Fall 2021

Finite Groups in Which the Number of Cyclic Subgroups is 3/4 the Order of the Group

James Alexander Cayley
Cayley101@live.missouristate.edu

FINITE GROUPS IN WHICH THE NUMBER OF CYCLIC SUBGROUPS IS 3/4 THE ORDER OF THE GROUP

A Master's Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Mathematics

By

James Alexander Cayley

December 2021

FINITE GROUPS IN WHICH THE NUMBER OF CYCLIC SUBGROUPS IS 3/4 THE ORDER OF THE GROUP

Mathematics

December 2021

Master of Science

James Alexander Cayley

ABSTRACT

Let G be a finite group, $c(G)$ denotes the number of cyclic subgroups of G and $\alpha(G) = c(G)/|G|$. In this thesis we go over some basic properties of alpha, calculate alpha for some families of groups, with an emphasis on groups with $\alpha(G) = 3/4$, as all groups with $\alpha(G) > 3/4$ have been classified by Garonzi and Lima (2018). We find all Dihedral group with this property, show all groups with $\alpha(G) = 3/4$ have at least $|G|/2 - 1$ involutions, and discuss existing work by Wall (1970) and Miller (1919) classifying all such groups.

KEYWORDS: group, subgroup, cyclic, nilpotent, abelian, involutions

FINITE GROUPS IN WHICH THE NUMBER OF CYCLIC SUBGROUPS IS 3/4 THE ORDER OF THE GROUP

By

James Alexander Cayley

A Master's Thesis
Submitted to the Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree of Master of Science, Mathematics

December 2021

Approved:

Richard Belshoff, Ph.D., Thesis Committee Co-Chair

Les Reid, Ph.D., Thesis Committee Co-Chair

Cameron Wickham, Ph.D., Thesis Committee Member

Julie Masterson, Ph.D., Dean of the Graduate College

ACKNOWLEDGEMENTS

I would like to thank all of the faculty and staff members who have supported me during my Master's. In particular, I'd like to thank Dr. Reid and Dr. Belshoff for all of their support and guidance, which they extended to me before I'd even considered becoming a student at MSU.

I would like to thank Dr. Marc Rieffel and Dr. Silvain Rideau for igniting my love for abstract algebra, and Dr. David Lloyd and Dr. Matthew Turner for giving me the opportunity to get involved in math research as an undergrad. I'd also like to thank Sebastien Zany, Max Hodak, Laura Deming, Ethan Perlstein, Sergio Baranzini, Dr. Apoorva Khare, Juan Ignacio Restrepo, Titu Andreescu, and Virgil Griffith for helping me nurture my passion for mathematics and science during my early teens.

I would like to thank Danielle Strachman and Rodrigo Cano for being my cheerleaders for almost a decade. I'd also like to thank my friends and my communities; in particular Gendered Intelligence, PROMO, Springfield Ballet, Orla Gartland's Secret Demo Club, Lee, Athena, Camillo, and Nat. Your support and encouragement have been invaluable.

Finally, I would like to thank my two favorite people in the world; Chiara Citterio for being an amazing friend, and Jane Henke for helping me see how strong I can be.

I dedicate this thesis to my trans siblings.

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

A group is a set closed under a binary operation which is associative, contains an identity element, and every element has an inverse. Cyclic groups have the property that the group can be generated by a single element. For example, the group of integers under addition can be generated by the element 1.

Denoting the number of cyclic subgroups of a group G by $c(G)$, we let $\alpha(G) = c(G)/|G|$. In 2018 Garonzi and Lima published a paper classifying all groups with $\alpha(G) > 3/4$ [1], and Tărnăuceanu and Lazorec published a paper exploring some nilpotent groups with $\alpha(G) = 3/4$ [2]. It is therefore a natural question to wonder if a full classification of groups with $\alpha(G) = 3/4$ can be obtained.

In Section 2 we go over notation and preliminary group theory results. Section 3 contains an overview of some basic properties of alpha and a formula to compute the number of cyclic subgroups of a group, and in Section 4 we compute $\alpha(G)$ for various groups and families of groups. In Section 5 we show some preliminary explorations of groups with $\alpha(G) = 3/4$, including all dihedral groups with this property, and we show that all nilpotent groups with $\alpha(G) = 3/4$ are 2-groups. Finally, in Section 6 we show all groups with $\alpha(G) = 3/4$ have $n_2 \geq |G|/2 - 1$, discuss Wall's families of groups with many involutions, Miller's first family of groups with $|G|/2 - 1$ involutions, and show that if $n_8(G) \geq 1$ and $\alpha(G) = 3/4$ then $G \cong D_{16} \times C_2^n$.

2. PRELIMINARIES AND BASIC RESULTS

Remark 2.1. The cyclic group of order n is denoted C_n.

Definition 2.2. An involution is a group element of order 2.

Definition 2.3. The center of G is the subgroup of G containing elements that commute with all elements of the group. The center is denoted $Z(G)$.

Fact 2.4. The order of $(g, h) \in G \times H$ is the least common multiple of the order of g in G and the order of h in H.

Remark 2.5. As usual, if N is a normal subgroup of G, we write $N \trianglelefteq G$.

Definition 2.6. The symmetric group, denoted S_n, is the group of permutations of the numbers $\{1, .., n\}$. Its elements can be represented as a product of disjoint cycles, where the cycle $(s_1 s_2 ... s_n)$ denotes the permutation sending s_1 to s_2, s_2 to s_3, ... , and s_n to s_1.

Example 2.7. The following permutation is an element of S_9

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 2 & 1 & 8 & 6 & 4 & 9 & 5 \end{pmatrix}.$$

In cycle notation it can be written as $(174)(23)(589)(6) = (174)(23)(589)$, the one-cycle is omitted by convention.

Definition 2.8. Dihedral groups, denoted D_{2n} are the groups of symmetries of a regular n-gon. D_{2n} has order $2n$ and can be generated by the following relations:

$$\langle r, s | r^n = s^2 = e, rs = sr^{-1} \rangle.$$

All of the powers of r represent rotations and the elements containing an s represent reflections.

