# The commutativity degree of 2-generated groups of nilpotency class 2

M. Hashemi

Department of Mathematics, Faculty of Science, University of Guilan, Rasht, Iran.
Email: m_hashemi@guilan.ac.ir

**Abstract**

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

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

In this paper we examine the commutativity degree of groups of nilpotency class 2 and by using the numerical solutions of the equation $xy \equiv zu(mod\ n)$, we give certain explicit formulas for some particular classes of finite groups. A lower bound for $d(G)$ is obtained for 2-generated groups of nilpotency class 2.

**AMS Subject Classification:** 11b39, 20K05.
**Keywords:** Commutativity degree, Finite groups.

**ARS COMBINATORIA 122(2015)**, pp. 149-159

## 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 d(G) and is called the commutativity degree of G. In obtaining the properties of $d(G)$, Gustafson [5] proved that for a non-abelian finite group $G$, $d(G) \leq \frac{5}{8}$, and P. Lescote [8] studied the groups where $d(G) \geq \frac{1}{2}$ and classified these groups. In [4], H. Doostie and M. Maghaseedi gave some explicit formulas of d(G) for some particular finite groups $G$. Also, Moghaddam and et al in [9] studied the n-nilpotency degree of finite groups (denoted by $d^n(G)$ ). In fact, for the special cases of the groups $N$ and $H$, they proved the equality $d^n(N \times H) = d^n(N) \times d^n(H)$.

**Lemma 1.1. (Von dyck's Lemma) [7, Proposition 4.2].** Let $F(X)$ be the free group on the set $X$ and let $\bar{R}$ denotes the normal closure of the subset $R$ of $F(X)$. If $G = \langle X|R\rangle$ and $H = \langle X|S\rangle$, where $R \subseteq S \subseteq F(X)$, then there exists an epimorphism $\phi : G \longrightarrow H$ fixing every $x \in X$ such that $\ker\phi = \bar{S}/\bar{R}$. Conversely, every factor group of $G = \langle X|R\rangle$ has a presentation $\langle X|S\rangle$ with $R \subseteq S$.

**Lemma 1.2. [8, Lemma 1.4.]** Let $G$ be a finite group and $N$ be a normal subgroup of $G$. Then

$$d(G) \leq d(N)d(\frac{G}{N}).$$

We consider the following finitely presented groups,

$$G_{mn} = \langle a, b | a^m = b^n = 1, \ [a,b]^a = [a,b], \ [a,b]^b = [a,b] \rangle,$$

where $m, \ n \geq 2$,

$$H_n = \langle a, b | a^{n^2} = b^n = 1, b^{-1}ab = a^{1+n} \rangle, \ n \geq 2,$$

$$K(n, \ l) = \langle a, b | ab^n = b^l a, \ ba^n = a^l b \rangle, \ where \ (n, l) = 1.$$

In Section 2 we state some results about our considered finitely presented groups and in Section 3 we solve the equation $xy \equiv zu (mod \ n)$, which is needed in next section. Section 4 is devoted to the commutativity degree of groups of nilpotency class 2. In this process, we first give an explicit formula for commutativity degree of $G_{mn}$, $H_n$ and $K(n, \ l)$ and using these results, we reach to our goal.

Most of results in Section 3 were suggested by data from a computer program written in the computational algebra system GAP [6].

## 2. Preliminaries

This section is devoted to explain some results concerned with $G_{mn}$, $H_n$ and $K(n, \ l)$. First, we state a lemma without proof that establishes some properties of groups of nilpotency class 2.

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

(i) $[uv, w] = [u, w][v, w]$ and $[u, vw] = [u, v][u, w]$.

(ii) $[u^k, v] = [u, v^k] = [u, v]^k$.

(iii) $(uv)^k = u^k v^k [v, u]^{k(k-1)/2}$.

(iv) If $G = \langle a, b \rangle$ then $G' = \langle [a, b] \rangle$.

The following lemmas can be seen in [3]:

**Lemma 2.2.** Let $d = g.c.d(m, n)$, then we have

(i) every element of $G_{mn}$ may be uniquely represented by $a^i b^j [a, b]^k$, where $0 \leq i \leq m-1$, $0 \leq j \leq n-1$ and $0 \leq k \leq d-1$.

(ii) $|G_{mn}| = mnd$.

