ORDER EVALUATION OF PRODUCTS OF SUBSETS IN
FINITE GROUPS AND ITS APPLICATIONS. II

Z. ARAD AND M. MUZYCHUK

Abstract. In this paper we give a new estimate of the cardinality of the
product of subsets $AB$ in a finite non-abelian simple group, where $A$ is normal
and $B$ is arbitrary. This estimate improves the one given in J. Algebra 182

1. Introduction

This paper is a continuation of [2], where the following question was considered.
Given a finite group $G$ and two arbitrary subsets $S, T \subset G$, how large may their
product $TS$ be, provided that $TS \neq G$?

In [2] the survey of related results was presented. In particular, we proved that
if $S$ is a normal subset, $|S| > 1$, and $G$ is finite non-abelian simple, then $ST \neq G$
yields that $|ST| \geq |S| + |T| - 1$. Furthermore, the equality $|ST| = |S| + |T| - 1$
holds if and only if either $|T| = 1$ or $T = S^{-1} g$, where $S$ denotes the complement
to $S$ in $G$.

As it was illustrated in [2], the above-mentioned result implies various interesting
applications which were stated there.

The purpose of this paper is to present a better estimation for $|AB|$. More
precisely, the main result of the paper is

Theorem 1.1. Let $G$ be a finite non-abelian simple group. Denote by $l$
the minimal cardinality of non-trivial conjugacy classes of $G$. Then for each normal $A \subset G$, such
that $1 < |A| \leq |G|/4$ and for any $B \subset G$,

$$|B| \geq 2, \quad |AB| \leq |G| - 2 \Rightarrow |AB| \geq |A| + |B| + (l - 18)/12.$$ 

In particular, if $A$ is a non-trivial conjugacy class, then either $|C_G(a)| = 3, a \in A$, or
the assumption $|A| \leq |G|/4$ holds by the simplicity of $G$. Non-abelian simple
groups $G$ with self-centralizing subgroup of order 3 are $A_5$ and $PSL(2,7)$ by [5]. If
$G = A_5$, then $l = 12$ and Theorem 1.1 holds by [2]. If $G = PSL(2,7)$, then $l = 21$
and $|A| = 56$. Here also one can prove that Theorem 1.1 holds. Therefore, if $A$ is a
non-trivial conjugacy class of $G$, then the assumption $|A| \leq |G|/4$ may be omitted.

Received by the editors September 25, 1995.

1991 Mathematics Subject Classification. Primary 20D99, 05A99; Secondary 05C25.

This work was done at the Gelbart and Emmy Noether Research Institutes for Mathematical
Sciences at Bar-Ilan University.

The second author was supported by the research grants from the Israeli Ministry of Science
and the German-Israeli Foundation for fundamental research.

©1997 American Mathematical Society

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
As an application of Theorem 1.1 we prove

**Theorem 1.2.** Let $G$ be a finite non-abelian simple group. Then for each normal $A \subset G$, such that $1 < |A| \leq |G|/4$ and for any $B \subset G$, it holds that
\[ |B| \geq 2, |AB| \leq |G| - 2 \Rightarrow |AB| \geq |A| + |B| + 3. \]

As a direct consequence we obtain the following omnibus theorem:

**Theorem 1.3.** Let $G$ be a finite non-abelian group with $k$ conjugacy classes and $\text{Cla}(G)^\#$ be the set of its non-trivial conjugacy classes. Then $G$ is not simple if one of the following holds:
1) $CD \subseteq C \cup D$ for some $C, D \in \text{Cla}(G)^\#$;
2) $CD \subseteq C^{-1} \cup D$ for some $C, D \in \text{Cla}(G)^\#$;
3) $CD \subseteq C^{-1} \cup D^{-1}$ for some $C, D \in \text{Cla}(G)^\#$;
4) $\prod_{B \in B} B \subseteq \bigcup_{B \in B} B \cup \{1\}$ for some $B \subset \text{Cla}(G)^\#$;
5) there exist $A, B \subset \text{Cla}(G)^\#$ such that
\[ \prod_{A \in A} A \subseteq \bigcup_{B \in B} B \cup \{1\}, \]
\[ \prod_{B \in B} B \subseteq \bigcup_{A \in A} A \cup \{1\}. \]
6) $CC^{-1} \subseteq C \cup C^{-1} \cup \{1\}$ for some $C \in \text{Cla}(G)^\#$;
7) $C^2 \subseteq C \cup C^{-1}$ for some $C \in \text{Cla}(G)^\#$;
8) $C^2 \subseteq \{1\} \cup D \cup D^{-1}$ for some $C, D \in \text{Cla}(G)^\#$;
9) $\prod_{C \in \text{Cla}(G)^\#} C \neq G$;
10) $|\prod_{C \in \text{Cla}(G)^\# \backslash \{D\}} C| < |G| - 1$, where $D \in \text{Cla}(G)^\#$ is a conjugacy class of minimal cardinality;
11) if $|C| \geq |G|/k - 2, k > 6, C \in \text{Cla}(G)^\#$ and $C^k \neq G$.

Parts 1) and 2) are known by [1]. Parts 3)-5), 7)-9) and 11) were open problems; a few of them were mentioned in [1]. Part 6) was proved in [1] by using CFSG. Part 9) is known due to R. Brauer (see [4]). The detailed structure of $G$ satisfying part 1) is known by [1]. In [1] it was shown that there is no finite group satisfying part 2).\(^1\)

Further research is needed for a better understanding of the structure of $G$ satisfying parts 3)-11).

2. Preliminaries

Let $A \subset G$ be a subset of a group $G$. In what follows we use $\overline{A}$ for $G \setminus A$. For an integer $i$ we define
\[ S_i(A) = \{ B \subset G \mid |B| > i \text{ and } |\overline{AB}| > i \}; \]
\[ \omega_i(A) = \min \{|AB| - |B| \mid B \in S_i(A)\}; \]
\[ \mathcal{E}_i(A) = \{ B \in S_i(A) \mid |AB| = |B| + \omega_i(A) \}. \]

Since $S_i(A) \subseteq S_j(A)$ when $i \leq j$, $\omega_i(A)$ is a non-decreasing function of $i$.

