ON THE NUMBER OF CYCLIC SUBGROUPS OF A FINITE GROUP

MARTINO GARONZI AND IGOR LIMA

Abstract. Let $G$ be a finite group and let $c(G)$ be the number of cyclic subgroups of $G$. We study the function $\alpha(G) = c(G)/|G|$. We explore its basic properties and we point out a connection with the probability of commutation. For many families $\mathcal{F}$ of groups we characterize the groups $G \in \mathcal{F}$ for which $\alpha(G)$ is maximal and we classify the groups $G$ for which $\alpha(G) > 3/4$. We also study the number of cyclic subgroups of a direct power of a given group deducing an asymptotic result and we characterize the equality $\alpha(G) = \alpha(G/N)$ when $G/N$ is a symmetric group.

1. Introduction

In this paper all the groups we consider are finite. Let $c(G)$ be the number of cyclic subgroups of a group $G$ and $\alpha(G) := c(G)/|G|$. It is clear that $0 < \alpha(G) \leq 1$.

Observe that every cyclic subgroup $\langle x \rangle$ of $G$ has $\varphi(o(x))$ generators, where $\varphi$ is Euler’s totient function and $o(x)$ denotes the order of the element $x$, hence

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

On a computational level this formula is probably best for computing $c(G)$ for arbitrary $G$, and it is what we employed to work out small groups using [3]. For $d$ a divisor of $|G| = n$ let $B_G(d)$ be the number of elements $x \in G$ such that $x^d = 1$. Denote by $\mu$ the standard M"obius function. In [4] another formula is given (from Lemma 7 (2) choosing $A(d)$ the number of elements of $G$ of order $d$, $B(d) = B_G(d)$ and $(r, s) = (1, 0)$), which is an easy application of the M"obius inversion formula, the following:

$$
c(G) = \sum_{d|n} \left( \sum_{i|n/d} \frac{\mu(i)}{\varphi(i)} \right) B_G(d).
$$

Using this formula in [4] Corollary 13 it was shown that ciclicity can be detected by the number of cyclic subgroups, more precisely that if $|G| = n$ then $c(G) \geq c(C_n)$ with equality if and only if $G \cong C_n$.

There is a connection between $\alpha(G)$ and the so-called “commuting probability” of $G$, denoted by $cp(G)$, that is the probability that two random elements of $G$ commute (studied extensively in [5], which we crucially employ in our study). More specifically we prove that if $\alpha(G) \geq 1/2$ then $cp(G) \geq (2\alpha(G) - 1)^2$. This implies that a group with many cyclic subgroups has big solvable radical and, if it is already solvable, it has big Fitting subgroup (see Section 3 for the details).
It is not hard to show that $\alpha(G) \leq \alpha(G/N)$ whenever $N$ is a normal subgroup of $G$, and if equality holds then $N$ must be an elementary abelian 2-group. It is an interesting question to ask what can we say about $G$ if $\alpha(G) = \alpha(G/N)$ given some information on $G/N$. In this paper we characterize equality $\alpha(G) = \alpha(G/N)$ when $G/N$ is a symmetric group (Theorem 1).

Given a family $\mathcal{F}$ of groups define
\[ \alpha_{\mathcal{F}} := \max \{ \alpha(G) : G \in \mathcal{F} \}, \quad m_{\mathcal{F}} := \{ G \in \mathcal{F} : \alpha(G) = \alpha_{\mathcal{F}} \}. \]

We are interested in computing $\alpha_{\mathcal{F}}$ and $m_{\mathcal{F}}$ for various families $\mathcal{F}$. In this paper we prove the following results.

1. If $\mathcal{F}$ is the family of all finite groups then $\alpha_{\mathcal{F}} = 1$ and $m_{\mathcal{F}}$ is the family of elementary abelian 2-groups (by 2.2).
2. If $\mathcal{F}$ is the family of non-abelian groups then
   \[ \alpha_{\mathcal{F}} = 7/8 = \alpha(D_8) \]
   and $m_{\mathcal{F}}$ is the family of groups of the form $C_2^n \times D_8$ for some $n \geq 0$ (by Corollary 2).
3. If $\mathcal{F}$ is the family of non-nilpotent groups then
   \[ \alpha_{\mathcal{F}} = 5/6 = \alpha(S_3) \]
   and $m_{\mathcal{F}}$ is the family of groups of the form $C_2^n \times S_3$ for some $n \geq 0$ (by Corollary 2).
4. If $\mathcal{F}$ is the family of non-solvable groups then
   \[ \alpha_{\mathcal{F}} = 67/120 = \alpha(S_5) \]
   and $m_{\mathcal{F}}$ is the family of groups of the form $C_2^n \times S_5$ for some $n \geq 0$ (Theorem 4).
5. If $\mathcal{F}$ is the family of non-supersolvable groups then
   \[ \alpha_{\mathcal{F}} = 17/24 = \alpha(S_4) \]
   and $m_{\mathcal{F}}$ is the family of groups of the form $C_2^n \times S_4$ for some $n \geq 0$ (Theorem 6).
6. If $p$ is an odd prime and $\mathcal{F}$ is the family of non-trivial groups of order divisible only by primes at least $p$ then
   \[ \alpha_{\mathcal{F}} = 2/p = \alpha(C_p) \]
   and $m_{\mathcal{F}} = \{ C_p \}$ (Proposition 1).
7. If $p$ is an odd prime and $\mathcal{F}$ is the family of groups $G$ with $C_p$ as an epimorphic image then
   \[ \alpha_{\mathcal{F}} = 2/p = \alpha(C_p) \]
and $m\mathcal{F}$ is the family of groups which are the direct product of an elementary abelian 2-group and a Frobenius group with 2-elementary abelian Frobenius kernel and Frobenius complements of order $p$ (Proposition 2).

We also classify the groups $G$ with $\alpha(G) > 3/4$ (Theorem 3), proving in particular that $3/4$ is the largest non-trivial accumulation point of the set of numbers of the form $\alpha(G)$. An easy consequence of this (Corollary 3) is that if $G$ is not an elementary abelian 2-group and it has $|G| - n$ cyclic subgroups then $|G| \leq 2n$. This extends and generalizes the results in [11], as we show right after the corollary. We also give a formula for $\alpha(G)$ when $G$ is a nilpotent group (Theorem 2) and we study $\alpha$ of a direct power (Theorem 3) proving that $G^n$ has roughly $|G^n|/\varphi(\exp(G))$ cyclic subgroups.

2. Basic properties of $\alpha$

In this section we prove some basic properties of the function $\alpha$.

2.1. If $A$ and $B$ are finite groups of coprime orders then $c(A \times B) = c(A)c(B)$ and hence $\alpha(A \times B) = \alpha(A)\alpha(B)$. The proof of this is straightforward.

