Journal of Knot Theory and Its Ramifications, Vol. 11, No. 4 (2002) 575–599
© World Scientific Publishing Company

A TEMPERLEY-LIEB BASIS COMING FROM THE BRAID GROUP

MATTHEW G. ZINNO*
Department of Mathematics, Columbia University,
2990 Broadway, New York, NY 10027, USA
matzinno@math.columbia.edu

Abstract

The Temperley-Lieb algebra A_{n-1}, into which the n-strand braid group B_n maps homomorphically, has dimension equal to the Catalan number $C_n = \frac{1}{n+1}\binom{2n}{n}$. The elements of the braid group called *canonical factors*, which come from the band presentation of that group and were used by Birman, Ko, and Lee in their solution to the word problem, form a set whose size is also C_n. In this paper, it is shown that the homomorphic images of the canonical factors form a basis for the vector space underlying the Temperley-Lieb algebra.

1 Introduction

As part of his study of von Neumann algebras and subfactors, Vaughan Jones, in [2] and [3], investigated two algebras into which the braid group B_n maps homomorphically: the Hecke algebra, which has dimension $n!$, and one of its quotients, the Temperley-Lieb algebra, whose dimension is the Catalan number $C_n = \frac{1}{n+1}\binom{2n}{n}$. His main result in [3] was the discovery of a one-variable polynomial arising from a trace function on the Temperley-Lieb algebra. This polynomial is an invariant not only for braids but for links, and is now known as the Jones polynomial.

These algebras also touch on knot theory and braid theory in several other ways beyond this polynomial. For example, Jones also analyzed the

*Partially supported by NSF grants DMS-9705019, DMS-9973232, and DMS-97-03756

semisimple structure of these algebras, from which one can study irreducible representations of the braid group. A small part of this research showed that the previously studied Burau representation, long thought to be the primary candidate for a faithful representation of the braid group, appeared as one of the irreducible representations of the Hecke algebra.

One aspect of the study of the braid groups which seemed unconnected to these algebras was the word problem, the question of determining whether two braid words are equivalent in the braid group. This problem and the related conjugacy problem had been solved by a method which involved putting the words into a certain normal form based on permutation braids. Recently, a new (though similar) solution to both problems was discovered by Birman, Ko, and Lee [1]. Its advantages were a faster algorithm than the previous solutions, and also a related solution to the shortest word problem for B_4. It was based on a new presentation for the braid group, in terms of *band generators*, and used short braids called *canonical factors* in place of the permutation braids. While there are $n!$ permutation braids for the braid group B_n, there are only $C_n = \frac{1}{n+1}\binom{2n}{n}$ canonical factors.

The recurrence of this Catalan number in two aspects of braid theory encourages a search for a connection between the canonical factors and the Temperley-Lieb algebra. In fact, this paper will show that the following connection holds: that these canonical factors, mapped into the Temperley-Lieb algebra, form a basis for the underlying vector space.

Acknowledgements

This paper contains work which is part of my Ph.D. thesis. I'd like to thank my advisor, Joan Birman, for her invaluable assistance. Besides her everyday commentary and guidance, she brought to my attention many of the structures and concepts used in this work, and had several ideas for ways to try to connect them.

I would also like to thank Vaughan Jones, Richard Stanley, and Radu Popescu for their assistance.

2 Braid Group

The braid group B_n has many definitions and interpretations. Perhaps the easiest to see is a pictorial one. A *braid* is a diagram consisting of two horizontal bars, one at the top and one at the bottom of the figure, with n nodes on each bar (usually drawn equally spaced), and n *strands*, always running strictly downward, connecting the upper and lower nodes. This figure represents an isotopy class of embeddings of the strands in 3-space, so the strands are allowed (in fact, required) to cross over and under each other rather than intersect, and the directions of these crossings are marked in a conventional way on the diagram. Among all braids, those which are isotopic via braids in $\mathbb{R} \times I$ are identified.

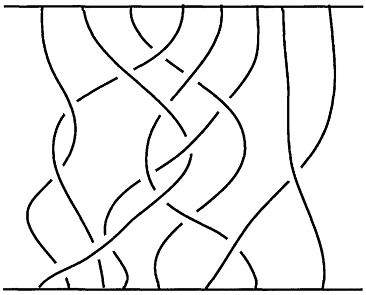

Figure 1: A sample braid diagram.

Braids form a group. The identity element is the braid with no crossings, multiplication is concatenation (draw one diagram above the other, and erase the center bar), and the standard set of generators (known as *Artin generators*) consists of braids σ_i $(1 \leq i < n)$, where the only crossing is that of the ith strand under the next strand. See Figure 2(a). The relations in the braid group are easily described:

$$\sigma_i \sigma_j = \sigma_j \sigma_i \text{ for } |i-j| \geq 2 \tag{1}$$

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}. \tag{2}$$

In [1], Birman, Ko, and Lee introduced an alternate presentation of the braid group, using *band generators* a_{ts} $(n \geq t > s \geq 1)$ which correspond pictorially to the crossing of arbitrary strands t and s, in front of all other strands. See Figure 2(b). They can therefore be expressed in the standard Artin presentation as the product

$$a_{ts} = \sigma_{t-1}\sigma_{t-2} \ldots \sigma_{s+1}\sigma_{s+1}^{-1} \ldots \sigma_{t-2}^{-1}\sigma_{t-1}^{-1}.$$

Notice that $a_{(i)(i-1)} = \sigma_i$.

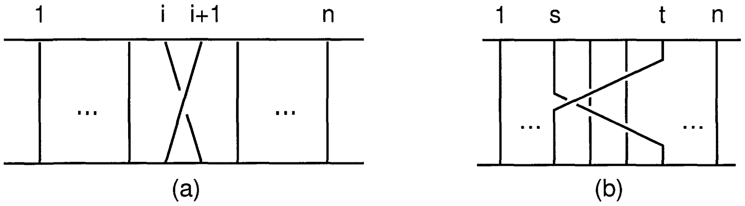

Figure 2: (a) The Artin generator σ_i. (b) The band generator a_{ts}.

Using the band generators as a generating set for the braid group, defining relations are:

$$a_{ts}a_{rq} = a_{rq}a_{ts} \text{ if } (t-r)(t-q)(s-r)(s-q) > 0 \quad (3)$$

$$a_{ts}a_{sr} = a_{tr}a_{ts} = a_{sr}a_{tr} \text{ for } t > s > r \quad (4)$$

A more intuitive way to express the condition on (3) is that the sets $\{t, s\}$ and $\{r, q\}$ do not separate each other on the number line.

A braid which can be written as a product of band generators such that every pair of adjacent letters is of the form $a_{ts}a_{sr}$ $(t > s > r)$ is a *descending cycle*. Descending cycles will be written with the sequence of indices enclosed in brackets: *e.g.*, the word $a_{86}a_{65}a_{52}a_{21}$ is written as $[8\ 6\ 5\ 2\ 1]$.

