4-20-2017

Word Length Perturbations in Certain Symmetric Presentations of Dihedral Groups

Michael P. Allocca
Muhlenberg College

Jason M. Graham
The University of Scranton

Candice R. Price
University of San Diego, cprice@smith.edu

Shannon N. Talbott
Moravian College

Jennifer F. Vasquez
The University of Scranton

Recommended Citation

Word Length Perturbations in Certain Symmetric Presentations of Dihedral Groups

Michael P. Allocca[a], Jason M. Graham[b], Candice R. Price[c], Shannon N. Talbott[d], Jennifer F. Vasquez[b]

[a]*Department of Mathematics and Computer Science, Muhlenberg College, Allentown, PA, USA*
[b]*Department of Mathematics, University of Scranton, Scranton, PA, USA*
[c]*Department of Mathematics, University of San Diego, San Diego, CA, USA*
[d]*Department of Mathematics and Computer Science, Moravian College, Bethlehem, PA, USA*

Abstract

Given a finite group with a generating subset there is a well-established notion of length for a group element given in terms of its minimal length expression as a product of elements from the generating set. Recently, certain quantities called λ_1 and λ_2 have been defined that allow for a precise measure of how stable a group is under certain types of small perturbations in the generating expressions for the elements of the group. These quantities provide a means to measure differences among all possible paths in a Cayley graph for a group, establish a group theoretic analog for the notion of stability in nonlinear dynamical systems, and play an important role in the application of groups to computational genomics. In this paper, we further expose the fundamental properties of λ_1 and λ_2 by establishing their bounds when the underlying group is a dihedral group. An essential step in our approach is to completely characterize so-called symmetric presentations of the dihedral groups, providing insight into the manner in which λ_1 and λ_2 interact with finite group presentations. This is of interest independent of the study of the quantities λ_1, λ_2. Finally, we discuss several conjectures and open questions for future consideration.

Keywords: Dihedral groups, Group presentations, Word length, Generating set, Minimal length

1. Introduction and Background

For a finite group, G, with generating set, S, there is a notion of length for any element $g \in G$: write g as a product of elements (*i.e.*, as a word) from S, using as few generators as possible. Then the length of g is the number of generators appearing in a minimal expression (*i.e.*, smallest word expression) for g. Furthermore, this notion of length provides a related notion of distance, or metric between two elements g, g' of G. From a geometric perspective, this is related to distances along paths of the Cayley graph for G associated with the generating set S.

Let G be a finite group with symmetric generating set $S = \{s_1, s_2, \ldots, s_n\}$, where symmetric means $1 \notin S$ and $s \in S \Rightarrow s^{-1} \in S$. One reason to consider symmetric generating sets is to ensure that a group element and its inverse have the same length. A word from S in G is any expression formed by taking products of elements in S. We refer to the elements of S as letters. Then, for any element $g \in G$, we define the length $l_S(g) \in [0, \infty)$ of g with respect to S to be the minimal number of letters in S for which g can be written as a word from S. Note that $l_S(g) = 0 \Leftrightarrow g = 1$. Recently, the following quantities have been defined [1]:

$$\lambda_1(G, S) := \max_{g \in G, \; s \in S} \{l_S(gsg^{-1})\}, \tag{1}$$

$$\lambda_2(G, S) := \max_{g \in G, \; s, s' \in S} \{l_S(gss'g^{-1})\}. \tag{2}$$

The quantities λ_1, λ_2 serve to precisely address the questions: given a word, what is the effect on its length after either the deletion of one letter (quantified by λ_1), or the replacement of one letter by another distinct letter (quantified by λ_2)? This presents an analogy between how large these measures can be, and the sensitivity of nonlinear dynamical systems to small perturbations in initial conditions, *i.e.*, the so-called "butterfly effect" [1].

There are several initial observations about λ_1 and λ_2 to note. First, there is the bound

$$\lambda_2(G, S) \leq 2\lambda_1(G, S), \tag{3}$$

which holds for any group G and symmetric generating set S, see [1]. Second, the values for λ_1 and λ_2 in two extreme cases, either when G is commutative, or when S is as large as possible can easily be derived:

Suppose that G is a nontrivial commutative group and S is any symmetric generating set. Then, $\lambda_1(G, S) = 1$ and $\lambda_2(G, S) \leq 2$. This follows because $sg = gs$ for any $g \in G$, $s \in S$ thus giving

$$l_S(gsg^{-1}) = l_S(s) = 1.$$

Therefore, $\lambda_1(G, S) = 1$.

On the other hand,

$$l_S(gss'g^{-1}) = l_S(ss') \leq 2.$$

Thus, we see that $\lambda_2(G, S) \leq 2$, and note that $\lambda_2(G, S)$ may be equal to 1 (for example, in the case that $ss' \in S$ for all $s, s' \in S$).

Now suppose that G is a nontrivial finite group and $S = G - \{1\}$. That is, we take as our symmetric generating set all elements of G except the identity. Then, for any $g \in G$, $s \in S$ we have that $g^{-1}sg = h$ for some $h \in G$. Now, either $h = 1$ or $h \in S$. Thus, either $l_S(g^{-1}sg) = 0$ or 1. Thus, we have that

$$\lambda_1(G, S) = \max_{g \in G, s \in S} l_S(g^{-1}sg) = 1,$$

whenever $S = G - \{1\}$. The same basic argument can be used to show that $\lambda_2(G, S) = 1$ whenever $S = G - \{1\}$. Note that this example exhibits the feature that a large generating set S gives small values of λ_1 and λ_2.

Finally, the main result of [1], Theorem 1 from that paper, establishes bounds on λ_1 and λ_2 in the cases where G is the symmetric group Σ_n of order $n!$ and S is one of three distinct generating sets, the transpositions, the reversals, and the Coxeter generators. This together with the aforementioned observations already shows that the values of λ_1, λ_2 are highly dependent on the specific choice of, and specific properties of both the group G and the particular symmetric generating set S.

We note that an important source of motivation for the definitions of the λ_i, $i = 1, 2$, comes from computational approaches to the study of genome rearrangements. For some time now, combinatorial methods and finite groups such as permutation groups have played a major role in the modeling and exploration of problems arising in combinatorial genomics, for more on such topics see [2, 3, 4, 5, 1]. The significance in relation to [1] is that the notion of distance described there relates to the evolutionary distance between species based on differences in their respective genomes.

In addition, it is the case that many groups, including Σ_n, may be described as finitely presented groups [6, 7, 8]. Furthermore, the so-called group of circular permutations, which is of particular relevance to computational genomics [4], can be described by adding a relation to the usual presentation for the affine symmetric group. Thus, when G is a finitely presented group, there is interest in computing the values for λ_i, $i = 1, 2$ and investigating questions such as how do the relations in a presentation for G affect the values of the λ_i, $i = 1, 2$. To date, very few efforts have been made in this direction.

In this work, we compute bounds or values for λ_1 and λ_2 for the dihedral groups D_n, $n > 2$, which are of course well known to be noncommutative groups of order $2n$, see *e.g.* [9, 8]. Specifically, we consider dihedral groups given as finitely presented groups for several small generating sets that have the additional feature of being symmetric as described below, and also examine how the λ_i values vary in both n and the nature of the presentation. First, this involves developing a thorough understanding of the possible symmetric presentations for D_n, which we do completely for symmetric generating sets of cardinality less than or equal to three. Next, it must be established how the relations affect computing values or bounds for the λ_i. An important step along the way is to understand when two or more particular concrete realizations of a presentation in terms of specific elements of D_n correspond to the same abstract presentation.

There are several reasons for considering the values of λ_1 and λ_2 for the dihedral groups. First, some computations are amenable to a direct approach which help to provide insight into certain aspects of the quantities λ_1 and λ_2. For example, when computing the values of λ_1 and λ_2 one is essentially concerned with the lengths of conjugates of elements of S and conjugates of products of pairs of elements of S. That is, we want to know the lengths of elements of the form $g^{-1}sg$ and $g^{-1}ss'g$ where $g \in G$, $s, s' \in S$. Now, it is not necessarily the case that this produces every element of the group. This can already been seen in the previous example where G is commutative and S is any symmetric generating set. The computations contained herein for the dihedral groups further illustrate this point. Second, the geometric properties of the dihedral groups [10] provide intuition valuable in the computation of the quantities λ_1 and λ_2.

