ANNALES UNIV. SCI. BUDAPEST., **59** (2016), 133–138

CONNECTIONS BETWEEN THE CARDINALITY OF SUMSETS AND DIFFERENCE SETS NEAR THE EXTREME

By
MÁRTON HORVÁTH AND IMRE Z. RUZSA
(Received January 13, 2017)

Abstract. We study connections between the cardinality of the sets $A + A$ and $A - A$, where A is a finite set in a commutative group and one of them is near to the maximal possible value. We improve earlier results of the second author [1].

1. Introduction

Let A be a finite nonempty set in a commutative group, and set $n = |A|$. The cardinality of the difference set $A - A$ is at most $n^2 - n + 1$ as the trivial differences $a - a$ all gives 0. By the commutativity of the group, we have $|A+A| \leq n(n+1)/2$. The second author [1] proved some estimates to express the phenomenon that if one of these quantities is near to the maximal possible value, then the other cannot be very small. Results of this kind are conveniently expressed in terms of the difference deficit and sum deficit introduced in [1]

$$\Delta_-(A) = n^2 - n + 1 - |A - A|,$$
$$\Delta_+(A) = \frac{n(n+1)}{2} - |A + A|.$$

The aim of this note is to improve certain estimates of [1].

Second author was supported by ERC–AdG Grant No.321104 and Hungarian National Foundation for Scientific Research (OTKA), Grants No.109789, and NK104183.

2. Differences near the maximum

The second author proved the following result in [1].

THEOREM 1. *Let A be a finite set in a commutative group, $|A| = n$. We have*

$$|A+A|\left(\Delta_-(A)^2 + \frac{n^3}{6}\right) \geq \frac{n^5}{20}.$$

In particular, if $|A+A| < n^2/10$, then

$$|A+A|\Delta_-(A)^2 \geq \frac{n^5}{30}.$$

The above theorem provides no information if $|A+A| > 0.3n^2$. Our first result extends this for the whole range up to $n^2/2$.

THEOREM 2. *We have*

$$|A+A|\Delta_-(A)^2 \geq \left(\frac{n}{2} - \frac{|A+A|}{n}\right)^4 \left(\frac{n}{2} + \frac{|A+A|}{n}\right).$$

If $|A+A| < cn^2$ for some constant $c < \frac{1}{2}$, then $|A+A|\Delta_-(A)^2 > c'n^5$ with

$$c' = \frac{(1-2c)^4(1+2c)}{32}.$$

PROOF. For a positive integer k, define the function f_k as

$$f_k(n) = \min\{\Delta_-(A) \colon |A+A| \leq k, |A| = n\}$$

for $1 \leq n \leq k$. Firstly, we study this function. Let A be a finite set such that $|A+A| \leq k, |A| = n$, and $\Delta_-(A)$ is minimal under these conditions, so $\Delta_-(A) = f_k(n)$.

Denote by $r(x)$ the number of representations of any element x as a sum from A, i.e.,

$$r(x) = |\{(a_1, a_2) \colon a_1, a_2 \in A, a_1 + a_2 = x\}|.$$

Obviously,

$$\sum_x r(x) = n^2. \tag{1}$$

We define a similar function as

$$q(x) = |\{(a_1, a_2, a_3) \colon a_1, a_2, a_3 \in A, a_1 + a_2 - a_3 = x\}|.$$

Counting the number of the quadruples (a_1, a_2, a_3, a_4) such that $a_1+a_2 = a_3+a_4$ in different ways, we have

$$\sum_x r^2(x) = \sum_{a\in A} q(a). \tag{2}$$

The inequality of arithmetic and quadratic means gives that

$$\sum_{a\in A} q(a) = \sum_x r^2(x) \geq \frac{(\sum_x r(x))^2}{|A+A|} \geq \frac{n^4}{k},$$

from which we conclude that there is an $a \in A$ such that $q(a) \geq \frac{n^3}{k}$. This means that there are at least $\frac{n^3}{k}$ triples (a_1, a_2, a_3) such that $a = a_1 + a_2 - a_3$.

Our goal is to give a lower bound to the increment of the difference deficit when we consider A instead of $A' = A \setminus \{a\}$. This increment is the number of "new" pairs (a_1, a_2) (that is, $a_1 = a$ or $a_2 = a$) which do not give a new difference.

We can write these differences in two different forms with an element $\tilde{a} \in A'$. The first ones are in the form $\tilde{a} - a$, when this difference is contained by the set $A' - A'$. The second ones are the differences $a - \tilde{a} \in A' - A$ (note the slight difference: elements of $A' - a$ are now old, counted in the first form). For our estimate, we count only the differences in the second form.

If $a = a_1 + a_2 - a_3$, where $a_1 \neq a$ and $a_2 \neq a$, then the differences $a - a_1 = a_2 - a_3$ and $a - a_2 = a_1 - a_3$ are in the set $A' - A$. Ruling out the cases when a is equal to a_1 or a_2, at least $n^3/k - 2n$ triples remain. Hence the number of elements that appear as a_1 or a_2 is at least $\sqrt{n^3/k - 2n}$. This gives that

$$\Delta_-(A) - \Delta_-(A \setminus \{a\}) \geq \sqrt{\frac{n^3}{k} - 2n},$$

which implies

$$f_k(n) - f_k(n-1) \geq \sqrt{\frac{n^3}{k} - 2n} = \sqrt{\frac{n}{k}}\sqrt{n^2 - 2k}. \tag{3}$$

The latter form shows that our bound is an increasing function of n.

