ANALYSIS & PDE

Volume 2 No. 2 2009

TOM SANDERS

ROTH'S THEOREM IN $\mathbb{Z}_4^n$

mathematical sciences publishers

ANALYSIS AND PDE
Vol. 2, No. 2, 2009

ROTH'S THEOREM IN $\mathbb{Z}_4^n$

TOM SANDERS

We show that if $A \subset \mathbb{Z}_4^n$ contains no three-term arithmetic progressions in which all the elements are distinct then $|A| = o(4^n/n)$.

1. Introduction

Let G be a finite abelian group. A three-term arithmetic progression in G is a triple $(x, x+d, x+2d)$ with $x, d \in G$; a proper progression is one in which all the elements are different, that is, $2d \neq 0_G$.

Roth [1953] famously proved that any subset of $\mathbb{Z}/N\mathbb{Z}$ of sufficiently large density contains a proper three-term arithmetic progression, a result which was generalised by Meshulam:

Theorem 1.1 [Meshulam 1995]. *Suppose that G is a finite abelian group of odd order and $A \subset G$ contains no proper three-term arithmetic progressions. Then*

$$|A| = O\big(|G|/\log^{\Omega(1)}|G|\big).$$

An explicit value for the $\Omega(1)$ constant can be read out of the proof, and it seems that in light of [Bourgain 2008] (itself improving on [Bourgain 1999; Szemerédi 1990; Heath-Brown 1987]) one could probably take any constant strictly less than $2/3$. While this appears to be the limit in general, for certain groups one can do better. Indeed, for $\mathbb{Z}_3^n$ (or, more generally, any abelian group of odd order and bounded exponent), Roth's original argument simplifies considerably to give the following result, which is qualitatively due to Brown and Buhler [1984].

Theorem 1.2 Roth–Meshulam. *Suppose that $G = \mathbb{Z}_3^n$ and $A \subset G$ contains no proper three-term arithmetic progressions. Then*

$$|A| = O\big(|G|/\log|G|\big).$$

The question of what the true bounds on $|A|$ are arises in many different studies [Frankl et al. 1987; Yekhanin and Dumer 2004; Edel 2004; Edel et al. 2007] and improving the bound is a well known open problem, as reported in [Green 2005; Croot and Lev 2007; Tao 2008, Section 3.1]; the closest anyone has come is in [Croot 2007; 2008]. While we are not able to make progress on this question, it is the purpose of this paper to show an improvement for a different class of groups.

It was quite natural in Theorem 1.1 to insist that G be of odd order: in the group $\mathbb{Z}_2^n$ every arithmetic progression is easily seen to be of the form (x, y, x), so no set contains a proper progression. Not all groups of even order are as trivial as $\mathbb{Z}_2^n$ and, as part of a more general corpus of results, Lev resolved the question of which abelian groups Meshulam's theorem could be extended to.

MSC2000: 42A05.

Keywords: Roth–Meshulam, cap set problem, Fourier, Freĭman, Balog–Szemerédi, characteristic 2, $\mathbb{Z}_4^n$, three-term arithmetic progressions.

Theorem 1.3 [Lev 2004]. *Suppose that $G = \mathbb{Z}_4^n$ and $A \subset G$ contains no proper three-term arithmetic progressions. Then*

$$|A| = O\big(|G|/\log|G|\big).$$

This special case of Lev's work follows rather easily from the method used to prove the Roth–Meshulam theorem coupled with a positivity observation. At considerable further expense we are able to establish a minor improvement:

Theorem 1.4. *Suppose that $G = \mathbb{Z}_4^n$ and $A \subset G$ contains no proper three-term arithmetic progressions. Then*

$$|A| = O\big(|G|/\log|G|\log\log^{\Omega(1)}|G|\big).$$

The requirement that *all* the elements of our progressions be distinct is essential in our work. It is easy to see by the Cauchy–Schwarz inequality that any set $A \subset G := \mathbb{Z}_4^n$ has at least $\alpha^2|G|^{3/2}$ progressions. It follows that if $\alpha^2|G|^{3/2} > |G|$ then A contains a progression in which not all the elements are the same; however, this may well be a degenerate one of the form (x, y, x).

The paper now splits as follows. In Section 2, we record the necessary information about the Fourier transform. In Section 3 and Section 4, we outline our approach to counting progressions and compare it with the Roth–Meshulam–Lev method to give some indication of where we are able to make gains. In Section 5 we define the notion of a family which we shall work with for the bulk of the paper and the proof of Theorem 1.4, which are in Sections 6–11. We close in Section 12 with a conjecture and a discussion of lower bounds.

2. The Fourier transform

We shall make considerable use of the Fourier transform, for which the classic [Rudin 1962] serves as the standard reference. Having said this, the style of our work has more in common with [Tao and Vu 2006], which is also to be recommended.

Suppose that G is a finite abelian group. $\widehat{G}$ denotes the *dual group* of G, that is the group of homomorphisms $\gamma : G \to S^1$, where $S^1 := \{z \in \mathbb{C} : |z| = 1\}$. G is endowed with a natural Haar probability measure, denoted $\mathbb{P}_G$, assigning mass $|G|^{-1}$ to each element of G; we denote integration against $\mathbb{P}_G$ by $\mathbb{E}_{x\in G}$ and, in general, $\mathbb{E}_{x\in S}$ corresponds to integration against the probability measure $\mathbb{P}_S$ assigning mass $|S|^{-1}$ to each $s \in S$.

For $p \in [1, \infty]$ we define the spaces $L^p(G)$ and $\ell^p(G)$ to be the vector space of functions $f : G \to \mathbb{C}$ endowed with the norms

$$\|f\|_{L^p(G)} := \big(\mathbb{E}_{x\in G}|f(x)|^p\big)^{1/p} \quad \text{and} \quad \|f\|_{\ell^p(G)} := \bigg(\sum_{x\in G}|f(x)|^p\bigg)^{1/p},$$

with the usual conventions when $p = \infty$. As vector spaces these are all the same (since G is finite), although the norms are different. A specific consequence of this normalisation is that

$$\langle f, g\rangle_{L^2(G)} = \mathbb{E}_{x\in G} f(x)\overline{g(x)} \quad \text{and} \quad \langle f, g\rangle_{\ell^2(G)} = \sum_{x\in G} f(x)\overline{g(x)}.$$

We define the Fourier transform in the usual way, mapping a function $f \in L^1(G)$ to $\widehat{f} \in \ell^\infty(\widehat{G})$, where

$$\widehat{f}(\gamma) := \mathbb{E}_{x\in G} f(x)\overline{\gamma(x)} = \frac{1}{|G|}\sum_{x\in G} f(x)\overline{\gamma(x)}.$$

The significance of the Fourier transform is, in no small part, determined by the effect it has on convolution: recall that if $f, g \in L^1(G)$ then their convolution $f * g$ is defined by

$$(f * g)(x) := \mathbb{E}_{x\in G} f(x)g(y-x).$$

The Fourier transform functions as an algebra isomorphism from $L^1(G)$ under convolution to $\ell^\infty(\widehat{G})$ under pointwise multiplication: $\widehat{f * g} = \widehat{f}\,\widehat{g}$.

(Note that both convolution and the Fourier transform are used on different groups at the same time through this work, and although it is always made clear, the reader should be alert to this.)

We are particularly interested in finite (abelian) groups of exponent 2, all of which are isomorphic to $\mathbb{Z}_2^n$ for some n; to avoid introducing an unnecessary parameter we shall refer to them in the former terms. On these groups the characters correspond to maps $x \mapsto (-1)^{r\cdot x}$, where $r \cdot x$ is the usual bilinear form on $\mathbb{Z}_2^n$ considered as a vector space over $\mathbb{F}_2$.

3. Counting progressions and analytic statement of results

It has been observed in many places that one may estimate the size of the largest subset of an abelian group not containing a three-term arithmetic progression by establishing a lower bound on the number of three-term arithmetic progressions. It should, therefore, come as little surprise that we are interested in the quantity

$$\Lambda(A) := \mathbb{E}_{x,d\in G} 1_A(x)\,1_A(x+d)\,1_A(x+2d).$$

which counts three-term arithmetic progressions: specifically $\Lambda(A)|G|^2$ is the number of three-term arithmetic progressions in A.

Denoting by $T(G)$ the number of trivial (that is, nonproper) three-term arithmetic progressions in G, we see that if $\Lambda(A)|G|^2 > T(G)$ then we must have a nontrivial three-term arithmetic progression. This perspective is, perhaps, inspired by an equivalence established in [Varnavides 1959], but we shall not dwell on this relationship here.

Meshulam's theorem is a simple corollary of the following result.

Theorem 3.1. *Suppose that G is a finite abelian group of odd order and $A \subset G$ has density $\alpha > 0$. Then*

$$\Lambda(A) \geqslant \exp(-\alpha^{-O(1)}).$$

To see how Meshulam's theorem follows, note that if G is of odd order then $(x, x+d, x+2d)$ is a proper progression if and only if $d \neq 0_G$. Thus $T(G) = |G|$ and so if $\Lambda(A)|G|^2 > |G|$ then A contains a proper progression; the result follows on inserting the bound for $\Lambda(A)$ from the theorem and rearranging.

Lev effectively removed the odd-order condition from Theorem 3.1:

Theorem 3.2 [Lev 2004]. *Suppose that G is a finite abelian group and $A \subset G$ has density $\alpha > 0$. Then*

$$\Lambda(A) \geqslant \exp(-\alpha^{-O(1)}).$$

In general abelian groups $T(G)$ may be comparable to $|G|^2$ which is why we are not able to conclude Meshulam's theorem without the odd order condition. Indeed, as noted before it is not always true.

It is instructive to consider two examples. First, in $G=\mathbb{Z}_2^n$ one sees that $T(G)=|G|^2$ — all progressions are trivial — so although we have many progressions,[1] none are proper.

Second, the group $G=\mathbb{Z}_4^n$ has $T(G)=|G|^{3/2}+O(|G|)$: any trivial progression (x,y,z) with $x+z=2y$ has $x=z$, $x=y$ or $y=z$. In the first case this implies that $x-y\in\{x'\in G:2x'=0_G\}$; in the second and third cases this implies that all three elements are equal. Thus, in the first case we have $|G|\left|\{x'\in G:2x'=0_G\}\right|$ progressions and in the second and third $|G|$ each. This leads to the claimed bound which in turn allows us to establish Meshulam's theorem for $\mathbb{Z}_4^n$.

In this particular case, however, one may proceed directly along the lines of the proof of the Roth–Meshulam theorem (coupled with the aforementioned positivity observation) to establish a stronger bound than in Theorem 3.2.

