On the probability that a group satisfies a law

Mohammad Farrokhi Derakhshandeh Ghouchan

Muroran Institute of Technology

Research on Finite Groups and Their Representations, Vertex Operator Algebras, and Algebraic Combinatorics
Kyoto University, RIMS
December 19, 2014

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-tuples of elements of G satisfies $w = g$ is defined by

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

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

Definition

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

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

Definition

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

Theorem (Erdös and Turan, 1968[1])

If G is a finite group, then

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

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

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

Joseph's conjectures

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

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

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

Joseph's conjectures

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

Conjecture (Joseph, 1977[1,2])

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

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

Joseph's conjectures

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

Conjecture (Joseph, 1977[1,2])

(1) Every limit point of $\mathcal{D}$ is rational.

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

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

Joseph's conjectures

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

Conjecture (Joseph, 1977[1,2])

(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 $\mathcal{D} \cap (l - \epsilon, l) = \emptyset$.

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

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

Joseph's conjectures

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

Conjecture (Joseph, 1977[1,2])

(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 $\mathbb{R}$.

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

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

Joseph's conjectures

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

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

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

Joseph's conjectures

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

Theorem (Givens, 2008[1])

The set $\mathcal{D}'$ is dense in $[0, 1]$.

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

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

Joseph's conjectures

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

Theorem (Givens, 2008[1])

The set $\mathcal{D}'$ is dense in $[0, 1]$.

Theorem (Ponomarenko and Selinski, 2012[2])

We have $\mathcal{D}' = \mathbb{Q} \cap [0, 1]$.

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

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

Joseph's conjectures

Theorem (Joseph, 1969[1]; Gustafson, 1973[2])

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 $G/Z(G) \cong C_2 \times C_2$.

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

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

Joseph's conjectures

Theorem (Rusin, 1979[1])

The values of $d(G)$ above $\frac{11}{32}$ are precisely

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

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

Joseph's conjectures

Theorem (Das and Nath, 2011[1])

Let G be a group of odd order. The values of $d(G)$ above $\frac{11}{75}$ are precisely

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

[1] 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.

Joseph's conjectures

Theorem (Hegarty, 2013[1])

If $l \in (\frac{2}{9}, 1]$ is a limit point of $\mathcal{D}$, then

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

Joseph's conjectures

Theorem (Hegarty, 2013[1])

If $l \in (\frac{2}{9}, 1]$ is a limit point of $\mathcal{D}$, then

(i) *l is rational, and*

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

Joseph's conjectures

Theorem (Hegarty, 2013[1])

If $l \in (\frac{2}{9}, 1]$ is a limit point of $\mathcal{D}$, then

(i) *l is rational, and*

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

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

Nilpotency, solvability and supersolvability results

Theorem (Neumann, 1989[1])

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,

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

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

Nilpotency, solvability and supersolvability results

Theorem (Lévai and Pyber, 2000[1])

Let G be a profinite group with positive commutitivity degree. Then G is abelian-by-finite.

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

Nilpotency, solvability and supersolvability results

Theorem (Rusin, 1979[1]; Lescot, 1995[2])

Let G be a finite group. Then

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

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

Nilpotency, solvability and supersolvability results

Theorem (Rusin, 1979[1]; Lescot, 1995[2])

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.*

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

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

Nilpotency, solvability and supersolvability results

Theorem (Rusin, 1979[1]; Lescot, 1995[2])

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.*

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

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

Nilpotency, solvability and supersolvability results

Theorem (Barry, MacHale and Ní Shé, 2006[1])

Let G be a finite group. If $d(G) > \frac{1}{3}$, then G is supersolvable.

[1] 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.

Nilpotency, solvability and supersolvability results

Theorem (Barry, MacHale and Ní Shé, 2006[1])

Let G be a finite group. If $d(G) > \frac{1}{3}$, then G is supersolvable.

