COMMUTATIVITY DEGREE, ITS GENERALIZATIONS, AND CLASSIFICATION OF FINITE GROUPS

ABSTRACT

RAJAT KANTI NATH
DEPARTMENT OF MATHEMATICS

SUBMITTED
IN PARTIAL FULFILMENT OF THE
REQUIREMENT OF THE DEGREE OF

DOCTOR OF PHILOSOPHY
IN
MATHEMATICS

TO

NORTH-EASTERN HILL UNIVERSITY
SHILLONG - 793022, INDIA

JULY, 2010

Classification of finite groups is a central problem in theory of groups. Even though finite abelian groups have been completely classified, a lot still remains to be done as far as non-abelian groups are concerned. People all over the world have used various types of invariants for classifying finite groups, particularly the non-abelian ones. The commutativity degree of a finite group is one such invariant, and it seems that many interesting results are possible to obtain with the help of this notion and its generalizations.

In recent years there has been a growing interest in the use of the probabilistic methods in the theory of finite groups. These methods have proved useful in the solution of several difficult problems on groups. In some cases the probabilistic nature of the problem is apparent from its formulation, but in other cases the connection to probability seems surprising and can not be anticipated by the nature of the problem.

The roots of the subject matter of this thesis lie in a series of papers by P. Erdös and P. Turán (see [5, 6, 7, 8]) published between 1965 and 1968, and also in the Ph. D thesis of K. S. Joseph [16] submitted in 1969, wherein some problems of statistical group theory and commutativity in non-abelian groups have been considered. In 1973, W. H. Gustafson [14] considered the question – *what is the probability that two group elements commute?* The answer is given by what is known as the commutativity degree of a group. It may be mentioned here that the question, in some sense, was also considered by Erdös and Turán [8].

Formally, the commutativity degree of a finite group G, denoted by $\Pr(G)$, is defined as the ratio

$$\Pr(G) = \frac{\text{Number of ordered pairs } (x, y) \in G \times G \text{ such that } xy = yx}{\text{Total number of ordered pairs } (x, y) \in G \times G}.$$

In other words, commutativity degree is a kind of measure for abelianness of a group. Note that $\Pr(G) > 0$, and that $\Pr(G) = 1$ if and only if G is abelian. Also, given a finite group G, we have $\Pr(G) \leq \frac{5}{8}$ with equality if and only if $\frac{G}{Z(G)}$ has order 4 (see [2, 14]), where $Z(G)$ denotes the center of G. This gave rise to the problem of determining the numbers in the interval $(0, \frac{5}{8}]$ which can be realized as the commutativity degrees of some finite groups, and also to the problem of classifying all finite groups with a given commutativity degree.

In 1979, D. J. Rusin [23] computed, for a finite group G, the values of $\Pr(G)$ when $G' \subseteq Z(G)$, and also when $G' \cap Z(G)$ is trivial, where G' denotes the commutator subgroup of G. He determined all numbers lying in the interval $(\frac{11}{32}, 1]$ that can be realized as the commutativity degree of some finite groups, and also classified all finite groups whose commutativity degrees lie in the interval $(\frac{11}{32}, 1]$.

In 1995, P. Lescot [17] classified, up to isoclinism, all finite groups whose commutativity degrees are greater than or equal to $\frac{1}{2}$. It may be mentioned here that the concept of isoclinism between any two groups was introduced by P. Hall [15]. A pair (ϕ, ψ) is said to be an *isoclinism* from a group G to another group H if the following conditions hold:

(a) ϕ is an isomorphism from $G/Z(G)$ to $H/Z(H)$,

(b) ψ is an isomorphism from G' to H', and

(c) the diagram

$$\begin{array}{ccc} \dfrac{G}{Z(G)} \times \dfrac{G}{Z(G)} & \xrightarrow{\phi \times \phi} & \dfrac{H}{Z(H)} \times \dfrac{H}{Z(H)} \\ \Big\downarrow a_G & & \Big\downarrow a_H \\ G' & \xrightarrow{\psi} & H' \end{array}$$

commutes, that is, $a_H \circ (\phi \times \phi) = \psi \circ a_G$, where a_G and a_H are given respectively by $a_G(g_1 Z(G), g_2 Z(G)) = [g_1, g_2]$ for all $g_1, g_2 \in G$ and $a_H(h_1 Z(H), h_2 Z(H)) = [h_1, h_2]$ for all $h_1, h_2 \in H$. Here, given $x, y \in G$, $[x, y]$ stands for the commutator $xyx^{-1}y^{-1}$ of x and y in G.

In 2001, Lescot [18] has also classified, up to isomorphism, all finite groups whose commutativity degrees lie in the interval $[\frac{1}{2}, 1]$.

In 2006, F. Barry, D. MacHale and Á. Ní Shé [1] have shown that if G is a finite group with $|G|$ odd and $\Pr(G) > \frac{11}{75}$, then G is supersolvable. They also proved that if $\Pr(G) > \frac{1}{3}$, then G is supersolvable. It may be mentioned here that a group G is said to be *supersolvable* if there is a series of the form

$$\{1\} = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_r = G,$$

where $A_i \trianglelefteq G$ and A_{i+1}/A_i is cyclic for each i with $0 \leq i \leq r-1$.

In the same year 2006, R. M. Guralnick and G. R. Robinson [12] re-established a result of Lescot (see [13]) which says that if G is a finite group with $\Pr(G)$ greater than $\frac{3}{40}$, then either G is solvable, or $G \cong A_5 \times B$, where A_5 is the alternating group of degree 5 and B is some abelian group.

The classical notion of commutativity degree has been generalized in a number of ways. In 2007, A. Erfanian, R. Rezaei and P. Lescot [9] studied the probability $\Pr(H, G)$ that an element of a given subgroup H of a finite group G commutes with an element of G. Note that $\Pr(G, G) = \Pr(G)$. In 2008, M. R. Pournaki and R. Sobhani [22] studied the probability $\Pr_g(G)$ that the commutator of an arbitrarily chosen pair of elements in a finite group G equals a given group element g. They have also extended some of the results obtained by Rusin. It is easy to see that $\Pr_g(G) = \Pr(G)$ if $g = 1$, the identity element of G.

In Chapter 1, we briefly recall a few definitions and well-known results from several relevant topics, which constitute the minimum prerequisites for the subsequent chapters. In this chapter, we also fix certain notations. Given a subgroup K of a group G and an element $x \in G$, we write $C_K(x)$ and $C\ell_K(x)$ to denote the sets $\{k \in K : kx = xk\}$ and $\{kxk^{-1} \in G : k \in K\}$ respectively; noting that, for $K = G$, these sets coincide respectively with the centralizer and the conjugacy class of x in G. Also, given any two subgroups H and K of a group G, we write $C_K(H) = \{k \in K : hk = kh \text{ for all } h \in H\}$. Note that $C_K(x) = C_K(\langle x \rangle)$, where $\langle x \rangle$ denotes the cyclic subgroup of G generated by $x \in G$.

Further, we write $\mathrm{Irr}(G)$ to denote the set of all irreducible complex characters of G, and $\mathrm{cd}(G)$ to denote the set $\{\chi(1) : \chi \in \mathrm{Irr}(G)\}$. If $\chi(1) = |G : Z(G)|^{1/2}$ for some $\chi \in \mathrm{Irr}(G)$, then the group G is said to be of *central type*.

In Chapter 2, which is based on our papers [19] and [21], we determine, for a finite group G, the value of $\Pr(G)$ and the size of $\frac{G}{Z(G)}$ when $|G'| = p^2$ and $|G' \cap Z(G)| = p$, where p is a prime such that $\gcd(p-1, |G|) = 1$. The main result of Section 2.2 is given as follows.

Theorem 2.2.6. *Let G be a finite group and p be a prime such that $\gcd(p-1, |G|) = 1$. If $|G'| = p^2$ and $|G' \cap Z(G)| = p$, then*

$$\text{(a)}\ \Pr(G) = \begin{cases} \frac{2p^2-1}{p^4} & \text{if } C_G(G') \text{ is abelian} \\ \frac{1}{p^4}\left(\frac{p-1}{p^{2s-1}} + p^2 + p - 1\right) & \text{otherwise.} \end{cases}$$

$$\text{(b)}\ \left|\frac{G}{Z(G)}\right| = \begin{cases} p^3 & \text{if } C_G(G') \text{ is abelian} \\ p^{2s+2} \text{ or } p^{2s+3} & \text{otherwise,} \end{cases}$$

where $p^{2s} = |C_G(G') : Z(C_G(G'))|$. Moreover,

$$\left|\frac{G}{G' \cap Z(G)} : Z\left(\frac{G}{G' \cap Z(G)}\right)\right| = \left|\frac{G}{Z(G)} : Z\left(\frac{G}{Z(G)}\right)\right| = p^2.$$

This theorem together with few other supplementary results, enable us to classify all finite groups G of odd order with $\Pr(G) \geq \frac{11}{75}$. In the process we also point out a few small but significant lacunae in the work of Rusin [23]. The main result of Section 2.3 is given as follows.

Theorem 2.3.3. *Let G be a finite group. If $|G|$ is odd and $\Pr(G) \geq \frac{11}{75}$, then the possible values of $\Pr(G)$ and the corresponding structures of G', $G' \cap Z(G)$ and $G/Z(G)$ are given as follows:*

Pr(G)	G'	$G' \cap Z(G)$	$G/Z(G)$
1	$\{1\}$	$\{1\}$	$\{1\}$
$\frac{1}{3}(1+\frac{2}{3^{2s}})$	C_3	C_3	$(C_3 \times C_3)^s,\ s \geq 1$
$\frac{1}{5}(1+\frac{4}{5^{2s}})$	C_5	C_5	$(C_5 \times C_5)^s,\ s \geq 1$
$\frac{5}{21}$	C_7	$\{1\}$	$C_7 \rtimes C_3$
$\frac{55}{343}$	C_7	C_7	$C_7 \times C_7$
$\frac{17}{81}$	C_9 *or* $C_3 \times C_3$ $C_3 \times C_3$	C_3 $C_3 \times C_3$	$(C_3 \times C_3) \rtimes C_3$ C_3^3
$\frac{121}{729}$	$C_3 \times C_3$	$C_3 \times C_3$	C_3^4
$\frac{7}{39}$	C_{13}	$\{1\}$	$C_{13} \rtimes C_3$
$\frac{3}{19}$	C_{19}	$\{1\}$	$C_{19} \rtimes C_3$
$\frac{29}{189}$	C_{21}	C_3	$C_3 \times (C_7 \rtimes C_3)$
$\frac{11}{75}$	$C_5 \times C_5$	$\{1\}$	$(C_5 \times C_5) \rtimes C_3$

In the above table C_n denotes the cyclic group of order n and $\rtimes$ stands for semidirect product.

In [22, Corollary 2.3], M. R. Pournaki and R. Sobhani have proved that, for a finite group G satisfying $|\operatorname{cd}(G)| = 2$, one has

$$\Pr(G) \geq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{|G : Z(G)|}\right)$$

with equality if and only if G is of central type. In Section 2.4, we have improved this result as follows.

Theorem 2.4.1. *If G is a finite group, then*

$$\Pr(G) \geq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{|G : Z(G)|}\right).$$

In particular, $\Pr(G) > \frac{1}{|G'|}$ *if G is non-abelian.*

There are several equivalent conditions that are necessary as well as sufficient for the attainment of the above lower bound for $\Pr(G)$.

Theorem 2.4.3. *For a finite non-abelian group G, the statements given below are equivalent.*

(a) $\Pr(G) = \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{|G : Z(G)|}\right)$.

(b) $\mathrm{cd}(G) = \{1, |G : Z(G)|^{1/2}\}$, *which means that G is of central type with* $|\mathrm{cd}(G)| = 2$.

(c) $|\mathrm{C}\ell_G(x)| = |G'|$ *for all $x \in G - Z(G)$.*

(d) $\mathrm{C}\ell_G(x) = G'x$ *for all $x \in G - Z(G)$; in particular, G is a nilpotent group of class* 2.

(e) $C_G(x) \trianglelefteq G$ *and* $G' \cong \frac{G}{C_G(x)}$ *for all $x \in G - Z(G)$; in particular, G is a CN-group, that is, the centralizer of every element is normal.*

(f) $G' = \{[y, x] : y \in G\}$ *for all $x \in G - Z(G)$; in particular, every element of G' is a commutator.*

Theorem 2.4.1 and Theorem 2.4.3 not only allow us to obtain some characterizations for finite nilpotent groups of class 2 whose commutator subgroups have prime order, but also enable us to re-establish certain facts (essentially due to K. S. Joseph [16]) concerning the smallest prime divisors of the orders of finite groups.

Proposition 2.4.4. *Let G be a finite group and p be the smallest prime divisor of $|G|$.*

(a) *If $p \neq 2$, then $\Pr(G) \neq \frac{1}{p}$.*

(b) *When G is non-abelian, $\Pr(G) > \frac{1}{p}$ if and only if $|G'| = p$ and $G' \subseteq Z(G)$.* .

Corrolary 2.4.5. *If G is a finite group with $\Pr(G) = \frac{1}{3}$, then $|G|$ is even.*

Proposition 2.4.7. *Let G be a finite group and p be a prime. Then the following statements are equivalent.*

(a) *$|G'| = p$ and $G' \subseteq Z(G)$.*

(b) *G is of central type with $|\operatorname{cd}(G)| = 2$ and $|G'| = p$.*

(c) *G is a direct product of a p-group P and an abelian group A such that $|P'| = p$ and $\gcd(p, |A|) = 1$.*

(d) *G is isoclinic to an extra-special p-group; consequently, $|G : Z(G)| = p^{2k}$ for some positive integer k.*

In particular, if G is non-abelian and p is the smallest prime divisor of $|G|$, then the above statements are also equivalent to the condition $\Pr(G) > \frac{1}{p}$.

In [18], Lescot deduced that $\Pr(D_{2n}) \longrightarrow \frac{1}{4}$ and $\Pr(Q_{2^{n+1}}) \longrightarrow \frac{1}{4}$ as $n \longrightarrow \infty$, where D_{2n} and $Q_{2^{n+1}}$ denote the dihedral group of order $2n$, $n \geq 1$, and the quaternion group of order 2^{n+1}, $n \geq 2$, respectively. He also enquired whether there are other natural families of finite groups with the same property. In 2007, I. V. Erovenko and B. Sury [10] have shown, in particular, that for every integer $k > 1$ there exists a family $\{G_n\}$ of finite groups such that $\Pr(G_n) \to \frac{1}{k^2}$ as $n \to \infty$. In the last section of Chapter 2 we have considered the question posed by Lescot mentioned above. Moreover, we make the following observation.

Proposition 2.5.1. *For every integer $k > 1$ there exists a family $\{G_n\}$ of finite groups such that $\Pr(G_n) \to \frac{1}{k}$ as $n \to \infty$.*

In the same line, we also have the following result.

Proposition 2.5.2. *For every positive integer n there exists a finite group G such that $\Pr(G) = \frac{1}{n}$.*

In Chapter 3, which is based on our papers [3] and [4], we generalize the following result of F. G. Frobenius [11]:

If G is a finite group and $g \in G$, then the number of solutions of the commutator equation $xyx^{-1}y^{-1} = g$ in G defines a character on G, and is given by

$$\zeta(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|}{\chi(1)} \chi(g).$$

We write $F(x_1, x_2, \ldots, x_n)$ to denote the free group of words on n generators $x_1, x_2, \ldots, x_n$. For $1 \leq i \leq n$, we write '$x_i \in \omega(x_1, x_2, \ldots, x_n)$' to mean that x_i has a non-zero index (that is, x_i^k forms a syllable, with $0 \neq k \in \mathbb{Z}$) in the word $\omega(x_1, x_2, \ldots, x_n) \in F(x_1, x_2, \ldots, x_n)$. We call a word $\omega(x_1, x_2, \ldots, x_n)$ *admissible* if each $x_i \in \omega(x_1, x_2, \ldots, x_n)$ has precisely two non-zero indices, namely, $+1$ and -1. We write $\mathscr{A}(x_1, x_2, \ldots, x_n)$ to denote the set of all admissible words in $F(x_1, x_2, \ldots, x_n)$.

Given a finite group G and an element $g \in G$, let $\zeta_n^{\omega}(g)$ denote the number of solutions $(g_1, g_2, \ldots, g_n) \in G^n$ of the word equation $\omega(x_1, x_2, \ldots, x_n) = g$, where $G^n = G \times G \times \cdots \times G$ (n times). Thus,

$$\zeta_n^{\omega}(g) = |\{(g_1, g_2, \ldots, g_n) \in G^n : \omega(g_1, g_2, \ldots, g_n) = g\}|.$$

The main result of Section 3.1 is given as follows.

Theorem 3.1.4. *Let $\omega(x_1, x_2, \ldots, x_n) \in \mathscr{A}(x_1, x_2, \ldots, x_n)$, $n \geq 1$. If G is a finite group, then the map $\zeta_n^{\omega} : G \longrightarrow \mathbb{C}$ defined by*

$$\zeta_n^{\omega}(g) = |\{(g_1, g_2, \ldots, g_n) \in G^n : \omega(g_1, g_2, \ldots, g_n) = g\}|, \quad g \in G,$$

is a character of G.

Given any two finite sets X and Y, a function $f : X \longrightarrow Y$ is said to be *almost measure preserving* if there exists a sufficiently small positive real number ϵ such that

$$\left| \frac{|f^{-1}(Y_0)|}{|X|} - \frac{|Y_0|}{|Y|} \right| < \epsilon \quad \text{for all } Y_0 \subseteq Y.$$

In Section 3.2, we consider the following question posed by Aner Shalev [24, Problem 2.10]:

Which words induce almost measure preserving maps on finite simple groups?

More precisely, given an admissible word $\omega(x_1, x_2, \ldots, x_n)$ and the induced word map $\alpha_\omega : G^n \to G$ defined by $\alpha_\omega(g_1, g_2, \ldots, g_n) = \omega(g_1, g_2, \ldots, g_n)$, we proved that

Corollary 3.2.7. *Let G be a finite simple group, and $o(1)$ be a real number depending on G which tends to zero as $|G| \to \infty$.*

(a) *If* $Y \subseteq G$, *then* $\frac{|(\alpha_\omega)^{-1}(Y)|}{|G|^n} = \frac{|Y|}{|G|} + o(1)$. *This means that the map* α_ω *is almost measure preserving.*

(b) *If* $X \subseteq G^n$, *then* $\frac{|\alpha_\omega(X)|}{|G|} \geq \frac{|X|}{|G|^n} - o(1)$; *in particular, if* X *is such that* $|X| = (1 - o(1))|G|^n$, *then* $|\alpha_\omega(X)| = (1 - o(1))|G|$. *This means that almost all the elements of* G *can be expressed as* $\omega(g_1, g_2, \dots, g_n)$ *for some* $g_1, g_2, \dots, g_n \in G$.

In the last section of Chapter 3, we obtain yet another generalization of Frobenius' result mentioned above. The main results of this section are given as follows.

Theorem 3.3.1. *Let* G *be a finite group,* $H \trianglelefteq G$ *and* $g \in G$. *If* $\tilde{\zeta}(g)$ *denotes the number of elements* $(h_1, g_2) \in H \times G$ *satisfying* $[h_1, g_2] = g$, *then* $\tilde{\zeta}$ *is a class function of* G *and*

$$\tilde{\zeta}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|H|[\chi_H, \chi_H]}{\chi(1)} \chi(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|H|[\chi_H^G, \chi]}{\chi(1)} \chi(g).$$

Corollary 3.3.2. *Let* G *be a finite group. Then, with notations as above,* $\tilde{\zeta}$ *is a character of* G.

Proposition 3.3.3. *Let* G *be a finite group,* $H \trianglelefteq G$ *and* $g \in G$. *If* $\tilde{\zeta}_{2n}(g)$, $n \geq 1$, *denotes the number of elements* $((h_1, g_1), \dots, (h_n, g_n)) \in (H \times G)^n$ *satisfying* $[h_1, g_1] \dots [h_n, g_n] = g$, *then* $\tilde{\zeta}_{2n}$ *is a character of* G *and*

$$\tilde{\zeta}_{2n}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|^{n-1}|H|^n[\chi_H, \chi_H]^n}{\chi(1)^{2n-1}} \chi(g).$$

Proposition 3.3.4. *Let H be a subgroup of a finite group G and $g \in G$. Then the number of elements $(g_1, h_2, g_3) \in G \times H \times G$ satisfying $g_1 h_2 g_1^{-1} g_3 h_2^{-1} g_3^{-1} = g$ defines a character of G and is given by*

$$\tilde{\zeta}_3(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G||H|[\chi_H, \chi_H]}{\chi(1)} \chi(g).$$

In Chapter 4, which is based on our paper [20], we study the probability $\mathrm{Pr}_g^\omega(G)$ that an arbitrarily chosen n-tuple of elements of a given finite group G is mapped to a given group element g under the word map induced by a non-trivial admissible word $\omega(x_1, x_2, \ldots, x_n)$. Formally, we write

$$\mathrm{Pr}_g^\omega(G) = \frac{\zeta_n^\omega(g)}{|G^n|},$$

where $\zeta_n^\omega(g) = |\{(g_1, g_2, \ldots, g_n) \in G^n : \omega(g_1, g_2, \ldots, g_n) = g\}|$. The main results of Section 4.1 are as follows.

Proposition 4.1.1. *Let G be a finite group and $\omega(x_1, x_2, \ldots, x_n)$ be a non-trivial admissible word. Then*

(a) $\mathrm{Pr}_1^\omega(G) \geq \dfrac{n|G : Z(G)| - n + 1}{|G : Z(G)|^n} \geq \dfrac{1}{|G : Z(G)|^n} \gneq 0,$

(b) $\mathrm{Pr}_1^\omega(G) = 1$ *if and only if* G *is abelian.*

Proposition 4.1.3. *Let G and H be two finite groups and (ϕ, ψ) be an isoclinism from G to H. If $g \in G'$ and $\omega(x_1, x_2, \ldots, x_n)$ is a non-trivial admissible word, then*

$$\mathrm{Pr}_g^\omega(G) = \mathrm{Pr}_{\psi(g)}^\omega(H).$$

Proposition 4.1.4. *Let G be a finite group and $\omega(x_1, x_2, \ldots, x_n)$ be a non-trivial admissible word. If $g, h \in G'$ generate the same cyclic subgroup of G, then $\Pr_g^\omega(G) = \Pr_h^\omega(G)$.*

Proposition 4.1.6. *Let G be a finite group, $g \in G'$ and $\omega(x_1, x_2, \ldots, x_n)$ be a non-trivial admissible word. Then*

(a) $\Pr_g^\omega(G) \leq \Pr_1^\omega(G) \leq \Pr(G)$,

(b) $\Pr_g^\omega(G) = \Pr_1^\omega(G)$ *if and only if* $g = 1$.

Let $m_G = \min\{\chi(1) : \chi \in \mathrm{Irr}(G), \chi(1) \neq 1\}$. Considering, in particular, the word $x_1x_2 \ldots x_n x_1^{-1}x_2^{-1} \ldots x_n^{-1}$, $n \geq 2$, and writing $\Pr_g^n(G)$ in place of $\Pr_g^\omega(G)$, we obtain the following results in the sections 4.2, 4.3 and 4.4.

Proposition 4.2.2. *Let G be a finite non-abelian group, $g \in G'$ and d be an integer such that $2 \leq d \leq m_G$. Then*

(a) $\left|\Pr_g^n(G) - \frac{1}{|G'|}\right| \leq \frac{1}{d^{n-2}}\left(\Pr(G) - \frac{1}{|G'|}\right)$. *In other words,*

$$\frac{1}{d^{n-2}}\left(-\Pr(G) + \frac{d^{n-2}+1}{|G'|}\right) \leq \Pr_g^n(G) \leq \frac{1}{d^{n-2}}\left(\Pr(G) + \frac{d^{n-2}-1}{|G'|}\right).$$

(b) $\left|\Pr_g^n(G) - \frac{1}{|G'|}\right| \leq \frac{1}{d^n}\left(1 - \frac{1}{|G'|}\right)$. *In other words,*

$$\frac{1}{d^n}\left(-1 + \frac{d^n+1}{|G'|}\right) \leq \Pr_g^n(G) \leq \frac{1}{d^n}\left(1 + \frac{d^n-1}{|G'|}\right).$$

In particular, $\Pr_g^n(G) \leq \frac{2^n+1}{2^{n+1}}$.

Proposition 4.2.3. *If G is a finite non-abelian simple group and $g \in G'$, then*

$$\left|\Pr_g^n(G) - \frac{1}{|G|}\right| \leq \frac{1}{3^{n-2}}\left(\frac{1}{12} - \frac{1}{|G|}\right).$$

In other words,

$$\frac{1}{3^{n-2}}\left(\frac{-1}{12} + \frac{3^{n-2}+1}{|G|}\right) \leq \Pr_g^n(G) \leq \frac{1}{3^{n-2}}\left(\frac{1}{12} + \frac{3^{n-2}-1}{|G|}\right).$$

In particular,

$$\Pr_g^n(G) \leq \frac{3^{n-2}+4}{3^{n-1} \times 20}.$$

Corollary 4.3.2. *Let G be a finite non-abelian group with $|\operatorname{cd}(G)| = 2$. Then every element of G' is a generalized commutator of length n for all $n \geq 2$; in particular, every element of G' is a commutator.*

Proposition 4.3.3. *Let G be a finite non-abelian group, $g \in G'$ and d be an integer such that $2 \leq d \leq m_G$. Then*

(a) $\Pr_g^n(G) = \dfrac{1}{d^{n-2}}\left(\Pr(G) + \dfrac{d^{n-2}-1}{|G'|}\right)$ *if and only if* $g = 1$ *and* $\operatorname{cd}(G) = \{1, d\}$.

(b) $\Pr_g^n(G) = \dfrac{1}{d^{n-2}}\left(-\Pr(G) + \dfrac{d^{n-2}+1}{|G'|}\right)$ *if and only if* $g \neq 1$, $\operatorname{cd}(G) = \{1, d\}$ *and* $|G'| = 2$.

Proposition 4.3.4. *Let G be a finite non-abelian group, $g \in G'$ and d be an integer such that $2 \leq d \leq m_G$. Then*

(a) $\Pr_g^n(G) = \dfrac{1}{d^n}\left(1 + \dfrac{d^n - 1}{|G'|}\right)$ *if and only if* $g = 1$ *and* $\operatorname{cd}(G) = \{1, d\}$.

(b) $\Pr_g^n(G) = \dfrac{1}{d^n}\left(-1 + \dfrac{d^n+1}{|G'|}\right)$ *if and only if* $g \neq 1$, $\mathrm{cd}(G) = \{1, d\}$ *and* $|G'| = 2$.

Proposition 4.3.7. *Let G be a finite non-abelian group, $g \in G'$ and p be the smallest prime divisor of $|G|$ Then*

$$\Pr_g^n(G) = \frac{p^n + p - 1}{p^{n+1}}$$

if and only if $g = 1$, *and G is isoclinic to*

$$\langle x, y \; : \; x^{p^2} = 1 = y^p,\ y^{-1}xy = x^{p+1}\rangle$$

In particular, putting $p = 2$, $\Pr_g^n(G) = \dfrac{2^n+1}{2^{n+1}}$ if and only if $g = 1$, and G is isoclinic to D_8, the dihedral group, and hence, to Q_8, the group of quaternions

Proposition 4.4.1. *Let G be a finite non-abelian group with $|\mathrm{cd}(G)| = 2$ and $g \in G'$ Then*

$$\Pr_1^n(G) \geq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{|G : Z(G)|^{n/2}}\right) \quad \textit{and}$$
$$\Pr_g^n(G) \leq \frac{1}{|G'|}\left(1 - \frac{1}{|G : Z(G)|^{n/2}}\right) \quad \textit{if } g \neq 1.$$

Moreover, in each case, the equality holds if and only if G is of central type

Corollary 4.4.2. *Let G be a finite non-abelian group and $g \in G'$ If G is of central type with $|\mathrm{cd}(G)| = 2$, then*

$$\Pr_1^n(G) \leq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{2^n}\right) \quad \textit{and}$$
$$\Pr_g^n(G) \geq \frac{1}{|G'|}\left(1 - \frac{1}{2^n}\right) \quad \textit{if } g \neq 1.$$

Proposition 4.4.3. *Let G be a finite non-abelian group and $g \in G'$. If $G' \subseteq Z(G)$ and $|G'| = p$, where p is a prime, then*

$$\Pr_g^n(G) = \begin{cases} \frac{1}{p}\left(1 + \frac{p-1}{p^{nk}}\right) & \text{if } g = 1 \\ \frac{1}{p}\left(1 - \frac{1}{p^{nk}}\right) & \text{if } g \neq 1, \end{cases}$$

where $k = \dfrac{1}{2}\log_p |G : Z(G)|$.

Proposition 4.4.5. *Let p be a prime. Let r and s be two positive integers such that $s \mid (p-1)$, and $r^j \equiv 1 \pmod{p}$ if and only if $s \mid j$. If $G = \langle a, b : a^p = b^s = 1, bab^{-1} = a^r \rangle$ and $g \in G'$, then*

$$\Pr_g^n(G) = \begin{cases} \dfrac{s^n + p - 1}{ps^n} & \text{if } g = 1 \\[2ex] \dfrac{s^n - 1}{ps^n} & \text{if } g \neq 1. \end{cases}$$

Proposition 4.4.6. *Let G be a finite non-abelian group and $g \in G'$. If $G' \cap Z(G) = \{1\}$ and $|G'| = p$, where p is a prime, then*

(a) *G is isoclinic to the group $\langle a, b : a^p = b^s = 1,\ bab^{-1} = a^r \rangle$, where $s \mid (p-1)$, and $r^j \equiv 1 \pmod{p}$ if and only if $s \mid j$,*

(b) $$\Pr_g^n(G) = \begin{cases} \dfrac{s^n + p - 1}{ps^n} & \text{if } g = 1 \\[2ex] \dfrac{s^n - 1}{ps^n} & \text{if } g \neq 1. \end{cases}$$

Proposition 4.4.7. *Let G be a finite non-abelian group and $g \in G'$. If $g \neq 1$, then $\Pr_g^n(G) < \frac{1}{p}$, where p is the smallest prime divisor of $|G|$. In particular, we have $\Pr_g^n(G) < \frac{1}{2}$.*

Proposition 4.4.8. *For each $\varepsilon > 0$ and for each prime p, there exists a finite group G such that*

$$\left|\Pr_g^n(G) - \frac{1}{p}\right| < \varepsilon$$

for all $g \in G'$.

Let G be a finite group and $g \in G'$. Let H and K be two subgroups of G. In Chapter 5, which is based on our paper [4], we study the probability $\Pr_g(H, K)$ that the commutator of a randomly chosen pair of elements (one from H and the other from K) equals g. In other words, we study the ratio

$$\Pr_g(H, K) = \frac{|\{(x, y) \in H \times K : [x, y] = g\}|}{|H||K|},$$

and further extend some of the results obtained in [9] and [22]. Without any loss, we may assume that G is non-abelian. The main results of the sections 5.1 and 5.2 are as follows.

Proposition 5.1.1. *Let G be a finite group and $g \in G'$. If H and K are two subgroups of G, then $\Pr_g(H, K) = \Pr_{g^{-1}}(K, H)$. However, if $g^2 = 1$, or if $g \in H \cup K$ (for example, when H or K is normal in G), we have $\Pr_g(H, K) = \Pr_g(K, H) = \Pr_{g^{-1}}(H, K)$.*

Theorem 5.1.3. *Let G be a finite group and $g \in G'$. If H and K are two subgroups of G, then*

$$\Pr_g(H, K) = \frac{1}{|H||K|} \sum_{\substack{x \in H \\ g^{-1}x \in \mathrm{C}\ell_K(x)}} |C_K(x)| = \frac{1}{|H|} \sum_{\substack{x \in H \\ g^{-1}x \in \mathrm{C}\ell_K(x)}} \frac{1}{|\,\mathrm{C}\ell_K(x)|},$$

where $C_K(x) = \{y \in K : xy = yx\}$ and $\mathrm{C}\ell_K(x) = \{yxy^{-1} : y \in K\}$, the K-conjugacy class of x.

This theorem plays a key role in the study of $\Pr_g(H, K)$. As an immediate consequence, we have the following generalization of the well-known formula $\Pr(G) = \frac{k(G)}{|G|}$.

Corollary 5.1.4. *Let G be a finite group and H, K be two subgroups of G. If $H \trianglelefteq G$, then*

$$\Pr(H, K) = \frac{k_K(H)}{|H|},$$

where $k_K(H)$ is the number of K-conjugacy classes that constitute H.

Proposition 5.1.5. *If H is an abelian normal subgroup of a finite group G with a complement K in G and $g \in G'$, then*

$$\Pr_g(H, G) = \Pr_g(H, K).$$

Corollary 5.1.6. *Let G be a finite group and $g \in G'$. If $H \trianglelefteq G$ with $C_G(x) = H$ for all $x \in H - \{1\}$, then*

$$\Pr_g(H, G) = \Pr_g(H, K),$$

where K is a complement of H in G. In particular,

$$\Pr(H, G) = \frac{1}{|H|} + \frac{|H| - 1}{|G|}.$$

Proposition 5.2.1. *Let G be a finite group and $g \in G'$. Let H and K be any two subgroups of G. If $g \neq 1$, then*

(a) $\Pr_g(H, K) \neq 0 \Longrightarrow \Pr_g(H, K) \geq \frac{|C_H(K)||C_K(H)|}{|H||K|}$,

(b) $\Pr_g(H,G) \neq 0 \Longrightarrow \Pr_g(H,G) \geq \dfrac{2|H \cap Z(G)||C_G(H)|}{|H||G|}$,

(c) $\Pr_g(G) \neq 0 \Longrightarrow \Pr_g(G) \geq \dfrac{3}{|G \cdot Z(G)|^2}$.

Proposition 5.2.2. *Let G be a finite group and $g \in G'$. If H and K are any two subgroups of G, then*

$$\Pr_g(H,K) \leq \Pr(H,K)$$

with equality if and only if $g = 1$.

Proposition 5.2.3. *Let G be a finite group and $g \in G'$, $g \neq 1$. Let H and K be any two subgroups of G. If p is the smallest prime divisor of $|G|$, then*

$$\Pr_g(H,K) \leq \frac{|H| - |C_H(K)|}{p|H|} < \frac{1}{p}.$$

Proposition 5.2.4. *Let H, K_1 and K_2 be subgroups of a finite group G with $K_1 \subseteq K_2$. Then*

$$\Pr(H,K_1) \geq \Pr(H,K_2)$$

with equality if and only if $\mathrm{C}\ell_{K_1}(x) = \mathrm{C}\ell_{K_2}(x)$ *for all $x \in H$.*

Proposition 5.2.5. *Let H, K_1 and K_2 be subgroups of a finite group G with $K_1 \subseteq K_2$. Then*

$$\Pr(H,K_2) \geq \frac{1}{|K_2 : K_1|}\left(\Pr(H,K_1) + \frac{|K_2| - |K_1|}{|H||K_1|}\right)$$

with equality if and only if $C_H(x) = \{1\}$ *for all $x \in K_2 - K_1$.*

Proposition 5.2.6. *Let $H_1 \subseteq H_2$ and $K_1 \subseteq K_2$ be subgroups of a finite group G and $g \in G'$. Then*

$$\Pr_g(H_1,K_1) \leq |H_2 : H_1||K_2 : K_1|\Pr_g(H_2,K_2)$$

with equality if and only if

$$\begin{aligned} & g^{-1}x \notin \mathrm{C}\ell_{K_2}(x) \ \ \textit{for all} \ \ x \in H_2 - H_1, \\ & g^{-1}x \notin \mathrm{C}\ell_{K_2}(x) - \mathrm{C}\ell_{K_1}(x) \ \ \textit{for all} \ \ x \in H_1, \\ \textit{and} \quad & C_{K_1}(x) = C_{K_2}(x) \ \ \textit{for all} \ \ x \in H_1 \ \ \textit{with} \ \ g^{-1}x \in \mathrm{C}\ell_{K_1}(x). \end{aligned}$$

In particular, for $g = 1$, the condition for equality reduces to $H_1 = H_2$, and $K_1 = K_2$.

Corollary 5.2.7. *Let G be a finite group, H be a subgroup of G and $g \in G'$. Then*

$$\Pr_g(H, G) \leq |G : H| \Pr(G)$$

with equality if and only if $g = 1$ and $H = G$.

Theorem 5.2.8. *Let G be a finite group and p be the smallest prime dividing $|G|$. If H and K are any two subgroups of G, then*

$$\begin{aligned} \Pr(H, K) &\geq \frac{|C_H(K)|}{|H|} + \frac{p(|H| - |X_H| - |C_H(K)|) + |X_H|}{|H||K|} \\ \textit{and } \Pr(H, K) &\leq \frac{(p-1)|C_H(K)| + |H|}{p|H|} - \frac{|X_H|(|K| - p)}{p|H||K|}, \end{aligned}$$

where $X_H = \{x \in H : C_K(x) = 1\}$. Moreover, in each of these bounds, H and K can be interchanged.

Corollary 5.2.9. *Let G be a finite group and p be the smallest prime dividing $|G|$. If H and K are two subgroups of G such that $[H, K] \neq \{1\}$, then*

$$\Pr(H, K) \leq \frac{2p - 1}{p^2}.$$

In particular, $\Pr(H, K) \leq \frac{3}{4}$.

Proposition 5.2.10. *Let G be a finite group and H, K be any two subgroups of G. If $\Pr(H, K) = \frac{2p-1}{p^2}$ for some prime p, then p divides $|G|$. If p happens to be the smallest prime divisor of $|G|$, then*

$$\frac{H}{C_H(K)} \cong C_p \cong \frac{K}{C_K(H)}, \quad \textit{and hence,} \quad H \neq K.$$

In particular, $\frac{H}{C_H(K)} \cong C_2 \cong \frac{K}{C_K(H)}$ *if* $\Pr(H, K) = \frac{3}{4}$.