Theorem 3.3. *Suppose that $G=\mathbb{Z}_4^n$ and $A\subset G$ has density $\alpha>0$. Then*

$$\Lambda(A)\geqslant\exp(-O(\alpha^{-1})).$$

On arranging α large enough so that $\Lambda(A)|G|^2>|G|^{3/2}+O(|G|)$ is guaranteed by the above theorem we get Theorem 1.3; the main result of this paper is the following refinement of Theorem 3.3 which by a similar arrangement implies Theorem 1.4.

Theorem 3.4. *Suppose that $G=\mathbb{Z}_4^n$ and $A\subset G$ has density $\alpha>0$. Then*

$$\Lambda(A)\geqslant\exp\bigl(-O(\alpha^{-1}\log^{-1/6}\alpha^{-1}\log\log^{5/3}\alpha^{-1})\bigr).$$

4. Outline of the proof

Our work is strongly influenced by the original Roth–Meshulam–Lev argument; to explain our extra purchase we shall recall a sketch of this. There are basically three ingredients. First, one has a lemma passing from a large Fourier coefficient to increased density on a subgroup.

Lemma 4.1. *Suppose that G is a group of bounded exponent, that $A\subset G$ has density $\alpha>0$, and that $\sup_{\gamma\neq 0_{\widehat{G}}}|\widehat{1_A}(\gamma)|\geqslant\epsilon\alpha$. Then there is a subgroup $G'\leqslant G$ of bounded index such that $\|1_A*\mathbb{P}_{G'}\|_{L^\infty(G)}\geqslant\alpha+\Omega(\alpha\epsilon)$.*

The proof of this is easy and we shall use some similar results in Section 6; we make no improvement on this ingredient and, indeed, the lemma is in many ways best possible.

The core of the argument is the following lemma and it is here that we shall do better. The lemma expresses the fact that either a set A is "uniform" having about the right number of three-term arithmetic progressions or else it has increased density on a subgroup of bounded index.

Lemma 4.2. *Suppose that G is a group of bounded exponent and $A\subset G$ has density $\alpha>0$. Then either $\Lambda(A)=\Omega(\alpha^3)$ or there is a subgroup $G'\leqslant G$ of bounded index such that $\|1_A*\mathbb{P}_{G'}\|_{L^\infty(G)}\geqslant\alpha+\Omega(\alpha^2)$.*

[1] It is easy to see this without Theorem 3.2: $A\subset\mathbb{Z}_2^n$ clearly contains $|A|^2$ progressions since every pair $(x,y)\in A^2$ generates a triple (x,y,x) which is a three-term arithmetic progression in $\mathbb{Z}_2^n$.

Sketch of proof. By the usual application of the inversion formula one has

$$\Lambda(A) = \sum_{\gamma \in \widehat{G}} \widehat{1_A}(\gamma)^2 \widehat{1_A}(2\gamma).$$

We write $H := \{\gamma \in \widehat{G} : 2\gamma = 0_{\widehat{G}}\}$, so that

$$\Lambda(A) = \alpha \sum_{\gamma \in H} \widehat{1_A}(\gamma)^2 + O\big(\sup_{\gamma \neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)|\alpha\big)$$

by Parseval's theorem. Note that if $\gamma \in H$ then γ is a real character, so $|\widehat{1_A}(\gamma)|^2 = \widehat{1_A}(\gamma)^2$; thus we certainly have

$$\sum_{\gamma \in H} \widehat{1_A}(\gamma)^2 = \sum_{\gamma \in H} |\widehat{1_A}(\gamma)|^2 \geqslant |\widehat{1_A}(0_{\widehat{G}})|^2 = \alpha^2.$$

This is the previously mentioned positivity observation of Lev. It follows that either $\Lambda(A) \geqslant \alpha^3/2$ and we are done or $\sup_{\gamma \neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)| = \Omega(\alpha^2)$ in which case we apply Lemma 4.1 and are done. □

Lemma 4.2 can be iterated to get Theorem 3.3, and again we shall use essentially the same style of iteration in Section 11 to prove Theorem 3.4.

Sketch of proof of Theorem 3.3. We apply the preceding lemma repeatedly, incrementing the density at each stage that we are in the second case of the lemma and terminating if we are in the first case.

At each stage we have $\alpha \mapsto \alpha + \Omega(\alpha^2)$. Thus, after $O(\alpha^{-1})$ iterations the density will have doubled. Since density cannot increase above 1, the iteration terminates after

$$O(\alpha^{-1}) + O((2\alpha)^{-1}) + O((4\alpha)^{-1}) + \cdots = O(\alpha^{-1})$$

steps.

When the iteration terminates we have some group $G' \leqslant G$ with $|G : G'| = \exp(O(\alpha^{-1}))$ such that $\Lambda(A) = \Omega(\alpha^3 |G : G'|^2) = \exp(O(\alpha^{-1}))$. The result follows. □

We shall exploit some of the additional structure of $\mathbb{Z}_4^n$ to effectively improve Lemma 4.2 and thereby gain our strengthening of the Roth–Meshulam–Lev argument.

In $G = \mathbb{Z}_4^n$ a triple (x, y, z) with $x + z = 2y$ must have x and z in the same coset of $\operatorname{im} 2$, where 2 denotes the map $x \mapsto 2x$. Thus it is natural to partition A by the cosets of $\operatorname{im} 2$, because when counting three-term arithmetic progressions we only ever need to consider sums $x + z$ with x and z in the same coset.

Since $\operatorname{im} 2 = \ker 2$ we shall index the elements of this partition of A by elements of $\ker 2$ and, for simplicity later, translate them all so that they lie in $\operatorname{im} 2$. Specifically, then, we proceed as follows.

Suppose that G is a finite abelian group and $A \subset G$. Define

$$f_A : \operatorname{im} 2 \to [0, 1]; u \mapsto \mathbb{E}_{z \in G : 2z = u} 1_A(z),$$

and note that

$$\begin{aligned}\Lambda(A) &= \mathbb{E}_{x,d \in G} 1_A(x) 1_A(x + 2d) \mathbb{E}_{d' \in G : 2d' = 2d} 1_A(x + d') \\ &= \mathbb{E}_{x,d \in G} 1_A(x) 1_A(x + 2d) f_A(2(x + d)) \\ &= \mathbb{E}_{x,u \in G} 1_A(x) 1_A(2u - x) f_A(2u).\end{aligned}$$

Now, for each $y \in \operatorname{im} 2$ let $t_y \in G$ be such that $2t_y = y$, and let $A_y := A \cap (t_y + \ker 2) - t_y \subset \ker 2$. Furthermore, for each $y \in \operatorname{im} 2$ let τ_y be "translation by y", defined by

$$\tau_y : L^1(\operatorname{im} 2) \to L^1(\operatorname{im} 2);\ f \mapsto (x \mapsto f(x+y)).$$

In this notation we have

$$\begin{aligned}\Lambda(A) &= \mathbb{E}_{y\in\operatorname{im}2}\mathbb{E}_{x\in t_y+\ker 2, v\in\operatorname{im}2} 1_{A_y}(x-t_y)1_{A_y}(v-x-t_y)f_A(v)\\ &= \mathbb{E}_{y\in\operatorname{im}2}\mathbb{E}_{z\in\ker 2, v\in\operatorname{im}2} 1_{A_y}(z)1_{A_y}(v-y-z)f_A(v)\\ &= \mathbb{E}_{y\in\operatorname{im}2}\langle \tau_y(1_{A_y} * 1_{A_y}),\, f_A\rangle_{L^2(\operatorname{im}2)}. \end{aligned} \tag{4-1}$$

Note that $*$ here denotes convolution on $\ker 2$, since this is where the sets A_y have been arranged to live. In $\mathbb{Z}_4^n$ we have $\operatorname{im} 2 = \ker 2$, which simplifies this expression so that it only involves one group.

Our argument will consider two cases depending on whether or not f_A supports large L^2-mass.

(i) Large L^2-mass: Suppose that $\|f_A\|^2_{L^2(\operatorname{im}2)} \geqslant \alpha^{5/3}$. Then, on average, A has density $\alpha^{2/3}$ on the fibres of the points in the set $2.A := \{2a : a \in A\}$. We wish to estimate inner products of the form $\langle \tau_y(1_{A_y} * 1_{A_y}),\, f_A\rangle_{L^2(\operatorname{im}2)}$, where the set A_y is the fibre of y. Plancherel's theorem tells us that

$$\big\langle \tau_y(1_{A_y} * 1_{A_y}),\, f_A\big\rangle_{L^2(\operatorname{im}2)} = \sum_{\gamma\in\widehat{\operatorname{im}2}} |\widehat{1_{A_y}}(\gamma)|^2\gamma(y)\widehat{f_A}(\gamma) = \alpha_y^2\alpha + O\big(\sup_{\gamma\neq 0_{\widehat{\operatorname{im}2}}} |\widehat{f_A}(\gamma)|\alpha_y\big),$$

where α_y is the density of the fibre. If $\alpha_y \geqslant \alpha^{2/3}$ then we get a nontrivial character at which $\widehat{f_A}(\gamma) = \Omega(\alpha^{5/3})$. This leads to a corresponding density increment which could only be iterated $O(\alpha^{-2/3})$ times before the density would have to exceed 1.

(ii) Small L^2-mass: Suppose that $\|f_A\|^2_{L^2(\operatorname{im}2)} \leqslant \alpha^{5/3}$. Then $2.A$ has density at least $\alpha^{1/3}$. We now replace f_A with $1_{2.A}$ and find, in much the same way as above, that we have a nontrivial Fourier mode (this time of a fibre) of size $\Omega(\alpha^{5/3})$. If one could now perform a density increment in a way that was simultaneous for all fibres then this could only happen $O(\alpha^{-2/3})$ times.

These two cases would combine to suggest that A contained $\exp\big(-O(\alpha^{-2/3})\big)$ three-term arithmetic progressions. Unfortunately the second is too optimistic; the content of this paper is in making a version of the sketch above work and, in particular, dealing with the harder case of small L^2-mass.

5. Families

We make a new definition for the remainder of the paper; it will help simplify some later inductive steps and should seem fairly natural given the discussion of the previous section.

Suppose that H is a finite (abelian) group of exponent 2. A *family* on H is a vector $\mathscr{A} = (A_h)_{h\in H}$, where $A_h \subset H$ for all $h \in H$; we call the set A_h a *fibre* of $\mathscr{A}$. We define the *density function* of $\mathscr{A}$ to be

$$f_{\mathscr{A}} : H \to [0,1];\ h \mapsto \mathbb{P}_H(A_h),$$

and refer to $\mathbb{E}_{x\in H} f_{\mathscr{A}}(x)$ as the *density* of $\mathscr{A}$ denoted $\mathbb{P}_H(\mathscr{A})$.