Definition 2.9. Let G be a group and $a, b \in G$. a and b are conjugate if there exists an element in G such that $gag^{-1} = b$. The conjugacy class of a is $\{gag^{-1} | g \in G\}$. We denote the number conjugacy classes in G by $k(G)$.

Definition 2.10. The normalizer of S in the group G is defined as

$$N_G(S) = \{g \in G | gS = Sg\} = \{g \in G | gSg^{-1} = S\}.$$

Theorem 2.11. Sylow's theorems Suppose $|G| = p^n m$ with $n > 0$ and p doesn't divide m. Then

1. There exists a subgroup of G of order p^n, called a Sylow p-subgroup of G.

2. All Sylow p-subgroups of G are conjugate to each other. That is, if H and K are Sylow p-subgroups of G then there exists an element $g \in G$ with $g^{-1}Hg = K$.

3. Let n_p be the number of Sylow p-subgroups of G. Then the following hold:

   - n_p divides m which is the index of the Sylow p-subgroup in G
   - $n_p \equiv 1 \mod p$
   - $n_p = |G : N_G(P)|$ where P is any Sylow p-subgroup of G and N_G denotes the normalizer.

Definition 2.12. The commutator of a and b, denoted $[a, b]$ is defined as $[a, b] = aba^{-1}b^{-1}$.

Definition 2.13. The number of cyclic subgroups of order k in G will be denoted $n_k(G)$.

3. SOME PROPERTIES OF ALPHA

Definition 3.1. We define

$$\alpha(G) = \frac{c(G)}{|G|},$$

where $c(G)$ is the number of cyclic subgroups of G. Note that $0 < \alpha(G) \leq 1$ (see Remark 4.4).

Definition 3.2. Euler's totient function, denoted $\varphi(n)$, calculates how many positive integers less than or equal to n are relatively prime to n. A formula is

$$\varphi(n) = n \prod_{\substack{p|n \\ p \text{ prime}}} (1 - \frac{1}{p}).$$

Proposition 3.3. The number of cyclic subgroups of a group G is given by

$$c(G) = \sum_{x \in G} \frac{1}{\varphi(|x|)}.$$

Proof. Let $\langle a \rangle \leq G$ have order n. Then this group is generated by a^i with i coprime to n. Hence

$$c(G) = \sum_{\langle a \rangle \leq G} 1 = \sum_{\langle a \rangle \leq G} \frac{\varphi(|a|)}{\varphi(|a|)} = \sum_{\langle a \rangle \leq G} \frac{\sum_{x, \langle x \rangle = \langle a \rangle} 1}{\varphi(|a|)} = \sum_{\langle a \rangle \leq G} \sum_{x, \langle x \rangle = \langle a \rangle} \frac{1}{\varphi(|x|)} = \sum_{x \in G} \frac{1}{\varphi(|x|)}.$$

$\square$

Example 3.4. S_3**: the group of permutations of** $\{1,2,3\}$

The order of S_3 is $3! = 6$. It has the following elements: $\{(1),(12),(13),(23),\ (123),(132)\}$ where (1) is the identity element. The order of an element of S_n is the least common multiple of the length of the cycles hence the elements have order $1,2,2,2,3,3$ respectively. The cyclic subgroups of S_3 are: $\langle(1)\rangle, \langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$and $\langle(123)\rangle$. Hence as $|S_3| = 6$ and $c(S_3) = 5$, it follows that $\alpha(S_3) = 5/6$. Using the formula given in Proposition 3.3 the same result is obtained:

$$c(S_3) = 1 + \frac{1}{1} + \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{2} = 5,$$

so $\alpha(S_3) = 5/6$.

Proposition 3.5. If A and B are groups of coprime orders then $c(A \times B) = c(A)c(B)$ and hence $\alpha(A \times B) = \alpha(A)\alpha(B)$.

Proof.

$$c(A \times B) = \sum_{(x,y)\in A\times B} \frac{1}{\varphi(|(x,y)|)}$$

We have $|x|$ divides $|A|$ and $|y|$ divides $|B|$. $|A|$ and $|B|$ are coprime, so $|x|$ and $|y|$ are also coprime and $\varphi(|x||y|) = \varphi(|x|)\varphi(|y|)$. Furthermore, since $|A|$ and $|B|$ are coprime, $|(x,y)| = \operatorname{lcm}(|x|,|y|) = |x||y|$. Hence

$$\sum_{(x,y)\in A\times B} \frac{1}{\varphi(|(x,y)|)} = \sum_{x\in A, y\in B} \frac{1}{\varphi(|x|)\varphi(|y|)} = \sum_{x\in A} \frac{1}{\varphi(|x|)} \sum_{x\in B} \frac{1}{\varphi(|x|)} =$$

$$\sum_{x\in A\times B} \frac{1}{\varphi(|x|)} = c(A)c(B).$$

Therefore

$$\alpha(A \times B) = \frac{c(A \times B)}{|A \times B|} = \frac{c(A)c(B)}{|A||B|} = \alpha(A)\alpha(B).$$

$\square$

Proposition 3.6. If $N \trianglelefteq G$ then $\alpha(G) \leq \alpha(G/N)$. Moreover $\alpha(G) = \alpha(G/N)$ if and only if $\varphi(|g|) = \varphi(|gN|)$ for every $g \in G$, where $|gN|$ denotes the order of the element gN in the group G/N.

Proof. If a divides b then $\varphi(a) \leq \varphi(b)$, so

$$c(G/N) = \sum_{gN \in G/N} \frac{1}{\varphi(|gN|)} = \sum_{g \in G} \frac{1}{|N|\varphi(|gN|)} \geq \sum_{g \in G} \frac{1}{|N|\varphi(|g|)} = \frac{c(G)}{|N|}.$$

So

$$\alpha(G/N) = \frac{c(G/N)}{|G/N|} \geq \frac{c(G)}{|N|} \cdot \frac{1}{|G/N|} = \frac{c(G)}{|G|} = \alpha(G).$$

$\square$

Proposition 3.7. $\alpha(G) = \alpha(G \times C_2^n)$.

