On the Linearity of Braid Groups

Jacob White

February 2006

1 Introduction

To understand what a braid group is, it is easiest to visualize a braid. Consider n strands, all parallel. Consider taking the ith strand and crossing it over the $i+1$th strand. This is an example of a braid. In general, a braid is any sequence of crossings of the bands, provided none of the bands are self-crossing. For instance, a loop, or a band which forms a loop in the middle, is not a braid.

Now, in order for the set of all braids of n bands to be group, we must be able to find a binary operation on the braids that satisfies certain properties. We consider a very simple operation which we call concatenation. We take two braids, and do the sequence of twists of the first one followed by the twists of the second braid. The result is another braid. Thus, this operation is closed.

The identity element for this operation is also obvious. Clearly, the bands not having any crossings is the identity, as this braid concatenated with any other braid is just the other braid. To find inverse element of x, one just takes the identity element, and do the exact opposite crossings of x in the exact opposite sequence than the sequence of crossings in x. Thus, the set of all braids on n strands forms a group under concatenation.

Artin [1] showed that the braid group is generated by the Artin generators, which obey two relations:

$$\sigma_i\sigma_j = \sigma_j\sigma_i, |i-j| > 1 \tag{1}$$

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, |i-j| = 1 \tag{2}$$

The first relation is called the swap relation, and the second relation is called the shift relation.

Thus, any braid can be decomposed into the Artin generators. Also, in terms of the n bands, the Artin generator σ_i stands for the $(i+1)$th strand crossing over the ith strand, leaving all other strands alone.

Consider this example. There are four bands, with the first crossing over the next two. Then the new top band crosses over the second band. Now let the third band cross over the second band. Finally, let the third band cross over the fourth band. This is a braid that is generated by $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_3$. A shift relation on the top quickly causes the braid to change into a braid where the second band goes over the third and fourth, and the new third band crosses under the top band. Thus, $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_3 = \sigma_2\sigma_3\sigma_1$.

In terms of viewing the braids from a geometric perspective, the Artin relations have a well-defined interpretation. Consider crossing the 1st band over the 2nd and the 3rd band over the 4th. Regardless of what order you do the crossings you end u p with the same result.

For the other relation, imagine three bands, the top one going over the other two, and the latter two also crossing over each other afterwards. It becomes clear that you can move the top strand to the right and still have the same braid. Yet both these braids are generated by different Artin generators. So the Artin generators for both braids must be the same. The result is the shift relation.

Another important fundamental idea to understanding this paper is the idea of a representation. A representation is a map $\rho : G \to GL(n, F)$, where G is a group, and $GL(n, F)$ is the group of $n \times n$ invertible matrices over the field F. Basically, a representation sends every element of the group to a corresponding matrix, and sends the group operation to matrix multiplication. This allows someone to study a group by studying the corresponding matrices, which is already a well-known theory.

An important aspect of representation theory is whether or not a representation is faithful. A representation is faithful if ρ is injective. Thus, every group element is sent to a unique matrix.

A theoretical result we have been investigating is the fact that braid groups are linear - that is, they have a faithful representation[2] . This representation is due to Lawerence and Krammer. In the third section we will examine the representation.

2 Symmetric Groups

First, we state some basic facts about symmetric groups. Let S_n denote the symmetric group on $I_n = \{1, 2, ..., n\}$, a set of n symbols. Let Ref denote the set of reflections in S_n. Thus, $x \in Ref$ if and only if there exists $i, j \in I_n$, such that $x(i) = j$ and $x(j) = i$, and for every $k \in \mathbb{Z}_n$, $k \neq i$, $k \neq j$, $x(k) = k$. Thus, an element is a reflection if it switches two symbols, while keeping the other symbols fixed. We denote such elements by $s(i, j)$, where i and j are the symbols that are flipped. A very elementary reflection is one of the form $s(i, i + 1)$. Such a reflection is called a transposition. Let S be the set of all transpositions.

