VICTORIA UNIVERSITY OF WELLINGTON
Te Whare Wānanga o te Ūpoko o te Ika a Māui

School of Mathematics and Statistics
Te Kura Mātai Tatauranga

PO Box 600
Wellington
New Zealand

Tel: +64 4 463 5341
Fax: +64 4 463 5045
Internet: sms-office@vuw.ac.nz

Braids and the Braid Group

Matthew Askes, 300366054

Submitted in partial fulfilment of the requirements for
MATH 440, a directed independent study in knots,
polynomials, and complexity.

Abstract

The study of braids and the braid group is a vast topic. This report introduces the basic ideas of braids and the braid group. This report is aimed at anyone with little to no knowledge of braids but who has some understanding of knot theory.

Contents

Chapter 1

Introduction

Braids can be found everywhere from a school girls hair, a French pâtisserie, to the ringing of church bells. They are a ubiquitous part of life. You could go into almost any primary school and you find school children playing with braids. Weather they are braiding each others' hair or making brackets. In a pâtisserie you will find many wonderful breads and pastries made using braids. And in the ringing of church bells braids are used to describe the sequence of the bells. Braids have a geometric beauty to them. It is their ubiquity and beauty that make braids of great interest to the both layperson and mathematician alike.

Braid groups first appeared in a disguised form by Hurwitz 1891 [8]. And were first formally introduced by Artin 1925 [3]. This early study was interest was not enough to inspire much further research. It was not until mid to late 20th century that braids came back into the Lyme light. It was while studying new representations of the braid group in 1987 that Vaughan Jones discovered the famous Jones' polynomial [9]. Jones' discovery has lead to a strong increase in the study of the braid group. In more recent years the study of braids has lead to many interesting applications including the stirring of fluids with sticks, [5] and theoretical physics where applications of braids help generalise the spin of subatomic particles.

The study of braids is vast, and we cannot even hope to cover more than a mere morsel. The purpose of this report is to provide a brief introduction into braids, the braid group, and their connection to knots. In this report we begin by defining braids and braid words. We then introduce and define the braid group. Next we show how knots and braids are interconnected by introducing Alexander's theorem and Vogel's algorithm. Finally, we conclude by examining two applications of braid theory.

Chapter 2

Braids

2.1 What is a braid

Consider two horizontal bars, with n strands between them. The strands start at the points $A_1, \ldots, A_n$ on the top bar and move continuously downwards towards the points $A'_1, \ldots, A'_n$. The strands may cross over and under each other, but they may not move upwards. For example Figure 2.1 is not a braid as the leftmost strand moves upwards to form a loop. A braid with n strands is called an n–braid. The trivial braid is a special braid where each $A_1, \ldots, A_n$ is connected to $A'_1, \ldots, A'_n$ respectively.

Definition 2.1 (n–braid)**.** Fix $n > 0$ a natural number. Let X, Y be two parallel planes in 3–space. An n–braid is an embedding of n disjoint non–self–intersecting curves into 3–space such that any plane that is parallel to X and Y and between X an Y passes through each curve exactly once.

The 2D representation of a braid is called the braid projection, for example figure 2.2 is the projection of the trivial braid.

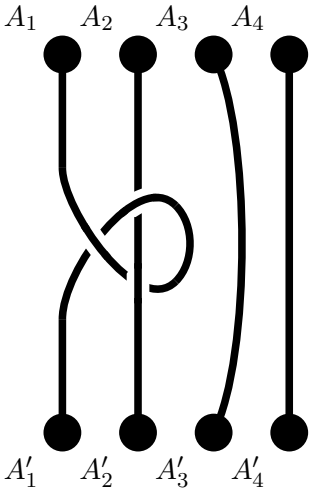

Figure 2.1: Not a braid

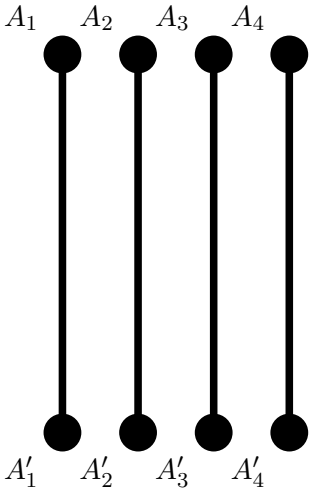

Figure 2.2: The trivial 4–braid

We consider two braids to be the equivalent if there is a continuous deformation of the strands, without passing any of the strands through each other, such that each braid can be transformed into the other. For example in figure 2.3 there are two projections that represent

the same braid.

