

S.T. Yau School Science Award (Asia)

2020

Research Report

The Team

Registration Number: Math-033

Name of team member: On Ki LUO

School: Pui Ching Middle School

Country: Hong Kong, China

Name of supervising teacher: Ho Fung LEE

Position: Mathematics Teacher

School: Pui Ching Middle School

Country: Hong Kong, China

Title of Research Report

Investigation on i -commuting probabilities on finite groups

Date

31 August 2020

2020 S.-T. Yau High School Science Award

Investigation on i -commuting probabilities on finite groups

On Ki Luo

Abstract

There is a well-known theorem in group theory called **the 5/8 theorem**. It states that if the probability of two randomly chosen elements in a finite group that commute exceeds $5/8$, then the group is abelian. The **commuting probability** is widely investigated by mathematicians throughout the years. In this project, we generalize the commuting probabilities to the i -commuting probabilities on finite groups, which consider the orders of the commutators.

The **i -commuting probability** $p_i(G)$ is defined as the probability of two randomly chosen elements x, y in a finite group G such that the order of their commutator is i , i.e. $\text{ord}([x, y]) = i$. With this definition, we proceed to compute the i -commuting probabilities of **dihedral groups**, **dicyclic groups** and **meta-cyclic groups**. We soon discover that they are of similar structures and hence the same method can be applied to compute their i -commuting probabilities. We transfer calculating the i -commuting probabilities of meta-cyclic groups into a number-theoretic problem and provide general formulae of some special cases of meta-cyclic groups.

We notice that some of the i -commuting probabilities of dihedral groups and dicyclic groups are the same. This inspires us to investigate on the abstract relation between groups with the same i -commuting probability for all $i \in \mathbb{N}$. In fact, this relation is called **isoclinism**, which is an equivalence relation. We first propose that $p_i(G) = p_i(H)$ for all $i \in \mathbb{N}$ if two groups G and H are isoclinic, and successfully prove this conjecture. Moreover, we develop some useful tools concerning isoclinism to help us with the computation of other groups.

Before the final computation of i -commuting probabilities of groups of small orders, we further investigate some unknown groups. Although we cannot find the general formulae of **symmetric groups** and **alternating groups**, we have obtained the lower bounds of $p_i(S_n)$ for particular i 's. The necessary and sufficient condition for $p_i(S_n) > 0$ and $p_i(A_n) > 0$ is also found. Moreover, we deduce the general formula of **generalized dihedral groups**. At last, we provide a number of examples of i -commuting probabilities of groups of orders less than 30, for instance, $\text{SmallGroup}(16,13)$, $C_9 \rtimes C_3$, $S_3 \times C_5$, and $(C_3 \times C_3) \rtimes C_2$.

Keywords: group theory, commuting probability, commutator subgroup, isoclinism, dihedral group, dicyclic group, meta-cyclic group, generalized dihedral group, symmetric group, alternating group

Acknowledgement

We would like to thank Mr Tin Wai Lau and Mr Yan Lam Fan for the advice for improvements. We would also like to thank Mr Tsz Fung Yu for providing assistance in programming.

2020 S.-T. Yau High School Science Award


Commitment on Academic Honesty and Integrity

We hereby declare that we

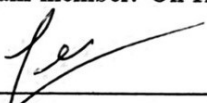
1. are fully committed to the principle of honesty, integrity and fair play throughout the competition.
2. actually perform the research work ourselves and thus truly understand the content of the work.
3. observe the common standard of academic integrity adopted by most journals and degree theses.
4. have declared all the assistance and contribution we have received from any personnel, agency, institution, etc. for the research work.
5. undertake to avoid getting in touch with assessment panel members in a way that may lead to direct or indirect conflict of interest.
6. undertake to avoid any interaction with assessment panel members that would undermine the neutrality of the panel member and fairness of the assessment process.
7. observe all rules and regulations of the competition.
8. agree that the decision of YHSA(Asia) is final in all matters related to the competition.

We understand and agree that failure to honour the above commitments may lead to disqualification from the competition and/or removal of reward, if applicable; that any unethical deeds, if found, will be disclosed to the school principal of team member(s) and relevant parties if deemed necessary; and that the decision of YHSA(Asia) is final and no appeal will be accepted.

(Signatures of full team below)

X 

 Name of team member: On Ki LUO

X 

 Name of supervising teacher: Ho Fung LEE

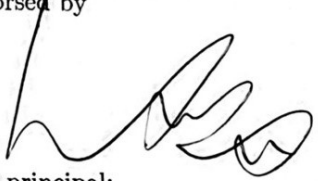
Noted and endorsed by
(signature) 
Name of school principal: Lik Ko HO

Table of Contents

Abstract	i
Acknowledgement	ii
Commitment on Academic Honesty and Integrity	iii
1 Introduction	1
1.1 Definition of i -commuting probability	1
1.2 Review on group theory	2
2 i-commuting probabilities of meta-cyclic groups	5
2.1 Dihedral group	5
2.2 Dicyclic group	10
2.3 Meta-cyclic group	11
3 Isoclinism	16
4 i-commuting probabilities of groups of small orders	19
4.1 Generalized dihedral group	19
4.2 Symmetric groups & Alternating groups	20
4.3 List of i -commuting probabilities of groups of orders less than 30	22
5 Conclusion	27
Reference	28
Appendix	29

1 Introduction

This project is inspired by a result in group theory called the 5/8 theorem [1], which concerns the probability when a randomly chosen pair of elements in G commutes. The commuting probability is defined below:

Definition 1.1 (commuting probability)

Let G be a finite group. Define the **commuting probability** $p(G)$ to be the probability that two randomly chosen elements commute, i.e.

$$p(G) = \frac{1}{|G|^2} \#\{(x, y) \in G^2 \mid xy = yx\}.$$

Notice that G is abelian if and only if $p(G) = 1$.

The 5/8 theorem concerns the upper bound of the commuting probabilities of finite non-abelian groups, it states that:

Theorem 1.2 (The 5/8 theorem [1])

Let G be a finite non-abelian group. Then $p(G) \leq 5/8$.

1.1 Definition of i -commuting probability

Recall that for $g \in G$, the **order** of g , denoted by $\text{ord}(g)$, is defined to be the smallest positive integer k such that $g^k = e$. And for $x, y \in G$, the commutator of x and y is defined as $[x, y] = xyx^{-1}y^{-1}$.

In Definition 1.1, one may notice that $xy = yx$ is equivalent to $xyx^{-1}y^{-1} = e$, i.e. $\text{ord}([x, y]) = 1$. With this idea, we generalize this notion by considering the orders of the commutators.

Definition 1.3 (i -commuting probability)

Let G be a finite group and $i \in \mathbb{N}$. Define the **i -commuting probability** $p_i(G)$ to be the probability that the order of two randomly chosen elements is i , i.e.

$$p_i(G) = \frac{1}{|G|^2} \#\{(x, y) \in G^2 \mid \text{ord}([x, y]) = i\}.$$

Notice that $p_1(G) = p(G)$ is the classical commuting probability as in Definition 1.1.

In this paper, we aim to find the i -commuting probabilities of finite groups. The following lemma is another useful yet trivial characterization of the i -commuting probability:

Lemma 1.4

Let G be a finite group. Define the **commutator map** $f : G \times G \rightarrow G$ given by $(x, y) \mapsto [x, y]$, and $G_i = \{g \in G \mid \text{ord}(g) = i\} \subseteq G$. Then

$$p_i(G) = \frac{1}{|G|^2} |f^{-1}(G_i)|.$$

Proof. This follows from the definition of preimage, i.e. $f^{-1}(G_i) = \{(x, y) \in G^2 \mid f(x, y) \in G_i\}$. □

Here we provide two trivial facts concerning the i -commuting probability. The first one helps us to compute $p_i(G)$ for a certain i when given other i -commuting probabilities of G .

Proposition 1.5

Let G be a finite group. For any $i \in \mathbb{N}$, $p_i(G) > 0$ only if i divides $|G|$.

Proof. If $p_i(G) > 0$, then there exist an element $[x, y] \in G$ such that $\text{ord}([x, y]) = i$. This shows $i \mid |G|$ by Lagrange's theorem [2]: for any $g \in G$, $g^{|G|} = e$, where e denotes the identity of the group G . \square

Proposition 1.6

For any finite group G ,

$$\sum_{i \in \mathbb{N}} p_i(G) = 1.$$

Notice that it is a finite sum.

Proof. Notice that $\{G_i\}_{i \in \mathbb{N}}$ partition G . Hence

$$f^{-1}(G) = \bigcup_{i \in \mathbb{N}} f^{-1}(G_i),$$

where it is a disjoint union. This gives

$$|G|^2 = |f^{-1}(G)| = \sum_{i \in \mathbb{N}} |f^{-1}(G_i)|.$$

The first equality comes from the fact that f is surjective. \square

In this project, we will first compute the i -commuting probabilities of some elementary finite groups, namely dihedral groups, dicyclic groups and meta-cyclic groups. We then try to find the abstract relation between groups with the same i -commuting probability for all $i \in \mathbb{N}$. At last, a list of all i -commuting probabilities of groups of orders less than 30 is computed using the methods we developed.

