University of Guilan

Computational Sciences and Engineering

journal homepage: https://cse.guilan.ac.ir/

A generalization of the n^{th}- commutativity degree in finite groups

M. Hashemi [a], M. Pirzadeh [a,*]

[a] Department of Pure Mathematics, University of Guilan, Rasht, Iran

ARTICLE INFO

Article history:
Received 10 March 2022
Received in revised form 13 April 2022
Accepted 15 April 2022
Available online 17 April 2022

Keywords:
Finite groups
Nilpotent groups
Commutativity degree,
GAP

ABSTRACT

In this paper, we study the number of solutions of commutator equation $[x^n, y] = g$ in two classes of finite groups. For $g \in G$, we consider $\rho_g^n(G) = \{(x, y) \mid x, y \in G, [x^n, y] = g\}$. Then the probability that the commutator equation $[x^n, y] = g$ has a solution in a finite group G, written $P_g^n(G)$, is equal to $|\rho_g^n(G)|/|G|^2$. By using the numerical solutions of the equation $xy - zu \equiv t(\bmod n)$, we derive formulas for calculating the probability of $\rho_g^n(G)$, for some finite groups G.

1. Introduction

In the last years there has been a growing interest in the use of probability in finite group theory. One of the most important aspects that have been studied is the probability that two elements of a finite group G commute. This is denoted by $P(G)$ and is called the commutativity degree of G. In obtaining the properties of $P(G)$, Gustafson [3] proved that for a non-abelian finite group G. M. Hashemi [4] gave some explicit formulas of $P(G)$ for some particular finite groups G. Also Hashemi and et al. [5] derived formulas for calculating the probability of $P_g(G)$ where G is a two generated group of nilpotency class two.

Definition 1.1. Let G be a finite group. The commutativity degree of G, written $P(G)$, is defined as the ratio

* Corresponding author.
E-mail addresses: m.pirzadeh.math@gmail.com (M. Pirzadeh)

http://dx.doi.org/10.22124/cse.2022.21977.1028

$$P(G)=\frac{|\{(x,y)\in G\times G: xy=yx\}|}{|G|^2}.$$

In [6], Pournaki and R. Sobhani have studied and generalized this concept for the group G and $g\in G$ as follows:

$$P_g(G)=\frac{|\{(x,y)\in G\times G:[x,y]=g\}|}{|G|^2}.$$

Note that for every $g\in G$, we have $0\le P_g(G)\le 1.$ In particular for $g\in G-G'$, we get $P_g(G)=0$ and $P_g(G)=1$ if and only if G is abelian and $g = e$.

For integers $m, n, k\ge 2$ where $k\,|(m,n)$, we consider the following finitely presented groups

G_{mn} and $H(m, n, k)$, as fallows;

$$G_{mn}=\left\langle a,b \middle| a^m=b^n=1,\quad [a,b]^a=[a,b],\quad [a,b]^b=[a,b]\right\rangle,$$
$$H(m,n,k)=\left\langle a,b,c \middle| a^m=b^n=c^k=1,[a,b]=c,[a,c]=[b,c]=1\right\rangle.$$

In Section 2, we state some results that are required in later section. Section 3 is devoted to compute the formula for $P_g(G)$ where $G=G_{mn}$, $H(m, n, k)$. These results can be checked for some groups with small orders, by GAP [2].

2. Preliminary

In this section, we state some lemmas and theorems which will be used in the next section. First, we state lemmas that establishes some properties of groups of nilpotency class two, where $[x,y]=x^{-1}y^{-1}xy$.

Lemma 2.1. If G is a group and $G'\subseteq Z(G)$, then the following hold for every integer k and $u,v,w\in G$:

(1) $[uv,w]=[u,w][v,w]$ *and* $[u,vw]=[u,v][u,w]$.
(2) $[u^k,v]=[u,v^k]=[u,v]^k$.
(3) $(uv)^k=u^kv^k[v,u]^{k(k-1)/2}$.
(4) *If* $G=\langle a,b\rangle$ *then* $G'=\langle [a,b]\rangle$.

Lemma 2.2. Let m,n be positive integer numbers and $d=g.c.d(m,n)$. Then $|G_{mn}|=d\times mn$.

