PROBABILITY OF MUTUALLY COMMUTING TWO FINITE SUBSETS OF A FINITE GROUP

R. BARZGAR P., A. ERFANIAN, AND M. FARROKHI D. G.

ABSTRACT. For a finite group G let P(m, n, G) denote the probability that two m-subset and n-subset of G commute elementwise and let P(n, G) = P(1, n, G) be the probability that an element commutes with an n-subset of G. Some lower and upper bounds are given for P(m, n, G) and it is shown that $\{P(m, n, G)\}_{m,n}$ is decreasing with respect to m and n. Also P(m, n, G) is computed for some classes of finite groups, including groups with central factor of order p^2 and P(n, G) is computed for groups with central factor of order p^3 and wreath products of finite abelian groups.

1. Introduction

If G is a finite group, then the commutativity degree of G denoted by d(G), is the probability that two randomly chosen elements of G commute. The commutativity degree first studied by Gustafson [4] and it is shown that $d(G) \leq \frac{5}{8}$ for every nonabelian finite group. Also there have given several lower and upper bounds for the commutativity degree in the case of p-groups, solvable groups and simple groups and it is computed for various classes of groups those of most important are semidirect products and wreath products of finite abelian groups. We refer the reader to [1, 3, 6, 7, 8] for more details.

²⁰⁰⁰ Mathematics Subject Classification. Primary 20P05; Secondary 20D15,20E22.

Key words and phrases. Probability, nilpotent group, p-group, wreath product.

Our aim is to generalize the commutativity degree to the case where two subsets of given sizes commute elementwise and obtain several results including lower and upper bounds. Moreover, the probability will be computed for some classes of finite groups including finite groups with central factors as p-groups of order at most p^3 and wreath products of finite abelian groups.

2. Lower and upper bounds

We begin with the following definition.

Definition. Let G be a finite group and $m, n \leq |G|$. Then the probability that two m-subset (subset of size m) and n-subset of G commute elementwise is

$$P(m, n, G) = \frac{|\{(X, Y) \in P_m(G) \times P_n(G) : [X, Y] = 1\}|}{\binom{|G|}{m}\binom{|G|}{n}},$$

where $P_k(G)$ is a set of all k-subsets of G. We denote P(1, n, G) by P(n, G) and as usual P(1, 1, G) by d(G).

Clearly P(m, n, G) = 1 if and only if G is an abelian group. If $|G|/p < m \le |G|$, then $P(m, n, G) = \binom{|Z(G)|}{n}/\binom{|G|}{n}$, where p is the least prime divisor of |G|. Hence we always assume that $m, n \le |G|/p$. Let \mathcal{G}_p denote the class of all finite groups with p as the smallest prime divisor of |G| for convenience.

Theorem 2.1. Let $G \in \mathcal{G}_p$ and $m, n \leq |G|/p$. Then

$$\frac{\binom{|Z(G)|}{m}}{\binom{|G|}{m}} \leq P(m,n,G) \leq \frac{\binom{|G|}{n} - \binom{\frac{|G|}{p}}{n}}{\binom{|G|}{m}\binom{|G|}{n}} \binom{|Z(G)|}{m} + \frac{\binom{\frac{|G|}{p}}{n}}{\binom{|G|}{n}}.$$

Proof. If $X \not\subseteq Z(G)$, then $|C_G(X)| \leq \frac{1}{p}|G|$. Now we have

$$P(m,n,G) = \frac{1}{\binom{|G|}{m}\binom{|G|}{n}} \sum_{X \in P_m(G)} \binom{|C_G(X)|}{n}$$

$$\begin{split} &= \frac{1}{\binom{|G|}{m}\binom{|G|}{n}} \left(\sum_{X \in P_m(Z(G))} + \sum_{\substack{X \in P_m(G) \\ X \not\in P_m(Z(G))}} \right) \binom{|C_G(X)|}{n} \\ &\leq \frac{1}{\binom{|G|}{m}\binom{|G|}{n}} \left(\binom{|Z(G)|}{m}\binom{|G|}{n} + \binom{|G|}{m} - \binom{|Z(G)|}{m} \right) \binom{\frac{|G|}{p}}{n} \right) \\ &\text{and the result follows.} & \Box \end{split}$$

Theorem 2.2. Let G be a finite group. Then the sequence $\{P(m,n,G)\}_{n\geq 1}$ is decreasing.

