Combinatorics, Probability and Computing (2011) 20, 793–798. © Cambridge University Press 2011
doi:10.1017/S0963548311000277

On Sumsets of Convex Sets

TOMASZ SCHOEN[1†] and ILYA D. SHKREDOV[2‡]

[1]Faculty of Mathematics and Computer Science, Adam Mickiewicz University,
Umultowska 87, 61-614 Poznań, Poland
(e-mail: schoen@amu.edu.pl)

[2]Division of Algebra and Number Theory, Steklov Mathematical Institute,
ul. Gubkina, 8, Moscow, 119991 Russia
(e-mail: ilya.shkredov@gmail.com)

Received 17 May 2011; revised 8 June 2011; first published online 7 July 2011

A set of reals $A = \{a_1, \dots, a_n\}$ is called convex if $a_{i+1} - a_i > a_i - a_{i-1}$ for all i. We prove, among other results, that for some $c > 0$ every convex A satisfies $|A - A| \geqslant c|A|^{8/5} \log^{-2/5} |A|$.

1. Introduction

Let $A = \{a_1, \dots, a_n\}$, $a_i < a_{i+1}$ be a set of real numbers. We say that A is *convex* if

$$a_{i+1} - a_i > a_i - a_{i-1}$$

for every $i = 2, \dots, n-1$. We use the Vinogradov notation $f \ll g$ to mean that $f \leqslant C|g|$ for some constant C (*i.e.*, $f = O(g)$), and $f \gg g$ for $g \ll f$. Hegyvári [6], answering a question of Erdős, proved that if A is convex then

$$|A + A| \gg |A| \log |A| / \log\log |A|.$$

This result was later improved by many authors. Konyagin [9] and Garaev [2] showed independently that the additive energy $\mathsf{E}(A) = \mathsf{E}(A, A)$ (defined in (2.1) below) of a convex set is $\ll |A|^{5/2}$, which immediately implies that

$$|A \pm A| \gg |A|^{3/2}.$$

Elekes, Nathanson and Ruzsa [1] proved that if A is convex then

$$|A + B| \gg |A|^{3/2}$$

† Supported by MNSW grant N201 543538.
‡ Supported by grant RFFI 06-01-00383, 11-01-00759 and grant Leading Scientific Schools 8684.2010.1.

https://doi.org/10.1017/S0963548311000277 Published online by Cambridge University Press

for every set B with $|B| = |A|$. Finally, Solymosi [15] generalized the above inequality, showing that if A is a set with distinct consecutive differences, *i.e.*, $a_{i+1} - a_i = a_{j+1} - a_j$ implies $i = j$, then

$$|A + B| \gg |A||B|^{1/2} \tag{1.1}$$

for every set B. For further related results see [3], [4], [5] and [7]. The aim of this note is to establish the following theorem.

Theorem 1.1. *Let A be a convex set. Then*

$$|A - A| \gg |A|^{8/5} \log^{-2/5} |A|, \quad |A + A| \gg |A|^{14/9} \log^{-2/3} |A|,$$

and

$$|A + A|^3 |A - A|^2 \log^2 |A| \gg |A|^8.$$

In the proof of Theorem 1.1 we use the obvious inequality

$$|(A + A) \cap (A + A + s)| \geqslant |A + (A \cap (A + s))|,$$

which has recently found many applications [8, 10, 11, 12, 13]. Roughly speaking, we show that if $|A - A|$ is not much bigger than $|A|^{3/2}$ then the energy $\mathsf{E}(A, A - A)$ is very large. On the other hand, we prove that this cannot be the case for a convex set A.

Let us also remark that a similar result to our Theorem 1.1 was proved independently by Solymosi and Szemerédi.

We conclude with few comments regarding the notation used in this paper. If A is a set, then we write $A(x)$ for its characteristic function, *i.e.*, $A(x) = 1$ if $x \in A$ and $A(x) = 0$ otherwise. All logarithms are to base 2.

