

# Weyl Group of $B_n$ as Automorphisms of $n$ -Cube: Isomorphism and Conjugacy

David Chen

University of California, Los Angeles

## Abstract

The Weyl groups are important for Lie algebras. Lie algebras arise in the study of Lie groups, coming from symmetries of differential equations, and of differentiable manifolds. The Weyl groups have been used to classify Lie algebras up to isomorphism. The Weyl group associated to a Lie algebra of type  $B_n$  and the group of graph automorphisms of the  $n$ -cube  $Aut(Q_n)$  are known to be isomorphic to  $\mathbb{Z}_2^n \rtimes S_n$ . We provide a direct isomorphism between them via correspondence of generators. Geck and Pfeiffer have provided a parametrization of conjugacy classes and an algorithm to compute standard representatives. We believe we have a more transparent account of conjugacy in the Weyl group by looking at  $Aut(Q_n)$ . We give a complete description of conjugacy in the automorphism group. We also give an algorithm to recover a canonical minimal length (in the Weyl group sense) representative from each conjugacy class, and an algorithm to recover that same representative from any other in the same conjugacy class. Under the correspondence with the Weyl group, this representative coincides precisely with the minimal length representative given by Geck and Pfeiffer, leading to an easier derivation of their result.

## 1 Introduction

The Weyl groups are important for Lie algebras. A gentle undergraduate introduction to Lie algebras is given in [3]. Lie algebras arise in the study of Lie groups, coming from symmetries of differential equations, and of differentiable manifolds. The Weyl groups and their associated root systems have been used to classify Lie algebras up to isomorphism. That is, we associate a Weyl group to a Lie algebra and that group is the same as a reflection group we associate to a finite set of vectors in  $\mathbb{R}^n$ , called a root system. Most Lie algebras fall into the types  $A_n$ ,  $B_n$ ,  $C_n$ , or  $D_n$ , which arise from different root systems. We'll define everything in the next section.

The Weyl group  $W$  of the root system of  $B_n$  has already been determined to be the semidirect product of the finite group of sign changes on a basis of an  $n$ -

dimensional Euclidean space and the group of permutations on  $n$  letters  $S_n$ . (see details in [5]) The graph automorphisms of the  $n$ -cube  $Q_n$ ,  $Aut(Q_n)$  (or simply  $Aut$ ), have also been determined to be the semidirect product of transpositions and of the coordinate permutations. Each are isomorphic abstractly to  $\mathbb{Z}_2^n \rtimes S_n$ . We will provide a canonical isomorphism directly between the two, via generators.

Geck and Pfeiffer [4] provide an account of conjugacy in all Weyl groups of the classical types. In doing so, they develop a lot of machinery: cuspidal classes, Coxeter elements, signed and unsigned blocks, etc.. The upside is that it generalizes to types  $A_n$ ,  $B_n$ , and  $D_n$ , with each as a particular case. The downside is that it lacks transparency and exhibits a general difficulty in determining conjugacy of two elements. We believe we can provide an easier account of conjugacy in  $W$  of type  $B_n$  by seeing  $W$  as  $Aut$ . We can provide a complete description of conjugacy. In particular, we can computationally determine the conjugacy of two elements.

Geck and Pfeiffer also are able to parametrize the classes by certain pairs of partitions of  $n$ , and provide an algorithm using blocks to compute a complete system of canonical minimal length representatives. We recover the same parametrization, provide algorithms in  $Aut$  to recover the same minimal length representatives and to recover, given any automorphism, its standard minimal length representative. By length in the Weyl group, we mean the minimal number of occurrences of generators required to write a member of the Weyl group. Length in the Weyl sense is tricky when viewed in  $Aut$  as it is not mentioned in general for graph automorphism groups. We provide a definition for length in the graph automorphism group of the cube that is equivalent to length in the Weyl group.

## 1.1 One Application to $n$ -cube

One graph construction from a graph  $G$  and its automorphisms  $A$  is the quotient graph  $G/A$ . In [1], Brouwer details this construction and its use. The quotient is the set of  $G$ -orbits under  $A$  with adjacency when two orbits contain two adjacent vertices. We often look at quotient graphs under a group generated by a single automorphism. It is an exercise to show that two conjugate automorphisms induce isomorphic quotient graphs. In particular, if we look at the  $n$ -cube, we use our parametrization to compute representatives from each conjugacy class. We know their quotient graphs make up all possible quotient graphs.

## 2 Preliminaries

In this section we define the vocabulary used above. The details about reflection groups and Weyl groups can be found in [5].

Fix a real inner product space  $V$  with basis  $e_1, \dots, e_n$ .

**Definition 2.1.** A *reflection*  $s_\alpha$  associated to  $\alpha \in V$  is a linear map from  $V$  to itself sending  $\alpha$  to  $-\alpha$  and fixing everything orthogonal to  $\alpha$ .

**Definition 2.2.** A *root system*  $\Phi$  is a finite subset of  $V$  such that, if the line generated by  $\alpha$ ,  $\mathbb{R}\alpha$ , intersects  $\Phi$  nontrivially, the intersection is  $\{\alpha, -\alpha\}$ , and all the reflections associated to  $\alpha \in \Phi$  permute  $\Phi$ .

An example of a root system is  $(1, 1), (1, -1), (-1, -1), (-1, 1)$  in  $\mathbb{R}^2$ .

**Definition 2.3.** A *reflection group* associated to a root system  $\Phi$  is the group  $\langle s_\alpha \rangle_{\alpha \in \Phi}$  generated by reflections associated to  $\alpha \in \Phi$ .

**Definition 2.4.** The *simple roots*  $\Phi'$  of root system  $\Phi$  are a subset of  $\Phi$  that generates all of  $\Phi$ .

