ON THE PROBABILITY THAT A GROUP SATISFIES A LAW; A SURVEY

M. FARROKHI D. G.

ABSTRACT. The aim of this paper is to give a survey of old and new results on probabilities on finite groups arising from words.

1. INTRODUCTION

The study of groups depends heavily on studying laws (word equations) on groups. The simplest example of this sort are abelian groups which admit the word equation $[x,y]=1$, where $[x,y]:=x^{-1}y^{-1}xy$. The next important families of groups defined by means of words are nilpotent and solvable groups, that is, a group is nilpotent or solvable if it satisfies the word equation $u_n=1$ or $v_n=1$ for some n, respectively. The words u_n and v_n are defined inductively as $u_2=v_2:=[x_1,x_2]$ $u_n:=[u_{n-1},x_n]$ and $v_n=[v_{n-1},v'_{n-1}]$ for all $n\geq 3$, where v_{n-1} and v'_{n-1} denote the same words with disjoint set of variables. We enjoy to remind two further families of groups arising from word equations, namely Engel groups which admits a word equation of the form $[y,x,\ldots,x]=1$ (x appears $n\geq 1$ times) and Burnside groups which admit a word equation of the form $x^n=1$ for some $n\geq 1$.

Let G be a group and $w=w(x_1,\ldots,x_n)$ be a word. Then w is said to be a *law* for G if $w(G)=1$, where

$$w(G)=\{w(g_1,\ldots,g_n):g_1,\ldots,g_n\in G\}.$$

The theory of groups is well developed in the past decades resulting in many tools and classification theorems which can be applied to describe finite groups. This makes us able to study the word equations $w=1$ in a much more generality, namely determining or estimating the number of solutions to the equation

$$w(g_1,\ldots,g_n)=1$$

with $g_1,\ldots,g_n\in G$. For instance, solving the equations $w_n=1$ with $w_n=x^n$ gives us the number of elements of a given order which is an important enumeration problem in finite groups. The equation $w=1$ arises a probabilistic notion in groups which is usually more easier to work with it, so we give a formal definition of it here.

Definition. Let G be a finite group, $g\in G$ be a fixed element and $w\in F_n$ be a nontrivial word. Then the probability that a randomly chosen n-tuple of elements of G satisfies $w=g$ is defined by

$$P(G,w=g)=\frac{|\{(g_1,\ldots,g_n)\in G^n:w(g_1,\ldots,g_n)=g\}|}{|G|^n}.$$

2000 *Mathematics Subject Classification.* Primary 20P05; Secondary 20F70, 20D99.
Key words and phrases. Probability, word, law.

If $g = 1$ is the identity element of G, then we simply write $P(G, w)$ instead of $P(G, w = 1)$.

The aim of this survey is to present all the well-known results concerning the quantities $P(G, w = g)$. Our illustration of the results lacks that of system of equation, which has been extensively studied in the literature. Also, we left the other important probabilities arising from automorphisms as well as generation of finite groups.

This paper is organized as follows: Section 2 considers special words which have been of more importance in the literature. Section 3 analyzes the behavior of $P(G, w = g)$ when G or w is fixed while the other ranges over a given set. Finally, section 4 deals with words for which the numbers $P(G, w = g)$ are non-zero when G ranges on an infinite class of groups. The famous conjecture of Ore is discussed in this section.

2. Special words

2.1. **The commutator word** $[x, y]$. Commutativity can be though of the most important concept in group theory on which many other concepts are based. Clearly, not all groups are abelian while sharing many properties with abelian groups. This arises the question how a group can be near to abelian groups. This introduces a measure on groups which is among the first probabilities studied till now.

Definition. The *commutativity degree* of a finite group is defined to be $P(G, [x, y])$ and it is denoted usually by $d(G)$.

The degree of commutativity has a nice relationship with the important invariant of groups which was first discovered by Erdös and Turan.

Theorem 2.1 (Erdös and Turan, 1968 [12]). *If G is a finite group, then*

$$d(G) = \frac{k(G)}{|G|},$$

where $k(G)$ denotes the number of conjugacy classes of G.

2.1.1. *Joseph's conjectures.* Most results concerning the degree of commutativity deals with two conjectures due to Joseph, which describes the set of all numbers $d(G)$ when G ranges over all finite groups. To this end, put

$$\mathcal{D} := \{d(G) : G \text{ is a finite group}\}.$$

The conjectures of Joseph are summarized as follow:

Conjecture 2.2 (Joseph, 1977 [38, 39]).

(1) *Every limit point of $\mathcal{D}$ is rational.*
(2) *If l is a limit point of $\mathcal{D}$, then there exists $\epsilon = \epsilon_l > 0$ such that $\mathcal{D} \cap (l - \epsilon, l) = \emptyset$.*
(3) *$\mathcal{D} \cup \{0\}$ is a closed subset of $\mathbb{R}$.*

Before to proceed the study of the set $\mathcal{D}$, we illustrate the results for semigroups, which is much easier than the case of groups. For this, put

$$\mathcal{D}' := \{d(S) : S \text{ is a finite semigroup}\}.$$

The following theorem describe the set $\mathcal{D}'$ completely.

Theorem 2.3 (Givens, 2008 [26]). *The set $\mathfrak{D}'$ is dense in* $[0,1]$.

Indeed, we have the following complete description of $\mathfrak{D}'$.

Theorem 2.4 (Ponomarenko and Selinski, 2012 [81]). *We have* $\mathfrak{D}' = \mathbb{Q} \cap [0,1]$.

Now, we turn back to Joseph's conjectures. The first and simplest result was first obtained by Joseph and Gustafson.

Theorem 2.5 (Joseph, 1969 [38]; Gustafson, 1973 [29]). *If G is a finite (rep. compact) non-abelian group, then*

$$d(G) \leq \frac{5}{8}$$

and the equality holds if and only if $G/Z(G) \cong C_2 \times C_2$.

The first major work toward Joseph's conjectures is made by Rusin and it is continued by many author, which we mention in the following.

Theorem 2.6 (Rusin, 1979 [83]). *The values of $d(G)$ above $\frac{11}{32}$ are precisely*

$$\frac{3}{8}, \frac{25}{64}, \frac{2}{5}, \frac{11}{27}, \frac{7}{16}, \frac{1}{2}, \ldots, \frac{1}{2}\left(1 + \frac{1}{2^{-2n}}\right), \ldots, \frac{1}{2}\left(1 + \frac{1}{2^2}\right), 1$$

Theorem 2.7 (Das and Nath, 2011 [10]). *Let G be a group of odd order. The values of $d(G)$ above $\frac{11}{75}$ are precisely*

$$\frac{11}{75}, \frac{29}{189}, \frac{3}{19}, \frac{7}{39}, \frac{121}{729}, \frac{17}{81}, \frac{55}{343}, \frac{5}{21}, \ldots, \frac{1}{5}\left(1 + \frac{4}{5^{-2n}}\right),$$
$$\ldots, \frac{1}{5}\left(1 + \frac{4}{5^2}\right), \ldots, \frac{1}{3}\left(1 + \frac{2}{3^{-2n}}\right), \ldots, \frac{1}{3}\left(1 + \frac{2}{3^2}\right), 1$$

However, the following result of Hegarty gives the best general result till now.

Theorem 2.8 (Hegarty, 2013 [31]). *If $l \in (\frac{2}{9}, 1]$ is a limit point of $\mathfrak{D}$, then*

(i) *l is rational, and*
(ii) *there exists an $\epsilon = \epsilon_l > 0$ such that $\mathfrak{D} \cap (l - \epsilon_l, l) = \emptyset$.*

2.1.2. *Nilpotency, solvability and supersolvability results.* Further results in the study of commutativity degrees utilizes other notions of group theory, namely nilpotency, supersolvability and solvability. The following two results give a general description of groups in terms of their commutativity degrees.

Theorem 2.9 (Neumann, 1989 [79]). *For any real number r, there exists numbers $n_1 = n_r(r)$ and $n_2 = n_2(r)$ such that if G is any finite group in which*

$$d(G) \geq \frac{1}{r},$$

then there exists normal subgroups H, K of G with $H \leq K$ such that K/H is abelian,

$$[G:K] \leq n_1 \text{ and } |H| \leq n_2.$$

Theorem 2.10 (Lévai and Pyber, 2000 [51]). *Let G be a profinite group with positive commutitivity degree. Then G is abelian-by-finite.*

Now, we state other results which describe the structure of a finite group when its degree of commutativity is sufficiently large.