The remainder of the paper is organized as follows: In section 2, we develop a complete classification of all symmetric presentations of D_n with the cardinality of the generating set less than or equal to three. In section

3, we establish some intermediate results used in the construction of bounds for the values of the λ_i that are also of interest independent of the quantities λ_i. In section 4, we carry out the construction of the bounds for λ_i using the aforementioned presentations, thus establishing the main results of the paper. After concluding remarks in section 5, we provide ancillary results connected to section 2 in an appendix.

2. Classification of Small Presentations for D_n

In this section, we give a complete classification of all symmetric presentations of the dihedral groups with the cardinality of the generating set less than or equal to three. This is carried out largely by looking at concrete realizations of order two and order three symmetric generating subsets of D_n, with its standard description, see (5).

We begin by recalling some basic features of the dihedral groups in order to establish notation and perspective. The dihedral group D_n is the group of order $2n$ with the following properties: D_n contains an order n cyclic subgroup and n distinct elements, each of order two, none of which belongs to the order n cyclic subgroup. From a geometric perspective D_n represents the symmetries of a regular n-gon under rigid motions. Often, D_n is described by the presentation

$$D_n = \left\langle r, f \mid r^n = f^2 = 1, rf = fr^{-1} \right\rangle, \tag{4}$$

e.g. [9]. Then, the dihedral groups can be written out as the $2n$ distinct elements

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, f, rf, r^2 f, \ldots, r^{n-1} f\}. \tag{5}$$

We also have that

$$(r^i)^{-1} = r^{n-i}, \tag{6}$$

$$rf = fr^{-1} = fr^{n-1}, \tag{7}$$

$$(r^i f)(r^i f) = 1, \text{ for any integer value of } 0 \le i \le n. \tag{8}$$

We refer to the elements of the form $r^i f$ as involutions, or involution elements. In fact, these are the only involution elements besides $r^{\frac{n}{2}}$, which only exists if n is even. See [9] for more information regarding the dihedral groups, which we note can also be viewed as a special class of Coxeter groups [11]. All of

the equations (6)-(8) will be used to facilitate the computations in the next sections.

Note that, while $\{r, f\}$ generates D_n, it is not symmetric. Thus, we now proceed to classify all presentations of D_n where the generating set S has cardinality less or equal to three and satisfies the symmetry condition that $s \in S \Rightarrow s^{-1} \in S$. We begin by classifying all symmetric generating sets with cardinality two, since there is no singleton $\{x\}$ such that there are relations on x leading to a presentation of D_n.

2.1. Classification of symmetric presentations using two elements

Consider a set $S = \{x, y\}$. If S is to be symmetric, then we must have either $xy = yx = 1$, or $x^2 = y^2 = 1$. However, in the first instance, $S = \{x, x^{-1}\}$ which only generates a cyclic group $\langle x \rangle$ and therefore is not D_n. Thus, if $S = \{x, y\}$ is a symmetric generating set for D_n we must have that $x^2 = y^2 = 1$. This implies that the product xy must generate the order n cyclic subgroup.

There is still the possibility that x or y is an element of order two and in the order n cyclic subgroup of D_n. This occurs if and only if one of them is $r^{\frac{n}{2}}$ in the previous notation, which may only occur in the case that n is even. But, this would then imply that $xy = yx$ which again does not generate D_n. Therefore, in the notation of (5), there are integers a, b such that $x = r^a f$ and $y = r^b f$. Considering this leads to the following:

Theorem 1. $D_n = \langle x, y \mid x^2 = y^2 = 1, |xy| = n \rangle$ *completely classifies the symmetric presentations of D_n with generating set $S = \{x, y\}$ of cardinality two.*

Proof. The elements $(xy), (xy)^2, (xy)^3, \cdots, (xy)^n = 1$ produce the order n cyclic subgroup of D_n. Then $(xy)x, (xy)^2x, (xy)^3x, \cdots, (xy)^nx$ are all distinct, as are $(xy)y, (xy)^2y, (xy)^3y, \cdots, (xy)^ny$. Now, we claim that there is an integer p so that $y = (xy)^px$. We have that $(xy)^n = (xy)^{n-1}xy = 1$. But then multiplying both of sides of the second equality by y on the right gives $(xy)^{n-1}x = y$. Thus, the sets $\{(xy)x, (xy)^2x, (xy)^3x, \cdots, (xy)^nx\}$ and $\{(xy)y, (xy)^2y, (xy)^3y, \cdots, (xy)^ny\}$ are really the same. This yields another n elements, each of which is its own inverse by the relations $x^2 = y^2 = 1$. This is illustrated by the expansion

$$(xy)^px(xy)^px = (xy)(xy)\cdots(xy)x(xy)(xy)\cdots(xy)x,$$

which, by the relations, reduces to 1. Further, since $x^2 = y^2 = 1$ and $xy \neq 1, yx \neq 1$, there are no other elements because words must alternate. Thus, this is a group with $2n$ elements, exactly half of which form a cyclic subgroup and the remaining are all involutions. $\square$

As we will see, the result from Theorem 1 will be important for much of what follows. An interesting concrete case to consider is that of D_4, the set $S = \{f, r^2 f\}$ does not generate the group. In fact, it is easy to see that the set $\{f, r^a f\}$ generates D_n if and only if a is relatively prime with n.

2.2. Classification of symmetric presentations using three elements

In this section, we categorize the symmetric presentations for D_n that use three elements as the generating set. These are distinguished by the types of relations that are necessary to impose and are motivated by the examples that accompany the results.

2.2.1. Two involutions and one cyclic element

Example 1. Let $n = 6$, and consider the generating set $S = \{f, rf, r^3\}$. In this example, the pair f, rf generates an order n cyclic subgroup, and in fact all of D_6. The additional involution element r^3 is not necessary to obtain D_6 but, as we will see later, it may affect the values of the λ_i.

Theorem 2. *For n even,*

$$D_n = \left\langle x, y, z \mid x^2 = y^2 = z^2 = 1, \ |xy| = n, \ z = (xy)^{\frac{n}{2}}, \ xz = zx, \ yz = zy \right\rangle$$

classifies the symmetric presentations of D_n using a generating set with three elements in the case where exactly one of them is an element of the order n cyclic subgroup.

Note that there is no analogous presentation for D_n when n is odd since in this case the center of the group is trivial. The proof that this gives a presentation of D_n is almost identical to that of Theorem 1. In fact, the element corresponding to $r^{\frac{n}{2}}$ is not needed in order to generate the group but may affect the values of the λ_i as we will see in section 4.2.1.

2.2.2. Two cyclic elements and one involution

Example 2. Let $n = 6$, and consider the generating set $S = \{f, r, r^5\}$. In this example, the pair f, r gives the standard presentation of D_6. The element r^5, being the inverse of r, is added simply to make the set symmetric.

7

Theorem 3. *For a positive integer n,*

$$D_n = \langle x, y, z \mid x^2 = 1, \ |y| = |z| = n, \ yx = xz, \ yz = zy = 1, \ |xy| = |xz| = 2 \rangle$$

classifies the symmetric presentations of D_n using a generating set with three elements in the case where exactly two of the elements are contained in the order n cyclic subgroup.

Notice that the second and fourth relations imply that $z = y^{n-1}$. Thus, this is exactly the usual presentation for D_n obtained by adding the inverse of r thereby making S symmetric. Then, it is clear that this gives a presentation for D_n.

2.2.3. Three involution elements

Before describing in detail the remainder of the three element presentations for D_n we present a simple result that will show that we do in fact end up with a complete classification. The basic idea is to understand what all of the possibilities are in the case that the three generators are all involutions, none of which belong to the order n cyclic subgroup.

Let a and b be nonnegative integers less than n, then for a subset $S = \{f, r^a f, r^b f\}$ of D_n, define the cyclic subgroups $H_1 = \langle r^a ff \rangle = \langle r^a \rangle$, $H_2 = \langle r^b ff \rangle = \langle r^b \rangle$, and $H_3 = \langle r^b fr^a f \rangle = \langle r^{b-a} \rangle$. Also, define the sets $H_1 H_2 H_3 = \{h_1 h_2 h_3 \mid h_i \in H_i, i = 1, 2, 3\}$ and $H_1 H_2 = \{h_1 h_2 \mid h_i \in H_i, i = 1, 2\}$.

