ACADEMIC PRESS

Available at WWW.MATHEMATICSWEB.ORG POWERED BY SCIENCE @ DIRECT

Journal of Number Theory 101 (2003) 338–348

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

Optimally small sumsets in finite abelian groups

Shalom Eliahou,[a,*] Michel Kervaire,[b] and Alain Plagne[c]

[a] *Département de Mathématiques, LMPA Joseph Liouville, Université du Littoral Côte d'Opale, Bâtiment Poincaré, 50, rue Ferdinand Buisson, B.P. 699, FR-62228 Calais, France*

[b] *Département de Mathématiques, Université de Genève, 2-4, rue du Lièvre, B.P. 240, 1211 Genève 24, Switzerland*

[c] *LIX, École polytechnique, 91128 Palaiseau Cedex, France*

Received 27 July 2002

Communicated by D. Goss

Abstract

Let G be a finite abelian group of order g. We determine, for all $1 \leqslant r, s \leqslant g$, the minimal size $\mu_G(r,s) = \min|A+B|$ of sumsets $A+B$, where A and B range over all subsets of G of cardinality r and s, respectively. We do so by explicit construction. Our formula for $\mu_G(r,s)$ shows that this function only depends on the cardinality of G, not on its specific group structure. Earlier results on μ_G are recalled in the Introduction.

MSC: Primary: 11B75, 20D60; 20K01; Secondary: 05A05, 11P70

Keywords: Additive number theory; Sumset; Cauchy-Davenport theorem; Kneser theorem; Initial segment

1. Introduction

Given a finite abelian group G, we shall denote by $\mu_G(r,s)$ the minimal cardinality of the sumset $A+B = \{a+b \mid a \in A, b \in B\}$ of two subsets $A, B \subset G$ of cardinalities $|A| = r \geqslant 1, |B| = s \geqslant 1$, respectively. That is,

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

Note that, by convention, $\mu_G(r,s)$ is only defined if $1 \leqslant r, s \leqslant |G|$.

*Corresponding author. Fax: +33-3-21-46-36-69.

E-mail addresses: eliahou@lmpa.univ-littoral.fr (S. Eliahou), michel.kervaire@math.unige.ch (M. Kervaire), plagne@lix.polytechnique.fr (A. Plagne).

0022-314X/03/$ - see front matter
doi:10.1016/S0022-314X(03)00060-X

Up to now, the function $\mu_G(r,s)$ was only known for a few classes of finite abelian groups G. The result for $G=\mathbf{Z}/p\mathbf{Z}$, with p prime, goes back to Cauchy [C] and Davenport [D]. The well-known Cauchy–Davenport Theorem provides the formula

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

In 1981, Yuzvinsky [Y] made important progress by treating the group $G=(\mathbf{Z}/2\mathbf{Z})^n$. In that case, he showed that $\mu_G(r,s)=r\circ s$, where $r\circ s$ is the famous Hopf–Stiefel–Pfister function occurring in Topology and Quadratic Forms theory.

The more general case of the group $G=(\mathbf{Z}/p\mathbf{Z})^n$, with p prime, has been treated by Bollobás and Leader [BL] and Eliahou and Kervaire [EK], independently and using completely different methods. The result in [EK] states that, for such a group G,

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

where $\beta_p(r,s)=\min\{k \mid (X+Y)^k\in(X^r, Y^s)\}$, and where (X^r, Y^s) denotes the ideal generated by X^r and Y^s in the polynomial ring $\mathbf{F}_p[X,Y]$.

Actually, Bollobás and Leader [BL] treated the case of *any* finite abelian p-group G, by showing that $\mu_G(r,s)$ only depends on $|G|$, not on its particular p-group structure.

Finally, very recently, Plagne [P] determined $\mu_G(r,s)$ for the cyclic group $G=\mathbf{Z}/g\mathbf{Z}$, where g is an arbitrary positive integer. His formula reads

$$\mu_{\mathbf{Z}/g\mathbf{Z}}(r,s)=\min_{d|g}\left\{\left(\left\lceil\frac{r}{d}\right\rceil+\left\lceil\frac{s}{d}\right\rceil-1\right)d\right\},$$

where $\lceil\xi\rceil$, the ceiling of $\xi\in\mathbf{R}$, is the smallest integer x such that $\xi\leqslant x$.

