JSSE Journal of Science & Science Education
https://so04.tci-thaijo.org/index.php/JSSE
วารสารวิทยาศาสตร์และวิทยาศาสตร์ศึกษา
ปีที่ 5 เล่มที่ 2 (ก.ค. – ธ.ค. 2565) | xx

บทความวิจัย

ความน่าจะเป็นของคุณสมบัติย้อนกลับบนกรุปการหมุนรูป

กนกพร ช่างทอง[1,*] และวรารัตน์ อรัญ[2]

[1]ภาควิชาคณิตศาสตร์ สถิติและคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยอุบลราชธานี

[2]หลักสูตรวิทยาศาสตรบัณฑิต สาขาคณิตศาสตร์ ภาควิชาคณิตศาสตร์ สถิติและคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยอุบลราชธานี

**Email: kanokporn.c@ubu.ac.th*

รับบทความ: 31 มีนาคม 2565 แก้ไขบทความ: 30 เมษายน 2565 ยอมรับตีพิมพ์: 9 พฤษภาคม 2565

บทคัดย่อ

เป็นที่ทราบกันดีว่า คุณสมบัติหนึ่งที่สำคัญของกรุปคือ คุณสมบัติการสลับที่ เราสนใจว่ากรุปไม่สลับที่บางกรุปนั้นห่างไกลจากคุณสมบัติการสลับที่เพียงใด Gallian (2010) ได้อธิบายวิธีที่จะวัดค่าการสลับที่ของกรุปจำกัด โดยใช้แนวคิดของความน่าจะเป็น และกำหนดให้ $P_2(G)$ แทนความน่าจะเป็นที่สองสมาชิกที่ถูกเลือกมาแบบสุ่มนั้นสลับที่ได้ในกรุปจำกัด G ต่อมา Clifton, Guichard และ Keef (2011) ได้ศึกษาความน่าจะเป็นดังกล่าวบนกรุปการหมุนรูป D_n เมื่อ n เป็นจำนวนเต็มบวก และพบรูปทั่วไปของ $P_2(D_n)$ งานวิจัยของ Langley, Levitt และ Rower (2011) ขยายความคิดไปสู่ $P_n(G)$ ซึ่งเป็นความน่าจะเป็นที่ผลคูณของสมาชิก n ตัวในกรุปจำกัด G มีคุณสมบัติย้อนกลับ งานวิจัยนี้ ศึกษาความน่าจะเป็นดังกล่าวและพบรูปทั่วไปของความน่าจะเป็นที่ผลคูณของสมาชิก 3 ตัวในกรุปการหมุนรูปที่มีคุณสมบัติย้อนกลับ นั่นคือ $P_3(D_n)$

คำสำคัญ: ความน่าจะเป็น กรุปการหมุนรูป คุณสมบัติย้อนกลับ

Research Article

Probabilities of Reverse Property on Dihedral Groups

Kanokporn Changtong[1,*] and Wararat Arun[2]

[1]Department of Mathematics Statistics and Computer, Faculty of Science, Ubon Ratchathani University

[2]Bachelor of Science Program in Mathematics, Department of Mathematics Statistics and Computer, Faculty of Science, Ubon Ratchathani University

**Email: kanokporn.c@ubu.ac.th*

Received <31 March 2022>; Revised <30 April 2022>; Accepted <9 May 2022>

Abstract

It is well-known that one of the important group properties is commutativity. We are investigating how far a non-abelian group from commutativity. Gallian (2010) described a way to measure the commutativity of a finite group G by using probability concept. The $P_2(G)$ is defined as the probability that two randomly selected elements of the group actually commute. Later, Clifton, Guichard and Keef (2011) studied this probability on the dihedral group D_n where n is a positive integer, and found the general form of $P_2(D_n)$. Langley, Levitt and Rower (2011) generalized $P_2(G)$ to $P_n(G)$, where $P_n(G)$ is the probability that a product of n group elements equal to its reverse. The objectives of this research is to understand these probabilities and we found the general form of the probability that a product of 3 group elements in Dihedral groups D_n equal to its reverse, namely $P_3(D_n)$.

