Rose-Hulman Undergraduate Mathematics Journal

Volume 23
Issue 2

Article 3

Generalizations of Commutativity in Dihedral Groups

Noah A. Heckenlively
Rose Hulman Institute of Technology, heckenna@rose-hulman.edu

ℝose-Hulman Undergraduate Mathematics Journal
Volume 23, Issue 2, 2022

Generalizations of Commutativity in Dihedral Groups

By *Noah Heckenlively*

Abstract. The probability that two elements commute in a non-Abelian finite group is at most $\frac{5}{8}$. We prove several generalizations of this result for dihedral groups. In particular, we give specific values for the probability that a product of an arbitrary number of dihedral group elements is equal to its reverse, and also for the probability that a product of three elements is equal to a permutation of itself or to a cyclic permutation of itself. We also show that for any r and n, there exists a dihedral group such that the probability that a product of n elements is equal to its reverse is $\frac{r}{q}$ for some q coprime to r, extending a known result.

1 Introduction

In a 2011 edition of *Mathematics Magazine*, Clifton, Guichard, and Keef [1] show the probability that two elements commute in a dihedral group and use that to prove results about commutativity of direct products of dihedral groups. In that same edition, Langley, Levitt, and Rower [4] find upper bounds on generalizations of commutativity in nonabelian finite groups. Thus, it is a natural exension of both works to investigate generalizations of cummutativity for dihedral groups.

For non-Abelian groups there exists some pair of elements that does not commute. Consider D_4, the dihedral group of the square. We'll denote the identity and counterclockwise rotations of the square by r_0, r_{90}, r_{180}, r_{270} and the horizontal, vertical, and two diagonal reflections as h, v, d, and d', respectively, as shown in fig. 1. In table 1, a one indicates that a pair of elements commute, a zero that the elements do not commute.

There are 40 ones among 64 entries, so $\frac{5}{8}$ of the pairs commute. If we define Comm(G) to be the number of commuting pairs in group G,

$$\mathrm{Comm}(G) = |\{(a,b) \in G \times G | ab = ba\}|,$$

we then can define the probability that two elements commute as

$$P_2(G) = \frac{\mathrm{Comm}(G)}{|G|^2}.$$

Mathematics Subject Classification. 16B99
Keywords. Commutativity Generalization, Dihedral Group, Non-Abelian

D_4	r_0	r_{90}	r_{180}	r_{270}	h	v	d	d'
r_0	1	1	1	1	1	1	1	1
r_{90}	1	1	1	1	0	0	0	0
r_{180}	1	1	1	1	1	1	1	1
r_{270}	1	1	1	1	0	0	0	0
h	1	0	1	0	1	1	0	0
v	1	0	1	0	1	1	0	0
d	1	0	1	0	0	0	1	1
d'	1	0	1	0	0	0	1	1

Table 1: Commutativity Table for D_4

It is well known that $P_2(G) \le \frac{5}{8}$ for non-Abelian groups [3, 5], so D_4 is as commutative as possible for a non-Abelian group. As such, dihedral groups are a natural family of groups to study and will be the focus of this paper. Define D_m to be the dihedral group of all rotations and reflections of an m-sided regular polygon. Clifton, Guichard, and Keef [1] give exact values of $P_2(D_m)$ for all m:

$$P_2(D_m) = \begin{cases} \frac{m+3}{4m} & \text{if } m \text{ is odd} \\ \frac{m+6}{4m} & \text{if } m \text{ is even} \end{cases} \tag{1}$$

In this paper, we will focus on various generalizations of this result by considering several generalizations of commutativity. For a permutation σ in the symmetric group S_n, define $(a_1 a_2 \cdots a_n)^\sigma$ to be the product of $a_1, a_2, \ldots, a_n$ with each a_i in position $\sigma(i)$. For example, $(a_1 a_2 a_3 a_4)^{(1,4)(2,3)} = a_4 a_3 a_2 a_1$. Since the equation $ab = ba$ can be written $ab = (ab)^{(1,2)}$, when generalizing commutativity we'll consider $P(a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_n)^\sigma)$ for various n and σ. First, we generalize the equation $ab = ba$ to $a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1$ with each $a_i \in G$. We'll denote the probability that the product of n group elements is equal to its reverse as

$$P_n(G) = \frac{|\{(a_1, a_2, \ldots, a_n) \in G^n | a_1 a_2 \cdots a_n = a_n a_{n-1} \cdots a_1\}|}{|G|^n}.$$

So with $n = 2$ we have $P(ab = ba) = P_2(G)$. Langley, Levitt, and Rower [4] give the upper bound

$$P_n(G) \le \frac{1}{2} + \frac{1}{2^{n+1}} \text{ if } n \text{ is even,}$$
$$P_n(G) = P_{n-1}(G) \text{ if } n \text{ is odd.}$$

Again, D_4 realizes this upper bound. We will show the following, generalizing (1):

Theorem 3.3. For $m \geq 3$,

$$\mathrm{P}_n(\mathrm{D}_m) = \begin{cases} \frac{m+k(2^n-1)}{2^n m} \text{ if n is even} \\ \mathrm{P}_{n-1}(\mathrm{D}_m) \text{ if n is odd} \end{cases}$$

where $k = 1$ if m is odd and $k = 2$ if m is even.

Next, we'll define a product of group elements $a_1 a_2 \cdots a_n$ to be **rewritable** if $a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_n)^\sigma$ for some nonidentity permutation σ. For example, abc is rewritable if abc is equal to at least one of acb, bac, bca, cab, cba. Note that ab is rewritable if $ab = ba$, naturally generalizing commutativity. We define $\mathrm{P}_n^{rew}(\mathrm{G})$ to be the probability that a product $a_1 a_2 \cdots a_n$ is rewritable:

$$\mathrm{P}_n^{rew}(\mathrm{G}) = \frac{|\{(a_1, a_2, \ldots, a_n) \in \mathrm{G}^n | a_1 a_2 \cdots a_n \text{ is rewritable}\}|}{|\mathrm{G}|^n}.$$

We define a group, G, to be **n-rewritable** if every product of n elements of G is rewritable, that is, $\mathrm{P}_n^{rew}(\mathrm{G}) = 1$. Thus every Abelian group is n-rewritable for all n. Ellenberg [2] shows that the analogous result to the $\frac{5}{8}$ bound for $\mathrm{P}_3^{rew}(\mathrm{G})$ for a finite group G is $\mathrm{P}_3^{rew}(\mathrm{G}) = 1$ or $\mathrm{P}_3^{rew}(\mathrm{G}) \leq \frac{17}{18}$. We will show the following for dihedral groups.

