TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 349, Number 11, November 1997, Pages 4401–4414
S 0002-9947(97)01866-7

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 (1996), 577–603.

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 $T = \overline{S}^{-1}g$, where $\overline{S}$ 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.

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 $Cla(G)^{\#}$ 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 $C, D \in Cla(G)^{\#}$;
2) $CD \subseteq C^{-1} \cup D$ for some $C, D \in Cla(G)^{\#}$;
3) $CD \subseteq C^{-1} \cup D^{-1}$ for some $C, D \in Cla(G)^{\#}$;
4) $\prod_{B \in \mathcal{B}} B \subseteq \bigcup_{B \in \mathcal{B}} B \cup \{1\}$ for some $\mathcal{B} \subset Cla(G)^{\#}$;
5) there exist $\mathcal{A}, \mathcal{B} \subset Cla(G)^{\#}$ such that

$$\prod_{A \in \mathcal{A}} A \subseteq \bigcup_{B \in \mathcal{B}} B \cup \{1\},$$

$$\prod_{B \in \mathcal{B}} B \subseteq \bigcup_{A \in \mathcal{A}} A \cup \{1\}.$$

6) $CC^{-1} \subseteq C \cup C^{-1} \cup \{1\}$ for some $C \in Cla(G)^{\#}$;
7) $C^2 \subseteq C \cup C^{-1}$ for some $C \in Cla(G)^{\#}$;
8) $C^2 \subseteq \{1\} \cup D \cup D^{-1}$ for some $C, D \in Cla(G)^{\#}$;
9) $\prod_{C \in Cla(G)^{\#}} C \neq G$;
10) $|\prod_{C \in Cla(G)^{\#} \setminus \{D\}} C| < |G| - 1$, where $D \in Cla(G)^{\#}$ is a conjugacy class of minimal cardinality;
11) if $|C| \geq |G|/k - 2, k > 6, C \in Cla(G)^{\#}$ 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

$$\mathcal{S}_i(A) = \{B \subset G \mid |B| > i \text{ and } |\overline{AB}| > i\};$$
$$\omega_i(A) = \ min\{|AB| - |B| \mid B \in \mathcal{S}_i(A)\};$$
$$\mathcal{E}_i(A) = \{B \in \mathcal{S}_i(A) \mid |AB| = |B| + \omega_i(A)\}.$$

Since $\mathcal{S}_i(A) \subseteq \mathcal{S}_j(A)$ 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 $|X \cap Y| > i, |\overline{AX \cup AY}| > i$. 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

$$|A(X \cup Y)| + |A(X \cap Y)| \leq |AX| + |AY| = |X| + |Y| + 2\omega_i(A). \tag{1}$$

The inequalities $|X \cap Y| > i, |\overline{AX \cup AY}| > i$ 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. $\diamondsuit$

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*

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

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

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 $|\overline{AB}| > i < |B| \leq |\overline{A^{-1}(\overline{AB})}|$. Therefore $\overline{AB} \in \mathcal{S}_i(A^{-1})$, which implies

$$\begin{aligned} |\overline{B}| &\geq |A^{-1}(\overline{AB})| \geq \omega_i(A^{-1}) + |\overline{AB}| = \omega_i(A^{-1}) + |G| - |AB| \\ &= \omega_i(A^{-1}) + |G| - |B| - \omega_i(A) = \omega_i(A^{-1}) + |\overline{B}| - \omega_i(A). \end{aligned} \tag{2}$$

(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:

$$\begin{aligned} |A^{-1}(\overline{AB})| &= |\overline{B}| = |G| - |B| = |AB| + |\overline{AB}| - |B| \\ &= \omega_i(A) + |\overline{AB}| = \omega_i(A^{-1}) + |\overline{AB}|. \end{aligned}$$

Proof of (iii) is a trivial exercise. Part (iv) is a direct consequence of (ii)-(iii) and normality of A. $\diamondsuit$

3. Estimation of $\omega_1(A)$ of a normal subset $A \subset G$

In what follows, we assume that $A \subseteq G, A \neq G$ is normal and $\mathcal{S}_1(A) \neq \emptyset$. It is easy to see that $\mathcal{S}_1(A) \neq \emptyset$ 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 $\mathcal{S}_1(A) \neq \emptyset$ 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

$$m(A) - 2 \geq \omega_1(A) - |A|. \tag{3}$$

Moreover the equality case in (3) holds if and only if $\mathcal{E}_1(A)$ contains a subset with two elements.