Keywords: Probability, dihedral group, reverse property

Introduction

One of the important group properties is commutativity. An abelian group G is a group with the property that $ab = ba$ for all a, b in G. Some groups fail for this property, for example, a group of all invertible 2×2 matrices under the multiplication with real entries, $M_2(\mathbb{R})$. The readers can find the contents on group theory in, for example, Rotman (1996), Nicholson (2012), and Gallian (2010) describes a way to measure the commutativity of a finite group G. Define $P_2(G)$ be the probability that two randomly selected elements of the group actually commute as follows.

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

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

Clifton, Guichard and Keef (2011) studied such probability on the dihedral group D_n where n is a positive integer. A **dihedral group** is the group of symmetries of a regular polygon which includes rotations and reflections. A **regular polygon** with n sides has n different symmetries, where $n \geq 3$ consisting of rotational symmetries and reflection symmetries. For $n = 4$, the dihedral group D_4 consists of 8 elements as presented in Figure 1.

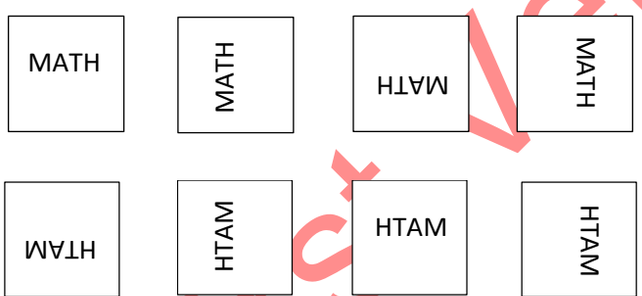

Figure 1 All elements in Dihedral group D_4

In other words, the dihedral group D_n is generated by two elements, r_n (for "rotation") and f_n (for "flip"), subject to the relation

$$r_n^n = f_n^2 = e_n \text{ and } f_n r_n = r_n^{-1} f_n,$$

where e_n is the identity of D_n. It follows that the elements of D_n can be written as

$$e_n, r_n, r_n^2, r_n^3, \ldots, r_n^{n-1}, f_n, r_n f_n, r_n^2 f_n, \ldots, r_n^{n-1} f_n.$$

Notice that the order of D_n denoted by $|D_n|$ is $2n$.

The following chart shows the commutativity of D_4, where a 1 indicates that the corresponding pair of elements commute, Sherman (1997).

	e_4	r_4	r_4^2	r_4^3	f_4	$r_4 f_4$	$r_4^2 f_4$	$r_4^3 f_4$
e_4	1	1	1	1	1	1	1	1
r_4	1	1	1	1	0	0	0	0

r_4^2	1	1	1	1	1	1	1	1
r_4^3	1	1	1	1	0	0	0	0
f_4	1	0	1	0	1	0	1	0
$r_4 f_4$	1	0	1	0	0	1	0	1
$r_4^2 f_4$	1	0	1	0	1	0	1	0
$r_4^3 f_4$	1	0	1	0	0	1	0	1

The chart produces forty 1s which means that there are forty pairs of the group elements commute. The set of these pairs is considered as the event, and the set of all ordered pairs of group elements as the sample space. So the probability $P_2(D_4) = 40/64 = 5/8$.

Clifton, Guichard and Keef (2011) found the general form of $P_2(D_n)$ as follows.

Theorem 1. If n is a positive integer, then

$$P_2(D_n) = \begin{cases} \dfrac{n+3}{4n}, & \text{if } n \text{ is odd;} \\ \dfrac{n+6}{4n}, & \text{if } n \text{ is even.} \end{cases}$$

Langley, Levitt and Rower (2011) generalized $P_2(G)$ to $P_n(G)$, where $P_n(G)$ is the probability that a product of n group elements equal to its reverse. Namely,

$$P_n(G) = \frac{Comm_n(G)}{|G|^n}$$

where $Comm_n(G) = |\{(a_1, a_2, \dots, a_n) \in G^n \mid a_1 a_2 \cdots a_n = a_n a_{n-1} \cdots a_2 a_1\}|$.

