ON A THEOREM OF SHKREDOV

TOM SANDERS

Abstract. We show that if A is a finite subset of an abelian group with additive energy at least $c|A|^3$ then there is a set $\mathcal{L} \subset A$ with $|\mathcal{L}| = O(c^{-1}\log|A|)$ such that $|A \cap \mathrm{Span}(\mathcal{L})| = \Omega(c^{1/3}|A|)$.

1. Introduction and notation

We shall prove the following theorem which is a slight strengthening of [Shk08a, Theorem 1.5].

Theorem 1.1. *Suppose that G is an abelian group and $A \subset G$ is a finite set with $\|1_A * 1_A\|_{\ell^2(G)}^2 \geqslant c|A|^3$. Then there is a set $\mathcal{L} \subset A$ with $|\mathcal{L}| = O(c^{-1}\log|A|)$ such that*[1] $|A \cap \mathrm{Span}(\mathcal{L})| = \Omega(c^{1/3}|A|)$.

It is immediate from the Cauchy-Schwarz inequality that if $|A+A| \leqslant K|A|$ then $\|1_A * 1_A\|_{\ell^2(G)}^2 \geqslant |A|^3/K$ whence the conclusion of the above result applies to A. This was noted by Shkredov in [Shk08a, Corollary 3.2], however, something slightly stronger is also true.[2]

Theorem 1.2. *Suppose that G is an abelian group and $A \subset G$ is a finite set with $|A + A| \leqslant K|A|$. Then there is a set $\mathcal{L} \subset A$ with $|\mathcal{L}| = O(K\log|A|)$ such that $A \subset \mathrm{Span}(\mathcal{L})$.*

Before we begin with our proofs it will be useful to recall some well-known tools; Rudin [Rud90] is the classic reference for these.

A subset $\mathcal{L}$ of an abelian group G is said to be *dissociated* if

$$\sum_{x\in\mathcal{L}} \sigma_x.x = 0_G \text{ and } \sigma \in \{-1,0,1\}^{\mathcal{L}} \text{ implies that } \sigma \equiv 0.$$

Algebraically, dissociativity is particularly useful in view of the following easy lemma.

Lemma 1.3. *Suppose that G is an abelian group and $A \subset G$ is finite. If $\mathcal{L} \subset A$ is a maximal dissociated subset of A then $A \subset \mathrm{Span}(\mathcal{L})$.*

Analytically, dissociativity can be handled very effectively using the Fourier transform which we take a moment to introduce.

Suppose that G is a (discrete) abelian group. We write $\widehat{G}$ for the dual group, that is the compact abelian group of homomorphisms from G to $S^1 := \{z \in \mathbb{C} : |z| = 1\}$

[1] Recall that $\mathrm{Span}(\mathcal{L})$ is the set of all sums $\sum_{x\in\mathcal{L}} \sigma_x.x$ where $\sigma \in \{-1,0,1\}^{\mathcal{L}}$.

[2] Since writing this note it has come to the author's attention [Shk08b] that Shkredov has also independently proved Theorem 1.2.

endowed with the Haar probability measure $\mu_{\widehat{G}}$, and define the Fourier transform of a function $f \in \ell^1(G)$ to be

$$\widehat{f} : \widehat{G} \to \mathbb{C}; \gamma \mapsto \sum_{x \in G} f(x)\overline{\gamma(x)}.$$

The following result is a key tool in harmonic analysis.

Proposition 1.4 (Rudin's inequality)**.** *Suppose that G is an abelian group and $\mathcal{L} \subset G$ is a dissociated set. Then, for each $p \in [2, \infty)$ we have*

$$\|\widehat{f}\|_{L^p(\mu_{\widehat{G}})} = O(\sqrt{p}\|f\|_{\ell^2(\mathcal{L})}) \text{ for all } f \in \ell^2(\mathcal{L}).$$

The proof may be found in many places (e.g. [Rud90]) and proceeds for even integral values of p (from which the general result follows immediately) where one may apply Parseval's theorem to get a physical space expression which counts additive relations; dissociativity tells us that there are few of these and so the norm is small.

