Parabola Volume 58, Issue 3 (2022)

The 5/8 Theorem

Isaac Lee[1]

1 Introduction

The goal of this paper is to give a short introduction to group theory, which is a very important branch of research in mathematics. After introducing the main concepts of group theory, we will present some examples of groups. We will also state and present the proof of a theorem that connects group theory and probability theory. More precisely, we will present a theorem addressing the following question:
What is the probability that two randomly chosen elements in a finite group commute?

2 A First Look Into Group Theory

We can equip the set of integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}\,.$$

with the addition operation $+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ on ordered pair of integers:

$$(a, b) \longmapsto a + b\,.$$

The operation above is the usual sum of integers. One can check that this operation satisfies important properties which turn $\mathbb{Z}$ into an algebraic structure called a *group*.

Definition 1. *A* group *is a set G equipped with a binary operation $\cdot$, that is, a function $\cdot : G \times G \longrightarrow G$ which satisfies the following properties.*

1 ***Associativity**:*
For all $a, b, c \in G$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)\,.$$

2 ***Existence of an Identity Element:***
There exists an element $e \in G$, called an identity element, *such that, for every $g \in G$,*

$$g \cdot e = e = e \cdot g\,,$$

3 ***Existence of an Inverse:***
For each $g \in G$, there exists an element $h \in G$, called an inverse *of g, such that*

$$g \cdot h = e = h \cdot g\,.$$

[1]Isaac Lee is a junior student at Brentwood School, Los Angeles, CA.

Usually, a group G as above is denoted by $(G, \cdot, e)$ to emphasize the group operation and the identity element that G is equipped with. When there is no risk of confusion, $(G, \cdot, e)$ will be simply denoted by G.

The image of an ordered pair (a, b) via the operation $\cdot$ is denoted by $a \cdot b$ (or sometimes simply by ab) in place of $\cdot(a, b)$. This is because a group operation should remind the reader of the usual multiplication of numbers. Indeed, as we are going to see, multiplication of numbers defines a group operation on suitable sets of numbers. However, the function $\cdot$ is not necessarily the usual multiplication operation for numbers; it can be one of many different operations.

The identity element of a group G, as above, is unique. More precisely, if $e' \in G$ satisfies the same property as the identity element e, then $e = e'$. This can be checked as follows. As e is an identity element, we must have $e \cdot e' = e'$. Since e' is also an identity element, we have $e \cdot e' = e$. Thus, $e = e \cdot e' = e'$, showing that the identity element is unique.

Similarly, for every element $g \in G$, there exists a unique inverse. The proof of this fact is quite simple and is therefore left as an exercise for the reader. This makes the following definition well-defined.

Definition 2. *The inverse of any element g of a group G is denoted by the symbol g^{-1}.*

Example 1. The set $\mathbb{Z}$ equipped with the usual addition operation $\cdot = +$ is a group with identity element $e = 0$. The inverse of an element $n \in \mathbb{Z}$ is $n^{-1} = -n$. Addition of integers also satisfies

$$a + b = b + a\,,$$

for every $a, b \in \mathbb{Z}$, so $\mathbb{Z}$ is an example of an abelian group, defined below.

Definition 3. *A group $(G, \cdot, e)$ is* abelian *if, for all $a, b \in G$,*

$$a \cdot b = b \cdot a\,.$$

Abelian groups are named after early 19th century mathematician Niels Henrik Abel and they are important because the order in which the "multiplication" of elements is performed does not matter.

Groups arise in a very natural way in mathematics. Here are common examples.

Example 2. Let $(\mathbb{Q}, +, 0)$ denote the set of fractions of the form m/n, where m and $n \neq 0$ are integers, equipped with the addition operation $+$ and the identity element 0. This group is abelian because the sum of two fractions does not change if you switch their order when adding them. Similarly, the set of real numbers $\mathbb{R}$, equipped with the usual addition $+$ of numbers and identity element 0, is an abelian group.

Example 3. Let $G = \mathbb{R}^\times$ be the set of non-zero real numbers. The usual multiplication of numbers, $\cdot = \times$, defines a binary operation on G. With this operation and the identity element $e = 1$, G is an abelian group because multiplying two real numbers always gives you the same product no matter in which order you multiply them.

