On Commutation Semigroups of Dihedral Groups

Darien DeWolf[1] Charles Edmunds[2] Christopher Levy[3]

In Memory of Narain Gupta

1 Introduction

For any group G with $g \in G$, the right and left commutation mappings associated with g are the mappings $\rho(g)$ and $\lambda(g)$ from G to G defined as

$$(x)\rho(g) = [x, g] \text{ and } (x)\lambda(g) = [g, x],$$

where the commutator of g and h is defined as $[g, h] = g^{-1}h^{-1}gh$. The set $\mathcal{M}(G)$ of all mappings from G to G forms a semigroup under composition of mappings. The *right commutation semigroup of* G, $\mathrm{P}(G)$, is the subsemigroup of $\mathcal{M}(G)$ generated by the set of *ρ-maps*, $\mathrm{P}_1(G) = \{\rho(g) : g \in G\}$, and *the left commutation semigroup of* G, $\Lambda(G)$, is the subsemigroup of $\mathcal{M}(G)$ generated by the set of *λ-maps*, $\Lambda_1(G) = \{\lambda(g) : g \in G\}$. If G is abelian the commutation semigroups are trivial semigroups consisting of one mapping sending each element of G to the identity element. We will study $\mathrm{P}(G)$ and $\Lambda(G)$ only when G is non-abelian.

In this paper we will discuss the commutation semigroups of dihedral groups. The dihedral group of order $2m$ has presentation

$$D_m = \left\langle a, b; a^m = 1, b^2 = 1, a^b = a^{-1} \right\rangle,$$

where the conjugate of a by b is denoted $a^b = b^{-1}ab$. Each element of D_m can be written uniquely in the form $a^i b^j$ with $i \in \mathbb{Z}_m$ and $j \in \mathbb{Z}_2$. Since D_3 is the smallest non-abelian dihedral group, we will assume, henceforth, that $m \geq 3$. Our primary goal is to develop explicit formulas for the orders of $\mathrm{P}(G)$ and $\Lambda(G)$.

In the mid-1960s B.H. Neumann pointed out to N.D. Gupta (oral communication) that $|\mathrm{P}(D_3)| = 6$ but $|\Lambda(D_3)| = 9$. One might have thought, at first glance, that the left and right commutator semigroups would be isomorphic. However, the smallest nonabelian group yields a counterexample and this raised the question of how these two semigroups are related. In [3], Gupta characterized those dihedral groups for which $\mathrm{P}(G)$ and $\Lambda(G)$ are isomorphic. He then went on to study the question of isomorphism for nilpotent groups, finding that, for groups of class 2, 3, and 4, one has $\mathrm{P}(G) = \Lambda(G)$, $\mathrm{P}(G) \cong \Lambda(G)$, and $|\mathrm{P}(G)| = |\Lambda(G)|$, respectively. He then gave an example of a class 5 group for which the commutation semigroups are not isomorphic. The question of whether $\mathrm{P}(G) \cong \Lambda(G)$ for class 4 groups is still open.

In the mid-1960s the Neumanns were making significant contributions to variety theory and it is reasonable to suppose that the purpose of the study of commutation semigroups was to further the understanding of the varieties of the groups with which they are associated. By interpreting the

[1]Mathematics Department, Dalhousie University, Halifax, Nova Scotia , Canada, B3H 4R2
[2]Mathematics Department, Mount Saint Vincent University, Halifax, Nova Scotia, Canada, B3M 2J6
[3]Mathematics Department, Dalhousie University, Halifax, Nova Scotia , Canada, B3H 4R2

group multiplication as (noncommutative) addition, Gupta [4] also studied these semigroups as the multiplicative structures of commutation near rings.

In 1970 James Countryman [1] wrote his Ph.D. thesis at the University of Notre Dame on the commutation semigroups of pq groups for p and q distinct primes with $p < q$. Each nonabelian pq group is a split extension of a cyclic group of order q by a cyclic group of order p. Among his results were the following:

Theorem C1 If G is a pq group the following statements are equivalent:

(a) $\mathrm{P}(G) = \Lambda(G)$,

(b) $\mathrm{P}(G) \cong \Lambda(G)$,

(c) $|\mathrm{P}(G)| = |\Lambda(G)|$.

Theorem C2 If G_1 and G_2 are pq groups, then $\mathrm{P}(G_1) \cong \mathrm{P}(G_2)$ implies $G_1 \cong G_2$.

Theorem C3 If G is a $2q$ group, then $\mathrm{P}(G) \subseteq \Lambda(G)$ or $\Lambda(G) \subseteq \mathrm{P}(G)$, or both.

Since the non-abelian $2q$ groups are among the dihedral groups, one might conjecture that these results hold for all dihedral groups. In the case of Theorem C1 it is clear, for any group, that $(a) \Rightarrow (b) \Rightarrow (c)$. We will show that, for dihedral groups in general, $(c) \not\Rightarrow (a)$, $(b) \not\Rightarrow (a)$, and $(c) \not\Rightarrow (b)$ On the positive side, we will derive Theorem 23, a left commutation semigroup version of Theorem C2. We note as well that Theorem C2, our Theorem 23, and Theorem C3 do not hold for dihedral groups in general.

The difficulty in identifying the elements of $\mathrm{P}(G)$ and $\Lambda(G)$ is that, although the generating sets $\mathrm{P}_1(G)$ and $\Lambda_1(G)$ are clearly defined, these generators must be multiplied together (composed) repeatedly to form the full set of mappings in $\mathrm{P}(G)$ and $\Lambda(G)$. We will develop a method which gives more control over this process than has been possible previously. The method evolved as joint work while the second author supervised the Honours Theses of the first and third authors at Mount Saint Vincent University. Their work was complementary, each author giving formulas for the orders of $\mathrm{P}(D_m)$ and $\Lambda(D_m)$; Levy for m odd or m a power of 2 and DeWolf for m even.

Theorem L1 (Levy [5]) If m is odd, then

(i) $|\mathrm{P}(D_m)| = m(ind_R(m) + 1)$, where $ind_R(m) = \min\left\{i \in \mathbb{Z}^+ : (-2)^i \equiv 1 \ (\mathrm{mod} m)\right\}$,

(ii) $|\Lambda(D_m)| = m(ind_L(m) + 1)$, where $ind_L(m) = \min\left\{i \in \mathbb{Z}^+ : 2^i \equiv 1 \ (\mathrm{mod} m)\right\}$.

Theorem L2 (Levy [5]) If $m = 2^\ell$, then $|\mathrm{P}(D_m)| = |\Lambda(D_m)| = 2^\ell + 2^{\ell-1} - 2$.

Theorem D (DeWolf [2]) If $m = 2^\ell n$ with n odd and $\ell, n \in \mathbb{Z}^+$,then

(i) $|\mathrm{P}(D_m)| = n(2^\ell + 2^{\ell-1} - 2 + m_R - \ell)$, where
$m_R = \min\left\{i > \ell : (-2)^i \equiv (-2)^\ell \ (\mathrm{mod} m)\right\}$ if n > 1, and $m_R = \ell$ if n $= 1$,

(ii) $|\Lambda(D_m)| = n(2^\ell + 2^{\ell-1} - 2 + m_L - \ell)$, where
$m_L = \min\left\{i > \ell : 2^i \equiv 2^\ell \ (\mathrm{mod} m)\right\}$ if n > 1, and $m_L = \ell$ if n $= 1$.

These formulas were used to generate the table at the end of this paper giving orders of the left and right commutation semigroups for D_m $(3 \leq m \leq 101)$. The formulas in Theorems L2 and D do have some similarities, but it is unsatisfying to have such different looking formulas for the various types of dihedral groups. It is possible, however, to give one formula each for the orders of $\mathrm{P}(D_m)$ and $\Lambda(D_m)$. This formula involves the orders of the terms of the upper central series of D_m, thereby hinting at the value of a more group theoretical approach to the questions surrounding commutation semigroups. We will prove the following formulas and derive the results of Levy and DeWolf from them.

Theorem 21 If $m = 2^\ell n > 3$ with n odd,

(i) $|\mathrm{P}(D_m)| = m\left(\frac{1}{|Z_1|} + \sum_{i=1}^{t-1}\frac{1}{|Z_i|}\right)$, where $t = \begin{cases} 1 + ord_m(-2) \text{ for } \ell = 0,\ n > 1 \\ \ell + per_m(-2) \text{ for } \ell > 0,\ n > 1 \\ \ell \text{ for } \ell > 0,\ n = 1 \end{cases}$,

(ii) $|\Lambda(D_m)| = m\left(\frac{1}{|Z_1|} + \sum_{i=1}^{t'-1}\frac{1}{|Z_i|}\right)$, where $t' = \begin{cases} 1 + ord_m(2) \text{ for } \ell = 0,\ n > 1 \\ \ell + per_m(2) \text{ for } \ell > 0,\ n > 1 \\ \ell \text{ for } \ell > 0,\ n = 1 \end{cases}$,

where Z_i is the i^{th} centre of D_m, that is, the i^{th} term of the upper central series.

In Section 2 we develop the initial ideas and notation used throughout the paper. Section 3 introduces containers, a method of binding the commutation mappings together into natural units. These containers actually form a quotient semigroup of a natural subsemigroup of $\mathcal{M}(G)$ implicit in Gupta [3]. Rather than working with individual mappings, we will show how these containers can be multiplied repeatedly to generate $\mathrm{P}(D_m)$ and $\Lambda(D_m)$. In Section 4 we calculate the cardinality of each container in terms of the upper central series. In Section 5 we state and prove our main theorem and give two applications. In Section 6 we show how to use our methods to derive the formulas of Levy and DeWolf and discuss possible generalizations of Countrymans theorems to all dihedral groups. It is hoped that this will show the merit of our approach to the reader.