More precisely, he obtained the above result by establishing both a lower bound and an upper bound on $\mu_G(r,s)$, where now G is an arbitrary abelian group of order g and exponent e:

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

Our purpose in this paper is to complete the determination of $\mu_G(r,s)$ for all finite abelian groups. We shall prove the following.

Theorem. *Let G be any finite abelian group of order g. For all r,s satisfying $1\leqslant r,s\leqslant g$, one has*

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

In particular, this result shows that $\mu_G(r,s)$ only depends on the cardinality of G, but not on its particular abelian group structure.

One noteworthy aspect of our proof below is that it provides, for any given r,s such that $1\leqslant r,s\leqslant|G|$, an explicit construction of pairs of subsets $A,B\subset G$

realizing the lower bound $\mu_G(r,s)$, i.e. such that $|A|=r$, $|B|=s$ and $|A+B|=\mu_G(r,s)$.

The proof of the Theorem is given in Sections 2 and 3. In Section 4, we recall the proof of the inequality in [P]

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

which is used in Section 3.

Finally, in Section 5 we mention some open questions. In particular, we discuss briefly the case of a non-commutative group G.

2. The inequality $\mu_G(r,s)\leqslant r+s-1$

The bulk of the proof of the above theorem is contained in the following seemingly weaker statement.

Lemma. *Let G be a finite abelian group and r,s two integers such that $1\leqslant r,s\leqslant |G|$. Then*

$$\mu_G(r,s)\leqslant r+s-1.$$

The proof of the Theorem will then follow as a simple corollary of this lemma in the next section (Section 3).

We prove the lemma by exhibiting subsets $A,B\subset G$ of cardinalities r,s such that $|A+B|\leqslant r+s-1$. For this purpose, we need to introduce a suitable order relation on G.

We choose a decomposition $G=\mathbf{Z}/n_1\mathbf{Z}\times\cdots\times\mathbf{Z}/n_k\mathbf{Z}$ as a direct product of cyclic groups. (We do not require that n_i divides n_{i+1} for any i.) In each factor $\mathbf{Z}/n_i\mathbf{Z}$, the residue classes mod n_i will be represented by the integers $0,1,\dots,n_i-1$ and then ordered by their natural order as integers. We then endow G with the lexicographic order corresponding to the direct product decomposition. That is, $(x_1,x_2,\dots,x_k)<(y_1,y_2,\dots,y_k)$ if and only if for some i in the interval $1\leqslant i\leqslant k$, we have $x_j=y_j$ for $j<i$ and $x_i<y_i$.

By definition, an *initial segment* of the ordered set G is then an ordered subset $A=\{a_1<a_2<\cdots<a_r\}\subset G$ with minimum $a_1=(0,0,\dots,0)\in G$, the neutral element of G, and with no element of G strictly between a_i and a_{i+1}. For instance, the initial segment of *length* n_k+1 is

$$\{(0,\dots,0,0),(0,\dots,0,1),\dots,(0,\dots,0,n_k-1),(0,\dots,1,0)\}.$$

We state our strengthened form of the above lemma as the following proposition:

Proposition. *Let G be a finite abelian group and $G=\mathbf{Z}/n_1\mathbf{Z}\times\cdots\times\mathbf{Z}/n_k\mathbf{Z}$ a decomposition of G as a direct product of cyclic groups. We view G as an ordered set as* *explained above. Let* $A, B \subset G$ *be two non-empty initial segments in* G. *Then*, $|A+B| \leqslant |A| + |B| - 1$.

In particular, $\mu_G(r,s) \leqslant r+s-1$ *for all* $1 \leqslant r, s \leqslant |G|$.

Proof. We proceed by induction on k, the number of cyclic factors in the given product decomposition of G.

For $k=1$, $G = \mathbf{Z}/n\mathbf{Z}$, let $A = \{0,1,\dots,r-1\}$ and $B = \{0,1,\dots,s-1\}$ be the initial segments of respective lengths $|A| = r \geqslant 1, |B| = s \geqslant 1$. Then, A and B are non-empty and thus

$$A+B = \begin{cases} \{0,1,\dots,r+s-2\} & \text{if } (r-1)+(s-1) = r+s-2 < n, \\ \{0,1,\dots,n-1\} & \text{if } n \leqslant r+s-2. \end{cases}$$

Hence, $|A+B| \leqslant r+s-1$ in both cases.