We make the following observations:

1. For each $i = 1, 2, 3$, H_i is a normal subgroup of D_n since it is generated by an element of the order n cyclic subgroup of D_n. For example, take H_1, then

$$r^k r^{ja} r^{-k} = r^{ja} \in H_1,$$
$$r^k fr^{ja} r^k f = r^{-ja} \in H_1.$$

2. $H_3 \subset H_1 H_2$. This follows since anything of the form $r^{j(b-a)}$, which is a typical element of H_3, is a special case of something of the form r^{nb+ma}, which is a typical element of $H_1 H_2$. Thus, we have that $H_1 H_2 H_3 = H_1 H_2$.

With this notation, we have the following lemma which provides a concise characterization of when three involutions will generate D_n.

8

Lemma 1. *For a and b be nonnegative integers less than n, let $S = \{f, r^a f, r^b f\} \subset D_n = \{1, r, \ldots, r^{n-1}, f, rf, \ldots, r^{n-1}f\}$. Then, S generates D_n if and only if $H_1 H_2 = \{h_1 h_2 \mid h_i \in H_i\} = \langle r \rangle = \{1, r, \ldots, r^{n-1}\}$. By the previous observation, this is equivalent to the condition that $H_1 H_2 H_3 = \langle r \rangle$.*

Proof. First suppose that $S = \{f, r^a f, r^b f\}$ generates D_n. Then there are integers j, k, l such that[1]

$$r = (r^a f f)^j (r^b f f)^k (r^b f)^l \in H_1 H_2 H_3 = H_1 H_2.$$

This implies that $\langle r \rangle \subset H_1 H_2$. On the other hand, by definition $H_1 H_2 \subset \langle r \rangle$. Thus, we have that $H_1 H_2 = \langle r \rangle$ and this proves the first direction.

Conversely, suppose that $H_1 H_2 = \langle r \rangle$, then we have the order n cyclic subgroup $\{1, r, \ldots, r^{n-1}\}$ of D_n. Note that the set $H_1 H_2 f = \{h_1 h_2 f \mid h_i \in H_i\}$ then gives exactly n distinct involution elements. $\qquad\square$

In order to obtain a slight generalization, suppose that we have a set $S = \{r^a f, r^b f, r^c f\}$, then take $S' = \{r^a f, r^{b-a}(r^a f), r^{c-a}(r^a f)\} = \{f', r^{a'} f', r^{b'} f'\}$, where $f' = r^a f$, $a' = b - a$, and $b' = c - a$. Then one can apply the previous result to S', since it is equivalent to S.

A consequence of Lemma 1 is that, given a subset $S = \{f, r^a f, r^b f\}$ of D_n, there are five possibilities with respect to the generating of D_n. Using the notation previously introduced, these are:

1. $H_1 = H_2 = H_3 = \langle r \rangle$

2. Exactly two of H_1, H_2, H_3 are $\langle r \rangle$

3. Exactly one of H_1, H_2, H_3 is $\langle r \rangle$

4. None of H_1, H_2, H_3 is $\langle r \rangle$ but $H_1 H_2 = \langle r \rangle$

5. $H_1 H_2$ is a strict subgroup of $\langle r \rangle$, in other words $S = \{f, r^a f, r^b f\}$ does not generate D_n.

---

[1]The reason that this is true is because r must be made up of an alternating product of the elements from S of even length. Then one can apply the pairwise commutativity property $abcd = cdab$ to rewrite this in the form $(r^a f f)^j (r^b f f)^k (r^b f)^l$.

This motivates the remainder of our classification of three element presentations of D_n. It is appropriate to note here that there are precise number-theoretic conditions for the exponents a, b in $S = \{f, r^a f, r^b f\}$ that can be used to distinguish the five cases above in concrete situations. The details of this are given in Section 6 so as not to detract from the main line of reasoning.

Theorem 4. *The following complete the classification of the presentations of D_n with generating set of cardinality three.*

(A) *For a positive integer n, D_n is $\langle x, y, z \rangle$ with relations $x^2 = y^2 = z^2 = 1$, $|xy| = |xz| = |yz| = n$; $\forall a, b, c, d \in \{x, y, z\}$, $abcd = cdab$; and $\langle xy \rangle = \langle xz \rangle = \langle yz \rangle$.*

(B) *For a positive integer n, D_n is $\langle x, y, z \rangle$ with relations $x^2 = y^2 = z^2 = 1$, $|xy| = |xz| = n$; $\forall a, b, c, d \in \{x, y, z\}$, $abcd = cdab$; and $\langle yz \rangle \subsetneq \langle xy \rangle = \langle xz \rangle$.*

(C) *For a positive integer n, D_n is $\langle x, y, z \rangle$ with relations $x^2 = y^2 = z^2 = 1$, $|xy| = n$; $\forall a, b, c, d \in \{x, y, z\}$, $abcd = cdab$; and $\langle xz \rangle \subsetneq \langle xy \rangle$, $\langle yz \rangle \subsetneq \langle xy \rangle$.*

(D) *For a positive integer n, D_n is $\langle x, y, z \rangle$ with relations $x^2 = y^2 = z^2 = 1$; $\forall a, b, c, d \in \{x, y, z\}$, $abcd = cdab$; and if $H_1 = \langle xy \rangle$, $H_2 = \langle xz \rangle$, $H_3 = \langle yz \rangle$ we have $H_1 H_2$ is an order n cyclic subgroup with $H_1 \subsetneq H_1 H_2$, $H_2 \subsetneq H_1 H_2$, and $H_3 \subsetneq H_1 H_2$.*

Proof. In each of the cases (A)-(D), it is clear that we obtain, at least n elements of a cyclic subgroup, and at least n distinct involution elements. Furthermore, each of the four presentations gives elements that are either contained in an order n cyclic subgroup, or are involutions. It remains to verify that there are exactly n elements that form a cyclic subgroup, and exactly n distinct involution elements. This is precisely what is given by the final condition in the statement of each of (A)-(D). $\square$

Next, we provide examples to illustrate each of the cases described in Theorem 4 (A) - (D).

Example 3. The following examples illustrate the presentations given in Theorem 4 (A)–(D).

(A) Let $n = 5$ and take $S = \{f, rf, r^2f\}$, here all three pairs $\{f, rf\}, \{f, r^2f\}, \{rf, r^2f\}$ generate D_5.

(B) Let $n = 6$ and take $S = \{f, rf, r^2f\}$, here only the two pairs $\{f, rf\}, \{rf, r^2f\}$ generate D_6.

(C) Let $n = 6$ and take $S = \{f, rf, f^4f\}$, here only the pair $\{r, rf\}$ generates D_6.

(D) Let $n = 30$ and take $S = \{f, r^3f, r^5f\}$, here no pair generates D_{30}, but the triple $\{f, r^3f, r^5f\}$ does.

Our problem now is to compute bounds on the values of $\lambda_1(D_n, S)$ and $\lambda_2(D_n, S)$ whenever S is one of the generating sets for any of the presentations of D_n that have been described in this section. First, we establish a technical lemma, Lemma 3, in the next section that will allow us to considerably reduce the workload.