1.2 Review on group theory

We first provide some elementary properties of commutator and commutator subgroup before our investigation [2].

Proposition 1.7 (Properties of commutator)

Let G, H be groups and $x, y \in G$. We have:

1. $[x, y] = [y, x]^{-1}$.
2. If $\phi : G \rightarrow H$ is a group homomorphism, then

$$\phi([x, y]) = [\phi(x), \phi(y)].$$

In particular, we have $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$, for any $g \in G$.

Proof. 1. This follows from the fact that $[x, y][y, x] = (xyx^{-1}y^{-1})(yxy^{-1}x^{-1}) = e$ and $[y, x][x, y] = (yxy^{-1}x^{-1})(xyx^{-1}y^{-1}) = e$.

2. Since ϕ is a group homomorphism, we have

$$\phi([x, y]) = \phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x^{-1})\phi(y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = [\phi(x), \phi(y)].$$

The particular case follows from setting $\phi : G \rightarrow G$ to be the group homomorphism, given by $x \mapsto gxg^{-1}$. \square

Definition 1.8 (Commutator subgroup)

Let G be a group. Define $G' := \langle [x, y] \mid x, y \in G \rangle$ to be the **commutator subgroup** of G .

Proposition 1.9 (Properties of commutator subgroup)

Let G be a group and G' be its commutator subgroup. Then:

1. G' is a normal subgroup of G .
2. The quotient group G/G' is abelian.
3. If N is a normal subgroup such that G/N is abelian, then $N \supseteq G'$.
4. If H is a subgroup of G such that $H \supseteq G'$, then H is a normal subgroup of G .

Proof. 1. For any $g \in G$ and $h \in G'$, we have $ghg^{-1} = (ghg^{-1}h^{-1})h \in G'$. Thus $G' \trianglelefteq G$.

2. Let $a, b \in G$. Since $ab = ba(a^{-1}b^{-1}ab) \in baG'$, $abG' \subseteq baG'$. Then $abG' = baG'$ follows from the fact that cosets are either equal or disjoint.

3. For any $a, b \in G$, $abN = baN$ gives $[a, b] = aba^{-1}b^{-1} \in N$. The result follows.

4. Take $g \in G$ and $h \in H$, then $ghg^{-1} = (ghg^{-1}h^{-1})h \in H$ since $ghg^{-1}h^{-1} \in G' \subseteq H$. Thus $H \trianglelefteq G$. \square

Definition 1.10 (Center and centralizer)

The **center** of G , denoted by $Z(G)$, is defined as $Z(G) := \{z \in G \mid \forall g \in G, gz = zg\} \trianglelefteq G$.

For $x \in G$, the **centralizer** of x is defined as $C_G(x) := \{g \in G \mid gxg^{-1} = x\} \leq G$.

Recall the **inner automorphism group** $\text{Inn}(G)$ be the image of group homomorphism $\theta : G \rightarrow \text{Aut}(G)$ via $\theta(g)(x) = gxg^{-1}$. Also by Exercise 3.3 in [2], $G/Z(G)$ is cyclic implies G is abelian.

Proposition 1.11 (Equality case for the 5/8 theorem)

Let G be a finite group. Then the following are equivalent:

1. $p(G) = 5/8$.
2. $|\text{Inn}(G)| = 4$.
3. $\text{Inn}(G) \cong C_2 \times C_2$, where C_2 is the cyclic group of order 2.

Proof. (1 \Rightarrow 2) As $p(G) \neq 1$, G is non-abelian. Hence by Theorem 1.2, the equality holds if and only if $|Z(G)|/|G| = 1/4$. This implies $|\text{Inn}(G)| = |G|/|Z(G)| = 4$. (Notice that $\text{Inn}(G) \cong G/Z(G)$ by first isomorphism theorem.)

(2 \Rightarrow 3) It remains to show $\text{Inn}(G) \not\cong \mathbb{Z}/4\mathbb{Z}$. However, it is trivial that $\text{Inn}(G)$ is not cyclic.

(3 \Rightarrow 1) $|\text{Inn}(G)| = 4$ gives $G \neq Z(G)$, which implies G is not abelian, so $p(G) \leq 5/8$.

Now we have $|Z(G)|/|G| = 1/4$. Let $g \in G \setminus Z(G)$, notice $Z(G)$ is a proper subgroup of $C(g)$, so it must have index 2 since $Z(G)$ has index 4 (by Lagrange's Theorem). Thus $|C(g)|/|G| = 1/2$ as required. \square

As an example, Q_8 , the quaternion group attains the equality.

2020 S.-T. Yau High School Science Award

2 i -commuting probabilities of meta-cyclic groups

In this section, we compute the i -commuting probabilities of different classes of groups, namely the dihedral groups, dicyclic groups and meta-cyclic groups. We will soon discover that they are of similar structures. First, we start with dihedral groups.

2.1 Dihedral group

Recall the definition of dihedral group,

Definition 2.1 (Dihedral Group)

Let $n \in \mathbb{N}$. Define the **dihedral group** D_{2n} as

$$D_{2n} := \langle \rho, \sigma \mid \rho^n = \sigma^2 = e, \sigma\rho\sigma^{-1} = \rho^{-1} \rangle = \{\rho^i\sigma^j \mid 0 \leq i \leq n-1, 0 \leq j \leq 1\}.$$

This group has $2n$ elements. Notice $\langle \rho \rangle$ (denoted by P) is a subgroup of D_{2n} , and the two right cosets $P, P\sigma$ partition D_{2n} .

Then we give all possibilities of what form a commutator can take using the identity $\sigma\rho^k\sigma^{-1} = \rho^{-k}$. We notice that the commutators in D_{2n} fall into one of the four categories.

- (A) $[\rho^a, \rho^b] = e$ since they commute.
- (B) $[\rho^a, \rho^b\sigma] = \rho^a\rho^b\sigma\rho^{-a}\sigma^{-1}\rho^{-b} = \rho^{2a}$.
- (C) $[\rho^a\sigma, \rho^b] = [\rho^a, \rho^b]^{-1} = \rho^{-2b}$.
- (D) $[\rho^a\sigma, \rho^b\sigma] = \rho^a\sigma\rho^b\sigma\sigma^{-1}\rho^{-a}\sigma^{-1}\rho^{-b} = \rho^{2a-2b}$.

Here, $0 \leq a, b \leq n-1$.

The next two propositions give the information of commutator subgroups and the centers of dihedral groups. The proofs are simple in light of the form of these commutators.

Proposition 2.2 (Commutator subgroup of dihedral group)

The commutator subgroup of D_{2n} is the cyclic group generated by ρ^2 .

Proof. From the computations above, every element in $H = \langle \rho^2 \rangle$ is a commutator, i.e. $\langle \rho^2 \rangle \subseteq D'_{2n}$. Now notice $\langle \rho^2 \rangle \trianglelefteq D_{2n}$ and consider the quotient group

$$D_{2n}/\langle \rho^2 \rangle = \{H, H\rho, H\sigma, H\rho\sigma\},$$

which is abelian. By Proposition 1.9(3), we have $H \supseteq D'_{2n}$. Hence by Proposition 1.9(4), we have $D'_{2n} = \langle \rho^2 \rangle$. \square

Proposition 2.3 (Center of dihedral group)

Let $n \in \mathbb{N}$ and $n \geq 3$. The center of the dihedral group D_{2n} is

$$Z(D_{2n}) = \begin{cases} \{e\}, & \text{if } n \text{ is odd.} \\ \{e, \rho^{n/2}\}, & \text{if } n \text{ is even.} \end{cases}$$

Proof. One can check that it indeed lies in the center of D_{2n} . Let $x \in Z(D_{2n})$. If $x = \rho^a$ for some $0 \leq a \leq n - 1$, then $[\rho^a, \rho\sigma] = \rho^{2a}$ gives $n \mid 2a$. Thus $a = 0$ or $n/2$. If $x = \rho^a\sigma$ for some $0 \leq a \leq n - 1$, note that $[\rho^a\sigma, \rho] = \rho^{-2}$, which is the identity only if $n \leq 2$. The proposition follows. \square

Remark. When $n \leq 2$, then D_{2n} is abelian, i.e. $Z(D_{2n}) = D_{2n}$.

Now we proceed to the computation of i -commuting probabilities of dihedral groups.

Proposition 2.4

Let $n, i \in \mathbb{N}$. Define \mathcal{S} to be the following set:

$$\mathcal{S} := \{0 \leq k \leq n - 1 \mid \text{ord}(\rho^k) = i\}.$$

Then we have the following formula:

$$p_i(D_{2n}) = \frac{1}{4n^2} \sum_{k \in \mathcal{S}} (|A_k| + |B_k| + |C_k| + |D_k|),$$

where

$$\begin{aligned} A_k &= \{(x, y) \in P \times P \mid [x, y] = \rho^k\} \\ B_k &= \{(x, y) \in P \times P\sigma \mid [x, y] = \rho^k\} \\ C_k &= \{(x, y) \in P\sigma \times P \mid [x, y] = \rho^k\} \\ D_k &= \{(x, y) \in P\sigma \times P\sigma \mid [x, y] = \rho^k\}. \end{aligned}$$

Proof. Let $G = D_{2n}$. We shall show that $f^{-1}(G_i) = f^{-1}(\mathcal{S}')$, where $\mathcal{S}' = \{\rho^k \in D_{2n} \mid \text{ord}(\rho^k) = i, 0 \leq k \leq n - 1\}$.