Example 4. The set $\mathbb{N}$ consisting of positive integers $0, 1, 2, \ldots$ equipped with the operation $+$ is not a group since only the element 0 has an inverse.

In order to introduce the next example, which is very important in group theory, we remind the reader that a function of sets $f : X \longrightarrow Y$ is bijective if and only if for every $y \in Y$ there exists a unique element $x \in X$ such that $y = f(x)$.

Example 5. Let $\underline{n} = \{1, 2, \ldots, n\}$ where n is a positive integer. The set of bijective functions on $\underline{n}$,

$$S_n = \{f : \underline{n} \to \underline{n} \ : \ f \textit{ is bijective}\},$$

equipped with the operation $\cdot$ given for every $f, g \in S_n$ by

$$g \cdot f = f \circ g$$

is a group called the *symmetric group* on n letters whose identity element is $e = \mathrm{id}_{\underline{n}}$. Here, $\circ$ is the usual composition of functions and $\mathrm{id}_{\underline{n}}$ is the identity function on $\underline{n}$. The elements of S_n are often called *permutations*. It is useful to note that $|S_n|$ letters is $n!$. Indeed, a bijective function from $\underline{n}$ to itself is just a way of ordering n elements.

In what follows, if n is a positive integer and $a_1, \ldots, a_k \in \underline{n}$ where $k \leq n$, then

$$(a_1 \cdots a_k) \in S_n$$

will denote the bijective function on $\overline{n}$ given by

$$a \longmapsto \begin{cases} a_{i+1} & \textit{if } a = a_i \textit{ and } i < k \\ a_1 & \textit{if } a = a_k \\ a & \textit{if } a \neq a_1, \ldots, a_k \,. \end{cases}$$

A function as above is called a *k-cycle*. Two cycles $(a_1 \cdots a_k), (b_1 \cdots b_h) \in S_n$ are *disjoint* if $a_i \neq b_j$ for all $i = 1, \ldots, k$ and $j = 1, \ldots, h$. As an exercise, the reader might show that every permutation of the symmetric group S_n can be written as a product of disjoint cycles. The reader is also invited to show that S_n is abelian if and only if $n = 2$.

Definition 4. *Let $(G, \cdot, e)$ be a group. A non-empty subset H of G is a subgroup of G if*

1 ***Closure under Products**: For all $x, y \in H$,*

$$x \cdot y \in H \,.$$

2 ***Closure under Inverses**: For all $x \in H$,*

$$x^{-1} \in H \,.$$

Example 6. The set of integers $(\mathbb{Z}, +, 0)$ under addition is a subgroup of the group $(\mathbb{Q}, +, 0)$ which is, in turn, a subgroup of the group of real numbers $(\mathbb{R}, +, 0)$.

Note that if H is a subgroup of a group $(G, \cdot, e)$, then H must contain the identity element e. Note also that every subgroup H of a group G is itself a group.

Definition 5. *The group consisting of just the identity element e is commonly known as the* trivial group*. Furthermore, if G is a group with identity e, then the trivial group is a subgroup of G and is therefore called the* trivial subgroup *of G.*

For any group $(G, \cdot, e)$ and any element $x \in G$, define the kth power of x as follows for each integer k:

$$x^k = \begin{cases} \overbrace{x \cdots x}^{k} & \text{if } k \geq 0 \\ e & \text{if } k = 0 \\ \underbrace{x^{-1} \cdots x^{-1}}_{|k|} & \text{if } k < 0\,. \end{cases}$$

Definition 6. *Let G be a group and H be a subgroup of G. If there exists $x \in G$ such that*

$$H = \{x^k \,:\, k \in \mathbb{Z}\} \subseteq G\,,$$

then H is a cyclic *subgroup of G* generated *by x. Note that $e = x^0$ is the identity element and that the inverse of $x^k \in H$ is x^{-k}.*

Example 7. Any group G of cardinality less than or equal to $n = 3$ is cyclic. This obvious when $n \leq 2$, so let us show the case $n = 3$. Let $G = \{e, x, y\}$. We are going to show that G is cyclic group generated by x, or in other words, that $y = x^2$.