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

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

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 $\varphi(o(g)) = 1$, so

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

This implies the result. \hfill $\square$

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

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

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

This implies the result. \hfill $\square$

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

**Proof.** If $n \in N$ then applying 2.3 we have $\varphi(o(n)) = \varphi(o(nN)) = \varphi(o(N)) = \varphi(1) = 1$ so $n^2 = 1$. \hfill $\square$

2.5. If $G$ is any finite group then $\alpha(G) = \alpha(G \times C_2^n)$ for all $n \geq 0$.

**Proof.** Choosing $N = \{1\} \times C_2^n$ gives $\varphi(o(x)) = \varphi(o(xN))$ for all $x \in G \times C_2^n$. The result follows from 2.3. \hfill $\square$
2.6. If $\alpha(G) = \alpha(G/N)$ and $L \leq G$, $L \subseteq N$ then $\alpha(G) = \alpha(G/L)$.

Proof. Since $G/N$ is a quotient of $G/L$ we have $\alpha(G/N) = \alpha(G) \leq \alpha(G/L) \leq \alpha(G/N)$ by 2.3 and the result follows.

2.7. If $\alpha(G) = \alpha(G/N)$ and $K \leq G$ then $\alpha(K) = \alpha(K/K \cap N)$.

Proof. Let $R := K \cap N$. By 2.3 is enough to show that if $x \in K$ then $o(xR) = o(xN)$ (because then $\varphi(o(xR)) = \varphi(o(xN)) = \varphi(o(x))$). Let $a = o(xR)$ and $b = o(xN)$. Since $R \subseteq N$ we have $x^a \in N$ so $b \leq a$. On the other hand $x^b \in K \cap N = R$ so $a \leq b$. Therefore $a = b$.

2.8. Suppose $\alpha(G) = \alpha(G/N)$. If $a \in G$ has order 2 modulo $N$ then $a$ centralizes $N$, in particular if $G/N$ can be generated by elements of order 2 then $N \subseteq Z(G)$.

Proof. We have $\varphi(o(a)) = \varphi(o(aN)) = \varphi(2) = 1$ by 2.3 and $a$ has order 2 modulo $N$, so $o(a) = 2$. If $n \in N$ then $\varphi(o(an)) = \varphi(o(anN)) = \varphi(o(aN)) = 1$ so $(an)^2 = 1$. This together with $a^2 = n^2 = 1$ (by 2.4) implies $an = na$. Recalling that $N$ is abelian (by 2.4) we deduce that if $G/N$ can be generated by elements of order 2 then $N \subseteq Z(G)$.

3. A characterization

Observe that $C_3$ is a quotient of $A_4$ and $\alpha(C_3) = \alpha(A_4) = 2/3$, so it is not always the case that $\alpha(G) = \alpha(G/N)$ implies $G \cong N \times G/N$. We can characterize the groups such that $\alpha(G) = \alpha(G/N)$ when $G/N$ is a symmetric group, for the following two reasons: the symmetric groups can be generated by elements of order 2 and their double covers are known.

**Theorem 1.** Let $G$ be a group and $N$ a normal subgroup of $G$ such that $G/N$ is isomorphic to a symmetric group. If $\alpha(G) = \alpha(G/N)$ then $N$ is an elementary abelian 2-group and it admits a normal complement in $G$, so that $G \cong N \times G/N$.

Proof. We prove the result by induction on the order of $G$. By 2.4 $N$ is an elementary abelian 2-group. Since $G/N \cong S_m$ can be generated by elements of order 2, 2.8 implies that $N$ is central in $G$. If $m = 2$ then the result follows from 2.2 so suppose $m \geq 3$. Let $R \cong C_2^l$ be a minimal normal subgroup of $G$ contained in $N$. By 2.6 we have $\alpha(G/R) = \alpha(G) = \alpha(S_m)$ so by induction, since $G/N$ is a quotient of $G/R$, we have $G/R = C_2^l \times S_m$ for some $l \geq 0$. Let $K \trianglelefteq G$ be the (normal) subgroup of $G$ such that $K/R = \{1\} \times S_m$. Observe that $K \cap N$ contains $R$, so $K \cap N/R$ is a normal 2-subgroup of $K/R \cong S_m$. If $m \neq 4$ this implies that $K \cap N = R$ because $S_m$ in this case does not admit non-trivial normal 2-subgroups (being $m \geq 3$). If $m = 4$ and $K \cap N \neq R$ then $K \cap N/R$ is the Klein group, and $K/K \cap N \cong S_3$. However in this case 2.3 and 2.7 imply that

$$17/24 = \alpha(S_3) = \alpha(K/R) \geq \alpha(K) = \alpha(K/K \cap N) = \alpha(S_3) = 5/6,$$

a contradiction. We deduce that $K \cap N = R$.

If $N \neq R$ then $|K| < |G|$ and $\alpha(K) = \alpha(K/R) = \alpha(S_m)$ by 2.7 (being $K \cap N = R$). By induction we deduce that $K \cong R \times S_m$. Set $M := \{1\} \times S_m \leq K$. Since

$$S_m \cong G/N \geq KN/N \cong K/K \cap N = K/R \cong S_m$$
we obtain $G = KN = MRN = MN$ so being $N$ central in $G$ and $N \cap M = N \cap R \cap M = R \cap M = \{1\}$ we deduce $G = N \times M \cong N \times G/N$. Assume now $N = R$, so $N$ is a minimal normal subgroup of $G$. Since $N$ is central, $|N| = 2$ and actually $N = (z) = Z(G)$ is the center of $G$ (being $G/N \cong S_m$ with $m \geq 3$).

Suppose by contradiction that $G$ is not a direct product $C_2 \times S_m$. We claim that $N$ is contained in the derived subgroup of $G$. Indeed $G'$ is contained in the subgroup $T$ of $G$ such that $T \supseteq N$, $T/N \cong A_m$ (being $|G/T| = 2$), so if $G'$ does not contain $N$ then $G'/N$ is a nontrivial normal subgroup of $G/N \cong S_m$ containing the derived subgroup of $S_m$ (that is, $A_m$) hence $G/N = T$ therefore letting $\varepsilon \in G$ represent a fixed element of order 2 of $G/N \cong S_m$ not belonging to $A_m$, $\varphi(o(\varepsilon)) = \varphi(2) = 1$ (by (2.3) hence $o(\varepsilon) = 2$ implying that $G'(\varepsilon) \cap N = \{1\}$ (otherwise $G'(\varepsilon) \supseteq N$ implying that $G'(\varepsilon) = G$ so $|G : G'| = 2$ hence $G \cong N \times G'$, a contradiction) therefore $G'(\varepsilon) \cong G'(\varepsilon)/N = G/N \cong S_m$; being $N$ the center of $G$ we deduce $G \cong C_2 \times S_m$, a contradiction. This implies that $N \subseteq G'$ so $G$ is a double cover of $S_m$ (that is, a stem extension of $S_m$ where the base normal subgroup has order 2), and looking at the known presentations of the double covers of the symmetric group (classified by Schur, see for example [9]) we see that $z$ is a square in $G$, that is there exists $x \in G$ with $x^2 = z$, so that $x$ has order 4 and $xN$ has order 2, contradicting $\varphi(o(x)) = \varphi(o(xN))$ (which is true by (2.3)).