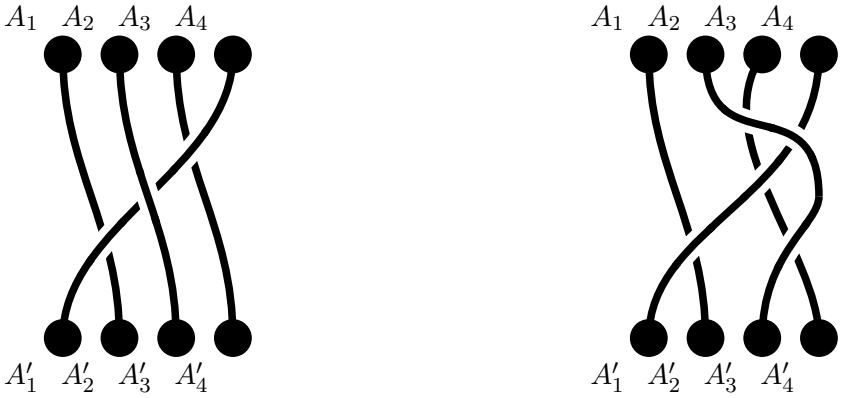

Figure 2.3: Two projections of the same braid

2.2 Braid words

An alternative way to define braids is to build them from single crossings. There are two types of crossings. A left over right called a σ_i crossing where we take ith strand and move it over the $(i+1)$th strand. And a right over left crossing, σ_i^{-1}, where we take $(i+1)$th strand and move it over the ith strand.

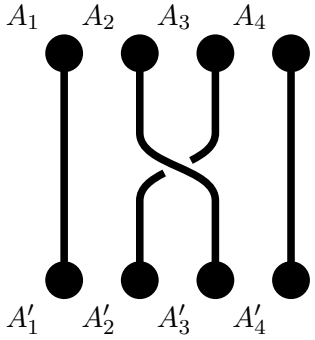

Figure 2.4: A σ_2 crossing

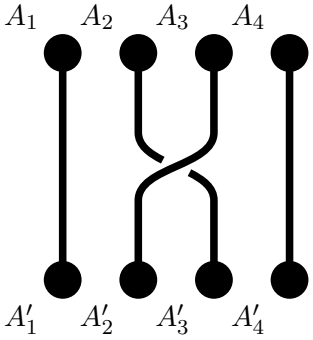

Figure 2.5: A σ_2^{-1} crossing

We can now define braids by building up σ_i and σ_i^{-1} crossings. An ordered string of σ_i's and σ_i^{-1}'s is called a braid word and uniquely defines a braid projection. For example figure 2.6 represents the braid word $\sigma_2^{-1}\sigma_3^{-1}\sigma_3\sigma_1\sigma_1^{-1}$.

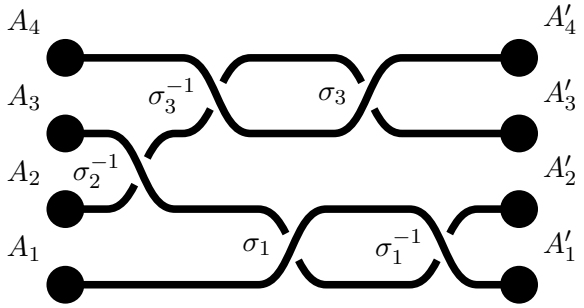

Figure 2.6: A braid

Braid words provide us with a simple way of describing braids. For example if you wanted to describe the sequence of steps necessary to 3 strand braid your hair you would describe it as the braid word of the form $\sigma_1^{-1}\sigma_2 \cdots$.

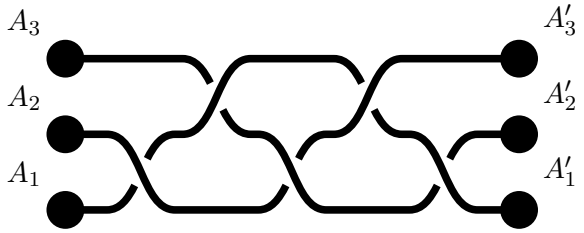

Figure 2.7: A 3 strand plait

It is clear that some braid words represent the same braids. Consider the 4–braids in figure 2.8, clearly they are the same braid. But, they have different braid words. Figure 2.8a has the braid word $\sigma_1\sigma_3$ whereas figure 2.8b has the braid word $\sigma_3\sigma_1$.

