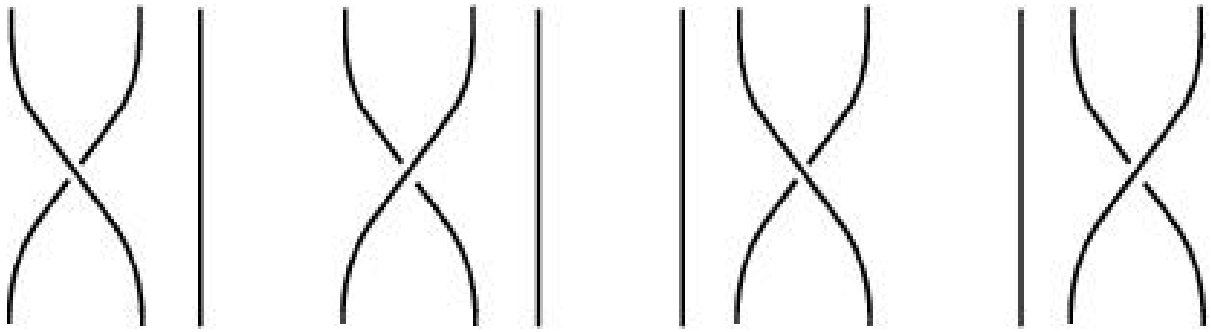


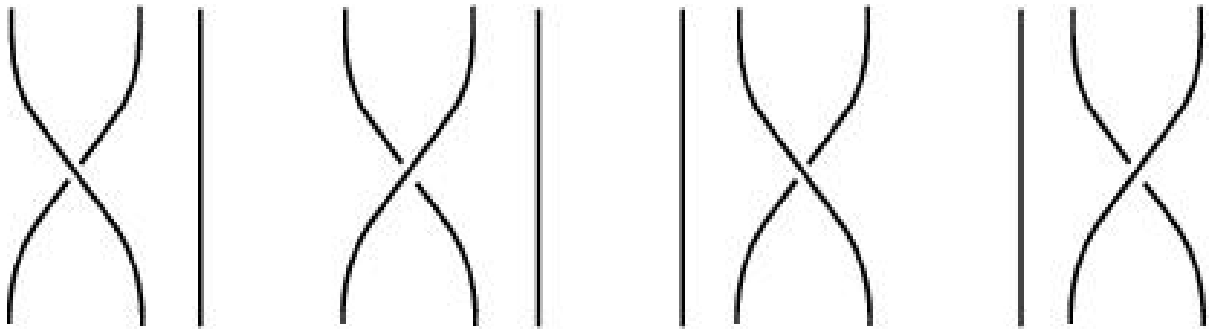
Figure 2: Pure Braid

$B_n$ has a presentation:
$\langle \sigma_1, ...\sigma_{n-1} \,|\, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1},\ \sigma_i\sigma_j = \sigma_j\sigma_i \rangle$
where $i = 1, ..., n-2$, $j = 1, ..., n-1$, $|i-j| > 1$

$B_n$ has a presentation:
$\langle \sigma_1, ...\sigma_{n-1} \,|\, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1},\ \sigma_i\sigma_j = \sigma_j\sigma_i \rangle$
where $i = 1, ..., n-2$, $j = 1, ..., n-1$, $|i-j| > 1$
In $B_3$:



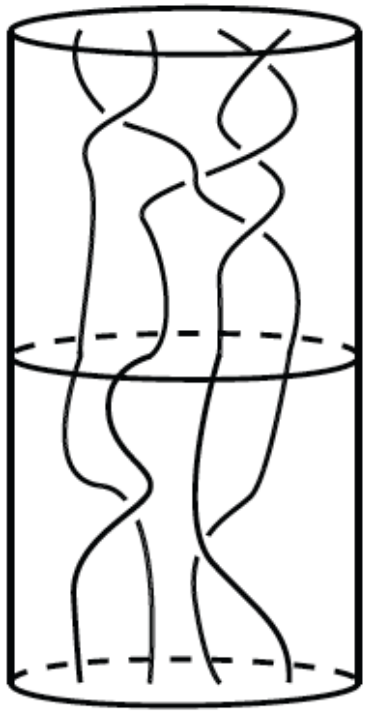
$B_n$ has a presentation:
$\langle \sigma_1, ...\sigma_{n-1} \,|\, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1},\ \sigma_i\sigma_j = \sigma_j\sigma_i \rangle$
where $i = 1, ..., n-2$, $j = 1, ..., n-1$, $|i-j| > 1$
In $B_3$:




In any $B_n$, $\sigma_i$'s continue to correspond to the simplest non trivial braids with one crossing between two adjacent strands.

## Definition (Multiplication in $P_n$ and $B_n$)

Concatenation of braids. This works both geometrically and algebraically.



$w_1 = \sigma_1^{-1}\sigma_3^{-2}\sigma_2\sigma_3^{-1}$
$w_2 = \sigma_1^{-1}\sigma_3$
$w_1 \times w_2 = \sigma_1^{-1}\sigma_3^{-2}\sigma_2\sigma_3^{-1}\sigma_1^{-1}\sigma_3$

In $P_n$, if one forgets the $n^{th}$ strand of an $n$ braid, one obtains an $n-1$ braid. Thus we have a homomorphism:

$$f : P_n \to P_{n-1}$$

The kernel of $f$, denoted by $\ker f$, turns out to be a free group on $n-1$ generators.

In $P_n$, if one forgets the $n^{th}$ strand of an $n$ braid, one obtains an $n-1$ braid. Thus we have a homomorphism:

$$f : P_n \to P_{n-1}$$

The kernel of $f$, denoted by ker$f$, turns out to be a free group on $n-1$ generators.
In fact we have an isomorphism:

$$\text{ker}f \to \pi_1(D - \{p_1, ..., p_{n-1}\}) = F(\alpha_1, ..., \alpha_{n-1})$$

In $P_3$: this looks like:

Because we also know that $P_{n-1}$ is a subgroup of $P_n$, the pure braid group on $n$ strands can be written as a semi-direct product:

$$P_n = F(\alpha_1, ..., \alpha_{n-1}) \rtimes P_{n-1}$$

This can be used to inductively produce presentations of $P_n$. For this we need a presentation of $P_{n-1}$, and we need to understand how $P_{n-1}$ acts of the free group $F$.The first interesting case is $n = 3$.

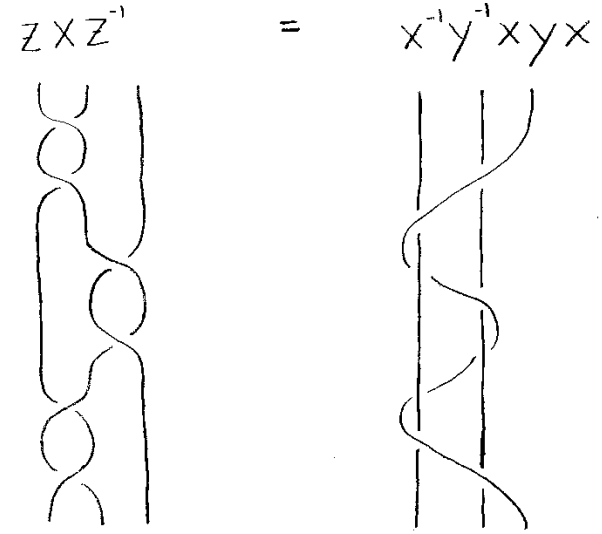
$P_2$ is infinite cyclic generated by $z = \sigma_1^2$
This leads to a presentation for $P_3$:

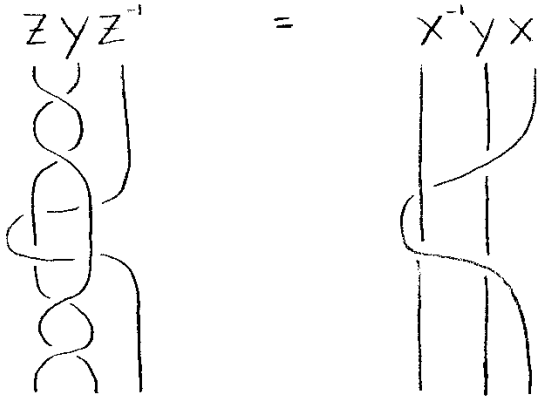
$$P_3 = < \alpha_1, \alpha_2, z \mid z\alpha_1 z^{-1} = w_1,\ z\alpha_2 z^{-1} = w_2 >,$$

We need to understand how to write $w_1$ and $w_2$ in terms of $\alpha_1$ and $\alpha_2$. It turns out that:
$w_1 = \alpha_1^{-1}\alpha_2^{-1}\alpha_1\alpha_2\alpha_1$

$w_2 = \alpha_1^{-1}\alpha_2\alpha_1$

Recall that: $\alpha_1 = \sigma_2^2$, $\alpha_2 = \sigma_2\sigma_1^2\sigma_2^{-1}$
The expressions for $w_1$ and $w_2$ are obtained by combing the appropriate braids.
For ease of notation $\alpha_1 = x$, $\alpha_2 = y$.


$zxz^{-1}$
=
$x^{-1}y^{-1}xyx$


$zyz^{-1}$
=
$x^{-1}yx$

In summary, we obtain the presentation:

$$\langle x, y, z \,|\, zxz^{-1} = x^{-1}y^{-1}xyx,\ zyz^{-1} = x^{-1}yx \rangle$$

where $x = \sigma_2^2$, $y = \sigma_2\sigma_1^2\sigma_2^{-1}$, $z = \sigma_1^2$ If we set $c = z^{-1}x^{-1}y^{-1}$, we obtain the presentation:

$$< x, y, c | xc = cx, yc = cy >$$

This shows that $P_3$ is a direct product

$$F(x, y) \times \langle c \rangle.$$

## Normal Form

Move all the c's to the right using the following relations:

$xc = cx$

$yc = cy$

## Word Problem

After putting the word in normal form and free reductions, if the result is the empty word, then the braid is trivial.

## Conjugacy Problem

Suppose we have two words, $w_1$ and $w_2$. We write these words in normal form:

$$w_1 = u_1 c^{m_1}, w_2 = u_2 c^{m_2}, \text{where } u_i \in F(x, y)$$

## Conjugacy Problem

Suppose we have two words, $w_1$ and $w_2$. We write these words in normal form:

$$w_1 = u_1 c^{m_1}, w_2 = u_2 c^{m_2}, \text{where } u_i \in F(x, y)$$

$$w_1 \sim w_2 \text{ if and only if } m_1 = m_2 \text{ and } u_1 \sim u_2 \text{ in } F(x, y)$$

Recall the conjugacy problem in the free group:
Given two words, $w_1$, $w_2$ in $F(x, y)$, cyclically reduce $w_i$ to $w_i'$.
Then, $w_1 \sim w_2 \Leftrightarrow w_2'$ is a cyclic permutation of $w_1'$.

Now that we have generators for $P_3$, we can say:
$P_4 = F(\alpha_1, \alpha_2, \alpha_3) \rtimes \langle x, y, c \,|\, xc = cx,\ yc = cy \rangle$
Then we start combing the braids

$$x\alpha_1 x^{-1},\ x\alpha_2 x^{-1},\ x\alpha_3 x^{-1},\ y\alpha_1 y^{-1},\ y\alpha_2 y^{-1}...$$

- J. G. Boiser. *Computational Problems in the Braid Group*. Masters Thesis. San Diego State University. 2009.
- D. Rolfsen. *Tutorial on the Braid Group*. in Braids: Introductory Lectures on Braids, Configurations and Their Applications, Lecture Note Series, Institute for Mathematical Sciences, National University of Sinapore. Vol 19. World Scinetific. 2009.