Two descending cycles $[t_j\ t_{j-1}\ \ldots\ t_1]$ and $[s_i\ s_{i-1}\ \ldots\ s_1]$ are *parallel* if every band generator in one commutes with every band generator in the other; that is, the sets $\{t_a, t_b\}$ and $\{s_c, s_d\}$ never separate each other on the number line, $\forall a, b, c, d$. This will mean one of two things: either all the indices of one cycle are strictly greater than all the indices of the other, or all the indices of one cycle (say $[s_i\ \ldots\ s_1]$) are strictly between two consecutive indices t_b, t_{b-1} of the other cycle. In the latter situation, we will refer to the first cycle as being *nested* inside the other cycle, or even inside the generator $[t_b\ t_{b-1}] = a_{t_b t_{b-1}}$.

A *canonical factor*, or *canfac*, is a braid which can be written as a product of parallel descending cycles. As shown in [1], the number of canonical factors in the n-strand braid group B_n is the Catalan number $C_n = \frac{1}{n+1}\binom{2n}{n}$. A braid written as a product of band generators is a canfac if and only if it contains no *obstructing pairs*, which are generators a_{ts} and a_{rq} appearing in that order (but not necessarily consecutively) in the word, such that either:

- $a_{ts} = a_{rq}$ (they match), or

- $\{t, s\}$ and $\{r, q\}$ separate each other on the number line (they interlace), or
- $a_{rq}a_{ts}$ is one of the forms given in equation (4).

3 Temperley-Lieb Algebra

The Temperley-Lieb algebra A_{n-1} can be defined on noninvertible generators e_i $(1 \leq i < n)$ with relations:

$$e_i e_j = e_j e_i \text{ for } |i-j| \geq 2 \tag{5}$$

$$e_i^2 = e_i \tag{6}$$

$$e_i e_{i\pm 1} e_i = \tau e_i \tag{7}$$

along with particular conditions on $\tau \in \mathbb{C}$ and a trace on the algebra.

Setting t such that $\tau^{-1} = 2 + t + t^{-1}$, and setting $g_i = (t+1)e_i - 1$, we can get an alternative presentation of A_{n-1}, with invertible generators g_i $(1 \leq i < n)$ which satisfy the relations:

$$g_i g_j = g_j g_i \text{ for } |i-j| \geq 2 \tag{8}$$

$$g_i g_{i+1} g_i = g_{i+1} g_i g_{i+1} \tag{9}$$

$$g_i^2 = (t-1)g_i + t \tag{10}$$

$$g_i g_{i+1} g_i + g_i g_{i+1} + g_{i+1} g_i + g_i + g_{i+1} + 1 = 0 \tag{11}$$

Notice that the braid group will map homomorphically into this algebra under $\phi : \sigma_i \mapsto g_i$, as the braid relations (1)-(2) are satisfied.

We will call a (monomial) word in the algebra (written in either generating set $\{e_i\}$ or $\{g_i\}$) *reduced* if it is written with no inverses of generators (irrelevant for $\{e_i\}$) and cannot be written as a linear combination of shorter words. Notice that elements of the algebra written as words in $\{g_i\}$ which contain inverses of generators can be written without inverses as sums of words of equal or lower wordlength, using $g_i^{-1} = t^{-1}g_i + (t^{-1} - 1)$.

It is easy to see that every non-reduced word in $\{e_i\}$ will be a multiple (specifically, by a power of τ) of a reduced word, since all the equivalence relations are on monomials.

It is not possible to have any word reduce in different ways to two reduced words which are not equivalent under commutativity. In [2], Jones discusses a unique ordering for reduced words (which he groups as being equivalent if you can travel between them using only the commutativity relation), involving using the commutativity relation to push the maximal index to the right as far as possible. This gives a unique representative for every class of reduced words equivalent under the commutativity relation only:

$$(e_{j_1}e_{j_1-1}\dots e_{k_1})(e_{j_2}e_{j_2-1}\dots e_{k_2})\dots(e_{j_p}e_{j_p-1}\dots e_{k_p})$$

where j_p is the maximal index in the word and $j_i \geq k_i$, $j_{i+1} > j_i$, $k_{i+1} > k_i$. Jones shows that the number of these unique representatives, called *ordered reduced words*, is the Catalan number $C_n = \frac{1}{n+1}\binom{2n}{n}$. He also points out that these words are linearly independent, and that all words are proportional (by some power of τ) to the reduced words which they reduce to. This means that if some word reduces in two different ways, the two resulting reduced words must be proportional to the original word, and thus proportional to each other. If they are not equivalent under commutativity, then they will each be equivalent to different ordered reduced words, which will therefore be proportional. However, this violates the linear independence of those words.

This allows us to speak of reduced words which are equivalent under the commutativity relation as simply being equivalent (in the algebra), as that relation would always be sufficient. However, we will also at times refer to reduced words without referring to equivalence; the specific spellings of reduced words matter for some arguments, and equivalent reduced words may not be substituted in such cases.

Lemma 1. *Let W be a word written in the alphabet $\{g_i\}$. Consider the corresponding word W' in the alphabet $\{e_i\}$, taken by keeping the same sequence of indices. Assuming that W is written only on positive generators, then W is reduced iff W' is.*

Proof. Unreduced positive words in the two alphabets have the same form. Any consecutive strings e_i^2 or g_i^2 cause the word to reduce, as do consecutive strings $e_ie_{i\pm1}e_i$ or $g_ig_{i\pm1}g_i$. If none of these are present in the word, or in any of its equivalents under the conjugation rule only, then the word is reduced. □

Theorem 1. *A word in the algebra is reduced if and only if for every index appearing more than once in the word, between any two successive instances of that index, the previous index and the next index occur in between exactly once.*

In other words, if we are working in the $\{e_i\}$, between any two successive instances of e_j there must be exactly one e_{j-1} and exactly one e_{j+1} for the word to be reduced.

Proof. We will prove the statement for $\{e_i\}$; it is obvious by Lemma 1 that the same holds for $\{g_i\}$. Notice also that the desired property is invariant under the commutativity relation, so it is sufficient to prove the lemma for equivalence classes of reduced words.

Consider a reduced word W, which contains at least two copies of e_j. We will look at two successive instances of e_j in the word, thus with no other letter e_j in between. Let $n(W)$ equal the number of letters in between those two instances. Consider the set of reduced words equivalent to W which we can get by repeated applications of the commutativity relation to those two instances of e_j (and, of course, the letters adjacent to them), and let W' be the word which minimizes n.

We know that $n(W')$ must be at least 2, otherwise the word would reduce by relation (6) or (7). We also know that the first of the $n(W')$ letters in between is either e_{j-1} or e_{j+1}, as is the last of the $n(W')$ letters. Let us leave aside for now the case where these two letters have the same index, and look at what happens if they are distinct.