4. Nilpotent groups

Let $G$ be a finite group. For $\ell$ a divisor of $|G|$ let $B_G(\ell)$ be the number of elements $g \in G$ with the property that $g^\ell = 1$ and let $r_G(\ell)$ be the number of elements of $G$ of order $\ell$. It is worth mentioning the famous result by Frobenius that if $G$ is any group and $\ell$ divides $|G|$ then $\ell$ divides $B_G(\ell)$. The idea of the following result, which is a reformulation of formula (11) in the nilpotent case, is to give a formula for $c(G)$ when $G$ is a nilpotent group in terms of the numbers $B_G(d)$, that in general are reasonably easy to deal with (consider for example the case in which $G$ is abelian).

**Theorem 2.** If $G$ is a nilpotent group of order $n$ then $c(G) = \sum_{d|n} B_G(d)/d$.

**Proof.** Assume first that $G$ is a $p$-group, $|G| = p^n$. Since $r_G(p^j) = B_G(p^j) - B_G(p^{j-1})$ whenever $j \geq 1$ we see that

$$
c(G) = \sum_{x \in G} \frac{1}{\varphi(o(x))} = \sum_{j=0}^{n} \frac{r_G(p^j)}{\varphi(p^j)} = 1 + \sum_{j=1}^{n} \frac{B_G(p^j) - B_G(p^{j-1})}{\varphi(p^j)} = 1 - B_G(1) \frac{1}{\varphi(p)} + \sum_{j=1}^{n-1} \left( \frac{1}{\varphi(p^j)} - \frac{1}{\varphi(p^{j+1})} \right) B_G(p^j) \frac{B_G(p^n)}{\varphi(p^n)} = \sum_{j=0}^{n} \frac{B_G(p^j)}{p^j}.
$$

Now consider the general case, and write the order of $G$ as $n = |G| = p_1^{n_1} \cdots p_t^{n_t}$ with the $p_i$’s pairwise distinct primes, $G$ is a direct product $\prod_{i=1}^{t} G_{p_i}$, where $G_{p_i}$ is the unique Sylow $p_i$-subgroup of $G$. Using (2.1) we obtain

$$
c(G) = \prod_{i=1}^{t} c(G_{p_i}) = \prod_{i=1}^{t} \left( \sum_{j=0}^{n} \frac{B_{G_{p_i}}(p_i^j)}{p_i^j} \right) = \sum_{d|n} B_G(d)/d.
$$

The last equality follows from the fact that since $G$ is nilpotent $B_G(ab)$ equals $B_G(a)B_G(b)$ if $a$ and $b$ are coprime divisors of $n$. 

□
5. An asymptotic result

We want to study $\alpha(G^n)$ where $G^n = G \times G \times \cdots \times G$ ($n$ times) in terms of the functions $B_G$ and $r_G$ defined in the previous section. Recall that the exponent of a group $G$, denoted $\exp(G)$, is the least common multiple of the orders of the elements of $G$. It is clear that $\exp(G^n) = \exp(G)$. The following result shows that $G^n$ has roughly $|G^n|/\varphi(\exp(G))$ cyclic subgroups.

**Theorem 3.** Let $G$ be a finite group. Then $\lim_{n \to \infty} \alpha(G^n) = 1/\varphi(\exp(G))$.

**Proof.** Observe that $r_{G^n}(\ell) \neq 0$ only if $\ell$ divides $|G|$, therefore

$$\alpha(G^n) = \frac{1}{|G^n|} \sum_{x \in G^n} \frac{1}{\varphi(\ell(x))} = \sum_{\ell \mid |G|} \frac{r_{G^n}(\ell)}{\varphi(\ell)|G|^n} = \sum_{\ell \mid |G|} \frac{r_{G^n}(\ell)}{\varphi(\ell)|G|^n}$$

so what we need to compute is the limit $L_\ell$ of $r_{G^n}(\ell)/|G|^n$ when $n \to \infty$, for $\ell$ a divisor of $|G|$. Clearly $r_{G^n}(\ell) \leq B_G(\ell)$ so $r_{G^n}(\ell)/|G|^n \leq (B_G(\ell)/|G|)^n$ so if $B_G(\ell) < |G|$ then $L_\ell = 0$. Now assume $B_G(\ell) = |G|$, in other words $\exp(G)$ divides $\ell$. If $\exp(G) < \ell$ then $r_{G^n}(\ell) = 0$ so $L_\ell = 0$. Now assume $\exp(G) = \ell$. Let $p$ vary in the set of prime divisors of $|G|$, and for every such $p$ define $a_p := B_G(\exp(G)/p)$. Clearly $G^n$ has at least $|G^n| - \sum_p a_p^n$ elements of order $\exp(G)$.

Observe that $a_p < |G|$ by definition of $\exp(G)$, so that $a_p/|G| < 1$, hence $(a_p/|G|)^n$ tends to 0 as $n \to \infty$, implying $L_{\exp(G)} = 1$. The result follows. \(\square\)

6. A connection with the probability of commutation

The probability that two elements in a group $G$ commute is denoted by $cp(G)$ (“commuting probability” of $G$) and is defined by $|S|/|G \times G|$ where $S$ is the set of pairs $(x, y) \in G \times G$ such that $xy = yx$. It is easy to show that $cp(G) = k(G)/|G|$ where $k(G)$ is the number of conjugacy classes of $G$. This invariant was studied by many authors, but we refer mostly to [3].

Let $I(G)$ be the size of the set $\{x \in G : x^2 = 1\}$. The following lemma is easily deducible from Theorem 2J of [1]. It can also be proved character-theoretically using the Frobenius-Schur indicator.

**Lemma 1.** $I(G)^2 \leq k(G)|G|$, in other words $cp(G) \geq (I(G)/|G|)^2$.

This together with [2] implies the following inequality.

**Lemma 2.** If $\alpha(G) \geq 1/2$ then $cp(G) \geq (2\alpha(G) - 1)^2$.

Let us include some other results from [3] that we will need in the following section.

6.1. If $G$ is a non-solvable group and $sol(G)$ is the maximal normal solvable subgroup of $G$ then $cp(G) \leq |G : sol(G)|^{-1/2}$. This follows from [3] Theorem 9 (which depends on the classification of the finite simple groups), and together with Lemma 2 implies that if $\alpha(G) > 1/2$ then $|G : sol(G)| \leq (2\alpha(G) - 1)^{-4}$.