Proof. Let $N = \{1\} \times C_2^n$. Then let $x = (g, t) \in G \times C_2^n$. Now $|x| =$lcm$(|g|, |t|) = |g|$ or $2|g|$. Note that $|xN| = |g|$ since $(g, t)^k = (g^k, t^k) \in N = 1 \times C_2^n$ if $g^k = 1$. If $|g| = |x|$ then $\varphi(|x|) = \varphi(|xN|)$. If $|x| = 2|g|, \varphi(|x|) = \varphi(2|g|) = \varphi(2)\varphi(|g|) = \varphi(|g|)$. Hence $\alpha(G \times C_2^n) = \alpha((G \times C_2^n)/N) = \alpha(G)$ for every $g \in G$. $\square$

Corollary 3.8. If $G \cong C_2^n$, then $\alpha(G) = 1$.

Definition 3.9. A group is a core group if it does not have C_2 as a summand.

Proposition 3.10. If $\alpha(G) = \alpha(G/N)$ then N is an elementary abelian 2-group.

Proof. By Proposition 3.7 if $n \in N, \varphi(|n|) = \varphi(|nN|) = \varphi(|N|) = \varphi(1) = 1$, which implies $n^2 = 1$. $\square$

4. SOME GROUPS WITH KNOWN ALPHA

Definition 4.1. The number of divisors of n, including 1 and n, is denoted $\tau(n)$. For example, the divisors of 6 are $\{1,2,3,6\}$ so $\tau(6) = 4$.

Theorem 4.2.

$$\alpha(C_n) = \frac{\tau(n)}{n}.$$

Proof. As all subgroups of C_n are cyclic and there is a subgroup corresponding to every divisor of n, so $c(G) = \tau(n)$, hence

$$\alpha(C_n) = \frac{\tau(n)}{n}.$$

□

Theorem 4.3.

$$\alpha(D_{2n}) = \frac{n + \tau(n)}{2n}.$$

Proof. There are n elements of the form $r^i s$ with $i = 1, ..., n$ in D_{2n}. Each of these elements has order two and generates one cyclic subgroup. Additionally, we have $\{1, r, ..., r^n\} \cong C_n$ which has $\tau(n)$ cyclic subgroups, hence $c(D_{2n}) = n + \tau(n)$ and

$$\alpha(D_{2n}) = \frac{n + \tau(n)}{2n}.$$

□

Remark 4.4. Since $\alpha(C_p) = 2/p$ for p prime, the bounds stated after Definition 3.1 are the best possible.

Theorem 4.5.

$$\alpha(S_4) = \frac{17}{24}.$$

Proof. To find the number of cyclic subgroups of S_4 we first look at the cycle structure, order, and number of each kind of element in S_4 (Table 1), and then apply Proposition 3.3.

Cycle Structure	Order	Number
4	4	$4!/4 = 6$
3 1	3	$4!/(3 \cdot 1) = 8$
2 2	2	$4!/(2^2 \cdot 2!) = 3$
2 1 1	2	$4!/(2 \cdot 1^2 \cdot 2!) = 6$
1 1 1 1	1	$4!/(1^4 \cdot 4!) = 1$

Table 1: Table to compute $c(S_4)$

$$c(S_4) = \frac{6}{\varphi(4)} + \frac{8}{\varphi(3)} + \frac{3}{\varphi(2)} + \frac{6}{\varphi(2)} + \frac{1}{\varphi(1)} = 3 + 4 + 3 + 6 + 1 = 17.$$

Therefore $\alpha(S_4) = 17/4! = 17/24$. $\square$

Theorem 4.6.

$$\alpha(S_5) = \frac{67}{120}.$$

Proof. We proceed as above. The cycle structures, order, and number of each kind of element in S_5 is below (Table 2). Now dividing the number of elements over φ of the order of

Cycle Structure	Order	Number
5	5	$5!/5 = 24$
4 1	4	$5!/(4 \cdot 1) = 30$
3 2	6	$5!/(3{\cdot}2) = 20$
3 1 1	3	$5!/(3{\cdot}1^2 \cdot 2!) = 20$
2 2 1	2	$5!/(2^2 \cdot 2!) = 15$
2 1 1 1	2	$5!/(2 \cdot 1^3 \cdot 3!) = 10$
1 1 1 1 1	1	$5!/(1^5 \cdot 5!) = 1$

Table 2: Table to compute $c(S_5)$

the elements we obtain

$$c(S_5) = \frac{24}{\varphi(5)} + \frac{30}{\varphi(4)} + \frac{20}{\varphi(6)} + \frac{20}{\varphi(3)} + \frac{10}{\varphi(2)} + \frac{15}{\varphi(2)} + \frac{10}{\varphi(2)} + \frac{1}{\varphi(1)} = 67$$

so $\alpha(S_5) = 67/5! = 67/120$ □

Theorem 4.7. If G is a non-abelian group of order pq, with primes $p < q$ (hence $p|q-1$), then

$$\alpha(G) = \frac{2+q}{pq}.$$

Proof. By Sylow's theorem, G has one Sylow q-subgroup. As G is non-abelian, it has q Sylow p-subgroups as if it had only one, G would be abelian. Since p and q are prime, these (and the trivial group) are the only cyclic subgroups of G, hence

$$\alpha(G) = \frac{q+2}{pq}.$$

□

Definition 4.8. The general affine group of degree 1 over $\mathbb{F}_p$ is

$$GA(1,p) = \langle a, b | a^p = b^{p-1}, bab^{-1} = a^k \rangle$$

where k has order $p-1$ in $(\mathbb{Z}_p)^\times$.

Theorem 4.9.

$$\alpha(GA(1,p)) = \frac{2 + p(\tau(p-1) - 1)}{p(p-1)}.$$

This result can be obtained using techniques similar to the ones employed above.

