Canad. Math. Bull. Vol. **56** (2), 2013 pp. 412–423
http://dx.doi.org/10.4153/CMB-2011-165-0

Structure in Sets with Logarithmic Doubling

T. Sanders

Abstract. Suppose that G is an abelian group, $A \subset G$ is finite with $|A+A| \leq K|A|$ and $\eta \in (0,1]$ is a parameter. Our main result is that there is a set $\mathcal{L}$ such that

$$|A \cap \mathrm{Span}(\mathcal{L})| \geq K^{-O_\eta(1)}|A| \quad \text{and} \quad |\mathcal{L}| = O(K^\eta \log |A|).$$

We include an application of this result to a generalisation of the Roth–Meshulam theorem due to Liu and Spencer.

1 Introduction

Suppose that G is an abelian group. We are interested in the structure of sets with small doubling, the prototypical examples of which are coset progressions. A set M is a *d-dimensional coset progression* if it can be written in the form

$$M = H + P_1 + \cdots + P_d,$$

where $H \leq G$ and $P_1, \ldots, P_d$ are arithmetic progressions. It is easy to see that if A is a proportion δ of a d-dimensional coset progression, then $|A+A| \leq \delta^{-1}2^d|A|$; A has "small doubling". Remarkably there is something of a converse to this.

Theorem 1.1 (Green–Ruzsa–Freĭman) *Suppose that G is an abelian group and $A \subset G$ has $|A+A| \leq K|A|$. Then there is an $O_\varepsilon(K^{4+\varepsilon})$-dimensional coset progression M such that $A \subset M$ and $|M| \leq \exp(O_\varepsilon(K^{4+\varepsilon}))|A|$.*

This result is due to Green and Ruzsa [6] building on Ruzsa's proof [15] of Freĭman's theorem [4] in the integers. There are other proofs (see [22], for example) and a large body of literature which we shall not survey here.

Whilst this resolves the situation from a qualitative perspective, quantitatively things are far less well understood. Shkredov [19] noticed that one may hope to say something quantitatively stronger if one changes the structure sought to that of spans: recall that if $\mathcal{L} \subset G$, then

$$\mathrm{Span}(\mathcal{L}) := \left\{ \sum_{x \in \mathcal{L}} \sigma_x . x : \sigma_x \in \{-1, 0, 1\} \text{ for all } x \in \mathcal{L} \right\}.$$

With this notation Shkredov established the following theorem.

Received by the editors July 5, 2010; revised February 22, 2011.
Published electronically September 15, 2011.
AMS subject classification: **11B25**.
Keywords: Fourier analysis, Freiman's theorem, capset problem.

Theorem 1.2 *Suppose that G is an abelian group and $A \subset G$ has $|A+A| \leq K|A|$. Then there is a set $\mathcal{L}$ such that*

$$A \subset \mathrm{Span}(\mathcal{L}) \quad \textit{and} \quad |\mathcal{L}| = O(K \log |A|).$$

Of course, a span is a type of coset progression, and so once K is about $\log^{1/3} |A|$, the above result supersedes the Green–Ruzsa–Freĭman theorem.

As it stands the result is essentially best possible: consider a set A of K generic points. However, if one weakens the containment hypothesis to mere correlation, then one can hope to do better and to this end we shall prove the following.

Theorem 1.3 *Suppose that G is an abelian group, $A \subset G$ has $|A+A| \leq K|A|$, and $\eta \in (0,1]$. Then there is a set $\mathcal{L}$ such that*

$$|A \cap \mathrm{Span}(\mathcal{L})| \geq K^{-O(\exp(O(\eta^{-1})))}|A| \quad \textit{and} \quad |\mathcal{L}| = O(K^{\eta} \log |A|).$$

The reader may wish to compare this with the (much stronger) polynomial Freĭman–Ruzsa conjecture.

To illustrate the utility of Theorem 1.3, we address a natural generalisation of the Roth–Meshulam theorem [11] considered by Liu and Spencer [9].

Theorem 1.4 *Suppose that $\mathbb{F}$ is a finite field, $G := \mathbb{F}^n$, $c_1, \dots, c_r \in \mathbb{F}^*$ are such that $c_1 + \cdots + c_r = 0$, and $A \subset G$ contains no solutions to $c_1.x_1 + \cdots + c_r.x_r = 0$ with $x_1, \dots, x_r \in A$ pair-wise distinct. Then $|A| = O_{|\mathbb{F}|,r}(|\mathbb{F}|^n / n^{r-2})$.*

The requirement that the elements be pair-wise distinct rules out degenerate solutions introduced by having shorter sub-sums of the c_is equal to zero. Nevertheless, it should be noted that for a number of special equations better bounds are available. For example, if $c_i = -c_{r-i}$ and r is even, then a simple application of the Cauchy–Schwarz inequality will give a power shaped saving in the bound on $|A|$. The different "types" of equation are given a comprehensive analysis by Ruzsa in [14]; we shall not address this problem here.

The result above is a special case of the work of Liu and Spencer [9] who considered r-fold sums in arbitrary abelian groups and (along with Zhao) generalised it further to systems of equations of complexity 1 in [10].

