On a subgroup contained in some words with a bounded length

Yahya Ould Hamidoune

Université Pierre et Marie Curie, UER 48, E. R. Combinatoire, 4 Place Jussieu, 75230 Paris, France

Received 10 November 1988
Revised 25 September 1989

Abstract


Let $G$ be a group and let $A$ and $B$ be two finite nonvoid subsets of $G$ such that $1 \leq B$. Using results of Kemperman, we show that either $|AB| \geq |A| + |B|$ or there exists a nonnull subgroup contained in $A \cup B \cup A B$. As an application we obtain the following result: Let $A_1, A_2, \ldots, A_k$ be subsets of a finite group $G$ such that $1 \leq A_i$; $2 \leq i \leq k$ and $|A_1| + |A_2| + \cdots + |A_k| \geq |G|$. The union of sets of the form $A_{i_1} A_{i_2} \cdots A_{i_j}$; $1 \leq i_1 < i_2 < \cdots < i_j \leq k$ must include a nonnull subgroup.

In particular if $B$ is a subset of $G \setminus 1$ such that $k |B| \geq |G|$, the set $B \cup B^2 \cup \cdots \cup B^k$ must contain a nonnull subgroup.

1. Introduction

The smallest integer not less than a real $x$ will be denoted by $\lceil x \rceil$. Let $G$ be a group and let $A, B$ be subsets of $G$. We write $AB = \{xy : x \in A$ and $y \in B\}$. We use the additive notation only for abelian groups. The subgroup generated by $A$ will be denoted by $\langle A \rangle$.

Theorem 1.1 (Kemperman [7, Theorem 5]). Let $G$ be a group and $A, B$ two finite subsets of $G$. Let $a \in A$ and $b \in B$. Then there exists a subgroup $H$ such that $aH \subseteq AB$ and $|AB| \geq |A| + |B| - |H|$.

Theorem 1.2 (Kemperman [7, Theorem 3]). Let $G$ be a group and $A, B$ two finite subsets of $G$ such that $1 \in A \cap B$ and $1 \notin (A \setminus 1)B$. Then $|AB| \geq |A| + |B| - 1$.

An other proof for this result is given by Olson [9, Theorem 4].

In this paper we apply the above two theorems in order to prove the following result: Let $G$ be a group and $A, B$ two finite nonvoid subsets of $G$ such that $1 \notin B$. 

0012-365X/92/$05.00 \copyright 1992 - Elsevier Science Publishers B.V. All rights reserved
Then either \(|A \cup B \cup AB| \geq |A| + |B|\) or there exists a nonnull subgroup \(H\) such that \(H \subseteq A \cup B \cup AB\).

As an application we obtain the following result: Let \(A_1, A_2, \ldots, A_k\) be subsets of a finite group \(G\) such that \(1 \notin A_i\), \(2 \leq i \leq k\) and \(|A_1| + |A_2| + \cdots + |A_k| \geq |G|\). The union of sets of the form \(A_{i_1}A_{i_2} \cdots A_{i_j}\), \(1 \leq i_1 < i_2 < \cdots < i_j \leq k\) must include a nonnull subgroup.

In particular if \(B\) is a subset of \(G \setminus 1\) such that \(k \, |B| \geq |G|\), the set \(B \cup B^2 \cup \cdots \cup B^k\) must contain a nonnull subgroup.

The above result generalizes a theorem of Diderrich, who obtained the same conclusion in the case \(|A_1| = |A_2| = \cdots = |A_k| = 1\), cf. [2, Theorem 3].

The following result is due to Kneser, cf. also [8].

**Theorem 1.3** (Kneser [4]). Let \(G\) be an abelian group and \(A\) and \(B\) two finite nonvoid subsets of \(G\). There exists a subgroup \(H\) of \(G\), such that \(A + H + B = A + B\) and \(|A + B| \geq |A + H| + |B + H| - |H|\).

Kneser's Theorem is an important Addition Theorem. It is applied in [5] to the geometry of numbers and to Haar measures in [6].

The following generalization of Kneser's Theorem 1.3 is due to Diderrich.

**Theorem 1.4** (Diderrich [2, Theorem 1]). Let \(G\) be a group and \(A\) and \(B\) two finite nonvoid subsets of \(G\) such the elements of \(B\) commute. There exists an abelian subgroup \(H\) of \(G\) such that \(A + B + H = A + B\) and \(|A + B| \geq |A + H| + |B + H| - |H|\).

We shall give a short proof of Theorem 4 based on Theorem 1.3.

**Theorem 1.5** (Olson [9, Theorem 1]). Let \(G\) be a group and \(A\) and \(B\) two finite nonvoid subsets of \(G\) such that \(1 \in B\). Then either \(AB = ABB\) or \(|AB| \geq |A| + \frac{1}{2}|B|\).