Symmetric groups play a large role when working with braid groups. For one thing, there is an obvious homomorphism r from S_n to B_n given by sending $s(i, i + 1)$ to σ_i. It is known that the Artin Generators also generate the symmetric group.

We define a length function $\ell : S_n \to \mathbb{Z}_{\geq 0}$ by $\ell(x) = k$, where k is the smallest natural number such that there exists $s_{i_1}, s_{i_2}, ..., s_{i_k} \in S$ such that $x = s_{i_1} s_{i_2} ... s_{i_k}$.

With the length function ℓ, we can define an ordering on S_n. For $x, y \in S_n$, $x \leq xy \Leftrightarrow \ell(xy) = \ell(x) + \ell(y)$.

Now, we can denote the image of r by Ω. This is used throughout the paper. Also, a braid $x \in \Omega$ is called a simple braid.

Now, back to the Symmetric group, we let $\mathcal{P}(Ref)$ denote the power set of Ref. we can define a function $L : S_n \to \mathcal{P}(Ref)$ by $L(s) = \{s(i, j) | 1 \leq i < j \leq n, s^{-1}i > s^{-1}j\}$. Intuitively, $L(s)$ is the set of all reflections that are reversed by x.

Example 2.1. Here is an example of an element of $L(S_5)$. Let $s(1, 3) \in S_5$. Then $L(s(1, 3)) = \{s(1, 2), s(2, 3), s(1, 3)\}$.

Lemma 2.2. *$L(xy) = L(x) \uplus xL(y)x^{-1}$, for all $x, y \in S_n$, where $\uplus$ denotes the symmetric difference.*

Lemma 2.3. *For all $x \in S_n$, $\ell(x) = |L(x)|$.*

Here is an example.

Example 2.4. Let $x \in S_4$ such that $x = s(1, 3)$. In transpositions, $x = s(1, 2)s(2, 3)s(1, 2)$. This is the shortest sequence of reflections. Thus, $\ell(x) = 3$. Now, $|L(s(1, 3))| = 3$. Thus, $|L(x)| = \ell(x)$.

Theorem 2.5. *The following are equivalent:*

i) $x \leq xy$

ii) $\ell(xy) = \ell(x) + \ell(y)$

iii) $L(xy) = L(x) \cup xL(y)x^{-1}$

iv) $L(x) \subset L(xy)$.

Proof. For brevity, we will only show the proof of ii) $\Leftrightarrow$ iii). Consider $x, y \in S_n$ such that $\ell(xy) = \ell(x) + \ell(y)$. On the right hand side, we know that $\ell(x) = |L(x)|$, and $\ell(y) = |L(y)|$. Also, a non-trivial fact is that $|L(y)| = |xL(y)x^{-1}|$. So, we have that $\ell(x) + \ell(y) = |L(x)| + |xL(y)x^{-1}|$.

Now, on the right hand side, we have that $\ell(xy) = |L(xy)| = |L(x) \uplus xL(y)x^{-1}|$. Since $\uplus$ is the symmetric difference, $|L(x) \uplus xL(y)x^{-1}| = |L(x)| + |xL(y)x^{-1}| - |L(x) \cap xL(y)x^{-1}|$. Thus, we have that $|L(x)| + |xL(y)x^{-1}| - |L(x) \cap xL(y)x^{-1}| = |L(x)| + |xL(y)x^{-1}|$. Thus, $|L(x) \cap xL(y)x^{-1}| = 0$. The intersection is empty, and thus $L(xy) = L(x) \uplus xL(y)x^{-1} = L(x) \cup xL(y)x^{-1}$.

Suppose that $L(xy) = L(x) \cup xL(y)x^{-1}$. Since $L(xy) = L(x) \uplus xL(y)x^{-1}$, it follows that $L(x) \cap xL(y)x^{-1}$ must be empty. We know that $|L(xy)| = |L(x)L(x) \uplus xL(y)x^{-1}| = |L(x)| + |xL(y)x^{-1}| - |L(x) \cap xL(y)x^{-1}| = |L(x)| + |xL(y)x^{-1}|$. Yet again, we know that $|xL(y)x^{-1}| = |L(y)|$, so $|L(xy)| = |L(x)| + |L(y)| = \ell(x) + \ell(y)$. Since $\ell(xy) = |L(xy)|$, we have shown that $\ell(xy) = \ell(x) + \ell(y)$. □

Now, we will investigate subsets of Ref that have a certain property.

