What is 5/8 theorem ?

Main references :

[Gustafson 1973] W.H. Gustafson, What is the probability that two group elements commute, AMM 1973.

[GR 2006] R.M. Guralnick and G. R. Robinson - On the commuting probability in finite groups. J. Alg. 2006.

(Paul Lescot - 1987, 1989, 1995 - Degré de commutativité et structure d'un groupe fini - Thm 11 of [GR 2006])

[HR 2012] K.H. Hoffmann and F. G. Russo - The probability that x and y commute in a compact group, - Math proc. Cambridge Phil. Soc 2012.

[Dixon 1969] J. Dixon - The probability of generating the symmetric group, Math Z. 1969.

[E-T- 1965 to 1968] P. Erdős, P. Turán - On some problems of statistical gp. th I - IV Acta Math. Acad. Sci Hungary

§1. Theorem (Gustafson 1973). Let G be a finite, non-abelian group. The probability that two randomly chosen elements of G commute is $\leq \frac{5}{8}$.

§2. Some necessary definitions. –

(2.1) A group G is a set together with an associative binary operation

$G \times G \to G$ (associativity: $a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad \forall a,b,c \in G$.)
$(a,b) \mapsto a\cdot b$

and a distinguished element $e \in G$ (called neutral, or identity) s.t.

$e\cdot a = a\cdot e = a \quad \forall a \in G$; and $\forall x \in G$, $\exists!\ \bar{x}^{-1} \in G$ s.t.
$x\cdot \bar{x}^{-1} = \bar{x}^{-1}\cdot x = e$.

We say G is abelian if $a\cdot b = b\cdot a \quad \forall a,b \in G$.

(2.2) Examples. – (a) $\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$; group operation = $+$
neutral elt. = 0.

(b) $\mathbb{Z}/_{n\mathbb{Z}} = \{0, 1, \ldots, n-1\}$; group operation = $+$ modulo n
neutral elt. = 0.

A group G is said to be cyclic if $\exists\ a \in G$ s.t. $G = \{a^n : n \in \mathbb{Z}\}$.
Every cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/_{N\mathbb{Z}}$ $(N = |G|)$.

(c) S_n = group of permutations on n letters.
$|S_n| = n!$

(d) D_n = dihedral group $= \langle s, r \mid s^2 = r^n = e$ and $srs = r^{-1} \rangle$

(e) $GL_2(F) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in F \text{ (field)},\ ad - bc \neq 0 \right\}$

(2.3) Let G be a group and X be a set. We say <u>G acts on X</u> (abbreviated as $G \curvearrowright X$) if we are given a function

$\alpha : G \times X \to X$ s.t. (i) $\alpha(e, x) = x \quad \forall\, x \in X$.

(ii) $\alpha(g_1, \alpha(g_2, x)) = \alpha(g_1 g_2, x)$

$\forall\, g_1, g_2 \in G,\ x \in X$.

Thus $g \mapsto \alpha(g, -)$ is a group hom. $G \to S_X$ (gp. of all bijections $X \to X$).

$G \curvearrowright X \rightsquigarrow$ An equiv. rel^n on X : $x \sim y$ if $\exists\, g \in G$ s.t. $g \cdot x = y$.

X/G := set of <u>equivalence classes</u> (called <u>orbits</u>)

For $x \in X$, $\mathcal{O}(x) := \{ g \cdot x \mid g \in G \} \subset X$ an orbit

$\mathrm{Stab}_G(x) := \{ g \in G \mid g \cdot x = x \} \subset G$ a subgroup of G

(Stabilizer of x).

(2.4) Counting lemma. - Let $G \curvearrowright X$ Then $X = \bigsqcup_{\mathcal{O} \in X/G} \mathcal{O}$.

For any $\mathcal{O} \in X/G$ and $x \in \mathcal{O}$, we have a bijection

$G/\mathrm{Stab}_G(x) \to \mathcal{O}$ (Note, $\mathrm{Stab}(x) \xrightarrow{\sim} \mathrm{Stab}(gx)$, $\sigma \mapsto g \sigma g^{-1}$)

Hence, if G and X are finite, $X/G = \{\mathcal{O}_1, \dots, \mathcal{O}_r\}$ and $x_j \in \mathcal{O}_j$,

then $$|X| = \sum_{i=1}^{r} |\mathcal{O}_i| = |G| \cdot \sum_{i=1}^{r} \frac{1}{|\mathrm{Stab}_G(x_i)|}$$

§3. Corollaries. - Assume G is a finite group.