Consider what indices might be represented in the remaining $n-2$ letters in between. There are no letters e_j, since we are looking in between two successive instances of e_j already. There may be another letter e_{j-1} or e_{j+1}, but if there is not, then we are done: the word W' exhibits the desired property for this value of j.

Our remaining case here is similar to the case left aside earlier. In both cases, our word contains two instances of either e_{j-1} or e_{j+1} in between the two instances of e_j we were looking at. But we can just apply the same process to this new pair (or a further interior pair, if this pair is not successive). From this we see that since there cannot be a e_j in this part of the word, we must again have a pair of the next larger or smaller index, and we repeat again with again the same result. Eventually, we will run out of both letters in the word and indices in the braid, and so this situation cannot occur. Between any two successive instances of e_j there must therefore be exactly one e_{j-1} and exactly one e_{j+1}.

We also need it to be true that all words of this form are reduced words. Notice that this condition is unchanged under application of the commutativity relation, since letters with adjacent indices cannot commute past each other. So no matter how you manipulate the word using this relation, there will be no way to get two letters with the same index closer to each other than three letters away. Equivalently, any three consecutive letters will always be distinct.

Let S be the set of equivalence classes of reduced words, and let T be the set of words with the desired property, also modulo the equivalence relation of commutativity. We have shown above that $S \subseteq T$. Using the ordered reduced words, Jones showed that there are $C_n = \frac{1}{n+1}\binom{2n}{n}$ equivalence classes of reduced words. According to Stanley [4], this is also the size of the set T. Since the sets are the same size, the inclusion of one in the other implies that the sets are identical. □

For any (monomial) word W written in one of the generating set $\{g_i\}$, consider the ordered (finite) sequence S consisting of the indices of the letters in the word. Any word written in the generating set $\{e_i\}$ whose similarly defined sequence of indices is a subsequence of S (including S itself) will be called a *subword* of the original word W. Beyond the strange fact that we are choosing to call a word written in a different generating set a subword, it is also important to note that the indices of a subword need not come from letters which are consecutive in the original word, as the term might otherwise imply.

The motivation for this strange definition comes from what happens when we try to express monomial words written in $\{g_i\}$ as vectors using the $\{e_i\}$ algebra generators. Any word W written in the alphabet $\{g_i\}$ can be written in the alphabet $\{e_i\}$ instead by using $g_i = (t+1)e_i - 1$ and $g_i^{-1} = t^{-1}(t+1)e_i - 1$. After multiplying and collecting like terms, we have W expressed as a linear combination of the corresponding word W' written in the $\{e_i\}$ (keeping the same sequence of indices) and all the words in $\{e_i\}$ whose letters, in order, are a subsequence of the letters of W'. Thus, with this definition, we say that W (a word in $\{g_i\}$) is a linear combination of all its subwords (which are words in $\{e_i\}$). Notice, however, that not all of these subwords are reduced.

One way to view the algebra is as a vector space V where multiplication of elements is also defined. One basis for this vector space consists of all the equivalence classes of reduced words in the generating set $\{e_i\}$, and the vector space is thus finite-dimensional, of dimension C_n.

Proposition 1. *Equivalence classes of reduced words in the generating set $\{g_i\}$ form a basis for V.*

Proof. Any reduced word W written in the alphabet $\{g_i\}$ can be written in the alphabet $\{e_i\}$ instead by using $g_i = (t+1)e_i - 1$. (Notice that $t+1 \in \mathbb{C}$ is invertible, from the definition of t via τ.) After multiplying and collecting like terms, we have W expressed as a linear combination of its subwords. Each of those subwords is proportional to a reduced word. So each reduced word W in $\{g_i\}$ is a linear combination of reduced words in $\{e_i\}$, the (unique) longest of which is W'.

Now if we take the lists of reduced words in $\{e_i\}$, $\{g_i\}$ (which are the same list) and order them by wordlength, then for all j, the j^{th} reduced word in the $\{g_i\}$ can be written as a sum involving only the first j reduced words in the $\{e_i\}$. Thus the matrix transforming the reduced words in $\{g_i\}$ to the reduced words in $\{e_i\}$ will be upper triangular, and the diagonal entries will be $(t+1)^{\mathbf{length}}$. The matrix is thus invertible, with its inverse telling us how to write each reduced word in $\{e_i\}$ in terms of the reduced words in $\{g_i\}$. The $\{g_i\}$ reduced words form a basis, and this matrix is the change-of-basis matrix. □

4 Canfacs

Recall from Section 2 the canonical factors, or canfacs, of the braid group. This set has size $C_n = \frac{1}{n+1}\binom{2n}{n}$, equal to the dimension of the Temperley-Lieb algebra. Because the braid group maps into the algebra by $\sigma_i \mapsto g_i$, we can map the canfacs into the algebra as well. For clarity, let us specify one particular word in the equivalence class of any canfac.

Write each canfac as a product of parallel descending cycles, ordered by the maximal number in each cycle. For example, the canfac [6 5 4][8 7][2 1][7 3] should be rearranged to [8 7 3][6 5 4][2 1]. Now write each cycle out in band generators, and write each band generator $[j\ i]$ as $\sigma_{j-1} \ldots \sigma_i \sigma_{i+1}^{-1} \ldots \sigma_{j-1}^{-1}$. Under the homomorphism $\phi : \sigma_i \mapsto g_i$, each band generator maps to a word in $\{g_i\}$ which we will call a *syllable*. The product (concatenation) of the syllables we get from each band generator gives us a word in the alphabet $\{g_i\}$, and we will identify each canfac with the word so obtained.

Theorem 2. *The canfacs form a basis for V.*

The proof of this theorem is very involved, and will occupy the remainder of this chapter. As in the proof of Proposition 1, we will attempt to construct a matrix with rows indexed by the reduced words in $\{e_i\}$, and columns indexed by the canfacs, and each column describing how to write the canfac as a linear combination of reduced words in $\{e_i\}$. We get these expressions by switching generating sets as before, which leaves us looking at a canfac (which is a monomial word in $\{g_i\}$) as a linear combination of its subwords (which are words in $\{e_i\}$). If this matrix is invertible, then its inverse will tell us how to write each reduced word in terms of canfacs, and so the matrix will be a change-of-basis matrix.

Before we construct the matrix, we will need several preliminary results about canfacs, syllables, and reduced words. We will also want to distinguish between two types of syllables, depending on their length. Band generators $[i+1\ \ i] = \sigma_i$ map to *short syllables* g_i, only one letter in length. Other band generators $[j\ \ i]$ with $|j-i| \geq 2$ map to *long syllables* of more than one letter:

$$g_{j-1}g_{j-2}\cdots g_i g_{i+1}^{-1}\cdots g_{j-2}^{-1}g_{j-1}^{-1}.$$

Notice that all the indices present in a long syllable are repeated, with the exception of the lowest index g_i. This letter we will call the *center* of the syllable, splitting the remainder of the syllable into the *left* and the *right*. Note that the exponent of a letter is negative iff the letter is on the right in its syllable. For ease of reference, we may also call the only letter of a short syllable the center.