Proof. Utilizing the fact that

$$\binom{k}{i+1} = \frac{k-i}{i+1} \binom{k}{i}$$

for each positive integers i and k with i < k, we get

$$P(m, n+1, G) = \frac{1}{\binom{|G|}{m}\binom{|G|}{n+1}} \sum_{X \in P_m(G)} \binom{|C_G(X)|}{n+1}$$

$$= \frac{1}{\binom{|G|}{m}\binom{|G|}{n}} \sum_{X \in P_m(G)} \frac{|C_G(X)| - n}{|G| - n} \binom{|C_G(X)|}{n}$$

$$\leq \frac{1}{\binom{|G|}{m}\binom{|G|}{n}} \sum_{X \in P_m(G)} \binom{|C_G(X)|}{n}$$

$$= P(m, n, G),$$

as required.

Corollary 2.3. Let G be a finite group. Then $P(m, n, G) \leq P(n, G) \leq d(G)$ for each $m, n \geq 1$.

In the sequel we will obtain an upper bound for P(m, n, G) in terms of d(G) and the index of Z(G) in G. The following simple lemma will be used in the next theorem.

Lemma 2.4. Let m, n and k be positive integers such that $2 \le k \le m, n$. Then

$$\binom{m}{k}\binom{n}{k} < \binom{mn}{k}.$$

Proof. The result follows by observing the fact that

$$\frac{m+1-i}{i} \cdot \frac{n+1-i}{i} < \frac{mn+1-i}{i}$$

for each $1 \le i \le k$.

Remark. For each non-abelian group $G \in \mathcal{G}_p$ and $k \geq 1$ let $A_k = \{X \in P_k(G) : X \not\subseteq Z(G) \text{ and } |C_G(X)| \geq k\}$. Then define $l(G) = \max\{k \in \mathbb{N} : k < |G| \text{ and } A_k \neq \emptyset\}$. It is clear that $l(G) \leq |G|/p$.

Theorem 2.5. If $G \in \mathcal{G}_p$ is a non-abelian group, then

$$P(m, n, G) \leq \frac{d(G)}{p^{m+n-2}} + \frac{1}{[G: Z(G)]} \cdot \frac{p^{m-1} - 1}{(p-1)p^{m+n-3}} + \left(\frac{[G: Z(G)]}{m}\right)^{-1} \cdot \frac{p^{n-1} - 1}{(p-1)p^{n-2}}$$

for all $m, n \leq l(G)$.

Proof. For each i < l(G) we have

$$P(m, i+1, G) = \frac{1}{\binom{|G|}{m} \binom{|G|}{i+1}} \sum_{X \in P_m(G)} \binom{|C_G(X)|}{i+1}$$
$$= \frac{1}{\binom{|G|}{m} \binom{|G|}{i}} \sum_{X \in P_m(G)} \frac{|C_G(X)| - i}{|G| - i} \binom{|C_G(X)|}{i}$$

$$= \frac{1}{\binom{|G|}{m}\binom{|G|}{i}} \left(\sum_{X \in P_m(Z(G))} + \sum_{\substack{X \in P_m(G) \\ X \notin P_m(Z(G))}} \frac{|C_G(X)| - i}{|G| - i} \binom{|C_G(X)|}{i} \right)$$

$$\leq \frac{1}{\binom{|G|}{m}\binom{|G|}{i}} \left(\sum_{X \in P_m(Z(G))} \binom{|G|}{i} + \sum_{\substack{X \in P_m(G) \\ X \notin P_m(Z(G))}} \frac{\frac{|G|}{p} - i}{|G| - i} \binom{|C_G(X)|}{i} \right)$$

$$= \frac{1}{p} P(m, i, G) + \left(1 - \frac{1}{p} \right) \frac{|G|}{|G| - i} \frac{\binom{|Z(G)|}{m}}{\binom{|G|}{m}}$$

$$< \frac{1}{p} P(m, i, G) + \frac{1}{\binom{|G:Z(G)|}{i}} \qquad \text{(By Lemma 2.4 and } n \leq \frac{|G|}{p} \text{)}$$

Thus

$$P(m,n,G) \leq \frac{P(m,G)}{p^{n-1}} + \frac{1}{\binom{[G:Z(G)]}{m}} \cdot \frac{p^{n-1}-1}{p^{n-2}(p-1)}$$

and by the same method

$$P(m,G) \le \frac{d(G)}{p^{m-1}} + \frac{1}{[G:Z(G)]} \cdot \frac{p^{m-1}-1}{p^{m-2}(p-1)},$$

П

from which the result holds.