Definition. A set $A \subset Ref$ is called closed if, for $1 \leq i < j \leq n$, then $s(i, j), s(j, k) \in A$ implies $s(i, k) \in A$.

Example 2.8. Looking at the example $L(s(1, 3))$, it becomes clear that $L(s(1, 3))$ is closed. In fact, this turns out to be true in general, as the next theorem states.

Theorem 2.7. *If $X \in L(S_n)$, then X is closed.*

Proof. Consider $X \in L(S_n)$. Then there exists $x \in S_n$ such that $X = L(x)$. Consider $s(i, j)$, $s(j, k) \in X$, where $1 \leq i < j < k \leq n$. By definition of X, this implies that $x^{-1}i > x^{-1}j$, and $x^{-1}j > x^{-1}k$. Thus, $x^{-1}i > x^{-1}k$. This implies that $s(i, k) \in X$. Since this is true for all $s(i, j), s(j, k) \in X$, it follows that X is closed. □

It is important to note that the converse is not true. There are closed sets that are not in $L(S_n)$.

Example 2.9. An example of such a closed set is

$$A = \{s(1,2), s(2,3), s(1,3), s(2,5), s(1,5)\}$$

Clearly, this set is closed. However, in order for there to be an $x \in S_n$ such that $A = L(x)$, then by definition, x would have to satisfy: $x^{-1}1 < x^{-1}4 < x^{-1}5$, and $x^{-1}1 > x^{-1}5$. This is not possible. So in general, a closed set is not necessarily in $L(S_n)$.

Most of these definitions and theorems regarding the symmetric group will be used in showing the faithfulness of the Lawerence-Krammer representation, $\mathcal{K}$.

In fact, there is another relation between the symmetric group and the braid group. Let B_n^+ denote the positive braids - braids that, when written as a sequence of Artin generators, have no negative powers. Then there is a partial ordering on B_n^+, denoted $<$, such that for all $a, b \in B_n^+$, $a < b$ if and only if there exists $c \in B_n^+$ such that $ac = b$. Using this partial ordering along with Ω, we can define a left-most factor.

Definition. Let $a \in \Omega$. Consider $A = \{b \in \Omega | b < a\}$. Since B_n^+ is a partially-ordered set, A has a maximum. We refer to this maximum as $LF(a)$, or the left-most factor of a.

Theorem 2.9. *For all $a, b \in B_n^+$, $LF(ab) = LF(aLF(b))$.*

3 Representation

We will the Lawerence-Krammer representation for the braid group. First we shall define the vector space. Let V denote a free R-module with basis $\{x_{i,j} | s(i,j) \in Ref\}$, where R is a commutative ring with two invertible elements, denoted q and t. We will think of R as being $\mathbb{R}[t^{\pm 1}]$, where $0 < q < 1$.

The representation is defined by $\mathcal{K} : B_n \to GL(m, \mathbb{Z}[t^{\pm 1}, q^{\pm 1}])$, where $m = (n(n-1))/2$. For the Artin generator σ_i, we define

$$\mathcal{K}(\sigma_k)(x_{i,j}) = \begin{cases} tq^2 x_{k,k+1} & i = k < k+1 = j; \\ (1-q)x_{i,k} + qx_{i,k+1} & i < k = j; \\ x_{i,k} + tq^{k-i+1}(q-1)x_{k,k+1} & i < k < k+1 = j; \\ tq(q-1)x_{k,k+1} + qx_{k+1,j} & i = k < k+1 < j; \\ x_{k,j} + (1-q)x_{k+1,j} & k < i = k+1 < j; \\ x_{i,j} & i < j < k \quad \text{or} \quad k+1 < i < j; \\ x_{i,j} + tq^{k-i}(q - 1^2 x_{k,k+1} & i < k < k+1 < j; \end{cases}$$