**Proposition 2.1.** Let $X, Y \in \mathcal{E}_i(A)$ and $|X \cap Y| > i, |\overline{AX} \cup \overline{AY}| > i$. Then $X \cap Y, X \cup Y \in \mathcal{E}_i(A)$.

---

\(^1\)Character theorems dual to parts 7) and 8) were considered in [7].
Proof. The identity

\[ |AX \cup AY| + |AX \cap AY| = |AX| + |AY| \]

implies

(1) \[ |A(X \cup Y)| + |A(X \cap Y)| \leq |AX| + |AY| = |X| + |Y| + 2\omega_i(A). \]

The inequalities \(|X \cap Y| > i, |AX \cup AY| > i\) guarantee that \(X \cap Y, X \cup Y \in \mathcal{S}_i(A)\). Therefore,

\[ |A(X \cup Y)| + |A(X \cap Y)| \geq |X \cup Y| + |X \cap Y| + 2\omega_i(A) = |X| + |Y| + 2\omega_i(A). \]

Combining this with (1) yields

\[ |A(X \cup Y)| = |X \cup Y| + \omega_i(A), \]
\[ |A(X \cap Y)| = |X \cap Y| + \omega_i(A), \]

as claimed. ◊

Proposition 2.2. (i) \(\omega_i(A) = \omega_i(A^{-1})\);
(ii) \(B \in \mathcal{E}_i(A) \Rightarrow A^{-1}(\overline{AB}) = \overline{B} \) and, consequently, \(\overline{AB} \in \mathcal{E}_i(A^{-1})\);
(iii) \(B \in \mathcal{E}_i(A) \Leftrightarrow Bg \in \mathcal{E}_i(A) \) for each \(g \in G\);
(iv) if \(A\) is normal, then

\[ B \in \mathcal{E}_i(A) \Rightarrow A(\overline{AB}^{-1}) = \overline{B}^{-1}, \text{ and, consequently, } \overline{AB}^{-1} \in \mathcal{E}_i(A), \]

\[ B \in \mathcal{E}_i(A) \Leftrightarrow gBh \in \mathcal{E}_i(A) \text{ for any } g, h \in G. \]

Proof. (i) It is sufficient to show that \(\omega_i(A^{-1}) \leq \omega_i(A)\). Take an arbitrary \(B \in \mathcal{E}_i(A)\). Then \(|AB| = |B| + \omega_i(A)|. If \(g \in \overline{AB}\), then \(A^{-1}g \cap B = \emptyset\), implying \(A^{-1}(\overline{AB}) \subset \overline{B}\). Thus \(|AB| > i < |B| \leq |A^{-1}(\overline{AB})|\). Therefore \(\overline{AB} \in \mathcal{S}_i(A^{-1})\), which implies

\[ |B| \geq |A^{-1}(\overline{AB})| \geq \omega_i(A^{-1}) + |\overline{AB}| = \omega_i(A^{-1}) + |G| - |AB| \]
\[ = \omega_i(A^{-1}) + |G| - |B| - \omega_i(A) = \omega_i(A^{-1}) + |\overline{B}| - \omega_i(A). \]

(ii) Since \(\omega_i(A) = \omega_i(A^{-1})\), the inequality (2) implies

\[ |G| - |B| \geq |A^{-1}(\overline{AB})| \geq |G| - |B|. \]

Therefore, \(|A^{-1}(\overline{AB})| = |\overline{B}|\). Combining this with an inclusion \(A^{-1}(\overline{AB}) \subset \overline{B}\) yields \(A^{-1}(\overline{AB}) = \overline{B}\). Now the inclusion \(\overline{AB} \in \mathcal{E}_i(A^{-1})\) easily follows from the following sequence of equalities:

\[ |A^{-1}(\overline{AB})| = |\overline{B}| = |G| - |B| = |AB| + |\overline{AB}| - |B| \]
\[ = \omega_i(A) + |\overline{AB}| = \omega_i(A^{-1}) + |\overline{AB}|. \]

Proof of (iii) is a trivial exercise. Part (iv) is a direct consequence of (ii)-(iii) and normality of \(A\). ◊
3. Estimation of $\omega_1(A)$ of a normal subset $A \subset G$

In what follows, we assume that $A \subset G$, $A \neq G$ is normal and $S_1(A) \neq \emptyset$. It is easy to see that $S_1(A) \neq \emptyset$ if and only if there exists $b \in G^\#$ with $|A \{1, b\}| \leq |G| - 2$. Denoting by $m(A)$ the minimal value of $|Ag \cup A| - |A|$, $g \in G^\#$, we can say that $S_1(A) \neq \emptyset$ if and only if $m(A) + |A| \leq |G| - 2$. Since $m(A) \leq |A|$, the latter inequality always holds in the case of $2|A| + 2 \leq |G|$. If $m(A) = 0$, then a subgroup $Sta(A) = \{g \in G \mid gA = A\}$ is a non-trivial proper normal subgroup of $G$. The parameter $m(A)$ gives us an upper bound for $\omega_1(A)$. Indeed, $|A \{1, b\}| \geq \omega_1(A) + 2$ whenever $1 \neq b$ and $|A \{1, b\}| \leq |G| - 2$. Therefore

$$(3) \quad m(A) - 2 \geq \omega_1(A) - |A|.$$ 

Moreover the equality case in (3) holds if and only if $E_1(A)$ contains a subset with two elements.