Improving the bound in Theorem 1.4 in the case $r = 3$ (and $|\mathbb{F}| = 3$) is a well-known open problem sometimes called the capset problem, as discussed in [3, 7, 21]. We shall use Theorem 1.3 to show that there is a non-negative valued function $E(r)$ with $E(r) = \Omega(\log r)$ for all r sufficiently large, such that the following theorem holds.

Theorem 1.5 *Suppose that $\mathbb{F}$ is a finite field, $G := \mathbb{F}^n$, $c_1, \dots, c_r \in \mathbb{F}^*$ are such that $c_1 + \cdots + c_r = 0$, and $A \subset G$ contains no solutions to $c_1.x_1 + \cdots + c_r.x_r = 0$ with $x_1, \dots, x_r \in A$ pair-wise distinct. Then $|A| = O_{|\mathbb{F}|,r}(|\mathbb{F}|^n / n^{r-2+E(r)})$.*

We emphasise that $E(r)$ only becomes non-zero once r is sufficiently large; with some care this can be taken to be 2^{20}.

https://doi.org/10.4153/CMB-2011-165-0 Published online by Cambridge University Press

The paper now splits as follows. In the next section we record the basics of the Fourier transform and structure of the spectrum which we require for the proof of Theorem 1.3. In §3 we prove an asymmetric version of Shkredov's theorem, and then in §4 a symmetry set version of Chang's theorem. These results are combined with a proposition from [16] to prove Theorem 1.3 in §5. Following this we record some results from additive combinatorics which we require for our application in §6. Theorem 1.5 is then established in §7.

It should be remarked that around the same time as this paper was written Schoen [17] came up with a far better way of using the same ingredients to prove the first good bounds for a Freĭman–Ruzsa-type theorem, and then a little later in an additional unpublished argument[1] was able to improve Theorem 1.5.

2 The Fourier Transform and the Large Spectrum

A good introduction to the Fourier transform may be found in Rudin [13], and for our work the more modern reference [22] of Tao and Vu. Suppose that G is a locally compact abelian group endowed with a Haar measure μ_G. We define the convolution of two functions $f, g \in L^1(\mu_G)$ point-wise by

$$f * g(x) := \int f(y)g(-y+x)\,d\mu_G(y),$$

and write $\widehat{G}$ for the dual group, that is, the locally compact abelian group of homomorphisms from G to $S^1 := \{z \in \mathbb{C} : |z| = 1\}$. Convolution operators are diagonalized by the Fourier transform: we define the Fourier transform of a function $f \in L^1(\mu_G)$ by

$$\widehat{f}\colon \widehat{G} \to \mathbb{C}\,;\ \gamma \mapsto \int f(x)\overline{\gamma(x)}d\mu_G(x).$$

If we declare G as discrete, then we take μ_G to be counting measure (that is the measure assigning mass 1 to every element of G) and if we declare G as compact, then we take μ_G to be $\mathbb{P}_G$, the unique Haar probability measure on G. When G is finite, it will be clear from context which measure we take.

Suppose now that G is compact and $f \in L^1(G)$. The Hausdorff–Young inequality tells us that $|\widehat{f}(\gamma)| \leq \|f\|_{L^1(G)}$ and so it is natural to define the *δ-large spectrum of f* to be

$$\mathrm{Spec}_\delta(f) := \{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geq \delta\|f\|_{L^1(G)}\}.$$

Chang initiated work studying the structure of the spectrum in [2] and this has since been refined by Shkredov [18].

Proposition 2.1 (Chang's theorem) *Suppose that G is a compact abelian group, $f \in L^1(G)$ and $\delta \in (0,1]$ is a parameter. Then there is a set $\mathcal{L}$ such that*

$$\mathrm{Spec}_\delta(f) \subset \mathrm{Span}(\mathcal{L}) \quad \textit{and} \quad |\mathcal{L}| = O\big(\delta^{-2}\log\|f\|_{L^2(G)}^2\|f\|_{L^1(G)}^{-2}\big).$$

The functional version of this result can be read out of the proof in Chang's original paper, but was popularised by Green.

[1] Personal communication.

https://doi.org/10.4153/CMB-2011-165-0 Published online by Cambridge University Press

3 An Asymmetric Version of Shkredov's Theorem

In this section we use Chang's theorem to prove the following asymmetric version of Shkredov's theorem. The key idea is the introduction of a certain auxiliary function, which is a trick used in [8, Theorem 6.10] for proving a result on very similar lines.

Proposition 3.1 *Suppose that G is a discrete abelian group and $A \subset G$ is a finite non-empty set with $|B+A| \leq K|A|$. Then there is a set $\mathcal{L}$ such that*

$$B \subset \mathrm{Span}(\mathcal{L}) \quad \textit{and} \quad |\mathcal{L}| = O(K \log |A|).$$

Proof Throughout this proof the Fourier transform is the Fourier transform on the compact group $\widehat{G}$.