2 Preliminaries

The fundamental concepts developed in this section are parallel to those developed by N.D. Gupta in [3]. Many of these ideas are explicitly or implicitly his.

The following commutator identities are easily verified by expansion.

Theorem CI If G is any group and $x, y, z \in G$ then

(i) $x^y = x[x, y]$,

(ii) $[y, x] = [x, y]^{-1}$,

(iii) $[xy, z] = [x, z]^y[y, z] = [x, z][x, z, y][y, z]$,

(iv) $[x, yz] = [x, z][x, y]^z = [x, z][x, y][x, y, z]$,

(v) $[x^{-1}, y] = [x, y]^{-x^{-1}}$. □

Note. For any group G and $a, b \in G$, we denote both $(a^{-1})^b$ and $(a^{-1})^b$ by a^{-b}. This is unambiguous since $(a^{-1})^b = b^{-1}a^{-1}b = (b^{-1}ab)^{-1} = (a^b)^{-1}$.

Notation. For each $s \geq 0$ let $\alpha_s = (-1)^s$ and $\beta_s = (-1)^s - 1$. Since the values of α_s and β_s are unique up to parity, it will cause no ambiguity to view s as an element of $\mathbb{Z}_2$.

We begin by calculating an explicit formula for each ρ- and λ-map.

Lemma 1. *Let D_m be the dihedral group with presentation as above. For each $i, r \in \mathbb{Z}_m$ and $j, s \in \mathbb{Z}_2$:*

$$(a^i b^j)\rho(a^r b^s) = a^{N_\rho} \text{ and } (a^i b^j)\lambda(a^r b^s) = a^{N_\lambda},$$

where $N_\rho \equiv i\alpha_j\beta_s - r\alpha_s\beta_j \equiv (-2)\alpha_{js}(is - jr)(\mathrm{mod} m)$ and $N_\lambda \equiv -N_\rho \equiv 2\alpha_{js}(is - jr)(\mathrm{mod} m)$.

Proof. Applying CI *(ii)*, CI *(iii)*, and CI *(iv)* we have,

$$\begin{aligned}(a^ib^j)\rho(a^rb^s) &= [a^ib^j, a^rb^s] = [a^i, a^rb^s]^{b^j}[b^j, a^rb^s] \\ &= \left([a^i, b^s]^{b^j}[a^i, a^r]^{b^sb^j}\right)\left([b^j, b^s][b^j, a^r]^{b^s}\right) \\ &= [a^i, b^s]^{b^j}[b^j, a^r]^{b^s} = [a^i, b^s]^{(-1)^j}\left([a^r, b^j]^{-(-1)^s}\right) \\ &= \left(a^{-i}(a^i)^{b^s}\right)^{(-1)^j}\left(a^{-r}(a^r)^{b^j}\right)^{-(-1)^s} \\ &= \left(a^{-i}(a^i)^{(-1)^s}\right)^{(-1)^j}\left(a^{-r}(a^r)^{(-1)^j}\right)^{-(-1)^s} \\ &= a^{i(-1+(-1)^s)(-1)^j - r(-1+(-1)^j)(-1)^s} = a^{N_\rho},\end{aligned}$$

where $N_\rho \equiv i\beta_s\alpha_j - r\beta_j\alpha_s$, as required. Checking each of the four cases for $(j, s) \in \mathbb{Z}_2^2$, we also see that $N_\rho \equiv (-2)\alpha_{js}(is - jr) (\mathrm{mod} m)$. The first part of the lemma can be used to prove the second part.

$$(a^ib^j)\lambda(a^rb^s) = [a^rb^s, a^ib^j] = (a^rb^s)\rho(a^ib^j) = a^{r\beta_j\alpha_s - i\beta_s\alpha_j} = a^{-N_\rho} = a^{N_\lambda}. \qquad \square$$

Definition. For each pair $(A, B) \in \mathbb{Z}_m \times \mathbb{Z}_m$ we define a μ-map $\mu(A, B) : D_m \to D_m$ by

$$(a^ib^j)\mu(A, B) = a^{N_\mu}, \text{ where } N_\mu = Ai\alpha_j - B\beta_j.$$

Each ρ- and λ-map can be identified as one of these μ-maps.

Lemma 2. *For each $r \in \mathbb{Z}_m$ and $s \in \mathbb{Z}_2$,*

(i) $\rho(a^rb^s) = \mu(\beta_s,\ r\alpha_s)$,

(ii) $\lambda(a^rb^s) = \mu(-\beta_s, -r\alpha_s)$.

Proof. $(a^ib^j)\mu(\beta_s,\ r\alpha_s) = a^N$, where $N \equiv (\beta_s)i\alpha_j - (r\alpha_s)\beta_j$. By Lemma 1 $(a^ib^j)\rho(a^rb^s) = a^{N_\rho}$ with $N_\rho \equiv i\alpha_j\beta_s - r\alpha_s\beta_j (\mathrm{mod}\, m)$. Since $N \equiv N_\rho$, *(i)* follows. To prove *(ii)*, consider $(a^ib^j)\mu(-\beta_s, -r\alpha_s) = a^{N'}$ where $N' \equiv (-\beta_s)i\alpha_j - (r(-\alpha_s))\beta_j \equiv r\alpha_s\beta_j - \beta_si\alpha_j$. By Lemma 1 $(a^ib^j)\lambda(a^rb^s) = a^{r\beta_j\alpha_s - i\beta_s\alpha_j}$, thus *(ii)* is established. $\square$

Lemma 3. *For each $A, A' \in \mathbb{Z}_m$ and $B, B' \in \mathbb{Z}_2$, $\mu(A, B) \circ \mu(A', B') = \mu(AA', BA')$.*

Proof. First note that $(a^ib^j)\mu(A, B) = a^N$, where $N \equiv Ai\alpha_j - B\beta_j$. Thus

$$(a^ib^j)(\mu(A, B) \circ \mu(A', B')) = (a^Nb^0)\mu(A', B') = a^{N'},$$

where $N' \equiv A'N\alpha_0 - B'\beta_0 \equiv A'N \equiv (Ai\alpha_j - B\beta_j)A' \equiv AA'i\alpha_j - BA'\beta_j$. On the other hand, $(a^ib^j)\mu(AA', BA') = a^{N''}$, where $N'' \equiv AA'i\alpha_j - BA'\beta_j$. The lemma follows. $\square$

Although compositions of ρ-maps (λ-maps) may not be ρ-maps (λ-maps), it follows from Lemma 3 that compositions of μ-maps are μ-maps. Closing the sets $\mathrm{P}_1(D_m)$ and $\Lambda_1(D_m)$ under multiplication to form semigroups will be facilitated by identifying the ρ-maps and λ-maps as μ-maps. Note also that the μ-maps form a subsemigroup, $\mathrm{M}(D_m)$, of $\mathcal{M}(D_m)$, and since $\mathrm{P}_1(D_m), \Lambda_1(D_m) \subseteq M(D_m)$, we have $\mathrm{P}(D_m), \Lambda(D_m)$ are subsemigroups of $\mathrm{M}(D_m)$. Thus $|\mathrm{M}(D_m)| = m^2$ is an upper bound on the orders of both $\mathrm{P}(D_m)$ and $\Lambda(D_m)$.

3 Containers

Viewed as μ-maps, the mappings in $\mathrm{P}(D_m)$ and $\Lambda(D_m)$ naturally bond together into sets with one parameter running over $\mathbb{Z}_m$.

Definition. If $A, B \in \mathbb{Z}_m$, the (A, B)-*container* is defined as

$$\mathcal{C}(A, B) = \{\mu(A, xB) : x \in \mathbb{Z}_m\}.$$

For $r \in \mathbb{Z}_m$ and $s \in \mathbb{Z}_2$, Lemma 2 implies that $\rho(a^r b^s) = \mu(\beta_s, r\alpha_s) \in \mathcal{C}(\beta_s, r\alpha_s)$. Since r is a parameter running through $\mathbb{Z}_m$, we can simplify this by writing $\rho(a^r b^s) \in \mathcal{C}(\beta_s, \alpha_s)$. Similarly, we can write $\lambda(a^r b^s) \in \mathcal{C}(-\beta_s, -\alpha_s)$. Thus our generating maps are in easily identified containers.