In this section we study the situation where $E_1(A)$ contains no 2-element subset, or, equivalently, $m(A) - 2 > \omega_1(A) - |A|$. The main result may be formulated as follows:

**Theorem 3.1.** Let $A \subset G$ be a normal subset of a finite group $G$ with $S_1(A) \neq \emptyset$ and $\omega_1(A) - |A| < m(A) - 2$. Let $B \in E_1(A)$ be of minimal cardinality such that $1 \in B$. If $|B| > \omega_1(A) - |A| + 3$, then $B$ is a subgroup of $G$ such that $[G : N_G(B)] \leq 2$.

As a direct consequence, we obtain the following two results.

**Theorem 3.2.** Let $A \subset G$ be a normal subset such that $S_1(A) \neq \emptyset$. Assume that $\omega_1(A) - |A| < (m(A) - 3)/2$. Then there exists a proper subgroup $H \subset G$ such that $[G : N_G(H)] \leq 2$ and $|AH| = \omega_1(A) + |H|$.

**Theorem 3.3.** Let $G$ be a non-abelian finite simple group. Let $A \subset G$ be an arbitrary normal subset of $G$ such that $S_1(A) \neq \emptyset$. Then

$$|B| \geq 2, \quad |G| - 2 \geq |AB| \Rightarrow |AB| \geq |A| + |B| + \frac{m(A) - 3}{2}$$

holds for any $B \subset G$.

The rest of this section contains the proof of Theorem 3.1. Thus we always assume that $S_1(A) \neq \emptyset$ and $m(A) - 2 > \omega_1(A) - |A|$. The following notation will be used throughout the section:

- $k := \omega_1(A) - |A|$;
- $B \in E_1(A)$ is of minimal cardinality, $m := |B|$, $m > 2$;
- $C := AB, n := |C|$.

We always have

$$(4) \quad |G| = \omega_1(A) + m + n \Leftrightarrow |G| = |A| + k + m + n.$$ 

According to Proposition 2.2 (iv), $C^{-1} \in E_1(A)$. Therefore $n \geq m \geq 3$.

**Lemma 3.1.** Let $B_1, B_2 \in E_1(A)$ and $|B_1| = |B_2| = m$. Write $AB_i = C_i, i = 1, 2$.

Then

(i) $|B_1 \cap B_2| \in \{0, 1, m\}$;

(ii) either $|B_1 \cap C_2^{-1}| = |B_2 \cap C_1^{-1}| = m$, or $|B_1 \cap C_2^{-1}| \leq 1 \geq |B_2 \cap C_1^{-1}|$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. (i) Assume the contrary, i.e., $1 < |B_1 \cap B_2| < m$. Then

$$|A(B_1 \cup B_2)| + |A(B_1 \cap B_2)| \leq |AB_1 \cup AB_2| + |AB_1 \cap AB_2|$$

$$= |AB_1| + |AB_2| = 2\omega_1(A) + 2|B|.$$

Since $|B_1 \cap B_2| > 1$, $|A(B_1 \cap B_2)| \geq \omega_1(A) + |B_1 \cap B_2|$, implying

$$|A(B_1 \cup B_2)| \leq 2\omega_1(A) + 2|B| - |A(B_1 \cap B_2)|$$

$$\leq \omega_1(A) + 2|B| - |B_1 \cap B_2| \leq \omega_1(A) + 2m - 2 \leq \omega_1(A) + m + n - 2 = |G| - 2.$$

Thus, $|B_1 \cap B_2| > 1 < |A(B_1 \cup B_2)|$, and, by Proposition 2.1, $B_1 \cap B_2 \in \mathcal{E}_1(A)$ contrary to a minimality of $B$.

(ii) Assume that at least one of the inequalities

$$|B_1 \cap C_2^{-1}| \leq 1,$$

$$|B_2 \cap C_1^{-1}| \leq 1$$

does not hold. WLOG $|B_1 \cap C_2^{-1}| > 1$. Since $B_1 \in \mathcal{S}_1(A)$ and $|B_1 \cap C_2^{-1}| > 1$, $B_1 \cap C_2^{-1} \in \mathcal{S}_1(A)$, which, in turn, implies

$$(5) \quad |A(B_1 \cap C_2^{-1})| \geq \omega_1(A) + |B_1 \cap C_2^{-1}|.$$

On the other hand,

$$|A(B_1 \cap C_2^{-1})| \leq |AB_1 \cap AC_2^{-1}| = |AB_1| + |AC_2^{-1}| - |A(B_1 \cup C_2^{-1})|.$$

Since $AC_2^{-1} = B_2^{-1}$, $i = 1, 2$, the right part of the above inequality may be rewritten as follows:

$$|AB_1| + |AC_2^{-1}| - |A(B_1 \cup C_2^{-1})|$$

$$= \omega_1(A) + |B_1| + \omega_1(A) + |C_2| - |C_1 \cup B_2^{-1}|$$

$$= |G| + \omega_1(A) - |C_1 \cap B_2^{-1}|$$

$$= \omega_1(A) + |C_1 \cap B_2^{-1}|.$$

Comparing (5) and (6) gives us

$$1 < |B_1 \cap C_2^{-1}| \leq |C_1 \cap B_2^{-1}| = |B_2 \cap C_1^{-1}|.$$

Applying the same arguments to $B_2 \cap C_1^{-1}$, we obtain the inverse inequality which yields

$$|B_1 \cap C_2^{-1}| = |B_2 \cap C_1^{-1}| > 1.$$

Now we have

$$|AC_1^{-1} \cup AB_2| = |B_1^{-1} \cup C_2| = |B_1^{-1} \cap C_2| = |G| - |B_1^{-1} \cap C_2| \leq |G| - 2.$$

Thus $|C_1^{-1} \cap B_2| > 1 < |A(C_1^{-1} \cap B_2)|$, whence, by Proposition 2.1, $C_1^{-1} \cap B_2 \in \mathcal{E}_1(A)$.