Objectives

The objectives of this research are to understand these probabilities on dihedral groups and to find the general form of the probability that a product of 3 group elements in Dihedral groups D_n equal to its reverse, namely $P_3(D_n)$.

Main Theorem

For the dihedral group D_n,

$$P_3(D_n) = \frac{Comm_3(D_n)}{|D_n|^3}$$

where $Comm_3(G) = |\{(a, b, c) \in D_n^3 \mid abc = cba\}|$. The triple $(a, b, c) \in D_n^3$ satisfies the **reverse property** if $abc = cba$.

Note that, on the dihedral group D_n, when n is even, the (rotate) element $r_n^{\frac{n}{2}}$ is itself inverse, that is $r_n^{-\frac{n}{2}} = \left(r_n^{\frac{n}{2}}\right)^{-1} = r_n^{\frac{n}{2}}$. For the convenience, we write the elements of D_n as

$$r, r^2, r^3, \dots, r^{n-1}, r^n = e, f, rf, r^2 f, \dots, r^{n-1} f.$$

Theorem 2. If n is a positive integer, then

$$P_3(D_n) = \begin{cases} \dfrac{n+3}{4n}, & \text{if } n \text{ is odd;} \\ \dfrac{n+6}{4n}, & \text{if } n \text{ is even.} \end{cases}$$

Proof Let $\mathcal{A} = \{(a,b,c) \in D_n^3 | abc = cba\}$ and $\mathcal{B} = \{(a,b,c) \in D_n^3 | (a,b,c)$ are of the following forms

1. (r^i, r^j, r^k), where$0 \le i,j,k < n$,
2. $(r^i, r^{-i}, r^j f)$, where $0 \le i,j < n$,
3. $(r^i, r^j f, r^i)$, where $0 \le i,j < n$,
4. $(r^j f, r^i, r^{-i})$, where $0 \le i,j < n$,
5. $(r^i, r^j f, r^j f)$, where $0 \le i,j < n$,
6. $(r^j f, r^i, r^j f)$, where $0 \le i,j < n$,
7. $(r^j f, r^j f, r^i)$, where $0 \le i,j < n$,
8. $(r^i f, r^j f, r^k f)$, where $0 \le i,j,k < n$,
9. $(r^i, r^{-i+\frac{n}{2}}, r^j f)$, where $0 \le i,j < n$ and n is even,
10. $(r^i, r^j f, r^{i+\frac{n}{2}})$, where $0 \le i,j < n$ and n is even,
11. $(r^j f, r^i, r^{-i+\frac{n}{2}})$, where $0 \le i,j < n$ and n is even,
12. $(r^i, r^j f, r^{j+\frac{n}{2}} f)$, where $0 \le i,j < n$ and n is even,
13. $(r^j f, r^i, r^{j+\frac{n}{2}} f)$, where $0 \le i,j < n$ and n is even,
14. $(r^j f, r^{j+\frac{n}{2}} f, r^i)$, where $0 \le i,j < n$ and n is even}.

To show that $\mathcal{A} \subseteq \mathcal{B}$, let $(a,b,c) \in \mathcal{A}$. Then a,b and c are either in the form r^i or $r^j f$ where $0 \le i,j < n$. There are all 8 patterns as follows.

Pattern 1. $(a,b,c) = (r^i, r^j, r^k)$, $0 \le i,j,k < n$.
Pattern 2. $(a,b,c) = (r^i, r^j, r^k f)$, $0 \le i,j,k < n$.
Pattern 3. $(a,b,c) = (r^i, r^j f, r^k)$, $0 \le i,j,k < n$.
Pattern 4. $(a,b,c) = (r^i f, r^j, r^k)$, $0 \le i,j,k < n$.
Pattern 5. $(a,b,c) = (r^i, r^j f, r^k f)$, $0 \le i,j,k < n$.
Pattern 6. $(a,b,c) = (r^i f, r^j, r^k f)$, $0 \le i,j,k < n$.
Pattern 7. $(a,b,c) = (r^i f, r^j f, r^k)$, $0 \le i,j,k < n$.
Pattern 8. $(a,b,c) = (r^i f, r^j f, r^k f)$, $0 \le i,j,k < n$.