In the last section of chapter 5, with H normal in G, we also develop and study a character theoretic formula for $\Pr_g(H, G)$ given by

$$\Pr_g(H, G) = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{[\chi_H, \chi_H]}{\chi(1)} \chi(g).$$

Proposition 5.3.1. *Let G be a finite group. If H is a normal subgroup of G and $g \in G'$, then*

$$\left| \Pr_g(H, G) - \frac{1}{|G'|} \right| \leq |G : H| \left(\Pr(G) - \frac{1}{|G'|} \right).$$

As an application, we obtain yet another condition under which every element of G' is a commutator.

Proposition 5.3.3. *Let G be a finite group and p be the smallest prime dividing $|G|$. If $|G'| \leq p^2$, then every element of G' is a commutator.*

We conclude the thesis with a discussion, in the last chapter, on some of the possible research problems related to the results obtained in the earlier chapters.

Bibliography

[1] F. Barry, D. MacHale and Á. Ní Shé, *Some supersolvability conditions for finite groups*, Math. Proc. Royal Irish Acad. **106A** (2) (2006), 163–177.

[2] S. M. Belcastro and G. J. Sherman, *Counting centralizers in finite groups*, Math. Magazine **67** (5) (1994), 366–374

[3] A. K. Das and R. K. Nath, *On solutions of a class of equations in a finite group*, Comm. Algebra **37** (11) (2009), 3904–3911.

[4] A. K. Das and R. K. Nath, *On generalized relative commutativity degree of a finite group*, International Electronic J. Algebra **7** (2010), 140–151.

[5] P. Erdös and P. Turán, *On some problems of a statistical group-theory. I*, Z. Wahrschein. Verw. Gebeite **4** (1965), 175–186.

[6] P. Erdös and P. Turán, *On some problems of a statistical group-theory. II*, Acta Math. Acad. Sci. Hungar. **18** (1967), 151–163.

[7] P. Erdös and P. Turán, *On some problems of a statistical group-theory. III*, Acta Math. Acad. Sci. Hungar. **18** (1967), 309–320.

[8] P. Erdös and P. Turán, *On some problems of a statistical group-theory. IV*, Acta. Math. Acad. Sci. Hungar. **19** (1968), 413–435.

[9] A. Erfanián, R. Rezaei and P. Lescot, *On the relative commutativity degree of a subgroup of a finite group*, Comm. Algebra **35** (12) (2007), 4183–4197.

[10] I. V. Erovenko and B. Sury, *Commutativity degree of wreath products of finite abelian groups*, Bull. Aus. Math. Soc. **77** (1) (2008), 31–36.

[11] F. G. Frobenius, *Über Gruppencharaktere*, Gesammelte Abhandlungen Band III, p. 1–37 (J. P. Serre, ed.) Springer-Verlag, Berlin, 1968.

[12] R. M. Guralnick and G. R. Robinson, *On the commuting probability in finite groups*, J. Algebra **300** (2) (2006), 509–528.

[13] R. M. Guralnick and G. R. Robinson, *Addendum to paper "On the commuting probability in finite groups" R. M. Guralnick and G. R. Robinson [J. Algebra 300 (2) (2006), 509–528]*, J. Algebra **319** (2) (2008), 1822.

[14] W. H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034.

[15] P. Hall, *The classification of prime-power groups*, J. Reine Angew. Math. **182** (1940), 130–141.

[16] K. S. Joseph, *Commutativity in non-abelian groups*, Unpublished Ph. D. thesis, University of California, Los Angeles, 1969.

[17] P. Lescot, *Isoclinism classes and commutativity degrees of finite groups*, J. Algebra **177** (1995), 847–869.

[18] P. Lescot, *Central extensions and commutativity degree*, Comm. Algebra **29** (10) (2001), 4451–4460.

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

[20] R. K. Nath and A. K. Das, *On generalized commutativity degree of a finite group*, Rocky Mountain J. Math. (to appear).

[21] R. K. Nath and A. K. Das, *A characterization of certain finite groups of odd order*, communicated.

[22] M. R. Pournaki and R. Sobhani, *Probability that the commutator of two group elements is equal to a given element*, J. Pure Appl. Algebra **212** (2008), 727–734.

[23] D. J. Rusin, *What is the probability that two elements of a finite group commute?*, Pacific J. Math. **82** (1979), 237–247.

[24] A. Shalev, *Commutators, words, conjugacy classes and character methods*, Turk. J. Math. **31** (2007), 131–148.

COMMUTATIVITY DEGREE, ITS GENERALIZATIONS, AND CLASSIFICATION OF FINITE GROUPS

BY

RAJAT KANTI NATH
DEPARTMENT OF MATHEMATICS

SUBMITTED
IN PARTIAL FULFILMENT OF THE
REQUIREMENT OF THE DEGREE OF

DOCTOR OF PHILOSOPHY
IN
MATHEMATICS

TO

NORTH-EASTERN HILL UNIVERSITY
SHILLONG - 793022, INDIA
JULY, 2010

Dedicated to my parents

Shri Bharat Chandra Nath

&

Smt. Aloka Devi

CERTIFICATE

I certify that the thesis entitled *"Commutativity degree, its generalizations, and classification of finite groups"* submitted by Mr. Rajat Kanti Nath in partial fulfilment of the requirement of the degree of Doctor of Philosophy in Mathematics is the outcome of a study undertaken by the candidate.

I certify that the sources from which ideas have been borrowed have been duly referred to.

The material in this thesis has not been presented for the award of a degree in any university before.

This thesis may be placed before the examiners for evaluation and necessary formalities. I certify that this thesis is worthy of consideration by the examiners.

Ashish Kumar Das

Supervisor
Department of Mathematics
North-Eastern Hill University
Shillong – 793022
Email: akdas@nehu.ac.in

Place: Shillong.
20^{th} July, 2010.

DR. ASHISH KUMAR DAS
ASSOCIATE PROFESSOR
MATHEMATICS DEPARTMENT
N. E. H. U., SHILLONG - 22

NORTH-EASTERN HILL UNIVERSITY

July, 2010

DECLARATION

I, Rajat Kanti Nath, hereby declare that the subject matter in this thesis is the record of work done by me, that the contents of this thesis did not form basis of the award of any previous degree to me or to the best of my knowledge to anybody else, and that the thesis has not been submitted by me for any research degree in any other university/institute.

This thesis is being submitted to the North-Eastern Hill University for the degree of Doctor of Philosophy in Mathematics.

Rajat Kanti Nath
Signature of the Candidate

Countersigned by:

Signature of the Head

HEAD
Department of Mathematics
N.E.H.U. Permanent Campus
Shillong-793022 (Meghalaya)

Signature of the Supervisor

DR. ASHISH KUMAR DAS
ASSOCIATE PROFESSOR
MATHEMATICS DEPARTMENT
N. E. H. U., SHILLONG - 22

ACKNOWLEDGEMENT

With deep sense of gratitude I wish to express my sincere thanks to my supervisor Dr. Ashish Kumar Das for his invaluable help and excellent guidance in writing this thesis. His constructive criticism, valuable comments, constant encouragement, and sometimes, soothing scolding, are some of the memories to be cherished the whole life. I hope this is not the end but just the beginning of a lifelong collaboration. I also express my indebtedness to his mother, Smt. Swapna Das and other family members for their love and affection towards me.

I express my profound gratitude to Prof. H. K. Mukerjee, Prof. S. S. Khare, Prof. M. B. Rege, Dr. P. K. Saikia and all other faculty members of Mathematics Department, NEHU, for their help and suggestions. I am immensely fortunate to have had the pleasure of coming across them. I am also thankful to all the non-teaching stuff of the department for their helping hands during the course.

I am no less grateful to Prof. N. D. Baruah, Dr. R. Barman and all other faculty members of the Department of Mathematical Sciences, Tezpur University, and Dr. Anupam Saikia (IIT, Guwahati) for their constant encouragement.

I wish to express my appreciation to my friends Sekhar, Deepak, Bharat, Jutirekha, Sarbani, Bineeta, Sarujinee, Hera Chandra, Tikaram, Jibitesh, Mertan, Jidon, Uma, Lalit, Manas, Abhishek, Banri, Sujeet, Anup, Sourav, Kundan, Kalyanjit, Promod, Gajen, Bibhuti, Mantu, Niranjan da, Prakash *da, Guna kokai, and all my research and hostel mates, who made many valuable suggestions and gave constructive advices and made my stay here in the campus a lively one*

I am also grateful to all my relatives, well-wishers and M. Sc. class mates for their support and for being my constant source of inspiration.

It was not possible for me to work without the economic support I gratefully acknowledge the financial support provided by UGC and the facilities provided by Mathematics Department, NEHU. I am also grateful to the Computer Centre, NEHU, for allowing me to use the super computer "Param Sheersh".

I am also thankful to the GAP forum for developing such a wonderful software without which my work would not have take the present shape.

Finally, I am grateful to all my family members, especially my parents, sisters, brothers-in-law, my dear Probir and Momi, for giving me constant encouragement and providing me with unbelievable opportunities to continue my studies. I dedicate this thesis to my parents who are much happier than me on the completion of the work

Rajat Kanti Nath

PREFACE

Classification of finite groups is a central problem in theory of groups. Even though finite abelian groups have been completely classified, a lot still remains to be done as far as non-abelian groups are concerned. People all over the world have used various types of invariants for classifying finite groups, particularly the non-abelian ones. The commutativity degree of a finite group is one such invariant, and it seems that many interesting results are possible to obtain with the help of this notion and its generalizations.

In recent years there has been a growing interest in the use of the probabilistic methods in the theory of finite groups. These methods have proved useful in the solution of several difficult problems on groups. In some cases the probabilistic nature of the problem is apparent from its formulation, but in other cases the connection to probability seems surprising and can not be anticipated by the nature of the problem.

The roots of the subject matter of this thesis lie in a series of papers by P. Erdös and P. Turán (see [9, 10, 11, 12]) published between 1965 and 1968, and also in the Ph. D thesis of K. S. Joseph [26] submitted in 1969, wherein some problems of statistical group theory and commutativity in non-abelian groups have been considered. In 1973, W. H. Gustafson [22] considered the question – *what is the probability that two group elements commute?* The answer is given by what is known as the commutativity degree of a group. It may be mentioned here that the question, in some sense, was also considered by Erdös and Turán [12].

Formally, the commutativity degree of a finite group G, denoted by $\Pr(G)$, is defined as the ratio

$$\Pr(G) = \frac{\text{Number of ordered pairs } (x, y) \in G \times G \text{ such that } xy = yx}{\text{Total number of ordered pairs } (x, y) \in G \times G}.$$

In other words, commutativity degree is a kind of measure for abelianness of a group. Note that $\Pr(G) > 0$, and that $\Pr(G) = 1$ if and only if G is abelian. Also, given a finite group G, we have $\Pr(G) \leq \frac{5}{8}$ with equality if and only if $\frac{G}{Z(G)}$ has order 4 (see [2, 22]), where $Z(G)$ denotes the center of G. This gave rise to the problem of determining the numbers in the interval $(0, \frac{5}{8}]$ which can be realized as the commutativity degrees of some finite groups, and also to the problem of classifying all finite groups with a given commutativity degree.

In 1979, D. J. Rusin [44] computed, for a finite group G, the values of $\Pr(G)$ when $G' \subseteq Z(G)$, and also when $G' \cap Z(G)$ is trivial, where G' denotes the commutator subgroup of G. He determined all numbers lying in the interval $(\frac{11}{32}, 1]$ that can be realized as the commutativity degree of some finite groups, and also classified all finite groups whose commutativity degrees lie in the interval $(\frac{11}{32}, 1]$.

In 1995, P. Lescot [30] classified, up to isoclinism, all finite groups whose commutativity degrees are greater than or equal to $\frac{1}{2}$. It may be mentioned here that the concept of isoclinism between any two groups was introduced by P. Hall [23]. A pair (ϕ, ψ) is said to be an *isoclinism* from a group G to another group H if the following conditions hold:

(a) ϕ is an isomorphism from $G/Z(G)$ to $H/Z(H)$,

(b) ψ is an isomorphism from G' to H', and

(c) the diagram

$$\begin{array}{ccc} \frac{G}{Z(G)} \times \frac{G}{Z(G)} & \xrightarrow{\phi \times \phi} & \frac{H}{Z(H)} \times \frac{H}{Z(H)} \\ \Big\downarrow a_G & & \Big\downarrow a_H \\ G' & \xrightarrow{\psi} & H' \end{array}$$

commutes, that is, $a_H \circ (\phi \times \phi) = \psi \circ a_G$, where a_G and a_H are given respectively by $a_G(g_1Z(G), g_2Z(G)) = [g_1, g_2]$ for all $g_1, g_2 \in G$ and $a_H(h_1Z(H), h_2Z(H)) = [h_1, h_2]$ for all $h_1, h_2 \in H$. Here, given $x, y \in G$, $[x, y]$ stands for the commutator $xyx^{-1}y^{-1}$ of x and y in G.

In 2001, Lescot [31] has also classified, up to isomorphism, all finite groups whose commutativity degrees lie in the interval $[\frac{1}{2}, 1]$.

In 2006, F. Barry, D. MacHale and Á. Ní Shé [1] have shown that if G is a finite group with $|G|$ odd and $\Pr(G) > \frac{11}{75}$, then G is supersolvable. They also proved that if $\Pr(G) > \frac{1}{3}$, then G is supersolvable. It may be mentioned here that a group G is said to be *supersolvable* if there is a series of the form

$$\{1\} = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_r = G,$$

where $A_i \trianglelefteq G$ and A_{i+1}/A_i is cyclic for each i with $0 \leq i \leq r-1$.

In the same year 2006, R. M. Guralnick and G. R. Robinson [20] re-established a result of Lescot (see [21]) which says that if G is a finite group with $\Pr(G)$ greater than $\frac{3}{40}$, then either G is solvable, or $G \cong A_5 \times B$, where A_5 is the alternating group of degree 5 and B is some abelian group.

The classical notion of commutativity degree has been generalized in a number of ways. In 2007, A. Erfanian, R. Rezaei and P. Lescot [13] studied the probability $\Pr(H, G)$ that an element of a given subgroup H of a finite group G commutes with an element of G. Note that $\Pr(G, G) = \Pr(G)$. In 2008, M. R. Pournaki and R. Sobhani [40] studied the probability $\Pr_g(G)$ that the commutator of an arbitrarily chosen pair of elements in a finite group G equals a given group element g. They have also extended some of the results obtained by Rusin. It is easy to see that $\Pr_g(G) = \Pr(G)$ if $g = 1$, the identity element of G.

In Chapter 1, we briefly recall a few definitions and well-known results from several relevant topics, which constitute the minimum prerequisites for the subsequent chapters. In this chapter, we also fix certain notations. Given a subgroup K of a group G and an element $x \in G$, we write $C_K(x)$ and $C\ell_K(x)$ to denote the sets $\{k \in K : kx = xk\}$ and $\{kxk^{-1} \in G : k \in K\}$ respectively; noting that, for $K = G$, these sets coincide respectively with the centralizer and the conjugacy class of x in G. Also, given any two subgroups H and K of a group G, we write $C_K(H) = \{k \in K : hk = kh \text{ for all } h \in H\}$. Note that $C_K(x) = C_K(\langle x \rangle)$, where $\langle x \rangle$ denotes the cyclic subgroup of G generated by $x \in G$.

Further, we write $\mathrm{Irr}(G)$ to denote the set of all irreducible complex characters of G, and $\mathrm{cd}(G)$ to denote the set $\{\chi(1) : \chi \in \mathrm{Irr}(G)\}$. If $\chi(1) = |G : Z(G)|^{1/2}$ for some $\chi \in \mathrm{Irr}(G)$, then the group G is said to be of *central type*.

In Chapter 2, which is based on our papers [37] and [39], we determine, for a finite group G, the value of $\Pr(G)$ and the size of $\frac{G}{Z(G)}$ when $|G'| = p^2$ and $|G' \cap Z(G)| = p$, where p is a prime such that $\gcd(p-1, |G|) = 1$. The main result of Section 2.2 is given as follows.

Theorem 2.2.6. *Let G be a finite group and p be a prime such that $\gcd(p-1, |G|) = 1$. If $|G'| = p^2$ and $|G' \cap Z(G)| = p$, then*

$$\text{(a)}\ \Pr(G) = \begin{cases} \frac{2p^2-1}{p^4} & \text{if } C_G(G') \text{ is abelian} \\ \frac{1}{p^4}\left(\frac{p-1}{p^{2s-1}} + p^2 + p - 1\right) & \text{otherwise,} \end{cases}$$

$$\text{(b)}\ \left|\frac{G}{Z(G)}\right| = \begin{cases} p^3 & \text{if } C_G(G') \text{ is abelian} \\ p^{2s+2} \text{ or } p^{2s+3} & \text{otherwise,} \end{cases}$$

where $p^{2s} = |C_G(G') : Z(C_G(G'))|$. Moreover,

$$\left|\frac{G}{G' \cap Z(G)} : Z\left(\frac{G}{G' \cap Z(G)}\right)\right| = \left|\frac{G}{Z(G)} : Z\left(\frac{G}{Z(G)}\right)\right| = p^2.$$

This theorem together with few other supplementary results, enable us to classify all finite groups G of odd order with $\Pr(G) \geq \frac{11}{75}$. In the process we also point out a few small but significant lacunae in the work of Rusin [44]. The main result of Section 2.3 is given as follows.

Theorem 2.3.3. *Let G be a finite group. If $|G|$ is odd and $\Pr(G) \geq \frac{11}{75}$, then the possible values of $\Pr(G)$ and the corresponding structures of G', $G' \cap Z(G)$ and $G/Z(G)$ are given as follows:*

$\Pr(G)$	G'	$G' \cap Z(G)$	$G/Z(G)$
1	$\{1\}$	$\{1\}$	$\{1\}$
$\frac{1}{3}(1+\frac{2}{3^{2s}})$	C_3	C_3	$(C_3 \times C_3)^s,\ s \geq 1$
$\frac{1}{5}(1+\frac{4}{5^{2s}})$	C_5	C_5	$(C_5 \times C_5)^s,\ s \geq 1$
$\frac{5}{21}$	C_7	$\{1\}$	$C_7 \rtimes C_3$
$\frac{55}{343}$	C_7	C_7	$C_7 \times C_7$
$\frac{17}{81}$	C_9 *or* $C_3 \times C_3$	C_3	$(C_3 \times C_3) \rtimes C_3$
	$C_3 \times C_3$	$C_3 \times C_3$	C_3^3
$\frac{121}{729}$	$C_3 \times C_3$	$C_3 \times C_3$	C_3^4
$\frac{7}{39}$	C_{13}	$\{1\}$	$C_{13} \rtimes C_3$
$\frac{3}{19}$	C_{19}	$\{1\}$	$C_{19} \rtimes C_3$
$\frac{29}{189}$	C_{21}	C_3	$C_3 \times (C_7 \rtimes C_3)$
$\frac{11}{75}$	$C_5 \times C_5$	$\{1\}$	$(C_5 \times C_5) \rtimes C_3$

In the above table C_n denotes the cyclic group of order n and $\rtimes$ stands for semidirect product.

In [40, Corollary 2.3], M. R. Pournaki and R. Sobhani have proved that, for a finite group G satisfying $|\operatorname{cd}(G)| = 2$, one has

$$\Pr(G) \geq \frac{1}{|G'|}\left(1 + \frac{|G'|-1}{|G : Z(G)|}\right)$$

with equality if and only if G is of central type. In Section 2.4, we have improved this result as follows.

Theorem 2.4.1. *If G is a finite group, then*

$$\Pr(G) \geq \frac{1}{|G'|}\left(1 + \frac{|G'|-1}{|G:Z(G)|}\right).$$

In particular, $\Pr(G) > \frac{1}{|G'|}$ *if G is non-abelian.*

There are several equivalent conditions that are necessary as well as sufficient for the attainment of the above lower bound for $\Pr(G)$.

Theorem 2.4.3. *For a finite non-abelian group G, the statements given below are equivalent.*

(a) $\Pr(G) = \dfrac{1}{|G'|}\left(1 + \dfrac{|G'|-1}{|G:Z(G)|}\right)$.

(b) $\mathrm{cd}(G) = \{1, |G:Z(G)|^{1/2}\}$, *which means that G is of central type with* $|\,\mathrm{cd}(G)| = 2$.

(c) $|\,\mathrm{C}\ell_G(x)| = |G'|$ *for all* $x \in G - Z(G)$.

(d) $\mathrm{C}\ell_G(x) = G'x$ *for all* $x \in G - Z(G)$*; in particular, G is a nilpotent group of class* 2.

(e) $C_G(x) \trianglelefteq G$ *and* $G' \cong \frac{G}{C_G(x)}$ *for all* $x \in G - Z(G)$*; in particular, G is a CN-group, that is, the centralizer of every element is normal.*

(f) $G' = \{[y,x] : y \in G\}$ *for all* $x \in G - Z(G)$*; in particular, every element of G' is a commutator.*

Theorem 2.4.1 and Theorem 2.4.3 not only allow us to obtain some characterizations for finite nilpotent groups of class 2 whose commutator subgroups have prime order, but also enable us to re-establish certain facts (essentially due to K. S. Joseph [26]) concerning the smallest prime divisors of the orders of finite groups.

Proposition 2.4.4. *Let G be a finite group and p be the smallest prime divisor of $|G|$.*

(a) *If $p \neq 2$, then $\Pr(G) \neq \frac{1}{p}$.*

(b) *When G is non-abelian, $\Pr(G) > \frac{1}{p}$ if and only if $|G'| = p$ and $G' \subseteq Z(G)$.*

Corrolary 2.4.5. *If G is a finite group with $\Pr(G) = \frac{1}{3}$, then $|G|$ is even.*

Proposition 2.4.7. *Let G be a finite group and p be a prime. Then the following statements are equivalent.*

(a) *$|G'| = p$ and $G' \subseteq Z(G)$.*

(b) *G is of central type with $|\operatorname{cd}(G)| = 2$ and $|G'| = p$.*

(c) *G is a direct product of a p-group P and an abelian group A such that $|P'| = p$ and $\gcd(p, |A|) = 1$.*

(d) *G is isoclinic to an extra-special p-group; consequently, $|G : Z(G)| = p^{2k}$ for some positive integer k.*

In particular, if G is non-abelian and p is the smallest prime divisor of $|G|$, then the above statements are also equivalent to the condition $\Pr(G) > \frac{1}{p}$.

In [31], Lescot deduced that $\Pr(D_{2n}) \longrightarrow \frac{1}{4}$ and $\Pr(Q_{2^{n+1}}) \longrightarrow \frac{1}{4}$ as $n \longrightarrow \infty$, where D_{2n} and $Q_{2^{n+1}}$ denote the dihedral group of order $2n$, $n \geq 1$, and the quaternion group of order 2^{n+1}, $n \geq 2$, respectively. He also enquired whether there are other natural families of finite groups with the same property. In 2007, I. V. Erovenko and B. Sury [16] have shown, in particular, that for every integer $k > 1$ there exists a family $\{G_n\}$ of finite groups such that $\Pr(G_n) \to \frac{1}{k^2}$ as $n \to \infty$. In the last section of Chapter 2 we have considered the question posed by Lescot mentioned above. Moreover, we make the following observation.

Proposition 2.5.1. *For every integer $k > 1$ there exists a family $\{G_n\}$ of finite groups such that $\Pr(G_n) \to \frac{1}{k}$ as $n \to \infty$.*

In the same line, we also have the following result.

Proposition 2.5.2. *For every positive integer n there exists a finite group G such that $\Pr(G) = \frac{1}{n}$.*

In Chapter 3, which is based on our papers [5] and [6], we generalize the following result of F. G. Frobenius [18]:

If G is a finite group and $g \in G$, then the number of solutions of the commutator equation $xyx^{-1}y^{-1} = g$ in G defines a character on G, and is given by

$$\zeta(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|}{\chi(1)} \chi(g).$$

We write $F(x_1, x_2, \ldots, x_n)$ to denote the free group of words on n generators $x_1, x_2, \ldots, x_n$. For $1 \leq i \leq n$, we write '$x_i \in \omega(x_1, x_2, \ldots, x_n)$' to mean that x_i has a non-zero index (that is, x_i^k forms a syllable, with $0 \neq k \in \mathbb{Z}$) in the word $\omega(x_1, x_2, \ldots, x_n) \in F(x_1, x_2, \ldots, x_n)$. We call a word $\omega(x_1, x_2, \ldots, x_n)$ *admissible* if each $x_i \in \omega(x_1, x_2, \ldots, x_n)$ has precisely two non-zero indices, namely, $+1$ and -1. We write $\mathscr{A}(x_1, x_2, \ldots, x_n)$ to denote the set of all admissible words in $F(x_1, x_2, \ldots, x_n)$.

Given a finite group G and an element $g \in G$, let $\zeta_n^{\omega}(g)$ denote the number of solutions $(g_1, g_2, \ldots, g_n) \in G^n$ of the word equation $\omega(x_1, x_2, \ldots, x_n) = g$, where $G^n = G \times G \times \cdots \times G$ (n times). Thus,

$$\zeta_n^{\omega}(g) = |\{(g_1, g_2, \ldots, g_n) \in G^n : \omega(g_1, g_2, \ldots, g_n) = g\}|.$$

The main result of Section 3.1 is given as follows.

Theorem 3.1.4. *Let $\omega(x_1, x_2, \ldots, x_n) \in \mathscr{A}(x_1, x_2, \ldots, x_n)$, $n \geq 1$. If G is a finite group, then the map $\zeta_n^{\omega} : G \longrightarrow \mathbb{C}$ defined by*

$$\zeta_n^{\omega}(g) = |\{(g_1, g_2, \ldots, g_n) \in G^n : \omega(g_1, g_2, \ldots, g_n) = g\}|, \quad g \in G,$$

is a character of G.

Given any two finite sets X and Y, a function $f : X \longrightarrow Y$ is said to be *almost measure preserving* if there exists a sufficiently small positive real number ϵ such that

$$\left| \frac{|f^{-1}(Y_0)|}{|X|} - \frac{|Y_0|}{|Y|} \right| < \epsilon \quad \text{for all } Y_0 \subseteq Y.$$

In Section 3.2, we consider the following question posed by Aner Shalev [46, Problem 2.10]:

Which words induce almost measure preserving maps on finite simple groups?

More precisely, given an admissible word $\omega(x_1, x_2, \ldots, x_n)$ and the induced word map $\alpha_\omega : G^n \to G$ defined by $\alpha_\omega(g_1, g_2, \ldots, g_n) = \omega(g_1, g_2, \ldots, g_n)$, we proved that

Corollary 3.2.7. *Let G be a finite simple group, and $o(1)$ be a real number depending on G which tends to zero as $|G| \to \infty$.*

(a) *If* $Y \subseteq G$, *then* $\frac{|(\alpha_\omega)^{-1}(Y)|}{|G|^n} = \frac{|Y|}{|G|} + o(1)$. *This means that the map* α_ω *is almost measure preserving.*

(b) *If* $X \subseteq G^n$, *then* $\frac{|\alpha_\omega(X)|}{|G|} \geq \frac{|X|}{|G|^n} - o(1)$; *in particular, if* X *is such that* $|X| = (1 - o(1))|G|^n$, *then* $|\alpha_\omega(X)| = (1 - o(1))|G|$. *This means that almost all the elements of* G *can be expressed as* $\omega(g_1, g_2, \ldots, g_n)$ *for some* $g_1, g_2, \ldots, g_n \in G$.

In the last section of Chapter 3, we obtain yet another generalization of Frobenius' result mentioned above. The main results of this section are given as follows.

Theorem 3.3.1. *Let* G *be a finite group,* $H \trianglelefteq G$ *and* $g \in G$. *If* $\tilde{\zeta}(g)$ *denotes the number of elements* $(h_1, g_2) \in H \times G$ *satisfying* $[h_1, g_2] = g$, *then* $\tilde{\zeta}$ *is a class function of* G *and*

$$\tilde{\zeta}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|H|[\chi_H, \chi_H]}{\chi(1)} \chi(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|H|[\chi_H^G, \chi]}{\chi(1)} \chi(g).$$

Corollary 3.3.2. *Let* G *be a finite group. Then, with notations as above,* $\tilde{\zeta}$ *is a character of* G.

Proposition 3.3.3. *Let* G *be a finite group,* $H \trianglelefteq G$ *and* $g \in G$. *If* $\tilde{\zeta}_{2n}(g)$, $n \geq 1$, *denotes the number of elements* $((h_1, g_1), \ldots, (h_n, g_n)) \in (H \times G)^n$ *satisfying* $[h_1, g_1] \ldots [h_n, g_n] = g$, *then* $\tilde{\zeta}_{2n}$ *is a character of* G *and*

$$\tilde{\zeta}_{2n}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|^{n-1}|H|^n[\chi_H, \chi_H]^n}{\chi(1)^{2n-1}} \chi(g).$$

Proposition 3.3.4. *Let H be a subgroup of a finite group G and $g \in G$. Then the number of elements $(g_1, h_2, g_3) \in G \times H \times G$ satisfying $g_1 h_2 g_1^{-1} g_3 h_2^{-1} g_3^{-1} = g$ defines a character of G and is given by*

$$\tilde{\zeta}_3(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G||H|[\chi_H, \chi_H]}{\chi(1)} \chi(g).$$

In Chapter 4, which is based on our paper [38], we study the probability $\mathrm{Pr}_g^{\omega}(G)$ that an arbitrarily chosen n-tuple of elements of a given finite group G is mapped to a given group element g under the word map induced by a non-trivial admissible word $\omega(x_1, x_2, \ldots, x_n)$. Formally, we write

$$\mathrm{Pr}_g^{\omega}(G) = \frac{\zeta_n^{\omega}(g)}{|G^n|},$$

where $\zeta_n^{\omega}(g) = |\{(g_1, g_2, \ldots, g_n) \in G^n : \omega(g_1, g_2, \ldots, g_n) = g\}|$. The main results of Section 4.1 are as follows.

Proposition 4.1.1. *Let G be a finite group and $\omega(x_1, x_2, \ldots, x_n)$ be a non-trivial admissible word. Then*

(a) $\mathrm{Pr}_1^{\omega}(G) \geq \dfrac{n|G : Z(G)| - n + 1}{|G : Z(G)|^n} \geq \dfrac{1}{|G : Z(G)|^n} \gneq 0$,

(b) $\mathrm{Pr}_1^{\omega}(G) = 1$ *if and only if* G *is abelian.*

Proposition 4.1.3. *Let G and H be two finite groups and (ϕ, ψ) be an isoclinism from G to H. If $g \in G'$ and $\omega(x_1, x_2, \ldots, x_n)$ is a non-trivial admissible word, then*

$$\mathrm{Pr}_g^{\omega}(G) = \mathrm{Pr}_{\psi(g)}^{\omega}(H).$$

Proposition 4.1.4. *Let G be a finite group and $\omega(x_1, x_2, \ldots, x_n)$ be a non-trivial admissible word. If $g, h \in G'$ generate the same cyclic subgroup of G, then* $\Pr_g^{\omega}(G) = \Pr_h^{\omega}(G)$.

Proposition 4.1.6. *Let G be a finite group, $g \in G'$ and $\omega(x_1, x_2, \ldots, x_n)$ be a non-trivial admissible word. Then*

(a) $\Pr_g^{\omega}(G) \leq \Pr_1^{\omega}(G) \leq \Pr(G)$,

(b) $\Pr_g^{\omega}(G) = \Pr_1^{\omega}(G)$ *if and only if* $g = 1$.

Let $m_G = \min\{\chi(1) : \chi \in \mathrm{Irr}(G), \chi(1) \neq 1\}$. Considering, in particular, the word $x_1 x_2 \ldots x_n x_1^{-1} x_2^{-1} \ldots x_n^{-1}$, $n \geq 2$, and writing $\Pr_g^n(G)$ in place of $\Pr_g^{\omega}(G)$, we obtain the following results in the sections 4.2, 4.3 and 4.4.

Proposition 4.2.2. *Let G be a finite non-abelian group, $g \in G'$ and d be an integer such that $2 \leq d \leq m_G$. Then*

(a) $\left|\Pr_g^n(G) - \frac{1}{|G'|}\right| \leq \frac{1}{d^{n-2}}\left(\Pr(G) - \frac{1}{|G'|}\right)$. *In other words,*

$$\frac{1}{d^{n-2}}\left(-\Pr(G) + \frac{d^{n-2}+1}{|G'|}\right) \leq \Pr_g^n(G) \leq \frac{1}{d^{n-2}}\left(\Pr(G) + \frac{d^{n-2}-1}{|G'|}\right).$$

(b) $\left|\Pr_g^n(G) - \frac{1}{|G'|}\right| \leq \frac{1}{d^n}\left(1 - \frac{1}{|G'|}\right)$. *In other words,*

$$\frac{1}{d^n}\left(-1 + \frac{d^n+1}{|G'|}\right) \leq \Pr_g^n(G) \leq \frac{1}{d^n}\left(1 + \frac{d^n-1}{|G'|}\right).$$

In particular, $\Pr_g^n(G) \leq \frac{2^n+1}{2^{n+1}}$.

Proposition 4.2.3. *If G is a finite non-abelian simple group and $g \in G'$, then*

$$\left|\Pr_g^n(G) - \frac{1}{|G|}\right| \leq \frac{1}{3^{n-2}}\left(\frac{1}{12} - \frac{1}{|G|}\right).$$

In other words,

$$\frac{1}{3^{n-2}}\left(\frac{-1}{12} + \frac{3^{n-2}+1}{|G|}\right) \leq \Pr_g^n(G) \leq \frac{1}{3^{n-2}}\left(\frac{1}{12} + \frac{3^{n-2}-1}{|G|}\right).$$

In particular,

$$\Pr_g^n(G) \leq \frac{3^{n-2}+4}{3^{n-1} \times 20}.$$

Corollary 4.3.2. *Let G be a finite non-abelian group with $|\operatorname{cd}(G)| = 2$. Then every element of G' is a generalized commutator of length n for all $n \geq 2$; in particular, every element of G' is a commutator.*

Proposition 4.3.3. *Let G be a finite non-abelian group, $g \in G'$ and d be an integer such that $2 \leq d \leq m_G$. Then*

(a) $\Pr_g^n(G) = \dfrac{1}{d^{n-2}}\left(\Pr(G) + \dfrac{d^{n-2}-1}{|G'|}\right)$ *if and only if* $g = 1$ *and* $\operatorname{cd}(G) = \{1, d\}$.

(b) $\Pr_g^n(G) = \dfrac{1}{d^{n-2}}\left(-\Pr(G) + \dfrac{d^{n-2}+1}{|G'|}\right)$ *if and only if* $g \neq 1$, $\operatorname{cd}(G) = \{1, d\}$ *and* $|G'| = 2$.

Proposition 4.3.4. *Let G be a finite non-abelian group, $g \in G'$ and d be an integer such that $2 \leq d \leq m_G$. Then*

(a) $\Pr_g^n(G) = \dfrac{1}{d^n}\left(1 + \dfrac{d^n-1}{|G'|}\right)$ *if and only if* $g = 1$ *and* $\operatorname{cd}(G) = \{1, d\}$.

(b) $\Pr_g^n(G) = \frac{1}{d^n}\left(-1 + \frac{d^n+1}{|G'|}\right)$ *if and only if* $g \neq 1$, $\mathrm{cd}(G) = \{1, d\}$ *and* $|G'| = 2$.

Proposition 4.3.7. *Let G be a finite non-abelian group, $g \in G'$ and p be the smallest prime divisor of $|G|$. Then*

$$\Pr_g^n(G) = \frac{p^n + p - 1}{p^{n+1}}$$

if and only if $g = 1$, *and G is isoclinic to*

$$\langle x, y \,:\, x^{p^2} = 1 = y^p,\ y^{-1}xy = x^{p+1}\rangle.$$

In particular, putting $p = 2$, $\Pr_g^n(G) = \frac{2^n+1}{2^{n+1}}$ if and only if $g = 1$, and G is isoclinic to D_8, the dihedral group, and hence, to Q_8, the group of quaternions.

Proposition 4.4.1. *Let G be a finite non-abelian group with $|\mathrm{cd}(G)| = 2$ and $g \in G'$. Then*

$$\Pr_1^n(G) \geq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{|G : Z(G)|^{n/2}}\right) \quad \textit{and}$$
$$\Pr_g^n(G) \leq \frac{1}{|G'|}\left(1 - \frac{1}{|G : Z(G)|^{n/2}}\right) \quad \textit{if } g \neq 1.$$

Moreover, in each case, the equality holds if and only if G is of central type.

Corollary 4.4.2. *Let G be a finite non-abelian group and $g \in G'$. If G is of central type with $|\mathrm{cd}(G)| = 2$, then*

$$\Pr_1^n(G) \leq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{2^n}\right) \quad \textit{and}$$
$$\Pr_g^n(G) \geq \frac{1}{|G'|}\left(1 - \frac{1}{2^n}\right) \quad \textit{if } g \neq 1.$$

Proposition 4.4.3. *Let G be a finite non-abelian group and $g \in G'$. If $G' \subseteq Z(G)$ and $|G'| = p$, where p is a prime, then*

$$\Pr_g^n(G) = \begin{cases} \frac{1}{p}\left(1 + \frac{p-1}{p^{nk}}\right) & \text{if } g = 1 \\ \frac{1}{p}\left(1 - \frac{1}{p^{nk}}\right) & \text{if } g \neq 1, \end{cases}$$

where $k = \dfrac{1}{2}\log_p |G : Z(G)|$.

Proposition 4.4.5. *Let p be a prime. Let r and s be two positive integers such that $s \mid (p-1)$, and $r^j \equiv 1 \pmod p$ if and only if $s \mid j$. If $G = \langle a, b : a^p = b^s = 1, bab^{-1} = a^r \rangle$ and $g \in G'$, then*

$$\Pr_g^n(G) = \begin{cases} \dfrac{s^n + p - 1}{ps^n} & \text{if } g = 1 \\ \dfrac{s^n - 1}{ps^n} & \text{if } g \neq 1. \end{cases}$$

Proposition 4.4.6. *Let G be a finite non-abelian group and $g \in G'$. If $G' \cap Z(G) = \{1\}$ and $|G'| = p$, where p is a prime, then*

(a) *G is isoclinic to the group $\langle a, b : a^p = b^s = 1, bab^{-1} = a^r \rangle$, where $s \mid (p-1)$, and $r^j \equiv 1 \pmod p$ if and only if $s \mid j$,*

(b) $$\Pr_g^n(G) = \begin{cases} \dfrac{s^n + p - 1}{ps^n} & \text{if } g = 1 \\ \dfrac{s^n - 1}{ps^n} & \text{if } g \neq 1. \end{cases}$$

Proposition 4.4.7. *Let G be a finite non-abelian group and $g \in G'$. If $g \neq 1$, then $\Pr_g^n(G) < \frac{1}{p}$, where p is the smallest prime divisor of $|G|$. In particular, we have $\Pr_g^n(G) < \frac{1}{2}$.*

Proposition 4.4.8. *For each $\varepsilon > 0$ and for each prime p, there exists a finite group G such that*

$$\left|\Pr_g^n(G) - \frac{1}{p}\right| < \varepsilon$$

for all $g \in G'$.