Example 3.1. Since this is a complicated formula, we will show an example of $\mathcal{K}(\sigma_3)$, where $\sigma_3 \in B_4$. The basis for B_4 will be $\{x_{1,2}, x_{1,3}, x_{1,4}, x_{2,3}, x_{2,4}, x_{3,4}\}$.

$$\mathcal{K}(\sigma_3) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1-q & 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1-q & 1 & 0 \\ 0 & 0 & 0 & q & 0 & 0 \\ 0 & 0 & tq^3(q-1) & 0 & tq^2(q-1) & tq^2 \end{pmatrix}$$

Another interesting question is whether or not this defines a representation. It is very computational to show that the representation satisfies the Artin generator relations, we will show an example for σ_1 and σ_3. We know that these two elements commute, so the following example will show that $\mathcal{K}(\sigma_1)$ and $\mathcal{K}(\sigma_3)$ also commute.

Example 3.2. $\mathcal{K}(\sigma_1) = \begin{pmatrix} tq^2 & tq(q-1) & tq(q-1) & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & q & 0 & 1-q & 0 & 0 \\ 0 & 0 & q & 0 & 1-q & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$.

So, $\mathcal{K}(\sigma_3)\mathcal{K}(\sigma_1) =$

$$\begin{pmatrix} tq^2 & -tq(q-1)^2 + tq^2(q-1) & tq(q-1) & 0 & 0 & 0 \\ 0 & 0 & 0 & 1-q & 1 & 0 \\ 0 & 0 & 0 & q & 0 & 0 \\ 0 & (1-q)q & q & (1-q)^2 & q(1-q) & 0 \\ 0 & q^2 & 0 & q(1-q) & 0 & 0 \\ 0 & 0 & tq^3(q-1) & 0 & tq^2(q-1) & tq^2 \end{pmatrix}.$$

Now, looking at $\sigma_1\sigma_3$, we have $\mathcal{K}(\sigma_1)\mathcal{K}(\sigma_3) =$

$$\begin{pmatrix} tq^2 & tq(q-1) & tq(q-1) & 0 & 0 & 0 \\ 0 & 0 & 0 & 1-q & 1 & 0 \\ 0 & 0 & 0 & q & 0 & 0 \\ 0 & (1-q)q & q & (1-q)^2 & q(1-q) & 0 \\ 0 & q^2 & 0 & q(1-q) & 0 & 0 \\ 0 & 0 & tq^3(q-1) & 0 & tq^3(q-1) - tq^2(q-1)^2 & tq^2 \end{pmatrix}.$$

The majority of the entries are clearly equal, and with some algebra, it can be shown that $tq(q-1) = -tq(q-1)^2 + tq^2(q-1)$ and $tq^2(q-1) = tq^3(q-1) - tq^2(q-1)^2$, and thus, the swap relation is in fact perserved.

We define the set $V_1 = \bigoplus_{s \in Ref} \mathbb{R}[t]x_s \subset V$. This is the set of all of all $v \in V$ where there are no negative powers of t in any of the coefficients.

Thus, we have that $B_n^+ V_1 \subset V_1$. In other words, when we apply $\mathcal{K}(a)$ to $x_{i,j}$, the result has no negative powers of t, for every $a \in B_n^+$, and every basis element $x_{i,j}$.

We note that for $\mathcal{K}(\sigma_k)$, the entries in the matrix are all in $\{0, 1, q, 1-q\} + t\mathbb{Z}[q, q^{-1}, t]\}$. Since $0 < q < 1$, we have that all the entries are in $\mathbb{R}_{\geq 0} + t\mathbb{R}[t]$.

Thus, we define V_2 to be the set of all $v \in V$, such that, when v is written as a linear combination of the basis elements, the coefficients are all elements of $\mathbb{R}_{\geq 0} + t\mathbb{R}[t]$. Yet again, $B_n^+ V_2 \subset V_2$.