Theorem (Barry, MacHale and Ní Shé, 2006[1])

Let G be a finite group of odd order. If $d(G) > \frac{11}{75}$, then G is supersolvable.

[1] 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.

Nilpotency, solvability and supersolvability results

Theorem (Lescot, Nguyen and Yang, 2014[1])

Let G be a finite group. If $d(G) > \frac{5}{16}$, then

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

Nilpotency, solvability and supersolvability results

Theorem (Lescot, Nguyen and Yang, 2014[1])

Let G be a finite group. If $d(G) > \frac{5}{16}$, then

(i) *G is supersolvable,*

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

Nilpotency, solvability and supersolvability results

Theorem (Lescot, Nguyen and Yang, 2014[1])

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*

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

Nilpotency, solvability and supersolvability results

Theorem (Lescot, Nguyen and Yang, 2014[1])

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.*

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

Nilpotency, solvability and supersolvability results

Theorem (Lescot, Nguyen and Yang, 2014[1])

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 (Lescot, Nguyen and Yang, 2014[1])

If G is a finite group. Then $d(G) = \frac{1}{3}$ if and only if G is isoclinic to A_4.

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

Nilpotency, solvability and supersolvability results

Theorem (Lescot, Nguyen and Yang, 2014[1])

Let G be a finite group of odd order. If $d(G) > \frac{35}{243}$, then

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

Nilpotency, solvability and supersolvability results

Theorem (Lescot, Nguyen and Yang, 2014[1])

Let G be a finite group of odd order. If $d(G) > \frac{35}{243}$, then

(i) *G is supersolvable, or*

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

Nilpotency, solvability and supersolvability results

Theorem (Lescot, Nguyen and Yang, 2014[1])

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 $(C_5 \times C_5) \rtimes C_3$.*

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

Nilpotency, solvability and supersolvability results

Theorem (Heffernan, MacHale and Ní Shé, 2014[1])

Let G be a finite group. If $d(G) > \frac{7}{24}$, then G is metabelian.

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

Nilpotency, solvability and supersolvability results

Theorem (Heffernan, MacHale and Ní Shé, 2014[1])

Let G be a finite group. If $d(G) > \frac{7}{24}$, then G is metabelian.

Theorem (Heffernan, MacHale and Ní Shé, 2014[1])

Let G be a finite group of odd order. If $d(G) > \frac{83}{675}$, then G' is nilpotent.

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

Nilpotency, solvability and supersolvability results

Theorem (Guralnick and Robinson, 2006[1])

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,

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

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

Nilpotency, solvability and supersolvability results

Theorem (Guralnick and Robinson, 2006[1])

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.

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

Nilpotency, solvability and supersolvability results

Theorem (Guralnick and Robinson, 2006[1])

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 (Guralnick and Robinson, 2006[1])

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 $d(G) = \frac{1}{12}$.

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

Nilpotency, solvability and supersolvability results

Theorem (Guralnick and Robinson, 2006[1])

Let G be a finite solvable groups of derived length $d \geq 4$. Then

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

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

Nilpotency, solvability and supersolvability results

Theorem (Guralnick and Robinson, 2006[1])

Let G be a finite solvable groups of derived length $d \geq 4$. Then

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

Theorem (Guralnick and Robinson, 2006[1])

Let G be a finite p-group of derived length $d \geq 2$. then

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

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

Definition

A *positive law* in groups is law $w = 1$, which can be stated 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 $u^{-1}v$.

Definition

A *positive law* in groups is law $w = 1$, which can be stated 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 $xy = yx$.

Theorem (Tărnăuceanu, 2009[1])

Let $G = D_{2n}$ be the dihedral group of order $2n$. Then

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

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

Theorem (Tărnăuceanu, 2009[1])

Let $G = D_{2n}$ be the dihedral group of order $2n$. Then

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

Corollary (Tărnăuceanu, 2009[1])

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

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

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

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

Theorem (Farrokhi, 2013[1]; Farrokhi and Saeedi, 2013[2,3])

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

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

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

Theorem (continued)

Theorem (continued)

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

Theorem (continued)

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

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

Theorem (continued)

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

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

Theorem (continued)

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

(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,

Theorem (continued)

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

(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,

Theorem (continued)

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

(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,

Theorem (continued)

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

(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.