6.2. If $G$ is a solvable group and $F(G)$ is the Fitting subgroup of $G$ then $cp(G) \leq |G : F(G)|^{-1/2}$. This follows from [3] Theorem 4, and together with Lemma 2 implies that if $\alpha(G) > 1/2$ then $|G : F(G)| \leq (2\alpha(G) - 1)^{-4}$. 


ON THE NUMBER OF CYCLIC SUBGROUPS OF A FINITE GROUP

| $G$         | $\text{Aut}(G)$ | $|G|$   | $\text{Float}(\alpha(G))$ | $\alpha(G)$ |
|------------|-----------------|--------|----------------------------|-------------|
| $\text{Alt}(5)$ | $\text{Sym}(5)$ | 60     | 0.533333                   | 8/15        |
| $\text{Sym}(5)$ | $\text{Sym}(5)$ | 120    | 0.558333                   | 67/120      |
| $\text{Alt}(6)$ | $\text{PGL}(2,9)$ | 360    | 0.463889                   | 167/360     |
| $\text{PGL}(2,9)$ | $\text{PGL}(2,9)$ | 720    | 0.394444                   | 71/180      |
| $\text{Sym}(6)$ | $\text{PGL}(2,9)$ | 720    | 0.502778                   | 181/360     |
| $M_{10}$      | $\text{PGL}(2,9)$ | 720    | 0.419444                   | 151/360     |
| $\text{PGL}(2,9)$ | $\text{PGL}(2,9)$ | 1440   | 0.426389                   | 307/720     |
| $\text{Alt}(7)$ | $\text{Sym}(7)$ | 2520   | 0.375794                   | 947/2520    |
| $\text{Sym}(7)$ | $\text{Sym}(7)$ | 5040   | 0.404563                   | 2039/5040   |
| $\text{PSL}(3,2)$ | $\text{PGL}(2,7)$ | 168    | 0.470235                   | 79/168      |
| $\text{PGL}(2,7)$ | $\text{PGL}(2,7)$ | 336    | 0.464286                   | 13/28       |
| $\text{PSL}(2,8)$ | $\text{PGL}(2,8)$ | 504    | 0.309524                   | 13/42       |
| $\text{PGL}(2,8)$ | $\text{PGL}(2,8)$ | 1512   | 0.362434                   | 137/378     |
| $\text{PSL}(2,11)$ | $\text{PGL}(2,11)$ | 660    | 0.369697                   | 61/165      |
| $\text{PGL}(2,11)$ | $\text{PGL}(2,11)$ | 1320   | 0.368182                   | 81/220      |
| $\text{PSL}(2,13)$ | $\text{PGL}(2,13)$ | 1092   | 0.335165                   | 61/182      |
| $\text{PGL}(2,13)$ | $\text{PGL}(2,13)$ | 2184   | 0.322344                   | 88/273      |
| $\text{PSL}(2,17)$ | $\text{PGL}(2,17)$ | 2448   | 0.306373                   | 125/408     |
| $\text{PGL}(2,17)$ | $\text{PGL}(2,17)$ | 4896   | 0.267777                   | 437/1632    |
| $\text{PSL}(2,19)$ | $\text{PGL}(2,19)$ | 3420   | 0.267251                   | 457/1710    |
| $\text{PSL}(2,16)$ | $\text{PGL}(2,16)$ | 4080   | 0.192157                   | 49/255      |

**Table 1.** Almost-simple groups of order at most 5397

### 7. Non-solvable groups

**Theorem 4.** Let $G$ be a finite non-solvable group. Then $\alpha(G) \leq \alpha(S_5)$ with equality if and only if $G \cong S_5 \times C_2^n$ for some integer $n \geq 0$.

**Proof.** Let $\alpha := \alpha(S_5) = 67/120$. We will show that if $G$ is any finite non-solvable group such that $\alpha(G) \geq \alpha$ then $G \cong S_5 \times C_2^n$ for some $n \geq 0$. Assume $\alpha(G) \geq \alpha$, in particular $\alpha(G) > 1/2$. By [6,1] we deduce $|G/\text{sol}(G)| \leq (2\alpha - 1)^{-1} = (60/7)^4 < 5398$ thus $|G/\text{sol}(G)| \leq 5397$. Observe that $G/\text{sol}(G)$ is non-trivial (being $G$ non-solvable), it does not have non-trivial solvable normal subgroups and $\alpha(G/\text{sol}(G)) \geq \alpha(G) \geq \alpha$. If we can show that $G/\text{sol}(G) \cong S_5$ it will follow that $67/120 = \alpha \leq \alpha(G) \leq \alpha(G/\text{sol}(G)) = \alpha(S_5) = 67/120$ therefore $\alpha(G) = \alpha(G/\text{sol}(G))$ and the result follows from Theorem 1.

We are left to show that if $G$ is a group without non-trivial solvable normal subgroups and such that $|G| \leq 5397$ and $\alpha(G) \geq \alpha(S_5) = 67/120$, then $G \cong S_5$. Let $N$ be a minimal normal subgroup of $G$, then $N = S^t$ with $S$ a non-abelian simple group. If $t \geq 2$ then being $|S| \geq 60$ and $|G| \leq 5397$ we deduce $G = N = A_5 \times A_5$, contradicting the minimality of $N$. So $t = 1$. We claim that there is no other minimal normal subgroup of $G$. Indeed if $M$ is a minimal normal subgroup of $G$ distinct from $N$ then $M$ is non-solvable (by assumption) so $|G:MN| = |G|/|MN| \leq 5397/60^2 < 2$ (the smallest order of a non-solvable group is 60) so $G = MN$ and actually $G = M \times N = A_5 \times A_5$ ($M$ is a direct power of a non-abelian simple group, the smallest orders of non-abelian simple groups are 60, 168 and 60·60^2, 60·168 are both larger than 5397) which is a contradiction because
\( \alpha(A_5 \times A_5) = 77/225 < \alpha(S_5). \) We deduce that \( N \) is the unique minimal normal subgroup of \( G \). Since \( N \) is non-solvable, it is non-abelian, so it is not contained in \( C_G(N) \), hence \( C_G(N) \) must be trivial (otherwise it would contain a minimal normal subgroup of \( G \) distinct from \( N \)) therefore \( G \) is almost-simple. Using \([7]\) and \([3]\) we computed the list of almost-simple groups \( G \) of size at most 5397 and for each of them we determined \( \alpha(G) \). The results are summarized in the above table. We deduce that the only almost-simple group \( G \) with \( |G| \leq 5397 \) and \( \alpha(G) \geq 67/120 \) is \( G = S_5 \).

This together with Lemma \([2]\) and \([6.2]\) implies the following.

**Corollary 1.** If \( \alpha(G) > \alpha(S_5) \) then \( G \) is solvable and the Fitting subgroup of \( G \) has index at most 5397.