Proof. Consider the subgroup $H=\langle x,[x,y]\rangle$ of G_{mn}. Obviously H is abelian and a simple coset enumeration by defining n coset as $1=H$ and $ib=i+1, 1\le i\le n-1$ shows that $|G:H|=n$. Using the modified Todd-coxeter coset enumeration algorithm, yields the following presentation for H:

$$H = \langle h_1, h_2 \mid h_1^m = h_2^m = h_1^n = h_2^n = 1, [h_1, h_2] = 1 \rangle.$$

So that $H \cong Z_m \times Z_d$ and $|G_{mn}| = |G : H| \times |H| = d \times mn$.

□

The following lemma can be seen in [1].

Proposition 2.3. Let $G = G_{mn}$. The

(1) $G' = \langle [x, y] \rangle$.

(2) Every element of G is in the form $a^i b^j g$ where $0 \le i \le m-1, 0 \le j \le n-1$ and $g \in G'$.

(3) $Z(G) = \langle a, b, c \mid a^{m/d} = b^{n/d} = c^d = [a,b] = [a,c] = [b,c] = 1 \rangle$.

For the particular case, consider $m = n$ then for $m \ge 2$ we get

$$G_m = G_{mm} = \left\langle a, b \mid a^m = b^m = 1, [a,b]^a = [a,b], [a,b]^b = [a,b] \right\rangle.$$

Lemma 2.4. Let $G = G_m$. Then

(1) Every element of G can be written uniquely in the form $a^r b^s [b,a]^t$ where $0 \le r, s, t \le m-1$.

(2) $Z(G) = G' = \langle [a,b] \rangle$ and $|Z(G_m)| = m$.

(3) $|G| = m^3$.

Proposition 2.5. Let $G = G_m$ and $x \in G$. For integers $m, n \ge 2$, we have

$$x^n = a^{nr} b^{ns} [a,b]^{nt - \frac{n(n-1)}{2} rs}.$$

Proof. We use an induction method on n. By part (1) of Lemma 2.4, the assertion holds for $n = 1$. Now, let

$$x^n = a^{nr} b^{ns} [a,b]^{nt - \frac{n(n-1)}{2} rs}.$$

Then

$$x^{n+1} = a^r b^s [b,a]^t a^{nr} b^{ns} [a,b]^{nt - \frac{n(n-1)}{2} rs}.$$

Since G_m is a group of nilpotency class two, $G' \subseteq Z(G)$. Hence by Lemma 2.1, we have

$$x^{n+1} = a^r b^s a^{nr} b^{ns} [a,b]^{(n+1)t - \frac{n(n-1)}{2} rs}$$
$$= a^{(n+1)r} b^s [b,a]^{nrs} b^{ns} [a,b]^{(n+1)t - \frac{n(n-1)}{2} rs}$$
$$= a^{(n+1)r} b^{(n+1)s} [a,b]^{(n+1)t - \frac{n(n-1)}{2} rs - nrs}$$
$$= a^{(n+1)r} b^{(n+1)s} [a,b]^{(n+1)t - \frac{n(n+1)}{2} rs}.$$

Thus the assertion holds.

□

We recall the Heisenberg group

$$H(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & r & s \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} \middle| r,s,t \in \mathbb{Z} \right\}.$$

By [7] (Section 2 of Chapter 7), we get

Proposition 2.6. (1) $H(\mathbb{Z}) \cong \langle a,b,c \mid [a,b]=c, [a,c]=[b,c]=1 \rangle$.

(2) Every element of $H(\mathbb{Z})$ may be written uniquely in the form $a^i b^j c^k$, where $i, j, k \in \mathbb{Z}$.

(3) $Z(H(\mathbb{Z})) = H'(\mathbb{Z}) = \langle c \rangle$.

In particular, for $n \geq 2$, we get

$$H(n,n,n) \cong H\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) = \left\{ \begin{pmatrix} 1 & r & s \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} \middle| r,s,t \in \frac{\mathbb{Z}}{n\mathbb{Z}} \right\} \leq SL\left(3, \frac{\mathbb{Z}}{n\mathbb{Z}}\right).$$

Proposition 2.7. For $G = H(m,n,k)$ and $T = G \times G$, we have

(1) Every element of G may be written uniquely in the form $a^r b^s c^t$, where $0 \leq r < m, 0 \leq s < n$ and $0 \leq t < k$.