Since $B_2$ has a minimal cardinality among the elements of $\mathcal{E}_1(A)$, $|C_1^{-1} \cap B_2| = |B_2|$, thus finishing the proof. \hfill \Box

Corollary 3.2. Let $B \in \mathcal{E}_1(A)$ with $|B| = m$. Then

(i) for any $x, y \in G$, $|B \cap B x y| \in \{0, 1, |B|\}$;

(ii) if $1 \in B$, then either $B$ is a subgroup of $G$ or $|gB \cap B| \leq 1 \geq |B y \cap B|$ holds for each $g \in G$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Lemma 3.3. If $|Bg \cap B| > 1$ for some $g \in G \setminus \{1\}$ (the case when $|gB \cap B| > 1$ is considered analogously). Then $Bg \in E_1(A)$ and by Lemma 3.1 $|Bg \cap B| = |B|$, or, equivalently, $Bg = B$. Thus $B$ is a union of the left cosets of the cyclic subgroup $\langle g \rangle$. This implies that $xB \cap B$ is a union of the left $\langle g \rangle$-cosets as well. In particular, $|xB \cap B|$ is divisible by the order $o(g)$ of $g$. On the other hand, $|xB \cap B| \in \{0, 1, |B|\}$ for all $x \in G$. Therefore $|xB \cap B| \in \{0, |B|\}$ for an arbitrary $x \in G$. That means $xB \cap B$ is either $\emptyset$ or $B$. Since $1 \in B$, $B$ is a subgroup of $G$. \hfill \Box

The latter statement makes it reasonable to split the general case into two subcases, depending on whether $B$ is a subgroup or not.

3.1. $B$ is not a subgroup of $G$. In this section we show that, under the assumptions of Theorem 3.1, $B$ should be a subgroup of $G$. In fact, we prove a stronger result.

**Lemma 3.3.** If $B$ is not a subgroup of $G$ and $1 \in B$, then

$$\frac{m(m-3)}{2} \leq k.$$

Write $AB = \overline{C}$, where $|B| = m, |C| = n$. For every $c \in C$ we have

$$AB = \overline{C}, \quad ABC^{-1} = \overline{C^{-1}}.$$

By applying Lemma 3.1, part (ii), we obtain that either

$$|B \cap (Cc)^{-1}| = |Bc^{-1} \cap C^{-1}| = |B|,$$

or

$$|B \cap (Cc^{-1})^{-1}| \leq 1 \geq |Bc^{-1} \cap C^{-1}|.$$

Since $1 \in B$ and $c \in C$, either

(7) $$C^{-1}c \supset B \subset cC^{-1},$$

or

(8) $$C^{-1}c \cap B = B \cap cC^{-1} = \{1\}.$$

Let $C_1$ be a set of those $c \in C$ satisfying (8) and $C_2$ be a set of those $c \in C$ satisfying (7). Clearly $C = C_1 \cup C_2$ and $C_1 \cap C_2 = \emptyset$.

**Proposition 3.4.** $|C_1| \geq m - 1$.

**Proof.** Assume the contrary, i.e. $|C_1| \leq m - 2$. Then $|C_2| = |C| - |C_1| = n - |C_1| \geq 2$.

As follows from (7)

$$B^{-1}C_2 \subset C \supset C_2B^{-1}.$$

This yields $Cb \supset C_2$ for each $b \in B$, whence

$$|ABB| = |\bigcup_{b \in B} Abb| = |\bigcup_{b \in B} \overline{Cb}| = |\bigcap_{b \in B} Cb| \leq |C_2| \leq |G| - 2.$$

Therefore $B^2 \in S_1(A)$, whence

(9) $$|AB^2| \geq \omega_1(A) + |B^2|.$$
On the other hand,
\[ |AB^2| \leq |C_2| = |G| - |C| + |C_1| \]
\[ = |G| - n + |C_1| \leq |G| - n + m - 2 = \omega_1(A) + 2m - 2. \]

Thus
\[ \omega_1(A) + |B^2| \leq \omega_1(A) + 2m - 2, \]
whence
\[ |B^2| \leq 2|B| - 2. \]

But now \(|B^2| \geq |B \cup Bb| = 2|B| - 1\) yields a contradiction (\(B\) is not a subgroup, so \(b \neq 1 \Rightarrow |B \cup Bb| = 2|B| - 1\)).

\[ \Box \]

Proof of Lemma 3.3. We have two equalities:
\[ ABc^{-1} = Cc^{-1}, \quad c \in C, \]
\[ AC^{-1} = B^{-1}. \]

Therefore,
\[ A(C^{-1} \cup BC_1^{-1}) = AC^{-1} \cup (\bigcup_{c \in C_1} ABc^{-1}) = B^{-1} \cup (\bigcup_{c \in C_1} Cc^{-1}) \]
\[ = B^{-1} \cap (\bigcap_{c \in C_1} Cc^{-1}) \subset G \setminus \{1\}. \]

This implies
\[ BC_1^{-1} \cup C^{-1} \subset A^{-1}, \]
whence
\[ (10) \quad |BC_1^{-1} \cup C^{-1}| \leq |G| - |A| = k + m + n. \]

By definition of \(C_1\):
\[ Bc^{-1} \cap C^{-1} = \{c^{-1}\} \]
for all \(c \in C_1\). Hence
\[ |BC_1^{-1} \cup C^{-1}| = |B^#C_1^{-1} \cup C^{-1}| = |B^#C_1^{-1}| + |C^{-1}| \]
(here \(B^# = B \setminus \{1\})). Together with (10) this yields
\[ (11) \quad |B^#C_1^{-1}| \leq k + m. \]

\(B\) is not a subgroup; therefore, by Corollary 3.2, \(|B^#c' \cap B^#c''| \leq 1\) whenever \(c' \neq c''\). Since \(|C_1| \geq |B| - 1 = m - 1\), we have at least \(m - 1\) sets \(B^#c, c \in C_1\) of cardinality \(m - 1\) such that any pair of them has at most one element in common. This implies that \(|B^#C_1^{-1}| \) has at least \(m(m - 1)/2\) elements. Together with (11), this implies \(m(m - 1)/2 \leq k + m\).  