We are interested in the quantity

$$\Lambda(\mathscr{A}) := \mathbb{E}_{h\in H}\langle \tau_h(1_{A_h} * 1_{A_h}),\, f_{\mathscr{A}}\rangle_{L^2(H)},$$

and it is useful to note that $|H|^4\Lambda(\mathscr{A})$ is the number of quadruples (a, a', y, h) with $a, a' \in A_h$ and $y \in A_{a+a'-h}$.

If $A \subset \mathbb{Z}_4^n$ then the family $\mathscr{A} := (A_y)_{y\in \operatorname{im} 2}$ defined earlier for use in (4-1) has $\Lambda(\mathscr{A}) = \Lambda(A)$ and density α. Conversely, given any family $\mathscr{A}$ on $\mathbb{Z}_2^n$ we can clearly construct a set A in $\mathbb{Z}_4^n$ such that $\Lambda(A) = \Lambda(\mathscr{A})$; families are simply a notational convenience. The bulk of the paper now concerns the proof that $\Lambda(\mathscr{A})$ is large in terms of the density of $\mathscr{A}$.

6. Density increments on families

The arguments of this section are straightforward and encode the various ways in which we shall try to increment the density of our family under certain circumstances. The simplest of these is the standard ℓ^∞-density increment lemma which follows.

Lemma 6.1. *Suppose that H is a finite abelian group of exponent 2, $f : H \to [0, 1]$ and γ is a nontrivial character. Then the subgroup $H' := \{\gamma\}^\perp$ has index 2 and $\|f * \mathbb{P}_{H'}\|_{L^\infty(H)} = \mathbb{E}_{h\in H} f(h) + |\widehat{f}(\gamma)|$.*

Proof. Let $h_0 \in H \setminus H'$ so that $h_0 + H'$ is the coset of H' in H not equal to H'. By definition

$$|\widehat{f}(\gamma)| = \left|\mathbb{E}_{h\in H} 1_{H'}(h) f(h) - \mathbb{E}_{h\in H} 1_{h_0+H'}(h) f(h)\right|.$$

We also have

$$\mathbb{E}_{h\in H} f(h) = \mathbb{E}_{h\in H} 1_{H'}(h) f(h) + \mathbb{E}_{h\in H} 1_{h_0+H'}(h) f(h),$$

which on being added to the previous tells us that

$$2\max\left\{\mathbb{E}_{h\in H} 1_{H'}(h) f(h), \mathbb{E}_{h\in H} 1_{h_0+H'}(h) f(h)\right\} = \mathbb{E}_{h\in H} f(h) + |\widehat{f}(\gamma)|.$$

Since the index of H' in H is 2 we have $2(\mathbb{P}_H)|_{H'} = \mathbb{P}_{H'}$, whence

$$\max\left\{(f * \mathbb{P}_{H'})(0_H), (f * \mathbb{P}_{H'})(h_0)\right\} = \mathbb{E}_{h\in H} f(h) + |\widehat{f}(\gamma)|,$$

and the result follows. □

The next lemma is a sort of simultaneous version of the above. If a family has a large number of its fibres having a large Fourier coefficient at the same nontrivial character γ then there is a related family with increased density.

Lemma 6.2. *Suppose that H is a finite abelian group of exponent 2, $\mathscr{A} = (A_h)_{h\in H}$ is a family on H and γ is a nontrivial character. Then there is a subgroup $H' \leqslant H$ of index 2 and a family $\mathscr{A}'$ on H' such that*

$$\Lambda(\mathscr{A}) \geqslant 2^{-4}\Lambda(\mathscr{A}') \quad \text{and} \quad \mathbb{P}_{H'}(\mathscr{A}') \geqslant \mathbb{P}_H(\mathscr{A}) + \mathbb{E}_{h\in H}|\widehat{1_{A_h}}(\gamma)|.$$

Proof. Let $H' := \{\gamma\}^\perp$ and let $h_0 \in H \setminus H'$ so that $h_0 + H'$ is the coset of H' in H not equal to H'. For each $h \in H$ apply Lemma 6.1 to see that

$$\|1_{A_h} * \mathbb{P}_{H'}\|_{L^\infty(H)} \geqslant \mathbb{E}_{\tilde{h}\in H} 1_{A_h}(\tilde{h}) + |\widehat{1_{A_h}}(\gamma)|.$$

Now let $x_h \in H$ be such that $\|1_{A_h} * \mathbb{P}_{H'}\|_{L^\infty(H)} = (1_{A_h} * \mathbb{P}_{H'})(x_h)$ and define $B_h := A_h \cap (x_h + H') - x_h \subset H'$, whence

$$\mathbb{P}_{H'}(B_h) \geqslant \mathbb{E}_{\tilde{h}\in H} 1_{A_h}(\tilde{h}) + |\widehat{1_{A_h}}(\gamma)| = f_{\mathscr{A}}(h) + |\widehat{1_{A_h}}(\gamma)|.$$

It follows that

$$\mathbb{E}_{h\in H}\mathbb{P}_{H'}(B_h) \geqslant \mathbb{E}_{h\in H} f_{\mathscr{A}}(h) + \mathbb{E}_{h\in H}|\widehat{1_{A_h}}(\gamma)|,$$

whence by averaging we deduce there is a coset $h_1 + H'$ of H such that

$$\mathbb{E}_{h\in h_1+H'}\mathbb{P}_{H'}(B_h) \geqslant \mathbb{E}_{h\in H} f_{\mathscr{A}}(h) + \mathbb{E}_{h\in H}|\widehat{1_{A_h}}(\gamma)|.$$

Now we define a family $\mathscr{A}'$ on H' as follows: for each $h' \in H'$ let $A'_{h'} := B_{h_1+h'}$. Clearly $\mathscr{A}'$ has the required density; it remains to show that $\Lambda(\mathscr{A}) \geqslant 2^{-4}\Lambda(\mathscr{A}')$, which is a relatively simple counting exercise.

There are $|H'|^4\Lambda(\mathscr{A}')$ quadruples (a'_0, a'_1, y', h') with $a'_0, a'_1 \in A'_{h'}$ and $y' \in A'_{a'_0+a'_1-h'}$. Every such quadruple corresponds uniquely to a quadruple

$$(a_0, a_1, y, h) := (a'_0 + x_{h_1+h'}, a'_1 + x_{h_1+h'}, y' + x_{a'_0+a'_1-h'+h_1}, h_1 + h');$$

unique since there is an obvious inverse on the image taking (a_0, a_1, y, h) to

$$(a'_0, a'_1, y', h') = (a_0 - x_h, a_1 - x_h, y - x_{a_0+a_1-h-2x_h+2h_1}, h - h_1).$$

Now,

$$a_0 = a'_0 + x_{h_1+h'} \in A'_h + x_{h_1+h'} = B_{h_1+h'} + x_{h_1+h'} \subset A_{h_1+h'} = A_h,$$

and similarly $a_1 \in A_h$. Furthermore

$$y = y' + x_{a'_0+a'_1-h'+h_1} \in A'_{a'_0+a'_1-h'} + x_{a'_0+a'_1-h'+h_1} = B_{a'_0+a'_1-h'+h_1} + x_{a'_0+a'_1-h'+h_1} \subset A_{a'_0+a'_1-h'+h_1} = A_{a_0+a_1-h},$$

since $2x_{h_1+h'} = 0_H$ and $2h_1 = 0_H$. It follows that every quadruple (a'_0, a'_1, y', h') with $a'_0, a'_1 \in A'_{h'}$ and $y' \in A'_{a'_0+a'_1-h'}$ corresponds to a unique quadruple (a_0, a_1, y, h) with $a_0, a_1 \in A_h$ and $y \in A_{a_0+a_1-h}$, whence

$$|H'|^4\Lambda(\mathscr{A}) \leqslant |H|^4\Lambda(\mathscr{A}).$$

The result follows on noting that $|H|^4 = 2^4|H'|^4$. □

The last part of this proof was a rather fiddly verification of a type which we shall have to do repeatedly, and while we were comprehensive in the details above, in the future we shall include fewer of them.

The final lemma of the section takes a family where the density function is nonuniform and produces a new family with a larger density, again very much in the spirit of the previous two lemmas.

Lemma 6.3. *Suppose that H is a finite abelian group of exponent 2, $\mathscr{A} = (A_h)_{h\in H}$ is a family on H and γ is a nontrivial character. Then there is a subgroup $H' \leqslant H$ of index 2 and a family $\mathscr{A}'$ on H' such that*

$$\Lambda(\mathscr{A}) \geqslant 2^{-4}\Lambda(\mathscr{A}') \quad \textit{and} \quad \mathbb{P}_{H'}(\mathscr{A}') \geqslant \mathbb{P}_H(\mathscr{A}) + |\widehat{f_{\mathscr{A}}}(\gamma)|.$$

Proof. Let $H' := \{\gamma\}^\perp$ and let $h_0 \in H \setminus H'$ so that $h_0 + H'$ is the coset of H' in H not equal to H'. Apply Lemma 6.1 so that we have

$$\|f_{\mathscr{A}} * \mathbb{P}_{H'}\|_{L^\infty(H)} = \mathbb{P}_H(\mathscr{A}) + |\widehat{f_{\mathscr{A}}}(\gamma)|.$$

Let $h_1 \in H'$ be such that $(f_{\mathscr{A}} * \mathbb{P}_{H'})(h_1) = \|f_{\mathscr{A}} * \mathbb{P}_{H'}\|_{L^\infty(H)}$. Now, define a family $\mathscr{A}'$ as follows: for each $h' \in H'$

(i) if $A_{h_1+h'} \cap H'$ is larger than $A_{h_1+h'} \cap (h_0 + H')$ then put $x_{h_1+h'} := 0_H$ and $A'_{h'} := A_{h_1+h'} \cap H'$;

(ii) otherwise put $x_{h_1+h'} := h_0$ and $A'_{h'} := A_{h_1+h'} \cap (h_0 + H') - h_0$.

By averaging we have $\mathbb{P}_{H'}(A'_{h'}) \geqslant \mathbb{P}_H(A_{h_1+h'})$, whence

$$\mathbb{E}_{h'\in H'}\mathbb{P}_{H'}(A'_{h'}) \geqslant (f_{\mathscr{A}} * \mathbb{P}_{H'})(h_1) = \mathbb{P}_H(\mathscr{A}) + |\widehat{f_{\mathscr{A}}}(\gamma)|,$$

which yields the required density condition. It remains, as before, to show that $\Lambda(\mathscr{A}) \geqslant 2^{-4}\Lambda(\mathscr{A}')$; we proceed as in the previous lemma.

