# A SUPERADDITIVITY AND SUBMULTIPLICATIVITY PROPERTY FOR CARDINALITIES OF SUMSETS

KATALIN GYARMATI, MÁTÉ MATOLCSI, AND IMRE Z. RUZSA

Abstract. For finite sets of integers $A_1, A_2 \dots A_n$ we study the cardinality of the $n$-fold sumset $A_1 + \dots + A_n$ compared to those of $n-1$-fold sumsets $A_1 + \dots + A_{i-1} + A_{i+1} + \dots A_n$. We prove a superadditivity and a submultiplicativity property for these quantities. We also examine the case when the addition of elements is restricted to an addition graph between the sets.

## 1. Introduction

Let $A_1, A_2, \dots A_n$ be finite sets of integers. How does the cardinality of the $n$-fold sumset $A_1 + A_2 + \dots + A_n$ compare to the cardinalities of the $n-1$-fold sums $A_1 + \dots + A_{i-1} + A_{i+1} + \dots A_n$?

In the special case when all the sets are the same, $A_i = A \subset \mathbb{Z}$, Vsevolod Lev [7] observed that the quantity $\frac{|kA|-1}{k}$ is increasing (where we have used the standard notation for the $k$-fold sum $A + A + \dots + A = kA$). The first cases of this result assert that

$$|2A| \geq 2|A| - 1 \tag{1.1}$$

and

$$|3A| \geq \frac{3}{2}|2A| - \frac{1}{2}. \tag{1.2}$$

Inequality (1.1) can be extended to different summands as

$$|A + B| \geq |A| + |B| - 1, \tag{1.3}$$

and this inequality also holds for sets of residues modulo a prime $p$, the only obstruction being that a cardinality cannot exceed $p$, i.e.

$$|A + B| \geq \min(|A| + |B| - 1, p); \tag{1.4}$$

this familiar result is known as the Cauchy-Davenport inequality.

The third author asked whether inequality (1.2) can also be extended to different summands in the following form:

$$|A + B + C| \geq \frac{|A + B| + |B + C| + |A + C| - 1}{2}. \tag{1.5}$$

1991 *Mathematics Subject Classification.* 11B50, 11B75, 11P70.

Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. T 43631, T 43623, T 49693.

Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. PF-64061, T-049301, T-047276.

Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. T 43623, T 42750, K 61908.

Lev noticed (personal communication) that this is true in the case when the sets have the same diameter. (The diameter of a set is the difference of its maximum and minimum.) In this paper we establish this property in general, for an arbitrary number of summands, and with the extra twist that in the $n$-fold sumset it is sufficient to use the smallest or largest element of at least one of the summands.

**Theorem 1.1.** *Let $A_1, \dots, A_k$ be finite, nonempty sets of integers. Let $A_i'$ be the two- (or possibly one-) element set containing the smallest and largest elements of $A_i$. Put*

$$S = A_1 + \cdots + A_k,$$
$$S_i = A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k,$$
$$S_i' = A_1 + \cdots + A_{i-1} + A_i' + A_{i+1} + \cdots + A_k,$$
$$S' = \bigcup_{i=1}^{k} S_i'.$$

*We have*

$$|S| \ge |S'| \ge \frac{1}{k-1} \sum_{i=1}^{k} |S_i| - \frac{1}{k-1}. \tag{1.6}$$

The possibility to extend inequality (1.2) to residues modulo a prime $p$ was investigated in a paper by Gyarmati, Konyagin, Ruzsa [5]. A naive attempt to extend it in the form

$$|3A| \ge \min\left(\frac{3}{2}|2A| - \frac{1}{2}, p\right)$$

holds only when $|A|$ is small in comparison to $p$, and for larger values the relationship between the sizes of $2A$ and $3A$ is complicated.

In a sense, Theorem 1.1 means that the cardinality of sumsets grows faster than linear. On the other hand, we show that it grows slower than exponential. For identical summands this means that $|kA|^{1/k}$ is decreasing. This was conjectured by the third author. Lev observed that this is a straightforward consequence of a Plünnecke-type inequality; more details will be given in Section 4.