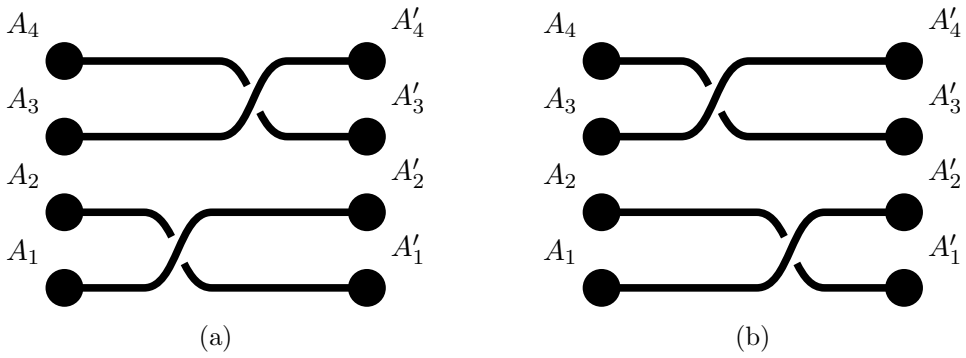

Figure 2.8: Two equivalent braids with different braid words

We can also see that the two braids in figure 2.9 are equivalent. We can get from (a) to (b) be shifting the A_2 strand through the crossing. Figure 2.9a has the braid word $\sigma_1\sigma_2\sigma_1$ whereas figure 2.9b has the braid word $\sigma_2\sigma_1\sigma_2$.

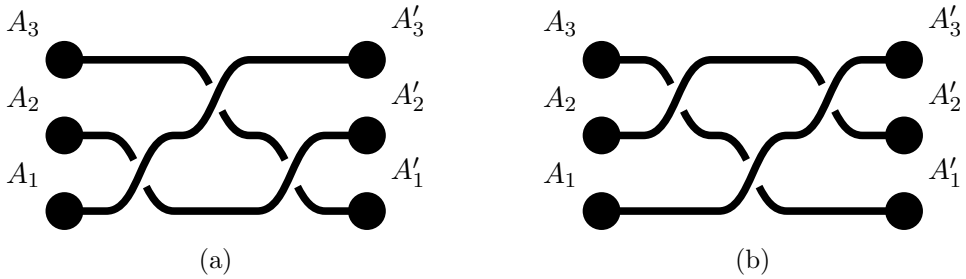

Figure 2.9: Two more equivalent braids with different braid words

We can also see from figure 2.10 that sequence $\sigma_i\sigma_i^{-1}$ just undoes the crossing.

Figure 2.10: Another two equivalent braids with different braid words

These operations can be formalised as follows.

(i) $\sigma_i\sigma_j = \sigma_j\sigma_i \qquad \text{if } |i-j| > 1$

(ii) $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$

(iii) $\sigma_i\sigma_i^{-1} = e$

These operations also hold for their inverses. For example $\sigma_1^{-1}\sigma_3^{-1} = \sigma_3^{-1}\sigma_1^{-1}$. In fact these operations are sufficient to show that two braid words represent equivalent braids [4]. In other words if B_1 and B_2 are braid words that represent equivalent projections then there exists a finite sequence of (i), (ii), and (iii) operations that transform B_1 into B_2 and vice versa.

Chapter 3

The Braid Group

3.1 What is a group?

Definition 3.1. A group $(X, \cdot)$ is a set, X, endowed with a binary operation, $\cdot$, that satisfies the following axioms.

(i) **Closure**: If $A, B \in X$ then $A \cdot B \in X$

(ii) **Associativity**: For all $A, B, C \in X$ $(A \cdot B) \cdot C = A \cdot (B \cdot C)$

(iii) **Identity**: There exists an element $I \in X$ such that for all $A \in X$ $I \cdot A = A \cdot I = A$

(iv) **Inverse**: For every element $A \in X$ there exists an $A^{-1} \in X$ such that $AA^{-1} = A^{-1}A = I$

3.2 Braids as a group

Consider the set of all braids with n strands and denote this set B_n. We endow B_n with the binary operation $\cdot$ as follows. Let A and B be braids with n strands. $A \cdot B$ is the braid obtained glueing the top bar to B to the bottom bar A. Alternatively if A and B are braid words then $A \cdot B$ is the braid word of B appended to the end of A. For example $\sigma_2\sigma_3 \cdot \sigma_1\sigma_2 = \sigma_2\sigma_3\sigma_1\sigma_2$. To show that B_n is a group we need to show that $\cdot$ satisfies the group axioms. Note that we call $A \cdot B$ the product of A and B.

We can see that B_n is closed under $\cdot$ as the result is clearly a braid with n strands.