Corollary 2.6. Let $G \in \mathcal{G}_p$ and $m, n \leq l(G)$. Then

(i) If G is non-abelian, then

$$P(m,n,G) \leq \frac{p^2+p-1}{p^{m+n+1}} + \frac{p^{m-1}-1}{(p-1)p^{m+n-1}} + \binom{p^2}{m}^{-1} \cdot \frac{p^{n-1}-1}{(p-1)p^{n-2}}.$$

(iii) If G is a finite p-group of derived length $d \geq 2$, then

$$P(m,n,G) \leq \frac{p^d + p^{d-1} - 1}{p^{m+n+2d-3}} + \frac{p^{m-1} - 1}{(p-1)p^{m+n-1}} + \binom{p^2}{m}^{-1} \cdot \frac{p^{n-1} - 1}{(p-1)p^{n-2}}.$$

Proof. The result follows by Theorem 2.5 and the facts that $d(G) \leq \frac{p^2+p-1}{p^3}$ (see [6, Lemma 1.3]) and if G is a p-group of

derived length $d \geq 2$, then $d(G) \leq \frac{p^d + p^{d-1} - 1}{p^{2d-1}}$ (see [7, Theorem 12(ii)]).

3. GROUPS WITH SMALL CENTRAL FACTORS

In this section we shall compute P(m, n, G) and P(n, G) for finite groups G such that G/Z(G) is a p-group of order p^2 and p^3 , respectively. The following theorem is a generalization of Theorem 2.4 in [2].

Theorem 3.1. If G is a finite group such that $\frac{G}{Z(G)} \cong \mathbb{Z}_p \times \mathbb{Z}_p$, then

$$P(m, n, G) = \frac{1}{\binom{|G|}{m} \binom{|G|}{n}} \times \left[(p+1) \left(\binom{\frac{|G|}{p}}{m} - \binom{|Z(G)|}{m} \right) \left(\binom{\frac{|G|}{p}}{n} - \binom{|Z(G)|}{n} \right) + \binom{|Z(G)|}{m} \binom{|G|}{n} + \binom{|Z(G)|}{n} \binom{|G|}{n} - \binom{|Z(G)|}{m} \binom{|Z(G)|}{n} \right].$$

Proof. Let X be an m-subset of G and $\mathcal{M} = \{M_1, \ldots, M_{p+1}\}$ be the set of all maximal subgroups of G containing Z(G). Also let \mathcal{A} , \mathcal{B} and \mathcal{C} denote the m-subsets of Z(G), M_i $(1 \le i \le p+1)$ and G, respectively. Now we consider the following cases.

- (i) If $X \in \mathcal{A}$, then $C_G(X) = G$ and there are $\binom{|Z(G)|}{m}$ such subsets.
 - (ii) If $X \in \mathcal{B} \setminus \mathcal{A}$, then $|C_G(X)| = |G|/p$ and there are

$$(p+1)\left(\binom{|G|}{p}-\binom{|Z(G)|}{m}\right)$$

such subsets.

(iii) If $X \in \mathcal{C} \setminus \mathcal{B}$, then $C_G(X) = Z(G)$ and the number of all such subsets is

$$\binom{|G|}{m} - (p+1) \left(\binom{\frac{|G|}{p}}{m} - \binom{|Z(G)|}{m} \right) - \binom{|Z(G)|}{m}.$$