Theorem (continued)

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

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

Theorem (continued)

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

Theorem (continued)

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

Theorem (continued)

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

Theorem (continued)

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

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

Theorem (continued)

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

(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

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

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

Theorem (continued)

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

(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

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

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

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

Theorem (continued)

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

(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) $F_2(A_5) = 237$,

Theorem (continued)

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

Theorem (continued)

Theorem (continued)

$$
(8.1)\quad F_2(PSL_2(p^n)) = \begin{cases} 2|L(PSL_2(p^n))| + 2p^n(p^{2n}-1)-1, & p=2, n>1, \\ 2|L(PSL_2(p^n))| + p^n(p^{2n}-1)-1, & p>2 \text{ and } (p^n-1)/2 \text{ is odd}, \\ & p^n \neq 3, 7, 11, 19, 23, 59, \\ 2|L(PSL_2(p^n))| - 1, & p>2 \text{ and } (p^n-1)/2 \text{ is even}, \\ & p^n \neq 5, 9, 29 \end{cases} \quad \text{and}
$$

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

if

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

respectively, and

Theorem (continued)

(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) $F_2(PGL_2(p^n)) =$
$$\begin{cases} 3p^n(p^{2n}-1) + 4|L(PGL_2(p^n))| - 2|L(PSL_2(p^n))| - 3, & n \text{ even or } p \equiv 1 \pmod 4, \\ 4p^n(p^{2n}-1) + 4|L(PGL_2(p^n))| - 2|L(PSL_2(p^n))| - 3, & n \text{ odd and } p \equiv 3 \pmod 4 \end{cases}$$ 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.

Theorem (Aivazidis, 2013[1])

We have

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

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

[2] S. Aivazidis, On the subgroup permutability degree of the simple Suzuki groups, To appear in *Monatsh. Math.*

Theorem (Aivazidis, 2013[1])

We have

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

Theorem (Aivazidis, 2014[2])

We have

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

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

[2] S. Aivazidis, On the subgroup permutability degree of the simple Suzuki groups, To appear in *Monatsh. Math.*

Conjecture

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

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

Conjecture

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

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

Conjecture

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.

Theorem (Erfanian and Farrokhi, 2013[1])

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.

[1] 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.

Theorem (Erfanian and Farrokhi, 2013[1])

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

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

[1] 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.

Theorem (Erfanian and Farrokhi, 2013[1])

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.

---

[1] 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.

Theorem (Mann and Martinez, 1998[1])

Let L be a finite Lie algebra of characteristic p, which is not n-Engel. Then

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

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

Definition

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

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

Definition

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

Theorem (Frobenius, 1895[1])

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.

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

Definition

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

Theorem (Frobenius, 1895[1])

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

If G is a finite group whose order is divisible by a number n, then

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

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

Conjecture (Frobenius, 1895[1])

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.

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

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

Conjecture (Frobenius, 1895[1])

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 (Iiyoria and Yamaki, 1991[2])

The conjecture of Frobenius is always true.

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

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

Theorem (Miller, 1907[1])

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.

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

[1] 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.

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

Theorem (Miller, 1907[1])

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 (Miller, 1919[2])

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.

---

[1] 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.

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

Theorem (Wall, 1970[1]; Liebeck and MacHale, 1972[2])

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

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

Theorem (Wall, 1970[1]; Liebeck and MacHale, 1972[2])

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,*

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

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

Theorem (Wall, 1970[1]; Liebeck and MacHale, 1972[2])

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*,*

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

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

Theorem (Wall, 1970[1]; Liebeck and MacHale, 1972[2])

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*

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

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

Theorem (Wall, 1970[1]; Liebeck and MacHale, 1972[2])

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*

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

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

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

Theorem (Potter, 1988[1])

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

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

Theorem (Hegarty, 2005[1])

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

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

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

Theorem (Mann, 1994[1])

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.