Let $A = a_1a_2 \cdots a_i$, $B = b_1b_2 \cdots b_j$, and $C = c_1c_2 \cdots c_k$ be n–braid words in B_n.

$$\begin{aligned}(A \cdot B) \cdot C &= (a_1a_2 \cdots a_i \cdot b_1b_2 \cdots b_j) \cdot c_1c_2 \cdots c_k \\ &= (a_1a_2 \cdots a_ib_1b_2 \cdots b_j) \cdot c_1c_2 \cdots c_k \\ &= a_1a_2 \cdots a_ib_1b_2 \cdots b_jc_1c_2 \cdots c_k \\ &= a_1a_2 \cdots a_i \cdot (b_1b_2 \cdots b_jc_1c_2 \cdots c_k) \\ &= a_1a_2 \cdots a_i \cdot (b_1b_2 \cdots b_j \cdot c_1c_2 \cdots c_k) \\ &= A \cdot (B \cdot C)\end{aligned}$$

Therefore the product of A, B, and C is associative. This can also be seen by the example in figure 3.1 where we take the product of three 3–braids.

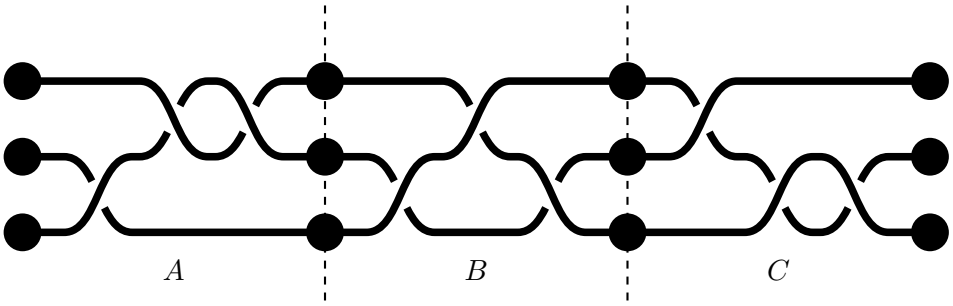

Figure 3.1: Assoctiativity of braids

The identity braid I in B_n is the trivial braid with n strands. This is because appending the trivial braid to any other braid doesn't introduce any new twists and hence is the same braid. This can be seen in figure 3.2.

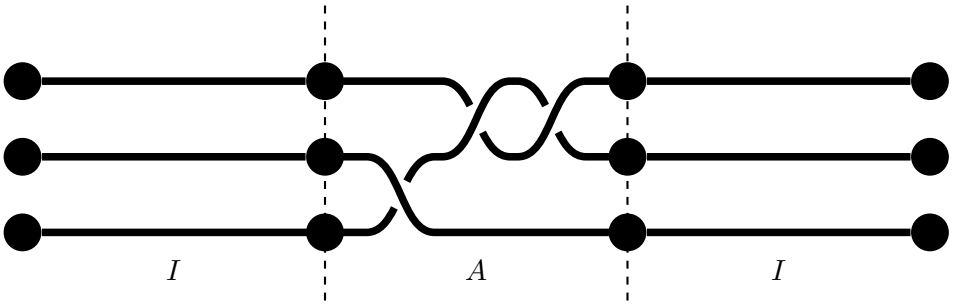

Figure 3.2: Identity braid

Let A be an n-braid. The inverse of A, A^{-1} is defined by mirroring A along one of its ends. In braid word terms, if $A = a_1 a_2 \cdots a_n$ then $A^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}$. This can be visualised by the example in figure 3.3. From the braid words of A and A^{-1} it is quite easy to see that all the terms will cancel, and we will be left with the identity. It is also not too difficult to see why this works by figure 3.3.

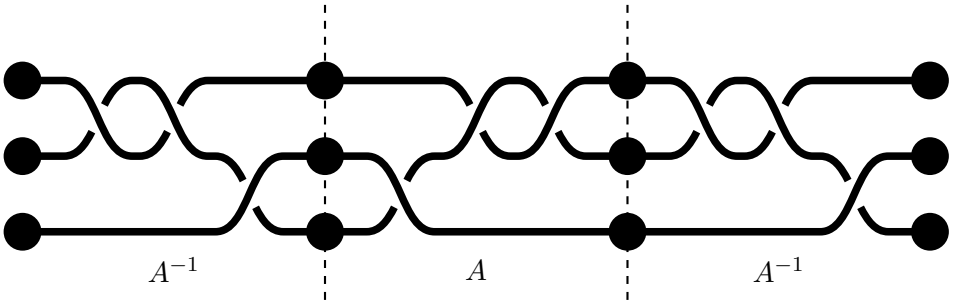

Figure 3.3: Inverse braid

3.3 Generators and Relations

In chapter 2 we stated that the following operations were enough to show equivalence of any two braids.