Theorem 2.11 (Rusin, 1979 [83]; Lescot, 1995 [49]). *Let G be a finite group. Then*

(i) *If $d(G) > \frac{1}{2}$, then G is isoclinic with an extra special 2-group. In particular, G is nilpotent.*

(ii) *If $d(G) = \frac{1}{2}$, then G is isoclinic to S_3.*

Theorem 2.12 (Barry, MacHale and Ní Shé, 2006 [7]). *Let G be a finite group. If $d(G) > \frac{1}{3}$, then G is supersolvable.*

Theorem 2.13 (Barry, MacHale and Ní Shé, 2006 [7]). *Let G be a finite group of odd order. If $d(G) > \frac{11}{75}$, then G is supersolvable.*

Theorem 2.14 (Lescot, Nguyen and Yang, 2014 [50]). *Let G be a finite group. If $d(G) > \frac{5}{16}$, then*

(i) *G is supersolvable,*

(ii) *G is isoclinic to A_4, or*

(iii) *$G/Z(G)$ is isoclinic to A_4.*

Corollary 2.15 (Lescot, Nguyen and Yang, 2014 [50]). *If G is a finite group. Then $d(G) = \frac{1}{3}$ if and only if G is isoclinic to A_4.*

Theorem 2.16 (Lescot, Nguyen and Yang, 2014 [50]). *Let G be a finite group of odd order. If $d(G) > \frac{35}{243}$, then*

(i) *G is supersolvable, or*

(ii) *G is isoclinic to $(C_5 \times C_5) \rtimes C_3$.*

Theorem 2.17 (Lescot, Nguyen and Yang, 2014 [50]). *Let $G = N \rtimes H$ be a finite group such that N is abelian. If $d(G) > 1/s$ $(s \geq 2)$, then G has a nontrivial conjugacy class of size at most $s-1$ in N. In particular, either $Z(G) \neq 1$ or G has a proper subgroup of index at most $s-1$.*

Theorem 2.18 (Heffernan, MacHale and Ní Shé, 2014 [30]). *Let G be a finite group. If $d(G) > \frac{7}{24}$, then G is metabelian.*

Theorem 2.19 (Heffernan, MacHale and Ní Shé, 2014 [30]). *Let G be a finite group of odd order. If $d(G) > \frac{83}{675}$, then G' is nilpotent.*

In 2006, Guralnick and Robinson studied the degree of commutativity in a much more general case and obtained some general bounds for it in terms of nilpotent and solvable radicals as well as derived length. In what follows, $F(G)$ denotes the Fitting subgroup (nilpotent radical) and $\mathrm{sol}(G)$ denotes the solvable radical of a group G.

Theorem 2.20 (Guralnick and Robinson, 2006 [27]). *Let G be a finite group. Then*

$$d(G) \leq d(F(G))^{\frac{1}{2}}[G:F(G)]^{-\frac{1}{2}} \leq [G:F(G)]^{-\frac{1}{2}}.$$

In particular,

$$d(G) \to 0 \text{ as } [G:F(G)] \to \infty.$$

Theorem 2.21 (Guralnick and Robinson, 2006 [27]). *If G is a finite group, then $d(G) \leq [G:\mathrm{sol}(G)]^{-\frac{1}{2}}$ with equality if and only if G is abelian.*

Theorem 2.22 (Guralnick and Robinson, 2006 [27]). *If G is a finite group such that $d(G) > \frac{3}{40}$, then either G is solvable, or $G \cong A_5 \times C_2^n$ $(n \geq 1)$, in which case $d(G) = \frac{1}{12}$.*

Theorem 2.23 (Guralnick and Robinson, 2006 [27]). *Let G be a finite solvable groups of derived length $d \geq 4$. Then*

$$d(G) \leq \frac{4d-7}{2^{d+1}}.$$

Theorem 2.24 (Guralnick and Robinson, 2006 [27]). *Let G be a finite p-group of derived length $d \geq 2$. then*

$$d(G) \leq \frac{p^d + p^{d-1} - 1}{p^{2d-1}}.$$

2.1.3. *Subgroups.* The notion of commutativity can be used simply is terms of subsets of a group and it is usually interpret as permutability. Indeed, two subsets (subgroup) X and Y of a group G are said to be *permutable* if $XY = YX$. This can be much more generalized to include general words.

Definition. A *positive law* in groups is a word equation $w = 1$, which can be restated as an equation of the form $u = v$, where u and v are words in a given free semigroup, that is, $w = uv^{-1}$ or $u^{-1}v$.

Example. The commutator law $[x, y] = 1$ is a positive law as it is equivalent to the equation $xy = yx$.

The above definition suggest us to work on the same probabilities as defined in the introduction with subgroups instead of elements. In this regard, Tărnăuceanu evaluates the quantities $P(L(G), xy = yx)$ when G has a simple structure, namely G is a dihedral group, a semi-dihedral group or a generalized quaternion group. We note that $L(G)$ is the lattice of all subgroups of a group G.

Theorem 2.25 (Tărnăuceanu, 2009 [84]). *Let $G = D_{2n}$ be the dihedral group of order $2n$. Then*

$$P(L(G), xy = yx) = \frac{\tau(n)^2 + 2\tau(n)\sigma(n) + 2^{\Omega(n)}\tau(n)\sigma(n)}{(\tau(n) + \sigma(n))^2},$$

where $\tau(n)$, $\sigma(n)$ and $\Omega(n)$ are the number of divisors, the sum of divisors and the number of prime divisors of the number n.

Corollary 2.26 (Tărnăuceanu, 2009 [84]).

$$P(L(D_{2^n}), xy = yx) = \frac{(n-2)2^{n+2} + n2^{n+1} + (n-1)^2 + 8}{(n-1+2^n)^2} \to 0$$

$$P(L(Q_{2^n}), xy = yx) = \frac{(n-3)2^{n+1} + n2^n + (n-1)^2 + 8}{(n-1+2^{n-1})^2} \to 0$$

$$P(L(SD_{2^n}), xy = yx) = \frac{(n-3)2^{n+1} + n2^n + (3n-2)2^{n-1} + (n-1)^2 + 8}{(n-1+3 \cdot 2^{n-2})^2} \to 0$$

Motivated by Tărnăuceanu's work, in 2013, we have computed the same probability for a much more complicated class of groups, that is, the projective special linear groups.

Theorem 2.27 (Farrokhi, 2013 [14]; Farrokhi and Saeedi, 2013 [20, 19]). *If $G = PSL_2(p^n)$, then*

$$P(L(G), xy = yx) = \frac{1 + \mathcal{N}_1' + \mathcal{N}_2' + \mathcal{N}_3' + \mathcal{N}_4' + \mathcal{N}_5' + \mathcal{N}_6' + \mathcal{N}_7' + \mathcal{N}_8'}{(1 + \mathcal{N}_1 + \mathcal{N}_2 + \mathcal{N}_3 + \mathcal{N}_4 + \mathcal{N}_5 + \mathcal{N}_6 + \mathcal{N}_7 + \mathcal{N}_8)^2},$$

in which

(1) $\mathcal{N}_1 = (p^n + 1)\sum_{m=1}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_p$,

(2) $\mathcal{N}_2 = \frac{p^n(p^n+1)}{2}\left(\tau\left(\frac{p^n-1}{d}\right) - 1\right) + \frac{p^n(p^n-1)}{2}\left(\tau\left(\frac{p^n+1}{d}\right) - 1\right)$,

(3) $\mathcal{N}_3 = \frac{1}{2}|G|\left(\frac{d}{p^n-1}\sigma\left(\frac{p^n-1}{d}\right) + \frac{d}{p^n+1}\sigma\left(\frac{p^n+1}{d}\right) - 2\right)$,

(4) $\mathcal{N}_4 = \frac{1}{12}|G|$ *if* $p > 2$ *and zero otherwise,*

(5) $\mathcal{N}_5 = \frac{1}{12}|G|$ *if* $p^n \equiv -1 \pmod 8$ *and zero otherwise,*

(6) $\mathcal{N}_6 = \frac{1}{30}|G|$ *if* $p^n \equiv \pm 1 \pmod{10}$ *and zero otherwise,*

(7) $\mathcal{N}_7 = p^n(p^n + 1)\left(\sum_{m|n} \alpha_{p,m}\beta_{p^m,\frac{n}{m}} - \beta_{p,n}\right)$, *where*

$$\alpha_{p,m} = |\{h : dh|p^m - 1, dh \nmid p^k - 1, k < m, k|m\}|,$$

is the number of generators of the field $GF(p^m)$ *in* $GF(p^m)^d$ *and*

$$\beta_{p^m,\frac{n}{m}} = \frac{1}{p^n}\sum_{l=1}^{\frac{n}{m}} \binom{\frac{n}{m}}{l}_{p^m} p^{ml} = \frac{1}{|V|}\sum_{0 \neq U \leq V} |U|,$$

in which $V = GF(p^n)/GF(p^m)$ *is a vector space of dimension* n/m *over a field of order* p^m.