(2) $Z(G) = G' = \langle c \rangle$ and $|G| = mnk$.

(3) Every element of T is uniquely expressible in the form $a_1^{r_{11}} b_1^{s_{11}} c_1^{t_{11}} a_2^{r_{12}} b_2^{s_{12}} c_2^{t_{12}}$; where $0 \leq r_{11}, r_{12} < m, 0 \leq s_{11}, s_{12} < n$ and $0 \leq t_{11}, t_{12} < k$.

(4) $Z(T) = T' = \langle c_1, c_2 \rangle$ and $|T| = (mnk)^2$.

By the results 2.3 and 2.7, we see that G_{mn} and $H(m, n, k)$ are finite.

The following results are of interest to consider and one may see the proof in [4].

Corollary 2.8. For the integer $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ and variables x, y, z and u, the number of solutions of the equation $xy \equiv zu (\bmod n)$ is

$$\prod_{i=1}^{k} p_i^{2\alpha_i - 1}(p_i^{\alpha_i + 1} + p_i^{\alpha_i} - 1).$$

Corollary 2.9. Let m, n be integers and x, y, z and u be variables where $1 \le x, z \le n$ and $1 \le y, u \le m$. Then the number of solutions of the equation $xy \equiv zu (\bmod d)$ is

$$(\frac{m}{d})^2 (\frac{n}{d})^2 \prod_{i=1}^{k} p_i^{2\alpha_i - 1}(p_i^{\alpha_i + 1} + p_i^{\alpha_i} - 1),$$

where $d = gcd(m, n) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

3. Computations on finite groups

This section is devoted to compute a generalization of commutativity degree of some classes of finite groups. First, we need the following Theorem.

Theorem 3.1. [5] For the integers t, n and variables x, y, u and z, the number of solutions of the equation $xy - uz \equiv t \ (\bmod n)$ is

$$\sum_{d|n} [\sum_{d_2|d_1} (\frac{n^2}{d} \phi(\frac{n}{d}) \phi(\frac{d}{d_2}) \times d_2)].$$

By elementary concepts of number theory, we have the following corollary:

Corollary 3.2. Let t, n be integers and i, j, r and s be variables, when $0 \le i, s < n$ and $0 \le r, j < n^2$. Then the number of solutions of the equation $ri - sj \equiv t \ (\bmod n)$ is

$$n^3 \sum_{d|n} [\sum_{d_2|d_1} (\frac{n}{d} \phi(\frac{n}{d}) \phi(\frac{d}{d_2}) \times d_2)].$$

Now, we get explicit formulas for the commutativity degree of generalized relative g the element of G of the finite group G_m.

Theorem 3.3. For the group $G = G_m$ and $g \in G'$, $P_g(G) = \alpha / m^6$, where

$$\alpha = m^3 [\sum_{d|m} (\sum_{d_2|(d, t_g)} \frac{m}{d} \phi(\frac{m}{d}) \phi(\frac{d}{d_2}) \times d_2)].$$

Proof. For the $g \in G'$, we obtain

$$
\begin{aligned}
|\rho_g(G)| &= |\{(x,y)\in G\times G;\ [x,y]=g\}| \\
&= |\{(x,y)\in G\times G;\ a^{m(r_2s_1-r_1s_2)}=a^{mt_g}\}| \\
&= |\{(r_1,s_1,r_2,s_2);\ r_2s_1-r_1s_2\equiv t_g (mod\ m)\}|.
\end{aligned}
$$

So that, by Corollary 3.2, we have

$|\rho_g(G)|=m^3\sum_{d|m}[\frac{m}{d}\phi(\frac{m}{d})(\sum_{d_2|d_1}\phi(\frac{d}{d_2})\times d_2)],$ where $d\,|\,m, d_1=(d,t_g)$. And the result follows from the $P_g(G)=\frac{|\rho_g(G)|}{|G|^2}$. □

In the present part, we consider $G=H(m,n,k)$. To compute the commutativity degree of G, let $x,y\in G$. Then by the first part of Proposition 2.7, we have $x=a^{r_1}b^{s_1}c^{t_1}$, $y=a^{r_2}b^{s_2}c^{t_2}$ where

$0\le r_1,r_2\le m-1$, $0\le s_1,s_2\le n-1$ and $0\le t_1,t_2\le k-1$. Hence by Lemma 2.1 and the relations of G, we get $[x,y]=c^{s_1r_2-s_2r_1}$.