There are $|H'|^4\Lambda(\mathscr{A}')$ quadruples (a'_0, a'_1, y', h') with $a'_0, a'_1 \in A'_{h'}$ and $y' \in A'_{a'_0+a'_1-h'}$. Every such quadruple corresponds uniquely to a quadruple

$$(a_0, a_1, y, h) := (a'_0 + x_{h_1+h'}, a'_1 + x_{h_1+h'}, y' + x_{a'_0+a'_1-h'+h_1}, h_1 + h')$$

with $a_0, a_1 \in A_h$ and $y \in A_{a_0+a_1-h}$, whence $|H'|^4\Lambda(\mathscr{A}) \leqslant |H|^4\Lambda(\mathscr{A})$ and the result follows on noting that $|H|^4 = 2^4|H'|^4$. □

7. Families with large mean square density

In this section we show how a family $\mathscr{A}$ for which $\|f_{\mathscr{A}}\|_{L^2(H)}$ is large (compared with its trivial lower bound of $\mathbb{P}_H(\mathscr{A})^2$) has $\Lambda(\mathscr{A})$ large. The basic idea is that if $\|f_{\mathscr{A}}\|_{L^2(H)}$ is large then most of the fibres A_h have large density and so are more easily "uniformised". When they are uniform the count $\Lambda(\mathscr{A})$ is easily seen to be large.

It is instructive to consider a simplified situation. Suppose that $\mathscr{A}$ is a family which is assumed to have fibres of density either 0 or δ and the support of $f_{\mathscr{A}}$ has density σ. This family has density $\delta\sigma$ and $\|f_{\mathscr{A}}\|^2_{L^2(H)} = \delta^2\sigma$, which is large compared with the trivial lower bound of $(\delta\sigma)^2$ if σ is small. Now, the standard Roth–Meshulam argument can be used to show that $\Lambda(\mathscr{A}) = \exp\big(O(\delta^{-1}\sigma^{-1})\big)$, and the proposition below asserts that this can be improved when σ is small.

Proposition 7.1. *Suppose that H is a finite abelian group of exponent 2 and $\mathscr{A} = (A_h)_{h\in H}$ is a family on H such that $f_{\mathscr{A}} = \delta 1_S$ for some $\delta \in (0, 1]$ and $S \subset H$ of density σ. Then $\Lambda(\mathscr{A}) = \exp\big(-O(\delta^{-1}\log\sigma^{-1})\big)$.*

Naturally the proof is iterative with the following lemma acting as the driver.

Lemma 7.2. *Suppose that H is a finite abelian group of exponent 2, $\mathscr{A} = (A_h)_{h\in H}$ is a family on H and $f_{\mathscr{A}} = \delta 1_S$ for some $\delta \in (0, 1]$ and $S \subset H$ of density σ. Then either*

$$\Lambda(\mathscr{A}) \geqslant \delta^3\sigma^2/2$$

or there is a subgroup $H' \leqslant H$ of index 2, a family $\mathscr{A}'$ on H' and set $S' \subset H'$ such that $f_{\mathscr{A}'} = \delta 1_{S'}$ and

$$\mathbb{P}_{H'}(S') \geqslant \sigma(1 + \delta/2) \quad \textit{and} \quad \Lambda(\mathscr{A}) \geqslant 2^{-4}\Lambda(\mathscr{A}').$$

Proof. Since $f_{\mathscr{A}} = \delta 1_S$ we have

$$\Lambda(\mathscr{A}) = \delta\mathbb{E}_{h\in H}\langle \tau_h(1_{A_h} * 1_{A_h}), 1_S\rangle_{L^2(H)}.$$

Applying Plancherel's theorem to the inner products we get

$$\Lambda(\mathscr{A}) = \delta\mathbb{E}_{h\in H}\sum_{\gamma\in\widehat{H}} |\widehat{1_{A_h}}(\gamma)|^2\widehat{1_S}(\gamma)\gamma(h).$$

The triangle inequality may be used on these inner sums to separate out the trivial mode. Indeed, since $\widehat{1_{A_h}}(0_{\widehat{H}}) = f_{\mathscr{A}}(h)$ and $\widehat{1_S}(0_{\widehat{H}}) = \sigma$ we get, after a little manipulation,

$$\mathbb{E}_{h\in H}\sum_{\gamma\neq 0_{\widehat{H}}}|\widehat{1_{A_h}}(\gamma)|^2|\widehat{1_S}(\gamma)| \geqslant \mathbb{E}_{h\in H} f_{\mathscr{A}}(h)^2\sigma - \delta^{-1}\Lambda(\mathscr{A}) = \delta^2\sigma^2 - \delta^{-1}\Lambda(\mathscr{A}).$$

Now, we are done unless $\Lambda(\mathscr{A}) \leqslant \delta^3\sigma^2/2$ (in fact, unless $\Lambda(\mathscr{A}) < \delta^3\sigma^2/2$, but we shall not use this), whence

$$\mathbb{E}_{h\in H}\sum_{\gamma\neq 0_{\widehat{H}}}|\widehat{1_{A_h}}(\gamma)|^2|\widehat{1_S}(\gamma)| \geqslant \delta^2\sigma^2/2.$$

On the other hand,

$$\mathbb{E}_{h\in H}\sum_{\gamma\neq 0_{\widehat{H}}}|\widehat{1_{A_h}}(\gamma)|^2 = \mathbb{E}_{h\in H}(f_{\mathscr{A}}(h) - f_{\mathscr{A}}(h)^2) = \delta(1-\delta)\sigma \leqslant \delta\sigma,$$

by Parseval's theorem. Using this with the triangle inequality in the previous expression tells us that S is linearly biased:

$$\sup_{\gamma\neq 0_{\widehat{H}}}|\widehat{1_S}(\gamma)| \geqslant \delta\sigma/2.$$

Thus, by Lemma 6.1 there is a subgroup $H' \leqslant H$ of index 2 such that

$$\|1_S * \mathbb{P}_{H'}\|_{L^\infty(H)} \geqslant \sigma(1+\delta/2). \tag{7-1}$$

Let $h_1 \in H$ be such that $(1_S * \mathbb{P}_{H'})(h_1) = \|1_S * \mathbb{P}_{H'}\|_{L^\infty(H)}$ and define a family $\mathscr{A}' := (A'_{h'})_{h'\in H'}$ as follows. For each $h' \in H'$ let $x_{h'+h_1}$ be such that $(1_{A_{h'+h_1}} * \mathbb{P}_{H'})(x_{h'+h_1})$ is maximal. If $(1_{A_{h'+h_1}} * \mathbb{P}_{H'})(x_{h'+h_1}) > 0$ then

$$0 < (1_{A_{h'+h_1}} * \mathbb{P}_{H'})(x_{h'+h_1})/2 \leqslant f_{\mathscr{A}}(h'+h_1) = \delta 1_S(h'+h_1),$$

whence

$$1_{A_{h'+h_1}} * \mathbb{P}_{H'}(x_{h'+h_1}) \geqslant \mathbb{E}_{h\in H} 1_{A_{h'+h_1}}(h) = f_{\mathscr{A}}(h'+h_1) = \delta,$$

and $A_{h'+h_1} \cap (x_{h'+h_1} + H') - x_{h'+h_1}$ contains a set of density δ; let $A'_{h'}$ be such a set. If

$$(1_{A_{h'+h_1}} * \mathbb{P}_{H'})(x_{h'+h_1}) = 0$$

then let $A'_{h'} = \varnothing$. Finally, we write $S' := S \cap (h_1 + H') - h_1$ and it remains to check that we have the required properties.

First, note that

$$f_{\mathscr{A}'}(h') = \mathbb{P}_{H'}(A'_{h'}) \leqslant 2\mathbb{P}_H(A_{h'+h_1}) = 2f_{\mathscr{A}}(h'+h_1),$$

thus if $f_{\mathscr{A}'}(h') > 0$ then $h'+h_1 \in S$ and so $h' \in S'$. Similarly,

$$f_{\mathscr{A}'}(h') = \mathbb{P}_{H'}(A'_{h'}) \geqslant \mathbb{P}_H(A_{h'+h_1}) = 2f_{\mathscr{A}}(h'+h_1),$$

so if $f_{\mathscr{A}'}(h') = 0$ then $h'+h_1 \notin S$, whence $h' \notin S'$. By design, $f_{\mathscr{A}'}$ takes only the values 0 and δ and so we have the representation $f_{\mathscr{A}'} = \delta 1_{S'}$.

Secondly, we have $\mathbb{P}_{H'}(S') = 1_S * \mathbb{P}_{H'}(h_1)$, whence $\mathbb{P}_{H'}(S') \geqslant \sigma(1+\delta/2)$ by (7-1). Lastly, we check that $\Lambda(\mathscr{A}) \geqslant 2^{-4}\Lambda(\mathscr{A}')$ in the usual fashion.

There are $|H'|^4\Lambda(\mathscr{A}')$ quadruples (a_0', a_1', y', h') with $a_0', a_1' \in A'_{h'}$ and $y' \in A'_{a_0'+a_1'-h'}$. Every such quadruple corresponds uniquely to a quadruple

$$(a_0, a_1, y, h) := (a_0' + x_{h_1+h'}, a_1' + x_{h_1+h'}, y' + x_{a_0'+a_1'-h'+h_1}, h_1 + h')$$

with $a_0, a_1 \in A_h$ and $y \in A_{a_0+a_1-h}$, whence $|H'|^4\Lambda(\mathscr{A}) \leqslant |H|^4\Lambda(\mathscr{A})$ and the result follows on noting that $|H|^4 = 2^4|H'|^4$. □

Proof of Proposition 7.1. Let $H_0 := H$, $\mathscr{A}_0 := \mathscr{A}$, $\alpha_0 := \delta\sigma$, $S_0 := S$ and $\sigma_0 := \sigma$. Suppose that we have a finite abelian group H_i of exponent 2 with a family $\mathscr{A}_i$ on H_i of density α_i and a set S_i of density σ_i such that $f_{\mathscr{A}_i} = \delta 1_{S_i}$. Apply Lemma 7.2 to see that either

$$\Lambda(\mathscr{A}_i) \geqslant \delta^3\sigma_i^2/2,$$

or there is a subgroup H_{i+1} of index 2 in H_i, a family $\mathscr{A}_{i+1}$ and a set S_{i+1} such that

$$f_{\mathscr{A}_{i+1}} = \delta 1_{S_{i+1}}, \sigma_{i+1} \geqslant \sigma_i(1+\delta/2) \quad \text{and} \quad \Lambda(\mathscr{A}_i) \geqslant 2^{-4}\Lambda(\mathscr{A}_{i+1}).$$

Since $\sigma_i \leqslant 1$ we see that this iteration must terminate at some stage i with $(1+\delta/2)^i \leqslant \sigma^{-1}$, that is, with $i \leqslant 2\delta^{-1}\log\sigma^{-1}$. It follows that

$$\Lambda(\mathscr{A}) \geqslant 2^{-8\delta^{-1}\log\sigma^{-1}}\delta^3\sigma^2/2,$$

which is the result. □

Proposition 7.1 will be used again in Section 9 but it may seem like the rather special form of the family considered is too restrictive. However, a standard dyadic decomposition lets us apply this proposition to an arbitrary family; we gain precisely in the case when $\|f_{\mathscr{A}}\|_{L^2(H)}^2\alpha^{-2} \to \infty$.