In this section we study the situation where $\mathcal{E}_1(A)$ 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 $\mathcal{S}_1(A) \neq \emptyset$ and $\omega_1(A) - |A| < m(A) - 2$. Let $B \in \mathcal{E}_1(A)$ 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 $\mathcal{S}_1(A) \neq \emptyset$. Assume that $\omega_1(A) - |A| < (m(A) - 3)/2$. Then there exists a proper subgroup $H < G$ 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 $\mathcal{S}_1(A) \neq \emptyset$. 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 $\mathcal{S}_1(A) \neq \emptyset$ and $m(A) - 2 > \omega_1(A) - |A|$. The following notation will be used throughout the section:

- $k := \omega_1(A) - |A|$;
- $B \in \mathcal{E}_1(A)$ is of minimal cardinality, $m := |B|, m > 2$;
- $C := \overline{AB}, n := |C|$.

We always have

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

According to Proposition 2.2 (iv), $C^{-1} \in \mathcal{E}_1(A)$. Therefore $n \geq m \geq 3$.

Lemma 3.1. *Let $B_1, B_2 \in \mathcal{E}_1(A)$ and $|B_1| = |B_2| = m$. Write $AB_i = \overline{C}_i, i = 1, 2$. 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 $|B_1 \cap C_2^{-1}| \leq 1 \geq |B_2 \cap C_1^{-1}|$.

Proof. (i) Assume the contrary, *i.e.,* $1 < |B_1 \cap B_2| < m$. Then

$$\begin{aligned}|A(B_1 \cup B_2)| + |A(B_1 \cap B_2)| &\leq |AB_1 \cup AB_2| + |AB_1 \cap AB_2| \\ &= |AB_1| + |AB_2| = 2\omega_1(A) + 2|B|.\end{aligned}$$

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

$$\begin{aligned}&|A(B_1 \cup B_2)| \leq 2\omega_1(A) + 2|B| - |A(B_1 \cap B_2)| \\ &\quad\leq \omega_1(A) + 2|B| - |B_1 \cap B_2| \leq \omega_1(A) + 2m - 2 \leq \omega_1(A) + m + n - 2 = |G| - 2.\end{aligned}$$

Thus, $|B_1 \cap B_2| > 1 < |\overline{A(B_1 \cup B_2)}|$, 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

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

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 $AC_i^{-1} = \overline{B}_i^{-1}, i = 1, 2$, the right part of the above inequality may be rewritten as follows:

$$\begin{aligned}&|AB_1| + |AC_2^{-1}| - |A(B_1 \cup C_2^{-1})| \\ &\qquad= \omega_1(A) + |B_1| + \omega_1(A) + |C_2| - |\overline{C}_1 \cup \overline{B}_2^{-1}| \\ &\qquad= |G| + \omega_1(A) - |\overline{C_1 \cap B_2^{-1}}| \\ &\qquad= \omega_1(A) + |C_1 \cap B_2^{-1}|.\end{aligned} \tag{6}$$

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

$$|AC_1^{-1} \cup AB_2| = |\overline{B}_1^{-1} \cup \overline{C}_2| = |\overline{B_1^{-1} \cap C_2}| = |G| - |B_1^{-1} \cap C_2| \leq |G| - 2.$$

Thus $|C_1^{-1} \cap B_2| > 1 < |\overline{A(C_1^{-1} \cap B_2)}|$, 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. $\diamondsuit$

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

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

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

Proof. (i) is a direct consequence of the previous claim and Proposition 2.2, part (ii).