Lemma 4. *If $A, B, B' \in \mathbb{Z}_m$ and B is invertible in $\mathbb{Z}_m$, then $\mathcal{C}(A, BB') = \mathcal{C}(A, B')$.*

Proof. Since B is invertible in $\mathbb{Z}_m$, $\mathbb{Z}_m B = \mathbb{Z}_m$. That is,

$$\{0B, 1B, \ldots, (m-1)B\} = \{0, 1, \ldots, m-1\}.$$

We then have that

$$\begin{aligned}\mathcal{C}(A, BB') &= \{\mu(A, 0B \cdot B'), \mu(A, 1B \cdot B'), \ldots, \mu(A, (m-1)B')\} \\ &= \{\mu(A, 0B'), \mu(A, 1B'), \ldots, \mu(A, (m-1)B')\} = \mathcal{C}(A, B').\end{aligned}$$ □

Lemma 5. *If $A, B, C \in \mathbb{Z}_m$, then $\mathcal{C}(A, BC) \subseteq \mathcal{C}(A, C)$.*

Proof. Let $\mu \in \mathcal{C}(A, BC)$, then there is an $x \in \mathbb{Z}_m$ with $\mu = \mu(A, xBC)$. Note that

$$\mu = \mu(A, xBC) = \mu(A, (xB)\, C)$$

and $xB \in \mathbb{Z}_m$; therefore $\mu \in \mathcal{C}(A, C)$. □

Lemma 6. *For all $A, A', B, B' \in \mathbb{Z}_m$, $\mathcal{C}(A, B) \cap \mathcal{C}(A', B') \neq \varnothing$ if and only if $A \equiv A' (\mathrm{mod} m)$.*

Proof. First suppose that $\mathcal{C}(A, B) \cap \mathcal{C}(A', B') \neq \varnothing$. It follows that there is a mapping $\mu \in \mathcal{C}(A, B)$ with $\mu \in \mathcal{C}(A', B')$ as well. We then conclude that there exist $x, y \in \mathbb{Z}_m$ such that $\mu = \mu(A, xB) = \mu(A', yB')$. Thus $(a)\mu(A, xB) = a^{Ai\alpha_j} = a^{A(1)(1)} = a^A$ and this must equal $(a)\mu(A', yB') = a^{A'}$. Thus it follows that $A \equiv A' \ (\mathrm{mod} m)$. Conversely, suppose that $A \equiv A' (\mathrm{mod} m)$. Then note that $\mu(A, 0) = \mu(A, 0B) \in \mathcal{C}(A, B)$, and $\mu(A, 0) = \mu(A, 0B') \in \mathcal{C}(A, B') = \mathcal{C}(A', B')$ since $A \equiv A'$. Therefore $\mu(A, 0) \in \mathcal{C}(A, B) \cap \mathcal{C}(A', B')$ and the intersection is nonempty. □

We can represent all ρ-maps and λ-maps as disjoint unions of containers as follows.

Lemma 7. $\mathrm{P}_1 = \mathcal{C}(0, 1) \,\dot\cup\, \mathcal{C}(-2, 1)$ *and* $\Lambda_1 = \mathcal{C}(0, 1) \,\dot\cup\, \mathcal{C}(2, 1)$.

Proof. For a fixed $s \in \mathbb{Z}_2$, Lemma 2 implies that,

$$\begin{aligned}\{\rho(a^x b^s) : x \in \mathbb{Z}_m\} &= \{\mu(\beta_s, x\alpha_s) : x \in \mathbb{Z}_m\} = \mathcal{C}(\beta_s, \alpha_s), \text{ and} \\ \{\lambda(a^x b^s) : x \in \mathbb{Z}_m\} &= \{\mu(-\beta_s, x(-\alpha_s)) : x \in \mathbb{Z}_m\} = \mathcal{C}(-\beta_s, -\alpha_s).\end{aligned}$$

Thus

$$\begin{aligned}\mathrm{P}_1 &= \{\rho(a^r b^s) : r \in \mathbb{Z}_m, s \in \mathbb{Z}_2\} = \{\rho(a^r) : r \in \mathbb{Z}_m\} \cup \{\rho(a^r b) : r \in \mathbb{Z}_m\} \\ &= \mathcal{C}(\beta_0, \alpha_0) \cup \mathcal{C}(\beta_1, \alpha_1) = \mathcal{C}(0, 1) \cup \mathcal{C}(-2, -1).\end{aligned}$$

Since -1 is invertible in $\mathbb{Z}_m$, Lemma 4 implies that $\mathcal{C}(-2, -1) = \mathcal{C}(-2, 1)$ and the result follows. The proof for Λ_1 is similar. Lemma 6 implies that both unions are disjoint. □

Instead of multiplying ρ-maps or λ-maps together repeatedly to find all the mappings in $\mathrm{P}(D_m)$ and $\Lambda(D_m)$, we can accomplish this more efficiently by multiplying containers.

Definition. For any two containers $\mathcal{C}(A,B)$ and $\mathcal{C}(A',B')$, we define their product as:

$$\mathcal{C}(A,B)\circ\mathcal{C}(A',B') = \{\mu_1\circ\mu_2 : \mu_1\in\mathcal{C}(A,B) \text{ and } \mu_2\in\mathcal{C}(A',B')\}.$$

Lemma 8. *For $A,A'\in\mathbb{Z}_m$ and $B,B'\in\mathbb{Z}_2$, $\mathcal{C}(A,B)\circ\mathcal{C}(A',B') = \mathcal{C}(AA',BA')$.*

Proof. For $\mu\in\mathcal{C}(A,B)\circ\mathcal{C}(A',B')$, we have $\mu=\mu_1\circ\mu_2$ with $\mu_1\in\mathcal{C}(A,B)$ and $\mu_2\in\mathcal{C}(A',B')$. Thus there exist $x,y\in\mathbb{Z}_m$ such that $\mu_1=\mu(A,xB)$ and $\mu_2=\mu(A',yB')$. Therefore, by Lemma 3, $\mu=\mu(AA',xBA')\in\mathcal{C}(AA',BA')$. On the other hand if $\mu\in\mathcal{C}(AA',BA')$, there is an $x\in\mathbb{Z}_m$ with $\mu=\mu(AA',xBA')$. But, by Lemma 3 again, $\mu(AA',xBA')=\mu(A,xB)\circ\mu(A',B')$, and it is clear that $\mu(A,xB)\in\mathcal{C}(A,B)$ and $\mu(A',B')=\mu(A',(1)B')\in\mathcal{C}(A',B')$. Therefore, $\mu\in\mathcal{C}(A,B)\circ\mathcal{C}(A',B')$ and the proof is complete. □

Although we will not use the fact here, it is interesting to note that the set of all containers endowed with this product forms a quotient semigroup of $M(D_m)$.

By Lemma 7, P_1 is the union of two containers. Forming all possible products with these two containers will produce containers holding all possible products of ρ-maps and, thus, express $\mathrm{P}(D_m)$ as a union of containers. Similarly the two containers holding the maps in Λ_1 can be multiplied repeatedly to generate $\Lambda(D_m)$. Before we generate these expressions, we take a few more preliminary steps.

Lemma 9. *For $A,B\in\mathbb{Z}_m$,*

(i) $\mathcal{C}(0,1)\circ\mathcal{C}(A,B)\subseteq\mathcal{C}(0,1)$,

(ii) $\mathcal{C}(A,B)\circ\mathcal{C}(0,1)\subseteq\mathcal{C}(0,1)$.

Proof. To establish part *(i)*, note that by Lemma 8,

$$\mathcal{C}(0,1)\circ\mathcal{C}(A,B)=\mathcal{C}(0\cdot A,1\cdot A)=\mathcal{C}(0,A)\subseteq\mathcal{C}(0,1).$$

The last containment follows by Lemma 5. Part *(ii)* also follows by Lemmas 8 and 5:

$$\mathcal{C}(A,B)\circ\mathcal{C}(0,1)=\mathcal{C}(A\cdot 0,B\cdot 0)=\mathcal{C}(0,0)\subseteq\mathcal{C}(0,1).$$ □

The following is a simple fact about congruences which we will use in several of the arguments below.

Lemma 10. *If x and y are positive integers, then for every $u,v\in\mathbb{Z}$, $xu\equiv xv\ (\mathrm{mod}xy)$ if and only if $u\equiv v\ (\mathrm{mod}y)$.*

Proof. Suppose first that $xu\equiv xv\ (\mathrm{mod}xy)$. Then $x(u-v)\equiv 0\ (\mathrm{mod}xy)$. 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 $u\equiv v\ (\mathrm{mod}y)$. If $u-v\neq 0$ then we obtain $u-v=ty$ by cancellation of x from both sides of $(*)$. Thus $u\equiv v\ (\mathrm{mod}y)$. Conversely, suppose that $u\equiv v\ (\mathrm{mod}y)$. It follows that there exists $t\in\mathbb{Z}$ such that $u-v=ty$. Thus $x(u-v)=txy$. Therefore $xu\equiv xv\ (\mathrm{mod}xy)$. □

It is well known that if S is a semigroup and $x\in S$, the positive powers of x, $\left\{x^i : i\in\mathbb{Z}^+\right\}$, form a subsemigroup of S called the *monogenic semigroup* generated by x, denoted $\langle x\rangle$. If S is finite, then for each $x\in S$ the powers of x begin to repeat at some point. Let c be the smallest positive integer such that there is a $k\in\mathbb{Z}^+$ with $x^c=x^{c+k}$ and k the least such positive integer. Here c and k are called the *index* and the *period* of x, and $\langle x\rangle=\left\{x^1,\ldots,x^{c+k-1}\right\}$ is the set of distinct powers of x.

When $S = \mathbb{Z}_m$ we denote the index and period of $x \in \mathbb{Z}_m$, by $ind_m(x)$ and $per_m(x)$ respectively. If $x \not\equiv 0$ and $ind_m(x) = 1$ then $x^{per_m(x)} \equiv 1 \pmod{m}$, $\langle x \rangle$ is the cyclic group of order $per_m(x)$, and this happens exactly when x is invertible in $\mathbb{Z}_m$. In this case we denote the order of x as an element of $(\mathbb{Z}_m, \cdot)$ by $ord_m(x)$.

The next result characterizes the indices for -2 and 2 in $\mathbb{Z}_m$ in terms of the number theoretic form of m. In some cases information about the period can also be given.

Lemma 11. *If $m = 2^\ell n \geq 3$ with n odd, $\ell \geq 0$, and $n \geq 1$, then for $x \in \{-2, 2\}$*

(i) if m is odd, then $ind_m(x) = 1$ and $per_m(x) = ord_m(x)$,

(ii) if m is even and $n > 1$, then $ind_m(x) = \ell$,

(iii) if m is even and $n = 1$, then $ind_m(x) = \ell$ and $per_m(x) = 1$.

Proof. We will give proofs of each part only for $x = -2$, since the proofs for $x = 2$ are quite similar.