Therefore the Proposition is satisfied whenever G is a cyclic group (with the ordering specified above). In addition, we see from the proof that *the sumset of any two non-empty initial segments in a cyclic group is again an initial segment*, a fact we shall use later on.

Assuming now $k \geqslant 2$, let us write $G = H_1 \times H_2$, where $H_1 = \mathbf{Z}/n_1\mathbf{Z}$ and H_2 is the product $\mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_k\mathbf{Z}$ of the $(k-1)$ remaining factors. By the induction hypothesis, we may assume that H_2 satisfies the assertion of the Proposition.

Suppose that $1 \leqslant r, s \leqslant |G|$ and let $A, B \subset G$ be the initial segments of G with cardinalities r, s, respectively.

We want to prove that $|A+B| \leqslant r+s-1$.

Let $r = r_1|H_2| + r_2$ and $s = s_1|H_2| + s_2$ be the Euclidean divisions of r, s by $|H_2|$ with $0 \leqslant r_2 < |H_2|$, $0 \leqslant s_2 < |H_2|$.

From the above description of initial segments, we see that

$$A = (A_1 \times H_2) \cup (\{a\} \times A_2), \quad B = (B_1 \times H_2) \cup (\{b\} \times B_2),$$

where A_2, B_2 are the initial segments of lengths r_2, s_2 in H_2, respectively, $A_1 \subset A_1 \cup \{a\}$ are the initial segments in H_1 of lengths $|A_1| = r_1$ and $|A_1| + 1 = r_1 + 1$, respectively, and $B_1 \subset B_1 \cup \{b\}$ are the initial segments in H_1 of lengths $|B_1| = s_1$ and $|B_1| + 1 = s_1 + 1$, respectively.

It may of course very well happen that some of the cardinalities r_1, r_2, s_1, s_2 vanish, but not r_1 and r_2 simultaneously, nor s_1 and s_2 simultaneously though.

The various possible cases will be treated separately.

If $r_1 = s_1 = 0$, that is $A_1 = B_1 = \emptyset$, then

$$|A+B| = |A_2 + B_2| \leqslant |A_2| + |B_2| - 1 = |A| + |B| - 1,$$

by induction hypothesis on H_2, because A_2, B_2 of lengths $r_2 = r, s_2 = s$ are non-empty initial segments of H_2.

Similarly, if $r_2 = s_2 = 0$, then $A_2 = B_2 = \emptyset$. We have

$$|A_1 + B_1| \leqslant |A_1| + |B_1| - 1,$$

because H_1 is cyclic and again A_1, B_1 are non-empty initial segments of H_1. Using $A = A_1 \times H_2, B = B_1 \times H_2$, and thus $A + B = (A_1 + B_1) \times H_2$, because H_2 is a subgroup, we get

$$\begin{aligned}|A + B| &= |A_1 + B_1| \cdot |H_2| \\ &\leqslant (|A_1| + |B_1| - 1) \cdot |H_2| \\ &= |A| + |B| - |H_2| \leqslant r + s - 1,\end{aligned}$$

as desired.

Suppose now that $B_2 = \emptyset$ and $A_2 \neq \emptyset$. Then, $B = B_1 \times H_2$ with $B_1 \neq \emptyset$. We get

$$A + B \subset ((A_1 \cup \{a\}) + B_1) \times H_2.$$

Even if A_1 is empty, both $A_1 \cup \{a\}$ and B_1 are non-empty initial segments of H_1 and thus

$$|A + B| \leqslant (|A_1| + |B_1|) \cdot |H_2| = |A| - |A_2| + |B| \leqslant r + s - 1.$$

The case $A_2 = \emptyset$ with $B_2 \neq \emptyset$ is symmetrical, interchanging A and B.

We may thus assume that both A_2 and B_2 are non-empty.

Finally, let us examine the case where $A_1 \neq \emptyset$ and $B_1 = \emptyset$. In this case, b is necessarily the 0-element in H_1 and we have

$$A + B \subset ((A_1 + \{b\}) \times H_2) \cup (\{a + b\} \times (A_2 + B_2)).$$

We obtain for the cardinality of $A + B$ the estimate

$$|A + B| \leqslant |A_1| \cdot |H_2| + |A_2| + |B_2| - 1 = |A| + |B| - 1.$$

The case $A_1 = \emptyset$ and $B_1 \neq \emptyset$ is again symmetrical and we have thus completed the examination of the exceptional cases where at least one of the sets A_1, B_1, A_2, B_2 is empty.