Define h and k by inversion so that $\widehat{h} = 1_{B+A}$ and $\widehat{k} = 1_{-A}$, and put $g := hk$. If $x \in B$, then $1_{B+A} * 1_{-A}(x) = |A|$, so

$$B \subset \{x : 1_{B+A} * 1_{-A}(x) \geq |A|\} = \mathrm{Spec}_{|A|/\|g\|_{L^1(\widehat{G})}}(g).$$

Applying Chang's theorem to this, we get a set $\mathcal{L}$ such that

$$B \subset \mathrm{Span}(\mathcal{L}) \quad \text{and} \quad |\mathcal{L}| = O\big(\|g\|^2_{L^1(\widehat{G})}|A|^{-2} \log \|g\|^2_{L^2(\widehat{G})}\|g\|^{-2}_{L^1(\widehat{G})}\big).$$

This is an increasing function of $\|g\|_{L^1(\widehat{G})}$ and $\|g\|_{L^2(\widehat{G})}$, so it remains to provide upper bounds for these quantities. First,

$$\begin{aligned}\|g\|_{L^1(\widehat{G})} &= \int |hk| \, d\mathbb{P}_{\widehat{G}} \\ &\leq \|h\|_{L^2(\widehat{G})}\|k\|_{L^2(\widehat{G})} \\ &= \sqrt{|B+A|.|-A|} \leq \sqrt{K}|A|,\end{aligned}$$

by the Cauchy–Schwarz inequality and Parseval's theorem. Second,

$$\begin{aligned}\|g\|^2_{L^2(\widehat{G})} &= \|1_{B+A} * 1_{-A}\|^2_{\ell^2(G)} \\ &\leq \|1_{B+A} * 1_{-A}\|_{\ell^\infty(G)}\|1_{B+A} * 1_{-A}\|_{\ell^1(G)} \\ &= |B+A||-A|^2 \leq K|A|^3\end{aligned}$$

by Parseval's theorem and then Hölder's inequality. It follows that

$$|\mathcal{L}| = O((\sqrt{K}|A|)^2|A|^{-2} \log(K|A|^3/(\sqrt{K}|A|)^2)) = O(K \log |A|)$$

as required. ∎

https://doi.org/10.4153/CMB-2011-165-0 Published online by Cambridge University Press

4 Structure in Symmetry Sets

Recall from [22] that if G is a discrete abelian group, $A \subset G$ is a finite non-empty set, and $\eta \in (0,1]$, then the *symmetry set of A at threshold η* is

$$\mathrm{Sym}_\eta(A) := \{x \in G : 1_A * 1_{-A}(x) \geq \eta|A|\}.$$

Symmetry sets are essentially dual to spectra so it should come as no surprise that they also have a structure theorem along the lines of Chang's theorem.

Proposition 4.1 (Chang's theorem for symmetry sets) *Suppose that G is a discrete abelian group, $A \subset G$ is a finite non-empty set and $\eta \in (0,1]$ is a parameter. Then there is a set $\mathcal{L}$ such that*

$$\mathrm{Sym}_\eta(A) \subset \mathrm{Span}(\mathcal{L}) \quad \textit{and} \quad |\mathcal{L}| = O(\eta^{-2}\log|A|).$$

Proof Symmetry sets are dual to spectra in the sense that $\mathrm{Sym}_\eta(A) = \mathrm{Spec}_\eta(f)$, where $f := |\widehat{1_A}|^2$. To see this, note that

$$\|f\|_{L^1(\widehat{G})} = \||\widehat{1_A}|^2\|_{L^1(\widehat{G})} = \|\widehat{1_A}\|^2_{L^2(\widehat{G})} = \|1_A\|^2_{\ell^2(G)} = |A|$$

by Parseval's theorem. In light of this we apply Chang's theorem to get that $\mathrm{Sym}_\eta(A)$ is contained in $\mathrm{Span}(\mathcal{L})$ for some set $\mathcal{L}$ with

$$|\mathcal{L}| = O\big(\eta^{-2}\log\|f\|^2_{L^2(\mathbb{P}_G)}\|f\|^{-2}_{L^1(\mathbb{P}_G)}\big).$$

The argument of the logarithm may then be bounded above by Hölder's inequality and the Hausdorff–Young inequality:

$$\|f\|^2_{L^2(\mathbb{P}_G)}\|f\|^{-2}_{L^1(\mathbb{P}_G)} \leq \|f\|_{L^\infty(\widehat{G})}\|f\|^{-1}_{L^1(\widehat{G})} = \||\widehat{1_A}|^2\|_{L^\infty(\widehat{G})}/|A| \leq |A|.$$

The result is proved. ∎

5 The Proof of Theorem 1.3

In light of Proposition 4.1 we should like to show that if A has small doubling, then it correlates with a symmetry set having large threshold. To this end we recall the following result.

Proposition 5.1 ([16, Proposition 1.3]) *Suppose that G is a discrete abelian group, A is a non-empty subset of G with $|A+A| \leq K|A|$, and $\epsilon \in (0,1]$ is a parameter. Then there is a non-empty set $A' \subset A$ such that*

$$|\mathrm{Sym}_{1-\epsilon}(A'+A)| \geq \exp(-K^{O(1/\log(1/(1-\epsilon)))}\log K)|A|.$$

In fact, the above is true for non-abelian groups as well (with the obvious changes of sums to products) but our other results are not. We shall use it in the range when ϵ is close to 1; the fact that it still has content in this region is an idea due to Tao.