Lemma 2. *For any canfac w_1 written in the form given above, removal of the final letter still yields a canfac written in this form.*

Proof. Let the final letter of w_1 be g_i^{ε} (where $\varepsilon = \pm 1$), then $w_1 = w_2 g_i^{\varepsilon}$. We wish to show that w_2 is a canfac. If $\varepsilon = +1$, then the final syllable of w_1 was a short syllable, and we have removed it. The effect on the cycle structure of the canfac is to either remove the final cycle or to shorten it by removing the final number in that cycle. Either way, what we have left is obviously still a canfac.

If $\varepsilon = -1$, then we've replaced the final syllable

$$g_{j-1}g_{j-2}\cdots g_i g_{i+1}^{-1}\cdots g_{j-2}^{-1}g_{j-1}^{-1} = [j\ \ i]$$

with

$$(g_{j-1})g_{j-2}\cdots g_i g_{i+1}^{-1}\cdots g_{j-3}^{-1}g_{j-2}^{-1} = [j\ \ j-1][j-1\ \ i] = [j\ \ j-1\ \ i].$$

Since this is the end of the last cycle in the word, no other cycles are in the gap between $j-1$ and i, so this is still a canfac. □

Proposition 2. *Let ϕ denote the map from B_n into A_{n-1} corresponding to $\sigma_i \mapsto g_i$, as used above. Let $\beta \in B_n$ be a canfac in the specific form described above, such that, somewhere in the word β, we can apply the canfac commutativity relation $a_{ts}a_{rq} = a_{rq}a_{ts}$, $t > s > r > q$, to get a different braid word β'. Then $w = \phi(\beta)$ (which we have identified as the canfac in the algebra) and $w' = \phi(\beta')$ are equivalent in the algebra under the commutativity relation $g_ig_j = g_jg_i$, $|i-j| \geq 2$.*

Proof. The only movement from w to w', corresponding to the movement from β to β', is the movement of the letters in $\phi(a_{ts})$ and $\phi(a_{rq})$. The indices of the letters involved are sufficiently separated to commute as desired. □

Corollary 1. *When trying to find a word which is equivalent to a subword of a given canfac $\phi(\beta)$, it is sufficient to find a subword of a word $\phi(\beta')$, as defined in Proposition 2.*

5 Full Reduced Words

Lemma 3. *In any subword of a canfac, the contribution from any syllable contains each distinct letter at most once.*

Proof. The statement is clearly trivial for short syllables, which consist of only one letter. Any long syllable contains any index at most twice, so to violate the statement it sould have to contribute both of its instances of some letter $g_k^{\pm 1}$. But the letters in between have excusively lower indices, and thus such a word cannot be reduced. □

In reference to a subword of a canfac, any syllable which contributes each of its distinct letters exactly once will be called *full.* If every syllable is full, we also call the subword *full.*

Proposition 3. *Suppose A is a syllable of a canfac, and that A contains the letters g_k and g_{k-1}. Suppose that in a given reduced subword of this canfac, e_k and e_{k-1} are contributed by A, and also assume that every syllable nested in A is full. If e_k appears on the right of A or any later syllable, then that letter e_k must appear on the right of <u>each</u> of these syllables in which it appears.*

Proof. Suppose that in our reduced subword, one of the relevant syllables contributes e_k on the right and another contributes e_k on the left or center.

Somewhere there must be two such syllables, A_1 (appearing earlier in the word) and A_2 (appearing later), with no e_k in between. Any e_k in the center of its syllable must be the last e_k in the word, so A_1 does not contribute its e_k in the center; therefore, the lowest index in A_1 must be $k - 1$ or lower.

Since A_1 and A_2 both contain e_k, the cycle containing A_2 must be nested inside A_1. Any syllables between these come from canfacs of three types: they may be from syllables later in A_1's cycle, in which case the highest index is less than $k - 1$; they may be from syllables earlier in A_2's cycle, in which case the lowest index is greater than k; or they may be from cycles between those of A_1 and A_2, in which case they are also nested in A_1 but have higher indices than A_2's cycle.

Since A_1 and A_2 both contribute e_k, there must be exactly one e_{k-1} in between, for the subword to be reduced. By the argument above, no syllable between A_1 and A_2 can contribute one, so either A_1 or A_2 must contribute it.

Notice that if a syllable contributes both e_k and e_{k-1}, the e_k must not be the center of the syllable, and the e_{k-1} must be contributed closer to the center of the syllable than is the e_k. So if A_1 is to contribute the e_{k-1} which is required between its e_k and that of A_2, it must contribute its e_k on the left. Conversely, if A_1 contributes e_k on the left, it contributes its e_{k-1} later in the subword, thus between the two instances of e_k. So the required e_{k-1} will come from A_1 iff A_1 contributes e_k on the left. Similarly, A_2 will contribute an e_{k-1} between the two instances of e_k iff its e_k is on the right.

Our hypothesis is that exactly one of A_1 and A_2 contributes its e_k on the right. However, we will see that this gives a contradiction. If e_k is on the right in A_1, then the e_{k-1} we require must come from A_2, implying that its e_k is on the right, contradicting our hypothesis. If, on the other hand, e_k is on the right in A_2, then A_2 supplies the e_{k-1} we require, and A_1 may not, implying that A_1 must contribute its e_k in the right or center. However, e_k being the center of A_1 makes no sense, as any e_k in the center of its syllable must be the last e_k in the word. So our initial supposition must be false, and the lemma is proved. □

Corollary 2. *$\forall k$, if e_k appears on the right of a syllable in a full reduced subword of a canfac, then that letter e_k will appear on the right of* <u>*each*</u> *syllable in which it appears.*

Clearly, if $g_i^{\pm 1}$ occurs only once in w_1, then it is either its own (short) syllable, or it is the center of a long syllable; either way, its exponent must be positive. If $g_i^{\pm 1}$ occurs more than once, then the rightmost cycle it appears in must be nested inside any other cycles it appears in, and those earlier cycles must contain the letter twice each (once with positive exponent, once with negative), and that index is neither the highest nor the lowest in the earlier such cycles. This also implies that if $g_i^{\pm 1}$ occurs exactly twice in w_1, then it occurs in only one syllable, which contains $g_i \dots g_i^{-1}$.