(i) if $|i - j| > 1$ then $\sigma_i \sigma_j = \sigma_j \sigma_i$

(ii) $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$

(iii) $\sigma_i\sigma_i^{-1} = \emptyset$

In terms of the braid group B_n all the equations of the form (i) and (ii) are called the relations of the braid group. For example the braid group B_3 has the relations $\sigma_1\sigma_3 = \sigma_3\sigma_1$, $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$, and $\sigma_2\sigma_3\sigma_2 = \sigma_1\sigma_2\sigma_3$. Two elements of the braid group are equal if there is a sequence of relations that convert one to the other.

We do not consider (iii) to be a bona fide relation. We also have the relation $\sigma_i\sigma_j = \sigma_i\sigma_j$, but again we do not consider this a bona fide relation. These two relations are called the trivial relations.

Definition 3.2. Let $(X, \cdot)$ be a group. A generator for X is a subset A of X such that every element in X can be built by products of elements in A.

In terms of the braid group B_n the braids $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ and their inverses can be combined in a way that generates the entire group and hence known as the generators for B_n.

We can now express the braid group B_n in terms of its generators and relations, [4]. That is,

$$B_n = \left(\sigma_1, \sigma_2, \ldots, \sigma_{n-1} \middle| \begin{matrix} \sigma_i\sigma_j = \sigma_j\sigma_i & |i-j| > 1 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & i \in \{1, \ldots, n-1\} \end{matrix} \right)$$

Chapter 4

Knots as braids

4.1 Knots and Links

The simplest way of think a knot is simply as a knotted loop of string. Formally a knot is a closed non–self–intersecting curve in 3–space. A link is the union of multiple disjoint knots. Each knot that forms part of a link is called a component of the link. The projection of a knot or link is a representation of the knot or link onto the plane. Figure 4.2 is an example of a knot and figure 4.3 an example of a link. The trivial knot is the knot with no crossings, figure 4.1, the trivial link with n components is the union of n trivial knots.

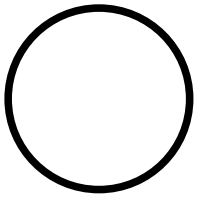

Figure 4.1:
The trivial knot

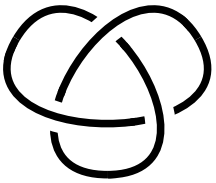

Figure 4.2:
The trefoil knot

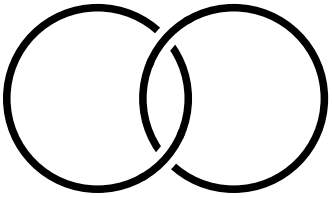

Figure 4.3:
The Hoph link

An orientation of a link is defined by choosing a direction to travel around each component in the link. We call such a link an orientated link.

As with braids we consider two links (or knots) to be the same if there is a continuous deformation from one to the other such that the strands do not cross.

4.2 Closed Braids

Consider an n–braid, B. We close B by connecting $A_1, \ldots, A_n$ to $A'_1, \ldots, A'_n$ with a series of parallel strands travelling outside the braid. The link K formed in this way is the closure of the n–braid B and is called a closed braid. It is easy to see how this forms a link by considering figure 4.4.

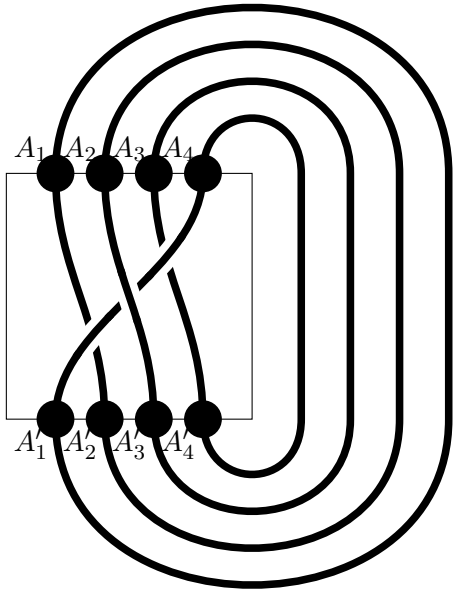

Figure 4.4: A closed braid

We now have an easy way to convert braids into knots. The converse is not as obvious, but every link can be converted into a braid. This was first shown in 1923 by J. W. Alexander.

Theorem 4.1 (Alexander 1923 [1])**.** *Given any link then it is equivalent to some closed braid.*

A complete proof of theorem 4.1 is beyond the scope of this report. But we provide an algorithm that generates a closed braid from any given link.