\[ \Box \]
3.2. The case of $B$ being a subgroup of $G$. Denote $l = |G : N_G(B)|$. If $l \leq 2$, then we are done. Thus we may assume that $l \geq 3$. Let $B_1 = B, B_2, ..., B_l$ be a complete set of conjugates to $B$.

\[(12)\quad AB_i = C_i, \quad AC_i^{-1} = B_i^{-1}, \quad i = 1, ..., l.\]

By Lemma 3.1, $B_i \cap B_j = \{1\}$ whenever $i \neq j$. In other words, $B$ should be a TI-subgroup of $G$. Each $C_i$ is a union of $B_i$-cosets; therefore $m | n$. To prove Theorem 3.1 we consider two separate cases:

(i) $|C_i \cap C_j| \leq 1$ for each $i \neq j$.

(ii) there exists a pair $i \neq j$ with $|C_i \cap C_j| \geq 2$.

The first case is settled below.

**Proposition 3.5.** Case (i) is impossible.

**Proof.** We have $AC_i^{-1} = B_i^{-1}, i = 1, 2, ..., l$. Therefore,$\quad A(C_1^{-1} \cup C_2^{-1} \cup C_3^{-1}) \subset G \setminus \{1\}.$

This implies $\quad C_1^{-1} \cup C_2^{-1} \cup C_3^{-1} \subset A^{-1},$

whence $\quad 3n - 3 \leq |C_1^{-1} \cup C_2^{-1} \cup C_3^{-1}| \leq |G| - |A| = k + m + n.$

Since $m \leq n$, we obtain $m \leq k + 3$, a contradiction. $\Box$

To consider the second case, we may assume that $|C_1 \cap C_2| \geq 2$.

Denote $D = C_1 \cap C_2$. For each $d \in D$ we can write

\[(13)\quad AB_1 d^{-1} = C_1 d^{-1},\]

\[(14)\quad AB_2 = C_2.\]

By Lemma 3.1, part (ii), either $\quad B_1 d^{-1} \subset C_2^{-1}$ and $B_2 \subset (C_1 d^{-1})^{-1},$

or $\quad |B_1 d^{-1} \cap C_2^{-1}| \leq 1 \geq |B_2 \subset (C_1 d^{-1})^{-1}|.$

Equivalently, either

\[(15)\quad dB_1 \subset C_2 \quad \text{and} \quad B_2 d \subset C_1,\]

or

\[(16)\quad B_1 \cap C_2^{-1} d = B_2 \cap dC_1^{-1} = \{1\}\]

Now Theorem 3.1 is a direct consequence of the following claim.

**Lemma 3.6.** If $|C_1 \cap C_2| \geq 2$, then $m \leq k + 2$.

**Proof.** First assume that there exist at least two elements $d_1, d_2 \in D$ which satisfy (16), i.e.,

\[(17)\quad B_1 \cap C_2^{-1} d_i = B_2 \cap d_i C_1^{-1} = \{1\}, \quad i = 1, 2.\]
Then we have three equalities
\[ AB_1 d_1^{-1} = \overline{C_1 d_1^{-1}} \subset G \setminus \{1\}, \]
\[ AB_1 d_2^{-1} = \overline{C_1 d_2^{-1}} \subset G \setminus \{1\}, \]
\[ AC_2^{-1} = \overline{B_2^{-1}} \subset G \setminus \{1\}. \]

Now \( A(B_1 d_1^{-1} \cup B_1 d_2^{-1} \cup C_2^{-1}) \subset G \setminus \{1\}, \) whence \( B_1 d_1^{-1} \cup B_1 d_2^{-1} \cup C_2^{-1} \subset \overline{A^{-1}}. \)
This gives us the following inequality
\[ |B_1 d_1^{-1} \cup B_1 d_2^{-1} \cup C_2^{-1}| \leq |G| - |A| = \omega_1(A) - |A| + m + n = k + m + n. \]

By (17) the left side may be estimated as follows: \(^2\)
\[ |B_1 d_1^{-1} \cup B_1 d_2^{-1} \cup C_2^{-1}| = 2|B_2| - 2 + |C| = 2m + n - 2. \]

Hence \( 2m + n - 2 \leq k + m + n, \) as required.

Thus we may assume that the number of elements of \( D \) satisfying (16) is not greater than 1. Therefore, there is a subset \( F \subset D \) such that \( |F| \geq |D| - 1 \) and
\[ fB_1 \subset C_2, \quad B_2 f \subset C_1 \]
holds for all \( f \in F. \)

We claim that \( FB_1 = F. \) Indeed, \( fB_1 \subset C_2 \) for each \( f \in F. \) On the other hand, \( f \in C_1 \) and \( C_1 B_1 = C_1, \) implying \( fB_1 \subset C_1. \) Therefore, \( fB_1 \subset C_1 \cap C_2 = D \) This shows that an element \( fb, b \in B_1 \) doesn’t satisfy (16) for each \( b \in B_1. \) Hence \( fb \)
satisfies (15), whence \( fb \in F. \)

Write
\[ |AB_2 B_1| = |(AB_1 \cup AB_2) B_1| = |(\overline{C_1} \cup \overline{C_2}) B_1| = |\overline{D} B_1| \]
\[ = | \bigcup_{b \in B_1} \overline{D} b | \leq |F| = |G| - |F| \leq |G| - |D| + 1. \]

Since \( FB_1 = F \) and \( F \neq \emptyset, |F| \geq |B_1| = m. \) Hence \( |AB_2 B_1| \leq |G| - 2 \) and we can write
\[ |AB_2 B_1| \geq \omega_1(A) + |B_2 B_1| = \omega_1(A) + |B|^2 = \omega_1(A) + m^2. \]