Proposition 4.10. Let p be a prime, then

$$\alpha(C_p^n) = \frac{p^n + p - 2}{p^n(p-1)}$$

Proof. Clearly C_p^n has one element of order 1 and $p^n - 1$ elements of order p, so

$$c(C_p^n) = 1 + \frac{p^n - 1}{p - 1}$$

and hence

$$\alpha(C_p^n) = \frac{1 + \frac{p^n - 1}{p - 1}}{p^n} = \frac{p^n + p - 2}{p^n(p-1)}$$

□

Proposition 4.11.

$$\alpha(C_4^n) = \frac{2^n + 1}{2^{n+1}}$$

Proof. Clearly C_4^n has one element of order 1, and $2^n - 1$ elements of order 2, so it has $2^{2n} - 2^n$ elements of order 4. Therefore

$$c(C_4^n) = \frac{2^{2n} - 2^n}{\varphi(4)} + \frac{2^n - 1}{\varphi(2)} + \frac{1}{\varphi(1)} = \frac{2^{2n} - 2^n}{2} + 2^n - 1 + 1 = 2^{2n-1} + 2^{n-1}.$$

So

$$\alpha(C_4^n) = \frac{2^{2n-1} + 2^{n-1}}{2^{2n}} = \frac{2^n + 1}{2^{n+1}}.$$

$\square$

Theorem 4.12. For every $1 \leq \beta \leq \beta_k$ the number of cyclic subgroups of order p^β in the finite abelian p-group

$$C_p^{\beta_1} \times \ldots \times C_p^{\beta_k}$$

is

$$g_p^k(\beta) = \frac{p^\beta h_p^{k-1}(\beta) - p^{\beta-1} h_p^{k-1}(\beta - 1)}{p^\beta - p^{\beta-1}}$$

where

$$h_p^{k-1}(\beta) = \begin{cases} p^{(k-1)\beta} & \text{if } 0 \leq \beta \leq \beta_1 \\ p^{(k-2)\beta+\beta_1} & \text{if} \beta_1 \leq \beta \leq \beta_2 \\ \ldots & \\ p^{\beta+\beta_1+\ldots+\beta_{k-1}} & \text{if} \beta_{k-1} \leq \beta \end{cases} \tag{4.1}$$

Proof. See pages 10-12 of [5]. $\square$

Proposition 4.13. Up to isomorphism all finite abelian 2-groups with $\alpha = 1/2$ are of the form $C_8 \times C_2^n$ for $n \in \mathbb{N}$.

Proof. Let $m \in \mathbb{N}$ and G be a finite abelian 2-group of order 2^m such that $\alpha(G) = 1/2$. If

$$G \cong C_{2^{d_1}} \times C_{2^{d_2}} \times ... \times C_{2^{d_k}}$$

where $1 \leq d_1 \leq d_2 \leq ... \leq d_k$ then

$$\frac{d_k + 1}{2^{d_k}} = \alpha(C_{2^{d_k}}) = \alpha(G/(C_{2^{d_1}} \times C_{2^{d_2}} \times ... \times C_{2^{d_{k-1}}} \times \{1\})) \geq \alpha(G) = \frac{1}{2}.$$

This leads to $d_k \leq 3$ and hence $\exp(G) \leq 8$. If $\exp(G) = 2$ then $G \cong C_2^k$, which implies $\alpha(G) = 1$. If $\exp(G) = 4$ then $\alpha(G) = 1/2$ leads to the following conditions:

$$\begin{cases} 2^m = 1 + n_2(G) + 2n_4(G) \\ 2^{m-1} = 1 + n_2(G) + n_4(G). \end{cases} \tag{4.2}$$

Solving for $n_2(G)$ we obtain $n_2(G) = -1$, a contradiction. Hence $\exp(G) = 8$ and

$$G \cong C_2^n \times C_4^a \times C_8^b \text{ with } a, b, n \in \mathbb{N}.$$

Note that at least one of a and b must be strictly positive or we would have $\alpha(G) = 1$.

Similarly, the following set of conditions hold:

$$\begin{cases} 2^m = 1 + n_2(G) + 2n_4(G) + 4n_8(G) \\ \\ 2^{m-1} = 1 + n_2(G) + n_4(G) + n_8(G). \end{cases} \tag{4.3}$$

The above equations imply that

$$n_4(G) + 3n_8(G) = 2^{m-1},$$

so $1 + n_2(G) = 2n_8(G)$. By Theorem 4.12 the number of cyclic subgroups of order 2 and 8 are

$$n_2(G) = 2^{n+a+b} - 1$$

and

$$n_8(G) = 2^{n+2a+2b-2}(2^b - 1)$$

respectively. Then we obtain

$$1 + n_2(G) = 2n_8(G)$$

if and only if

$$2^{n+a+b} = 2^{n+2a+2b-1}(2^b - 1)$$

if and only if

$$1 = 2^{a+b-1}(2^b - 1)$$

if and only if $a = 0$ and $b = 1$. Therefore $G \cong C_2^n \times C_8, n \in \mathbb{N}$ and

$$\alpha(G) = \alpha(C_2^n \times C_8) = \alpha(C_8) = \frac{1}{2}.$$

$\square$

5. GROUPS WITH $\alpha = 3/4$

All groups with $\alpha > 3/4$ have been classified by Garonzi and Lima (2018) [1], using results from the paper "On groups consisting mostly of involutions" by Wall (1970) [6]. It is a natural question to examine the groups where $\alpha = 3/4$.

A partial classification of nilpotent groups with $\alpha = 3/4$ was published by Tarnauceanu and Lazorec (2018) [2].

Definition 5.1. A group G is nilpotent if it has a lower central series of finite length, i.e. $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$ with $G_{i+1}/G_i \leq Z(G/G_i)$.

The following useful characterization of nilpotent groups is well known.

Theorem 5.2. A finite group is nilpotent if and only if it is a product of its Sylow subgroups.

Proposition 5.3. If G is nilpotent and $\alpha(G) = 3/4$ then G is a 2-group.

Proof. We have $G \cong \prod_p S_p$ where the S_p are the Sylow p-subgroups of G. By Proposition 3.5, $\alpha(G) = \prod_p \alpha(S_p)$. Now, finite p-groups contain normal subgroups with index p^i for all possible i. Taking $i = 1$ we have $N_p \trianglelefteq S_p$ with $S_p/N_p \cong C_p$. Therefore by Proposition 3.6,

$$\alpha(S_p) \leq \alpha(C_p) = \frac{2}{p} < \frac{3}{4}$$

if $p \geq 3$. Thus $|G|$ cannot have any prime factor greater than 2, i.e. G is a 2-group. $\square$

Therefore we tried to find a complete classification of groups with $\alpha = 3/4$, starting with a computational analysis using the GAP computer algebra system [5]. What follows are our preliminary investigations.