(8) $\mathcal{N}_8 = |G|\left(\sum_{m|n} \frac{1}{|PSL(2,p^m)|} + \sum_{2m|n} \frac{1}{|PGL(2,p^m)|}\right)$,

and $\mathcal{N}'_i = \sum_{S \in L_i^*(G)} \mathcal{N}_S F_2(S)$, *in which* $L_i^*(G)$ *is the set of representatives of isomorphism classes of subgroups of* G *of type (i), and*

(1) $F_2(C_p^n) = \sum_{0 \leq i+j \leq n} p^{ij} \begin{bmatrix} n \\ i,j \end{bmatrix}_p$,

(2) $F_2(C_n) = \prod_{p^\alpha \| n}(2\alpha + 1)$,

(3) $F_2(D_{2n}) = \begin{cases} \phi_n + 2\delta_n, & \text{odd } n, \\ \phi_n + 2\phi_{\frac{n}{2}} + 2\delta_n, & \text{even } n, \end{cases}$, *where*

$$\phi_n = \prod_{p^\alpha \| n}\left(2\frac{p^{\alpha+1} - 1}{p-1} - 1\right) \text{ and } \delta_n = \prod_{p^\alpha \| n}\left(\alpha + \frac{p^{\alpha+1} - 1}{p-1}\right),$$

(4) $F_2(A_4) = 27$,

(5) $F_2(S_4) = 177$,

(6) $F_2(A_5) = 237$,

(7) $F_2(C_p^m \rtimes C_k) = \sum_{C_k = XY} \Xi_1(H, (E_{C_k}^{\times 2}); (E_X^{\times 2}), (E_Y^{\times 2}))$, *where*

$$\Xi_n(V, F; E_1, E_2) = \sum_{\substack{V = U_1 + U_2 \\ U_1/E_1 \leq V/E_1 \\ U_2/E_2 \leq V/E_2}} \left(\frac{|V|}{|U_1|} \cdot \frac{|V|}{|U_2|}\right)^n = \sum_{\substack{V = U_1 + U_2 \\ U_1/E_1 \leq V/E_1 \\ U_2/E_2 \leq V/E_2}} \frac{|V|^n}{|U_1 \cap U_2|^n},$$

where V *is a vector space over the field* F *and* E_1, E_2 *are subfields of* F, *and*

(8.1) $F_2(PSL_2(p^n)) =$

$$\begin{cases} 2|L(PSL_2(p^n))| + 2p^n(p^{2n} - 1) - 1, & p = 2, n > 1, \\ 2|L(PSL_2(p^n))| + p^n(p^{2n} - 1) - 1, & p > 2 \text{ and } (p^n - 1)/2 \text{ is odd,} \\ & p^n \neq 3, 7, 11, 19, 23, 59, \\ 2|L(PSL_2(p^n))| - 1, & p > 2 \text{ and } (p^n - 1)/2 \text{ is even,} \\ & p^n \neq 5, 9, 29 \end{cases}$$

and

$$F_2(G) = 17, 27, 237, 1141, 2033, 4935, 17223, 48261, 68799, 780695$$

if

$$p^n = 2, 3, 5, 7, 9, 11, 19, 23, 29, 59,$$

respectively, and
(8.2) $F_2(PGL_2(p^n)) =$

$$\begin{cases} 3p^n(p^{2n}-1) + 4|L(PGL_2(p^n))| - 2|L(PSL_2(p^n))| - 3, & n \textit{ even or } p \equiv 1 \pmod 4, \\ 4p^n(p^{2n}-1) + 4|L(PGL_2(p^n))| - 2|L(PSL_2(p^n))| - 3, & n \textit{ odd and } p \equiv 3 \pmod 4) \end{cases}$$

if $p^n > 29$ *and* $F_2(G)$ *equals*

$$177, 1103, 3083, 4919, 15549, 14529, 31093, 58429, 111567, 99527, 144297, 192349$$

if p^n *equals*

$$3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29,$$

respectively.

Recall that $\begin{bmatrix} n \\ m \end{bmatrix}_p$ and $\begin{bmatrix} n \\ i,j \end{bmatrix}_p$ are the Gaussian binomial and trinomial coefficients defined as

$$\begin{bmatrix} n \\ m \end{bmatrix}_p = \frac{(p^n-1)\cdots(p-1)}{(p^m-1)\cdots(p-1)(p^{n-m}-1)\cdots(p-1)}$$

and

$$\begin{bmatrix} n \\ i,j \end{bmatrix}_p = \frac{(p^n-1)\cdots(p-1)}{(p^i-1)\cdots(p-1)(p^j-1)\cdots(p-1)(p^{n-i-j}-1)\cdots(p-1)}.$$

An asymptotic version of our result above studied later by Aivazidis who showed that the corresponding probabilities tends to zero as long as the order of groups tends to infinity.

Theorem 2.28 (Aivazidis, 2013 [3]). *We have*

$$\lim_{n\to\infty} P(L(PSL_2(2^n)), xy = yx) = 0.$$

Theorem 2.29 (Aivazidis, 2014 [2]). *We have*

$$\lim_{n\to\infty} P(L(Sz(2^{2n+1})), xy = yx) = 0.$$

The above results suggest us the following two conjectures.

Conjecture 2.30. *Let G denotes a non-abelian finite simple group. Then*

$$\lim_{|G|\to\infty} P(L(G), xy = yx) = 0.$$

Conjecture 2.31. *Let G be a finite group. If*

$$P(L(G), xy = yx) > P(L(A(5)), xy = yx) = \frac{861}{3481},$$

then G is solvable.

2.2. **The Engel words** $[x,_n y]$. The next special words to be considered are Engel words. These words are more difficult to be studied, so there is only few results in this case that we mention here.

Theorem 2.32 (Erfanian and Farrokhi, 2013 [13]). *Let G be a finite 3-metabelian group which is not a 2-Engel group. If $p=\min\pi(G)$, then*

$$P(G,[x,y,y])\leq\frac{1}{p}+\left(1-\frac{1}{p}\right)\frac{|L_2(G)|}{|G|}$$

and if $L_2(G)\leq G$, then

$$P(G,[x,y,y])\leq\frac{2p-1}{p^2}.$$

Moreover, both of the upper bounds are sharp at any prime p.

Conjecture 2.33. *If G is a finite non-2-Engel group, then $P(G,[x,y,y])\leq\frac{13}{16}$.*

Theorem 2.34 (Erfanian and Farrokhi, 2013 [13]). *Let G be a finite 3-metabelian group which is not a 2-Engel group. If $p=\min\pi(G)$, then*

$$P(G,[x,y,y])\geq d(G)-(p-1)\frac{|Z(G)|}{|G|}+(p-1)\frac{k_G(L(G))}{|G|}$$

and if either G is a p-group or G' has a unique involution, then

$$P(G,[x,y,y])\geq pd(G)-(p-1)\frac{|Z(G)|}{|G|}.$$

Moreover, both of the lower bounds are sharp at any prime p.

We enjoy to mention the following Lie algebra analogue of Mann and Martinez.

Theorem 2.35 (Mann and Martinez, 1998 [73]). *Let L be a finite Lie algebra of characteristic p, which is not n-Engel. Then*

$$P(L,[x,_n y])\leq 1-\frac{1}{2^{n+1}}.$$

2.3. **The power word** x^n. The next important words after commutator words which have attracted many attentions are the power words.

Definition. Let G be a finite group and $w_n=x^n$. Then the probability that an element of G satisfies the word equation $w_n=1$ is denoted by $p_n(G)$.

Power words are first considered by Frobenius while counting the number of elements of a given order in finite groups.

Theorem 2.36 (Frobenius, 1895 [24]). *Let G be a finite group whose order is divisible by a number n. Then the number of solutions to the equation $x^n=1$ is a multiple of n.*

Corollary 2.37. *If G is a finite group whose order is divisible by a number n, then*

$$p_n(G)\geq\frac{n}{|G|}.$$

Frobenius, in his paper, poses the following interesting long-standing conjecture, whose proof is eventually completed by Iiyoria and Yamaki in 1991.

