



Some extensions of the Cauchy-Davenport theorem

Shalom Eliahou^{1,2}

*LMPA-ULCO
Université du Littoral Côte d'Opale
Calais, France*

Michel Kervaire³

*Section de Mathématiques
Université de Genève
Genève, Suisse*

Abstract

The Cauchy-Davenport theorem states that, if p is prime and A, B are nonempty subsets of cardinality r, s in $\mathbb{Z}/p\mathbb{Z}$, the cardinality of the sumset $A + B = \{a + b \mid a \in A, b \in B\}$ is bounded below by $\min(r + s - 1, p)$; moreover, this lower bound is sharp. Natural extensions of this result consist in determining, for each group G and positive integers $r, s \leq |G|$, the analogous sharp lower bound, namely the function

$$\mu_G(r, s) = \min\{|A + B| \mid A, B \subset G, |A| = r, |B| = s\}.$$

Important progress on this topic has been achieved in recent years, leading to the determination of μ_G for all abelian groups G . In this note we survey the history of earlier results and the current knowledge on this function.

Keywords: Sumsets, Cauchy-Davenport theorem, Kneser theorem, Hopf-Stiefel function, Alon-Tarsi polynomial method, Hamidoune isoperimetric method

1 Introduction

Let G be a group written additively and r, s positive integers such that $r, s \leq |G|$. We denote by

$$\mu_G(r, s) = \min\{|A + B| \mid A, B \subset G, |A| = r, |B| = s\}$$

the minimal cardinality of the sumsets

$$A + B = \{a + b \mid a \in A, b \in B\},$$

where A, B range over all subsets of G of cardinality $|A| = r, |B| = s$.

Getting upper bounds for $\mu_G(r, s)$ is usually achieved by explicit construction of subsets $A, B \subset G$ with $|A| = r, |B| = s$ and $|A + B|$ small. Proving lower bounds for $\mu_G(r, s)$ is difficult in general and requires tools, such as:

- Dyson's and Kemperman's transforms,
- Kneser's theorem,
- Alon-Tarsi's polynomial method,
- Hamidoune's isoperimetric method.

The simplest example is provided by the group of integers $G = \mathbb{Z}$. We have

$$\mu_{\mathbb{Z}}(r, s) = r + s - 1$$

for all integers $r, s \geq 1$. The upper bound \leq is provided by the explicit pair $A = \{0, 1, \dots, r - 1\}, B = \{0, 1, \dots, s - 1\}$, for which $A + B = \{0, 1, \dots, r + s - 2\}$ is of cardinality $r + s - 1$. The lower bound \geq easily follows from the ordered nature of \mathbb{Z} . Indeed, if $A = \{a_1 < \dots < a_r\}, B = \{b_1 < \dots < b_s\}$, then $A + B$ contains the $(r + s - 1)$ -subset

$$\{a_1 + b_1 < a_2 + b_1 < \dots < a_r + b_1 < a_r + b_2 < \dots < a_r + b_s\}.$$

Determining μ_G for other groups is much more demanding. This is a short survey of the history and current knowledge on the function $\mu_G(r, s)$ for various classes of groups G .

¹ The first author gratefully acknowledges partial support from the Fonds National Suisse pour la Recherche Scientifique during the preparation of this paper.

² Email: eliahou@lmpa.univ-littoral.fr

³ Email: kervaire@math.unige.ch

2 Early results

The first result on μ_G dates back to 1813, when Cauchy [2] proved that if $G = \mathbb{Z}/p\mathbb{Z}$ with p prime, then

$$\mu_{\mathbb{Z}/p\mathbb{Z}}(r, s) = \min(r + s - 1, p)$$

for all $1 \leq r, s \leq p$. This result was later rediscovered by Davenport [3] and is known as the Cauchy-Davenport theorem.

The upper bound $\mu_{\mathbb{Z}/p\mathbb{Z}}(r, s) \leq \min(r + s - 1, p)$ is easily achieved by the pair of subsets $A = \{0, \dots, r - 1\}$, $B = \{0, \dots, s - 1\}$ of $\mathbb{Z}/p\mathbb{Z}$.