Using the above results we have

$$\begin{split} &P(m,n,G) \\ &= \frac{1}{\binom{|G|}{m}\binom{|G|}{n}} \sum_{X \in P_m(G)} \binom{|C_G(X)|}{n} \\ &= \frac{1}{\binom{|G|}{m}\binom{|G|}{n}} \left(\sum_{X \in \mathcal{A}} + \sum_{X \in \mathcal{B} \backslash \mathcal{A}} + \sum_{X \in \mathcal{C} \backslash \mathcal{B}} \right) \binom{|C_G(X)|}{n} \\ &= \frac{1}{\binom{|G|}{m}\binom{|G|}{n}} \left(|\mathcal{A}|\binom{|G|}{n} + |\mathcal{B} \backslash \mathcal{A}|\binom{\frac{|G|}{p}}{n} + |\mathcal{C} \backslash \mathcal{B}|\binom{|Z(G)|}{n} \right) \end{split}$$

and by substituting the size of \mathcal{A} , $\mathcal{B} \setminus \mathcal{A}$ and $\mathcal{C} \setminus \mathcal{B}$ the result follows.

Corollary 3.2. Let $G \in \mathcal{G}_p$ be a non-abelian group. Then $\frac{G}{Z(G)} \cong \mathbb{Z}_p \times \mathbb{Z}_p$ if and only if

$$P(n,G) = \left(1 - \frac{\binom{|G|}{p}}{\binom{|G|}{n}}\right) \frac{1}{p^2} + \frac{\binom{|G|}{p}}{\binom{|G|}{n}}.$$

Proof. If $\frac{G}{Z(G)} \cong \mathbb{Z}_p \times \mathbb{Z}_p$, then it is enough to put m = 1 in Theorem 3.1. Conversely, by Theorem 2.1, we get $[G: Z(G)] \leq p^2$, which follows that $[G: Z(G)] = p^2$.

The following theorem gives a partial generalization of the above corollary.

Theorem 3.3. If G is a finite nilpotent group of class 2 such that |G'| = p, then

$$P(n,G) = \left(1 - \frac{\binom{|G|}{n}}{\binom{|G|}{n}}\right) \frac{1}{[G:Z(G)]} + \frac{\binom{|G|}{n}}{\binom{|G|}{n}}.$$

Proof. If $x \in G \setminus Z(G)$, then $|x^G| = |x[x,G]| = |[x,G]|$, where [x,G] is a subgroup of G'. Hence $|x^G| = p$ and so $|C_G(x)| = \frac{|G|}{p}$. The result follows easily.

Theorem 3.4. Let G be a finite group such that $\frac{G}{Z(G)}$ is a p-group of order p^3 .

(i) If G has no abelian maximal subgroup, then

$$P(n,G) = \frac{|Z(G)|}{\binom{|G|}{n}} \left[\binom{|G|}{n} + (p^3 - 1) \binom{p|Z(G)|}{n} \right].$$

(ii) If G has an abelian maximal subgroup, then

$$P(n,G) = \frac{|Z(G)|}{\binom{|G|}{n}} \left[\binom{|G|}{n} + (p^2 - 1) \binom{\frac{|G|}{p}}{n} + p^2(p-1) \binom{\frac{|G|}{p^2}}{n} \right].$$

Proof. (i) If G has no abelian maximal subgroups, then $C_G(x) = \langle Z(G), x \rangle$ and so $|C_G(x)| = |G|/p^2$ for each $x \in G \setminus Z(G)$. Hence

$$P(n,G) = \frac{1}{\binom{|G|}{n}} \left[\sum_{x \in Z(G)} \binom{|C_G(x)|}{n} + \sum_{x \in G \setminus Z(G)} \binom{|C_G(x)|}{n} \right]$$
$$= \frac{1}{\binom{|G|}{n}} \left[|Z(G)| \binom{|G|}{n} + |G \setminus Z(G)| \binom{\frac{|G|}{p^2}}{n} \right]$$

and the result follows.

(ii) Assume that G has a unique abelian maximal subgroup M, which of course is unique. If $x \in M \setminus Z(G)$, then $C_G(x) = M$ and so $|C_G(x)| = |G|/p$. Also if $x \in G \setminus M$, then $C_G(x) = \langle Z(G), x \rangle$ that is $|C_G(x)| = |G|/p^2$. Now we have

$$P(n,G)$$

$$= \frac{1}{\binom{|G|}{n}} \left(\sum_{x \in Z(G)} + \sum_{x \in M \setminus Z(G)} + \sum_{x \in G \setminus M} \right) \binom{|C_G(x)|}{n}$$

$$= \frac{1}{\binom{|G|}{n}} \left[|Z(G)| \binom{|G|}{n} + |M \setminus Z(G)| \binom{\frac{|G|}{p}}{n} + |G \setminus M| \binom{\frac{|G|}{p^2}}{n} \right]$$

and the result follows.