Proposition 5.4. The only dihedral groups with $\alpha = 3/4$ are D_{16} and D_{24}.

Proof. The number of cyclic subgroups of the dihedral group D_{2n} is $\tau(n) + n$. Therefore

$$\alpha = \frac{3}{4} \Leftrightarrow \frac{\tau(n) + n}{2n} = \frac{3}{4} \Leftrightarrow \tau(n) = \frac{n}{2}.$$

We know that n and $n/2$ are divisors of n (the latter as n is even). The next largest possible divisor is $n/3$ so we can bound $\tau(n)$ by $n/3 + 2$ (with equality when every number between 1 and $n/3$ divides n). Hence

$$\tau(n) = \frac{n}{2} \leq \frac{n}{3} + 2 \Rightarrow 3n \leq 2n + 12 \Rightarrow n \leq 12$$

so all possible values of n are: $2, 4, 6, 8$ or 12. As $\tau(2) = 2, \tau(4) = 3, \tau(6) = 4, \tau(8) = 4, \tau(10) = 4, \tau(12) = 6$; it follows that

$$\tau(n) = \frac{n}{2} \Leftrightarrow n \in \{8, 12\}.$$

$\square$

Definition 5.5. A group G is simple if $G \neq \{e\}$ and its only normal subgroups are $\{e\}$ and G.

Proposition 5.6. Let $I(G)$ denote the number of elements $g \in G$ such that $g^2 = 1$. Then

$$\frac{I(G)}{|G|} \geq 2\alpha(G) - 1.$$

In particular $\alpha(G) = 1$ if and only if G is an elementary abelian 2-group.

Proof. If $g \in G$ then $g^2 = 1$ if and only if $\varphi(|g|) = 1$ so

$$c(G) = \sum_{x \in G} \frac{1}{\varphi|x|} \leq I(G) + \frac{1}{2}(|G| - I(G)) = \frac{1}{2}(I(G) + |G|).$$

The result is then obtained by dividing both sides by $|G|$. $\square$

Definition 5.7. We denote the probability that two elements in a group G commute (i.e. commuting probability) by $\mathrm{cp}(G) = |S|/|G \times G|$, where S is the set of pairs $(x, y) \in G \times G$ such that $xy = yx$. Note that $\mathrm{cp}(G) = k(G)/|G|$ where $k(G)$ is the number of conjugacy classes of G (see Section 6 of Garonzi-Lima [1]).

Proposition 5.8. If $\alpha(G) \geq 1/2$ then $\mathrm{cp}(G) \geq (I(G)/|G|)^2$.

Proof. By Lemma 1 of Garonzi and Lima's paper [1], $\mathrm{cp}(G) \geq (I(G)/|G|)^2$ for all G. The result follows from Proposition 5.6. $\square$

Definition 5.9. Let V be a vector space over the field F. The general linear group of V, denoted $GL(V)$, is the group of all automorphisms of V, with composition of functions as the operation.

The general linear group of degree n over F, $GL(n, F)$, is the group of all invertible $n \times n$ matrices over a field F.

Note: if $\dim(V_F) = n$ then $GL(V) \cong GL(n, F)$.

Definition 5.10. A representation of a group G on a vector space V over $\mathbb{C}$ is a group homomorphism from G to $GL(V)$.

Definition 5.11. A representation ρ is faithful if $\rho : G \to GL(V)$ is injective.

Proposition 5.12. Let G be a non-abelian simple group. Then $k(G) \leq |G|/12$.

Proof. If $k(G) < |G|/12$ then we are done. Therefore, assume $k(G) \geq |G|/12$. From representation theory we know that G has $k(G)$ distinct irreducible representations with degrees

$$d_1 = 1 \leq d_2 \leq ... \leq d_{k(G)}$$

satisfying

$$d_1^2 + ... + d_{k(G)}^2 = |G|.$$

Since G is non-abelian, only the trivial representation of G has degree 1, so $d_2 \geq 2$. Furthermore, $d_2 \leq 3$, since if $d_2 \geq 4$ then

$$|G| = d_1^2 + ... + d_{k(G)}^2 \geq 1 + 4^2 + ... + 4^2 = 1 + 16(k(G) - 1).$$

But $k(G) \geq |G|/12$ implies that $|G| \leq 45$. This is a contradiction, because the smallest non-abelian simple group has order 60. Hence $d_2 = 2$ or 3. Since G is simple, the corresponding representation of G is faithful so G is isomorphic to a subgroup of $GL_2(\mathbb{C})$ or $GL_3(\mathbb{C})$. These groups are known [3], and the only simple groups on this list are A_5 of orders 60 and $PSL(2,7)$ 168. If $G \cong PSL(2,7)$ then

$$6 = k(G) \geq \frac{|G|}{12} = 14,$$

a contradiction. If $G \cong A_5$, then

$$5 = k(G) = \frac{|G|}{12}.$$

$\square$

Proposition 5.13. Let G be a non-abelian simple group, then

$$\alpha(G) < \frac{1}{2} + \frac{1}{4\sqrt{3}} \approx .64434$$

Proof. Since $\mathrm{cp}(G) \leq 1/12$ for non-abelian, simple groups, by Proposition 5.6,

$$(2\alpha(G) - 1)^2 \leq \mathrm{cp}(G) \leq 1/12.$$

Hence

$$2\alpha(G) - 1 \leq \frac{1}{\sqrt{12}}$$

and solving for $\alpha(G)$ we obtain

$$\alpha(G) \leq \frac{1}{2} + \frac{1}{4\sqrt{3}}.$$

□

Remark 5.14. Better upper bounds for α exist, Garonzi and Lima have shown that if G is non-solvable then $\alpha(G) \leq \alpha(S_5) = 67/120 \approx .5583$. [1]

Corollary 5.15. If G is a simple group then $\alpha(G) \neq \frac{3}{4}$.

