COMMUTATION SEMIGROUPS OF DIHEDRAL GROUPS OF ORDER 2N WHERE N IS EVEN

DARIEN DEWOLF

April 2012

Mount Saint Vincent University

Department of Mathematics and Computer Science

Honours thesis supervised by Dr. Charles Edmunds

Introduction

Let G be a group and let $\Lambda(G)$ and $\mathrm{P}(G)$ denote the left and right commutation semigroups of G, respectively. B.H. Neumann first noted that if $G = D_3$, the dihedral group of order 6, then $|\Lambda(G)| = 9$ and that $|\mathrm{P}(G)| = 6$ and that $\mathrm{P}(G) \subset \Lambda(G)$. N.D. Gupta [1] explored these commutation semigroups for dihedral groups, exploring what conditions are needed to ensure isomorphism between the two sets. C.D. Levy [2] then determined the cardinality of the left and right commutation semigroups of the dihedral group D_n where n is odd and when n is a power of two.

Theorem (Levy): Let $n = 2^r s$ where $r \in \mathbb{Z}_0^+$ and s is odd. Then:

$$|\mathrm{P}(D_n)| = \begin{cases} 2^r + 2^{r-1} - 2 & s = 0 \\ n(\mathrm{ind}_R(n) + 1) & r = 0 \end{cases} \qquad |\Lambda(D_n)| = \begin{cases} 2^r + 2^{r-1} - 2 & s = 0 \\ n(\mathrm{ind}_L(n) + 1) & r = 0 \end{cases}$$

Where $\mathrm{ind}_R(n)$ (for n odd and thus coprime to both -2 and 2. This guarantees that some power of 2 and -2 is one) is the least positive integer such that $(-2)^{\mathrm{ind}_R(n)} = 1 (\mathrm{mod}\, n)$ and $\mathrm{ind}_L(n)$ is the least positive integer such that $2^{\mathrm{ind}_L(n)} = 1 (\mathrm{mod}\, n)$.

The purpose of this paper is to address the cardinality of the left and right commutation semigroups for dihedral groups D_n where n is neither a power of two nor odd. That is, if we define m_R and m_L as follows:

$$m_R = \begin{cases} \min\left\{x > r : (-2)^x = (-2)^r (\mathrm{mod}\, n)\right\} & \text{if } s > 1 \\ r & \text{if } s = 1 \end{cases} \qquad m_L = \begin{cases} \min\left\{x > r : 2^x = 2^r (\mathrm{mod}\, n)\right\} & \text{if } s > 1 \\ r & \text{if } s = 1 \end{cases}$$

Then:

Theorem3.5: Let D_n be a dihedral group where $n = 2^r s$ ($r > 0, s > 0$ is odd) and let m_R as defined. Then $|\mathrm{P}(D_n)| = s(2^r + 2^{r-1} - 2) + s(m_R - r)$.

Theorem 4.3: Let D_n be a dihedral group where $n = 2^r s$ ($r > 0, s > 0$ is odd) and let m_L be as defined. Then $|\Lambda(D_n)| = s(2^{r-1} + 2^r - 2) + s(m_L - r)$.

Acknowledgement

I would like to thank Dr. Charles Edmunds, professor of Mathematics at Mount Saint Vincent University, for all that he did to aid me in creating this thesis; his endless patience, his unbelievable insight and his gentle encouragement and h is great stories were each invaluable in the quest to solve this problem and to finish this thesis.

1. Notation and Definitions

Definition: Let *G* be a group and let *a* and *b* be any elements of *G*. Then the commutator of *a* and *b* is defined as:

$$[a,b] = a^{-1}b^{-1}ab$$

Definition: Let *G* be a group and let *a* be a fixed element of *G*. We define the following functions:

$$\rho_a : G \to G \text{ such that } \forall g \in G, (g)\rho_a = [g,a]$$
$$\lambda_a : G \to G \text{ such that } \forall g \in G, (g)\lambda_a = [a,g]$$

Then the left and right commutation semigroups of *G* are defined[1] (with the product of mappings defined as their composition) as:

$$\mathrm{P}(G) = \langle \rho_a : a \in G \rangle$$
$$\Lambda(G) = \langle \lambda_a : a \in G \rangle$$

Definition: The dihedral group of order *2n* is defined as:

$$D_n = \langle a,b : a^n = b^2 = 1, b^{-1}ab = a^{-1} \rangle$$

Note: Any element *g* in D_n has either the form $g = a^k$ or $g = ba^k$, for some $k \in \mathbb{Z}_n$, both of which I will be using without reference. It is a direct consequence of this that many proofs in section two will be done twice, once for each representation.

Example: Let us observe the dihedral group of order 6, D_6. The presentation for this group is

$$D_3 = \langle a,b : a^3 = b^2 = 1, a^b = a^{-1} = a^2 \rangle$$

And its elements are $\{1, a, a^2, b, ba, ba^2\}$. Let us now look at the functions ρ and λ and where they map for each element of D_3.

---

[1] For all elements $s_1,...,s_n$ in a semigroup S, we denote by $\langle s_1,...,s_n \rangle$ the subsemigroup of S generated by $s_1,...,s_n$

For example, if we take powers of *a* in D_3 and commute it on either the left or right by another power of *a*, we get the group identity as they are commutative. In the proceeding two tables, we show the mappings ρ and λ in detail, along with three compositions of λ mappings.