It is well known that every root system  $\Phi$  admits a subset of simple roots. It is also well known that  $\langle s_\alpha \rangle_{\alpha \in \Phi} = \langle s_\alpha \rangle_{\alpha \in \Phi'}$  (see [3] for both results). We thus only need to look at the simple roots.

**Definition 2.5.** Fix simple roots  $\Phi' = \{e_1, e_1 - e_2, \dots, e_{n-1} - e_n\}$ . The *Weyl group* of  $B_n$  is  $\langle s_\alpha \rangle_{\alpha \in \Phi'}$ . We denote it  $W$ .

**Definition 2.6.** Let  $w \in W$ . The *length* of  $w$  is the minimal number of occurrences of generators to write  $w$  as a product of generators.

The  $n$ -cube is the generalization of the line segment (1-cube), square (2-cube), and cube (3-cube) to higher dimensions. Formally, we have:

**Definition 2.7.** The  $n$ -cube, denoted  $Q_n$ , is a simple graph with vertices  $\mathbb{Z}_2^n$  and adjacency when exactly one component differs.

**Definition 2.8.** Let  $G$  be a graph, with  $\sim$  as the edge relation. Then  $\pi : G \rightarrow G$  is a *graph automorphism* if it is bijective and for all  $a, b$  in  $G$ ,  $a \sim b$  iff  $\pi(a) \sim \pi(b)$ .

We denote the group of graph automorphisms of the  $n$ -cube as  $Aut(Q_n)$ , or simply  $Aut$ . We look at two particular types of automorphisms on the  $n$ -cube: translations and coordinate permutations.

**Definition 2.9.** A *translation*  $t \in (\mathbb{Z}_2^n; +)$  acts on vertex  $v$  by  $tv = t + v$ . We write  $t = +a_1 \dots a_n$ , with  $a_i \in \mathbb{Z}_2$ .

**Definition 2.10.** A *permutation*  $\sigma \in S_n$  acts on vertex  $v = a_1 \dots a_n$  by  $\sigma v = a_{\sigma 1} \dots a_{\sigma n}$ .

It is well known that permutations can be written in cycles and are unique products (up to order) of disjoint cycles (see [2] for details). We will use this fact again and again.

**Definition 2.11.** Let  $H$  and  $K$  be finite groups. The set of ordered pairs  $H \times K$  together with the following multiplication is the *semidirect product* of  $H$  and  $K$ , denoted  $H \rtimes K$ . Let  $h_i \in H$ ,  $k_i \in K$ . Define  $(h_1, k_1)(h_2, k_2) = (h_1 k_1 h_2 k_1^{-1}, k_1 k_2)$ . We identify  $H$  with  $\{(h, 1) : h \in H\}$  and  $K$  with  $\{(1, k) : k \in K\}$ .  $H$  is normal in  $H \rtimes K$ , and  $H \cap K = 1$ .  $|H \rtimes K| = |H||K|$ .

Much more on semidirect product groups can be found in [2].

We are interested in a particular semidirect product group  $\mathbb{Z}_2^n \rtimes S_n$ . It is comprised of ordered pairs of a translation (under  $+$ ) and a permutation. Multiplication is defined as:  $(t', \pi')(t, \pi) = (t' + \pi' \cdot t, \pi' \pi)$ , with  $\pi' \cdot t$  as  $+a_{\pi'(1)} \dots a_{\pi'(n)}$  for  $t = +a_1 \dots a_n$ .  $(s, \sigma)^{-1} = (\sigma^{-1} \cdot s, \sigma^{-1})$ . For reference,  $(s, \sigma)(t, \pi)(s, \sigma)^{-1} = (s + \sigma \cdot t + \sigma \pi \sigma^{-1} \cdot s, \sigma \pi \sigma^{-1})$ .

### 3 A Canonical Isomorphism between $W$ and $Aut$

We'll start with determining the automorphism group of the  $n$ -cube. The details are provided in [6].

One can check that the coordinate permutations normalize the translations. We thus have:

**Proposition 3.1.** *The translations and coordinate permutations each form subgroups of  $Aut$ , and intersect trivially, with the translations making a normal subgroup. Together, the two subgroups induce  $\mathbb{Z}_2^n \rtimes S_n \subseteq Aut$ .*

*Proof.* To see that two subgroups  $H$  and  $K$  of group  $G$  induce a semidirect product  $H \rtimes K$ , it follows from the definition of semidirect product that it suffices to show  $H \cap K = 1$  and that for  $h \in H$ ,  $k \in K$ , we have  $khk^{-1} \in H$ . One can check that the translations and coordinate permutations form subgroups of  $Aut$ . Here,  $(\mathbb{Z}_2^n; +)$  is  $H$ , and  $S_n$  is  $K$ . Clearly  $\mathbb{Z}_2^n \cap S_n = 1$ . Take  $t = +a_1 \dots a_n \in \mathbb{Z}_2^n$  and  $\sigma \in S_n$ . We have  $\sigma t \sigma^{-1} = +a_{\sigma 1} \dots a_{\sigma n} \in \mathbb{Z}_2^n$ .  $\square$

*Remark.* To establish  $\mathbb{Z}_2^n \rtimes S_n \cong Aut$ , we need only show  $|Aut| \leq 2^n n!$ . We use a counting argument. Any automorphism will map a vertex to one of all  $2^n$  vertices. Then it must permute the neighbors, of which there are  $n!$  choices. Once the permutation of neighbors is chosen, all other points are determined because the  $n$ -cube is an  $(0, 2)$ -graph.

In fact, we do not need the above isomorphism. From now, we proceed only knowing that all transpositions and coordinate permutations are automorphisms.

For a real inner product space  $V$  with basis  $e_1, \dots, e_n$ ,  $W$  arises as the group generated by the reflections  $s_{\alpha_i}$  where  $\alpha_i$  is a simple root. Canonically,  $\alpha_1 = e_1 - e_2, \dots, \alpha_{n-1} = e_{n-1} - e_n, \alpha_n = e_1$ . The reflections corresponding to the simple roots generate  $W$ .