Proof. If G is non-abelian, the result follows from Proposition 5.11. If G is abelian, then $G \cong C_p$ with p prime, so $\alpha(G) = 2/p \neq 3/4$. □

Definition 5.16. A group G is solvable if there are subgroups

$$1 = G_0 < G_1 < ... < G_k = G$$

such that G_i is normal in G and G_i/G_{i-1} is an abelian group for $i = 1, 2, ..., k$.

Corollary 5.13 can be generalized as follows:

Proposition 5.17. If $\alpha(G) = 3/4$ then G is solvable.

Proof. If $\alpha(G) = 3/4$, then by Proposition 5.8 $\mathrm{cp}(G) > 1/4$. From Theorem 11 in [2] if G is finite with $\mathrm{cp}(G) > 3/40$ then either G is solvable or $G \cong A_5 \times T$ for some abelian group T. However,

$$\alpha(A_5 \times T) \leq \alpha(A_5) = \frac{38}{60} < \frac{3}{4},$$

a contradiction. Therefore G is solvable. □

Proposition 5.18. If G is the non-abelian group of order pq, where p and q are prime and $p|(q-1)$ then $\alpha(G) \neq 3/4$.

Proof. By Theorem 4.9

$$\alpha(G) = \frac{q+2}{pq} = \frac{3}{4}.$$

If $\alpha(G) = 3/4$ then $8 = q(3p-4)$, so q must divide 8, and hence we obtain the following possibilities for (p, q): $(1, 8), (2, 4), (4, 1)$. However, none of these is a pair of primes, hence $\alpha(G) \neq 3/4$. □

Proposition 5.19. If $G \cong GA(1, p)$, then $\alpha(G) \neq \frac{3}{4}$.

Proof. Assume $G \cong GA(1, p)$. Then G has p conjugacy classes and order $p(p-1)$ so

$$\mathrm{cp}(G) = \frac{p}{p(p-1)} \frac{1}{p-1}.$$

By Proposition 5.6 if $\alpha(G) = 3/4$ then $\mathrm{cp}(G) \geq (2(3/4) - 1)^2 = 1/4$. Hence $p \in \{2, 3, 5\}$. But by Theorem 4.9 $\alpha(GA(1, 2)) = 1$, $\alpha(GA(1, 3)) = 5/6$, and $\alpha(GA(1, 5)) = 3/5$. Hence $\alpha(G) \neq 3/4$. □

6. WALL'S AND MILLER'S GROUPS WITH MANY INVOLUTIONS

In 1919, Miller published a paper classifying all groups containing $|G|/2 - 1$ involutions into 15 families [4]. In a paper published in 1970, Wall classified all groups containing at least $|G|/2$ involutions into four families [6]. In this section we explore the connection between these families and groups with $\alpha = 3/4$.

Proposition 6.1. For a group G, if $\alpha = 3/4$, then $n_2(G) \geq |G|/2 - 1$.

Proof. We have

$$\sum_{k=1}^{|G|} n_k(G) = c(G) = \frac{3|G|}{4}$$

and

$$\sum_{k=1}^{|G|} n_k(G)\varphi(k) = |G|.$$

Subtracting we obtain

$$\sum_{k=3}^{|G|} (\varphi(k) - 1)n_k(G) = \frac{1}{4}|G|$$

so

$$\sum_{k=3}^{|G|} 2(\varphi(k) - 1)n_k(G) = \frac{1}{2}|G|.$$

Now if $\varphi(k) \geq 2$, then $2(\varphi(k) - 1) \geq \varphi(k)$. Hence

$$\frac{1}{2}|G| = \sum_{k=3}^{|G|} 2(\varphi(k) - 1)n_k(G) \geq \sum_{k=3}^{|G|} \varphi(k)n_k(G),$$

so

$$1 + n_2(G) + \frac{1}{2}|G| \geq \sum_{k=1}^{|G|} \varphi(k) n_k(G) = |G|.$$

$\square$

If $n_2(G) = |G|/2 - 1$, G belongs to one of the families described by Miller. If $n_2(G) > |G|/2 - 1, G$ belongs to one of the families described in Wall's paper.

If $n_k(G) \neq 0$ for any $k \neq 1, 2, 3, 4, 6$ the inequalities above are strict and G is in one of the families described in Wall's paper.

We will now describe Wall's four families of groups containing more than $|G|/2 - 1$ involutions.

Let $G = G_0 \times C_2^n$ where G_0 is a core group. Then G_0 belongs to one of the following families:

1. The core group G_0 has the presentation

   $$\langle a \in A,\ t \mid t^2 = 1,\ tat^{-1} = a^{-1}\ \forall a \in A \rangle$$

   where A is a finite core abelian group. Note that $|G_0| = 2|A|$.

2. The core group G_0 is the product of two dihedral groups of order 8.

3. The core group G_0 has the presentation

$$G_0 = \langle c, x_1, y_1, ..., x_r, y_r | c^2 = x_i^2 = y_i^2 = 1,\ \text{all pairs of generators commute}$$

$$\text{except}[x_i, y_i] = c \rangle$$

4. The core group G_0 has the presentation

$$G_0 = \langle c, x_1, y_1, ..., x_n, y_n | c^2 = x_i^2 = y_i^2 = 1, \text{ all commute except } [c, x_i] = y_i \rangle.$$

6.1 Wall's First Family

Proposition 6.2. The groups in Wall's First Family with $\alpha = 3/4$ are of the form $G = D_{16} \times C_2^n$ or $D_{24} \times C_2^n$.

Proof. Let $G_0 = A \rtimes C_2$ where A is abelian. The action is $x \mapsto x^{-1}$. Let $C_2 = \langle t \rangle$, we have

$$(at)^2 = atat = atat^{-1}t^2 = aa^{-1}t^2$$

so $(at)^2 = 1$ for all $a \in A$. This gives $|A|$ cyclic subgroups of order 2. Hence

$$c(G_0) = c(A) + |A| = c(A) + \frac{|G_0|}{2}$$

and

$$\alpha(G_0) = \frac{c(A) + |A|}{2|A|} = \frac{3}{4} \Rightarrow \alpha(A) = \frac{1}{2}.$$

If A contains a C_p (p prime), then there is an N so that $A/N = C_p$, hence

$$\alpha(A) \leq \alpha(C_p) = \frac{2}{p}$$

so $1/2 \leq 2/p$, which implies $p \leq 4$, and thus $p = 2$ or $p = 3$.