Conjecture 2.38 (Frobenius, 1895 [24]). *Let G be a finite group whose order is divisible by a number n. If the set $L_n(G)$ of solutions to the equation $x^n=1$ has n elements, then $L_n(G)$ is a subgroup of G.*

Theorem 2.39 (Iiyoria and Yamaki, 1991 [35]). *The conjecture of Frobenius is always true.*

The first systematic study of power words is initiated by Miller who obtained lower and upper bounds for the number solutions to a power word equation. Theorems 2.40–2.49 state all results concerning the mentioned lower and upper bounds including the results of Miller and others.

Theorem 2.40 (Miller, 1907 [78]). *Let G be a non-abelian finite group. Then $p_2(G) \leq \frac{3}{4}$. Moreover, if $p_2(G) > \frac{1}{2}$, then $p_2(G)$ is equal to one of the following numbers.*

$$\ldots, \frac{2^n+1}{2^{n+1}}, \ldots, \frac{17}{32}, \frac{9}{16}, \frac{5}{8}, \frac{3}{4}$$

Theorem 2.41 (Miller, 1907 [77]). *Let G be a non-abelian finite group of order $2^k m$ (m odd). Then $p_2(G) \leq \frac{1}{2} + \frac{1}{2m}$ with equality if and only if $G = H \times C_2^n$ $(n \geq 0)$, where H is a generalized dihedral group with an odd order abelian subgroup of index two.*

Theorem 2.42 (Miller, 1919 [76]). *Let G be a non-abelian finite group of even order which is not a 2-group. If $p_2(G) > \frac{1}{2}$, then G is a generalized dihedral group.*

Theorem 2.43 (Wall, 1970 [85]; Liebeck and MacHale, 1972 [59]). *Let G be a non-abelian finite group such that $p_2(G) > \frac{1}{2}$. Then either $G = H \times E$, where E is an elementary abelian 2-group and H is one of the following groups:*

(1) *a generalized dihedral group,*
(2) *direct product of two copies of dihedral groups of order 8,*
(3) *a central product of dihedral groups of order 8, or*
(4) *a group of with the following presentation*

$$\begin{aligned}\langle x_1, y_1, \ldots, x_n, y_n, z : x_i^2 = y_i^2 = z^2 = [x_i, x_j] = [y_i, y_j] \\ = [x_i, y_j] = [y_i, z] = 1, [x_i, z] = y_i, i, j = 1, \ldots, n\rangle.\end{aligned}$$

Theorem 2.44 (Potter, 1988 [82]). *Let G be a non-solvable group with $p_2(G) > \frac{1}{4}$. Then G is isomorphic to the product of A_5 with an elementary abelian 2-group. In this case, $p_2(G) = \frac{4}{15}$.*

Theorem 2.45 (Hegarty, 2005 [32]). *Let G be a finite solvable group of derived length $n \geq 3$*

$$p_2(G) \leq \frac{1}{2}\left(\frac{3}{4}\right)^{n-3}.$$

Moreover, if $n = 5$ then

$$p_2(G) \leq \frac{4}{15}.$$

Theorem 2.46 (Mann, 1994 [72]). *Let G be a finite group. If $p_2(G) \geq r + \frac{1}{|G|}$, then G contains a normal subgroup H such that both $[G : H]$ and H' are bounded by some function of r.*

Theorem 2.47 (Laffey, 1976 [41]). *Let G be a finite group, p be a prime divisor of $|G|$ and assume that is not a p-group. Then*

$$p_p(G) \leq \frac{p}{p+1}.$$

Theorem 2.48 (Laffey, 1976 [42]). *Let $G$ be a finite 3-group. Then*

$$p_3(G) \leq \frac{7}{9}.$$

Theorem 2.49 (Laffey, 1979 [43]). *Let $G$ be a finite group which is not a 2-group. Then*

$$p_4(G) \leq \frac{8}{9}.$$

The above bounds are, in a sense, valid in a more generality according to a result of Mann and Martinez in 1996.

Theorem 2.50 (Mann and Martinez, 1996 [74]). *Let $G$ be an $m$-generated finite group of exponent not dividing $n$. Then*

$$P_n(G) < \frac{R(m,n^2)}{R(m,n^2)+1},$$

where $R(m,n)$ is the order of largest $m$-generated finite group of exponent $n$.

Theorem 2.51 (Mann and Martinez, 1996 [74]). *Let $G$ be an $m$-generated finite $p$-group of exponent $> p^n$. Then*

$$P_{p^n}(G) \leq \frac{pR(m,p^n)-1}{pR(m,p^n)}.$$

Theorem 2.52 (Mann and Martinez, 1998 [73]). *Let $G$ be a finite $p$-group such that*

$$p_p(G) > \frac{3^p-2}{3^p-1}.$$

Then $L(G)$ is an $(p-1)$-Engel Lie algebra.

The following two results give a precise evaluation of the number of solutions to a power word equation in a powerful $p$-group.

Definition. A finite $p$-group $G$ is called *powerful* if $G' \subseteq G^p$ when $p$ is odd and $G' \subseteq G^4$ when $p = 2$.

Theorem 2.53 (Héthelyi and Lévai, 2003 [34]). *Let $G$ be a powerful $p$-group. Then*

$$P_p(G) = \frac{1}{|G^p|}.$$

Theorem 2.54 (Mazur, 2007 [75]; Fernández-Alcober, 2007 [22]). *Let $G$ be a powerful $p$-group and $k \geq 1$. Then*

$$P_{p^k}(G) = \frac{1}{|G^{p^k}|}.$$

2.4. **Sets of words.** We conclude this section with considering the join of words arising from a combinatorial problem in groups.

Definition. A group $G$ is said to satisfy the deficient kth power property on $m$-subsets if $|X^k| < |X|^k$ for any $m$-subset $X$ of $G$. The set of all finite groups with the deficient square property on $m$-subsets is denoted by $DS(m)$.

Notation.

- Let $W(m,n)$ be the set of all nontrivial words $x_{i_1}\cdots x_{i_n}x_{j_n}^{-1}\cdots x_{j_1}^{-1}$, where $i_1,\ldots,i_n,j_1,\ldots,j_n = 1,\ldots,m$.

- The probability that a randomly chosen m-tuple of G satisfies at least one of the words in $W \subseteq F_m \setminus \{1\}$ is denoted by $\tilde{P}(G, W)$.

Freiman, while studying latin squares arising from multiplication table of groups, obtained the following classification of groups with the deficient 2-power property on 2-subsets of a group.

Theorem 2.55 (Freiman, 1981 [22]). *Let G be a finite group. Then*

$$\tilde{P}(G, W(2,2)) = 1,$$

if and only if either G is abelian or $G \cong Q_8 \times C_2^n \times O$ for some $n \geq 0$ and abelian odd order group O.

For groups not in $DS(2)$ we have the following upper bound.

Theorem 2.56 (Farrokhi and Jafari, 2014 [16]). *Let G be a finite group which does not belong to $DS(2)$. Then*

$$\tilde{P}(G, W(2,2)) \leq \frac{27}{32}$$

and the equality holds if and only if $G \cong D_8 \times C_2^n \times O$ for some $n \geq 0$ and abelian odd order group O.

Further results about the quantities $\tilde{P}(G, W(m,n))$ for $m > 2$ or $n > 2$ can be found in [8, 33, 55, 56, 57, 58, 61] and we omit the details.

Joining words arises while studying many other problems. Here, we mention one of the appearances of join of words in our works.

Definition. Let G be a finite group and H be a subgroup of G. Then the *degree of normality* of H in G in defined to be

$$P_N(G, H) := \frac{|\{(g,h) \in G \times H : h^g \in H\}|}{|G||H|}.$$

Indeed, $P_N(G, H) = \tilde{P}((G, H), W(G, H))$, where

$$W(G, H) = \{[x_1, x_2] = h : h \in H\}.$$

Let $\mathcal{P}_N$ denote the set of normality degrees of subgroups of finite groups. Also, let $\mathcal{P}_N^* = \mathcal{P}_N \setminus \{1\}$.

Utilizing the above notations we have the following results.

Theorem 2.57 (Farrokhi, Jafari and Saeedi, 2011 [17]). *If G is a finite simple group, then $\max \mathcal{P}_N^*(G) \leq \frac{8}{15}$. Moreover the bound is sharp.*

Theorem 2.58 (Farrokhi and Saeedi, 2012 [20]). *If G is a finite group such that $\mathcal{P}_N^*(G) \subseteq (0, \frac{1}{2}]$ or $(\frac{3}{10}, 1)$, then G is a solvable group. Moreover both of the intervals are sharp.*

Theorem 2.59 (Farrokhi and Saeedi, 2012 [20]).

$$\mathcal{P}_N \cap \left(\frac{1}{2}, 1\right] = \left\{\ldots, \frac{1}{2} + \frac{1}{2n}, \ldots, \frac{1}{2} + \frac{1}{4}, 1\right\} = \left\{\frac{1}{2} + \frac{1}{2n}\right\}_{n=1}^{\infty}.$$

Our computations along with the above results suggest us the following two conjectures.