In Pattern 1 and Pattern 8, it is obvious that $(a,b,c) = (r^i, r^j, r^k) \in \mathcal{B}$, and $(a,b,c) = (r^i f, r^j f, r^k f) \in \mathcal{B}$ for $0 \le i,j,k < n$.

Pattern 2. $(a,b,c) = (r^i, r^j, r^k f)$, $0 \le i,j,k < n$. It satisfies $abc = cba$ that is $r^i r^j r^k f = r^k f r^j r^i$. Then

$$\begin{aligned} r^i r^j r^k f = r^k f r^j r^i &\leftrightarrow r^{i+j+k} = r^{k-j-i} \\ &\leftrightarrow i+j+k \equiv k-j-i \pmod n \\ &\leftrightarrow 2i \equiv -2j \pmod n \end{aligned} \qquad (*)$$

If n is odd, then $(2,n)=1$. Equation (*) becomes $\equiv -i \pmod n$. If n is even, then $(2,n)=2$. Equation (*) becomes $j \equiv -i \pmod{\frac{n}{2}}$. Hence $j=-i+\frac{n}{2}q,\ q\in\mathbb{Z}$. If q is even, then $q=2t, t\in\mathbb{Z}$. We have $j \equiv -i+\frac{n}{2}q \equiv -i+\frac{n}{2}(2t) \equiv -i+nt \equiv -i \pmod n$. If q is odd, then $q \equiv 1 \pmod 2$. Thus $nq \equiv n \pmod{2n}$. Since $(2,2n)=2$, $\frac{n}{2}q \equiv \frac{n}{2} \pmod n$. It implies that

$$j \equiv -i+\frac{n}{2}q \equiv -i+\frac{n}{2} \pmod n$$

Therefore, in case n is even, we have either $j \equiv -i \pmod n$ or $j \equiv -i+\frac{n}{2} \pmod n$
Hence, in Pattern 2, for $n\in\mathbb{N}$ and $0\le i,j,k<n$, $(a,b,c)=\left(r^i,r^j,r^kf\right)=\left(r^i,r^{-i},r^kf\right)\in\mathcal{B}$.
In addition, when n is even, (a,b,c) can be in another form which

$$(a,b,c)=\left(r^i,r^j,r^kf\right)=\left(r^i,r^{-i+\frac{n}{2}},r^kf\right)\in\mathcal{B}.$$

For Pattern 3.-7., they can be proved in similar fashion.

Now, we show that $\mathcal{B}\subseteq\mathcal{A}$. Let $(a,b,c)\in\mathcal{B}$. It runs through each form. To show that $(a,b,c)\in\mathcal{A}$, we prove that $abc=cba$.

Case 1. (a,b,c) is of the form (r^i,r^j,r^k), where $0\le i,j,k<n$. The commutativity holds among the rotate elements. Then done.

Case 2. (a,b,c) is of the form (r^i,r^{-i},r^jf), where $0\le i,j<n$. Then
$r^ir^{-i}r^jf=r^jf=r^jfr^{-i}r^i$.

Case 3. (a,b,c) is of the form (r^i,r^jf,r^i), where $0\le i,j<n$. It is obvious.

Case 4. (a,b,c) is of the form (r^jf,r^i,r^{-i}), where $0\le i,j<n$. Then
$r^jfr^ir^{-i}=r^jf=r^{-i}r^ir^jf$.