Proposition 4. *Suppose A is a syllable of a canfac w_1, and that A contains the letters g_k and g_{k-1}. Suppose that in a given reduced subword of this canfac, e_k and e_{k-1} are contributed by A, and also assume that every syllable nested in A is full. If the last occurrence of $g_k^{\pm 1}$ in w_1 has positive exponent, then e_k appears on the left in A and its nested syllables.*

Proof. If the last occurrence of $g_i^{\pm 1}$ in the word w_1 has positive exponent, then it must be in the center of its syllable (which may be long or short). By Proposition 3, no previous occurrence in A or any later syllable can be on the right; it also cannot be the center, since only the final occurrence in the word can be a center. □

Corollary 3. *Let m be any full reduced subword of a canfac w_1. For all i, if the last occurrence of $g_i^{\pm 1}$ in w_1 has positive exponent, then all previous occurrences of e_i in m are on the left in their syllables.*

Although we now have two important results about full reduced subwords of canfacs, we have yet to show that any exist. In fact, every canfac has at least one full reduced subword. We will construct such a subword, inductively.

Theorem 3. *For any canfac w_1, there exists a full reduced subword d_1 such that $\forall i$, if the last occurrence of $g_i^{\pm 1}$ in w_1 has negative exponent, then all occurrences of e_i in d_1 are on the right in their syllables.*

Proof. We induct on the length of the word w_1, which is written in the generators $\{g_i\}$. The base case is length zero, $w_1 = e$ (trivial canfac), with $d_1 = 1$ (identity element in algebra). d_1 is full, it is reduced, and it is a subword; the rest of the claim is vacuously true.

Now to induct, we remove the last letter from $w_1 = w_2 g_i^{\varepsilon}$ ($\varepsilon = \pm 1$) to obtain the canfac w_2. By our inductive hypothesis, we may assume that it has a full reduced subword d_2 with the appropriate property. Now we will construct d_1 from d_2 depending on that excised letter:

Case I. If $\varepsilon = -1$ (equivalently, $g_i^{\pm 1}$ occurs in w_1 an even number of times), consider d_2 as a subword of $w_1 = w_2 g_i^{\varepsilon}$, and move each e_i in d_2 to the right in its syllable of w_1. The resulting word is d_1.

Case II. If $\varepsilon = 1$ and e_i is not already present in d_2 (equivalently, $g_i^{\pm 1}$ occurs in w_1 exactly once), then let $d_1 = d_2 e_i$.

Case III. If $\varepsilon = 1$ and e_i is already present in d_2 (equivalently, $g_i^{\pm 1}$ occurs in w_1 an odd number of times, but more than once), then move each g_i in d_2 to the left in its syllable, and then append e_i. The resulting word is d_1.

We now need to show that this new word d_2 exhibits the desired properties.

d_1 is a subword. d_2 is a subword of w_2, and the only actions performed in any part of the construction of d_1 from d_2 are switching some letters from one side of syllables to the other (Cases I and III), and appending e_i (Cases II and III). The first action still gives us a subword of w_2, and with or without the second action, we end up with a subword of $w_2 g_i^{\varepsilon} = w_1$.

d_1 is full as a subword of w_1. We know that d_2 is full as a subword of w_2; let's see how this interacts with each case. In Case II, we add a new syllable, and its contribution is full. In Case III, we also add a new syllable, and its contribution is full, but we also rearrange the contributions of previous syllables. But those contributions are still full.

For Case I, care must be taken because w_1 and w_2 are broken into syllables differently. The last syllable of w_1, $g_j \dots g_i g_{i+1}^{-1} \dots g_j^{-1} = [j{+}1\ i]$. These letters become the last two syllables of w_2: $(g_j)(g_{j-1} \cdots g_i g_{i+1}^{-1} \cdots g_{j-1}^{-1} = [j+1\ j][j\ i]$. (The earlier syllables are, of course, unaffected, and shared by w_1 and w_2.) Since d_2 is full as a subword of w_2, those last two syllables contribute, respectively, a g_j and every letter from g_{j-1} to g_i. Considering d_2 now as a subword of w_1, we see that this new last syllable is still full, contributing every letter from g_j to g_i. We then rearrange within syllables, but this does not affect the fullness of the contributions.

d_1 is reduced. We know that d_2 is reduced, or equivalently, $\forall i$, between any two successive instances of g_i in d_2 is exactly one g_{i-1} and exactly one g_{i+1}. What happens when we construct d_1 from d_2? First, in Cases I and III, we might move all copies of e_i from one side of their respective syllables to the other. Any reshuffling of letters in the subword which can be achieved by application of the commutativity relation in the algebra will not change our criterion for the word being reduced; the only other reshuffling that happens in this inductive construction is e_i's movement past any instances of e_{i-1}. So

after this rearrangement, our reduction condition is obviously satisfied for all indices except possibly i and $i-1$ (since it was already satisfied in the original word d_2).

At this point we need to notice that if we are performing this rearrangement, the word d_2 contains an equal number of e_i and e_{i-1} (and of course, they're alternating, since d_2 is reduced). The reason is as follows. In Case III, the canfac w_1 ends with the short syllable g_i. Any previous occurrences of g_i or g_{i-1} in w_1 (and thus also w_2) occur in syllables which this last syllable nests inside, and those syllables do contain both letters g_i and g_{i-1}. Since d_2 is full, each syllable contributes both letters, and so there are an equal number of each. Similarly, in Case I, the last two syllables form the cycle $[j+1\ j][j\ i]=[j+1\ j\ i]$, and so any prior occurrences of either index occur only in syllables which this cycle nests in, so they are contributed together and in equal amounts.

Since d_2 has equal numbers of e_i and e_{i-1}, alternating, the rearrangement in question will preserve this property. The other rearrangements that occur will not affect whether the word is reduced, and so this step in the process yields a reduced word.

The remaining step we might take in constructing d_1 is appending an e_i coming from the final letter g_i^{+1}, in Cases II and III. Since d_2 is reduced, we only need to look at whether an e_{i+1} and e_{i-1} occur after the last e_i in d_2. If we are appending in Case II, then there is no prior e_i, and so there is no problem. In Case III, first notice that the previous e_i is in a syllable also containing e_{i-1} and e_{i+1}. The previous step in our construction was to move all previous e_i to the left. So the last e_i has to be on the left of its syllable, and an e_{i-1} is contributed to the right of it by that syllable. For e_{i+1} we have two cases. If e_{i+1} appears in d_2 after that syllable, then it obviously occurs after the last e_i. If, on the other hand, e_{i+1} does not appear in d_2 after that syllable, then its last occurrence in the word is in that syllable and thus has negative exponent. Because d_2 satisfies our inductive hypothesis, e_{i+1} is contributed on the right in the syllable, thus after the e_i.

We now need only to prove that extra claim on d_1, that $\forall i$, if the last occurrence of $g_i^{\pm 1}$ in w_1 has negative exponent, then all occurrences of e_i in d_1 are on the right in their syllables. The claim is clearly true for all indices except that belonging to the final letter of the word, since we are not changing positions of letters with any other indices from their locations in d_2, and d_2 satisfies the property by induction. If the final letter in w_1 has negative exponent, our construction of d_1 from d_2 lands us in Case I, where we move all letters with that index to the right, and the claim is satisfied. □

These subwords d_1 are important for the construction of our matrix, and we will take the procedure above as a definition for the subword d_1 associated to any canfac w_1. An alternate characterization is available in Corollary 5, below.