The lower bound $\mu_{\mathbb{Z}/p\mathbb{Z}}(r, s) \geq \min(r + s - 1, p)$ can be proved by various methods. A simple combinatorial one proceeds by induction of $|B|$, and makes use of the Dyson transform of a pair of subsets A, B in an abelian group G , defined by

$$A' = A \cup (B + e)$$

$$B' = (A - e) \cap B$$

for suitable $e \in G$. Two key properties of this transform are:

- $A' + B' \subset A + B$,
- $|A'| + |B'| = |A| + |B|$.

In 1956, Kemperman [13] determined the function μ_G for an arbitrary torsion-free group G , abelian or not. He proved that

$$\mu_G(r, s) = r + s - 1$$

for all integers $r, s \geq 1$. (Compare with the case $G = \mathbb{Z}$ above.)

Realizing $r + s - 1$ as upper bound is easy, since any torsion-free group G contains a copy of \mathbb{Z} . Proving the lower bound $\mu_G(r, s) \geq r + s - 1$ can be achieved by Kemperman’s transform, better suited to nonabelian groups: replace the pair $A, B \subset G$ by either pair A', B' or A'', B'' :

$$A' = A \cup (A + e)$$

$$A'' = A \cap (A - e)$$

$$B' = B \cap (-e + B)$$

$$B'' = B \cup (e + B),$$

for suitable $e \in G$. The proof proceeds by cleverly iterating this transform.

Another nice proof of this theorem uses Hamidoune’s isoperimetric method [12].

3 Abelian p -groups

In his study of sums of squares and the Hurwitz problem, Yuzvinsky [17] treated the case $G = (\mathbb{Z}/2\mathbb{Z})^N$ and proved that

$$\mu_G(r, s) = r \circ s$$

for all $1 \leq r, s \leq |G|$, where $r \circ s$ is the famous Hopf-Stiefel function which arises in Topology and in the theory of quadratic forms. An important step was accomplished in 1996 by Bollobás and Leader [1] who proved that, for p prime and $N \geq 1$, *all abelian p -groups G of order p^N have the same function μ_G* . They give explicit, though quite complicated formulas for μ_G .

Independently, we treated the case of the elementary p -groups $G = (\mathbb{Z}/p\mathbb{Z})^N$ with simpler proofs [4], using the polynomial method of Alon-Tarsi. We proved that

$$\mu_G(r, s) = r \circ_p s,$$

a natural generalisation of the Hopf-Stiefel function. The function $r \circ_p s$ is defined as the smallest positive integer n such that the polynomial $(X + Y)^n$ falls in the ideal (X^r, Y^s) of the polynomial ring $\mathbb{F}_p[X, Y]$. We provide a simple explicit formula for $r \circ_p s$ in terms of the p -adic expansions of $r - 1, s - 1$.

4 General abelian groups

New developments occurred after 2002, with the use of Kneser's theorem as a tool for proving lower bounds on μ_G for G abelian. Very shortly after Plagne settled the case of cyclic groups, we showed in [11] that *for every finite abelian group G of order n and all $1 \leq r, s \leq n$, one has*

$$\mu_G(r, s) = \min_{d|n} \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d.$$

The general abelian case, without any finiteness condition, was finally settled in [6]. Our result is expressed in terms of the numerical function

$$\kappa_G(r, s) = \min_{h \in \mathcal{H}(G)} \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h,$$

where G is any group and $\mathcal{H}(G)$ is the set of orders of finite subgroups of G .

Theorem 4.1 ([6]) *Let G be an arbitrary abelian group. Then $\mu_G(r, s) = \kappa_G(r, s)$ for all positive integers $r, s \leq |G|$.*

Recall that if G is finite abelian of order n , then $\mathcal{H}(G)$ coincides with the set of divisors of n . Thus, Theorem 4.1 yields, as it should, the result given above in that particular case.

The difficulty in going from the finite to the infinite abelian case does not lie so much in the proofs, which are similar, but in properly guessing, in the first place, what the correct answer should be. Interestingly, the clue was provided by our work in [5] on nonabelian groups.

As mentioned above, the lower bound on μ_G in Theorem 4.1 uses the following classical result of Kneser [14].