We now have all the ingredients necessary for the proof of our main result.

https://doi.org/10.4153/CMB-2011-165-0 Published online by Cambridge University Press

Proof of Theorem 1.3 We begin by applying Proposition 5.1 with parameter $\epsilon = 1 - K^{\eta/2}$ to get that there is a non-empty set $A' \subset A$ with

$$|\operatorname{Sym}_{K^{-\eta/2}}(A'+A)| \geq K^{-\exp(O(\eta^{-1}))}|A|.$$

We apply Proposition 3.1 to get a set $\mathcal{L}$ such that

$$S := \operatorname{Sym}_{K^{-\eta/2}}(A'+A) \subset \operatorname{Span}(\mathcal{L}) \quad \text{and} \quad |\mathcal{L}| = O(K^{\eta}\log|A|).$$

On the other hand, $1_{A'+2A} * 1_{-A}(x) \geq |A|.1_{A'+A}(x)$ for all $x \in G$, whence

$$\begin{aligned}|A|^2.K^{-\eta/2}|A'+A||S| &\leq |A|^2.\langle 1_{A'+A} * 1_{-(A'+A)}, 1_S\rangle \\ &\leq \langle 1_{A'+2A} * 1_{-A} * 1_A * 1_{-(A'+2A)}, 1_S\rangle \\ &\leq \|1_{A'+2A} * 1_{-(A'+2A)} * 1_A\|_{\ell^1(G)}\|1_A * 1_S\|_{\ell^\infty(G)} \\ &= |A'+2A|^2|A|\|1_A * 1_S\|_{\ell^\infty(G)}.\end{aligned}$$

Since $A' \subset A$ and $|A+A| \leq K|A|$, we have, by Plünnecke's inequality, that $|A'+2A| \leq K^3|A|$, and so

$$\|1_A * 1_S\|_{\ell^\infty(G)} \geq K^{3-\eta/2}|S| \geq K^{-\exp(O(\eta^{-1}))}|A|.$$

It follows that there is some x such that $|A \cap (x+S)| \geq K^{-\exp(O(\eta^{-1}))}|A|$, but then $x + S \subset \operatorname{Span}(\mathcal{L}')$, where $\mathcal{L}' := \mathcal{L} \cup \{x\}$. ∎

6 Some Tools of the Trade in Additive Combinatorics

In this section we shall record some of the standard tools used in additive combinatorics for the purposes of proving Theorem 1.3 in the next section.

Chang's theorem from §2 was proved using Rudin's inequality, and in our context this may be seen as an estimate for the higher energy norms of the spectrum. Shkredov [18] encoded this idea formally, and we shall now record a weak version of one of his results saying that the large spectrum has large additive energy; we include a proof since it is so short.

Proposition 6.1 *Suppose that G is a compact abelian group, $A \subset G$ has density $\alpha > 0$ and $S \subset \operatorname{Spec}_\delta(A)$. Then $E(S) := \|1_S * 1_{-S}\|^2_{\ell^2(\widehat{G})} \geq \delta^8\alpha|S|^4$.*

Proof We begin by applying Plancherel's theorem and Hölder's inequality to the inner product

$$|\langle \widehat{1_A}1_S, \widehat{1_A}\rangle_{\ell^2(\widehat{G})}| = |\langle 1_A * \widehat{1_S}, 1_A\rangle_{L^2(G)}| \leq \|1_A * \widehat{1_S}\|_{L^4(G)}\|1_A\|_{L^{4/3}(G)}.$$

By a trivial instance of Young's inequality and Parseval's theorem we have

$$\|1_A * \widehat{1_S}\|_{L^4(G)} \leq \|1_A\|_{L^1(G)}\|\widehat{1_S}\|_{L^4(G)} = \alpha E(S)^{1/4},$$

and even more trivially we have $\|1_A\|_{L^{4/3}(G)} \leq \alpha^{3/4}$. On the other hand.

$$\langle \widehat{1_A}1_S, \widehat{1_A}\rangle_{\ell^2(\widehat{G})} \geq \delta^2\alpha^2|S|,$$

from which the result follows on rearranging. ∎

https://doi.org/10.4153/CMB-2011-165-0 Published online by Cambridge University Press

Shkredov [18] extended the above in two ways: first, by considering different powers in Hölder's inequality he got a lower bound on the $2k$-th energy (that is , $\|\widehat{1_S}\|_{L^{2k}(G)}^{2k}$); second, by dyadically decomposing the range of $|\widehat{1_A}|$, he improved the δ^8 to $\Omega(\delta^4)$.

It is easy to see from Parseval's inequality that S has size at most $\delta^{-2}\alpha^{-1}$; the reader should think of the situation when the size is close to this, δ is fixed but possibly small, and $\alpha \to 0$. Then $|S|$ tends to infinity in size and $E(S) \geq \delta^{O(1)}|S|^3$; it has large additive energy.

In the situation described above we have the celebrated Balog–Szemerédi–Gowers theorem (see [1,5]) which we now recall.

Theorem 6.2 *Suppose that G is an abelian group and $A \subset G$ has $E(A) \geq c|A|^3$. Then there is a subset $A' \subset A$ such that $|A'| = \Omega(c^{O(1)}|A|)$ and $|A' + A'| = O(c^{-O(1)}|A'|)$.*

Gowers [5] made the important observation that this could then naturally be combined with a Freĭman-type theorem in many applications, and our present work is another such example.