---

### 8. Groups with many cyclic subgroups

In this section we will study groups with \( \alpha(G) \) “large”, specifically, we will classify all the finite groups \( G \) such that \( \alpha(G) > 3/4 \). This is a natural choice because 3/4 turns out to be the largest non-trivial accumulation point of the set of numbers of the form \( \alpha(G) \). To do such classification the idea is to observe that if \( \alpha(G) > 3/4 \) then \( I(G)/|G| > 1/2 \) and use Wall’s classification \([10]\) Section 7).

**Theorem 5.** Let \( X \) be a group with \( \alpha(X) > 3/4 \). Then \( X \) is a direct product of an elementary abelian 2-group with a group \( G, \alpha(X) = \alpha(G), \) \( G \) does not have \( C_2 \) as a direct factor, and either \( G \) is trivial (in which case \( \alpha(X) = 1 \)) or one of the following occurs.

1. **Case I.** \( G \cong A \rtimes \langle \varepsilon \rangle \), where \( \langle \varepsilon \rangle = C_2 \) acts on \( A \) by inversion and there exists an integer \( n \geq 1 \) such that one of the following occurs.
   \[
   A = C_3^n, \quad \alpha(G) = \frac{3 \cdot 3^n + 1}{4 \cdot 3^n} \quad \text{or} \quad A = C_4^n, \quad \alpha(G) = \frac{3 \cdot 2^n + 1}{4 \cdot 2^n}.
   \]

2. **Case II.** \( G \cong D_8 \times D_8 \) and \( \alpha(G) = 25/32 \).

3. **Case III.** \( G \) is a quotient \( D_8^r / N \) where \( N = \{(a_1, \ldots, a_r) \in Z(D_8)^r : \alpha_1 \cdots \alpha_r = 1\} \) and
   \[
   \alpha(G) = \frac{3 \cdot 2^r + 1}{4 \cdot 2^r}.
   \]

4. **Case IV.** \( G \) is a semidirect product \( V \rtimes \langle c \rangle \) where \( V = \mathbb{F}_2^{2r} \) has a basis \( \{x_1, y_1, \ldots, x_r, y_r\}, c \) has order 2, it acts trivially on each \( y_i \), \( x_i^c = cx_ic = [c, x_i]x_i = x_iy_i \) for \( i = 1, \ldots, r \), and
   \[
   \alpha(G) = \frac{3 \cdot 2^r + 1}{4 \cdot 2^r}.
   \]

**Proof.** We know by \([2.3]\) that \( \alpha(X) = \alpha(G) \). Also, we may assume that \( G \) is non-trivial. Since \( \alpha(G) > 3/4 \), by \([2.2]\) we have \( I(G)/|G| \geq 2\alpha(G) - 1 > 1/2 \) so \( G \) appears in Wall’s classification \([10]\) Section 7). Case II is immediate, we will treat cases I, III and IV.

**Case I** of Wall’s classification. \( G \) is a semidirect product \( A \rtimes \langle \varepsilon \rangle \) with \( A \) an abelian group, \( \langle \varepsilon \rangle \cong C_2 \) and every element of \( G - A \) has order 2. Observe that \( A \) does not admit \( C_2 \) as a direct factor. Indeed if \( a \in A \) then since \( ae \notin A, ae \) has order 2 so \( \varepsilon = a^{-1} \), hence \( \varepsilon \) acts on \( A \) as inversion and a direct factor of order 2 in \( A \) would yield a direct factor of order 2 in \( G \). It follows that \( c(G) = c(A) + |G|/2 \),
so that $3/4 < \alpha(G) = \alpha(A)/2 + 1/2$ implying $\alpha(A) > 1/2$. If the prime $p$ divides the order of $A$ then $C_p$ is a quotient of $A$ so $1/2 < \alpha(A) \leq \alpha(C_p) = 2/p$ whence $p \leq 3$, that is, $p$ is either 2 or 3. Write $A = P_2 \times P_3$ where $P_2$ is an abelian 2-group and $P_3$ is an abelian 3-group. Observe that $C_3$ is not a quotient of $A$ because otherwise $1/2 < \alpha(A) \leq \alpha(C_3) = 1/3$, a contradiction. Therefore if $P_2$ is trivial then $A \cong C_3^n$ for some $n \geq 1$, an easy computation shows $\alpha(A) = \frac{3^{n+1}}{2^{2n+1}}$, and the result follows. Suppose now that $P_2$ is non-trivial. If $P_3$ is non-trivial then since $P_2$ is not elementary abelian (because $A$ does not have $C_2$ as a direct factor) there is a quotient of $A$ isomorphic to $C_{12}$, however $1/2 < \alpha(A) \leq \alpha(C_{12}) = 1/2$ gives a contradiction. So $P_3 = \{1\}$, in other words $A$ is an abelian 2-group and we may write $A = \prod_{i=1}^{\beta} C_{2^n}$. Since $A$ does not have $C_2$ as a direct factor we deduce $a_i \geq 2$ for all $i$, on the other hand if one of the $a_i$’s is at least 3 then $C_3$ is a quotient of $A$ but $1/2 < \alpha(A) \leq \alpha(C_3) = 1/2$ is a contradiction. So $A \cong C_4^n$ hence an easy computation shows $\alpha(A) = \frac{2^{n+1}}{2^{2n+1}}$, and the result follows.

**Case III of Wall’s classification.** $G$ is a direct product of $D_8$’s with the centers amalgamated. $G = G(r)$ has a presentation

$$G(r) = \langle c, x_1, y_1, \ldots, x_r, y_r : c^2 = x_i^2 = y_i^2 = 1, \text{ all pairs of generators commute except } [x_i, y_i] = c \rangle.$$ 

A more practical description of the group in question is $G = D_8^r/N$ where $N = \{(z_1, \ldots, z_r) \in Z^r : z_1 \cdots z_r = 1\}$ where $Z = \langle z \rangle$ (cyclic of order 2) is the center of $D_8$. $N$ is a subgroup of $Z(D_8^r) = Z^r$ of index 2, so $|G| = 2 \cdot 4^r$. An element $(a_1, \ldots, a_r)N \in G$ squares to 1 if and only if $(a_1^2, \ldots, a_r^2) \in N$, that is, $a_1^2 \cdots a_r^2 = 1$. Observe that every $a_i^2$ is either 1 or $z$, so this condition means that there are an even number of indices $i$ such that $a_i^2 = z$. Since $D_8$ contains 6 elements that square to 1 and 2 elements that square to $z$, $D_8^r$ contains exactly $\beta_r = \sum_{k=0}^{[r/2]} \binom{r}{2k} 2^{2k}6^{r-2k}$ elements $(a_1, \ldots, a_r)$ such that $a_1^2 \cdots a_r^2 = 1$. Hence $G$ contains exactly $\beta_r/2^{r-1}$ elements that square to 1. Observe that

$$8^r = (2 + 6)^r = \sum_{h=0}^{r} \binom{r}{h} 2^h 6^{r-h}, \quad 4^r = (-2 + 6)^r = \sum_{h=0}^{r} \binom{r}{h} (-1)^h 2^h 6^{r-h}$$

so adding them together gives exactly $2\beta_r$. This means that $\beta_r = \frac{1}{2}(8^r + 4^r)$, so $G$ has exactly $\beta_r/2^{r-1} = 4^r + 2^r$ elements that square to 1 and exactly $|G| - \beta_r/2^{r-1} = 2 \cdot 4^r - 4^r - 2^r = 4^r - 2^r$ elements of order 4. Therefore

$$\alpha(G) = \frac{1}{2 \cdot 4^r} \left(4^r + 2^r + \frac{1}{2}(4^r - 2^r)\right) = \frac{3 \cdot 2^r + 1}{4 \cdot 2^r}.$$