Conjecture 2.60 (Farrokhi and Saeedi, 2012 [20]). *The values of $\mathcal{P}_N$ in the interval $(\frac{1}{3}, \frac{1}{2}]$ fall into the following seven sequences*

$$\left\{\frac{2i+1}{5i+4}\right\}, \left\{\frac{2i+1}{5i+3}\right\}, \left\{\frac{2i+1}{5i+2}\right\}, \left\{\frac{2i+1}{5i+1}\right\}, \left\{\frac{2i+1}{4i+8}\right\}, \left\{\frac{2i+1}{4i+4}\right\}, \left\{\frac{i}{3i-6}\right\}.$$

Conjecture 2.61 (Farrokhi and Saeedi, 2012 [20]). *For each natural number n, the set $\mathcal{P}_N \cap (\frac{1}{n+1}, \frac{1}{n}]$ is the union of some finitely many sequences of the form*

$$\left\{\frac{ai+b}{ci+d}\right\}_{i=1}^{\infty}.$$

3. General words

The aim of this section is to review the results concerning the number of solutions to a word equation $w = 1$ when w is an arbitrary word or G is an arbitrary group. The following fundamental result of Solomon along with Frobeniu's result mentioned before provide a divisibility criterion for the number of solutions to a word equation $w = 1$ for any arbitrary word w.

Theorem 3.1 (Solomon, 1969 [71]). *Let G be a finite group and w be a word on two or more letters. Then the number of solutions to the equation $w = 1$ is a multiple of $|G|$.*

Corollary 3.2. *If G is a finite group and $w = w(x_1, \ldots, x_n)$ is a word on $n > 1$ letters, then*

$$P(G, w) \geq \frac{1}{|G|^{n-1}}.$$

3.1. **A fixed group: Amit's conjectures.** Similar to Joseph's conjecture in the study of commutativity degrees, the following theorem of Amit and conjectures succeeding it play important roles in the study of $P(G, w)$ for a general word w. Amit's studies these quantities by fixing a finite group G and letting w varies over all possible words.

Theorem 3.3 (Amit [4]). *If G is a finite nilpotent group, then there exists a constant $c > 0$ such that*

$$\inf\{P(G, w) : w \in F_\infty\} \geq c.$$

Conjecture 3.4 (Amit [4]). *If G is a finite solvable group, then there exists a constant $c > 0$ such that*

$$\inf\{P(G, w) : w \in F_\infty\} \geq c.$$

Conjecture 3.5 (Amit [4]). *If G is a finite nilpotent group, then*

$$\inf\{P(G, w) : w \in F_\infty\} \geq \frac{1}{|G|}.$$

Question (Amit [4]). Let G is a finite non-solvable group, then

$$\inf\{P(G, w) : w \in F_\infty\} = 0.$$

Amit's conjectures are answered affirmatively in many cases as we mention below.

Theorem 3.6 (Levy, 2011 [53]). *Let G be a finite group of nilpotency class 2. Then the set*

$$\inf\{P(G,w) : w \in F_\infty\} \geq \frac{1}{|G|}.$$

Theorem 3.7 (Levy, 2011 [53]). *Let $G = A \rtimes H$ be a finite group where A is abelian. If*

$$P(H,w) \geq \frac{1}{|H|}$$

for a word w, then

$$P(G,w) \geq \frac{1}{|G|}.$$

Theorem 3.8 (Nikolov and Segal, 2007 [80]). *Let G be a finite group. Then G is nilpotent if and only if*

$$\inf\{P(G,w=g) : w \in F_\infty, g \in G\} \setminus \{0\} > 0.$$

Theorem 3.9 (Abért, 2006 [1]). *Let G be a finite group. Then for all n there exists a word $w \in F_n$ such that for all $g_1,\ldots,g_n \in G$, the tuple $(g_1,\ldots,g_n)$ satisfies w if and only if the subgroup $\langle g_1,\ldots,g_n\rangle$ of G is solvable.*

Theorem 3.10 (Nikolov and Segal, 2007 [80]). *Let G be a finite group. Then G is solvable if and only if*

$$\inf\{P(G,w) : w \in F_\infty\} > 0.$$

Theorem 3.11 (Abért, 2006 [1]). *Let G be a finite just non-solvable group. Then the set*

$$\{P(G,w) : w \in F_\infty\}$$

is dense in $[0,1]$.

3.2. **A fixed word.** Now, it's time to fix a word w and let G varies over all finite groups. This problem is more studied over non-abelian finite simple groups and the first result is due to Jones who showed that the class of non-abelian finite simple ring is not verbal in the sense that there is no nontrivial word w such that $w(G) = 1$ for all finite simple groups G.

Theorem 3.12 (Jones, 1974 [37]). *Let $w \neq 1$ be a word. Then $P(G,w) < 1$ for all but finitely many non-abelian finite simple groups G.*

Jone's result is generalized and strengthened by Shalev and his colleagues recently.

Theorem 3.13 (Dixon, Pyber, Seress and Shalev, 2003 [11]). *Let $w \in F_2$ be a word. Then*

$$\lim_{|G|\to\infty} P(G,w) = 0,$$

where G ranges over non-abelian finite simple groups.

Theorem 3.14 (Larsen and Shalev, 2012 [45]). *For every word $w \neq 1$ there exists $\epsilon = \epsilon(w) > 0$ such that*

$$P(G,w) \leq |G|^{-\epsilon}$$

for all non-abelian finite simple groups G of order at least $N = N(\epsilon) > 0$.

Theorem 3.15 (Larsen and Shalev, 2012 [45]). *For every $1 \neq w \in F_n$, there exists a number $\epsilon = \epsilon(w) > 0$ and a constant c such that*

$$P(G, w = g) \leq c|G|^{-\epsilon}$$

for all non-abelian finite simple groups G and elements $g \in G$.

4. Word maps

This last section is devoted to the non-homogeneous word equations which was inspired originally by the Ore's conjecture on the non-homogeneous commutator equation. All results in this section deals with non-abelian finite simple groups as the problem is almost trivial or uninteresting in case of solvable groups and also general groups.

Definition. Let $w \in F_n$ be a word on $x_1, \ldots, x_n$. For any group G, the word w determines a map

$$\begin{array}{rcl} w : G^n & \longrightarrow & G \\ (g_1, \ldots, g_n) & \longmapsto & w(g_1, \ldots, g_n) \end{array}$$

and it is called a *word map.*

We note that if w is a word and G is a finite group, then the word map defined by w is surjective if and only if $P(G, w = g) > 0$ for all $g \in G$.

The main question in this section is: *when a non-homogeneous word equation has a nontrivial solution?* This is equivalent to say that when the word maps defined above are surjective or non-surjective. We first give examples of non-surjective words on some classes of groups and then consider the more interesting problem that under which conditions a word map is surjective.

4.1. Non-surjective maps.

The following results show that not all nontrivial words are surjective over non-abelian finite simple groups even if the order of groups are sufficiently large.

Theorem 4.1 (Levy, 2012 [54]). *Let n be a number and let C denote any equivalence class in A_n with support size at most* 10. *Then there exists a word $w = w_C$ such that $(A_n)_w = \{1\} \cup C$.*

Theorem 4.2 (Levy, 2012 [54]). *For every $n \geq 2$ and $q = 2^{2^n}$, there exists a word w in F_2 such that $SL_2(q)_w$ consists of the identity and a single equivalence class of elements of order* 17.

