IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 17, Issue 4 Ser. II (Jul. – Aug. 2021), PP 53-59
www.iosrjournals.org

The Commutativity Degree of Finite Groups via Class Equation

Jelten, B. Naphtali[1*], V. K. Joshua [2], Hassan S. Bade[3]
1. Department of Mathematics, University of Jos, P.M.B. 2084, Plateau State, Nigeria
2. Department of Mathematics, University of Jos, P.M.B. 2084, Plateau State, Nigeria
3. Department of Mathematics Federal College of Education, Yola, P. M. B. 2042 Adamawa State, Nigeria
**E-mail of the corresponding author: jeltenn2012@gmail.com*

The concept of commutativity degree for finite groups is an aspect of abstract algebra that places the subject on a numerical scale. Cody, C (2010) has determined the maximum size of the centre of finite groups while Anna, C (2010) obtained the equivalent in terms of commutativity degree. In this paper we obtained the commutativity degrees of finite groups of order less that one hundred where the groups have orders of the form $|G| = p^a q^b$, $a > b$ *using the conjugacy classes via the class equation as instruments where* p *is an even prime while* q *is an odd prime such that* $q < 10$, $2 < a \leq 6$ *and* $0 \leq b \leq 2$ ..

Key words: Group; Commutativity; Centre; Conjugacy class; Prime

---

Date of Submission: 07-08-2021 Date of Acceptance: 21-08-2021

I. Introduction

1.1 Definition

A group is a non-empty set G on which is defined a rule for combining two elements a,b $\in$ G such that the following axioms are satisfied for all a,b$\in$ G:

1. ab$\in$ G
2. a (b c) = (ab) c
3. these exists an element e $\in$ G called the identity element in G such that ae = a = ea
4. there exists an element $a^{-1} \in$ G called the inverse element of G such that:
   $aa^{-1} = e = a^{-1} a$.

A set G which satisfies axiom 1 only is called a groupoid. If G satisfies axiom 2 it is called a semi group. A semi group which satisfies 3 is said to be a monoid.

1.2 Definition

A group *G* with the property that *ab = ba* for some pair of elements *a,b*$\in$ *G* is said to be a commutative group. A group in which there exist a pair of elements *a, b* $\in$ *G* endowed with the property that $ab \neq ba$ is called a non - commutative group.

1.3 Definition

Let *G* be a group and $H < G$. For $q \in G$ the subset $Hq = \{hq : h \in H\}$ of *G* is called a right coset of *H* in *G*. Distinct right cosets of *H* in *G* form a partition of *G*. That is every element of *G* is precisely in one of them. Left coset is similarly defined. If *G* is commutative we just talk of coset of *H*. The number of distinct right cosets of *H* in *G* is called the index of *H* in *G* denoted by $|G : H|$ If *G* is finite so is *H* and *G* is partitioned into |*G:H*| cosets each of order |*H*| and we write:

$$|G| = |G : H||H|$$

and note that |*H*| and |*G:H*| divide |*G*|.

The next definition, decomposes a group into smaller groups and we give an analogous definition of subsets in groups.

1.4 Definition

A non - empty subset *N* of a group *G* is said to be a subgroup of *G* written $N \leq G$, if *N* is a group under the operation inherited from *G*. If $N \neq G$, then *N* is said to be a proper subgroup of *G*.

A subgroup *N* of *G* such that every left coset is a right coset and vice versa is called a normal subgroup of *G*. That is $Nx = xN$ or $x^{-1}Nx \leq N$ and we write $N \lhd G$. A normal subgroup is characterized by the fact that it does

not possess any conjugate subgroup apart from itself. That is $aH = Ha$ or $a^{-1}Ha = H$ for all a in G. If G is commutative then every subgroup of G is commutative
Next we count the number of element in groups

1.5 Definition

The number of elements in a group G denoted by $|G|$ is called the order of the group. If G is finite of order n we have $|G| = n$ otherwise $|G| = \infty$ if G has infinite order.
The least number n if it exists such that $a^n = 1$for a in G is called the order of a and we write $o(a) = n$. That is $o(a) = \min\{a > 0: a^n = 1\}$. If no such n exists then $o(a) = \infty$. In the latter we say that powers of a are distinct but not all are distinct in the former..