Theorem 4.2. For $m \geq 3$,

$$\mathrm{P}_3^{rew}(\mathrm{D}_m) = \frac{3m^2 + 3km - 2k^2}{4m^2}$$

where $k = 1$ if m is odd and $k = 2$ if m is even.

Note that substituting $m = 4$ and $k = 2$ into **theorem 4.2** gives $\mathrm{P}_3^{rew}(\mathrm{D}_4) = 1$, so this is an example of a non-Abelian group that is 3-rewritable. By substituting $m = 6$ and $k = 2$, we also see that $\mathrm{P}_3^{rew}(\mathrm{D}_6) = \frac{17}{18}$, achieving the upper bound of $\mathrm{P}_3^{rew}(\mathrm{G}) \leq \frac{17}{18}$.

For the next generalization of commutativity, we'll define a product of group elements $a_1 a_2 \ldots a_n$ to be **cyclic rewritable** if it is equal to some nonidentity cyclic rearrangement of itself, that is, $a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_n)^\sigma$ where $\sigma = (1, 2, 3, \ldots, n)^k$ for some $k < n$. For example, abc is cyclic rewritable if abc is equal to cab or bca. Note that ab is cyclic rewrtable if $ab = ba$, giving another natural extension of commutativity. We define $\mathrm{P}_n^{cyc}(\mathrm{G})$ to be the probability that a product $a_1 a_2 \ldots a_n$ is cyclic rewritable:

$$\mathrm{P}_n^{cyc}(\mathrm{G}) = \frac{|\{(a_1, a_2, \ldots, a_n) \in \mathrm{G}^n | a_1 a_2 \ldots a_n \text{ is cyclic rewritable}\}|}{|\mathrm{G}|^n}.$$

Of course, any Abelian group has $\mathrm{P}_n^{cyc}(\mathrm{G}) = 1$. Langley, Levitt, and Rower [4] show that for non-Abelian groups the upper bound is $\mathrm{P}_n^{cyc}(\mathrm{G}) \leq 1 - \frac{3}{2^{n+1}}$, and thus $\mathrm{P}_3^{cyc}(\mathrm{G}) \leq \frac{13}{16}$. We will show the following for dihedral groups.

Theorem 5.1. For $m \geq 3$,

$$P_3^{cyc}(D_m) = \frac{3m^2 + 9km - 4k^2}{8m^2} = \frac{3m^3 + 9km^2 - 4k^2 m}{|D_m|^3}$$

where $k = 1$ if m is odd and $k = 2$ if m is even.

Note that substituting $m = 4$ and $k = 2$ into **theorem 5.1** gives $P_3^{cyc}(D_4) = \frac{13}{16}$. This achieves the upper bound of $\frac{13}{16}$ for $P_3^{cyc}(G)$.

Next, we show two additional facts regarding $P_n(D_m)$. Clifton, Guichard, and Keef [1] show that if r is a positive integer, then there exists D_m such that $P_2(D_m) = \frac{r}{q}$ where q is relatively prime to r. We will generalize this result for $P_n(D_m)$:

Theorem 6.1. For all positive integers $r \geq 2$, $n \geq 2$, there exists D_m such that $P_n(D_m) = \frac{r}{q}$ where r and q are relatively prime.

Clifton, Guichard, and Keef [1] also show that there exists a direct product of i dihedral groups such that

$$P_2(D_{m_1} \oplus \ldots \oplus D_{m_i}) = \frac{1}{r}$$

for any positive integer r. The natural generalization would be that for a fixed n there exists a direct product of i dihedral groups such that $P_n(D_{m_1} \oplus \ldots \oplus D_{m_i}) = \frac{1}{r}$ for any positive integer r. However, we will show that this generalized statement is not true.

The proofs for the above theorems in this paper heavily depend on the fact that D_m is generated by two elements, a rotation ρ and a reflection ϕ, subject to the relations

$$\rho^m = \phi^2 = e \text{ and } \phi\rho = \rho^{-1}\phi.$$

The outline for the remainder of the paper is as follows. In the next section, we will show why $P_2(G) \leq \frac{5}{8}$ for all finite non-Abelian groups G as well as provide insight into why D_4 achieves this bound. We then prove **theorem 3.3**, **theorem 4.2**, and **theorem 5.1** in the three subsequent sections. We will conclude by demonstrating that the methods used in this paper can be extended to find formulas for other permutations of elements.

2 5/8 Bound on Commutativity

In this section we discuss the $\frac{5}{8}$ bound on commutativity, and give some background on dihedral group structure essential to the proofs in subsequent sections. First, let us consider a non-Abelian group G with center Z(G). For $a \in G$, let $C(a)$ denote the centralizer of a. We know Z(G) and $C(a)$ are a subgroups of G. If a is not in Z(G), then

$Z(G) \subsetneq C(a) \subsetneq G$. So by Lagrange's theorem, $|C(a)| \le \frac{|G|}{2}$ and $|Z(G)| \le \frac{|C(a)|}{2}$, implying $|Z(G)| \le \frac{|G|}{4}$ for all $a \notin G$. Note that Comm(G)$= \sum_{a\in G} |C(a)|$, so

$$
\begin{aligned}
P_2(G) &= \frac{1}{|G|^2} \sum_{a\in G} |C(a)| \\
&= \frac{1}{|G|^2} \sum_{a\in Z(G)} |G| + \frac{1}{|G|^2} \sum_{a\notin Z(G)} |C(a)| \\
&\le \frac{1}{|G|^2} \cdot \frac{|G|}{4} \cdot |G| + \frac{1}{|G|^2} \cdot \frac{3|G|}{4} \cdot \frac{|G|}{2} \\
&\le \frac{1}{4} + \frac{3}{8} \\
&\le \frac{5}{8}.
\end{aligned}
$$