Corollary 7.3. *Suppose that H is a finite abelian group of exponent 2, $\mathscr{A} = (A_h)_{h\in H}$ is a family on H of density α and $\|f_{\mathscr{A}}\|_{L^2(H)} = K\alpha^2$ for some $K \geqslant 2$. Then*

$$\Lambda(\mathscr{A}) = \exp\bigl(-O(\alpha^{-1}K^{-1}\log^2 K)\bigr).$$

Proof. Let $S_i := \bigl\{h \in H : 2^{-(i+1)} \leqslant f_{\mathscr{A}}(h) \leqslant 2^{-i}\bigr\}$ and $S' := \bigl\{h \in H : f_{\mathscr{A}}(h) \leqslant \alpha/2\bigr\}$. We may use these sets to partition the range of summation in $\|f_{\mathscr{A}}\|_{L^2(H)}^2$: by the triangle inequality

$$\sum_{i \leqslant \lceil \log_2 \alpha^{-1}\rceil} 2^{-2i}\mathbb{P}_H(S_i) + (\alpha/2)^2 \geqslant \|f_{\mathscr{A}}\|_{L^2(H)}^2.$$

The Cauchy–Schwarz inequality tells us that $\|f_{\mathscr{A}}\|_{L^2(H)}^2 \geqslant \alpha^2$, whence

$$\sum_{i \leqslant \lceil \log_2 \alpha^{-1}\rceil} 2^{-2i}\mathbb{P}_H(S_i) \geqslant 3\|f_{\mathscr{A}}\|_{L^2(H)}^2/4. \tag{7-2}$$

Now let $\epsilon \in (0, 1]$ be a parameter to be chosen later and note that

$$\sum_{i \leqslant \lceil \log_2 \alpha^{-1}\rceil} 2^{\epsilon i} \leqslant 2\alpha^{-\epsilon} \sum_{i \leqslant \lceil \log_2 \alpha^{-1}\rceil} 2^{\epsilon(i - \lceil \log_2 \alpha^{-1}\rceil)} \leqslant 2\alpha^{-\epsilon}\sum_{j=0}^{\infty} 2^{-\epsilon j} = \frac{2\alpha^{\epsilon}}{1-2^{-\epsilon}} \leqslant 2\epsilon^{-1}\alpha^{-\epsilon}.$$

Returning to (7-2) we see that

$$\sum_{i\leqslant\lceil\log_2\alpha^{-1}\rceil} 2^{\epsilon i}\,2^{-(2+\epsilon)i}\mathbb{P}_H(S_i) \geqslant 3\|f_{\mathscr{A}}\|^2_{L^2(H)}/4,$$

and so by averaging from our previous calculation there is some $i\leqslant\lceil\log_2\alpha^{-1}\rceil$ such that

$$(2\epsilon^{-1}\alpha^{-\epsilon})\,2^{-(2+\epsilon)i}\mathbb{P}_H(S_i)\geqslant 3\|f_{\mathscr{A}}\|^2_{L^2(H)}/4. \tag{7-3}$$

Moreover $2^{-(i+1)}\mathbb{P}_H(S_i)\leqslant\mathbb{E}_{h\in H}f_{\mathscr{A}}(h)=\alpha$; so, recalling that $\|f_{\mathscr{A}}\|^2_{L^2(H)}=K\alpha^2$ we have

$$2^{-(1+\epsilon)i}\geqslant 3\epsilon K\alpha^{1+\epsilon}/16.$$

If we take $\epsilon=1/(1+\log K)$, we get

$$2^{-(i+1)}=\Omega(\alpha K/\log K). \tag{7-4}$$

Let $\mathscr{A}'$ be a family defined as follows. If $h\in S_i$ then A'_h is a subset of A_h of density $2^{-(i+1)}$ and A'_h is empty otherwise. By comparison of the terms in $\Lambda(\mathscr{A})$ with those in $\Lambda(\mathscr{A}')$ we see that $\Lambda(\mathscr{A})\geqslant\Lambda(\mathscr{A}')$.

We now apply Proposition 7.1 to $\mathscr{A}'$; it is easy to see from (7-3) and (7-4) that $\delta^{-1}=2^{(i+1)}=O(\alpha^{-1}K^{-1}\log K)$ and

$$\log\sigma^{-1}=\log\mathbb{P}_H(S_i)^{-1}=O\big(\log((\delta\alpha^{-1})^{2+\epsilon}K^{-1}\log K)\big)=O(\log K\delta\alpha^{-1}).$$

The result follows on noting that

$$\Lambda(\mathscr{A})=\exp\big(-O(\delta^{-1}\log K\delta\alpha^{-1})\big)$$

increases as δ decreases. □

It should be noted that one cannot completely remove the logarithmic term in this corollary. We might have $K\sim\alpha^{-1}$, but $\Lambda(\mathscr{A})$ may still be $\exp(-\Omega(\log K))$. To see this consider, for example, the family $\mathscr{A}$, where every fibre A_h is a random set of density α. Of course, the logarithmic power will not significantly affect our final result and is only critical when K is much smaller than α^{-1}, in which case it may be possible to remove it entirely.

8. A quasirandom Balog–Szemerédi–Gowers–Freĭman theorem

The Balog–Szemerédi–Gowers–Freĭman theorem is a now ubiquitous result in additive combinatorics introduced by Gowers [1998]. It combines (a refined proof of) the Balog–Szemerédi theorem [1994] with the structure theorem of Freĭman [1973] concerning sets with small sum set. Since we are working in finite abelian groups of exponent 2 we actually require the far easier torsion version of Freĭman's theorem proved in [Ruzsa 1999]. In fact, in this setting a version of the Balog–Szemerédi–Gowers–Freĭman theorem is known with relatively good bounds.

Theorem 8.1 [Green and Tao 2009, Theorem 1.7]. *Suppose that H is a group of exponent 2, $A\subset H$ has density α and $\|1_A*1_A\|^2_{L^2(H)}\geqslant c\alpha^3$. Then there is an element $x\in H$ and a subgroup $H'\leqslant H$ such that*

$$\mathbb{P}_H(H')=\exp\big(-O(c^{-1}\log c^{-1})\big)\alpha \quad \textit{and} \quad (1_A*\mathbb{P}_{H'})(x)\geqslant c/2.$$

We actually require a slightly modified version of this result which also ensures that A' behaves uniformly on H'. This can essentially be read out of the proof in [Green and Tao 2009]; however, for completeness, we include a "decoupled" proof here.

Corollary 8.2. *Suppose that H is a group of exponent 2, $A \subset H$ has density α and $\|1_A * 1_A\|_{L^2(H)}^2 \geqslant c\alpha^3$, and $\epsilon \in (0, 1]$ is a parameter. Then there is an element $x \in H$ and a subgroup $H' \leqslant H$ such that*

$$\mathbb{P}_H(H') = \exp\big(-O((c^{-1} + \epsilon^{-1}) \log c^{-1})\big)\alpha \quad \text{and} \quad (1_A * \mathbb{P}_{H'})(x) \geqslant c/2,$$

and writing $A' := A \cap (x + H') - x \subset H'$ one has

$$\sup_{\gamma \neq 0_{\widehat{H'}}} |\widehat{1_{A'}}(\gamma)| \leqslant \epsilon \mathbb{P}_{H'}(A').$$

Proof. We apply Theorem 8.1 to get an element $x_0 \in H$ and a subgroup $H_0 \leqslant H$ such that

$$\mathbb{P}_H(H_0) = \exp\big(-O(c^{-1} \log c^{-1})\big) \quad \text{and} \quad (1_A * \mathbb{P}_{H_0})(x_0) \geqslant c/2.$$

Put $A_0 := A \cap (x_0 + H_0) - x_0 \subset H_0$ and $\alpha_0 := \mathbb{P}_{H_0}(A_0)$. Now, suppose that we have been given an element $x_i \in H$, a subgroup H_i and a subset A_i of H_i of density α_i. If

$$\sup_{\gamma \neq 0_{\widehat{H_i}}} |\widehat{1_{A_i}}(\gamma)| \leqslant \epsilon \alpha_i, \tag{8-1}$$

then we terminate the iteration; otherwise we apply Lemma 6.1 to get a subgroup H_{i+1} of index 2 in H_i such that

$$\|1_{A_i} * \mathbb{P}_{H_{i+1}}\|_{L^\infty(H_i)} \geqslant \alpha_i(1 + \epsilon).$$

Let x_{i+1} be such that $(1_{A_i} * \mathbb{P}_{H_{i+1}})(x_{i+1}) = \|1_{A_i} * \mathbb{P}_{H_{i+1}}\|_{L^\infty(H_i)}$, and $A_{i+1} = A_i \cap (x_{i+1} + H_{i+1}) - x_{i+1} \subset H_{i+1}$.

Since $\alpha_i \leqslant 1$ we see that this iteration must terminate at some stage i with $(1 + \epsilon)^i \leqslant \alpha_0^{-1}$, that is, with $i \leqslant \epsilon^{-1} \log \alpha_0^{-1} = O(\epsilon^{-1} \log c^{-1})$. We put $x := x_0 + \cdots + x_i$ and $H' := H_i$ so that H_i has index $O(\epsilon^{-1} \log c^{-1})$ in H_0 and $A' = A_i$ has density at least $c/2$. Thus

$$\mathbb{P}_H(H') = \mathbb{P}_H(H_0)\, \mathbb{P}_{H_0}(H_k) = \exp\big(-O((c^{-1} + \epsilon^{-1}) \log c^{-1})\big)\alpha,$$

and it remains to note that the final condition of the corollary holds in view of the fact that we must have (8-1) for the iteration to terminate. □

The iteration in this proof is essentially the iteration at the core of the usual Roth–Meshulam argument (given in the sketch proof in Section 4) and consequently if one could improve the ϵ-dependence in the above result one could probably improve the Roth–Meshulam argument directly. Unfortunately in our use of this corollary ϵ and c are comparable; thus, even in the presence of Marton's conjecture, more commonly called the polynomial Freĭman–Ruzsa conjecture [Green 2005], we would see no significant improvement in our final result.

9. Families with high fibered energy

In this section we use our previous work to show that if a family $\mathscr{A}$ has large additive energy in its fibres then $\Lambda(\mathscr{A})$ is large. The actual statement of the result is rather technical so we take a moment now to sketch the approach.