Since neither x nor y is the identity element e, it follows that $x \cdot y \neq x$ and $x \cdot y \neq y$. As $x \cdot y \in G$, we must therefore have $x \cdot y = e$.

Suppose that $x^2 = e$; then $x = x \cdot e = x \cdot (x \cdot y) = x^2 \cdot y = e \cdot y = y$, a contradiction. Therefore, $x^2 \neq e$. If $x^2 = x$, then $x = x \cdot e = x \cdot (x \cdot y) = x^2 \cdot y = x \cdot y = e$, a contradiction. Therefore, $x^2 \neq x$. Since x^2 is neither e nor x, we see that x^2 must equal y.

The example above shows that every group of order 3 can be thought as the cyclic subgroup of S_3 generated by the 3-cycle $(123) \in S_3$.

Example 8. A Rubik's Cube is a cube with 6 faces: up, left, front, right, back and down. Each face consists of 9 coloured squares called *facets*. note that in a Rubik's Cube we have 54 facets; see Figure 1. An *elementary cube move* rotates one of the 6 faces: $90°$, $180°$, $270°$, or $360°$ (the face we are rotating goes back to its initial position). A *cube move* is a sequence of elementary cube moves. As an elementary cube move does not change the position of centre facets, any cube move, being just a sequence of elementary cube moves, does the same.

Now we describe how to turn the set of cube moves into a group. First, number the facets, excluding the centre facets of each face, of the cube with numbers from 1 to 48. Then, note that a cube move corresponds to a bijective function $\underline{48} \to \underline{48}$. This shows that the set of cube moves is a subset of the symmetric group on 48 letters. In other words, each elementary cube move corresponds to a permutation of the number labels, and each cube move is a combination of these permutations. The composition of two

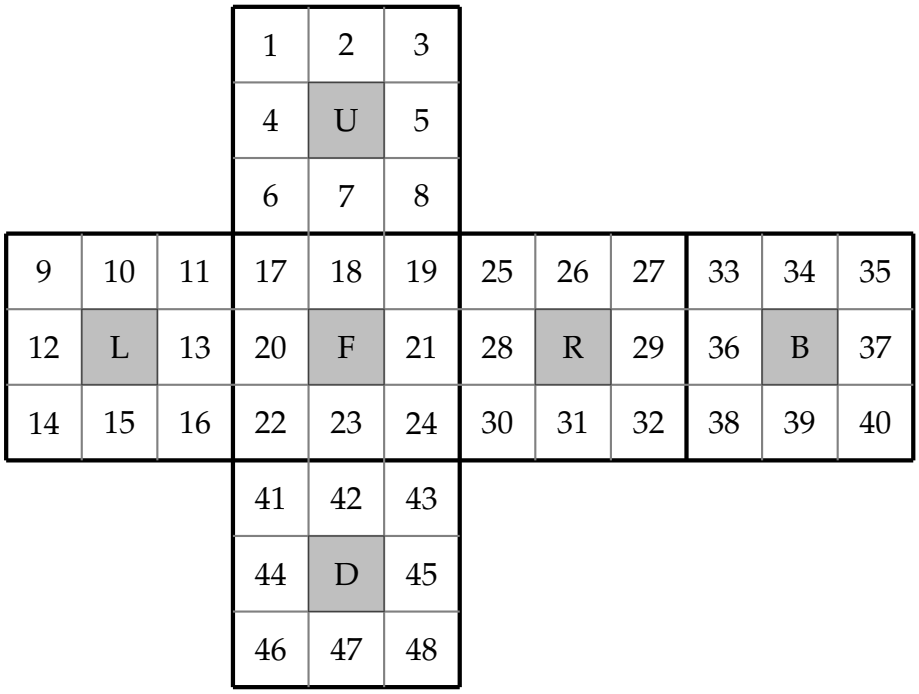

Figure 1: Numeration of the facets on a Rubik's Cube.

cube moves is still a cube move because it will still end up being a combination of elementary cube moves. Similarly, the inverse of a cube move is still a cube move, since, again, it is just a composition of elementary cube moves. Therefore, if we equip the set of cube moves with the operation $\cdot$ being the composition of cube moves, meaning one cube move performed after another, then we obtain a subgroup of S_{48}, and hence, a group. This group is called the *Rubik's Cube Group*.