When the center is its largest, $\frac{|G|}{4}$, we reach this bound. Since $Z(D_4) = \{r_0, r_{180}\}$, $P_2(D_4) = \frac{5}{8}$. When $|Z(G)| < \frac{|G|}{4}$, determining exact values of $P_2(G)$ becomes difficult since centeralizers of noncentral elements do not all have order $\frac{|G|}{2}$. By taking advantage of the structure of the dihedral groups, though, we can achieve precise results. As previously mentioned in the introduction, D_m is generated by a rotation, ρ, and a reflection, ϕ, under the relations $\rho^m = \phi^2 = e$ and $\phi\rho = \rho^{-1}\phi$. From this definition for D_m we can derive the relations $\rho^i\phi = \phi\rho^{-i}$ and $\rho^i\rho^j = \rho^j\rho^i$ to describe the behavior of the elements in D_m. The rotation ρ has order m, so any rotation can be written as ρ^i for some i. The reflection ϕ has order 2, and an arbitrary reflection can be written as $\phi\rho^i$. The relations are used to show that rotations commute with each other as well as provide the way for rotational elements to commute through reflection elements. As a result, the elements of D_m are the rotations $e = \rho^0, \rho^1, \dots, \rho^{m-1}$ and the reflections $\phi, \phi\rho^1, \dots, \phi\rho^{m-1}$. For example, in D_4, $\rho = r_{90}$ and $\phi = h$. Other elements can just be rewritten as combinations of ρ and ϕ, such as $v = \rho^2\phi$ and $r_{270} = \rho^3$. The letter k will be used to denote the number of rotations equal to their own inverse, so $k = 1$ for odd m and $k = 2$ for even m because ρ^0 and $\rho^{m/2}$ are the only possible such elements. These facts form the basis of the proofs in the following sections.

3 Generalization of the Reverse

In this section we prove our first generalized commutativity result for dihedral groups, the probability that a product of elements in D_m is equal to its reverse. We start with two lemmas that lead to the proof of **theorem 3.3**. For each element a_i in the product $a_1 a_2 \cdots a_n$, we consider the cases where a_i is a rotation or a reflection. In each case, we will move the ϕ's to the right in the product using the identity $\rho^i\phi = \phi\rho^{-i}$. Next, the identity $\rho^i\rho^j = \rho^j\rho^i$ is used to rearrange the rotations back into the original order for comparison.

For example, consider the case that a_1 and a_3 are the only reflections when determining the probability that $a_1 a_2 a_3 a_4 = a_4 a_3 a_2 a_1$. We would write our rotations in the form of ρ^{i_j} and reflections of the form $\phi\rho^{i_j}$.

We have

$$a_1 a_2 a_3 a_4 = (\phi\rho^{i_1})\rho^{i_2}(\phi\rho^{i_3})\rho^{i_4} = \rho^{-i_1}\rho^{-i_2}\rho^{i_3}\rho^{i_4}\phi^2 = \rho^{-i_1-i_2+i_3+i_4}$$

and

$$a_4 a_3 a_2 a_1 = \rho^{i_4}(\phi\rho^{i_3})\rho^{i_2}(\phi\rho^{i_1}) = \rho^{i_4}\rho^{-i_3}\rho^{-i_2}\rho^{i_1}\phi^2 = \rho^{i_1-i_2-i_3+i_4}.$$

So

$$\begin{aligned} \mathrm{P}((\phi\rho^{i_1})\rho^{i_2}(\phi\rho^{i_3})\rho^{i_4} = \rho^{i_4}(\phi\rho^{i_3})\rho^{i_2}(\phi\rho^{i_1})) &= \mathrm{P}(\rho^{-i_1-i_2+i_3+i_4} = \rho^{i_1-i_2-i_3+i_4}) \\ &= \mathrm{P}(\rho^{-i_1+i_3} = \rho^{i_1-i_3}) \\ &= \mathrm{P}(\rho^{z} = \rho^{-z}) \\ &= \frac{k}{m}, \end{aligned}$$

where $k = 1$ if m is odd and $k = 2$ if m is even. This is because we defined k as the number or rotations that are equal to their inverse, and there are m rotations in D_m.

Lemma 3.1. *Let σ be a permutation in S_n. In D_m, consider all products $a_1 a_2 \cdots a_n$ with a fixed sequence of rotations and reflections. That is, for each i, a_i is always a rotation or always a reflection. If there exists an a_i with an odd number of reflections to its left in $a_1 a_2 \cdots a_n$ and an even number to its left in $(a_1 a_2 \cdots a_n)^\sigma$, or vice versa, then*

$$\mathrm{P}(a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_n)^\sigma) = \frac{k}{m}.$$

If no such a_i exists, then

$$\mathrm{P}(a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_n)^\sigma) = 1.$$

Proof. Fix a sequence of reflections and rotations in $a_1 a_2 \cdots a_n$. Using the identities $\rho^i\phi = \phi\rho^{-i}$ and $\rho^i\rho^j = \rho^j\rho^i$, the products $a_1 a_2 \cdots a_n$ and $(a_1 a_2 \cdots a_n)^\sigma$ can each be written as $\rho^{\pm j_1 \pm j_2 \pm \ldots \pm j_n}\phi^l$ where $a_i = \rho^{j_i}$ or $a_i = \phi\rho^{j_i}$ and l is the number of reflection terms. The question of $\mathrm{P}(a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_n)^\sigma)$ is then equivalent to $\mathrm{P}(\rho^{\pm j_1 \pm j_2 \pm \cdots \pm j_n} = \rho^{\pm j_1 \pm j_2 \pm \cdots \pm j_n})$, where the $\pm$ may be different on each side. If a j_i term has the same sign in both products then since $\phi\rho^i = \rho^{-i}\phi$, there are an odd number of reflections before a_i or an even number of reflections before a_i in both product. If a j_i term has opposite signs in each product, then there are an odd number of reflections before a_i in one permutation and an even number of reflections before a_i in the other product. So if the number of reflections to the left of each a_i has the same parity in both products, every j_i has the same sign, and therefore $a_1a_2\cdots a_n = (a_1a_2\cdots a_n)^\sigma$. So

$$P(a_1a_2\cdots a_n = (a_1a_2\cdots a_n)^\sigma) = 1.$$

If the number of reflections to the left of some a_i has opposite parity in each product, then $P(a_1a_2\cdots a_n = (a_1a_2\cdots a_n)^\sigma) = P(\rho^z = \rho^{-z})$ where z is the sum of the j_i associated with all such a_i. So

$$P(a_1a_2\cdots a_n = (a_1a_2\cdots a_n)^\sigma) = \frac{k}{m}.$$

□

Lemma 3.2. *Let σ be a permutation in S_n. In D_m, consider all products $a_1a_2\cdots a_n$ with a fixed sequence of rotations and reflections. That is, for each i, a_i is always a rotation or always a reflection. If one of a_i and a_{i+1} is a reflection and the other a rotation, and the product $a_{i+1}a_i$ appears in $(a_1a_2\cdots a_n)^\sigma$, then $P(a_1a_2\cdots a_n = (a_1a_2\cdots a_n)^\sigma) = \frac{k}{m}$.*