1.6 Lemma

Any group of even order contains an element of order 2. That is for $g \in G$ with $g \neq 1$ then $g^2 = 1$. In fact there is an odd number of such elements which are called involutions.

A consequence of the decomposition, in 1.3 naturally leads to an important theorem in this paper: The Lagrange's Theorem which is next.

1.7 Theorem

If G is a finite group and H is a subgroup of G then the order of H divides the order of G.

Proof

By 1.2 we have that the right cosets of H form a partition of G. Thus each element of G belongs to at least one right coset of H in G and no element can belong to two distinct right cosets of H in G. Therefore every element of G belongs to exactly one right coset of H. Moreover each right coset of H in G contains |H| elements. Therefore if the number of right cosets of H in G is n, then $|G| = n|H|$. Hence the order of H divides the order of G.

1.8 Remark

Lagrange's Theorem greatly simplifies the problem of determining all the subgroups of a finite group. The converse of theorem 1.6 is not true in general except for groups of prime order power.

1.9 Definition

Let a, $q \in G$. Then a is conjugate to q in G if there exist an element $g \in G$ such that $q=g^{-1}ag$. The set of all elements of G that are conjugate to a in G is called the conjugacy class of a in G which we denote by C(a). And as such:

$$C(a) = \{g^{-1} ag : g \in G\}$$

Its to be noted that C(a) is a subgroup of G and by 1.6 its order divides that of G. Subgroups belonging to the same conjugacy class are conjugates. Such subgroups are isomorphic. The reverse does not hold in general as we have in the case of abelian groups where two isomorphic subgroups may not be conjugates. However conjugate elements lie in the same conjugacy class and have the same order.

1.10 Definition

The centre Z(G) of a group G is the set of all elements z in G that commute with every element q in G. We write:

$$Z(G)=\{z \in G : zq=qz, \text{ for all } q \in G\}$$

Z(G) is a commutative normal subgroup of G and G modulo its centre Z(G) is isomorphic to the inner automorphism, inn(G) of G. If $Z(G) = \{1\}$ where 1 is the identity element of G, then G is said to have a trivial centre . The centre of a group G is its subgroup of largest order that commute with every element in the group. The divisors of |G| reveal a lot about the order of Z(G) and the conjugacy classes of G. If N is a normal subgroup of G such that $|N|=2$, then $N \subseteq Z(G)$.

We have the properties of the subgroups of the centre of the group G from Louis (1975) as follows .

1.11 Proposition

If H is a subgroup of Z(G), the centre of the group G, then H is a normal subgroup of G. In particular Z(G) is normal in G.

Next we define an important concept and relate it to the conjugacy class.

1.12 Definition

The centralizer $C_G(q)$ of an element q in G is the set of all elements $g \in G$ that commute with q. That is:

$$C_G(q) = \{g \in G : gq=qg, \text{ for some } q \in G\}.$$

This is a subgroup of G but not a normal subgroup in general. However, the index of $C_G(q)$ in G is the size of the conjugacy class C(q) of q in G. That is

$$|C(q)|=|G:C_G(q)|.$$

Consequently the quotient of G by $C_G(q)$ is not a group In particular |C(q)| divides |G|. If $q \in Z(G)$ then $|C(q)|=1$ and $q^{-1}gq=q$. in this case $C_G(q) = G$.

What follows is a corollary from James and Martin (2001)

1.13 Corollary

If G is a finite group, then:

(i) every group is a union of its conjugacy classes and distinct conjugacy classes are disjoint;

(ii) conjugacy class is an equivalence relation where the equivalence classes are the conjugacy classes.

The next lemma relates the centre of G to the centralizer of the elements of G is:

1.14 Lemma

The centre Z(G) of a group G is the intersection of the centralizers $C_G(a)$ of elements a in G.