Definition 7. *The centre of a group G is the subgroup*

$$Z(G) = \{z \in G : z \cdot g = g \cdot z \text{ for all } g \in G\}\,.$$

Note that a group G is abelian if and only if $G = Z(G)$.

Example 9. The centre of the symmetric group S_n is S_n itself if $n = 2$ and the trivial subgroup $\{\mathrm{id}_{\underline{n}}\} \subseteq S_n$ if $n > 2$.

To show the latter, suppose that $Z(G)$ contains an element $t \neq \mathrm{id}_{\underline{n}}$. Then there are at least two distinct elements $a, b \in$ such that $t(a) = b$. We also know that $c = t(b)$ is different from both a and b. This fact can be verified as follows.

On the one hand, if $c = b$, then $t(b) = c = t(a)$, so since t is bijective, we have $a = b$, which is a contradiction. On the other hand, if $c = a$, then t does not belong to centre of S_n. Indeed, since $n > 2$, there exists $s \neq a, b$, so

$$(a\,s) \cdot (a\,b) = (a\,s\,b) \neq (a\,b\,s) = (a\,b) \cdot (a\,s)\,.$$

Now, let $s \in S_n$ be the permutation interchanging b and c and fixing the other elements of $\underline{n}$. On the one hand,

$$(ts)(b) = (s \circ t)(b) = s(t(b)) = s(c) = b\,.$$

On the other hand,

$$(st)(b) = (t \circ s)(b) = t(s(b)) = t(c) \neq b\,,$$

so, since t is injective, $b = t(a)$ and $a \neq c$. This shows that if $t \in Z(S_n)$, then t must be the identity element of S_n. Thus, the centre of the symmetric group S_n is the trivial subgroup $\{id_{\underline{n}}\}$ if $n > 2$.

Definition 8. *Let $(G, \cdot, e)$ be a group and $a \in G$. The* centralizer *of $a \in G$ is the subgroup*

$$C_G(a) = \{g \in G : a \cdot g = g \cdot a\}\,.$$

Note that $C_G(a) = G$ if and only if $a \in Z(G)$.

Example 10. Let us compute the centralizer C of $(12) \in S_3$. By definition, a permutation t is contained in C if and only if t stabilises $\{1, 2\}$, i.e., if $t \circ (12) = (12) \circ t$ or, equivalently, $(12) \circ t \circ (12) = t$. Let $k \in \underline{3}$; then

$$(t \circ (12))(k) = t((12)(k)) = \begin{cases} t(2) & \text{if } k = 1 \\ t(1) & \text{if } k = 2 \\ t(3) & \text{if } k = 3\,. \end{cases}$$

Let $s = (12) \circ t \circ (12)$. We must have $s(k) = t(k)$ for every $k \in \underline{3}$, and the equation above, for $k = 3$, implies that $(12)(t(3)) = t(3)$. Therefore, t must fix 3 but the only permutations of S_3 fixing 3 are (12) and $\mathrm{id}_{\underline{3}}$. This shows that

$$C = \{\mathrm{id}_{\underline{3}}, (12)\}\,.$$

Definition 9. *Two elements $x, y \in G$ are* conjugate *if there exists an element $z \in G$ such that*

$$y = z \cdot x \cdot z^{-1}\,.$$

The subset of G consisting of elements conjugate to x is called the conjugacy class *of x. Any subgroups H and K of G are* conjugate *if there exists $g \in G$ such that*

$$H = gKg^{-1} = \{gkg^{-1} \ : \ k \in K\}\,.$$

One can check that if H and K as above are conjugate subgroups of G, then $|H| = |K|$.

Definition 10. *A subgroup N of G is* normal, *and we write $N \trianglelefteq G$, if $gng^{-1} \in N$ for all $g \in G$ and $n \in N$.*

Note that if H is a subgroup of an abelian group G, then H is automatically normal. Indeed, $g \cdot h \cdot g^{-1} = (g \cdot g^{-1}) \cdot h = h \in H$ for all $g \in G$ and $h \in H$.