The key tool is the corollary of the Balog–Szemerédi–Gowers–Freĭman theorem established in Section 8. This may be applied individually to the fibres of $\mathscr{A}$ in each case, producing a subgroup on which the fibre is very dense. If all of these subgroups are very different then it is easy to see that $\Lambda(\mathscr{A})$ must be large; if not then by expanding them a little bit we find one subgroup on which a lot of fibres of $\mathscr{A}$ are very dense and we may use Proposition 7.1 to get that $\Lambda(\mathscr{A})$ is large.

Concretely, then, the purpose of this section is to prove the following.

Lemma 9.1. *Suppose that H is a finite abelian group of exponent 2, and $\mathscr{A} = (A_h)_{h\in H}$ is a family on H of density α such that*

$$\sup_{\gamma\neq 0_{\widehat{H}}} |\widehat{f_{\mathscr{A}}}(\gamma)| \leqslant L\alpha^2,$$

for some parameter $L \geqslant 1$. Suppose further that S is a set of density σ and $K \geqslant 1$ is a parameter such that

(i) *$K\alpha \geqslant f_{\mathscr{A}}(h) \geqslant K\alpha/2$ for all $h \in S$;*

(ii) *and $\|1_{A_h} * 1_{A_h}\|_{L^2(H)}^2 \geqslant c f_{\mathscr{A}}(h)^3$ for all $h \in S$.*

Then

$$\Lambda(\mathscr{A}) \geqslant \exp\Big(-O\Big(L(\log^2\alpha^{-1} + \log\sigma^{-1})\,\exp\big(O\big((c^{-1} + K^{1/2}c^{-1/2})\log c^{-1}\big)\big)\Big)\Big).$$

Proof. By Corollary 8.2 (with $\epsilon = 2^{-2}\sqrt{c/K}$) we see that for each $h \in S$ there is an element $x_h \in H$ and a subgroup $H_h \leqslant H$ such that the set $A_h' := A_h \cap (x_h + H_h) - x_h$ has

$$\mathbb{P}_H(H_h) = \exp\Big(-O\big((c^{-1} + K^{1/2}c^{-1/2})\log c^{-1}\big)\Big) f_{\mathscr{A}}(h) \quad \text{and} \quad \mathbb{P}_{H_h}(A_h') \geqslant c/2,$$

and, furthermore,

$$\sup_{\gamma\neq 0_{\widehat{H_h}}} |\widehat{1_{A_h'}}(\gamma)| \leqslant \epsilon \mathbb{P}_{H_h}(A_h'). \tag{9-1}$$

Now, let $S_0 := \{h \in S : (f_{\mathscr{A}} * \mathbb{P}_{H_h})(h) \geqslant \alpha/2\}$ and $S_1 := S \setminus S_0$; we shall now split into two cases according to which of S_0 or S_1 is larger.

Case 1. Suppose that $\mathbb{P}_H(S_0) \geqslant \sigma/2$. Then

$$\Lambda(\mathscr{A}) \geqslant \alpha^3\sigma \exp\Big(-O\big((c^{-1} + K^{1/2}c^{-1/2})\log c^{-1}\big)\Big).$$

Proof. By nonnegativity of the terms in $\Lambda(\mathscr{A})$ we have

$$\Lambda(\mathscr{A}) \geqslant \mathbb{E}_{h\in H} 1_{S_0}(h)\langle \tau_h(1_{A_h} * 1_{A_h}),\, f_{\mathscr{A}}\rangle_{L^2(H)}.$$

We analyse these inner products individually. Suppose that $h \in S_0$ and note that

$$\big\langle \tau_h(1_{A_h} * 1_{A_h}),\, f_{\mathscr{A}}\big\rangle_{L^2(H)} \geqslant \mathbb{P}_H(H_h)^2 \langle \tau_h(1_{A_h'} * 1_{A_h'}),\, f_{\mathscr{A}}\rangle_{L^2(h+H_h)}.$$

As usual this inner product is analysed using the Fourier transform: by Plancherel's theorem we have

$$\big\langle 1_{A_h'} * 1_{A_h'},\, \tau_{-h}(f_{\mathscr{A}})\big\rangle_{L^2(H_h)} = \sum_{\gamma\in\widehat{H_h}} |\widehat{1_{A_h'}}(\gamma)|^2 \widehat{\tau_{-h}(f_{\mathscr{A}})}(\gamma).$$

Separating out the contribution from the trivial character we get

$$\big\langle 1_{A'_h} * 1_{A'_h}, \tau_{-h}(f_{\mathcal{A}})\big\rangle_{L^2(H_h)} \geqslant \mathbb{P}_{H_h}(A'_h)^2 (f_{\mathcal{A}} * \mathbb{P}_{H_h})(h) - \sum_{\gamma \neq 0_{\widehat{H_h}}} \big|\widehat{1_{A'_h}}(\gamma)\big|^2 \big|\widehat{\tau_{-h}(f_{\mathcal{A}})}(\gamma)\big|. \tag{9-2}$$

This last term sum can be estimated as follows using Hölder's inequality and the Cauchy–Schwarz inequality:

$$\begin{aligned}\sum_{\gamma \neq 0_{\widehat{H_h}}} \big|\widehat{1_{A'_h}}(\gamma)\big|^2 \big|\widehat{\tau_{-h}(f_{\mathcal{A}})}(\gamma)\big| &\leqslant \sup_{\gamma \neq 0_{\widehat{H_h}}} \big|\widehat{1_{A'_h}}(\gamma)\big| \sum_{\gamma \in \widehat{H_h}} \big|\widehat{1_{A'_h}}(\gamma)\big| \big|\widehat{\tau_{-h}(f_{\mathcal{A}})}(\gamma)\big| \\ &\leqslant \sup_{\gamma \neq 0_{\widehat{H_h}}} \big|\widehat{1_{A'_h}}(\gamma)\big| \bigg(\sum_{\gamma \in \widehat{H_h}} \big|\widehat{1_{A'_h}}(\gamma)\big|^2\bigg)^{1/2} \bigg(\sum_{\gamma \in \widehat{H_h}} \big|\widehat{\tau_{-h}(f_{\mathcal{A}})}(\gamma)\big|^2\bigg)^{1/2}\end{aligned}$$

By Parseval's theorem,

$$\sum_{\gamma \in \widehat{H_h}} \big|\widehat{1_{A'_h}}(\gamma)\big|^2 = \mathbb{P}_{H_h}(A'_h) \quad \text{and} \quad \sum_{\gamma \in \widehat{H_h}} \big|\widehat{\tau_{-h}(f_{\mathcal{A}})}(\gamma)\big|^2 = \big|f_{\mathcal{A}}\big|^2_{L^2(h+H_h)},$$

and combining all this with (9-1) tells us that

$$\sum_{\gamma \neq 0_{\widehat{H_h}}} \big|\widehat{1_{A'_h}}(\gamma)\big|^2 \big|\widehat{\tau_{-h}(f_{\mathcal{A}})}(\gamma)\big| \leqslant \epsilon \mathbb{P}_{H_h}(A'_h)^{3/2} \|f_{\mathcal{A}}\|_{L^2(h+H_h)} \leqslant \epsilon \mathbb{P}_{H_h}(A'_h)^{3/2} \sqrt{2K} (f_{\mathcal{A}} * \mathbb{P}_{H_h})(h).$$

The last inequality here follows from the fact that $h \in S_0$ ensures that $f_{\mathcal{A}}(h) \leqslant K\alpha$ and $(f_{\mathcal{A}} * \mathbb{P}_{H_h})(h) \geqslant \alpha/2$. Finally, our choice of ϵ tells us that

$$\sum_{\gamma \neq 0_{\widehat{H_h}}} |\widehat{1_{A'_h}}(\gamma)|^2 |\widehat{\tau_{-h}(f_{\mathcal{A}})}(\gamma)| \leqslant \mathbb{P}_{H_h}(A'_h)^2 (f_{\mathcal{A}} * \mathbb{P}_{H_h})(h)/2,$$

whence, inserting this in (9-2), we get

$$\big\langle 1_{A'_h} * 1_{A'_h}, \tau_{-h}(f_{\mathcal{A}})\big\rangle_{L^2(H_h)} \geqslant \mathbb{P}_{H_h}(A'_h)^2 (f_{\mathcal{A}} * \mathbb{P}_{H_h})(h)/2.$$

Thus, our earlier averaging tells us that

$$\Lambda(\mathcal{A}) \geqslant \mathbb{E}_{h \in H} 1_{S_0}(h) \mathbb{P}_H(H_h)^2 \, \mathbb{P}_{H_h}(A'_h)^2 (f_{\mathcal{A}} * \mathbb{P}_{H_h})(h)/2,$$

and hence immediately that

$$\Lambda(\mathcal{A}) \geqslant 2^{-3} c^2 \alpha \mathbb{E}_{h \in H} 1_{S_0}(h) \mathbb{P}_H(H_h)^2 = \alpha^3 \sigma \exp\Big(-O\big((c^{-1} + K^{1/2} c^{-1/2}) \log c^{-1}\big)\Big).$$

The case is complete. □

Case 2. Suppose that $\mathbb{P}_H(S_1) \geqslant \sigma/2$. Then

$$\Lambda(\mathcal{A}) \geqslant \exp\bigg(-O\Big(L(\log^2 \alpha^{-1} + \log \sigma^{-1}) \exp\big(O\big((c^{-1} + K^{1/2} c^{-1/2}) \log c^{-1}\big)\big)\Big)\bigg).$$

Proof. Suppose that $h \in S_1$ so that $(f_{\mathcal{A}} * \mathbb{P}_{H_h})(h) \leqslant \alpha/2$. By the Fourier inversion formula we have

$$\sum_{\gamma \in H_h^\perp} \widehat{f_{\mathcal{A}}}(\gamma) \gamma(h) = (f_{\mathcal{A}} * \mathbb{P}_{H_h})(h) \leqslant \alpha/2.$$

Separating out the trivial mode where $\widehat{f_{\mathscr{A}}}(0_{\widehat{H}}) = \alpha$ and applying the triangle inequality we have

$$\sum_{0_{\widehat{H}} \neq \gamma \in H_h^\perp} |\widehat{f_{\mathscr{A}}}(\gamma)| \geqslant \alpha/2.$$

Write $\mathscr{L}' := \{\gamma : |\widehat{f_{\mathscr{A}}}(\gamma)| \geqslant \mathbb{P}_H(H_h)\alpha/4\}$ and note that since $|H_h^\perp| = \mathbb{P}_H(H_h)^{-1}$ we have

$$\sum_{0_{\widehat{H}} \neq \gamma \in \mathscr{L}' \cap H_h^\perp} |\widehat{f_{\mathscr{A}}}(\gamma)| \geqslant \sum_{0_{\widehat{H}} \neq \gamma \in H_h^\perp} |\widehat{f_{\mathscr{A}}}(\gamma)| - \sum_{\gamma \in H_h^\perp \setminus \mathscr{L}'} |\widehat{f_{\mathscr{A}}}(\gamma)| \geqslant \alpha/4.$$