Let G be a finite group and $g \in G'$. Let H and K be two subgroups of G. In Chapter 5, which is based on our paper [6], we study the probability $\Pr_g(H, K)$ that the commutator of a randomly chosen pair of elements (one from H and the other from K) equals g. In other words, we study the ratio

$$\Pr_g(H, K) = \frac{|\{(x, y) \in H \times K : [x, y] = g\}|}{|H||K|},$$

and further extend some of the results obtained in [13] and [40]. Without any loss, we may assume that G is non-abelian. The main results of the sections 5.1 and 5.2 are as follows.

Proposition 5.1.1. *Let G be a finite group and $g \in G'$. If H and K are two subgroups of G, then $\Pr_g(H, K) = \Pr_{g^{-1}}(K, H)$. However, if $g^2 = 1$, or if $g \in H \cup K$ (for example, when H or K is normal in G), we have $\Pr_g(H, K) = \Pr_g(K, H) = \Pr_{g^{-1}}(H, K)$.*

Theorem 5.1.3. *Let G be a finite group and $g \in G'$. If H and K are two subgroups of G, then*

$$\Pr_g(H, K) = \frac{1}{|H||K|} \sum_{\substack{x \in H \\ g^{-1}x \in C\ell_K(x)}} |C_K(x)| = \frac{1}{|H|} \sum_{\substack{x \in H \\ g^{-1}x \in C\ell_K(x)}} \frac{1}{|C\ell_K(x)|},$$

where $C_K(x) = \{y \in K : xy = yx\}$ and $C\ell_K(x) = \{yxy^{-1} : y \in K\}$, the K-conjugacy class of x.

This theorem plays a key role in the study of $\Pr_g(H, K)$. As an immediate consequence, we have the following generalization of the well-known formula $\Pr(G) = \frac{k(G)}{|G|}$.

Corollary 5.1.4. *Let G be a finite group and H, K be two subgroups of G. If $H \trianglelefteq G$, then*

$$\Pr(H, K) = \frac{k_K(H)}{|H|},$$

where $k_K(H)$ is the number of K-conjugacy classes that constitute H.

Proposition 5.1.5. *If H is an abelian normal subgroup of a finite group G with a complement K in G and $g \in G'$, then*

$$\Pr_g(H, G) = \Pr_g(H, K).$$

Corollary 5.1.6. *Let G be a finite group and $g \in G'$. If $H \trianglelefteq G$ with $C_G(x) = H$ for all $x \in H - \{1\}$, then*

$$\Pr_g(H, G) = \Pr_g(H, K),$$

where K is a complement of H in G. In particular,

$$\Pr(H, G) = \frac{1}{|H|} + \frac{|H| - 1}{|G|}.$$

Proposition 5.2.1. *Let G be a finite group and $g \in G'$. Let H and K be any two subgroups of G. If $g \neq 1$, then*

(a) $\Pr_g(H, K) \neq 0 \Longrightarrow \Pr_g(H, K) \geq \dfrac{|C_H(K)||C_K(H)|}{|H||K|}$,

(b) $\Pr_g(H,G) \neq 0 \Longrightarrow \Pr_g(H,G) \geq \dfrac{2|H \cap Z(G)||C_G(H)|}{|H||G|}$,

(c) $\Pr_g(G) \neq 0 \Longrightarrow \Pr_g(G) \geq \dfrac{3}{|G : Z(G)|^2}$.

Proposition 5.2.2. *Let G be a finite group and $g \in G'$. If H and K are any two subgroups of G, then*

$$\Pr_g(H,K) \leq \Pr(H,K)$$

with equality if and only if $g = 1$.

Proposition 5.2.3. *Let G be a finite group and $g \in G'$, $g \neq 1$. Let H and K be any two subgroups of G. If p is the smallest prime divisor of $|G|$, then*

$$\Pr_g(H,K) \leq \frac{|H| - |C_H(K)|}{p|H|} < \frac{1}{p}.$$

Proposition 5.2.4. *Let H, K_1 and K_2 be subgroups of a finite group G with $K_1 \subseteq K_2$. Then*

$$\Pr(H,K_1) \geq \Pr(H,K_2)$$

with equality if and only if $C\ell_{K_1}(x) = C\ell_{K_2}(x)$ *for all $x \in H$.*

Proposition 5.2.5. *Let H, K_1 and K_2 be subgroups of a finite group G with $K_1 \subseteq K_2$. Then*

$$\Pr(H,K_2) \geq \frac{1}{|K_2 : K_1|}\left(\Pr(H,K_1) + \frac{|K_2| - |K_1|}{|H||K_1|}\right)$$

with equality if and only if $C_H(x) = \{1\}$ *for all $x \in K_2 - K_1$.*

Proposition 5.2.6. *Let $H_1 \subseteq H_2$ and $K_1 \subseteq K_2$ be subgroups of a finite group G and $g \in G'$. Then*

$$\Pr_g(H_1,K_1) \leq |H_2 : H_1||K_2 : K_1|\Pr_g(H_2,K_2)$$

with equality if and only if

$$\begin{aligned} &g^{-1}x \notin \mathrm{C}\ell_{K_2}(x) \ \ \textit{for all} \ \ x \in H_2 - H_1, \\ &g^{-1}x \notin \mathrm{C}\ell_{K_2}(x) - \mathrm{C}\ell_{K_1}(x) \ \ \textit{for all} \ \ x \in H_1, \\ \textit{and} \quad &C_{K_1}(x) = C_{K_2}(x) \ \ \textit{for all} \ \ x \in H_1 \ \ \textit{with} \ \ g^{-1}x \in \mathrm{C}\ell_{K_1}(x). \end{aligned}$$

In particular, for $g = 1$*, the condition for equality reduces to* $H_1 = H_2$*, and* $K_1 = K_2$.

Corollary 5.2.7. *Let* G *be a finite group,* H *be a subgroup of* G *and* $g \in G'$*. Then*

$$\Pr_g(H, G) \leq |G : H| \Pr(G)$$

with equality if and only if $g = 1$ *and* $H = G$.

Theorem 5.2.8. *Let* G *be a finite group and* p *be the smallest prime dividing* $|G|$*. If* H *and* K *are any two subgroups of* G*, then*

$$\begin{aligned} \Pr(H, K) &\geq \frac{|C_H(K)|}{|H|} + \frac{p(|H| - |X_H| - |C_H(K)|) + |X_H|}{|H||K|} \\ \textit{and} \ \ \Pr(H, K) &\leq \frac{(p-1)|C_H(K)| + |H|}{p|H|} - \frac{|X_H|(|K| - p)}{p|H||K|}, \end{aligned}$$

where $X_H = \{x \in H : C_K(x) = 1\}$*. Moreover, in each of these bounds,* H *and* K *can be interchanged.*

Corollary 5.2.9. *Let* G *be a finite group and* p *be the smallest prime dividing* $|G|$*. If* H *and* K *are two subgroups of* G *such that* $[H, K] \neq \{1\}$*, then*

$$\Pr(H, K) \leq \frac{2p - 1}{p^2}.$$

In particular, $\Pr(H, K) \leq \frac{3}{4}$.

Proposition 5.2.10. *Let G be a finite group and H, K be any two subgroups of G. If $\Pr(H, K) = \frac{2p-1}{p^2}$ for some prime p, then p divides $|G|$. If p happens to be the smallest prime divisor of $|G|$, then*

$$\frac{H}{C_H(K)} \cong C_p \cong \frac{K}{C_K(H)}, \quad \textit{and hence,} \quad H \neq K.$$

In particular, $\frac{H}{C_H(K)} \cong C_2 \cong \frac{K}{C_K(H)}$ if $\Pr(H, K) = \frac{3}{4}$.

In the last section of chapter 5, with H normal in G, we also develop and study a character theoretic formula for $\Pr_g(H, G)$ given by

$$\Pr_g(H, G) = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{[\chi_H, \chi_H]}{\chi(1)} \chi(g).$$

Proposition 5.3.1. *Let G be a finite group. If H is a normal subgroup of G and $g \in G'$, then*

$$\left| \Pr_g(H, G) - \frac{1}{|G'|} \right| \leq |G : H| \left(\Pr(G) - \frac{1}{|G'|} \right).$$

As an application, we obtain yet another condition under which every element of G' is a commutator.

Proposition 5.3.3. *Let G be a finite group and p be the smallest prime dividing $|G|$. If $|G'| \leq p^2$, then every element of G' is a commutator.*

We conclude the thesis with a discussion, in the last chapter, on some of the possible research problems related to the results obtained in the earlier chapters.

Contents

List of Symbols

$\mathbb{Z}$	set of all integers
$\mathbb{C}$	set of all complex numbers
$H \leq G$	H is a subgroup of G
$H \trianglelefteq G$	H is a normal subgroup of G
$\|G : H\|$	index of H in G
G/N	quotient group of G by N
HK	$\{hk \,:\, h \in H,\ k \in K\}$
$H \times K$	direct product of the groups H and K
G^n	direct product of n copies of G
$H \rtimes K$	semidirect product of the groups H and K
aH	$\{ah \,:\, h \in H\}$, left coset of H
$G \cong H$	G and H are isomorphic
$\langle a \rangle$	the cyclic group generated by a
$\langle g_1, g_2, \cdots, g_n \rangle$	subgroup generated by $g_1, g_2, \cdots, g_n$
$o(g)$	order of a group element g
$\|G\|$	order of the group G
$[x, y]$	$xyx^{-1}y^{-1}$, the commutator of x and y
$[H, K]$	$\langle \{[x, y] \,:\, x \in H, y \in K\} \rangle$
G'	the commutator subgroup of G
y^g	gyg^{-1}
$C\ell_G(g)$	conjugacy class of g in G

$Z(G)$	center of the group G
$C_G(x)$	centralizer of x in G
$C_K(H)$	$\{k \in K : hk = kh \text{ for all } h \in H\}$
$k(G)$	number of conjugacy classes of G
$\text{orb}(x)$	orbit of x
$\text{stab}(x)$	stabilizer of x
$\text{Aut}(G)$	automorphism group of G
$N_G(H)$	normalizer of H in G
$\text{Irr}(G)$	set of all irreducible characters of G
$\text{Lin}(G)$	set of all linear characters of G
$\text{cd}(G)$	$\{\chi(1) : \chi \in \text{Irr}(G)\}$
$\ker \chi$	$\{g \in G : \chi(g) = \chi(1)\}$
C_n	cyclic group of order n
D_{2n}	dihedral group of order $2n$
Q_{2^n}	quaternion group of order 2^n
S_n	symmetric group of degree n
A_n	alternating group of degree n
$GL(n, \mathbb{F})$	group of all $n \times n$ non-singular matrices over the field $\mathbb{F}$
$M_n(\mathbb{F})$	algebra of all $n \times n$ matrices over $\mathbb{F}$
$\mathbb{F}[G]$	group algebra of G over $\mathbb{F}$
δ_{ij}	Kronecker delta function

Chapter 1

Preliminaries

In this chapter we briefly recall a few definitions and well-known results, some of which are pinpointed as per our requirements, and fix certain notations. All these constitute the minimum prerequisites for the forthcoming chapters.

1.1 Some topics from the theory of groups

Let G be a group with *center* $Z(G) = \{x \in G : xy = yx \text{ for all } y \in G\}$. If $x \in G$, then the *centralizer* and the *conjugacy class* of x in G are given by $C_G(x) = \{y \in G : xy = yx\}$ and $C\ell_G(x) = \{x^y \in G : y \in G\}$ respectively, where $x^y = yxy^{-1}$. Note that $Z(G) = \bigcap_{x \in G} C_G(x)$.

Given any two subgroups H and K of G, we write $C_K(H)$ to denote the set $\{k \in K : hk = kh \text{ for all } h \in H\}$. In particular, when $K = G$, the set $C_G(H) = \{x \in G : xh = hx \text{ for all } h \in H\}$ is called the *centralizer* of H in G. Also, given a subgroup H of G, the set $N_G(H) = \{x \in G : xHx^{-1} = H\}$

is called the *normalizer* of H in G. Clearly, $N_G(H) = G$ if and only if $H \trianglelefteq G$. In this regard, we have the following result.

Result 1.1.1. [43, page 130] *Let H be a subgroup of a group G. Then there is a homomorphism, with kernel $C_G(H)$, from $N_G(H)$ to* $\mathrm{Aut}(H)$*, the group of all automorphisms of H. That is, $C_G(H) \trianglelefteq N_G(H)$ and the quotient group $N_G(H)/C_G(H)$ can be regarded as a subgroup of* $\mathrm{Aut}(H)$.

(A) Commutators and commutator subgroup.

Given $x, y \in G$, the element $[x, y] = xyx^{-1}y^{-1} \in G$ is called the *commutator* of x and y in G. Clearly, $[x, y] = [y, x]^{-1}$ for all $x, y \in G$. In fact, we also have the following slightly more complicated *commutator identities* (see [43, pages 92–93])

$$[x,\ yz] = [x,\ y][x,\ z]^y \text{ and } [xy,\ z] = [y,\ z]^x[x,\ z], \tag{1.1.a}$$

$$[x,\ [y^{-1},\ z]]^y[y,\ [z^{-1},\ x]]^z[z,\ [x^{-1},\ y]]^x = 1, \tag{1.1.b}$$

where $x, y, z \in G$. Equation (1.1.b) is also known as the *Jacobi identity*. It may be mentioned here that, given $x_1, x_2, \ldots, x_n \in G$, we can form commutators by suitably positioning $n-1$ pairs of brackets across them in such a way that each pair of brackets gives rise to a commutator. The commutators so obtained are called *n-fold commutators*, for example, $[[x_1, x_2], [x_3, x_4]]$, $[x_1, [x_2, [x_3, x_4]]]$ are 4-fold commutators; on the other hand, $[x_1, x_2, \ldots, x_n] = x_1x_2\ldots x_nx_1^{-1}x_2^{-1}\ldots x_n^{-1}$ is called a *generalized commutator of length n*. Note that if $n \geq 3$, then a generalized commutator of length n is not necessarily a commutator, whereas every n-fold commutator is a commutator.

The subgroup G' of G generated by all commutators in G is called the *commutator subgroup* of G. More generally, given any two subgroups H and K of G, one also talks about the subgroup $[H, K]$ of G generated by all commutators of the form $[h, k]$, where $h \in H$ and $k \in K$. Obviously, $[G, G] = G'$. Note that $G' \trianglelefteq G$ and the quotient group G/G' is abelian. Moreover, given $H \leq G$, we have $H \trianglelefteq G$ with G/H abelian if and only if $G' \subseteq H$.

Remark 1.1.2. Commutators originated over 125 years ago through the hands of Dedekind. The fact that the commutators do not always constitute a subgroup led to the study of finding various conditions under which every element of the commutator subgroup is a commutator. In [27], L. C. Kappe and R. F. Morse have made a detailed survey describing a number of such conditions available till date.

If $G' \subseteq Z(G)$, then the group G is said to be *nilpotent* of class 2. If $(G/Z(G))' \subseteq Z(G/Z(G))$, then G is said to be nilpotent of class 3. In this way one defines nilpotent groups of class $m \geq 2$.

Result 1.1.3. [43, page 91] *A finite group is nilpotent if and only if it is the direct product of its Sylow subgroups.*

Result 1.1.4. [1, Lemma 3.8] *Let G be a finite group and p be the smallest prime divisor of $|G|$. If p is odd and $G' \cong C_p \times C_p$, then G is nilpotent.*

A subgroup H of G is said to be *central subgroup* if $H \subseteq Z(G)$, and H is called a *characteristic subgroup* if it is invariant under every automorphism of G, that is, if $\sigma(H) \subseteq H$ for all $\sigma \in \mathrm{Aut}(G)$.

Result 1.1.5. [35, Lemma 7] *If a group G has a cyclic, characteristic, non-central subgroup, then there is no group K such that $G \cong K'$.*

A finite p-group G is called *extra-special* if G' and $Z(G)$ coincide and have order p. Any non-abelian group of order p^3 is extra-special. More generally, we have

Result 1.1.6. [42, page 146] *An extra-special p-group is a central product of a finite number of non-abelian normal subgroups of order p^3, and so has order p^{2k+1} for some positive integer k. Conversely, a finite central product of non-abelian groups of order p^3 is an extra-special p-group.*

It may be recalled here that a group G is said to be the *central product* of its normal subgroups $G_1, G_2, \ldots, G_n$ if $G = G_1 G_2 \ldots G_n$, $[G_i, G_j] = \{1\}$ for $i \neq j$, and $G_i \cap \prod_{j \neq i} G_j = Z(G)$ for all i. Clearly, $Z(G_i) = Z(G)$ for all i.

(B) Class equation.

It is well-known that if G is a finite group, then $|\,C\ell_G(x)|$ divides $|G|$ for all $x \in G$; in fact, we have

$$|G : C_G(x)| \;=\; |\,C\ell_G(x)| \;=\; |[G, x]| \;\leq\; |G'| \qquad (1.1.c)$$

for all $x \in G$, where $[G, x] = \{[y, x] \;:\; y \in G\} \subseteq G'$. Note that $[G, x]$ is not necessarily a subgroup of G. Since $x^y = yxy^{-1}x^{-1}x \in G'x$ for all $x, y \in G$, we also have

$$C\ell_G(x) \subseteq G'x \qquad (1.1.d)$$

for all $x \in G$.

It is easy to see that G is the disjoint union of its conjugacy classes, and that $Z(G)$ consists of precisely those elements of G whose conjugacy classes have exactly one element. So, it follows that if G is a finite group, then

$$|G| = |Z(G)| + \sum_i |G : C_G(x_i)|, \tag{1.1.e}$$

where one x_i is chosen from each conjugacy class having more than one element. This is known as the *class equation* of G.

(C) Semidirect product of groups.

Let H and N be any two groups, and $\theta : H \longrightarrow \mathrm{Aut}(N)$ be a homomorphism. Let us write $\theta(h) = \theta_h$ for all $h \in H$. Then the Cartesian product $N \times H$ forms a group under the binary operation

$$(n_1, h_1)(n_2, h_2) = (n_1\theta_{h_1}(n_2), h_1h_2),$$

where $(n_i, h_i) \in N \times H$, $i = 1, 2$. This group is known as the *semidirect product* of N and H (with respect to θ), and is denoted by $N \rtimes_\theta H$. It is easy to see that if θ is the trivial homomorphism, then $N \rtimes_\theta H = N \times H$, the direct product of N and H. Quite often we drop the suffix θ from $\rtimes_\theta$, provided there is no ambiguity regarding the choice of a non-trivial homomorphism θ. Such groups play a very significant role in the construction of finite non-abelian groups.

Let G be a group with subgroups N and H such that $N \trianglelefteq G$, $NH = G$ and $N \cap H = \{1\}$. Then, considering the homomorphism $\theta : H \longrightarrow \mathrm{Aut}(N)$ given by $\theta_h(n) = hnh^{-1}$ for all $h \in H$ and for all $n \in N$, it is not difficult to see that $G = N \rtimes_\theta H$.

A subgroup N of a group G is said to have a *complement* in G if there exists a subgroup H of G such that $N \cap H = \{1\}$ and $NH = G$. In this regard we have the following result, often called *Schur-Zassenhaus Theorem.*

Result 1.1.7. [29, Theorem 6.2.1] *Let G be a group and $N \trianglelefteq G$ such that* $\gcd(|N|, |G : N|) = 1$. *Then N has a complement H in G, and hence, G is a semidirect product of N and H.*

(D) Isoclinism of groups.

Let G and H be any two groups. Then a pair $(\phi, \ \psi)$ is said to be an *isoclinism*, a concept introduced by P. Hall [23, page 133], from G to H if the following conditions hold:

(a) ϕ is an isomorphism from $G/Z(G)$ to $H/Z(H)$,

(b) ψ is an isomorphism from G' to H', and

(c) the diagram

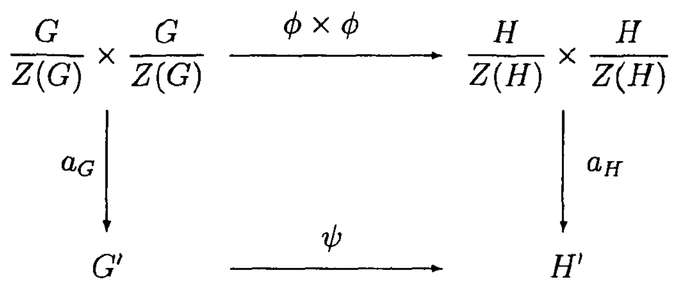

Figure 1.1: Isoclinism from G to H

commutes, that is, $a_H \circ (\phi \times \phi) = \psi \circ a_G$, where a_G and a_H are given respectively by $a_G(g_1Z(G), g_2Z(G)) = [g_1, g_2]$ for all $g_1, g_2 \in G$ and $a_H(h_1Z(H), h_2Z(H)) = [h_1, h_2]$ for all $h_1, h_2 \in H$.

It is easy to see that isoclinism is an equivalence relation among groups. If there is an isoclinism from G to H, we say that G and H are *isoclinic.*

Result 1.1.8. [23, page 135] *Given a group G, there exists a group H such that H is isoclinic to G and $Z(H) \subseteq H'$. If G is finite, so is any such H.*

Result 1.1.9. [23, page 135] *If G is a group and N is a normal subgroup of G such that $G' \cap N = \{1\}$, then G is isoclinic to G/N.*

1.2 Characters of finite groups

Given a positive integer n, let V be an n-dimensional vector space over the field $\mathbb{C}$ of complex numbers. For definiteness, we may assume that $V = \mathbb{C}^n$. Let $GL(V)$ be the group of all invertible linear operators on V. It is well-known that there is an isomorphism from $GL(V)$ onto $GL(n, \mathbb{C})$, the group of all invertible $n \times n$ matrices over $\mathbb{C}$, which maps each linear operator on V to its matrix representation with respect to a fixed basis of V. Thus, without any loss, we may identify $GL(V)$ with $GL(n, \mathbb{C})$. It may be mentioned here that most of the materials in this section have been collected from [25].

Let G be a finite group. A homomorphism $\Phi : G \longrightarrow GL(n, \mathbb{C}) \approx GL(V)$ is called a (complex) *representation of G of degree n.* Note that Φ may also be viewed as an algebra homomorphism, using the method of linear extension, from the group algebra $\mathbb{C}[G]$ of G over $\mathbb{C}$ to the algebra $M_n(\mathbb{C})$ of all $n \times n$

matrices over $\mathbb{C}$. We usually use the same symbol to denote a representation of G and the corresponding linearly extended algebra homomorphism.

Two representations $\Phi_1,\ \Phi_2 : G \longrightarrow GL(n, \mathbb{C})$ of G are said to be *similar* if there exists a $P \in GL(n, \mathbb{C})$ such that $\Phi_1(g) = P^{-1}\Phi_2(g)P$ for all $g \in G$.

Given a representation $\Phi : G \longrightarrow GL(n, \mathbb{C}) \approx GL(V)$ of G, a subspace W of V is said to be *G-invariant* if it is invariant under the linear operator $\Phi(g)$, that is, $\Phi(g)(W) \subseteq W$ for all $g \in G$. The representation Φ is said to be *irreducible* if there is no G-invariant subspace of V other than $\{0\}$ and V itself.

The following result is also sometimes referred to as *Schur's lemma* for irreducible representations.

Result 1.2.1. [25, page 26] *Let Φ be an irreducible representation of degree n of a finite group G. If A is an $n \times n$ matrix over $\mathbb{C}$ which commutes with $\Phi(g)$ for all $g \in G$, then $A = \alpha I_n$ for some $\alpha \in \mathbb{C}$, where I_n is the $n \times n$ identity matrix over $\mathbb{C}$.*

Let $\Phi : G \longrightarrow GL(n, \mathbb{C})$ be a representation of G. Then the (complex) *character of G afforded by Φ* is defined to be the function $\chi : G \longrightarrow \mathbb{C}$ given by $\chi(g) = \operatorname{tr}\Phi(g)$, the trace of $\Phi(g)$, for all $g \in G$. Note that $\chi(1) = n$, the degree of Φ. $\chi(1)$ is called the *degree of χ*. A character of G of degree 1 is called a *linear character*. In particular, the constant function $1_G : G \longrightarrow \mathbb{C}$, given by $1_G(g) = 1$ for all $g \in G$, is a linear character, called the *principal character* of G. We write $\operatorname{Lin}(G)$ to denote the set of all linear characters of G. It is well-known (see [25, page 25]) that

$$|\operatorname{Lin}(G)| = |G : G'|, \quad \text{and} \quad G' = \bigcap_{\chi \in \operatorname{Lin}(G)} \ker \chi, \qquad (1.2.a)$$

where $\ker\chi = \{g \in G : \chi(g) = \chi(1)\}$, called the kernel of χ. If $g \in G$ and χ is a character of G, then it is also known (see [25, page 20]) that

$$|\chi(g)| \leq \chi(1) \text{ and } \chi(g^{-1}) = \overline{\chi(g)}, \qquad (1.2.b)$$

where '—' stands for complex conjugate.

Result 1.2.2. [25, page 72] *Let G be a finite group and χ be a rational valued character of G. If $g, h \in G$ generate the same cyclic subgroup of G, then $\chi(g) = \chi(h)$.*

A complex number is called an *algebraic integer* if it satisfies a monic polynomial with coefficients in $\mathbb{Z}$, the set of all integers. Note that the rational algebraic integers are precisely the elements of $\mathbb{Z}$.

Result 1.2.3. [25, page 35] *Let χ be a character of a finite group G. Then $\chi(g)$ is an algebraic integer for all $g \in G$.*

It is easy to see that similar representations of G afford equal characters (in fact, as noted in [25, page 17], the converse is also true). Characters afforded by irreducible representations are called *irreducible characters*. The set of all irreducible characters of G is denoted by $\mathrm{Irr}(G)$. Clearly, all linear characters of G are irreducible. It is a fact (see [25, page 16]) that G is abelian if and only if all its irreducible characters are linear. More generally, we have $|\,\mathrm{Irr}(G)| = k(G)$, the number of conjugacy classes of G, and

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2, \qquad (1.2.c)$$

which is called the *degree equation* of G. It is also known (see [25, page 38]) that $\chi(1)$ divides $|G|$ for all $\chi \in \mathrm{Irr}(G)$; in fact, $\chi(1)$ divides $|G : Z(G)|$ for all $\chi \in \mathrm{Irr}(G)$.

Let $\chi \in \mathrm{Irr}(G)$, and Φ_χ be a representation of G which affords χ. Let I_χ be the $\chi(1) \times \chi(1)$ identity matrix over $\mathbb{C}$. Let $z \in Z(\mathbb{C}[G])$, the center of the group algebra $\mathbb{C}[G]$ of G over $\mathbb{C}$. Then, considering Φ_χ as an algebra homomorphism from $\mathbb{C}[G]$ to $M_n(\mathbb{C})$, it follows from Result 1.2.1 (Schur's lemma) that $\Phi_\chi(z) = \alpha I_\chi$. Since the only matrix similar to αI_χ is αI_χ itself, there exists a well-defined algebra homomorphism $\omega_\chi : Z(\mathbb{C}[G]) \longrightarrow \mathbb{C}$ given by $\Phi_\chi(z) = \omega_\chi(z) I_\chi$ for all $z \in Z(\mathbb{C}[G])$. Let $\mathscr{K}$ be a conjugacy class of G with class sum $K = \sum_{x \in \mathscr{K}} x$ in $\mathbb{C}[G]$ and let $g \in \mathscr{K}$. Note (see [25, page 15]) that the class sums of all the conjugacy classes of G form a basis for $Z(\mathbb{C}[G])$. In this regard, we have the following result.

Result 1.2.4. [25, pages 35–36] *Let G be a finite group. Then, with notations same as above, $\omega_\chi(K)$ is an algebraic integer and*

$$\omega_\chi(K) = \frac{\chi(g)|\mathscr{K}|}{\chi(1)}.$$

From the above-mentioned Schur's lemma, it also follows (see [49, page 5354]) that

$$\sum_{x \in G} \Phi_\chi(xyx^{-1}) = \frac{|G|}{\chi(1)} \chi(y)\, \mathrm{I}_\chi \qquad (1.2.d)$$

for all $y \in G$.

A function $\varphi : G \longrightarrow \mathbb{C}$ is called a *class function* of G if it is constant on the conjugacy classes of G. One can easily see that all characters of G are class functions.

Result 1.2.5. [25, page 16] *Every class function φ of a finite group G can be uniquely expressed as*

$$\varphi = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi, \tag{1.2.e}$$

where $a_\chi \in \mathbb{C}$. Moreover, φ is a character of G if and only if each a_χ is a non-negative integer and $\varphi \neq 0$.

Let φ and ϑ be any two class functions on G. Then

$$[\varphi, \vartheta] = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\vartheta(g)} \tag{1.2.f}$$

defines the inner product of φ and ϑ.

Let $\mathrm{Irr}(G) = \{\chi_1, \chi_2, \dots, \chi_k\}$. Then, for $1 \leq i, j \leq k$ and for $h \in G$, we have

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(gh) \chi_j(g^{-1}) = \delta_{ij} \frac{\chi_i(h)}{\chi_i(1)}. \tag{1.2.g}$$

This is known as the *generalized orthogonality relation* (see [25, page 19]). In particular, putting $h = 1$ in (1.2.g), we have

$$[\chi_i, \chi_j] = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \chi_j(g^{-1}) = \delta_{ij}. \tag{1.2.h}$$

This is known as the *first orthogonality relation* (see [25, page 20]). In view of this relation, Result 1.2.5 may be reformulated as follows

Result 1.2.6. *Every class function φ of a finite group G can be expressed as*

$$\varphi = \sum_{\chi \in \mathrm{Irr}(G)} [\varphi, \chi] \chi. \tag{1.2.i}$$

Moreover, φ is a character of G if and only if $[\varphi, \chi]$ is a non-negative integer for all $\chi \in \mathrm{Irr}(G)$ and $\varphi \neq 0$.

On the other hand, if $g, h \in G$, then

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = \begin{cases} |\,\mathrm{C}\ell_G(g)| & \text{if } h \in \mathrm{C}\ell_G(g) \\ 0 & \text{otherwise.} \end{cases} \tag{1.2.j}$$

This is known as the *second orthogonality relation* (see [25, page 21]).

Let H be a subgroup of G. Let ϑ be a class function of G. Then the restriction of ϑ to H is a class function of H, and it is denoted by ϑ_H. In particular, if χ is a character of G, then χ_H is a character of H and we have (see [25, page 28])

$$[\chi_H, \chi_H] \leq |G : H|[\chi, \chi]. \tag{1.2.k}$$

On the other hand, for any class function ϕ of H, the induced class function ϕ^G on G is given by

$$\phi^G(g) = \frac{1}{|H|} \sum_{x \in G} \phi^o(xgx^{-1}),$$

where $\phi^o(h) = \phi(h)$ if $h \in H$ and $\phi^o(y) = 0$ if $y \notin H$. In this regard, we have

$$[\phi, \vartheta_H] = [\phi^G, \vartheta], \tag{1.2.l}$$

where ϕ and ϑ are class functions on H and G respectively. This is known as *Frobenius Reciprocity* (see [25, page 62]).

Let $\mathrm{cd}(G) = \{\chi(1) : \chi \in \mathrm{Irr}(G)\}$. It is well-known (see [25, page 28]) that $|G : Z(G)|^{1/2}$ is an upper bound for $\mathrm{cd}(G)$. The group G is said to be of *central type* if this upper bound is attained, that is, if $\chi(1) = |G : Z(G)|^{1/2}$ for some $\chi \in \mathrm{Irr}(G)$.

Result 1.2.7. [25, Problem 2.13] *If p is a prime and G is a finite group with $|G'| = p$ and $G' \subseteq Z(G)$, then $\chi(1)^2 = |G : Z(G)|$ for every non-linear $\chi \in \mathrm{Irr}(G)$, that is, G is of central type with $|\operatorname{cd}(G)| = 2$.*

Result 1.2.8. [28, page 1701] *If p is a prime and G is a finite group with $|G'| = p$, then $|\operatorname{cd}(G)| = 2$*

Result 1.2.9. [25, Problem 2.18] *Let G be a finite group, $A \lhd G$ such that $A = C_G(a)$ for every $a \in A$ with $a \neq 1$, and G/A be abelian. Then G has exactly $\frac{|A|-1}{|G:A|}$ non-linear irreducible characters all having degree equal to $|G : A|$.*

Result 1.2.10. [24, Proposition 6.8] *Let G be a finite simple non-abelian group. Then there does not exist any $\chi \in \mathrm{Irr}(G)$ with $\chi(1) = 2$.*

Result 1.2.11. [25, Corollary 12.6] *Let G be a finite group. If $|\operatorname{cd}(G)| = 2$, then G' is abelian.*

Result 1.2.12. [25, Theorem 12.11] *Let G be a finite non-abelian group and p be a prime. Then $\operatorname{cd}(G) = \{1, p\}$ if and only if one of the following holds.*

(a) *There exists abelian $A \lhd G$ with $|G : A| = p$.*

(b) $|G : Z(G)| = p^3$.

Result 1.2.13. [25, Lemma 12.12] *Let G be a finite group. If $A \lhd G$ with A abelian and G/A cyclic, then $|A| = |G'||A \cap Z(G)|$.*

1.3 Equations in a finite group

F. G. Frobenius is perhaps the first among a large number of mathematicians who have made elaborate studies of equations in finite groups. One of his classical results (see [18]) says that if G is a finite group and $g \in G$, then the number of solutions of the commutator equation $xyx^{-1}y^{-1} = g$ in G defines a character on G, and is given by

$$\zeta(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|}{\chi(1)} \chi(g). \tag{1.3.a}$$

In [28, Corollary 1], P. Kellersch and K. Meyberg have shown that, for $n \geq 1$, the number of solutions of the equation

$$x_1 x_2 x_1^{-1} x_2^{-1} \dots x_{2n-1} x_{2n} x_{2n-1}^{-1} x_{2n}^{-1} = g \tag{1.3.b}$$

is given by

$$\xi_n(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|^{2n-1}}{\chi(1)^{2n-1}} \chi(g). \tag{1.3.c}$$

Recently, T. Tambour [49, Theorem 1] has proved that, for $n \geq 1$, the number of solutions of the equation

$$x_1 x_2 \dots x_n x_1^{-1} x_2^{-1} \dots x_n^{-1} = g \tag{1.3.d}$$

is given by

$$\eta_n(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|^{n-1}}{\chi(1)^{n-\varepsilon_n}} \chi(g), \tag{1.3.e}$$

where $\varepsilon_n = 1$ or 2 according as n is even or odd. It may be mentioned here that Tambour has also reproved the result in (1.3.c).

Note that, as $\chi(1)$ divides $|G|$ for all $\chi \in \mathrm{Irr}(G)$, the functions ζ, ξ_n and η_n given by (1.3.a), (1.3.c) and (1.3.e) respectively define characters of G.

On the other hand, S. P. Strunkov [48, Theorem 2] considers two abstract functions $f_1(x_1)$ and $f_2(x_2)$ defined on two sets X_1 and X_2 with their values in G. He proves that if the numbers of solutions of the equations $f_1(x_1) = g$ and $f_2(x_2) = g$, in the finite subsets $\Omega_1 \subseteq X_1$ and $\Omega_2 \subseteq X_2$, define characters on G and are given by

$$\psi_1(g) = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi(g) \quad \text{and} \quad \psi_2(g) = \sum_{\chi \in \mathrm{Irr}(G)} b_\chi \chi(g)$$

respectively, where a_χ and b_χ are non-negative integers, then the number of solutions of the equation $f_1(x_1)f_2(x_2) = g$, in the subset $\Omega_1 \times \Omega_2 \subseteq X_1 \times X_2$, define a character on G and is given by

$$\psi(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|}{\chi(1)} a_\chi b_\chi \chi(g). \tag{1.3.f}$$

Strunkov [47, Lemma 1] also derives that if H is a subgroup of G and $g \in G$, then the number of elements $(g_1, g_2, h_3, h_4) \in G \times G \times H \times H$ satisfying $g_1 h_3 g_1^{-1} g_2 h_4 g_2^{-1} = g$ is given by

$$\tilde{\psi}(g) = |G||H|^2 \sum_{\chi \in \mathrm{Irr}(G)} \frac{[\chi_H, 1_H]^2}{\chi(1)} \chi(g). \tag{1.3.g}$$

Once again, it is easy to see that $\tilde{\psi}$ defines a character of G.

1.4 Equidistributed and measure preserving maps

Let X, Y be two finite sets, and let $\epsilon > 0$. A function $f : X \longrightarrow Y$ is said to be *ϵ-equidistributed* if there exists a subset $Y' \subseteq Y$ with the following properties:

(a) $|Y'| \geq |Y|(1-\epsilon)$;

(b) $\frac{|X|}{|Y|}(1-\epsilon) \leq |f^{-1}(y)| \leq \frac{|X|}{|Y|}(1+\epsilon)$ uniformly for all $y \in Y'$.

In particular, if ϵ is sufficiently small, then f is called *almost equidistributed.*

A function $f : X \longrightarrow Y$ is said to be *almost measure preserving* if there exists a sufficiently small positive real number ϵ such that

$$\left|\frac{|f^{-1}(Y_0)|}{|X|} - \frac{|Y_0|}{|Y|}\right| < \epsilon \quad \text{for all } Y_0 \subseteq Y.$$

It is known that a function $f : X \longrightarrow Y$ is almost measure preserving if it is almost equidistibuted. In fact, we have

Result 1.4.1. [19, Proposition 3.2] *If $f : X \longrightarrow Y$ is ϵ-equidistributed, then*

(a) $\left|\frac{|f^{-1}(Y_0)|}{|X|} - \frac{|Y_0|}{|Y|}\right| \leq 3\epsilon$ *for all* $Y_0 \subseteq Y$,

(b) $\frac{|f(X_0)|}{|Y|} \geq \frac{|X_0|}{|X|} - 3\epsilon$ *for all* $X_0 \subseteq X$.