$g \in D_3$	$(g)\rho_1$	$(g)\rho_a$	$(g)\rho_{a^2}$	$(g)\rho_b$	$(g)\rho_{ba}$	$(g)\rho_{ba^2}$
1	1	1	1	1	1	1
a	1	1	1	a	a	a
a^2	1	1	1	a^2	a^2	a^2
b	1	a^2	a	1	a^2	a
ba	1	a^2	a	a	1	a^2
ba^2	1	a^2	a	a^2	a	1

$g \in D_3$	$(g)\lambda_1$	$(g)\lambda_a$	$(g)\lambda_{a^2}$	$(g)\lambda_b$	$(g)\lambda_{ba}$	$(g)\lambda_{ba^2}$	$(g)\lambda_b \circ \lambda_b$	$(g)\lambda_{ba} \circ \lambda_{ba}$	$(g)\lambda_{ba^2} \circ \lambda_{ba^2}$
1	1	1	1	1	1	1	1	1	1
a	1	1	1	a^2	a^2	a^2	a	a	a
a^2	1	1	1	a	a	a	a^2	a^2	a^2
b	1	a	a^2	1	a	a^2	1	a^2	a
ba	1	a	a^2	a^2	1	a	a	1	a^2
ba^2	1	a	a^2	a	a^2	1	a^2	a	1

Observe that the mappings obtained when we commute on the left are not equal to those we obtain from commuting on the right. It shall also now be noted that these elements are <u>not</u> the only elements of the commutation semigroups $\mathrm{P}(D_n)$ and $\Lambda(D_n)$ but that these mappings serve as their generators. To build $\mathrm{P}(D_n)$ and $\Lambda(D_n)$, we must take products of these mappings and products of *their* products until we close up the set where no more new elements can be generated, as we have done in the above table. This can be a tedious task, as some semigroups close up more quickly than others. It is not in general true that the left and right commutator semigroups are isomorphic; in D_3, it is not only the ρ and λ mappings that differ but also $\mathrm{P}(D_n)$ and $\Lambda(D_n)$. In fact, it is seen above that $\mathrm{P}(D_n)$ and $\Lambda(D_n)$ do not even have the same order, having 6 and 9 elements, respectively.

2. Preliminary Theory

Within this section, we follow the discussion presented by Gupta in [1]. He started by defining a function $\mu(i,j)$ from a dihedral group into itself. Though this function seems isolated from our area of study, Gupta discovered that its mappings are directly related to the right and left commutator semigroups of dihedral groups and that they will facilitate (for reasons not so obvious) our study of them. I have provided proofs for many of the lemmas in this section about these mappings in Appendix A. Throughout the discussion, it will be assumed that we are studying the dihedral group of order $2n$, D_n.

Definition: For any two fixed $i, j \in \mathbb{Z}_n$ define the following mapping:

$$\mu(i,j) : D_n \to D_n$$

Such that:

$$(a^k)\mu(i,j) = a^{ki} \quad \text{And that } (ba^k)\mu(i,j) = a^{ki+j}$$

Lemma 2.1 [Gupta]: For every $i,i',j,j' \in \mathbb{Z}_n$, $\mu(i,j) = \mu(i',j')$ if, and only if $i = i', j = j'$

Lemma 2.2 [Gupta]: For all $i,i',j,j' \in \mathbb{Z}_n$ $\mu(i,j)\mu(i',j') = \mu(ii', ji')$

Note: It is as a result of the injection shown in Lemma 2.1 and the product defined in Lemma 2.2 that we can conclude that $\mathrm{M} = \{\mu(i,j) : i,j \in \mathbb{Z}_n\}$ is a semigroup of order n^2.

As previously stated, these $\mu(i,j)$ maps seem isolated; they appear to come out of nowhere. However, these mappings were so properly constructed by Gupta that they completely describe the left and right commutator semigroups.

Lemma 2.3 [Gupta]: For all $j \in \mathbb{Z}_n$ $\rho_{a^{-j}} = \mu(0,-2j)$ and $\rho_{ba^{-j}} = \mu(-2,-2j)$

Lemma 2.4 [Gupta]: For all $j \in \mathbb{Z}_n$ $\lambda_{a^{-j}} = \mu(0,2j)$ and $\lambda_{ba^{-j}} = \mu(2,2j)$

Using lemmas 2.3 and 2.4, we completely describe the generators ρ and λ of the left and right commutator semigroups $\mathrm{P}(D_n)$ and $\Lambda(D_n)$ using these $\mu-$mappings. It should be noted as such, then, that because M is of order n^2 we have an upper bound on the cardinality of the commutation semigroups. That is, we know that $|\Lambda(D_n)|, |\mathrm{P}(D_n)| \le n^2$ .Also, the elements of the left and right commutator semigroups, powers of these generators, are products of these $\mu-$mappings. It will also be noted that we need only take products of $\mu-$mappings that have a non-zero i as a parameter for:

Lemma 2.5: Every element of $\mathrm{P}(D_n)$ is of the form $\mu(0,-2j)$ or $\mu((-2)^l,(-2)^l j)$ for some $j \in \mathbb{Z}_n$.

Lemma 2.6: Every element of $\Lambda(D_n)$ is of the form $\mu(0,2j)$ or $\mu(2^l,2^l j)$ for some $j \in \mathbb{Z}_n$.

It directly follows from lemmas 2.5 and 2.6 that to determine the order of the sets

$$\{\mu(0,-2j) : j \in \mathbb{Z}_n\} \cup \{\mu((-2)^l,(-2)^l j) : j \in \mathbb{Z}_n, l \in \mathbb{Z}^+\}$$

and $\{\mu(0,2j) : j \in \mathbb{Z}_n\} \cup \{\mu(2^l,2^l j) : j \in \mathbb{Z}_n, l \in \mathbb{Z}^+\}$

is to determine the order of $\mathrm{P}(D_n)$ and $\Lambda(D_n)$, respectively.