We need Olson's Theorem only for abelian groups. In this case, Olson mentioned in [9] that Theorem 1.5 is an easy corollary of Kneser's Theorem 3. It follows that Theorem 1.3 and Theorem 1.4 are essentially the same. Diderrich conjectured in [2] the validity of Theorem 4 when the elements of \(B\) do not commute. But Olson found a counterexample to this conjecture in [6].

2. A subgroup contained in short words

Using Kemperman's Theorems 1.3 and 1.4, we shall obtain the following result.

**Proposition 2.1.** Let \(G\) be a group of order \(\geq 2\) and \(A, B\) two finite nonvoid subsets of \(G\) such that \(1 \notin B\). Then either \(|A \cup B \cup AB| \geq |A| + |B|\) or there exists a nonnull subgroup \(H\) such that \(H \subseteq A \cup B \cup AB\).
On a subgroup contained in some words

Proof. Let $A' = A \cup \{1\}$ and let $B' = B \cup \{1\}$. We clearly have

$$A'B' = A \cup B \cup AB \cup \{1\} \quad \text{and} \quad |B'| = |B| + 1.$$  \hspace{1cm} (1)

Case 1: $1 \in AB$.

By Kemperman’s Theorem 1.1, applied to $A'$ and $B'$ with $a = b = 1$ there exists a subgroup $H$ such that $|A'B'| \geq |A'| + |B'| - |H|$ and $H \subseteq A'B'$. By (1), $H \subseteq A'B' = A \cup B \cup AB$. We may then assume $H = \{1\}$. It follows that

$$|A \cup B \cup AB| = |A'B'| \geq |A'| + |B'| - 1 \geq |A| + |B|.$$  \hspace{1cm} (2)

Case 2: $1 \notin AB$.

In this case we have $1 \in A'B'$ and $1 \notin A'B = B \cup AB$. By Kemperman’s Theorem 2, applied to $A'$ and $B'$, $|A'B'| \geq |A'| + |B'| - 1$. By (1), we have $|A \cup B \cup AB \cup \{1\}| \geq |A'| + |B'|$. By considering the 2 cases $1 \in A$ and $1 \notin A$, we see that $|A \cup B \cup AB| \geq |A| + |B|$. \hfill $\square$

Proposition 2.2. Let $G$ be a finite group and $S_1$ a nonvoid subset of $G$. Let $S_2, \ldots, S_k$ be nonvoid subsets of $G \setminus \{1\}$ such that $\sum_{1 \leq i \leq k} |S_i| \geq n$, then

$$\bigcup_{1 \leq i_1 < i_2 \cdots < i_k \leq k} S_{i_1}S_{i_2} \cdots S_{i_k}$$

contains a nonnull subgroup of $G$.

Proof. Suppose that $\bigcup_{1 \leq i_1 < i_2 \cdots < i_k \leq k} S_{i_1}S_{i_2} \cdots S_{i_k}$ contains no nonnull subgroup. Using the obvious equality

$$\bigcup_{1 \leq i_1 < \cdots < i_k \leq k} S_{i_1}S_{i_2} \cdots S_{i_k} = \bigcup_{1 \leq i_1 < \cdots < i_{k-1} \leq k} S_{i_1}S_{i_2} \cdots S_{i_{k-1}} \cup S_k$$

$$\bigcup_{1 \leq i_1 < \cdots < i_{k-1} \leq k-1} S_{i_1}S_{i_2} \cdots S_{i_{k-1}}S_k,$$

and Proposition 2.1, we have for $k \geq 2$,

$$\left| \bigcup_{1 \leq i_1 < \cdots < i_k \leq k} S_{i_1}S_{i_2} \cdots S_{i_k} \right| \geq \left| \bigcup_{1 \leq i_1 < \cdots < i_{k-1} \leq k-1} S_{i_1}S_{i_2} \cdots S_{i_{k-1}} \right| + |S_k|.$$

Using the above relation, we obtain

$$\left| \bigcup_{1 \leq i_1 < \cdots < i_k \leq k} S_{i_1}S_{i_2} \cdots S_{i_k} \right| \geq \sum_{1 \leq i_1 < \cdots < i_k \leq k} |S_i| \geq |G|,$$

a contradiction. \hfill $\square$

Corollary 2.3 (Diderrich [2, Theorem 3]). Let $G$ be a finite group of order $v \geq 2$ and let $a_1, a_2, \ldots, a_v$ be a sequence of elements of $G \setminus \{1\}$. The set of products $a_{i_1}a_{i_2} \cdots a_{i_v}$, $1 \leq i_1 < i_2 < \cdots < i_v \leq v$ must include a nontrivial subgroup of $G$.

Proof. We apply Proposition 2.2 with $S_i = \{a_i\}$, $1 \leq i \leq v$. \hfill $\square$
Corollary 2.4. Let $G$ be a finite group of order $n \geq 2$ and let $S$ be a subset of $G \setminus \{1\}$ with cardinality $s$. Then there exists a nonnull subgroup $H$ such that $H \subseteq S \cup S^2 \cup \cdots \cup S^k$, where $k = \lfloor n/s \rfloor$.