We come now to the main case where we assume that all four initial segments A_1, B_1, A_2, B_2 are non-empty. To ease notation, we set

$$X_a = (A_1 \cup \{a\}) + B_1 \subset H_1,$$

and similarly

$$X_b = A_1 + (B_1 \cup \{b\}) \subset H_1.$$

Denote by $X = X_a \cup X_b$ their union in H_1. Using the explicit descriptions $A = (A_1 \times H_2) \cup (\{a\} \times A_2)$ and $B = (B_1 \times H_2) \cup (\{b\} \times B_2)$, we have by direct observation

$$A + B \subset (X \times H_2) \cup (\{a+b\} \times (A_2 + B_2)).$$

Claim. $|X| \leqslant |A_1| + |B_1|$.

Indeed, as observed earlier, the sumset $U + V$ of two initial segments U and V in a cyclic group is again an initial segment. It follows in particular that X_a and X_b are initial segments in H_1. Thus, one of them is contained in the other, $X_a \subset X_b$ or $X_b \subset X_a$ and we may assume without loss of generality that $X_a \subset X_b$. It follows that $X = X_b = A_1 + (B_1 \cup \{b\})$. Since A_1 and $B_1 \cup \{b\}$ are non-empty initial segments in H_1, we have $|X| \leqslant |A_1| + |B_1|$ as claimed. □

Using this estimate for $|X|$, and the fact that A_2, B_2 are non-empty initial segments in H_2, the inclusion $A + B \subset (X \times H_2) \cup (\{a+b\} \times (A_2 + B_2))$ implies

$$\begin{aligned} |A+B| &\leqslant |X|\,|H_2| + |A_2 + B_2| \\ &\leqslant (|A_1| + |B_1|)|H_2| + |A_2| + |B_2| - 1 \\ &= r + s - 1. \end{aligned}$$

This finishes the proof of the Proposition. □

The Theorem, which we prove in the next section, is a simple corollary of the above Lemma.

3. Completion of the proof of the Theorem

Let G be a finite abelian group of order g and recall Plagne's inequality

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

In this section, we prove that the lemma in Section 2 implies

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

Let h be a positive integer dividing g and such that

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

Since G is an abelian group, there exists a subgroup H of G, of order h. Let $G_0 = G/H$ and $g_0 = g/h$ the order of G_0.

We set $r_0 = \lceil \frac{r}{h} \rceil$, $s_0 = \lceil \frac{s}{h} \rceil$. Of course, we have $1 \leqslant r_0, s_0 \leqslant g_0$.

Let $A_0, B_0 \subset G_0$ be two subsets of G_0 of respective cardinalities r_0 and s_0, such that

$$|A_0 + B_0| = \mu_{G_0}(r_0, s_0).$$

According to the Lemma in Section 2, we have

$$|A_0 + B_0| \leqslant r_0 + s_0 - 1.$$

Let us define

$$A' = \pi^{-1}(A_0) \quad \text{and} \quad B' = \pi^{-1}(B_0),$$

where $\pi : G \to G_0$ denotes the natural projection.
We have

$$|A'| = r' = r_0 \cdot h, \quad |B'| = s' = s_0 \cdot h.$$

Since $r_0 = \lceil \frac{r}{h} \rceil \geqslant \frac{r}{h}$ and $s_0 = \lceil \frac{s}{h} \rceil \geqslant \frac{s}{h}$, we have

$$r' = r_0 \cdot h \geqslant r \quad \text{and} \quad s' = s_0 \cdot h \geqslant s.$$

Now let $A \subset A'$ and $B \subset B'$ be subsets of cardinalities $|A| = r, \ |B| = s$. We have $A + B \subset A' + B'$ and

$$|A + B| \leqslant |A' + B'| = |A_0 + B_0| h \leqslant (r_0 + s_0 - 1)h.$$

Thus,

$$\begin{aligned} |A + B| &\leqslant (r_0 + s_0 - 1)h \\ &= \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h \\ &= \min_{d|g} \left\{ \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d \right\} \leqslant \mu_G(r, s). \end{aligned}$$

Since, of course, $\mu_G(r, s) \leqslant |A + B|$, equality holds in this string of inequalities, and in particular

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

Remark. (1) Observe that in the above proof, we must necessarily have

$$\mu_{G_0}(r_0, s_0) = r_0 + s_0 - 1.$$

Indeed, if $|A_0 + B_0|$ were strictly smaller than $r_0 + s_0 - 1$, then the above construction would lead to sets $A \subset \pi^{-1}(A_0)$, $B \subset \pi^{-1}(B_0)$ with $|A| = r, \ |B| = s$ such that $|A + B|$ would be strictly smaller than $\mu_G(r, s)$, which is absurd.