(\subseteq) Take $(x, y) \in f^{-1}(G_i)$, $[x, y] \in G_i$. By Lemma 2.2 we have $[x, y] = \rho^k$ for some $0 \leq k \leq n - 1$. Hence $[x, y] \in \mathcal{S}'$ and $(x, y) \in f^{-1}(\mathcal{S}')$.

(\supseteq) follows directly from $\mathcal{S}' \subseteq G_i$.

Hence by Lemma 1.4 we have

$$p_i(D_{2n}) = \frac{1}{4n^2} \sum_{k \in \mathcal{S}} \#\{(x, y) \in G^2 \mid f(x, y) = \rho^k\}.$$

We partition G^2 into four cases, namely $P \times P$, $P \times P\sigma$, $P\sigma \times P$ and $P\sigma \times P\sigma$. The result follows. \square

Proposition 2.5

Using the same notation as in Proposition 2.4, we have

$$|A_k| = \begin{cases} n^2, & \text{if } k = 0. \\ 0, & \text{if } k \neq 0. \end{cases}$$

$$|B_k| = |C_k| = |D_k| = \begin{cases} n, & \text{if } n \text{ is odd.} \\ 2n, & \text{if } n \text{ and } k \text{ are both even.} \\ 0, & \text{if } n \text{ is even and } k \text{ is odd.} \end{cases}$$

Proof. For $|A_k|$, notice $[x, y] = e$ for any $(x, y) \in P \times P$, thus $|A_k| = n^2$ if $k = 0$ and $|A_k| = 0$ if $k \neq 0$.

For $|B_k|$, notice $(\rho^a, \rho^b\sigma) \in P \times P\sigma$, $[\rho^a, \rho^b\sigma] = \rho^{2a} = \rho^k$ if and only if $2a \equiv k \pmod{n}$. The possibilities of a depend on the parities of n and k :

Case 1: If n is odd, then $a \equiv 2^{-1}k \pmod{n}$. We only have one solution of a . In this case we have $B_k = \{(\rho^a, \rho^b\sigma) \in P \times P\sigma \mid 0 \leq b \leq n-1\}$, i.e. $|B_k| = n$.

Case 2: If n and k are both even, then $a \equiv -k/2 \pmod{n/2}$. This gives two solutions, namely $(n-k)/2$ and $(2n-k)/2$. Hence $|B_k| = 2n$.

Case 3: If n is even and k is odd, then $2a \equiv k \pmod{n}$ has no solution, i.e. $|B_k| = 0$.

The exact same method can be applied to $|C_k|$ and $|D_k|$, and the result follows. □

Proposition 2.6

Using the same notation as in Proposition 2.4. If $k \in \mathcal{S}$, then

$$k = n/i \cdot m,$$

for some $m \in \mathbb{N}$ such that $\gcd(m, n) = 1$. We have $|\mathcal{S}| = \varphi(i)$, where φ is the Euler totient function.

Consequentially, when both n and n/i are even, then k is even for any $k \in \mathcal{S}$. On the other hand, when n is even and n/i is odd, then k is odd for any $k \in \mathcal{S}$.

Proof. As P is cyclic, ρ^k has order $n/\gcd(n, k)$. Hence for $k \in \mathcal{S}$, we have $\gcd(n, k) = n/i$. This gives $k = n/i \cdot m$ for some $m \in \mathbb{N}$ such that $\gcd(m, n) = 1$. Consider the map

$$\{0 \leq m \leq i-1 \mid \gcd(m, i) = 1\} \rightarrow \{0 \leq k \leq n-1 \mid \gcd(n, k) = n/i\}$$

$$m \mapsto n/i \cdot m$$

This gives a bijection between the sets and thus $|\mathcal{S}| = \varphi(i)$. The rest is clear since m is odd, or else $\gcd(m, n) \neq 1$. □

Theorem 2.7 (*i*-commuting probabilities of dihedral groups)

Let $i \in \mathbb{N}$. And $g : \mathbb{N} \rightarrow \mathbb{R}$ be the function given by

$$g(i) = \begin{cases} 1/4, & \text{if } i = 1. \\ 0, & \text{if } i > 1. \end{cases}$$

Notice that $g(i)$ will appear in this paper frequently.

Then we have

$$p_i(D_{2n}) = \begin{cases} \frac{3}{4n}\varphi(i) + g(i), & \text{if } n \text{ is odd.} \\ \frac{3}{2n}\varphi(i) + g(i), & \text{if } n \text{ and } n/i \text{ are both even.} \\ 0, & \text{if } n \text{ is even but } n/i \text{ is odd.} \end{cases}$$

If i does not divide n , then $p_i(D_{2n}) = 0$.

Proof. Notice if $i = 1$, i.e. $\mathcal{S} = \{0\}$. Then for any $k \in \mathcal{S}$, $|A_k| = n^2$. If $i > 1$, then $0 \notin \mathcal{S}$, then $|A_k| = 0$, i.e. $|A_k| = 4n^2g(i)$.

We first consider the case that n is odd. By Proposition 2.5, we have $|B_k| = |C_k| = |D_k| = n$ and so by Proposition 2.5, we obtain

$$p_i(D_{2n}) = \frac{1}{4n^2} \sum_{k \in \mathcal{S}} |A_k| + |B_k| + |C_k| + |D_k| = \frac{1}{4n^2} \sum_{k \in \mathcal{S}} (4n^2g(i) + 3n) = \frac{|\mathcal{S}|}{4n^2} (4n^2g(i) + 3n) = \frac{3\varphi(i)}{4n} + g(i)\varphi(i).$$

One can check that $g(i)\varphi(i) = g(i)$ and the result follows.

For n and n/i both even, by Proposition 2.6, we have for any $k \in \mathcal{S}$, k is even. Thus by Proposition 2.6 $|B_k| = |C_k| = |D_k| = 2n$. By Proposition 2.4, we obtain

$$p_i(D_{2n}) = \frac{1}{4n^2} \sum_{k \in \mathcal{S}} (4n^2g(i) + 6n) = \frac{\varphi(i)}{4n^2} (4n^2g(i) + 6n) = \frac{3\varphi(i)}{2n} + g(i)\varphi(i).$$

For n is even and n/i is odd, by Proposition 2.6, k is odd for any $k \in \mathcal{S}$. Then by Proposition 2.5, $|B_k| = |C_k| = |D_k| = 0$. Also, notice $i \neq 1$ or else n and n/i will have same parity. Hence $p_i(D_{2n}) = 0$. \square

Using Theorem 2.7, we can now compute the i -commuting probabilities of dihedral groups. The following example verifies our formula.

Example 2.8 (Dihedral group of order 8)

The following table shows the elements in D_8 that commutes. Denote \oplus is for the elements that also commutes when n is odd and \otimes represent the additional elements that only commutes when n is even.

	e	ρ	ρ^2	ρ^3	σ	$\rho\sigma$	$\rho^2\sigma$	$\rho^3\sigma$
e	\oplus	\oplus	\oplus	\oplus	\oplus	\oplus	\oplus	\oplus
ρ	\oplus	\oplus	\oplus	\oplus				
ρ^2	\oplus	\oplus	\oplus	\oplus	\otimes	\otimes	\otimes	\otimes
ρ^3	\oplus	\oplus	\oplus	\oplus				
σ	\oplus		\otimes		\oplus		\otimes	
$\rho\sigma$	\oplus		\otimes			\oplus		\otimes
$\rho^2\sigma$	\oplus		\otimes		\otimes		\oplus	
$\rho^3\sigma$	\oplus		\otimes			\otimes		\oplus

Notice all other commutator in unfilled cell is ρ^2 , which is of order 2.

Then we shall use the formula above to verify the i -commuting probability of D_8 for all $i \in \mathbb{N}$.

$$p_1(D_8) = \frac{3\varphi(1)}{2 \times 4} + \frac{1}{4} = \frac{5}{8},$$

$$p_2(D_8) = \frac{3\varphi(2)}{2 \times 4} = \frac{3}{8}.$$

This result can also be applied to $p_i(D_{2n})$ of larger n .

Example 2.9 (Dihedral group of order 48)

The following gives the i -commuting probabilities of D_{48} for all $i \in \mathbb{N}$ using the formula above.

$$p_1(D_{48}) = \frac{3\varphi(1)}{2 \times 24} + \frac{1}{4} = \frac{5}{16},$$

$$p_2(D_{48}) = \frac{3\varphi(2)}{2 \times 24} = \frac{1}{16},$$

$$p_3(D_{48}) = \frac{3\varphi(3)}{2 \times 24} = \frac{1}{8},$$

$$p_4(D_{48}) = \frac{3\varphi(4)}{2 \times 24} = \frac{1}{8},$$

$$p_6(D_{48}) = \frac{3\varphi(6)}{2 \times 24} = \frac{1}{8},$$

$$p_{12}(D_{48}) = \frac{3\varphi(12)}{2 \times 24} = \frac{1}{4}$$

And $p_i(D_{48}) = 0$ for all other $i \in \mathbb{N}$.