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

Theorem (Laffey, 1976[1])

Let G be a finite group, p be a prime divisor of $|G|$ and assume that is not a p-group. Then

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

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

Theorem (Laffey, 1976[1])

Let G be a finite 3-group. Then

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

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

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

Theorem (Laffey, 1976[1])

Let G be a finite 3-group. Then

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

Theorem (Laffey, 1979[2])

Let G be a finite group which is not a 2-group. Then

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

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

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

Definition

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

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

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 (Héthelyi and Lévai, 2003[1])

Let G be a powerful p-group. Then

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

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

Theorem (Mazur, 2007[1]; Fernández-Alcober, 2007[2])

Let G be a powerful p-group and $k \geq 1$. Then

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

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

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

Theorem (Mann and Martinez, 1996[1])

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.

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

Theorem (Mann and Martinez, 1996[1])

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 (Mann and Martinez, 1996[1])

Let G be an m-generated finite p-group of exponent $> p^n$. Then

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

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

Theorem (Mann and Martinez, 1998[1])

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.

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

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 $DS(m)$.

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

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 $i_1, \ldots, i_n, j_1, \ldots, j_n = 1, \ldots, m$.

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 $\tilde{P}(G, W)$.

Theorem (Freiman, 1981[1])

Let G be a finite group. Then

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

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

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

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

Theorem (Freiman, 1981[1])

Let G be a finite group. Then

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

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

Theorem (Farrokhi and Jafari, 2014[2])

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 $G \cong D_8 \times C_2^n$ for some $n \geq 0$.

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

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

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 $\mathcal{P}_N^* = \mathcal{P}_N \setminus \{1\}$.

Theorem (Farrokhi, Jafari and Saeedi, 2011[1])

If G is a finite simple group, then $\max \mathcal{P}_N^*(G) \leq \frac{8}{15}$. *Moreover the bound is sharp.*

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

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

Theorem (Farrokhi, Jafari and Saeedi, 2011[1])

If G is a finite simple group, then $\max \mathcal{P}_N^*(G) \leq \frac{8}{15}$. Moreover the bound is sharp.

Theorem (Farrokhi and Saeedi, 2012[2])

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.

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

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

Lemma (Farrokhi and Saeedi, 2012[1])

Let $\mathcal{A}$ be the set of all numbers $\frac{1}{n}\left(1+\sum_{i=1}^{n-1}\frac{1}{m_i}\right)$, which satisfy the following inequalities

$$\frac{1}{2} < \frac{1}{n}\left(1+\sum_{i=1}^{n-1}\frac{1}{m_i}\right) \leq \frac{1}{2}+\frac{1}{2n}$$

and $n, m_1, \ldots, m_{n-1} \geq 2$. Then $\mathcal{A} \subseteq \{\frac{1}{2}+\frac{1}{k}\}$.

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

Lemma (Farrokhi and Saeedi, 2012[1])

Let $\mathcal{A}$ be the set of all numbers $\frac{1}{n}\left(1+\sum_{i=1}^{n-1}\frac{1}{m_i}\right)$, which satisfy the following inequalities

$$\frac{1}{2} < \frac{1}{n}\left(1+\sum_{i=1}^{n-1}\frac{1}{m_i}\right) \leq \frac{1}{2}+\frac{1}{2n}$$

and $n, m_1, \ldots, m_{n-1} \geq 2$. Then $\mathcal{A} \subseteq \{\frac{1}{2}+\frac{1}{k}\}$.