(3.1) If $H \subset G$ is a subgroup (i.e. $e \in H$; $h_1, h_2 \in H \Rightarrow h_1^{-1} \cdot h_2 \in H$)

then $|H|$ divides $|G|$.

(Consider $H \curvearrowright G$ by left mult. Show that each orbit has the same cardinality as H - hence $\frac{|G|}{|H|} = |G/H| \in \mathbb{N}$.)

In particular $|G| = p$ prime implies that every non-trivial element of G generates G, and $G \cong \mathbb{Z}/p\mathbb{Z}$.

(3.2) Consider $G \curvearrowright G$ by conjugation - i.e. $\begin{array}{l} G \times G \to G \\ (g, x) \mapsto gxg^{-1} \end{array}$.

Orbits under this action are called <u>conjugacy classes</u>.

Stabilizers $\rightsquigarrow$ Centralizer of $x \in G$ $\quad Z_G(x) := \{a \in G \mid axa^{-1} = x\}$ i.e. $ax = xa$

$Z(G) = \{a \in G \mid ab = ba \ \forall b \in G\}$ is called <u>the center of G</u>.

Remark. - $Z(G) \subset G$ is a <u>normal subgroup</u> ($H \subset G$ is normal if $ghg^{-1} \in H$ $\forall g \in G, h \in H$)

G/H inherits a group structure from $G \Leftrightarrow H$ is normal in G.

§4. Lemma (Erdős - Turán, 1968). Let $C \subset G \times G$ be given by

$$C = \{(a, b) \in G \times G \mid ab = ba\}.$$

Then $\operatorname{cp}(G) := \frac{|C|}{|G|^2} = \frac{\#\text{ of conjugacy classes in } G}{|G|}$.

(commuting probability)

Proof. Note $C = \bigcup_{a \in G} (a, Z_G(a))$. So,

$$|C| = \sum_{a \in G} |Z_G(a)| .$$ As $|Z_G(a)| = |Z_G(\sigma a \sigma^{-1})|$,

we get $$|C| = \sum_{\substack{K \subset G \text{ a} \\ \text{conjugacy class}}} |K| \cdot |Z_G(x_K)| \qquad (x_K \in K \text{ arbitrary representative}$$

$$= \sum_{K \in \text{Conj. Classes}(G)} |G| = |G| \cdot \#\text{ of conjugacy classes in } G.$$

(by $|G| = |\text{Orbit } O| \cdot |\text{Stab}_G(x_O)|$) □

Examples. - (1) $G = S_n$, Conjugacy classes in G are labelled by partitions of n.

$$\{ \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_\ell \mid \lambda_1 + \ldots + \lambda_\ell = n \}$$
$$\lambda_j \in \mathbb{N}$$

$$cp(S_n) = \frac{p(n)}{n!} .$$

$p(n)$ = partition fn. of n = # of partitions of n.

$p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$, $\cdots$

(Hardy-Ramanujan : $p(n) \sim \exp\left(\pi \sqrt{\frac{2}{3}} \cdot \sqrt{n}\right)$)

$$cp(S_n) \sim \frac{e^{K \cdot \sqrt{n}}}{n!}$$

$$\Gamma(z) \sim z^{z-\frac{1}{2}} \cdot e^{-z} \sqrt{2\pi} \, (1 + O(z^{-1}))$$

asymptotics of factorial.

Remark.- Erdős-Turán (1965-1973) studied questions regarding S_n as $n \to \infty$. For instance,

Theorem.- For any $\varepsilon, \delta > 0$, $\exists\ n_0 \in \mathbb{N}$ $(n_0(\varepsilon,\delta))$ s.t. $\forall\ n > n_0$

$$\exp\left(\left(\tfrac{1}{2}-\varepsilon\right)\log^2(n)\right) \leq \operatorname{ord}(x) \leq \exp\left(\left(\tfrac{1}{2}+\varepsilon\right)\log^2 n\right)$$

holds for all except $\delta \cdot n!$ elements.