One may notice that $\sum_{i \in \mathbb{N}} p_i(D_{48})$ is indeed 1.

2.2 Dicyclic group

We now turn the attention to dicyclic groups.

Definition 2.10 (Dicyclic group)

Let $n \in \mathbb{N}$. Define the **dicyclic group** Q_{4n} as

$$Q_{4n} := \langle a, x \mid x^{2n} = 1, x^2 = a^n, x^{-1}ax = a^{-1} \rangle = \{a^i x^j \mid 0 \leq i \leq 2n - 1, j = 0, 1\}.$$

This group has order $4n$. Notice $\langle a \rangle$ (denoted by A) is a subgroup of Q_{4n} . Hence the two right coset A and Ax partition Q_{4n} .

Similarly, we compute commutators using the identity $xa^kx^{-1} = a^{-k}$ in dicyclic groups before finding the i -commuting probabilities, which again falls into one of the four categories:

- (A) $[a^k, a^m] = e$ since they commute.
- (B) $[a^k, a^m x] = a^k a^m x a^{-k} x^{-1} a^{-m} = a^{2k}$.
- (C) $[a^k x, a^m] = a^k x a^m x^{-1} a^{-k} a^{-m} = a^{-2m}$.
- (D) $[a^k x, a^m x] = a^k x a^m x x^{-1} a^{-k} x^{-1} a^{-m} = a^k (x a^{m-k} x^{-1}) a^{-m} = a^{2k-2m}$.

This holds for $0 \leq k, m \leq 2n - 1$.

Proposition 2.11 (Commutator subgroup of dicyclic group)

The commutator subgroup of Q_{4n} is the cyclic group generated by a^2 .

Proof. By the above, every element in $H = \langle a^2 \rangle$ is a commutator, i.e. $\langle a^2 \rangle \subseteq Q'_{4n}$. Now notice that $\langle a^2 \rangle \trianglelefteq Q_{4n}$ and consider the quotient group

$$Q_{4n}/\langle a^2 \rangle = \{H, Ha, Hx, Hax\},$$

which is abelian. By Proposition 1.9, we have $H \supseteq Q'_{4n}$. Hence we have $Q'_{4n} = \langle a^2 \rangle$. \square

Proposition 2.12 (Center of dicyclic group)

Let $n \in \mathbb{N}$ and $n > 1$. The center of Q_{4n} is $\{e, a^n\}$.

Proof. One can check they indeed lies in center of Q_{4n} . Let $g \in Z(Q_{4n})$. If $g = a^k$ for some $0 \leq k \leq 2n - 1$, then $[a^k, ax] = a^{2k}$ gives $n \mid k$. Thus $k = 0$ or n . If $g = a^k x$ for some $0 \leq k \leq 2n - 1$, note that $[a^k x, a] = a^{-2}$, which is the identity only if $n = 1$. The proposition follows. \square

Theorem 2.13 (*i*-commuting probabilities of dicyclic groups)

Let $i \in \mathbb{N}$. We have

$$p_i(Q_{4n}) = \begin{cases} 0 & \text{if } 2n/i \text{ is odd} \\ \frac{3}{4n}\varphi(i) + g(i) & \text{if } 2n/i \text{ is even} \end{cases}$$

where $g(i)$ has the same definition as Theorem 2.7.

Proof. This is similar to the computation of dihedral groups, hence we skipped it. □

2.3 Meta-cyclic group

Notice that the computations of *i*-commuting probabilities of dihedral groups and dicyclic groups are similar. This makes us wonder whether similar methods can be applied to a specific class of groups. In fact, both dihedral groups and dicyclic groups are meta-cyclic groups, which is defined as follows:

Definition 2.14 (Meta-cyclic group [5])

A group M is said to be **meta-cyclic** if it can be written as the following form:

$$M = \langle a, b \mid a^m = 1, b^s = a^t, b^{-1}ab = a^r \rangle,$$

where $m, s, t, r \in \mathbb{Z}$ satisfy $r^s \equiv 1 \pmod{m}$ and $m \mid t(r - 1)$. This group has order ms .

We developed several lemmas to find the *i*-commuting probabilities of meta-cyclic groups.

Lemma 2.15

Let M be a meta-cyclic group. For any $n \in \mathbb{N}, k \in \mathbb{Z}$, we have $b^{-n}a^k b^n = a^{kr^n}$.

Proof. We prove by induction on n , notice that $b^{-1}a^k b = \underbrace{((b^{-1}ab)(b^{-1}ab) \cdots (b^{-1}ab))}_{k \text{ times}} = (a^r)^k$. Then for $k \in \mathbb{Z}$, we have $(b^{-1}a^{-k}b)^{-1} = b^{-1}a^k b$, which implies $b^{-1}a^{-k}b = a^{(-k)r}$.

For $n \in \mathbb{N}$, assume that $b^{-n}a^k b^n = a^{kr^n}$. And

$$\begin{aligned} b^{-n-1}a^k b^{n+1} &= b^{-1}(b^{-n}a^k b^n)b \\ &= a^{kr^n r} = a^{kr^{n+1}}. \end{aligned}$$

□

Lemma 2.16

Let $0 \leq \alpha, \gamma \leq m - 1, 0 \leq \beta, \delta \leq s - 1$, we have

$$[a^\alpha b^\beta, a^\gamma b^\delta] = a^{\alpha + \gamma r^{ms - \beta} - \alpha r^{ms - \delta} - \gamma}.$$

Proof. Consider

$$\begin{aligned}
 [a^\alpha b^\beta, a^\gamma b^\delta] &= a^\alpha b^\beta a^\gamma b^\delta b^{-\beta} a^{-\alpha} b^{-\delta} a^{-\gamma} \\
 &= a^\alpha (b^\beta a^\gamma b^{-\beta}) (b^\delta a^{-\alpha} b^{-\delta}) a^{-\gamma} \\
 &= a^\alpha b^{\beta-ms} a^\gamma b^{-\beta+ms} b^{\delta-ms} a^{-\alpha} b^{ms-\delta} a^{-\gamma} \\
 &= a^{\alpha+\gamma r^{ms-\beta} - \alpha r^{ms-\delta} - \gamma}.
 \end{aligned}$$

Theorem 2.17 (*i*-commuting probabilities of meta-cyclic groups)

Let $\mathcal{S} := \{0 \leq k \leq ms - 1 \mid \text{ord}(a^k) = i\}$. Then

$$\begin{aligned}
 p_i(M) &= \frac{1}{(ms)^2} \sum_{k \in \mathcal{S}} \#\{(\alpha, \beta, \gamma, \delta) \mid \alpha + \gamma r^{ms-\beta} - \alpha r^{ms-\delta} - \gamma \equiv k \pmod{m}\} \\
 &= \frac{\varphi(i)}{(ms)^2} \#\{(\alpha, \beta, \gamma, \delta) \mid \alpha + \gamma r^{ms-\beta} - \alpha r^{ms-\delta} - \gamma \equiv k \pmod{m}\}
 \end{aligned}$$

Proof. We shall show that $f^{-1}(M_i) = f^{-1}(\mathcal{S}')$, where $M_i = \{g \in M \mid \text{ord}(g) = i\}$ and $\mathcal{S}' = \{a^k \in M \mid \text{ord}(a^k) = i, 0 \leq k \leq ms - 1\}$.

(\subseteq) Take $(x, y) \in f^{-1}(M_i)$, $[x, y] \in M_i$. By Theorem 2.16, we have $[x, y] = a^k$ for some $0 \leq k \leq ms - 1$. Hence $[x, y] \in \mathcal{S}'$ and $(x, y) \in f^{-1}(\mathcal{S}')$.

(\supseteq) The converse direction follows from $\mathcal{S}' \supseteq M_i$.

$|\mathcal{S}| = \varphi(i)$ as the commutator subgroup is cyclic. □

The calculation of *i*-commuting probabilities of meta-cyclic groups is transferred into a number theoretic problem. We now provide two corollaries of special cases.

Corollary 2.18

Let M be a meta-cyclic group. If $r = -1$, then

$$p_i(M) = \begin{cases} \frac{3}{4m} \varphi(i) + g(i), & \text{if } n \text{ is odd.} \\ \frac{3}{2m} \varphi(i) + g(i), & \text{if } n \text{ and } n/i \text{ are both even.} \\ 0, & \text{if } n \text{ is even but } n/i \text{ is odd.} \end{cases}$$

Proof. First, by the condition $r^s = (-1)^s \equiv 1 \pmod{m}$, s is even. Consider

$$N = \{\alpha + \gamma(-1)^{sm-\beta} - \alpha(-1)^{sm-\delta} - \gamma \equiv k \pmod{2}\}.$$

When $(\beta, \delta) \equiv (0, 0) \pmod{2}$, the equation becomes $0 \equiv k \pmod{m}$, which has solution if and only if $k = 0$. This gives $|N| = m^2$ when $i = 1$.

When $(\beta, \delta) \equiv (0, 1) \pmod{2}$, the equation becomes $2\alpha \equiv k \pmod{m}$. Consider the following cases:

Case 1: If m is odd, then $a \equiv 2^{-1}k \pmod{m}$. We only have one solution of a , i.e. $|N| = m$.