Thus
\[ \omega_1(A) + m^2 \leq |G| + 1 - |D| = |G| - |C_1 \cap C_2| + 1 = |\overline{C_1} \cup \overline{C_2}| + 1 \]
\[ = |\overline{C_1} \cup \overline{C_2}| + 1 = |AB_1 \cup AB_2| + 1 \]
\[ \leq 2 \omega_1(A) + 2|B| - |A| + 1 = 2 \omega_1(A) - |A| + 2m + 1. \]

Finally,
\[ m^2 - 2m \leq \omega_1(A) - |A| + 1 = k + 1. \]
Since \( m \geq 3, m \leq m^2 - 2m < k + 2 \) as desired. \( \Box \)

**Proof of Theorem 3.2.** Let \( B \in \mathcal{E}_1(A) \) be of minimal cardinality \( m. \) WLOG \( 1 \in B. \)
Since \( \omega_1(A) < (m(A) - 3)/2 + |A| < m(A) - 2 + |A|, \) \( m > 2. \) If \( |B| > \omega_1(A) - |A| + 3, \) then we have completed our proof via Theorem 3.1. Otherwise, \( |B| \leq \omega_1(A) - |A| + 3 \) and \( |AB| = |A| + |B| + k \leq |A| + 2k + 3. \) But \( |B| > 2. \) Therefore \( |AB| \geq |A| + m(A). \) Consequently, \( 2k + 3 \geq m(A), \) contrary to our assumption
\[ \omega_1(A) - |A| = k < \frac{m(A) - 3}{2}. \]
This is a contradiction. \( \Box \)

\(^2\)Since \( B_1 d_1^{-1} \cap C_2^{-1} = \{ d_1^{-1} \} \) and \( d_1 \neq d_2, B_1 d_1^{-1} \) and \( B_1 d_2^{-1} \) are disjoint \( B_1 \)-cosets.
4. The estimation of $m(A)$

In this section we assume that $G$ is a finite non-abelian simple group with a normal subset $A$, $|A| \leq |G|/4$.

For each $\lambda \geq 0$ we define

$$A_\lambda = \{ g \in G \mid |A \cup Ag| \leq |A| + \lambda \} = \{ g \in G \mid |A \cap Ag| \geq |A| - \lambda \}.$$  

Clearly, $A_\lambda$ is a normal subset of $G$ and $A_\lambda \subset A_\mu$ whenever $\lambda \leq \mu$. Further, $A_\lambda = G$ for each $\lambda \geq |A|$. The simple calculations give us

$$\sum_{g \in G \setminus \{1\}} |A \cap Ag| = |A|^2 - |A|.$$  

**Lemma 4.1.** $A_\lambda A_\mu \subset A_{\lambda + \mu}$.

**Proof.** Take an arbitrary $g \in A_\lambda$ and $h \in A_\mu$. One can write

$$|A \cup Ahg| = |Ag^{-1} \cup Ah| \leq |Ag^{-1} \cup Ah \cup A|$$

$$= |(Ag^{-1} \cup A) \cup (Ah \cup A)| = |Ag^{-1} \cup A| + |Ah \cup A| - |(Ag^{-1} \cup A) \cap (Ah \cup A)|$$

$$\leq |A| + \lambda + |A| + \mu - |A| = |A| + \lambda + \mu.$$  

Since $1 \in A_\lambda$ for each $\lambda \geq 0$, then $|A_\lambda| \geq 1$ for all $\lambda \geq 0$. As follows from the definition, $m(A)$ is the minimal $\lambda$ with $|A| > 1$. We abbreviate $m := m(A)$. Since $G$ is simple, $0 < m$. In what follows we write $F_n = A_{nm} \setminus A_{m(n-1)}$, $n \geq 1$. In particular, $F_1 = A_1 \setminus \{1\}$. It is clear that $F_n$, $n \geq 1$ are disjoint and $A_{nm} = \{1\} \cup F_1 \cup \ldots \cup F_n$.

**Lemma 4.2.** If $A_{nm} \neq G$ for some $n \geq 2$, then

$$A_{nm} \geq |F_1| + |A_{m(n-1)}|;$$

$$|F_n| \geq |F_1|;$$

$$|A_{nm}| \geq 1 + n|F_1|.$$  

**Proof.** (i) Since $G$ is simple, the implication

$$|AB| \neq |G| \Rightarrow |AB| \geq |A| + |B| - 1$$

holds for each pair $A, B$ of normal subsets (see Theorem 1.4 of [2]).

By Lemma 4.1 $A_m A_{m(n-1)} \subset A_{nm} \neq G$, whence

$$|A_{nm}| \geq |A_m| + |A_{m(n-1)}| - 1 = |F_1| + |A_{m(n-1)}|.$$  

(ii) Since $A_{nm} \supset A_{m(n-1)}$, $|F_n| = |A_{nm}| - |A_{m(n-1)}|$ and (ii) follows.

Part (iii) of the claim follows from (i) and (ii).  

**Lemma 4.3.** If $|F_1| \geq |A|$, then $3m > |A|$.

**Proof.** At first consider the case $A_{2m} = G$. Since $|A \cap Ag| \geq |A| - \lambda$ for all $g \in A_\lambda$, the inequality $|A \cap Ag| \geq |A| - 2m$ holds for all $g \in G$. By applying (20) we obtain

$$|A|(|A| - 1) \geq (|A| - 2m)(|G| - 1) > (|A| - 2m) \cdot 3|A|.$$  

After cancellation we obtain

$$|A| - 1 > 3|A| - 6m$$

and the claim follows.
Assume now that \( A_{2m} \neq G \). Then \( \{1\} \cup F_1 \cup F_2 \neq G \) and, due to (20),
\[
|A|(|A| - 1) \geq \sum_{g \in F_1} |A \cap Ag| + \sum_{g \in F_2} |A \cap Ag| \geq (|A| - m)|F_1| + (|A| - 2m)|F_2|.
\]
But \( |F_2| \geq |F_1| \geq |A| \) by Lemma 4.2. Therefore \( |A|(|A| - 1) \geq (2|A| - 3m)|A| \). This completes the proof. \( \diamondsuit \)

Let us order the elements of \( G = \{g_0, \ldots, g_{n-1}\}, n = |G| \), in such a way that \( i < j \) implies \( \lambda_i \leq \lambda_j \), where \( \lambda_j = |A \cap Ag_j| \).