Theorem 4.3 (Kassabov and Nikolov, 2013 [40]). *For every $n \geq 7$, $n \neq 13$, there is a word $w = w(x_1, x_2) \in F_2$ such that $(A_n)_w$ consists of the identity and all 3-cycles. When $n = 13$, there is a word $w = w(x_1, x_2, x_3) \in F_3$ with the same property.*

Theorem 4.4 (Kassabov and Nikolov, 2013 [40]). *For every n and $q \geq 2$ with the possible exception of $SL_4(2)$, there is a word $w = w(x_1, x_2) \in F_2$ such that $SL_n(q)_w$ consists of the identity and the conjugacy class of all transvections. For $SL_4(2)$, the word $w = x_1^{210}$ takes values the identity, the transvections and the double transvections with Jordan normal form $J_2(1) \cdot J_2(1)$.*

Theorem 4.5 (Jambor, Liebeck and O'Brien, 2013 [36]). *Let $k \geq 2$ be an integer such that $2k+1$ is a prime and let $w = x_1^2[x_1^{-2}, x_2^{-1}]^k$. If $p \neq 2k+1$ be a prime of inertia degree $m > 1$ in $\mathbb{Q}(\zeta + \zeta^{-1})$, where ζ is a primitive $(2k+1)$th root of unity, and $(2/p) = 1$, then the word map associated to w is non-surjective on $PSL_2(q)$ for all $q = p^n$ where n is a positive integer not divisible by 2 or by m.*

Corollary 4.6. *The above theorem satisfies if $p \neq 2k+1$ is a prime such that $p^2 \not\equiv 1 \pmod{16}$, $p^2 \not\equiv 1 \pmod{2k+1}$ and m is the smallest positive integer with $p^{2m} \equiv 1 \pmod{2k+1}$.*

The above partial results are generalized by Lubotzky to include any non-abelian finite simple group, which is further extended to any non-abelian almost finite simple group by Levy.

Theorem 4.7 (Lubotzky, 2014 [62]). *Let G be a non-abelian finite simple group and X be an $\mathrm{Aut}(G)$-invariant subset of G containing the identity. Then there exists a word $w \in F_2$ such that $w(G) = X$.*

Corollary 4.8 (Lubotzky, 2014 [62]). *For every non-abelian finite simple group G, there exists a word $w = w(x,y) \in F_2$ such that $w(a,b) \neq 1$ if and only if $G = \langle a,b \rangle$ for all elements $a, b \in G$.*

Theorem 4.9 (Levy, 2014 [52]). *Let G be a non-abelian almost simple group with simple socle S and suppose that $G \trianglelefteq \mathrm{Aut}(S)$. Let X be an $\mathrm{Aut}(G)$-invariant subset of S containing the identity. Then there exists a word $w \in F_2$ such that $w(G) = X$.*

4.2. **Special words.** Before to deal with a general word, we discuss several special words which arises historically.

4.2.1. *Commutator maps: The Ore conjecture.* The most important word to be considered first and is of special interest in the literature arises from Ore's works.

Conjecture 4.10 (Ore, 1951 [66]). *The commutator map is surjective over all non-abelian finite simple groups.*

Ore's conjecture is prove affirmatively from a probabilistic point view by Shalev.

Theorem 4.11 (Shalev, 2009 [70]). *Let $w = [x,y]$ be the commutator word. Then*

$$\lim_{|G|\to\infty} \frac{|w(G)|}{|G|} = 1,$$

where G ranges over non-abelian finite simple groups.

Now, we turn back to the main Ore's conjecture. Here is the list of achievements on Ore's conjecture, which finally resulted in the complete proof of it.

- Alternating groups (Ore, 1951),
- $PSL_n(q)$ (Thompson, 1961-1962),
- Sporadic simple groups (Neubüser, Pahlings and Cleuvers, 1984),
- $PSp_{2n}(q)$ with $q \equiv 1 \pmod 4$ (Gow, 1988),
- Exceptional groups of Lie type of rank at most 4 (Bonten, 1993),
- Groups of Lie type over a finite field of order ≥ 8 (Ellers and Gordeev, 1998),
- Semisimple elements of finite simple groups of Lie type (Gow, 2000),
- Groups of Lie type over a finite field of order $q < 8$ (Liebeck, O'Brien, Shalev and Tiep, 2010).

The main and last progress on the proof of Ore's conjecture is based on the following well-known character theoretical formula of Frobenius.

Theorem 4.12 (Frobenius, 1896 [23]). *Let G be a finite group and $g \in G$. The number of solutions to the equation $[x, y] = g$ equals*

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

Liebeck, O'Brien, Shalev and Tiep use the following identity

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} = 1 + \sum_{1 \neq \chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)}$$

and show that the last term on right is sufficiently smaller that 1 for the remained groups which results in the proof of Ore's conjecture. Shalev uses the same arguments to strengthen the result of Ore's conjecture from a probabilistic point of view as follows:

Definition. Let G be a finite group and s be a complex number. Then

$$\zeta^G(s) = \sum_{\chi \in \mathrm{Irr}(R)} \chi(1)^{-s}$$

is the *Witten's zeta function* of G.

Lemma 4.13 (Shalev, 2008 [69]). *If G is a finite non-abelian simple group, then*

$$\lim_{|G| \to \infty} \zeta^G(2) \to 1.$$

Theorem 4.14 (Garion and Shalev, 2009 [25]). *Let G be a finite group and $\theta = \theta_G$ be the commutator map. Then*

$$\left| \frac{|\theta^{-1}(Y)|}{|G|^2} - \frac{|Y|}{|G|} \right| \leq 3\epsilon(G)$$

for every subset Y of G, and

$$\frac{|\theta(X)|}{|G|} \geq \frac{|X|}{|G|^2} - 3\epsilon(G)$$

for every subset X of $G \times G$, where $\epsilon(G) = (\zeta^G(2) - 1)^{\frac{1}{4}}$.

4.2.2. *Engels maps and beyond.* The next words which have attracted attention of some authors are the Engel words. This arises from the works of Shalev who made the following two conjectures.

Conjecture 4.15 (Shalev, 2007 [68]). *The n-th Engel word ($n \geq 1$) map is surjective for any finite simple non-abelian group G.*

Conjecture 4.16 (Shalev, 2007 [68]). *Let $w \neq 1$ be a word which is not a proper power of another word. Then there exists a number $C(w)$ such that if G is either A_r or a finite simple group of Lie type of rank r, where $r > C(w)$, then $w(G) = G$.*

The above conjectures are studied by Bandman, Garion and Grunewald who obtained the following partial answers.

Theorem 4.17 (Bandman, Garion and Grunewald, 2012 [5]). *The n-th Engel word ($n \geq 1$) map is almost surjective for the group $SL_2(q)$ provided that $q \geq q_0(n)$ is sufficiently large.*

Corollary 4.18. *The n-th Engel word ($n \leq 4$) map is surjective for all groups $PSL_2(q)$.*

4.2.3. *Power maps.* The last words we mention here are the power maps. In this regard, the squaring words are of special interest. Utilizing the following computational results of Lucido and Pournaki, in 2005 Das shows that the set $w(G)$ has any possible magnitude of order in comparison with the order of G.

Theorem 4.19 (Lucido and Pournaki, 2005 [63]). *If* $w = x^2$, *then*

(i) *If* $G = PSL_2(q)$ $(q = p^f)$, *then*

$$\frac{|w(G)|}{|G|} = \begin{cases} \frac{3}{4}, & q \text{ is odd,} \\ \frac{q-1}{q}, & q \text{ is even.} \end{cases}$$

(ii) *If* $G = Sz(q)$ $(q = 2^{2f+1})$, *then*

$$\frac{|w(G)|}{|G|} = \frac{q-1}{q}.$$

(iii) *If* $G = R(q)$ $(q = 3^{2f+1})$, *then*

$$\frac{|w(G)|}{|G|} = \frac{5}{8}.$$

(iv) *If* $G \doteq PSU_3(q^2)$ $(q = p^f$ *and* $d = \gcd(3, q+1))$, *then*

$$\frac{|w(G)|}{|G|} = \begin{cases} \frac{5q^2+3q-4}{8q(q+1)}, & q \text{ is odd,} \\ \frac{q^2-q-d}{q^2(q+1)}, & q \text{ is even.} \end{cases}$$

Theorem 4.20 (Das, 2005 [9]). *Let* $w = x^2$. *Then the values of* $|w(G)|/|G|$ *are dense in the unit interval* $[0, 1]$ *as* G *ranges over all finite groups.*

Das, in his paper, poses the following conjecture which we have answered it partially.

Question (Das, 2005 [9]). Let $w = x^2$ and $\mathcal{S} = \{|w(G)|/|G| : G \text{ is a finite group}\}$. Is it true that $\mathcal{S} = \mathbb{Q} \cap [0, 1]$?

Proposition 4.21 (Farrokhi, 2008 [15]). *Let* $w = x^2$. *Then for every rational number* $r \in [0, 1]$, *there exists a number* n *and a finite group* G *such that*

$$\frac{|w(G)|}{|G|} = \frac{1}{2^n} \cdot r.$$

Despite the above facts, the size of $w(G)$, for a power word w, can be under control when G is a fixed group. This is the content of the following result which was already known in a much more generality by Bannai, Deza, Frankl, Kim and Kiyota.