Their work was inspired by earlier result in this direction by

E. Landau (1909)

Let $g(n) := \underset{x \in S_n}{\operatorname{Max}} \operatorname{Ord}(x)$. Then $\lim_{n\to\infty} \dfrac{\log G(n)}{\sqrt{n \log n}} = 1$.

Around the same time, Dixon (1969) proved:

1. Probability that two elements of S_n generate $S_n \to \frac{3}{4}$ as $n \to \infty$

$$\frac{\#\left\{(x,y) \in S_n \times S_n \mid \langle x,y\rangle = A_n \text{ or } S_n\right\}}{(n!)^2} \geq 1 - \frac{2}{(\log\log(n))^2}$$

for $n >> 0$.

§5. Proof of Thm 1. - Let G be a finite, non-abelian group.

Let $K_1, \dots, K_\ell \subset G$ be non-trivial conjugacy classes. (i.e. $|K_j| \geq 2$ $\forall\, 1 \leq j \leq \ell$)

Thus $$G = Z(G) \cup \bigcup_{i=1}^{\ell} K_i$$

Let $N = |G|$, $z = |Z(G)|$. Then $$N = z + \sum_{i=1}^{\ell} |K_i| \geq z + 2\ell$$

$$\Rightarrow \quad \ell \leq \frac{N - z}{2}.$$

So, $$cp(G) = \frac{z+\ell}{N} \leq \frac{N+z}{2N} = \frac{1}{2} + \frac{z}{2N}.$$

Lemma. - If $G/Z(G)$ is cyclic then G is abelian.

(proof - easy. - left as an exercise.)

Since groups of size $1, 2, 3$ are cyclic, this means that

G : non-abelian $\Rightarrow \left| G/Z(G) \right| \geq 4$ i.e. $\frac{z}{N} \leq \frac{1}{4}$.

Hence $$cp(G) \leq \frac{1}{2} + \frac{z}{2N} \leq \frac{1}{2} + \frac{1}{8} = \frac{5}{8}. \qquad \square$$

Example. $G = D_n$.

$$\#\text{ of Conjugacy classes in } G = \begin{cases} \frac{n+3}{2} & n \text{ odd} \\ \frac{n+6}{2} & n \text{ even} \end{cases}$$

$$cp(D_n) = \frac{1}{4} + \begin{cases} \frac{3}{4n} & n \text{ odd} \\ \frac{6}{4n} & n \text{ even} \end{cases} ; \quad cp(D_4) = \frac{5}{8}.$$

Example. $GL_2(\mathbb{F}_q)$

Conjugacy classes representatives: $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ $a \in \mathbb{F}_q^\times$

$\begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$

$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$. For every $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ $\langle \sigma \rangle = \mathrm{Aut}(\mathbb{F}_{q^2}/\mathbb{F}_q)$

$a, b \in \mathbb{F}_q^\times$; $a \neq b$

up to $(a,b) \leftrightarrow (b,a)$

$\begin{bmatrix} 0 & -a\cdot\sigma(a) \\ 1 & a+\sigma(a) \end{bmatrix}$

$$2(q-1) + \frac{(q-1)(q-2)}{2} + \frac{q^2-q}{2} = q^2-1.$$

$$cp(G) = \frac{q^2-1}{(q^2-1)(q^2-q)} = \frac{1}{q(q-1)}.$$

§6. Assume $|G| = p^r$, p prime, $r \geq 1$ s.t. G is non-abelian.

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

Same proof as before except - $|K_i| \geq p \ \forall i$, so, $\ell \leq \frac{N-z}{p}$

and $\frac{z}{N} \leq \frac{1}{p^2}$

$$\Rightarrow \quad cp(G) \ \# = \frac{z+\ell}{N} \leq \frac{1}{N}\left(z + \frac{N-z}{p}\right)$$

$$= \frac{1}{p} + \left(1-\frac{1}{p}\right)\frac{z}{N} \leq \frac{1}{p} + \frac{p-1}{p^3} \qquad \square$$

Example.- Let $G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a,b,c \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \right\}$

Conjugacy classes: $\left\{ \begin{bmatrix} 1 & 0 & \lambda \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}_{\lambda \in \mathbb{Z}/p\mathbb{Z}}$, $\left\{ \begin{bmatrix} 1 & a & x \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} : x \in \mathbb{Z}/p\mathbb{Z} \right\}_{(a,b) \in (\mathbb{Z}/p\mathbb{Z})^2 \setminus \{(0,0)\}}$

$$\#\,\text{Conj.-classes}(G) = p^2 + p - 1.$$

$$cp(G) = \frac{p^2+p-1}{p^3}.$$

More on elements of order = power of a prime and commuting probability in

T.C. Burness, R. Guralnick, A. Moretó, G. Navarro -
On the commuting probability of p-elements in a finite gp.
Alg. N.T. (2023)

§7. Some remarks on compact groups.