Proposition 5. *Suppose A is a syllable of a canfac w_1, and that A contains the letters g_k and g_{k-1}. Suppose that in a given reduced subword m of this canfac, e_{k-1} is contributed by A and also by every syllable nested in A which similarly contains the letters g_k and g_{k-1}. If e_k appears on the left in the subword d_1, then e_k appears in A and later syllables of m on the left.*

Proof. By Theorem 3, the last occurrence of $g_k^{\pm 1}$ in w_1 must have positive exponent. Proposition 4 then implies the desired conclusion. □

Corollary 4. *$\forall k$, if e_k appears on the left of its syllables in the subword d_1, then e_k appears on the left of its syllables in any full reduced subword of w_1.*

Corollary 5. *Of the full reduced subwords of w_1, d_1 occurs first in dictionary order.*

Proof. Let m_1 be the full reduced subword of W_1 which occurs first in dictionary order; we will show that $m_1 = d_1$. Note that d_1 and m_1 are the same length, since they're both full subwords of w_1. If they are not the same word, then let e_i be the first letter in d_1 which is different from m_1. The letter in that position in m_1 has a lower index (since m_1 has to come earlier in dictionary order), so e_i is on the left in d_1 and on the right in m_1. This is impossible, by Corollary 4, so our assumption that d_1 and m_1 are different words must be false. □

Theorem 4. *All reduced words are equivalent to subwords of some canfac.*

Proof. In fact, every reduced word m with highest index j and lowest index i is equivalent to a subword of the canfac $[j+1 \dots i][j \dots i+1][j-1 \dots i+2]$ $\dots$. (The trivial word 1 is vacuously a subword.) Notice that by Theorem 1, e_j and e_i each occur only once.

We induct on the difference $j - i$. If the difference is 0, then the highest and lowest indices are the same, thus our word is simply e_i=$[i+1\ i]$. If the difference is 1, our word is either $e_i e_{i-1}$ or $e_{i-1} e_i$, both of which are subwords of $g_i g_{i-1} g_i^{-1}$=$[i+1\ i-1]$.

Now we induct. If the difference is greater than 2, then using the commutativity relation, push the unique lowest-index letter e_i to the left, along with whichever letters it fails to commute past. The indices in the word up to that letter e_i will then be consecutive and strictly decreasing. Now look at the remainder of the word, to the right of e_i. Let the highest index appearing in this remainder be k (it may be that $k = j$, but we may have $k < j$ if e_j is now at the beginning of the word). For similar reasons as before, e_k must appear only once in the remainder. As we did with e_i, commute e_k towards the left, this time not commuting anything past the new location of e_i. The indices in the word following e_i are now consecutive and strictly increasing until we reach e_k. The letters in the word from the beginning until that e_k form some subword of $g_j g_{j-1} \cdots g_{i+1} g_i g_{i+1}^{-1} \cdots g_{j-1} g_j = [j+1\ i]$. What remains has a lower highest index and a higher lowest index, so follows by induction. □

Theorem 5. *All reduced subwords of w_1 other than d_1 are equivalent to reduced subwords of shorter canfacs.*

The proof of this theorem is intricate, and relies on constructions and intermediate propositions which are of little interest outside the scope of the proof. Consequently, it will be provided separately, in Section 7.

Theorem 6. *The map from canfacs to equivalence classes of reduced words, defined by $w_1 \mapsto d_1$, is a bijection.*

Proof. Since the sets are the same size, it is sufficient to show that the map is onto. Let s be any reduced word written in $\{e_i\}$. By Theorem 4, it is a subword of some canfac. Let w_1 be the shortest canfac of which s or any equivalent reduced word is a subword. Then by Theorem 5, this subword either is d_1 or is equivalent to a reduced subword of a *shorter* canfac. But we've chosen w_1 to be the shortest canfac, so s is equivalent to d_1. □

6 Constructing the Matrix

We will now use these subwords d_1 to help construct our matrix. We order the canfacs, which index the C_n columns of the matrix, in ascending order by length in the letters $\{g_i\}$. Though this criterion only gives us a partial ordering, as there will be many canfacs of the same length, any total ordering which respects this word length will be sufficient. Now we order the equivalence classes of reduced subwords in $\{e_i\}$, which index the C_n rows of our matrix, according to the bijection $w_1 \leftrightarrow d_1$. The entries in the matrix are obtained by expanding each canfac into a linear combination of its reduced subwords in $\{e_i\}$, as in the proof of Proposition 1. (First multiply out the product obtained by writing all $g_i^{\pm 1}$ in terms of $\{e_i\}$, then reduce and collect like terms.) We need to show that this matrix is invertible; we will do this by showing that the matrix is upper triangular, with invertible diagonal entries.

Proposition 6. *In each column w_1 of our matrix, all reduced subwords of w_1 appear on or above the diagonal.*

Proof. Induction on the columns, from left to right. The leftmost column is the trivial canfac, which has word length 0. w_1 is the trivial word 1, and so is d_1. They are equal, so the first column is the first elementary unit vector. For later columns, we use Theorem 5 to tell us that all reduced subwords of w_1 are either d_1 (whose coefficient is our diagonal entry) or are equivalent to reduced words of shorter canfacs, so appear in a previous column. There, they're on or above the diagonal, so here, where the diagonal is lower, they are always above the diagonal. □

Proposition 7. *The coefficient of d_1 in the expansion of w_1 in the algebra is invertible in $\mathbb{C}$.*

Proof. To write w_1 as an element of the algebra, as a linear combination of all the reduced words in V, we first take the Artin generator expansion of w_1 and replace every g_i with $(t+1)e_i - 1$ and every g_i^{-1} with $t^{-1}(t+1)e_i - 1$, and multiply out to get a linear combination of subwords of w_1. Before reducing or collecting, we have $2^{\text{length}(w_1)}$ separate terms, each corresponding to a choice of e_i or 1 for each letter $g_i^{\pm 1}$ in w_1. We then reduce each subword as necessary to get a linear combination of reduced words. The coefficient of any particular reduced word, such as d_1, in the expansion will be the sum of the coefficients of all the subwords of w_1 which reduce to that reduced word.

First, we notice that only one set of choices between e_i and 1 for the letters of w_1 will result in the subword d_1. Recall that d_1 is full, so contains $(\forall i)$ exactly one e_i for each syllable of w_1 containing $g_i^{\pm 1}$. The location of that e_i in the syllable is completely determined by conditions on w_1, as we can read from Corollary 3 and Theorem 3.

This does not, however, rule out the possibility that some of the nonreduced words in the expansion will reduce to d_1. Consider what happens when we reduce a subword using either one of the relations (6) or (7), thus replacing e_i^2 with e_i or $e_ie_{\pm 1}e_i$ with e_i (possibly after commuting the subword to an appropriate form). In either case, our shorter word is a subword of the word just modified, thus still (equivalent to) a subword of w_1. Moreover, the resulting subword of w_1 itself can appear in our expansion through at least two separate choices: either the first e_i could be chosen and not the second, or vice versa.

