Optimally small sumsets in general Abelian groups

Alain Plagne

Centre de Mathématiques Laurent Schwartz, UMR 7640 du CNRS, École polytechnique,
91128 Palaiseau cedex, France

Received 15 June 2005; accepted 1 September 2005
Available online 24 October 2005

Abstract

When $G$ is a finite Abelian group, a formula for the $\mu_G$ function in terms of the divisors of $|G|$ was already known. In this short paper, we show how a simple argument allows us to extend this formula to all Abelian groups.

$\copyright$ 2005 Elsevier Inc. All rights reserved.

1. Introduction

Let $G$ be a finite group and $r, s$ be two positive integers $\leq |G|$. We define $\mu_G(r, s)$ as the minimal cardinality of a (Minkowski) sumset $A + B = \{a + b, a \in A, b \in B\}$ with $A, B \subset G$ and $|A| = r, |B| = s$. The study of $\mu_G$ is classical in additive number theory (see [4,5] for a general introduction to this field).

It is known that if $G$ is a finite Abelian group, then

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

This type of formula was introduced by the author in [6]. In that paper, (1) is proved to hold in the case of $p$-groups (the case of $\mathbb{Z}/p\mathbb{Z}$ reduces to the Cauchy–Davenport theorem [1,2]). It was then generalized to finite Abelian groups in [3].

E-mail address: plagne@math.polytechnique.fr.
Recently François Hennecart, in Saint-Étienne, asked whether a similar formula holds in the case of general Abelian groups (not only finite ones).

It is the aim of this Note to provide such a formula.

**Theorem.** Let $G$ be any Abelian group. Then for any integers $r, s$ satisfying $1 \leq r, s \leq |G|$, we have

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

where $D$ is the set of integers that are the cardinality of a finite subgroup of $G$.

The proof is direct, short and elementary (having (1) at hand).

2. The proof

Let us fix the positive integers $1 \leq r, s \leq |G|$. We choose some pair of sets $A, B \subset G$, $|A| = r$, $|B| = s$ in which the quantity $\mu_G(r, s)$ is attained. We consider the subgroup of $G$ generated by $A$ and $B$, say $H = \langle A \cup B \rangle$. We clearly have $|A + B| = \mu_G(r, s) = \mu_H(r, s)$ since $H \leq G$ and the definition of the $\mu$-functions imply $|A + B| = \mu_G(r, s) \leq \mu_H(r, s) \leq |A + B|$. Since $H$ is a finite type Abelian group, by the general structure theorem, it is isomorphic to $\mathbb{Z}^k \times T$ where $k$ is some nonnegative integer and $T$ is a finite product of cyclic groups. Without loss of generality, we shall assume $H = \mathbb{Z}^k \times T$.

For any positive integer $p$, denote by $\pi_p$ the canonical projection from $H = \mathbb{Z}^k \times T$ onto $(\mathbb{Z}/p\mathbb{Z})^k \times T$. Clearly, if $p$ is large enough, we have $|\pi_p(A)| = |A|$, $|\pi_p(B)| = |B|$ and $|\pi_p(A) + \pi_p(B)| = |\pi_p(A + B)| = |A + B|$ (this is in some sense a “cyclification principle” in contrast to the so-called rectification principle). It follows that for $p$ large enough,

$$
\mu_H(r, s) = |A + B| = |\pi_p(A) + \pi_p(B)| \geq \mu_{(\mathbb{Z}/p\mathbb{Z})^k \times T}(r, s).
$$

We apply this formula with $p$ a prime larger than $\mu_H(r, s) + 1$. By (1), we obtain

$$
\mu_H(r, s) \geq \min_{d | p^k | T} \left( \left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d.
$$

Let $d_0$ be a divisor of $p^k | T|$ in which the minimum in the right-hand side of this inequality is attained, then $p$ cannot divide $d_0$ otherwise

$$
p - 1 \geq \mu_H(r, s) \geq \left( \left\lceil \frac{r}{d_0} \right\rceil + \left\lceil \frac{s}{d_0} \right\rceil - 1 \right) d_0 \geq d_0 \geq p,
$$

a contradiction. Therefore, we finally get

$$
\mu_G(r, s) = \mu_H(r, s) \geq \min_{d | |T|} \left( \left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d \geq \min_{d \in D} \left( \left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d,
$$

(2)
because any divisor of $|T|$ is the cardinality of a finite subgroup of $T$ and thus of $G$.

Let now $d \in D$. By definition, there is some finite subgroup, say $V$, of $G$ with $|V| = d$. Since $V$ is a subgroup of $G$, $\mu_G(r, s) \leq \mu_V(r, s)$. Now using (1) for $V$, we obtain

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

Since this is valid for any $d \in D$, we finally obtain

$$\mu_G(r, s) \leq \min_{d \in D} \left( \left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d,$$

which implies, with (2), the Theorem.

References