It is now evident as to why the representation of the elements of the left and right commutator semigroups as $\mu-\text{mappings}$ is advantageous. One *could* take products of the mappings in our semigroups (as we did in our earlier example involving S_3) until it is shown that no more new mappings can be produced. However, the number of new mappings produced depends on the group and thus requires an undetermined amount of calculation. Reducing every left and right commutator semigroup of every dihedral group to a representation as the set of $\mu-$mappings above (which we will show to have predictable and easily calculable orders) solves this problem and allows us to make general statements about their orders.

3. The Order of the Right Commutator Semigroup

C.D. Levy showed [2] that:

$$\left|\mathrm{P}(D_n)\right| = \begin{cases} 2^r + 2^{r-1} - 2 & n = 2^r, r \in \mathbb{Z}^+ \\ n(\mathrm{ind}_R(n) + 1) & n \text{ is odd} \end{cases}$$

Where $\mathrm{ind}_R(n)$ (for n odd and thus coprime to -2. This guarantees that some power of two is one) is the least positive integer such that $(-2)^{\mathrm{ind}_R(n)} = 1 (\mathrm{mod}\, n)$.

Levy calculated the order of the left and right commutator semigroups of any dihedral group D_n where n is odd or a power of two. This leaves open the question of dihedral groups D_n where $n = 2^r s$ where $r \in \mathbb{Z}^+$ and $s > 1$ is odd. We shall determine these orders by calculating how many $\mu - \text{mappings}$ are contained in $\{\mu(0, -2j) : j \in \mathbb{Z}_n\} \cup \{\mu((-2)^l, (-2)^l j) : j \in \mathbb{Z}_n, l \in \mathbb{Z}^+\}$ as first explored in section two. For ease of discussion, I make:

Definition: For any two fixed $a, b \in \mathbb{Z}_n$, we define the $(a,b) - container$ to be the set denoted $\mathcal{C}(a,b) = \{\mu(a, kb) : k \in \mathbb{Z}_n\}$.

We now establish with the following two lemmas some sense of distinctness amongst the containers in D_n:

Lemma 3.1: For any $A, B, C, D \in \mathbb{Z}_n$, $\mathcal{C}(A,B) \cap \mathcal{C}(C,D) = \varnothing$ if and only if $A \neq C$.

Our challenge of determining the order of $\mathrm{P}(D_n)$ rests in first determining how many distinct $((-2)^l, (-2)^l) - \text{containers}$ exist, then determining how many $(0, 2j) - \text{containers}$ exist and how many $\mu - \text{mappings}$ are contained in each container. We know there is only one $(0, 2j) - \text{container}$ and by lemma 2.1 and lemma 3.1 we know that any two $((-2)^l, (-2)^l) - \text{containers}$ are equal only if their arguments are equal. Our dihedral groups are of finite order *2n* and the mappings are defined such that their arguments are modulo *n*. We can thus conclude that if we take products of the arguments of containers modulo n, they will repeat eventually. To formalise this notion of repeating, I define:

Definition: With $n = 2^r s$ ($r \in \mathbb{Z}^+$, $s > 0$ odd), let m_R be defined as:

$$m_R = \begin{cases} \min\left\{x > r : (-2)^x = (-2)^r (\mathrm{mod}\, n)\right\} & \text{if } s > 1 \\ r & \text{if } s = 1 \end{cases}$$

It is easy enough to define m_R. The following lemma, however ensures our ability to do so without worry of its existence:

Lemma 3.2: For $n = 2^r s$ with $r > 1$ and s odd there exists a positive integer $k > r$ such that $(-2)^k = (-2)^r \pmod n$

Now that we have an index of sorts to use as a means to enumerate our containers, we now do so with:

Lemma 3.3: There are $m_R - 1$ distinct $((-2)^l, (-2)^l) - \text{containers}$, for $l \in \mathbb{Z}^+$.

Example: Let us look at D_{36} with $n = 36 = 2^2 \cdot 9$ ($r = 2, s = 9$) and let us observe how many $((-2)^l, (-2)^l) - \text{containers}$ exist in D_{36} and determine the cardinality of each of these $((-2)^l, (-2)^l) - \text{containers}$.

The Containers	Its Parameters (MOD n)	How Many
μ(0,-2j) = μ(0,34j)	0,2,4,6,8,10,12,14,16,18,20,22 24,26,28,30,32,34	18
μ(-2,-2j) = μ(34,34j)	0,2,4,6,8,10,12,14,16,18,20,22 24,26,28,30,32,34	18
μ(4,4j)	0,4,8,12,16,20,24,28,32	9
μ(-8,-8j) = μ(28,28j)	0,8,16,24,32,4,12,20,28	9
μ(16,16j)	0,20,4,24,8,28,12,32,16	9
μ(-32,-32j) = μ(4,4j) REPEAT	NO NEW MAPPINGS - STOP	

In this example we can see that we first have μ(0,-2j) on top, the first part of the union, giving us 18 distinct elements of $\mathrm{P}(D_{36})$. We then have the $\{\mu((-2)^l, (-2)^l j : j \in \mathbb{Z}_n, l \in \mathbb{Z}^+\}$. It is noted now that there are $4 = m_R - 1 = 5 - 1$ distinct $((-2)^l, (-2)^l) - \text{containers}$ where $m = 5$ because it is the least positive integer greater than $r = 2$ such that $(-2)^2 = (-2)^{m_R} \pmod n$. ■

Now that we know how many containers there are for dihedral groups, we now count how many $\mu-$mappings are in each container. For each $\mu-$mapping, there is a j being multiplied by the second parameter. Because these parameters again are modulo *n*, they repeat after a finite number of multiplications. Thus, these containers have finite and calculable order.
In our example, we note that the containers each contained 18, 18, 9, 9 and 9 mappings in the order presented here. We can thus conclude that $\mathrm{P}(G)$ has 63 elements.