Theorem 4.2 *Let G be an abelian group. Let $A, B \subset G$ be finite nonempty subsets. Then there is a finite subgroup $H \leq G$ such that*

$$|A + B| \geq |A + H| + |B + H| - |H|.$$

On the other hand, proving the upper bound $\mu_G(r, s) \leq \kappa_G(r, s)$ is obtained by explicit construction of small sumsets in abelian groups. Curiously, the main step lies in proving the seemingly much weaker bound $\mu_G(r, s) \leq r + s - 1$.

5 The small sumsets property

Definition 5.1 Let G be any group. We say that G has the *small sumsets property* if

$$\mu_G(r, s) \leq r + s - 1$$

for all integers $1 \leq r, s \leq |G|$.

A key step in proving the upper bound in Theorem 4.1 is the following.

Theorem 5.2 ([6]) *Let G be an abelian group. Then G satisfies the small sumsets property.*

The proof is by explicit construction:

- If G is finite, then $G \cong C_1 \times \cdots \times C_k$, a direct product of cyclic groups. Order G lexicographically. Let $I_t \subset G$ be the initial segment of length t . Then one can show that $|I_r + I_s| \leq r + s - 1$.
- If G is infinite, either it contains \mathbb{Z} , or else it contains arbitrarily large finite subgroups.

What other groups satisfy the small sumsets property? The answer is not known. Possibly, the alternating group A_5 of order 60 might not satisfy it. For instance, it is believed, though not yet proved, that $\mu_{A_5}(13, 13) > 25$.

However, every finite group of odd order satisfies the small sumsets property. This combinatorial statement relies on deep group theory, as mentioned below.

6 Solvable groups

Theorem 6.1 ([7,9]) *Let G be a solvable group. Then G satisfies the small sumsets property.*

This applies in particular to finite groups of odd order, which are solvable by the famous Feit-Thompson Theorem.

We can prove sharper bounds. To state them, we need to introduce some variants of the above kappa function. Given a group G , denote by $\mathcal{N}(G)$ the set of orders of finite normal subgroups of G , and by $\mathcal{D}(G)$ the set of divisors d of orders h of finite subgroups of G . We have $\mathcal{N}(G) \subset \mathcal{H}(G) \subset \mathcal{D}(G)$.

Our variants of the kappa function are defined as follows:

$$\begin{aligned}\mathcal{D}\kappa_G(r, s) &= \min_{h \in \mathcal{D}(G)} \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h \\ \mathcal{N}\kappa_G(r, s) &= \min_{h \in \mathcal{N}(G)} \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h\end{aligned}$$

In particular, as numerical functions, one has $\mathcal{D}\kappa_G(r, s) \leq \kappa_G(r, s) \leq \mathcal{N}\kappa_G(r, s)$. We recently obtained the following result.

Theorem 6.2 ([9,10]) *Let G be a finite solvable group. Then*

$$\mathcal{D}\kappa_G(r, s) \leq \mu_G(r, s) \leq \mathcal{N}\kappa_G(r, s)$$

for all positive integers $r, s \leq |G|$.

For dihedral groups, as for abelian groups, we now have a sharp result.

Theorem 6.3 ([10]) *Let D_n be the dihedral group of order $2n$. Then*

$$\mu_{D_n}(r, s) = \kappa_{\mathbb{Z}/2n\mathbb{Z}}(r, s)$$

for all positive integers $r, s \leq 2n$.

7 General nonabelian groups

Interestingly, the equality $\mu_G(r, s) = \kappa_G(r, s)$, valid for every abelian group G and integers $1 \leq r, s \leq |G|$, sometimes also occurs for nonabelian groups G and

suitable arguments r, s . This is the case for dihedral groups (see above), and also for torsion-free groups. Indeed, Kemperman’s theorem cited in Section 2, according to which $\mu_G(r, s) = r + s - 1$ for all $r, s \geq 1$, can be expressed as $\mu_G(r, s) = \kappa_G(r, s)$, since $\mathcal{H}(G) = \{1\}$ in the torsion-free case.