Here we establish a more general result for different summands.

**Theorem 1.2.** *Let $A_1, \dots, A_k$ be finite, nonempty sets in an arbitrary commutative semigroup. Put*

$$S = A_1 + \cdots + A_k,$$
$$S_i = A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k.$$

*We have*

$$|S| \le \left(\prod_{i=1}^{k} |S_i|\right)^{\frac{1}{k-1}}. \tag{1.7}$$

For three summands this inequality was established earlier by the third author ([11], Theorem 5.1). The proof given in [11] is different and works also for noncommutative groups with a proper change in the formulation. On the other hand, that argument relied on the invertibility of the operation, so we do not have any result for noncommutative semigroups. Neither could we extend that argument for more than three summands, and hence the following question remains open.

**Problem 1.3.** Let $A_1, \dots, A_k$ be finite, nonempty sets in an arbitrary noncommutative group. Put

$$S = A_1 + \cdots + A_k,$$

$$n_i = \max_{a \in A_i} |A_1 + \cdots + A_{i-1} + a + A_{i+1} + \cdots + A_k| .$$

Is it true that

$$|S| \le \left( \prod_{i=1}^{k} n_i \right)^{\frac{1}{k-1}} \quad ? \tag{1.8}$$

The superadditivity property clearly does not hold in such a general setting (as it fails already mod $p$, see [5]). However, it can easily be extended to torsion-free groups (just as everything that holds for finite sets of integers) with the change of formulation that "smallest" and "largest" do not make sense in such generality.

**Theorem 1.4.** *Let $A_1, \dots, A_k$ be finite, nonempty sets in a torsion-free group $G$,*

$$S = A_1 + \cdots + A_k,$$

$$S_i = A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k.$$

*There are subsets $A_i' \subset A_i$ having at most two elements such that with*

$$S_i' = A_1 + \cdots + A_{i-1} + A_i' + A_{i+1} + \cdots + A_k,$$

$$S' = \bigcup_{i=1}^{k} S_i'$$

*we have*

$$|S| \ge |S'| \ge \frac{1}{k-1} \sum_{i=1}^{k} |S_i| - \frac{1}{k-1}. \tag{1.9}$$

Another natural way of generalizing Theorem 1.2 is to restrict the summation of elements to a prescribed addition graph. A possible meaning of this in the case $k = 3$ (and identical sets) could read as follows. We consider a graph $G$ on our set $A$; on the right hand side of the proposed inequality we take the number of different sums of connected pairs; on the left hand side we take the number of different sums of those triplets where each pair is connected. However, the resulting inequality, $|A \overset{G}{+} A \overset{G}{+} A|^2 \le |A \overset{G}{+} A|^3$, can fail spectacularly. Take $A = [1, n]$, let $S \subset (2n/3, 4n/3)$ be a set of even integers and connect two elements of $A$ if their sum is in $S$. Then for every $s_1, s_2, s_3 \in S$ we can find $a_1, a_2, a_3 \in A$, $a_1 = (-s_1 + s_2 + s_3)/2$, etc., whose pairwise sums give these $s_i$'s. Also, $a_1 + a_2 + a_3 = (s_1 + s_2 + s_3)/2$. Therefore, if $S$ is such that all the triple sums $s_1 + s_2 + s_3$ are distinct, then the above mapping $(s_1, s_2, s_3) \mapsto (a_1, a_2, a_3)$ is injective, and the left side of the inequality will be $\binom{|S|}{3}^2 \approx \frac{1}{6}|S|^6$, much larger than the right hand side, which is $S^3$.

It would be interesting to say something when the graphs are sufficiently dense.

However, we will prove a similar statement in the case when only one pair of summands is restricted.

**Theorem 1.5.** *Let $A, B_1, B_2$ be finite sets in a commutative group, and $S \subset B_1 + B_2$. Then*

$$|S + A|^2 \leq |S||A + B_1||A + B_2| \tag{1.10}$$

The analogous statement for more than three sets remains an open problem.