We now determine, in general, how many $\mu-$mappings each container contains. We see first of all that the $((-2)^l,(-2)^l)-\text{container}$ has $\frac{n}{2}$ mappings contained in it. Because both $-2j$ and *n* are even, we can cycle through and get all of the even numbers between 0 and *n-1* but we can not get any of the odd ones. This is the same for the $((-2),(-2))-\text{containers}$. When double the parameter to, say,
μ(-4,-4j), we effectively skip over another half of the half we had and we thus have $\frac{n}{4}$ $\mu-$ mappings within . This technique is used by Chris Levy in [2] to prove how many $\mu-$mappings are contained by these containers when *n* is a power of two. In our case, however, there will come a time when we can no longer divide by two because we have an odd part, *s.* But there may be containers whose arguments do not divide *n* and we must thus consider these containers and the $\mu-$mappings they contain.
In our example, this happens after only the first division. We go from 18 to 9 being generated but then 9 are generated in each mapping proceeding. In other words, if we can't divide it by two, we generate *s* mappings in each new mapping. Following this discussion, we have established:

Lemma 3.4: Let D_n be a dihedral group where $n=2^r s, s>1$ with mapping $\mu(i,j)$ as defined in Section 2. Then for some fixed positive integer *l :*

$$\left|\{\mu(q,(-2)^l j): j\in\mathbb{Z}_n)\}\right| = \begin{cases}\dfrac{n}{2^l} & l\le r\\ s & otherwise\end{cases}$$

□

We know how many containers exist for any dihedral group where $n=2^r s$ and we now know how many $\mu-$mappings exist in each container based on its parameters. The goal now is to structure these containers in some kind of order so that we can count the $\mu-$mappings and thus determine the order of $\mathrm{P}(D_n)$. First, our $\mu(0,-2j)$ will go first and if we use lemma 3.4 with *q= 0*, we have $\mu(0,-2j)$ containing $n/2$ mappings. So far:

$$\left|\mathrm{P}(D_n)\right| = \frac{n}{2}+\ldots \qquad (*)$$

Now let us add in to the mix our $\mu-$mappings which have parameters dividing $n=2^r s$. These are the $\mu-$containers of the form $\mu(-2,-2j)$, $\mu((-2)^2,(-2)^2 j)$, $\mu((-2)^3,(-2)^3 j)$, …, $\mu((-2)^r,(-2)^r j)$. As we are dividing *n,* it is not possible to have a power of two of greater power than *r* dividing *n.* Otherwise, *s* would have another factor of two which we could factor out and *s* would thus be even. Using lemma 3.4 with $q=l$ for $l=1,2,\ldots,r$ we have that the orders of these $\mu-$container are $\frac{n}{2}$, $\frac{n}{4}$,..., $\frac{n}{2^r}$ so these $\mu-$containers add $\frac{n}{2}+\frac{n}{4}+\cdots+\frac{n}{2^r}=\sum_{i=1}^{r}\frac{n}{2^i}$ $\mu-$mappings to $\mathrm{P}(D_n)$. Adding this to equation (*), we have:

$$\left|\mathrm{P}(G)\right|=\frac{n}{2}+\sum_{i=1}^{r}\frac{n}{2^i}+\ldots \qquad (**)$$

We now have left to consider the containers whose parameters do not divide $n=2^r s$. How many of these are there? We know that $\{\mu((-2)^l,(-2)^l j : j\in\mathbb{Z}_n, l\in\mathbb{Z}^+\}$ has m_R-1 $\mu-$containers as elements and we have accounted for, in equation (**), *r* of these $\mu-$containers. There are thus $(m_R-1)-r$ $\mu-$containers left to account for. Because these $\mu-$containers do not have parameters dividing $n=2^r s$, we know that they each generate *s* $\mu-$mappings by lemma 3.4. These $\mu-$containers together thus contain $(m_R-r-1)s$ distinct $\mu-$mappings. Adding this to equation (**), we have shown that:

$$\left|\mathrm{P}(D_n)\right|=\frac{n}{2}+\sum_{i=1}^{r}\frac{n}{2^i}+s(m_R-1-r)$$

Using a well-known series $\sum_{i=1}^{r}\frac{1}{2^i}=\frac{2^r-1}{2^r}$, we can simplify this equation as

$$\left|\mathrm{P}(D_n)\right|=\frac{n}{2}+\sum_{i=1}^{r}\frac{n}{2^i}+s(m_R-1-r)=\frac{2^r s}{2}+2^r s\frac{\left(2^r-1\right)}{2^r}+s\left(m_R-1-r\right)=s\left(2^{r-1}+2^r-2\right)+s\left(m_R-r\right)$$

This is true if $s>1$. If $s=0$, however, we have $m_R=r$ and:

$$\left|\mathrm{P}(D_n)\right|=s(2^r+2^{r-1}-2)+s(m_R-r)=2^r+2^{r-1}-2+(r-r)=2^r+2^{r-1}-2$$

This is exactly the formula proved by C.D. Levy. Therefore, we have now proved:

Theorem 3.5: Let D_n be a dihedral group where $n=2^r s$ ($r>0, s>0$ is odd) and let m_R be as defined. Then $\left|\mathrm{P}(D_n)\right|=s(2^r+2^{r-1}-2)+s(m_R-r)$.