4.3 Vogel's Algorithm

Introduced in Vogel 1990 [13] Vogel's algorithm provides us with a simple procedure of generating closed braids from links. That is for any link K Vogel's algorithm finds a braid whose closure is K. Hence a proof of Vogel's algorithm is a proof of theorem 4.1. Again a full proof is beyond the scope of this report. The following explanation is derived from [7], where a complete proof can be found.

We summarise the algorithm as follows. Let K be a link and fix a projection of K.

Step 1: Orientate the link, K.

Step 2: Let P be a point in K such that all the strands bordering the region containing P travel in the same direction.

Step 3: Move a strand that travels counter to the region about P over the entire link.

Step 4: Repeat until all the strands travel in the same direction.

Step 5: Cut the link radiating outwards from P to form a braid.

Now for a complete walk–through with an example. Let K be an link and fix a projection. If K is not oriented then we assign an arbitrary orientation to all the components of K. Let P a point inside the link such that all the strands bordering the region containing P travel

in the same direction. As an example we will consider the figure 8 knot in figure 4.5. The goal is to have all the strands in the link travelling around P in the same direction, either clockwise or anticlockwise.

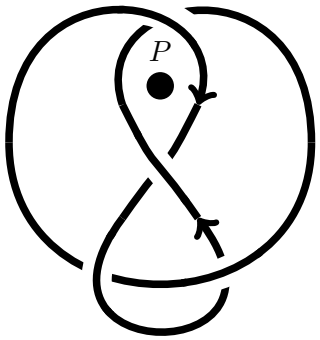

Figure 4.5: An oriented figure 8 knot

We define a troubled section as a strand of the link that is oriented in the direction opposite to our chosen orientation. In figure 4.6 the troubled section for the figure eight knot is highlighted red. To remove a troubled section we move it over the rest of the link and the point P. This can be represented in the projection as a series of Reidemeister moves and hence the new projection is equivalent to the old one.

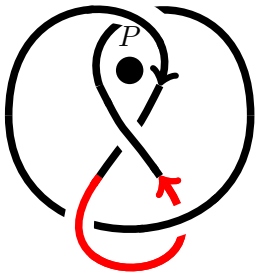

Figure 4.6: A troubled section

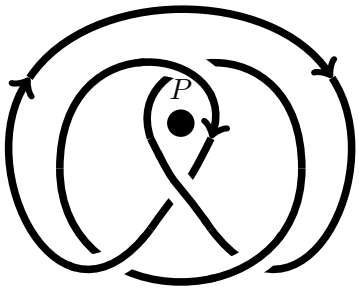

Figure 4.7: Resolved trouble section

We keep shifting troubled sections over the link. Each time we remove a troubled section the total number of such sections goes down and therefore eventually all the strands will travel around P in the same direction.

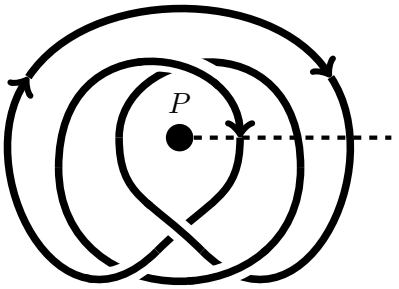

Figure 4.8: A slice in the knot

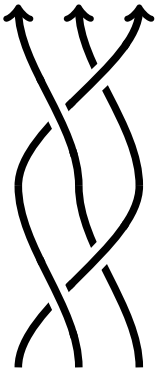

Figure 4.9: The braid of the figure 8 knot

Once all the strands travel clockwise (or counter clockwise) we slice the link from P outwards. The ends of the cut strands become the ends of the braid.

4.4 Markov moves

In Vogel's algorithm the next troubled section we remove is chosen arbitrarily. So we may get different braids whose closures are the same link. This raises the question, which braids represent the same links? The Markov solve this problem by introducing a pair of operations that change the braid but not the link represented.

Definition 4.2. Let $B =$ be an n–braid.

(i) A type I Markov move takes B to $\alpha B \alpha^{-1}$, where α is an n–braid.

(ii) A type II Markov move takes B to $B\sigma_n$ or $B\sigma_n^{-1}$.