Theorem (Farrokhi and Saeedi, 2012[1])

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

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

Conjecture (Farrokhi and Saeedi, 2012[1])

The values of $\mathcal{P}_N$ in the interval $(\frac{1}{3}, \frac{1}{2}]$ fall into the following seven sequences

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

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

Conjecture (Farrokhi and Saeedi, 2012[1])

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 (Farrokhi and Saeedi, 2012[1])

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

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

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

Theorem (Solomon, 1969[1])

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 $|G|$.

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

Theorem (Solomon, 1969[1])

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

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

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

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

Theorem (Amit[1])

If G is a finite nilpotent group, then there exists a constant $c > 0$ such that

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

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

Conjecture (Amit[1])

If G is a finite solvable group, then there exists a constant $c > 0$ such that

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

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

Conjecture (Amit[1])

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 (Amit[1])

If G is a finite nilpotent group, then

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

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

Question (Amit[1])

Let G is a finite non-solvable group, then

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

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

Theorem (Levy, 2011[1])

Let G be a finite group of nilpotency class 2. Then the set

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

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

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

Theorem (Levy, 2011[1])

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 (Nikolov and Segal, 2007[2])

Let G be a finite group. Then G is nilpotent if and only if

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

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

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

Theorem (Nikolov and Segal, 2007[1])

Let G be a finite group. Then G is solvable if and only if

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

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

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

Theorem (Nikolov and Segal, 2007[1])

Let G be a finite group. Then G is solvable if and only if

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

Theorem (Abért, 2006[2])

Let G be a finite just non-solvable group. Then the set

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

is dense in $[0,1]$.

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

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

Theorem (Jones, 1974[1])

Let $w \neq 1$ be a word. Then $P(G, w) < 1$ for all but finitely many non-abelian finite simple groups G.

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

[2] 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.

Theorem (Jones, 1974[1])

Let $w \neq 1$ be a word. Then $P(G, w) < 1$ for all but finitely many non-abelian finite simple groups G.

Theorem (Dixon, Pyber, Seress and Shalev, 2003[2])

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.

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

[2] 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.

Theorem (Larsen and Shalev, 2012[1])

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 $N = N(\epsilon) > 0$.

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

Theorem (Larsen and Shalev, 2012[1])

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 (Larsen and Shalev, 2012[1])

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 $g \in G$.

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

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

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

and it is called a *word map*.

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*.

Remark

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 $g \in G$.

Theorem (Lubotzky, 2014[1])

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 $w(G) = X$.

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

Theorem (Lubotzky, 2014[1])

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 (Lubotzky, 2014[1])

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 $a, b \in G$.

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

Theorem (Levy, 2014[1])

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 $w(G) = X$.

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

Commutator maps: The Ore conjecture

Conjecture (Ore, 1951[1])

The commutator map is surjective over all non-abelian finite simple groups.

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

Commutator maps: The Ore conjecture

Theorem (Shalev, 2009[1])

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.

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

Commutator maps: The Ore conjecture

- Alternating groups (Ore, 1951),

Commutator maps: The Ore conjecture

- Alternating groups (Ore, 1951),
- $PSL_n(q)$ (Thompson, 1961-1962),

Commutator maps: The Ore conjecture

- Alternating groups (Ore, 1951),
- $PSL_n(q)$ (Thompson, 1961-1962),
- Sporadic simple groups (Neubüser, Pahlings and Cleuvers, 1984),

Commutator maps: The Ore conjecture

- 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),

Commutator maps: The Ore conjecture

- 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),

Commutator maps: The Ore conjecture

- 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),

Commutator maps: The Ore conjecture

- 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),

Commutator maps: The Ore conjecture

- 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).

Commutator maps: The Ore conjecture

Theorem (Frobenius, 1896[1])

Let G be a finite group and $g \in G$. The number of solutions to the equation $[x, y] = g$ equals

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

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

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

Commutator maps: The Ore conjecture

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.

[1]A. Shalev, Mixing and generation in simple groups, *J. Algebra* **319** (2008), 2075–2096.