Finally, we need to record how we pass from large Fourier coefficients to increased density on a subspace when $G := \mathbb{F}^n$. The key to the simplicity of this in the finite field model is the following easy calculation. Suppose that $W \leq \widehat{G}$. Then

$$\widehat{\mathbb{P}_{W^\perp}}(\gamma) = \begin{cases} 1 & \text{if } \gamma \in W, \\ 0 & \text{otherwise.} \end{cases}$$

We are now in a position to record the Roth–Meshulam increment lemma.

Lemma 6.3 ($\ell^\infty(\widehat{G})$-increment lemma) *Suppose that $\mathbb{F}$ is a finite field, $G := \mathbb{F}^n$, $A \subset G$ has density α, and $\sup_{\gamma \neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)| \geq \epsilon\alpha$. Then there is a subspace $V \leq G$ wth $\operatorname{cod} V = 1$ and $\|1_A * \mathbb{P}_V\|_{L^\infty(G)} \geq \alpha(1 + \epsilon/2)$.*

Proof We do the obvious thing and define $V = \{\gamma\}^\perp$ so that

$$((1_A - \alpha) * \mathbb{P}_V)^\wedge(\gamma) = \widehat{1_A}(\gamma),$$

whence by the Hausdorff–Young inequality we have $\|(1_A - \alpha) * \mathbb{P}_V\|_{L^1(G)} \geq \epsilon\alpha$. On the other hand,

$$\int ((1_A - \alpha) * \mathbb{P}_V) d\mathbb{P}_G = 0,$$

whence $2\sup_{x \in G} (1_A - \alpha) * \mathbb{P}_V(x) \geq \epsilon\alpha$. The result follows on dividing by 2 and adding α to both sides. ∎

It is also possible to get a very large correlation with a subspace if one has a large $\ell^2(\widehat{G})$ mass of $\widehat{1_A}$. This is an idea introduced by Szemerédi in [20] and encoded in the model setting by the following lemma.

Lemma 6.4 ($\ell^2(\widehat{G})$-increment lemma) *Suppose that $\mathbb{F}$ is a finite field, $G := \mathbb{F}^n$, $A \subset G$ has density $\alpha > 0$, and $W \leq \widehat{G}$ is such that $\sum_{\gamma \in W} |\widehat{1_A}(\gamma)|^2 \geq \epsilon\alpha$. Then there is a subspace $V \leq G$ wth $\operatorname{cod} V = \dim W$ and $\|1_A * \mathbb{P}_V\|_{L^\infty(G)} \geq \epsilon$.*

https://doi.org/10.4153/CMB-2011-165-0 Published online by Cambridge University Press

Proof We do the obvious thing and define $V = W^{\perp}$ and so $(1_A * \mathbb{P}_V)^{\wedge}(\gamma) = \widehat{1_A}(\gamma)$ whenever $\gamma \in W$. Thus by Parseval's theorem and the hypothesis we have that

$$\int (1_A * \mathbb{P}_V)^2 \, d\mathbb{P}_G = \sum_{\gamma \in W} |\widehat{1_A}(\gamma)|^2 \geq \epsilon\alpha.$$

The result then follows by Hölder's inequality and the fact that

$$\int 1_A * \mathbb{P}_V \, d\mathbb{P}_G = \alpha,$$

on dividing by α. ∎

7 Proof of Theorem 1.4

The argument follows the usual iterative method pioneered by Roth [12] and exposed as particularly elegant in $\mathbb{F}_3^n$ by Meshulam in [11]. The key quantity of interest is the number of solutions to the given equation.

Suppose that $\mathbb{F}$ is a finite field, $G := \mathbb{F}^n$, $c \in (\mathbb{F}^*)^r$, and $A \subset G$. Then we write

$$\Lambda_c(A) := \int 1_{-c_1.A}(c_2.x_2 + \cdots + c_r.x_r) \prod_{i=2}^{r} 1_A(x_i) d\mathbb{P}_G(x_2) \cdots d\mathbb{P}_G(x_r).$$

Using the inversion formula, we may put

$$1_A(x_i) = \sum_{\gamma_i \in \widehat{G}} \widehat{1_A}(\gamma_i)\gamma_i(x_i) \quad \text{for all } x_i \in G.$$

We insert this expression for 1_A into each instance in $\Lambda_c(A)$, and via the orthogonality relations get that $c_i.\gamma_i = c_j.\gamma_j =: \gamma$ for all i, j. This gives a Fourier expression for $\Lambda_c(A)$ as follows:

$$\Lambda_c(A) = \sum_{\gamma \in \widehat{G}} \prod_{i=1}^{r} \widehat{1_A}(c_i^{-1}.\gamma). \tag{7.1}$$

Of course, we shall use the above Fourier expression in the following driving lemma for our argument.