4. The Order of the Left Commutator Semigroup

Christopher Levy again showed in [2] that:

$$\left|\Lambda(D_n)\right| = \begin{cases} 2^r + 2^{n-1} - 2 & n = 2^r, r \in \mathbb{Z}^+ \\ n(\text{ind}_L(n)+1) & n \text{ odd} \end{cases}$$

Where $\text{ind}_L(n)$ (for n odd and thus coprime to 2. This guarantees that some power of two is one) is the least positive integer such that $(2)^{\text{ind}_L(n)} = 1(\text{mod}\, n)$.

We then ask the orders of the left commutation semigroup of dihedral groups D_n where $n = 2^r s$ where $r \in \mathbb{Z}^+$ and $s > 1$ is odd. As with the right commutation semigroups, we need to concern ourselves with how many $\mu-$containers are in $\{\mu(0,2j) : j \in \mathbb{Z}_n\} \cup \{\mu(2^l, 2^l j) : j \in \mathbb{Z}_n, l \in \mathbb{Z}^+\}$ and how many $\mu-$mappings each of these containers contain. Again, these powers of two are eventually going to repeat thus giving us a finite number of $(2^l, 2^l) - \text{containers}$ in which to seek $\mu-$mappings. The definition of our limiting index, however, changes to accommodate the powers of two all being positive. Let us now define:

Definition: With $n = 2^r s$ ($r \in \mathbb{Z}^+$, $s > 0$ odd), let m_L be defined as:

$$m_L = \begin{cases} \min\left\{x > r : 2^x = 2^r (\text{mod}\, n)\right\} & \text{if } s > 1 \\ r & \text{if } s = 1 \end{cases}$$

Lemma 4.1: For $n = 2^r s$ with $r > 1$ and s odd there exists a positive integer $k > r$ such that $2^k = 2^r (\text{mod}\, n)$

Again, we know that m_L exists and that there are $m_L - 1$ $(2^l, 2^l) - \text{containers}$.

Example: Let us look at once more D_{36} with $n = 36 = 2^2 \cdot 9$ and let us observe out its left commutation $\mu-$mappings differ from the right in how many $(2^l, 2^l) - \text{containers}$ exist and how many $\mu-$mappings are contained in each of them.

The Containers	Its Parameters (MOD n)	How Many
μ(0,2j)	0,2,4,6,8,10,12,14,16,18,20,22 24,26,28,30,32,34	18
μ(2,2j)	0,2,4,6,8,10,12,14,16,18,20,22 24,26,28,30,32,34	18
μ(4,4j)	0,4,8,12,16,20,24,28,32	9
μ(8,8j)	0,8,16,24,32,4,12,20,28	9
μ(16,16j)	0,16,32,12,28,8,24,4,20	9
μ(32,32j)	0,32,28,24,20,16,12,8,4	9
μ(64,64j) = μ(28,28j)	0,28, 20,12,4,32,24,16,8	9
μ(128,128j) = μ(20,20j)	0,20,4,24,8,28,12,32,16	
μ(256,256j) = μ(4,4j) REPEAT	NO NEW MAPPINGS - STOP	

In this example we can see that this change in definition of the index m_L made quite a difference in that the left commutation semigroups act in a very similar, yet quite distinct, way. We found here that $\Lambda(D_{36})$ has 81 distinct elements and that the $\mu-$containers' parameters repeat after eight multiplications, compared to five when we were looking at the right. Aside from this being interesting in being another example that $\left|\mathrm{P}(G)\right| \neq \left|\Lambda(G)\right|$, we do see that we can construct a formula for the order of $\Lambda(D_n)$ in the same manner that we constructed one for $\mathrm{P}(G)$.■

Because these are again, powers of two, we notice that the $\mu-$containers here have similar orders to those we calculated in their right commutation counterparts and that we can use the same logic applied in our proof of lemma 3.4 to determine the orders of the μ containers of the left commutation semigroups. We observe the same halving of the orders of each $\mu-$container until we once again reach a point where no more halving can occur because no more powers of two can be factored out of *n*. We also observe the same orders appearing for the same types of numbers as in lemma 3.4. We make a small modification and we have:

Lemma 4.2: Let D_n be a dihedral group where $n = 2^r s, s > 1$ with mapping $\mu(i, j)$ as defined in Section 2. Then for some fixed positive integer *l* :

$$\left|\left\{\mu(q, 2^l j) : j \in \mathbb{Z}^+\right\}\right| = \begin{cases} \dfrac{n}{2^l} & l \le r \\ s & otherwise \end{cases}$$

□

We can now start constructing the formula for $\left|\Lambda(D_n)\right|$. On top, we have $\mu(0, 2j)$ so using lemma 4.2 with *q = 0*, we have $\mu(0, 2j)$ containing $n/2$ $\mu-$mappings and thus far, we have:

$$\left|\Lambda(D_n)\right| = \frac{n}{2} + \cdots \qquad (*)$$

Using similar reasoning to that of the right, we have *r* containers of the form $\mu(2, 2j)$, $\mu(2^2, 2^2 j)$, $\mu(2^3, 2^3 j)$, ..., $\mu(2^k, 2^k j)$ each containing their own $\frac{n}{2}$, $\frac{n}{4}$,..., $\frac{n}{2^r}$ $\mu-$mappings, by lemma 4.2 with $q = 1, 2, \ldots, r$. These containers thus add $\frac{n}{2} + \frac{n}{4} + \ldots + \frac{n}{2^r} = \sum_{i=1}^{r} \frac{n}{2^i}$ $\mu-$mappings to $\Lambda(D_n)$. Amending equation (*), we get:

$$\left|\Lambda(D_n)\right| = \frac{n}{2} + \sum_{i=1}^{r} \frac{n}{2^i} + \ldots \qquad (**)$$