4. Wreath products of finite abelian groups

We use the notations and terminologies in [3]. Let A and B be any groups and A^* be the weak direct product of copies of A indexed by elements of B. If $\sigma_a(b)$ denotes the element of A^* with a on b-th component and 1 elsewhere, then an arbitrary element of A^* can be written in the form

$$\sigma_{a_1}(b_1)\cdots\sigma_{a_s}(b_s),$$

where b_1, \ldots, b_s are distinct elements of B and a_1, \ldots, a_s are any elements of A. Then the wreath product $A \wr B$ is the semidirect product of A^* and B, with respect to the following action of B on A^* :

$$\sigma_a(b)^{\tau_c} = \sigma_a(bc^{-1}),$$

where we denote an element c of B by τ_c in the canonical copy of B in $A \wr B$. An arbitrary element of $A \wr B$ can be written uniquely in the form

$$\sigma_{a_1}(b_1)\cdots\sigma_{a_s}(b_s)\tau_b,$$

where $\sigma_{a_1}(b_1)\cdots\sigma_{a_s}(b_s)$ is an element of A^* and τ_b is an element of B. In the following theorem we give an analogue of Theorem 1.1 in [3].

Theorem 4.1. Let $G = A \wr B$ be the wreath product of finite abelian groups A and B. Then

$$P(n,G) = \frac{1}{|G|\binom{|G|}{n}} \sum_{s,t_1,\dots,t_n \in B} \left(\prod_{b \in B} \binom{|A|^{\beta(s)}}{l_b} \right) |A|^{|B|-\beta(s)+\alpha(s,t_1,\dots,t_n)},$$

where l_b is the number of i such that $t_i = b$ and $\beta(s)$ and $\alpha(s, t_1, \ldots, t_n)$ are the index of subgroups $\langle s \rangle$ and $\langle s, t_1, \ldots, t_n \rangle$ in B, respectively, for each $s, t_1, \ldots, t_n, b \in B$.

Proof. First suppose that $B = \mathbb{Z}_m$ is a cyclic group. Fix the elements $s, t_1, \ldots, t_n \in B$ and let $g, h_1, \ldots, h_n \in G$ be elements with the following expressions

$$g = \sigma_{a_1} \cdots \sigma_{a_m} \tau_{-s}$$

and

$$h_i = \sigma_{x_{i,1}} \cdots \sigma_{x_{i,m}} \tau_{-t_i},$$

where h_i are pairwise distinct. Also let $\beta(s) = \gcd(m, s)$ and $\alpha(s, t_1, \ldots, t_n) = \gcd(m, s, t_1, \ldots, t_n)$ be the index of subgroups $\langle s \rangle$ and $\langle s, t_1, \ldots, t_n \rangle$ in B. According to the proof of [3, Theorem 1.1], g and h_i commute if and only if the following system of equations hold for each $i = 1, \ldots, \beta(s)$ and $j = 1, \ldots, n$:

$$x_{i} - x_{i+s} = a_{i} - a_{i+t_{j}}$$

$$x_{i+s} - x_{i+2s} = a_{i+s} - a_{i+s+t_{j}}$$

$$\vdots$$

$$x_{i+ds} - x_{i+(d+1)s} = a_{i+ds} - a_{i+(d+1)s+t_{j}}$$

and

(1)
$$a_i + a_{i+s} + \dots + a_{i+ds} = a_{i+t_j} + a_{i+s+t_j} + \dots + a_{i+ds+t_j}$$

where $n = (d+1)\beta(s)$.