2. The proof of Theorem 1.1

Our proof of Theorem 1.1 is guided by Shkredov [Shk08a] although we are able to make some simplifications and improvements by using some standard facts about the $L^p(\mu_{\widehat{G}})$-norms.

We require the following lemma which is implicit in the paper [Bou90] of Bourgain.

Lemma 2.1. *Suppose that G is a abelian group, $A \subset G$ is finite, l is a positive integer and $p \geqslant 2$. Then there is a set $A' \subset A$ such that all dissociated subsets of A' have size at most l and*

$$\|\widehat{1_A} - \widehat{1_{A'}}\|_{L^p(\mu_{\widehat{G}})} = O(\sqrt{p/l}|A|).$$

Proof. We define sets $A_0 \supset A_1 \supset \cdots \supset A_s$ and $\mathcal{L}_0, \mathcal{L}_1, \ldots, \mathcal{L}_s$ iteratively starting with $A_0 := A$. Suppose that we have defined A_i.

(i) If there is no dissociated subset of A_i with size l then terminate the iteration;
(ii) if there is a dissociated subset of A_i with size l then let $\mathcal{L}_i$ be any such set and put $A_{i+1} = A_i \setminus \mathcal{L}_i$.

The algorithm terminates at some stage s with $s \leqslant |A|/l$ since $|A_{i+1}| = |A_i| - l$. Write $A' := A_s$ which consequently has no dissociated subset of size greater than l.

Since A is the disjoint union of the sets $\mathcal{L}_0, \ldots, \mathcal{L}_{s-1}$ and A', and the Fourier transform is linear we have

$$\|\widehat{1_A} - \widehat{1_{A'}}\|_{L^p(\mu_{\widehat{G}})} = \|\sum_{i=0}^{s-1} \widehat{1_{\mathcal{L}_i}}\|_{L^p(\mu_{\widehat{G}})} \leqslant \sum_{i=0}^{s-1} \|\widehat{1_{\mathcal{L}_i}}\|_{L^p(\mu_{\widehat{G}})}.$$

Now each summand is $O(\sqrt{p}\|1_{\mathcal{L}_i}\|_{\ell^2(\mathcal{L}_i)}) = O(\sqrt{pl})$, by Rudin's inequality, whence

$$\|\widehat{1_A} - \widehat{1_{A'}}\|_{L^p(\mu_{\widehat{G}})} = O(s\sqrt{pl}) = O(\sqrt{p/l}|A|),$$

in view of the upper bound on s. □

Proof of Theorem 1.1. Write $p := 2 + \log|A|$ and let l be an integer with $l = O(pc^{-(p-2)/p}|A|^{2/p}) = O(c^{-1}\log|A|)$ such that when we apply Lemma 2.1 to A we get a set $A' \subset A$ for which

$$\|\widehat{1_A} - \widehat{1_{A'}}\|_{L^p(\mu_{\widehat{G}})} \leqslant c^{(p-2)/2p}|A|^{(p-1)/p}/4. \tag{2.1}$$

Let $\mathcal{L}$ be a maximal dissociated subset of A'. We have $|\mathcal{L}| \leqslant l = O(c^{-1}\log|A|)$ by the choice of l, and $A' \subset \mathrm{Span}(\mathcal{L})$ by Lemma 1.3, whence $|A \cap \mathrm{Span}(\mathcal{L})| \geqslant |A'|$ and the result will follow from a lower bound on $|A'|$.