Case 5. (a,b,c) is of the form (r^i,r^jf,r^jf), where $0\le i,j<n$. Then
$r^ir^jfr^jf=r^ir^jr^{-j}f^2=r^i=r^jr^{-j}f^2r^i=r^jr^{-j}ffr^i=r^jfr^jfr^i$.

Case 6. (a,b,c) is of the form (r^jf,r^i,r^jf), where $0\le i,j<n$. It is obvious.

Case 7. (a,b,c) is of the form (r^jf,r^jf,r^i), where $0\le i,j<n$. Then
$r^jfr^jfr^i=r^jr^{-j}f^2r^i=r^i=r^ir^jr^{-j}f^2=r^ir^jr^{-j}ff=r^ir^jfr^jf$.

Case 8. (a,b,c) is of the form (r^if,r^jf,r^kf), where $0\le i,j,k<n$.
$r^ifr^jfr^kf=r^{i-j+k}f^3=r^{k-j+i}f=r^kf^2r^{-j}r^if=r^kffr^{-j}r^if=r^kfr^jfr^if$.

Case 9. (a,b,c) is of the form $(r^i,r^{-i+\frac{n}{2}},r^jf)$, where $0\le i,j<n$ and n is even. Then

$$\begin{aligned}\left(r^i\right)\left(r^{-i+\frac{n}{2}}\right)\left(r^jf\right)&=r^{\frac{n}{2}+j}f\\&=r^{\frac{n}{2}+j}fr^{-i+i}\\&=r^j(r^n)^{\frac{1}{2}}(f^2)^{\frac{1}{2}}r^{-i+i}\\&=r^j(f^2)^{\frac{1}{2}}(r^n)^{\frac{1}{2}}r^{-i+i}\end{aligned}$$

$$= (r^j f)\left(r^{-i+\frac{n}{2}}\right)(r^i).$$

Case 10. (a,b,c) is of the form $(r^i, r^j f, r^{i+\frac{n}{2}})$, where $0 \le i,j < n$ and n is even. Since the (rotate) element $r^{\frac{n}{2}}$ is itself inverse, we obtain that

$$(r^i)(r^j f)\left(r^{i+\frac{n}{2}}\right) = r^{i+j-i-\frac{n}{2}} f = r^{i-\frac{n}{2}} r^j r^{-i} f = \left(r^{i+\frac{n}{2}}\right)(r^j f)(r^i).$$

Case 11. (a,b,c) is of the form $(r^j f, r^i, r^{-i+\frac{n}{2}})$, where $0 \le i,j < n$ and n is even. By the same argument of case 10, we obtain that

$$(r^j f)(r^i)\left(r^{-i+\frac{n}{2}}\right) = \left(r^{-i+\frac{n}{2}}\right)(r^i)(r^j f).$$

Case 12. (a,b,c) is of the form $(r^i, r^j f, r^{j+\frac{n}{2}} f)$, where $0 \le i,j < n$ and n is even. Since the (rotate) element $r^{\frac{n}{2}}$ is itself inverse, we obtain that

$$(r^i)(r^j f)\left(r^{j+\frac{n}{2}} f\right) = r^{i+j-j-\frac{n}{2}} f^2 = r^{j-\frac{n}{2}} r^{i-j} = r^{j+\frac{n}{2}} f^2 r^{-j} r^i = \left(r^{j+\frac{n}{2}} f\right)(r^j f)(r^i).$$

By the same argument of case 12, we obtain cases 13 and 14 which are as follows.

Case 13. (a,b,c) is of the form $(r^j f, r^i, r^{j+\frac{n}{2}} f)$, where $0 \le i,j < n$ and n is even.

Case 14. (a,b,c) is of the form $(r^j f, r^{j+\frac{n}{2}} f, r^i)$, where $0 \le i,j < n$ and n is even.

Now, we count how many triples for each case.

