Available online at www.sciencedirect.com
SCIENCE @ DIRECT®
ELSEVIER
C. R. Acad. Sci. Paris, Ser. I 337 (2003) 499–503
COMPTES RENDUS MATHEMATIQUE

Combinatorics/Number Theory

On multiple sum and product sets of finite sets of integers

Jean Bourgain [a], Mei-Chu Chang [b]

[a] *Institute for Advanced Study, Olden Lane, Princeton, NJ 08540, USA*
[b] *Mathematics Department, University of California, Riverside, CA 92521, USA*

Received 11 August 2003; accepted 30 August 2003

Presented by Jean Bourgain

Abstract

Let $A \subset \mathbb{Z}$ be a finite set of integers of cardinality $|A| = N \geqslant 2$. Given a positive integer k, denote kA (resp. $A^{(k)}$) the set of all sums (resp. products) of k elements of A. We prove that for all $b > 1$, there exists $k = k(b)$ such that $\max(|kA|, |A^{(k)}|) > N^b$. This answers affirmably questions raised in Erdős and Szemerédi (Stud. Pure Math., 1983, pp. 213–218), Elekes et al. (J. Number Theory 83 (2) (2002) 194–201) and recently, by S. Konjagin (private communication). The method is based on harmonic analysis techniques in the spirit of Chang (Ann. Math. 157 (2003) 939–957) and combinatorics on graphs. ***To cite this article: J. Bourgain, M.-C. Chang, C. R. Acad. Sci. Paris, Ser. I 337 (2003).***

Résumé

Sur les ensembles de sommes et produits multiples d'ensembles finis d'entiers. Soit $A \subset \mathbb{Z}$ un ensemble fini d'entiers et $|A| = N \geqslant 2$. Pour tout entier positif k, denotons kA (resp. $A^{(k)}$) l'ensemble de toutes les sommes (resp. produits) de k éléments de A. On démontre que pour tout $b > 1$, il existe $k = k(b)$ tel que $\max(|kA|, |A^{(k)}|) > N^b$. Ceci répond affirmativement à des questions posées dans Erdős et Szemerédi (Stud. Pure Math., 1983, pp. 213–218), Elekes et al. (J. Number Theory 83 (2) (2002) 194–201) et, récemment, par S. Konjagin (communication privée). La méthode est basée sur des arguments d'analyse harmonique dans l'esprit de Chang (Ann. Math. 157 (2003) 939–957) et de la combinatoire sur des graphes. ***Pour citer cet article : J. Bourgain, M.-C. Chang, C. R. Acad. Sci. Paris, Ser. I 337 (2003).***

1. Preliminaries and statement of the result

For a finite subset of integers $A \subset \mathbb{Z}$, denote

$$kA = \underbrace{A + \cdots + A}_{k}, \quad \text{the } k\text{-fold sumset}$$

and

$$A^{(k)} = \underbrace{A \times \cdots \times A}_{k}, \quad \text{the } k\text{-fold product set.}$$

E-mail addresses: bourgain@math.ias.edu (J. Bourgain), mcc@math.ucr.edu (M.-C. Chang).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2003.08.010

A number of results and problems going back to the seminal paper of Erdös and Szemerédi [4] express the fact that kA and $A^{(k)}$ cannot be both 'small'. More precisely, it is conjectured in [4] that for all $k \in \mathbb{Z}_+$ and $\varepsilon > 0$

$$|kA| + \left|A^{(k)}\right| > c(k,\varepsilon)|A|^{k-\varepsilon}. \tag{1}$$

This problem is still open, even for $k = 2$. In the case $k = 2$, the best results obtained so far are based on geometric combinatorics such as the Szemerédi–Trotter theorem (this approach works equally well for sets of real numbers). The record to date is due to Solymosi [8]

$$|2A| \cdot \left|A^{(2)}\right| > c(\varepsilon)|A|^{14/11-\varepsilon}. \tag{2}$$

Also based on the Szemerédi–Trotter theorem, it was shown in [3] that for general $k \in \mathbb{Z}_+$

$$|kA| \cdot \left|A^{(k)}\right| > c|A|^{3-2^{1-k}}. \tag{3}$$

In view of conjecture (1) and the lower bound (3), it is natural to explore first the issue whether

$$\inf_{A\subset\mathbb{Z},\ |A|\geqslant 2} \frac{\log(|kA| + |A^{(k)}|)}{\log|A|} \to \infty, \quad k \to \infty. \tag{4}$$

This problem was formulated in [3] and also, more recently by Konjagin [5] (motivated by issues concerning exponential sums). Our main result is an affirmative answer.

Theorem 1.1. *For all $b > 1$ there is $k \in \mathbb{Z}_+$ and that if $A \subset \mathbb{Z}$ is an arbitrary finite set, with $|A| = N \geqslant 2$, then*

$$|kA| + \left|A^{(k)}\right| > N^b. \tag{5}$$

Remark 1. (i) Our argument gives some explicit lower bound on how large k has to be (it involves exponential dependence on b), but we made no attempt here to optimize the result (of course, if (1) is true, we may take in (5) any $k \in \mathbb{Z}_+,\ k > b$, provided N is sufficiently larger).