**Problem 1.6.** Let $A, B_1, \dots B_k$ be finite sets of integers, and $S \subset B_1 + \dots + B_k$. Is it true that

$$|S + A|^k \leq |S| \prod_{i=1}^{k} |A + B_1 + \dots + B_{i-1} + B_{i+1} + \dots + B_k| \ ? \tag{1.11}$$

## 2. Proof of superadditivity

In this section we prove Theorems 1.1 and 1.4.

*Proof of Theorem 1.1.* Both sides of the inequality are invariant under translation, therefore we can assume that the smallest element of each $A_i$ is 0. Also, let us denote the largest element of $A_i$ by $a_i$. Then $S$ is a subset of the interval $[0, a_1 + a_2 + \dots + a_k]$.

Make $k-1$ copies of the set $S$. In the first copy mark the elements of $0 + A_1 + \dots + A_{k-1}$. They all belong to the interval $[0, a_1 + \dots + a_{k-1}]$. In the remaining interval $(a_1 + \dots + a_{k-1}, a_1 + \dots + a_{k-1} + a_k]$ of the first copy of $S$ mark the elements of $a_{k-1} + A_1 + A_2 + \dots + A_{k-2} + A_k$ which fall in there. These elements correspond exactly to the elements of $A_1 + A_2 + \dots + A_{k-2} + A_k$ which are larger than $a_1 + \dots + a_{k-2}$. We denote this latter set by $(A_1 + A_2 + \dots + A_{k-2} + A_k)_{>a_1+\dots+a_{k-2}}$.

Then, for $2 \leq i \leq k-2$, in the $i$th copy of $S$ mark the elements of $0 + (A_1 + A_2 + \dots + A_{k-i} + A_{k-i+2} + \dots + A_k)_{\leq a_1+\dots+a_{k-i}}$, and the elements of $a_{k-i} + (A_1 + \dots + A_{k-i-1} + A_{k-i+1} + \dots + A_k)_{>a_1+\dots a_{k-i-1}}$. Finally, in the $k-1$st copy of $S$ mark the elements of $0 + (A_1 + A_3 + \dots + A_k)_{\leq a_1}$ and the elements of $a_1 + (A_2 + \dots + A_k)_{>a_1}$.

Note that all marked elements belong to $S'$. Also, for $1 \leq i \leq k-2$ the number of marked elements in the second section of the $i$th copy and the first section of the $i+1$st copy of $S$ is exactly $|A_1 + \dots + A_{k-i-1} + A_{k-i+1} + \dots + A_k|$. Furthermore, the number of marked elements in the first section of the first copy is $|A_1 + \dots + A_{k-1}|$, while in the second section of the last copy it is $|A_2 + A_3 + \dots + A_k| - 1$. Let $M$ denote the set of marked elements. Then, by construction,

$$(k-1)|S| \geq (k-1)|S'| \geq |M| = \sum_{i=1}^{k} |S_i| - 1 \tag{2.1}$$

and we are done. □

*Proof of Theorem 1.4.* This is a standard reduction argument to the case of integers. Let $H$ denote the subgroup generated by the elements of $\cup_{i=1}^{k} A_i$. As a finitely generated torsion-free group $H$ is isomorphic to $\mathbb{Z}^d$ for some $d$, therefore we can assume without loss of generality that $A_i \subset \mathbb{Z}^d$. Then, for a large enough integer $m$ the homomorphism $\phi_m : \mathbb{Z}^d \to \mathbb{Z}$ defined by $(z_1, z_2, \dots z_d) \mapsto mz_1 + m^2 z_2 + \dots m^d z_d$ preserves the additive identities of all elements of sumsets involved in the desired inequality (this means that $\phi_m$ is one-to-one restricted to these elements). Finally, if $B_i$ denotes the image of $A_i$ under $\phi_m$ then the desired two-element subsets $A_i'$ can be chosen as $A_i' = \phi_m^{-1}(B_i')$. □

## 3. Proof of submultiplicativity

In this section we prove Theorem 1.2. We begin with a lemma on the size of projections.