Lemma 7.1 (Iteration lemma) *There is a non-negative valued function ν with $\nu(r) = \Omega(r^{-1}\log r)$ for r greater than some absolute constant such that if $\mathbb{F}$ is a finite field, $G := \mathbb{F}^n$, $c_1, \ldots, c_r \in \mathbb{F}^*$, and $A \subset G$ has density $\alpha > 0$, then at least one of the following is true:*

(i) *(Many solutions) we have the lower bound $\Lambda_c(A) \geq \alpha^r/2$;*

(ii) *(Small correlation with low co-dimension subspace) there is a subspace $V \leq G$ with $\operatorname{cod} V = 1$ such that $\|1_A * \mathbb{P}_V\|_{L^\infty(G)} \geq \alpha(1 + \Omega(\alpha^{(1-\nu(r))/(r-2)}))$;*

https://doi.org/10.4153/CMB-2011-165-0 Published online by Cambridge University Press

(iii) *(Large correlation with a large co-dimension subspace) there is a subspace* $V \leq G$ *with* $\operatorname{cod} V = O_r(\alpha^{-1/2(r-2)})$ *such that* $\|1_A * \mathbb{P}_V\|_{L^\infty(G)} \geq \Omega(\alpha^{1/2})$.

Proof If we are in the first case of the lemma we are done; assume not, so that from (7.1) we get

$$\Big|\sum_{\gamma\in\widehat{G}}\prod_{i=1}^{r}\widehat{1_A}(c_i^{-1}.\gamma)\Big| \leq \alpha^r/2.$$

As usual we extract the trivial mode: we have $\widehat{1_A}(\gamma) = \alpha$, whence

$$\Big|\alpha^r + \sum_{\gamma\neq 0_{\widehat{G}}}\prod_{i=1}^{r}\widehat{1_A}(c_i^{-1}.\gamma)\Big| \leq \alpha^r/2.$$

Thus, by the triangle inequality we get

$$\sum_{\gamma\neq 0_{\widehat{G}}}\prod_{i=1}^{r}|\widehat{1_A}(c_i^{-1}.\gamma)| \geq \alpha^r/2.$$

We apply the r-function version of Hölder's inequality to this to get that

$$\prod_{i=1}^{r}\Big(\sum_{\gamma\neq 0_{\widehat{G}}}|\widehat{1_A}(c_i^{-1}.\gamma)|^r\Big)^{1/r} \geq \alpha^2/2.$$

Now each $c_i \in \mathbb{F}^*$, whence $c_i^{-1}.(\widehat{G}\setminus\{0_{\widehat{G}}\}) = (\widehat{G}\setminus\{0_{\widehat{G}}\})$ and

$$\sum_{\gamma\neq 0_{\widehat{G}}}|\widehat{1_A}(c_i^{-1}.\gamma)|^r = \sum_{\gamma\neq 0_{\widehat{G}}}|\widehat{1_A}(\gamma)|^r \quad \text{for all } 1\leq i\leq r.$$

Inserting this back into our inequality we see that each factor is the same and we get that

$$\sum_{\gamma\neq 0_{\widehat{G}}}|\widehat{1_A}(\gamma)|^r \geq \alpha^r/2. \tag{7.2}$$

This inequality will let us analyse the large spectrum of 1_A: write

$$\epsilon := \alpha^{1/(r-2)}/4 \quad \text{and} \quad S := \operatorname{Spec}_\epsilon(1_A)\setminus\{0_{\widehat{G}}\}.$$

It follows from the definition of the spectrum and Parseval's theorem that

$$\sum_{\gamma\notin\operatorname{Spec}_\epsilon(1_A)}|\widehat{1_A}(\gamma)|^r \leq (\epsilon\alpha)^{r-2}\sum_{\gamma\in\widehat{G}}|\widehat{1_A}(\gamma)|^2 = \alpha.4^{-(r-2)}.\alpha^{r-2}.\alpha \leq \alpha^r/4,$$

since $r\geq 3$. Thus, by the triangle inequality and (7.2) we have

$$\sum_{\gamma\in S}|\widehat{1_A}(\gamma)|^r \geq \alpha^r/2 - \sum_{\gamma\notin\operatorname{Spec}_\epsilon(1_A)}|\widehat{1_A}(\gamma)|^r \geq \alpha^r/4. \tag{7.3}$$

https://doi.org/10.4153/CMB-2011-165-0 Published online by Cambridge University Press

Now suppose that $M \geq 1$ is a real to be optimised later. If

$$\sup_{\gamma \neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)| \geq \alpha^{-M/(r-2)r} \epsilon \alpha,$$

then we shall be in the second case of the lemma by Lemma 6.3 once we optimise for M. To proceed we therefore assume not, so that

$$\sup_{\gamma \neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)| \leq \alpha^{-M/(r-2)r} \epsilon \alpha.$$

Inserting this into (7.3) we see that $|S| \,.\, (\alpha^{-M/(r-2)r} \epsilon \alpha)^r \geq \alpha^r/4$, which can be rearranged to give

$$|S| \geq \alpha^r \,.\, 4^{-1} \,.\, \alpha^{-r} \,.\, 4^r \,.\, \alpha^{-r/(r-2)} \,.\, \alpha^{M/(r-2)} = 4^{r-1} \alpha^{(M-2)/(r-2)} \,.\, \alpha^{-1}.$$

Now by Proposition 6.1 S has large additive energy. Specifically

$$\begin{aligned} E(S) &\geq \epsilon^8 \alpha |S|^4 \geq \alpha^{8/(r-2)} 4^{-8} 4^{r-1} \alpha^{(M-2)/(r-2)} |S|^3 \\ &= \alpha^{(M+6)/(r-2)} 4^{r-9} |S|^3 = \Omega(\alpha^{O(M/r)}). \end{aligned}$$