By the log-convexity of the $L^p(\mu_{\widehat{G}})$ norms we have

$$\begin{aligned}
\|\widehat{1_A} - \widehat{1_{A'}}\|_{L^4(\mu_{\widehat{G}})}^4 &\leqslant \|\widehat{1_A} - \widehat{1_{A'}}\|_{L^2(\mu_{\widehat{G}})}^{(2p-8)/(p-2)}\|\widehat{1_A} - \widehat{1_{A'}}\|_{L^p(\mu_{\widehat{G}})}^{2p/(p-2)}\\
&= \|1_{A\setminus A'}\|_{L^2(\mu_{\widehat{G}})}^{(2p-8)/(p-2)}\|\widehat{1_A} - \widehat{1_{A'}}\|_{L^p(\mu_{\widehat{G}})}^{2p/(p-2)}\\
&\leqslant |A|^{(p-4)/(p-2)}\|\widehat{1_A} - \widehat{1_{A'}}\|_{L^p(\mu_{\widehat{G}})}^{2p/(p-2)},
\end{aligned}$$

by Parseval's theorem and the fact that $A' \subset A$. Now, inserting the bound in (2.1) we get that

$$\|\widehat{1_A} - \widehat{1_{A'}}\|_{L^4(\mu_{\widehat{G}})}^4 \leqslant |A|^{(p-4)/(p-2)}.c|A|^{(2p-4)/(p-2)}/2^{4p/(p-2)} \leqslant \|\widehat{1_A}\|_{L^4(\mu_{\widehat{G}})}^4/2^4.$$

On the other hand, by the triangle inequality,

$$\|\widehat{1_A} - \widehat{1_{A'}}\|_{L^4(\mu_{\widehat{G}})} \geqslant \|\widehat{1_A}\|_{L^4(\mu_{\widehat{G}})} - \|\widehat{1_{A'}}\|_{L^4(\mu_{\widehat{G}})}$$

whence, on combination with the previous, we have

$$\|1_{A'}\|_{L^4(\mu_{\widehat{G}})}^4 \geqslant \|1_A\|_{L^4(\mu_{\widehat{G}})}^4/2^4 \geqslant c|A|^3/2^4. \tag{2.2}$$

Finally, we note that

$$\|\widehat{1_{A'}}\|_{L^4(\mu_{\widehat{G}})}^4 \leqslant \|\widehat{1_{A'}}\|_{L^2(\mu_{\widehat{G}})}^2\|\widehat{1_{A'}}\|_{L^\infty(\mu_{\widehat{G}})}^2 \leqslant |A'|^3,$$

by Hölder's inequality, Parseval's theorem and the Hausdorff-Young inequality. The result follows on taking cube roots. □

3. The proof of Theorem 1.2

The proof is essentially Theorem 6.10 of López and Ross [LR75] coupled with Lemma 1.3.

Proof of Theorem 1.2. Write $f := 1_{A+A} * 1_{-A}$. Then

$$\begin{aligned}
\|\widehat{f}\|_{L^1(\mu_{\widehat{G}})} &= \int |\widehat{1_{A+A}}(\gamma)\widehat{1_{-A}}(\gamma)|d\mu_{\widehat{G}}(\gamma)\\
&\leqslant \left(\int |\widehat{1_{A+A}}(\gamma)|^2 d\mu_{\widehat{G}}(\gamma)\right)^{1/2}\left(\int |\widehat{1_{-A}}(\gamma)|^2 d\mu_{\widehat{G}}(\gamma)\right)^{1/2}\\
&= \sqrt{|A+A||-A|} \leqslant \sqrt{K}|A|,
\end{aligned}$$

by the Cauchy-Schwarz inequality, Parseval's theorem and the doubling condition $|A+A| \leqslant K|A|$. Furthermore $\|f\|_{\ell^\infty(G)} \leqslant |A|$ and $\|f\|_{\ell^1(G)} = |A||A+A|$ and so

$$\|\widehat{f}\|_{L^2(\mu_{\widehat{G}})}^2 = \|f\|_{\ell^2(G)}^2 \leqslant \|f\|_{\ell^\infty(G)}.\|f\|_{\ell^1(G)} \leqslant |A|^2|A+A| \leqslant K|A|^3,$$

by Parseval's theorem, Hölder's inequality and the doubling condition. Whence, by log-convexity of the $L^{p'}(\mu_{\widehat{G}})$ norms, we have

$$\|\widehat{f}\|_{L^{p'}(\mu_{\widehat{G}})} \leqslant \sqrt{K}|A|^{2-1/p'} \text{ for all } p' \in [1,2].$$