The goal of this section is to prove the following theorem given by a remarkable correspondence between the simple root  $e_i - e_{i+1}$  and the transposition  $(i \ i + 1)$ , and between  $e_1$  and the translation  $+10 \dots 0$ . In our particular root system, the roots have one of two Euclidean lengths. We note that translations correspond to reflections in short roots, while coordinate permutations correspond to those in long roots. So for example, we get other translations  $+000 \dots 1 \dots 000$  (1 in  $i$ th position) by reflection in  $e_i$ .

**Theorem 3.2.** *There is a one-to-one correspondence between the reflections induced by the simple roots and the automorphisms of the  $n$ -cube induced by*

these reflections. These automorphisms generate  $Aut$  and satisfy the relations of the Weyl group  $W$  of type  $B_n$ . This establishes the canonical isomorphism  $W \cong Aut$ .

The idea behind the proof is essentially to first embed the graph into the unit cube in  $V$ , translate it to the origin, apply a reflection given by a simple root, translate the image back to the unit cube, then recover a new graph from images of the embedded graph. This process induces an automorphism. From there we find that each reflection induces a unique automorphism, and each automorphism recovers a unique reflection. We then show that the images of the generators of  $W$  preserve the relations, thereby achieving our isomorphism.

- Lemma 3.3.**
1. *There is a map  $g$  embedding the vertices of an  $n$ -cube,  $\mathbb{Z}_2^n$ , into  $V$ . This map  $g$  is bijective to the set of vectors  $S \in V$  with coordinates 0 or 1.*
  2. *The translation  $t$  in  $V$  by  $-0.5(1e_1 + \dots + 1e_n)$  is injective.*
  3. *The reflection  $s_\alpha$  on  $V$  moving root  $\alpha$ , when restricted to  $t(S)$  is a permutation.*
  4. *The map  $\sigma_\alpha = g^{-1} \circ t^{-1} \circ s_\alpha \circ t \circ g$  on  $V$  is a well defined graph automorphism.*

*Proof.* Define the natural map  $g : \mathbb{Z}_2^n \rightarrow \mathbb{R}^n$  taking  $a_1 \dots a_n$  to  $a_1e_1 + \dots + a_ne_n$ , with  $a_i = 1$  or 0. The idea is to have, for example in  $\mathbb{R}^2$ , the graph's vertex 01 rest at  $0e_1 + 1e_2$ , 11 rest at  $1e_1 + 1e_2$ , etc., so the graph rests naturally inside  $\mathbb{R}^2$ . The translation  $t$  as above centers the graph. The image of  $S$  under  $t$ ,  $t(S)$ , is clearly a root system. As such,  $s_\alpha$  restricted to  $t(S)$  is a permutation. Applying the reflection should fix the embedded graph, as we are reflecting roots. Undoing  $t$  translates the vectors of  $t(S)$  back to  $S$ , so we apply  $g^{-1}$  to  $S$  to recover a graph, with incidence when two vertices differ by exactly one entry.

The map  $\sigma_\alpha = g^{-1} \circ t^{-1} \circ s_\alpha \circ t \circ g$  on  $V$  is a well defined graph permutation, as each map in the composition is bijective.

The map  $\sigma_\alpha$  preserves the edge relation because  $s_\alpha$  permutes and preserves orthogonality, in particular, relative distance in  $V$  by exactly 1. Using  $g$  and  $g^{-1}$  will preserve the difference in exactly one entry between two vertices.  $\square$

**Example.** Take  $V = \mathbb{R}^2$  and consider the 2-cube with vertices 00, 10, 01, 11. The map  $g$  puts 00 at  $0e_1 + 0e_2$ , 10 at  $1e_1 + 0e_2$ , 01 at  $0e_1 + 1e_2$ , and 11 at  $1e_1 + 1e_2$ . If we apply the reflection now, we wouldn't stay in  $S = \{\text{vectors with coordinates 0 or 1}\}$ . We translate via  $t$  our four vectors about the origin and apply the reflection. The idea is to make  $S$  into a root system and closed under reflection.

Let's apply the flip across the x-axis  $s_{e_2}$ . A quick check tells us the image of  $e_2$  under  $s_{e_2}$  is  $t(S)$ . Undoing  $t$ , we see  $0e_1 + 0e_2$  is sent to  $0e_1 + 1e_2$ ,  $1e_1 + 0e_2$  is sent to  $1e_1 + 1e_2$ ,  $0e_1 + 1e_2$  is sent to  $0e_1 + 0e_2$ , and  $1e_1 + 1e_2$  is sent to  $1e_1 + 0e_2$ . Applying  $g^{-1}$  to each image and establishing adjacency in the usual way recovers the 2-cube. Thus our  $\sigma_{e_2}$  is an automorphism.

**Proposition 3.4.** *There is a one-to-one correspondence between simple root  $e_i - e_{i+1}$  and the automorphism given by the coordinate permutation  $(i \ i + 1)$ , and the simple root  $e_1$  and the automorphism given by translation by  $+10 \dots 0$ , via  $s_\alpha \leftrightarrow \sigma_\alpha$ .*

*Proof.* Reflections in  $V$  are of the form  $s_a(v) = v - 2(v, a)/(a, a)a$ ,  $a \in V$ . A routine check of  $s_\alpha \circ t(a_1 \dots a_n)$ , where  $\alpha$  is a simple root and  $a_1 \dots a_n \in \mathbb{Z}_2^n$ , will demonstrate  $s_\alpha$  induces the desired  $\sigma_\alpha$ . Going backwards from  $\sigma_\alpha$ , we must have  $s_\alpha$  because each map is bijective by the Lemma and reflections are unique up to scalars.  $\square$