Herstein (1964) has it that if G is a finite group then the number of elements conjugate to a in G is the index of the normalizer of a in G.

1.15 Remark

Let G be a group and h, g be elements of G. If the conjugacy classes of g and h overlap then the conjugacy classes are equal. The number of distinct or non-equivalent conjugacy classes is called the class number of the group G. In the symmetric group on n objects, each conjugacy class belongs to exactly one partition of n. The number of such conjugacy classes is equal to the number of integer partitions of n. The conjugacy classes of a group are disjoint and hence we recover G from their union, from 1.13.

The next theorem presents the class equation for finite groups whose proof follows readily from 1.12

1.16 Theorem

Let G be a finite group then

$$|G| = \sum|G: C_G(q_i)| \quad \text{(i)},$$

where the sum runs over the elements from each conjugacy class of G.

We note that from 1.13, equation (i) becomes

$$|G|= |Z(G)| + \sum|G: C_G(q_i)| \quad \text{(ii)}$$

Here the sum in (ii) runs over q_i from each conjugacy class such that q_i is not an element of Z(G). equation (ii) above we have:

$$|G|=|Z(G)| + \sum|C(q_i)| \quad \text{(iii)}$$

1.17 Remark

In the abelian environment, the sum in equation (iii) of 1.18 is zero. Consequently, the class equation is relevant only when we are in the non abelian environment. The fact that each element of Z(G) forms a conjugacy class containing just itself gives rise to the class equation.

Just as there are only n finite number of groups up to isomorphism with a given size, we also have that there is a finite number of groups up to isomorphism with a given number of conjgacy classes. Hence we have:

1.18 Lemma

Let G be a group of order p^n, with $n \geq 1$ then: If $\{1\} \neq H \triangleleft G$, we have that $H \cap Z(G) \neq \{1\}$. In particular $Z(G) \neq \{1\}$;

Proof

Since $|G| = p^n$, $H \triangleleft G$. From 1.6 we have that |H| divides the order of G. This implies that $|H|$ is a power of p. Furthermore, $Z(G) \leq G$ and given that $Z(G) \neq \{1\}$, we have that p divides the order of G. Now p also divides the orders of H and $Z(G)$. Therefore $H \cap Z(G) \neq \{1\}$ and $Z(G) \neq \{1\}$.

James and Martin (2001) proved the next Lemma.

1.19 Lemma

Let G be a group of order p^n with $1 \leq i \leq 4$. Then G contains an abelian subgroup of index p.

Mark (2011) proves the next theorem.

1.20 Theorem

If a finite group G has a centre Z(G) and G/Z(G) is cyclic then G is abelian.

From 1.7 we have:

1.21 Corollary
The order of an element a in G divides the order of G since <a> is a subgroup of G generated by a.

Houshang and Hamid (2009) hence the proposition that follows which is a consequence of 1.16

1.22 Proposition
If the order of a finite group G is a power of a prime p then G has a non trivial centre. Equivalently the centre of a p - group contain more than one element.

Proof
Let G be the union between its centre and the conjugacy classes say J_i of size greater than 1.
Then from equation (iii) of 1.18

$$|G|=|Z(G)|+\sum|C(J_i)|$$

Each conjugacy class J_i has size of a power w say of prime p such that $w \geq 1$. In this case $w = 0$ for the conjugacy classes whose elements are central elements. Since each conjugacy class J_i has size a power of p then $|J_i|$ is divisible by p. Furthermore as p divides |G|, it follows that p also divides |Z(G)|. Accordingly Z(G) is non-trivial.
Observe that from 1.22 there are elements of G other than the identity that commute with every element of G.
What follow is an important theorem as in Cody (2010) and Jelten and Momoh (2014)

1.23 Theorem
If G is a finite non abelian group, then the maximum possible order of the centre of G is ¼|G|.That is, $|Z(G)| \leq 1/4|G|$.