**Lemma 2.3.** (i) Every element of $H_n$ may be uniquely represented by $b^j a^i$, where $0 \leq i \leq n^2 - 1$ and $0 \leq j \leq n - 1$.

(ii) $|H_n| = n^3$.

Now, we state some known results concerning $K(n, l)$, the proofs of which can be found in [1, 2].

**Theorem 2.4.** The groups $K(n, l)$ have the following properties:

(i) $|K(n, l)| = |l - n|^3$, if $(l, n) = 1$ and is infinite otherwise;

(ii) if $(l, n) = 1$, then $|a| = |b| = (l - n)^2$;

(iii) if $(n, l) = 1$, then $a^{l-n} = b^{n-l}$.

**Lemma 2.5.** (i) For every $m \geq 3$, $K(n, l) \cong K(1, 2 - l)$.

(ii) For every $i \geq 2$ and $(n, i) = 1$, $K(n, n + i) \cong K(1, i + 1)$.

**Note:** If $(l, n) = 1$, then $K(n, l) \cong K(1, l - n + 1)$, which we may write as $K_{l-n+1}$. Hence we only calculate $d(K_m)$.

**Lemma 2.6.** Every element of $K_m$ may be uniquely presented by $x = a^{\beta} b^{\gamma} a^{(m-1)\delta}$, where $1 \leq \beta,\ \gamma,\ \delta \leq m - 1$.

**Proof.** By parts (ii) and (iii) of Theorem 2.4, every element of $K_m$ can be written in this form. Since $|K_m| = |m - 1|^3$, that expression is unique. □

**Lemma 2.7.** In $K_m$, $[a,b]=b^{m-1}\in Z(K_m)$.

**Proof.** Since $a^{m-1}=b^{1-m}$ then $a^{m-1}\in Z(K_m)$. By the relations of $K_m$ we have

$$[a,b]=a^{-1}b^{-1}ab=a^{-1}b^{-1}b^m a=a^{-1}b^{m-1}a=b^{m-1}\in Z(K_m),$$

as desired. □

## 3. Solving the equation $xy\equiv zu(mod\ n)$

In this section we will solve $xy\equiv zu(mod\ n)$ , $n\geq 2$ where $x,y,z$ and $u$ are variables. For this, let $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$. Then $(r_1,s_1,r_2,s_2)$ is a solution of this equation if and only if for every $i$, $(1\leq i\leq k)$, $(r_1,s_1,r_2,s_2)$ is a solution of the following equations;

$$xy\equiv zu(mod\ p_i^{\alpha_i}).$$

By the above argument, we solve the equation

$$xy\equiv zu(mod\ p^{\beta}). \qquad (1)$$

If $(y,p)=1$, then for every $z$, $u$ when $1\leq z,u\leq p^{\beta}$, we have $x\equiv y^*zu\ (mod\ p^{\beta})$ is a solution, where $y^*$ is the arithmetic inverse of $y$ respect to $p$. The following lemma is crucial for the rest of the paper.

**Lemma 3.1.** For the integer $\alpha$, $(0\leq\alpha\leq\beta)$ and variables $x$, $i$ and $j$, the number of solutions of the equation $p^{\alpha}x\equiv ij\ (mod\ p^{\beta})$ is $p^{2\beta-1}((\alpha+1)p-\alpha)$.

**Proof.** Clearly, for $1 \leq i, j \leq p^\beta$ the equation $p^\alpha x \equiv ij \ (mod\, p^\beta)$ has solution if and only if $p^\alpha | ij$. For $0 \leq t < \beta$, let $D_{p^t} = \{(i,j)|\ 1 \leq i, j \leq p^\beta,\ p^t|\ ij\}$, then $D_{p^{t+1}} = D_{p^t} - M$, where

$$M = \{(i,j) \in D_{p^t}|\ g.c.d(p^{t+1},\ ij) = p^t\}.$$

First, we calculate $|M|$. We have $M = \{(i,j) \in D_{p^t}|\ \exists\ s \in \{0, 1, ..., t\}$ *such that* $i = p^s k_1,\ j = p^{t-s} k_2$ *and* $(k_1, p) = (k_2, p) = 1\}$. Hence

$$|M| = \sum_{s=0}^{t} \phi(p^{\beta-s})\phi(p^{\beta-t+s}) = \sum_{s=0}^{t} (p-1)^2 p^{\beta-s-1} p^{\beta-t+s-1}$$

$$= \sum_{s=0}^{t} (p-1)^2 p^{2\beta-t-2} = (t+1)(p-1)^2 p^{2\beta-t-2}.$$

Now by induction on $t$, we obtain that $|D_{p^\alpha}| = p^{2\beta-\alpha-1}((\alpha+1)p-\alpha)$.