This implies that no unreduced word in the expansion can give us d_1. Consequently, d_1 only results from one of the $2^{\text{length}(w_1)}$ terms in our expansion, even after recuding and collecting like terms. Its coefficient will be exactly the coefficient we get from that one term, which we can easily calculate. Every time we choose an e_i from the left or center of its syllable, thus coming from a g_i^{+1}, we multiply by $(t+1)$, and every time we choose an e_i from the right, coming from a g_i^{-1}, we multiply by $t^{-1}(t+1)$. Every time we choose a 1 instead of an e_i, we multiply by (-1). Putting these together, we can see that the coefficient of d_1 in the expansion of w_1 will be

$$(-1)^{l-k}t^{-j}(t+1)^k$$

where l is the length of w_1, k is the length of d_1, and j is the number of times that a e_i was chosen on the right. Recall our definition of t in terms of τ, and notice that $t=0$ and $t=-1$ are impossible values. For all other values of t in $\mathbb{C}$, this coefficient is an invertible complex number. □

These invertible coefficients are the diagonal entries in the matrix. Since the matrix is upper triangular, it is therefore invertible, and it is a change-of-basis matrix from the known basis of equivalence classes of reduced words in the letters $\{e_i\}$, to the new basis of canfacs.

7 Proof of Theorem 5

Any reduced subword s which is not d_1 must differ from it in at least one syllable. Our proof will be by induction, on the length of the shortest syllable of w_1 where the contribution to d_1 differs from the contribution to s.

If d_1 and s differ in some short syllable, then its contribution to d_1 is its only letter (since d_1 is full). The only way it can contribute differently to s is by contributing nothing. If we remove this short syllable from w_1, we get a new canfac, of which s is a subword. (It may be that this new canfac is not in our stated form, if some cycle was nested inside a syllable earlier in the cycle which was cut. However, moving it into reduced form only involves commuting externally parallel cycles, which doesn't affect the equivalence class of s, by Corollary 1.)

Now we may assume that d_1 and s only differ in long syllables. Call the shortest one where they differ $A = [j+1\ m] = g_j \dots g_m \cdots g_j^{-1}$ (if there is more than one such syllable of minimal size, pick any one). By induction, we may assume that the theorem is true for any reduced subword s' which differs from d_1 in any syllable shorter than A.

We will try two different strategies, one of which will succeed for any given A. The first strategy, described in Subsection 7.1, will construct a shorter word than w_1 which has s (or, in some cases, an equivalent word) as s subword. In the cases where this new word is a canfac, we are done by direct construction of the shorter canfac.

If the new word is not a canfac, we throw it out and adopt a different strategy, relying on results found in Subsection 7.2. This second strategy, described in Subsection 7.3, will find an s', equivalent to s, which differs from d_1 in a syllable which is shorter than A. In these cases, we are done by induction.

7.1 Primary Strategy: Construction of A'

Our primary strategy will be to alter A to a shorter syllable (or cycle) A', in such a way that the contribution s receives from A can also be received from A' (in some cases, after applying the commutativity relation to s), and such that the new word we get from altering w_1 in this way is still a canfac.

It is easy to define A' in terms of A in such a way as to ensure that it can contribute to s in the same way that A does. Consider the lowest-index letter in A which is contributed to s differently than d_1. We delete that letter from the right or center of A to get a word A' which corresponds (after applying the commutativity relation) to two syllables in a canfac cycle:

- If the letter in question is the center of A (in which case that letter is not contributed to s), we delete it (and the following letter) to get:

$$\text{delete } g_m g_{m+1}^{-1} \to A' = g_j \cdots g_{m+1} \cdots g_j^{-1} = [j+1\ \ m+1]. \qquad (12)$$

- For any other letter, we delete the copy on the right of A:

$$\begin{aligned} \text{delete } g_i^{-1} \to A' &= g_j \cdots g_i (g_{i-1} \cdots g_m \cdots g_{i-1}^{-1}) g_{i+1}^{-1} \cdots g_j^{-1} \\ &= (g_j \cdots g_i g_{i+1}^{-1} \cdots g_j^{-1})(g_{i-1} \cdots g_m \cdots g_{i-1}^{-1}) = [j+1 \;\; i \;\; m] \end{aligned} \tag{13}$$

(In the case $i = j$, we do not need to commute.)

If the letter is not contributed to s, it should be clear that s is a subword of the resulting word for both formulas. For the case where the letter is contributed to s, notice that A satisfies the conditions of Proposition 5. If the letter were on the left in d_1, it could not be different in s, so it must be on the right in d_1 and the left in s. We can see here too that s is a subword of our new word.

The only remaining detail is whether this word is a canfac. The word as written may not be in the form specified for a canfac word, particularly if the cycles are listed in the wrong order. If this is the case, we can simply commute parallel cycles to put the word in the desired form. However, there may be times when the descending cycle structure for our words actually does not form a canfac. In these cases, we will need to instead use our secondary strategy.

7.2 Obstructions

If the new word constructed in Subsection 7.1 cannot be rearranged to a canfac, it will be the result of obstructing pairs in our cycle structure. In shortening A to A', we might end up with some syllable of A' being incompatible with some other syllable B of w_1 which was nested inside A, thus $B = [k_1 \;\; k_2]$ with $j \geq k_1 > k_2 > m$. For precision, define B as the first such obstruction.

Notice in all cases that B must be a shorter syllable than A. Therefore, by our induction hypothesis, B contributes to s and d_1 in the same way. In particular, B must be full with respect to s. Also notice that there may be other syllables between A and B. These may consist of syllables later in A's cycle, in which case the highest index is less than m; syllables earlier in B's cycle, in which case all indices are higher than those in B; or they may be from cycles between those of A and B, in which case they are also nested in A but have higher indices than B's cycle. Let D denote the section of the word consisting of all these syllables.

Lemma 4. *If $A' = [j+1 \ \ i \ \ m]$ has a nested obstruction, then the first such obstruction B contains the letter g_i, and A is not full with respect to s.*

Proof. Since B is defined to be the first syllable which obstructs A', it must be the first syllable nested inside A which contains either g_i or g_{i-1}.

Suppose that B does not contain g_i. It therefore must contain g_{i-1}, and since it contributes all of its letters, it must contribute e_{i-1} to s. We also know that A contributes e_{i-1} to s, since e_i is the lowest-index letter which A contributes differently to s and d_1 (and g_{i-1} must be in A, since B is nested). For s to be reduced, there must be an e_i in between. This letter cannot be contributed by B, and it also cannot be contributed by D (since B is the first obstruction). The required e_i must be contributed by A, and be on the right there. Since s differs from d_1 at this letter, d_1 must have it on the left. But then Proposition 5 gives us a contradiction, so this case cannot occur.