Example 11. Let G be a group and Z be its centre. The centre Z is a normal subgroup of G. Indeed, if $g \in G$ and $z \in Z$, then since z commutes with every element of G, we have

$$(g \cdot z \cdot g^{-1}) = z \in Z\,.$$

Example 12. The subgroup $N = \{\mathrm{id}_{\underline{3}}, (123), (132)\}$ of S_3 is normal, since $(sts^{-1}) \in N$ for all $t \in N$ and $s = (ij) \in S_3$ with distinct $i, j \in \underline{3}$.

Definition 11. *Let N be a subgroup a group G. The* right coset *of N in G associated to g is*

$$Ng = \{ng : n \in N\}\,.$$

The set of right cosets of N in G is denoted by $N\backslash G$.

If G is finite, then the cardinality of the set of right cosets of N in G is

$$|N\backslash G| = \frac{|G|}{|N|}\,.$$

This identity can be proven by *Lagrange's Theorem*.

Theorem 12 (Lagrange)**.** *Let H be a subgroup of a finite group G. Then $|H|$ divides $|G|$.*

This theorem is fundamental in group theory and its proof can be found in most Abstract Algebra textbooks, such as [2].

Example 13. Let G be a finite group with identity element e, and let $x \in G$. Let n be the least positive integer such that $x^n = e$. We already know that x generates a cyclic subgroup of G, with cardinality n. By Lagrange's Theorem, we know that n divides $|G|$.

Example 14. The Rubik's Cube Group is a subgroup of the symmetric group on 48 letters S_{48}, so its cardinality divides the cardinality of S_{48}. Indeed, the cardinality of the Rubik's Cube Group is $43,252,003,274,489,856,000 = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11^1$, and the cardinality of S_{48} is $48!$. Lagrange's Theorem ensures that the first divides the latter.

If N is a normal subgroup of $(G, \cdot, e)$, then one can check that the operation $\cdot$ on $N\backslash G$, defined for all $g, h \in G$ by

$$(Ng) \cdot (Nh) = N(gh)$$

turns $N\backslash G$ into a group with identity element Ne.

Definition 13. *Let N be a normal subgroup of a group G. The quotient group associated to N is $N\backslash G$, equipped with the operation and the identity element showed above.*

Example 15. Let $n \geq 2$ be an integer. As $\mathbb{Z}$ is abelian, the cyclic subgroup

$$n\mathbb{Z} = \{nk \ : \ k \in \mathbb{Z}\}$$

generated by n is normal. The quotient group $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is called the *group of integers modulo n*. Usually, the right cosets $n\mathbb{Z} + x$ of $n\mathbb{Z}$ in $\mathbb{Z}$ are denoted by $[x]_n$. Note that $[x]_n = [y]_n$ if and only if $x - y$ is an integer multiple of n.

Lemma 14. *Let Z be the centre of a finite group G. If $Z\backslash G$ is cyclic, then G is abelian.*

Proof. As $Z\backslash G$ is cyclic, there exists $x \in G$ such that

$$Z\backslash G = \{Z \cdot x^k \ : \ k \in \mathbb{Z}\}\,,$$

so every element $g \in G$ can be written as $g = z \cdot x^k$ for suitable $z \in Z$ and $k \in \mathbb{Z}$. So, if $g, h \in G$, then there exist $z, w \in Z$ and $r, s \in \mathbb{Z}$ such that $g = x^r \cdot z$ and $h = w \cdot x^s$. Thus,

$$\begin{array}{rcll} g \cdot h & = & (z \cdot x^r) \cdot (w \cdot x^s) & \\ & = & z \cdot (x^r \cdot w) \cdot x^s & \textit{(Associativity)} \\ & = & z \cdot (w \cdot x^r) \cdot x^s & (w \in Z) \\ & = & (w \cdot z) \cdot x^{s+r} & \textit{(Associativity)} \ + \ (z, w \in Z) \\ & = & w \cdot (x^s \cdot z) \cdot x^r & \textit{(Associativity)} \ + \ (z \in Z) \\ & = & (w \cdot x^s) \cdot (z \cdot x^r) & \textit{(Associativity)} \\ & = & h \cdot g\,. & \end{array}$$