Suppose that $\mathcal{L}$ is a maximal dissociated subset of A and (p, p') is a conjugate pair of exponents with $p' \in (1, 2]$. Then, by Rudin's inequality, we have

$$\begin{aligned}\|f\|_{\ell^2(\mathcal{L})}^2 = \langle \widehat{f1_{\mathcal{L}}}, \widehat{f}\rangle_{L^2(\mu_{\widehat{G}})} &\leqslant \|\widehat{f1_{\mathcal{L}}}\|_{L^p(\mu_{\widehat{G}})}\|\widehat{f}\|_{L^{p'}(\mu_{\widehat{G}})}\\ &= O(\sqrt{p}.\|f\|_{\ell^2(\mathcal{L})}\|\widehat{f}\|_{L^{p'}(\mu_{\widehat{G}})}).\end{aligned}$$

The construction of f ensures that for any $a \in A$, $f(a) = 1_{A+A} * 1_{-A}(a) \geqslant |A|$ so, canceling $\|f\|_{\ell^2(\mathcal{L})}$ above we get

$$\sqrt{|\mathcal{L}|.|A|^2} \leqslant \|f\|_{\ell^2(\mathcal{L})} = O(\sqrt{p}\|\widehat{f}\|_{L^{p'}(\mu_{\widehat{G}})}) = O(\sqrt{pK}|A|^{2-1/p'}).$$

Putting $p = 2 + \log|A|$ and some rearrangement tells us that $|\mathcal{L}| = O(K \log|A|)$. Since $\mathcal{L}$ was maximal Lemma 1.3 then yields the result. □

4. Concluding remarks

In some ways the results are close to best possible. In Theorem 1.2 suppose that A is the union of K highly dissociated points and a long arithmetic progression (or subgroup if G has a lot of torsion). It is easy to see that in this case if $\mathcal{L}$ is such that $A \subset \operatorname{Span}(\mathcal{L})$ then $|\mathcal{L}| = \Omega(K + \log|A|)$. If K is around $\log^{O(1)}|A|$ then this is close to the upper bound in the theorem; if $K = \log^{o(1)}|A|$ then there are better results known: this is the celebrated Green-Ruzsa-Freĭman theorem [GR07].

In Theorem 1.1 the $c^{1/3}$ cannot be improved: consider an arithmetic progression (or, again, subgroup if G has a lot of torsion) of length $c^{1/3}|A|$ unioned with $|A|$ dissociated points. This satisfies the lower bound on the energy but one cannot hope to find any structure other than the progression, *i.e.* in more than a proportion $\Omega(c^{1/3})$ of the set. Of course, this bound is not the important bound in the result; the bound on $\mathcal{L}$ is what is really of interest.

References

[Bou90] J. Bourgain. On arithmetic progressions in sums of sets of integers. In *A tribute to Paul Erdős*, pages 105–109. Cambridge Univ. Press, Cambridge, 1990.

[GR07] B. J. Green and I. Z. Ruzsa. Freĭman's theorem in an arbitrary abelian group. *J. Lond. Math. Soc. (2)*, 75(1):163–175, 2007.

[LR75] J. M. López and K. A. Ross. *Sidon sets*. Marcel Dekker Inc., New York, 1975. Lecture Notes in Pure and Applied Mathematics, Vol. 13.

[Rud90] W. Rudin. *Fourier analysis on groups*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1990. Reprint of the 1962 original, A Wiley-Interscience Publication.

[Shk08a] I. D. Shkredov. On sets with small doubling. *Mat. Zametki*, 84(6):927–947, 2008.

[Shk08b] I. D. Shkreov. Personal communication. 2008.

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, England

E-mail address: t.sanders@dpmms.cam.ac.uk