Introduction

Braid groups were introduced by Emil Artin in 1925, and by now play a role in various parts of mathematics including knot theory, low dimensional topology, and public key cryptography. Expanding from the Artin presentation of braids we now deal with braids defined on general manifolds as in [3] as well as several of Birman’s other works.

1 Preliminaries

We begin by laying the groundwork for the Artinian version of the braid group. While braids can be dealt with using a number of different representations and levels of abstraction we will confine ourselves to what can be called the geometric braid groups.

Let $E^3$ denote Euclidean 3-space, and let $E^2_0$ and $E^2_1$ be the parallel planes with z-coordinates 0 and 1 respectively. For $1 \leq i \leq n$, let $P_i$ and $Q_i$ be the points with coordinates $(i, 0, 1)$ and $(i, 0, 0)$ respectively such that $P_1, P_2, \ldots, P_n$ lie on the line $y = 0$ in the upper plane, and $Q_1, Q_2, \ldots, Q_n$ lie on the line $y = 0$ in the lower plane.

An $n$-braid, specifically a geometric $n$-braid, is comprised of $n$ strands $(s_1, s_2, \ldots, s_n)$, such that $s_i$ connects the point $P_i$ to the point $Q_{\pi(i)}$, for some $\pi$ where $\pi$ is the permutation of the braid; if $\pi$ is trivial then the braid is said to be a pure braid. Furthermore:

- Each strand $s_i$ intersects the plane $z = t$ exactly once for each $t \in [0, 1]$. 
• The strands $s_1, s_2, \ldots, s_n$ intersect the plane $z = t$ at $n$ distinct points for each $t \in [0, 1]$.

Simply, an $n$-braid is comprised of $n$ strands which cross each other a finite number of times without intersecting, and travel strictly “downwards”.

![Figure 1.1: An example $\alpha$ of a 5-Braid](image)

For $n$-braids $\alpha$ and $\beta$ there is a natural operation of composition as seen in Figure 1.2. The resulting braid $\alpha \beta$ is constructed by identifying $Q_i$ of $\alpha$ with $P_i$ of $\beta$, thereby creating continuous strands. This operation defines a group operation on the set of $n$-braids.

![Figure 1.2: Composition of Braids in $B_3$](image)

The group of $n$-braids is denoted $B_n$ with $\mathcal{PB}_n$ denoting the subgroup of $B_n$ formed by braids with trivial permutations, $\pi(i) = i$, called the pure braid group. The identity of $B_n$ is the braid consisting of $n$ parallel strands with no crossings, while the inverse $\beta^{-1}$ of a braid $\beta$ is the vertical reflection of $\beta$.

Note, in graphical representations of braids we will use “∗” to denote composition of braids while when dealing with braids algebraically we will use the convention of adjacency.
When considering braids, strands can be deformed continuously without altering the structure of the braid, as can be seen in Figure 1.3 with \( \beta \beta^{-1} = I_n \) where \( I_n \) denotes the identity braid in \( n \)-strands. When dealing with the braids it can be helpful to consider the simplest form of each braid, to this end we can comb the braid meaning we will continuously deform the strands until there are the fewest possible crossings of strands. A braid that is of this simple form can be referred to as a **combed braid**.

Notice then that any \( n \)-braid can be represented as the composition of a finite number of elementary braids \( \sigma_1, \ldots, \sigma_{n-1} \) and their inverses where \( \sigma_i \) denotes a braid differentiated from \( I_m \) solely by the \( i \)th strand crossing over the \((i + 1)\)th strand. Thus, \( \sigma_i^{-1} \) is the braid where the \( i \)th strand crosses under the \((i + 1)\)th strand.

**Example 1.4.** Consider Figure 1.1, \( \alpha = \sigma_1 \sigma_3^{-1} \sigma_2 \sigma_4^{-1} \sigma_1 \sigma_3^{-1} \).

We can then note that given \( i \) and \( j \), if \( i \) and \( j \) differ by more than one, the elementary braids \( \sigma_i \) and \( \sigma_j \) commute. It is not generally the case that arbitrary braids commute in \( B_n \) for \( n \geq 3 \).

**Theorem 1.5 (Center of the Braid Group).** For \( n > 2 \), the center of \( B_n \) is \( \langle \Delta^2 \rangle \) where

\[
\Delta = \sigma_1(\sigma_2\sigma_1)(\sigma_3\sigma_2\sigma_1) \cdots (\sigma_{n-1}\sigma_{n-2} \cdots \sigma_1).
\]

Notice here that \( \Delta \) reverses the order of points \( (\pi(i) = 1 + n - i) \), and thus \( \Delta^2 \) preserves the order of points \( (\pi(i) = i) \).
Remark 1.7 (Center of $B_1$ and $B_2$). The trivial braid group $B_1$ consists solely of $I_1$, thus it is obvious that the center of $B_1$ is $B_1$ as the identity is always in the center. The center of $B_2$ (which has only two nontrivial braids) is $\langle \sigma_1 \rangle$.