1. The pattern (r^i, r^j, r^k), where $0 \le i,j,k < n$, gives different n^3 triples.
2. The pattern $(r^i, r^{-i}, r^j f)$, where $0 \le i,j < n$, gives different n^2 triples.
3. The pattern $(r^i, r^j f, r^i)$, where $0 \le i,j < n$, gives different n^2 triples.
4. The pattern $(r^j f, r^i, r^{-i})$, where $0 \le i,j < n$, gives different n^2 triples.
5. The pattern $(r^i, r^j f, r^j f)$, where $0 \le i,j < n$, gives different n^2 triples.
6. The pattern $(r^j f, r^i, r^j f)$, where $0 \le i,j < n$, gives different n^2 triples.
7. The pattern $(r^j f, r^j f, r^i)$, where $0 \le i,j < n$, gives different n^2 triples.
8. The pattern $(r^i f, r^j f, r^k f)$, where $0 \le i,j,k < n$, gives different n^3 triples.
9. The pattern $(r^i, r^{-i+\frac{n}{2}}, r^j f)$, where $0 \le i,j < n$ and n is even, gives different n^2 triples.
10. The pattern $(r^i, r^j f, r^{i+\frac{n}{2}})$, where $0 \le i,j < n$ and n is even, gives different n^2 triples.
11. The pattern $(r^j f, r^i, r^{-i+\frac{n}{2}})$, where $0 \le i,j < n$ and n is even, gives different n^2 triples.
12. The pattern $(r^i, r^j f, r^{j+\frac{n}{2}} f)$, where $0 \le i,j < n$ and n is even, gives different n^2 triples.
13. The pattern $(r^j f, r^i, r^{j+\frac{n}{2}} f)$, where $0 \le i,j < n$ and n is even, gives different n^2 triples.
14. The pattern $(r^j f, r^{j+\frac{n}{2}} f, r^i)$, where $0 \le i,j < n$ and n is even, gives different n^2 triples.

For n is odd, the triples formed by 3 group elements in Dihedral groups D_n where its product equal to its reverse satisfy case 1-8. Whereas, for n is even, the triples satisfy case 1-14. Hence, for calculating the event, there are $2n^3 + 6n^2$ triples when n is odd and there are $2n^3 + 12n^2$ triples when n is even. The sample space $|D_n|^3 = 8n^3$.

When n is odd, the probability

$$P_3(D_n) = \frac{Comm_3(D_n)}{|D_n|^3} = \frac{2n^3+6n^2}{8n^3} = \frac{n+3}{4n}.$$

When n is even, the probability

$$P_3(D_n) = \frac{Comm_3(D_n)}{|D_n|^3} = \frac{2n^3+12n^2}{8n^3} = \frac{n+6}{4n}.$$

Conclusion and Discussion

It turns out that the general forms for $P_2(D_n)$ and $P_3(D_n)$ are the same, but the proofs show that they both have different cases which lead to different counting. The counting on $P_3(D_n)$ is more complicated. The further work that could be done is to find the general form for $P_n(D_n)$ but it may need more advance counting. Other works are to investigate the probability on other properties which are, for a, b, c in a group G,

$$abc = acb, abc = bac, abc = bca \text{ and } abc = cab.$$

Acknowledgements

The author is very grateful to the Department of Mathematics, Statistics and Computer, Faculty of Science, Ubon Ratchathani University for all the facilities' support.

References

Clifton, C., Guichard, D. and Keef, P. (2011). How commutative are direct products of Dihedral groups. **Mathematics Magazine**, 84, 137-140.

Gallian, J. (2010). **Contemporary Abstract Algebra (7th ed)**. Belmont, CA: Brooks Cole.

Langley, T., Levitt, D. and Rower, J. (2011). Two generalizations of 5/8 bound on commutativity in nonabelian finite groups. **Mathematics Magazine**, 84, 128-136.

Nicholson, W. K., (2012). **Introduction to Abstract Algebra (4th ed)**. New Jersey: Wiley.

Rotman, J. J. (1996). **A first Course in Abstract Algebra**. New Jersey: Prentice Hall.

Sherman, G.J. (1997). Trying to do group theory with undergraduates and computers. **Journal of Symbolic Computation**.23, 577-587.