Definition. For $A \subset Ref$, define D_A to be the set of all $v \in V_2$, such that, when written as a linear combination, the coefficients in front of the basis term $x_{i,j}$ has a zero constant term if and only if $x_{i,j} \in A$.

Let $a \in B_n^+$, $A \subset Ref$. Then there is a unique $B \subset Ref$ such that $aD_A \subset D_B$. We will define B shortly. We denote $B = aA$. The map $B_n^+ \times \mathcal{P}(Ref) \to \mathcal{P}(Ref)$, given by $(a, A) \mapsto aA$, is an action of B_n^+ on $\mathcal{P}(Ref)$. We can show an explicit formula for aA. This is the subject of the Lemma 3.3. First we will show an example.

Lemma 3.3. *Let $A \subset Ref$ and $1 \leq k \leq n-1$. Then $\sigma_k A$ is the set of $s(i,j)$, $1 \leq i < j \leq n$, such that*

$$\begin{cases} true & i = k, j = k+1; \\ \{s(i,k), s(i,k+1)\} \subset A & i < k, j = k; \\ s(i,k) \in A & i < k, j = k+1; \\ s(k+1,j) \in A & i = k, j > k+1; \\ \{s(k+1,j), s(k,j)\} \subset A & i = k+1, j > k+1; \\ s(i,j) \in A & \{i,j\} \cap \{k, k+1\} = \emptyset. \end{cases}$$

Since this explicit formula is confusing, we shall present an example. The first one shows some justification for this formula.

Example 3.4. Let $A = \{s(1,2), s(2,3), s(1,3)\}$. Consider $w \in D_A$, where $w = tx_{1,2} + t^2 x_{1,3} + q^{-3} x_{1,4} + qt^2 x_{2,3} + q^{-2} x_{2,4} + x_{3,4}$. Clearly, $w \in D_A$. Now we consider what $\mathcal{K}(\sigma_3)w$ looks like. Let $u = \mathcal{K}(\sigma_3)w$.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1-q & 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1-q & 1 & 0 \\ 0 & 0 & 0 & q & 0 & 0 \\ 0 & 0 & tq^3(q-1) & 0 & tq^2(q-1) & tq^2 \end{pmatrix} \begin{pmatrix} t \\ t^2 \\ q^{-3} \\ qt^2 \\ q^{-2} \\ 1 \end{pmatrix} = \begin{pmatrix} t \\ (1-q)t^2+q^{-3} \\ qt^2 \\ (1-q)t^2-q^{-2} \\ q^2t^2 \\ 2t(q-1)+tq^2 \end{pmatrix}.$$

Thus, u has nonzero constant terms on basis elements $x_{1,3}, x_{2,3}$, and zero constant terms for the rest of the basis. Thus, $u \in D_{\sigma_3 A}$.

Now we will show what $\sigma_3 A$ looks like for a much larger A.

Example 3.5. Let

$$A = \{s(1,2), s(2,3), s(1,3), s(2,5), s(1,5)\}$$

After some calculations, it turns out that

$$\sigma_3 A = \{s(3,4), s(1,4), s(1,2), s(2,5), s(1,5), s(2,4)\}$$

$s(3,4)$ is trivially in $\sigma_3 A$ by definition. Since $s(1,3) \in A$, $s(1,4) \in \sigma_3 A$. Since $s(2,3) \in A$, $s(2,4) \in \sigma_3 A$. The reason for both these is that if $s(p,k) \in A$, $s(p,k+1) \in \sigma_k A$. Since $\{1,2\} \cap \{3,4\} = \emptyset$, $s(1,2) \in \sigma_3 A$. In fact, by this same reasoning, $s(2,5), s(1,5) \in \sigma_3 A$. This example will be used later.

4 Closed Sets and Braid Groups

Our primary goal with this section is to define certain subsets of V by denoting them C_x, where $x \in B_n$. These subsets will have certain properties that are used to prove the faithfulness of $\mathcal{K}$.

Let CL denote all closed subsets of S_n. Using the above definition of $\sigma_k A$, we get the following theorem.