The Weyl group  $W$  of type  $B_n$  and indeed all finite Weyl groups have been determined (see [5]).  $W$  is  $\langle s_{\alpha_1}, \dots, s_{\alpha_n} \rangle$  satisfying:

1.  $\alpha_i$  simple
2.  $s_{\alpha_i}^2 = 1$
3.  $s_{\alpha_i} s_{\alpha_{i+1}} s_{\alpha_i} = s_{\alpha_{i+1}} s_{\alpha_i} s_{\alpha_{i+1}}$  for  $i + 1 < n$
4.  $s_{\alpha_1} s_{\alpha_n} s_{\alpha_1} s_{\alpha_n} = s_{\alpha_n} s_{\alpha_1} s_{\alpha_n} s_{\alpha_1}$
5.  $s_{\alpha_i} s_{\alpha_j} = s_{\alpha_j} s_{\alpha_i}$  for  $|i - j| > 1$ .

**Proposition 3.5.** *The images of  $s_{\alpha_i}$  under the correspondence in the previous proposition satisfy the same relations as above.*

*Proof.* The images are transpositions  $(i \ i + 1)$  following the usual rules. The only thing tricky is the relation with  $+10 \dots 0$ . Keeping in mind the semidirect product multiplication, one can check the relation holds.  $\square$

## 4 Conjugacy in $Aut$

### 4.1 Conjugacy Classes of $Aut$

We have a simple description of the conjugacy classes of the Weyl group of  $B_n$  which can be seen by looking at  $Aut$  as ordered pairs of translations normalized by permutations, following the usual rules of semidirect product multiplication. The conjugacy classes behave in a nice way, and deciding conjugacy is simple. We prove necessary and sufficient conditions for deciding conjugacy.

$Aut \cong \mathbb{Z}_2^n \rtimes S_n$  is comprised of ordered pairs of a translation (under  $+$ ) and a permutation. Multiplication works as in semidirect products:  $(t', \pi')(t, \pi) = (t' + \pi' \cdot t, \pi' \pi)$ , with  $\pi' \cdot t$  as  $+a_{\pi'(1)} \dots a_{\pi'(n)}$  for  $t = +a_1 \dots a_n$ . We also have  $(s, \sigma)^{-1} = (\sigma^{-1} \cdot s, \sigma^{-1})$ . For reference,  $(s, \sigma)(t, \pi)(s, \sigma)^{-1} = (s + \sigma \cdot t + \sigma \pi \sigma^{-1} \cdot s, \sigma \pi \sigma^{-1})$ . Clearly if  $(t', \pi') \sim (t, \pi)$  (conjugacy) then  $\pi' \sim \pi$ .

We need to first introduce some definitions and notation. Let  $(t, \pi) \in Aut$ . Let  $\pi = \prod_{i=1}^p c_i$ , a product of disjoint nontrivial cycles, with the shorter length cycles indexed lower. Explicitly,  $c_i = (k_{i,1} \dots k_{i,n_i})$ , where  $n_i$  is the length of  $c_i$  and  $n_i > 1$ . A standard result tells us the product is unique up to order and

cyclically permuting the terms inside each cycle (see [2]). For example, we have  $\pi = (1\ 3)(4\ 7\ 8) = (8\ 4\ 7)(3\ 1)$ .

**Definition 4.1.** The *cycle structure* of  $\pi$  is the sequence  $(n_1, \dots, n_p)$ .

For example, if  $\pi = (1\ 2)(4\ 3\ 7)$ , the cycle structure of  $\pi$  is  $(2, 3)$ .

**Definition 4.2.** Consider the *moved positions* of  $t$  under a cycle  $c_i$  those indices in the cycle (as  $t \in \mathbb{Z}_2^n$ ).

**Definition 4.3.** Consider the *fixed positions* of  $t$  those indices moved by no cycle.

We finish the section by proving the following theorem.

**Theorem 4.4.** Let  $(t', \pi'), (t, \pi) \in \text{Aut}$ . Denote  $m_{t_i}$  the number of 1's among the moved positions of  $t$  under cycle  $c_i$ , and  $f_t$  the number of 1's among the fixed positions. Then  $(t', \pi') \sim (t, \pi)$  (conjugacy) iff

1.  $\pi \sim \pi'$
2.  $m_{t'_i} \equiv m_{t_i} \pmod{2}$ , all  $i$ , though the indices of cycles of the same length may be permuted.
3.  $f_{t'} = f_t$

Denote these conditions by  $\mathbb{D}$ .

By the second condition in the theorem above, we mean that for example,  $m_{t_1} \equiv m_{t'_2}$  and  $m_{t'_1} \equiv m_{t_2}$ , with  $\pi = c_1 c_2 = (1\ 2)(3\ 4)$  and  $\pi' = c'_1 c'_2 = (1\ 2)(3\ 4)$ . That is,  $m_{t_1}$  and  $m_{t'_1}$  don't exactly match up, but there is exactly one other cycle that matches it in parity, and for  $c_2$ , there is also exactly one cycle matching it in parity.

We use the following commonly known lemma and theorem (see details in [2]):

**Lemma 4.5.** If permutation  $\rho = \prod c_i$ , where  $c_i = (k_{i,1} \dots k_{i,n_i})$ , then we have  $\sigma \rho \sigma^{-1} = \prod (\sigma k_{i,1} \dots \sigma k_{i,n_i})$ .