It follows by the Balog–Szemerédi–Gowers theorem that there is some set $S' \subset S$ such that

$$|S'| \geq \Omega(\alpha^{O(M/r)})|S| \quad \text{and} \quad |S' + S'| \leq O(\alpha^{-O(M/r)})|S'|.$$

Now apply Theorem 1.3 with some parameter η to get a set $\mathcal{L}$ such that

$$|S' \cap \mathrm{Span}(\mathcal{L})| \geq \Omega(\alpha)^{O(\exp(O(\eta^{-1}))M/r)}|S'| \quad \text{and} \quad |\mathcal{L}| = O(\alpha^{-O(\eta M/r)} \log |S'|).$$

This means that we may pick $\eta = \Omega(1/M)$ such that

$$|S' \cap \mathrm{Span}(\mathcal{L})| \geq \alpha^{O(\exp(O(M))/r}|S'| \quad \text{and} \quad |\mathcal{L}| = O(\alpha^{-1/4(r-2)} \log |S'|).$$

Write W for the subspace generated by $\mathcal{L}$ and note that by the lower bound on $|S'|$ we thus have

$$\sum_{\gamma \in W \setminus \{0_{\widehat{G}}\}} |\widehat{1_A}(\gamma)|^2 \geq (\epsilon\alpha)^2 |S' \cap \mathrm{Span}(\mathcal{L})| = \Omega(\alpha^{1+O(\exp(O(M)))/r}).$$

It follows that if $r \geq C$ for some absolute constant $C > 0$, then we may pick $M = \Omega(\log r)$ in a way independent of A and c such that

$$\sum_{\gamma \in W \setminus \{0_{\widehat{G}}\}} |\widehat{1_A}(\gamma)|^2 \geq \Omega(\alpha^{1+1/2}).$$

This is how the function ν is determined if $r \geq C$: $\nu(r) = M/r$. On the other hand, by Parseval's theorem we have that $|S'| \leq |S| \leq (\epsilon\alpha)^{-2}.\alpha \leq O(\alpha^{-O(1)})$, whence $\dim W = O(\alpha^{1/4(r-2)} \log |S'|) = O(\alpha^{1/4(r-2)} \log \alpha^{-1})$.

We now apply Lemma 6.4 to get the third conclusion of the lemma. If $r \leq C$, then $\nu(r) = 0$ and we simply note that S is, in any case, non-empty and apply Lemma 6.3 to any character in this set to get the conclusion. ∎

https://doi.org/10.4153/CMB-2011-165-0 Published online by Cambridge University Press

With the above lemma we are ready to apply the usual iterative method.

Proof of Theorem 1.5 We proceed by creating a sequence of subspaces $G =: V_0 \geq V_1 \geq \cdots \geq V_k$ and sets $A_i \subset V_i$ with density α_i such that

$$\Lambda_c(A) \geq |G : V_i|^{r-1}\Lambda_c(A_i) \text{ and } \alpha_i \geq \alpha_0. \tag{7.4}$$

We begin by setting $A_0 := A$ and suppose that we have defined A_i and V_i. We apply Lemma 7.1. If we are in the first or third cases, we shall terminate. If we are in the second case, we have some $x \in V_i$ and $V_{i+1} \leq V_i$ of codimension 1 such that

$$\int 1_{x+A_i}\, d\mathbb{P}_{V_{i+1}} \geq \alpha_i(1 + \alpha_i^{(1-\nu(r))/(r-2)}).$$

We set $A_{i+1} := (x + A_i) \cap V_{i+1}$. Since $c_1 + \cdots + c_r = 0$ we certainly have (7.4). However, we also have that $\alpha_{i+1} \geq \alpha_i(1 + \Omega(\alpha_i^{(1-\nu(r))/(r-2)}))$. It follows that after $I = O(\alpha_i^{-(1-\nu(r))/(r-2)}))$ iterations we have $\alpha_{i+I(i)} \geq 2\alpha_i$. However, since the density is always at most 1 the iteration must terminate within

$$O(\alpha_0^{-(1-\nu(r))/(r-2)})) + O((2\alpha_0)^{-(1-\nu(r))/(r-2)})) + O((4\alpha_0)^{-(1-\nu(r))/(r-2)})) + \cdots$$

steps. Summing the geometric progression, we see that we are either in the first or third cases of the lemma within $O_r(\alpha^{-(1-\nu(r))/(r-2)})$ iterations. In the first case we see trivially that

$$\begin{aligned}\Lambda_c(A) \geq |G : V_i|^{r-1}\Lambda_c(A_i) &\geq |G : V_i|^{r-1}\alpha_i^r/2\\ &\geq \exp(-O_{|\mathbb{F}|,r}(\alpha^{-(1-\nu(r))/(r-2)})).\end{aligned}$$

