European Journal of Combinatorics 34 (2013) 1436–1453

Contents lists available at SciVerse ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

A structure theorem for small sumsets in nonabelian groups

Oriol Serra [a], Gilles Zémor [b]

[a] *Dept Matemàtica Aplicada 4, Universitat Politècnica de Catalunya, BarcelonaTech, Jordi Girona, 1, E-08034 Barcelona, Spain*

[b] *Institut de Mathématiques de Bordeaux, UMR 5251, université Bordeaux 1, 351 cours de la Libération, 33405 Talence, France*

ARTICLE INFO

Article history:
Available online 14 June 2013

ABSTRACT

Let G be an arbitrary finite group and let S and T be two subsets such that $|S| \geq 2$, $|T| \geq 2$, and $|TS| \leq |T| + |S| - 1 \leq |G| - 2$. We show that if $|S| \leq |G| - 4|G|^{1/2}$ then either S is a geometric progression or there exists a non-trivial subgroup H such that either $|HS| \leq |S| + |H| - 1$ or $|SH| \leq |S| + |H| - 1$. This extends to the nonabelian case classical results for abelian groups. When we remove the hypothesis $|S| \leq |G| - 4|G|^{1/2}$ we show the existence of counterexamples to the above characterization whose structure is described precisely.

1. Introduction

Let $(G, +)$ be a finite abelian group written additively. Let S be a subset of G such that $T + S \neq G$ and

$$|T + S| \leq |T| + |S| - 2 \tag{1}$$

for some subset T of G. A Theorem of Mann [17] says that S must be well covered by cosets of a subgroup. More precisely, there must exist a proper subgroup H of G such that

$$|S + H| \leq |S| + |H| - 2.$$

Mann's Theorem can be thought of as simplified, or one-sided, version of Kneser's Theorem [16] which gives a structural result for the pair of subsets $\{S, T\}$ rather than a single subset. If one weakens the condition (1) to

$$|T + S| \leq |T| + |S| - 1 \tag{2}$$

E-mail addresses: oriol.serra@upc.edu (O. Serra), zemor@math.u-bordeaux1.fr (G. Zémor).

0195-6698/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ejc.2013.05.026

for some set T such that $|S+T| \leq |G|-2$, then a structural change occurs because the sets S and T can be arithmetic progressions and not well covered by cosets. However, this is the only alternative i.e. if $|T| \geq 2$ and S is not an arithmetic progression, then a simple, one-sided, version of the Kemperman Structure Theorem [15] says that there must exist a proper subgroup such that

$$|S+H| \leq |S| + |H| - 1. \tag{3}$$

In the present work we are interested in the nonabelian counterpart of the above results. Caution is in order because the two-sided abelian additive theorems do not seem to generalize. In particular counter-examples to the intuitive nonabelian generalization of Kneser's Theorem were found by Olson [18] and the second author [21]. However, Mann's theorem was generalized to the nonabelian setting [21,4]. It was obtained that, if S is a subset of a finite group $(G, \times)$ (from now on written multiplicatively to emphasize that G is not necessarily abelian) for which there is a subset T such that $TS \neq G$ and

$$|TS| \leq |T| + |S| - 2,$$

then there must exist a proper subgroup H such that S is well-covered by either left or right cosets modulo a subgroup H, i.e. we have

$$\text{either} \quad |SH| \leq |S| + |H| - 2 \quad \text{or} \quad |SH| \leq |H| + |S| - 2.$$

Note that the difference with the abelian case is that we cannot control whether S is covered by left or right cosets.

Our main result is to obtain a structural result on S under a generalization of (2) to nonabelian groups. Specifically, we prove:

Theorem 1. *Let S be a subset of a finite group G for which there exists a subset T such that $2 \leq |T|$ and $|TS| \leq \min(|G|-2, |T|+|S|-1)$. Then one of the following holds*

(i) *S is a geometric progression, i.e. there exist $g, a \in G$ such that gS equals $\{1, a, a^2, \ldots, a^{|S|-1}\}$;*
(ii) *there exists a proper subgroup H of G such that*

$$|HS^\varepsilon| \leq |H| + |S| - 1$$

where S^ε denotes either S or S^{-1};
(iii) *there exists a subgroup H and an element a of G such that $|HaH| = |H|^2$ and, letting $A = H \cup Ha$,*

$$|AS^\varepsilon| = |A| + |S| - 1 = |G| - |A|.$$

Note that property (iii) collapses to a particular case of (i) if the group G is abelian, since then we can only have $H = \{1\}$. Condition $|HaH| = |H|^2$ in (iii) also implies that it can only occur for subsets S of G that are quite close to being the whole group, since we must clearly have $|H| \leq |G|^{1/2}$ and $|S| = |G| + 1 - 4|H|$, in other words:

Corollary 2. *Let S be a subset of a finite group G for which there exists a subset T such that $2 \leq |T|$ and $|TS| \leq \min(|G|-2, |T|+|S|-1)$ and such that $|S| \leq |G| - 4|G|^{1/2}$: then*

- *either S is a geometric progression,*
- *or there exists a proper subgroup H of G such that*

$$|HS^\varepsilon| \leq |H| + |S| - 1.$$

The condition $|S| \leq |G| - 4|G|^{1/2}$ in Corollary 2 is unlikely to be improved upon asymptotically, for we shall show in the final section that, assuming a number-theoretic conjecture (the existence of an infinite number of Sophie Germain primes), there exist infinite families of groups G with subsets S such that $|S| \leq |G| - O(\sqrt{|G|})$ and that satisfy the hypothesis of Corollary 2 but not its conclusion.

We shall use Hamidoune's atomic method to derive Theorem 1. If S is a generating subset containing 1 of a finite group, then A is a k-atom of S if it is of minimum cardinality among subsets X such that $|X| \geq k$, $|XS| \leq |G| - k$ and $|XS| - |X|$ is of minimum possible cardinality (see Section 2