*Proof.* To see this, we consider permutations  $\sigma, \tau = (a_1 \dots a_n)$ . We can show that  $\sigma \tau \sigma^{-1} = (\sigma a_1 \dots \sigma a_n)$ . To achieve the lemma, we simply extend the result for all permutations by inserting  $\sigma^{-1} \sigma$  between all the  $c_i$  and  $c_{i+1}$ .  $\square$

**Theorem 4.6.** Two permutations are conjugate iff they have the same cycle structure.

That is, consider  $\rho = \prod_{i=1}^r c_i$  and  $\pi = \prod_{i=1}^p d_i$ , where  $c_i = (k_{i,1} \dots k_{i,n_i})$ , and  $d_i = (l_{i,1} \dots l_{i,m_i})$ , and  $m_i, n_i > 1$ . Then  $\rho \sim \pi$  iff  $r = p$  and  $(n_1, \dots, n_r) = (m_1, \dots, m_p)$ .

One can easily prove the following lemma:

**Lemma 4.7.** *Any permutation with a given cycle structure is conjugate to the permutation with  $1, 2, \dots$  running through the cycle structure. For example  $(a_1 a_2)(a_3 a_4 a_5) \sim (1 2)(3 4 5)$ , and so  $(t, (a_1 a_2)(a_3 a_4 a_5)) \sim (t, (1 2)(3 4 5))$ .*

**Proposition 4.8.**  *$(t', \pi') \sim (t, \pi)$  via  $(s, \sigma)$  satisfy  $\mathbb{D}$ .*

*Proof.* Reduce to the case of  $\pi = \pi'$ , with  $1, \dots, k$  running through the cycle structure of  $\pi$ . By assumption,  $t' = s + \sigma \cdot t + \sigma \pi \sigma^{-1} \cdot s$ . Because  $\pi = \pi' = \sigma \pi \sigma^{-1}$ ,  $\sigma$  permutes the first  $k$  positions, and  $\sigma \pi \sigma^{-1}$  by construction permutes the first  $k$  positions and fixes those after  $k$ .  $\sigma$  permutes cyclically within each cycle, and so  $\sigma \pi \sigma^{-1}$  as well, so the stronger  $m_{t'_i} = m_{t_i} + 2l_i \equiv m_{t_i} \pmod{2}$  for the number of 1's  $l_i$  under a cycle, each  $i$ th cycle. Note that when there are two  $k$ -cycles, their indices may be permuted for matching up the  $m_{t_i}$ 's, as on a pair of  $k$ -cycles,  $\sigma$  may permute not only cyclically within a cycle but also permute the  $k$ -cycles themselves (see the remark under the above theorem). After  $k$ ,  $\sigma \pi \sigma^{-1} \cdot s$  and  $s$  coincide. Adding them gives 0 after  $k$ , and we satisfy  $\mathbb{D}$ . □

**Proposition 4.9.**  *$(t', \pi')$  and  $(t, \pi)$  satisfying  $\mathbb{D}$  are conjugate.*

*Proof.* We prove it for base case of  $\pi$  as a  $k$ -cycle, then proceed by induction by assuming it holds for all  $k$ -cycles and prove it for a product of  $k$ -cycles.

Reduce to the case of  $\pi = \pi' = (1 2 \dots k)$ . We want  $t' = s + \sigma \cdot t + \sigma \pi \sigma^{-1} \cdot s$  with appropriate choice of  $(s, \sigma)$ . First set  $\sigma = 1$  on moved positions and have it change  $t$  to  $t'$  on fixed positions. We can impose the latter requirement because  $f_t = f_{t'}$ . By construction, we reduce the task to proving  $t' = s + \sigma \cdot t + \pi \cdot s$ .

Looking at the fixed positions, we see  $t' = \sigma \cdot t$ . By construction,  $s = \pi \cdot s$ . Thus  $t' = s + t' + s = s + \sigma \cdot t + \pi \cdot s$ , for any choice of  $s$ .

Looking at moved positions, we see  $\sigma \cdot t = t$ . We'll pick  $s$  satisfying  $t' + t = s + \pi \cdot s$ . Let  $s = a_1 \dots a_k$ .  $\pi \cdot s = a_k a_1 \dots a_{k-1}$ . For notational simplicity, let  $t + t' = 1 \dots 10 \dots 0$ , with an even number  $e$  of 1's by hypothesis. Then  $a_1 \dots a_k$  satisfy:  $a_1 + a_k = 1, a_2 + a_1 = 1, \dots, a_e + a_{e-1} = 1, a_{e+1} + a_e = 0, \dots, a_k + a_{k-1} = 0$ . Setting  $a_1 = 0$ , we have  $a_i = 1$  for  $i$  even,  $a_i = 0$  if odd,  $i \leq e$ , and  $a_j = 1$  for  $e \leq j \leq k$ . This  $s$  works.

Induction Step: we lift the  $s$ 's found in the previous proposition for each  $k$ -cycle to a solution for  $\pi$ . Again let  $\sigma = 1$  on moved positions and let it morph  $t$  to  $t'$  on fixed positions. For  $s$ , we concatenate the fragments of  $s$ 's corresponding to each cycle, as they were only computed for their own moved positions and could behave regardless of what's chosen in fixed positions. That is,  $s = s_1 \dots s_p \dots$  for  $\pi = \prod c_i$ ,  $p$  cycles, and  $s_i$  is the part of  $s$  computed for  $c_i$  as above stripped of its fixed positions and adjusted for reindexing. Anything after  $s_p$  in  $s$  is whatever is desired. □

**Example.** Take  $(1111001, (1 2)(3 4 5)) = (t', \pi)$  and  $(0001110, (1 2)(3 4 5)) = (t, \pi)$  in  $\text{Aut}(7)$ . We'll find  $(s, \sigma)$  establishing conjugacy. Note  $m_{t'_{(1 2)}} \equiv m_{t_{(1 2)}} \pmod{2}$  and  $m_{t'_{(3 4 5)}} \equiv m_{t_{(3 4 5)}} \pmod{2}$ . Note  $f_{t'} = f_t$ . As in the proof above,

we reduce the task to proving  $t' = s + \sigma \cdot t + \pi \cdot s$ , as  $\pi$  and  $\sigma$  are chosen to be disjoint.