Proof. Fix a sequence of rotations and reflection in $a_1a_2\cdots a_n$. First suppose a_i is a reflection and a_{i+1} is a rotation. In $a_1a_2\cdots a_n$, either a_i has an even and a_{i+1} has an odd number of reflections to the left, or a_i has odd and a_{i+1} has even number of reflections to the left. In $(a_1a_2\cdots a_n)^\sigma$,if $a_{i+1}a_i$ appears, then a_i and a_{i+1} both have on odd number of reflections or even number of reflections to their left. As a result, we know that either a_i or a_{i+1} has an odd number of reflections to the left in one product and an even number of reflections to the left in the other product, so by **lemma 3.1** we know that

$$P(a_1a_2\cdots a_n = (a_1a_2\cdots a_n)^\sigma) = \frac{k}{m}.$$

A similar argument shows the result if a_i is a rotation and a_{i+1} is a reflection. □

We are now ready to prove **theorem 3.3**.

Theorem 3.3. *For $m \geq 3$,*

$$P_n(D_m) = \begin{cases} \frac{m+k(2^n-1)}{2^n m} & \text{if } n \text{ is even} \\ P_{n-1}(D_m) & \text{if } n \text{ is odd} \end{cases}$$

where $k = 1$ if m is odd and $k = 2$ if m is even.

Proof. We'll determine $P(a_1a_2\cdots a_n = a_n\cdots a_2a_1)$ in the dihedral group D_m by looking at three cases: every a_i is a rotation, every a_i is a reflection, and there exists some a_i that is a rotation and some a_j that is a reflection.

Case 1: Each a_i is a rotation. Since half the elements of D_m are rotations, $\frac{1}{2^n}$ of the products $a_1a_2\cdots a_n$ fall into this case. Since rotations commute, $a_1a_2\cdots a_n = a_n\cdots a_2a_1$.

Case 2: At least one a_i is a rotation and another is a reflection. This is $\frac{2^n-2}{2^n}$ of the products because there are 2^n total rotation/reflection sequences, and two of those have every element as a rotation or every element as a reflection.

We then could find some pair of consecutive elements, $a_i a_{i+1}$, where one is a reflection and the other is a rotation. Since $a_{i+1}a_i$ appears in $a_n \cdots a_2 a_1$, by **lemma 3.2** we know that $\mathrm{P}(a_1 a_2 \cdots a_n = a_n \cdots a_1 a_2) = \frac{k}{m}$ for these $\frac{2^n-2}{2^n}$ cases.

Case 3: Each a_i is a reflection. This accounts for $\frac{1}{2^n}$ products. Each a_I has $i-1$ reflections to its left in $a_1 a_2 \cdots a_n$ and $n-i$ reflections to its left in $a_n \cdots a_2 a_1$. If n is even, then for each i, either $n-i$ is even and $i-1$ is off, or $n-i$ is odd and $i-1$ even. So by**lemma 3.1**,

$$\mathrm{P}(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) = \frac{k}{m}$$

for this case.

If n is odd, then $n-i$ and $i-1$ are both odd or both even for all i. By **lemma 3.1**,

$$\mathrm{P}(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) = 1$$

for this case.

Combining Cases 1, 2, and 3, if n is even we have

$$\begin{aligned}\mathrm{P}(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) &= \left(\frac{1}{2^n}\right)\left(\frac{2^n-2}{2^n}\right)\left(\frac{k}{m}\right) + \left(\frac{1}{2^n}\right)\left(\frac{k}{m}\right) \\ &= \frac{m}{2^n m} + \frac{(2^n-2)k}{2^n m} + \frac{k}{2^n m} \\ &= \frac{m + (2^n-1)k}{2^n m}\end{aligned}$$

and if n is odd we have

$$\begin{aligned}\mathrm{P}(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) &= \left(\frac{1}{2^n}\right)\left(\frac{2^n-2}{2^n}\right)\left(\frac{k}{m}\right) + \left(\frac{1}{2^n}\right)(1) \\ &= \frac{m}{2^n m} + \frac{(2^n-2)k}{2^n m} + \frac{m}{2^n m} \\ &= \frac{2m + (2^n-2)k}{2^n m} \\ &= \frac{m + (2^{n-1}-1)k}{2^{n-1} m}\end{aligned}$$

So for n even $\mathrm{P}_n(\mathrm{D}_m) = \frac{m+(2^n-1)k}{2^n m}$. For n odd, $\mathrm{P}_n(\mathrm{D}_m) = \frac{m+(2^{n-1}-1)k}{2^{n-1}m} = \mathrm{P}_{n-1}(\mathrm{D}_m)$.

□

4 Rewritability

In this section, we will prove the formula for $P_3^{rew}(D_m)$ given in **theorem 4.2**. We will start with a lemma that will be useful for the next two theorems.