Note that neither C_9 nor C_{16} is a subgroup of A. If they were then

$$\frac{1}{2} = \alpha(A) \leq \alpha(C_9) = \frac{1}{3} \quad \text{or} \quad \frac{1}{2} \leq \alpha(C_{16}) = \frac{5}{16}.$$

Since G_0 has no C_2 as a summand, and neither does A. Let

$$A \cong C_4^m \times C_8^l \times C_3^n.$$

We claim that if $l > 0$, then $A \cong C_8$. Suppose $A \cong C_8 \times N$ with $N \neq 0$. Now $N \ncong C_2^k$ so $\alpha(A) < \alpha(A/N)$ by Proposition 3.10, so

$$\frac{1}{2} = \alpha(A) < \alpha(A/N) = \alpha(C_8) = \frac{1}{2},$$

giving a contradiction. So we may assume $A \cong C_4^m \times C_3^n$. If $n = 0$, then $A \cong C_4^m$, and hence by Proposition 4.11

$$\alpha(A) = \frac{2^m + 1}{2 \cdot 2^m} > \frac{1}{2}.$$

Similarly, if $m = 0$, then $A \cong C_3^n$, and hence by Proposition 4.10

$$\alpha(A) = \frac{3^n + 1}{2 \cdot 3^n} > \frac{1}{2}.$$

If $m, n \geq 1$ note that $C_4 \times C_3 = C_{12}$ and $\alpha(C_{12}) = 1/2$. If $|A| > 12$, then there is an N in A that is not an elementary abelian 2-group with $A/N = C_{12}$ so by Proposition 3.6

$$\frac{1}{2} = \alpha(A) < \alpha(C_{12}) = \frac{1}{2}.$$

In conclusion, $A = C_8$ or C_{12} and hence $G_0 = D_{16}$ or D_{24}. □

6.2 Wall's Second Family

Proposition 6.3. The core group in Wall's Second Family has $\alpha = 25/32$.

Proof. The core group in Wall's second family are of the form $D_8 \times D_8$. This group contains

- 1 element of order 1: e.
- 35 elements of order 2: $(e, *), (*, *), (*, e)$, where $*$ is arbitrary of order 2.
- 28 elements of order 4.

Applying Proposition 3.3 we obtain

$$c(D_8 \times D_8) = \frac{1}{\varphi(1)} + \frac{35}{\varphi(2)} + \frac{28}{\varphi(4)} = 1 + 35 + 14 = 50.$$

Hence

$$\alpha(D_8 \times D_8) = \frac{50}{64} = \frac{25}{32} > \frac{3}{4}.$$

□

6.3 Wall's Third Family

Proposition 6.4. None of the groups in Wall's Third Family have $\alpha = 3/4$.

Proof. The core groups in Wall's third family have the following presentation

$$G_0 = \langle x_i, y_i, c | x_i^2 = y_i^2 = c^2 = 1, \text{ all commute except } x_i y_i x_i^{-1} = c \rangle.$$

Let $w = x_1^{e_1} y_1^{f_1} ... x_n^{e_n} y_n^{f_n} c^g$ be a word in canonical form. If w doesn't contain both an x_i and a y_i, then all the terms commute and hence $w^2 = 1$. If w has exactly one x_i-y_i pair, then $(x_i y_i)^2 = x_i y_i x_i y_i = c$, so w has order 4. If there are two such pairs in w, then $(x_i y_i x_j y_j)^2 = (x_i y_i)^2 (x_j y_j)^2 = cc = 1$. Similarly, if w has an odd number of pairs, then w has order 4. If there is an even number, then the order is 2 (with the exception of the identity element).

Let $f(n)$ be the number of words of the form $x_1^{e_1} y_1^{f_1} ... x_n^{e_n} y_n^{f_n}$ having order 2 or less. Then the number of elements of order 2 or less in G_0 is $2f(n)$, where the factor of 2 accounts for whether or not the word contain a c.

Choose a subset I of $\{1, 2, ..., n\}$ of size $2i$ and let J be its complement. There are $\binom{n}{2i}$ ways of choosing I, and

$$w = \prod_{i \in I} x_i b_i \prod_{i \in J} x_i^{e_i} y_i^{f_i}$$

where $(e_i, f_i) = (0,0), (0,1), (1,0)$ but not $(1,1)$.

Therefore we have

$$f(n) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{2i} 3^{n-2i}.$$

By the binomial theorem

$$(3+1)^n = \sum_{i=0}^{n} \binom{n}{i} 3^{n-i}$$

and

$$(3-1)^n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} 3^{n-1}.$$

Adding these equations gives

$$4^n + 2^n = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{2i} 3^{n-2i} = 2f(n)$$

which is the number of elements of order 2 or less. Therefore the number of elements of order 4 is

$$2 \cdot 4^n - (4^n + 2^n) = 4^n - 2^n.$$

Finally, the number of cyclic subgroups of G_0 is

$$4^n + 2^n + \frac{4^n - 2^n}{2} = \frac{3}{2}4^n + 2^{n-1}$$

so

$$\alpha(G_0) = \frac{\frac{3}{2}4^n + 2^{n-1}}{2 \cdot 4^n} = \frac{3}{4} + \frac{2^{n-2}}{4^n} > \frac{3}{4}.$$

Therefore none of the groups in this family has $\alpha = 3/4$. $\square$

6.4 Wall's Fourth Family

Proposition 6.5. None of the groups in Wall's Fourth Family have $\alpha = 3/4$.

Proof. The core groups have the presentation

$$G_0 = \langle c, x_1, y_1, ..., x_n, y_n | c^2 = x_i^2 = y_i^2 = 1, \text{ all commute except } [c, x_i] = y_i \rangle.$$

Since we have $cx_icx_i = y_i$, $cx_i = x_iy_ic$. Let w be a word in x_is and y_j's. Then $w^2 = 1$. If w has no x_i's then $(wc)^2 = 1$. If w has any x_i's let $\overline{w}$ be the word obtained by replacing each x_i with x_iy_i. Then $cw = \overline{w}c$, as the c commutes with y_i and $cx_i = x_iy_ic$. So $(wc)^2 = wcwc = w\overline{w}c^2 = w\overline{w} \neq 1$. Since $w\overline{w}$ is a word in y_i's and the y_i's have order 2, $w\overline{w}$ has order 2, so wc has order 4.