We first look at  $(11\dots, (1\ 2))$  and  $(00\dots, (1\ 2))$ . We can ignore the fixed positions even when they don't have exact same number of 1's. On moved positions 1, 2, set  $\sigma = 1$ , so  $\sigma \cdot 00\dots = 00\dots$ . We want  $s_{(1\ 2)}$  so that  $11\dots + 00\dots = s_{(1\ 2)} + (1\ 2) \cdot s$ . For  $s_{(1\ 2)} = a_1a_2\dots$ ,  $(1\ 2) \cdot s_{(1\ 2)} = a_2a_1\dots$ . Set  $11 = a_1a_2 + a_2a_1$  and set  $a_1 = 0$ , so  $a_2 = 1$ . Thus our  $s_{(1\ 2)} = 01\dots$

Now look at  $(\dots 110\dots, (3\ 4\ 5))$  and  $(\dots 011\dots, (3\ 4\ 5))$ . Ignore the fixed positions again. On moved positions 3, 4, 5 set  $\sigma = 1$ , so  $\sigma \cdot \dots 011\dots = \dots 011\dots$ . We want  $s_{(3\ 4\ 5)}$  so that  $\dots 110\dots + \dots 011\dots = s_{(3\ 4\ 5)} + (3\ 4\ 5) \cdot s_{(3\ 4\ 5)}$ . For  $s_{(3\ 4\ 5)} = \dots a_3a_4a_5\dots$ ,  $(3\ 4\ 5) \cdot s_{(3\ 4\ 5)} = \dots a_5a_3a_4\dots$ . Set  $101 = a_3a_4a_5 + a_5a_3a_4$  and set  $a_3 = 0$ , so  $a_4 = 0$  and  $a_5 = 1$ . Thus our  $s_{(3\ 4\ 5)} = \dots 001\dots$

Now lift the  $s_{(1\ 2)}$  and  $s_{(3\ 4\ 5)}$  to  $s = s_{(1\ 2)}s_{(3\ 4\ 5)}00 = 0100100$ . Set  $\sigma = (6\ 7)$ . Then  $t' = s + \sigma \cdot t + \pi \cdot s = 0100100 + 0001101 + 1010000$ . We establish conjugacy.

## 4.2 Parametrization of Conjugacy Classes and Algorithm for Minimal Length Representative for Each

We give algorithms to compute conjugacy class representatives from elements of a class, and from a parametrization, with the latter's conditions given by Geck and Pfeiffer. We define 3 different notions of a representative using the same name, but we also prove they all coincide.

We first note that a permutation may be written as a unique product of nontrivial cycles, and that trivial cycles may be inserted anywhere in the product, changing neither the cycle structure nor the permutation. For example  $(1\ 2)(5\ 8\ 6) = (3)(1\ 2)(9)(5\ 8\ 6)$ . We will need to consider the trivial cycles in this section.

### 4.2.1 Representatives and Algorithms

**Definition 4.10.** For  $(t, \pi)$  when  $\pi$  has  $1, \dots, n$  running through its cycle structure, the *block* of  $t$  moved by the cycle  $c_i$  is the subtuple of  $t$  with indices the same as in  $c_i$ .

For example, let  $t = +1001$  and  $\pi = (1\ 2)(3\ 4)$ . The block of  $t$  moved by cycle  $(1\ 2)$  is 10.

**Definition 4.11.** For  $(t, \pi)$ , the  $(r, \rho)$  computed by the algorithm below is called the *L-representative* (*Lrep*) computed from  $(t, \pi)$ .

We call it an *L-representative* because it will be shown to have minimal length.

**Algorithm 4.12.** Compute  $f_t, m_{t_i}$ . Initially form  $\rho$  to consist of, from left to right,  $f_t$  trivial cycles, then the cycle structure of  $\pi$ , with  $1, \dots, n$  running through. Initially form  $r$ , put a 1 on each fixed position, then for cycles  $c_i$  where

$m_{t_i} \equiv 0$ , put 0's on the positions it moves, for cycles where  $\equiv 1$ , put 1 on the least moved position and 0's on all other moved positions. Permute the blocks of  $r$  moved by the cycles so that the those of  $\equiv 1$  are to the left, with shorter cycles more left. This is  $r$ . Then permute the cycles of  $\rho$  to reflect  $r$ ; Order the cycles where  $\equiv 0$  so the longer cycles are more left. Lastly have  $1, \dots, n$  running through again. This is  $\rho$ .

By all the work above, the *Lrep* computed from  $(t, \pi)$  is conjugate to  $(t, \pi)$ . Because conjugate automorphisms meet all the conditions  $\mathbb{D}$ , an inspection of the algorithm will show that the construction only depended on the cycle structure and the numbers in  $\mathbb{D}$ , which are the same to the algorithm. Also notice if even one number changes, or the cycle structures differ, we get a different automorphism. We thus have:

**Lemma 4.13.** *Automorphisms are conjugate iff they compute the same  $L$  – representative.*

With this uniqueness, we can associate an *Lrep* to a conjugacy class.

**Definition 4.14.** Given a conjugacy class  $C$  of *Aut*, let the *L – representative* of  $C$ ,  $w_C$ , be the *L – representative* of any element in  $C$ .

