The Co-Prime Probability of p-Groups

Norarida Abd Rhani [1]*, Nor Muhainiah Mohd Ali [2], Nor Haniza Sarmin [3] and Ahmad Erfanian [4]

[1]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Kelantan, Bukit Ilmu, Machang, Kelantan, Malaysia
norarida@uitm.edu.my
[2,3]Department of Mathematical Sciences, Faculty of Science,Universiti Teknologi Malaysia, Johor Bahru, Malaysia
normuhainiah@utm.my, nhs@utm.my
[4]Department of Pure Mathematics, Faculty of Mathematical Sciences, Ferdowsi University of Mashhad, Mashhad, Iran
erfanian@um.ac.ir
*Corresponding author

Abstract: The commutativity degree of G can be used to measure how close a group is to be abelian. This concept has been extended to the probability that two random integers are co-prime. Two integers s and t are said to be co-prime if their greatest common divisor is equal to one. This concept has been further extended to the co-prime probability of G, where the probability of the order of a random pair of elements in the group are co-prime. In this paper, the co-prime probability for all p-groups, where p is prime number is determined.

Keywords: Commutativity degree, Co-prime probability, Finite group, p-Groups

1   Introduction

The commutativity degree of a group G, denoted as $P(G)$, is the probability that two random elements in G commute. In late 60s, Erdos and Turan [1], applied the concept of commutativity degree for symmetric groups. Then, Erfanian *et al.* [2] introduced the relative commutativity degree of G where they define this probability as the probability for an element of a subgroup H and element of a group G commute with one another, denoted and gave several bounds for it.

Furthermore, Bureaux and Enriquez [3] introduced the concept of $P(G)$ to the probability that two random integers are co-prime. Two integers s and t are said to be prime to one another or co-prime if their greatest common divisor is equal to one, i.e, $(s,t)=1$. The numbers $s,t,u,...,k$ are said to be co-prime if every two of them are co-prime. For $(s,t,u,...,k)=1$, which means that there is no number except 1 which divides all of $s,t,u,...,k$. In 2008, Hardy and Wright [4] established the result in number theory that (Theorem 332)

$$\lim_{n\to\infty}\frac{\left|\left\{(s,t)\in[n]^2,\gcd(s,t)=1\right\}\right|}{n^2}=\frac{6}{\pi^2}.$$

where $[n]=\{1, 2, ..., n\}$. They concluded that n positive integers chosen arbitrarily and independently are co-prime is $\frac{6}{\pi^2}\approx 0.608$.

In this paper, the co-prime probability is introduced. This concept is defined as the probability of the order of two random elements in the group are relatively prime, denoted as $P_{copr}(G)$. Furthermore, by using the definition of the co-prime probability of a group, this probability is determined for p-groups, where p is prime number.

Hence, this paper consists of three parts where the first part provides some basic ideas on the commutativity degree and its extensions. The second part states some basic concepts, which are related

to the commutativity degree, as well as to the co-prime probability of a group. The main results are presented in the third part.

2   Preliminaries

The definitions of the dihedral groups, the quaternion group and a p-group, where p is a prime number together with formal definitions of the commutativity degree and its generalization are provided in this section.

Definition 1 [5] The Dihedral Group

For $n \geq 3$, the n-th dihedral group is defined as a group consists of rigid motions of a regular n-gon, denoted by D_n. The dihedral groups, D_n of order $2n$ can be presented in a form of generators and relations given as follows:

$$D_n = \left\langle a, b : a^n = b^2 = e, ba = a^{-1}b \right\rangle.$$

Definition 2 [5] The Quaternion Group

The quaternion group, Q_8, is defined by

$$Q_8 = \left\{ 1, -1, i, -i, j, -j, k, -k \right\}$$

Definition 3 [6] A p-Group

A group G is a p-group if and only if the order of G is a power of p, where p is a prime number.

Definition 4 [1] The Commutativity Degree of a Group

Suppose that s and t are two random elements of a group G. The commutativity degree of a group is given as follows:

$$P(G) = \frac{\left| (s,t) \in G \times G : st = ts \right|}{\left| G \right|^2}.$$

3   Results and Discussion

The co-prime probability of G is determined for p-groups. This probability is defined as the probability of the order of two random elements in the group are co-prime.

Definition 5 The Co-Prime Probability of a Group

The co-prime probability of a group G, denoted as $P_{copr}(G)$, is defined as:

$$P_{copr}(G) = \frac{\left|\{(s,t) \in G \times G : (|s|,|t|) = 1\}\right|}{|G|^2}.$$

The following proposition provides the co-prime probability of *p*-groups.