Lemma 4.1. *For* $m \geq 3$*,*

$$P(\rho^i = \rho^{-i} \text{ or } \rho^j = \rho^{-j}) = \frac{2km - k^2}{m^2}$$

and

$$P(\rho^i = \rho^{-i} \text{ or } \rho^j = \rho^{-j} \text{ or } \rho^{i+j} = \rho^{-i-j}) = \frac{3km - 2k^2}{m^2}.$$

Proof. The probability that a rotation is equal to its inverse is $\frac{k}{m}$ since there are k rotations of order less than or equal to 2 and there are m total rotations. So

$$P(\rho^i = \rho^{-i} \text{ and } \rho^j = \rho^{-j}) = P(\rho^i = \rho^{-i})P(\rho^j = \rho^{-j}) = \frac{k}{m} \cdot \frac{k}{m} = \frac{k^2}{m^2}.$$

Thus,

$$\begin{aligned} P(\rho^i = \rho^{-i} \text{ or } \rho^j = \rho^{-j}) &= P(\rho^i = \rho^{-i}) + P(\rho^j = \rho^{-j}) - P(\rho^i = \rho^{-i} \text{ and } \rho^j = \rho^{-j}) \\ &= \frac{k}{m} + \frac{k}{m} - \frac{k^2}{m^2} \\ &= \frac{2km - k^2}{m^2}. \end{aligned}$$

For $P(\rho^i = \rho^{-i} \text{ or } \rho^j = \rho^{-j} \text{ or } \rho^{i+j} = \rho^{-i-j})$, we have an interesting situation where either 0, 1, or 3 of the conditions are true. We can never have exactly two of the conditions true since two of them true implies the third condition is also true. Thus we have to take this into account when applying the inclusion-exclusion principle. Specifically, we have

$$\begin{aligned} P(\rho^i = \rho^{-i} \text{ or } \rho^j = \rho^{-j} \text{ or } \rho^{i+j} = \rho^{-i-j}) &= P(\rho^i = \rho^{-i}) + P(\rho^j = \rho^{-j}) + P(\rho^{i+j} = \rho^{-i-j}) \\ &\quad - P(\rho^i = \rho^{-i} \text{ and } \rho^j = \rho^{-j}) - P(\rho^i = \rho^{-i} \text{ and } \rho^{i+j} = \rho^{-i-j}) \\ &\quad - P(\rho^{i+j} = \rho^{-i-j} \text{ and } \rho^j = \rho^{-j}) \\ &\quad + P(\rho^i = \rho^{-i} \text{ and } \rho^j = \rho^{-j} \text{ and } \rho^{i+j} = \rho^{-i-j}) \\ &= \frac{k}{m} + \frac{k}{m} + \frac{k}{m} - \frac{k^2}{m^2} - \frac{k^2}{m^2} - \frac{k^2}{m^2} + \frac{k^2}{m^2} \\ &= \frac{3k}{m} - \frac{2k^2}{m^2} \\ &= \frac{3km - 2k^2}{m^2}. \end{aligned}$$

□

We now turn to the proof of **theorem 4.2**.

Theorem 4.2. *For* $m \geq 3$,

$$P_3^{rew}(D_m) = \frac{3m^2 + 3km - 2k^2}{4m^2}$$

where $k = 1$ *if* m *is odd and* $k = 2$ *if* m *is even.*

Proof. Let the rotation component of a_j be ρ^{i_j}. We consider the following cases to determine when $a_1 a_2 a_3$ is equal to a rearrangement of itself.

Case 1: All terms are rotations. Then we know that all the elements commute, so $a_1 a_2 a_3$ equals every other rearrangement of a_1, a_2, and a_3.

Case 2: Only a_1 is a reflection. Then $a_1 a_2 a_3 = a_1 a_3 a_2$ since a_2 and a_3 are both rotations and therefore commute.

Case 3: Only a_2 is a reflection. Then we are not guaranteed that $a_1 a_2 a_3$ is equal to some other rearrangement. We'll consider this case in more detail below.

Case 4: Only a_3 is a reflection. Then $a_1 a_2 a_3 = a_2 a_1 a_3$ since a_1 and a_2 commute.

Case 5: Only a_1 and a_2 are reflections. Then $a_1 a_2 a_3 = a_3 a_1 a_2$ since $a_1 a_2$ is a rotation and therefore commutes with the rotation a_3

Case 6: Only a_1 and a_3 are reflections. Then we are not guaranteed that $a_1 a_2 a_3$ is equal to some other rearrangement. We will also consider this case below.

Case 7: Only a_2 and a_3 are reflections. Then $a_1 a_2 a_3 = a_2 a_3 a_1$ for the same reason as Case 5.

Case 8: If all three elements are reflections, then $a_1 a_2 a_3 = a_3 a_2 a_1$ because

$$\begin{aligned} a_1 a_2 a_3 &= \phi\rho^{i_1}\phi\rho^{i_2}\phi\rho^{i_3} \\ &= \rho^{-i_1+i_2-i_3}\phi \\ &= \rho^{-i_3+i_2-i_1}\phi \\ &= \phi\rho^{i_3}\phi\rho^{i_2}\phi\rho^{i_1} \\ &= a_3 a_2 a_1. \end{aligned}$$

Now, we'll look at Cases 3 and 6 in more depth. Let's first look at the case where only a_2 is a reflection.

1. To determine the conditions for $a_1a_2a_3 = a_1a_3a_2$, we have
$$a_1a_2a_3 = \rho^{i_1}(\phi\rho^{i_2})\rho^{i_3} = \rho^{i_1-i_2-i_3}$$
and
$$a_1a_3a_2 = \rho^{i_1}\rho^{i_3}(\phi\rho^{i_2}) = \rho^{i_1-i_2+i_3}.$$
So $a_1a_2a_3 = a_1a_3a_2$ if and only if $\rho^{-i_3} = \rho^{i_3}$.

2. To determine the conditions for $a_1a_2a_3 = a_2a_1a_3$, we have
$$a_1a_2a_3 = \rho^{i_1}(\phi\rho^{i_2})\rho^{i_3} = \rho^{i_1-i_2-i_3}$$
and
$$a_2a_1a_3 = (\phi\rho^{i_2})\rho^{i_1}\rho^{i_3} = \rho^{-i_1-i_2-i_3}.$$
So $a_1a_2a_3 = a_2a_1a_3$ if and only if $\rho^{-i_1} = \rho^{i_1}$.

3. To determine the conditions for $a_1a_2a_3 = a_2a_3a_1$, we have
$$a_1a_2a_3 = \rho^{i_1}(\phi\rho^{i_2})\rho^{i_3} = \rho^{i_1-i_2-i_3}$$
and
$$a_2a_3a_1 = (\phi\rho^{i_2})\rho^{i_3}\rho^{i_1} = \rho^{-i_1-i_2-i_3}.$$
So $a_1a_2a_3 = a_2a_3a_1$ if and only if $\rho^{i_1} = \rho^{-i_1}$.