1. Same proof as for finite case: let G be a cpct topological group and μ a probability measure on G.

$$C = \{(a,b) \mid ab = ba\} \subset G \times G$$

$$C = f^{-1}(e) \quad \text{where} \quad f : \begin{matrix} G \times G \to G \\ (a,b) \mapsto aba^{-1}b^{-1} \end{matrix}$$

Then $$(\mu \times \mu)(C) = \int_G \mu(Z_G(x))\, d\mu(x)$$

Note - if $x \notin Z(G)$, $\mu(Z_G(x)) \leq \frac{1}{2}$ since $[G : Z_G(x)] \geq 2$.

So, $$(\mu \times \mu)(C) = \mu(Z(G)) + \int_{G \setminus Z(G)} \mu(Z_G(x))\, d\mu(x)$$

$$\leq \mu(Z) + \frac{1}{2}(\mu(G) - \mu(Z))$$

$$= \frac{1}{2} + \frac{1}{2}\mu(Z) \quad . \text{ Again use } [G:Z] \geq 4 \text{ i.e. } \mu(Z) \leq \frac{1}{4}$$

to get $(\mu \times \mu)(C) \leq \frac{1}{2} + \frac{1}{8} = \frac{5}{8}$.

2. Compact groups usually have $cp = 0$.

e.g. $G = SU(2) = \left\{ \begin{bmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{bmatrix} : \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1 \right\}$

$Z_G\left(\begin{bmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{bmatrix}\right)$ = diagonal matrices $\cong S^1 \subset SU(2)$ has measure 0.

$\lambda \in S^1 \setminus \{\pm 1\}$

and $Z(G)$ has measure 0.

Thm. - (Hoffmann, Morris) Let G be a non-abelian, connected, compact topological group. let

$$X := \{ (a,b) \in G \times G \mid \langle a, b \rangle \cong \text{Free}(2) \text{ is dense in } G \}$$

Then $X \subset G \times G$ is dense and ~~$\mu(G \times G \setminus X) = 0$~~ $\mu \times \mu(X) = 1$.

Thm (Hoffmann, Russo) Again, let G be a cpct top. group. Then the following are equivalent:

(a) $\mu \times \mu(C) > 0$ (b) $F = \{ x \in G \mid \text{Conj}(x) \text{ is finite} \} \subset G$ is open

i.e. $Z_G(x) < G$ has finite index

§8. Representation-theoretic proof of 5/8 thm.-

G : finite non-abelian group. Let $N = |G|$ and r = # Conj. classes of G.

(Frobenius, Burnside) r = # of irred. f.d. repns of G (over $\mathbb{C}$) $= |\mathrm{Irr}_{fd}(G)|$

$$\mathrm{Irr}_{fd}(G) = \underbrace{\text{1-dim'l repns}}_{G/[G,G]\text{ - many}} \cup \underbrace{\ell \text{ repns. of dim - say } n_1, \dots, n_\ell \geq 2.}$$

($\ell = 0 \iff G$ is abelian)

So, $r = \left| G/_{[G:G]} \right| + \ell$

and $|G| = \sum_{V \in \mathrm{Irr}_{fd}(G)} \dim(V)^2 = \left| G/_{[G:G]} \right| + \sum_{i=1}^{\ell} n_i^2$

$$\geq \left| G/_{[G:G]} \right| + 4\ell$$

Let $a = \left| G/_{[G:G]} \right| \leq \frac{N}{2}$. Previous inequality: $\ell \leq \frac{N-a}{4}$

$$\Rightarrow \quad cp(G) = \frac{a+\ell}{N} \leq \frac{1}{N}\left(a + \frac{N-a}{4}\right) = \frac{1}{4} + \frac{3}{4}\frac{a}{N}$$

$$\leq \frac{1}{4} + \frac{3}{8} = \frac{5}{8}.$$

□