The chain of equalities above shows that $G = Z$. □

If $x \in G$, then there is a bijective correspondence

$$C_G(x)/G \longrightarrow [x] \subseteq G\,,$$

where $[x]$ is the subset of G consisting of elements conjugate to x. Indeed, the association

$$C_G(x) \cdot g \longmapsto gxg^{-1}$$

defines a bijective function. In particular, if G is a finite group, then

$$\big|[x]\big| = \frac{|G|}{|C_G(x)|}\,.$$

Definition 15. *Let G be a group and let $x \in G$. The* conjugacy class *of x in G is the set*

$$[x] = \{gxg^{-1} \ : \ g \in G\}\,.$$

Two elements $x, y \in G$ are equivalent *if there exists $g \in G$ such that $y = g \cdot x \cdot g^{-1}$.*

If $x, y \in G$, then their conjugacy classes $[x]$ and $[y]$ are either equal or disjoint, i.e. $[x] = [y]$ or $[x] \cap [y] = \emptyset$. To see this, suppose that $z \in [x] \cap [y]$. Then there exist $s, t \in G$ such that $sxs^{-1} = z = tyt^{-1}$; therefore,

$$y = (t^{-1}s)x(t^{-1}s)^{-1}$$

which means that $y \in [x]$; hence, $[x] = [y]$.

Note that the cardinality of the conjugacy class of $z \in G$ is equal to 1 if and only if $z \in Z(G)$. Therefore, if G is a finite group, then there exist finitely many elements $x_1, \ldots, x_t \in G$ such that

$$G = Z(G) \cup [x_1] \cup \cdots [x_t]\,.$$

Since $Z(G), [x_1], \ldots, [x_t]$ are disjoint,

$$|G| = |Z(G)| + \sum_{i=1}^{t} \big|[x_i]\big|\,.$$

Lemma 16. *If G is a finite group and $x_1, \ldots, x_k \in G$ are representatives of its conjugacy, then*

$$k \leq \frac{5}{8} |G| .$$

Proof. By renumbering the elements $x_1, \ldots, x_k$, we can assume that $x_1, \ldots, x_t$ with $t \leq k$ are all the representatives of the conjugacy relation which do not belong to $Z(G)$. Then

$$|G| = |Z(G)| + \sum_{i=1}^{t} \left| [x_i] \right| .$$

The conjugacy classes of $x_1, \ldots, x_t$ are nontrivial, so $\left| [x_i] \right| \geq 2$ for $i = 1, \ldots, t$. Therefore,

$$\frac{|G| - |Z(G)|}{2} \geq t ,$$

so

$$k = t + |Z(G)| \leq \frac{|G| + |Z(G)|}{2} .$$

By assumption, G is not abelian, so thanks to Lemma 14, the cardinality of $|G|/|Z(G)|$ must be at least 4, because groups of size 3 or smaller are cyclic, and in particular, abelian. This shows that $|Z(G)| \leq |G|/4$. Combining this inequality with the inequality above, we obtain

$$k \leq \frac{5}{8} |G| .$$

□

Definition 17. *For a finite group $(G, \cdot, e)$, define*

$$\text{Comm}(G) = \{(a, b) \in G \times G : a \cdot b = b \cdot a\} .$$

3 The 5/8 Theorem

Now we are finally ready to state and prove the main theorem of this paper. More precisely, we show that the probability that two randomly chosen elements of a finite non-abelian group commute is bounded by $5/8$. This theorem was first proven by Paul Erdős and Pál Turán [4].