**Lemma 3.1.** *Let $d \geq 2$ be an integer, $X_1, \ldots, X_d$ arbitrary sets,*

$$B \subset X_1 \times \cdots \times X_d$$

*be a finite subset of their Cartesian product. Let*

$$B_i \subset X_1 \times \cdots \times X_{i-1} \times X_{i+1} \times \cdots \times X_d$$

*be the corresponding "projection" of $B$:*

$$B_i = \{(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_d) : \exists x \in X_i \text{ such that } (x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_d) \in B\}.$$

*We have*

$$|B|^{d-1} \leq \prod_{i=1}^{d} |B_i| \,. \tag{3.1}$$

This lemma is not new. It is essentially equivalent to an entropy inequality of Han [6], see also Cover–Thomas [4], Theorem 16.5.1. It follows from Shearer's inequality [3] or from Bollobás and Thomason's Box Theorem [2]. We include a proof for fun.

*Proof.* We prove this lemma by induction on $d$. For $d = 2$ the statement is obvious. Assume now that the statement holds for $d-1$, and consider the case $d$.

Make a list $\{b_1, b_2, \ldots, b_t\}$ of those elements of $X_1$ which appear as a first coordinate of some element in $B$. Partition the set $B$ according to these first coordinates as

$$B = B(b_1) \cup B(b_2) \cup \cdots \cup B(b_t), \tag{3.2}$$

where

$$B(b_i) = \{(b_i, x_2, x_3, \ldots, x_d) = b : \ b \in B\}. \tag{3.3}$$

By the inductive hypothesis we have $|B(b_i)|^{d-2} \leq |B(b_i)_2| \cdots |B(b_i)_d|$, that is,

$$|B(b_i)|^{\frac{d-2}{d-1}} \leq (|B(b_i)_2| \cdots |B(b_i)_d|)^{\frac{1}{d-1}} \,. \tag{3.4}$$

It is also clear that $|B(b_i)| \leq |B_1|$, and hence

$$|B(b_i)| \leq (|B(b_i)_2| \cdots |B(b_i)_d|)^{\frac{1}{d-1}} \, |B_1|^{\frac{1}{d-1}} \,. \tag{3.5}$$

Using this and Hölder's inequality we obtain

$$|B| = \sum_{i=1}^{t} |B(b_i)| \leq |B_1|^{\frac{1}{d-1}} \sum_{i=1}^{t} (|B(b_i)_2| \cdots |B(b_i)_d|)^{\frac{1}{d-1}} \leq \tag{3.6}$$

$$\leq |B_1|^{\frac{1}{d-1}} \prod_{j=2}^{d} \left( \sum_{i=1}^{t} |B(b_i)_j| \right)^{\frac{1}{d-1}} = \prod_{j=1}^{d} |B_j|^{\frac{1}{d-1}} \,, \tag{3.7}$$

which proves the statement. □

We now turn to the proof of Theorem 1.2.

*Proof.* Let us list the elements of the sets $A_1, A_2, \dots, A_k$ in some order:

$$\begin{aligned} A_1 &= \{c_{11}, c_{12}, \dots, c_{1t_1}\}, \\ A_2 &= \{c_{21}, c_{22}, \dots, c_{2t_2}\}, \\ &\vdots \\ A_k &= \{c_{k1}, c_{k2}, \dots, c_{kt_k}\}. \end{aligned}$$

For each $s \in S$ let us consider the decomposition

$$s = c_{1i_1} + c_{2i_2} + \cdots + c_{ki_k}, \tag{3.8}$$

where the finite sequence $(i_1, i_2, \dots, i_k)$, composed of the (second) indices of $c_{ji_j}$, is minimal in lexicographical order. Let us define a function $f$ from $S$ to the Cartesian product $A_1 \times A_2 \times \cdots \times A_k$, by

$$f(s) = (c_{1i_1}, c_{2i_2}, \dots, c_{ki_k}) \in A_1 \times \cdots \times A_k. \tag{3.9}$$