(ii) Assume that $|Bg \cap B| > 1$ for some $g \in G\backslash\{1\}$ (the case when $|gB \cap B| > 1$ is considered analogously). Then $Bg \in \mathcal{E}_1(A)$ 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. $\diamondsuit$

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*

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

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

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

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

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

or

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

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

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

or

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

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. $|C_1| \ge m - 1$.

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

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

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

Therefore $B^2 \in \mathcal{S}_1(A)$, whence

$$|AB^2| \ge \omega_1(A) + |B^2|. \tag{9}$$

On the other hand,

$$|AB^2| \leq |\overline{C}_2| = |G| - |C| + |C_1|$$

$$= |G| - n + |C_1| \leq |G| - n + m - 2 = \omega_1(A) + 2m - 2.$$

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 $b \neq 1 \Rightarrow |B \cup Bb| = 2|B| - 1$). $\diamondsuit$

Proof of Lemma 3.3. We have two equalities:

$$AB c^{-1} = \overline{Cc^{-1}}, \qquad c \in C,$$

$$AC^{-1} = \overline{B^{-1}}.$$

Therefore,

$$A(C^{-1} \cup BC_1^{-1}) = AC^{-1} \cup (\bigcup_{c \in C_1} ABc^{-1}) = \overline{B^{-1}} \cup (\bigcup_{c \in C_1} \overline{Cc^{-1}})$$

$$= \overline{B^{-1} \cap (\bigcap_{c \in C_1} Cc^{-1})} \subset G \setminus \{1\}.$$

This implies

$$BC_1^{-1} \cup C^{-1} \subset \overline{A^{-1}},$$

whence

$$|BC_1^{-1} \cup C^{-1}| \leq |G| - |A| = k + m + n. \tag{10}$$

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

$$|B^{\#}C_1^{-1}| \leq k + m. \tag{11}$$

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 $B^{\#}c, c \in C_1^{-1}$ 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 $m(m-1)/2 \leq k + m$. $\diamondsuit$

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

$$AB_i = \overline{C}_i, \quad AC_i^{-1} = \overline{B_i^{-1}}, \qquad i = 1, ..., l. \tag{12}$$

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

(i) $|C_i \cap C_j| \le 1$ for each $i \ne j$.

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

The first case is settled below.

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

Proof. We have $AC_i^{-1} = \overline{B_i^{-1}}, i = 1, 2, ..., l$. Therefore,

$$A(C_1^{-1} \cup C_2^{-1} \cup C_3^{-1}) \subset G \setminus \{1\}.$$

This implies

$$C_1^{-1} \cup C_2^{-1} \cup C_3^{-1} \subset \overline{A^{-1}},$$

whence

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

Since $m \le n$, we obtain $m \le k + 3$, a contradiction. ◊

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

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

$$AB_1 d^{-1} = \overline{C_1 d^{-1}}, \tag{13}$$

$$AB_2 = \overline{C}_2. \tag{14}$$

By Lemma 3.1, part (ii), either

$$B_1 d^{-1} \subset C_2^{-1} \ \text{ and } B_2 \subset (C_1 d^{-1})^{-1},$$

or

$$|B_1 d^{-1} \cap C_2^{-1}| \le 1 \ge |B_2 \subset (C_1 d^{-1})^{-1}|.$$

Equivalently, either

$$dB_1 \subset C_2 \ \text{ and } B_2 d \subset C_1, \tag{15}$$

or

$$B_1 \cap C_2^{-1} d = B_2 \cap dC_1^{-1} = \{1\} \tag{16}$$

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

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

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

$$B_1 \cap C_2^{-1} d_i = B_2 \cap d_i C_1^{-1} = \{1\}, \qquad i = 1, 2. \tag{17}$$

Then we have three equalities

$$AB_1d_1^{-1} = \overline{C_1d_1^{-1}} \subset G \setminus \{1\},$$
$$AB_1d_2^{-1} = \overline{C_1d_2^{-1}} \subset G \setminus \{1\}, \tag{18}$$
$$AC_2^{-1} = \overline{B_2^{-1}} \subset G \setminus \{1\}.$$