Theorem 4.22 (Lucido and Pournaki, 2008 [64]). *Let* G *be a finite group of even order and* $w = x^2$. *Then*

$$\frac{|w(G)|}{|G|} \leq 1 - \frac{\lfloor\sqrt{|G|}\rfloor}{|G|}.$$

Theorem 4.23 (Bannai, Deza, Frankl, Kim and Kiyota, 1989 [6]). *Let* G *be a finite group and* $w = x^n$, *when* n *is a divisor of* $|G|$. *Then*

$$\frac{|w(G)|}{|G|} \leq 1 - \frac{\lfloor\sqrt{|G|}\rfloor}{|G|}.$$

4.2.4. *Power maps: Lagrange's four square theorem for groups.* Motivated by Lagrange's four square theorem in number theory concerning sum of powers, Liebeck, O'Brien, Shalev and Tiep in 2012 present the following interesting stronger results for groups instead of numbers, which was already proved in a weaker version by Martinez, Zelmanov, Saxl and Wilson.

Theorem 4.24 (Martinez and Zelmanov, 1996 [65]; Saxl and Wilson, 1997 [67]). *For every d, there is an integer $n = n(d)$ such that for every finite simple group G not of exponent dividing d we have*

$$G = \{g_1^d \cdots g_n^d : g_1, \ldots, g_n \in G\}.$$

Theorem 4.25 (Liebeck, O'Brien, Shalev and Tiep, 2012 [60]). *Every element of every non-abelian finite simple group G is a product of two squares.*

Theorem 4.26 (Liebeck, O'Brien, Shalev and Tiep, 2012 [60]). *Every element of every finite non-abelian simple group G is a product of two p-th powers provided that $p > 7$ is a prime.*

4.3. **General words.** We conclude this section with considering a general non-homogeneous word equation. Larsen in 2004 obtains the first estimation on the number of solutions to a non-homogeneous word equation over non-abelian finite simple groups.

Theorem 4.27 (Larsen, 2004 [44]). *For every nontrivial word w and $\epsilon > 0$ there exists a number $C(w, \epsilon)$ such that if G is a finite simple group with $|G| > C(w, \epsilon)$, then $|w(G)| \geq |G|^{1-\epsilon}$.*

Motivated by Larsen's achievements, one can ask whether a word is surjective over a sufficiently large non-abelian finite simple group. This problem is almost solved by Shalev and his colleagues as we follows:

Theorem 4.28 (Shalev, 2009 [70]). *Let $w \neq 1$ be a group word. Then there exists a positive integer $N = N(w)$ such that for every finite simple group G with $|G| \geq N(w)$ we have $w(G)^3 = G$.*

Theorem 4.29 (Larsen and Shalev, 2009 [46]). *For each pair of nontrivial words w_1, w_2, there exists a number $N = N(w_1, w_2)$ such that for all integers $n \geq N$ we have $w_1(A_n)w_2(A_n) = A_n$.*

Theorem 4.30 (Larsen and Shalev, 2009 [46]). *Given an integer d and two nontrivial words w_1 and w_2, there exists a number $N = N(d, w_1, w_2)$ such that if Γ is a simply connected almost simple algebraic group of dimension d over a finite field F, $G = \Gamma(F)/Z(\Gamma(F))$ is the finite simple group associated to Γ over F, and $|G| \geq 5N$, then we have $w_1(G)w_2(G) = G$.*

Theorem 4.31 (Larsen and Shalev, 2009 [46]). *For each triple of nontrivial words w_1, w_2, w_3, there exists a number $N = N(w_1, w_2, w_3)$ such that if G is a finite simple group of order at least N, then $w_1(G)w_2(G)w_3(G) = G$.*

Conjecture 4.32 (Larsen and Shalev, 2009 [46]). *For each pair of nontrivial words w_1, w_2, there exists a number $N = N(w_1, w_2)$ such that if G is a finite simple group of order at least N, then $w_1(G)w_2(G) = G$.*

Theorem 4.33 (Larsen, Shalev and Tiep, 2013 [48]). *If w_1, w_2 and w_3 are nontrivial words, then for all finite quasisimple groups G of sufficiently large order, $w_1(G)w_2(G)w_3(G) = G$.*

Theorem 4.34 (Larsen, Shalev and Tiep, 2011 [47]). *Let $w_1, w_2 \in F_d$ be nontrivial words. Then there exists a constant $N = N(w_1, w_2)$ such that for all non-abelian finite simple groups G of order greater than N, we have $w_1(G)w_2(G) = G$.*

Corollary 4.35 (Larsen, Shalev and Tiep, 2011 [47]). *For every positive integer k there exists a constant $N = N_k$ such that for all non-abelian finite simple groups G of order greater than N, every element in G can be written as $x^k y^k$ for some $x, y \in G$.*

As before, the above results on non-abelian finite simple groups can be stated in a larger class of groups, namely, the class of finite quasisimple groups.

Theorem 4.36 (Guralnick and Tiep, 2013 [28]). *Let w_1 and w_2 be two nontrivial words. Then there exists a constant $N = N(w_1, w_2)$ depending on w_1 and w_2 such that for all finite quasisimple groups G of order greater than N we have $w_1(G)w_2(G) \supseteq G \setminus Z(G)$.*

Theorem 4.37 (Guralnick and Tiep, 2013 [28]). *Let $s, t \geq 1$ be any two integers and let $m := \max(s, t)$. If G is any finite simple group of order at least m^{8m^2}, then every element in G can be written as $x^s y^t$ for some $x, y \in G$.*

References

[1] M. Abért, On the probability of satisfying a word in a group, *J. Group Theory* **9** (2006), 685–694.

[2] S. Aivazidis, On the subgroup permutability degree of the simple Suzuki groups, *Monatsh. Math.* **176** (2015), 335–358.

[3] S. Aivazidis, The subgroup permutability degree of projective special linear groups over fields of even characteristic, *J. Group Theory* **16** (2013), 383–396.

[4] A. Amit, On equations in nilpotent groups, Unpublished.

[5] T. Bandman, S. Garion and F. Grunewald, *Groups Geom. Dyn.* **6** (2012), 409–439

[6] E. Bannai, M. Deza, P. Frankl, A. C. Kim and M. Kiyota, On the number of elements which are not n-th powers in finite groups, *Comm. Algebra* **17**(11) (1989), 2865–2870.

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

[8] Y. G. Berkovich, G. A. Freiman and C. Praeger, Small squaring and cubing properties for finite groups, *Bulll Austral Math. Soc.* **44** (1991), 429–450.

[9] A. K. Das, On group elements having square roots, *Bull. Iranian Math. Soc.* **31**(2), 33–36.

[10] A. K. Das and R. K. Nath, A characterisation of certain finite groups of odd order, *Math. Proc. Royal. Irish Acad* **111**A(2) (2011), 69–78.

[11] J. D. Dixon, L. Pyber, Á. Seress and A. Shalev, Residual properties of free groups and probabilistic methods, *J. Reine Angew. Math.* **556** (2003), 159–172.

[12] P. Erdös and P. Turan, On some problems of a statistical group-theory, IV, *Acta Math. Hungar.* **19**(3-4) (1968), 413–435.

[13] A. Erfanian and M. Farrokhi D. G., On the probability of being a 2-Engel group, *Int. J. Group Theory* **2**(4) (2013), 31–38.

[14] M. Farrokhi D. G., Factorization numbers of finite abelian groups, *Int. J. Group Theory* **2**(2) (2013), 1-8.

[15] M. Farrokhi D. G., Problems and solutions, *Amer. Math. Monthly* **115**(8) (2008), p. 758.

[16] M. Farrokhi D. G. and S. H. Jafari, On the probability of being a deficient square group on 2-element subsets, *Preprint.*

[17] M. Farrokhi D. G., S. H. Jafari and F. Saeedi, Subgroup normality degrees of finite groups I, *Arch. Math.* **96** (2011), 215–224.

[18] M. Farrokhi D. G. and F. Saeedi, Factorization numbers of some finite groups, *Glasgow Math. J.* **54** (2012), 345–354.

[19] M. Farrokhi D. G. and F. Saeedi, Subgroup permutability degree of $PSL(2, p^n)$, *Glasgow Math. J.* **55** (2013), 581–590.

[20] M. Farrokhi D. G. and F. Saeedi, Subgroup normality degrees of finite groups II, *J. Algebra Appl.* **11**(4) (2012), 8 pp.

[21] G. A. Fernández-Alcober, Omega subgroups of powerful p-groups, *Israel J. Math.* **162** (2007), 75–79.

[22] G. A. Freiman, On two- and three-element subsets of groups, *Aequationes Math.* **22** (1981), 140–152.

[23] F. G. Frobenius, Über Gruppencharaktere, *Sitzber. Preuss. Akad. Wiss.* (1896), 985–1021.