(ii) At this point, we do not have the analogue of the theorem for sets $A \subset \mathbb{R}$ of real numbers. As in [2], our approach makes essential use of prime factorization.

2. Brief description of the argument

The proof uses several ingredients of combinatorial and analytical nature. In particular, we do rely on Freiman's lemma and Gowers' improved version of the Balog–Szemerédi theorem, the basic harmonic analysis inequality from [2] and finally, the 'induction on scales' argument from [1] to bootstrap the estimates. The general strategy of our proof bears resemblance to [2] in the sense that we assume $|A^{(k)}|$ 'small' and prove that then $|kA|$ has to be large. However, 'smallness' of $|A \cdot A|$ in [2] is the assumption

$$|A \cdot A| < K|A| \tag{6}$$

with K a constant (a condition much too restrictive for our purpose).

If (6) holds, it is shown in [2] that

$$|A + A| > c(K)|A|^2 \tag{7}$$

and more generally

$$|hA| > c(K,h)|A|^h. \tag{8}$$

Let us briefly recall the approach.

Consider the map given by prime factorization

$$\mathbb{Z}_+ \longrightarrow \mathcal{R} = \prod_p \mathbb{Z}_{\geqslant 0},$$
$$n = \prod_p p^{\alpha_p} \longrightarrow \alpha = (\alpha_p)_p,$$

where p runs in the set $\mathcal{P}$ of primes.

The set A is mapped to $\mathcal{A} \subset \mathcal{R}$ satisfying by (6)

$$|2\mathcal{A}| < K|\mathcal{A}|. \tag{9}$$

Freiman's lemma implies then that $\dim \mathcal{A} < K$ (where 'dim' refers to the smallest vector space containing $\mathcal{A}$). Hence there is a subset $I \subset \mathcal{P}$, $|I| < K$, such that the restriction π_I is one-to-one restricted to $\mathcal{A}$. Harmonic analysis implies then that

$$\lambda_q(A) < (Cq)^K \tag{10}$$

for an absolute constant C, and for all $q > 2$. By $\lambda_q(A)$, we mean the Λ_q-constant of the finite set $A \subset \mathbb{Z}$, defined by

$$\lambda_q(A) = \max \left\| \sum_{n \in A} c_n \, \mathrm{e}^{2\pi \mathrm{i} n\theta} \right\|_{L^q(\mathbb{T})}, \tag{11}$$

where $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ and the max is taken over all sequences $(c_n)_{n \in A}$ with $(\sum c_n^2)^{1/2} \leqslant 1$. See [7] for more details.

Eq. (10) results from the following more general inequality that will also be crucial here (see [2]):

Proposition 2.1. *Let $p_1, \ldots, p_k$ be distinct primes and associate to each $\alpha = (\alpha_1, \ldots, \alpha_k) \in (\mathbb{Z}_{\geqslant 0})^k$ a trigonometric polynomial F_α on $\mathbb{T}$ such that*

$$(n, p) = 1, \quad \text{for all } n \in \operatorname{supp} \widehat{F_\alpha}, \text{ and for all } p \in \mathcal{P}_0.$$

Then, for any moment $q \geqslant 2$

$$\left\| \sum_\alpha F_\alpha\big(p_1^{\alpha_1} \cdots p_k^{\alpha_k} \theta\big) \right\|_q < (Cq)^k \Big(\sum \|F_\alpha\|_q^2 \Big)^{1/2}. \tag{12}$$

Thus (10) follows from (12) taking $F_\alpha(\theta) = \mathrm{e}^{2\pi \mathrm{i}\theta}$ and $\{p_1, \ldots, p_k\} = I \subset \mathcal{P}$.

Denoting for $h \geqslant 2$

$$r_h(n; A) = \big|\big\{(x_1, \ldots, x_h) \in A^h \,|\, n = x_1 + \cdots + x_h\big\}\big|.$$

A simple application of Parseval's identity gives

$$\sum_{n \in hA} r_h(n; A)^2 \leqslant \lambda_{2h}(A)^{2h} \cdot |A|^h$$

and using Cauchy–Schwartz inequality on $\sum_{n \in hA} r_h(n; A)$, it follows that

$$|hA| \geqslant \frac{|A|^h}{\lambda_{2h}(A)^{2h}}. \tag{13}$$

Thus we obtain (8) with

$$c(K, h) > (Ch)^{-2hK}. \tag{14}$$

Obviously, this statement has no interest unless $K \ll \log|A|$.

The main point in what follows is to be able to carry some of the preceding analysis under a much weaker assumption $K < |A|^{\varepsilon}$, ε small. We will prove the following statement:

Proposition 2.2. *Given $\gamma > 0$ and $q > 2$, there is a constant $\Lambda = \Lambda(\gamma, q)$ such that if $A \subset \mathbb{Z}$ is a finite set, $|A| = N$, $|A \cdot A| < KN$, then*

$$\lambda_q(A) < K^{\Lambda} N^{\gamma}. \tag{15}$$

Thus fixing q, Proposition 2.2 provides already nontrivial information assuming $K < N^{\delta}$, with $\delta > 0$ sufficiently small.