Since $\sup_{\gamma \neq 0_{\widehat{H}}} |\widehat{f_{\mathscr{A}}}(\gamma)| \leqslant L\alpha^2$ we conclude that

$$|\mathscr{L}' \cap H_h^\perp| \geqslant \alpha^{-1}/4L.$$

Let $I_h \subset \mathscr{L}' \cap H_h^\perp$ be a set of $d := \lfloor \log_2(\alpha^{-1}/4L) \rfloor$ independent elements — possible since $2^d \leqslant |\mathscr{L}' \cap H_h^\perp|$ — and put $H_h' := I_h^\perp$. Since $I_h \subset H_h^\perp$, it follows that $H_h' = I_h^\perp \supset H_h$, whence $H_h \leqslant H_h'$. Since the elements of I_h are independent, we have

$$\mathbb{P}_H(H_h') = |I_h|^{-1} = 2^{-d} \leqslant 8L\alpha.$$

Since $h \in S_1$ we also have

$$\mathbb{P}_H(H_h) = \exp\Big(-O\big((c^{-1} + K^{1/2}c^{-1/2})\log c^{-1}\big)\Big)\alpha,$$

whence

$$|H_h' : H_h| \leqslant L\exp\Big(O\big((c^{-1} + K^{1/2}c^{-1/2})\log c^{-1}\big)\Big),$$

and it follows that

$$\mathbb{P}_{H_h'}(A_h') \geqslant L^{-1}\exp\Big(-O\big((c^{-1} + K^{1/2}c^{-1/2})\log c^{-1}\big)\Big).$$

Thus there is some δ with $\delta|H|$ an integer and

$$\delta \geqslant L^{-1}\exp\Big(-O\big((c^{-1} + K^{1/2}c^{-1/2})\log c^{-1}\big)\Big)$$

such that $\mathbb{P}_{H_h'}(A_h') \geqslant \delta$ for all $h \in S_1$; for each $h \in S_1$ let A_h'' be a subset of A_h' of density δ.

Each H_h' is defined by the set $I_h \subset \mathscr{L}'$ and there are at most $\binom{|\mathscr{L}'|}{d}$ such sets. Hence there is some space $H' \leqslant H$ such that $H_h' = H'$ for at least a proportion $\binom{|\mathscr{L}'|}{d}^{-1}$ of the elements of S_1; call this set S_2.

We now turn to estimating the density of S_2. First, by Parseval's theorem

$$|\mathscr{L}'|(\mathbb{P}_H(H_h)\alpha/4)^2 \leqslant \sum_{\gamma \in \widehat{H}} |\widehat{f_{\mathscr{A}}}(\gamma)|^2 = \|f_{\mathscr{A}}\|_{L^2(H)}^2 \leqslant K\alpha^2.$$

It follows from the lower bounds in $\mathbb{P}_H(H_h)$ that

$$|\mathscr{L}'| \leqslant \alpha^{-2}\exp\Big(O\big((c^{-1} + K^{1/2}c^{-1/2})\log c^{-1}\big)\Big),$$

whence

$$\binom{|\mathscr{L}'|}{d} \leqslant \exp\Big(O\big((c^{-1} + K^{1/2}c^{-1/2})\log^2 \alpha^{-1}\log c^{-1}\big)\Big).$$

This tells us that

$$\mathbb{P}_H(S_2) \geqslant \mathbb{P}_H(S_1)\big/\tbinom{|\mathscr{S}'|}{d} \geqslant \sigma \exp\Big(-O\big((c^{-1}+K^{1/2}c^{-1/2})\log^2\alpha^{-1}\log c^{-1}\big)\Big).$$

Finally, by averaging let h_1+H' be a coset of H' on which S_2 has at least the above density and define a new family $\mathscr{A}'''$ on H' as follows. For each $h' \in S_2-h_1$, let $A'''_{h'} := A''_{h_1+h'}$; if $h' \in H'\setminus(S_2-h_1)$ then let $A'''_{h'} := \varnothing$. By the definition of S_2 for each $h' \in S_2-h_1$ $A''_{h_1+h'}$ is a subset of $H' = H'_{h_1+h'}$ of density δ. Thus by Proposition 7.1 we have

$$\begin{aligned}\Lambda(\mathscr{A}''') &= \exp\Big(-O\Big(\delta^{-1}\big(\log^2\alpha^{-1}(c^{-1}+K^{1/2}c^{-1/2})\log c^{-1}+\log\sigma^{-1}\big)\Big)\Big)\\ &= \exp\Big(-O\Big(L(\log^2\alpha^{-1}+\log\sigma^{-1})\exp\big(O\big((c^{-1}+K^{1/2}c^{-1/2})\log c^{-1}\big)\big)\Big)\Big).\end{aligned}$$

Finally it remains for us to check that $|H|^4\Lambda(\mathscr{A}) \geqslant |H'|^4\Lambda(\mathscr{A}''')$ from which the case follows; we proceed in the usual manner.

There are $|H'|^4\Lambda(\mathscr{A}')$ quadruples (a'_0,a'_1,y',h') with $a'_0,a'_1 \in A'''_{h'}$ and $y' \in A'''_{a'_0+a'_1-h'}$. Every such quadruple corresponds uniquely to a quadruple

$$(a_0,a_1,y,h) := (a'_0+x_{h_1+h'}, a'_1+x_{h_1+h'}, y'+x_{a'_0+a'_1-h'+h_1}, h_1+h')$$

with $a_0,a_1 \in A_h$ and $y \in A_{a_0+a_1-h}$, whence $|H'|^4\Lambda(\mathscr{A}) \leqslant |H|^4\Lambda(\mathscr{A})$ and the result follows. □

Having concluded both cases it remains to note that certainly one of $\mathbb{P}_H(S_1)$ and $\mathbb{P}_H(S_0)$ is at least $\sigma/2$ and so at least one of the cases occurs. □

10. Families with small mean square density

In this section we use our previous work to establish the following lemma which is the main driver in the proof of Theorem 3.4 in the case when the density function has small mean square.

Lemma 10.1. *Suppose that H is a finite abelian group of exponent 2, $\mathscr{A}=(A_h)_{h\in H}$ is a family on H of density α, $\|f_{\mathscr{A}}\|^2_{L^2(H)} = K\alpha^2$ and $L \geqslant \max\{K,2\}$ is a parameter. Then there is an absolute constant $C_{\mathscr{S}}>0$ such that either*

$$\Lambda(\mathscr{A}) \geqslant \exp\big(-(1+\log^2\alpha^{-1})\exp(C_{\mathscr{S}}L^3\log^2 L)\big)$$

or there is a subgroup $H'\leqslant H$ of index 2 and a family $\mathscr{A}'$ on H' such that

$$\mathbb{P}_{H'}(\mathscr{A}') \geqslant \alpha + L\alpha^2/4K \quad \text{and} \quad \Lambda(\mathscr{A}) \geqslant 2^{-4}\Lambda(\mathscr{A}').$$

Proof. Let $S_L := \{h\in H : f_{\mathscr{A}}(h) \geqslant 4K\alpha\}$ and $S_S := \{h\in H : f_{\mathscr{A}}(h)\leqslant \alpha/4\}$. Now,

$$\mathbb{E}_{h\in H}1_{S_L}(h)f_{\mathscr{A}}(h) \leqslant \frac{1}{4K\alpha}\,\mathbb{E}_{h\in H}1_{S_L}(h)f_{\mathscr{A}}(h)^2 \leqslant \frac{\alpha}{4},$$

and

$$\mathbb{E}_{h\in H}1_{S_S}(h)f_{\mathscr{A}}(h) \leqslant \alpha/4$$

trivially, whence, putting $S := H \setminus (S_L \cup S_S)$, we have that

$$\mathbb{E}_{h\in H} 1_S(h) f_{\mathscr{A}}(h) \geqslant \alpha/2.$$

Let $S_i := \{h \in S : 2^{i-2}\alpha \leqslant f_{\mathscr{A}}(h) \leqslant 2^{i-1}\alpha\}$ and note that

$$\sum_{i\leqslant \lceil \log K\rceil +1} \mathbb{E}_{h\in H} 1_{S_i}(h)\, 2^{i-1}\alpha \geqslant \alpha/2,$$

and thus by averaging there is some $i \leqslant \lceil \log K\rceil + 1$ such that

$$\mathbb{E}_{h\in H} 1_{S_i}(h)\, 2^{i-1}\alpha \geqslant \alpha/2\big(\lceil \log K\rceil + 1\big).$$

As a byproduct note that $\mathbb{P}_H(S_i) = \Omega(1/K(1+\log K))$. We write $K_i = 2^{i-1}$, so that

$$K_i\alpha \geqslant f_{\mathscr{A}}(h) \geqslant K_i\alpha/2 \quad \text{for all } h \in S_i$$

and

$$\mathbb{E}_{h\in H} 1_{S_i}(h) f_{\mathscr{A}}(h) = \Omega\big(\alpha/(1+\log K)\big).$$

Now suppose that $\mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2 \geqslant L\alpha^3$. Since $|\widehat{1_{A_h}}(\gamma)| \leqslant 4K\alpha$ if $h \in S$, we then conclude that

$$\mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)| \geqslant L\alpha^2/4K.$$

Applying Lemma 6.2 we find we are in the second case of Lemma 10.1. Similarly, by Lemma 6.3 we are done if $|\widehat{f_{\mathscr{A}}}(\gamma)| \geqslant L\alpha^2/4K$. Thus we may assume that

$$\sup_{\gamma\neq 0_{\widehat{H}}} \mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2 \leqslant L\alpha^3, \tag{10-1}$$

$$\sup_{\gamma\neq 0_{\widehat{H}}} \mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)| \leqslant L\alpha^2/4K, \tag{10-2}$$

$$\sup_{\gamma\neq 0_{\widehat{H}}} |\widehat{f_{\mathscr{A}}}(\gamma)| \leqslant L\alpha^2/4K. \tag{10-3}$$

As usual, by the nonnegativity of the terms in $\Lambda(\mathscr{A})$, we have

$$\Lambda(\mathscr{A}) \geqslant \mathbb{E}_{h\in H} 1_{S_i}(h) \big\langle \tau_h(1_{A_h} * 1_{A_h}),\, f_{\mathscr{A}}\big\rangle_{L^2(H)}.$$