(2) Observe also that once a decomposition of G_0 as a direct product of cyclic groups has been chosen, then the Proposition in Section 2 yields explicit sets $A_0, B_0 \subset G_0$ with $|A_0 + B_0| = r_0 + s_0 - 1$, and thus explicit inverse images $A' = \pi^{-1}(A_0), B' = \pi^{-1}(B_0)$.

Hence, given G of order g and integers r, s such that $1 \leqslant r, s \leqslant g$, the arbitrary choices to be made in order to arrive at a pair A, B with $|A| = r, |B| = s$ and $|A + B| = \mu_G(r, s)$ are as follows:

- Choice of h dividing g such that

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

In general, an integer h with this property is not unique. For instance, for $|G| = 4, r = 2, s = 4$, we have $\mu_G(2, 4) = 4$. The minimum $\mu_G(2, 4)$ of $(\lceil \frac{2}{d} \rceil + \lceil \frac{4}{d} \rceil - 1)d$ for d dividing 4 is attained at both $d = 2$ and 4.

One could of course specify h by the requirement to be the smallest possible choice.

- Choice of a subgroup H of order h in G.
- Choice of a decomposition of $G_0 = G/H$ as a direct product of cyclic groups.
- Choice of a pair of sets A, B such that $A \subset A', B \subset B'$ with the right cardinalities r, s.

The last choice is rather trivial. The two choices dealing with H and the direct product decomposition of G_0 of course largely depend on the automorphism groups of G and G_0.

4. The inequality $\mu_G(r, s) \geqslant \min_{d|g}\{(\lceil \frac{r}{d} \rceil + \lceil \frac{s}{d} \rceil - 1)d\}$

Let G be a finite abelian group of order g and let r, s be two positive integers satisfying $1 \leqslant r, s \leqslant g$.

In this section we repeat, for the sake of completeness, the proof from Plagne [P] of the lower bound

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

which we have used in the proof of the above Theorem.

We choose two subsets $A \subset G$ and $B \subset G$ of cardinalities r, s respectively, such that

$$|A + B| = \mu_G(r, s),$$

and appeal to the theorem of Kneser (see [K] or [M, Theorem 1.5, p. 6] or [N, Theorem 4.3, p. 116]). Kneser's theorem asserts that there exists a subgroup $H \subset G$

such that

$$|A+B| \geqslant |A+H| + |B+H| - |H|,$$

and we obtain

$$|A+B| \geqslant \left(\frac{|A+H|}{|H|} + \frac{|B+H|}{|H|} - 1\right) \cdot |H| \\ \geqslant \left(\left\lceil\frac{r}{h}\right\rceil + \left\lceil\frac{s}{h}\right\rceil - 1\right)h,$$

where h denotes the cardinality of H.

Indeed, $\frac{|A+H|}{|H|} \geqslant \frac{|A|}{|H|} = \frac{r}{h}$, and as $A+H$ is a disjoint union of H-cosets, $\frac{|A+H|}{|H|}$ is an integer. Thus, $\frac{|A+H|}{|H|} \geqslant \lceil \frac{r}{h} \rceil$, the ceiling of $\frac{r}{h}$. Similarly, we have $\frac{|B+H|}{|H|} \geqslant \lceil \frac{s}{h} \rceil$.

Since h is a divisor of g, the order of G, it follows that

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

as required. □

5. Related open problems

(1) There is of course the Inverse Problem of characterizing the pairs of subsets $A, B \subset G$ with the prescribed cardinalities $|A| = r$, $|B| = s$ which realize the minimal sumset size $|A+B| = \mu_G(r,s)$.

(2) We now briefly discuss the non-commutative case.

(2.1) The formula for $\mu_G(r,s)$ given in our theorem definitely cannot hold in general for non-abelian groups.

In fact, we have the following assertion.