3. Automorphisms of D_n that preserve the λ_i values

In this section we construct certain automorphisms on the dihedral groups, represented as finitely presented groups, that have the feature of preserving the values of $\lambda_1(G, S)$ and $\lambda_2(G, S)$. These will serve as an important tool in our computation of bounds for $\lambda_1(G, S)$ and $\lambda_2(G, S)$ in section 4. For a fuller discussion regarding D_n automorphisms, see [12]. To motivate the results of this section, consider the following example for $n = 3$:

Example 4. Let $S_1 = \{f, rf\}$ and $S_2 = \{f, r^2f\}$ be two different generating sets for $D_3 = \{1, r, r^2, f, rf, r^2f\}$. We define a map $S_1 \to S_2$ by $f \mapsto f$, $rf \mapsto r^2f$. This produces an automorphism on D_3 by extending the mapping to the set of words from S_i, which sends generators to generators. Observe:

$$
\begin{align}
1 &\mapsto 1, & (9)\\
r = (rf)(f) &\mapsto (r^2f)(f) = r^2, & (10)\\
r^2 = (f)(rf) &\mapsto (f)(r^2f) = r, & (11)\\
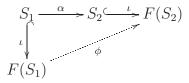f &\mapsto f, & (12)\\
rf &\mapsto r^2f, & (13)\\
r^2f = (f)(rf)(f) &\mapsto (f)(r^2f)(f) = rf. & (14)
\end{align}
$$

11

Notice that in this example, the lengths of words are preserved under the automorphism on D_3, which is essentially defined by sending $f \mapsto f$, $rf \mapsto r^2 f$, and then extending to words[2]. Another important point, discussed in greater detail below, is that the mapping just described preserves all of the important relations between elements in S_1. In this section, we prove that this phenomenon generalizes in a specific manner.

We begin with a lemma that we refer to as the Van Dyck isomorphism property. In the following we denote by ι the usual inclusion map on a set.

Lemma 2. *For two symmetric generating sets $S_1 = \{x, y\}$ and $S_2 = \{x', y'\}$ of D_n that share all of the same relations, the mapping $\alpha : S_1 \to S_2$ defined by $\alpha(x) = x'$, and $\alpha(y) = y'$ extends to a unique automorphism $\Phi : D_n \to D_n$ that maps generators to generators.*

Proof. Let $F(S)$ denote the free group on the set S and let R denote the normal subgroup of $F(S)$ determined by any relations set on the elements of S. Then, the universal property for free groups leads to a unique homomorphism $\phi : F(S_1) \to F(S_2)$, which makes the following diagram commute.

$$
\begin{array}{ccc}
S_1 & \xrightarrow{\ \alpha\ } & S_2 \xhookrightarrow{\ \iota\ } F(S_2) \\
{\scriptstyle \iota}\downarrow & \nearrow & \\
F(S_1) & {\scriptstyle \phi} &
\end{array}
$$

This homomorphism is defined by the formula

$$\phi\left((x)^{\epsilon_1} (y)^{\delta_1} \cdots (x)^{\epsilon_k} (y)^{\delta_k} \right) \tag{15}$$

$$= (x')^{\epsilon_1} (y')^{\delta_1} \cdots (x')^{\epsilon_k} (y')^{\delta_k}, \tag{16}$$

where $\epsilon_i, \delta_i \in \mathbb{Z}$. Next, consider the map $\pi \circ \phi : F(S_1) \to F(S_2)/R_2$, where π is the canonical projection. The kernel of this map is R_1 since S_1 and S_2 have the same relations. Then the first isomorphism theorem applied to $\pi \circ \phi$ gives a unique isomorphism $\Phi : F(S_1)/R_1 \to F(S_2)/R_2$ such that the following diagram commutes.
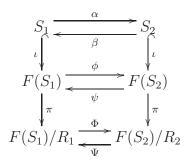
---

[2]The mapping $f \mapsto r^2 f$ and $rf \mapsto f$ would also work. This point is addressed further at the end of this section.

$$F(S_1) \xrightarrow{\phi} F(S_2) \xrightarrow{\pi} F(S_2)/R_2$$
$$\downarrow{\pi}$$
$$\Phi$$
$$F(S_1)/R_1$$

By defining a map $\beta : S_2 \to S_1$ by: $\beta(x') = x$, and $\beta(y') = y$ and interchanging S_1 and S_2, we obtain maps ψ and Ψ that are the inverses of ϕ and Φ respectively. Altogether we obtain the following commutative diagram

$$
\begin{array}{ccc}
S_1 & \xrightarrow{\alpha} & S_2 \\
& \xleftarrow{\beta} & \\
\iota \downarrow & & \downarrow \iota \\
F(S_1) & \xrightarrow{\phi} & F(S_2) \\
& \xleftarrow{\psi} & \\
\pi \downarrow & & \downarrow \pi \\
F(S_1)/R_1 & \xrightarrow{\Phi} & F(S_2)/R_2 \\
& \xleftarrow{\Psi} &
\end{array}
$$

from which the conclusion of the lemma follows. $\square$

Using Lemma 2, we now establish when the homomorphism is also length-preserving. This will serve as an important tool in establishing bounds on the quantities $\lambda_1(G, S)$ and $\lambda_2(G, S)$.

Lemma 3. *If $S_1 = \{x, y\}$ and $S_2 = \{x', y'\}$ are symmetric generating sets of D_n that share all of the same relations, then*

$$\max_{g \in D_n} \{l_{S_1}(g)\} = \max_{g \in D_n} \{l_{S_2}(g)\}.$$

Proof. Let $\alpha : S_1 \to S_2$ and $\Psi : D_n \to D_n$ be as in the previous lemma. Let $h \in D_n$ such that $l_{S_1}(h) = M_1 := \max_{g \in D_n} \{l_{S_1}(g)\}$, and let $\bar{h} \in D_n$ such that $l_{S_2}(\bar{h}) = M_2 := \max_{g \in D_n} \{l_{S_2}(g)\}$. Now suppose that $M_2 > M_1$. We claim that this implies that there is no element $g \in D_n$ such that $\Psi(g) = \bar{h}$ thereby implying that Ψ is not an automorphism in contradiction to the previous lemma. If there were such a g, then we can write it as a product of generators with no more that M_1 terms. But then since Ψ is a homomorphism that maps generators to generators this would be an element with length in S_2 less than or equal to M_1 contradicting that $M_2 > M_1$. By switching the roles of S_1 and M_1 with that of S_2 and M_2 we obtain the result. $\square$

13

Remark: Lemma 2 is related to a result in the theory of group presentations sometimes known as Van Dyck's theorem, see [13, 7, 8]. Furthermore, there is nothing particularly special about the role of D_n, or the sizes of S_1 and S_2, in Lemma 2 since the universal property for free groups and the first isomorphism theorem apply in more general settings. Thus, Lemma 2 generalizes in an obvious way to give rise to a more general version of Lemma 3. However, as we exhibit with an example, one must take care to be sure that a mapping from one specific generating set to another does in fact preserve all relations.

Example 5. First, consider the situation with $n = 7$, $S_1 = \{x_1 = f, y_1 = rf, z_1 = r^2f\}$ and $S_2 = \{x_2 = f, y_2 = r^3f, z_2 = r^4f\}$. The mapping $f \mapsto f$, $rf \mapsto r^3f$, $r^2f \mapsto r^4f$ does not preserve the relation $z_1 = (y_1x_1)^2x_1 = (y_1x_1)y_1$ since in S_1 we have $(rff)^2f = r^2f$ but in S_2 we have $z_2 = r^4f = (y_2x_2)^4x_2 = (r^3ff)^4f$. On the other hand, it can be shown that the mapping $S_1 = \{x_1 = f, y_1 = rf, z_1 = r^2f\} \to S_2 = \{x_2 = r^3f, y_2 = f, z_2 = r^4f\}$ given by $f \mapsto r^3f$, $rf \mapsto f$, $r^2f \mapsto r^4f$ does preserve all relations, and hence preserves the λ_i values. In contrast, for $n = 9$, $S_1 = \{x_1 = f, y_1 = rf, z_1 = r^2f\}$ and $S_2 = \{x_2 = f, y_2 = rf, z_2 = r^3f\}$, there is no mapping $S_1 \to S_2$ that will preserve all relations. This is due to the fact that in S_1, all of the products $(x_1y_1), (x_1z_1)$, and (y_1z_1) have order $n = 9$, while in S_2 the product (x_2z_2) has order $3 < n = 9$.

These examples also serve to illustrate that the order in which generators are taken does matter. Furthermore, these examples illustrate the necessity of several of the relations we have imposed. However, even with all of this in mind, it will come to light in the next section that not all relations play a role in the actual computation of the λ_i values.

4. Bounds for λ_i values

In this section we discuss computing bounds for λ_1 and λ_2 corresponding to each of the presentations for D_n given in Section 2. We apply the results from Section 3 in order to work with concrete generating sets for D_n. We begin by computing bounds for the λ_i in the case where the symmetric generating set has cardinality equal to two.