Clearly then, we have:

**Proposition 4.15.** *The set of  $L$  – representatives from all conjugacy classes form a complete system of representatives of the conjugacy classes.*

**Example.** Care needs to be taken when computing an *Lrep*. Consider  $t = 10100111, \pi = (1\ 2)(6\ 7)(3\ 4\ 5)$ .  $f = 1, m_{(1\ 2)} = 1, m_{(6\ 7)} = 2, m_{(3\ 4\ 5)} = 1$ . Applying the algorithm, we have  $\rho = (1)(2\ 3)(4\ 5)(6\ 7\ 8)$  and one would guess  $r = 11000100$ . That is not exactly right: we need to have  $r$  reflect the cycle structure  $(1)(2\ 3)(6\ 7\ 8)(4\ 5)$ , so that all the chunks of 1's and 0's corresponding to cycles with a 1 are to the left. We can do this because cycle structure is unique only in counting the number of  $k$ -cycles. Then the real  $r = 11010000$ .

**Definition 4.16.** Consider a pair of partial partitions of  $n$ ,  $(\alpha, \beta)$  with  $\alpha + \beta = n$ . The *L – representative* computed from  $(\alpha, \beta)$ , denoted  $w_{(\alpha, \beta)}$  is the automorphism computed using the following algorithm:.

**Algorithm 4.17.** Let  $\beta = n_1 + \dots + n_k$  and  $\alpha = n_{k+1} + \dots + n_m$ . For  $1 \leq i \leq k$ , set  $r_i = 10 \dots 0, n_i - 1$  0's. For  $k + 1 \leq i \leq m$ , set  $r_i = 0 \dots 0, n_i$  0's. Then set  $r = r_1 \dots r_m$ . Set  $c_i$  as an  $n_i$ -cycle. Set  $\rho = \prod c_i$  with  $1 \dots n$  running through the cycle structure including the trivial cycles.  $w_{(\alpha, \beta)} = (r, \rho)$ .

*Remark.* The algorithm to compute the *Lrep* from  $(\alpha, \beta)$  computes the same representative, under isomorphism, computed by the algorithm given by Geck and Pfeiffer that takes as argument  $(\alpha, \beta)$ . Indeed, we chose notation  $w_{(\alpha, \beta)}$  to coincide with theirs.

**Example.** We'll compute an *Lrep* from  $\alpha = 2 + 1$ ,  $\beta = 1 + 3$ .  $r_1 = 1$ ,  $r_2 = 100$ ,  $r_3 = 00$ ,  $r_4 = 0$ , so  $r = 1100000$ .  $c_1 = 1$ ,  $c_2 = (1\ 2\ 3)$ ,  $c_3 = (1\ 2)$ ,  $c_4 = 1$ , so  $\rho = (2\ 3\ 4)(5\ 6)$ .

It's easy to see that with  $\alpha$  decreasing and  $\beta$  increasing,  $w_{(\alpha,\beta)}$  is trivially reduced to the *Lrep* computed from it. Thus:

**Lemma 4.18.** *The  $L$ -representative computed from  $(\alpha, \beta)$  with  $\alpha$  decreasing and  $\beta$  increasing, in conjugacy class  $C$ , is exactly the  $L$ -representative of the same conjugacy class.*

#### 4.2.2 Parametrization and Proof

With the definitions in place (except length: see next section), we present the main theorem of the section:

**Theorem 4.19.** *(Geck and Pfeiffer) There is a one-to-one correspondence between the pairs of partitions of  $n$ ,  $(\alpha, \beta)$ , with  $\alpha$  decreasing and  $\beta$  increasing,  $\alpha + \beta = n$ , and the conjugacy classes of *Aut*. Furthermore, there is a way to compute a canonical representative of minimal length from these  $(\alpha, \beta)$ , and all of them are representatives from all conjugacy class of *Aut*. Namely, the *Lrep* from  $(\alpha, \beta)$  is that canonical representative.*

To prove the correspondence exists, we prove the following:

**Proposition 4.20.** *The  $L$ -representatives computed from pairs of partial partitions of  $n$ ,  $(\alpha, \beta)$ ,  $\alpha$  decreasing,  $\beta$  increasing,  $\alpha + \beta = n$ , are representatives from all conjugacy class of *Aut*, with each pair picking out a distinct conjugacy class.*

**Lemma 4.21.** *Let  $(\alpha, \beta)$  and  $(\alpha', \beta')$  be distinct pairs of partial partitions of  $n$ , with  $\alpha + \beta = \alpha' + \beta' = n$ , with  $\alpha$  and  $\alpha'$  decreasing,  $\beta$  and  $\beta'$  increasing. Then the *Lrep*'s they compute are not conjugate.*

*Proof.* Let  $\alpha = \sum_{i=1}^e n_i$ ,  $\beta = \sum_{i=e+1}^m n_i$ , and without loss let  $\alpha' = n_1 + 1 + \sum_{i=2}^e n_i$ ,  $\beta' = n_{e+1} - 1 + \sum_{i=e+2}^m n_i$ . We have  $\rho_{\alpha\beta} = \prod_{i=1}^m c_i$  and  $\rho_{\alpha'\beta'} = \prod_{i=1}^m c'_i$ , with  $c_i$  an  $n_i$ -cycle, even a 1-cycle. For simplicity, suppose we have conjugacy and that  $c_i$  corresponds to  $c'_i$ , in terms of number of 1's. Imposing the restriction of the same cycle structure, we have that  $c'_{n_1+1}$  corresponds to  $c_{n_{e+1}}$  and  $c_{n_1}$  corresponds to  $c'_{n_{e+1}-1}$ , as  $c_{n_1}$  cannot correspond to  $c'_{n_1+1}$  as their lengths differ. We can't however impose this correspondence as each in each pair has different numbers of 1's. Thus we can't have conjugacy.  $\square$

With the previous lemma, we provide injectivity:

**Proposition 4.22.** *Distinct pairs of partitions of  $n$ ,  $(\alpha, \beta)$ , with  $\alpha$  decreasing and  $\beta$  increasing,  $\alpha + \beta = n$ , correspond to distinct conjugacy classes of *Aut* by computing  $L$ -representatives of distinct conjugacy classes.*

Now for surjectivity. We start by noting that when we lift the restriction of  $\alpha$  decreasing,  $\beta$  increasing, we get repeats, as we state in the following lemma.