Theorem 18. *Let G be a finite non-abelian group. Then the probability that two randomly chosen elements in G commute is*

$$Pr(G) \leq \frac{5}{8} .$$

Proof. First note that the probability that two randomly chosen elements of G commute with each other is

$$Pr(G) = \frac{|\text{Comm}(G)|}{|G \times G|} ,$$

Note that the subset of elements of G which commute with any given element x is exactly the centralizer $C_G(x)$. Therefore,

$$|\text{Comm}(G)| = \sum_{x \in G} |C_G(x)| \,.$$

Now note that if two elements $x, y \in G$ are conjugate, then their centralizers $C_G(x)$ and $C_G(y)$ are conjugate subgroups. In particular, they have the same number of elements. This means that if $y_1, \ldots, y_n$ are all the elements in the conjugacy class of x, then

$$\sum_{i=1}^{n} |C_G(y_i)| = n|C_G(x)| \,.$$

The number of elements which are conjugate to an element $x \in G$ is $|G|/|C_G(x)|$. Let $x_1, \ldots, x_k$ be representatives of the conjugacy classes in G. Then

$$|\text{Comm}(G)| = \sum_{i=1}^{k} |C_G(x_i)| \frac{|G|}{|C_G(x)|} = k|G| \,.$$

The equation above along with Lemma 16 shows that

$$Pr(G) \leq \frac{5}{8} \,. \qquad \square$$

$\cdot$	e	ρ	ρ^2	τ	$\rho\tau$	$\rho^2\tau$
e	e	ρ	ρ^2	τ	$\rho\tau$	$\rho^2\tau$
ρ	ρ	ρ^2	e	$\rho\tau$	$\rho^2\tau$	τ
ρ^2	ρ^2	e	ρ	$\rho^2\tau$	τ	$\rho\tau$
τ	τ	$\rho^2\tau$	$\rho\tau$	e	ρ^2	ρ
$\rho\tau$	$\rho\tau$	τ	$\rho^2\tau$	ρ	e	ρ^2
$\rho^2\tau$	$\rho^2\tau$	$\rho\tau$	τ	ρ^2	ρ	e

Figure 2: Multiplication table for S_3

We now present an example to help convince the reader that the theorem is true.

Example 16. Let $G = S_3$. To compute $Pr(G)$, we need to count the number of pairs of permutations $(\alpha, \beta) \in G \times G$ such that $\alpha\beta = \beta\alpha$. To do this easily, one can create a *Cayley table* describing the structure of $G = S_3$. The Cayley table of a finite group G, named after the 19th century British mathematician Arthur Cayley, is just a list of all the possible products of all the group's elements. The Cayley table for S_3 is given in Figure 2, where each element of S_3 is expressed as a product of the elements $\rho = (1\,2\,3)$ and $\tau = (1\,2)$. Using this table, we can determine the commuting probability of the symmetric group S_3. In particular, the table shows that there are 18 of the 36 ordered pairs of elements that commute, so $Pr(G) = 18/36 = 1/2 < 5/8$.

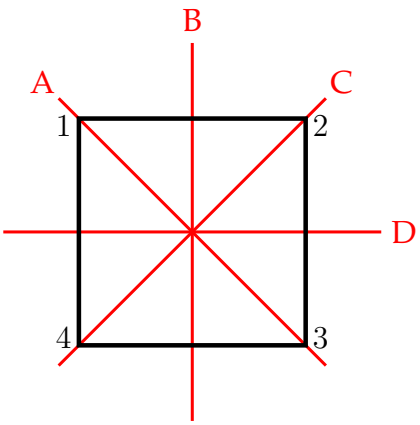

Figure 3: The Dihedral Group D_4

$\cdot$	e	ρ	ρ^2	ρ^3	σ_A	σ_B	σ_C	σ_D
e	e	ρ	ρ^2	ρ^3	σ_A	σ_B	σ_C	σ_D
ρ	ρ	ρ^2	ρ^3	e	σ_D	σ_A	σ_B	σ_C
ρ^2	ρ^2	ρ^3	e	ρ	σ_C	σ_D	σ_A	σ_B
ρ^3	ρ^3	e	ρ	ρ^2	σ_B	σ_C	σ_D	σ_A
σ_A	σ_A	σ_B	σ_C	σ_D	e	ρ	ρ^2	ρ^3
σ_B	σ_B	σ_C	σ_D	σ_A	ρ^3	e	ρ	ρ^2
σ_C	σ_C	σ_D	σ_A	σ_B	ρ^2	ρ^3	e	ρ
σ_D	σ_D	σ_A	σ_B	σ_C	ρ	ρ^2	ρ^3	e

Figure 4: Multiplication table for D_4

Example 17. The dihedral group D_4 is the group consisting of symmetries of the square. More precisely, it is the smallest group containing the rotational and reflectional symmetries about the symmetries axes of the square, as shown in Figure **??**. The dihedral group D_4 can be identified as a subgroup of the symmetric group S_4, since the symmetries of the square can be identified as bijective functions of the set $\underline{4}$ as follows.