By using the above information, we prove that;

Theorem 3.4. For the group $G=H(m,n,k)$, we have $P_g(G)=\frac{\beta}{(mnk)^2}$ where

$$\beta=\frac{1}{t^2}\sum_{d|t}\left[\sum_{d_2|d}\phi\left(\frac{t}{d}\right)\phi\left(\frac{d}{d_2}\right)\frac{d_2}{d}\right].$$

Proof. For $g=c^{t_g}\in G'$, we have

$$
\begin{aligned}
|\rho_g| &= |\{(x,y)\in G\times G;\ [x,y]=g\}| \\
&= \left|\left\{(x,y)\in G\times G;\ c^{r_1s_2-r_2s_1}=c^{t_g}\right\}\right| \\
&= \left|\left\{\left(r_1,s_1,t_1,r_2,s_2,t_2\right); r_1s_2-r_2s_1\equiv t_g\,(\operatorname{mod} k)\right\}\right|.
\end{aligned}
$$

$$
\begin{aligned}
\beta =& |\left\{\left(r_1,s_1,t_1,r_2,s_2,t_2\right); 0\le r_1,r_2\le m-1, 0\le s_1,s_2\le n-1, 0\le t_1,t_2\le k-1,\right. \\
& \left. r_1s_2-r_2s_1\equiv ti\,(\operatorname{mod} t)\right\}| = |\left\{\left(r_1,s_1,t_1,r_2,s_2,t_2\right); 0\le r_1,r_2\le m-1, 0\le s_1,s_2\le n-1, 0\le t_1,t_2\le k-1,\right. \\
& \left. r_1s_2-r_2s_1\equiv 0\ (\operatorname{mod} t)\right\}| = \frac{(mnk)^2}{t^2}\sum_{d|t}\left[\sum_{d_2|d}\phi\left(\frac{t}{d}\right)\phi\left(\frac{d}{d_2}\right)\frac{d_2}{d}\right] \\
&= \frac{(mnk)^2}{t^4}\sum_{d|t}\left[\sum_{d_2|d}\frac{t^2}{d}\phi\left(\frac{t}{d}\right)\phi\left(\frac{d}{d_2}\right)\times d_2\right].
\end{aligned}
$$

We now turn to a generalization of $P_g(G)$. For everyr, we conside $n \geq 2$ $[x^n, y] = g$, Then the probability that the commutator equation $\rho_g^n(G) = \{(x,y) \in G \times G; [x^n, y] = g\}$. written $P_g^n(G)$, is equal to $\frac{|\rho_g^n(G)|}{|G \times G|}$. That is $P_g^n(G) = \frac{|\rho_g^n(G)|}{|G \times G|}$. Now, for the group $n \geq 1$ and integer G_m, $g \in G_m$ .ads us to prove the main resultThese facts le $[x^n, y] = g.$; we consider the commutator equation

Theorem 3.5. For the group G_m, $g = [a,b]^t \in G'_m$ and, we have $n \in \mathbb{N}$

(1) the equation $[x^n, y] = g$ has a solution in G_m if and only if $l \mid t$, where $l = gcd(m,n)$.

(2) $P_g^n(G_m) = \gamma / m^6$, where $\gamma = \sum_{d \mid \frac{m}{l}} [\sum_{d_2 \mid (d, \frac{t}{l})} (\frac{m^2}{l^2 d} \phi(\frac{m}{ld}) \phi(\frac{d}{d_2}) \times d_2)]$.