This function is well-defined, and it maps the set $S$ to a set $B \subset A_1 \times \cdots \times A_k$ such that $|B| = |A_1 + \cdots + A_k|$. Applying Lemma 3.1 to the set $B$ we get

$$|B|^{k-1} \le |B_1|\,|B_2| \cdots |B_k|. \tag{3.10}$$

Therefore, it is sufficient to show that

$$|B_j| \le |A_1 + A_2 + \cdots + A_{j-1} + A_{j+1} + \cdots + A_k|. \tag{3.11}$$

This inequality, however, follows easily from the fact that sum of the coordinates is distinct for each element in $B_j$. Indeed, assume that there exist two elements $z \neq z' \in B_j$ such that

$$\begin{aligned} z &= (c_{1i_1}, c_{2i_2}, \dots, c_{j-1i_{j-1}}, c_{j+1i_{j+1}}, \dots c_{ki_k}), \\ z' &= (c_{1i'_1}, c_{2i'_2}, \dots, c_{j-1i'_{j-1}}, c_{j+1i'_{j+1}}, \dots, c_{ki'_k}), \end{aligned}$$

and

$$c_{1i_1} + c_{2i_2} + \cdots + c_{ki_k} = c_{1i'_1} + c_{2i'_2} + \cdots + c_{ki'_k}.$$

We may assume that

$$(i_1, i_2, \dots, i_{j-1}, i_{j+1}, \dots, i_k) < (i'_1, i'_2, \dots, i'_{j-1}, i'_{j+1}, \dots, i'_k).$$

in lexicographical order.

Now, $z' \in B_j$ therefore there exists an element $d \in A_j$ and $u \in S$, such that

$$u = c_{1i'_1} + c_{2i'_2} + \cdots + c_{j-1i'_{j-1}} + d + c_{j+1i'_{j+1}} + \cdots + c_{ki'_k},$$

and

$$f(u) = (c_{1i'_1}, c_{2i'_2}, \dots, c_{j-1i'_{j-1}}, d, c_{j+1i'_{j+1}}, \dots, c_{ki'_k}) \in B.$$

Note that

$$u = c_{1i_1} + c_{2i_2} + \cdots + c_{j-1i_{j-1}} + d + c_{j+1i_{j+1}} + \cdots + c_{ki_k},$$

also holds. However, with $d = c_{ji_j}$ we have

$$(i_1, i_2, \dots, i_{j-1}, i_j, i_{j+1}, \dots, i_k) < (i'_1, i'_2, \dots, i'_{j-1}, i_j, i'_{j+1}, \dots, i'_k).$$

in lexicographical order, therefore the definition of $f$ implies that
$f(u) \neq (c_{1i'_1}, c_{2i'_2}, \dots, c_{j-1i'_{j-1}}, d, c_{j+1i'_{j+1}}, \dots, c_{ki'_k})$, a contradiction. □

A similar method is used by Alon [1] for the particular case when we have sets instead of numbers, the operation is intersection, and the sets $A_i$ are identical. As Alon observes, the same approach works for general semigroups where the elements are idempotent.

## 4. Restricted sums and Plünnecke-type results

Plünnecke [10] developed a graph-theoretic method to estimate the density of sumsets $A+B$, where $A$ has a positive density and $B$ is a basis. The third author published a simplified version of his proof [12, 13]. Accounts of this method can be found in Malouf [8], Nathanson [9], Tao and Vu [14].

The simplest instance of Plünnecke's inequality for finite sets goes as follows.

**Theorem 4.1.** *Let $i < k$ be integers, $A$, $B$ sets in a commutative group and write $|A| = m$, $|A + iB| = \alpha m$. There is an $X \subset A$, $X \neq \emptyset$ such that*

$$|X + kB| \leq \alpha^{k/i}|X|. \tag{4.1}$$

As Lev observed, this is sufficient to deduce the monotonicity of $|kA|^{1/k}$. Indeed, in the above result replace $B$ by $A$ and $A$ by $\{0\}$. Then $\alpha = |iA|$, the only possibility is $X = \{0\}$ and (4.1) reduces to $|kA| \leq |iA|^{k/i}$.