Case 2: If m and k are both even, then $a \equiv -k/2 \pmod{n/2}$. This gives two solutions, namely $(m - k)/2$ and $(2m - k)/2$. Hence $|N| = 2m$.

Case 3: If n is even and k is odd, then $2a \equiv k \pmod{m}$ has no solution, i.e. $|N| = 0$.

The cases where $(\beta, \delta) \equiv (1, 0)$ or $(1, 1) \pmod{2}$ are similar as above.

On the other hand, $|\mathcal{S}| = \varphi(i)$ as commutators of M are in the form a^k for some $k \in \mathbb{N}$. The result follows. \square

Corollary 2.19

Let M be a meta-cyclic group. If m is a prime, then

$$p_1(M) = \frac{s^2 + m - 1}{ms^2}$$

$$p_m(M) = \frac{(s^2 - 1)(m - 1)}{ms^2}.$$

And $p_i(M) = 0$ for all other $i \in \mathbb{N}$.

Proof. Notice that $\alpha + \gamma r^{ms-\beta} - \alpha r^{ms-\delta} - \gamma \equiv 0 \pmod{m}$ if and only if $\beta = \delta = 0$ when m is prime. This yields $s^2 - 1$ cases to be considered, as $0 \leq \beta, \delta \leq s - 1$. Since m is prime, there are m solutions to (α, γ) in every case. Also $\varphi(m) = m - 1$ by the fact that m is prime.

Hence we have

$$p_1(M) = \frac{m(s^2 - 1)}{(ms)^2} + \frac{1}{s^2} = \frac{s^2 + m - 1}{ms^2}$$

$$p_m(M) = \frac{m(s^2 - 1)(m - 1)}{ms^2} = \frac{(s^2 - 1)(m - 1)}{ms^2}$$

after simplifications. \square

Here we provide a few examples of meta-cyclic groups to verify Theorem 2.17.

Example 2.20 (Dihedral groups & dicyclic groups)

Notice that $t = m, s = 2$ and $r = -1$ in D_{2m} and $2t = m, s = 2$ and $r = -1$ in Q_{4m} . It directly follows from Corollary 2.18.

One should notice that this gives us the same answer as in Theorem 2.7 and 2.13.

Now we shall try to apply Theorem 2.17 to some meta-cyclic groups that are not dihedral or dicyclic. The following two examples use Corollary 2.18 and 2.19 respectively.

Example 2.21 ($C_4 \rtimes C_4$)

Notice that $C_4 \rtimes C_4 = \langle x, y \mid x^4 = y^4 = e, yxy^{-1} = x^{-1} \rangle$. Then we can deduce the useful identity $yx^a = x^{-a}y$. Here we compute the commutators of $C_4 \rtimes C_4$ after some tedious work.

	x^a	$x^a y$	$x^a y^2$	$x^a y^{-1}$
x^b	e	x^{2a}	e	x^{2b}
$x^b y$	x^{-2a}	x^{2b-2a}	x^{-2a}	x^{2b-2a}
$x^b y^2$	e	x^{2a}	e	x^{2b}
$x^b y^{-1}$	x^{-2b}	x^{2a-2b}	x^{-2b}	x^{-2a-2b}

It remains to consider $k \in \mathbb{N}$ such that $k \equiv 2a \pmod{4}$. The result follows:

$$p_i(C_4 \rtimes C_4) = \begin{cases} \frac{3\varphi(i)}{8} + g(i) & \text{if } i \mid n \\ 0 & \text{if } i \nmid n \end{cases}$$

where $g(i) = 1/4$ only if $i = 1$. Thus

$$p_1 = \frac{3\varphi(1)}{8} + \frac{1}{4} = \frac{5}{8}$$

$$p_2 = \frac{3\varphi(2)}{8} = \frac{3}{8}.$$

On the other hand, $m = t = s = 4$ and $r = -1$. By Corollary 2.18,

$$p_1(C_4 \rtimes C_4) = \frac{3\varphi(1)}{2 \times 4} + \frac{1}{4} = \frac{5}{8},$$

$$p_2(C_4 \rtimes C_4) = \frac{3}{2 \times 4} = \frac{3}{8}.$$

Notice that these two methods gives us the same answer, thus verifies Theorem 2.17 and Corollary 2.18.

Example 2.22 ($C_5 \rtimes C_4$)

Notice that $C_5 \rtimes C_4 = \langle a, b \mid a^5 = b^4 = e, bab^{-1} = a^2 \rangle$, i.e. $m = 5, s = 4$ and $r = 2$. By Corollary 2.19, we have

$$p_1(C_5 \rtimes C_4) = \frac{4^2 + 5 - 1}{5 \times 4^2} = \frac{1}{4}$$

$$p_5(C_5 \rtimes C_4) = \frac{(4^2 - 1)(5 - 1)}{5 \times 4^2} = \frac{3}{4}.$$

The following example does not fulfill the conditions in Corollary 2.18 or 2.19, thus we directly apply Theorem 2.17.

Example 2.23 ($C_9 \rtimes C_3$)

Notice that $C_9 \rtimes C_3 = \langle a, b \mid a^9 = b^3 = e, bab^{-1} = a^4 \rangle$, i.e. $m = 9, s = 3$ and $r = 4$. Consider

$$N = \{ \alpha + \gamma \cdot 4^{18-\beta} - \alpha \cdot 4^{18-\delta} - r \equiv k \pmod{9} \},$$

where $0 \leq \alpha, \gamma \leq 8$ and $0 \leq \beta, \delta \leq 2$.

Notice that $4^0 \equiv 1 \pmod{9}$, $4^1 \equiv 4 \pmod{9}$ and $4^2 \equiv 7 \pmod{9}$.

	0	1	2
0	0	-6α	-3α
1	6γ	$6(\gamma - \alpha)$	$3(2\gamma - \alpha)$
2	3γ	$3(\gamma - 2\alpha)$	$3(\gamma - \alpha)$

Hence we have

$$|N| = \begin{cases} 3 \times 9 = 27 & \text{if } 3 \mid k \\ 0 & \text{if } 3 \nmid k \end{cases}$$

This gives

$$p_1(C_9 \rtimes C_3) = \frac{27\varphi(1) \times 8}{(3 \times 9)^2} + \frac{1}{9} = \frac{11}{27}.$$

$$p_3(C_9 \rtimes C_3) = \frac{27\varphi(3) \times 8}{(3 \times 9)^2} = \frac{16}{27}.$$

One should notice that $g(i) = \frac{1}{9} \neq \frac{1}{4}$ when $i = 1$ in this case. It is because the two elements only commute in one out the nine cases.

2020 S.T. Y.

3 Isoclinism

In this section, we try to build the abstract relation between groups of the same i -commuting probabilities for all $i \in \mathbb{N}$. One may observe that D_{2n} and Q_{4n} share similar general formulae of i -commuting probabilities. Indeed, they share a special relation named isoclinism, defined below:

Definition 3.1 (Isoclinism)

Let G_1 and G_2 be finite groups. G_1 and G_2 are said to be **isoclinic**, denoted by $G_1 \sim G_2$, if there exist isomorphisms

$$\begin{aligned} \phi &: G_1/Z(G_1) \rightarrow G_2/Z(G_2), \text{ and} \\ \psi &: G'_1 \rightarrow G'_2 \end{aligned}$$

such that the following diagram commutes:

$$\begin{array}{ccc} G_1/Z(G_1) \times G_1/Z(G_1) & \xrightarrow{\phi \times \phi} & G_2/Z(G_2) \times G_2/Z(G_2) \\ \downarrow \rho_1 & & \downarrow \rho_2 \\ G'_1 & \xrightarrow{\psi} & G'_2 \end{array}$$

where $\rho_j : G_j/Z(G_j) \times G_j/Z(G_j) \rightarrow G'_j$ defined by $(xZ(G_j), yZ(G_j)) \mapsto [x, y]$ for $j = 1, 2$.

Notice that isoclinism is an equivalence relation.

When two groups G and H are isoclinic, $p_1(G) = p_1(H)$ [3]. We generalize this idea to i -commuting probabilities for all $i \in \mathbb{N}$.

Theorem 3.2

Let G, H be groups. If G and H are isoclinic, then $p_i(G) = p_i(H)$ for all $i \in \mathbb{N}$.

Proof. Consider

$$\begin{aligned} |G/Z(G)|^2 p_i(G) &= \frac{1}{|Z(G)^2|} |G|^2 p_i(G) \\ &= \frac{1}{|Z(G)^2|} |\{(x, y) \in G \times G : \text{ord}([x, y]) = i\}| \\ &= \frac{1}{|Z(G)^2|} |\{(x, y) \in G \times G : \text{ord}([xZ(G), yZ(G)]) = i\}| \\ &= |\{(a, b) \in (G/Z(G))^2 : \text{ord}(\rho_1(a, b)) = i\}|. \end{aligned}$$

As ψ is an isomorphism, this equals to

$$|\{(a, b) \in (G/Z(G))^2 : \text{ord}(\psi(\rho_1(a, b))) = i\}|.$$

From the commutative diagram,

$$\text{ord}(\psi(\rho_1(a, b))) = \text{ord}(\rho_2(\phi(a), \phi(b))) = i.$$

Finally since ϕ is an isomorphism, this equals to

$$|\{(c, d) \in (H/Z(H)^2) : \text{ord}(\rho_2(c, d)) = i\}|.$$

Thus we have

$$\begin{aligned} \left| \frac{G}{Z(G)} \right|^2 p_i(G) &= \left| \frac{H}{Z(H)} \right|^2 p_i(H) \\ p_i(G) &= p_i(H). \end{aligned}$$

□

It is natural to propose the following question:

Question 3.3

Is the converse of Theorem 3.2 true?