4. To determine the conditions for $a_1a_2a_3 = a_3a_1a_2$, we have
$$a_1a_2a_3 = \rho^{i_1}(\phi\rho^{i_2})\rho^{i_3} = \rho^{i_1-i_2-i_3}$$
and
$$a_3a_1a_2 = \rho^{i_3}\rho^{i_1}(\phi\rho^{i_2}) = \rho^{i_1-i_2+i_3}.$$
So $a_1a_2a_3 = a_3a_1a_2$ if and only if $\rho^{-i_3} = \rho^{i_3}$.

5. To determine the conditions for $a_1a_2a_3 = a_3a_2a_1$, we have
$$a_1a_2a_3 = \rho^{i_1}(\phi\rho^{i_2})\rho^{i_3} = \rho^{i_1-i_2-i_3}$$
and
$$a_3a_2a_1 = \rho^{i_3}(\phi\rho^{i_2})\rho^{i_1} = \rho^{-i_1-i_2+i_3}.$$
So $a_1a_2a_3 = a_3a_2a_1$ if and only if $\rho^{i_1-i_3} = \rho^{-i_1+i_3}$.

Thus we know the probability that $a_1a_2a_3$ can be rewritten as some other rearrangement when only a_2 is a reflection is equivalent to finding the probability that $\rho^{i_3} = \rho^{-i_3}, \rho^{i_1} = \rho^{-i_1}$, or $\rho^{i_1-i_3} = \rho^{-i_1+i_3}$. So, by **lemma 4.1**, if a_2 is the only reflection, then the probability that $a_1a_2a_3$ is equal to some other rearrangement is $\frac{3km-2k^2}{m^2}$.

Now we will look at the case where only a_1 and a_3 are reflections.

1. To determine the conditions for $a_1a_2a_3 = a_1a_3a_2$, we have
$$a_1a_2a_3 = (\phi\rho^{i_1})\rho^{i_2}(\phi\rho^{i_3}) = \rho^{-i_1-i_2+i_3}$$
and
$$a_1a_3a_2 = (\phi\rho^{i_1})(\phi\rho^{i_3})\rho^{i_2} = \rho^{-i_1+i_2+i_3}.$$
So $a_1a_2a_3 = a_1a_3a_2$ if and only if $\rho^{-i_2} = \rho^{i_2}$.

2. To determine the conditions for $a_1a_2a_3 = a_2a_1a_3$, we have
$$a_1a_2a_3 = (\phi\rho^{i_1})\rho^{i_2}(\phi\rho^{i_3}) = \rho^{-i_1-i_2+i_3}$$
and
$$a_2a_1a_3 = \rho^{i_2}(\phi\rho^{i_1})(\phi\rho^{i_3}) = \rho^{-i_1+i_2+i_3}.$$
So $a_1a_2a_3 = a_2a_1a_3$ if and only if $\rho^{-i_2} = \rho^{i_2}$.

3. To determine the conditions for $a_1a_2a_3 = a_2a_3a_1$, we have
$$a_1a_2a_3 = (\phi\rho^{i_1})\rho^{i_2}(\phi\rho^{i_3}) = \rho^{-i_1-i_2+i_3}$$
and
$$a_2a_3a_1 = \rho^{i_2}(\phi\rho^{i_3})(\phi\rho^{i_1}) = \rho^{i_1+i_2-i_3}.$$
So $a_1a_2a_3 = a_2a_3a_1$ if and only if $\rho^{-i_1-i_2+i_3} = \rho^{i_1+i_2-i_3}$.

4. To determine the conditions for $a_1a_2a_3 = a_3a_1a_2$, we have
$$a_1a_2a_3 = (\phi\rho^{i_1})\rho^{i_2}(\phi\rho^{i_3}) = \rho^{-i_1-i_2+i_3}$$
and
$$a_3a_1a_2 = (\phi\rho^{i_3})(\phi\rho^{i_1})\rho^{i_2} = \rho^{i_1+i_2-i_3}.$$
So $a_1a_2a_3 = a_3a_1a_2$ if and only if $\rho^{-i_1-i_2+i_3} = \rho^{i_1+i_2-i_3}$.

5. To determine the conditions for $a_1a_2a_3 = a_3a_2a_1$, we have
$$a_1a_2a_3 = (\phi\rho^{i_1})\rho^{i_2}(\phi\rho^{i_3}) = \rho^{-i_1-i_2+i_3}$$
and
$$a_3a_2a_1 = (\phi\rho^{i_3})\rho^{i_2}(\phi\rho^{i_1}) = \rho^{i_1-i_2-i_3}.$$
So $a_1a_2a_3 = a_3a_2a_1$ if and only if $\rho^{i_1-i_3} = \rho^{-i_1+i_3}$.

Thus we know the probability that $a_1a_2a_3$ can be rewritten as some other rearrangement when only a_1 and a_3 are reflections is equivalent to finding the probability that $\rho^{i_2} = \rho^{-i_2}, \rho^{i_1-i_2-i_3} = \rho^{-i_1+i_2+i_3}$, or $\rho^{i_1-i_3} = \rho^{-i_1+i_3}$ when only a_1 and a_3 are reflections. Because $i_2 + (i_1 - i_2 - i_3) = i_1 - i_3$, we can apply **lemma 4.1**. Thus, if a_2 is the only reflection, then the probability that $a_1a_2a_3$ is equal to some other rearrangement is $\frac{3km-2k^2}{m^2}$.

So, for $\frac{6}{8}$ of the cases, we are guaranteed that $a_1a_2a_3$ can be rewritten as another rearrangement of the terms. For the other $\frac{2}{8}$ cases, $a_1a_2a_3$ can only be rewritten $\frac{3km-k^2}{m^2}$ of the time. Therefore the probability is

$$\begin{aligned} P_3^{rew}(D_m) &= \frac{3}{4} + \frac{1}{4}\left(\frac{3km-2k^2}{m^2}\right) \\ &= \frac{3m^2+3km-2k^2}{4m^2}. \end{aligned}$$

□

5 Cyclic Rewritability

In this section, we will prove **theorem 5.1** using **lemma 4.1**.

Theorem 5.1. *For $m \geq 3$,*

$$P_3^{cyc}(D_m) = \frac{3m^2+9km-4k^2}{8m^2} = \frac{3m^3+9km^2-4k^2m}{|D_m|^3}$$

where $k = 1$ if m is odd and $k = 2$ if m is even.