The application to different summands is less straightforward. We start from the following result from [12], which extends the case $i = 1$ of Theorem 4.1 to the addition of different sets.

**Theorem 4.2.** *Let $A$, $B_1, \ldots, B_h$ be finite sets in a commutative group and write $|A| = m$,*
*$|A + B_i| = \alpha_i m$, for $1 \leq i \leq h$. There exists an $X \subset A$, $X \neq \emptyset$ such that*

$$|X + B_1 + \cdots + B_h| \leq \alpha_1\alpha_2 \ldots \alpha_h|X|. \tag{4.2}$$

In the sequel we will need a 'large' subset $X \subset A$, not just a non-empty one. This will be achieved by the following result.

**Theorem 4.3.** *Let $A$, $B_1, \ldots, B_h$ be finite sets in a commutative group and write $|A| = m$,*
*$\prod |A + B_i| = s$, $B_1 + \cdots + B_h = B$. Let an integer $k$ be given, $1 \leq k \leq m$. There is an $X \subset A$, $|X| \geq k$ such that*

$$|X + B| \leq \frac{s}{m^h} + \frac{s}{(m-1)^h} + \cdots + \frac{s}{(m-k+1)^h} + (|X| - k)\frac{s}{(m-k+1)^h}. \tag{4.3}$$

*Proof.* We use induction on $k$. The case $k = 1$ is Theorem 4.2.

Assume we know it for $k$; we prove it for $k+1$. The assumption gives us a set $X$, $|X| \geq k$ with a bound on $|X + B|$ as given by (4.3). We want to find a set $X'$ with $|X'| \geq k + 1$ and

$$|X' + B| \leq \frac{s}{m^h} + \frac{s}{(m-1)^h} + \cdots + \frac{s}{(m-k)^h} + (|X'| - k - 1)\frac{s}{(m-k)^h}. \tag{4.4}$$

If $|X| \geq k+1$, we can put $X' = X$. If $|X| = k$, we apply Theorem 4.2 to the sets $A \setminus X$, $B_1$, …, $B_h$. This yields a set $Y \subset A \setminus X$ such that

$$|Y + B| \leq \frac{s}{(m-k)^h}|Y|$$

and we put $X' = X \cup Y$. □

The following variant will be more comfortable for calculations.

**Theorem 4.4.** *Let $A$, $B_1, \dots, B_h$ be finite sets in a commutative group and write $|A| = m$,*
*$\prod |A + B_i| = s$, $B_1 + \dots + B_h = B$. Let a real number $t$ be given, $0 \le t < m$. There is an $X \subset A$, $|X| > t$ such that*

$$|X + B| \le \frac{s}{h-1}\left(\frac{1}{(m-t)^{h-1}} - \frac{1}{m^{h-1}}\right) + (|X| - t)\frac{s}{(m-t)^h}. \tag{4.5}$$

*Proof.* We apply Theorem 4.3 with $k = [t] + 1$. The right side of (4.5) can be written as $s\int_0^{|X|} f(x)\,dx$, where $f(x) = (m-x)^{-h}$ for $0 \le x \le t$, and $f(x) = (m-t)^{-h}$ for $t < x \le |X|$. Since $f$ is increasing, the integral is $\ge f(0) + f(1) + \dots + f(|X| - 1)$. This exceeds the right side of (4.3) by a termwise comparison. □

*Proof of Theorem 1.5.* Let us use the notation $|A| = m$, $s = |A + B_1||A + B_2|$, as above.
Observe that if $|S| \le s/m^2$ then

$$|S + A| \le |S||A| = \sqrt{|S|}\sqrt{|S|}|A| \le \sqrt{|S|}(\sqrt{s}/m)|A| = \sqrt{s|S|} \tag{4.6}$$

and we are done.

