Braid Groups

Jahrme Risner
Mathematics and Computer Science
University of Puget Sound
jrisner@pugetsound.edu

17 April 2016

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' 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 $\mathcal{E}^3$ denote Euclidean 3-space, and let $\mathcal{E}_0^2$ and $\mathcal{E}_1^2$ 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 π where π is the **permutation** of the braid; if π 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 wich cross each other a finite number of times without intersecting, and travle strictly "downwards".

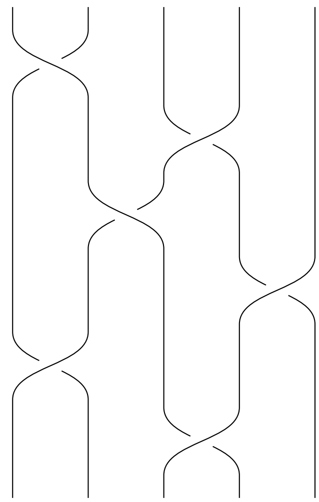

Figure 1.1: An example α of a 5-Braid

For n-braids α and β there is a natural operation of **composition** as seen in Figure 1.2.[1] The resulting braid $\alpha\beta$ is constructed by identifying Q_i of α with P_i of β, thereby creating continuous strands. This operation defines a group operation on the set of n-braids.

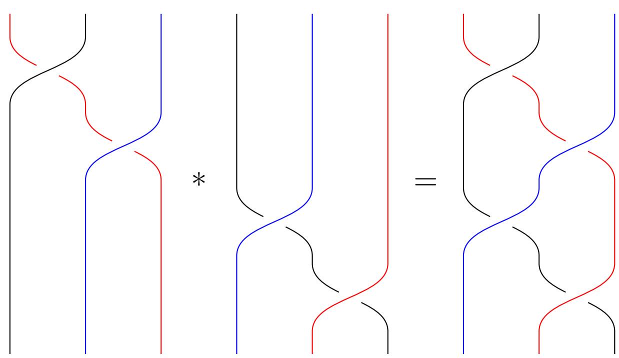

Figure 1.2: Composition of Braids in $\mathcal{B}_3$

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

[1]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.

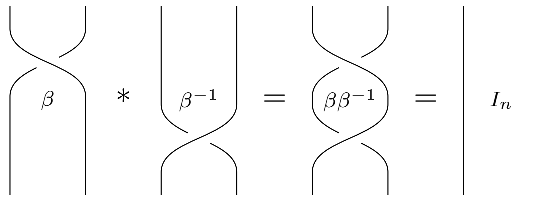

Figure 1.3: Inverse and Identity in $\mathcal{B}_2$

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 σ_i denotes a braid differentiated from I_m solely by the ith strand crossing over the $(i+1)$th strand. Thus, σ_i^{-1} is the braid where the ith strand crosses under the $(i+1)$th strand.

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

We can then note that given i and j, if i and j differ by more than one, the elementary braids σ_i and σ_j commute. It is not generally the case that arbitrary braids commute in $\mathcal{B}_n$ for $n \geq 3$.

Theorem 1.5 (Center of the Braid Group)**.** *For $n > 2$, the center of $\mathcal{B}_n$ 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 Δ reverses the order of points ($\pi(i) = 1 + n - i$), and thus Δ^2 preserves the order of points ($\pi(i) = i$).

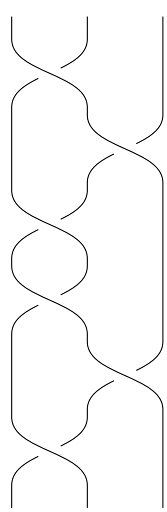

Figure 1.6: Δ^2 for $\mathcal{B}_3$

Remark 1.7 (Center of $\mathcal{B}_1$ and $\mathcal{B}_2$)**.** The trivial braid group $\mathcal{B}_1$ consists solely of I_1, thus it is obvious that the center of $\mathcal{B}_1$ is $\mathcal{B}_1$ as the identity is always in the center. The center of $\mathcal{B}_2$ (which has only two nontrivial braids) is $\langle\sigma_1\rangle$.

