ON A GENERALIZATION OF THE CAUCHY-DAVENPORT THEOREM

Matt DeVos[1]
Math Dept., Simon Fraser University, Burnaby, British Columbia, Canada
mdevos@sfu.ca

Received: 11/15/15, Revised: 12/27/15, Accepted: 1/15/16, Published: 1/21/16

Abstract

A generalization of the Cauchy-Davenport Theorem to arbitrary finite groups was suggested by Károlyi and proved independently by Károlyi and Wheeler. Here we give a short proof of the following small extension of this result (which also applies to infinite groups): If A, B are finite nonempty subsets of a (multiplicatively written) group G then $|AB| \geq \min\{p(G), |A| + |B| - 1\}$ where $p(G)$ denotes the smallest order of a nontrivial finite subgroup of G, or ∞ if no such subgroups exist.

1. The Result

The following famous theorem discovered independently by Cauchy [1] and Davenport [2] is one of the founding theorems in additive combinatorics and the starting point for this work.

Theorem 1 (Cauchy-Davenport). *Let p be prime and let $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ be nonempty. Then the set $A + B = \{a + b \mid a \in A \text{ and } b \in B\}$ satisfies the following bound:*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}$$

We will be interested in more general groups G which we write multiplicatively. If $A, B \subseteq G$ then we define $AB = \{ab \mid a \in A \text{ and } b \in B\}$, and for $g \in G$ we abbreviate $\{g\}A$ by gA and $A\{g\}$ by Ag. Following Károlyi we will generalize the above theorem to arbitrary groups G by giving a similar lower bound on $|AB|$ except with "p" replaced by the parameter $p(G)$, which we define to be the order of the smallest nontrivial finite subgroup of G, or ∞ if no such subgroups exist. Namely, we prove the following.

Theorem 2. *If A, B are finite nonempty subsets of G then*

$$|AB| \geq \min\{p(G), |A| + |B| - 1\}.$$

The restriction of this theorem to finite groups gives the result of Károlyi [3] and Wheeler [5]. Interestingly, these authors used very different methods to achieve their

[1]Supported in part by an NSERC Discovery Grant

results: Károlyi used group extensions (and also generalized Vosper's Theorem) while Wheeler utilized the Feit-Thompson Odd Order Theorem and the structure of solvable groups. Our approach is based on a transform which seems to have first appeared in a paper of Kemperman [4] and is by comparison quite elementary.

Proof of Theorem 2. Suppose (for a contradiction) that the theorem is false and choose a counterexample (A, B) so that:

1. $|AB|$ is minimum,
2. $|A| + |B|$ is maximum subject to 1,
3. $|A|$ is minimum subject to 1 and 2.

Note that our assumptions imply $|A| \leq |B|$ as otherwise the pair (B^{-1}, A^{-1}) contradicts the choice of (A, B) (since $|B^{-1}A^{-1}| = |(AB)^{-1}| = |AB|$). If $|A| = 1$ then $|AB| = |B| = |A| + |B| - 1$ giving us a contradiction. So $|A| \geq 2$ and we may choose $g \in G \setminus \{1\}$ so that $Ag \cap A \neq \emptyset$. If $Ag = A$ then A is a union of left $\langle g \rangle$ cosets and we have the contradiction $|AB| \geq |A| \geq p(G)$. It follows that $Ag \cap A$ is a proper nonempty subset of A. Next consider the two pairs of sets:

$$(A \cap Ag, B \cup g^{-1}B) \qquad (A \cup Ag, B \cap g^{-1}B)$$

It follows from basic principles that the product set associated to each of these pairs is a subset of AB (ex. if $x \in A \cup Ag$ and $y \in B \cap g^{-1}B$ then either $x \in A$ so $xy \in AB$ or $x \in Ag$ so $xy \in Ag \cdot g^{-1}B = AB$). If $B \cap g^{-1}B = \emptyset$ then we have the contradiction $|AB| \geq |(A \cap Ag)(B \cup g^{-1}B)| \geq |B \cup g^{-1}B| = 2|B| \geq |A| + |B|$. Therefore all four of the sets appearing in our two pairs are nonempty. If $|A \cup Ag| + |B \cap g^{-1}B| > |A| + |B|$ then the pair $(A \cup Ag, B \cap g^{-1}B)$ contradicts the choice of (A, B) (this pair is also a counterexample since $|(A \cup Ag)(B \cap g^{-1}B)| \leq |AB| < \min\{p(G), |A| + |B| - 1\} \leq \min\{p(G), |A \cup Ag| + |B \cap g^{-1}B| - 1\}$). It follows from this and $|A \cap Ag| + |A \cup Ag| + |B \cup g^{-1}B| + |B \cap g^{-1}B| = 2|A| + 2|B|$ that $|A \cap Ag| + |B \cup g^{-1}B| \geq |A| + |B|$. However, now the pair $(A \cap Ag, B \cup g^{-1}B)$ contradicts the choice of (A, B) by similar reasoning, and this completes the proof. □

References

[1] Cauchy, A. L. Recherches sur les nombres. *J. Ecole Polytech.* **9** (1813), 99-116.

[2] Davenport, H. On the addition of residue classes. *J. London Math. Soc.* **10** (1935), 30-32.

[3] Károlyi, G. Cauchy-Davenport theorem in group extensions. *Enseign. Math.* **(2) 51** (2005), no. 3-4, 239-254.

[4] J.H.B. Kemperman, On complexes in a semigroup, *Indag. Math.* **18** (1956), 247-254.

[5] Wheeler, J.P. The Cauchy-Davenport Theorem for Finite Groups. *arXiv:* 1202.1816