We will answer this question after computing the i -commuting probabilities of more groups.

The below proposition states the isoclinism between dihedral groups and dicyclic groups.

Proposition 3.4

Let $m \geq 2$. The following are isoclinic,

1. The dicyclic group of order $4m$, Q_{4m} .
2. The dihedral group of order $4m$, D_{4m} .
3. The dihedral group of order $2m$, D_{2m} , provided m being odd.

Proof. (1 ~ 2) By Proposition 2.3 and 2.12, we have $Z(D_{4m}) = \{e, \rho^m\}$ and $Z(Q_{4m}) = \{e, a^m\}$, which are both isomorphic to C_2 . One can check that $\phi : D_{4m}/Z(D_{4m}) \rightarrow Q_{4m}/Z(Q_{4m})$ via $\rho \mapsto a$ and $\sigma \mapsto x$ is indeed an isomorphism.

We have shown $D'_{4m} \cong C_m$ in Proposition 2.2 and $Q'_{4m} \cong C_m$ in 2.11. This gives $D'_{4m} \cong Q'_{4m}$ with ψ defined as $\rho \mapsto a$.

Now it remains to show that the diagram commutes.

As ϕ is an isomorphism, $[\phi(x), \phi(y)] = \phi([x, y])$. Take $(\rho Z(D_{4m}), \sigma Z(D_{4m})) \in D_{4m}/Z(D_{4m}) \times D_{4m}/Z(D_{4m})$. It is mapped by $\phi \times \phi$ to $(aZ(Q_{4m}), xZ(Q_{4m})) \in Q_{4m}/Z(Q_{4m}) \times Q_{4m}/Z(Q_{4m})$, then to $[a, x] \in Q'_{4m}$ by ρ_2 . On the other hand, it is mapped by ρ_1 to $[\rho, \sigma] \in D'_{4m}$, then to $[a, x] \in Q'_{4m}$. The result follows.

(2 ~ 3) Similar as above.

As isoclinism is an equivalence relation, we have $Q_{4m} \sim D_{4m}$ for all $m \in \mathbb{N}$ and $Q_{4m} \sim D_{4m} \sim D_{2m}$ if m is odd. \square

The following theorem provides us with a useful fact to compute the i -commuting probabilities of unknown groups. It is stated in Exercise 2 in [4].

Proposition 3.5

Let G, A be finite groups. G is isoclinic to $G \times A$ if and only if A is abelian.

Question 3.6

Let G, H be finite groups. Is it true that $p_i(G) \times p_i(H) = p_i(G \times H)$, for all $i \in \mathbb{N}$?

Answer 3.7. When $i = 1$, this is always true [3]. Otherwise, the claim is incorrect. As a counterexample, consider D_6 and C_2 , $p_3(D_6) \times p_3(C_2) = 1/2 \times 0 = 0$, which does not equal to $p_3(D_6 \times C_2) = 1/2$.

2020 S.-T. Yau High School Science Award

4 *i*-commuting probabilities of groups of small orders

In the previous sections, we have developed methods to compute the *i*-commuting probabilities of different classes of groups. In this section, we will investigate on other groups. Moreover, we will apply these methods and compute the *i*-commuting probabilities of non-abelian groups (up to isomorphism) of orders less than 30.

4.1 Generalized dihedral group

Definition 4.1 (Semi-direct product)

Let N and H be groups, and suppose $\phi : H \rightarrow \text{Aut}(N)$ is a homomorphism. The group $G = N \rtimes_{\phi} H$ is defined as the set of ordered pairs (n, h) with $n \in N, h \in H$, and the group operation being given by the formula

$$(n, h) \cdot (n_1, h_1) = (n\phi(h)(n_1), hh_1).$$

Definition 4.2 (Generalized dihedral group)

Let H be an abelian group. Let $\phi : C_2 \rightarrow \text{Aut}(H)$ be defined by $\phi(0)$ as the identity map and $\phi(1)$ as inversion.

Define the semi-direct product $H \rtimes_{\phi} C_2$ be the **generalized dihedral group**, denoted by $\text{Dih}(H)$.

Notice that H is cyclic if and only if $H \rtimes_{\phi} C_2$ is a dihedral group.

Here is the multiplication table of generalized dihedral group. Let $g, h \in H$.

$$\begin{aligned} (g, 0) \cdot (h, 0) &= (g\phi(0)(h), 0) = (gh, 0). \\ (g, 0) \cdot (h, 1) &= (g\phi(0)(h), 1) = (gh, 1). \\ (g, 1) \cdot (h, 0) &= (g\phi(1)(h), 1) = (gh^{-1}, 1). \\ (g, 1) \cdot (h, 1) &= (g\phi(1)(h), 0) = (gh^{-1}, 0). \end{aligned}$$

Also $(h, 0)^{-1} = (h^{-1}, 0)$ and $(h, 1)^{-1} = (h, 1)$. We can now compute the commutators in $\text{Dih}(H)$, which fall into one of the four categories.

- (A) $[(g, 0), (h, 0)] = (0, 0)$ since they commutes.
- (B) $[(g, 0), (h, 1)] = (gh, 1)(g^{-1}, 0)(h^{-1}, 1) = (g^2, 0)$.
- (C) $[(g, 1), (h, 0)] = (gh^{-1}, 1)(g^{-1}, 1)(h^{-1}, 0) = (h^{-2}, 0)$.
- (D) $[(g, 1), (h, 1)] = (gh^{-1}, 0)(g^{-1}, 1)(h^{-1}, 1) = (g^2h^{-2}, 0)$.

where $g, h \in H$.

Theorem 4.3 (*i*-commuting probability of generalized dihedral group)

Let $i \in \mathbb{N}$, we have

$$p_i(\text{Dih}(H)) = \frac{3|\mathcal{S}|}{4|H|} + g(i)$$

where $\mathcal{S} = \{h \in H \mid \text{ord}(h^2) = i\}$.

Proof. Notice that all the commutators in $\text{Dih}(H)$ are in the form of g^2 , where $g \in H$. Hence it suffices to find $|\mathcal{S}|$. Using the similar method in calculating the *i*-commuting probabilities of dihedral groups, the result follows. \square

Example 4.4 (Dihedral group)

Note that when H is cyclic, $H \rtimes C_2$ is a dihedral group discussed above. In fact, D_{2n} is isomorphic to $C_n \rtimes C_2$. In this case, $\mathcal{S} = \{h \in C_n \mid \text{ord}(h^2) = i\}$. One can check that $|\mathcal{S}| = \varphi(i)$ when n is odd, and $|\mathcal{S}| = 2\varphi(i)$ when n and n/i is even.

Example 4.5 ($\text{Dih}(\mathbb{Z}_3 \times \mathbb{Z}_2)$)

Let $G = \text{Dih}(\mathbb{Z}_3 \times \mathbb{Z}_2)$. By Theorem 4.3, we have

$$\begin{aligned} p_1(G) &= \frac{3 \times 2}{4 \times 12} + \frac{1}{4} = \frac{3}{8} \\ p_2(G) &= \frac{3 \times 2}{4 \times 12} = \frac{1}{8} \\ p_3(G) &= \frac{3 \times 4}{4 \times 12} = \frac{1}{4} \\ p_6(G) &= \frac{3 \times 4}{4 \times 12} = \frac{1}{4}. \end{aligned}$$

And $p_i(G) = 0$ for all other $i \in \mathbb{N}$.

4.2 Symmetric groups & Alternating groups

Definition 4.6 (Symmetric group)

The **symmetric group** on n letters is the set of bijections from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$, with the group operation being composition. It is denoted by S_n .

Definition 4.7 (Alternating group)

The subgroup of even permutations of the symmetric group S_n is called the **alternating group**, and is denoted by A_n .

Here is a fact concerning the commutator subgroup that will help us compute the *i*-commuting probabilities of S_n and A_n .

Proposition 4.8 (Commutator subgroup of S_n and A_n)

The commutator subgroup of S_n is equal to A_n . For $n \geq 5$, the commutator subgroup of A_n is equal to A_n itself.

Proof. Since S_n/A_n is abelian, the commutator subgroup $S'_n \leq A_n$. Conversely, we have $[(ab), (ac)] = (abc)$, showing that every 3-cycle is in S'_n . As A_n is generated by 3-cycles, so $S'_n = A_n$ is as required.

For the second statement, the result follows by the fact that A_n is simple. □

Corollary 4.9

For all $i \in \mathbb{N}$, $p_i(S_n) > 0$ if and only if $x \in A_n$ such that $\text{ord}(x) = i$.

Proof. It follows from Proposition 4.8 and A_n is generated by commutators in S_n . □

Notice that A_n is a simple group. Recall that a **simple group** is a group whose only normal subgroups are the trivial group and the group itself. The following theorem provides us with more understanding of its commutators.