Theorem 4.1. *Let $x \in B_n^+$, $A \in CL$. Then $(rx)A \in CL$.*

Proof. Let $A \in CL$. Based on the fact that every element of B_n^+ is a sequence of Artin generators, it suffices to prove the theorem using the Artin generators. Consider σ_k. Consider $s(p,q), s(q,r) \in \sigma_k A$. For brevity, we will demonstrate the case $r = k$, and $\{p,q\} \cap \{k, k+1\}$ is empty. Since $\{p,q\} \cap \{k, k+1\}$ is empty, $s(p,q) \in A$. Since $s(q,r) \in \sigma_k A$, it follows that $s(q,r), s(q,k+1) \in A$, by Lemma 3.3. Since $s(p,q), s(q,k+1) \in A$,

$s(p, k+1) \in A$, since A is closed. By Lemma 3.3, $s(p, r), s(p, k+1) \in A$ implies that $s(p, r) \in \sigma_k A$. Thus, we have established one case. By similar arguements, it can be shown that $\sigma_k A$ is closed. □

Example 4.2. We note that in Example 3.5, we defined an A, and calculated $\sigma_3 A$. A is closed, and with checking, it turns out that $\sigma_3 A$ is also closed.

Another note is that it is very difficult to tell the difference between xA as defined when $x \in B_n^+$, and $xA = \{a | xa \in Ref\}$. We will avoid confusion by always using $(rx)A$ to denote the action of B_n^+ on $\mathcal{P}(Ref)$.

As noted earlier in the paper, not every element of $L(S_n)$ is closed, that is, $L(S_n) \neq CL$. This may present a difficulty when working with closed sets, yet the following theorem allows us to avoid this difficulty.

Theorem 4.3. *For every $A \in CL$, there is a $B \in L(S_n)$ such that $B \subset A$ and, for all $C \in L(S_n)$, if $C \subset A$, then $C \subset B$. We denote B by $Pro(A)$.*

Here is an example of the theorem in use.

Example 4.4. Let $A = \{s(1,2), s(2,3), s(1,3), s(2,5), s(1,5)\}$. A is a closed set, and it was shown in example 2.8 that A is not an element of $L(S_n)$. However, $L(s(1,3)) \subset A$. So $Pro(A)$ is at least as big as $L(s(1,3))$. There are 5 possible subsets containing 4 elements. However, $A - \{s(1,3)\}$ and $A - \{s(1,5)\}$ are not closed. The remaining three subsets still have $s(1,3)$ and $s(1,5)$, and thus, the same arguement from before applies. Thus $Pro(A) = L(s(1,3))$.

Now we show the usefulness of $Pro(A)$.

Definition. Let GB denote the map $rL^{-1}Pro : CL \to \Omega$. We call GB the greatest braid.

In order to understand what GB does, let us look at the individual parts. Let $A \in CL$. Then we know that $Pro(A) \in L(S_n)$. Thus, L is defined for $Pro(A)$, and since L is bijective, we can take L^{-1} of $Pro(A)$. This gives us an element of the symmetric group. Then we use our map r to get a braid in Ω. Since $Pro(A)$ is the largest element of $L(S_n)$ such that $Pro(A) \subset A$, the element of a symmetric group that L maps to $Pro(A)$ must be the largest element that maps to a subset of A. Thus, the resulting braid is the "largest" braid that can be made out of the elements of A. There is another fact about GB that we will define a little later.

Example 4.5. Here is one final example involving

$$A = \{s(1,2), s(2,3), s(1,3), s(2,5), s(1,5)\}$$

We have already shown that $Pro(A) = L(s(1,3))$, and that $s(1,3) = s(1,2)s(2,3)s(1,2)$. Thus,

$GB(A) = rL^{-1}Pro(A) = rL^{-1}L(s(1,3)) = rs(1,3) = r(s(1,2)s(2,3)s(1,2)) = \sigma_1\sigma_2\sigma_1$

Definition. Now we will define C_x. For $x \in \Omega$, define

$$C_x = \cup\{D_A | A \in CL, GB(A) = x\}$$

5 Faithfulness

We will give a basic sketch of the theorems used to prove the faithfulness of $\mathcal{K}$.