Proof. Take $S_1 = S_2 = \cdots = S_k = S$. We clearly have
$$\bigcup_{1 \leq i_1 < i_2 < \cdots < i_k \leq k} S_{i_1}S_{i_2}\cdots S_{i_k} = S \cup S^2 \cup \cdots \cup S^k.$$ The result now follows by Proposition 2.2. $\square$

As far as we are aware, the conclusion $1 \in S \cup S^2 \cup \cdots \cup S^k$, for $k \geq \lfloor n/s \rfloor$, was proved for the first time for cyclic groups by Shepherdson [11, Corollary 1]. But his proof works for all abelian groups. The same result for non-abelian groups was first stated in [3, Theorem 5.2].

Example. Let $G = \mathbb{Z}_n$ and let $S = \{1, 2, \ldots, s\}$. We have clearly $0 \not\in S \cup 2S \cup \cdots \cup kS$, for any $k < \lfloor n/s \rfloor$. This example shows that the above results are best possible.

The problem considered here has some analogy with the covering questions considered in [1, p. 13].

3. On Kneser’s Addition Theorem

In this section we use Olson’s Theorem 5 to show that Diderrich’s Theorem 4 is equivalent to Kneser’s Theorem 3.

A short proof of Theorem 4. The validity of Theorem 4 for $B a$ implies its validity for $B$. We may then assume without loss of generality that $1 \in B$.

Let $\{x_i: 1 \leq i \leq k\}$ be a family of distinct representatives of the left cosets modulo $\langle B \rangle$ intersecting $A$. Take $A_i = A \cup x_i \langle B \rangle$, $1 \leq i \leq k$.

We clearly have
$$A_iB \subseteq A_i \langle B \rangle = x_i \langle B \rangle,$$ (1)

Therefore,
$$A_iB \cap A_jB = \emptyset, \quad \text{for} \quad i \neq j, \quad 1 \leq i, j \leq k.$$ (2)

Case 1: There are $r, s, 1 \leq r < s \leq k$, $A_rB \neq A_sBB$ and $A_rBB \neq A_rB$.

By (1) we have
$$x_j^{-1}A_j \subseteq \langle B \rangle, \quad j = r, s.$$ (3)

By Olson’s Theorem 4, applied to the abelian group $\langle B \rangle$, we have
$$|(x_j^{-1}A_j)B| \geq |x_j^{-1}A_j| + \frac{1}{2} |B|, \quad j = r, s.$$
It follows that

\[ |A_rB| \leq |A_r| + \frac{1}{2} |B|, \quad j = r, s. \quad (4) \]

It follows using (2) and (4), that

\[ |AB| = |\bigcup A_rB| \geq \sum_{i \neq r, s} |A_i| + |A_r| + |A_s| + |B| = |A| + |B|. \quad (5) \]

By (5), we can take \( H = \{1\} \).

Case 2: There exists \( r, 1 \leq r \leq k, A_rBB = A_rB, \) for all \( s \neq r \).

We choose \( r = 1 \). It follows that \( x_1^{-1}A_1 \subset \langle B \rangle \). By Theorem 3, applied to \( \langle B \rangle \), there exists a subgroup \( H \) (abelian of course) of \( \langle B \rangle \) such that

\[ x_1^{-1}A_1H = x_1^{-1}A_1B \quad \text{and} \quad |x_1^{-1}A_1| \geq |x_1^{-1}A_1| + |B| - |H|. \]

Hence

\[ A_1HB = A_1B \quad \text{and} \quad |A_1B| \geq |A_1H| + |BH| - |H|. \quad (6) \]

We shall prove that

\[ A_iHB = A_iB, \quad i \neq 1. \quad (7) \]

Take \( i, 1 \neq i \). By iterating the relation \( A_iB = A_iBB \), we see that \( A_iB^n = A_iB, \) for all \( n \). It follows that \( A_i \langle B \rangle \subset A_iB \). Hence \( A_iHB \subset A_i \langle B \rangle B = A_i \langle B \rangle \subset A_iB \).

The other inclusion is obvious.

Now we have using (6) and (7)

\[ AHB = \bigcup A_iHB = \bigcup A_iB = AB. \quad (8) \]

Also we have using (2), (6) and (7),

\[ |AB| = |\bigcup A_iB| = \sum_{i \neq 1} |A_iB| + |A_iB| \geq \sum_{i \neq 1} |A_iHB| + |A_iH| + |BH| - |H| \]

\[ \geq \sum_{i \neq 1} |A_iH| + |A_iH| + |BH| - |H| \geq |AH| + |BH| - |H|. \quad (9) \]

Equations (8) and (9) imply Theorem 1.4. \( \square \)

References