**Case IV of Wall’s classification.** $G = G(r)$ has a presentation

$$G(r) = \langle c, x_1, y_1, \ldots, x_r, y_r : c^2 = x_i^2 = y_i^2 = 1, \text{ all pairs of generators commute except } [c, x_i] = [c, y_i] \rangle.$$ 

A more practical description of the group in question is $G \cong V \rtimes \langle c \rangle$ where $V = C_2^{2r} = \langle x_1, y_1, \ldots, x_r, y_r \rangle$, $c$ has order 2, it acts trivially on each $y_i$ and $x_i^c = cx_i c = [c, x_i]x_i = x_iy_i$ for $i = 1, \ldots, r$. Thinking of $V$ as a vector space over $\mathbb{F}_2$, if $v \in V$
then $vc$ has order 2 or 4, and it has order 4 exactly when $v^e \neq v$. Observe that with respect to the given basis of $V$ the operator $c$ (acting from the right) has a diagonal block matrix form with $J = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ on each diagonal block entry. Thus there are precisely $2^r$ vectors $v$ with $v^e = v$, they are of the form $(0, b_1, 0, b_2, \ldots, 0, b_r)$. Therefore $G$ has $2^{2r} - 2^r$ elements of order 4 and $c(G) = 2^{2r} + 2^r + (2^{2r} - 2^r)/2$. This implies that $\alpha(G) = \frac{3 \cdot 2^{2r} + 1}{2^{2r} + 1}$.

The following corollary is immediate. It implies that if $G$ is a non-nilpotent group then $\alpha(G) \leq 5/6$ with equality if and only if $G$ is a direct product $C_2^n \times S_3$.

**Corollary 2.** Let $G$ be a group such that $\alpha(G) \geq 5/6 = \alpha(S_3)$. Then either

1. $G \cong C_2^n \times S_3$ for some $n \geq 0$ and $\alpha(G) = 5/6$, or
2. $G \cong C_2^n \times D_8$ for some $n \geq 0$ and $\alpha(G) = 7/8$, or
3. $G \cong C_2^n$ for some $n \geq 0$ and $\alpha(G) = 1$.

We can deduce a bound of $|G|$ in terms of $|G| - c(G)$. The inequality $\alpha(G) \leq 7/8$ can be written as $|G| \leq 8(|G| - c(G))$, so we obtain the following.

**Corollary 3.** If $G$ is any finite group which is not an elementary abelian 2-group then $|G| \leq 8(|G| - c(G))$ with equality if and only if $G \cong D_8 \times C_2^n$ for some non-negative integer $n$.

Observe that the above results extend and generalize the results in [11]. As an example of application let us determine the groups $G$ with $|G| = 9$ cyclic subgroups. In this case we have $|G| - c(G) = 9$ so $|G| \leq 72$ and a GAP check yields that $G$ is one of $C_{11}$, $D_{22}$ and $C_4 \times S_3$.

9. Special families of groups

**Proposition 1.** Let $p \geq 3$ be a prime number. Let $G$ be a non-trivial group of order divisible only by primes at least $p$. Then $\alpha(G) \leq 2/p$ with equality if and only if $G \cong C_p$.

In particular if $G$ belongs to the family of groups of odd order then $\alpha(G) \leq 2/3$ with equality if and only if $G \cong C_3$.

**Proof.** If $1 \neq x \in G$ and $q$ is a prime divisor of the order of $x$ then $p \leq q$ so $\varphi(o(x)) \geq \varphi(q) = q - 1 \geq p - 1$, so since $|G| \geq p$ we have

$$\alpha(G) = \frac{1}{|G|} \sum_{x \in G} \frac{1}{\varphi(o(x))} \leq \frac{1}{|G|} \left(1 + \frac{|G| - 1}{p - 1}\right) = \frac{1}{|G|(p - 1)} + \frac{1}{p - 1} \leq \frac{p - 2}{p(p - 1)} + \frac{1}{p - 1} = \frac{2}{p}.$$

If equality holds the above inequalities are equalities and using $p \geq 3$ it is easy to deduce that $|G| = p$, that is, $G \cong C_p$. \hfill \Box

**Proposition 2.** Let $G$ be a group and $p$ an odd prime, and suppose $G$ has $C_p$ as epimorphic image (in other words $p$ divides $|G/G'|$). Then $\alpha(G) \leq 2/p$ with equality if and only if $G$ is a direct product of an elementary abelian 2-group with a Frobenius group with 2-elementary abelian kernel and complements of order $p$.

Observe that a bound of $2/p$ when $p = 2$ would be trivial. This is why we are only considering the odd case.
Proof. Since \( C_p \) is a quotient of \( G \) we have \( \alpha(G) \leq \alpha(C_p) = 2/p \). Now assume equality holds. Then \( \alpha(G) = \alpha(C_p) \) and there exists \( N \leq G \) with \( G/N \cong C_p \), so \( N \) is an elementary abelian 2-group by 2.4, say \( N \cong C_2^m \). If \( G \) has elements of order 2 then it has \( C_2 \) as a direct factor (for example by Maschke’s theorem), so now assume \( G \) does not have elements of order 2. A subgroup of \( G \) of order \( p \) acts fixed point freely on \( N \) so \( G \) is a Frobenius group with Frobenius kernel equal to \( N \) and Frobenius complement of order \( p \). Now assume \( G \) is a Frobenius group with 2-elementary abelian kernel of size \( 2^m \) and Frobenius complement of order \( p \). The element orders of \( G \) are 1, 2, and \( p \), and \( G \) has precisely \( 2^m - 1 \) elements of order 2 and \( 2^m(p - 1) \) elements of order \( p \). We have

\[
\alpha(G) = \frac{1}{|G|} \sum_{x \in G} \frac{1}{\varphi(|x|)} = \frac{1}{2^m \cdot p} \left( 2^m + \frac{2^m(p - 1)}{p - 1} \right) = \frac{2}{p}.
\]

This concludes the proof. \( \square \)