2. Preliminaries

We collect here results which will be used in the course of the proof of Theorem 1.1. Denote by $\delta_{A,B}(s)$ and $\sigma_{A,B}(s)$ the number of representations of s in the form $a - b$ and $a + b$, $a \in A$, $b \in B$, respectively. If $A = B$ we simply write $\delta_A(s) = \delta_{A,A}(s)$. Furthermore, put

$$\mathsf{E}(A, B) = \sum_s \delta_A(s)\delta_B(s) = \sum_s \delta_{A,B}(s)^2 = \sum_s \sigma_{A,B}(s)^2 \tag{2.1}$$

and

$$\mathsf{E}_3(A) = \sum_s \delta_A(s)^3.$$

Let $A_s = A \cap (A + s)$. Clearly, $|A_s| = \delta_A(s)$. The following lemma was proved in [13].

Lemma 2.1. *Let $\mathbf{G}$ be an abelian group. For every finite set $A \subseteq \mathbf{G}$ we have*

$$\sum_s \mathsf{E}(A, A_s) = \mathsf{E}_3(A).$$

https://doi.org/10.1017/S0963548311000277 Published online by Cambridge University Press

Denote by P and P' the set of all $s \in A-A$ such that $\delta_A(s) \geqslant |A|^2/(2|A-A|)$ and $\delta_A(s) \geqslant |A|^2/(2|A+A|)$, respectively. Observe that

$$\sum_{s \notin P} |A_s| < (1/2)|A|^2,$$

so

$$\sum_{s \in P} |A_s| > (1/2)|A|^2. \tag{2.2}$$

Further,

$$\frac{|A|^4}{|A+A|} \leqslant \mathsf{E}(A,A) = \sum_{s \in A-A} |A_s|^2.$$

Thus

$$\frac{|A|^4}{2|A+A|} \leqslant \sum_{s \in P'} |A_s|^2. \tag{2.3}$$

The next result is a straightforward modification of Corollary 3.2 from [13].

Corollary 2.2. *Let A be a subset of an abelian group, $P_* \subseteq A-A$ and $\sum_{s \in P_*} |A_s| = \eta |A|^2$, $\eta \in (0,1]$. Then*

$$\sum_{s \in P_*} |A \pm A_s| \geqslant \eta^2 |A|^6 \mathsf{E}_3^{-1}(A).$$

Proof. By the Cauchy–Schwarz inequality we have

$$|A||A_s| = \sum_x \delta_{A,A_s}(x) = \sum_x \sigma_{A,A_s}(x) \leqslant \mathsf{E}(A,A_s)^{1/2} |A \pm A_s|^{1/2},$$

so that applying the Cauchy–Schwarz inequality once again and then inserting the equality of Lemma 2.1, we get that

$$\sum_{s \in P_*} |A||A_s| \leqslant \left(\sum_{s \in P_*} \mathsf{E}(A,A_s)\right)^{1/2} \left(\sum_{s \in P_*} |A \pm A_s|\right)^{1/2} \leqslant \mathsf{E}_3(A)^{1/2} \left(\sum_{s \in P_*} |A \pm A_s|\right)^{1/2}. \qquad \square$$

Order the elements $s \in A-A$ such that $\delta_A(s_1) \geqslant \delta_A(s_2) \geqslant \dots \geqslant \delta_A(s_t)$, $t = |A-A|$. The next lemma was proved in [2] and in [7].

Lemma 2.3. *Let A be a convex set. Then, for every $r \geqslant 1$ we have*

$$\delta_A(s_r) \ll |A|/r^{1/3}.$$

Corollary 2.4. *Let A be a convex set. Then*

$$\mathsf{E}_3(A) \ll |A|^3 \log |A|.$$

https://doi.org/10.1017/S0963548311000277 Published online by Cambridge University Press

The last lemma is a consequence of the Szemerédi–Trotter theorem [16]; see also [7]. We call a set $\mathcal{L}$ of continuous plane curves a *pseudo-line system* if any two members of $\mathcal{L}$ share at most one point in common.

Theorem 2.5 ([16]). *Let $\mathcal{P}$ be a set of points and let $\mathcal{L}$ be a pseudo-line system. Then*

$$\mathcal{I}(\mathcal{P},\mathcal{L}) = |\{(p,l) \in \mathcal{P}\times\mathcal{L} : p \in l\}| \ll |\mathcal{P}|^{2/3}|\mathcal{L}|^{2/3} + |\mathcal{P}| + |\mathcal{L}|.$$

Lemma 2.6. *Let A be a convex set and $A' \subseteq A$. Then, for every set B we have*

$$|A'+B| \gg |A'|^{3/2}|B|^{1/2}|A|^{-1/2}.$$

Furthermore, for every $\tau \geqslant 1$ we have

$$|\{x \in A-B : \delta_{A,B}(x) \geqslant \tau\}| \ll \frac{|A||B|^2}{\tau^3}.$$