Given a function $f : X \longrightarrow Y$, let P_f denote the *probability distribution* (associated to f) on Y defined by

$$P_f(y) = \frac{|f^{-1}(y)|}{|X|}, \ y \in Y.$$

Let U be the *uniform distribution* on Y given by $U(y) = \frac{1}{|Y|}$, $y \in Y$. Let $||P_f - U||_1$ denote the L_1*-distance* between P_f and U given by

$$||P_f - U||_1 = \sum_{y \in Y} \left| P_f(y) - \frac{1}{|Y|} \right|.$$

In this regard, we have

Result 1.4.2. [19, Lemma 3.1(ii)] *Let $\delta > 0$. If $||P_f - U||_1 \leq \delta$, then f is $\sqrt{\delta}$-equidistributed.*

Consider now a finite group G, and let P be a probability distribution on G which is also a class function on G. Then, by (1.2.e), we have

$$P = |G|^{-1} \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi,$$

with suitable complex coefficients a_χ. It has been proved in [19, Lemma 2.3] that

$$||P - U||_1 \leq \Big(\sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi \neq 1_G}} |a_\chi|^2 \Big)^{1/2}. \tag{1.4.a}$$

1.5 Commutativity degree of finite groups

Let G be a finite group. The *commutativity degree* of G, denoted by $\Pr(G)$, is the probability that a randomly chosen pair of elements of G commute and is given by

$$\Pr(G) = \frac{|\{(x, y) \in G \times G : [x, y] = 1\}|}{|G \times G|}. \tag{1.5.a}$$

Clearly, $\Pr(G) = 1$ if and only if G is abelian. W. H. Gustafson [22] has shown that

$$\Pr(G) = \frac{k(G)}{|G|}, \tag{1.5.b}$$

where $k(G)$ is the number of conjugacy classes of G. He has also proved that $\Pr(G) \leq \frac{5}{8}$ if G is non-abelian. In [2, Theorem 3], S. M. Belcastro and G. J. Sherman have proved that $\Pr(G) = \frac{5}{8}$ if and only if $|\frac{G}{Z(G)}| = 4$. More generally, we have

Result 1.5.1. [33, Theorem 3] *Let G be a finite non-abelian group and p be the smallest prime divisor of $|G|$. Then*

$$\Pr(G) \leq \frac{p^2 + p - 1}{p^3}$$

with equality if and only if $|\frac{G}{Z(G)}| = p^2$.

The following result, possibly due to K. S. Joseph [26], can be derived easily from the degree equation (1.2.c).

Result 1.5.2. *Let G be a finite non-abelian group and p be the smallest prime divisor of $|G|$. Then*

$$\Pr(G) \leq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{p^2}\right) = \frac{1}{p^2}\left(1 + \frac{p^2 - 1}{|G'|}\right)$$

with equality if and only if $\mathrm{cd}(G) = \{1, p\}$.

In [44, Section IV], D. J. Rusin has characterized all finite non-abelian groups G with $\Pr(G) > \frac{11}{32}$ and tabulated his findings as follows:

$\Pr(G)$	G'	$G' \cap Z(G)$	$G/Z(G)$
$\frac{1}{2}(1+\frac{1}{2^{2s}})$	C_2	C_2	$(C_2)^{2s}, s \geq 1$
$\frac{1}{2}$	C_3	$\{1\}$	S_3
$\frac{7}{16}$	C_4 or $C_2 \times C_2$	C_2	D_8
	$C_2 \times C_2$	$C_2 \times C_2$	C_2^3 or C_2^4
$\frac{11}{27}$	C_3	C_3	$C_3 \times C_3$
$\frac{2}{5}$	C_5	$\{1\}$	D_{10}
$\frac{25}{64}$	$C_2 \times C_2$	$C_2 \times C_2$	C_2^3 or C_2^4
$\frac{3}{8}$	C_6	C_2	$C_2 \times S_3$ or T

Table 1.5.3: Groups with $\Pr(G) > \frac{11}{32}$

In this table, C_n denotes the cyclic group of order n, D_{2n} denotes the dihedral group of order $2n$ and T stands for the non-abelian group of order 12 besides A_4 and $C_2 \times S_3$.

$\Pr(G)$ may be regarded as a completely multiplicative arithmetic function of finite groups, in the sense of [4]. In other words, we have

Result 1.5.4. [22, page 1033] *If H and K are any two finite groups, then*

$$\Pr(H \times K) = \Pr(H)\Pr(K).$$

P. Lescot has proved that $\Pr(G)$ is an invariant under isoclinism of groups. More precisely, we have

Result 1.5.5. [30, Lemma 2.4] *If G and H are any two isoclinic finite groups, then* $\Pr(G) = \Pr(H)$.

Some of the useful results regarding $\Pr(G)$ may be listed as follows.

Result 1.5.6. [36, Proposition 3.3] *Let G be a finite non-abelian group and p be the smallest prime divisor of $|G|$. If $G' \cap Z(G) = \{1\}$, then* $\Pr(G) \leq \frac{1}{p}$.

Result 1.5.7. [20, Lemma 2(i)] *If G is a finite group and H is a proper subgroup of G, then*

$$\frac{\Pr(H)}{|G:H|^2} < \Pr(G) \leq \Pr(H).$$

In particular, $\Pr(G) \geq \frac{1}{|G:H|^2}$ *if H is an abelian subgroup of G.*

Result 1.5.8. [44, Section II] *Let p be a prime. If G is a finite p-group with $G' \subseteq Z(G)$, then*

$$\Pr(G) = \frac{1}{|G'|}\left(1 + \sum_{\substack{K \leq G', \\ G'/K \text{ cyclic}}} \frac{(p-1)|G':K|}{p|G:K^*|}\right),$$

where $K^* = \{x \in G : [G,x] \subseteq K\} \trianglelefteq G$ and $\frac{G}{K^*} \cong \prod(C_{p^{n_i}} \times C_{p^{n_i}})$ with $p \leq p^{n_i} \leq p^{n_1} = p^k = |G':K|$.

As a consequence of the above result we also have

Result 1.5.9. *Let p be a prime and G be a finite group with $|G'| = p$. If $G' \subseteq Z(G)$, then $\frac{G}{Z(G)} \cong (C_p \times C_p)^s$, for some $s \geq 1$, and*

$$\Pr(G) = \frac{1}{p}\left(1 + \frac{p-1}{p^{2s}}\right).$$

Result 1.5.10. [44, page 243] *Let p be a prime. Let r and s be two positive integers such that $s \mid (p-1)$, and $r^j \equiv 1 \pmod p$ if and only if $s \mid j$. If $G = \langle a, b : a^p = b^s = 1, bab^{-1} = a^r \rangle$, then*

$$\Pr(G) = \frac{s^2 + p - 1}{ps^2}.$$

Result 1.5.11. [44, Proposition 5] *Let p be a prime and G be a finite group with $|G'| = p$. If $Z(G) = \{1\}$, then $G = \langle a, b : a^p = b^s = 1, bab^{-1} = a^r \rangle$, where $s \mid (p-1)$, and $r^j \equiv 1 \pmod p$ if and only if $s \mid j$.*

Combining Result 1.5.10 and Result 1.5.11, we have

Result 1.5.12. [44, Section III] *Let p be a prime and G be a finite group with $|G'| = p$. If $G' \cap Z(G) = \{1\}$, then*

(a) $\frac{G}{Z(G)} = \langle a, b : a^p = b^s = 1, bab^{-1} = a^r \rangle$,

where $s \mid (p-1)$, and $r^j \equiv 1 \pmod p$ if and only if $s \mid j$.

(b) $\Pr(G) = \Pr(\frac{G}{Z(G)}) = \dfrac{s^2 + p - 1}{ps^2}.$

Result 1.5.13. [3, page 303] *Let G be a finite group and p be a prime. If G is non-abelian, $H \trianglelefteq G$ and $|G : H| = p$, then*

$$\Pr(G) = \frac{\Pr(H)}{p^2} + \frac{p+1}{p|G|^2} \sum_{x \in G-H} |C_G(x)|.$$

Moreover, if H is abelian, then $|\frac{G}{Z(G)}| = p|G'|$, $|C_G(x)| = |G : G'|$ for all $x \in G - H$ and

$$\Pr(G) = \frac{1}{p^2} + \frac{p^2 - 1}{p^2|G'|}.$$

The concept of commutativity degree has been considered and generalized by several authors. Given a subgroup H of a finite group G, A. Erfanian, R. Rezaei and P. Lescot [13] have considered the probability $\Pr(H,G)$ for an element of H to commute with an element of G. They proved – among others – the following result.

Result 1.5.14. [13, Theorem 3.5] *Let H be a subgroup of a finite group G and p be the smallest prime dividing $|G|$. Then*

$$\frac{|Z(G)\cap H|}{|H|}+\frac{p(|H|-|Z(G)\cap H|)}{|H||G|}\leq \Pr(H,G)\leq \frac{|Z(G)\cap H|+|H|}{2|H|}.$$

In [40], M. R. Pournaki and R. Sobhani have considered the probability $\Pr_g(G)$ that the commutator of an arbitrarily chosen pair of elements in a finite group G equals a given group element g. Some of the results proved by them are as follows.

Result 1.5.15. [40, Theorem 2.1] *Let G be a finite group and $g \in G'$. Then*

$$\Pr_g(G)=\frac{1}{|G|}\sum_{\chi\in \mathrm{Irr}(G)}\frac{\chi(g)}{\chi(1)}.$$

Result 1.5.16. [40, Proposition 5.1] *Let G be a finite group and $g \in G'$. Then* $\Pr_g(G)\leq \Pr(G)$ *with equality if and only if $g=1$.*

Result 1.5.17. [40, Proposition 5.2] *Let G be a finite group and g be a non-identity element of G'. Then* $\Pr_g(G)<\frac{1}{2}$.

Result 1.5.18. [40, Proposition 5.3] *For each positive real number ε there exists a finite group G and an element $g\in G'$ such that*

$$\frac{1}{2}-\varepsilon<\Pr_g(G)<\frac{1}{2}.$$

Chapter 2

Revisiting commutativity degree of finite groups

In this chapter we obtain a characterization for all finite groups of odd order having commutativity degree at least $\frac{11}{75}$. We also obtain a lower bound for commutativity degree and derive some necessary and sufficient conditions for attaining this bound. Finally, we compute the value of commutativity degree for certain standard families of finite groups.

This chapter is based on the papers [37] and [39].

2.1 Some auxiliary results

Let G be a finite group. Let p be the smallest prime divisor of $|G|$. Then, from (1.1.c), we have

$$p \leq |\,\mathrm{C}\ell_G(x)| \leq |G'| \iff x \in G - Z(G). \tag{2.1.a}$$

Clearly, if $|\,C\ell_G(x)| = p$, then $G/C_G(x)$ forms an abelian group (in fact, a cyclic group of order p), and so, $G' \subseteq C_G(x)$, which means that $x \in C_G(G')$. So, for all $x \in G - C_G(G')$, we have

$$p < |\,C\ell_G(x)|. \tag{2.1.b}$$

Note that $C_G(G') = \bigcap_{x\in G'} C_G(x) \trianglelefteq G$, using Result 1.1.1. So, by (1.1.c), $|\,C\ell_G(x)|$ divides $|\frac{G}{C_G(G')}|$ for all $x \in G'$. Moreover, $\frac{G}{C_G(G')}$ is abelian if and only if G' is abelian, and in either case $[C_G(G'), x]$ is a subgroup of G' for all $x \in G$, which can be easily deduced from the commutator identities in (1.1.a). Also, using the Jacobi identity (1.1.b), we have

$$(C_G(G'))' \subseteq Z(G) \subseteq Z(C_G(G')). \tag{2.1.c}$$

In view of the above discussion, we have

Lemma 2.1.1. *Let G be a finite group and p be a prime. Then*

(a) $\frac{G}{C_G(G')}$ *can be embedded in* $\mathrm{Aut}(G')$, *and so,* $|\,C\ell_G(x)|$ *divides* $|\,\mathrm{Aut}(G')|$ *for all $x \in G'$. In particular, if* $\gcd(p-1, |G|) = 1$ *and* $|G'| = p$, *then* $G' \subseteq Z(G)$.

(b) *If* $\frac{G}{C_G(G')} \cong C_p$, *then* $\langle x, C_G(G')\rangle = G$, $[G, x] = [C_G(G'), x]$ *and* $|\,C\ell_G(x)|$ *divides* $|G'|$ *for all* $x \in G - C_G(G')$.

Proof. Part (a) follows from Result 1.1.1, noting, for the particular case, that $|\,\mathrm{Aut}(C_p)| = p-1$. Part (b) follows from (1.1.c) and the identities in (1.1.a), noting that $[C_G(G'), x]$ is a subgroup of G'. □

In view of Result 1.5.4, the following generalization of Result 1.1.4 simplifies our task considerably.

Lemma 2.1.2. *Let G be a finite non-abelian group and p be a prime such that* $\gcd(p-1, |G|) = 1$. *If $|G'| = p^2$ and $|G' \cap Z(G)| = p$, then G is nilpotent of class* 3; *in particular, $G \cong P \times A$, where A is an abelian group and P is a p-group such that $|P'| = p^2$ and $|P' \cap Z(P)| = p$.*

Proof. We have

$$\left|\left(\frac{G}{Z(G)}\right)'\right| = \left|\frac{G'Z(G)}{Z(G)}\right| = \left|\frac{G'}{G' \cap Z(G)}\right| = p.$$

So, it follows from Lemma 2.1.1(a) that $G/Z(G)$ is nilpotent of class 2, and hence, G is nilpotent of class 3. Thus, in particular, G is the direct product of its Sylow subgroups. The proof follows considering P to be the p-Sylow subgroup and A to be the product of the rest of the Sylow subgroups. □

Given $H \subseteq G$, consider the set $H^* = \{x \in G : [G, x] \subseteq H\}$. Then, as observed in [44, Section I], we have

Lemma 2.1.3. *Let G be a finite group. If H, H_1, $H_2 \trianglelefteq G$, then*

(a) $(G' \cap H)^* = H^*$, $\{1\}^* = Z(G)$, *and* $(G')^* = G$,

(b) $(H_1 \cap H_2)^* = H_1^* \cap H_2^*$, *and* $H_1^* H_2^* \subseteq (H_1 H_2)^*$,

(c) $H_1 \subseteq H_2 \implies H_1^* \subseteq H_2^*$,

(d) $H \trianglelefteq H^* \trianglelefteq G$, *and* $Z(G/H) = H^*/H$,

(e) G/H^* *is never a non-trivial cyclic group.*

Proof. Parts (a), (b), (c) and (d) follow from the definition of $(\,)^*$ operation. For part (e), note that $G/H^* \cong \frac{G/H}{Z(G/H)}$. □

2.2 Groups with $|G'| = p^2$ and $|G' \cap Z(G)| = p$

Let G be a finite group. Recall that the commutativity degree of G, denoted by $\Pr(G)$, is defined as the ratio

$$\Pr(G) = \frac{|\{(x,y) \in G \times G : [x,y] = 1\}|}{|G \times G|}.$$

As noted in Result 1.5.8 and Result 1.5.12, D. J. Rusin has computed the values of $\Pr(G)$ when $G' \subseteq Z(G)$, and when $G' \cap Z(G) = \{1\}$. In this section we determine the value of $\Pr(G)$ and the size of $\frac{G}{Z(G)}$ when $|G'| = p^2$ and $|G' \cap Z(G)| = p$, where p is a prime such that $\gcd(p-1, |G|) = 1$. It may be noted here that, on a number of occasions, the structure of $\frac{G}{Z(G)}$ is determined by its size. For example, using GAP [51] and the notion of semidirect product (see Section 1.1), we have

Result 2.2.1. *If G is a finite group with $G' \not\subseteq Z(G)$, then $\frac{G}{Z(G)}$ is isomorphic to $C_7 \rtimes C_3$, $(C_3 \times C_3) \rtimes C_3$, $C_{13} \rtimes C_3$, $C_{19} \rtimes C_3$, $C_3 \times (C_7 \rtimes C_3)$ or $(C_5 \times C_5) \rtimes C_3$ according as $|\frac{G}{Z(G)}|$ is $21, 27, 39, 57, 63$ or 75.*

We begin with a few lemmas.

Lemma 2.2.2. *Let G be a finite group and p be a prime. If $|G' \cap Z(G)| = p$ and $C_G(G')$ is non-abelian, then $\frac{C_G(G')}{Z(C_G(G'))} \cong (C_p \times C_p)^s$ and*

$$\Pr(C_G(G')) = \frac{1}{p}\left(1 + \frac{p-1}{p^{2s}}\right),$$

for some positive integer s.

Proof. In view of (2.1.c), the lemma follows from Result 1.5.9. □

Lemma 2.2.3. *Let p be a prime and G be a finite group such that $G' \nsubseteq Z(G)$ and one of the following conditions holds:*

(a) $G' \cong C_{p^2}$ *and* $\gcd(p-1, |G|) = 1$,

(b) $G' \cong C_p \times C_p$ *and* $\gcd(p^2-1, |G|) = 1$.

Then $|\frac{G}{C_G(G')}| = |G' \cap Z(G)| = |\operatorname{C\ell}_G(x)| = p$ *for all* $x \in G' - Z(G)$.

Proof. Since $|\operatorname{Aut}(C_{p^2})| = p(p-1)$ and $|\operatorname{Aut}(C_p \times C_p)| = p(p+1)(p-1)^2$, the result follows from Lemma 2.1.1(a), noting that $G' - Z(G)$ is a union of conjugacy classes of G. □

Lemma 2.2.4. *Let G be a finite group and p be the smallest prime divisor of $|G|$. If $G' \nsubseteq Z(G)$ and $|\frac{G}{C_G(G')}| = |G' \cap Z(G)| = p$, then $Z(G)^* \subsetneq C_G(G')$ and $\frac{C_G(G')}{Z(G)^*}$ can be embedded in $\frac{G'}{G' \cap Z(G)}$.*

Proof. By Lemma 2.1.3(d), we have $Z(G)^* \neq C_G(G')$. Let $z \in Z(G)^*$. Then, using (1.1.c) and the definition of $Z(G)^*$, we have $|\operatorname{C\ell}_G(z)| \leq |G' \cap Z(G)| = p$. This, in view of (2.1.$b$), implies that $z \in C_G(G')$. Thus, $Z(G)^* \subsetneq C_G(G')$. Again, let $x \in G - C_G(G')$. Since $\frac{G}{C_G(G')}$, and hence, G' is abelian, it can be easily seen, using (1.1.a), that the mapping $f : C_G(G') \longrightarrow G'Z(G)/Z(G)$, defined by $f(z) = [z, x]Z(G)$, is a homomorphism. Also, using the definition of $Z(G)^*$ together with (2.1.c) and Lemma 2.1.1(b), we have $\ker f = Z(G)^*$. Thus, it follows that $C_G(G')/Z(G)^*$ is isomorphic to a subgroup of $\frac{G'Z(G)}{Z(G)}$. This completes the proof. □

Lemma 2.2.5. *Let p be a prime. If G is a finite p-group such that $|G'| = p^2$ and $|G' \cap Z(G)| = p$, then $Z(G)^* \cap Z(C_G(G')) = G'Z(G)$.*

Proof. By Lemma 2.2.3, $\frac{G}{C_G(G')}$ is abelian. Also, by Lemma 2.1.2, G is nilpotent of class 3. So, it follows that $G'Z(G) \subseteq Z(G)^* \cap Z(C_G(G'))$. For the converse, we first fix $x \in G - C_G(G')$ and $y \in G' - Z(G)$. Then, by Lemma 2.1.1(b), $C_G(x) \cap Z(C_G(G')) = Z(G)$. Therefore, since $y \notin Z(G)$, we have $[y^{-1}, x] \neq 1$. Now, let $z \in Z(G)^* \cap Z(C_G(G'))$. Note that both z and y are in $Z(G)^*$, and so, $[z, x], [y^{-1}, x] \in G' \cap Z(G)$, which is cyclic of order p. Hence, it follows that there is a positive integer i with $1 \leq i \leq p-1$ such that

$$\begin{aligned} & [y^{-1}, x]^i = [z, x] \\ \Longrightarrow\ & [y^i z, x] = 1 \\ \Longrightarrow\ & y^i z \in C_G(x) \\ \Longrightarrow\ & y^i z \in Z(G), \text{ since } y^i z \in Z(C_G(G')) \\ \Longrightarrow\ & z \in G'Z(G), \text{ since } y^i \in G'. \end{aligned}$$

This completes the proof. □

The main result of this section is given as follows.

Theorem 2.2.6. *Let G be a finite group and p be a prime such that $\gcd(p-1, |G|) = 1$. If $|G'| = p^2$ and $|G' \cap Z(G)| = p$, then*

(a) $$\Pr(G) = \begin{cases} \frac{2p^2-1}{p^4} & \text{if } C_G(G') \text{ is abelian} \\ \frac{1}{p^4}\left(\frac{p-1}{p^{2s-1}} + p^2 + p - 1\right) & \text{otherwise,} \end{cases}$$

(b) $|\frac{G}{Z(G)}| = \begin{cases} p^3 & \textit{if } C_G(G') \textit{ is abelian} \\ p^{2s+2} \textit{ or } p^{2s+3} & \textit{otherwise,} \end{cases}$

where $p^{2s} = |C_G(G') : Z(C_G(G'))|$. *Moreover,*

$$|\frac{G}{G' \cap Z(G)} : Z(\frac{G}{G' \cap Z(G)})| = |\frac{G}{Z(G)} : Z(\frac{G}{Z(G)})| = p^2.$$

Proof. In view of Lemma 2.1.2, we can assume that G is a p-group. So, by Lemma 2.2.3, we have $|G : C_G(G')| = p$.

(a) If $x \in G - C_G(G')$, then it follows from Lemma 2.1.1(b) and (2.1.b) that $|C\ell_G(x)| = p^2$, and hence, $|C_G(x)| = |G|/p^2$. Thus, the result follows from Result 1.5.13 and Lemma 2.2.2.

(b) By Lemma 2.2.4, we have $|C_G(G') : Z(G)^*| = p$. Therefore, using the second isomorphism theorem [43, page 25] and Lemma 2.2.5, we have

$$|Z(C_G(G')) : G'Z(G)| = \begin{cases} p & \text{if } C_G(G') \text{ is abelian} \\ 1 \text{ or } p & \text{otherwise.} \end{cases}$$

Hence, using the first part of Lemma 2.2.2, the result follows from the normal series $Z(G) \subseteq G'Z(G) \subseteq Z(C_G(G')) \subseteq C_G(G') \subseteq G$.

The final statement follows from Lemma 2.2.4 and Lemma 2.1.3(a)(c). □

2.3 Groups of odd order with $\Pr(G) \geq \frac{11}{75}$

In [1, Theorem 4.12], F. Barry, D. MacHale and Á. Ní Shé have proved that if G is a finite group with $|G|$ odd and $\Pr(G) > \frac{11}{75}$, then G is supersolvable.

It may be recalled that a group G is said to be *supersolvable* if there is a series of the form

$$\{1\} = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_r = G,$$

where $A_i \trianglelefteq G$ and A_{i+1}/A_i is cyclic for each i with $0 \leq i \leq r-1$.

In this section we obtain a characterization (similar to the one mentioned in Table 1.5.3 obtained by Rusin) for all finite groups G of odd order with $\Pr(G) \geq \frac{11}{75}$. We also point out a few small but significant lacunae in the work of Rusin. As usual, we begin with a few lemmas.

Lemma 2.3.1. *Let G be a finite group such that $|G|$ is odd.*

(a) *If $G' \cong C_{15}$, then $G' \subseteq Z(G)$.*

(b) *If $G' \cong C_{21}$ and $G' \nsubseteq Z(G)$, then $|\frac{G}{C_G(G')}| = |G' \cap Z(G)| = 3$ and exactly one of the following conditions holds:*

   (i) $|\mathrm{C}\ell_G(x)| = 21$ *for all* $x \in G - C_G(G')$.

   (ii) *There exists a subset X of $G - C_G(G')$ such that*

$$\begin{aligned} |X| &= 2|Z(C_G(G'))| \quad \text{and} \\ |\mathrm{C}\ell_G(x)| &= \begin{cases} 7 & \text{if } x \in X \\ 21 & \text{if } x \in G - (C_G(G') \cup X). \end{cases} \end{aligned}$$

Proof. Note that $|\mathrm{Aut}(C_{15})| = 8$ and $|\mathrm{Aut}(C_{21})| = 12$. Therefore, (a) and the first part of (b) follow from Lemma 2.1.1(a).

For the second part of (b), we first observe, using (2.1.b) and Lemma 2.1.1(b), that $|\mathrm{C}\ell_G(x)| = 7$ or 21 for all $x \in G - C_G(G')$. Now, assume that the condition (i) fails. Then there is an $x_0 \in G - C_G(G')$ such that $|\,\mathrm{C}\ell_G(x_0)| = 7$. Since $|\frac{G}{C_G(G')}| = 3$, it is easy to see that

$$G - C_G(G') = x_0 C_G(G') \sqcup x_0^{-1} C_G(G'). \tag{2.3.a}$$

Let $X = x_0 Z(C_G(G')) \sqcup x_0^{-1} Z(C_G(G'))$. Clearly, $X \subseteq G - C_G(G')$. Since $|\,\mathrm{C}\ell_G(x_0)| = |\,\mathrm{C}\ell_G(x_0^{-1})|$, it follows from (1.1.$c$), (1.1.$a$) and Lemma 2.1.1(b) that $|\,\mathrm{C}\ell_G(x)| = 7$ for all $x \in X$. On the other hand, suppose that $x \in G - (C_G(G') \cup X)$. Then, by (2.3.$a$), we have $x = x_0 w$ or $x_0^{-1} w$ for some $w \in C_G(G') - Z(C_G(G'))$. Choose $w_1 \in C_G(G') - Z(C_G(G'))$ such that $[w_1, w] \neq 1$. Then, by (1.1.a) and (2.1.c), we have

$$[w_1, x] = \begin{cases} [w_1, x_0][w_1, w] & \text{if } x = x_0 w \\ [w_1, x_0^{-1}][w_1, w] & \text{if } x = x_0^{-1} w. \end{cases}$$

Note that $o([w_1, w]) = 3$ and $o([w_1, x_0]) = o([w_1, x_0^{-1}]) = 1$ or 7, and hence, it follows that $o([w_1, x]) = 3$ or 21. Thus, using (1.1.c), we have $|\,\mathrm{C}\ell_G(x)| = 21$. This completes the proof. □

Lemma 2.3.2. *Let G be a finite group. If $|G| \equiv 3 \pmod 6$, $G' \cong C_5 \times C_5$ and $|G' \cap Z(G)| = 1$, then*

(a) $|\,\mathrm{C}\ell_G(x)| = 3$ *for all* $x \in G' - Z(G)$,

(b) $|\frac{G}{C_G(G')}| = 3$.

Proof. Note that no non-identity element of G is conjugate to its inverse, and also that $G' - Z(G)$ is a union of conjugacy classes of G.

(a) Let $x \in G' - Z(G)$. Since $|G' - Z(G)| = 24$, we have $|\,\mathrm{C}\ell_G(x)| \leq 12$. This, in view of Lemma 2.1.1(a), implies that $|\,\mathrm{C}\ell_G(x)| = 3$ or 5. On the other hand, since $x^5 = 1$, it is a routine matter to see that the classes $\mathrm{C}\ell_G(x)$, $\mathrm{C}\ell_G(x^2)$, $\mathrm{C}\ell_G(x^3)$ and $\mathrm{C}\ell_G(x^4)$ are all distinct and have the same size. Thus, considering the possible partitions of 24 with 3 and 5 as summands, we have $|\mathrm{C}\ell_G(x)| = 3$ for all $x \in G' - Z(G)$.

(b) Suppose that there exist two elements $x, y \in G' - Z(G)$ such that $C_G(x) \neq C_G(y)$. Then, as seen above, $|G : C_G(x)| = |G : C_G(y)| = 3$, and so

$$\left|\frac{C_G(x)}{C_G(x) \cap C_G(y)}\right| = \left|\frac{C_G(x)C_G(y)}{C_G(y)}\right| = \left|\frac{G}{C_G(y)}\right| = 3.$$

Therefore, using the series

$$C_G(G') \subseteq C_G(x) \cap C_G(y) \subseteq C_G(x) \subseteq G,$$

we see that 9 divides $|\frac{G}{C_G(G')}|$. However, in view of Lemma 2.1.1(a), we have $|\frac{G}{C_G(G')}| = 3$, 5, or 15. Hence, it follows that $C_G(x) = C_G(y)$ for all $x, y \in G' - Z(G)$. This completes the proof. $\square$

We are now in a position to characterize all finite groups of odd order with commutativity degree at least $\frac{11}{75}$, essentially replicating the technique used by Rusin in [44, Section IV].

Theorem 2.3.3. *Let G be a finite group. If $|G|$ is odd and $\Pr(G) \geq \frac{11}{75}$, then the possible values of $\Pr(G)$ and the corresponding structures of G', $G' \cap Z(G)$ and $G/Z(G)$ are given as follows:*

$\Pr(G)$	G'	$G' \cap Z(G)$	$G/Z(G)$
1	$\{1\}$	$\{1\}$	$\{1\}$
$\frac{1}{3}(1+\frac{2}{3^{2s}})$	C_3	C_3	$(C_3 \times C_3)^s,\ s \geq 1$
$\frac{1}{5}(1+\frac{4}{5^{2s}})$	C_5	C_5	$(C_5 \times C_5)^s,\ s \geq 1$
$\frac{5}{21}$	C_7	$\{1\}$	$C_7 \rtimes C_3$
$\frac{55}{343}$	C_7	C_7	$C_7 \times C_7$
$\frac{17}{81}$	C_9 *or* $C_3 \times C_3$	C_3	$(C_3 \times C_3) \rtimes C_3$
	$C_3 \times C_3$	$C_3 \times C_3$	C_3^3
$\frac{121}{729}$	$C_3 \times C_3$	$C_3 \times C_3$	C_3^4
$\frac{7}{39}$	C_{13}	$\{1\}$	$C_{13} \rtimes C_3$
$\frac{3}{19}$	C_{19}	$\{1\}$	$C_{19} \rtimes C_3$
$\frac{29}{189}$	C_{21}	C_3	$C_3 \times (C_7 \rtimes C_3)$
$\frac{11}{75}$	$C_5 \times C_5$	$\{1\}$	$(C_5 \times C_5) \rtimes C_3$

Table 2.3.4: Groups with $|G|$ odd and $\Pr(G) \geq \frac{11}{75}$

Proof. Without any loss, we can assume that G is non-abelian. Now, by Result 1.5.2, we have $|G'| \leq 25$. Also, by Result 1.1.5, G' is not isomorphic to the unique non-abelian group of order 21. So, it follows that G' is isomorphic to $C_3 \times C_3$, C_9, C_{15}, C_{21}, $C_5 \times C_5$, C_{25} or C_p, where p is an odd prime with $p \leq 23$. We analyze these possibilities as follows:

Case 1. $G' \subseteq Z(G)$.

If $G' \cong C_p$, with p as above, then, by Result 1.5.9, there is a positive integer s such that $\frac{G}{Z(G)} \cong (C_p \times C_p)^s$ and

$$\Pr(G) = \frac{1}{p}\left(1 + \frac{p-1}{p^{2s}}\right).$$

It follows that s can have infinitely many values for $p = 3$ and 5, whereas $s = 1$ is the only possibility if $p = 7$. For the rest of the values of p, we have $\Pr(G) < \frac{11}{75}$.

If $G' \cong C_3 \times C_3$, then, by Result 1.5.8, we have

$$\Pr(G) = \frac{1}{9}\left(1 + \frac{2}{3^{2m_1}} + \frac{2}{3^{2m_2}} + \frac{2}{3^{2m_3}} + \frac{2}{3^{2m_4}}\right)$$

with $3^{2m_i} = |\frac{G}{K_i^*}|$, $1 \leq i \leq 4$, where K_1, K_2, K_3 and K_4 are the proper non-trivial subgroups of G'. Note that if $1 \leq i \neq j \leq 4$, then $K_i \cap K_j = \{1\}$, and so, by Lemma 2.1.3, we have $K_i^* \cap K_j^* = Z(G)$. Without any loss, we may assume that $1 \leq m_1 \leq m_2 \leq m_3 \leq m_4$. Thus, for $m_2 \geq 2$, we have

$$\Pr(G) \leq \frac{1}{9}\left(1 + \frac{2}{9} + \frac{2}{3^4} + \frac{2}{3^4} + \frac{2}{3^4}\right) < \frac{11}{75}.$$

Also, we have

$$|K_1^*||K_2^*| = |K_1^*K_2^*||K_1^* \cap K_2^*| = |K_1^*K_2^*||Z(G)| \leq |G||K_4^*|,$$

which implies that $|\frac{G}{K_1^*}||\frac{G}{K_2^*}| \geq |\frac{G}{K_4^*}|$. This, in turn, gives $m_1 + m_2 \geq m_4$. Hence, it follows that, for $\Pr(G) \geq \frac{11}{75}$, we must have $m_1 = m_2 = 1$ and $1 \leq m_3 \leq m_4 \leq 2$. Now, by Result 1.5.8, $\frac{G}{K_1^*}$ and $\frac{G}{K_2^*}$ are elementary abelian 3-groups. Therefore, given $g \in G$, we have $g^3 \in K_1^* \cap K_2^* = Z(G)$, and thus $\frac{G}{Z(G)}$ is also an elementary abelian 3-group. Moreover, by Lemma 2.1.3, we have

$$\left|\frac{G}{Z(G)}\right| = \left|\frac{G}{K_1^*}\right|\left|\frac{K_1^*}{Z(G)}\right| = 9\left|\frac{K_1^*K_2^*}{K_2^*}\right| \leq 9\left|\frac{G}{K_2^*}\right| = 81.$$

On the other hand, for $m_4 = 2$, we have

$$\left|\frac{G}{Z(G)}\right| = \left|\frac{G}{K_4^*}\right|\left|\frac{K_4^*}{Z(G)}\right| \geq 81,$$

and hence $|\frac{G}{Z(G)}| = 81$.

Let $m_1 = m_2 = m_3 = 1$ and $m_4 = 2$. Let $x \in K_1^*$ and $y \in K_3^*$. Then, by the definition of $(\ )^*$ operation, $[x, y] \in K_3$ and $[x, y]^{-1} = [y, x] \in K_1$. So, $[x, y] \in K_1 \cap K_3 = \{1\}$. Therefore, $K_1^* \subseteq C_G(K_3^*)$. Similarly, $K_2^* \subseteq C_G(K_3^*)$, and hence $K_1^*K_2^* \subseteq C_G(K_3^*)$. If $C_G(K_3^*) = G$, then it follows that $K_3^* = Z(G)$, and so $|\frac{G}{Z(G)}| = |\frac{G}{K_3^*}| = 9$, a contradiction. Thus, we have $K_1^*K_2^* \neq G$. But, by Lemma 2.1.3, we have

$$\frac{|G|}{|K_1^*K_2^*|} = \frac{|G||Z(G)|}{|K_1^*||K_2^*|} = 1,$$

and so $K_1^*K_2^* = G$, a contradiction. Therefore, it is not possible to have $m_1 = m_2 = m_3 = 1$ and $m_4 = 2$. Hence, $\frac{17}{81}$ (if $m_1 = m_2 = m_3 = m_4 = 1$) and $\frac{121}{729}$ (if $m_1 = m_2 = 1, m_3 = m_4 = 2$) are the only values of $\Pr(G)$, in the interval $[\frac{11}{75}, 1]$, and, as noted above, on each occasion $\frac{G}{Z(G)}$ is an elementary abelian 3-group with $|\frac{G}{Z(G)}| \leq 81$. In fact, if $\Pr(G) = \frac{121}{729}$, then we have $|\frac{G}{Z(G)}| = 81$. On the other hand, if $\Pr(G) = \frac{17}{81}$, then equality holds in Result 1.5.2, and so, using Result 1.2.12 and the second part of Result 1.5.13, we have $|\frac{G}{Z(G)}| = 27$.

For the rest of the possibilities for G', we have $\Pr(G) < \frac{11}{75}$, using Result 1.5.4 and Result 1.5.8.

Case 2. $\quad G' \cap Z(G) = \{1\}$.

In this case, by (2.1.c), $C_G(G')$ is an abelian group. Moreover, in view of Lemma 2.1.1(a), Lemma 2.2.3 and Lemma 2.3.1, it is not possible to have

$|G'| = 3, 5, 9, 15, 17$ or 21.

If $|G'| = 7, 11, 13, 19$ or 23, then $\Pr(G)$ and $|\frac{G}{Z(G)}|$ are determined by Result 1.5.12. More precisely, since there is a unique odd divisor $n > 1$ of $p-1$ for each $p \in \{7, 11, 13, 23\}$, we have $\Pr(G) = \frac{5}{21}$ and $|\frac{G}{Z(G)}| = 21$ if $|G'| = 7$, and $\Pr(G) = \frac{7}{39}$ and $|\frac{G}{Z(G)}| = 39$ if $|G'| = 13$, while $\Pr(G) < \frac{11}{75}$ if $|G'| = 11$ or 23. On the other hand, if $p = 19$, then there are two such odd divisors ($n = 3$ and $n = 9$) of $p - 1$. It can be seen that if $n = 3$, then $\Pr(G) = \frac{3}{19}$ and $|\frac{G}{Z(G)}| = 57$, whereas $\Pr(G) < \frac{11}{75}$ if $n = 9$.

If $|G'| = 25$, then, by Lemma 2.2.3, we must have $G' \cong C_5 \times C_5$ and $|G| \equiv 3 \pmod 6$. So, using Lemma 2.3.2(b) and the second part of Result 1.5.13, we have $\Pr(G) = \frac{11}{75}$ and $|\frac{G}{Z(G)}| = 75$.