Proof. We use the same methods as in the proof of **theorem 4.2** to consider different cases for the elements in a product $a_1a_2a_3$.

Case 1: All terms are rotations. Then all the elements commute, so $a_1a_2a_3$ equals every other rearrangement of a_1, a_2, and a_3. Thus, the probability that $a_1a_2a_3$ equals another cyclic rearrangement is 1 for the triples in this case.

Case 2: Only a_1 is a reflection. Then $a_1a_2a_3 = a_3a_1a_2$ if and only if $\rho^{i_3} = \rho^{-i_3}$ and $a_1a_2a_3 = a_2a_3a_1$ if and only if $\rho^{i_2+i_3} = \rho^{-i_2-i_3}$. Thus $a_1a_2a_3$ is only equal to a cyclic rearrangment if ρ^{i_3} or $\rho^{i_2+i_3}$ equal their inverse. So, by **lemma 4.1**, $\frac{2km-k^2}{m^2}$ of the triples in this case are cyclic rewritable.

Case 3: Only a_2 is a reflection. Then $a_1a_2a_3 = a_3a_1a_2$ if and only if $\rho^{i_3} = \rho^{-i_3}$ and $a_1a_2a_3 = a_2a_3a_1$ if and only if $\rho^{i_1} = \rho^{-i_1}$. Thus $a_1a_2a_3$ is only equal to a cyclic rearrangment if ρ^{i_1} or ρ^{i_3} equal their inverse. So, by **lemma 4.1**, $\frac{2km-k^2}{m^2}$ of the triples in this case are cyclic rewritable.

Case 4: Only a_3 is a reflection. Then $a_1a_2a_3 = a_3a_1a_2$ if and only if $\rho^{i_1+i_2} = \rho^{-i_1-i_2}$ and $a_1a_2a_3 = a_2a_3a_1$ if and only if $\rho^{i_1} = \rho^{-i_1}$. Thus $a_1a_2a_3$ is only equal to a cyclic rearrangment if ρ^{i_1} or $\rho^{i_1+i_2}$ equal their inverse. So $\frac{2km-k^2}{m^2}$ of the triples in this case are cyclic rewritable.

Case 5: Only a_1 and a_2 are reflections. Then we are guaranteed that $a_1a_2a_3 = a_3a_1a_2$ because a_1a_2 is a rotation and therefore commutes with a_3. Thus, the probability that $a_1a_2a_3$ equals another cyclic rearrangement is 1 for the triples in this case.

Case 6: Only a_1 and a_3 are reflections. Then $a_1a_2a_3 = a_3a_1a_2$ if and only if $\rho^{i_1-i_2-i_3} = \rho^{-i_1+i_2+i_3}$ and $a_1a_2a_3 = a_2a_3a_1$ if and only if $\rho^{i_1-i_2-i_3} = \rho^{-i_1+i_2+i_3}$. Thus $a_1a_2a_3$ is only equal to another cyclic rearrangement if $\rho^{i_1-i_2-i_3} = \rho^{-i_1+i_2+i_3}$, so $\frac{k}{m}$ of the triples are cyclic rewritable.

Case 7: Only a_2 and a_3 are reflections. Then we are guaranteed that $a_1a_2a_3 = a_2a_3a_1$ because a_2a_3 is a rotation and therefore commutes with a_1. Thus, the probability that $a_1a_2a_3$ equals another cyclic rearrangement is 1 for the triples in this case.

Case 8: If all three elements are reflections, then $a_1a_2a_3 = a_3a_1a_2$ if and only if $\rho^{i_i-i_2} = \rho^{-i_1+i_2}$ and $a_1a_2a_3 = a_2a_3a_1$ if and only if $\rho^{i_2-i_3} = \rho^{-i_2+i_3}$. Thus $a_1a_2a_3$ only equals another cyclic rearrangment if $\rho^{i_1-i_2}$ or $\rho^{i_2-i_3}$ equal their inverse, so $\frac{2km-k^2}{m^2}$ of the triples are equal to another cyclic rearrangement in this case.

Hence, our probability is

$$\begin{aligned} \mathrm{P}_n^{cyc}(\mathrm{D}_m) &= \frac{3}{8} + \frac{1}{2}\left(\frac{2km-k^2}{m^2}\right) + \frac{1}{8}\frac{k}{m} \\ &= \frac{3m^2}{8m^2} + \frac{8km-4k^2}{8m^2} + \frac{km}{8m^2} \\ &= \frac{3m^2+9km-4k^2}{8m^2} \\ &= \frac{3m^3+9km^2-4k^2m}{8m^3} \\ &= \frac{3m^3+9km^2-4k^2m}{|\mathrm{D}_m|^3}. \end{aligned}$$

□

6 Generalizations for Properties of Dihedral Comutativity

In this section, we prove **theorem 6.1** and demonstrate why the $\mathrm{P}_n(\mathrm{D}_{m_1} \oplus \cdots \oplus \mathrm{D}_{m_i}) = \frac{1}{r}$ result does not generalize from $n = 2$ to arbitrary n. Recall that Clifton, Guichard, and

Koef [1] show that for any positive integer r, there exists a D_m such that $\mathrm{P}_2(\mathrm{D}_m) = \frac{r}{q}$ for some q relatively prime to r. Theorem 6 generalizes this for $\mathrm{P}_n(\mathrm{D}_m)$.

Theorem 6.1. *For all positive integers $r \geq 2$, $n \geq 2$, there exists D_m such that $\mathrm{P}_n(\mathrm{D}_m) = \frac{r}{q}$ where r and q are relatively prime.*

Proof. Since $\mathrm{P}_n(\mathrm{D}_m) = \mathrm{P}_{n-1}(\mathrm{D}_m)$ if n is odd, we will assume n is even. Let $m = (2^n - 1)(2^n r - 1)$. Then m is odd, so $k = 1$ in **theorem 3.3**. Therefore

$$\begin{aligned}\mathrm{P}_n(\mathrm{D}_m) &= \frac{m + k(2^n - 1)}{2^n m} \\ &= \frac{(2^n - 1)(2^n r - 1) + (2^n - 1)}{2^n (2^n - 1)(2^n r - 1)} \\ &= \frac{(2^n r - 1) + 1}{2^n (2^n r - 1)} \\ &= \frac{2^n r}{2^n (2^n r - 1)} \\ &= \frac{r}{2^n r - 1}.\end{aligned}$$