Proof of (i). With m odd, it follows that -2 is invertible in $\mathbb{Z}_m$; thus it has an order, say $ord_m(-2) = k$. Thus we have $1 \equiv (-2)^k$ and hence, $(-2)^1 = (-2)^{1+k}$ and part *(i)* of the lemma follows easily.

Proof of (ii). With m even ($\ell > 0$) and $n > 1$, we know that -2 has an index and a period, say $ind_m(-2) = c$ and $per_m(-2) = k$. We wish to show that $c = \ell$. First suppose that $c < \ell$. We can rewrite $(-2)^c \equiv (-2)^{c+k} \pmod{m}$ as $(-1)^c 2^c \equiv (-1)^c 2^c (-2)^k \pmod{2^c 2^{\ell-c} n}$.

Applying Lemma 10 we have, $(-1)^c \equiv (-1)^c (-2)^k \pmod{2^{\ell-c} n}$. Multiplying on both sides by $(-1)^c$ we obtain $1 \equiv (-2)^k \pmod{2^{\ell-c} n}$. But this implies that -2 is invertible modulo $2^{\ell-c} n$ with $\ell - c > 0$. Since $\gcd(-2, 2^{\ell-c} n) = 2 \neq 1$, -2 is not invertible, and we have a contradiction. Now suppose that $c > \ell$. Since $n > 1$ is odd, $\gcd(n, -2) = 1$ and, therefore, -2 is invertible modulo n. Letting $r = ord_n(-2)$, we have $1 \equiv (-2)^r \pmod{n}$. By Lemma 10, $2^\ell = 2^\ell (-2)^k \pmod{2^\ell n}$. Multiplying on both sides by $(-1)^\ell$ gives $(-2)^\ell \equiv (-2)^{\ell+k} \pmod{m}$. But since $c > \ell$, this contradicts the minimality of the originally selected index, c. It follows that $\ell = c = ind_m(-2)$.

Proof of (iii). In this case we have $m = 2^\ell$. Note that

$$(-2)^\ell \equiv (-1)^\ell 2^\ell \equiv 0 \pmod{2^\ell}$$

and that for each $t \in \mathbb{Z}^+$, $(-2)^{\ell+t} \equiv 0 \pmod{2^\ell}$; thus $(-2)^\ell = (-2)^{\ell+1}$. We will argue that $ind_{2^\ell}(-2) = \ell$ and, consequently, $per_{2^\ell}(-2) = 1$. We will first prove that the terms in the sequence $(s) = \left((-2)^1, (-2)^2, \ldots, (-2)^\ell\right)$ are distinct modulo 2^ℓ. Once this is established, we will know that $(-2)^\ell$ is the only power of -2 in (s) which is congruent to 0. Thus if a higher power of -2 is congruent to a term of (s), it is congruent to $(-2)^\ell$ only. Once the terms of (s) are shown to be distinct, it is then impossible for $ind_m(-2) < \ell$, and the result follows.

To show that the terms in (s) are distinct, suppose that $0 < u < v \leq \ell$, but that $(-2)^u \equiv (-2)^v \pmod{2^\ell}$. We can rewrite this as

$$(-1)^u 2^u \equiv (-1)^u 2^u (-2)^{v-u} \pmod{2^u 2^{\ell-u}}$$

and conclude, by Lemma 10, that $(-1)^u \equiv (-1)^u (-2)^{v-u} \pmod{2^{\ell-u}}$. Multiplying on both sides by $(-1)^u$, we get $1 \equiv (-2)^{v-u} \pmod{2^{\ell-u}}$ and, hence, -2 is invertible modulo $2^{\ell-u}$. Since and $u < v \leq \ell$ we see that $\gcd(-2, 2^{\ell-u}) = 2 \neq 1$ which contradicts the invertibility of -2. Thus the powers of -2 in (s) are distinct. □

We are now able to express the right and left commutation semigroups as disjoint unions of containers.

Theorem 12. *For $m = 2^\ell n \geq 3$ with n odd, $\ell \geq 0$, and $n \geq 1$,*

(i) $\mathrm{P}(D_m) = \mathcal{C}(0,1) \cup \left(\bigcup_{i=1}^{t} \mathcal{C}((-2)^i, (-2)^{i-1}) \right)$, *where* $t = \begin{cases} ord_m(-2) \text{ for } \ell = 0,\ n > 1 \\ \ell + per_m(-2) - 1 \text{ for } \ell > 0,\ n > 1 \\ \ell - 1 \text{ for } \ell > 0,\ n = 1 \end{cases}$

(ii) $\Lambda(D_m) = \mathcal{C}(0,1) \cup \left(\bigcup_{i=1}^{t'} \mathcal{C}(2^i, 2^{i-1}) \right)$, *where* $t' = \begin{cases} ord_m(2) \text{ for } \ell = 0,\ n > 1 \\ \ell + per_m(2) - 1 \text{ for } \ell > 0,\ n > 1 \\ \ell - 1 \text{ for } \ell > 0,\ n = 1 \end{cases}$,

and these unions are disjoint.

Proof of (i). As mentioned earlier, $\mathrm{P}(D_m)$ is generated by repeated multiplication of the containers $\mathcal{C}(0,1)$ and $\mathcal{C}(-2,1)$. Lemma 9 shows that the μ-maps in any container produced by a product having $\mathcal{C}(0,1)$ as a factor are already in $\mathcal{C}(0,1)$; thus, after we include $\mathcal{C}(0,1)$ in the union, we need only use $\mathcal{C}(-2,1)$ in forming these products. To this end, we list the sequence of "powers" of $\mathcal{C}(-2,1)$ taken according to Lemma 8:

$$\mathcal{C}(-2,1), \mathcal{C}((-2)^2, -2), \mathcal{C}((-2)^3, (-2)^2), \ldots, \mathcal{C}((-2)^i, (-2)^{i-1}), \ldots. \tag{3.1}$$

We now divide the argument into three cases: (a) m odd, (b) $m = 2^\ell n$ with n odd and $n > 1$, (c) $m = 2^\ell$.

Case (a). Applying Lemma 11*(i)* to the first coordinates of the containers in (3.1), we see that there is a first repeat of the powers of -2 when $(-2)^1 \equiv (-2)^{1+d}$ with $d = ord_m(-2)$. Keeping an eye on the second coordinates we pass from the last container in the union given in Theorem 12*(i)*, $\mathcal{C}((-2)^d, (-2)^{d-1})$, to the next container, $\mathcal{C}((-2)^{d+1}, (-2)^d)$, by forming the product

$$\mathcal{C}((-2)^d, (-2)^{d-1}) \circ \mathcal{C}(-2,1) = \mathcal{C}((-2)^{d+1}, (-2)^d) = \mathcal{C}(-2,1).$$

Clearly we did not need to include $\mathcal{C}((-2)^{d+1}, (-2)^d)$ or any further containers in our union, since they will already appear earlier. This establishes *(i)* for Case (a).

Case (b). In the same way, we apply Lemma 11*(ii)* to find that $ind_m(-2) \equiv \ell$. Therefore we have $(-2)^\ell \equiv (-2)^{\ell+d}$ where $d = per_m(-2)$. Since $(-2)^{\ell+d} \equiv (-2)^\ell$, when we form the product of $\mathcal{C}(-2,1)$ with $\mathcal{C}((-2)^{\ell+d-1}, (-2)^{\ell+d-2})$, the last container mentioned in Theorem 12*(i)*, we have

$$\begin{aligned} \mathcal{C}((-2)^{\ell+d-1}, (-2)^{\ell+d-2}) \circ \mathcal{C}(-2,1) &= \mathcal{C}((-2)^{\ell+d}, (-2)^{\ell+d-1}) \\ &= \mathcal{C}((-2)^\ell, (-2)^{\ell-1}) \end{aligned}$$

As in the previous case, this container, and subsequent containers from (3.1), are already present in (3.1) and, thus, we may stop forming containers at this point.

Case (c). By Lemma 11*(iii)*, we have $(-2)^\ell = (-2)^{\ell+1}$. In this case, the last container listed in the union in (3.1) is $\mathcal{C}((-2)^{\ell-1}, (-2)^{\ell-2})$. Forming the next product we obtain

$$\begin{aligned} \mathcal{C}((-2)^{\ell-1}, (-2)^{\ell-2}) \circ \mathcal{C}(-2,1) &= \mathcal{C}((-2)^\ell, (-2)^{\ell-1}) \\ &= \mathcal{C}(0, (-2)^{\ell-1}) \subseteq \mathcal{C}(0,1). \end{aligned}$$

Thus this and subsequent containers are contained within $\mathcal{C}(0,1)$ and we are able to stop the procedure with $\mathcal{C}((-2)^{\ell-1}, (-2)^{\ell-2})$ as the last container in the union.

Note that in any case, Lemma 6 implies that all the containers in the union, Theorem 12*(i)*, are disjoint.

Proof of (ii). The proof for $\Lambda(D_m)$ is essentially the same. We generate the "powers" of $\mathcal{C}(2,1)$ and apply the same reasoning, quoting Lemma 11 at the appropriate points. □

Since both unions in Theorem 12 are disjoint, we can calculate the orders of these semigroups if we know the cardinality of each container and the periods of -2 and 2 in $\mathbb{Z}_m$. There is no known formula for these periods, so they must be calculated individually for each value of m; however, in the next section, we will calculate the cardinality of each container.

4 The Cardinality of $\mathcal{C}(A, B)$

Since $\mathcal{C}(A,B) = \{\mu(A, xB) : x \in Z_m\}$, it contains at most m distinct mappings. Our goal here is to determine which, if any, of these mappings are equal. This will then allow us to find the cardinality of each container. Our first task is to find the upper central series of D_m.