Lemma 5.1. *If $x \in B_n^+$, $A \in CL$, $y = GB(A)$, then $GB((rx)A = LF(xy))$.*

Here is another important proposition that validates the reason behind defining C_x.

Proposition 5.2. *Suppose we are given subsets $C_x \subset V$, where $x \in \Omega$. Suppose that for $x, y \in \Omega$, C_x, C_y are non-empty, and $C_x \cap C_y$ is empty. Suppose also that $\sigma_k C_y \subset C_{LF(\sigma_k y)}$ holds for all k, $1 \leq k \leq n$, and for all $y \in \Omega$. Then for all $x \in B_n^+$, $xC_y \subset C_{LF(xy)}$. Moreover, the B_n-action on V is faithful.*

Theorem 5.3. *$\mathcal{K}$ is faithful.*

Proof. We use proposition 5.2 to prove the faithfulness of $\mathcal{K}$. Consider $x \in \Omega$, and define C_x as noted previously. Consider $GB(L(r^{-1}x))$. Well, $Pro(L(r^{-1}x) = L(r^{-1}x)$, and $rL^{-1}Lr^{-1}x = x$. So $GB(L(r^{-1}x)) = x$. Thus, $\emptyset \neq D_{L(r^{-2}x)} \subset C_x$. So the C_x are nonempty. It also turns out that the C_x are also pairwise disjoint. Now we must show that for all $_k$, $1 \leq k \leq n$, and for all $y \in \Omega$, the inclusion $\sigma_k C_y \subset C_{LF(\sigma_k y)}$. Since $C_y = \cup\{D_A | A \in CL, GB(A) = y\}$, it suffices to show that for each of the D_A, $\sigma_k D_A \subset C_{LF(\sigma_k y)}$. By Lemma 3.3, there is an $\sigma_k A$ with $\sigma_k D_A \subset D_{\sigma_k A}$. Since $A \in CL$, by a previous theorem $\sigma_k A \in CL$. Thus, Pro is defined for $\sigma_k A$, and thus, so is $GB(\sigma_k A)$. By definition of $C_{GB(\sigma_k A)}$, it follows that $D_{\sigma_k A} \subset C_{GB(\sigma_k A)}$. By Lemma 5.1, $GB(\sigma_k A) = LF(y)$, we have finished our proof. Thus, by Proposition 5.2, $\mathcal{K}$ is faithful.

□

6 Future work

We have done a great deal of research into braid groups. We have found that there is a second set of generators, called the band generators, that also generates $B_n[3]$. These generators are of the form a_{rs}, where $1 \leq s < r \leq n$. In this braid, the rth and sth band are lifted up and crossed over each other, the rth band passing over the sth band, and then placed back in the braid. Basically, the rth band and sth band switch positions, with the rth band crossing on top, and both bands crossing on top of all the bands between r and s.

One of our goals will be to define $\mathcal{K}$ in terms of the band generators, which seem to be more closely related to the basis for V. Another interesting thing we may explore is whether or not we can find $\mathcal{K}^{-1}$ as an explicit formula. Currently, one would have to break the matrix down into matrices of the Artin generators, and then apply $\mathcal{K}^{-1}$ to them, and then rebuild the braid from there.

Another interesting fact is that there is another representation for the braid group, called the Burau representation. The Burau representation has been proven to be unfaithful for $n > 5$. However, all the proofs are topological in nature. It is a good question whether or not an "algebraic" proof of this fact is possible.

References

Emil Artin, *Theory of Braids*, Annals of Math., v. 48 (1947), 101-126.

Daan Krammer, *Braid groups are linear*, Annals of Math., v. 151 (2002), 131-156.

J. S. Birman, K. H. Ko, and S. J. Lee, *A New Approach to the Word and Conjugacy Problem in the Braid Groups*, Advances in Mathematics 139 (1998), 322-353.