We have four rotational symmetries ρ, ρ^2, ρ^3 and ρ^4 (the identity map), generated by the a rotation of the square ρ of $\pi/2$ degrees corresponding to the cycle $(1\,2\,3\,4)$. Note that ρ^4 is equivalent to the identity element e. Then, we have the reflection σ_A about the A-axis corresponding to the cycle $(2\,4)$, the reflection σ_B about the B-axis corresponding to the permutation $(1\,2)(3\,4)$, the reflection σ_C about the C-axis corresponding to the cycle $(1\,3)$ and finally, the reflection σ_D about the D-axis corresponding to the permutation $(1\,4)(2\,3)$.

By the multiplication table in Figure 4, the number of pairs of elements which commute in D_4 is 40, which is exactly $5/8$ of the total number of pairs, showing that the upper bound in the $5/8$ Theorem is realized by this group.

4 Discussion

The bound found in the theorem can be refined for some specific classes of nonabelian finite groups. For instance, this can be done for nonabelian finite simple groups.

Definition 19. *A group $(G, \cdot, e)$ is* simple *if its normal subgroups of G are just $\{e\}$ and G.*

Example 18. Let G be the cyclic subgroup generated by the cycle $(1\,2\,3) \in S_3$. The group G is simple. Indeed, the only subgroups of G are $\{\mathrm{id}_{\underline{3}}\}$ and G itself.

Example 19. The group S_3 is not simple. Indeed, the subgroup G of the example above is normal, as one can easily check by looking at the multiplication table of Figure 2.

One can show that the bound for the commuting probability can be refined for non-abelian finite simple groups, as the following theorem demonstrates.

Theorem 20. *If G is a non-abelian finite simple group, then*

$$Pr(G) \leq \frac{1}{12}.$$

Proof. See [3]. □

In this case too, one can prove that the bound of the theorem above is sharp. The simplest example of a group where this bound is achieved is the alternating group A_5.

Example 20. Given a permutation $\sigma \in S_n$, one can show that this can be decomposed as a product of transpositions. This follows from the fact that every cycle $(a_1 \cdots a_k)$ can be written as $(a_1\, a_2) \cdot (a_1\, a_3) \cdots (a_1\, a_k)$. One can check that the parity of the number of transpositions in the product decomposition of a permutation does not depend on the particular decomposition, so we can say that a permutation is *even* if the number of transpositions in one of its product decomposition is even and *odd* otherwise. The alternating group A_n is the subgroup of S_n generated by even permutations. Clearly, every 3-cycle is even, so A_n is generated by all 3-cycles in S_n.

In general, the cardinality of A_n is $\frac{1}{2}n!$. As we said above, the simplest example where the upper bound of the $5/8$ Theorem for simple groups is achieved is A_5. However, we do not include the multiplication table of A_5 since the cardinality of A_5 is 60.

As we saw above, the $5/8$ Theorem can be refined for finite, nonabelian simple groups and many other classes of groups. In the future, we hope to be able to refine the $5/8$ Theorem for other classes of groups like symmetric groups.

Acknowledgements

I would like to thank Vincenzo Zaccaro for teaching me this material and helping me overall with this paper. I would also like to thank Dr. Thomas Britz and Dr. Arnaud Brothier for overlooking my paper and guiding me in the right directions.

References

[1] W.H. Gustafson, What is the probability that two group elements commute?, *The American Mathematical Monthly* **80** (1973), 1031–1034.

[2] W.R. Scott, *Group Theory*, Courier Corporation, 2012.

[3] Problems for Solution, *Canadian Mathematical Bulletin* **6** (1963), pp. 302.

[4] P. Erdős and P. Turán, On some problems of a statistical group-theory. IV., *Acta Mathematica Academiae Scientiarum Hungaricae* **19** (1968), 413–435.