We have one element of order 1. The $2^{2n} - 1$ non-identity words containing no c have order 2. The 2^n word of the form wc where w contains no x_i have order 2. The remaining $2^{2n} - 2^n$ words have order 4. Therefore there are $2^{2n} - 2^n$ of the form wc with w containing an x_i that have order 4. Hence

$$c(G_0) = 1 + (2^{2n} - 1) + 2^n + \frac{2^{2n} - 2^n}{2} = 3 \cdot 2^{2n-1} + 2^{n-1}.$$

Therefore

$$\alpha(G_0) = \frac{3 \cdot 2^{2n-1} + 2^{n-1}}{2^{2n+1}} = \frac{3}{4} + \frac{1}{2^{n+2}} > \frac{3}{4}.$$

Hence the groups in this family don't have $\alpha = 3/4$. □

Therefore, Wall's first family is the only family containing groups with $\alpha(G) = 3/4$, namely, D_{16} and D_{24}.

Theorem 6.6. If $\alpha(G) = 3/4$ and G contains an element of order 8, it is of the form $D_{16} \times C_2^n$ for $n \geq 0$.

Proof. Since we have $n_k(G) \neq 0$ for $k \neq 1, 2, 3, 4, 6$, by the remark after Proposition 6.1, G belongs to one of Wall's families. The only groups in Wall's families with $\alpha(G) = 3/4$ are $D_{24} \times C_2^n$ and $D_{16} \times C_2^n$. However, D_{24} has no elements of order 8. Therefore $G \cong$

$D_{16} \times C_2^n$. $\square$

6.5 Miller's First Family

Proposition 6.7. All the groups in Miller's First Family have $\alpha = 3/4$.

Proof. The core groups in Miller's first family are

$$G_0 = \langle x_1, ..., x_n, y_1, ..., y_n, t | x_i^2 = y_i^2 = t^4 = 1, \text{all commute except } [t, y_i] = x_i y_i \rangle.$$

Note that since

$$t^2 y_i t^{-2} = t x_i y_i t^{-1} = x_i x_i y_i = y_i,$$

t^2 commutes with all x_i and y_i. Let w be a word in x_i's and y_i's. We now compute $c(G_0)$. The elements of each order are the following:

- Order 1: 1.
- Order 2: If $w \neq 1$, then w has order 2. Words of the form wt^2 have order 2 since w and t^2 have order 2 and they commute.
- Order 4: Let $\overline{w}$ denote the word obtained by replacing each y_i with $x_i y_i$. Then

$$(wt)^2 = wtwt = wtwt^{-1}t^2 = w\overline{w}t^2$$

where $w\overline{w}$ is a word in x_i's and y_i's. Hence $w\overline{w}t^2$ has order 2 and therefore wt has order 4. Similarly wt^3 has order 4.

Hence

$$c(G_0) = \frac{2 \cdot 2^{2n}}{1} + \frac{2 \cdot 2^{2n}}{2} = 3 \cdot 2^{2n}$$

and

$$\alpha(G_0) = \frac{3 \cdot 2^{2n}}{4 \cdot 2^{2n}} = \frac{3}{4}.$$

$\square$

7. CONCLUSION

Classifying groups with a specific number of cyclic subgroups, and understanding their properties, is still an area that requires further work. Our research has built upon work by Tărnăuceanu, Lazorec, Garonzi, and Lima and provided greater insight into groups with $\alpha = 3/4$. In addition to the work already presented, we used GAP to explore groups with $\alpha = 3/4$, see the Appendix (Table 3). Interestingly, we did not find any core groups of order 512 that had $\alpha = 3/4$.

By Proposition 6.1 the only groups with $\alpha = 3/4$ left to be discovered are "described" in Miller's paper. Unfortunately, we were only able to fully characterize three of Miller's families. Further work translating Miller's paper into modern mathematical terms is the key to understanding all groups with $\alpha = 3/4$. To conclude this thesis, we have included a result that we hoped we'd be able to prove.

Conjecture 7.1. If $\alpha(G) = 3/4$ and G is not nilpotent, then $G \cong D_{24} \times C_2^n$.

REFERENCES

[1] Garonzi, M., & Lima, I.; On the number of cyclic subgroups of a finite group, Bull. Braz. Math. Soc., New Series (2018), 49(3), 515–530.

[2] Tarnauceanu, M.; Finite groups with a certain number of cyclic subgroups. Amer. Math. Monthly 122 (2015), no. 3, 275–276.

[3] Miller, G. A., Blichfeldt, H. F., & Dickson, L. E.; Theory and applications of finite groups, Dover Publications (1961).

[4] Miller, G. A.; Groups of order g containing $g/2$-1 involutions, Tohoku Math. J. 17 (1920), 88-102.

[5] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.11.1; 2021. (https://www.gap-system.org)

[6] Wall, C. T. C.; On groups consisting mostly of involutions. Proc. Cambridge Philos. Soc. 67 1970 251–262.

8. APPENDIX

Here's a table showing the core groups with $\alpha(G) = 3/4$ up to order 512 that we found using GAP. If the groups belong to one of Miller's first 3 families the corresponding family is indicated in the table.

GAP ID	Family	Description
(4,1)	Miller's 1st Family	C_4
(16,3)	Miller's 1st Family	
(16,7)	Wall's 1st Family	D_{16}
(16,13)	Miller's 2nd Family	
(24,6)	Wall's 1st Family	D_{24}
(64,60)	Miller's 1st Family	
(64,73)		
(64,215)	Miller's 3rd Family	
(64,216)		
(64,266)		
(128,1135)	Miller's 3rd Family	
(128,1165)		
(128,2216)		
(128,2230)		
(256,7667)	Miller's 1st Family	
(256,56091)		

Table 3: Core groups up to order 512 found with GAP

Remark 8.1. (16,13) is the only core group in Miller's second family; (64,215) and (128,1135) are the only core groups in Miller's third family.