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 $L \subset A$ with $|L| = o(c^{-1} \log |A|)$ such that $|A \cap \operatorname{Span}(L)| = \Omega(c^{1/2} |A|)$.

1. Introduction and notation

We shall prove the following theorem which is a slight strengthening of [Shk07, Theorem 1.5].

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

It is immediate from the Cauchy-Schwarz inequality that if $|A + A| \leq K |A|$ then $\|1_A * 1_A\|_{L^2(G)} \geq |A|^3/K$ whence the conclusion of the above result applies to $A$. This was noted by Shkredov in [Shk07, Corollary 3.2], however, something slightly stronger is also true.

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

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 $L$ of an abelian group $G$ is said to be dissociated if

$$\sum_{x \in L} \sigma_x x = 0_G$$

and $\sigma \in \{-1, 0, 1\}^L$ 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 $L \subset A$ is a maximal dissociated subset of $A$ then $A \subset \operatorname{Span}(L)$.

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 $\hat{G}$ for the dual group, that is the compact abelian group of homomorphisms from $G$ to $S^1 := \{z \in \mathbb{C} : |z| = 1\}$.

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

\[\text{Since writing these notes it has come to the author’s attention that Shkredov has also independently proved Theorem 1.2.}\]
endowed with the Haar probability measure $\mu_G$, and define the Fourier transform of a function $f \in \ell^4(G)$ to be

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

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

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

2. **The Proof of Theorem 1.1**

Our proof of Theorem 1.1 is guided by Shkredov [Shk07] although we are able to make some simplifications by using some standard facts about the $L^p(\mu_G)$-norms.

We require the following lemma which is contained 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 $p \gg 2$. Then there is a set $A' \subset A$ such that all dissociated subsets of $A'$ have size at most $l$ and

$$\|\hat{1}_A - \hat{1}_{A'}\|_{L^p(\mu_G)} = O(\sqrt{l}|A|).$$

**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 $s \leq |A|/l$ 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 $A'$ we have

$$\|\hat{1}_A - \hat{1}_{A'}\|_{L^p(\mu_G)} = \|\sum_{i=0}^{s-1} 1_{\mathcal{L}_i}\|_{L^p(\mu_G)} \leq \sum_{i=0}^{s-1} \|1_{\mathcal{L}_i}\|_{L^p(\mu_G)}.$$

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

$$\|\hat{1}_A - \hat{1}_{A'}\|_{L^p(\mu_G)} = O(s\sqrt{p}) = O(\sqrt{p}/l|A|),$$

in view of the upper bound on $s$. \hfill \Box

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

$$(2.1) \quad \|\hat{1}_A - \hat{1}_{A'}\|_{L^p(\mu_G)} \leq c^{(p-2)/2p}|A|^{(p-1)/p}/2.$$ 

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

By the log-convexity of the $L^p(\mu_G)$ norms we have

$$\|\hat{1}_A\|_{L^p(\mu_G)} \leq \|\hat{1}_A\|_{L^2(\mu_G)}^{(2p-8)/(p-2)} \|\hat{1}_A\|_{L^p(\mu_G)}^{2p/(p-2)} = |A|^{(p-4)/(p-2)} \|\hat{1}_A\|_{L^p(\mu_G)}^{2p/(p-2)},$$

and
where the equality is by Parseval’s theorem. However, we are given that the left hand side is at least $c|A|^3$, whence we get the lower bound
\begin{equation}
\| \widehat{1_A} \|_{L^p(\mu_G)} \geq c^{(p-2)/2p} |A|^{(p-1)/p}.
\end{equation}

On the other hand using Hölder’s inequality we have the upper bound
\[ \| \widehat{1_A} \|_{L^p(\mu_G)} \leq \| \widehat{1_A} \|_{L^2(\mu_G)}^{2/p} \| \widehat{1_A} \|_{L^\infty(\mu_G)}^{(p-2)/p} \leq \|A\|^{(p-1)/p}, \]
where the second inequality is by Parseval’s theorem and the Hausdorff-Young inequality applied to the $L^2$-norm and $L^\infty$-norm respectively.

By the triangle inequality, this and (2.2) give
\[ \| \widehat{1_A - 1_A} \|_{L^p(\mu_G)} \geq c^{(p-2)/2p} |A|^{(p-1)/p} - \|A\|^{(p-1)/p}. \]
Using the upper bound on the left hand side from (2.1) it follows that
\[ |A'| \geq c^{(p-2)/2(p-1)} 2^{-n/(p-1)} |A| \geq c^{1/2} |A|/4, \]
as required. \hfill \square

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 $f := 1_{A+A} \ast 1_{-A}$. Then
\begin{align*}
\| \widehat{f} \|_{L^1(\mu_G)} &= \int |\widehat{1_{A+A}}(\gamma) \widehat{1_{-A}}(\gamma)| d\mu_G(\gamma) \\
&\leq \left( \int |\widehat{1_{A+A}}(\gamma)|^2 d\mu_G(\gamma) \right)^{1/2} \left( \int |\widehat{1_{-A}}(\gamma)|^2 d\mu_G(\gamma) \right)^{1/2} \\
&= \sqrt{|A+A| - |A|} \leq \sqrt{K} |A|,
\end{align*}
by the Cauchy-Schwarz inequality, Parseval’s theorem and the doubling condition $|A+A| \leq K|A|$. Furthermore, $\|f\|_{L^\infty(G)} \leq |A|$ and $\|f\|_{L^1(G)} = |A| |A+A|$ and so
\[ \| \widehat{f} \|_{L^2(\mu_G)}^2 = \|f\|_{L^2(G)} \lesssim \|f\|_{L^\infty(G)} \|f\|_{L^1(G)} \leq |A|^2 |A+A| \leq K |A|^3, \]
by Parseval’s theorem, Hölder’s inequality and the doubling condition. Whence, by log-convexity of the $L^{p'}(\mu_G)$ norms, we have
\[ \| \widehat{f} \|_{L^{p'}(\mu_G)} \leq \sqrt{K} |A|^{(p'+1)/2} \text{ for all } p' \in [1, 2]. \]

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{align*}
\|f\|_{L^2(\mu_G)}^2 &= \langle \widehat{1\mathcal{L}}, \widehat{f} \rangle_{L^2(\mu_G)} \leq \|f\|_{L^2(G)}^2 \|\widehat{1\mathcal{L}}\|_{L^{p'}(\mu_G)} \\
&= O(\sqrt{p} \|f\|_{L^2(G)} \|\widehat{1\mathcal{L}}\|_{L^{p'}(\mu_G)}).
\end{align*}
The construction of $f$ ensures that for any $a \in A$, $f(a) = 1_{A+A} \ast 1_{-A}(a) \geq |A|$ so, canceling $\|f\|_{L^2(G)}$ above we get
\[ \sqrt{|\mathcal{L}| |A|^2} \leq \|f\|_{L^2(G)} = O(\sqrt{p} \|\widehat{f}\|_{L^{p'}(\mu_G)}) = O(\sqrt{p} K |A|^{(p'+1)/2}). \]
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. \hfill \square
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.

[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.

[Shk] I. D. Shkreov. Personal communication.

[Shk07] I. D. Shkredov. On sets with small doubling. Preprint, 2007.

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