For an arbitrary finite group G , we can prove the equality

$$\mu_G(r, s) = \kappa_G(r, s)$$

in the following cases:

- $r + s > |G|$. Then $\mu_G(r, s) = \kappa_G(r, s) = |G|$. [15, Theorem 1.1]
- $r + s = |G|$. Here $\mu_G(r, s) = \kappa_G(r, s) = |G| - h_G(r)$, where $h_G(r)$ is the largest order of a subgroup of G dividing r . [5, Theorem 4.2]
- $\kappa_G(r, s) < s + r/2$. [5, Theorem 4.4]
- $1 \leq r \leq 3$ and $1 \leq s \leq |G|$. [5, Theorem 4.6]

The desired equality fails for the nonabelian group $G = \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$, for which one has $\kappa_G(5, 9) = 12$ and $\mu_G(5, 9) = 13$. Nevertheless, we conjecture that the lower bound $\mu_G(r, s) \geq \kappa_G(r, s)$ should be true for any group G .

We do have a general lower bound on μ_G , weaker than the one conjectured above. Yet it is again a variant of the kappa function. Given $t \geq 1$, set

$$\mathcal{H}_t(G) = \{h \in \mathcal{H}(G) \mid h \leq t\}.$$

The *weak kappa function* is defined as

$$\mathcal{W}\kappa_G(r, s) = \min_{h \in \mathcal{H}_{r+s-1}(G)} \left(\left\lceil \frac{r+s}{h} \right\rceil - 1 \right) h.$$

Theorem 7.1 ([9]) *For any group G and positive integers $r, s \leq |G|$, we have*

$$\mu_G(r, s) \geq \mathcal{W}\kappa_G(r, s).$$

The main ingredient for the proof is a theorem of Olson [16], a Kneser-type theorem for nonabelian groups.

References

[1] Bollobás, Béla, and Imre Leader, *Sums in the grid*, *Discrete Mathematics* **162** (1996), 31–48.

- [2] Cauchy, Augustin-Louis, *Recherches sur les nombres*, J. École Polytechnique **9** (1813), 99–123.
- [3] Davenport, Harold, *On the addition of residue classes*, J. London Math. Soc. **10** (1935), 30–32.
- [4] Eliahou, Shalom, and Michel Kervaire, *Sumsets in Vector Spaces over Finite Fields*, J. Number Theory **71** (1998), 12–39.
- [5] Eliahou, S., and M. Kervaire, *Some Results on Minimal Sumset Sizes in Finite Non-Abelian groups*, LMPA-ULCO, preprint **205**, 2003; *J. Number Theory*, to appear.
- [6] Eliahou, S., and M. Kervaire, *Minimal Sumsets in Infinite Abelian groups*, *J. Algebra* **287** (2005), 449–457.
- [7] Eliahou, S., and M. Kervaire, *The small sumsets property for solvable finite groups*, *European J. Combinatorics* **27** (2006), 1102–1110.
- [8] Eliahou, S., and M. Kervaire, *Sumsets in Dihedral groups*, *European J. Combinatorics* **27** (2006), 617–628.
- [9] Eliahou, S., and M. Kervaire, *Bounds on the minimal sumset size function in groups*, LMPA-ULCO, preprint **284**, 2006.
- [10] Eliahou, S., and M. Kervaire, *Minimal Sumsets in Finite Solvable Groups*, LMPA-ULCO, preprint **302**, 2006.
- [11] Eliahou, S., M. Kervaire, and A. Plagne, *Optimally Small Sumsets in Finite Abelian Groups*, J. Number Theory **101** (2003), 338–348.
- [12] Hamidoune, Yahya O., *An isoperimetric method in additive theory*, J. Algebra **179** (1996), 622–630.
- [13] Kemperman, J.H.B., *On complexes in a semigroup*, *Indag. Math.* **18** (1956), 247–254.
- [14] Kneser, Martin, *Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen* *Math. Z.* **61** (1955), 429–434.
- [15] Mann, Henry B., “Addition Theorems”, Interscience Publishers, John Wiley & Sons, 1965.
- [16] Olson, John E., *On the Sum of Two Sets in a Group*, J. Number Theory **18** (1984), 110–120.
- [17] Yuzvinsky, Sergei, *Orthogonal pairings of Euclidean spaces*, *Michigan Math. J.* **28** (1981), 131–145.