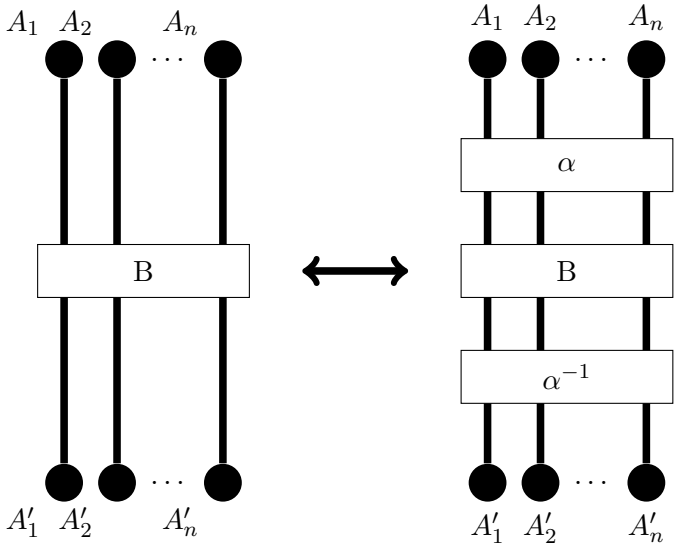

Figure 4.10: Type I Markov move

By using Markov moves we can find equivalences between braids and their link representation. This was first discovered in Markov 1936 [11], and hence we have the theorem 4.3.

Theorem 4.3 (Markov's theorem [11])**.** *Two braids represent the same link if and only if the braids are equivalent or there if a series of Markov moves from one to the other.*

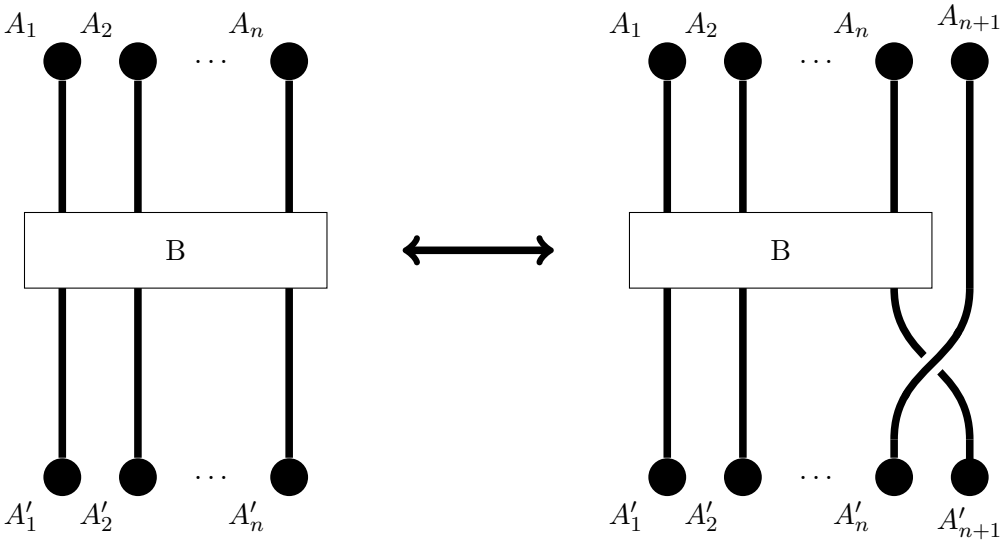

Figure 4.11: Type II Markov move

A full proof of theorem 4.3 is beyond the scope of this report. But we provide some intuition for why Markov moves don't change the associated knot. Fix some braid B. If we apply a type I Markov move to B we get $\alpha B \alpha^{-1}$ as our new braid. We can close the braid to find the associated link. However, when we do this α and α^{-1} are now connected and so cancel out, leaving us with the closure of B. If we apply a type II Markov move to B we have added a single twist to the link represented by B. Twists can be undone without changing the link. Hence B represents the same link before and after a type II Markov move.

Chapter 5

Applications

5.1 Change ringing

All over the world church bells are used to call people to worship, in celebration, and remembrance. Change ringing is a particular form of bell ringing. In change ringing each bell is attached to a large wheel and is rung by a ringer (a person who rings bells) by pulling a rope attached to the wheel. By attaching the bells to wheels it allows the bells to be swung in a full circle and back again. The wheels also give ringers far greater control over the bells.[6]

The Bells are numbered from sequentially, with 1 being the lightest bell and the bells getting progressively heaver as the number increases. A *row* is any permutation of the bell numbers. For example with 6 bells 254163 and 123564 are both rows. When a row is rung the bells are rung from left to right. As the bells are on wheels they have a natural period to them. This means that a row can only be altered by swapping any two adjacent bells in the row, known as a *change*. For example $123456 \rightarrow 123465$ is a valid change but $123456 \rightarrow 612345$ is not. A sequence of changes define a *method* and describes a tune to be played. A method that starts and ends in order and every permutation is played no more than once is known as a *extent*. For example with 3 bells figure 5.1 is an extent. We can represent this method pictorially as a braid as in figure 5.2. [10]