Now let B contain g_i, and assume A is full with respect to s. Consequently, it contributes e_i to s on the left but to d_1 on the right. B also contributes e_i to d_1, so there must be an e_{i-1} contributed in between. This letter cannot come from D (again, because B is the first obstruction), so it must come from either A or B. A cannot contribute the required e_{i-1} to d_1, since its e_i is on the right. But because A also satisfies the conditions of Proposition 3, and is also the shortest syllable with a different contribution to s than to d_1, it must be the shortest syllable of w_1 which has g_i in a non-central position. Therefore, g_i is the center of B, and B cannot contribute an e_{i-1} to d_1. No e_{i-1} is available, and we again get a contradiction. □

Recall that our other potential formula for A' came only from the situation where the center letter of A was the only one contributed differently, and was thus missing from s. Along with the previous lemma, this gives us:

Lemma 5. *If A' has a nested obstruction, then A is not full with respect to s.*

7.3 Secondary Strategy: Commute into A

Our secondary strategy will be to apply the commutative relation to s to yield an equivalent word s' for which the theorem is true. Specifically, we will move some letter of s from DB to A, yielding an s' which differs from d_1 in a shorter syllable than A, and is therefore covered by our induction hypothesis.

Our method may be best introduced through an example. Suppose our canfac is [6 1][5 2][4 3] $= (g_5g_4g_3g_2g_1g_2^{-1}g_3^{-1}g_4^{-1}g_5^{-1})(g_4g_3g_2g_3^{-1}g_4^{-1})(g_3) = w_1$, and our reduced subword is $s = (e_2e_1e_4e_5)(e_3e_2e_4)e_3$, with the contributions from A and B marked with parentheses. In this case, A fails to contribute e_3, but amending A to A'=[6 3 1] causes an obstruction with B=[5 2]. The solution to this is to commute the e_3 contributed by B to the left, until it is in a position where it could have been contributed by A. Since it cannot commute past the e_4 on the right in A, we push that to the left as well, to get the equivalent word $s' = (e_4e_2e_1e_3e_5)(e_2e_4)e_3$. Now, the shortest syllable which is different from d_1 is the shorter syllable in the middle, thus our induction hypothesis says that this subword is equivalent to a reduced subword of a shorter canfac.

This is indicative of what we want to do in general. We will find a letter contributed by B (or some other syllable nested in A) which will commute within s to a location where it could have been contributed by A instead. We then have an equivalent word s' which differs from d_1 in some shorter syllable than A, to which we can apply our induction hypothesis.

We need to ensure in each case that such a letter exists. This will be accomplished by the following two lemmas.

Lemma 6. *There exists an index k which satisfies the following conditions:*

1. *e_k is contributed to s by DB.*
2. *Further, e_k is contributed to s by DB on the left or center.*
3. *e_k is not contributed to s by A.*
4. *g_k is in A (thus e_k could be contributed).*

Note that although the set of syllables denoted by D may include syllables which are not nested in A, the first and fourth conditions combined imply that the letter will come from some syllable which is nested in A.

Lemma 7. *Let k be the highest index which satisfies the conditions in Lemma 6, and look at the earliest occurrence of e_k in DB. This letter e_k can indeed commute to the appropriate spot in A, where it can be considered to be contributed by A on the right.*

Proof. (*Lemma 6)* Proving that such a k exists, we have two cases to examine. First, recall that in the case $A' = [j+1\ i\ m]$, we know from Lemma 4 that e_i is skipped by A, but is contributed by B. It therefore satisfies conditions 1, 3, and 4 given above; we only need to show that it is not contributed by B on the right. Unless e_i is in the center of B, B also contains e_{i-1}. Nesting of B in A implies that A contains g_{i-1}, and it therefore contributes e_{i-1} since e_i is the lowest index it fails to contribute to s. There must be an e_i in between, which cannot come from A or D, so B must contribute its e_i on the left.

In the second case, with $A' = [j+1\ m+1]$, a nested obstruction must be of the form $B = [k_1\ m+1]$ (for some k_1). e_{m+1} is therefore the center letter, and satisfies conditions 1, 2, and 4. If it fails to satisfy condition 3, and thus is contributed to s by A, then s needs to have an e_m between the copies of e_{m+1} coming from A and B. Of A, D, and B, only A has a letter g_m which it could contribute, but we know that it does not. □

Proof. (*Lemma 7)*

As we try to commute this earliest e_k leftwards from DB, we can only be obstructed by the letters e_{k-1} or e_{k+1}. We can see that there are no opportunities for e_{k-1} to be in its path: other letters in B which occur earlier than our e_k's initial position, as well as other letters in A which occur later than its final position, have only higher indices; and earlier syllables of D will have either indices either strictly higher than k or strictly lower than $k-1$.

We may, however, be obstructed by letters e_{k+1} which occur in ADB. If there is an obstruction in DB, first notice that it cannot be on the right. The obstruction either comes from the same syllable as the e_k we are moving, in which case it is on the left in that syllable; or it comes from an earlier syllable of D, in which case it must be the center of that syllable (otherwise, that syllable would have its own e_k, but we have focused on the earliest one).

We now claim that in this situation, A must contribute e_{k+1}. Since k is the maximal index that satisfies the numbered conditions above, $k+1$ must have failed one of those conditions. It obviously satisfies condition 4, since e_k is contributed by a syllable which is nested in A. And we have already established that e_{k+1} is on the left or center in DB, thus it satisfies conditions 1 and 2. So $k+1$ must fail condition 3, thus be contributed by A.

However, there must then be an e_k between the copies of e_{k+1} coming from A and B. A does not contribute e_k, and the earliest copy in DB comes too far to the right. Therefore the only possible obstruction to our commuting of

e_k is an e_{k+1} on the right in A. We eliminate the obstruction by commuting that letter as well, as we did in the example above. A contributes no e_k, and so nothing obstructs the e_{k+1} on the right from commuting to the appropriate position on the left. □

It should be noted that this strategy is not usable for all subwords s; not only may it fail, but it is not even valid to consider commuting a letter into the contribution from A, unless its contribution to s is known to be missing a letter. We only use this strategy in the cases where the first strategy fails, since Lemma 5 guarantees us this condition.

References

[1] J. Birman, K. H. Ko, and S. J. Lee, *A new approach to the word and conjugacy problems in the braid groups.*, Adv. Math. **139** (1998), no. 2, 322–353.

[2] V. F. R. Jones, *Index for Subfactors,* Invent. Math. **72** (1983), no. 1, 1–25.

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

[4] R. P. Stanley, *Enumerative Combinatorics, Vol. 2,* Cambridge University Press, 1999.

[5] B. W. Westbury, *The representation theory of the Temperley-Lieb algebras,* Math. Zeit. **219** (1995), no. 4, 539-565.