Up until now we have been addressing what are called open braids. However, by wrapping a braid once around an axis and identifying $P_i$ with points $Q_i$, we get what is called a closed braid. On closed braids we allow the same type of deformations as on open braids, namely those that are continuous without causing the strands to intersect.

The problem of classification of closed braids is a group theoretic one in which two closed braids, $A$ and $B$ can be considered equal if and only if $B = XAX^{-1}$ for some open braid $X$.

2 Braid Groups as Extensions of Symmetric Groups

Braid groups naturally give rise to a surjective group homomorphism $\gamma : B_n \to S_n$.

Definition 2.1. Let $\beta$ be an $n$-braid, given that strands connect points $P_i$ to $Q_{\pi(i)}$, we define a homomorphism $\gamma : B_n \to S_n$ such that

$$\gamma(\beta) = \begin{pmatrix} 1 & \ldots & i & \ldots & n \\ \pi(1) & \ldots & \pi(i) & \ldots & \pi(n) \end{pmatrix}$$

This homomorphism is in essence the result of disregarding how the strands cross.

Example 2.2. Consider Figure 1.1, $\gamma(\alpha) = (14)(35)$ in cycle notation.

Remark 2.3 (Disjoint Permutations Commute). By “disjoint” elementary braids and disjoint cycles commuting, the image of composition of braids is the same as the composition of images of braids.

Also similar to the symmetric groups, the braid groups can be easily coerced into larger groups, i.e. there is a natural way to fit $B_n$ into $B_{n+1}$. In both cases additional “elements” may be included.

For instance, a cycle representation of a permutation on $n$ letters in the symmetric group can be applied to a set of $m$ letters, $m > n$, simply by considering the unlisted numbers as being within their own cycle. For example, the cycle $(132)$ representing a permutation of three letters can also represent a permutation on four letters as in $S_4$, $(123) = (123)(4)$. Similarly, consider an arbitrary $n$-braid, and then add a single trivial strand connecting points $P_{n+1}$ and $Q_{n+1}$. In both cases there is a natural way to expand elements to elements of the larger group. There are many interesting results regarding braid groups which while not difficult to understand do not fall nicely into a designated place, here we will address one such interesting results which concerns the presentation of a specifically generated subset of $B_n$.

Conjecture 2.4 (The Tits Conjecture). Let $T_i = \sigma_i^2$, then $G \subset B_n$ has the presentation

$$\langle T_1, \ldots, T_{n-1} | T_i T_j = T_j T_i \text{ if } |i - j| \geq 2 \rangle.$$

The generalized form of the Tits Conjecture (the generalization is in regard to the arbitrary choice of power) was proved in 2001 by J. Crisp and L. Paris, see [4].
3 Cryptography

In the early 2000s a number of public key cryptosystems based on combinatorial group theory problems, including those concerning braid groups, were proposed. Part of this push to diversify the tools for encryption was that as quantum computers come closer to reality many current systems will be able to be broken in subexponential time.

As such, in combination with a desire to prevent wide scale security failure should the current cryptosystem(s) be broken, there is an increasing need for a wider range of more secure cryptosystems. In essence, we should not be placing all of our encryption keys in one basket.

The cryptosystem seeming to be the most written upon using braid groups was introduced by Ko et. al. [11] in 2000. The problem used as the base of the cryptosystem was base on a Diffie-Hellman like problem: for $a \in B_n$, $x \in G_1$, $y \in G_1$ where $G_1, G_2 \subset B_n$ commute with each other, given $(a, x^{-1}ax, y^{-1}ay)$, find $y^{-1}x^{-1}axy$.

After an algorithm was proposed to solve this problem in a reasonable time frame with relative accuracy a revised problem was released which can be roughly stated as: given $(a, x_1ax_2)$ find $z_1, z_2$ such that $z_1az_2 = x_1ax_2$ where $a \in B_n$ and $x_1, x_2, z_1, z_2 \in G \subset B_n$.

Lee and Park’s paper [12] proposes two improvements to the algorithm solving the original problem, one of which is more efficient with the same success rate, while the other has a higher success rate at a lower efficiency. While the details of solving the BPKE problem proposed by Ko et. al. is outside the scope of this paper we will give an outline.

The general approach to solving group theoretic problems in braid groups, as it pertains to cryptosystems, is to transform the given braid representation into an equivalent representation in which the problem is easier to solve and then lifting the result back to the initial representation. There are a number of ways to do this, one way which was addressed in Lee and Park’s paper was to utilize a braid representation called the “Burau Representation” which utilize matrices.

References

  http://www.jstor.org/stable/1969218

  http://www.jstor.org/stable/27826294


  http://arxiv.org/pdf/math/0409205


https://people.math.osu.edu/glasscock.4/braid_groups.pdf


http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80.4420&rep=rep1&type=pdf


http://www.math.uchicago.edu/~may/VIGRE/VIGRE2011/REUPapers/Lieber.pdf

http://archive.numdam.org/article/AMBP_2011__18_1_15_0.pdf