If $|S| > s/m^2$ then define $t = m - \sqrt{s/|S|}$, and use Theorem 4.4 above to find a set $X \subset A$ such that $|X| = r > t$ and (4.5) holds with $h = 2$. For such an $X$ we have

$$|S + X| \le |B_1 + B_2 + X| \le \frac{s}{m-t} - \frac{s}{m} + (|X| - t)\frac{s}{(m-t)^2} \tag{4.7}$$

and

$$|S + (A \setminus X)| \le |S||A \setminus X|. \tag{4.8}$$

We conclude that

$$|S + A| \le |S + X| + |S + (A \setminus X)| \le \frac{s}{m-t} - \frac{s}{m} + (r-t)\frac{s}{(m-t)^2} + \tag{4.9}$$

$$+|S|\,((m-t) - (r-t)) = 2\sqrt{s|S|} - s/m \le 2\sqrt{s|S|}.$$

This inequality is nearly the required one, except for the factor of 2. We can dispose of this factor as follows. Consider the sets $A' = A^k$, $B_1' = B_1^k$, $B_2' = B_2^k$ and $S' = S^k$ in the $k$'th direct power of the original group. Applying equation (4.9) to $A'$, etc., we obtain

$$|S' + A'| \le 2\sqrt{s'|S'|}. \tag{4.10}$$

Since $|S' + A'| = |S + A|^k$, $s' = s^k$ and $|S'| = |S|^k$, we get

$$|S + A| \le 2^{1/k}\sqrt{s|S|}. \tag{4.11}$$

Taking the limit as $k \to \infty$ we obtain the desired inequality

$$|S + A| \le \sqrt{s|S|}. \tag{4.12}$$

□

**Acknowledgement.** The authors are grateful to Vsevolod Lev for several relevant comments quoted in the paper, and to Katalin Marton for discussions on entropy connection and for directing our attention to some relevant sources.

## References


1. N. Alon, *Problems and results in extremal combinatorics I.*, Discrete Math. **273** (2003), 31–53.
2. B. Bollobás and A. Thomason, *Projections of bodies and hereditary properties of hypergraphs*, Bull. London Math. Soc. **27** (1995), 417–424.
3. F. R. K. Chung, R. L. Graham, P. Frankl, and J. B. Shearer, *Some intersection theorems for ordered sets and graphs*, J. Combin. Theory Ser. A **43** (1986), 23–37.
4. T. M. Cover and J. A. Thomas, *Elements of information theory*, Wiley, New York – Chichester etc., 1991.
5. K. Gyarmati, S. Konyagin, and I. Z. Ruzsa, *Double and triple sums modulo a prime*, CRM Workshop on combinatorial number theory, to appear.
6. T. S. Han, *Nonnegative entropy measures of multivariate symmetric correlations*, Inform. Contr. **36** (1978), 133–156.
7. V. F. Lev, *Structure theorem for multiple addition and the Frobenius problem*, J. Number Theory **58** (1996), 79–88.
8. J. L. Malouf, *On a theorem of Plünnecke concerning the sum of a basis and a set of positive density*, J. Number Theory **54**.
9. M. B. Nathanson, *Additive number theory: Inverse problems and the geometry of sumsets*, Springer, 1996.
10. H. Plünnecke, *Eine zahlentheoretische anwendung der graphtheorie*, J. Reine Angew. Math. **243** (1970), 171–183.
11. I. Z. Ruzsa, *Cardinality questions about sumsets*, Montréal school on combinatorial number theory, to appear.
12. ———, *An application of graph theory to additive number theory*, Scientia, Ser. A **3** (1989), 97–109.
13. ———, *Addendum to: An application of graph theory to additive number theory*, Scientia, Ser. A **4** (1990/91), 93–94.
14. T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge University Press, Cambridge, 2006.



Alfréd Rényi Institute of Mathematics, Budapest, Pf. 127, H-1364 Hungary
*E-mail address*: gykati@cs.elte.hu

Alfréd Rényi Institute of Mathematics, Budapest, Pf. 127, H-1364 Hungary
*E-mail address*: matomate@renyi.hu

Alfréd Rényi Institute of Mathematics, Budapest, Pf. 127, H-1364 Hungary
*E-mail address*: ruzsa@renyi.hu
*E-mail address*: To all authors: triola@renyi.hu