4.1. Cardinality Two Case

Fix an involution f of D_n and set $S_f = \{f, rf\}$, where r generates the order n cyclic subgroup of D_n. Clearly S_f generates D_n and $f^2 = (rf)^2 = 1$,

that is, f and rf are both involution elements of D_n. Thus the set S_f is a symmetric generating set for D_n. We call this S_f the symmetric order two simple generating set for D_n. Furthermore, it is the case that there is no smaller symmetric generating set for D_n. The following results hold:

Theorem 5. *Let $G = D_n$ and $S_f = \{f, rf\}$, then*

(a) $\lambda_1(D_n, S_f) \le n$,

(b) $\lambda_2(D_n, S_f) = 2$.

Proof. We begin by proving Theorem 5 (a): In order to establish this result, we make the two following observations. First, since f, rf are both involution elements, if $s = f$ or if $s = rf$ then $(g^{-1}sg)(g^{-1}sg) = 1$, thus $g^{-1}sg$ is also an involution. Hence, either $g^{-1}sg = r^{\frac{n}{2}}$ or $g^{-1}sg = r^i f$ for some integer i, since these are the only involution elements in D_n. Second, again since f, rf are both involution elements, words in the generators f, rf must be alternating. So it is not difficult to construct Tables 1 and 2, tables of words where the ith entry is the ith alternating product $s_1 s_2 s_1 \dots$ which is $(s_1 s_2)^{\frac{i}{2}}$ for i even and is $(s_1 s_2)^{\frac{i-1}{2}} s_1$ for i odd.

Table 1: Alternating products of generators, n odd.

1	f	rf
2	$frf = r^{n-1} = r^{-1}$	$rff = r$
3	$frff = fr$	$rffrf = r^2 f$
4	$frffrf = r^{n-2} = r^{-2}$	$rffrff = r^2$
5	$frffrff = fr^2$	$rffrffrf = r^3 f$
$\vdots$	$\vdots$	$\vdots$
n	$= fr^{\frac{n-1}{2}}$	$= r^{\frac{n+1}{2}} f$

There is an important fact regarding the entries in Tables 1 and 2: In the odd case $fr^{\frac{n-1}{2}} = fr^{\frac{n+1}{2}}$ and in the even case $r^{-\frac{n}{2}} = r^{\frac{n}{2}}$ but otherwise all of the other elements that appear are distinct. Thus, the entries in the table together with the identity element exhausts the list of elements for D_n. Now the longest element that appears has length n which shows that $\lambda_1(D_n, S) \le n$ and thereby establishes part (a).

Table 2: Alternating products of generators, n even.

1	f	rf
2	$frf = r^{n-1} = r^{-1}$	$rff = r$
3	$frff = fr$	$rffrf = r^2 f$
4	$frffrf = r^{n-2} = r^{-2}$	$rffrff = r^2$
5	$frffrff = fr^2$	$rffrffrf = r^3 f$
$\vdots$	$\vdots$	$\vdots$
n	$= r^{-\frac{n}{2}}$	$= r^{\frac{n}{2}}$

Proof for Theorem 5 (b): To compute λ_2, we need $l_s(g^{-1}ss'g)$. However, if $s = s'$, $l_s = 1$ since each element in S is symmetric.
Therefore, there are two remaining cases, each containing two sub-cases.

Case 1: $ss' = r^{-1}$

    $g = r^i f$: Then $g^{-1}ss'g = r$, therefore, $l_s = 2$.

    $g = r^i$: Then $g^{-1}ss'g = r^{-1}$, therefore, $l_s = 2$.

Case 2: $ss' = r$

    $g = r^i f$: Then $g^{-1}ss'g = r^{-1}$, therefore, $l_s = 2$.

    $g = r^i$: Then $g^{-1}ss'g = r$, therefore, $l_s = 2$.

Therefore $\lambda_2(D_n, S) = 2$ for all n. $\qquad\square$

Remark: It is actually possible to say more than what is stated in Theorem 5 (a). First note that equality in (a) may be achieved if $n + 1$ is divisible by 4. To see this, set $s = f$ and $g^{-1} = r^{\frac{n+1}{4}}$. Then

$$g^{-1}sg = r^{\frac{n+1}{4}} f r^{-\frac{n+1}{4}},$$
$$= r^{2\frac{n+1}{4}} f,$$
$$= r^{\frac{n+1}{2}} f,$$

16

and where $\frac{n+1}{2}$ is even. The proof of (a) and in particular Tables 1 and 2 shows that this gives an element of length n. This is an interesting contrast with the result stated in Theorem 1 (ii) in [1], where both the order of the group and the generating set increase with n; whereas if $G = D_n$ and $S_f = \{f, rf\}$, only the order of the group increases with n. Furthermore, note that if $s = f$ then gsg^{-1} produces an element of D_n of the form $r^{2k}f$, and if $s = rf$ then gsg^{-1} produces an element of D_n of the form $r^{2k+1}f$. Thus, upon conjugating $s = f$ and $s = rf$ with each element of D_n we obtain each of the involution elements of D_n except $r^{\frac{n}{2}}$. Taking this into account, Tables 1 and 2 then show that $\lambda_1(D_n, S_f) = n$ if n is odd and $\lambda_1(D_n, S_f) = n - 1$ if n is even.

Now, applying Lemma 3 to Theorem 5, we obtain the following result:

Theorem 6. *For any order two symmetric generating set* $S = \{r^a f, f\}$ *of* D_n, *we have*

(a) $\lambda_1(D_n, S) \leq n$,

(b) $\lambda_2(D_n, S) \leq 2$,

and furthermore, $\lambda_1(D_n, S) = n$ *if* n *is odd and* $\lambda_1(D_n, S) = n - 1$ *if* n *is even.*

4.2. Cardinality Three Cases

In this section we consider the bounds for $\lambda_1(D_n, S)$ and $\lambda_2(D_n, S)$ for the cases when the generating set S has three distinct elements. These cases correspond to the presentations described by Theorems 2, 3, and 4 (A)-(D).

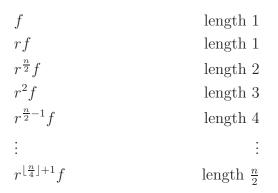#### 4.2.1. Two involutions and one cyclic element

The first case we consider is when the generating set S is composed of three involutions, where exactly one of which is also contained in the order n cyclic subgroup. This case is only relevant whenever n is even. Furthermore, the result we obtain shows how the addition of a single generator may sometimes have a significant impact on the lengths of group elements. One may view this as an instance of what can happen with regard to the values for $\lambda_1(G, S)$ and $\lambda_2(G, S)$ when one makes a slight change in the presentation of the group G. We have the following result.

Theorem 7. *Let* $G = D_n$ *and* $S_f = \{f, rf, r^{\frac{n}{2}}\}$, *then*

(a) $\lambda_1(D_n, S_f) = \frac{n}{2}$,

17

(b) $\lambda_2(D_n, S_f) = \lambda_1(D_n, S_f)$.

Proof. To obtain the value for $\lambda_1(D_n, S_f)$, we essentially look at the lengths of elements in Tables 1 and 2 and then examine how we may use $r^{\frac{n}{2}}$ to reduce the number of generators required to write each element of the group as product from $S_f = \{f, rf, r^{\frac{n}{2}}\}$. First, observe that for any $s \in S_f$ we have that gsg^{-1} is either $r^{\frac{n}{2}}$, which happens exactly when $s = r^{\frac{n}{2}}$, or $gsg^{-1} = r^k f$ for some $0 \leq k \leq n-1$. Furthermore, since $r^k f = fr^{-k} = fr^{n-k}$ and, with respect to $\{f, rf\}$, the length of $r^k f$ is the same as the length of fr^{k-1}, it suffices to consider only elements of the form $r^k f$ with $0 \leq k \leq \frac{n}{2}$. Now we can begin to list these elements and their lengths with respect to $S_f = \{f, rf, r^{\frac{n}{2}}\}$. Notice that f, rf have length one and $r^{\frac{n}{2}} f$ has length two. Furthermore, if we multiply by r or r^{-1} we add two to the length. Then, provided that $n > 4$ is even, we have

f	length 1
rf	length 1
$r^{\frac{n}{2}} f$	length 2
$r^2 f$	length 3
$r^{\frac{n}{2}-1} f$	length 4
$\vdots$	$\vdots$
$r^{\lfloor \frac{n}{4} \rfloor + 1} f$	length $\frac{n}{2}$

which shows that the longest such element has length $\frac{n}{2}$. If $n = 2, 4$ one can see directly that $\lambda_1(D_n, S_f) = 2$.