Proof
Let $z \in Z(G)$. Since G is non abelian, $Z(G) \neq G$. Thus there exist an element $q \in G$ such that q is not in the centre. This imply that $C_G(q) \neq G$ and $C_G(q) \neq Z(G)$. Since $z \in Z(G)$ every element in G commute with z, so qz = zq. It follows that $z \in C_G(q)$. As $q \in C_G(q)$, we have that Z(G) is a proper subset of $C_G(q)$. Since a group that is a subset of a subgroup under the same operation is itself a subgroup of the subgroup, we find that Z(G) is a proper subgroup of $C_G(q)$. By 1.6 and Jelten, N. B (2015), it follows that:

$$|Z(G)| \leq 1/2|C_G(q)|.$$

Now, since we assumed $C_G(q) \neq G$, then $C_G(q)$ is a proper subset of G. Therefore by 1.6 and the fact that the centralizer of any group element is a subgroup of G, we find that $|C_G(q)| \leq 1/2|G|$.That is:

$$\begin{aligned} |Z(G)| &\leq 1/2|C_G(q)| \\ &\leq 1/2(1/2|G|) \\ &= 1/4|G|. \end{aligned}$$

We relate the centralizer of an element to the size of a finite non abelian group G proved by Cody, C. (2010)

1.24 Lemma
Let G be a finite non abelian group and $t \in G$ such that $t \notin Z(G)$, then:

$C_G(t) = |G|/2$.

1.25 Remark
In a commutative group, Z(G) = G, $C_G(t) = G$ for all t in G. But, $C_G(t) < G$ if G is non abelian. In which case $Z(G) < G$. The number of the centralizers that are equal to G is |Z(G)|.
From Jelten, N and Apine, E (2015) we have the next two theorems

1.26 Theorem
Let G be a finite nonabelian group whose order is p^r with centre of order p^n. Let the order of the centralizer of an element x be p^m where m, n and r are positive integers such that $n \leq m$ $n < r$ and $m < r$, then $|C| = \frac{1}{4}(2p^w + p^r)$, where |C| the number of conjugacy classes.

Proof
From the class equation we have

$$|G| = |Z(G)| + \sum_{i=1+|Z(G)|}^{|C|-|Z(G)|} |G : C_G(x_i)|, \quad x \notin Z(G) \quad \text{with } |C(x)| \geq 2.$$

So that $|G| \geq |Z(G)| + 2(|C| - |Z(G)|)$

$$|G| \geq \frac{1}{2}C_G(x) + 2|C| - 2|Z(G)|$$

$$|G| \geq \frac{1}{2}C_G(x) + 2|C| - |C_G(x)|$$

$$2|G| \geq C_G(x) + 4|C| - 2|C_G(x)|$$

$$2p^w + p^r \geq 4|C|$$

$$\frac{2p^w + p^r}{4} \geq |C|$$

$$\frac{1}{4}(2p^w + p^r) \geq |C| \text{ as required}$$

1.27 Theorem

Given that a finite group G is of prime power order with centre Z(G), then we count the number of conjugacy classes from the centralizer as follows: $|C| \leq \frac{1}{4}(3|G| - |C_G(x)|)$.

$$|G| = |Z(G)| + \sum_{i=1+|Z(G)|}^{|C|-|Z(G)|} |G : C_G(x_i)|, \quad x \notin Z(G) \quad \text{with } |C(x)| \geq 2, \text{ from 1.24}$$

So that $|G| \geq |Z(G)| + 2(|C| - |Z(G)|)$

$$|G| \geq \frac{1}{2}C_G(x) + 2|C| - 2|Z(G)|$$

$$|G| \geq \frac{1}{2}C_G(x) + 2|C| - \frac{1}{2}|G|$$

$$2|G| \geq C_G(x) + 4|C| - |G|$$

$$3|G| \geq C_G(x) + 4|C|$$

$$\frac{3|G| - |C_G(x)|}{4} \geq |C|$$

$$\frac{1}{4}(3|G| - |C_G(x)|) \geq |C|$$

That is $|C| \leq \frac{1}{4}(3|G| - |C_G(x)|)$

Anna, C (2010) has the next definition.