Proposition. *Let G be a finite group and let r be an integer such that* $1 \leqslant r \leqslant |G|$. *Then,* $\mu_G(r,r) = r$ *if and only if G contains a subgroup of order r.*

We include the proof of this proposition in view of its simplicity.

Proof. Observe first that if $1 \leqslant s, t \leqslant |G|$, then $\mu_G(s,t) \geqslant \max\{s,t\}$ because if $A, B \subset G$, then $A \cdot B$ contains at least the left-translate of B by an element of A, and the right-translate of A by an element of B.

In particular, $\mu_G(r,r) \geqslant r$ for any r.

If $H \leqslant G$ is a subgroup of order r, then $H \cdot H = H$, whence $\mu_G(r,r) = r$.

Conversely, if $\mu_G(r,r) = r$, let $A, B \subset G$ with $|A| = |B| = |A \cdot B| = r$. We may assume $1 \in A \cap B$ by left translating A and/or right translating B if necessary. It follows that A and B are both contained in $A \cdot B$. Since $|A| = |B| = |A \cdot B|$, we must have $A = B = A \cdot B$ implying that A is a subgroup of G. $\square$

If now G is a (necessarily non-abelian) finite group with no subgroup of order d for some divisor d of $|G|$, then $\mu_G(d,d) > d$. In contrast, for the same d, and for $g = |G|$, we have $\mu_{\mathbf{Z}/g\mathbf{Z}}(d,d) = d$.

As an example, let G be the alternating group A_4 of order 12 consisting of the even permutations in S_4. It is well known that G contains no subgroup of order 6. Therefore, $\mu_G(6,6) > 6$.

We have determined (by machine calculation) the entire set of values of the function μ_G for $G = A_4$. Interestingly, the behavior of μ_G can be summarized by the formula

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

where the minimum is taken over all orders $d = 1,2,3,4,12$ of subgroups of G.

In particular, for $r = s = 6$, we have $\mu_G(6,6) = 9$, attained at $d = 3$ in the formula. An optimal pair $A, B \subset A_4$, with $|A| = |B| = 6$, realizing the minimal possible value $|A \cdot B| = 9$ is for instance $A = \{1, a, ac, bc, ac^2, abc^2\}$, $B = \{1, a, c, ac, bc^2, abc^2\}$, where $a = (1,2)(3,4)$, $b = (1,3)(2,4)$ and $c = (1,2,3)$ in cycle notation (we use multiplication from left to right, whence $ca = abc, cb = ac$).

It is not clear whether, in general, μ_G can be described by such a simple formula for an arbitrary finite non-abelian group G.

(2.2) As a weaker problem than the one above, is it true that $\mu_G(r,s)$ is bounded below by $\mu_{\mathbf{Z}/g\mathbf{Z}}(r,s)$ with $g = |G|$, i.e.

$$\mu_{\mathbf{Z}/g\mathbf{Z}}(r,s) \leqslant \mu_G(r,s)$$

for any finite (non-abelian) group G of order g?

(2.3) As yet another weaker problem than in (2.1), can one at least expect the upper bound

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

for any (finite) group G? We can prove that this upper bound holds true for finite solvable groups.

Acknowledgments

During the preparation of this paper, the first author has partially benefited from a research contract with the Fonds National Suisse pour la Recherche Scientifique.

References

[BL] B. Bollobás, I. Leader, Sums in the grid, Discrete Math. 162 (1996) 31–48.
[C] A.-L. Cauchy, Recherches sur les nombres, J. École Polytechnique 9 (1813) 99–123.
[D] H. Davenport, On the addition of residue classes, J. London Math. Soc. 10 (1935) 30–32.
[EK] S. Eliahou, M. Kervaire, Sumsets in vector spaces over finite fields, J. Number Theory 71 (1998) 12–39.
[K] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, Math. Z. 58 (1953) 459–484.
[M] H.B. Mann, Addition Theorems, Interscience Publishers, Wiley, New York, 1965.
[N] M.B. Nathanson, Additive number theory: inverse problems and the geometry of sumsets, in: Graduate Text in Mathematics, Vol. 165, Springer, Berlin, 1996.
[P] A. Plagne, Additive number theory sheds extra light on the Hopf–Stiefel $\circ$ function, L'Enseignement Mathématique, to appear.
[Y] S. Yuzvinsky, Orthogonal pairings of Euclidean spaces, Michigan Math. J. 28 (1981) 109–119.