10. NON-SUPERSOLVABLE GROUPS

Let \( G \) be a solvable group and let \( F_i \) be normal subgroups of \( G \) defined as follows:

\[
F_0 = \{1\}, \quad F_{i+1}/F_i := F(G/F_i) \quad \forall i \geq 0,
\]

where \( F(G/F_i) \) denotes the Fitting subgroup of \( G/F_i \). In particular \( F_1 \) is the Fitting subgroup of \( G \). Since \( G \) is solvable, there exists a minimal \( h \) such that \( F_h = G \), such \( h \) is called the “Fitting height” of \( G \). Observe that

\[
F(F_i/F_{i-1}) = F_i/F_{i-1} \quad \forall l \geq i \geq 1,
\]

indeed \( F_i/F_{i-1} \) is nilpotent and normal in \( F_i/F_{i-1} \) hence \( F_i/F_{i-1} \subseteq F(F_i/F_{i-1}) \), and \( F(F_i/F_{i-1}) \) is nilpotent and characteristic in \( F_i/F_{i-1} \), which is normal in \( G/F_{i-1} \), so \( F(F_i/F_{i-1}) \) is normal in \( G/F_{i-1} \) hence \( F(F_i/F_{i-1}) \subseteq F(G/F_{i-1}) = F_i/F_{i-1} \). This implies in particular that \( F_i/F_{i-1} \) has Fitting height \( l - i \).

The following consequence of the solution of the \( k(GV) \) problem is proved in [5] Lemma 3, proof of (i) (see also [6]).

Proposition 3. Let \( G \) be a group and let \( F \) be the Fitting subgroup of \( G \). If \( G/F \) is nilpotent (that is, \( G \) has Fitting height 2) then \( k(G) \leq |F| \), so that

\[
\text{cp}(G) \leq \frac{1}{|G:F|}.
\]

The following result shows that \( S_4 \) is a “maximal” non-supersolvable group in terms of \( \alpha(G) \).

Theorem 6. Let \( G \) be a group. If \( G \) is not supersolvable then \( \alpha(G) \leq \alpha(S_4) \) with equality if and only if \( G \cong C_2^n \times S_4 \) for some non-negative integer \( n \).

Proof. We prove that if \( \alpha(G) \geq \alpha(S_4) \) and \( G \) is not supersolvable then \( G \) is isomorphic to \( C_2^n \times S_4 \) for some non-negative integer \( n \). We have \( \alpha(G) \geq \alpha(S_4) = 17/24 > 67/120 \) so \( G \) is solvable by Theorem 4, so the Fitting subgroup \( F \) of \( G \) is non-trivial, and since \( G \) is not supersolvable \( G \neq F \). Since \( 2/3 < 17/24 \), Proposition 1 implies that \( G \) does not have non-trivial quotients of odd order. Also, since \( 17/24 > 1/2 \) we have \( \text{cp}(G) \geq (2\alpha(G) - 1)^2 \geq 25/144 \) by Lemma 2.
In the following discussion we will use Proposition 3 the inequality \( \text{cp}(G) \leq \text{cp}(N) \cdot \text{cp}(G/N) \) for \( N \leq G \) (see [5, Lemma 1]) and the obvious fact that the commuting probability is always at most 1. Let \( F_i \) be the subgroups defined above and let \( h \) be the Fitting height of \( G \). We distinguish three cases.

1. \( h = 2 \). In this case \( G = F_2 > F_1 > \{1\} \). We have that \( G/F_1 \) is nilpotent so \( 25/144 \leq \text{cp}(G) \leq 1/|G : F_1| \) so \( |G : F_1| \leq 5 \). However \( |G : F_1| \notin \{3, 5\} \) because \( G \) does not have non-trivial quotients of odd order, so \( G/F_1 \) is one of \( C_2, C_4 \) and \( C_2 \times C_2 \).

2. \( h = 3 \). In this case \( G = F_3 > F_2 > F_1 > \{1\} \). We have \( 25/144 \leq \text{cp}(G) \leq \text{cp}(F_2) \leq 1/|F_2 : F_1| \) and \( 25/144 \leq \text{cp}(G) \leq \text{cp}(G/F_1) \leq 1/|G : F_2| \) so \( |F_2 : F_1| \leq 5 \) and \( |G : F_2| \leq 5 \). Also \( G/F_1 \) is not a group of prime power order (because it is not nilpotent) and \( |G : F_2| \) is not 3 or 5 because \( G \) does not have quotients of odd order. Therefore \( G/F_1 \) is a group of order 6, 10, 12 or 20, its Fitting subgroup has order at most 5 and \( \alpha(G/F_1) \geq \alpha(G) \geq 17/24 \). We deduce \( G/F_1 \cong S_3 \) by [3].

3. \( h \geq 4 \). In this case \( G \geq F_4 > F_3 > F_2 > F_1 > \{1\} \). We have \[
\frac{25}{144} \leq \text{cp}(G) \leq \text{cp}(F_2) \cdot \text{cp}(F_4/F_2) \leq \frac{1}{|F_2 : F_1|} \cdot \frac{1}{|F_4 : F_3|}
\]
so \( |F_2 : F_1| \cdot |F_4 : F_3| \leq 5 \) implying that \( |F_2 : F_1| = |F_4 : F_3| = 2 \). But then \( F(F_3/F_1) = F_2/F_1 \subseteq Z(F_3/F_1) \) implying \( F_3/F_1 = F_2/F_1 \) (because the Fitting subgroup contains its own centralizer), a contradiction.

We deduce that \( G/F \) is one of \( C_2, C_4, C_2 \times C_2 \) and \( S_3 \).

Since \( G \) is not supersolvable there exists a maximal subgroup \( M \) of \( G \) whose index \( |G : M| \) is not a prime number (see [8, 9.4.4]). Let \( M_G \) the normal core of \( M \) in \( G \), that is, the intersection of the conjugates of \( M \) in \( G \). Let \( X := G/M_G \), \( K := M/M_G \), so that \( |G : M| = |X : K| \). Then \( \alpha(S_4) \leq \alpha(G) \leq \alpha(X) \). This implies that if \( X \cong S_4 \) then the result follows from Theorem 11 so all we have to prove is that \( X \cong S_4 \). The subgroup \( M/M_G \) of \( X \) is maximal and it has trivial normal core, so \( X \) is a primitive solvable group. We will make use of the known structural properties of primitive solvable groups, see for example [2] Section 15 of Chapter A. \( X \) is a semidirect product \( X = V \rtimes K \) with \( V = C_p^n \), \( p \) a prime, \( V \) is the unique minimal normal subgroup of \( X \) and it equals the Fitting subgroup of \( X \). Since \( |V| = |X : K| \) is not a prime, \( n \geq 2 \), so \( |X| > 6 \geq |G/F| \) hence \( F \not\subseteq M_G \) so \( FM_G/M_G \) is a non-trivial nilpotent normal subgroup of \( X \) so it equals \( V \), hence \[
K \cong X/V = (G/M_G)/(FM_G/M_G) \cong G/FM_G
\]
is a quotient of \( G/F \) so \( K \) is one of \( C_2, C_4, C_2 \times C_2 \) and \( S_3 \).