To obtain the value for $\lambda_2(D_n, S_f)$, begin by noticing that $gss'g^{-1} = r, r^{-1}$ if $s, s' \in \{f, rf\}$ and $s \neq s'$, otherwise $gss'g^{-1}$ can be any element of D_n of the form $r^{2k \pm \frac{n}{2}} f$ or $r^{2k+1 \pm \frac{n}{2}} f$. Therefore, we can write any element of D_n of the form $r^p f$ as $gss'g^{-1}$ where $s, s' \in \{f, rf, r^{\frac{n}{2}}\}$. This proves that $\lambda_2(D_n, S_f) = \lambda_1(D_n, S_f)$. $\qquad\square$

Now, applying Lemma 3 to Theorem 7, we obtain the following result.

Theorem 8. *Let $G = D_n$ and $S_f = \{f, r^a f, r^{\frac{n}{2}}\}$, where r^a generates an order n cyclic subgroup, then*

(a) $\lambda_1(D_n, S_f) = \frac{n}{2}$,

(b) $\lambda_2(D_n, S_f) = \lambda_1(D_n, S_f)$.

18

4.2.2. Two cyclic elements and one involution

Let $G = D_n$. Set $S_f = \{f, r, r^{n-1}\}$, where r and f are the group elements of D_n previously described. Note $f^2 = 1$ and $rr^{n-1} = 1$, thus the set S_f is a symmetric generating set for D_n. We call this S_f *the simple chiral symmetric generating set for* D_n. The following results hold:

Theorem 9. *Let* $G = D_n$ *and* $S_f = \{f, r, r^{n-1}\}$, *then*

(a) $\lambda_1(D_n, S_f) = \begin{cases} \lfloor \frac{n}{2} \rfloor + 1 & \text{if } 4 \mid n, \\ \lfloor \frac{n}{2} \rfloor & \text{if } 2 \mid n \text{ and } 4 \nmid n, \\ \lfloor \frac{n}{2} \rfloor + 1 & \text{if } n \text{ is odd,} \end{cases}$

(b) $\lambda_2(D_n, S_f) = \begin{cases} \lfloor \frac{n}{2} \rfloor & \text{if } 4 \mid n, \\ \lfloor \frac{n}{2} \rfloor + 1 & \text{if } 4 \nmid n, \end{cases}$

where $\lfloor x \rfloor$ *denotes the greatest integer* $m \le x$.

Proof. We proceed by first looking for the elements of D_n whose reduced word length, in terms of elements of S_f, is maximal. Choose a representative of such elements, call it ϕ_0. We must determine if and how ϕ_0 can be realized as a conjugate of the form $g^{-1}sg$ or $g^{-1}ss'g$. If ϕ_0 can be realized as a conjugate of the form $g^{-1}sg$ then we have found λ_1. On the other hand, if ϕ_0 can be realized as a conjugate of the form $g^{-1}ss'g$ then we have found λ_2. If ϕ_0 can't be realized in this conjugate form then we look for a next longest element of D_n, call it ϕ_{-1}, and then proceed as just described. If necessary, continue to reduce to "the next longest element" until this process eventually ends and yields the values of λ_1 and λ_2.

Now, some elements with maximal length in D_n with respect to the generating set S_f are

$$\phi_0 = \begin{cases} r^{\frac{n}{2}}f & \text{when } n \text{ is even,} \\ r^{\lfloor \frac{n}{2} \rfloor}f, \text{ or } r^{\lceil \frac{n}{2} \rceil}f & \text{when } n \text{ is odd,} \end{cases} \tag{17}$$

with $l_S\left(r^{\frac{n}{2}}f\right) = l_S\left(r^{\lfloor \frac{n}{2} \rfloor}f\right) = l_S\left(r^{\lceil \frac{n}{2} \rceil}f\right) = \lfloor \frac{n}{2} \rfloor + 1$. These facts come from a direct examination of the elements of D_n as listed in (5).

For $s = f$, and $g^{-1} = r^k$ with $0 \le k \le \lfloor \frac{n}{2} \rfloor$, we have that

$$g^{-1}sg = g^{-1}fg \tag{18}$$
$$= r^k f r^{-k}, \tag{19}$$
$$= r^{2k}f, \tag{20}$$

where we have made use of the identities from (6)-(8).

Case 1. Observe that if n is divisible by 4 then we can choose $k = \frac{n}{4}$ and achieve $g^{-1}sg = \phi_0 = r^{\frac{n}{2}}f$. This shows that $\lambda_1(D_n, S) = \frac{n}{2} + 1$ whenever $4 \mid n$.

Case 2. On the other hand, if n is even and not divisible by 4 then it is not possible to achieve $\phi_0 = r^{\frac{n}{2}}f$ with an element of the form $g^{-1}sg$. Instead, take $k = \lfloor \frac{n}{4} \rfloor$ which gives $g^{-1}sg = r^{\frac{n}{2}-1}f = \phi_{-1}$, the next longest element of D_n so that in this case $\lambda_1(D_n, S) = \frac{n}{2}$.

Case 3. If n is odd, then take $k = \lfloor \frac{n}{4} \rfloor$ and we get $g^{-1}sg = r^{\lfloor \frac{n}{2} \rfloor}f = \phi_0$ so again $\lambda_1(D_n, S) = \frac{n}{2} + 1$.

This proves theorem 9 (a).

To obtain the result of theorem 9 part (b), the proof is similar to that for part (a) except that now the relevant conjugates of the form $g^{-1}ss'g$ that lead to either an element of maximal length ϕ_0 (only possible if n is odd) or a next longest element ϕ_{-1} of D_n, which are of the form $r^{2k+1}f$ or $r^{2k-1}f$. Notice these elements are products of f with odd powers of r. These come from taking $g^{-1} = r^{-k}$ with $0 \le k \le \lfloor \frac{n}{2} \rfloor$ and either $s = r$, $s' = f$; or $s = r^{-1}$, $s' = f$.

Finally, observe that if n is divisible by 4 then the longest element is an even multiple of r times f and thus is not realizable as $g^{-1}ss'g$. However, in this case a next longest element is realizable as $g^{-1}ss'g$ so that $\lambda_2(D_n, S) = \frac{n}{2}$ whenever $4 \mid n$. If n is even but not divisible by 4 then the longest element ϕ_0 is a product of f with an odd power of r and thus is realizable as a conjugate of the form $g^{-1}ss'g$. Thus, in the case n is even and $4 \nmid n$ we have $\lambda_2(D_n, S) = \frac{n}{2} + 1$. Lastly, if n is odd then since $l_S\left(r^{\lfloor \frac{n}{2} \rfloor}f\right) = l_S\left(r^{\lceil \frac{n}{2} \rceil}f\right) = \lfloor \frac{n}{2} \rfloor + 1$ one of $\lfloor \frac{n}{2} \rfloor$ or $\lceil \frac{n}{2} \rceil$ is odd and hence is realizable as $g^{-1}ss'g$. Therefore $\lambda_2(D_n, S) = \lfloor \frac{n}{2} \rfloor + 1$. $\qquad\square$

Combining the result of Theorem 9 together with the remark following Lemma 3 from section 3 gives the following:

Theorem 10. *Let $G = D_n$ and $S = \{r^a f, r^b, r^{-b}\}$ and suppose that r^b generates an order n cyclic subgroup of D_n, then*

(a) $\lambda_1(D_n, S_f) = \begin{cases} \lfloor \frac{n}{2} \rfloor + 1 & \text{if } 4 \mid n, \\ \lfloor \frac{n}{2} \rfloor & \text{if } 2 \mid n \text{ and } 4 \nmid n, \\ \lfloor \frac{n}{2} \rfloor + 1 & \text{if } n \text{ is odd,} \end{cases}$

20

(b) $\lambda_2(D_n, S_f) = \begin{cases} \lfloor \frac{n}{2} \rfloor & \textit{if } 4 \mid n, \\ \lfloor \frac{n}{2} \rfloor + 1 & \textit{if } 4 \nmid n, \end{cases}$

where $\lfloor x \rfloor$ denotes the greatest integer $m \le x$.