1.28 Definition

The commutativity degree of a finite group G is the probability p(G) that two elements of G chosen randomly commute.

The commutativity degree of a finite group G is the probability p(G) that two elements of G selected at random (with replacement) commute. That is:

p(G)={(x,y):xy=yx, for any x and y in G} and p(G)=|C|/|G|.

So commutativity is the outcome (x,y) for which xy = yx.

1.29 Remark

When two element x and y are randomly selected from a group G, the outcome (x, y) is called a commutativity and (x, y) = (y, x)

The set of all commutativities is the event 'randomly chosen x and y commute'. We denote this by c(G) defined as c(G)= {(x, y): xy = yx} with total outcome as G × G.

Commutativity degree of a group measures the extent to which the group is commutative.

The next theorem is credited to Anna, C, (2010) where commutativity degree is defined in terms of the size of the conjugacy class of the group followed by the proof.

1.30 Theorem

Let G be a finite group. Then the degree of commutativity p(G) of G is p(G) = |C|/|G|.

Proof

Let $\{C(h_i), 1 \leq i \leq |C|\}$ be the set of distinct conjugacy classes of G. As G is the union of disjoint conjugacy classes, then from remark*:

$$C(G) = \{(x,y) \in G \text{ X } G : xy = yx\}.$$

Where C(G) is the set of the commuting elements of G. So that for $x \in G$, $(x,y) \in Com(G)$ if and only if $y \in C_G(x)$ and we have :

$$|C(G)| = \sum|C_G(x)|, x \in G$$
$$= \sum|C(x_i)||C_G(x_i)|, \text{from definition } 1 \leq i \leq |C|,$$
$$= \sum|G:C_G(x_i)||\ C_G(x_i)|, \text{ definition 1.16 (ii)}$$
$$= \sum|G|$$
$$= |C||G|, \text{ since } 1 \leq i \leq |C|$$

Therefore:

$$P(G) = |C(G)|/|GXG|$$
$$= |C||G|/|GXG| = |C|/|G|.$$

Consequently, the commutativity degree of a finite group is the same as counting the number of conjugacy classes of G.

In the next theorem we obtain the maximum commutativity degree for a non abelian groups as in Anna, C (2010).

1.31 Theorem

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

Proof

From theorem 1.16

$$|G| = |Z(G)| + \sum|C(x_i)|, |Z(G)| + 1 \leq i \leq |C|; x_i \notin Z(G).$$
$$|G| \geq |Z(G)| + 2(|C| - |Z(G)|),$$

since for each i, $|C(x_i)| \geq 2$, from 1.24

Solving for |C| gives:

$$|C| \leq 1/2(|G| + |Z(G)|).$$

From theorem 3.1.6, $|Z(G)| \leq |G|/4$, therefore:

$$|C| \leq 1/2(|G| + |G|/4) = 5/8|G|.$$

And we have $P(G) = |C|/|G| \leq 5/8$.

OUR RESULTS

2.1 Theorem

Let G be a finite group of order $|G| = p^a q^b$, $a > b$, with $x, y \in G$, $xy \neq yx$. Then the commutativity degree of g is $p(G) = \dfrac{|z(G)| + 2}{2|G|}$, for $\min |z(G)|$ where $z(G)$ denotes the centre of G.