In the same manner that we approached the right commutation semigroups, we know that $\{\mu(2^l, 2^l j) : j \in \mathbb{Z}_n, l \in \mathbb{Z}^+\}$ has $m_L - 1$ $\mu-$containers as elements and that we have accounted for *r* of them already. We thus conclude that there are $(m_L - 1) - k$ of these $\mu-$containers left to consider. Because each of them have parameters not dividing $n = 2^r s$, each $\mu-$container contains *s* $\mu-$mappings by lemma 4.2. Thus all such $\mu-$containers contribute $s(m_L - 1 - r)$ elements to $\Lambda(D_n)$. Adding this to equation (**), we have shown:

$$\left|\Lambda(D_n)\right| = \frac{n}{2} + \sum_{i=1}^{r} \frac{n}{2^i} + s(m_L - 1 - r)$$

Using a well-known series $\sum_{i=1}^{r}\frac{1}{2^i}=\frac{2^r-1}{2^r}$, we can simplify this equation as

$$\left|\Lambda(D_n)\right|=\frac{n}{2}+\sum_{i=1}^{r}\frac{n}{2^i}+s(m_L-1-r)=\frac{2^r s}{2}+2^r s\frac{\left(2^r-1\right)}{2^r}+s\left(m_L-1-r\right)=s\left(2^{r-1}+2^r-2\right)+s\left(m_L-r\right)$$

This is true if $s>1$. If $s=0$, however, we have $m_R=r$ and:

$$\left|\Lambda(D_n)\right|=s(2^r+2^{r-1}-2)+s(m_L-r)=2^r+2^{r-1}-2+(r-r)=2^r+2^{r-1}-2$$

This is again exactly the formula proved by C.D. Levy. Therefore, we have now proved:

Theorem 4.3: Let D_n be a dihedral group where $n=2^r s$ ($r>0, s>0$ is odd) and let m_L be defined as above. Then $\left|\Lambda(D_n)\right|=s(2^r+2^{r-1}-2)+s(m_L-r)$.

Appendix A: Proofs

Lemma 2.1: For every $i,i',j,j' \in \mathbb{Z}_n$, $\mu(i,j) = \mu(i',j')$ if and only if $i = i'$ and $j = j'$.

Proof: First suppose that $i = i'$ and $j = j'$ then it is trivially true that $\mu(i,j) = \mu(i',j')$.

Conversely, suppose that $\mu(i,j) = \mu(i',j')$. Then $(a)\mu(i,j) = (a)\mu(i',j')$ and $a^i = a^{i'}$ and thus $i = i'$. Suppose that $i = 0 = i'$ then $(b)\mu(0,j) = (b)\mu(0,j')$ and $a^j = a^{j'}$ and thus $j = j'$.

□

Lemma 2.2: For all $i,i',j,j' \in \mathbb{Z}_n$, $\mu(i,j)\mu(i',j') = \mu(ii', ji')$

Proof: If $g = a^k$ then $(a^k)\mu(i,j)\mu(i',j') = (a^{ki})\mu(i',j') = a^{kii'} = (a^k)\mu(ii', ji')$.

If $g = a^k b$ then $a^k b\mu(i,j)\mu(i',j') = a^{ki+j}\mu(i',j') = a^{(ki+j)i'} = a^{kii'+ji'} = a^k b\mu(ii', ji')$

□

Lemma 2.3: For all $j \in \mathbb{Z}_n$ $\rho_{a^{-j}} = \mu(0,-2j)$ and $\rho_{ba^{-j}} = \mu(-2,-2j)$

Proof: Let $g \in G$.

If $g = a^k$ then $(a^k)\mu(0,-2j) = a^{k0} = a^0 = 1$.

Also, $(a^k)\rho_{a^{-j}} = [a^k, a^{-j}] = 1 = (a^k)\mu(0,-2j)$.

If $g = ba^k$ then $(ba^k)\mu(0,-2j) = a^{k0-2j} = a^{-2j}$.

Also, $(ba^k)\rho_{a^{-j}} = \left[ba^k, a^{-j}\right] = a^{-k}ba^j ba^k a^{-j} = a^{-k}(a^j)^b a^{k-j} = a^{-k}a^{-j}a^{k-j}$

$= a^{-2j} = (ba^k)\mu(0,-2j)$.

Thus, $\rho_{a^{-k}} = \mu(0,-2j)$.

Similarly, if $g = a^k$, $(a^k)\mu(-2,-2j) = a^{-2j}$.

Also, $(a^k)\rho_{ba^{-j}} = \left[a^k, ba^{-j}\right] = a^{-k}a^j ba^k ba^{-j} = a^{-k}a^j(a^k)^b a^{-j}$

$= a^{-k}a^j a^{-k}a^{-j} = a = a^{-2j}$.

If $g = ba^k$, $(ba^k)\mu(-2,-2j) = a^{-2k-2j}$.

Also,

$(ba^k)\rho_{ba^{-j}} = \left[ba^k, ba^{-j}\right] = a^{-k}ba^j bba^k ba^{-j} = a^{-k}(a^{j+k})^b a^{-j}$

$= a^{-j-k}a^{-j} = a^{-2k-2j} = (ba^k)\mu(-2,-2j)$

Thus, $\rho_{ba^{-j}} = \mu(-2,-2j)$.