Finally, the number of solutions of the equation $p^\alpha x \equiv ij \ (mod\, p^\beta)$ is

$$p^\alpha p^{2\beta-\alpha-1}((\alpha+1)p-\alpha) = p^{2\beta-1}((\alpha+1)p-\alpha).$$

Thus the assertion holds. □

**Proposition 3.2.** For the integer $\beta$ and variables $x$, $y$, $i$ and $j$, the number of solutions of the equation $xy \equiv ij \ (mod\ p^\beta)$ is $p^{2\beta-1}(p^{\beta+1} + p^\beta - 1)$.

**Proof.** By Lemma 2.1, the number of solutions of $xy \equiv ij \ (mod\, p^\beta)$ is

$$\sum_{\alpha=0}^{\beta} \phi(p^{\beta-\alpha}) p^{2\beta-1}((\alpha+1)p-\alpha).$$

To complete the proof, we have

$$\sum_{\alpha=0}^{\beta} \phi(p^{\beta-\alpha})p^{2\beta-1}((\alpha+1)p-\alpha)$$

$$= p^{2\beta-1}((\beta+1)p-\beta) + p^{3\beta-2}(p-1)\sum_{\alpha=0}^{\beta-1}\frac{(\alpha+1)p-\alpha}{p^\alpha}$$

$$= p^{2\beta-1}((\beta+1)p-\beta) + p^{3\beta-2}(p-1)(p+2\sum_{t=0}^{\beta-1}\frac{1}{p^t} - \frac{\beta+1}{p^{\beta-1}})$$

$$= p^{3\beta} - p^{3\beta-1} + 2p^{2\beta-1}(p-1)\frac{p^\beta-1}{p-1} + p^{2\beta-1}$$

$$= p^{2\beta-1}(p^{\beta+1}+p^\beta-1).$$

The proposition is proved. □

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

**Corollary 3.3.** For the integer $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ and variables $x$, $y$, $i$ and $j$, the number of solutions of the equation $xy \equiv ij \ (mod\ n)$ is $\prod_{i=1}^k p_i^{2\alpha_i-1}(p_i^{\alpha_i+1}+p_i^{\alpha_i}-1)$.

**Corollary 3.4.** Let $m$, $n$ be integers and $x$, $y$, $i$ and $j$, be variables when $0 \le x, i < n$ and $0 \le y, j < m$. Then, the number of solutions of the equation $xy \equiv ij \ (mod\ d)$ 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 $d = g.c.d(m,n) = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$.

## 4. Results and Conclusion

In this section, first we calculate the commutativity degree of $G_{mn}$, $H_n$ and $K(m)$. Then using these results and Lemmas 1.1, 1.2, we give a lower bound for the commutativity degree of groups of nilpotency class 2.

**Proposition 4.1.** For every integers $m,\ n \geq 2$,

(i) if $G = G_{mn}$ and $d = g.c.d(m,n) = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, then

$$d(G) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} + p_i^{\alpha_i} - 1}{p_i^{2\alpha_i+1}};$$

(ii) if $G = H_n$ and $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, then

$$d(G) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} + p_i^{\alpha_i} - 1}{p_i^{2\alpha_i+1}};$$

(iii) if $G = K_m$ and $m - 1 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, then

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

**Proof.** Let $A = |\{(x,y)|x, y \in G,\ xy = yx\}|$. To prove (i), let $d = g.c.d(m,n)$. Then by Lemma 2.2, every element $x$ of $G_{mn}$ may be represented as $x = a^i b^j [b,a]^k$, where $i \in \{0,1,...,m-1\}$, $j \in \{0,1,...,n-1\}$ and $k \in \{0,1,...,d-1\}$. For every $x = a^{r_1} b^{s_1} [b,a]^{k_1}$ and $y = a^{r_2} b^{s_2} [b,a]^{k_2}$ of $G$, if $xy = yx$ then

$$a^{r_1} b^{s_1} [b,a]^{k_1} a^{r_2} b^{s_2} [b,a]^{k_2} = a^{r_2} b^{s_2} [b,a]^{k_2} a^{r_1} b^{s_1} [b,a]^{k_1}$$