Proof. Let $x = a^{r_1} b^{s_1} [b,a]^{t_1}, y = a^{r_2} b^{s_2} [b,a]^{t_2} \in G_m$, we have 2.4. Then by the first part of Lemma $x, y \in G_m$, where $1 \leq r_1, r_2, s_1, s_2, t_1, t_2 \leq m$. Now, using Lemma 2.1, Proposition 2.4 and the relations of G_m, we get

$$x^n y = a^{nr_1 + r_2} b^{ns_1 + s_2} [a,b]^{nt_1 + t_2 - \frac{n(n-1)}{2} r_1 s_1 - nr_2 s_1}$$

and

$$yx^n = a^{nr_1 + r_2} b^{ns_1 + s_2} [a,b]^{nt_1 + t_2 - \frac{n(n-1)}{2} r_1 s_1 - nr_1 s_2}.$$

Thus

$$[x^n, y] = [a,b]^{n(r_1 s_2 - r_2 s_1)}.$$

On the other hand by the second part of Lemma 2.4, for $x, y, g \in G$ where $g = [x,y] \in G' = \langle [a,b] \rangle$ there is $1 \leq t \leq m$ such that $g = [x,y] = [a,b]^t$. Now, for $g \in G'$, we obtain

$$\begin{aligned} |\rho_g(G)| &= |\{(x,y) \in G \times G; [x,y] = g\}| \\ &= |\{(x,y) \in G \times G; [a,b]^{n(r_1 s_2 - r_2 s_1)} = [a,b]^t\}| \\ &= |\{(r_1, s_1, t_1, r_2, s_2, t_2); n(r_1 s_2 - r_2 s_1) \equiv t \,(mod\, m)\}|. \end{aligned}$$

For the calculating of $\rho_g^n(G)$, let $l = gcd(m,n)$. Then $\frac{n}{l}(r_1 s_2 - r_2 s_1) \equiv \frac{t}{l} (\mathrm{mod} \frac{m}{l})$. Since $(\frac{n}{l}, \frac{m}{l}) = 1$, we have $r_1 s_2 - r_2 s_1 \equiv \frac{t}{l} (\mathrm{mod} \frac{m}{l})$. So, the congruence has the solution if and only if $l \mid t$. Therefore, by Theorem 3.1, the result follows.

The Table 1 is a verified result of GAP [2], where $2 \le n \le 10$ and some values of $m,\ t$.

***Table 1*:** The number of solutions of $n(r_1s_2 - r_2s_1) \equiv t(\bmod m)$.

n	m	t	The number of solutions of $n(r_1s_2 - r_2s_1) \equiv t(\bmod m)$.
2	2	2	16
3	6	3	486
4	8	4	1536
5	10	5	3750
6	4	2	96
7	7	14	2401
8	6	2	384
9	3	6	81
10	15	5	15000

4. Conclusions

In this paper, by using the properties of G_m, we obtain $\rho_g^n(G)$ for $g \in G$ and $n \ge 1$. For these, it is enough to compute the $[x^n, y] = g$ where $x, y \in G_m$. We note that, this method can be generalized to finite groups of small orders.

Acknowledgment

The authors would like to thank reviewers for the reading and their useful comments in this paper.

References

[1] Doostie, H., Hashemi, M. (2006.).“Fibonacci lenghts involving the Wall number K(n) ”, *J. Appl. Math. Computing*, Vol. 20, pp. 171– 180.
[2] The GAP Group, GAP,(2020). “Groups, Algorithms and Programming”, Version 4.1.10, www.gap-system.org.
[3] Gustafson, W. H. (1973). “What is the probability that two group elements commute*?”,Amer Math. Monthly*, Vol. 80, pp. 1031–1034.
[4] Hashemi, M. (2015).“The commutative degree on 2-generated groups with nilpotency class 2”, Ars Combin, Vol. 122, pp. 149– 159.
[5] Hashemi, M., Pirzadeh, M., and Gorjian, S. A., “The probability that the commutator equation [x, y] = g has solution in a finite group”, *Journal of Algebra and Related Topics*, Vol. 7, No. 2, pp. 47–61, 2020.
[6] Pournaki, M. R., Sobhani, R (2008). “Probability that the commutator of two group elements is equal to a given element”, *J. Pure and Applied Algebra*, Vol. 212, pp. 727–734.
[7] Johnson, D. L. Presentations of Groups (1997). *Cambridge University Press.*