This theorem establishes the values of $\lambda_1(D_n, S)$ and $\lambda_2(D_n, S)$ for any presentation with a form as in Theorem 3.

4.2.3. Three involution elements

In this section we discuss bounds for $\lambda_1(D_n, S)$ and $\lambda_2(D_n, S)$ with S a generating set of the form described in Theorem 4 (A) - (D). While proving a bound for $\lambda_2(D_n, S)$ in this case is straightforward, doing so for $\lambda_1(D_n, S)$ is challenging and a complete proof is currently elusive. Therefore, in this section we present, by way of Theorem 11, strong evidence for the following conjecture:

Conjecture 1. *For a generating set S composed of three involutions, none of which belong to the order n cyclic subgroup of D_n, we conjecture that $\lambda_1(D_n, S) \le \lfloor \frac{n}{2} \rfloor + 1$.*

Before describing the evidence for this conjecture we discuss some properties of the sets $S_1 = \{f, rf, r^2 f\}$ and $S_2 = \{f, rf, r^3 f\}$. Since for any $n \ge 2$ the pair $\{f, rf\}$ generates D_n we have that S_1 generates D_n if $n > 2$, and S_2 generates D_n if $n > 3$. Furthermore, depending on whether n is odd or even, S_1 is representative of the case in Theorem 4 (A) or (B) respectively, and depending on n, S_2 could correspond to any of the cases in Theorem 4 (A) - (C). We will show that $\lambda_1(D_n S_1), \lambda_1(D_n, S_2) \le \lfloor \frac{n}{2} \rfloor + 1$ thereby establishing

Theorem 11. *Consider the dihedral group D_n with $n \ge 2$. Then there exists a generating set of the form $S = \{f, r^a f, r^b f\}$ such that $\lambda_1(D_n, S) \le \lfloor \frac{n}{2} \rfloor + 1$, where $a \ne b$ and $a, b \ge 1$.*

Theorem 11 is an immediate consequence of either of Lemma 4 or Lemma 5 below. However, before establishing these two lemmas we make some observations regarding the two sets S_1 and S_2. There are three points that are useful to note:

(i) The calculations for $\lambda_1(D_n, S)$ where $S = S_1$ or $S = S_2$ are independent of n.

21

(ii) In order to obtain a bound on the length of the elements of the order n cyclic subgroup of D_n, it suffices to do so for each r^m where $0 < m \leq \lfloor \frac{n}{2} \rfloor$. This is because an element and its inverse have the same length, so once we have the length for the first $\lfloor \frac{n}{2} \rfloor$ powers of r we obtain the others using the inverse property.

(iii) In fact, once you obtain a bound on the lengths of the powers of r, you get a bound on the lengths of flips by way of the following computation. Let $S = \{f, r^a f, r^b f\}$. Consider $r^m f$ then

$$r^m f = r^{m-a} \left(r^a f \right) = r^{m-b} \left(r^b f \right).$$

Now, use the bound on r^m, r^{m-a}, or r^{m-b}, whichever gives the shortest length, then add one to account for f, $r^a f$, or $r^b f$, whichever is appropriate.

Observation (iii) yields the following conjecture, whose truth does not influence the results of Lemma 4 or Lemma 5 below.

Conjecture 2. *For all $0 < m < n$, $l_S(r^m f) \leq \max\limits_{0 \leq k < n} \{l_S(r^k)\}$, where l_S is the length defined in previous sections.*

There is strong evidence for this conjecture. Now we proceed to prove the aforementioned lemmas. Based on the preceding observations, we only need to compute the lengths r^m with $0 < m \leq \lfloor \frac{n}{2} \rfloor$. If the conjecture is correct then in some cases we can tighten the bound by one.

Lemma 4. *Let $S = \{f, rf, r^2 f\}$. Then for any $n > 2$, S generates D_n and $\lambda_1(D_n, S) \leq \lfloor \frac{n}{2} \rfloor + 1$.*

Proof. For $S = \{f, rf, r^2 f\}$, let $A = (rf)(f) = r$ and $B = (r^2 f)(f) = r^2$. Now, for an integer $0 < m \leq \lfloor \frac{n}{2} \rfloor$ we split into two cases, m even, and m odd. If m is even, then

$$r^m = B^{\frac{m}{2}},$$

which has length $l \leq 2\frac{m}{2} \leq \lfloor \frac{n}{2} \rfloor$. On the other hand, if m is odd then

$$r^m = r^{m-1} r = B^{\frac{m-1}{2}} A,$$

where we have used the fact that m odd implies $m - 1$ is even. Now $B^{\frac{m-1}{2}}$ has length less or equal to $2\frac{m-1}{2} = m - 1$ and A has length two. Thus we see that in case m is odd, then r^m has length $l \leq m + 1 \leq \lfloor \frac{n}{2} \rfloor + 1$.

22

Using the points noted above we can already see that for this generating set we have that $\lambda_1 \leq \lfloor \frac{n}{2} \rfloor + 2$. In this case, we can tighten this bound by one.

Next, consider $r^p f$. Again we split computations into the even and odd cases. If m is even, then write

$$r^p f = r^{p-2} r^2 f.$$

Now since $p - 2$ is even, by the previous result with $m = p - 2$ we see that the length of $r^p f$ satisfies $l \leq p - 2 + 1 = p - 1 \leq \lfloor \frac{n}{2} \rfloor - 1$. If p is odd then

$$r^p f = r^{p-2} r^2 f,$$

with $p - 2$ odd. Thus, the length of $r^p f$ will satisfy $l \leq p - 2 + 1 = p - 1 \leq \lfloor \frac{n}{2} \rfloor + 1 - 1 = \lfloor \frac{n}{2} \rfloor$.

This finally shows that for any value of $n > 2$ if we take the generating set $S = \{f, rf, r^2 f\}$ for D_n then $\lambda_1 \leq \lfloor \frac{n}{2} \rfloor + 1$. $\qquad\square$

Lemma 5. *Let $S = \{f, rf, r^3 f\}$. Then for any $n > 3$, S generates D_n and $\lambda_1(D_n, S) \leq \lfloor \frac{n}{2} \rfloor + 1$.*

Proof. For $S = \{f, rf, r^3 f\}$, let $A = (rf)(f) = r$, $B = (r^3 f)(f) = r^3$, and $C = (r^3 f)(rf) = r^2$. For an integer $0 < m \leq \lfloor \frac{n}{2} \rfloor$ we again split the calculations into two cases, m even, and m odd. If m is even, then

$$r^m = C^{\frac{m}{2}},$$

which has length $l \leq 2\frac{m}{2} \leq \lfloor \frac{n}{2} \rfloor$. On the other hand, if m is odd then either $m = 1$, in which case $r^m = r$ has length 2; $m = 3$, in which case $r^m = r^3$ has length 2; or $m > 3$. If $m > 3$ is odd, then $m - 3$ is even. Thus, since

$$r^m = r^{m-3} r^3 = r^{m-3} B,$$

and $m - 3$ is even, we have that r^m has length $l \leq m - 3 + 2 \leq m - 1 \leq \lfloor \frac{n}{2} \rfloor - 1$.

From this we already see that if $n > 3$, then with $S = \{f, rf, r^3 f\}$ generating D_n we have that $\lambda_1 \leq \lfloor \frac{n}{2} \rfloor + 1$. $\qquad\square$

Remark: There are examples to illustrate that, at least for some values of n, this the minimal upper bound. For a specific example take the following.

Example 6. Consider $n = 3$ with $S = \{f, rf, r^2 f\}$. Then $D_3 = \{1, r = (rf)(f), r^2 = (r^2 f)(f), f, rf, r^2 f\}$ and thus $\lambda_1 = 2 = \lfloor \frac{n}{2} \rfloor + 1$.

We currently have not discovered a way to construct, for *any* n, a set of the form $S = \{f, r^a f, r^b f\}$ such that $\lambda_1(D_n, S) \leq \lfloor \frac{n}{2} \rfloor + 1$.