Proposition 1

Let *G* be a finite *p*-group of order p^n, where $n \geq 1$. Then $P_{copr}(G) = \frac{2p^n - 1}{p^{2n}}$.

Proof

Suppose *G* is a *p*-group where *p* is a prime number. Thus $|G| = p^n$, $n \geq 1$. Let $s, t \in G$.

Case 1: If $s = e$, then *e* is co-prime to all elements *t* in *G*, since $(|e|,|t|=1)$. Let $B = \{(e,t) \in G \times G\}$. Then, the total pair of elements *s* and *t* that are relatively prime is $|B| = |G| = p^n$.

Case 2: If $t = e$, then all elements in $s \in G$ are co-prime with *t*, since $(|s|,|e|=1)$. Let $B = \{(s,e) \in G \times G : s \neq e\}$. Then the total pair of elements *s* and *t* that are relatively prime is $|B| = |G| - |\{e\}| = p^n - 1$.

Case 3: If *s* and *t* are two non-identity elements of *G*, then $|s| = p^v$, where $1 \leq v \leq n$ and $|t| = p^w$, where $1 \leq w \leq n$. Thus $(|s|,|t|) \geq p^r$, where $1 \leq r \leq n$ which implies $(|s|,|t|) \neq 1$. Hence *s* and *t* are not co-prime.

Let $A = \{(s,t) \in G \times G \mid (|s|,|t|) = 1\}$. By considering all cases, $A = B \cup C$. Then, the number of possible pairs of *s* and *t* that are relatively prime in *G* is $|A| = |B| + |C|$. Thus, $|A| = p^n + p^n - 1 = 2p^n - 1$. By Definition 5, $P_{copr}(G) = \frac{\left|\{(s,t) \in G \times G : (|s|,|t|) = 1\}\right|}{|G|^2} = \frac{|A|}{|G|^2} = \frac{2p^n - 1}{(p^n)^2} = \frac{2p^n - 1}{p^{2n}}.$ □

To illustrate Proposition 1, the following examples can be considered.

Example 1

Suppose D_8 is the dihedral group of order 16 or 2^4, i.e, $D_8 = \langle a,b : a^8 = b^2 = e, ba = a^{-7}b \rangle$. In D_8, there are $|e| = 1$, $|a| = |a^3| = |a^5| = |a^7| = 8, |a^2| = |a^6| = 4, |a^4| = 2$ and $|b| = |ab| = |a^2b| = |a^3b| = |a^4b| = |a^5b| = |a^7b| = 2$. Firstly, the value of the co-prime probability of D_8 is computed by using Definition 5. If $s = e$,

and $t \in D_8$, then s and t are co-prime. If $t = e,$ and $s \in D_8 \setminus \{e\}$, then s and t are also co-prime. Otherwise, s and t are not co-prime. Hence, $P_{copr}(D_8) = \dfrac{31}{256}$.

Next, the value of co-prime probability of D_8 is computed by using the formula. Thus, by Proposition 1, $P_{copr}(G) = \dfrac{2p^n - 1}{p^{2n}}$ which implies $P_{copr}(D_8) = \dfrac{2(2)^4 - 1}{(2^4)^2} = \dfrac{31}{256}$, the similar result.

4   Conclusion

In this paper, the co-prime probability is introduced. The co-prime probability of G has been found for p-groups. It has been found that for p-groups, the co-prime probability is equal to $\dfrac{2p^n - 1}{p^{2n}}$.

References

[1] Erdos, P. and Turan, P. On Some Problems of a Statistical Group Theory. IV. Acta Mathematica Hungarica. 1968. 19: 413-435.
[2] Erfanian, A., Rezaei, R. and Lescot, P. On The Relative Commutativity Degree of a Subgroup of a Finite Group. Communications in Algebra. 2007. 35(12): 4183-4197.
[3] Bureaux, J. and Enriquez, N. The Probability that Two Random Integers are Co-Prime. arXiv:1612.03700v1 [math.PR] 12 Dec 2016, 1-4, 2016.
[4] Hardy, G. H. and Wright, E. M. An Introduction to the Theory of Numbers. 4th ed. Oxford University Press. 2018.
[5] Dummit, D. S. and Foote, R.M. Abstract Algebra. USA: John Wiley and Son. 2004.
[6] Judson, T. W. Abstract Algebra: Theory and Application. Ann Arbor, Michigan: Orthogonal Publishing L3C. 2015.