Case 3. $G' \nsubseteq Z(G)$ and $G' \cap Z(G) \neq \{1\}$.

In this case, $|G'| = 9, 21$ or 25 ($|G'| \neq 15$, by Lemma 2.3.1(a)).

If $|G'| = 9$, then $|G' \cap Z(G)| = 3$. Using Theorem 2.2.6, we see that $\frac{17}{81}$ is the only value of $\Pr(G)$, in the interval $[\frac{11}{75}, 1]$, and it occurs when $C_G(G')$ is abelian. Also, in that case, we have $|\frac{G}{Z(G)}| = 27$.

If $|G'| = 21$, then, by Lemma 2.3.1(b), $|\frac{G}{C_G(G')}| = |G' \cap Z(G)| = 3$. Using Result 1.5.13 together with Lemma 2.2.2 and Lemma 2.3.1(b), we see that $\frac{29}{189}$ is the only value of $\Pr(G)$, in the interval $[\frac{11}{75}, 1]$, and it occurs when $C_G(G')$ is abelian. Also, in that case $|\frac{C_G(G')}{Z(G)}| = 21$ (using Result 1.2.13), and hence $|\frac{G}{Z(G)}| = 63$.

Finally, if $|G'| = 25$, then $|G' \cap Z(G)| = 5$. But, using Theorem 2.2.6, we see that $\Pr(G) < \frac{11}{75}$.

Thus, in view of Remark 2.2.1, the theorem is completely proved. $\square$

We conclude the section with the following remark.

Remark 2.3.5. In [44, Section IV], Rusin classifies all finite groups G with $\Pr(G) > \frac{11}{32}$. However, there are a few of points that are worth noting.

(a) In Case 2, he surprisingly misses out one situation, namely,

$$\Pr(G) = \frac{5}{14},\ G' \cong C_7,\ G' \cap Z(G) = \{1\},\ \frac{G}{Z(G)} \cong D_{14},$$

where D_{14} is the dihedral group of order 14. Accordingly, this situation does not appear in Table 1.5.3.

(b) In Case 3, he claims to have been able to show that if $|G'| = 4$ and $|G' \cap Z(G)| = 2$, then

$$\Pr(G) = \frac{1}{4}\left(1 + \frac{1}{2^{2t}} + \frac{1}{2} \cdot \frac{1}{2^{2s}}\right),$$

where $2^{2s} = |C_G(G') : Z(C_G(G'))|$, $2^{2t} = |\frac{G}{G' \cap Z(G)} : Z(\frac{G}{G' \cap Z(G)})|$ and $s + 1 \geq t \geq 1$. But, as noted in Theorem 2.2.6, we always have $t = 1$, and in that case, the value of $\Pr(G)$ obtained by him coincides with the one given by Theorem 2.2.6(a) for $p = 2$.

(c) While summarizing all the possibilities for $\Pr(G)$, Rusin writes that if $C_2 \times C_2 \cong G' \subseteq Z(G)$, then $\frac{G}{Z(G)} \cong C_2^3$ or C_2^4, no matter whether $\Pr(G) = \frac{7}{16}$ or $\frac{25}{64}$ (compare with Table 1.5.3). However, arguing in the same manner as we have done in a similar situation in the proof of Theorem 2.3.3, namely, $C_3 \times C_3 \cong G' \subseteq Z(G)$, it can be seen that $\frac{G}{Z(G)} \cong C_2^3$ or C_2^4 according as $\Pr(G) = \frac{7}{16}$ or $\frac{25}{64}$.

(d) He also writes that if $\Pr(G) = \frac{3}{8}$, $G' \cong C_6$ and $G' \cap Z(G) \cong C_2$, then $\frac{G}{Z(G)} \cong C_2 \times S_3$ or T, where T is the non-abelian group of order 12 besides A_4 and $C_2 \times S_3$ (compare with Table 1.5.3). However, it is well-known that $T \ncong \frac{G}{Z(G)}$ for any G.

2.4 A lower bound for $\Pr(G)$

Given a finite group G with $|\operatorname{cd}(G)| = 2$, M. R. Pournaki and R. Sobhani [40, Corollary 2.3] have proved that

$$\Pr(G) \geq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{|G : Z(G)|}\right)$$

with equality if and only if G is of central type.

In this section, we obtain this lower bound for $\Pr(G)$ without imposing any additional restriction on G. We also derive certain necessary and sufficient conditions, in terms of standard group-theoretic concepts, for the attainment of this bound. As a consequence we obtain some characterizations for finite nilpotent groups whose commutator subgroups have prime order. In particular, we prove certain results, concerning finite groups having p as the smallest prime dividing their orders, whose proofs are either not available or not easily accessible in the literature.

Theorem 2.4.1. *If G is a finite group, then*

$$\Pr(G) \geq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{|G : Z(G)|}\right).$$

In particular, $\Pr(G) > \frac{1}{|G'|}$ if G is non-abelian.

Proof. We prove this theorem in two different ways — one using the class equation (1.1.e) and the other using the degree equation (1.2.c).

Class equation method: Let $x_1, x_2, \ldots, x_t$ constitute the complete set of representatives of the conjugacy classes in G consisting of non-central elements. Clearly, $t = k(G) - |Z(G)|$. So, by the class equation, we have

$$|G| \;=\; |Z(G)| + \sum_{i=1}^{t} |\operatorname{C\ell}_G(x_i)| \;\leq\; |Z(G)| + |G'|(k(G) - |Z(G)|),$$

using (1.1.d). Thus,

$$\Pr(G) = \frac{k(G)}{|G|} \geq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{|G : Z(G)|}\right).$$

Degree equation method: Note that $\chi(1)^2 \leq |G : Z(G)|$ for all $\chi \in \operatorname{Irr}(G)$. Also, the number of linear characters in $\operatorname{Irr}(G)$ is given by $|G : G'|$. So, by the degree equation,

$$\begin{aligned} |G| &= |G : G'| + \sum_{\substack{\chi \in \operatorname{Irr}(G) \\ \chi(1) \neq 1}} \chi(1)^2 \\ &\leq |G : G'| + \sum_{\substack{\chi \in \operatorname{Irr}(G) \\ \chi(1) \neq 1}} |G : Z(G)| \\ &= |G : G'| + |G : Z(G)|(k(G) - |G : G'|). \end{aligned}$$

Thus, once again, we have the desired inequality. □

Remark 2.4.2. If G is a finite group, then, using Result 1.5.7 with $H = Z(G)$, we also have

$$\Pr(G) \geq \frac{1}{|G : Z(G)|^2}.$$

However, it can be readily checked that

$$\frac{1}{|G:Z(G)|^2} \leq \frac{1}{|G'|}\left(1+\frac{|G'|-1}{|G:Z(G)|}\right)$$

with equality if and only if G is abelian.

The following theorem while providing us with several equivalent conditions, that are necessary as well as sufficient for equality to hold in Theorem 2.4.1, relates itself to the subject matter of [17] and [36], dealing respectively with the groups of central type that are nilpotent and the CN-groups, that is, the groups in which the centralizer of every element is normal. It is also very much in line with Remark 1.1.2.

Theorem 2.4.3. *For a finite non-abelian group G, the statements given below are equivalent.*

(a) $\Pr(G) = \dfrac{1}{|G'|}\left(1+\dfrac{|G'|-1}{|G:Z(G)|}\right)$.

(b) $\mathrm{cd}(G) = \{1, |G:Z(G)|^{1/2}\}$, *which means that G is of central type with* $|\,\mathrm{cd}(G)| = 2$.

(c) $|\,\mathrm{C}\ell_G(x)| = |G'|$ *for all* $x \in G - Z(G)$.

(d) $\mathrm{C}\ell_G(x) = G'x$ *for all* $x \in G - Z(G)$*; in particular, G is a nilpotent group of class* 2.

(e) $C_G(x) \trianglelefteq G$ *and* $G' \cong \frac{G}{C_G(x)}$ *for all* $x \in G - Z(G)$*; in particular, G is a CN-group.*

(f) $G' = \{[y,x] : y \in G\}$ *for all* $x \in G - Z(G)$*; in particular, every element of G' is a commutator.*

Proof. The equivalence of (a) and (b) follows from the degree equation method used for proving Theorem 2.4.1; on the other hand, the class equation method gives the equivalence of (a) and (c).

The equivalence of (c) and (d) follows from (1.1.*d*). For the particular case in (d), note that if $G' \nsubseteq Z(G)$, then there exists a commutator $g \in G - Z(G)$, and so, we have $C\ell_G(g) = G'g = G'$, which is impossible.

If (d) holds, then, for each $x \in G - Z(G)$, the map $f : G \longrightarrow G'$, given by $f(y) = yxy^{-1}x^{-1}$, defines a surjective homomorphism with kernel $C_G(x)$. Thus (e) holds. On the other hand, (c) follows immediately from (e).

Finally, it is easy to see that (d) and (f) are equivalent. □

Theorem 2.4.1 and Theorem 2.4.3 not only allow us to obtain some characterizations for finite nilpotent groups of class 2 whose commutator subgroups have prime order, but also enable us to re-establish certain facts (essentially due to K. S. Joseph [26]) concerning the smallest prime divisors of the orders of finite groups.

Proposition 2.4.4. *Let G be a finite group and p be the smallest prime divisor of $|G|$.*

(a) *If $p \neq 2$, then* $\Pr(G) \neq \frac{1}{p}$.

(b) *When G is non-abelian,* $\Pr(G) > \frac{1}{p}$ *if and only if* $|G'| = p$ *and* $G' \subseteq Z(G)$.

Proof. (a) If $\Pr(G) = \frac{1}{p}$, then Result 1.5.2 gives $|G'| \leq p + 1$. In addition, if $p \neq 2$, we have $|G'| = p$. But then, by Theorem 2.4.1, we have $\Pr(G) > \frac{1}{p}$ which is a contradiction. This proves part (a).

(b) If $\Pr(G) > \frac{1}{p}$, Result 1.5.2 gives $|G'| < p+1$, whence $|G'| = p$. Now, by Lemma 2.1.1(a), we have

$$\left|\frac{G}{C_G(G')}\right| \leq |\operatorname{Aut}(G')| = p-1.$$

Hence, we must have $C_G(G') = G$; equivalently, $G' \subseteq Z(G)$. This proves part (b), noting that its converse follows from Theorem 2.4.1. □

As an immediate consequence, we have

Corollary 2.4.5. *If G is a finite group with $\Pr(G) = \frac{1}{3}$, then $|G|$ is even.*

From Proposition 2.4.4, we also have, as an immediate corollary, the following improvement to Result 1.5.6.

Corollary 2.4.6. *Let G be a finite group and $p \neq 2$ be the smallest prime divisor of $|G|$. If G is non-abelian with $G' \cap Z(G) = \{1\}$, then $\Pr(G) < \frac{1}{p}$.*

Finally, in this section we have the following result.

Proposition 2.4.7. *Let G be a finite group and p be a prime. Then the following statements are equivalent.*

(a) *$|G'| = p$ and $G' \subseteq Z(G)$.*

(b) *G is of central type with $|\operatorname{cd}(G)| = 2$ and $|G'| = p$.*

(c) *G is a direct product of a p-group P and an abelian group A such that $|P'| = p$ and $\gcd(p, |A|) = 1$.*

(d) *G is isoclinic to an extra-special p-group; consequently, $|G : Z(G)| = p^{2k}$ for some positive integer k.*

In particular, if G is non-abelian and p is the smallest prime divisor of $|G|$, then the above statements are also equivalent to the condition $\Pr(G) > \frac{1}{p}$.

Proof. The equivalence of (a) and (b) follows from Theorem 2.4.3(b)(d) and Result 1.2.7.

In view of Result 1.1.3, (c) follows from (a), considering P to be the Sylow p-subgroup of G and A, the product of the other Sylow subgroups (if any) of G.

If (c) holds, then G is isoclinic to the p-group P. Since $|P'| = p$ and $P' \cap Z(P) \neq \{1\}$, we have $P' \subseteq Z(P)$. Therefore, from Result 1.1.8, it follows that P is isoclinic to a finite group H such that $Z(H) = H' \cong P'$, which in view of Result 1.1.3, makes H into an extra-special p-group. Thus, (d) follows from the fact that isoclinism is transitive (using Result 1.1.6 for the second part).

If (d) holds, then it follows that $|G'| = p$ and $G/Z(G)$ is abelian. Hence, we have (a).

The particular case follows from Proposition 2.4.4(b). □

Remark 2.4.8. In view of Result 1.2.8, the expression $|\operatorname{cd}(G)| = 2$ in the statement (b) of Proposition 2.4.7 is superfluous.

2.5 Some additional observations

Consider the symmetric group S_n of degree $n \geq 3$ and the corresponding alternating group A_n. It is well-known that

$$\Pr(S_n) = \frac{P(n)}{n!}, \tag{2.5.a}$$

where $P(n)$ denotes the number of partitions of n. This, in fact, follows from a well-known result that $k(S_n) = P(n)$, where $k(S_n)$ is the number of conjugacy classes of S_n.

In [7], J. Dénes, P. Erdös and P. Turán have derived that $k(A_n) = \frac{1}{2}(P(n)+3Q(n))$, where $Q(n)$ is the number of partitions of n having distinct odd parts. Therefore, it follows that

$$\Pr(A_n) = \Pr(S_n) + \frac{3Q(n)}{n!}.$$

Thus, $\Pr(A_n) > \Pr(S_n)$.

Consider the dihedral group D_{2n}, $n \geq 1$, and the quaternion group $Q_{2^{n+1}}$, $n \geq 2$. In [31], P. Lescot has deduced that

$$\Pr(D_{2n}) = \begin{cases} \dfrac{n+3}{4n} & \text{if } n \text{ is odd} \\ \dfrac{n+6}{4n} & \text{if } n \text{ is even} \end{cases}$$

and

$$\Pr(Q_{2^{n+1}}) = \frac{2^{n-1}+3}{2^{n+1}}.$$

Clearly, $\Pr(D_{2n}) \to \frac{1}{4}$ and $\Pr(Q_{2^{n+1}}) \to \frac{1}{4}$ as $n \to \infty$. In this regard, Lescot enquired whether there is any other natural family of groups with the same property. It may be mentioned here that the following groups also have the same property:

$$\begin{aligned} M_{2mn} &= \langle a, b : a^m = b^{2n} = 1, bab^{-1} = a^{-1} \rangle, \\ Q_{4m} &= \langle a, b : a^{2m} = 1, b^2 = a^m, bab^{-1} = a^{-1} \rangle \\ \text{and} \quad SD_{2^n} &= \langle a, b : a^{2^{n-1}} = b^2 = 1, bab^{-1} = a^{-1+2^{n-2}} \rangle. \end{aligned}$$

This is because certain tedious computations yield

$$\Pr(M_{2mn}) = \begin{cases} \dfrac{m+3}{4m} & \text{if } m \text{ is odd} \\ \dfrac{m+6}{4m} & \text{if } m \text{ is even,} \end{cases}$$

$$\Pr(Q_{4m}) = \frac{m+3}{4m}$$

$$\text{and} \quad \Pr(SD_{2^n}) = \frac{2^{n-2}+3}{2^n}.$$

In [16, Corollary 1.2], I. V. Erovenko and B. Sury have shown, in particular, that for every integer $k > 1$ there exists a family $\{G_n\}$ of finite groups such that $\Pr(G_n) \to \frac{1}{k^2}$ as $n \to \infty$. In this connection, we have the following observation.

Proposition 2.5.1. *For every integer $k > 1$ there exists a family $\{G_n\}$ of finite groups such that $\Pr(G_n) \to \frac{1}{k}$ as $n \to \infty$.*

Proof. In view of Result 1.5.4, it is enough to show the existence of a family of finite groups $\{G_n\}$ such that $\Pr(G_n) \to \frac{1}{p}$ as $n \to \infty$. Put $G_n = ES(n, p)$, an extra-special p-group of order p^{2n+1}. Then by Result 1.5.9, we have

$$\Pr(G_n) = \frac{1}{p} + \frac{p-1}{p^{2n+1}} \to \frac{1}{p} \quad \text{as } n \to \infty.$$

This completes the proof. □

We conclude this section with the following proposition which says that the reciprocal of every positive integer can be realized as the commutativity degree of some finite group.

Proposition 2.5.2. *For every positive integer n there exists a finite group G such that $\Pr(G) = \frac{1}{n}$.*

Proof. We shall prove the proposition by induction on n. If $n = 1$, we may take G to be any abelian group. If $n = 2$, we may take, in view of (2.5.a), $G = S_3$. So, assume that $n \geq 3$ and that the proposition is true for all positive integers $k < n$.

Case 1. $n \equiv 0$ or $2 \pmod 4$.

In this case, $n = 2^\alpha.m$, where α, m are positive integers and m is odd. Clearly $m < n$. So, by induction hypothesis there exists a finite group G such that $\Pr(G) = \frac{1}{m}$. Hence, using (2.5.a) and Result 1.5.4, we have

$$\Pr(G \times (S_3)^\alpha) = \Pr(G).(\Pr(S_3))^\alpha = \frac{1}{m.2^\alpha} = \frac{1}{n}.$$

Case 2. $n \equiv 1 \pmod 4$.

In this case, $\frac{n+3}{4}$ is a positive integer and $\frac{n+3}{4} < n$. So, by induction hypothesis, there exists a finite group G such that $\Pr(G) = \frac{4}{n+3}$. Hence,

$$\Pr(D_{2n} \times G) = \frac{n+3}{4n}.\frac{4}{n+3} = \frac{1}{n}.$$

Case 3. $n \equiv 3 \pmod 4$.

In this case, $\frac{n+1}{4}$ is a positive integer and $\frac{n+1}{4} < n$. So, by induction hypothesis, there exists a finite group G such that $\Pr(G) = \frac{4}{n+1}$. Hence,

$$\Pr(D_{6n} \times G) = \frac{3n+3}{12n}.\frac{4}{n+1} = \frac{1}{n}.$$

This completes the proof. □

Chapter 3

A class of word equations and word maps

In this chapter we generalize the classical result of F. G. Frobenius regarding the number of solutions of a commutator equation in a finite group. As a consequence, we obtain a class of almost measure preserving word maps on finite simple groups.

This chapter is based on our papers [5] and [6].

3.1 A generalization of Frobenius' result

Let $F(x_1, x_2, \ldots, x_n)$ be the free group of words on n generators $x_1, x_2, \ldots, x_n$. For $1 \leq i \leq n$, we write '$x_i \in \omega(x_1, x_2, \ldots, x_n)$' to mean that x_i has a non-zero index (that is, x_i^k forms a syllable, with $0 \neq k \in \mathbb{Z}$) in the word $\omega(x_1, x_2, \ldots, x_n) \in F(x_1, x_2, \ldots, x_n)$. Let us call a word $\omega(x_1, x_2, \ldots, x_n)$

admissible if each $x_i \in \omega(x_1, x_2, \ldots, x_n)$ has precisely two non-zero indices, namely, $+1$ and -1. Let $\mathscr{A}(x_1, x_2, \ldots, x_n)$ denote the set of all admissible words in $F(x_1, x_2, \ldots, x_n)$.

Given a finite group G and an element $g \in G$, let $\zeta_n^{\omega}(g)$ denote the number of solutions $(g_1, g_2, \ldots, g_n) \in G^n$ of the word equation $\omega(x_1, x_2, \ldots, x_n) = g$, where $G^n = G \times G \times \cdots \times G$ (n times). Thus,

$$\zeta_n^{\omega}(g) = |\{(g_1, g_2, \ldots, g_n) \in G^n : \omega(g_1, g_2, \ldots, g_n) = g\}|,$$

where $\omega(g_1, g_2, \ldots, g_n)$ denotes the image of $\omega(x_1, x_2, \ldots, x_n)$ under the unique natural homomorphism $\tau : F(x_1, x_2, \ldots, x_n) \longrightarrow G$ which maps x_i to g_i, $1 \leq i \leq n$. Conventionally, $\zeta_0^{\omega}(g) = 1$ if $g = 1$ and zero otherwise.

Lemma 3.1.1. *Let G be a finite group. Let f be an automorphism of $F(x_1, x_2, \ldots, x_n)$, $n \geq 1$. If $\omega_1(x_1, x_2, \ldots, x_n)$ and $\omega_2(x_1, x_2, \ldots, x_n)$ are any two admissible words in $F(x_1, x_2, \ldots, x_n)$ such that $f(\omega_1(x_1, x_2, \ldots, x_n)) = \omega_2(x_1, x_2, \ldots, x_n)$, then*

$$\zeta_n^{\omega_1}(g) = \zeta_n^{\omega_2}(g)$$

for all $g \in G$.

Proof. Let $(g_1, g_2, \ldots, g_n) \in G^n$ be such that $\omega_2(g_1, g_2, \ldots, g_n) = g$. This means that, if $\tau : F(x_1, x_2, \ldots, x_n) \to G$ denotes the unique natural homomorphism given by $x_i \mapsto g_i$ for $1 \leq i \leq n$, we have

$$\begin{aligned} &\tau(\omega_2(x_1, x_2, \ldots, x_n)) = g \\ \text{or,} \quad &(\tau \circ f)(\omega_1(x_1, x_2, \ldots, x_n)) = g \\ \text{or,} \quad &\omega_1(h_1, h_2, \ldots, h_n) = g, \end{aligned}$$

putting $h_i = (\tau \circ f)(x_i) \in G$ for $1 \leq i \leq n$; it may be noted here that $\tau \circ f$ is the unique natural homomorphism from $F(x_1, x_2, \ldots, x_n)$ to G which maps each x_i to h_i. Thus, to every solution $(g_1, g_2, \ldots, g_n)$ of $\omega_2(x_1, x_2, \ldots, x_n) = g$ there corresponds a solution $(h_1, h_2, \ldots, h_n)$ of $\omega_1(x_1, x_2, \ldots, x_n) = g$. Since f is an automorphism, it follows that this correspondence is bijective. This proves the lemma. □

Remark 3.1.2. For each $\sigma \in S_n$, the symmetric group of degree n, and for each $e_i \in \{1, -1\}$, $1 \leq i \leq n$, we have an automorphism

$$f : F(x_1, x_2, \ldots, x_n) \longrightarrow F(x_{\sigma(1)}^{e_1}, x_{\sigma(2)}^{e_2}, \ldots, x_{\sigma(n)}^{e_n}) = F(x_1, x_2, \ldots, x_n)$$

which maps each x_i to $x_{\sigma(i)}^{e_i}$, $1 \leq i \leq n$.

Remark 3.1.3. If $\omega(x_1, x_2, \ldots, x_n) \in \mathscr{A}(x_1, x_2, \ldots, x_n)$ with $x_i \notin \omega(x_1, x_2, \ldots, x_n)$ for some i, then

$$\omega(x_1, x_2, \ldots, x_n) = \omega_i(x_1, \ldots, \widehat{x}_i, \ldots, x_n)$$

for some $\omega_i(x_1, \ldots, \widehat{x}_i, \ldots, x_n) \in \mathscr{A}(x_1, \ldots, \widehat{x}_i, \ldots, x_n)$, where $\widehat{x}_i$ means that x_i is omitted. Moreover, we have

$$\zeta_n^{\omega}(g) = |G|\zeta_{n-1}^{\omega_i}(g) \;\; \forall \;\; g \in G.$$

We now state and prove the main result of this section as follows.

Theorem 3.1.4. *Let $\omega(x_1, x_2, \ldots, x_n) \in \mathscr{A}(x_1, x_2, \ldots, x_n)$, $n \geq 1$. If G is a finite group, then the map $\zeta_n^{\omega} : G \longrightarrow \mathbb{C}$ defined by*

$$\zeta_n^{\omega}(g) = |\{(g_1, g_2, \ldots, g_n) \in G^n : \omega(g_1, g_2, \ldots, g_n) = g\}|, \;\; g \in G,$$

is a character of G.

Proof. We shall, in fact, derive several inductive formulae for $\zeta_n^\omega(g)$. First note that $\forall\ h, g \in G$, the maps $g_i \mapsto h^{-1}g_ih$, $1 \leq i \leq n$, give rise to a one to one correspondence between the solutions of the equations

$$\omega(x_1, x_2, \ldots, x_n) = g \quad \text{and} \quad \omega(x_1, x_2, \ldots, x_n) = h^{-1}gh.$$

So, it follows that $\zeta_n^\omega : G \to \mathbb{C}$ is a class function on G. We also observe, by Remark 3.1.3, that if $\omega(x_1, x_2, \ldots, x_n) = 1$, the trivial word, then

$$\zeta_n^\omega(g) = \begin{cases} |G|^n & \text{if } \ g = 1 \\ 0 & \text{if } \ g \neq 1. \end{cases}$$

This clearly defines a character of G, namely, the multiple of the regular character of G by $|G|^{n-1}$. It may be recalled that by a *regular character* of G we mean a character $\rho : G \longrightarrow \mathbb{C}$ such that, for $g \in G$, $\rho(g) = |G|$ or 0 according as $g = 1$ or $g \neq 1$. So, it is enough to prove the theorem for non-trivial words in $\mathscr{A}(x_1, x_2, \ldots, x_n)$, and we shall do so using induction on n, the numbers of generators $x_1, x_2, \ldots, x_n$.

Obviously, there is nothing to prove when $n = 1$. So, let us assume that the theorem is true for all $n < k$, where $k \geq 2$.

Let $\omega(x_1, x_2, \ldots, x_k) \in \mathscr{A}(x_1, x_2, \ldots, x_k)$. Then, in view of Lemma 3.1.1 and Remark 3.1.2, we may permute $x_1, x_2, \ldots, x_k$ suitably to see that the equation $\omega(x_1, x_2, \ldots, x_k) = g$ possesses the same number of solutions in G^k as does the equation

$$x_1\omega_1(x_2, x_3, \ldots, x_k)x_1{}^{-1}\omega_2(x_2, x_3, \ldots, x_k) = g, \tag{3.1.a}$$

where $\omega_1(x_2, x_3, \ldots, x_k), \omega_2(x_2, x_3, \ldots, x_k) \in F(x_1, x_2, \ldots, x_k)$ with the property that, $\forall\ i = 1, 2$, each $x_j \in \omega_i(x_2, x_3, \ldots, x_k)$, $2 \leq j \leq k$, has index

+1 and/or −1. Note that we may or may not have $\omega_i(x_2, x_3, \ldots, x_k) \in \mathscr{A}(x_2, x_3, \ldots, x_k)$. In fact, $\omega_1(x_2, x_3, \ldots, x_k) \in \mathscr{A}(x_2, x_3, \ldots, x_k)$ if and only if $\omega_2(x_2, x_3, \ldots, x_k) \in \mathscr{A}(x_2, x_3, \ldots, x_k)$. Also, it is possible that we may have $\omega_2(x_2, x_3, \ldots, x_k) = 1$. However, if $\omega_1(x_2, x_3, \ldots, x_k) = 1$, then, by the induction hypothesis, there is nothing to prove.

We shall complete the proof of the theorem considering some cases and subcases as follows:

Case 1. $\omega_2(x_2, x_3, \ldots, x_k) \in \mathscr{A}(x_2, x_3, \ldots, x_k)$.

In this case, we also have $\omega_1(x_2, x_3, \ldots, x_k) \in \mathscr{A}(x_2, x_3, \ldots, x_k)$, as mentioned above, and we shall settle this case in two subcases.

Subcase 1.1. $\omega_2(x_2, x_3, \ldots, x_k) \neq 1$.

In this case, since

$$x_1\omega_1(x_2, x_3, \ldots, x_k){x_1}^{-1}\omega_2(x_2, x_3, \ldots, x_k) \in \mathscr{A}(x_1, x_2, \ldots, x_k),$$

it follows that $\omega_2(x_2, x_3, \ldots, x_k)$ and $x_1\omega_1(x_2, x_3, \ldots, x_k)x_1^{-1}$ are admissible words in less than k generators (see Remark 3.1.3). In fact, there exist positive integers $r, s < k$ with $r + s = k$ such that

$$\omega_2(x_2, x_3, \ldots, x_k) = \omega_3(x_{i_1}, x_{i_2}, \ldots, x_{i_r}) \in \mathscr{A}(x_{i_1}, x_{i_2}, \ldots, x_{i_r})$$

and

$$x_1\omega_1(x_2, x_3, \ldots, x_k){x_1}^{-1} = \omega_4(x_1, x_{j_2}, \ldots, x_{j_s}) \in \mathscr{A}(x_1, x_{j_2}, \ldots, x_{j_s}),$$

where $2 \leq i_p \neq j_q \leq k \;\; \forall\, p = 1, 2, \ldots, r$ and $\forall\, q = 2, 3, \ldots, s$. Consider now the word equations

$$\omega_3(x_{i_1}, x_{i_2}, \ldots, x_{i_r}) = h$$

$$\text{and} \qquad \omega_4(x_1, x_{j_2}, \ldots, x_{j_s}) = gh^{-1},$$

where $h \in G$. By induction hypothesis, both $\zeta_r^{\omega_3}$ and $\zeta_s^{\omega_4}$ are characters of G. Then, the number of solutions of the word equation $(3.1.a)$ is given by

$$\begin{aligned}
\zeta_k^{\omega}(g) &= \sum_{h\in G}\zeta_r^{\omega_3}(h)\,\zeta_s^{\omega_4}(gh^{-1}) \\
&= \sum_{h\in G}\Big(\sum_{\chi\in \mathrm{Irr}(G)}[\zeta_r^{\omega_3},\chi]\,\chi(h)\Big)\Big(\sum_{\psi\in \mathrm{Irr}(G)}[\zeta_s^{\omega_4},\psi]\,\psi(gh^{-1})\Big) \\
&= \sum_{\chi\in \mathrm{Irr}(G)}[\zeta_r^{\omega_3},\chi][\zeta_s^{\omega_4},\chi]\,\frac{|G|}{\chi(1)}\,\chi(g) \qquad (3.1.b)
\end{aligned}$$

using the generalized orthogonality relation $(1.2.g)$. Hence, it follows that ζ_k^{ω} is a character of G.

Subcase 1.2. $\quad \omega_2(x_2, x_3, \ldots, x_k) = 1$.

In this case, the word equation $(3.1.a)$ becomes

$$x_1\omega_1(x_2, x_3, \ldots, x_k)x_1^{-1} = g. \qquad (3.1.c)$$

For $h \in G$, consider the equation

$$\omega_1(x_2, x_3, \ldots, x_k) = h^{-1}gh.$$

By induction hypothesis, $\zeta_{k-1}^{\omega_1}$ is a character of G. So, the number of solutions of the word equation $(3.1.c)$, that is, of the word equation $(3.1.a)$, is given by

$$\zeta_k^{\omega}(g) = \sum_{h\in G}\zeta_{k-1}^{\omega_1}(h^{-1}gh) = |G|\zeta_{k-1}^{\omega_1}(g). \qquad (3.1.d)$$

Hence, it follows that ζ_k^ω is a character of G.

Case 2. $\omega_2(x_2, x_3, \ldots, x_k) \notin \mathscr{A}(x_2, x_3, \ldots, x_k)$.

In this case, there exists an x_i, $2 \leq i \leq k$, such that the index of x_i in $\omega_2(x_2, x_3, \ldots, x_k)$ is either $+1$ or -1. In view of Lemma 3.1.1 and Remark 3.1.2, we may assume without any loss that $i = 2$ and the index of x_2 in $\omega_2(x_2, x_3, \ldots, x_k)$ is $+1$. Consequently, the index of x_2 in $\omega_1(x_2, x_3, \ldots, x_k)$ is -1.

Let us put $\omega_2(x_2, x_3, \ldots, x_k) = \xi$. Then we can write

$$x_2 = \omega_3(x_3, \ldots, x_k)\xi\omega_4(x_3, \ldots, x_k) \qquad (3.1.e)$$

for some $\omega_3(x_3, \ldots, x_k)$, $\omega_4(x_3, \ldots, x_k) \in F(x_3, \ldots, x_k)$. Putting this value of x_2 in $\omega_1(x_2, x_3, \ldots, x_k)$ and then replacing ξ by x_2^{-1}, we may rewrite the word equation $(3.1.a)$ as

$$x_1\omega_5(x_2, \ldots, x_k)x_1^{-1}x_2^{-1} = g, \qquad (3.1.f)$$

where $\omega_5(x_2, \ldots, x_k) \in F(x_2, \ldots, x_k)$. From $(3.1.e)$, it follows that the free group $F(x_1, x_2, \ldots, x_k)$ is also generated by $x_1, \xi, x_3, \ldots, x_k$. As such, there is an automorphism of $F(x_1, x_2, \ldots, x_k)$ which maps ξ to x_2^{-1} and fixes each x_i, where $i \neq 2$. This automorphism transforms the word equation $(3.1.a)$ into the word equation (3.1.*f*), and so, from Lemma 3.1.1, it follows that the two equations have the same number of solutions in G^k. Now,

$$\omega_5(x_2, \ldots, x_k) = \omega_6(x_3, \ldots, x_k)x_2\omega_7(x_3, \ldots, x_k), \qquad (3.1.g)$$

where $\omega_6(x_3, \ldots, x_k)$, $\omega_7(x_3, \ldots, x_k) \in F(x_3, \ldots, x_k)$. Note that we may have one or both of $\omega_6(x_3, \ldots, x_k)$ and $\omega_7(x_3, \ldots, x_k)$ equal to 1.

Let $(g_1, g_2, \ldots, g_k) \in G^k$. Let $\chi \in \mathrm{Irr}(G)$, and Φ_χ be a representation of G affording χ. Then, using (1.2.d), we have

$$\sum_{g_1 \in G} \Phi_\chi(g_1 \omega_5(g_2, \ldots, g_k) g_1^{-1}) = \frac{|G|}{\chi(1)} \chi(\omega_5(g_2, \ldots, g_k))\, \mathrm{I}_\chi .$$

Multiplying this equality on the right by $\Phi_\chi(g_2^{-1})$ and then summing over all $g_2, g_3, \ldots, g_k \in G$, we get

$$\sum_{g_1, \quad, g_k \in G} \Phi_\chi(g_1 \omega_5(g_2, \ldots, g_k) g_1^{-1} g_2^{-1}) = \frac{|G|}{\chi(1)} \sum_{g_2, \quad, g_k \in G} \chi(\omega_5(g_2, \ldots, g_k)) \Phi_\chi(g_2^{-1}).$$

This, on taking trace, gives

$$\sum_{g_1, \quad, g_k \in G} \chi(g_1 \omega_5(g_2, \ldots, g_k) g_1^{-1} g_2^{-1}) = \frac{|G|}{\chi(1)} \sum_{g_2, \quad, g_k \in G} \chi(\omega_5(g_2, \ldots, g_k)) \chi(g_2^{-1}).$$

The left side of this equality is

$$\sum_{g \in G} \zeta_k^\omega(g) \chi(g) = |G| \overline{[\zeta_k^\omega, \chi]}.$$

Thus, we have

$$\overline{[\zeta_k^\omega, \chi]} = \frac{1}{\chi(1)} \sum_{g_2, \quad, g_k \in G} \chi(\omega_5(g_2, \ldots, g_k)) \chi(g_2^{-1}). \qquad (3.1.h)$$

Note that, if $k = 2$, then, in view of the first orthogonality relation (1.2.h), the expression (3.1.h) becomes

$$[\zeta_2^\omega, \chi] = \frac{|G|}{\chi(1)}.$$

This in turn gives the famous formula due to Frobenius, namely,

$$\zeta_2^{\omega}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|}{\chi(1)} \chi(g).$$

Thus, ζ_2^{ω} is a character of G. So, we assume that $k \geq 3$.

Consider now the word equation

$$\omega_8(x_3, \ldots, x_k) = \omega_7(x_3, \ldots, x_k)\omega_6(x_3, \ldots, x_k) = h, \qquad (3.1.i)$$

where $h \in G$. By induction hypothesis, $\zeta_{k-2}^{\omega_8}$ is a character of G. Also, since $\omega_6(g_3, \ldots, g_k)g_2\omega_7(g_3, \ldots, g_k)$ and $g_2\omega_7(g_3, \ldots, g_k)\omega_6(g_3, \ldots, g_k)$ are conjugates in G, it follows from (3.1.g) that

$$\chi(\omega_5(g_2, \ldots, g_k)) = \chi(g_2\omega_7(g_3, \ldots, g_k)\omega_6(g_3, \ldots, g_k)).$$

So, from (3.1.h), we have

$$\begin{aligned}
\overline{[\zeta_k^{\omega}, \chi]} &= \frac{1}{\chi(1)} \sum_{g_3, \ldots, g_k \in G} \sum_{g_2 \in G} \chi(g_2\omega_7(g_3, \ldots, g_k)\omega_6(g_3, \ldots, g_k))\chi(g_2^{-1}) \\
&= \frac{1}{\chi(1)} \sum_{h \in G} \zeta_{k-2}^{\omega_8}(h) \sum_{g_2 \in G} \chi(g_2 h)\chi(g_2^{-1}), \qquad \text{using } (3.1.i) \\
&= \frac{1}{\chi(1)} \sum_{h \in G} \zeta_{k-2}^{\omega_8}(h) \frac{\chi(h)}{\chi(1)} |G|, \qquad \text{using } (1.2.g) \\
&= \left(\frac{|G|}{\chi(1)}\right)^2 \overline{[\zeta_{k-2}^{\omega_8}, \chi]} \qquad \text{for all } \chi \in \mathrm{Irr}(G).
\end{aligned}$$

Thus,

$$\zeta_k^{\omega}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \left(\frac{|G|}{\chi(1)}\right)^2 [\zeta_{k-2}^{\omega_8}, \chi]\, \chi(g). \qquad (3.1.j)$$

Hence, it follows that ζ_k^{ω} is a character of G. This completes the proof of the theorem. □

It may be mentioned here that if the structure of the admissible word $\omega(x_1, x_2, \ldots, x_n)$ is known to us, then, for each $g \in G$, the technique adopted in the proof of Theorem 3.1.4 can also be used to derive an explicit formula for the number of solutions of the word equation $\omega(x_1, x_2, \ldots, x_n) = g$ in terms of the irreducible characters of G. We illustrate this as follows.