**Proposition 4.4.** If \( j \leq |F_1| i \), then \( \lambda_j \geq |A| - m i \).

**Proof.** We claim that \( j \leq |F_1| i \) implies that \( g_j \in A_m \). Indeed, this inclusion is evident in the case \( A_m = G \). Thus, we can assume that \( A_m \neq G \), which implies, according to (23), that \( |A_m| \geq 1 + i|F_1| \). Therefore, \( A_m \) contains \( m|F_1| + 1 \) first elements of \( G \), i.e., \( g_j \in A_m \) for each \( 0 \leq j \leq i|F_1| \). As follows from the definition of \( A_m \), \( \lambda_j = |A \cap Ag_j| \geq |A| - m i \). \( \diamondsuit \)

**Proposition 4.5.** Let \( n \) be an integer satisfying
\[
\frac{2|A|}{3m} \leq n \leq \frac{2|A|}{3m} + 1
\]
and \( |F_1| \leq |A| \). Then \( n|F_1| \leq |G| - 3 \).

**Proof.** Denote \( a = |A| \). Since \( |F_1| \leq |A| \) and \( |G| \geq 4|A| \), it is sufficient to show that \( |F_1|(n - 1) \leq 3a - 3 \). Assume the contrary, i.e., \( |F_1|(n - 1) \geq 3a - 2 \). Then, by Proposition 4.4, \( \lambda_{3a-2} \geq a - (n - 1)m \), whence
\[
\lambda_{3a-2} \geq a - (n - 1)m \geq a - \frac{2a}{3m} m = \frac{a}{3}.
\]
Therefore, \( \lambda_i \geq a/3 \) for all \( 1 \leq i \leq 3a - 2 \). But this implies that \( a(a - 1) \geq a(3a - 2)/3 \), which is a contradiction. \( \diamondsuit \)

**Theorem 4.1.** At least one of two inequalities
\[
|F_1| < 3m, \quad |A| < 6m
\]
holds.

**Proof.** Assume the contrary, i.e., \( |F_1| \geq 3m \) and \( |A| \geq 6m \). By Lemma 4.3, \( |F_1| < |A| \). Take an integer \( n \) such that \( \frac{2a}{3m} \leq n \leq \frac{2a}{3m} + 1 \).

Due to Proposition 4.5, \( n|F_1| \leq |G| - 3 \). Consider the sets \( S_i = \{g_j \mid i|F_1| \geq j > (i - 1)|F_1|, i = 1, \ldots, n\} \). Clearly \( |S_j| = |F_1| \). Since \( n|F_1| \leq |G| - 3 \), \( S_1 \cup \ldots \cup S_n \subset G \setminus \{e\} \). By Proposition 4.4, \( \lambda_j \geq a - mi \) for all \( j \) satisfying \( g_j \in S_i \). Therefore,
\[
a(a - 1) \geq \sum_{i=1}^{n} (a - mi)|S_i| = |F_1| \left( na - m \frac{n(n + 1)}{2} \right) \geq 3m \left( na - m \frac{n(n + 1)}{2} \right).
\]

By the choice of \( n \), \( m \geq \frac{2a}{3n} \), whence
\[
a(a - 1) \geq 3 \cdot \frac{2a}{3n} \left( na - m \frac{n(n + 1)}{2} \right) = 2a^2 - am(n + 1).
\]

(Here, as before, \( a = |A| \).)
After simple transformations, we obtain \( m(n + 1) \geq a + 1 \). On the other hand, \( n + 1 \leq \frac{2a}{3m} + 2 \), whence

\[
\left( \frac{2a}{3m} + 2 \right) m \geq a + 1 \iff \frac{2a}{3} + 2m \geq a + 1 \iff 2m \geq \frac{a}{3} + 1
\]

contrary to \( m \leq a/6 \). ♦

As a corollary we obtain the following:

**Theorem 4.2.** Let \( A \) be a normal subset of \( G \) with \( |A| \leq |G|/4 \). Denote by \( l \) the cardinality of the smallest non-trivial conjugacy class of \( G \). Then

\[
m(A) > \min \left( \frac{l}{3}, \frac{|A|}{6} \right) \geq \frac{l}{6}.
\]

**Proof.** Due to Theorem 4.1, \( m(A) = m > |F_1|/3 \) or \( m(A) = m > |A|/6 \). But \( F_1 \) is a non-trivial normal set. Therefore \( m(A) > l/3 \) or \( m(A) > |A|/6 \), as desired. ♦

It is easy to see that Theorem 1.1 is a direct consequence of this result and of Theorem 3.3.

5. PROOFS OF THEOREMS 1.2, 1.3

**Proof of Theorem 1.2.** Denote by \( l \) the minimal cardinality of non-trivial conjugacy classes of \( G \). If \( l \geq 43 \), then Theorem 1.1 implies our claim. Thus we may assume that \( l \leq 42 \) which implies that \( G \) has a primitive permutation representation of a degree of 42 at most. The classification of all primitive groups of a degree of 50 at most, was done in [8] without CFSG. According to [3], either \( G = A_n \) or a point stabilizer of \( G \) has a trivial centre. Thus, in the case of \( G \neq A_n \), \( G \) has a maximal subgroup of index of, at most, 21. Due to [3], \( G \) is one of the following groups given in Table 1.