123
213
231
321
312
123

Figure 5.1: A 3 bell method

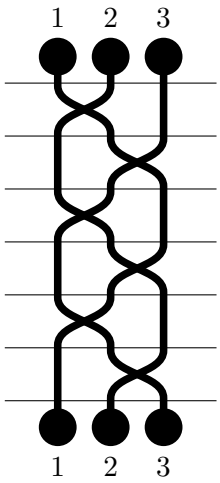

Figure 5.2: Braid representation

We can arbitrarily choose crossings as the type of crossing makes no difference for methods. In change ringing the braids are used to define a sequence of permutations. Bell ringers are interested in generating new extents. But the restrictions to extents makes generating new pieces of music is a non–trivial problem. But by representing extents as braids we reduce the problem to a problem on braids.

5.2 Public Key Cryptography

In Symmetric key encryption users use the same key to both encrypt and decrypt data, this is the most common form of encryption. In public key encryption two different keys are used, one to encrypt the data (the public key) and a second secret key to decrypt the data (the private key). Once the data has been encrypted using the public key it cannot be decrypted without knowing the private key. This allows secure sending of data over public networks. One common use of public key encryption is to securely distribute encryption keys to users. We present one such approach by Unit 2005 [12] to private key distribution using the conjugacy problem of the braid group. This approach was first seen in Iris Anshel, Michael Anshel and Dorian Goldfeld 1999 [2].

Definition 5.1 (Conjugacy Problem)**.** Let x, y be elements of the braid group B_n. The *conjugacy problem* asks, is there a $z \in B_n$ such that $x = z^{-1}yz$.

The conjugacy problem is, in general, difficult. That is there is no known algorithm that can solve the conjugacy problem in polynomial time.

Suppose Alice and Bob wish to send encrypted messages to each other. Alice and Bob fix some integer n and choose some arbitrary subsets of B_n as follows,

$$S_{\text{Alice}} = \{a_1, a_2 \ldots, a_m\}, \qquad S_{\text{Bob}} = \{b_1, b_2, \ldots, b_l\}$$

S_{Alice} and S_{Bob} become the public keys, and a freely distributed.

Alice and Bob choose secret elements $a \in S_{\text{Alice}}$ and $b \in S_{\text{Bob}}$ respectively. Alice then transmits the elements

$$a^{-1}b_1a, a^{-1}b_2a, \ldots, a^{-1}b_la$$

Similarly Bob transmits the elements

$$b^{-1}a_1b, b^{-1}a_2b, \ldots, b^{-1}a_mb$$

Alice and bob can now calculate the elements $b^{-1}ab$ and $a^{-1}ba$ respectively. This allows them both to calculate $a^{-1}bab^{-1}$, which becomes their shared private key.

Bibliography

[1] J. W. Alexander, *A lemma on systems of knotted curves*, Proceedings of the National Academy of Sciences **9** (1923), no. 3, 93–95.

[2] Iris Anshel, Michael Anshel, and Dorian Goldfeld, *An algebraic method for public-key cryptography*, 1999.

[3] Emil Artin, *Theorie der Zöpfe*, Abh. Math. Sem. Univ. Hamburg **4** (1925), no. 1, 47–72. MR 3069440

[4] F. Bohnenblust, *The algebraical braid group*, Ann. of Math. (2) **48** (1947), 127–136. MR 19088

[5] PHILIP L. BOYLAND, HASSAN AREF, and MARK A. STREMLER, *Topological fluid mechanics of stirring*, Journal of Fluid Mechanics **403** (2000), 277–304.

[6] CCBR, *What is bell ringing?*, `https://cccbr.org.uk/bellringing/what-is-bell-ringing/`, 2020, Accessed: 2020-06-28.

[7] RUTH GOLDSTEIN-ROSE, *Introduction to knots and braids using seifert circles*, (2017).

[8] A. Hurwitz, *Ueber Riemann'sche Flächen mit gegebenen Verzweigungspunkten*, Math. Ann. **39** (1891), no. 1, 1–60. MR 1510692

[9] V. F. R. Jones, *Hecke algebra representations of braid groups and link polynomials*, Ann. of Math. (2) **126** (1987), no. 2, 335–388. MR 908150

[10] Frank H. King, *Ringing elementary minor methods on handbells*, 1974.

[11] Andrei Markoff, *Über die freie äquivalenz der geschlossenen zöpfe*, (1936).

[12] ISIK Umut, *Computational problems in the braid group with applications to cryptography*, (2005).

[13] Pierre Vogel, *Representation of links by braids: a new algorithm*, Comment. Math. Helv. **65** (1990), no. 1, 104–113. MR 1036132