Commutator maps: The Ore conjecture

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 (Shalev, 2008[1])

If G is a finite non-abelian simple group, then

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

[1] A. Shalev, Mixing and generation in simple groups, *J. Algebra* **319** (2008), 2075–2086.

Commutator maps: The Ore conjecture

Theorem (Garion and Shalev, 2009[1])

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 $\epsilon(G) = (\zeta^G(2) - 1)^{\frac{1}{4}}$.

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

Engels maps and beyond

Conjecture (Shalev, 2007[1])

The n-th Engel word $(n \geq 1)$ map is surjective for any finite simple non-abelian group G.

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

Engels maps and beyond

Conjecture (Shalev, 2007[1])

The n-th Engel word ($n \geq 1$) map is surjective for any finite simple non-abelian group G.

Conjecture (Shalev, 2007[1])

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 $w(G) = G$.

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

Engel maps

Theorem (Bandman, Garion and Grunewald, 2012[1])

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.

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

Engel maps

Theorem (Bandman, Garion and Grunewald, 2012[1])

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

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

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

Power maps

Theorem (Bannai, Deza, Frankl, Kim and Kiyota, 1989[1])

Let G be a finite group and $w = x^n$, when n is a divisor of $|G|$. Then

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

[1] 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.

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

Power maps

Theorem (Bannai, Deza, Frankl, Kim and Kiyota, 1989[1])

Let G be a finite group and $w = x^n$, when n is a divisor of $|G|$. Then

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

Theorem (Das, 2005[2])

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.

[1] 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.

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

Power maps

Question (Das, 2005[1])

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

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

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

Power maps

Question (Das, 2005[1])

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

Proposition (Farrokhi, 2008[2])

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

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

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

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

Power maps

Theorem (Martinez and Zelmanov, 1996[1]; Saxl and Wilson, 1997[2])

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

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

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

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

Power maps: Lagrange's four square theorem for groups

Theorem (Liebeck, O'Brien, Shalev and Tiep, 2012[1])

Every element of every non-abelian finite simple group G is a product of two squares.

[1] 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.

Power maps: Lagrange's four square theorem for groups

Theorem (Liebeck, O'Brien, Shalev and Tiep, 2012[1])

Every element of every non-abelian finite simple group G is a product of two squares.

Theorem (Liebeck, O'Brien, Shalev and Tiep, 2012[1])

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.

[1] 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.

Theorem (Larsen, 2004[1])

For every non-trivial 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 $|w(G)| \geq |G|^{1-\epsilon}$.

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

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

Theorem (Larsen, 2004[1])

For every non-trivial 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 $|w(G)| \geq |G|^{1-\epsilon}$.

Theorem (Shalev, 2009[2])

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 $w(G)^3 = G$.

---

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

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

Theorem (Larsen and Shalev, 2009[1])

For each triple of non-trivial 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 $w_1(G)w_2(G)w_3(G) = G$.

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

Theorem (Larsen and Shalev, 2009[1])

For each triple of non-trivial 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 (Larsen and Shalev, 2009[1])

For each pair of non-trivial 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 $w_1(G)w_2(G) = G$.

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

Theorem (Larsen, Shalev and Tiep, 2013[1])

If w_1, w_2 and w_3 are nontrivial words, then for all finite quasisimple groups G of sufficiently large order, $w_1(G)w_2(G)w_3(G) = G$.

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

Theorem (Larsen, Shalev and Tiep, 2011[1])

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 $w_1(G)w_2(G) = G$.

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

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

Theorem (Larsen, Shalev and Tiep, 2011[1])

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 $w_1(G)w_2(G) = G$.

Theorem (Guralnick and Tiep, 2013[2])

Let w_1 and w_2 be two non-trivial 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 $w_1(G)w_2(G) \supseteq G \setminus Z(G)$.

---

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

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

Thank You for Your Attention!