So we can set $q = 2^n r - 1$, which is relatively prime to r because it differs from a multiple of r by 1. Therefore, we can use $m = (2^n - 1)(2^n r - 1)$ to find a $\mathrm{P}_n(\mathrm{D}_m)$ with numerator of r relatively prime to denominator q. □

Clifton, Guichard, and Koef [1] also show there exists a direct product of i dihedral groups such that $\mathrm{P}_2(\mathrm{D}_{m_1} \oplus \cdots \oplus \mathrm{D}_{m_i}) = \frac{1}{r}$ for any positive integer r. A generalized statement would be that for a fixed n there exists a direct product of i dihedral groups such that $\mathrm{P}_n(\mathrm{D}_{m_1} \oplus \cdots \oplus \mathrm{D}_{m_i}) = \frac{1}{r}$ for any positive integer r. However, this generalized statement is not true.

Proof. By taking $n = 4$ and $r = 3$, we would be looking for $\mathrm{P}_4(\mathrm{D}_{m_1} \oplus \cdots \oplus \mathrm{D}_{m_i}) = \frac{1}{3}$. Recalling the upper bound $\mathrm{P}_n(\mathrm{G}) \leq \frac{1}{2} + \frac{1}{2^{n+1}}$ if n is even, we have $\mathrm{P}_4(\mathrm{G}) \leq \frac{17}{32}$. So $\mathrm{P}_4(\mathrm{G}_1)\mathrm{P}_4(\mathrm{G}_2) \leq \left(\frac{17}{32}\right)^2 < \frac{1}{3}$. Therefore, since $\mathrm{P}_n(\mathrm{G}_1 \oplus \mathrm{G}_2) = \mathrm{P}_n(\mathrm{G}_1)\mathrm{P}_n(\mathrm{G}_2)$, we have $\mathrm{P}_4(\mathrm{D}_{m_1} \oplus \mathrm{D}_{m_2}) < \frac{1}{3}$. So for the statement to be true, we would have to find a single D_m such that $\mathrm{P}_4(\mathrm{D}_m) = \frac{1}{3}$. From Theorem 1, $\mathrm{P}_4(\mathrm{D}_m) = \frac{m+15k}{16m}$. Setting this equal to $\frac{1}{3}$ gives

$$\begin{aligned}\frac{1}{3} &= \frac{15k + m}{16m} \\ 16m &= 45k + 3m \\ 13m &= 45k \\ m &= \frac{45k}{13},\end{aligned}$$

which is impossible since m must be an integer. Therefore we have shown that for $r = 3$ and $n = 4$, there cannot exist a D_m such that $P_4(D_m) = \frac{1}{3}$, so the generalizaed statement does not hold. □

7 Further Consideration

As we have seen, for a given permutation σ, we can determine how often $a_1 a_2 \cdots a_n$ equals $(a_1 a_2 \cdots a_n)^\sigma$ by checking each fixed sequence of rotations and reflections. Using **lemma 3.1** for each such sequence, we can find a generalization of **theorem 3.3** to show $P(a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_n)^\sigma)$. For example, if we define a word, w, of length n to be a product of n consecutive group elements and use the notation w^R to denote the reverse of word w, then we can use this method to find$P^x_n(G) = P(w_1 w_2 \cdots w_x = w^R_1 w^R_2 \cdots w^R_x)$ where each word has length n.

By following a similar structure to the proof of **theorem 3.3**, and using its result as a base case, it can be shown that

$$P^x_n(D_m) = \begin{cases} \frac{m+k(2^{xn}-1)}{2^{xn}m} & \text{if } n \text{ is even} \\ P^x_{n-1}(D_m) & \text{if } n \text{ is odd.} \end{cases}$$

Furthermore, by letting $n = 2$, we can use that result to show that

$$P(a_1 b_1 a_2 b_2 \cdots a_x b_x = b_1 a_1 b_2 a_2 \cdots b_x a_x) = \frac{(4^x - 1)k + m}{4^x m}.$$

Because D_4 often reaches the upper bound of $P(a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_n)^\sigma)$, this can be used to gain insight into a permutation's upper bound when investigating other generalizations of commutativity.

References

[1] Cody Clifton, David Guichard, and Patrick Keef. How commutative are direct products of dihedral groups? *Mathematics Magazine*, 84(2):137–140, 2011.

[2] E. J. Ellenberg. An upper bound for 3-rewriteability in finite groups. MS TR 91-02, 1991.

[3] W. H. Gustafson. What is the probability that two group elements commute? *The American Mathematical Monthly*, 80(9):1031–1034, 1973.

[4] Thomas Langley, David Levitt, and Joseph Rower. Two generalizations of the 5/8 bound on commutativity in nonabelian finite groups. *Mathematics Magazine*, 84:128–136, 04 2011.

[5] David J. Rusin. What is the probability that two elements of a finite group commute? *Pacific Journal of Mathematics*, 82(1):237 – 247, 1979.

Noah Heckenlively
Rose-Hulman Institute of Technology
heckenna@rose-hulman.edu

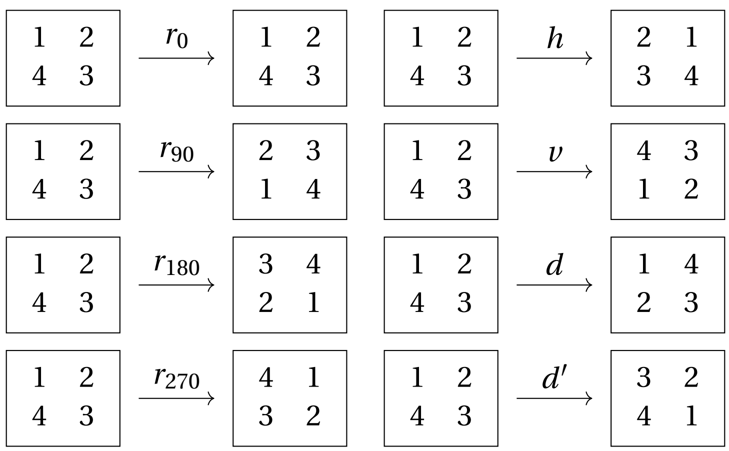

Figure 1: Elements of D_4