Since $G' = \langle [b,a] \rangle \subseteq Z(G)$, by Lemma 2.1, we get $[b,a]^{r_2 s_1 - s_2 r_1} = e$. Furthermore, $|G'| = d$, hence $r_2 s_1 \equiv s_2 r_1 (mod\ d)$. Also each of the integers $k_1$ and $k_2$ take $d$ possible values, then by Corollary 3.4 we have $A = m^2(\frac{n}{d})^2 \prod_{i=1}^{k} p_i^{2\alpha_i - 1}(p_i^{\alpha_i+1} + p_i^{\alpha_i} - 1)$. Now, the result follows from the definition of $d(G)$ and Lemma 2.2.(ii).

To prove the second part of the proposition, we note that by part (i) of Lemma 2.3, $xy = yx$ if and only if

$$a^{r_1}b^{s_1}a^{r_2}b^{s_2} = a^{r_2}b^{s_2}a^{r_1}b^{s_1}.$$

So by using the Lemma 2.1 we get $[b,a]^{r_2 s_1 - s_2 r_1} = e$. Also $[b,a] = a^m$, so that $r_2 s_1 \equiv s_2 r_1 (mod\ m)$ and by the Corollary 3.4, $A = m^2 \prod_{i=1}^{k} p_i^{2\alpha_i-1}(p_i^{\alpha_i+1} + p_i^{\alpha_i} - 1)$. Then by the definition of $d(G)$ and part (ii) of Lemma 2.3, we get the required result as

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

Part (iii) may be achieved by using the Lemma 2.6 in almost a similar way as above. □

The following corollary is now a result of part (iv) of Lemma 2.1 and the proof of Proposition 4.1.

**Corollary 4.2.** Let $G = G_{mn}$, $H_n$ or $K(m)$ and $l = |G'|$. Then

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

where $l = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$.

We are now in a position to find a lower bound for the commutativity degree of two generator groups of nilpotency class two.

Let G be a 2-generated finite group of nilpotency class 2. Then $G \cong \langle a, b | R \rangle$, where $\{a^m,\ b^n,\ [a,b]^a[b,a],\ [a,b]^b[b,a]\} \subseteq R$, for some $m,\ n \geq 2$.

**Corollary 4.3.** By the above notations, we have

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

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

**Proof.** By Lemma 1.1, we get $G \cong \frac{G_{mn}}{N}$ for some normal subgroups $N$ of $G_{mn}$ and integers $m,\ n \geq 2$. Then the result follows from Lemma 1.2 and the fact that $d(N) \leq 1$. □

# References


[1] C. M. Campbell, P. P. Campel, H. Doostie and E. F. Robertson, Fibonacci length for Metacyclic Groups, Algebra Colloq., (2004), 215-222.

[2] C. M. Campbell, E. F. Robertson, On a group presentation due to Fox, Canada. Math. Bull. 19 (1976) 247-248.

[3] H. Doostie and M. Hashemi, Fibonacci lenghts involving the Wall number **k(n)**, J. Appl. Math. Computing, Vol. 20 (2006), No. 1-2, 171-1800.

[4] H. Doostie and M. Maghasedi, Certain classes of groups with commutativity degree $d(G) \leq \frac{1}{2}$, Ars. Combinatoria 89(2008). pp. 263-270.

[5] W. H. Gustafson, What is the propability that two group elements commute? Amer Math. Monthly. 80(1973). 1031-1034.

[6] The GAP Group, GAPGroups, Algorithms, and programming version 4.4 packages AutPGroup and Small Groups http. A. R.

[7] D. L. Johnson, Presentations of groups, 2nd edition London Math. Soc. Student Texts 15, Cambridge University Press, Cambridge, (1997).

[8] P. Lescot, Isoclinsm classes and commutativity degrees of finite groups, J. of Algebra 177 (1995), 847-869.

[9] M. R. R. Moghaddam, A. R. Salemkar and K. Chiti, n-isoclinism classes and n-nilpotency degree of finite groups, Algebra Colloquium, 12.2(2005), 255-261.