By the first system of equations (x_{i1}, \ldots, x_{im}) can be chosen in $|A|^{\beta(s)}$ different many ways, for each $i=1,\ldots,n$. We shall count the number of n-tuples (x_{i1},\ldots,x_{in}) is such a way that h_1,\ldots,h_n are distinct. Clearly $h_i\neq h_j$ if $t_i\neq t_j$ and no restriction on x_{ik} and x_{jk} is needed. Moreover, if $t_i=t_j$, then we should have $(x_{i1},\ldots,x_{im})\neq (x_{j1},\ldots,x_{jm})$. Let l_i be the number of t_j equal to i. Then $l_1+\cdots+l_n=m$ and any solution to this equation is equivalent to an n-subset $\{t_1,\ldots,t_n\}$ of B. Hence the number of n-tuples (h_1,\ldots,h_n) is

$$\binom{|A|^{\beta(s)}}{l_1}\cdots \binom{|A|^{\beta(s)}}{l_n}.$$

On the other hand, the equation (1) holds for each t_j and one easily see that

(2)
$$a_i + a_{i+s} + \dots + a_{i+ds} = a_{i+t} + a_{i+s+t} + \dots + a_{i+ds+t}$$

for each linear combination t of t_1, \ldots, t_n . Let $t = \gcd(t_1, \ldots, t_n)$. Then the equation (2) distribute $\alpha(s, t_1, \ldots, t_n)$ independent

subsystems

$$a_{i} + a_{i+s} + \dots + a_{i+ds} = a_{i+t} + a_{i+s+t} + \dots + a_{i+ds+t}$$

$$a_{i+t} + a_{i+s+t} + \dots + a_{i+ds+t} = a_{i+2t} + a_{i+s+2t} + \dots + a_{i+ds+2t}$$

$$\vdots$$

$$a_{i+(u-1)t} + a_{i+s+(u-1)t} + \dots + a_{i+ds+(u-1)t}$$

$$= a_{i+ut} + a_{i+s+ut} + \dots + a_{i+ds+ut}$$

where $u = \beta(s)/\alpha(s, t_1, \ldots, t_n)$ is the order of subgroup $\langle t + \langle s \rangle \rangle = \langle t_1 + \langle s \rangle, \ldots, t_n + \langle s \rangle \rangle$ of $B/\langle s \rangle$. Hence the number of n-tuples (a_1, \ldots, a_m) is

$$|A|^{m-(u-1)\alpha(s,t_1,...,t_n)} = |A|^{m-\beta(s)+\alpha(s,t_1,...,t_n)}.$$

Clearly the result holds by assuming $B = \{b_i : i \in I\}$ is any abelian group and replacing s, t_i by b_s, b_{t_i} . Hence the proof is complete.

Acknowledgement. The authors are grateful the referee for some helpful comments and reminding us the Dossti and Maghasadi's paper [1] on the commutativity degree of semidirect and wreath products of abelian groups.

REFERENCES

- [1] H. Doosti and M. Maghasedi, Certain classes of groups with commutativity degree d(G) < 1/2, Ars Combin., 89 (2008), 263-270.
- [2] A. Erfanian and F. Russo, Probability of mutually commuting n-tuples in some classes of compact groups, Bull. Iranian Math. Soc., 34(2) (2008), 27-37.
- [3] I. V. Erovenko and B. Sury, Commutativity degrees of wreath products of finite abelian groups, Bull. Asut. Math. Soc., 77 (2008), 31-36.
- [4] W. H. Gustafson, What is the probability that two groups elements commute?, Amer. Math. Monthly 80 (1973), 1031-1304.
- [5] P. Lescot, Central extention and commutativity degree, Comm. Algebra, 29(10) (2001), 4451-4460.
- [6] P. Lescot, Isoclinism classes and commutativity degrees of finite groups, J. Algebra, 177 (1995), 847-869.
- [7] R. M. Guralnick and G. R. Robinson, On the commuting probability in finite groups, J. Algebra, 300(2) (2006), 509-528.

[8] R. K. Nath and A. K. Das, On a lower bound of commutativity degree, Rend. Circ. Mat. Palermo, 59 (2010), 137-142.

DEPARTMENT OF MATHEMATICS AND CENTER OF EXCELLENCE IN ANALYSIS ON ALGEBRAIC STRUCTURES, FERDOWSI UNIVERSITY OF MASHHAD, MASHHAD, IRAN.

E-mail address: ro.gbps@gmail.com
E-mail address: erfanian@math.um.ac.ir
E-mail address: m.farrokhi.d.g@gmail.com