Consider the word equation

$$x_1 x_2 \ldots x_{n+1} x_1^{-1} x_{n+2} x_2^{-1} \ldots x_{n+1}^{-1} x_{n+2}^{-1} = g, \qquad (3.1.k)$$

where $n \geq 1$. Then, proceeding in the same way as we did in *Case* 2 in the proof of Theorem 3.1.4, we have

$$\begin{aligned} \omega(x_1, x_2, \ldots, x_{n+2}) &= x_1 x_2 \ldots x_{n+1} x_1^{-1} x_{n+2} x_2^{-1} \ldots x_{n+1}^{-1} x_{n+2}^{-1} \\ \text{and} \quad \omega_8(x_3, x_4, \ldots, x_{n+2}) &= x_{n+2} x_3 x_4 \ldots x_{n+1} x_3^{-1} x_4^{-1} \ldots x_{n+1}^{-1} x_{n+2}^{-1}. \end{aligned}$$

In view of Remark 3.1.2, we see, using $(3.1.d)$ and $(1.3.e)$, that the number of solutions of the word equation

$$\omega_8(x_3, x_4, \ldots, x_{n+2}) = h,$$

where $h \in G$, is given by

$$\zeta_n^{\omega_8}(h) \;=\; |G|\eta_{n-1}(h) \;=\; \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|^{n-1}}{\chi(1)^{n-1-\varepsilon_{n-1}}}\, \chi(h).$$

Therefore, by $(3.1.j)$, the number of solutions of the word equation $(3.1.k)$ is given by

$$\zeta_{n+2}^{\omega}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|^{n+1}}{\chi(1)^{n+1-\varepsilon_{n-1}}}\, \chi(g).$$

In particular, putting $n = 1$ in the word equation (3.1.*k*) and then using (1.3.*f*), we can at once see that the number of solutions of the word equation

$$x_1 x_2 x_1^{-1} x_3 x_2^{-1} x_3^{-1} \dots x_{3n-2} x_{3n-1} x_{3n-2}^{-1} x_{3n} x_{3n-1}^{-1} x_{3n}^{-1} = g$$

is given by

$$\zeta_{3n}^{\omega}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|^{3n-1}}{\chi(1)^{2n-1}} \chi(g). \tag{3.1.l}$$

Remark 3.1.5. It may be noted here that the expression (1.3.*c*) obtained by P. Kellersch and K. Meyberg can also be derived from the expressions (1.3.*a*) and (1.3.*f*) obtained by F. G. Frobenius and S. P. Strunkov respectively.

3.2 Certain measure preserving word maps

The terminologies used in this section have been described in Section 1.4 and in Section 3.1. Let G be a finite group. Let $\omega(x_1, x_2, \dots, x_n)$ be a word in $F(x_1, x_2, \dots, x_n)$, and $\alpha_\omega : G^n \longrightarrow G$ be the corresponding word map given by $\alpha_\omega(g_1, g_2, \dots, g_n) = \omega(g_1, g_2, \dots, g_n)$. In this case, we say that the map α_ω is induced by ω. In [46, Problem 2.10], A. Shalev asks — *Which words induce almost measure preserving maps on finite simple groups.* In this section, we show that if G is simple and $\omega(x_1, x_2, \dots, x_n)$ is a non-trivial admissible word, then α_ω is almost measure preserving, and almost all the elements of G can be expressed as $\omega(g_1, g_2, \dots, g_n)$ for some $g_1, g_2, \dots, g_n \in G$. It may be mentioned here that S. Garion and A. Shalev [19, Theorem 7.4, Corollary 7.5] have made such conclusions considering the word $x_1^2 x_2^2$ and the words which correspond to n-fold commutators in some arrangement of brackets.

Needless to mention that every admissible word does not correspond to an n-fold commutator, for example, $x_1x_2\dots x_nx_1^{-1}x_2^{-1}\dots x_n^{-1}$.

Let $\omega(x_1, x_2, \dots, x_n)$ be a non-trivial admissible word in $F(x_1, x_2, \dots, x_n)$ and $g \in G$. Note that

$$(\alpha_\omega)^{-1}(g) = \{(g_1, g_2, \dots, g_n) \in G^n : \omega(g_1, g_2, \dots, g_n) = g\}.$$

So, we have $|(\alpha_\omega)^{-1}(g)| = \zeta_n^\omega(g)$, the number of solutions of the word equation $\omega(x_1, x_2, \dots, x_n) = g$. Therefore, the corresponding probability distribution on G (associated to α_ω) is given by

$$P_\omega(g) := P_{\alpha_\omega}(g) = \frac{|(\alpha_\omega)^{-1}(g)|}{|G^n|} = \frac{\zeta_n^\omega(g)}{|G|^n}. \qquad (3.2.a)$$

Since ζ_n^ω is a class function on G (see Theorem 3.1.4), we have

$$\zeta_n^\omega = \sum_{\chi \in \mathrm{Irr}(G)} [\zeta_n^\omega, \chi]\chi.$$

Therefore, by (3.2.a), we have

$$P_\omega = |G|^{-1} \sum_{\chi \in \mathrm{Irr}(G)} \frac{[\zeta_n^\omega, \chi]}{|G|^{n-1}}\chi. \qquad (3.2.b)$$

The following crucial result, in fact, plays the pivotal role in enabling us to replicate the technique used by Garion and Shalev.

Proposition 3.2.1. *Let G be a finite group and $\chi \in \mathrm{Irr}(G)$. Then*

$$0 \lneq [\zeta_n^\omega, \chi] \leq \frac{|G|^{n-1}}{\chi(1)}.$$

Proof. The proof is essentially same as that of Theorem 3.1.4, except that the induction here starts at $n = 2$, when by Frobenius' formula (1.3.*a*) we have

$$\zeta_2^\omega = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|}{\chi(1)} \chi,$$

and so, for all $\chi \in \mathrm{Irr}(G)$,

$$[\zeta_2^\omega, \chi] = \frac{|G|}{\chi(1)} \gneq 0.$$

For the rest of the proof, we assume, as usual, that the result is true for all $n < k$, where $k \geq 3$. Then, for each of the expressions of ζ_k^ω, as mentioned in (3.1.*b*), (3.1.*d*) and (3.1.*j*), we have, using the induction hypothesis,

$$0 \lneq [\zeta_k^\omega, \chi] \leq \frac{|G|^{k-1}}{\chi(1)} \quad \text{for all } \chi \in \mathrm{Irr}(G).$$

This completes the proof. □

Rest of our results are quite similar to the ones obtained by Garion and Shalev. Accordingly, the so called Witten zeta function (see [50]) given by

$$\zeta^G(s) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-s}, \tag{3.2.c}$$

where s is a real number, and the quantities

$$\delta(G) = \left(\zeta^G(2) - 1\right)^{1/2},$$
$$\epsilon(G) = \left(\zeta^G(2) - 1\right)^{1/4}$$

once again play significant roles in the proofs. In [32, Theorem 1.1], it has been proved that if G is simple and $s > 1$, then $\zeta^G(s) \to 1$ as $|G| \to \infty$, which implies that $\epsilon(G) \to 0$ as $|G| \to \infty$.

Let U be the uniform distribution on G given by $U(g) = \frac{1}{|G|}$, $g \in G$. Then we have

Proposition 3.2.2. *Let G be a finite group. Then, with notations as above,* $||P_\omega - U||_1 \leq \delta(G)$.

Proof. In view of (3.2.b) and (1.4.a), we have

$$\begin{aligned}
||P_\omega - U||_1 &\leq \left(\sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi \neq 1_G}} \left| \frac{[\zeta_n^\omega, \chi]}{|G|^{n-1}} \right|^2 \right)^{1/2} \\
&\leq \left(\sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi \neq 1_G}} \frac{1}{\chi(1)^2} \right)^{1/2}, \quad \text{using Proposition 3.2.1} \\
&= \left(\zeta^G(2) - 1\right)^{1/2}, \quad \text{using (3.2.}c\text{)}.
\end{aligned}$$

This completes the proof. □

As a consequence, we obtain a lower bound for the number of group elements that are of the form $\omega(g_1, g_2, \ldots, g_n)$, where $g_1, g_2, \ldots, g_n \in G$.

Corollary 3.2.3. *Let G be a finite group. Then, with notations as above,* $|\operatorname{im} \alpha_\omega| \geq (1 - \delta(G))|G|$.

Proof. Using Proposition 3.2.2, we have

$$
\begin{aligned}
\delta(G) &\geq \sum_{g \in G} \left| P_\omega(g) - \frac{1}{|G|} \right| \\
&\geq \sum_{g \in G - \mathrm{im}\,\alpha_\omega} \left| P_\omega(g) - \frac{1}{|G|} \right| \\
&= \sum_{g \in G - \mathrm{im}\,\alpha_\omega} \left| \frac{-1}{|G|} \right| = \frac{|G| - |\mathrm{im}\,\alpha_\omega|}{|G|}.
\end{aligned}
$$

Hence, the result follows. □

The equidistribution and measure preserving properties of the map α_ω in terms of the parameter $\epsilon(G)$ are given as follows.

Proposition 3.2.4. *Every finite group G has a subset S with the following properties:*

(a) $|S| \geq (1 - \epsilon(G))|G|$;

(b) $(1 - \epsilon(G))|G|^{n-1} \leq |(\alpha_\omega)^{-1}(g)| \leq (1 + \epsilon(G))|G|^{n-1}$, *or equivalently,*

$$\frac{1 - \epsilon(G)}{|G|} \leq P_\omega(g) \leq \frac{1 + \epsilon(G)}{|G|} \quad \textit{for all } g \in S.$$

Proof. It is enough to see, using Proposition 3.2.2 and Result 1.4.2, that the map α_ω is $\epsilon(G)$-equidistributed. □

Proposition 3.2.5. *Let G be a finite group. Then, with notations as above, the map α_ω satisfies the following conditions:*

(a) $\left| \dfrac{|(\alpha_\omega)^{-1}(Y)|}{|G|^n} - \dfrac{|Y|}{|G|} \right| \leq 3\epsilon(G) \quad$ *for all* $Y \subseteq G$.

(b) *If* $X \subseteq G^n$, *then* $\dfrac{|\alpha_\omega(X)|}{|G|} \geq \dfrac{|X|}{|G|^n} - 3\epsilon(G)$.

Proof. The results follow from Result 1.4.1, noting that the map α_ω is $\epsilon(G)$-equidistributed. $\square$

Remark 3.2.6. As noted in [19, page 4633], Proposition 3.2.2 through Proposition 3.2.5 have some significance only when $G = G'$, that is, when G is a perfect group.

Finally, through the following corollary, we achieve our goal mentioned at the beginning of this section.

Corollary 3.2.7. *Let G be a finite simple group, and $o(1)$ be a real number depending on G which tends to zero as $|G| \to \infty$.*

(a) *If $Y \subseteq G$, then $\dfrac{|(\alpha_\omega)^{-1}(Y)|}{|G|^n} = \dfrac{|Y|}{|G|} + o(1)$. This means that the map α_ω is almost measure preserving.*

(b) *If $X \subseteq G^n$, then $\dfrac{|\alpha_\omega(X)|}{|G|} \geq \dfrac{|X|}{|G|^n} - o(1)$; in particular, if X is such that $|X| = (1 - o(1))|G|^n$, then $|\alpha_\omega(X)| = (1 - o(1))|G|$. This means that almost all the elements of G can be expressed as $\omega(g_1, g_2, \ldots, g_n)$ for some $g_1, g_2, \ldots, g_n \in G$.*

Proof. Follows from Proposition 3.2.5, noting that $\epsilon(G) = o(1)$. $\square$

3.3 Equations having restricted variables

In this section, we consider the number of solutions of word equations in a finite group G by restricting the choice of the values of some of the variables to a given subgroup of G. In the process we obtain yet another generalization of

Frobenius' result given by (1.3.a). Let H be a subgroup of G and $g \in G$. Let $\tilde{\zeta}(g)$ denote the number of elements $(h_1, g_2) \in H \times G$ satisfying $[h_1, g_2] = g$.

Theorem 3.3.1. *Let G be a finite group. If $H \trianglelefteq G$, then $\tilde{\zeta}$ is a class function on G and*

$$\tilde{\zeta}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|H|[\chi_H, \chi_H]}{\chi(1)} \chi(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|H|[\chi_H^G, \chi]}{\chi(1)} \chi(g)$$

for all $g \in G$.

Proof. Since for each $a \in G$, the map $(h_1, g_2) \mapsto (ah_1a^{-1}, ag_2a^{-1})$ defines a one to one correspondence between the sets $\{(h_1, g_2) \in H \times G : [h_1, g_2] = g\}$ and $\{(h_1, g_2) \in H \times G : [h_1, g_2] = aga^{-1}\}$, it follows that $\tilde{\zeta}$ is a class function on G. Thus, by (1.2.i), we have

$$\tilde{\zeta}(g) = \sum_{\chi \in \mathrm{Irr}(G)} [\tilde{\zeta}, \chi]\chi(g). \qquad (3.3.a)$$

Let $\chi \in \mathrm{Irr}(G)$, and let Φ_χ be a representation of G which affords χ. Then, using (1.2.d), we have

$$\sum_{g_2 \in G} \Phi_\chi(g_2 h_1^{-1} g_2^{-1}) = \frac{|G|}{\chi(1)} \chi(h_1^{-1})\, \mathrm{I}_\chi,$$

where $h_1 \in H$. Multiplying both sides by $\Phi_\chi(h_1)$, and summing over all $h_1 \in H$, we get

$$\sum_{(h_1, g_2) \in H \times G} \Phi_\chi(h_1 g_2 h_1^{-1} g_2^{-1}) = \frac{|G|}{\chi(1)} \sum_{h_1 \in H} \Phi_\chi(h_1)\chi(h_1^{-1}).$$

Taking trace, we have

$$\sum_{(h_1,g_2)\in H\times G} \chi(h_1g_2h_1^{-1}g_2^{-1}) = \frac{|G|}{\chi(1)}\sum_{h_1\in H}\chi(h_1)\chi(h_1^{-1})$$
$$\Longrightarrow \sum_{g\in G}\chi(g)\tilde{\zeta}(g) = \frac{|G|}{\chi(1)}\sum_{h_1\in H}\chi_H(h_1)\overline{\chi_H(h_1)}$$
$$\Longrightarrow [\chi,\tilde{\zeta}] = \frac{|H|[\chi_H,\chi_H]}{\chi(1)}.$$

Hence, in view of (3.3.a) and (1.2.l), the theorem follows. □

In particular, we have

Corollary 3.3.2. *Let G be a finite group. Then, with notations as above, $\tilde{\zeta}$ is a character of G.*

Proof. It is enough to show that $\chi(1)$ divides $|H|[\chi_H,\chi_H]$ for each $\chi\in\mathrm{Irr}(G)$. So, let $\chi\in\mathrm{Irr}(G)$ and Φ_χ be a representation of G which affords χ. Then, in view of the discussion preceding Result 1.2.4, there is an algebra homomorphism $\omega_\chi : Z(\mathbb{C}[G]) \longrightarrow \mathbb{C}$ given by $\Phi_\chi(z) = \omega_\chi(z)\,\mathrm{I}_\chi$ for all $z\in Z(\mathbb{C}[G])$. Since $H\trianglelefteq G$, there exist $h_1,h_2,\ldots,h_r\in H$ such that $H=\bigcup_{1\le i\le r}\mathrm{C}\ell_G(h_i)$. Let $K_i=\sum_{x\in \mathrm{C}\ell_G(h_i)} x$, the class sum corresponding to $\mathrm{C}\ell_G(h_i)$, $1\le i\le r$. By Result 1.2.4, $\omega_\chi(K_i)$ is an algebraic integer with

$$\omega_\chi(K_i) = \frac{\chi(h_i)|\,\mathrm{C}\ell_G(h_i)|}{\chi(1)},\ 1\le i\le r.$$

Therefore, it follows that

$$|H|[\chi_H,\chi_H] = \sum_{h\in H}\chi(h)\chi(h^{-1}) = \sum_{1\le i\le r}|\,\mathrm{C}\ell_G(h_i)|\chi(h_i)\chi(h_i^{-1})$$
$$= \sum_{1\le i\le r}\chi(1)\omega_\chi(K_i)\chi(h_i^{-1}).$$

Thus,

$$\frac{|H|[\chi_H, \chi_H]}{\chi(1)} = \sum_{1\le i\le r} \omega_\chi(K_i)\chi(h_i^{-1}),$$

which, in view of Result 1.2.3, is an algebraic integer, and hence, an integer. This completes the proof. □

The following proposition is a generalization of the result of P. Kellersch and K. Meyberg given by (1.3.c).

Proposition 3.3.3. *Let G be a finite group, $H \trianglelefteq G$ and $g \in G$. If $\tilde{\zeta}_{2n}(g)$, $n \ge 1$, denotes the number of elements $((h_1, g_1), \ldots, (h_n, g_n)) \in (H \times G)^n$ satisfying $[h_1, g_1]\ldots[h_n, g_n] = g$, then $\tilde{\zeta}_{2n}$ is a character of G and*

$$\tilde{\zeta}_{2n}(g) = \sum_{\chi\in \mathrm{Irr}(G)} \frac{|G|^{n-1}|H|^n[\chi_H, \chi_H]^n}{\chi(1)^{2n-1}}\chi(g).$$

Proof. In view of Theorem 3.3.1 and Corollary 3.3.2, the proposition follows from the result of Strunkov given by (1.3.f). □

As a slight modification of Strunkov's result mentioned in (1.3.g), we also have the following result.

Proposition 3.3.4. *Let H be a subgroup of a finite group G and $g \in G$. Then the number of elements $(g_1, h_2, g_3) \in G\times H\times G$ satisfying $g_1h_2g_1^{-1}g_3h_2^{-1}g_3^{-1} = g$ defines a character of G and is given by*

$$\tilde{\zeta}_3(g) = \sum_{\chi\in \mathrm{Irr}(G)} \frac{|G||H|[\chi_H, \chi_H]}{\chi(1)}\chi(g).$$

Proof. For each $a \in G$, $(g_1, h_2, g_3) \mapsto (ag_1, h_2, ag_3)$ defines a one to one correspondence between the sets $\{(g_1, h_2, g_3) \in G\times H\times G : g_1h_2g_1^{-1}g_3h_2^{-1}g_3^{-1} = g\}$

and $\{(g_1, h_2, g_3) \in G \times H \times G : g_1 h_2 g_1^{-1} g_3 h_2^{-1} g_3^{-1} = aga^{-1}\}$. So, it follows that $\tilde{\zeta}_3$ is a class function on G. Thus, we have

$$\tilde{\zeta}_3(g) = \sum_{\chi \in \mathrm{Irr}(G)} [\tilde{\zeta}_3, \chi]\, \chi(g). \tag{3.3.b}$$

Let $\chi \in \mathrm{Irr}(G)$, and Φ_χ be a representation of G which affords χ. Then, using (1.2.*d*), we have

$$\sum_{g_1 \in G} \Phi_\chi(g_1 h_2 g_1^{-1}) = \frac{|G|}{\chi(1)} \chi(h_2)\, \mathrm{I}_\chi,$$

where $h_2 \in H$. Multiplying both sides by $\Phi_\chi(g_3 h_2^{-1} g_3^{-1})$, and summing over all $h_2 \in H$ and $g_3 \in G$, we get

$$\sum_{(g_1, h_2, g_3) \in G \times H \times G} \Phi_\chi(g_1 h_2 g_1^{-1} g_3 h_2^{-1} g_3^{-1}) = \frac{|G|}{\chi(1)} \sum_{(h_2, g_3) \in H \times G} \chi(h_2) \Phi_\chi(g_3 h_2^{-1} g_3^{-1}).$$

Taking trace, we have

$$\begin{aligned} \sum_{(g_1, h_2, g_3) \in G \times H \times G} \chi(g_1 h_2 g_1^{-1} g_3 h_2^{-1} g_3^{-1}) &= \frac{|G|}{\chi(1)} \sum_{(h_2, g_3) \in H \times G} \chi(h_2) \chi(h_2^{-1}) \\ \Longrightarrow \sum_{g \in G} \chi(g) \tilde{\zeta}_3(g) &= \frac{|G|^2}{\chi(1)} \sum_{h_2 \in H} \chi_H(h_2) \chi_H(h_2^{-1}) \\ \Longrightarrow [\chi, \tilde{\zeta}_3] &= \frac{|G||H|[\chi_H, \chi_H]}{\chi(1)}, \end{aligned}$$

which is clearly a non-negative integer since $\chi(1)$ divides $|G|$. Hence, in view of (3.3.*b*), the proposition follows. □

As an immediate consequence, it follows from (1.3.*f*) that the number of elements $((g_1, h_2, g_3), \ldots, (g_{3n-2}, h_{3n-1}, g_{3n})) \in (G \times H \times G)^n$ satisfying

$g_1 h_2 g_1^{-1} g_3 h_2^{-1} g_3^{-1} \dots g_{3n-2} h_{3n-1} g_{3n-2}^{-1} g_{3n} h_{3n-1}^{-1} g_{3n}^{-1} = g$ defines a character of G and is given by

$$\tilde{\zeta}_{3n}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|^{2n-1}|H|^n [\chi_H, \chi_H]^n}{\chi(1)^{2n-1}} \chi(g).$$

This, is in fact, a generalization of (3.1.l).

Chapter 4

Commutativity degree generalized through words

In this chapter we study the probability that an arbitrarily chosen n-tuple of elements of a given finite group is mapped to a given group element under the word map induced by an admissible word. This generalizes the existing notion of the probability that the commutator of an arbitrarily chosen pair of group elements equals a given group element. In particular, considering an admissible word that corresponds to a generalized commutator, we also obtain certain characterizations of the given finite group.

This chapter is based on our paper [38].

4.1 Definition and basic properties

Let G be a finite group and g be an element of G'. Let $\omega(x_1, x_2, \ldots, x_n)$ be a non-trivial admissible word (see Section 3.1) in $F(x_1, x_2, \ldots, x_n)$ and $\alpha_\omega : G^n \longrightarrow G$ be the corresponding word map induced by ω. Let us define $\mathrm{Pr}_g^\omega(G)$ to be the probability that an arbitrarily chosen n-tuple in G^n is mapped to g under α_ω. In other words,

$$\mathrm{Pr}_g^\omega(G) = \frac{\zeta_n^\omega(g)}{|G^n|}, \tag{4.1.a}$$

where $\zeta_n^\omega(g) = |\{(g_1, g_2, \ldots, g_n) \in G^n : \omega(g_1, g_2, \ldots, g_n) = g\}|$. Comparing (4.1.$a$) with (3.2.$a$), one can also observe that $\mathrm{Pr}_g^\omega(G) = P_\omega(g)$, where P_ω is the probability distribution of G associated to α_ω.

Note that, for $\omega(x_1, x_2) = x_1 x_2 x_1^{-1} x_2^{-1}$, we have $\mathrm{Pr}_g^\omega(G) = \mathrm{Pr}_g(G)$, a notion used and studied extensively by M. R. Pournaki and R. Sobhani [40], which coincides with the usual commutativity degree $\mathrm{Pr}(G)$ of G if we take $g = 1$, the identity element of G.

It is easy to see that $0 \leq \mathrm{Pr}_g^\omega(G) \leq 1$. Also, we have

Proposition 4.1.1. *Let G be a finite group and $\omega(x_1, x_2, \ldots, x_n)$ be a non-trivial admissible word. Then*

(a) $\mathrm{Pr}_1^\omega(G) \geq \dfrac{n|G : Z(G)| - n + 1}{|G : Z(G)|^n} \geq \dfrac{1}{|G : Z(G)|^n} \gneq 0,$

(b) $\mathrm{Pr}_1^\omega(G) = 1$ *if and only if* G *is abelian.*

Proof. (a) Consider an n-tuple $(g_1, g_2, \ldots, g_n) \in G^n$ in which $n - 1$ coordinates are chosen from the center $Z(G)$. Clearly, $\omega(g_1, g_2, \ldots, g_n) = 1$ and the number of such n-tuples is $|Z(G)|^{n-1}(n\,|G|-(n-1)|Z(G)|)$. Hence, part (a) follows.

(b) We are to show that $\omega(g_1, g_2, \ldots, g_n) = 1$ for all $g_1, g_2, \ldots, g_n \in G$ if and only if G is abelian. Since ω is admissible, the 'if' part is obvious. So, let

$$\omega(g_1, g_2, \ldots, g_n) = 1 \tag{4.1.b}$$

for all $g_1, g_2, \ldots, g_n \in G$. We first show, using induction on n, that

$$\omega(x_1, x_2, \ldots, x_n) = \omega_1\, u\, \omega_2\, v\, \omega_3\, u^{-1}\, \omega_4\, v^{-1}\, \omega_5, \tag{4.1.c}$$

where $u = x_i$ or x_i^{-1} and $v = x_j$ or x_j^{-1} for some i, j with $1 \leq i \neq j \leq n$, and each ω_k, $1 \leq k \leq 5$, is a word in the remaining $n-2$ letters; we may have $\omega_k = 1$ for some or all k. Clearly, (4.1.c) holds if $n = 2$.

Assume that $n > 2$. Then

$$\omega(x_1, x_2, \ldots, x_n) = y\, \omega_6\, y^{-1}\, \omega_7, \tag{4.1.d}$$

where $y = x_r$ or x_r^{-1} for some r with $1 \leq r \leq n$, and ω_6, ω_7 are words in the remaining $n-1$ letters; noting that we may have $\omega_7 = 1$, but we always have $\omega_6 \neq 1$. If ω_6 is an admissible word, then, by induction hypothesis, ω_6, and hence $\omega(x_1, x_2, \ldots, x_n)$ has the form given by (4.1.c). On the other hand, if ω_6 is not an admissible word, then

$$\omega_6 = \omega_8\, z\, \omega_9 \tag{4.1.e}$$

$$\text{and} \quad \omega_7 = \omega_{10}\, z^{-1}\, \omega_{11}, \tag{4.1.f}$$

where $z = x_s$ or x_s^{-1} for some s with $1 \leq s \neq r \leq n$, and $\omega_8, \omega_9, \omega_{10}, \omega_{11}$ are words in the $n-2$ letters in the set $\{x_1, x_2, \ldots, x_n\} - \{x_r, x_s\}$. Thus, once again, it follows, from (4.1.d), (4.1.e) and (4.1.f), that $\omega(x_1, x_2, \ldots, x_n)$ has the form given by (4.1.c). This establishes our claim.

Finally, let a, b be any two elements of G. In (4.1.c), let us put $x_i = a$, $x_j = b$ and $x_t = 1$ for all t such that $1 \leq i \neq t \neq j \leq n$. Then, using (4.1.$b$), we have $a\,b\,a^{-1}\,b^{-1} = 1$ for all $a, b \in G$, showing that G is abelian. This completes the proof of part (b). □

Note that $\mathrm{Pr}_g^{\omega}(G)$ may be regarded as a completely multiplicative arithmetic function of finite groups in the sense of [4]. More precisely, we have

Proposition 4.1.2. *Let H and K be two finite groups and $\omega(x_1, x_2, \ldots, x_n)$ be a non-trivial admissible word. If $(h, k) \in H' \times K'$, then*

$$\mathrm{Pr}_{(h,k)}^{\omega}(H \times K) = \mathrm{Pr}_h^{\omega}(H)\mathrm{Pr}_k^{\omega}(K).$$

Proof. Note that the elements $((h_1, k_1), \ldots, (h_n, k_n)) \in (H \times K)^n$ satisfying $\omega((h_1, k_1), \ldots, (h_n, k_n)) = (h, k)$ are in one to one correspondence with the elements $((h_1, \ldots, h_n), (k_1, \ldots, k_n)) \in H^n \times K^n$ satisfying $\omega(h_1, \ldots, h_n) = h$ and $\omega(k_1, \ldots, k_n) = k$. Hence, the result follows from (4.1.a). □

The following result shows that $\mathrm{Pr}_g^{\omega}(G)$ is an invariant under isoclinism (see Section 1.1) of finite groups.

Proposition 4.1.3. *Let G and H be two finite groups and (ϕ, ψ) be an isoclinism from G to H. If $g \in G'$ and $\omega(x_1, x_2, \ldots, x_n)$ is a non-trivial admissible word, then*

$$\mathrm{Pr}_g^{\omega}(G) = \mathrm{Pr}_{\psi(g)}^{\omega}(H).$$

Proof. Since $\omega(x_1, x_2, \ldots, x_n)$ is an admissible word, the induced word map $\alpha_\omega : G^n \longrightarrow G$ factors through the quotient group $G^n/Z(G^n) = (G/Z(G))^n$. Therefore, we have

$$\begin{aligned}
&|\{(g_1, g_2, \ldots, g_n) \in G^n : \omega(g_1, g_2, \ldots, g_n) = g\}| \\
&= |\{(g_1Z(G), g_2Z(G), \ldots, g_nZ(G)) \in (G/Z(G))^n : \omega(g_1, g_2, \ldots, g_n) = g\}| \\
&\quad \times |Z(G)|^n. \qquad (4.1.g)
\end{aligned}$$

Let K be the subgroup of G generated by $g_1, g_2, \ldots, g_n$. Note that $g_1K', g_2K', \ldots, g_nK' \in K/K'$, an abelian group. Since $\omega(x_1, x_2, \ldots, x_n)$ is an admissible word, it follows that

$$\begin{aligned}
&\omega(g_1K', g_2K', \ldots, g_nK') = K', \quad \text{the identity element of } K/K' \\
&\Longrightarrow \omega(g_1, g_2, \ldots, g_n)K' = K' \\
&\Longrightarrow \omega(g_1, g_2, \ldots, g_n) \in K'.
\end{aligned}$$

Thus, $\omega(g_1, g_2, \ldots, g_n)$ is a product of commutators in K. In other words, there exits an even positive integer m such that

$$\omega(g_1, g_2, \ldots, g_n) = [\omega_1, \omega_2][\omega_3, \omega_4] \ldots [\omega_{m-1}, \omega_m], \qquad (4.1.h)$$

where $\omega_j = \omega_j(g_1, g_2, \ldots, g_n)$ for some $\omega_j(x_1, x_2, \ldots, x_n) \in F(x_1, x_2, \ldots, x_n)$, $1 \le j \le m$. Choose $h_i \in H$ such that $\phi(g_iZ(G)) = h_iZ(H)$, $1 \le i \le n$. Put $\tilde{\omega}_j = \omega_j(h_1, h_2, \ldots, h_n)$, $1 \le j \le m$. Then, from (4.1.h), using Figure 1.1, we have

$$\begin{aligned}
\psi(g) &= \psi([\omega_1, \omega_2]) \ldots \psi([\omega_{m-1}, \omega_m]) \\
&= \psi(a_G(\omega_1 Z(G), \omega_2 Z(G))) \ldots \psi(a_G(\omega_{m-1} Z(G), \omega_m Z(G)))
\end{aligned}$$

$$
\begin{aligned}
&= a_H(\phi(\omega_1 Z(G)), \phi(\omega_2 Z(G))) \ldots a_H(\phi(\omega_{m-1} Z(G)), \phi(\omega_m Z(G))) \\
&= a_H(\tilde{\omega}_1 Z(H), \tilde{\omega}_2 Z(H)) \ldots a_H(\tilde{\omega}_{m-1} Z(H), \tilde{\omega}_m Z(H)) \\
&= [\tilde{\omega}_1, \tilde{\omega}_2] \ldots [\tilde{\omega}_{m-1}, \tilde{\omega}_m] \\
&= \omega(h_1, h_2, \ldots, h_n).
\end{aligned}
$$

It follows that there is an one to one correspondence between the n-tuples $(g_1 Z(G), g_2 Z(G), \ldots, g_n Z(G)) \in (G/Z(G))^n$ satisfying $\omega(g_1, g_2, \ldots, g_n) = g$ and the n-tuples $(h_1 Z(H), h_2 Z(H), \ldots, h_n Z(H)) \in (H/Z(H))^n$ satisfying $\omega(h_1, h_2, \ldots, h_n) = \psi(g)$. Hence, by (4.1.$g$) and the corresponding equation for H, we have

$$
\begin{aligned}
\Pr_g^\omega(G) &= \frac{\zeta_n^\omega(g)}{|G^n|} \\
&= \frac{|\{(g_1 Z(G), \ldots, g_n Z(G)) \in (G/Z(G))^n : \omega(g_1, \ldots, g_n) = g\}|}{|G : Z(G)|^n} \\
&= \frac{|\{(h_1 Z(H), \ldots, h_n Z(H)) \in (H/Z(H))^n : \omega(h_1, \ldots, h_n) = \psi(g)\}|}{|H : Z(H)|^n} \\
&= \frac{\zeta_n^\omega(\psi(g))}{|H^n|} \\
&= \Pr_{\psi(g)}^\omega(H),
\end{aligned}
$$

noting that $|G : Z(G)| = |H : Z(H)|$. This completes the proof. □

If G is a finite group and $\omega(x_1, x_2, \ldots, x_n)$ is a non-trivial admissible word, then, by Theorem 3.1.4, ζ_n^ω is a character (in particular, a class function) of G. So, it follows from (4.1.a) that if $g, h \in G'$ are conjugates in G, then $\Pr_g^\omega(G) = \Pr_h^\omega(G)$. In the same line, we also have the following result.

Proposition 4.1.4. *Let G be a finite group and $\omega(x_1, x_2, \ldots, x_n)$ be a non-trivial admissible word. If $g, h \in G'$ generate the same cyclic subgroup of G, then* $\mathrm{Pr}_g^{\omega}(G) = \mathrm{Pr}_h^{\omega}(G)$.

Proof. Note that ζ_n^{ω} is a rational valued character of G. Hence, in view of Result 1.2.2, the proposition follows from (4.1.a). □

Since ζ_n^{ω} is a character of G, it follows from Result 1.2.6 and (4.1.a) that

$$\mathrm{Pr}_g^{\omega}(G) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{[\zeta_n^{\omega}, \chi]}{|G|^n} \chi(g), \tag{4.1.i}$$

where, by Proposition 3.2.1, we have $[\zeta_n^{\omega}, \chi] \gtrsim 0$ for all $\chi \in \mathrm{Irr}(G)$. This formula enables us to show that $\mathrm{Pr}_g^{\omega}(G) \leq \mathrm{Pr}(G)$. However, we need the following lemma, which is also used extensively in the forthcoming sections.

Lemma 4.1.5. *If $\sum_{i=1}^{n} r_i(a_i - 1) = 0$, where r_i's are positive rational numbers, and $a_i \in \mathbb{C}$, $|a_i| \leq 1$ for all $i = 1, 2, \ldots, n$. Then $a_i = 1$ for $1 \leq i \leq n$.*

Proof. Note that

$$0 = \sum_{i=1}^{n} \mathrm{Re}(r_i(a_i - 1)) = \sum_{i=1}^{n} r_i(\mathrm{Re}(a_i) - 1) \leq \sum_{i=1}^{n} r_i(|a_i| - 1) \leq 0.$$

Hence, for $1 \leq i \leq n$, we have $\mathrm{Re}(a_i) = |a_i| = 1$ which means that $a_i = 1$. □

Proposition 4.1.6. *Let G be a finite group, $g \in G'$ and $\omega(x_1, x_2, \ldots, x_n)$ be a non-trivial admissible word. Then*

(a) $\mathrm{Pr}_g^{\omega}(G) \leq \mathrm{Pr}_1^{\omega}(G) \leq \mathrm{Pr}(G)$,

(b) $\mathrm{Pr}_g^{\omega}(G) = \mathrm{Pr}_1^{\omega}(G)$ *if and only if* $g = 1$.

Proof. (a) Using (4.1.i), we have

$$\begin{aligned}
\Pr_g^\omega(G) &= \left|\sum_{\chi\in\mathrm{Irr}(G)} \frac{[\zeta_n^\omega,\chi]}{|G|^n}\chi(g)\right| \\
&\le \sum_{\chi\in\mathrm{Irr}(G)} \frac{[\zeta_n^\omega,\chi]}{|G|^n}|\chi(g)|, \quad \text{since } [\zeta_n^\omega,\chi] \gneq 0 \\
&\le \sum_{\chi\in\mathrm{Irr}(G)} \frac{[\zeta_n^\omega,\chi]}{|G|^n}\chi(1) = \Pr_1^\omega(G), \quad \text{using } (1.2.b) \\
&\le \sum_{\chi\in\mathrm{Irr}(G)} \frac{|G|^{n-1}}{\chi(1)}\frac{\chi(1)}{|G|^n}, \quad \text{by Proposition 3.2.1} \\
&= \frac{k(G)}{|G|} = \Pr(G), \quad \text{using } (1.5.b).
\end{aligned}$$

This proves part (a).

(b) Note that, for all $\chi \in \mathrm{Irr}(G)$, we have $[\zeta_n^\omega,\chi] \gneq 0$, and, by (1.2.$b$), we also have $|\chi(g)| \le \chi(1)$. Therefore,

$$\begin{aligned}
& \Pr_g^\omega(G) = \Pr_1^\omega(G) \\
\Longleftrightarrow\ & \sum_{\chi\in\mathrm{Irr}(G)} \frac{[\zeta_n^\omega,\chi]\chi(1)}{|G|^n}\left(\frac{\chi(g)}{\chi(1)} - 1\right) = 0, \quad \text{using } (4.1.i) \\
\Longleftrightarrow\ & \chi(g) = \chi(1) \quad \forall\, \chi \in \mathrm{Irr}(G), \quad \text{using Lemma 4.1.5} \\
\Longleftrightarrow\ & g = 1.
\end{aligned}$$

This proves part (b). □

Since $\Pr_g^\omega(G) \le 1$ for all $g \in G'$, it follows from Proposition 4.1.1(b) and Proposition 4.1.6 that $\Pr_g^\omega(G) = 1$ if and only if $g = 1$ and G is abelian. Of course, if G is abelian and $g \neq 1$, then it is easy to see that $\Pr_g^\omega(G) = 0$, as ω is an admissible word. Hence, it is enough to study the notion $\Pr_g^\omega(G)$ assuming that G is non-abelian.