Proof. Set $I = \{1,\dots,|A|\}$ and let f be any continuous strictly convex function such that $f(i) = a_i$ for every $i \in I$. Let $Q \subseteq I$ be the set satisfying $f(Q) = A'$. For integers α,β put $l_{\alpha,\beta} = \{(q,f(q)) : q \in Q\} + (\alpha,\beta)$. We consider the pseudo-line system $\mathcal{L} = \{l_{\alpha,\beta} : \alpha \in I,\ \beta \in B\}$, and the set of points $\mathcal{P} = (Q+I)\times(A'+B)$. Thus, $\mathcal{L} = |I||B|$ and $|\mathcal{P}| = |Q+I||A'+B|$. Since each curve $l_{\alpha,\beta}$ contains $|Q|$ points from $\mathcal{P}$, it follows by the Szemerédi–Trotter theorem that

$$|Q||I||B| \leqslant \mathcal{I}(\mathcal{P},\mathcal{L}) \ll (|\mathcal{P}||\mathcal{L}|)^{2/3} + |\mathcal{P}| + |\mathcal{L}|,$$

where $\mathcal{I}(\mathcal{P},\mathcal{L})$ stands for the number of incidences between $\mathcal{P}$ and $\mathcal{L}$. Clearly, $|Q+I| \leqslant 2|I| = 2|A|$, so that

$$|A'+B| \gg |A'|^{3/2}|B|^{1/2}|A|^{-1/2}.$$

Obviously, it is enough to prove the second assertion for $1 \ll \tau \leqslant \min\{|A|,|B|\}$. Let $\mathcal{P}_\tau$ be the set of points of $\mathcal{P}$ belonging to at least τ curves from $\mathcal{L}$. Clearly, $\mathcal{I}(\mathcal{P}_\tau,\mathcal{L}) \geqslant \tau|\mathcal{P}_\tau|$ and by the Szemerédi–Trotter theorem we have

$$\tau|\mathcal{P}_\tau| \ll (|\mathcal{P}_\tau||I||B|)^{2/3} + |I||B| + |\mathcal{P}_\tau|. \tag{2.4}$$

We prove that $|\mathcal{P}_\tau| \ll |I|^2|B|^2/\tau^3$. If $(|\mathcal{P}_\tau||I||B|)^{2/3} \geqslant |I||B|$ then $|\mathcal{P}_\tau| \ll |I|^2|B|^2/\tau^3$. Otherwise, we have $|\mathcal{P}_\tau| \ll |I||B|/\tau \ll |I|^2|B|^2/\tau^3$. Finally, each $x \in A+B$ with $\delta_{A,B}(x) \geqslant \tau$ gives at least $|I|$ points $p \in \mathcal{P}_\tau$ having the same ordinate. Therefore, by (2.4),

$$|\{x \in A-B : \delta_{A,B}(x) \geqslant \tau\}| \leqslant |\mathcal{P}_\tau|/|I| \ll |I||B|^2/\tau^3,$$

which completes the proof. □

3. Proof of Theorem 1.1

Put $D = A-A$, $S = A+A$ and $|D| = K|A|$, $|S| = L|A|$. Observe that, for every s,

$$A - A_s \subseteq D \cap (D-s) \quad \text{and} \quad A + A_s \subseteq S \cap (S+s),$$

https://doi.org/10.1017/S0963548311000277 Published online by Cambridge University Press

so $\delta_D(s) \geqslant |A - A_s|$ and $\delta_S(s) \geqslant |A + A_s|$. By Corollary 2.2 and (2.2), we have

$$\frac{|A|^6}{4\mathsf{E}_3(A)} \leqslant \sum_{s\in P} |A - A_s| \leqslant \sum_{s\in P} \delta_D(s),$$

and hence

$$\frac{|A|^7}{8K\mathsf{E}_3(A)} \leqslant \sum_s \delta_A(s)\delta_D(s) = \mathsf{E}(A, D).$$

