François Hennecart
Gilles Robert
Alexander Yudin

On the number of sums and differences

Astérisque, tome 258 (1999), p. 173-178
<http://www.numdam.org/item?id=AST_1999__258__173_0>

Astérisque **258**, 1999, p. 173–178

ON THE NUMBER OF SUMS AND DIFFERENCES

by

François Hennecart, Gilles Robert & Alexander Yudin

Abstract. — It is proved that $\inf_{A\subset\mathbb{Z}} \ln|A+A|/\ln|A-A|$ is less than .7865, improving a previous result due to G. Freiman and W. Pigarev.

1. Introduction

Let A be a set of integers. Write

$$\begin{aligned} \mathbf{2}A = A + A &:= \{x + y \mid x, y \in A\} \\ \mathbf{D}A = A - A &:= \{x - y \mid x, y \in A\}, \end{aligned}$$

and

$$\alpha(A) = \frac{\ln|\mathbf{2}A|}{\ln|\mathbf{D}A|}.$$

If $|A| = n$, then we have

$$\begin{aligned} 2n - 1 &\leq |\mathbf{2}A| \leq \frac{n^2 + n}{2} \\ 2n - 1 &\leq |\mathbf{D}A| \leq n^2 - n + 1, \end{aligned}$$

where equality on the left side occurs for arithmetical progressions, and on the right side for "generic" sets, in which there is no nontrivial coincidence between sums and differences. Denote for any $n \geq 1$

$$\alpha_n = \inf_{A\subset N, |A|=n} \frac{\ln|\mathbf{2}A|}{\ln|\mathbf{D}A|}.$$

The lower bound $\alpha_n \geq 3/4$ follows from the inequality (see Freiman and Pigarev [1] or Ruzsa [6])

$$|\mathbf{D}A|^{3/4} \leq |\mathbf{2}A|. \tag{1}$$

1991 ***Mathematics Subject Classification.*** — 11P99, 11B75, 05B10.

Key words and phrases. — Additive number theory, combinatorial number theory, difference sets, sumsets.

In fact, Ruzsa proved a sharper result, namely

$$|A| \cdot |\mathbf{D}A| \leq |\mathbf{2}A|^2. \tag{2}$$

By squaring (2) and using $|\mathbf{D}A| \leq |A|^2$, we obtain (1).

Conversely, Freiman and Pigarev have shown that

$$\liminf_{n \to +\infty} \alpha_n < 0.89. \tag{3}$$

Here we shall improve this result by showing

Theorem. — *The sequence $(\alpha_n)_{n\geq 1}$ converges to $\alpha := \inf_A \alpha(A)$ and we have*

$$3/4 \leq \alpha \leq \ln 2/\ln(1+\sqrt{2}) < .7865.$$

Let us notice that inequality (2) implies that there is no set A such that $\alpha(A) = 3/4$. Furthermore a set A such that $\alpha(A) \leq 3/4 + \epsilon$, where $\epsilon > 0$, satisfies $|\mathbf{D}A| \geq |\mathbf{2}A|^{4/3-2\epsilon}$, and then again from (2) we deduce $|A|^{3/2} \geq |\mathbf{2}A| \geq |A|^{3/2-5\epsilon}$ and $|A|^2 \geq |\mathbf{D}A| \geq |A|^{2-10\epsilon}$.

This shows that if the value of α is 3/4, then there exists a set A with arbitrary large cardinality, which is almost a generic set to insure that $\ln|\mathbf{D}A|$ is close to $2\ln|A|$, even when in the same time $\ln|\mathbf{2}A|$, which should be close to $1.5\ln|A|$, does not at all correspond to a generic set A. In [5], Ruzsa was interested by such sets, and proved that there exist $c > 0$ and arbitrary large sets A such that $|\mathbf{D}A| = |A|^2(1+o(1))$ and $|\mathbf{2}A| \leq |A|^{2-c}$.

2. The convergence of α_n

In this section, we study the convergence of α_n.

In the table below, we give the value of α_n for small n: to compute them, we have looked for all the sequences $s = (s_k)_{k\in\mathbb{Z}}$ and $d = (d_k)_{k\in\mathbb{Z}}$ of nonnegative integers such that

$$\sum_{k\in\mathbb{Z}} s_k = n^2, \quad \sum_{k\in\mathbb{Z}} d_k = n^2 \quad \text{and} \quad \sum_{k\in\mathbb{Z}} s_k^2 = \sum_{k\in\mathbb{Z}} d_k^2. \tag{4}$$

For a finite set of integers A with $|A| = n$, these three conditions are satisfied by the sequences $(s_k(A))_{k\in\mathbb{Z}}$ and $(d_k(A))_{k\in\mathbb{Z}}$ where $s_k(A)$ (resp. $d_k(A)$) is the number of representations of k as a sum (resp. a difference) of two elements of A. For any pairs of solutions $s = (s_k)$ and $d = (d_k)$ of (4), we denote by N_s (resp. N_d) the number of integers k such that $s_k \neq 0$ (resp. $d_k \neq 0$).

From the inclusion

$$\{\alpha(A) \ : \ |A| = n\} \subset E_n = \{\ln N_s/\ln N_d \ : \ (s,d) \text{ solution of } (4)\},$$

we obtain α_n by exhibiting a set A of cardinality n which achieves the minimum of the finite set E_n.

For $1 \leq n \leq 7$, the infimum of $\alpha(A)$ is reached for set A for which both $|\mathbf{2}A|$ and $|\mathbf{D}A|$ are maximal. It is no more the case when $n = 8$.

n	1	2	3	4	5	6	7
α_n	1	1	.9208	.8977	.8895	.8866	.8859

Observe that α_n seems to be decreasing. In fact we are only able to prove that α_n has a limit when n tends to infinity.