Theorem 4.10 (Ore Conjecture (proved) [6])

Let A be a non-abelian simple group. For all $g \in A$, g is a commutator.

This theorem gives us the inspiration of the condition of which $p_i(A_n) > 0$.

Proposition 4.11

For all $i \in \mathbb{N}$, $p_i(A_n) > 0$ if and only if there exist $x \in A_n$ such that $\text{ord}(x) = i$.

Proof. (\Leftarrow) By Theorem 4.10, such $x = [a, b]$ for some $a, b \in A_n$. This gives $p_i(A_n) > 0$.

(\Rightarrow) The converse direction is trivial. □

Hence we obtain the necessary and sufficient conditions for $p_i(S_n) > 0$ and $p_i(A_n) > 0$. Then we try to develop a bound to $p_i(S_n)$ for some particular i 's.

Proposition 4.12

For any symmetric group S_n , $p_3(S_n) \geq \frac{1}{(n!)^2} n(n-1)(n-2)$.

Proof. Let $(ab), (ac)$ be transpositions in S_n . Notice that $(ab)^{-1} = (ab)$. Thus we have $[(ab), (ac)] = (ab)(ab)(ac)(ac) = (abc)$, which has order 3. The result follows. □

The following example verifies this inequality.

Example 4.13 ($p_3(S_n)$)

Consider S_n for $3 \leq n \leq 5$. Their i -commuting probabilities are computed by computer program.

$$\begin{aligned}
 p_3(S_3) &= \frac{1}{2} \geq \frac{1}{(3!)^2} \times 3 \times 2 \times 1 = \frac{1}{6} \\
 p_3(S_4) &= \frac{1}{2} \geq \frac{1}{(4!)^2} \times 4 \times 3 \times 2 = \frac{1}{24} \\
 p_3(S_5) &= \frac{7}{20} \geq \frac{1}{(5!)^2} \times 5 \times 4 \times 3 \times 2 = \frac{1}{240}
 \end{aligned}$$

As the i -commuting probabilities of S_n and A_n are rather hard to compute, we used a program to compute its commutators and calculate their orders. The code is attached in the appendix.

4.3 List of i -commuting probabilities of groups of orders less than 30

Now we aim to find the i -commuting probabilities of groups of orders less than 30. We first divide the groups into different classes. The list of the groups is from [7].

Type 1: Dihedral groups, dicyclic groups & generalized dihedral groups

We can directly apply Theorem 2.7, 2.13 and 4.3.

Type 2: Direct product of a group of Type 1, 3 or 4 and an abelian group

By Proposition 3.5, $p_i(G) = p_i(G \times A)$ for all $i \in \mathbb{N}$ if A is abelian. As the groups of direct product of orders less than 30 are all a known group with an abelian group, we can now easily find their i -commuting probabilities.

Type 3: Meta-cyclic groups

These can be computed by Theorem 2.17 as special cases. One should notice that the semi-direct product of two cyclic groups is meta-cyclic. For $r = -1$, Corollary 2.18 is used. For m is a prime, Corollary 2.19 is used. Otherwise, we will directly compute the i -commuting probabilities using the similar method as Example 2.23.

Type 4: S_n and A_n

These are calculated by computer program attached in the appendix. Also notice that $|S_n| = n!$ and $|A_n| = n!/2$ so only S_3, S_4, A_4 appeared in our table.

Type 5: Other groups

These groups are not in any classes as above. However, most of them have special structures that make the computations less tedious.

- **SmallGroup(16,3)**: It has the presentation $G := \langle a, b, c \mid a^4 = b^2 = c^2 = e, ab = ba, bc = cb, cac^{-1} = ab \rangle$.

By [9], its commutator subgroup is isomorphic to C_2 . Hence $p_1(G) + p_2(G) = 1$. On the other hand, the center of SmallGroup(16,3) is the Klein four group. By Proposition 1.11(3), $p_1(G) = 5/8$, thus $p_2(G) = 3/8$.

- **SmallGroup(16,13)**: It is defined by the central product of D_8 and C_4 , which has the presentation $G := \langle a, x, y \mid a^4 = x^2 = e, a^2 = y^2, xax^{-1} = a^{-1}, ay = ya, xy = yx \rangle$ [10]. The elements are in the form $a^\alpha x^\beta y^\gamma$ where $0 \leq \alpha \leq 3, 0 \leq \beta, \gamma \leq 1$. The computations of commutators are shown in the following table:

	a^k	$a^k x$	$a^k y$	$a^k xy$
a^m	e	a^{2m}	e	a^{2m}
$a^m x$	a^{-2k}	a^{2m-2k}	a^{-2k}	a^{2m-2k}
$a^m y$	e	a^{2m}	e	a^{2m}
$a^m xy$	a^{-2k}	a^{2m-2k}	a^{-2k}	a^{2m}

Notice that all commutators are in the form of a^m , for some $0 \leq m \leq 3$. Therefore, $|\mathcal{S}| := \#\{k \in \mathbb{N} \mid \text{ord}(a^k) = i\} = \varphi(i)$. It remains to solve $2a \equiv k \pmod{4}$ for $0 \leq a \leq 3$, which has 0, 2, 0, 2 solutions for $k = 1, 2, 3, 4$ respectively. This gives

$$p_1(G) = \frac{12 \times 2 \times 4\varphi(i)}{16^2} + \frac{1}{4} = \frac{5}{8},$$

$$p_2(G) = \frac{12 \times 2 \times 4\varphi(i)}{16^2} = \frac{3}{8}.$$

However, there are three groups that we failed to compute their i -commuting probabilities, namely $\text{SL}(2,3)$, $C_3 \rtimes D_8$ and $C_3^2 \rtimes C_3$. $\text{SL}(2,3)$ has the presentation $\langle a, b, c \mid a^3 = b^3 = c^2 = abc \rangle$ [11], which we cannot think of a method to find its i -commuting probability. On the other hand, unfortunately, the presentations of $C_3 \rtimes D_8$ and $C_3^2 \rtimes C_3$ cannot be found so we have to give them up reluctantly.

2020 S.-T. Yau High School Science Award

Group	Type	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}	p_{13}	p_{14}	p_{15}
6	1	1/2	0	1/2	0	0	0	0	0	0	0	0	0	0	0	0
8	1	5/8	3/8	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	5/8	3/8	0	0	0	0	0	0	0	0	0	0	0	0	0
10	1	2/5	0	0	0	3/5	0	0	0	0	0	0	0	0	0	0
12	1	1/2	0	1/2	0	0	0	0	0	0	0	0	0	0	0	0
	4	1/3	2/3	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1/2	0	1/2	0	0	0	0	0	0	0	0	0	0	0	0
14	1	5/14	0	0	0	0	0	9/14	0	0	0	0	0	0	0	0
16	SmallGroup(16,3)	5	5/8	3/8	0	0	0	0	0	0	0	0	0	0	0	0
	$C_4 \times C_4$	3	5/8	3/8	0	0	0	0	0	0	0	0	0	0	0	0
	M_{16}	3	7/16	3/16	0	3/8	0	0	0	0	0	0	0	0	0	0
16	D_{16}	1	7/16	3/16	0	3/8	0	0	0	0	0	0	0	0	0	0
	QD_{16}	3	5/8	3/8	0	0	0	0	0	0	0	0	0	0	0	0
	Q_{16}	1	7/16	3/16	0	3/8	0	0	0	0	0	0	0	0	0	0
	$D_8 \times C_2$	2	5/8	3/8	0	0	0	0	0	0	0	0	0	0	0	0
	$Q_8 \times C_2$	2	5/8	3/8	0	0	0	0	0	0	0	0	0	0	0	0
SmallGroup(16,13)	5	5/8	3/8	0	0	0	0	0	0	0	0	0	0	0	0	