Now $A(B_1d_1^{-1} \cup B_1d_2^{-1} \cup C_2^{-1}) \subset G \setminus \{1\}$, whence $B_1d_1^{-1} \cup B_1d_2^{-1} \cup C_2^{-1} \subset \overline{A^{-1}}$. This gives us the following inequality

$$|B_1d_1^{-1} \cup B_1d_2^{-1} \cup C_2^{-1}| \le |G| - |A| = \omega_1(A) - |A| + m + n = k + m + n.$$

By (17) the left side may be estimated as follows: [2]

$$|B_1d_1^{-1} \cup B_1d_2^{-1} \cup C_2^{-1}| = 2|B_1| - 2 + |C| = 2m + n - 2.$$

Hence $2m + n - 2 \le k + m + n$, 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 $|F| \ge |D| - 1$ and

$$fB_1 \subset C_2, \quad B_2f \subset C_1 \tag{19}$$

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 $C_1B_1 = C_1$, 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

$$|AB_2B_1| = |(AB_1 \cup AB_2)B_1| = |(\overline{C}_1 \cup \overline{C}_2)B_1| = |\overline{D}B_1|$$
$$= |\bigcup_{b\in B_1} \overline{Db}| \le |\overline{F}| = |G| - |F| \le |G| - |D| + 1.$$

Since $FB_1 = F$ and $F \ne \emptyset$, $|F| \ge |B_1| = m$. Hence $|AB_2B_1| \le |G| - 2$ and we can write

$$|AB_2B_1| \ge \omega_1(A) + |B_2B_1| = \omega_1(A) + |B|^2 = \omega_1(A) + m^2.$$

Thus

$$\omega_1(A) + m^2 \le |G| + 1 - |D| = |G| - |C_1 \cap C_2| + 1 = |\overline{C_1 \cap C_2}| + 1$$
$$= |\overline{C}_1 \cup \overline{C}_2| + 1 = |AB_1 \cup AB_2| + 1$$
$$\le 2\omega_1(A) + 2|B| - |A| + 1 = 2\omega_1(A) - |A| + 2m + 1.$$

Finally,

$$m^2 - 2m \le \omega_1(A) - |A| + 1 = k + 1.$$

Since $m \ge 3$, $m \le m^2 - 2m < k + 2$ as desired. $\diamondsuit$

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, $|B| \le \omega_1(A) - |A| + 3$ and $|AB| = |A| + |B| + k \le |A| + 2k + 3$. But $|B| > 2$. Therefore $|AB| \ge |A| + m(A)$. Consequently, $2k + 3 \ge m(A)$, contrary to our assumption

$$\omega_1(A) - |A| = k < \frac{m(A) - 3}{2}.$$

This is a contradiction. $\diamondsuit$

[2]Since $B_1d_i^{-1} \cap C_2^{-1} = \{d_i^{-1}\}$ and $d_1 \ne d_2$, $B_1d_1^{-1}$ and $B_1d_2^{-1}$ 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_λ 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

$$\sum_{g \in G \setminus \{1\}} |A \cap Ag| = |A|^2 - |A|. \tag{20}$$

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

$$\begin{aligned} |A \cup Ahg| &= |Ag^{-1} \cup Ah| \leq |Ag^{-1} \cup Ah \cup A| \\ = |(Ag^{-1} \cup A) \cup (Ah \cup A)| &= |Ag^{-1} \cup A| + |Ah \cup A| - |(Ag^{-1} \cup A) \cap (Ah \cup A)| \\ &\leq |A| + \lambda + |A| + \mu - |A| = |A| + \lambda + \mu. \quad \diamondsuit \end{aligned}$$

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 λ with $|A_\lambda| > 1$. We abbreviate $m := m(A)$. Since G is simple, $0 < m$. In what follows we write $F_n = A_{nm} \backslash A_{m(n-1)}$, $n \geq 1$. In particular, $F_1 = A_m \setminus \{1\}$. It is clear that F_n, $n \geq 1$ are disjoint and $A_{nm} = \{1\} \cup F_1 \cup ... \cup F_n$.