A repeated application of this inequality gives

$$\begin{aligned} f_k(n) \geq f_k(n) - f_k(n-t-1) &\geq \sum_{i=0}^{t} \sqrt{\frac{n-i}{k}}\sqrt{(n-i)^2 - 2k} \\ &\geq (t+1)\sqrt{\frac{n-t}{k}}\sqrt{(n-t)^2 - 2k} \end{aligned}$$

for $t < n - \sqrt{2k}$.

We put

$$t = \left\lfloor \frac{n}{2} - \frac{k}{n} \right\rfloor .$$

With this choice

$$n - t \ge \frac{n}{2} + \frac{k}{n}, \ (n-t)^2 - 2k \ge \left(\frac{n}{2} - \frac{k}{n}\right)^2,$$

hence

$$f_k(n) \ge \left(\frac{n}{2} - \frac{k}{n}\right)^2 \left(\frac{n}{2} + \frac{k}{n}\right)^{1/2} k^{-1/2}.$$

By squaring, multiplying by k and putting $k = |A + A|$ we get the claim of the theorem. ∎

The constant $1/32$ could be reduced by a more careful calculation.

3. Sums near the maximum

In [1] it is shown that

$$|A - A|\Delta_+(A)^2 > n^4/9 \tag{4}$$

assuming $|A - A| < n^2/2$, and it is conjectured that the lower bound can be improved to cn^5. We prove an estimate which improves (4), though it is not as strong as the conjectured one.

THEOREM 3. *We have*

$$|A - A|\Delta_+(A) > \frac{(n - \sqrt{2|A-A|})^2 (n + 2\sqrt{2|A-A|})}{3}.$$

If $|A - A| < cn^2$ *for some constant* $c < \frac{1}{2}$, *then* $|A - A|\Delta_+(A) > c'n^3$ *with*

$$c' = \frac{(1 - \sqrt{2c})^2 (1 + 2\sqrt{2c})}{3}.$$

This bound has a different form; the bound we get for Δ_+ behaves like (4) when $|A - A|$ is of order n^2, and like the conjectural improvement when $|A - A| = O(n)$.

PROOF. We proceed similarly to the previous proof. We introduce

$$g_k(n) = \min\{\Delta_+(A) \colon |A - A| \le k, \ |A| = n\}$$

for $1 \le n \le k$.

Instead of the function r we consider the difference-counting function

$$d(x) = |\{(a_1, a_2) \colon a_1, a_2 \in A, a_1 - a_2 = x\}|.$$

The analogs of the equations (1), (2) are true for the function d, i.e.,

$$\sum_x d(x) = n^2, \qquad \sum_x d^2(x) = \sum_{a \in A} q(a).$$

As in the previous proof, we apply the inequality of arithmetic and quadratic means to get

$$\sum_{a \in A} q(a) = \sum_x d^2(x) \geq \frac{(\sum_x d(x))^2}{|A - A|} \geq \frac{n^4}{k},$$

so there is an $a \in A$ such that $q(a) \geq \frac{n^3}{k}$.

If $a = a_1 + a_2 - a_3$, then $a + a_3 = a_1 + a_2$, so the sum $a + a_3$ is not a new sum in $A + A$ compared to $A' + A'$ except in the trivial cases when $a = a_1$ or $a = a_2$. For an element a_3, there might be at most n distinct pairs (a_1, a_2) which implies

$$g_k(n) - g_k(n-1) \geq \Delta_+(A) - \Delta_+(A') \geq \frac{\frac{n^3}{k} - 2n}{n} = \frac{n^2}{k} - 2.$$

(Observe that this is weaker than (3); we could obtain the conjectured bound if we had a similar estimate here.)

A repeated application of this inequality gives

$$g_k(n) \geq g_k(n) - g_k(n-t-1) \geq \sum_{i=0}^{t} \left(\frac{(n-i)^2}{k} - 2 \right).$$

The best choice is $t = \left\lfloor n - \sqrt{2k} \right\rfloor$. As the function is decreasing, we can estimate the sum by an integral to conclude

$$g_k(n) > \int_0^{n-\sqrt{2k}} \left(\frac{(n-x)^2}{k} - 2 \right) dx = \frac{(n - \sqrt{2k})^2 (n + 2\sqrt{2k})}{3k}.$$

By multiplying by k and putting $k = |A - A|$ we get the claim of the theorem. ∎

In Theorem 2, $n^2/2$ was a natural boundary, while here it is not. However, the situation for $|A - A| > n^2/2$ is already satisfactorily described in [1] in the form

$$\Delta_-(A) \leq 2(\Delta_+(A)^2 + \Delta_+(A)),$$

with examples of equality.

References

[1] IMRE Z. RUZSA, Many differences, few sums, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.*, **51** (2008), 27–38.

Márton Horváth
Budapest University
of Technology and Economics
Budapest, Hungary
horvathm@math.bme.hu

Imre Z. Ruzsa
Alfréd Rényi Institute of Mathematics
Budapest, Hungary
ruzsa@renyi.hu