4.2 A computing formula and some bounds

Let G be a finite non-abelian group and g be an element of G'. In the previous section, we have introduced and studied the notion $\Pr_g^{\omega}(G)$ considering an arbitrary non-trivial admissible word ω. However, for a particular choice of ω, the apparently insignificant-looking formula (4.1.i) becomes quite significant and it enables us to characterize G in terms of certain identities involving the generalized notion of commutativity degree mentioned in Section 4.1. This is exactly what has been done in this and the following sections. Accordingly, from now onwards we deal with the admissible word $x_1x_2\ldots x_nx_1^{-1}x_2^{-1}\ldots x_n^{-1}$, $n \geq 2$, which corresponds to a generalized commutator in G of length n. Also, we write $\Pr_g^n(G)$ in place of $\Pr_g^{\omega}(G)$. Thus, in this case, we have

$$\Pr_g^n(G) = \frac{|\{(g_1, g_2, \ldots, g_n) \in G^n \ : \ [g_1, g_2, \ldots, g_n] = g\}|}{|G^n|}, \qquad (4.2.a)$$

where $[g_1, g_2, \ldots, g_n] = g_1g_2\cdots g_ng_1^{-1}g_2^{-1}\cdots g_n^{-1}$. Needless to mention that all the results obtained in the previous section hold good also for $\Pr_g^n(G)$.

In view of the above consideration, it follows from (1.3.e) and (4.1.a) that

$$\Pr_g^n(G) = \frac{1}{|G|}\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)^{n-\varepsilon_n}}, \qquad (4.2.b)$$

where ε_n is 1 or 2 according as n is even or odd. It is easy to see that if n is even, then $\Pr_g^n(G) = \Pr_g^{n+1}(G)$. Hence, without any loss we may assume that n is even, that is, $\varepsilon_n = 1$. Using (1.2.a), the formula (4.2.b) may be rewritten as

$$\Pr_g^n(G) = \frac{1}{|G'|} + \frac{1}{|G|}\sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1) \neq 1}} \frac{\chi(g)}{\chi(1)^{n-1}}. \qquad (4.2.c)$$

In particular, putting $g = 1$, we have

$$\frac{1}{|G'|} < \mathrm{Pr}_1^n(G) \leq \mathrm{Pr}_1^2(G) = \mathrm{Pr}(G); \tag{4.2.d}$$

noting that G has at least one non-linear irreducible character. From (4.2.c), using (1.2.b), we also have

$$\left|\mathrm{Pr}_g^n(G) - \frac{1}{|G'|}\right| \leq \frac{1}{|G|} \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1) \neq 1}} \frac{1}{\chi(1)^{n-2}}. \tag{4.2.e}$$

Let $m_G = \min\{\chi(1) : \chi \in \mathrm{Irr}(G), \chi(1) \neq 1\}$. If p is the smallest prime divisor of $|G|$, then it is easy to see that

$$\chi(1) \geq m_G \geq p \geq 2 \tag{4.2.f}$$

for all $\chi \in \mathrm{Irr}(G)$ with $\chi(1) \neq 1$.

In order to have some non-trivial bounds for $\mathrm{Pr}_g^n(G)$ we need the following lemma, which, in view of (4.2.f), also generalizes Result 1.5.2.

Lemma 4.2.1. *Let G be a finite non-abelian group and d be an integer such that $2 \leq d \leq m_G$. Then*

$$\mathrm{Pr}(G) \leq \frac{1}{d^2}\left(1 + \frac{d^2 - 1}{|G'|}\right)$$

with equality if and only if $\mathrm{cd}(G) = \{1, d\}$.

Proof. By (4.2.f), $\chi(1) \geq d$ for all $\chi \in \mathrm{Irr}(G)$ with $\chi(1) \neq 1$. Also, by (1.2.a), the number of non-linear irreducible characters of G is given by $k(G) - |G : G'|$. Therefore, from the degree equation (1.2.c), we have

$$|G| = |G : G'| + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1) \neq 1}} \chi(1)^2 \geq |G : G'| + d^2(k(G) - |G : G'|)$$

with equality if and only if $\chi(1) = d$ for all $\chi \in \mathrm{Irr}(G)$ with $\chi(1) \neq 1$. Hence, noting that $\Pr(G) = \frac{k(G)}{|G|}$, the lemma follows. □

Proposition 4.2.2. *Let G be a finite non-abelian group, $g \in G'$ and d be an integer such that $2 \leq d \leq m_G$. Then*

(a) $\left|\Pr_g^n(G) - \frac{1}{|G'|}\right| \leq \frac{1}{d^{n-2}}\left(\Pr(G) - \frac{1}{|G'|}\right)$. *In other words,*

$$\frac{1}{d^{n-2}}\left(-\Pr(G) + \frac{d^{n-2}+1}{|G'|}\right) \leq \Pr_g^n(G) \leq \frac{1}{d^{n-2}}\left(\Pr(G) + \frac{d^{n-2}-1}{|G'|}\right).$$

(b) $\left|\Pr_g^n(G) - \frac{1}{|G'|}\right| \leq \frac{1}{d^{n}}\left(1 - \frac{1}{|G'|}\right)$. *In other words,*

$$\frac{1}{d^{n}}\left(-1 + \frac{d^{n}+1}{|G'|}\right) \leq \Pr_g^n(G) \leq \frac{1}{d^{n}}\left(1 + \frac{d^{n}-1}{|G'|}\right).$$

In particular, $\Pr_g^n(G) \leq \dfrac{2^n+1}{2^{n+1}}$.

Proof. (a) By (4.2.*f*), $\chi(1) \geq d$ for all $\chi \in \mathrm{Irr}(G)$ with $\chi(1) \neq 1$. Also, by (1.2.*a*), the number of non-linear irreducible characters of G is given by $k(G) - |G : G'|$. Hence, it follows from (4.2.*e*) that

$$\left|\Pr_g^n(G) - \frac{1}{|G'|}\right| \leq \frac{1}{d^{n-2}}\left(\frac{k(G)}{|G|} - \frac{1}{|G'|}\right) = \frac{1}{d^{n-2}}\left(\Pr(G) - \frac{1}{|G'|}\right).$$

This proves part (a).

(b) In view of Lemma 4.2.1, part (b) follows from part (a); noting, for the particular case, that $d \geq 2$ and $|G'| \geq 2$. □

As an immediate consequence of Proposition 4.2.2(a), we have

$$\lim_{n\to\infty} \Pr_g^n(G) = \frac{1}{|G'|}. \tag{4.2.g}$$

Proposition 4.2.3. *If G is a finite non-abelian simple group and $g \in G'$, then*

$$\left|\Pr_g^n(G) - \frac{1}{|G|}\right| \leq \frac{1}{3^{n-2}}\left(\frac{1}{12} - \frac{1}{|G|}\right).$$

In other words,

$$\frac{1}{3^{n-2}}\left(\frac{-1}{12} + \frac{3^{n-2}+1}{|G|}\right) \leq \Pr_g^n(G) \leq \frac{1}{3^{n-2}}\left(\frac{1}{12} + \frac{3^{n-2}-1}{|G|}\right).$$

In particular,

$$\Pr_g^n(G) \leq \frac{3^{n-2}+4}{3^{n-1}\times 20}.$$

Proof. It has been proved by J. D. Dixon [8] that, for a finite non-abelian simple group G, $\Pr(G) \leq \frac{1}{12}$. Also, for such groups, we have $m_G \geq 3$, using Result 1.2.10. Hence, using the fact that $G = G'$, the result follows from Proposition 4.2.2(a) with $d = m_G$. For the particular case, note that $|G| \geq 60$, since A_5 is the smallest finite non-abelian simple group and its order is 60. □

4.3 Some characterizations

Let G be a finite non-abelian group and $g \in G'$. In this section we show that G has some special properties expressible in standard group-theoretic terms if and only if $\Pr_g^n(G)$ satisfies certain identities given by some of its upper and lower bounds mentioned in Section 4.2.

We begin with the following observation.

Lemma 4.3.1. *Let G be a finite non-abelian group and $1 \neq g \in G'$. If $\mathrm{cd}(G) = \{1, d\}$, then*

$$\Pr_g^n(G) = \frac{1}{|G'|}\left(1 - \frac{1}{d^n}\right) \gneq 0.$$

Proof. Using the second orthogonality relation (1.2.j), we have

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\chi(1) = 0$$

$$\Longrightarrow \quad \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1) \neq 1}} \chi(g) = -\frac{|G : G'|}{d}, \quad \text{using (1.2.}a\text{).}$$

The result now follows from (4.2.c); noting that $d \geq 2$, since G is non-abelian. □

As an immediate consequence, we have the following corollary which is related to Remark 1.1.2, Result 1.2.11 and Theorem 2.4.3.

Corollary 4.3.2. *Let G be a finite group with $|\,\mathrm{cd}(G)| = 2$. Then every element of G' is a generalized commutator of length n for all $n \geq 2$; in particular, every element of G' is a commutator.*

Proof. In view of Proposition 4.1.1(a) and Lemma 4.3.1, we have $\Pr_g^n(G) \gneq 0$ for all $g \in G'$. Hence, using (4.2.a), the result follows. □

Now, corresponding to Proposition 4.2.2(a), we have

Proposition 4.3.3. *Let G be a finite non-abelian group, $g \in G'$ and d be an integer such that $2 \leq d \leq m_G$. Then*

(a) $\Pr_g^n(G) = \dfrac{1}{d^{n-2}}\left(\Pr(G) + \dfrac{d^{n-2}-1}{|G'|}\right)$ *if and only if*

$g = 1$ *and* $\mathrm{cd}(G) = \{1, d\}$.

(b) $\Pr_g^n(G) = \dfrac{1}{d^{n-2}}\left(-\Pr(G) + \dfrac{d^{n-2}+1}{|G'|}\right)$ *if and only if*

$g \neq 1$, $\mathrm{cd}(G) = \{1, d\}$ *and* $|G'| = 2$.

Proof. (a) Note that

$$
\begin{aligned}
& \Pr_1^n(G) - \frac{1}{|G'|} = \frac{1}{d^{n-2}}\left(\Pr(G) - \frac{1}{|G'|}\right) \\
\Longleftrightarrow\quad & \frac{1}{|G|}\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)\neq 1}} \frac{1}{\chi(1)^{n-2}} = \frac{1}{d^{n-2}}\frac{1}{|G|}\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)\neq 1}} 1, \qquad \text{using (4.2.}c\text{)} \\
\Longleftrightarrow\quad & \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)\neq 1}} \frac{1}{d^{n-2}}\left(\frac{d^{n-2}}{\chi(1)^{n-2}} - 1\right) = 0 \\
\Longleftrightarrow\quad & d = \chi(1) \quad \forall\, \chi \in \mathrm{Irr}(G) \text{ with } \chi(1) \neq 1, \qquad \text{using Lemma 4.1.5} \\
\Longleftrightarrow\quad & \mathrm{cd}(G) = \{1, d\}.
\end{aligned}
$$

This, in view of Proposition 4.1.6 and Proposition 4.2.2(a), completes the proof of part (a).

(b) Note that

$$\begin{aligned}
& \mathrm{Pr}_g^n(G) - \frac{1}{|G'|} = -\frac{1}{d^{n-2}}\left(\mathrm{Pr}(G) - \frac{1}{|G'|}\right) \\
\Longrightarrow\ & \frac{1}{|G|}\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)\neq 1}} \frac{\chi(g)}{\chi(1)^{n-1}} = -\frac{1}{d^{n-2}}\frac{1}{|G|}\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)\neq 1}} 1, \qquad \text{using (4.2.}c\text{)} \\
\Longrightarrow\ & \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)\neq 1}} \frac{1}{d^{n-2}}\left(\frac{-\chi(g)d^{n-2}}{\chi(1)^{n-1}} - 1\right) = 0 \\
\Longrightarrow\ & -\chi(g)d^{n-2} = \chi(1)^{n-1} \quad \text{for all } \chi\in\mathrm{Irr}(G) \text{ with } \chi(1)\neq 1,
\end{aligned}$$

using (1.2.b) and Lemma 4.1.5, and noting that $\chi(1) \geq d$ for all $\chi \in \mathrm{Irr}(G)$ with $\chi(1) \neq 1$. Thus, we have $g \neq 1$, $\chi(g)$ is real, and $-\chi(g) = \chi(1) = d$ for all $\chi \in \mathrm{Irr}(G)$ with $\chi(1) \neq 1$. In particular, we have $\mathrm{cd}(G) = \{1, d\}$. Also, using the second orthogonality relation (1.2.j), we have

$$\begin{aligned}
& \sum_{\chi\in\mathrm{Irr}(G)} \chi(g)\chi(1) = 0 \\
\Longrightarrow\ & |G:G'| - d^2\left(k(G) - |G:G'|\right) = 0 \\
\Longrightarrow\ & \mathrm{Pr}(G) = \frac{d^2+1}{d^2|G'|} \\
\Longrightarrow\ & |G'| = 2, \qquad \text{using Lemma 4.2.1.}
\end{aligned}$$

Conversely, if $g \neq 1$, $\mathrm{cd}(G) = \{1, d\}$, $|G'| = 2$, then, by Lemma 4.2.1 and Lemma 4.3.1, we have

$$\frac{1}{d^{n-2}}\left(-\mathrm{Pr}(G) + \frac{d^{n-2}+1}{|G'|}\right) = \frac{1}{2}\left(1 - \frac{1}{d^n}\right) = \mathrm{Pr}_g^n(G).$$

This completes the proof of part (b). □

Corresponding to Proposition 4.2.2(b), we have

Proposition 4.3.4. *Let G be a finite non-abelian group, $g \in G'$ and d be an integer such that $2 \leq d \leq m_G$. Then*

(a) $\Pr_g^n(G) = \frac{1}{d^n}\left(1 + \frac{d^n - 1}{|G'|}\right)$ *if and only if*

$g = 1$ *and* $\text{cd}(G) = \{1, d\}$.

(b) $\Pr_g^n(G) = \frac{1}{d^n}\left(-1 + \frac{d^n + 1}{|G'|}\right)$ *if and only if*

$g \neq 1$, $\text{cd}(G) = \{1, d\}$ *and* $|G'| = 2$.

Proof. Using Proposition 4.2.2(a) and the first part of Lemma 4.2.1, we have

$$\Pr_g^n(G) - \frac{1}{|G'|} \leq \frac{1}{d^{n-2}}\left(\Pr(G) - \frac{1}{|G'|}\right) \leq \frac{1}{d^n}\left(1 - \frac{1}{|G'|}\right).$$

Hence, part (a) follows from Proposition 4.3.3(a) using the second part of Lemma 4.2.1.

Again, using Proposition 4.2.2(a) and the first part of Lemma 4.2.1, we have

$$\Pr_g^n(G) - \frac{1}{|G'|} \geq \frac{-1}{d^{n-2}}\left(\Pr(G) - \frac{1}{|G'|}\right) \geq \frac{-1}{d^n}\left(1 - \frac{1}{|G'|}\right).$$

Hence, part (b) follows from Proposition 4.3.3(b) using the second part of Lemma 4.2.1. □

Lemma 4.3.5. *Let G be a finite non-abelian group, and p be the smallest prime divisor of $|G|$. Then*

$$|G : Z(G)| = p^2 \iff \mathrm{cd}(G) = \{1, p\} \textit{ and } |G'| = p.$$

Proof. By the first part of Result 1.5.2, we have

$$\Pr(G) \leq \frac{1}{p^2}\left(1 + \frac{p^2-1}{|G'|}\right) \leq \frac{1}{p^2}\left(1 + \frac{p^2-1}{p}\right).$$

So, by the second part of Result 1.5.2, we have

$$\Pr(G) = \frac{1}{p^2}\left(1 + \frac{p^2-1}{p}\right) \iff \mathrm{cd}(G) = \{1, p\} \text{ and } |G'| = p.$$

On the other hand, using Result 1.5.1, we have

$$\Pr(G) = \frac{1}{p^2}\left(1 + \frac{p^2-1}{p}\right) \iff |G : Z(G)| = p^2.$$

Hence, the lemma follows. □

Lemma 4.3.6. *Let G be a finite group and p be a prime. Then $|G : Z(G)| = p^2$ if and only if G is isoclinic to the group presented as*

$$\langle x, y \;:\; x^{p^2} = 1 = y^p,\ y^{-1}xy = x^{p+1}\rangle.$$

Proof. It has been observed in [23, page 136] that upto isoclinism, there exists precisely one non-abelian group of order p^3, and that the groups which are isoclinic to a group of order p^3 are characterized by the property that their center has index p^2. Hence, the lemma follows. □

In view of the observations made in the above lemmas, we have the following result.

Proposition 4.3.7. *Let G be a finite non-abelian group, $g \in G'$ and p be the smallest prime divisor of $|G|$. Then*

$$\Pr_g^n(G) = \frac{p^n + p - 1}{p^{n+1}}$$

if and only if $g = 1$, and G is isoclinic to

$$\langle x, y \,:\, x^{p^2} = 1 = y^p,\ y^{-1}xy = x^{p+1} \rangle.$$

In particular, putting $p = 2$, $\Pr_g^n(G) = \dfrac{2^n + 1}{2^{n+1}}$ if and only if $g = 1$, and G is isoclinic to D_8, the dihedral group, and hence, to Q_8, the group of quaternions.

Proof. By Proposition 4.2.2(b) with $d = p$, we have

$$\Pr_g^n(G) \le \frac{1}{p^n}\left(1 + \frac{p^n - 1}{|G'|}\right) \le \frac{1}{p^n}\left(1 + \frac{p^n - 1}{p}\right).$$

So, by Proposition 4.3.4(a), we have

$$\Pr_g^n(G) = \frac{1}{p^n}\left(1 + \frac{p^n - 1}{p}\right) \iff g = 1, \mathrm{cd}(G) = \{1, p\} \text{ and } |G'| = p.$$

Hence, the result follows from Lemma 4.3.5 and Lemma 4.3.6. □

We conclude the section with the following remark.

Remark 4.3.8. If G is a finite non-abelian simple group, then the equality in Proposition 4.2.3 can never hold. Because in that case we would have equality in Proposition 4.2.2. This, in view of Proposition 4.3.3, would imply that $|\,\mathrm{cd}(G)| = 2$, which, by Result 1.2.11, is impossible.

4.4 Some more bounds and identities

As an immediate consequence of Proposition 4.3.4(a) and Lemma 4.3.1, we have

Proposition 4.4.1. *Let G be a finite non-abelian group with $|\operatorname{cd}(G)| = 2$ and $g \in G'$. Then*

$$\begin{aligned} \Pr_1^n(G) &\geq \frac{1}{|G'|}\left(1 + \frac{|G'|-1}{|G:Z(G)|^{n/2}}\right) \quad \textit{and} \\ \Pr_g^n(G) &\leq \frac{1}{|G'|}\left(1 - \frac{1}{|G:Z(G)|^{n/2}}\right) \quad \textit{if } g \neq 1. \end{aligned}$$

Moreover, in each case, the equality holds if and only if G is of central type.

Corollary 4.4.2. *Let G be a finite non-abelian group and $g \in G'$. If G is of central type with $|\operatorname{cd}(G)| = 2$, then*

$$\begin{aligned} \Pr_1^n(G) &\leq \frac{1}{|G'|}\left(1 + \frac{|G'|-1}{2^n}\right) \quad \textit{and} \\ \Pr_g^n(G) &\geq \frac{1}{|G'|}\left(1 - \frac{1}{2^n}\right) \quad \textit{if } g \neq 1. \end{aligned}$$

Proof. In this case, the equality holds in each of the inequalities mentioned in Proposition 4.4.1. Also, since G is non-abelian, we have $|\frac{G}{Z(G)}| \geq 4$. Hence, the corollary follows. □

Proposition 4.4.3. *Let G be a finite non-abelian group and $g \in G'$. If $G' \subseteq Z(G)$ and $|G'| = p$, where p is a prime, then*

$$\Pr_g^n(G) = \begin{cases} \frac{1}{p}\left(1 + \frac{p-1}{p^{nk}}\right) & \textit{if } \ g = 1 \\ \frac{1}{p}\left(1 - \frac{1}{p^{nk}}\right) & \textit{if } \ g \neq 1, \end{cases}$$

where $k = \dfrac{1}{2}\log_p |G : Z(G)|$.

Proof. If $G' \subseteq Z(G)$ and G' is of prime order, then G is of central type with $|\operatorname{cd}(G)| = 2$, by Result 1.2.7. That is $\operatorname{cd}(G) = \{1, |G : Z(G)|^{1/2}\}$. Hence, in view of Proposition 2.4.7(a)(d), the result follows from Proposition 4.4.1. □

More generally, we have

Corollary 4.4.4. *Let G be a finite non-abelian group and $g \in G'$. If $|G'|$ is square free and $G' \subseteq Z(G)$, then*

$$\operatorname{Pr}_g^n(G) = \prod_{p \mid |G'|} \left(\frac{1}{p}\left(1 - \frac{1}{p^{nk_p}}\right)\right)^{\delta_p} \left(\frac{1}{p}\left(1 + \frac{p-1}{p^{nk_p}}\right)\right)^{1-\delta_p},$$

where $k_p = \dfrac{1}{2}\log_p |G_p : Z(G_p)|$, G_p is the Sylow p-subgroup of G, and $\delta_p = 1$ or 0 according as $p \mid o(g)$ or $p \nmid o(g)$.

Proof. Note that G, being nilpotent, is the direct product of its Sylow subgroups. Therefore, since $G' \subseteq Z(G)$ and $|G'|$ is squarefree, it follows that, for each prime divisor p of $|G'|$, the Sylow p-subgroup G_p of G satisfies the conditions $G_p' \subseteq Z(G_p)$ and $|G_p'| = p$. It also follows that, all other Sylow subgroups (if any) of G are abelian. Hence, using Proposition 4.1.2 and Proposition 4.4.3, the corollary follows. □

We now generalize a few results mentioned in Section 1.5. We begin with two results that generalize Result 1.5.10 and Result 1.5.12.

Proposition 4.4.5. *Let p be a prime. Let r and s be two positive integers such that $s \mid (p-1)$, and $r^j \equiv 1 \pmod{p}$ if and only if $s \mid j$. If $G = \langle a, b : a^p = b^s = 1, bab^{-1} = a^r\rangle$ and $g \in G'$, then*

$$\Pr_g^n(G) = \begin{cases} \dfrac{s^n + p - 1}{ps^n} & \textit{if } g = 1 \\ \dfrac{s^n - 1}{ps^n} & \textit{if } g \neq 1. \end{cases}$$

Proof. It is easy to see that $|G'| = p$ and $G' = C_G(x)$ for every $x \neq 1, x \in G'$. Therefore by Result 1.2.9 we have $\text{cd}(G) = \{1, s\}$. Now the result follows from Lemma 4.3.1 and Proposition 4.3.4(a). □

Proposition 4.4.6. *Let G be a finite non-abelian group and $g \in G'$. If $G' \cap Z(G) = \{1\}$ and $|G'| = p$, where p is a prime, then*

(a) *G is isoclinic to the group $\langle a, b \,:\, a^p = b^s = 1,\, bab^{-1} = a^r \rangle$, where $s \mid (p-1)$, and $r^j \equiv 1 \pmod p$ if and only if $s \mid j$,*

(b) $$\Pr_g^n(G) = \begin{cases} \dfrac{s^n + p - 1}{ps^n} & \textit{if } g = 1 \\ \dfrac{s^n - 1}{ps^n} & \textit{if } g \neq 1. \end{cases}$$

Proof. Here $(\frac{G}{Z(G)})' \cong G'$, which is of order p. On the other hand, we have $Z(\frac{G}{Z(G)}) = \frac{H}{Z(G)}$, where $Z(G) \leq H \leq G$, and so, $[G,\, H] \leq G' \cap Z(G) = \{1\}$. This implies that $H = Z(G)$, that is, $Z(\frac{G}{Z(G)}) = \{1\}$. Therefore by Result 1.5.11, we have

$$\frac{G}{Z(G)} = \langle a, b \,:\, a^p = b^s = 1,\, bab^{-1} = a^r \rangle,$$

where $s \mid (p-1)$, and $r^j \equiv 1 \pmod p$ if and only if $s \mid j$. Hence, part (a) follows from Result 1.1.9, and part (b) follows from Proposition 4.4.5 using Proposition 4.1.3. □

The following two results generalize Result 1.5.17 and Result 1.5.18.

Proposition 4.4.7. *Let G be a finite non-abelian group and $g \in G'$. If $g \neq 1$, then $\mathrm{Pr}_g^n(G) < \frac{1}{p}$, where p is the smallest prime divisor of $|G|$. In particular, we have $\mathrm{Pr}_g^n(G) < \frac{1}{2}$.*

Proof. If $\mathrm{Pr}_g^n(G) \geq \frac{1}{p}$, then, from (4.2.$d$) and Proposition 4.1.6 (a)(b), it follows that $\mathrm{Pr}(G) > \frac{1}{p}$. Therefore, from Result 1.5.2, we have $|G'| < p + 1$, and so, $|G'| = p$. Hence, we have either $G' \subseteq Z(G)$ or $G' \cap Z(G) = \{1\}$. In both the situations, we have, from Proposition 4.4.3 and Proposition 4.4.6, $\mathrm{Pr}_g^n(G) < \frac{1}{p}$. This contradiction proves the result. □

Proposition 4.4.8. *For each $\varepsilon > 0$ and for each prime p, there exists a finite group G such that*

$$\left|\mathrm{Pr}_g^n(G) - \frac{1}{p}\right| < \varepsilon$$

for all $g \in G'$.

Proof. In view of Proposition 4.4.3, it is enough to choose a positive integer k such that $k > -\frac{1}{n}\log_p \varepsilon$, and consider G to be an extra-special p-group of order p^{2k+1}. □

We conclude this chapter with the following remark.

Remark 4.4.9. Let G be a finite non-abelian group. Then it follows from (4.2.c) that $\mathrm{Pr}_1^{n+2}(G) < \mathrm{Pr}_1^n(G)$. On the other hand, if $g \in G'$, $g \neq 1$ and $|\operatorname{cd}(G)| = 2$, then, using Lemma 4.3.1, we have $\mathrm{Pr}_g^{n+2}(G) > \mathrm{Pr}_g^n(G)$.

Chapter 5

A generalization of relative commutativity degree

In the previous chapter we have generalized the existing notion of the probability that the commutator of an arbitrarily chosen pair of elements of a given finite group equals a given group element. This chapter also deals with a generalization of the same notion; however, unlike the previous chapter, we choose the two group elements in the commutator from two given subgroups of the given finite group.

This chapter is based on our paper [6].

5.1 Definition, some basic properties and a computing formula

Let G be a finite group and $g \in G'$. Let H and K be two subgroups of G. Let us define $\Pr_g(H,K)$ to be the probability that the commutator of a randomly chosen pair of elements (one from H and the other from K) equals g. In other words,

$$\Pr_g(H,K) = \frac{|\{(x,y) \in H \times K : [x,y] = g\}|}{|H||K|}. \qquad (5.1.a)$$

If $g = 1$, the identity element of G, then for brevity we write $\Pr_1(H,K) = \Pr(H,K)$. Note that for $H = K = G$, we have $\Pr_g(H,K) = \Pr_g(G)$, a notion studied originally by M. R. Pournaki and R. Sobhani [40]. On the other hand, if $K = G$ and $g = 1$, then $\Pr_g(H,K) = \Pr(H,G)$, a notion, called the relative commutativity degree of H in G, studied originally by A. Erfanian, R. Rezaei and P. Lescot [13].

Consider the subgroup $[H,K]$ of G generated by the commutators $[x,y]$, where $x \in H$ and $y \in K$. Clearly,

$$\begin{aligned} \Pr(H,K) = 1 &\iff [H,K] = \{1\}, \\ \text{and} \quad \Pr_g(H,K) = 0 &\iff g \notin \{[x,y] : x \in H, y \in K\}. \end{aligned}$$

Henceforth, in view of the above implications, the finite group G has been assumed to be non-abelian. It is also easy to see that if $C_K(x) = \{1\}$ for all $x \in H - \{1\}$, then

$$\Pr(H,K) = \frac{1}{|H|} + \frac{1}{|K|} - \frac{1}{|H||K|}. \qquad (5.1.b)$$

The following proposition says that $\Pr_g(H,K)$ is not very far from being symmetric with respect to H and K.

Proposition 5.1.1. *Let G be a finite group and $g \in G'$. If H and K are two subgroups of G, then $\Pr_g(H,K) = \Pr_{g^{-1}}(K,H)$. However, if $g^2 = 1$, or, if $g \in H \cup K$ (for example, when H or K is normal in G), we have $\Pr_g(H,K) = \Pr_g(K,H) = \Pr_{g^{-1}}(H,K)$.*

Proof. The first part follows from the fact that $[x,y]^{-1} = [y,x]$. For the second part, it is enough to note that if $g \in H$, then $(x,y) \mapsto (y^{-1}, yxy^{-1})$, and if $g \in K$, then $(x,y) \mapsto (xyx^{-1}, x^{-1})$ define bijective maps from the set $\{(x,y) \in H \times K : [x,y] = g\}$ to the set $\{(y,x) \in K \times H : [y,x] = g\}$. □

$\Pr_g(H,K)$ respects the Cartesian product in the following sense.

Proposition 5.1.2. *Let G_1 and G_2 be two finite groups with subgroups $H_1, K_1 \subseteq G_1$ and $H_2, K_2 \subseteq G_2$. Let $g_1 \in G_1'$ and $g_2 \in G_2'$. Then*

$$\Pr_{(g_1,g_2)}(H_1 \times H_2, K_1 \times K_2) = \Pr_{g_1}(H_1,K_1)\Pr_{g_2}(H_2,K_2).$$

Proof. It is enough to note that for all $x_1, y_1 \in G_1$ and for all $x_2, y_2 \in G_2$ we have $[(x_1,x_2),(y_1,y_2)] = ([x_1,y_1],[x_2,y_2])$. □

We now derive a computing formula which plays a key role in the study of $\Pr_g(H,K)$.

Theorem 5.1.3. *Let G be a finite group and $g \in G'$. If H and K are two subgroups of G, then*

$$\Pr_g(H,K) = \frac{1}{|H||K|} \sum_{\substack{x \in H \\ g^{-1}x \in \mathrm{C}\ell_K(x)}} |C_K(x)| = \frac{1}{|H|} \sum_{\substack{x \in H \\ g^{-1}x \in \mathrm{C}\ell_K(x)}} \frac{1}{|\,\mathrm{C}\ell_K(x)|},$$

where $C_K(x) = \{y \in K : xy = yx\}$ *and* $C\ell_K(x) = \{yxy^{-1} : y \in K\}$*, the* K*-conjugacy class of* x.

Proof. We have

$$\{(x, y) \in H \times K : [x, y] = g\} = \bigcup_{x \in H} \{x\} \times K_x,$$

where $K_x = \{y \in K : [x, y] = g\}$. Note that, for any $x \in H$, we have

$$K_x \neq \phi \Longleftrightarrow g^{-1}x \in C\ell_K(x).$$

Let $K_x \neq \phi$ for some $x \in H$. Fix an element $y_0 \in K_x$. Then $y \mapsto gy_0^{-1}y$ defines a one to one correspondence between the set K_x and the coset $gC_K(x)$. This means that $|K_x| = |C_K(x)|$.

Thus, we have

$$|\{(x, y) \in H \times K : [x, y] = g\}| = \sum_{x \in H} |K_x| = \sum_{\substack{x \in H \\ g^{-1}x \in C\ell_K(x)}} |C_K(x)|.$$

The first equality in the theorem now follows from (5.1.a).

For the second equality, consider the action of K on G by conjugation. Then, for all $x \in G$, we have

$$|\,C\ell_K(x)| = |\,\mathrm{orb}(x)| = |K : \mathrm{stab}(x)| = \frac{|K|}{|C_K(x)|}. \qquad (5.1.c)$$

This completes the proof. ☐

As an immediate consequence, we have the following generalization of the well-known formula $\Pr(G) = \frac{k(G)}{|G|}$.

Corollary 5.1.4. *Let G be a finite group and H, K be two subgroups of G. If $H \trianglelefteq G$, then*

$$\Pr(H, K) = \frac{k_K(H)}{|H|},$$

where $k_K(H)$ is the number of K-conjugacy classes that constitute H.

Proof. Note that K acts on H by conjugation. The orbit of any element $x \in H$ under this action is given by $C\ell_K(x)$, and so H is the disjoint union of these classes. Hence, we have

$$\Pr(H, K) = \frac{1}{|H|}\sum_{x \in H}\frac{1}{|\,C\ell_K(x)|} = \frac{k_K(H)}{|H|};$$

noting that, for $g = 1$, the condition $g^{-1}x \in C\ell_K(x)$ is superfluous. □

If $H \trianglelefteq G$ with $C_G(x) \subseteq H$ for all $x \in H - \{1\}$, then, using Sylow's theorems and the fact that non-trivial p-groups have non-trivial centers, we have $\gcd(|H|, |G : H|) = 1$. So, by Result 1.1.7 (the Schur-Zassenhaus Theorem), H has a complement in G. Such groups belong to a well-known class of groups called the Frobenius groups; for example, the alternating group A_4, the dihedral groups of order $2n$ with n odd, the non-abelian groups of order pq, where p and q are primes with $q|(p-1)$.

Proposition 5.1.5. *If H is an abelian normal subgroup of a finite group G with a complement K in G and $g \in G'$, then*

$$\Pr_g(H, G) = \Pr_g(H, K).$$

Proof. Let $x \in H$. Since H is abelian, we have

$$C_{HK}(x) = \{hk : hkx = xhk\} = \{hk : kx = xk\} = HC_K(x).$$

Thus, $|C_{HK}(x)| = |H|\,|C_K(x)|$. Also, since H is abelian and normal, $C\ell_K(x) = C\ell_{HK}(x)$. Hence, from Theorem 5.1.3, it follows that

$$\Pr_g(H, G) = \frac{1}{|H|^2|K|} \sum_{\substack{x \in H \\ g^{-1}x \in C\ell_{HK}(x)}} |C_{HK}(x)| = \Pr_g(H, K).$$

This completes the proof. □

Corollary 5.1.6. *Let G be a finite group and $g \in G'$. If $H \trianglelefteq G$ with $C_G(x) = H$ for all $x \in H - \{1\}$, then*

$$\Pr_g(H, G) = \Pr_g(H, K),$$

where K is a complement of H in G. In particular,

$$\Pr(H, G) = \frac{1}{|H|} + \frac{|H| - 1}{|G|}.$$

Proof. The first part follows from the discussion preceding the above proposition, and the second part follows from (5.1.b). □

5.2 Some bounds and inequalities

Let H and K be any two subgroups of a finite group G. Then we have

$$(C_H(K) \times K) \cup (H \times C_K(H)) \subseteq \{(x, y) \in H \times K : [x, y] = 1\}.$$

Therefore, from (5.1.a), it follows that

$$\Pr(H, K) \geq \frac{|C_H(K)|}{|H|} + \frac{|C_K(H)|(|H| - |C_H(K)|)}{|H||K|}.$$

On the other hand, we have

Proposition 5.2.1. *Let G be a finite group and $g \in G'$. Let H and K be any two subgroups of G. If $g \neq 1$, then*

(a) $\Pr_g(H, K) \neq 0 \Longrightarrow \Pr_g(H, K) \geq \dfrac{|C_H(K)||C_K(H)|}{|H||K|}$,

(b) $\Pr_g(H, G) \neq 0 \Longrightarrow \Pr_g(H, G) \geq \dfrac{2|H \cap Z(G)||C_G(H)|}{|H||G|}$,

(c) $\Pr_g(G) \neq 0 \Longrightarrow \Pr_g(G) \geq \dfrac{3}{|G : Z(G)|^2}$.

Proof. If $\Pr_g(H, K) \neq 0$, then there is a pair $(x, y) \in H \times K$ such that $g = [x, y]$. Since $g \neq 1$, we have $x \notin C_H(K)$ and $y \notin C_K(H)$. Consider the left coset $T_{(x,y)} = (x, y)(C_H(K) \times C_K(H))$ of $C_H(K) \times C_K(H)$ in $H \times K$. Clearly, $|T_{(x,y)}| = |C_H(K)||C_K(H)|$, and $[a, b] = g$ for all $(a, b) \in T_{(x,y)}$. This proves part (a).

Similarly, part (b) follows considering the two disjoint cosets $T_{(x,y)}$ and $T_{(x,yx)}$ with $K = G$, while part (c) follows considering the three disjoint cosets $T_{(x,y)}$, $T_{(xy,x)}$ and $T_{(x,yx)}$ with $H = K = G$. □

As a generalization of Result 1.5.16, we have

Proposition 5.2.2. *Let G be a finite group and $g \in G'$. If H and K are any two subgroups of G, then*

$$\Pr_g(H, K) \leq \Pr(H, K)$$

with equality if and only if $g = 1$.

Proof. By Theorem 5.1.3, we have

$$\begin{aligned}\Pr_g(H,K) &= \frac{1}{|H||K|}\sum_{\substack{x\in H\\ g^{-1}x\in C\ell_K(x)}} |C_K(x)|\\ &\le \frac{1}{|H||K|}\sum_{x\in H}|C_K(x)| = \Pr(H,K).\end{aligned}$$

Clearly, the equality holds if and only if $g^{-1}x \in C\ell_K(x)$ for all $x \in H$, that is, if and only if $g = 1$. □

The following is an improvement to Result 1.5.17.

Proposition 5.2.3. *Let G be a finite group and $g \in G'$, $g \neq 1$. Let H and K be any two subgroups of G. If p is the smallest prime divisor of $|G|$, then*

$$\Pr_g(H,K) \le \frac{|H| - |C_H(K)|}{p|H|} < \frac{1}{p}.$$

Proof. Without any loss, we may assume that $C_H(K) \neq H$. Let $x \in H$ be such that $g^{-1}x \in C\ell_K(x)$. Then, since $g \neq 1$, we have $x \notin C_H(K)$ and $|C\ell_K(x)| > 1$. But $|C\ell_K(x)|$ is a divisor of $|K|$, and hence, of $|G|$. Therefore, $|C\ell_K(x)| \ge p$. Hence, by Theorem 5.1.3, we have

$$\Pr_g(H,K) \le \frac{1}{|H|}\sum_{\substack{x\in H\\ g^{-1}x\in C\ell_K(x)}} \frac{1}{p} \le \frac{|H| - |C_H(K)|}{p|H|} < \frac{1}{p}.$$

This completes the proof. □

$\Pr(H,K)$ is monotonic in the following sense.

Proposition 5.2.4. *Let H, K_1 and K_2 be subgroups of a finite group G with $K_1 \subseteq K_2$. Then*

$$\Pr(H,K_1) \ge \Pr(H,K_2)$$

with equality if and only if $\mathrm{C}\ell_{K_1}(x) = \mathrm{C}\ell_{K_2}(x)$ *for all* $x \in H$.