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

$$\text{(i)} \qquad |A_{mn}| \geq |F_1| + |A_{m(n-1)}|; \tag{21}$$

$$\text{(ii)} \qquad |F_n| \geq |F_1|; \tag{22}$$

$$\text{(iii)} \qquad |A_{nm}| \geq 1 + n|F_1|. \tag{23}$$

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). $\diamondsuit$

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 $G = \{g_0 = 1, ..., g_{n-1}\}, n = |G|$, 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 $\lambda_j \geq |A| - mi$.*

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

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 [3]

$$\frac{2a}{3m} \leq n \leq \frac{2a}{3m} + 1.$$

Due to Proposition 4.5, $n|F_1| \leq |G| - 3$. Consider the sets $S_i = \{g_j \mid i|F_1| \geq j > (i-1)|F_1|\}, i = 1, ..., n$. Clearly $|S_j| = |F_1|$. Since $n|F_1| \leq |G| - 3$, $S_1 \cup ... \cup S_n \subset G \setminus \{e\}$. 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

$$a(a-1) \geq 3 \cdot \frac{2a}{3n} \left(na - m\frac{n(n+1)}{2} \right) = 2a^2 - am(n+1).$$

[3]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

$$\left(\frac{2a}{3m}+2\right)m \geq a+1 \Leftrightarrow \frac{2a}{3}+2m \geq a+1 \Leftrightarrow 2m \geq \frac{a}{3}+1$$

contrary to $m \leq a/6$. $\diamondsuit$

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*

$$m(A) > min(l/3, |A|/6) \geq l/6.$$

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. $\diamondsuit$

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

G	degree
A_5	6
A_6	10
$L_2(8)$	9
$L_2(16)$	17
$L_2(7)$	7
$L_2(11)$	11
$L_2(13)$	14
$L_2(17)$	18
$L_2(19)$	20
$L_3(3)$	13
M_{11}	11
M_{12}	12
A_n	$n \leq 42$

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.*

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

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 $B \leq A_5, |B| \leq 5$. $\diamondsuit$

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

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

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

a contradiction.

10) Assume that G is simple and $Cla(G)^{\#} = \{C_1, ..., C_k\}$ with $|C_1| \leq |C_2| \leq ... \leq |C_k|$.

Consider $C_2 \cdot ... \cdot C_k$. We claim that $|C_2 \cdot ... \cdot C_k| \geq |G| - 1$. Indeed, if it is not true, then by Theorem 1.2 $|C_2 \cdot ... \cdot C_k| \geq |C_2| + ... + |C_k| + 3$, implying $|C_2 \cdot ... \cdot C_k| \geq |C_2| + ... + |C_k| + |C_1| = |G| - 1$. Again, a contradiction.

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

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

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

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

References

[1] Z.Arad, H.Blau, On table algebras and their applications to finite group theory, J. Algebra, 138 (1991), 137-185. MR **92f:**20007

[2] Z.Arad, E.Fisman, M.Muzychuk. Order evaluation of products of subsets in finite groups and its applications.I, J. Algebra 182 (1996), 577–603. CMP 96:15

[3] I.D.Dixon, B. Mortimer. The primitive permutation groups of degree less than 1000, Math. Proc. Camb. Phil. Soc., **103** (1988), 213-238. MR **89b:**20014

[4] W.Feit. Characters of Finite Groups, Benjamin, New York, Amsterdam, 1967. MR **36:**2715

[5] W.Feit and J.Thompson. Finite groups which contain a self-centralizing subgroup of order 3. Nagoya Math. J. 21, (1962), pp. 185-197. MR **26:**192

[6] B.Huppert, N.Blackburn, Finite groups II, Springer-Verlag, 1982. MR **84i:**20001a

[7] I.M.Isaacs and Ilan Zisser. Squares of characters with a few constituents in finite groups. Arch. Math. 63, 1994, pp. 197-207. MR **95e:**20015

[8] B.A.Pogorelov, Primitive groups of permutations of small degrees. II, Algebra i Logika, 19 1980, n.4, pp. 423-457. MR **82j:**20009b

Department of Mathematics & Computer Science, Bar-Ilan University, 52900 Ramat-Gan, Israel