In what follows we will use the known representation theory of small groups over the field with \( p \) elements. We will think of \( V \) as a vector space of dimension \( n \) over the field \( \mathbb{F}_p \), irreducible when seen as a \( \mathbb{F}_p[K] \)-module.
Suppose \( p \) divides \( |K| \). Observe that being not supersolvable, \( X \) is not a 2-group, hence \( K \) cannot be \( C_2, C_4 \) nor \( C_2 \times C_2 \), so \( K \cong S_3 \). The structure of the group algebras \( \mathbb{F}_2[S_3] \) and \( \mathbb{F}_3[S_3] \) implies that \( n \geq 2 \) forces \( n = p = 2 \) and hence \( X \cong S_4 \).

Suppose now \( p \) does not divide \( |K| \), so that \( |K| \) and \( |V| \) are coprime.

Suppose \( \mathbb{F}_p \) is a splitting field for \( K \). Since \( n \geq 2 \), the only possibility is \( K \cong S_3 \), \( n = 2 \), and the action of \( K \) on \( V \) defining the group structure of \( X = V \rtimes K \) is the following: \( K \cong S_3 \) permutes the coordinates of the vectors in the fully deleted module

\[
V = \{(a, b, c) \in \mathbb{F}_p^3 : a + b + c = 0\}.
\]

The elements of order 2 in \( X \) are of the form \( (a, b, c)k \) with \( k \in K \), \( o(k) = 2 \) and the fixed coordinate is zero, so there are 3\( p \) of them. The elements of order 3 in \( X \) are of the form \( vk \) with \( v \in V \) arbitrary and \( k \in K \), \( o(k) = 3 \), so there are 2\( p^2 \) of them. The elements of order \( p \) in \( X \) are the non-trivial elements of \( V \) (being \( p \) coprime to \( |K| = 6 \)) so there are \( p^2 - 1 \) of them. The elements of order \( 2p \) in \( X \) are of the form \( vk \) with \( v \in V \), \( k \in K \), \( o(k) = 2 \) and \( o(vk) \neq 2 \) so there are \( 3p^2 - 3p \) of them. The exponent of \( X \) is 6\( p \) and \( X \) has no elements of order 6, 3\( p \) or 6\( p \). This implies that

\[
c(X) = \sum_{x \in X} \frac{1}{\varphi(o(x))} = 1 + 3p + \frac{2p^2}{2} + \frac{p^2 - 1}{p - 1} + \frac{3p^2 - 3p}{p - 1} = p^2 + 7p + 2.
\]

Using \( p \geq 5 \) and \( |X| = 6p^2 \) we deduce \( \alpha(X) < 17/24 \), a contradiction.

Suppose \( \mathbb{F}_p \) is not a splitting field for \( K \). Since \( n \geq 2 \), the only possibility is \( K \cong C_4 \), \( n = 2 \), and the polynomial \( t^2 + 1 \) does not split modulo \( p \), that is, \( p \equiv 3 \mod 4 \). Let \( x \) be a generator of the cyclic group \( K \). We may interpret \( x \) as a matrix of order 4, so that by irreducibility the minimal polynomial of \( x \) is \( t^2 + 1 \) (the only irreducible factor of degree 2 of \( t^4 - 1 \)). This implies that \( x^2 = -1 \). Choosing a nonzero vector \( v_1 \in V \) and \( v_2 := v_1^x \), since \( v_1, v_2 \) are linearly independent (otherwise \( v_1 \) would be an eigenvector for \( x \) contradicting irreducibility), and \( v_2^x = v_1 v_2 = -v_1 \), the matrix of \( x \) in the base \( \{v_1, v_2\} \) is

\[
\begin{pmatrix}
0 & 1 \\
-1 & 0
\end{pmatrix}
\]

acting by right multiplication. \( X = V \rtimes K \) has \( p^2 - 1 \) elements of order \( p \) (the non-trivial elements of \( V \), being \( p \) coprime to \( |K| = 4 \)), \( p^2 \) elements of order 2 (the elements of the form \( vx^2 \) with \( v \in V \) arbitrary) and \( 2p^2 \) elements of order 4 (the elements of the form \( vx \) or \( vx^3 \) with \( v \in V \) arbitrary). The exponent of \( X \) is 4\( p \) and there are no elements of order 2\( p \) or 4\( p \), therefore

\[
c(X) = \sum_{x \in X} \frac{1}{\varphi(o(x))} = 1 + p^2 + \frac{2p^2}{2} + \frac{p^2 - 1}{p - 1} = 2p^2 + p + 2.
\]

Using \( p \geq 3 \) and \( |X| = 4p^2 \) we deduce \( \alpha(X) < 17/24 \), a contradiction.

\[\square\]

11. Acknowledgements

We would like to thank the referee for carefully reading a previous version of this paper and having very useful suggestions.
References

[1] R. Brauer, K. A. Fowler; On groups of even order. Ann. of Math. (2) 62 (1955), 565–583.
[2] K. Doerk and T. Hawkes, Finite Soluble Groups, de Gruyter Expositions in Mathematics 4, de Gruyter (1992).
[3] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.
[4] Garonzi M., Patassini M.; Inequalities detecting structural properties of a finite group. Comm. Algebra 45 (2017), no. 2, 677–687.
[5] Guralnick R. M., Robinson G. R.; On the commuting probability in finite groups. J. Algebra 300 (2006), no. 2, 509–528.
[6] Knorr R.; On the number of characters in a p-block of a p-solvable group. Illinois J. Math. 28 (1984) 181–210.
[7] D. Leemans, L. Vauthier; An atlas of abstract regular polytopes for small groups. Aequationes Math. 72 (2006), no. 3, 313–320.
[8] D. J. S. Robinson, A course in the theory of groups; Second edition; Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1996.
[9] Schur, J; On the representation of the symmetric and alternating groups by fractional linear substitutions. Translated from the German [J. Reine Angew. Math. 139 (1911), 155–250] by Marc-Félix Otto. Internat. J. Theoret. Phys. 40 (2001), no. 1, 413–458.
[10] Wall, C. T. C.; On groups consisting mostly of involutions. Proc. Cambridge Philos. Soc. 67 1970 251–262.
[11] Tarnauceanu, M.; Finite groups with a certain number of cyclic subgroups. Amer. Math. Monthly 122 (2015), no. 3, 275–276.

(Martino Garonzi) Departamento de Matemática, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Brasília-DF, 70910-900, Brazil.
E-mail address: mgaronzi@gmail.com

(Igor Lima) Universidade Federal de Goiás, IMTec - Regional Catalão, Av. Dr. Lamartine P. de Avelar, 1120 Setor Universitário Catalão-GO, 75704-020, Brazil.
E-mail address: igor.matematico@gmail.com