Assuming Proposition 2.2, let us derive the theorem. We may assume that $A \subset \mathbb{Z}_+$ to simplify the situation.

Fix b and assume (5) fails for some large $k = 2^{\ell}$ (to be specified). Hence, passing to $\mathcal{A}$

$$|k\mathcal{A}| < N^b,$$

$$\frac{|2^{\ell}\mathcal{A}|}{|2^{\ell-1}\mathcal{A}|} \frac{|2^{\ell-1}\mathcal{A}|}{|2^{\ell-2}\mathcal{A}|} \cdots \frac{|2\mathcal{A}|}{|\mathcal{A}|} < N^{b-1} \tag{16}$$

and we may find $k_0 = 2^{\ell_0}$ such that

$$\frac{|2k_0\mathcal{A}|}{|k_0\mathcal{A}|} < N^{(b-1)/\ell}. \tag{17}$$

Denote $\mathcal{B} = k_0\mathcal{A} \subset \mathcal{R}$ and $B = A^{(k_0)}$, the corresponding subset of $\mathbb{Z}_+$. Thus by (17)

$$|B \cdot B| < N^{(b-1)/\ell}|B|. \tag{18}$$

Apply Proposition 2.2 to the set B, $|B| \equiv N_0$, $K = N^{(b-1)/\ell}$ with τ, γ specified later.

Hence from (15)

$$\lambda_q(A) \leqslant \lambda_q(B) < N^{((b-1)/\ell)\Lambda} N_0^{\gamma} < N^{(b-1)/\ell\Lambda + b\gamma}. \tag{19}$$

Taking $q = 2h$, (13) and (19) imply

$$|hA| > N^{(1-2((b-1)/\ell)\Lambda - 2b\gamma)h}. \tag{20}$$

Take $h = 2b < k$, $\gamma = \frac{1}{100b}$. Recall that $\Lambda = \Lambda(\gamma, q)$, hence $\Lambda = \Lambda(b)$. Take $\ell = 100b\Lambda(b)$, so that $k = 2^{\ell} \equiv k(b)$. Inequality (20) then clearly implies that

$$|kA| > N^b.$$

This proves the theorem.

Returning to Proposition 2.2, it will suffice to prove the following weaker version

Proposition 2.3. *Given $\gamma > 0$, $\tau > 0$ and $q > 2$, and A as in Proposition 2.2, there is a subset $A' \subset A$ satisfying*

$$|A'| > N^{1-\tau}, \tag{21}$$

$$\lambda_q(A') < K^{\Lambda} N^{\gamma}, \tag{22}$$

where $\Lambda = \Lambda(\tau, \gamma, q)$.

3. Proof of Proposition 2.2 assuming Proposition 2.3

Denoting χ the indicator function, one has obviously

$$\sum_{z \in A/A'} \chi_{zA'} \geqslant |A'|\, \chi_A. \tag{23}$$

Let A' be the subset obtained in Proposition 2.3. Then (23) is easily seen to imply

$$|A'|\lambda_q(A) \leqslant \sum_{z\in A/A'} \lambda_q(zA') = \left|\frac{A}{A'}\right|\lambda_q(A') \leqslant \left|\frac{A}{A}\right| K^{\Lambda} N^{\gamma}. \tag{24}$$

If $\mathcal{A} \subset \mathcal{R}$ is the set introduced before, application of Ruzsa's inequality on sum-difference sets [6] gives

$$\left|\frac{A}{A}\right| = |\mathcal{A} - \mathcal{A}| \leqslant K^2|\mathcal{A}| = K^2 N. \tag{25}$$

Thus, by (21), (24) and (25), we have

$$\lambda_q(A) \leqslant K^{\Lambda+2} N^{\tau+\gamma}, \tag{26}$$

where $\Lambda = \Lambda(\tau, \gamma, q)$. Replacing γ by $\frac{\gamma}{2}$ and $\tau = \frac{\gamma}{2}$, (15) follows.

Proposition 2.2 is derived from more technical statements involving graphs.

References

[1] J. Bourgain, On the Erdős–Volkmann and Katz–Tao Ring Conjectures, Geom. Funct. Anal. 13 (2003).
[2] M. Chang, The Erdős–Szemerédi problem on sum set and product set, Ann. of Math. 157 (2003) 939–957.
[3] G. Elekes, M. Nathanson, I. Ruzsa, Convexity and sumsets, J. Number Theory 83 (2) (2000) 194–201.
[4] P. Erdős, E. Szemerédi, On Sums and Products of Integers, in: Stud. Pure Math., Birkhäuser, Basel, 1983, pp. 213–218.
[5] S. Konjagin, Private communication.
[6] M.B. Nathanson, Additive Number Theory, Inverse Problems and the Geometry of Sumsets, in: Graduate Text in Math., Vol. 165, Springer-Verlag, New York, 1996.
[7] W. Rudin, Trigonometric series with gaps, J. Math. Mech. 9 (1960) 203–227.
[8] J. Solymosi, On the number of sums and products, Preprint, 2003.