□

Lemma 2.4: For all $j \in \mathbb{Z}_n$ $\lambda_{a^{-j}} = \mu(0,2j)$ and $\lambda_{ba^{-j}} = \mu(2,2j)$

Proof: Let $g \in G$.

If $g = a^k$ then $\mu(0,2j) = a^{k0} = a^0 = 1$.

Also, $(a^k)\lambda_{a^{-j}} = \left[a^{-j}, a^k\right] = a^j a^{-k} a^{-j} a^k = a^{j-k-j+k} = a^0 = 1 = (a^k)\mu(0,2j)$.

If $g = ba^k$ then $(ba^k)\mu(0,2j) = a^{k0+2j} = a^{2j}$.

Also, $(ba^k)\lambda_{a^{-j}} = \left[a^{-j}, ba^k\right] = a^j a^{-k} ba^{-j} ba^k = a^j a^{-k} (a^{-j})^b a^k = a^j a^{-k} a^j a^k$

$= a^{2j} = (ba^k)\mu(i,j)$

Thus, $\lambda_{a^{-j}} = \mu(0,2j)$.

Similarly, if $g = a^k$ then $(a^k)\mu(2,2j) = a^{2k}$.

Also, $(a^k)\lambda_{ba^{-j}} = \left[ba^{-j}, a^k\right] = a^j ba^{-k} ba^{-j} a^k = a^j (a^{-k})^b a^{-j} a^k = a^j a^k a^{-j} a^k$

$= a^{2k} = (a^k)\mu(2,2j)$.

If $g = ba^k$ then $(ba^k)\mu(2,2j) = a^{2k+2j}$.

Also, $\lambda_{ba^{-j}} = \left[ba^{-j}, ba^k\right] = a^j ba^{-k} bba^{-j} ba^k = a^j (a^{-k})^b (a^{-j})^b a^k$

$= a^j a^k a^j a^k = a^{2k+2j} = (ba^k)\mu(2,2j)$.

Thus, $\lambda_{ba^{-j}} = (ba^k)\mu(2,2j)$.

□

Lemma 1: For all $a,b,d \in \mathbb{Z}_n$, $\mu(d,a)\mu(0,b) = \mu(0,0)$.

Proof: Let $a,b \in \mathbb{Z}_n$ then by Lemma 2.2, $\mu(d,a)\mu(0,b) = \mu(d \times 0, a \times 0) = \mu(0,0)$

□

Lemma 2.5: Every element of $\mathrm{P}(D_n)$ is of the form $\mu(0,-2j)$ or $\mu((-2)^l,(-2)^l j)$ for some $j \in \mathbb{Z}_n$.

Proof: By Lemma 2.3, $\rho_g = \mu(0,-2j)$ or $\rho_g = \mu(-2,-2j)$ for all $g \in D_n$. To look at each element of $\mathrm{P}(D_n)$, we look at all possible products (by lemma 2.2) of these ρ's.

By lemma 1, For any $r,s \in \mathbb{Z}_n$, $\mu(0,-2r)\mu(0,-2s) = \mu(0,0) = \mu(0,-2j)$ for $j = 0$.

For any $r,s \in \mathbb{Z}_n$, $\mu(0,-2r)\mu(-2,-2s) = \mu(0 \times -2, -2 \times -2s) = \mu(0,(-2)^2 s) = \mu(0,(-2)^l j)$ for $l = 2$ and $j = s$.

By lemma 1, For any $r,s \in \mathbb{Z}_n$, $\mu(-2,-2r)\mu(0,-2s) = \mu(0,0) = \mu(0,-2j)$ for $j = 0$.

For any $r,s \in \mathbb{Z}_n$, $\mu(-2,-2r)\mu(-2,-2s) = \mu((-2)^2,(-2)^2 r) = \mu((-2)^l,(-2)^l j)$ for $j = 0$ and $l = 2$.

□

Lemma 2.6: Every element of $\Lambda(D_n)$ is of the form $\mu(0,2j)$ or $\mu(2^l,2^l j)$ for some $j \in \mathbb{Z}_n$.
Proof: By Lemma 2.4, $\lambda_g = \mu(0,2j)$ or $\lambda_g = \mu(2,2j)$ for all $g \in D_n$. To look at each element of $\Lambda(D_n)$, we look at all possible products (by lemma 2.2) of these λ's.
By lemma 1, For any $r,s \in \mathbb{Z}_n$, $\mu(0,2r)\mu(0,2s) = \mu(0,0) = \mu(0,2j)$ for $j = 0$.
For any $r,s \in \mathbb{Z}_n$, $\mu(0,2r)\mu(2,2s) = \mu(0\times 2, 2\times 2s) = \mu(0,2^2 s) = \mu(0,2^l j)$ for $l = 2$ and $j = s$.
By lemma 1, For any $r,s \in \mathbb{Z}_n$, $\mu(2,2r)\mu(0,2s) = \mu(0,0) = \mu(0,2j)$ for $j = 0$.
For any $r,s \in \mathbb{Z}_n$, $\mu(2,2r)\mu(2,2s) = \mu(2^2,2^2 r) = \mu(2^l,2^l j)$ for $j = 0$ and $l = 2$.