On the other hand, since A contains no solutions to $c_1.x_1 + \cdots + c_r.x_r = 0$ with $x_1, \ldots, x_r \in A$ pair-wise distinct we see that $\Lambda_c(A) = O_r(|G|^{-1})$ and it follows that

$$\alpha = O_{|\mathbb{F}|,r}(n^{(r-2)/(1-\nu(r))}). \tag{7.5}$$

Finally, if we terminate in the third case of the iteration lemma, then we get a space $V \leq V_i$ such that

$$|G : V| = |G : V_i|.|V_i : V| = O_{|\mathbb{F}|,r}(\alpha^{-(1-\nu(r))/(r-2)})$$

and the density of A on V is $\Omega(\alpha^{1/2})$. If $\log|G : V| \geq \log|G|/2$, then it follows that we have the bound (7.5) again; otherwise apply Theorem 1.4 to see that

$$\alpha = O_{|\mathbb{F}|,r}(n^{2(r-2)}).$$

The result follows in view of the definition of ν. ∎

Acknowledgements The author should like to thank Ben Green and Terry Tao for may useful conversations, Tomasz Schoen for bringing the paper [17] to the author's attention, Ilya Shkredov for remarks concerning Theorem 1.3, and two anonymous referees for many useful remarks concerning generalisations and exposition.

References

[1] A. Balog and E. Szemerédi, *A statistical theorem of set addition.* Combinatorica **14**(1994), no. 3, 263–268. http://dx.doi.org/10.1007/BF01212974

[2] M.-C. Chang, *A polynomial bound in Freĭman's theorem.* Duke Math. J. **113**(2002), no. 3, 399–419. http://dx.doi.org/10.1215/S0012-7094-02-11331-3

[3] E. S. Croot and V. F. Lev, *Open problems in additive combinatorics.* In: Additive Combinatorics. CRM Proc. Lecture Notes 43. American Mathematical Societh, Providence, RI, 2007, pp. 207–233.

[4] G. A. Freĭman, *Foundations of a Structural Theory of Set Addition*. Translations of Mathematical Monographs 37. American Mathematical Society, Providence, RI, 1973.

[5] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four.* Geom. Funct. Anal. **8**(1998), no. 3, 529–551. http://dx.doi.org/10.1007/s000390050065

[6] B. J. Green and I. Z. Ruzsa, *Freĭman's theorem in an arbitrary abelian group.* J. Lond. Math. Soc. **75**(2007), no. 1, 163–175. http://dx.doi.org/10.1112/jlms/jdl021

[7] B. J. Green, *Finite field models in additive combinatorics.* In: Surveys in Combinatorics 2005. London Math. Soc. Lecture Note Ser. 327. Cambridge Univ. Press, Cambridge, 2005, pp. 1–27.

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

[9] Y.-R. Liu and C. V. Spencer, *A generalization of Meshulam's theorem on subsets of finite abelian groups with no 3-term arithmetic progression.* Des. Codes Cryptogr. **52**(2009), no. 1, 83–91. http://dx.doi.org/10.1007/s10623-009-9268-0

[10] Y.-R. Liu, C. V. Spencer, and X. Zhao, *A generalization of Meshulam's theorem on subsets of finite abelian groups with no 3-term arithmetic progression. II.* European J. Combin. **32**(2011), no. 2, 258–264. http://dx.doi.org/10.1016/j.ejc.2010.09.008

[11] R. Meshulam. *On subsets of finite abelian groups with no* 3*-term arithmetic progressions.* J. Combin. Theory Ser. A **71**(1995), no. 1, 168–172. http://dx.doi.org/10.1016/0097-3165(95)90024-1

[12] K. F. Roth, *On certain sets of integers.* J. London Math. Soc. **28**(1953), 104–109. http://dx.doi.org/10.1112/jlms/s1-28.1.104

[13] W. Rudin, *Fourier Analysis on Groups*. Reprint of the 1962 original. John Wiley & Sons, New York, 1990.

[14] I. Z. Ruzsa, *Solving a linear equation in a set of integers. I.* Acta Arith. **65**(1993), no. 3, 259–282.

[15] ———, *Generalized arithmetical progressions and sumsets.* Acta Math. Hungar. **65**(1994), no. 4, 379–388. http://dx.doi.org/10.1007/BF01876039

[16] T. Sanders, *On a non-abelian Balog–Szemerédi-type lemma.* J. Aust. Math. Soc. **89**(2010), no.1, 127–132.

[17] T. Schoen, *Near optimal bounds in Freĭman's theorem.* Preprint, 2010.

[18] I. D. Shkredov, *On sets of large trigonometric sums.* Izv. Ross. Akad. Nauk Ser. Mat. **72**(2008), no. 1, 161–182.

[19] ———, *On sets with small doubling.* Mat. Zametki **84**(2008), no. 6, 927–947.

[20] E. Szemerédi, *Integer sets containing no arithmetic progressions.* Acta Math. Hungar. **56**(1990), no. 1-2, 155–158. http://dx.doi.org/10.1007/BF01903717

[21] T. C. Tao, *Structure and Randomness. Pages from Year One of a Mathematical Blog.*. American Mathematical Society, Providence, RI, 2008.

[22] T. C. Tao and H. V. Vu, *Additive Combinatorics.* Cambridge Studies in Advanced Mathematics 105. Cambridge University Press, Cambridge, 2006.

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Cambridge CB3 0WB, UK
e-mail: t.sanders@dpmms.cam.ac.uk