Definition. If G is a group, the *left normed commutator of weight* $w \geq 2$ with entries $g_1, g_2, \ldots, g_w \in G$ is the iterated commutator $[\ldots[[g_1, g_2], g_3], \ldots, g_w]$ written, more simply, as $[g_1, g_2, g_3, \ldots, g_w]$. In the special case of a repeated entry, we write $[x, (n)y] = [x, y, y, \ldots, y]$ (n times).

Definition. The *upper central series of a group* G is the series of subgroups of G,

$$Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_n(G) \leq \cdots$$

with $Z_0(G) = \{1\}$ and $Z_n(G) = \{g \in G : [g, g_1, g_2, \ldots, g_n] = 1, \text{ for all } g_1, g_2, \ldots, g_n \in G\}$. We call $Z_n(G)$ the n-th-centre of G and, where no ambiguity arises, denote it Z_n.

Each term of the upper central series is normal in G. For G finite, there is a least possible $c \geq 0$ for which $Z_c = Z_{c+1} = Z_{c+2} = \cdots$. If the upper central series reaches G (i.e. $Z_c = G$), then we say G is nilpotent of class c; otherwise G is non-nilpotent and $Z_c(G) < G$. Among dihedral groups only the 2-groups, D_{2^ℓ} ($\ell \in \mathbb{Z}^+$), are nilpotent and, in this case, $\{1\} = Z_0(D_{2^\ell}) < Z_1(D_{2^\ell}) < \cdots < Z_\ell(D_{2^\ell}) = D_{2^l}$.

The following characterization of the terms of the upper central series for D_m is well-known and proved routinely.

Theorem 13.

(a) If $u \geq 0$ and m is odd, then $Z_u(D_m) = \{1\}$,

(b) If $u \geq 0$ and m is even with $m = 2^\ell n$ ($n > 0$ and n odd), then

(i) if $n > 1$, then

$$Z_u(D_m) = \begin{cases} \left\{a^N : N = (2^{\ell-u}n)x \text{ and } 0 \leq x < 2^u\right\} & \text{for } u < \ell \\ \left\{a^{nx} : 0 \leq x < 2^\ell\right\} & \text{for } u \geq \ell \end{cases},$$

(ii) if $n = 1$, then

$$Z_u(D_m) = \begin{cases} \left\{a^N : N = 2^{\ell-u}x \text{ and } 0 \leq x < 2^u\right\} & \text{for } u < \ell \\ D_m \text{ for } u \geq \ell \end{cases}.$$

□

We will adopt exponential notation for repeated composition of mappings. For any mapping μ and any $t \in \mathbb{Z}^+$, we will write $\mu^t = \mu \circ \mu \circ \cdots \circ \mu$ (t times), and μ^0 for the identity mapping on D_m. The following lemma takes us back from the μ-maps in our containers to the ρ-maps they represent.

Lemma 14. *For $u > 0$ and $x \in \mathbb{Z}_m$,*

(i) $\mu((-2)^u, x(-2)^{u-1}) = \rho(a^{-x}b) \circ \rho(b)^{u-1}$,

(ii) $\mu(2^u, x2^{u-1}) = \lambda(a^{-x}b) \circ \lambda(b)^{u-1}$.

Proof. To prove *(i)* we will apply both maps to an arbitrary $a^i b^j \in D_m$. Note from Lemma 2 that, $\rho(a^{-x}b) = \mu(\beta_1, -x\alpha_1) = \mu(-2, x)$. Therefore, $(a^i b^j)\rho(a^{-x}b) = (a^i b^j)\mu(-2, x) = a^N$ with $N = -2i\alpha_j - x\beta_j$. Note also that $\rho(b) = \mu(-2, 0)$. Thus, by use of Lemma 3 repeatedly, we have $(a^i b^j)\rho(a^{-x}b) \circ \rho(b)^{u-1} = a^{N'}$ where $N' = N(-2)^{u-1}$. Now $(a^i b^j)\mu((-2)^u, x(-2)^{u-1}) = a^{N''}$ where $N'' = (-2)^u i\alpha_j - x(-2)^{u-1}\beta_j = (-2i\alpha_j - x\beta_j)(-2)^{u-1} = N(-2)^{u-1} = N'$ and the result follows. The proof of *(ii)* follows similarly. □

A group G is metabelian (or solvable of length 2) if its commutator subgroup, G', is abelian. The dihedral groups are metabelian since $D'_m \leq \langle a \rangle$,which is cyclic, and hence abelian. The following commutator identities, which hold in any metabelian group, will be used in our arguments.

Theorem MCI

(i) $[xy, z_1, z_2, \ldots, z_n] = [[x, z_1]^y, z_2, \ldots, z_n][y, z_1, z_2, \ldots, z_n]$,

(ii) $[[x, y][u, v], z_1, z_2, \ldots, z_n] = [x, y, z_1, z_2, \ldots, z_n][u, v, z_1, z_2, \ldots, z_n]$,

(iii) $[[x, y]^{-1}, z_1, z_2, \ldots, z_n] = [x, y, z_1, z_2, \ldots, z_n]^{-1}$. □

The following theorem is true for any metabelian group and, therefore, holds for D_m.

Theorem 15. *Let G be a metabelian group with $u > 0$ and $g_1, g_2 \in G$, then*

$$[g_1, x_1, x_2, \ldots, x_u] = [g_2, x_1, x_2, \ldots, x_u] \tag{4.1}$$

for every $x_1, x_2, \ldots, x_u \in G$ if and only if $g_1^{-1}g_2 \in Z_u(G)$.

Proof. ($\Rightarrow$) To show that $g_1^{-1}g_2 \in Z_u(G)$ it suffices to verify that

$$[g_1^{-1}g_2, x_1, x_2, \ldots, x_u] = 1.$$

Therefore,

$$\begin{aligned}
[g_1^{-1}g_2, x_1, x_2, \ldots, x_u] &= [[g_1^{-1}, x_1][g_1^{-1}, x_1, g_2][g_2, x_1], x_2, \ldots, x_u] \text{ by CI (iii)} \\
&= [g_1^{-1}, x_1, x_2, \ldots, x_u][[g_1^{-1}, x_1], g_2, x_2, \ldots, x_u][g_2, x_1, x_2, \ldots, x_u \text{ by MCI (ii)} \\
&= [g_1^{-1}, x_1, x_2, \ldots, x_u][g_2, [g_1^{-1}, x_1], x_2, \ldots, x_u]^{-1}[g_2, x_1, x_2, \ldots, x_u] \\
&\quad \text{by CI (ii) and MCI (iii).}
\end{aligned}$$

Similarly,

$$\begin{aligned}
1 = [g_1^{-1}g_1, x_1, x_2, \ldots, x_u] &= [[g_1^{-1}, x_1][g_1^{-1}, x_1, g_1][g_1, x_1], x_2, \ldots, x_u] \\
&= [g_1^{-1}, x_1, x_2, \ldots, x_u][g_1^{-1}, x_1, g_1, x_2, \ldots, x_u][g_1, x_1, x_2, \ldots, x_u] \\
&= [g_1^{-1}, x_1, x_2, \ldots, x_u][g_1, [g_1^{-1}, x_1], x_2, \ldots, x_u]^{-1}[g_1, x_1, x_2, \ldots, x_u].
\end{aligned}$$

Comparing the last lines of these two calculations, we see that the first factors are identical, the second factors are equal using the hypothesis (4.1) with x_1 replaced by $[g_1^{-1}, x_1]$, and the third factors are equal by (4.1). Thus we obtain $[g_1^{-1}g_2, x_1, x_2, \ldots, x_u] = 1$, and the implication follows.

($\Leftarrow$) Since $g_1^{-1}g_2 \in Z_u(G)$, we know that for every $x_1, x_2, \ldots, x_u \in G$, $[g_1^{-1}g_2, x_1, x_2, \ldots, x_u] = 1$. Therefore,

$$\begin{aligned}
1 &= [g_1^{-1}g_2, x_1, x_2, \ldots, x_u] \\
&= [[g_1^{-1}, x_1]^{g_2}, x_2, \ldots, x_u][[g_2, x_1], x_2, \ldots, x_u] \text{ by MCI (i)} \\
&= [[g_1, x_1]^{-g_1^{-1}g_2}, x_2, \ldots, x_u][g_2, x_1, x_2, \ldots, x_u] \text{ by CI (v)} \\
&= [[g_1, x_1]^{g_1^{-1}g_2}, x_2, \ldots, x_u]^{-1}[g_2, x_1, x_2, \ldots, x_u] \text{ by MCI (iii)} \\
&= [[g_1, x_1][g_1, x_1, g_1^{-1}g_2], x_2, \ldots, x_u]^{-1}[g_2, x_1, x_2, \ldots, x_u] \text{ by CI (i)} \\
&= ([[g_1, x_1], x_2, \ldots, x_u][[[g_1, x_1], g_1^{-1}g_2], x_2, \ldots, x_u])^{-1}[g_2, x_1, x_2, \ldots, x_u] \text{ by MCI (ii)} \\
&= ([[g_1, x_1], x_2, \ldots, x_u][[g_1^{-1}g_2, [g_1, x_1], x_2, \ldots, x_u])^{-1}[g_2, x_1, x_2, \ldots, x_u] \text{ by CI(ii) and MCI(iii)}
\end{aligned}$$

Since $g_1^{-1}g_2 \in Z_u(G)$, we know that the middle term in the last line is trivial. Thus we have

$$1 = [g_1, x_1, x_2, \ldots, x_u]^{-1}[g_2, x_1, x_2, \ldots, x_u].$$

Therefore, $[g_1, x_1, x_2, \ldots, x_u] = [g_2, x_1, x_2, \ldots, x_u]$, as required. □