The definition of $\alpha(A)$ still has a sense if $A \subset \mathbb{Z}^m$, and even if A is a subset of a lattice Λ generated by a basis $\{\omega_j\}_{1\leq j\leq m}$ in $\mathbb{R}^m$. Now we map A into $\mathbb{Z}$ by

$$x_1\omega_1 + \cdots + x_m\omega_m \longmapsto x_1 + qx_2 + \cdots + q^{m-1}x_m.$$

If q is sufficiently large, then this mapping conserves the number of sums and differences of our set. Thus we have

$$\alpha_n = \inf\left\{ \frac{\ln|\mathbf{2}A|}{\ln|\mathbf{D}A|} \ : \ A \subset \Lambda \text{ lattice in } \mathbb{R}^m \text{ for some } m \text{ and } |A| = n \right\}.$$

For any set A of integers, and any $k \geq 1$, we denote by A^k the cartesian product

$$A^k = \{(a_1, \ldots, a_k) \ : \ a_j \in A\}.$$

This set satisfies

$$\begin{aligned} |\mathbf{2}A^k| &= |\mathbf{2}A|^k \\ |\mathbf{D}A^k| &= |\mathbf{D}A|^k, \end{aligned}$$

whence

(5) $$\alpha(A^k) = \alpha(A).$$

We are now in position to prove that (α_n) converges.

Let $\varepsilon > 0$. There exist an integer n and a set A with $|A| = n$ such that

(6) $$\alpha < \alpha(A) < \alpha + \varepsilon/2.$$

Let q be an integer. We can write $n^k \leq q < n^{k+1}$ for some integer k. We define B_q as being any subset of A^{k+1} of cardinality q, and containing $A^k \times \{a\}$ for some a in A. This is possible because $|B_q| \geq |A^k| = n^k$. Then we have

$$A^k \times \{a\} - A^k \times \{a\} \subset B_q - B_q,$$

and

$$B_q + B_q \subset A^{k+1} + A^{k+1},$$

whence by (5)

$$\alpha(B_q) - \alpha(A) \leq \frac{\alpha(A)}{k}.$$

In view of (6) and using $\alpha_q \geq \alpha$, we obtain that for any sufficiently large q,

$$|\alpha_q - \alpha| < \varepsilon.$$

Thus α_q converges to α.

3. The upper bound

From the previous section, we deduce that $\alpha \leq \alpha(A)$ for any set A. To show the upper bound in the theorem, we shall construct a sequence of finite sets A_ℓ of integers such that $\lim_{\ell\to+\infty}\alpha(A_\ell) = \ln 2/\ln(1+\sqrt{2})$.

Analyzing the proof in [1] of the upper bound (3), we see that as a set with comparatively small number of sums and large number of differences, an isomorphic (in the sense of G. Freiman [2]) image of vertices of a simplex in $\mathbb{R}^6$ was taken. It corresponds to the result of C.A. Rogers and G.G. Shephard [3], that for each convex set K of $\mathbb{R}^m$ we have

$$\text{mes}(\mathbf{D}K) \leq \binom{2m}{m}\text{mes}(K) \tag{7}$$

The equality in (7) is achieved only in the case when K is a simplex. Therefore, in order to get an estimate for α, it is natural to take a set of points of some lattice in a simplex.

Let $\{e_1, \ldots, e_m\}$ be an orthonormal basis of $\mathbb{R}^m$ and let Λ be the lattice it generates. Let $A(m, L)$ be the subset of Λ, consisting in points $x = (x_1, \ldots, x_m)$, such that $\forall j$, $x_j \geq 0$ and $\sum_{j=1}^{m} x_j \leq L$, where $L \in \mathbb{Z}^+$.
In addition, let $\text{Sim}(m,L) = \text{card}\, A(m,L)$, i.e., $\text{Sim}(m,L)$ is a number of points of the lattice Λ in a rectilinear closed simplex with an edge of length L.
We shall use two lemmas.

Lemma 1. — *We have*

$$\text{Sim}(m,L) = \binom{m+L}{L}.$$

This result is standard and its proof is left to the reader.

Lemma 2. — *We have*

$$|\mathbf{D}A(m,L)| = \sum_{k=0}^{\min(m,L)}\binom{m}{k}\binom{L}{k}\binom{L+m-k}{m-k} = \sum_{k=0}^{\min(m,L)}\binom{m}{k}^2\binom{L+m-k}{m}.$$

Proof. — For any set of integers $P \subset \{1, 2\ldots, m\}$, we define the sets $\mathcal{S}_>(P, L)$

$$= \{\ (x_1, \ldots, x_m) \in \mathbb{Z}^m\ :\ x_j > 0 \text{ for } j \in P,\ x_j = 0 \text{ if } j \notin P \text{ and } \sum_{j\in P} x_j \leq L\ \},$$

and $\mathcal{S}_\leq(P, L)$

$$= \{\ (x_1, \ldots, x_m) \in Z^m\ :\ x_j \leq 0 \text{ for } j \in P,\ x_j = 0 \text{ if } j \notin P \text{ and } \sum_{j\in P} x_j \geq -L\ \}.$$

If we denote by $\overline{P}$ the complementary set of P in $\{1, 2, \ldots, m\}$, then we have the following decomposition into disjoint sets

$$\mathbf{D}A(m,l) = \bigcup_{P\subset\{1,\ldots,m\}} \mathcal{S}_>(P,L) \oplus \mathcal{S}_\leq(\overline{P}, L).$$