**Lemma 4.23.** *The  $L$ -representative computed from  $(\alpha, \beta)$  with  $\alpha$  increasing or  $\beta$  decreasing is conjugate to some  $L$ -representative computed from  $(\alpha, \beta)$  with  $\alpha$  decreasing and  $\beta$  increasing.*

*Proof.* If  $\beta$  is not increasing, start the reduction by permuting the blocks with 1's until the shortest are more to the left. If  $\beta$  is increasing and  $\alpha$  is not decreasing, start by changing the cycle structure to have the cycles where  $\equiv 0$  of greater length are more to the left after the cycles  $\equiv 1$ . In either case we have nontrivial reductions to  $L$ reps of the class.  $\square$

Every conjugacy class gets hit by the  $(\alpha, \beta)$  parametrization.

**Proposition 4.24.** *Let  $C$  be any conjugacy class. From the  $L$ rep of  $C$ ,  $w_C$ , we recover a pair of partial partitions  $(\alpha, \beta)$ ,  $\alpha$  decreasing,  $\beta$  increasing,  $\alpha + \beta = n$ , so that  $w_C = w_{(\alpha, \beta)}$ .*

*Proof.* Compute  $w_C = (r, \rho = \prod_{i=1}^m c_i)$ , including trivial cycles. The product can be naturally split between the last  $i$  with  $c_i$  has  $m_i \equiv 1$ , and the first  $i$  where  $m_i \equiv 0$ . Denote the first  $i$  where  $m_i \equiv 0$  with  $i = 1$ : it goes along for  $e$  cycles. Then  $\rho = \prod_{i=e+1}^m c_i \prod_{i=1}^e c_i$ . Letting  $n_i$  be the length of  $c_i$ , we see  $n = \sum_{i=1}^e n_i + \sum_{i=e+1}^m n_i = \alpha + \beta$ . By construction of  $w_C$ ,  $\alpha$  is decreasing and  $\beta$  is increasing. A review of the algorithm for computing  $w_{(\alpha, \beta)}$  tells us  $w_C = w_{(\alpha, \beta)}$ .  $\square$

We thus establish the surjectivity and the correspondence. That leaves minimal length.

### 4.2.3 Length in $Aut$ and Proof of Minimal Length

We'll define a length in  $Aut$  to be compatible to that in the Weyl group, where it is the least number of simple reflections needed to write an element. We'll define length individually on  $\mathbb{Z}_2^n$  and  $S_n$ , then let length in  $Aut$  be their sum.

**Definition 4.25.** For  $0 \dots 010 \dots 0 \in \mathbb{Z}_2^n$ , with 1 in the  $i$ th place, let the *length*  $l$  be  $2i - 1$ . Extend by additivity.

**Definition 4.26.** For  $\sigma \in S_n$ , let the *length*  $l$  be the least number of  $(i \ i + 1)$  needed to write  $\sigma$ .

**Definition 4.27.** For  $(t, \sigma) \in Aut$ , let the *length*  $l = l(t) + l(\sigma)$ . This definition makes sense because of the Weyl group relations under isomorphism.

The above notion of length in  $Aut$  seems defined arbitrarily, but one can check it is exactly length in the Weyl group under isomorphism. Length in  $\mathbb{Z}_2^n$  is obtained by examining the conjugation action on  $10 \dots 0$ .

**Proposition 4.28.** *In conjugacy class  $C$  of  $Aut$ ,  $w_C$  has minimal length in  $C$ .*

*Proof.* Let  $w_C = (r, \rho)$ . The length  $l(r)$  is minimal because we pushed all the 1's as left as possible while preserving the number of 1's and 1's mod 2 among cycles, with minimal 1's. Then let's prove that  $l(\rho)$  is minimal among all  $(t, \sigma) \in C$  with  $l(t) = l(r)$ . But even this easily follows by construction. The cycle structure of  $\rho$  has  $1 \dots n$  running through it. This guarantees that each  $k$ -cycle has minimal length among all  $k$ -cycles. Any conjugate to  $\rho$  with strictly lower length would need to have the same cycle structure and not have  $1 \dots n$  running through each cycle, which isn't possible.  $\square$

We thus establish that the representative computed from our parametrization is of minimal length. We thus recover the entire picture, up to isomorphism, of conjugacy of the Weyl group of type  $B_n$  given by Geck and Pfeiffer. We also provide a quick check to see if any two elements are conjugate.

## Acknowledgements

I completed the work for this paper at the Summer 2009 Math Research Experience for Undergraduates at the University of Georgia under Professor Leonard Chastkofsky. I'd like to thank Professor Chastkofsky for all the guidance he gave during and after the program. He helped me start the paper and has continued to help me until publication. I'd also like to thank the University of Georgia for hosting the REU, and to the staff and faculty who made it run smoothly. A special thank you to the referees from the Rose-Hulman Undergraduate Math Journal for their reviews and suggestions. I greatly appreciate their comments on improving the paper.

## References

- [1] Andries E. Brouwer. Classification of small (0,2)-graphs. *J. Combinatorial Theory*, 2006.
- [2] David Steven Dummit and Richard M. Foote. *Abstract Algebra*. Wiley, 3rd edition, 2004.
- [3] Karin Erdmann and Mark J. Wildon. *Introduction to Lie Algebras*. Birkhauser, 2006.
- [4] Meinolf Geck and Gotz Pfeiffer. *Characters of finite Coxeter groups and Iwahori-Hecke algebras*. Oxford University Press, 2000.
- [5] James E. Humphreys. *Reflection Groups and Coxeter Groups*. Cambridge University Press, 1992.
- [6] Jennifer Muskovin. On (0,2)-graphs and semiplanes. Master's thesis, University of Georgia, 2009.