Lemma 16. *For $u > 0$ and $1 \le j \le u$ let $i, r_j \in \mathbb{Z}_m$, $s_j \in \mathbb{Z}_2$, then*

$$[a^i, a^{r_1}b^{s_1}, a^{r_2}b^{s_2}, \ldots, a^{r_u}b^{s_u}] = \left\{ \begin{array}{c} \textit{1 if some } s_k = 0 \\ [a^i, (u-1)b] \textit{ if all } s_k = 1 \end{array} \right\}.$$

Note that if all $s_k = 1$, then

$$[a^i, (u-1)b] = a^N \textit{ with } N \equiv (-2)^u i.$$

Proof. Note first that for $i, r \in \mathbb{Z}_m$, $s \in \mathbb{Z}_2$, CI*(iv)* implies that $[a^i, a^r b^s] = [a^i, b^s][a^i, a^r]^{b^s} = [a^i, b^s]$. It follows that

$$[a^i, a^{r_1}b^{s_1}] = [a^i, b^{s_1}] = a^{-i}(a^i)^{b^{s_1}} = a^{-i}(a^i)^{(-1)^{s_1}} = a^{\beta_{s_1} i}.$$

Similarly,

$$[a^i, a^{r_1}b^{s_1}, a^{r_2}b^{s_2}] = [a^{\beta_{s_1} i}, a^{r_2}b^{s_2}] = [a^{\beta_{s_1} i}, b^{s_2}] = a^{\beta_{s_1}\beta_{s_2} i},$$

and, inductively, $[a^i, a^r b^s, a^{r_1}b^{s_1}, \ldots, a^{r_{u-1}}b^{s_{u-1}}] = a^N$ with $N = \beta_{s_1} \cdots \beta_{s_u} i$. If some $s_j = 0$, then $\beta_{s_j} = 0$, and it follows that $N \equiv 0 \pmod{m}$. In this case we have $a^N = 1$ as stated in the lemma. Otherwise, $s_j = 1$ for each j. Thus, $\beta_j = -2$ for each j, and therefore $a^N = (-2)^u i$, as required. □

Lemma 17. *Let $m \ge 3$, and $u > 0$ and $g_1, g_2 \in D_m$, then*

$$[g_1, x_1, x_2, \ldots, x_u] = [g_2, x_1, x_2, \ldots, x_u] \textit{ for every } x_1, x_2, \ldots, x_u \in D_m \tag{4.2}$$

if and only if

$$\rho(g_1) \circ \rho(b)^{u-1} = \rho(g_2) \circ \rho(b)^{u-1}. \tag{4.3}$$

Proof. ($\Rightarrow$) Let $x \in D_m$, then

$$\begin{aligned}
&(x)\rho(g_1) \circ \rho(b)^{u-1} \\
=&[x, g_1, (u-1)b] \\
=&[g_1, x, (u-1)b]^{-1} \text{ by CI (ii) and MCI (iii)} \\
=&[g_2, x, (u-1)b]^{-1} \text{ by (4.2)} \\
=&[x, g_2, (u-1)b] \text{ by CI (ii) and MCI (iii)} \\
=&(x)\rho(g_2) \circ \rho(b)^{u-1}.
\end{aligned}$$

($\Leftarrow$) Letting $[g_1, x_1] = a^i$ for some $i \in \mathbb{Z}_m$ and writing each x_k as $a^{r_k}b^{s_k}$, we obtain

$$\begin{aligned}
[g_1, x_1, x_2, \ldots, x_u] &= [a^i, a^{r_2}b^{s_2}, \ldots, a^{r_u}b^{s_u}] \\
&= \left\{ \begin{array}{c} 1 \text{ if some } s_k = 0 \\ [a^i, (u-1)b] \text{ if } s_k = 1 \ \ (2 \leq k \leq u) \end{array} \right\},
\end{aligned}$$

by Lemma 16. Similarly, if $[g_2, x_1] = a^j$, then

$$[g_2, x_1, x_2, \ldots, x_u] = \left\{ \begin{array}{c} 1 \text{ if some } s_k = 0 \\ [a^j, (u-1)b] \text{ if } s_k = 1 \ \ (2 \leq k \leq u) \end{array} \right\}.$$

If $s_k = 0$ for some k, then both expressions equal 1, and (4.2) holds. Thus we may suppose that $s_k = 1$ for $2 \leq k \leq u$. Here the equation in (4.2) becomes $[a^i, (u-1)b] = [a^j, (u-1)b]$. Replacing a^i by $[x_1, g_1]$ and a^j by $[x_1, g_2]$, we obtain, $[[x_1, g_1], (u-1)b]^{-1} = [[x_1, g_2], (u-1)b]^{-1}$. This is equivalent to $(x_1)(\rho(g_1) \circ \rho(b)^{u-1}) = (x_1)(\rho(g_2) \circ \rho(b)^{u-1})$ which then follows from our assumption (4.3). □

Corollary 18. *If $u > 0$, $Z_u(D_m) \leq \langle a \rangle$, and $x, y \in Z_m$, then $\rho(a^x b) \circ (\rho(b))^{u-1} = \rho(a^y b) \circ (\rho(b))^{u-1}$ if and only if $a^x Z_u = a^y Z_u$ in the quotient group $\langle a \rangle / Z_u$.*

Proof. Note first that $Z_u \triangleleft G$ and, therefore, if $Z_u \leq \langle a \rangle$, then $Z_u \triangleleft \langle a \rangle$ and the quotient group $\langle a \rangle / Z_u$ exists. Letting $g_1 = a^x b$ and $g_2 = a^y b$, we have $g_1^{-1} g_2 = (a^x b)^{-1}(a^y b) = b^{-1} a^{-x+y} b = a^{y-x}$. Thus, from Theorem 15 and Lemma 17, $\rho(a^x b) \circ (\rho(b))^{u-1} = \rho(a^y b) \circ (\rho(b))^{u-1}$ if and only if $a^{y-x} \in Z_u$. This is equivalent to saying that $a^x Z_u = a^y Z_u$ in the quotient group $\langle a \rangle / Z_u$. □

We are now able to calculate the cardinality of the containers used in producing $\mathrm{P}(D_m)$ and $\Lambda(D_m)$.

Theorem 19. *If $u > 0$ and $Z_u(D_m) \leq \langle a \rangle$, then*

(i) $\left| \mathcal{C}((-2)^u, (-2)^{u-1}) \right| = \dfrac{m}{|Z_u(D_m)|}$,

(ii) $\left| \mathcal{C}(2^u, 2^{u-1}) \right| = \dfrac{m}{|Z_u(D_m)|}$.

Proof. (i). By definition of container,

$$\mathcal{C}((-2)^u, (-2)^{u-1}) = \left\{ \mu((-2)^u, x(-2)^{u-1}) : x \in \mathbb{Z}_m \right\}.$$

If the domain of x is $\mathbb{Z}_m$, then the domain of $-x$ is also $\mathbb{Z}_m$; thus, it follows by Lemma 14 that

$$\left\{ \mu((-2)^u, x(-2)^{u-1}) : x \in \mathbb{Z}_m \right\} = \left\{ \rho(a^x b) \circ \rho(b)^{u-1} : x \in \mathbb{Z}_m \right\}.$$

Then it is clear that

$$\left\{\rho(a^x b)\circ\rho(b)^{u-1} : x\in\mathbb{Z}_m\right\} = \left\{\rho(a^x b)\circ\rho(b)^{u-1} : a^x\in\langle a\rangle\right\}.$$

Now, applying Corollary 18, we see that the number of distinct mappings in this last set is the order of the quotient group $|\langle a\rangle/Z_u| = \dfrac{m}{|Z_u|}$.

(ii). The argument proceeds as above noting that

$$\begin{aligned}\left\{\mu(2^u, x2^{u-1}) : x\in\mathbb{Z}_m\right\} &= \left\{\lambda(a^x b)\circ\lambda(b)^{u-1} : x\in\mathbb{Z}_m\right\}\\ &= \left\{(-1)^u\left(\rho(a^x b)\circ\rho(b)^{u-1}\right) : x\in\mathbb{Z}_m\right\}.\end{aligned}$$

Corollary 18 applies here, as it did in part *(i)*, and the result follows in the same manner. □

Lemma 20. $|\mathcal{C}(0,1)| = \dfrac{m}{|Z_1|}$.

Proof. Let $x, y\in\mathbb{Z}_m$ and let $\mu(0,x), \mu(0,y)$ be arbitrary elements of $\mathcal{C}(0,1)$. If $\mu(0,x) = \mu(0,y)$, then for every $i\in\mathbb{Z}_m, j\in\mathbb{Z}_2$, we have:

$$(a^i b^j)\mu(0,x) = (a^i b^j)\mu(0,y).$$

This is true if and only if, for each j, $a^{-x\beta_j} = a^{-y\beta_j}$.And this is true if and only if $x\beta_j \equiv y\beta_j \pmod m$, or, alternately, $(x-y)\,\beta_j \equiv 0 \pmod m$. If $j=0$ then $\beta_0 = 0$, so we need only consider the condition when $j=1$ and, thus, $\beta_1 = -2$. Thus we have $\mu(0,x) = \mu(0,y)$ if and only if $-2(x-y)\equiv 0 \pmod m$. Since -1 is invertible in $\mathbb{Z}_m$, this is equivalent to

$$2x \equiv 2y \pmod m. \tag{4.4}$$

If m is odd, 2 is invertible in $\mathbb{Z}_m$, thus (4.4) is equivalent to $x\equiv y \pmod m$ and, therefore, each mapping $\mu(0,x)$ in $\mathcal{C}(0,1)$ is distinct and $|\mathcal{C}(0,1)| = m$. In this case the statement of the lemma is true since, by Theorem 13, $|Z_1| = 1$. If m is even, let us write $m = 2^\ell n$ with $\ell > 0$ and n odd. Condition (4.4) is then $2x\equiv 2y \pmod{2^\ell t}$. This is equivalent to $x\equiv y \pmod{2^{\ell-1}t}$ by Lemma 10. Therefore the elements of $\mathcal{C}(0,1)$ are equal in pairs; $\mu(0,x) = \mu(0, x+2^{\ell-1}n)$ for $x = 0, 1, \ldots, 2^{\ell-1}n - 1$. Thus $|\mathcal{C}(0,1)| = \dfrac{m}{2}$. By Theorem 13 we see that $|Z_1| = 2$ and the result is verified. □

5 The Main Theorem

We are now prepared to give formulas for the exact orders of $\mathrm{P}(D_m)$ and $\Lambda(D_m)$.