□

Lemma 3.1: For any $A,B,C,D \in \mathbb{Z}_n$, $\mathcal{C}(A,B) \cap \mathcal{C}(C,D) = \varnothing$ if, and only if, $A \neq C$.
Proof: Let $A,B,C,D \in \mathbb{Z}_n$
First suppose that $A = C$. Then $\mathcal{C}(C,D) = \mathcal{C}(A,D)$. Then $\mu_0 = \mu(A,0) \in \mathcal{C}(A,B)$ because $\mu(A,0) = \mu(A,Bi)$ for $i = 0$. Similarly, $\mu_0 \in \mathcal{C}(A,D) = \mathcal{C}(C,D)$. So $\mu_0 \in \mathcal{C}(A,B) \cap \mathcal{C}(C,D) \neq \varnothing$.
Conversely, suppose that $\mathcal{C}(A,B) \cap \mathcal{C}(C,D) \neq \varnothing$ and let $\mu_0 \in \mathcal{C}(A,B) \cap \mathcal{C}(C,D)$. Then $\mu_0 = \mu(A,Bi) = \mu(C,Dj)$ for some $i,j \in \mathbb{Z}_n$. Then $(a)\mu(A,Bi) = (a)\mu(C,Dj)$ iff $a^A = a^B$ iff $A = B$.

□

Lemma 2: If x,y are coprime positive integers, then for every $u,v \in \mathbb{Z}$, $xu \equiv xv \pmod{xy}$ if and only if $u \equiv v \pmod{y}$.
Proof: First suppose that $xu = xv \pmod{xy}$. Then $x(u-v) \equiv 0 \pmod{xy}$. Thus there exists a $t \in \mathbb{Z}$ such that $x(u-v) = txy$. If $u - v = 0$ then $u = v$ and it follows that $u = v \pmod{y}$. If $u - v \neq 0$ then $u - v = ty$ and thus $u \equiv v \pmod{y}$.
Conversely suppose that $u \equiv v \pmod{y}$. Then there exists $t \in \mathbb{Z}$ such that $u - v = ty$. Thus $x(u-v) = txy$ and $xu = xy \pmod{xy}$.

□

Lemma 3.2: There exists a positive integer $k > r$ such that $(-2)^r = (-2)^k \pmod{n}$.
Proof: Consider the powers of (-2) modulo s. Since s is odd and $-2 \equiv s - 2 \pmod{s}$, s is coprime to -2 and therefore -2 is invertible modulo s and the powers of -2 form a subgroup of the multiplicative semigroup $\mathbb{Z}_s$. There is then a least positive integer t for which $(-2)^t = 1 \pmod{s}$. It follows then by Lemma 2 that $(-2)^{r+t} = (-2)^r(-2)^t \equiv (-2)^r \pmod{2^r s}$. Letting $k = r + t$, we are done.

□

Lemma 3.3: There are $m_R - 1$ distinct $((-2)^l, (-2)^l) - \text{containers}$, for $l \in \mathbb{Z}^+$.
Proof: To show that, for $n = 2^r s$, there are exactly $m_R - 1$ distinct $((-2)^l, (-2)^l) - \text{containers}$, it will suffice to show that :
$(-2)^1, (-2)^2, \ldots, (-2)^{m_R - 1}$ are all distinct, and
$(-2)^t = (-2)^i (n)$ for some $t > m_R - 1$ and some $i \leq m_R - 1$. That is, any power of negative two larger than $m_R - 1$ gives us an already generated parameter for a container.

Firstly, BWOC suppose that there exists integers p, q such that $1 \leq p < r \leq m_R - 1$ such that $(-2)^r = (-2)^p (n)$. However, $p < m_R$, contradicting the fact that m_R is the least integer such that $(-2)^r = (-2)^{m_R} (n)$.

Secondly, suppose that $t \geq m_R > m_R - 1$ is an integer such that for some non-negative integer k, $t = m_R + k$. Define now a positive integer $\pi = m_R - r$. Because m_R is the first power at which $2^r = 2^{m_R} (n)$, π can be interpreted a periodic measure and thus for any positive integer a: $2^{m_R + a\pi} = 2^{m_R} (n)$. By the Quotient-Remainder Theorem, we know that there exist integers a, q ($0 \leq q < \pi$) such that $k = a\pi + q$. Then $2^t = 2^{m_R + k} = 2^{m_R + a\pi + q} = 2^{m_R + q} (n) = 2^{r+q} (n)$. Also, $q < m_R - r = \pi$ and so $r + q \leq m_R - 1 < m_R$ and thus $2^t = 2^i (n)$ for some $1 \leq i = r + q \leq m_R - 1$.

□

Lemma 4.1: There exists a positive integer $k > r$ such that $2^r = 2^k (\text{mod}\, n)$.
Proof: Consider the powers of 2 modulo s. Since s is odd, s is coprime to 2 and therefore 2 is invertible modulo s and the powers of 2 form a subgroup of the multiplicative semigroup $\mathbb{Z}_s$. There is then a least positive integer t for which $2^t = 1 (\text{mod}\, s)$. It follows then by Lemma 2 that $2^{r+t} = 2^r 2^t \equiv 2^r (\text{mod}\, 2^r s)$. Letting $k = r + t$, we are done.

□

n	$\|P(D_n)\|$	$\|\Lambda(D_n)\|$
3	6	9
4	4	4
5	25	25
6	6	9
7	49	28
8	10	10
9	36	63
10	25	25
11	66	121
12	15	18
13	169	169
14	49	28
15	75	75
16	22	22
17	153	153
18	36	63
19	190	361
20	40	40
21	147	147
22	66	121
23	529	276
24	33	36
25	525	525
26	169	169
27	270	513
28	70	49
29	841	841
30	75	75
31	341	186
32	46	46
33	198	363
34	153	153
35	455	455

References

[1] Gupta, N. D., 'On commutation semigroups of a group', *J . Austral. Math. Soc.* **6** (1966), 36-45.

[2] Levy, C.D., 'Investigation of commutation semigroups of dihedral groups', Honours Thesis, *Mount Saint Vincent University* (2008).