Up until now we have been addressing what are called **open braids**. Howeverm 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 an 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 $\gamma : \mathcal{B}_n \to S_n$.

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

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

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 $\mathcal{B}_n$ into $\mathcal{B}_{n+1}$. 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 $(1\,3\,2)$ representing a permutation of three letters can also represent a permutation on four letters as in S_4, $(1\,2\,3) = (1\,2\,3)(4)$. 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 $\mathcal{B}_n$.

Conjecture 2.4 (The Tits Conjecture)**.** *Let $T_i = \sigma_i^2$, then $G \subset \mathcal{B}_n$ has the presentation*

$$\langle T_1, \cdots, T_{n-1} \mid T_iT_j = T_jT_i \text{ if } |i-j| \geq 2\rangle.$$

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 $a \in \mathcal{B}_n, x \in G_1, y \in G_1$ where $G_1, G_2 \subset \mathcal{B}_n$ 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 $a \in \mathcal{B}_n$ and $x_1, x_2, z_1, z_2 \in G \subset \mathcal{B}_n$.

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

[**1**] Emil Artin, *Theory of Braids*, Annals of Mathematics (1947).
http://www.jstor.org/stable/1969218

[**2**] Emil Artin, *The Theory of Braids*, American Scientist **38** no. 1 (1950).
http://www.jstor.org/stable/27826294

[**3**] Joan Birman, *Braids, Links, and Mapping Class Groups*, (1975).

[**4**] Joan Birman and Tara Brendle, *Braids: A Survey*, Handbook of Knot Theory (2005).
http://arxiv.org/pdf/math/0409205

[**5**] Jae Choon Cha, Ki Hyoung Ko, Sang Jin Lee, Jae Woo Han, and Jung Hee Cheon, *An Efficient Implementation of Braid Groups*, Advances in Cryptology (2001).
http://www.iacr.org/archive/asiacrypt2001/22480144.pdf

[**6**] Charles O. Christenson and William L. Voxman (Bryan A. Smith, Editor), *Aspects of Topology*, Second Edition, (1998).

[**7**] Francois Digne, Ivan Marin, and Jean Michel, *The Center of Pure Complex Braid Groups*, Journal of Algebra **374** no. 1 (2011).
http://www.sciencedirect.com/science/article/pii/S0021869311004145

[**8**] David Garber, *Braid Group Cryptography*, Braids: Introductory Lectures on Braids, Configurations and Their Applications no. 19 (2010).
http://arxiv.org/pdf/0711.3941.pdf

[**9**] Daniel Glasscock, *What is a Braid Group?*, (2012).
https://people.math.osu.edu/glasscock.4/braid_groups.pdf

[**10**] Nicholas Jackson, *Notes on Braid Groups*, (2004).

[**11**] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park, *New Public-Key Cryptosystem Using Braid Groups*, Advances in Cryptology (2000).
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80.4420&rep=rep1&type=pdf

[**12**] Eonkyung Lee and Je Hong Park, *Cryptoanalysis of the Public-Key Encryption Based on Braid Groups*, Advances in Cryptology (2003).
http://diyhpl.us/~bryan/papers2/security/advances-in-cryptology/Advances%20in%20Cryptology%20-%20EUROCRYPT%202003(LNCS2656,%20Springer,%202003)(ISBN%203540140395)(662s).pdf

[**13**] Joshua Lieber, *Introduction to Braid Groups*, (2011).
http://www.math.uchicago.edu/~may/VIGRE/VIGRE2011/REUPapers/Lieber.pdf

[**14**] Juan Gonzalez-Meneses, *Basic Results on Braid Groups*, Annales Mathematiques Blaise Pascal **18** no. 1 (2011).
http://archive.numdam.org/article/AMBP_2011__18_1_15_0.pdf