Theorem 21. *If $m = 2^\ell n > 3$ with n odd,*

(i) $|\mathrm{P}(D_m)| = m\left(\dfrac{1}{|Z_1|} + \displaystyle\sum_{i=1}^{t-1}\frac{1}{|Z_i|}\right)$, *where* $t = \begin{cases} 1 + ord_m(-2) \text{ for } \ell = 0,\ n > 1 \\ \ell + per_m(-2) \text{ for } \ell > 0,\ n > 1 \\ \ell \text{ for } \ell > 0,\ n = 1 \end{cases}$,

(ii) $|\Lambda(D_m)| = m\left(\dfrac{1}{|Z_1|} + \displaystyle\sum_{i=1}^{t'-1}\frac{1}{|Z_i|}\right)$, *where* $t' = \begin{cases} 1 + ord_m(2) \text{ for } \ell = 0,\ n > 1 \\ \ell + per_m(2) \text{ for } \ell > 0,\ n > 1 \\ \ell \text{ for } \ell > 0,\ n = 1 \end{cases}$,

Proof of (i). By Theorem 12*(i)* we have expressed $\mathrm{P}(D_m)$ as the disjoint union of containers

$$\mathcal{C}(0,1) \cup \left(\bigcup_{i=1}^{t} \mathcal{C}((-2)^i, (-2)^{i-1}) \right), \tag{5.1}$$

where $t = ord_m(-2)$ for m odd, $t = \ell + per_m(-2) - 1$ for $n > 1$ and $t = \ell - 1$ for $n = 1$. To find $|\mathrm{P}(D_m)|$ we shall simply add the cardinalities of the containers in (5.1). These cardinalities are given in Theorem 19*(i)* and Lemma 20 ; however, the hypothesis, $Z_u(D_m) \leq \langle a \rangle$, in Theorem 19 is not met in every case. Theorem 13*(ii)*, shows that the only case in which this hypothesis is not met is when $n = 1$ and $u \geq \ell$. Thus consider the case in which $m = 2^\ell$ and $u \geq \ell$. Here we see that we are taking the union as i goes from 1 to t, but here $t = \ell - 1 < \ell \leq u$. Thus we will not need to apply Theorem 19 in such a case and the hypothesis is irrelevant.

To complete the proof we apply Theorem 19*(i)* and Lemma 20 to the disjoint union (5.1) to obtain,

$$\begin{aligned} |\mathrm{P}(D_m)| &= |\mathcal{C}(0,1)| + \left(\sum_{i=1}^{t} \left| \mathcal{C}((-2)^i, (-2)^{i-1}) \right| \right) \\ &= \frac{m}{|Z_1|} + \left(\sum_{i=1}^{t} \frac{m}{|Z_i|} \right) = m \left(\frac{1}{|Z_1|} + \left(\sum_{i=1}^{t} \frac{1}{|Z_i|} \right) \right). \end{aligned}$$

The proof of *(ii)* is quite similar for $\Lambda(D_m)$. □

At the end of the paper we have given a table displaying the orders of the commutation semigroups of dihedral groups D_m for $3 \leq m \leq 101$. Looking at this table, many conjectures present themselves. For example, if p is an odd prime less than 50, the table shows that $|\mathrm{P}(D_p)| = |\mathrm{P}(D_{2p})|$ and $|\Lambda(D_p)| = |\Lambda(D_{2p})|$. We will prove this true for all odd primes p. The proof will serve as an example of how our approach can be applied to the study of such questions.

Theorem 22. *If p is an odd prime, then*

(i) $|\mathrm{P}(D_p)| = |\mathrm{P}(D_{2p})|$,

(ii) $|\Lambda(D_p)| = |\Lambda(D_{2p})|$.

Proof. The condition that $|\mathrm{P}(D_p)| = |\mathrm{P}(D_{2p})|$ can be written in terms of our formulas. First for p,

$$|\mathrm{P}(D_p)| = p \left(\frac{1}{|Z_1(D_p)|} + \sum_{i=1}^{t-1} \frac{1}{|Z_i(D_p)|} \right),$$

where $t = 1 + ord_p(-2)$. For $2p$ we have,

$$|\mathrm{P}(D_{2p})| = 2p \left(\frac{1}{|Z_1(D_{2p})|} + \sum_{i=1}^{t'-1} \frac{1}{|Z_i(D_{2p})|} \right),$$

where $t' = 1 + per_{2p}(-2)$. By Theorem 13, Each $Z_i(D_p) = \{1\}$, thus we have

$$|\mathrm{P}(D_p)| = p \cdot t = p \cdot (1 + ord_p(-2)).$$

Looking at D_{2p}, we see that since $\ell = 1$ in this case, thus we are interested in $Z_u(D_{2p})$ for $u \geq \ell$. Theorem 13*(b)(i)* then shows that $|Z_u(D_{2p})| = 2^\ell (= 2)$ for $u \geq 1$. Thus we have

$$|\mathrm{P}(D_{2p})| = 2p \left(\frac{1}{2} + \sum_{i=1}^{t'-1} \frac{1}{2} \right) = p \cdot t' = p \cdot (1 + per_{2p}(-2)).$$

To prove part *(i)* of the theorem, it suffices to show that $ord_p(-2) = per_{2p}(-2)$. By similar arguments, the same equation will imply that part *(ii)* is true.

Since -2 is coprime to p it is invertible in $\mathbb{Z}_p$, it has an order. Letting $ord_p(-2) = k$, we have $(-2)^k \equiv 1 \pmod{p}$. Note that $ind_p(-2) = 1$. By Lemma 10, $2(-2)^k \equiv 2 \pmod{2p}$, and multiplying both sides by -1 gives us, $(-2)^{1+k} \equiv (-2)^1 \pmod{2p}$. This shows that $ind_{2p}(-2) = 1$. We see that the period of -2 is at most k, so suppose $per_{2p}(-2) = t < k$. Then $(-2)^{1+t} \equiv (-2)^1 \pmod{2p}$. Rewrite this as $-2(-2)^t \equiv -2 \pmod{2p}$ and multiply both sides by -1 to obtain, $2(-2)^t \equiv 2 \pmod{2p}$. Applying Lemma 10 gives us $(-2)^t \equiv 1 \pmod{p}$, contradicting the minimality of k, the order of -2 in $\mathbb{Z}_p$. Therefore $per_{2p}(-2) = k = ord_p(-2)$ and the result follows. □

In the Introduction we quoted Theorem C2, proved by Countryman in [1]. We can reprove this using our methods, but, more interestingly, we can prove a new result parallel to his. Our proof of Theorem C2 is similar to the proof below.

Theorem 23. *If p and q are primes, then $\Lambda(D_p) \cong \Lambda(D_q)$ implies $p = q$.*

Proof. We will suppose that $p < q$ and derive a contradiction. Note that if $p = 2$, D_2 is abelian and, as mentioned earlier, $|\Lambda(D_2)| = 1$. With q an odd prime, D_q is nonabelian, thus $|\Lambda(D_q)| > 1$. The hypothesis is not met in such a case and, thus, we may assume that both p and q are odd primes.

From our assumption, $\Lambda(D_p) \cong \Lambda(D_q)$, it follows that $|\Lambda(D_p)| = |\Lambda(D_q)|$. Since p and q are both odd, Theorem 13 implies that $Z_i = \{1\}$ in both cases. Thus Theorem 21 gives,

$$p\left(\frac{1}{|Z_1|} + \sum_{i=1}^{t-1} \frac{1}{|Z_i|}\right) = |\Lambda(D_p)| = |\Lambda(D_q)| = q\left(\frac{1}{|Z_1|} + \sum_{i=1}^{t'-1} \frac{1}{|Z_i|}\right), \tag{5.2}$$

where $t = 1 + ord_p(2)$ and $t' = 1 + ord_q(2)$. From (5.2) we deduce that $p\,(t) = q\,(t')$ and, hence, that $p\,(1 + ord_p(2)) = q\,(1 + ord_q(2))$. Since we are assuming that p and q are distinct primes we conclude that $q \,|\, 1 + ord_p(2)$ and, therefore, $q \leq 1 + ord_p(2)$. But $ord_p(2) < p$, since $ord_p(2) \,|\, \phi(p)$, and $\phi(p) = p - 1$. Thus we have $q \leq 1 + ord_p(2) < p$, which contradicts our assumption that $p < q$. □

Note that the hypothesis, $\Lambda(D_p) \cong \Lambda(D_q)$, can be "weakened" to $|\Lambda(D_p)| = |\Lambda(D_q)|$.