Proof

First we count the count the conjugacy classes $|c|$ in terms of the centre using the class equation.

$$|G| \geq |z(G)| + \sum_{|z(G)|+1}^{|c|-|z(G)|} |G : C_G(t)|, \quad C_G(t) \text{ is the centralizer of } t \text{ such that } t \in G \text{ but, from 1.16 } t \notin z(G)$$

and

$|C_G(t)| \geq 2$, then, $|G| \geq |z(G)| + 2(|C| - |z(G)|)$

$$|G| \geq |z(G)| + 2|C| - 2|z(G)|$$

$$|G| \geq 2|C| - |z(G)|$$

$$\frac{|G| + |z(G)|}{2} \geq |C|, \min |z(G)| \geq 2$$

That is $|C| \leq \frac{|G|+2}{2}$. Hence the commutativity degree is $p(G)$ is $p(G) = \frac{|z(G)|+2}{2|G|}$

2.2 Theorem

Let G be a finite group of order $|G| = p^a q^b$, $a > b$, with $x, y \in G$, $xy \neq yx$. Then the commutativity degree of g is $p(G) = \frac{5|z(G)|}{2|G|}$, for max $|z(G)|$ where $z(G)$ denotes the centre of G.

Proof

First we count the count the conjugacy classes $|c|$ in terms of the centre using the class equation.

$|G| \geq |z(G)| + \sum_{|z(G)|+1}^{|c|-|z(G)|} |G : C_G(t)|$, $C_G(t)$ is the centralizer of t such that $t \in G$ but $t \notin z(G)$ and

$|C_G(t)| \geq 2$, then, $|G| \geq |z(G)| + 2(|C| - |z(G)|)$

$|G| \geq |z(G)| + 2|C| - 2|z(G)|$

$|G| \geq 2|C| - |z(G)|$

from 1.23 this becomes $4|z(G)| \geq 2|C| - |z(G)|$. That is $5|z(G)| \geq 2|C|$ and we have:

$|C| \leq \frac{5|z(G)|}{2}$. Consequently the commutativity degree is $p(G) = \frac{5|z(G)|}{2|G|}$ for max $|z(G)|$

DISCUSSION

We use our results to determine the commutativity of groups of order $|G| < 100$, with the property that for $x, y \in G$, $xy \neq yx$. When the centre is at its minimum, we obtained the minimum commutativity of two groups with $0 < p \leq 3$, $q = 0$. When the centre is fixed at its maximum our results show that for $2 < a \leq 6$, $b = 0$, four groups satisfy the conditions while for $2 < a \leq 6$ with $0 < b \leq 2$, seven groups satisfy the conditions. So given the schemes in our results with max $|z(G)|$, we determine the maximum commutativity degrees of eleven groups in the range under consideration. We first count the conjugacy classes using the centre via the class equation and from there obtain the commutativity degrees.

II. Conclusion

Our results are simplified reduced to a single variable, the centre unlike in Anna (2010), Cody C (2010) and Jelten et al (2014). All that is required is the group cardinality, from which the centre cardinality can be determined and the commutativity using our results. The scheme we obtained work for large groups and the numerical results agree with those of Cody C (2010) and Anna C (2010).

References

[1]. Anna, C. (2010). Commutativity degree of finite groups. Unprinted Thesis: Wake Forest University , Winston – Salem, North Carolina.

[2]. Cody, C. . Commutativity in non abelian groups. www.whitman.edu/mathematics/ .../2010/seniorproject.codyclifton. 2010: Retrieved on 2/9/2012. 1-18.

[3]. Herstein, I. N.. Topics in Algebra. Massachusetts USA: Blaisdell Publishing Company. 1964

[4]. Houshang, B. and Hamid, M.. A note on p-groups of order $\leq p^4$. Proc. Indian Acad. Sci. (Math. Sci.), 2009: 119(2): 137-143.

[5]. Jelten, N.B. and Momoh, S.U.. Minimum and maximum number of irreducible representations of prime degree of non abelian group using the centre. Journal of Natural Sciences Research. 2014. 4(10):63 - 59.

[6]. Louis, S.. Introduction to abstract algebra. New York: McGraw – Hill Inc. 1975.

[7]. Mark, R.. Notes on group theory. https://www2,bc.edu/-/development-group- Theoryhtml,. 201.1 Retrieved on 9/9/ 2012: 4-9

[8]. Jelten and Elijah. Counting the conjugacy classes of finite groups from the centralizer.

[9]. International journal of mathematics and statistics invention. 2015: 3 (1): pp 38 - 47