On the other hand,

$$\frac{|A|^4}{K\log|A|} \ll \mathsf{E}(A, D) \ll \sum_{s:\,\delta_{A,D}(s)\geqslant\Delta} \delta_{A,D}(s)^2,$$

where $\Delta = |A|^2/(K^2\log|A|)$. Therefore, by Lemma 2.6 and a dyadic argument, we have

$$\frac{|A|^4}{K\log|A|} \ll \sum_{j\geqslant 1} \Delta^2 2^{2j}\frac{K^2|A|^3}{\Delta^3 2^{3j}} = K^4|A|\log|A|,$$

so that

$$K \gg |A|^{3/5}\log^{-2/5}|A|.$$

Next we prove the second and the third inequalities. By Corollary 2.2, (2.2) and Lemma 2.6, we see that

$$\frac{|A|^7}{8K\mathsf{E}_3(A)} \leqslant \sum_s \delta_{A,S}(s)^2 \ll L^3K|A|\log|A|,$$

whence

$$|A|^8 \ll |A + A|^3|A - A|^2\log^2|A|.$$

Lemma 2.6 and (2.3) give

$$\frac{|A|^3}{L} \ll \sum_{s\in P':\,|A_s|\ll L} |A_s|^2.$$

Thus, there exists $j \geqslant 1$, $2^j \leqslant L^2/|A|$ such that

$$\sum_{s:\,2^{j-1}|A|/L<|A_s|\leqslant 2^j|A|/L} |A_s| \gg \frac{|A|^2}{2^j\log|A|}.$$

Hence, by Corollary 2.2 and Lemma 2.6 we get

$$|A|^3 \ll L^5 2^{2j}\log^6|A| \ll \frac{L^9}{|A|^2}\log^6|A|,$$

so

$$L \gg |A|^{5/9}\log^{-2/3}|A|,$$

as required. □

https://doi.org/10.1017/S0963548311000277 Published online by Cambridge University Press

References

[1] Elekes, G., Nathanson, M. and Ruzsa, I. Z. (2000) Convexity and sumsets. *J. Number Theory* **83** 194–201.

[2] Garaev, M. Z. (2000) On lower bounds for the L_1-norm of exponential sums. *Math. Notes* **68** 713–720.

[3] Garaev, M. Z. (2007) On an additive representation associated with the L_1-norm of an exponential sum. *Rocky Mountain J. Math.* **56** 1551–1556.

[4] Garaev, M. Z. (2007) On the number of solutions of a diophantine equation with symmetric entries. *J. Number Theory* **125** 201–209.

[5] Garaev, M. Z. and Kueh, K.-L. (2005) On cardinality of sumsets. *J. Aust. Math. Soc.* **78** 221–224.

[6] Hegyvári, N. (1986) On consecutive sums in sequences. *Acta Math. Acad. Sci. Hungar.* **48** 193–200.

[7] Iosevich, A., Konyagin, V. S., Rudnev, M. and Ten, V. (2006) Combinatorial complexity of convex sequences. *Discrete Comput. Geom.* **35** 143–158.

[8] Katz, N. H. and Koester, P. (2010) On additive doubling and energy. *SIAM J. Discrete Math.* **24** 1684–1693.

[9] Konyagin, V. S. (2000) An estimate of the L_1-norm of an exponential sum. In *The Theory of Approximations of Functions and Operators: Abstracts of Papers of the International Conference Dedicated to Stechkin's 80th Anniversary* (in Russian), pp. 88–89.

[10] Sanders, T. (2010) On a non-abelian Balog–Szemerédi-type lemma. *J. Aust. Math. Soc.* **89** 127–132.

[11] Sanders, T. On Roth's theorem on progressions. *Ann. of Math.*, to appear.

[12] Schoen, T. (2011) Near optimal bounds in Freiman's theorem. *Duke Math. J.* **158** 1–12.

[13] Schoen, T. and Shkredov, I. D. Additive properties of multiplicative subgroups of $\mathbb{F}_p$. *Quart. J. Math.*, to appear.

[14] Shkredov, I. D. and V'ugin, I. V. Additive shifts of multiplicative subgroups. *Mat. Sbornik*, to appear.

[15] Solymosi, J. (2009) Sumas contra productos. *Gaceta de la Real Sociedad Matematica Española*, **12** (4).

[16] Szemerédi, E. and Trotter, W. T. (1983) Extremal problems in discrete geometry. *Combinatorica* **3** 381–392.

https://doi.org/10.1017/S0963548311000277 Published online by Cambridge University Press