	Group	Type	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}	p_{13}	p_{14}	p_{15}
18	D_{18}	1	$1/3$	0	$1/6$	0	0	0	0	0	$1/2$	0	0	0	0	0	0
	$S_3 \times C_3$	2	$1/2$	0	$1/2$	0	0	0	0	0	0	0	0	0	0	0	0
	$(C_3 \times C_3) \times C_2$	1	$1/3$	$2/3$	0	0	0	0	0	0	0	0	0	0	0	0	0
20	Q_{20}	1	$2/5$	0	0	0	$3/5$	0	0	0	0	0	0	0	0	0	0
	$C_5 \times C_4$	5	$1/4$	0	0	0	$3/4$	0	0	0	0	0	0	0	0	0	0
	D_{20}	1	$2/5$	0	0	0	$3/5$	0	0	0	0	0	0	0	0	0	0
21	$C_7 \times C_3$	3	$5/21$	0	0	0	0	0	$16/21$	0	0	0	0	0	0	0	0
	D_{22}	1	$7/22$	0	0	0	0	0	0	0	0	0	$15/22$	0	0	0	0
24	$C_3 \times C_8$	3	$11/32$	0	$21/32$	0	0	0	0	0	0	0	0	0	0	0	0
	$SL(2,3)$	5	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Q_{24}	1	$3/8$	$1/8$	$1/4$	0	0	$1/4$	0	0	0	0	0	0	0	0	0
	$S_3 \times C_4$	2	$1/2$	0	$1/2$	0	0	0	0	0	0	0	0	0	0	0	0
	D_{24}	1	$3/8$	$1/8$	$1/4$	0	0	$1/4$	0	0	0	0	0	0	0	0	0
$Q_{12} \times C_2$	1	$1/2$	0	$1/2$	0	0	0	0	0	0	0	0	0	0	0	0	0
$C_3 \times D_8$	5	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
$D_8 \times C_3$	1	$5/8$	$3/8$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$Q_8 \times C_3$	1	$5/8$	$3/8$	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	Group	Type	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}	p_{13}	p_{14}	p_{15}
24	S_4	4	5/24	7/2	1/2	0	0	0	0	0	0	0	0	0	0	0	0
	$A_4 \times C_2$	2	1/3	2/3	0	0	0	0	0	0	0	0	0	0	0	0	0
	$D_{12} \times C_2$	1	1/2	0	1/2	0	0	0	0	0	0	0	0	0	0	0	0
26	D_{26}	1	4/13	0	0	0	0	0	0	0	0	0	0	0	9/13	0	0
27	$(C_3 \times C_2) \times C_3$	5	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	$C_9 \times C_3$	3	11/27	0	16/27	0	0	0	0	0	0	0	0	0	0	0	0
28	$C_7 \times C_4$	3	11/56	0	0	0	0	0	45/56	0	0	0	0	0	0	0	0
	D_{28}	1	5/14	0	0	0	0	0	9/14	0	0	0	0	0	0	0	0
30	$S_3 \times C_5$	2	1/2	0	1/2	0	0	0	0	0	0	0	0	0	0	0	0
	$D_{10} \times C_3$	1	2/5	0	0	0	3/5	0	0	0	0	0	0	0	0	0	0
	D_{30}	1	3/10	0	1/10	0	1/5	0	0	0	0	0	0	0	0	0	2/5

After computing the i -commuting probabilities of groups of orders less than 30, we gain a deeper understanding of the i -commuting probabilities. The following answer regards to Question 3.3:

Answer 4.14. No. Consider the counterexample A_4 and $(C_3 \times C_3) \rtimes C_2$, we have $p_1(A_4) = p_1((C_3 \times C_3) \rtimes C_2) = 1/3$ and $p_2(A_4) = p_2((C_3 \times C_3) \rtimes C_2) = 2/3$. However, notice that the commutator subgroup of A_4 is V_4 , which has order 4. While the commutator subgroup of $(C_3 \times C_3) \rtimes C_2$ is generated by

$$\begin{aligned} [((0, 1), 0)((0, 1), 1)] &= ((0, 2), 1) \\ [((0, 1), 0)((0, 2), 0)] &= ((0, 2), 0) \\ [((1, 0), 0)((0, 1), 1)] &= ((2, 0), 1) \\ [((1, 0), 0)((0, 2), 0)] &= ((2, 0), 0) \\ [((1, 1), 0)((0, 1), 1)] &= ((2, 2), 0), \end{aligned}$$

which has order ≥ 5 . Hence there does not exist an isomorphism between these two commutator subgroups, thus disprove the question.

By [8], there are totally 3 Hall-Senior families in groups of order 16, i.e. the number of equivalence classes up to isoclinism is 3. One should notice that one of the classes consists only of abelian groups. From our computation, we verify that there two classes of groups that has equal $p_i(G)$, namely

- $p_1(G) = 5/8$ and $p_2(G) = 3/8$: $\text{SmallGroup}(16,3)$, $C_4 \rtimes C_4$, QD_{16} , $D_8 \times C_2$, $Q_8 \times C_2$ and $\text{SmallGroup}(16,13)$, and
- $p_1(G) = 7/16$, $p_2(G) = 3/16$ and $p_4(G) = 3/8$: D_{16} and Q_{16} .

This ends our results. However, we cannot solve the cases of symmetric groups and alternating groups. This hinders us to calculate the i -commuting probabilities of all groups. We may also try develop some stronger bounds of the i -commuting probabilities of S_n and A_n .

5 Conclusion •

We found the general formulae for finding i -commuting probabilities of dihedral groups, dicyclic groups, meta-cyclic groups, and generalized dihedral groups. We have transferred the calculation of i -commuting probabilities of meta-cyclic groups into a number-theoretic problem and provided the general formulae of some special cases.

We also investigated on the abstract relation between groups with the same i -commuting probability for all $i \in \mathbb{N}$, called isoclinism. Moreover, we developed some useful tools concerning isoclinism to help us with the computation of other groups.

Although we cannot find the general formulae of symmetric groups and alternating groups, we have found the lower bound of $p_3(S_n)$ and the necessary and sufficient condition for $p_i(S_n) > 0$ and $p_i(A_n) > 0$.

At last, we use these methods to compute the i -commuting probabilities of all of the groups of orders less than 30, though with three exceptions.

References

- [1] AZIMUTH PROJECT OFFICIAL BLOG (2018). “*The 5/8 Theorem*”
<https://johncarloshbaez.wordpress.com/2018/09/16/the-5-8-theorem/>
- [2] JOSEPH J. ROTMAN (1995). “*An Introduction to Theory of Groups*”, 4th edition, pp. 26, 33.
- [3] MADELEINE WHYBROW (2014). “*The Limit Points of The Commuting Probability Function on Finite Groups*”, pp. 11-12, 16.
- [4] M. F. NEWMAN (1990). *Groups of Prime-Power Order*, pp. 286.
- [5] D.L. JOHNSON (1997). “*Presentations of Groups, volume 15 of Student texts*”, pp. 88-89.
- [6] MARTIN LIEBECK, E.A. O’BRIEN, ANER SHALEV, PHAM HUU TIEP (2013). “*The Ore conjecture*”.
- [7] GROUPPROPS. “*Groups of a particular order*”.
https://groupprops.subwiki.org/wiki/Category:Groups_of_a_particular_order
- [8] GROUPPROPS. “*Groups of order 16*”
https://groupprops.subwiki.org/wiki/Groups_of_order_16
- [9] GROUPPROPS. “*SmallGroup(16,3)*”.
[https://groupprops.subwiki.org/wiki/SmallGroup\(16,3\)](https://groupprops.subwiki.org/wiki/SmallGroup(16,3))
- [10] GROUPPROPS. “*Central product of D_8 and Z_4* ”.
https://groupprops.subwiki.org/wiki/Central_product_of_D8_and_Z4
- [11] GROUPPROPS. “*Special linear group: $SL(2,3)$* ”.
[https://groupprops.subwiki.org/wiki/Special_linear_group:SL\(2,3\)](https://groupprops.subwiki.org/wiki/Special_linear_group:SL(2,3))

Appendix

This is the program for computing i -commuting probabilities of symmetric groups and alternating groups. It is written in C++ language.

```

#include<cstdio>
#include<algorithm>
#include<cstring>
using namespace std;
int i,j,k,l,m,n;
int a[362882],b[362882],c[362882],d[362882],ans[362882];
struct p{
    int x,y;
} inv[362882];
bool bo(p const&r,p const&s){
    return r.y<s.y;
}
int gcd(int a, int b) {
    if (b==0) return a;
    return gcd(b,a%b);
}
int lcm(int a,int b){
    return a*b/gcd(a,b);
}
void go(){
    int e[362882];
    bool f[362882]={0};
    for (int i=0;i<n;i++) e[i]=a[b[c[d[i ]]]];
    int now=1;
    for (int i=0;i<n;i++){
        int ct=0;
        if (!f[i]){
            int j=i;
            while (!f[j]){
                f[j]=1;
                j=e[j];
                ct++;
            }
            // printf (" ct=%d\n",ct);
            now=lcm(ct,now);
        }
    }
    ans[now]++;

```

```

    return ;
}
int main(){
    scanf("%d",&n);
    for (i=0;i<n;i++) a[i]=i;
    for (i=0;i<n;i++) b[i]=i;
    m=n;
    l=1;
    for (i=1;i<=m;i++) l*=i;
    for (i=0;i<l;i++){
        for (j=0;j<l;j++){
            for (k=0;k<n;k++) inv[k].x=k;
            for (k=0;k<n;k++) inv[k].y=a[k];
            sort (inv , inv+n,bo);
            for (k=0;k<n;k++) c[k]=inv[k].x;
            for (k=0;k<n;k++) inv[k].x=k;
            for (k=0;k<n;k++) inv[k].y=b[k];
            sort (inv , inv+n,bo);
            for (k=0;k<n;k++) d[k]=inv[k].x;
            /*
            printf ("%d %d\n",i,j);
            for (k=0;k<n;k++) printf("%d ",a[k]); printf("\n");
            for (k=0;k<n;k++) printf("%d ",b[k]); printf("\n");
            for (k=0;k<n;k++) printf("%d ",c[k]); printf("\n");
            for (k=0;k<n;k++) printf("%d ",d[k]); printf("\n");
            printf ("\n");
            */
            go();
            next_permutation(b,b+n);
        }
        next_permutation(a,a+n);
    }
    for (i=1;i<=20;i++) printf("%d ",ans[i]); printf("\n");
    return 0;
}

```