[24] F. G. Frobenius, Verallgemeinerung des Sylowschen Satze, *Berliner Sitz.* (1895), 981–993.

[25] S. Garion and A. Shalev, Commutator maps, measure preservation, and T-systems, Trans. Amer. Math. Soc. **361**(9) (2009), 4631–4651.

[26] B. Givens, The probability that two semigroup elements commute can be almost anything, *College Math. J.* **39**(5) (2008), 399–400.

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

[28] R. M. Guralnick and P. H. Tiep, The Waring problem for finite quasisimple groups. II, Preprint.

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

[30] R. Heffernan, D. MacHale and Á. Ní Shé, Restrictions on commutativity ratios in finite groups, *Int. J. Group Theory* **3**(4) (2014), 1–12.

[31] P. V. Hegarty, Limit points in the range of the commuting probability function on finite groups, *J. Group Theory* **16**(2) (2013), 235–247.

[32] P. V. Hegarty, Soluble groups with an automorphism inverting many elements, *Math. Proc. Royal Irish Acad.* **105**A(1) (2005), 59–73.

[33] M. Herzog, P. Longobardi and M. Maj, On a combinatorial problem in group theory, *Israel J. Math.* **82** (1993), 329–340.

[34] L. Héthelyi and L. Lévai, On elements of order p in powerful p-groups, *J. Algebra* **270** (2003), 1–6.

[35] N. Iiyori and H. Yamaki, On a conjecture of Frobenius, *Bull. Amer. Math. Soc.* **25** (1991), 413–416.

[36] S. Jambor, M. W. Liebeck and E. A. O'Brien, Some word maps that are non-surjective on infinitely many finite simple groups, *Bull. London Math. Soc.* **45** (2013) 907–910.

[37] G. A. Jones, Varieties and simple groups, *J. Aust. Math. Soc.* **17** (1974) 163173.

[38] K. S. Joseph, *Commutativity in non-abelian groups*, Ph.D. Thesis, UCLA (1969).

[39] K. S. Joseph, Several conjectures on commutativity in algebraic structures, *Amer. Math. Monthly* **84** (1977), 550–551.

[40] M. Kassabov and N. Nikolov, Words with few values in finite simple groups, *Q. J. Math.* **64** (2013), 1161–1166.

[41] T. J. Laffey, The number of solutions of $x^p = 1$ in a finite group, *Math. Proc. Cambridge Philos. Soc.* **80** (1976), 229–231.

[42] T. J. Laffey, The number of solutions of $x^3 = 1$ in a 3-group, *Math. Z.* **149** (1976), 43–45.

[43] T. J. Laffey, The number of solutions of $x^4 = 1$ in finite groups, *Math. Proc. Roy. Irish Acad.* **79**A(4) (1979), 29–36.

[44] M. Larsen, Word maps have large image, *Israel J. Math.* **139** (2004), 149–156.

[45] M. Larsen and A. Shalev, Fibers of word maps and some applications, *J. Algebra* **354** (2012), 36–48.

[46] M. Larsen and A. Shalev, Word maps and Waring type problems, *J. Amer. Math. Soc.* **22**(2) (2009), 437–466.

[47] M. Larsen, A. Shalev and P. H. Tiep, The Waring problem for finite simple groups, *Ann. Math.* **174** (2011), 1885–1950.

[48] M. Larsen, A. Shalev and P. H. Tiep, Waring problem for finite quasisimple groups, Int. Math. Res. Not. Vol. **2013**, No. 10, 2323–2348.

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

[50] P. Lescot, H. N. Nguyen and Y. Yang, On the commuting probability and supersolvability of finite groups, *Monatsh. Math.* **174** (2014), 567–576.

[51] L. Lévai and L. Pyber, Profinite groups with many commuting pairs or involutions, *Arch. Math.* **75** (2000), 1–7.

[52] M. Levy, Images of word maps in almost simple groups and quasisimple groups, *Internat. J. Algebra Comput.* **24**(1) (2014), 47–58.

[53] M. Levy, On the probability of satisfying a word in nilpotent groups of class 2, *Preprint.*

[54] M. Levy, Word maps with small image in simple groups, *Preprint.*

[55] Y. Li and Y. Tan, On $B(4,k)$ groups, *J. Algebra Appl.* **9**(1) (2010), 27–42.

[56] Y. Li and Y. Tan, On $B(4,13)$ 2-groups, *Comm. Algebra* **39**(10) (2011), 3769–3780.

[57] Y. Li and X. Pan, On $B(5,k)$ groups, *Bull. Aust. Math. Soc.* **84**(3) (2011), 393–407.

[58] Y. Li and Y. Tan, On B_5-groups, *Ars Combin.* **114** (2014), 3–14.

[59] H. Liebeck and D. MacHale, Groups with automorphisms inverting most elements, *Math. Z.* **124** (1972), 51–63.

[60] M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep, Products of squares in finite simple groups, *Proc. Amer. Math. Soc.* **140**(1) (2012), 21–33.

[61] P. Longobardi and M. Maj, The classification of groups with the small squaring property on 3-sets, *Bull. Austral Math. Soc.* **46** (1992), 263–269.

[62] A. Lubotzky, Images of word maps in finite simple groups, *Glasgow Math. J.* **56**(2) (2014), 465–469.

[63] M. S. Lucido and M. R. Pournaki, Probability that an element of a finite group has a square root, *Algebra Colloq.* **12**(4) (2005), 677–690.

[64] M. S. Lucido and M. R. Pournaki, Probability that an element of a finite group has a square root, *Colloq. Math.* **112**(1) (2008), 147–155.

[65] C. Martinez and E. Zelmanov, Products of powers in finite simple groups, *Israel J. Math.* **96** (1996), 469–479.

[66] O. Ore, Some remarks on commutators, *Proc. Amer. Math. Soc.* **2** (1951), 307–314.

[67] J. Saxl and J. S. Wilson, A note on powers in simple groups, *Math. Proc. Camb. Phil. Soc.* **122** (1997), 91–94.

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

[69] A. Shalev, Mixing and generation in simple groups, *J. Algebra* **319** (2008), 3075–3086.

[70] A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem, *Ann. Math.* **170** (2009), 1383–1416.

[71] L. Solomon, The solution of equations in groups, *Arch. Math.* **20**(3) (1969), 241–247.

[72] A. Mann, Finite groups containing many involutions, *Proc. Amer. Math. Soc.* **122**(2) (1994), 383–385.

[73] A. Mann and C. Martinez, Groups nearly of prime exponent and nearly Engel Lie algebras, *Arch. Math.* **71** (1998), 5–11.

[74] A. Mann and C. Martinez, The exponent of finite groups, *Arch. Math.* **67** (1996), 8–10.

[75] M. Mazur, On powers in powerful p-groups, *J. Group Theory* **10** (2007), 431–433.

[76] G. A. Miller, Groups containing a relatively large number of operators of order two, *Bull. Amer. Math. Soc.* **25**(9) (1919), 408–413.

[77] G. A. Miller, Note on the possible number of operators of order 2 in a group of order 2^m, *Ann. Math. (2)* **7**(2) (1907), 55–60.

[78] G. A. Miller, On the minimum number of operators whose orders exceed two in any finite group, *Bull. Amer. Math. Soc.* **13**(5) (1907), 235–239.

[79] P. M. Neumann, Two combinatorial problems in group theory, *Bull. London Math. Soc.* **21** (1989), 456–458.

[80] N. Nikolov and D. Segal, A characterization of finite soluble groups, *Bull. London Math. Soc.* **39** (2007) 209–213.

[81] V. Ponomarenko and N. Selinski, Two semigroup elements can commute with any positive rational probability, *College Math. J.* **43**(4) (2012), 334–336.

[82] W. M. Potter, Nonsolvable groups with an automorphism inverting many elements, *Arch. Math.* **50** (1988), 292–299.

[83] D. Rusin, What is the probability that two elements of a finite group commute, *Pacific. J. Math.* **82**(1) (1979), 237–247.

[84] M. Tărnăuceanu, Subgroup commutativity degrees of finite groups, *J. Algebra* **321**(9) (2009), 2508–2520.

[85] C. T. C. Wall, On groups consisting mostly of involutions, *Math. Proc. Camb. Phil. Soc.* **67** (1970), 251–262.

M. FARROKHI D. G.

Mathematical Science Research Unit, College of Liberal Arts, Muroran Institute of Technology, 27-1, Mizumoto, Muroran 050-8585, Hokkaido, Japan.

E-mail address: m.farrokhi.d.g@gmail.com