To conclude this section, we now obtain a bound on $\lambda_2(D_n, S)$.

Theorem 12. *Let $S = \{f, r^a f, r^b f\}$, then $\lambda_2(D_n, S) = 2$.*

Proof. Direct computation shows that $gss'g^{-1}$ with $s, s' \in S$ produces each of $1, r, r^{-1}, r^a, r^{-a}, r^b, r^{-b}, r^{a-b}, r^{b-a}$ and the maximal length of these is two. □

5. Conclusion

By classifying all possible finite presentations of the dihedral groups with symmetric generating sets of cardinality less than or equal to three, and establishing that the values of the quantities $\lambda_1(G, S)$ and $\lambda_2(G, S)$ defined in [1] are preserved by certain automorphism that preserves relations, we have proven a family of bounds for $\lambda_1(G, S)$ and $\lambda_2(G, S)$ with $G = D_n$ and S one of several different generating sets. These results serve to illustrate some of the characteristics of $\lambda_1(G, S)$ and $\lambda_2(G, S)$ that where merely hinted at in [1]. One novel feature of our work is the utilization of the group presentation point of view. Thus, our approach may be adapted to other finitely presented groups. This is of interest in both theory and in applications. For example, since finitely presented groups play an important role in both combinatorial genomics and formal language theory, see *e.g.* [14], one may expect that the study of the quantities $\lambda_1(G, S)$ and $\lambda_2(G, S)$ for finitely presented groups should be relevant to those fields.

Of course there is more that one can say about $\lambda_1(G, S)$ and $\lambda_2(G, S)$ for $G = D_n$. First off, what if S has cardinality greater than three? Besides the trivial case with $S = D_n - \{1\}$, already discussed in general in the introduction, one may consider an additional "extreme" case with $S = \{f, rf, \ldots, r^{n-1}f\}$. It is easy to see for this choice of S that $\lambda_1(D_n, S) = 1$ and $\lambda_2(D_n, S) = 2$. Then, probably the most interesting remaining cases are when $3 < |S| < n$. It is likely that each of these cases can be tackled using the approaches we have developed here. However, the computations quickly become prohibitively tedious. Thus, it is desirable, if possible, to have a more unified approach to computing $\lambda_1(G, S)$ and $\lambda_2(G, S)$, at least when $G = D_n$.

24

6. Appendix

Consider a dihedral group D_n described as in equation (5). The goal of this appendix is to establish a number-theoretic condition on the exponents a, b in $S = \{r^a f, r^b f\}$ to distinguish how many pairs it takes to generate. This allows one to realize the presentations described in section 2.1 in a more concrete manner. More significantly, this will allow for the direct computation of bounds for the quantities $\lambda_1(D_n)$ and $\lambda_2(D_n)$.

We begin with the observation that, given $S = \{r^a f, r^b f\}$, we can change notation by defining $r^{\tilde{a}} = r^{b-a}$ and $\tilde{f} = r^a f$, then $r^b f = r^{b-a} r^a f = r^{\tilde{a}} \tilde{f}$ and thus $S = \{\tilde{f}, r^{\tilde{a}} \tilde{f}\}$. In light of this observation, to generate D_n it suffices to establish conditions on an integer a for a subset $S = \{f, r^a f\}$ of D_n, with $f^2 = 1$ and r^a an element of the order n cyclic subgroup of D_n. This will be the case if and only if the product $(r^a f)(f) = r^a$ generates an order n cyclic subgroup, which will happen if and only if there is a solution to the equation $xa \equiv 1 \mod n$. From this we obtain the following result.

Lemma 6. *A subset $S = \{f, r^a f\}$ of D_n, with $f^2 = 1$ and r^a an element of the order n cyclic subgroup of D_n, will generate D_n if and only if a is relatively prime with n.*

Now it is easy to apply this lemma to obtain conditions on a subset $S = \{f, r^a f, r^b f\}$ of D_n, which correspond to the situations described abstractly in Theorem 4 (A)–(C), to determine when one, two, or all three pairs from S generate D_n. It only remains to give a concrete realization of the situation described abstractly by Theorem 4 (D).

Theorem 13. *For a subset $S = \{f, r^a f, r^b f\}$ of D_n, with $f^2 = 1$ and r^a, r^b belonging to the order n cyclic subgroup of D_n, it is the case that none of the pairs $\{f, r^a f\}, \{f, r^b f\}, \{r^a f, r^b f\}$ generate D_n and the triple $\{f, r^a f, r^b f\}$ does, if and only if the following hold:*

1. *a is not relatively prime with n*

2. *b is not relatively prime with n*

3. *$b - a$ is not relatively prime with n*

4. *a, b are relatively prime with one another.*

Proof: Suppose that none of the pairs $\{f, r^a f\}, \{f, r^b f\}, \{r^a f, r^b f\}$ generate D_n, but the triple $\{f, r^a f, r^b f\}$ does. It is then clear from Lemma 6 that none of a, b, and $b - a$ are relatively prime with n. Now, $\langle f, r^a f, r^b f \rangle \subseteq \langle r^{as_1+bt_1}, r^{as_2+bt_2} f \rangle$. Thus, $r \in \langle r^{as_1+bt_1}, r^{as_2+bt_2} f \rangle$ implies that there exist s_1, t_1 such that $as_1 + bt_1 = 1$, i.e. a and b are relatively prime.

On the other hand, if none of a, b, and $b - a$ are relatively prime with n, then it is clear from Lemma 6 that none of the pairs $\{f, r^a f\}, \{f, r^b f\}, \{r^a f, r^b f\}$ can generate D_n. Suppose that a, b are relatively prime. Then there exist integers k, l such that $ka + lb = 1$ thus $(r^a ff)^k (r^b ff)^l = r^{ka+lb} = r$, from which it follows that D_n can be generated.

$\square$

Acknowledgements

References

[1] V. Moulton, M. Steel, The 'butterfly effect' in Cayley graphs with applications to genomics, J. Math. Biol. 65 (6-7) (2012) 1267–1284.

[2] V. Bafna, P. A. Pevzner, Genome rearrangements and sorting by reversals, SIAM J. Comput. 25 (2) (1996) 272–289.

[3] A. Bergeron, A very elementary presentation of the Hannenhalli-Pevzner theory, Discrete Appl. Math. 146 (2) (2005) 134–145.

[4] A. Egri-Nagy, V. Gebhardt, M. M. Tanaka, A. R. Francis, Group-theoretic models of the inversion process in bacterial genomes, J. Math. Biol. 69 (1) (2014) 243–265.

[5] S. Hannenhalli, P. A. Pevzner, Transforming cabbage into turnip: polynomial algorithm for sorting signed permutations by reversals, J. ACM 46 (1) (1999) 1–27.

[6] H. S. M. Coxeter, W. O. J. Moser, Generators and relations for discrete groups, 4th Edition, Vol. 14 of Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas], Springer-Verlag, Berlin-New York, 1980.

[7] D. L. Johnson, Presentations of groups, 2nd Edition, Vol. 15 of London Mathematical Society Student Texts, Cambridge University Press, Cambridge, 1997.

[8] G. Smith, O. Tabachnikova, Topics in group theory, Springer Undergraduate Mathematics Series, Springer-Verlag London, Ltd., London, 2000.

[9] D. S. Dummit, R. M. Foote, Abstract algebra, 3rd Edition, John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[10] N. C. Carter, Visual group theory, Classroom Resource Materials Series, Mathematical Association of America, Washington, DC, 2009.

[11] J. E. Humphreys, Reflection groups and Coxeter groups, Vol. 29 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1990.

[12] K. K. A. Cunningham, T. Edgar, A. G. Helminck, B. F. Jones, H. Oh, R. Schwell, J. F. Vasquez, On the structure of involutions and symmetric spaces of dihedral groups, Note Mat. 34 (2) (2014) 23–40.

[13] M. H. Fenrick, Introduction to the Galois correspondence, 2nd Edition, Birkhäuser Boston, Inc., Boston, MA, 1998.

[14] I. Chiswell, A course in formal languages, automata and groups, Universitext, Springer-Verlag London, Ltd., London, 2009.