**Table 1**

<table>
<thead>
<tr>
<th>( G )</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A_5 )</td>
<td>6</td>
</tr>
<tr>
<td>( A_6 )</td>
<td>10</td>
</tr>
<tr>
<td>( L_2(8))</td>
<td>9</td>
</tr>
<tr>
<td>( L_2(16))</td>
<td>17</td>
</tr>
<tr>
<td>( L_2(7))</td>
<td>7</td>
</tr>
<tr>
<td>( L_2(11))</td>
<td>11</td>
</tr>
<tr>
<td>( L_2(13))</td>
<td>14</td>
</tr>
<tr>
<td>( L_2(17))</td>
<td>18</td>
</tr>
<tr>
<td>( L_2(19))</td>
<td>20</td>
</tr>
<tr>
<td>( L_3(3))</td>
<td>13</td>
</tr>
<tr>
<td>( M_{11} )</td>
<td>11</td>
</tr>
<tr>
<td>( M_{12} )</td>
<td>12</td>
</tr>
<tr>
<td>( A_n ), ( n \leq 42 )</td>
<td></td>
</tr>
</tbody>
</table>

The groups \( A_n, n \geq 7, L_3(3), M_{11}, M_{12} \) have no non-trivial conjugacy class with fewer than 43 elements.

The groups \( L_2(p), p \) odd, \( p > 7, L_2(8), L_2(16) \) have no non-trivial conjugacy class with fewer than 40 elements according to 8.27 of [6].
In the case of $G = A_6$, there are only two normal subsets $A$ of $G$ satisfying the assumption $|A| \leq |G|/4$, namely: the conjugacy classes $C_1$ and $C_2$ of cyclic types [3] and [3, 3], respectively. Using the multiplication tables of the conjugacy classes of $A_6$, one can easily check that $m(A) \geq 8$ in both cases, $A = C_1$ and $A = C_2$. Therefore, by Theorem 3.3,

$$|AB| \geq |A| + |B| + (m(A) - 3)/2 > |A| + |B| + 2,$$

as desired.

The case of $G = L_2(7)$ may be settled analogously.

Consider now the remaining case $G = A_5$. Denote by $C_1, C_2, C_3, C_4$ all its non-trivial conjugacy classes (we assume that $|C_1| = |C_2| = 12, |C_3| = 15, |C_4| = 20$). There are only three normal subsets $A$ of $A_5$ satisfying $|A| \leq |G|/4$: $A = C_1, A = C_2, A = C_3$. If $A = C_3$, then $m(A) \geq 8$ and we are done. Since $C_1$ and $C_2$ are conjugate by an outer automorphism of $A_5$, it is enough to consider the only case of $A = C_1$. In this case, $m(A) = 7$ and the arguments we used before do not work. To show that our claim remains true even in this case, we assume the contrary, i.e.

$$\exists B \subset G, |B| > 1 \text{ and } |G| - 2 \geq |AB| \leq |A| + |B| + 2.$$

We also assume that $B$ has a minimal cardinality among all subsets of $A_5$ satisfying the above conditions.

If $B$ is not a subgroup, then by Lemma 3.3 $|B| (|B| - 3)/2 \leq \omega_1(A) - |A| \leq 2$. Therefore $|B| \leq 4$, whence $|AB| \leq |A| + |B| + 2 \leq |A| + 6$. On the other hand, $|B| \geq 2$ implies that $|AB| \geq |A| + m(A) = |A| + 7$. This is a contradiction. Hence $B$ should be a subgroup of $A_5$. By Theorem 3.1 $|B| \leq 3 + \omega_1(A) - |A| \leq 5$. But direct calculations show that $|AB| \geq |A| + |B| + 3$ for each subgroup $B \leq A_5, |B| \leq 5$.

As a direct consequence we obtain the proof of Theorem 1.3. 1)-4) and 6)-9) are immediate corollaries of Theorem 4.2.

5) If $G$ is simple, then

$$3 + \sum_{A \in A} |A| \leq | \prod_{A \in A} A | \leq 1 + \sum_{B \in B} |B|,$$

$$3 + \sum_{B \in B} |B| \leq | \prod_{B \in B} B | \leq 1 + \sum_{A \in A} |A|,$$

a contradiction.

10) Assume that $G$ is simple and $Cla(G)^\# = \{C_1, \ldots, C_k\}$ with $|C_1| \leq |C_2| \leq \ldots \leq |C_k|$. Consider $C_2 \cdot \ldots \cdot C_k$. We claim that $|C_2 \cdot \ldots \cdot C_k| \geq |G| - 1$. Indeed, if it is not true, then by Theorem 1.2 $|C_2 \cdot \ldots \cdot C_k| \geq |C_2| + \ldots + |C_k| + 3$, implying $|C_2 \cdot \ldots \cdot C_k| \geq |C_2| + \ldots + |C_k| + |C_1| = |G| - 1$. Again, a contradiction.

Thus $|C_2 \cdot \ldots \cdot C_k| \geq |G| - 1$.

11) If $|C_k^k| \leq |G| - 2$, then $|G| - 2 \geq |C_k| \geq k|C| + 3(k - 1) \geq |G| + k - 3$, implying $k \leq 1$, a contradiction. Thus $|C_k^k| = |G| - 1$ is the unique case we have to consider. In this case, $C_k^k = G \setminus \{1\}$, which, in turn, implies $C_k^{k - 1} \subset C^{-1}$. Hence

$$|C| (k - 1) + 3(k - 2) \leq |C_k^{k - 1}| \leq |G| - |C|.$$

Consequently, $|C| k + 3k - 6 \leq |G| \leq k|C| + 2k$. Whence $k \leq 6$, contrary to the assumption.

\[\square\]
REFERENCES


DEPARTMENT OF MATHEMATICS & COMPUTER SCIENCE, BAR-ILAN UNIVERSITY, 52900 RAMAT-GAN, ISRAEL