6 Formulas and counterexamples

First we will derive the formulas of Levy and DeWolf quoted in the Introduction. Note that Theorem D covers all even values of m including the nilpotent case ($m = 2^\ell$) proved earlier by Levy in Theorem L2; thus, for brevity, we will derive only Theorems L1 and D. Translating from the notation of these theorems into the notation of this paper we have, $ind_R(m) = per_m(-2)$, $ind_L(m) = per_m(2)$. Also, for $n > 1$, $m_R = \ell + per_m(-2)$ and $m_L = \ell + per_m(2)$, and for $n = 1$, $m_R = m_L = \ell$.

Derivation of Theorem L1. First we will establish part *(i)*. From Theorem 21 and Theorem 13, for m odd, we have $|\mathrm{P}(D_m)| = m\left(\frac{1}{|Z_1|} + \sum_{i=1}^{t-1} \frac{1}{|Z_i|}\right)$ with $t = 1 + ord_m(-2)$ and each $Z_i(D_m) = \{1\}$. Thus

$$|\mathrm{P}(D_m)| = m\,(1 + (t-1)) = mt = m(1 + ord_m(-2)) = m(per_m(-2) + 1).$$

The proof for part *(ii)* is similar. □

Derivation of Theorem D. We first prove part *(i)*. Letting $m = 2^\ell s$, with s odd, and $\ell, s \in \mathbb{Z}^+$, we will break into two cases: $s > 1$ and $s = 1$. Supposing that $s > 1$, Theorem 13 implies that $|Z_i| = 2^i$ for $i < \ell$ and $|Z_i| = 2^\ell$ for $i \geq \ell$. From Theorem 21 we see that

$$|\mathrm{P}(D_m)| = m\left(\frac{1}{|Z_1|} + \sum_{i=1}^{t-1} \frac{1}{|Z_i|}\right), \tag{6.1}$$

with $t = \ell + per_m(-2)$. Note that

$$\begin{aligned}\sum_{i=1}^{t-1} \frac{1}{|Z_i|} &= \sum_{i=1}^{\ell-1} \frac{1}{2^i} + \sum_{i=\ell}^{t-1} \frac{1}{2^\ell} = \frac{2^{\ell-1}-1}{2^{\ell-1}} + \frac{t-\ell}{2^\ell} \\ &= \frac{2^\ell - 2 + t - \ell}{2^\ell} = \frac{2^\ell - 2 + per_m(-2)}{2^\ell}.\end{aligned} \tag{6.2}$$

Substituting the outcome of (6.2) into (6.1) we arrive at,

$$\begin{aligned}|\mathrm{P}(D_m)| &= m\left(\frac{1}{|Z_1|} + \sum_{i=1}^{t-1} \frac{1}{|Z_i|}\right) = m\left(\frac{1}{2} + \frac{2^\ell - 2 + per_m(-2)}{2^\ell}\right) \\ &= 2^\ell s\left(\frac{2^\ell + 2^{\ell-1} - 2 + per_m(-2)}{2^\ell}\right) = s\left(2^\ell + 2^{\ell-1} + per_m(-2) - 2\right).\end{aligned}$$

The proof of part *(ii)* is similar. □

Having shifted among notations to come up with these derivations, we would like to give here the simplest numerical formulas we know for $\mathrm{P}(D_m)$ and $\Lambda(D_m)$.

(i) For m odd,
$$|\mathrm{P}(D_m)| = m(ord_m(-2) + 1) \text{ and } |\Lambda(D_m)| = m(ord_m(2) + 1),$$

(ii) For $m = 2^\ell n$ with n odd and $n > 1$,
$$|\mathrm{P}(D_m)| = s(2^\ell + 2^{\ell-1} - 2 + per_m(-2)) \text{ and } |\Lambda(D_m)| = s(2^\ell + 2^{\ell-1} - 2 + per_m(2)).$$

(iii) For $m = 2^\ell$, $|\mathrm{P}(D_m)| = |\Lambda(D_m)| = 2^\ell + 2^{\ell-1} - 2$.

Lastly, we will comment on the three theorems of Countryman on pq groups quoted in the Introduction.

We show here that $|\mathrm{P}(D_8)| = |\Lambda(D_8)|$ and $\mathrm{P}(D_8) \cong \Lambda(D_8)$, but $\mathrm{P}(D_8) \neq \Lambda(D_8)$, thereby giving counterexamples to the statements $(c) \Rightarrow (a)$ and $(b) \Rightarrow (a)$ in Theorem C1 for dihedral groups in general. Applying Theorem 12 to the dihedral group of order 16,we see that

$$\mathrm{P}(D_8) = \mathcal{C}(0,1) \dot\cup \mathcal{C}(6,1) \dot\cup \mathcal{C}(4,2) \text{ while } \Lambda(D_8) = \mathcal{C}(0,1) \dot\cup \mathcal{C}(2,1) \dot\cup \mathcal{C}(4,2).$$

By Lemma 20, $|\mathcal{C}(0,1)| = \dfrac{8}{|Z_1|} = \dfrac{8}{2} = 4$, $|\mathcal{C}(6,1)| = \dfrac{8}{|Z_1|} = \dfrac{8}{2} = 4$, $|\mathcal{C}(2,1)| = \dfrac{8}{|Z_1|} = \dfrac{8}{2} = 4$, and $|\mathcal{C}(4,2)| = \dfrac{8}{|Z_2|} = \dfrac{8}{4} = 2$.Therefore $|\mathrm{P}(D_8)| = 10 = |\Lambda(D_8)|$, however, by Lemma 6, $\mathcal{C}(6,1) \cap \mathcal{C}(2,1) = \varnothing$ and, therefore, $\mathrm{P}(D_8) \neq \Lambda(D_8)$. To show that $\mathrm{P}(D_8) \cong \Lambda(D_8)$, we define a mapping $\phi : \mathrm{P}(D_8) \to \Lambda(D_8)$ by $\phi(\mu(x,y)) = \mu(3x, y)$. This can be shown to be an isomorphism. Note also that the container decomposition above shows that $\mathrm{P}(D_8) \not\subseteq \Lambda(D_8)$ and $\mathrm{P}(D_8) \not\subseteq \Lambda(D_8)$, thus providing a counterexample to the generalization of Theorem C3 to dihedral groups in general.

We will show that $(c) \Rightarrow (b)$ fails for D_{15}. Note by our Theorem 21 it follows that $|\mathrm{P}(D_{15})| = 75 = |\Lambda(D_{15})|$. To see that $\mathrm{P}(D_{15}) \ncong \Lambda(D_{15})$ we shall apply the following theorem:

Theorem 1 (Gupta, [3]) $\mathrm{P}(D_m) \cong \Lambda(D_m)$ if and only if $ord_p(2) \equiv 0 \pmod 4$ for every odd prime factor of m.

Since $ord_3(2) = 2 \not\equiv 0 \pmod 4$, it follows that $\mathrm{P}(D_{15}) \ncong \Lambda(D_{15})$, and we have our counterexample.

It is also the case that $\mathrm{P}(D_{10}) \cong \mathrm{P}(D_5)$ and $\Lambda(D_{10}) \cong \Lambda(D_5)$. This gives a counterexample to the generalization of Theorem C2 and our Theorem 23. The container decomposition has proven quite useful in finding these isomorphisms.

m	$\lvert\mathrm{P}(D_m)\rvert$	$\lvert\Lambda(D_m)\rvert$	m	$\lvert\mathrm{P}(D_m)\rvert$	$\lvert\Lambda(D_m)\rvert$	m	$\lvert\mathrm{P}(D_m)\rvert$	$\lvert\Lambda(D_m)\rvert$
3	6	9	36	63	90	69	1587	1587
4	4	4	37	1369	1369	70	455	455
5	25	25	38	190	361	71	5041	2556
6	6	9	39	507	507	72	117	144
7	49	28	40	70	70	73	1387	730
8	10	10	41	861	861	74	1369	1369
9	36	63	42	147	147	75	1575	1575
10	25	25	43	344	645	76	247	418
11	66	121	44	99	154	77	2387	2387
12	15	18	45	585	585	78	507	507
13	169	169	46	529	276	79	6241	3160
14	49	28	47	2209	1128	80	130	130
15	75	75	48	69	72	81	2268	4455
16	22	22	49	2107	1078	82	861	861
17	153	153	50	525	525	83	3486	6889
18	36	63	51	459	459	84	210	210
19	190	361	52	208	208	85	765	765
20	40	40	53	2809	2809	86	344	645
21	147	147	54	270	513	87	2523	2523
22	66	121	55	1155	1155	88	165	220
23	529	276	56	112	91	89	2047	1068
24	33	36	57	570	1083	90	585	585
25	525	525	58	841	841	91	1183	1183
26	169	169	59	1770	3481	92	598	345
27	270	513	60	120	120	93	1023	1023
28	70	49	61	3721	3721	94	2209	1128
29	841	841	62	341	186	95	3515	3515
30	75	75	63	441	441	96	141	144
31	341	186	64	94	94	97	4753	4753
32	46	46	65	845	845	98	2107	1078
33	198	363	66	198	363	99	1584	3069
34	153	153	67	2278	4489	100	600	600
35	455	455	68	204	204	101	10201	10201

References

[1] Countryman, James J., 'On the commutation semigroups of pq groups', Ph.D Thesis, University of Notre Dame (1970) pp. 58.

[2] DeWolf, Darien, 'Commutation semigroups of dihedral groups of order 2n where n is even', Honours Thesis, Mount Saint Vincent University (2012) pp. 20.

[3] Gupta, N.D., 'On commutation semigroups of a group', J. of the Australian Math. Soc., 6, (1966) pp. 36–45.

[4] Gupta, N.D., 'Commutation near-rings of a group', J. Australian Math. Soc., 7, (1967) pp. 135–140.

[5] Levy, Christopher D., 'Investigation of commutation semigroups of dihedral groups', Honours Thesis, Mount Saint Vincent University (2009) pp. 26.