Proof. Clearly, $\mathrm{C}\ell_{K_1}(x) \subseteq \mathrm{C}\ell_{K_2}(x)$ for all $x \in H$. So, by Theorem 5.1.3, we have

$$\Pr(H, K_1) = \frac{1}{|H|}\sum_{x\in H}\frac{1}{|\mathrm{C}\ell_{K_1}(x)|} \geq \frac{1}{|H|}\sum_{x\in H}\frac{1}{|\mathrm{C}\ell_{K_2}(x)|} = \Pr(H, K_2).$$

The condition for equality is obvious. □

Since $\Pr(H, K) = \Pr(K, H)$, it follows from the above proposition that if $H_1 \subseteq H_2$ and $K_1 \subseteq K_2$ are subgroups of G, then

$$\Pr(H_1, K_1) \geq \Pr(H_2, K_2).$$

Proposition 5.2.5. *Let* H, K_1 *and* K_2 *be subgroups of a finite group* G *with* $K_1 \subseteq K_2$. *Then*

$$\Pr(H, K_2) \geq \frac{1}{|K_2 : K_1|}\left(\Pr(H, K_1) + \frac{|K_2| - |K_1|}{|H||K_1|}\right)$$

with equality if and only if $C_H(x) = \{1\}$ *for all* $x \in K_2 - K_1$.

Proof. By Theorem 5.1.3, we have

$$\begin{aligned}\Pr(H, K_2) &= \frac{1}{|H||K_2|}\left(\sum_{x\in K_1}|C_H(x)| + \sum_{x\in K_2 - K_1}|C_H(x)|\right)\\ &\geq \frac{1}{|K_2 : K_1|}\left(\Pr(H, K_1) + \frac{|K_2| - |K_1|}{|H||K_1|}\right).\end{aligned}$$

Clearly, the equality holds if and only if

$$\sum_{x\in K_2 - K_1}(|C_H(x)| - 1) = 0,$$

that is, if and only if $C_H(x) = \{1\}$ for all $x \in K_2 - K_1$. □

In general, $\Pr_g(H,K)$ is not monotonic. For example, if we consider $G = S_3$, $g = (1\,2\,3)$, $H = \langle(1\,2)\rangle$, $K_1 = \langle(1)\rangle$, $K_2 = \langle(1\,3)\rangle$ and $K_3 = S_3$, then

$$\Pr_g(H,K_1) = 0 \lneq \Pr_g(H,K_2) = \frac{1}{4} \gneq \Pr_g(H,K_3) = \frac{1}{6}.$$

However, we have

Proposition 5.2.6. *Let $H_1 \subseteq H_2$ and $K_1 \subseteq K_2$ be subgroups of a finite group G and $g \in G'$. Then*

$$\Pr_g(H_1,K_1) \leq |H_2 : H_1||K_2 : K_1| \Pr_g(H_2,K_2)$$

with equality if and only if

$$\begin{aligned} & g^{-1}x \notin \mathrm{C}\ell_{K_2}(x) \ \ \textit{for all} \ \ x \in H_2 - H_1, \\ & g^{-1}x \notin \mathrm{C}\ell_{K_2}(x) - \mathrm{C}\ell_{K_1}(x) \ \ \textit{for all} \ \ x \in H_1, \\ \textit{and} \quad & C_{K_1}(x) = C_{K_2}(x) \ \ \textit{for all} \ \ x \in H_1 \ \ \textit{with} \ \ g^{-1}x \in \mathrm{C}\ell_{K_1}(x). \end{aligned}$$

In particular, for $g = 1$, the condition for equality reduces to $H_1 = H_2$, and $K_1 = K_2$.

Proof. By Theorem 5.1.3, we have

$$\begin{aligned} |H_1||K_1|\Pr_g(H_1,K_1) &= \sum_{\substack{x \in H_1 \\ g^{-1}x \in \mathrm{C}\ell_{K_1}(x)}} |C_{K_1}(x)| \\ &\leq \sum_{\substack{x \in H_2 \\ g^{-1}x \in \mathrm{C}\ell_{K_2}(x)}} |C_{K_2}(x)| = |H_2||K_2|\Pr_g(H_2,K_2). \end{aligned}$$

The condition for equality follows immediately. ☐

Using Propostion 5.2.2, we have

Corollary 5.2.7. *Let G be a finite group, H be a subgroup of G and $g \in G'$. Then*

$$\Pr_g(H, G) \leq |G : H| \Pr(G)$$

with equality if and only if $g = 1$ and $H = G$.

The following theorem generalizes Result 1.5.14.

Theorem 5.2.8. *Let G be a finite group and p be the smallest prime dividing $|G|$. If H and K are any two subgroups of G, then*

$$\Pr(H, K) \geq \frac{|C_H(K)|}{|H|} + \frac{p(|H| - |X_H| - |C_H(K)|) + |X_H|}{|H||K|}$$

$$\textit{and } \Pr(H, K) \leq \frac{(p-1)|C_H(K)| + |H|}{p|H|} - \frac{|X_H|(|K| - p)}{p|H||K|},$$

where $X_H = \{x \in H : C_K(x) = 1\}$. Moreover, in each of these bounds, H and K can be interchanged.

Proof. If $[H, K] = 1$, then there is nothing to prove, as in that case $C_H(K) = H$, and X_H equals H or an empty set according as K is trivial or non-trivial.

On the other hand, if $[H, K] \neq 1$, then $X_H \cap C_H(K) = \phi$, and so

$$\begin{aligned}\sum_{x \in H} |C_K(x)| &= \sum_{x \in X_H} |C_K(x)| + \sum_{x \in C_H(K)} |C_K(x)| + \sum_{x \in H - (X_H \cup C_H(K))} |C_K(x)| \\ &= |X_H| + |K||C_H(K)| + \sum_{x \in H - (X_H \cup C_H(K))} |C_K(x)|.\end{aligned}$$

But, for all $x \in H - (X_H \cup C_H(K))$, we have $\{1\} \neq C_K(x) \neq K$, which means that $p \leq |C_K(x)| \leq \frac{|K|}{p}$. Hence, using Theorem 5.1.3, we get the required bounds for $\Pr(H, K)$. The final statement of the theorem follows from the fact that $\Pr(H, K) = \Pr(K, H)$. □

As a consequence we have

Corollary 5.2.9. *Let G be a finite group and p be the smallest prime dividing $|G|$. If H and K are two subgroups of G such that $[H, K] \neq \{1\}$, then*

$$\Pr(H, K) \leq \frac{2p-1}{p^2}.$$

In particular, $\Pr(H, K) \leq \frac{3}{4}$.

Proof. Since, $[H, K] \neq \{1\}$, we have $K \neq \{1\}$ and $C_H(K) \neq H$. So, $|K| \geq p$ and $|C_H(K)| \leq \frac{|H|}{p}$. Therefore, by Theorem 5.2.8, we have

$$\Pr(H, K) \leq \frac{(p-1)|C_H(K)| + |H|}{p|H|} \leq \frac{\frac{p-1}{p} + 1}{p} = \frac{2p-1}{p^2} \leq \frac{3}{4},$$

since $p \geq 2$. □

One can see that the above bound is the best possible. For example, if we consider a finite non-abelian group G with p as the smallest prime divisor of $|G|$ and two cyclic subgroups H and K of order p generated by two non-commuting elements a and b, then, using (5.1.b), we have $\Pr(H, K) = \frac{2p-1}{p^2}$.

Proposition 5.2.10. *Let G be a finite group and H, K be any two subgroups of G. If $\Pr(H, K) = \frac{2p-1}{p^2}$ for some prime p, then p divides $|G|$. If p happens to be the smallest prime divisor of $|G|$, then*

$$\frac{H}{C_H(K)} \cong C_p \cong \frac{K}{C_K(H)}, \quad \textit{and hence, } H \neq K.$$

In particular, $\frac{H}{C_H(K)} \cong C_2 \cong \frac{K}{C_K(H)}$ *if* $\Pr(H, K) = \frac{3}{4}$.

Proof. The first part follows from the definition of $\Pr(H, K)$.

For the second part, by Theorem 5.2.8, we have

$$\begin{aligned} \frac{2p-1}{p^2} &\le \frac{(p-1)|C_H(K)| + |H|}{p|H|} \\ \Longrightarrow |H : C_H(K)| &\le p. \end{aligned}$$

Since p is the smallest prime divisor of $|G|$, it follows that $|H : C_H(K)| = p$, whence $\frac{H}{C_H(K)} \cong C_p$; noting that $C_H(K) \neq H$ because $\Pr(H, K) = \frac{2p-1}{p^2} \neq 1$. Similarly, we have $\frac{K}{C_K(H)} \cong C_p$. Since $\frac{H}{Z(H)}$ is never cyclic unless trivial, we have $H \neq K$.

The third part follows from the first two parts. □

5.3 A character theoretic formula

In this section, we derive a character theoretic formula for the generalized relative commutativity degree of a finite group G. As an application, we obtain yet another condition under which every element of G' is a commutator (compare with Remark 1.1.2, Theorem 2.4.3 and Corollary 4.3.2).

Let H be a normal subgroup of G. Let $\tilde{\zeta}(g)$ denote the number of solutions $(x, y) \in H \times G$ of the equation $[x, y] = g$. Then, by (5.1.a), we have

$$\Pr_g(H, G) = \frac{\tilde{\zeta}(g)}{|H||G|}. \tag{5.3.a}$$

It has been observed in Theorem 3.3.1 that

$$\tilde{\zeta}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|H|[\chi_H, \chi_H]}{\chi(1)} \chi(g).$$

Therefore, it follows that

$$\Pr_g(H,G) = \frac{1}{|G|}\sum_{\chi\in\mathrm{Irr}(G)} \frac{[\chi_H,\chi_H]}{\chi(1)}\chi(g). \tag{5.3.b}$$

This character theoretic formula enables us to strengthen Corollary 5.2.7 as follows.

Proposition 5.3.1. *Let G be a finite group. If H is a normal subgroup of G and $g \in G'$, then*

$$\left|\Pr_g(H,G) - \frac{1}{|G'|}\right| \le |G:H|\left(\Pr(G) - \frac{1}{|G'|}\right).$$

Proof. For all $\chi \in \mathrm{Irr}(G)$ with $\chi(1) = 1$, we have $G' \subseteq \ker\chi$ and $[\chi_H,\chi_H] = 1$. Also, $|G:G'|$ equals the number of linear characters of G. Therefore, by (5.3.b),

$$\Pr_g(H,G) = \frac{1}{|G'|} + \frac{1}{|G|}\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)\neq 1}} \frac{[\chi_H,\chi_H]}{\chi(1)}\chi(g).$$

Since $|\chi(g)| \le \chi(1)$ for all $\chi \in \mathrm{Irr}(G)$, we have, using (1.2.k),

$$\begin{aligned}\left|\Pr_g(H,G) - \frac{1}{|G'|}\right| &\le \frac{1}{|G|}\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)\neq 1}} [\chi_H,\chi_H] \\ &\le \frac{1}{|G|}\left(|\mathrm{Irr}(G)| - |G:G'|\right)|G:H| \\ &= |G:H|\left(\Pr(G) - \frac{1}{|G'|}\right).\end{aligned}$$

This completes the proof. □

In particular, we have

Corollary 5.3.2. *Let G be a finite group. If G' contains a non-commutator (an element which is not a commutator), then* $\Pr(G) \geq \frac{2}{|G'|}$.

Proof. The corollary follows by choosing a non-commutator $g \in G'$, and putting $H = G$. □

Finally, we have the following result.

Proposition 5.3.3. *Let G be a finite group and p be the smallest prime dividing $|G|$. If $|G'| \leq p^2$, then every element of G' is a commutator.*

Proof. By Result 1.5.2, we have

$$\Pr(G) \leq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{p^2}\right).$$

Hence, if G' contains a non-commutator, it follows, using Corollary 5.3.2, that $|G'| \geq p^2 + 1$. This completes the proof. □

Chapter 6

Conclusion and some possible research problems

In Chapter 2 through 5, we have studied and generalized the notion of commutativity degree of a finite group. We have obtained several identities and inequalities involving these notions and in a few occasions we could develop certain character theoretic formula for these notions. We have also observed that these concepts can very well be used to obtain certain characterizations of finite groups. More precisely, a finite group possesses certain special properties expressible in standard group theoretic terms if (and, quite often, only if) its commutativity degree (including its generalizations) satisfies certain identities and inequalities. For example, on more than one occasion, we are able to provide new conditions under which every element of the commutator subgroup of a finite group is actually a commutator. We are also able to provide certain conditions under which a finite group is of central type or nilpotent of class 2. In this chapter, we mention certain research problems, for further considerations, which are related to the results obtained in the earlier chapters.

6.1 Research problems

In Chapter 2, we have obtained a characterization for all finite groups G of odd order satisfying the condition $\Pr(G) \geq \frac{11}{75}$. It is not difficult to see that the technique used for this purpose is not applicable to the situation $\Pr(G) \leq \frac{1}{9}$. In this regard we have the following problem.

Problem 6.1.1. *To characterize all finite groups of odd order having commutativity degree greater than or equal to a number less than* $\frac{11}{75}$.

In the same line we also have another problem.

Problem 6.1.2. *To characterize all finite groups (not necessarily of odd order) having commutativity degree greater than or equal to* $\frac{11}{75}$.

In Chapter 3, we have seen that given an admissible word $\omega(x_1, x_2, \ldots, x_n)$, a finite group G and an element $g \in G$, the number of solutions of the word equation $\omega(x_1, x_2, \ldots, x_n) = g$ defines a character of G. In this regard we have the following problem.

Problem 6.1.3. *To explicitly determine a complex representation of* G *which affords the above-mentioned character.*

The same question can be asked for various characters of G obtained in Section 3.3.

Let $w(x_1, x_2, \ldots, x_n)$ denote the product of $x_1^{\alpha_1}$, $x_2^{\alpha_2}$, $\ldots$, $x_n^{\alpha_n}$, $x_1^{-\alpha_1}$, $x_2^{-\alpha_2}, \ldots$, $x_n^{-\alpha_n}$ in a randomly chosen order, where each α_i is a natural number, $1 \leq i \leq n$. In view of Section 3.1, one may also like to consider the following problem.

Problem 6.1.4. *Given a finite group G and $g \in G$, to determine whether the number of solutions of the word equation $w(x_1, x_2, \ldots, x_n) = g$ defines a character of G.*

Let $\omega(x_1, x_2, \ldots, x_n)$ be an admissible word and H be a subgroup of a finite group G. Let $g \in G$ and $\tilde{\zeta}_\omega(g)$ be the number of solutions of the word equation $\omega(x_1, x_2, \ldots, x_n) = g$, when the values of a given set of variables x_i are restricted to H. In this connection, we can pose the following problem (see Section 3.3).

Problem 6.1.5. *To determine whether $\tilde{\zeta}_\omega$ is a character of G.*

Moreover, as in Chapter 5, one can also try to tackle the following problem.

Problem 6.1.6. *To study the ratio $\text{Pr}_g^\omega(H, G) = \frac{\tilde{\zeta}_\omega(g)}{|H|^r |G|^{n-r}}$, where r is the number of variables that are restricted to H.*

Given a finite group G, an element $g \in G'$ and an admissible word ω, we have studied, in Chapter 4, the ratio $\text{Pr}_g^\omega(G)$ defined by (4.1.a). Let H be a subgroup of G. Consider the ratio

$$\text{Pr}_H^\omega(G) = \frac{|\{(g_1, g_2, \ldots, g_n) \in G^n \, : \, \omega(g_1, g_2, \ldots, g_n) \in H\}|}{|G^n|}.$$

Clearly, $\text{Pr}_H^\omega(G) = \sum\limits_{g \in H} \text{Pr}_g^\omega(G)$. Also, if H is cyclic of prime order, then, by Proposition 4.1.4, we have $\text{Pr}_H^\omega(G) = \text{Pr}_1^\omega(G) + (|H| - 1)\text{Pr}_h^\omega(G)$, where $1 \neq h \in H$. In this connection, the following problem is worth considering.

Problem 6.1.7. *To study* $\mathrm{Pr}_H^\omega(G)$ *under various group theoretic assumptions on* H*, and to see whether it helps in characterizing* G*.*

In Chapter 4, we have also studied the ratio $\mathrm{Pr}_g^\omega(G)$ assuming that ω is a generalized commutator. In this regard we have the following problem.

Problem 6.1.8. *To study the ratio* $\mathrm{Pr}_g^\omega(G)$ *assuming that* ω *is an* n*-fold commutator.*

In [34], D. MacHale has introduced the concept of the commutativity degree of finite rings. He noticed that there are a number of results on the commutativity degree of rings that are similar to the ones for groups, though the notion of conjugacy in groups has no obvious analogue in rings. Obviously, his techniques are quite different from those adopted for groups.

Problem 6.1.9. *To find ring theoretic analogues of various results obtained in the earlier chapters.*

The above problem can also be posed for other algebraic structures.

Since the days of W. H. Gustafson [22], a number of people, like A. Erfanian, R. Kamyabi-Gol, R. Rezaei and F. Russo (see [14, 15, 41, 45]) have studied the concept of commutativity degree of certain classes of compact groups. In this connection one may like to consider the following problem.

Problem 6.1.10. *To study the analogues of various results obtained in the earlier chapters in case of compact groups.*

Needless to mention that the methods and the techniques used in this thesis do not seem to be adequate enough to tackle the above mentioned problems. Moreover, a few of them are beyond the scope of this thesis.

Bibliography

[1] F. Barry, D. MacHale and Á. Ní Shé, *Some supersolvability conditions for finite groups*, Math. Proc. Royal Irish Acad. **106A** (2) (2006), 163–177.

[2] S. M. Belcastro and G. J. Sherman, *Counting centralizers in finite groups*, Math. Magazine **67** (5) (1994), 366–374.

[3] Y. G. Berkovich and E. M. Zhmud′, *Characters of Finite Groups*. Part 1, Transl. Math. Monographs **172**, Amer. Math. Soc., Providence, RI, 1998.

[4] A. K. Das, *On arithmetic functions of finite groups*, Bull. Austral. Math. Soc. **75** (2007), 45–58.

[5] A. K. Das and R. K. Nath, *On solutions of a class of equations in a finite group*, Comm. Algebra **37** (11) (2009), 3904–3911.

[6] A. K. Das and R. K. Nath, *On generalized relative commutativity degree of a finite group*, International Electronic J. Algebra **7** (2010), 140–151.

[7] J. Dénes, P. Erdös and P. Turán, *On some statistical properties of the alternating group of degree n*, Extrait de L'Enseignement mathédmatique, T. XV, (1969), 89–99.

[8] J. D. Dixon, Problem 176, Canad. Math. Bull. **16** (1973), 302.

[9] P. Erdös and P. Turán, *On some problems of a statistical group-theory. I*, Z. Wahrschein. Verw. Gebeite **4** (1965), 175–186.

[10] P. Erdös and P. Turán, *On some problems of a statistical group-theory. II*, Acta Math. Acad. Sci. Hungar. **18** (1967), 151–163.

[11] P. Erdös and P. Turán, *On some problems of a statistical group-theory. III*, Acta Math. Acad. Sci. Hungar. **18** (1967), 309–320.

[12] P. Erdös and P. Turán, *On some problems of a statistical group-theory. IV*, Acta. Math. Acad. Sci. Hungar. **19** (1968), 413–435.

[13] A. Erfanian, R. Rezaei and P. Lescot, *On the relative commutativity degree of a subgroup of a finite group*, Comm. Algebra **35** (12) (2007), 4183–4197.

[14] A. Erfanian and R. Kamyabi-Gol, *On the mutually commuting n-tuples in compact groups*, International J. Algebra **1**(6) (2007), 251–262.

[15] 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.

[16] I. V. Erovenko and B. Sury, *Commutativity degree of wreath products of finite abelian groups*, Bull. Aus. Math. Soc. **77** (1) (2008), 31-36.

[17] A. Espuelas, *On certain groups of central type*, Proc. Amer. Math. Soc. **97** (1) (1986), 16–18.

[18] F. G. Frobenius, *Über Gruppencharaktere*, Gesammelte Abhandlungen Band III, p. 1–37 (J. P. Serre, ed.) Springer-Verlag, Berlin, 1968.

[19] S. Garion and A. Shalev, *Commutator maps, measure preservation, and T-systems*, Trans. Amer. Math. Soc. **361** (9) (2009), 4631–4651.

[20] R. M. Guralnick and G. R. Robinson, *On the commuting probability in finite groups*, J. Algebra **300** (2) (2006), 509–528.

[21] R. M. Guralnick and G. R. Robinson, *Addendum to paper "On the commuting probability in finite groups" R. M. Guralnick and G. R. Robinson [J. Algebra 300 (2) (2006), 509–528]*, J. Algebra **319** (2) (2008), 1822.

[22] W. H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034.

[23] P. Hall, *The classification of prime-power groups*, J. Reine Angew. Math. **182** (1940), 130–141.

[24] B. Huppert, *Character Theory of Finite Groups*, Walter de Gruyter, Berlin, New York, 1998.

[25] I. M. Isaacs, *Character Theory of Finite Groups*, Dover Publications, Inc., New York, 1994.

[26] K. S. Joseph, *Commutativity in non-abelian groups*, Unpublished Ph. D. thesis, University of California, Los Angeles, 1969.

[27] L. C. Kappe and R. F. Morse, *On commutators in groups* (English summary), Groups St. Andrews 2005, Vol. 2, 531–558; London Math. Soc. Lecture Note ser. **340**, Cambridge Univ. Press, Cambridge, 2007.

[28] P. Kellersch and K. Meyberg, *On a Casimir element of a finite group*, Comm. Algebra **25** (6) (1997), 1695–1702.

[29] H. Kurzweil and B. Stellmacher, *The Theory of Finite Groups: An Introduction*, Springer, Universitext, New York, 2004.

[30] P. Lescot, *Isoclinism classes and commutativity degrees of finite groups*, J. Algebra **177** (1995), 847–869.

[31] P. Lescot, *Central extensions and commutativity degree*, Comm. Algebra **29** (10) (2001), 4451–4460.

[32] M. W. Liebeck and A. Shalev, *Fuchsian groups coverings of Riemann surfaces, subgroup growth, random quotients and random walks*, J. Algebra **276** (2004), 552–601.

[33] D. MacHale, *How commutative can a non-commutative group be?*, Math. Gaz. LVIII (1974), 199–202.

[34] D. MacHale, *Commutativity in finite rings*, Amer. Math. Monthly **83** (1976), 30–32.

[35] D. MacHale and P. Ó Murchú, *Commutator subgroups of groups with small central factor groups*, Math. Proc. Royal Irish Acad. **93A** (1993), 123–129.

[36] 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), 225–261.

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

[38] R. K. Nath and A. K. Das, *On generalized commutativity degree of a finite group*, Rocky Mountain J. Math. (to appear).

[39] R. K. Nath and A. K. Das, *A characterization of certain finite groups of odd order*, communicated.

[40] M. R. Pournaki and R. Sobhani, *Probability that the commutator of two group elements is equal to a given element*, J. Pure Appl. Algebra **212** (2008), 727–734.

[41] R. Rezaei and A. Erfanian, *On the commutativity degree of compact groups*, Arch. Math. **93** (2009), 345–356.

[42] D. J. S. Robinson, *A course in the Theory of Groups* (Second Edition), Graduate Text in Mathematics **80**, Springer, New York, 1996.

[43] J. J. Rotman, *An Introduction to the Theory of Groups* (third edition), Allyn and Bacon, Inc, 1984.

[44] D. J. Rusin, *What is the probability that two elements of a finite group commute?*, Pacific J. Math. **82** (1979), 237–247.

[45] F. Russo, *A probabilistic meaning of certain quasinormal subgroups*, International J. Algebra **1**(8) (2007), 385–392.

[46] A. Shalev, *Commutators, words, conjugacy classes and character methods*, Turk. J. Math. **31** (2007), 131–148.

[47] S. P. Strunkov, *Some conditions for the existence of p-blocks of defect* 0 *in finite groups*, English translation, Math. USSR-Sb. **70** (1991), 587–592.

[48] S. P. Strunkov, *On the theory of equations in finite groups*, English translation, Izv. Math. **59** (6) (1995) 1273–1282.

[49] T. Tambour, *The number of solutions of some equations in finite groups and a new proof of Itô's theorem*, Comm. Algebra **28** (11) (2000), 5353–5361.

[50] E. Witten, *On quantum gauge theories in two dimensions*, Comm. Math. Phys. **141** (1991), 153–209.

[51] The GAP Group, *GAP - Groups, Algorithms, and Programming*, Version 4.4.12; 2008, (`http://www.gap-system.org`).

Index

Brief Bio-data

1. Name:	RAJAT KANTI NATH
2. Sex:	Male
3. Date of birth:	2^{nd} February, 1982.
4. Father's Name:	Shri Bharat Chandra Nath
5. Nationality:	Indian
6. Permanent Address:	Vill - Suripara, P.O. - Dhanpur Dist. - Dhubri, Assam, Pin - 783 337.
7. E-mail:	rajatkantinath@yahoo.com, rknathnehu@gmail.com.
8. Academic Qualifications:	M. Phil. in Mathematics (North-Eastern Hill University), M. Sc. in Mathematics (Tezpur University).
9. Awards and Achievements:	(a) Gold Medal in M.Sc. (b) Certificate of Appreciation from Govt. of India.

10. Workshop/Conference attended:

(a) UGC-SAP workshop on *Algebra, Algebraic Topology and related topics*, held at North-Eastern Hill University, Meghalaya, organized by Dept. of Mathematics, NEHU, Meghalaya, from March 15 to 20, 2010.

(b) National Conference on *Recent trends in Mathematics and its applications*, held at Gauhati University, organized by Assam Science Society and Gauhati University, Assam, from September 12 to 13, 2009.

(c) Advanced Instructional School on *Combinatorics and Graph Theory (AIS-CGT)*, held at Bhaskaracharya Pratishthana, Pune. Organized by National Board of Higher Mathematics, India, from 8th May to 4th June, 2009.

(d) *Short term visit*, Tata Institute of Fundamental Research (TIFR), Mumbai, from June 4 to 12, 2009.

(e) *96th Indian Science Congress*, held at North-Eastern Hill University, Meghalaya. Organized by Indian Science Congress Association, from January 3 to 7, 2009.

(f) International Workshop and Conference on *Surface mapping class groups and related topics*, held at North-Eastern Hill University, Meghalaya. Organized by Department of Mathematics, North-Eastern Hill University, Meghalaya, from June 16 to 28, 2008.

(g) *CMFT Workshop, 2008*, held at Don Bosco Institute, Guwahati, Assam. Organized by CMFT, Germany, from January 3 to 10, 2008.

(h) Advanced Instructional School on *Algebraic and Analytic Number Theory*, held at Harish-Chandra Research Institute, Allahabad. Organized by National Board of Higher Mathematics, India, from December 3 to 28, 2007.

(i) North-East School on *Computational Geometry*, held at St. Anthony's College, Meghalaya. Organized by Advanced computing & Microelectronics Unit, Indian Statistical Institute, Kolkata, and Department of Computer Science, St. Anthony's College, Meghalaya, from November 1 to 3, 2007.

(j) Symposium on *Some recent advances in Mathematics*, held at North-Eastern Hill University, Meghalaya. Organized by Department of Mathematics, North-Eastern Hill University, Meghalaya, from April 4 to 5, 2007.

11. Papers presented:

(a) *On a lower bound of commutativity degree*, presented in the UGC-SAP Workshop on Algebra, Algebraic Topology and Related topics, held at North-Eastern Hill University, Meghalaya, organized by the Department of Mathematics, North-Eastern Hill University, Meghalaya, from March 15 to 20, 2010.

(b) *Some Generalizations of Commutativity degree and classifications of finite groups*, presented at the National Conference on Recent Trends in Mathematics and its Applications, held at Gauhati University, organized by Assam Science Society and Gauhati University, Assam, from September 12 to 13, 2009.

(c) *Certain generalizations of commutativity degree of finite groups*, presented at the 96th Indian Science Congress, held at North-Eastern Hill University, Meghalaya. Organized by Indian Science Congress Association, during January 3 to 7, 2009.

12. List of Research Papers published/accepted/communicated in refereed Journals:

(a) A. K. Das and R. K. Nath, *On solutions of a class of equations in a finite group*, Comm. Algebra **37** (11) (2009), 3904–3911.

(b) A. K. Das and R. K. Nath, *On generalized relative commutativity degree of a finite group*, International Electronic J. Algebra **7** (2010), 140–151.

(c) R. K. Nath and A. K. Das, *On a lower bound of commutativity degree*, Rend. Circ. Mat. Palermo **59** (2010), 137–142.

(d) R. K. Nath and A. K. Das, *On generalized commutativity degree of a finite group*, to appear in Rocky Mountain J. Math.

(e) R. K. Nath and A. K. Das, *A characterization of certain finite groups of odd order*, communicated.

Front-pages

of

Publications

Communications in Algebra®, 37 3904–3911, 2009

ISSN 0092-7872 print/1532-4125 online
DOI 10 1080/00927870902828777

ON SOLUTIONS OF A CLASS OF EQUATIONS IN A FINITE GROUP

A. K. Das and R. K. Nath
Department of Mathematics, North Eastern Hill University, Shillong, Meghalaya, India

Let G be a finite group and $\omega(x_1, x_2, \ldots, x_n)$ denote the product of $x_1, x_2, \ldots, x_n$, $x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}$ in a randomly chosen order. The object of this article is to prove that the number of solutions of the equation $\omega(x_1, x_2, \ldots, x_n) = g$, with $g \in G$, defines a character of G.

Key Words: Finite groups; Group characters.

2000 Mathematics Subject Classification: 20C15.

1. INTRODUCTION

Throughout this article, G denotes a finite group. Let $F(x_1, x_2, \ldots, x_n)$ denote the free group of words on n generators $x_1, x_2, \ldots, x_n$. For $1 \leq i \leq n$, we write $x_i \in \omega(x_1, x_2, \ldots, x_n)$ to mean that x_i has a nonzero index (i.e., x_i^k forms a syllable, with $0 \neq k \in \mathbb{Z}$) in the word $\omega(x_1, x_2, \ldots, x_n)$. A word $\omega(x_1, x_2, \ldots, x_n) \in F(x_1, x_2, \ldots, x_n)$ is called *admissible* if each $x_i \in \omega(x_1, x_2, \ldots, x_n)$ has precisely two nonzero indices, namely, $+1$ and -1. Let $\mathscr{A}(x_1, x_2, \ldots, x_n)$ denote the set of all admissible words in $F(x_1, x_2, \ldots, x_n)$. For $g \in G$, let $\zeta_n^{\omega}(g)$ denote the number of solutions $(a_1, a_2, \ldots, a_n) \in G^n$ of the equation $\omega(x_1, x_2, \ldots, x_n) = g$, where $G^n = G \times G \times \cdots \times G$ (n times). Thus,

$$\zeta_n^{\omega}(g) = |\{(a_1, a_2, \ldots, a_n) \in G^n : \omega(a_1, a_2, \ldots, a_n) = g\}|,$$

where $\omega(a_1, a_2, \ldots, a_n)$ denotes the image of $\omega(x_1, x_2, \ldots, x_n)$ under the unique natural homomorphism $\tau : F(x_1, x_2, \ldots, x_n) \longrightarrow G$ which maps x_i to a_i, $1 \leq i \leq n$. Conventionally, $\zeta_0^{\omega}(g) = 1$ if $g = 1$ and zero otherwise. In this article, we prove that, for each $\omega(x_1, x_2, \ldots, x_n) \in \mathscr{A}(x_1, x_2, \ldots, x_n)$, $n \geq 1$, the map $\zeta_n^{\omega} : G \to \mathbb{C}$ is a character of G. This is a generalization of a classical result of Frobenius [1].

Since the days of Frobenius, equations in finite groups have been studied by many authors who include Solomon [6], Isaacs [2], Kerber and Wagner [4], Strunkov [7, 8], Tambour [10], etc. Strunkov [9] has summarized the connections between

Received July 10, 2008; Revised November 14, 2008. Communicated by D. Macpherson.
Address correspondence to Dr A. K Das, Department of Mathematics, North Eastern Hill University, Permanent Campus, Shillong 793022, Meghalaya, India; E-mail akdas@nehu ac.in

INTERNATIONAL ELECTRONIC JOURNAL OF ALGEBRA
VOLUME 7 (2010) 140-151

ON GENERALIZED RELATIVE COMMUTATIVITY DEGREE OF A FINITE GROUP

A. K. Das and R. K. Nath

Received: 12 October 2009; Revised. 15 December 2009
Communicated by A. Çiğdem Özcan

ABSTRACT. Given any two subgroups H and K of a finite group G, and an element $g \in G$, the aim of this article is to study the probability that the commutator of an arbitrarily chosen pair of elements (one from H and the other from K) equals g.

Mathematics Subject Classification (2000): 20C15, 20D60, 20P05
Keywords: commutativity degree, commutators, group characters

1. Introduction

Throughout this paper G denotes a finite group, H and K two subgroups of G, and g an element of G. In [1], Erfanian et al. have considered the probability $\Pr(H, G)$ for an element of H to commute with an element of G. On the other hand, in [8], Pournaki et al. have studied the probability $\Pr_g(G)$ that the commutator of an arbitrarily chosen pair of group elements equals g (a generalization of this notion can be found also in [7]). The main object of this paper is to further generalize these notions and study the probability that the commutator of a randomly chosen pair of elements (one from H and the other from K) equals g. In other words, we study the ratio

$$\Pr_g(H, K) = \frac{|\{(x, y) \in H \times K : xyx^{-1}y^{-1} = g\}|}{|H||K|}, \tag{1}$$

and further extend some of the results obtained [1] and [8]. In the final section, with H normal in G, we also develop and study a character theoretic formula for $\Pr_g(H, G)$, which generalizes the formula for $\Pr_g(G)$ given in ([8], Theorem 2.1). In the process we generalize a classical result of Frobenius (see [2]).

Note that if $H = K = G$ then $\Pr_g(H, K) = \Pr_g(G)$, which coincides with the usual commutativity degree $\Pr(G)$ of G if we take $g = 1$, the identity element of G. It may be recalled (see, for example, [3]) that $\Pr(G) = \frac{k(G)}{|G|}$ where $k(G)$ denotes the number of conjugacy classes of G. On the other hand, if $K = G$ and $g = 1$ then $\Pr_g(H, K) = \Pr(H, G)$.

Rendiconti del Circolo Matematico di Palermo 59, 137–142 (2010)
DOI: 10.1007/s12215-010-0010-6

Rajat Kanti Nath · Ashish Kumar Das

On a lower bound of commutativity degree

Received: August 26, 2009 / Accepted: December 16, 2009 – © Springer-Verlag 2010

Abstract. The commutativity degree of a finite group G, denoted by $\Pr(G)$, is the probability that a randomly chosen pair of elements of G commute. The object of this paper is to derive a lower bound for $\Pr(G)$ and study some of its consequences towards characterizing G.

Keywords Finite groups · Group characters · Commutativity degree

Mathematics Subject Classification (2000) 20C15 · 20D60 · 20P05

1 Introduction

Given a finite group G, its commutativity degree, denoted by $\Pr(G)$, is the probability that a randomly chosen pair of elements of G commute. It may be recalled (see, for example, [2]) that $\Pr(G) = \frac{k(G)}{|G|}$ where $k(G)$ denotes the number of conjugacy classes of G.

The primary object of this paper is to derive a lower bound for $\Pr(G)$ with no restriction on the finite group G. It may be mentioned here that Pournaki (see [9], Corollary 2.3) has obtained this bound under an additional hypothesis that $|\mathrm{cd}(G)| = 2$, where $\mathrm{cd}(G) = \{\chi(1) : \chi \in \mathrm{Irr}(G)\}$ with $\mathrm{Irr}(G)$ denoting the set of all irreducible complex characters of G.

We also derive certain necessary and sufficient conditions under which this lower bound is attained, and as a consequence we obtain some characterizations for finite nilpotent groups whose commutator subgroups have prime

R.K. Nath · A.K. Das (✉)
Department of Mathematics, North-Eastern Hill University, Permanent Campus, Shillong-793022, Meghalaya, India.
E-mail: rknathnehu@gmail.com (R.K. Nath), akdas@nehu.ac.in (A.K. Das)

To appear in the Rocky Mountain Journal of Mathematics.
Accepted on 11 February 2009

ON GENERALIZED COMMUTATIVITY DEGREE OF A FINITE GROUP

R. K. NATH AND A. K. DAS*

Department of Mathematics, North-Eastern Hill University,
Permanent Campus, Shillong-793022, Meghalaya, India.
Email: rknathnehu@gmail.com, akdas@nehu.ac.in

Abstract: Commutativity degree of a finite group is the probability that the commutator of two arbitrarily chosen group elements equals the identity element of the group. The object of this paper is to study the probability that the generalized commutator of an arbitrarily chosen n-tuple of group elements equals a given group element.

Key words: finite groups, group characters, commutativity degree.
2000 Mathematics Subject Classification: 20C15, 20D60, 20P05.

1. Introduction

Throughout this paper G denotes a finite group, g an element of the commutator subgroup G', and $n \geq 2$ a positive integer. Recall that the generalized commutator of an n-tuple $(x_1, x_2, \ldots, x_n) \in G^n$, the n-fold product of G with itself, is given by

$$[x_1, x_2, \ldots, x_n] = x_1 x_2 \ldots x_n x_1^{-1} x_2^{-1} \ldots x_n^{-1} \in G'.$$

In [12], Pournaki et al. have considered the probability $\Pr_g(G)$ that the commutator of an arbitrarily chosen pair of group elements equals g, and extended the work of Rusin [14]. The main object of this paper is to study the ratio

$$\Pr_g^n(G) = \frac{|\{(x_1, x_2, \ldots, x_n) \in G^n \ : \ [x_1, x_2, \ldots, x_n] = g\}|}{|G|^n},$$

and further extend the results obtained by Pournaki et al. At the same time, we obtain some new results as well. It may be mentioned here that some of the works that have been carried out in [3], [5] and [11] are related to the present problem.

*Corresponding author.