We apply Plancherel's theorem to the inner products on the right to get

$$\big\langle \tau_h(1_{A_h} * 1_{A_h}),\, f_{\mathscr{A}}\big\rangle_{L^2(H)} = \sum_{\gamma\in\widehat{H}} |\widehat{1_{A_h}}(\gamma)|^2 \widehat{f_{\mathscr{A}}}(\gamma)\gamma(h).$$

Separating out the trivial mode and applying the triangle inequality then tells us that

$$\big\langle \tau_h(1_{A_h} * 1_{A_h}),\, f_{\mathscr{A}}\big\rangle_{L^2(H)} \geqslant f_{\mathscr{A}}(h)^2\alpha - \sum_{\gamma\neq 0_{\widehat{H}}} |\widehat{1_{A_h}}(\gamma)|^2 |\widehat{f_{\mathscr{A}}}(\gamma)|.$$

Thus

$$\sum_{\gamma\neq 0_{\widehat{H}}} \mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2 |\widehat{f_{\mathscr{A}}}(\gamma)| \geqslant \alpha \mathbb{E}_{h\in H} 1_{S_i}(h) f_{\mathscr{A}}(h)^2 - \Lambda(\mathscr{A}).$$

It follows that either

$$\Lambda(\mathscr{A}) \geqslant \alpha \mathbb{E}_{h\in H} 1_{S_i}(h) f_{\mathscr{A}}(h)^2/2 = \Omega\big(\alpha^3/(1+\log K)\big),$$

and we are done or

$$\sum_{\gamma\neq 0_{\widehat{H}}} \mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2|\widehat{f_{\mathcal{A}}}(\gamma)| \geqslant \alpha \mathbb{E}_{h\in H} 1_{S_i}(h) f_{\mathcal{A}}(h)^2/2, \tag{10-4}$$

which we now assume. Let

$$\mathcal{L} := \left\{\gamma \in \widehat{H} : \mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2 \geqslant \frac{(\mathbb{E}_{h\in H} 1_{S_i}(h) f_{\mathcal{A}}(h)^2)^2}{2^4 K \mathbb{E}_{h\in H} 1_{S_i}(h) f_{\mathcal{A}}(h)}\right\}.$$

We shall now show that

$$\sum_{\gamma\notin\mathcal{L}} \mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2|\widehat{f_{\mathcal{A}}}(\gamma)| \leqslant \alpha \mathbb{E}_{h\in H} 1_{S_i}(h) f_{\mathcal{A}}(h)^2/4. \tag{10-5}$$

We apply the triangle inequality to the left-hand side after swapping the order of summation to get that it is at most

$$\sup_{\gamma\notin\mathcal{L}} \big(\mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2\big)^{1/2} \sum_{\gamma\in\widehat{H}} \big(\mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2\big)^{1/2}|\widehat{f_{\mathcal{A}}}(\gamma)|.$$

Now apply the Cauchy–Schwarz inequality to this to see that the sum is at most

$$\left(\sum_{\gamma\in\widehat{H}} \mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2\right)^{1/2}\left(\sum_{\gamma\in\widehat{H}} |\widehat{f_{\mathcal{A}}}(\gamma)|^2\right)^{1/2} = \sqrt{\mathbb{E}_{h\in H} 1_{S_i}(h) f_{\mathcal{A}}(h) K\alpha^2}$$

by Parseval's theorem, after interchanging the order of summation again. The bound (10-5) now follows from the definition of $\mathcal{L}$. Combining this with (10-4) we see that

$$\sum_{0_{\widehat{H}}\neq\gamma\in\mathcal{L}} \mathbb{E}_{h\in H} 1_{S_i}(h)\big|\widehat{1_{A_h}}(\gamma)\big|^2\big|\widehat{f_{\mathcal{A}}}(\gamma)\big| \geqslant \alpha \mathbb{E}_{h\in H} 1_{S_i}(h) f_{\mathcal{A}}(h)^2/4 = \Omega\big(K_i\alpha^3/(1+\log K)\big).$$

Write

$$\mathcal{L}_j := \big\{\gamma \in \widehat{H} : 2^{-j} L\alpha^3 \geqslant \mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2 \geqslant 2^{-(j+1)} L\alpha^3\big\},$$

and note that by (10-1) we have $\mathcal{L}\setminus\{0_{\widehat{H}}\} = \bigcup_{j=0}^{j_0}\mathcal{L}_j$, where j_0 is the smallest integer such that

$$2^{-(j_0+1)} L\alpha^3 \leqslant \big(\mathbb{E}_{h\in H} 1_{S_i}(h) f_{\mathcal{A}}(h)^2\big)^2/2^4 K \mathbb{E}_{h\in H} 1_{S_i}(h) f_{\mathcal{A}}(h);$$

crucially,

$$j_0 = O(\log L) \quad \text{and} \quad 2^{-(j_0+1)} L\alpha^3 = \Omega\big(K_i^2\alpha^3/K(1+\log K)\big).$$

It follows by averaging (and since $L \geqslant \max\{2, K\}$) that there is some $j \leqslant j_0$ such that

$$\sum_{0_{\widehat{H}}\neq\gamma\in\mathcal{L}_j} \mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2|\widehat{f_{\mathcal{A}}}(\gamma)| = \Omega\big(K_i\alpha^3/(1+\log K)\log L\big).$$

Inserting (10-3) and dividing gives that

$$\sum_{0_{\widehat{H}}\neq\gamma\in\mathcal{L}_j} \mathbb{E}_{h\in H} 1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2 = \Omega\big(K_i K\alpha/(1+\log K)L\log L\big).$$

Now, the usual convexity of L^p-norms tells us that

$$\mathbb{E}_{h\in H}1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2 \leqslant \big(\mathbb{E}_{h\in H}1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|\big)^{2/3}\big(\mathbb{E}_{h\in H}1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^4\big)^{1/3}.$$

Thus, by (10-2) we have

$$\big(\mathbb{E}_{h\in H}1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^2\big)^3 \leqslant \frac{L^2\alpha^4}{2^4K^2}\mathbb{E}_{h\in H}1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^4.$$

Dividing out and summing over $\mathscr{L}_j$, using the fact that it is a dyadic range, tells us that

$$\sum_{\gamma\in\widehat{H}}\mathbb{E}_{h\in H}1_{S_i}(h)|\widehat{1_{A_h}}(\gamma)|^4 = \Omega\big(\alpha^3K_i^5K/(1+\log K)^3L^3\log L\big).$$

Thus Parseval's theorem reveals that

$$\mathbb{E}_{h\in H}1_{S_i}(h)\|1_{A_h}*1_{A_h}\|_{L^2(H)}^2 = \Omega\big(\alpha^3K_i^5K/(1+\log K)^3L^3\log L\big).$$

Finally, let

$$S_i' := \big\{h\in S_i : \|1_{A_h}*1_{A_h}\|_{L^2(H)}^2 \geqslant \mathbb{E}_{h\in H}1_{S_i}(h)\|1_{A_h}*1_{A_h}\|_{L^2(H)}^2/2\big\}$$

and note that if $h\in S_i'$ then $f_{\mathscr{A}}(h)\leqslant K_i\alpha$, whence

$$\|1_{A_h}*1_{A_h}\|_{L^2(H)}^2 = \Omega\big(\alpha^3K_i^2K/(1+\log K)^3L^3\log L\big).$$

Furthermore

$$\mathbb{E}_{h\in H}1_{S_i'}(h)\|1_{A_h}*1_{A_h}\|_{L^2(H)}^2 \geqslant \Omega\big(\alpha^3K_i^5K/(1+\log K)^3L^3\log L\big),$$

whence $\mathbb{P}_H(S)=\Omega(L^4)$. We now apply Lemma 9.1 to see that

$$\Lambda(\mathscr{A}) \geqslant \exp\Big(-(1+\log^2\alpha^{-1})\,\exp\big(O\big(K^{-1}(1+\log K)^3L^3\log L\big)\big)\Big).$$

However, $K^{-1}(1+\log K)^3 = O(1)$, whence we get the result. □

It may seem bizarre to have thrown away the extra strength of the $K^{-1}(1+\log K)^3$ term at the very end of this proof. However, in applications we shall have a dichotomy between the case when K is large and when K is small. In the latter we shall not, in fact, be able to guarantee that K is much bigger than 1 whence the above estimate of $K^{-1}(1+\log K)^3 = O(1)$ is tight.

11. Proof of Theorem 3.4

As will have become clear the proof of Theorem 3.4 is iterative and is driven by Lemma 10.1 and Corollary 7.3.

Proof of Theorem 3.4. Let $H_0 := \operatorname{im}2$ and $\mathscr{A}_0$ be the family corresponding to the set A, which has density $\alpha_0=\alpha$. We shall define a sequence of families $(\mathscr{A}_i)_i$ on subgroups $(H_i)_i$ with density α_i and the properties:

$$\Lambda(\mathscr{A}_{i+1}) \leqslant 2^{-4}\Lambda(\mathscr{A}_i) \leqslant 2^{-4i}\Lambda(A), \qquad \alpha_{i+1}\geqslant \alpha_i\big(1+\Omega(\alpha_i\log^{1/6}\alpha_i^{-1}\log\log^{-5/3}\alpha_i^{-1})\big).$$

It is useful to define auxiliary variables K_i and L_i such that

$$C_{\mathcal{G}} L_i^3 \log^2 L_i = \log \alpha_i^{-1}/2 \quad \text{and} \quad K_i := \alpha_i^{-2} \|f_{\mathcal{A}_i}\|_{L^2(H_i)}^2.$$

Suppose that we are at stage i of the iteration; we consider two cases:

(i) If $L_i \leqslant 2 + K_i^2/(1+\log K_i)^2$ then apply Corollary 7.3 and terminate the iteration with

$$\Lambda(\mathcal{A}_i) = \exp\bigl(-O(\alpha_i^{-1} K_i^{-1} \log^2 K_i)\bigr) = \exp\bigl(-O(\alpha^{-1} \log^{-1/6} \alpha^{-1} \log\log^{5/3} \alpha^{-1})\bigr).$$

(ii) If $L_i > 2 + K_i^2/(1+\log K_i)^2$ then apply Lemma 10.1 with parameter L_i. If we have the first conclusion of the lemma then

$$\Lambda(\mathcal{A}_i) \geqslant \exp\bigl(-(1+\log \alpha_i^{-1})^2 \exp(C_{\mathcal{G}} L_i^3 \log^2 L_i)\bigr).$$

In view of the definition of L_i and the fact that $\alpha_i \geqslant \alpha$ we conclude that $\exp(C_{\mathcal{G}} L_i^3 \log^2 L_i) \leqslant \alpha^{-1/2}$, whence we certainly have

$$\Lambda(\mathcal{A}_i) = \exp\bigl(-O(\alpha^{-1} \log^{-1/6} \alpha^{-1} \log\log^{5/3} \alpha^{-1})\bigr)$$

again. The other conclusion of Lemma 10.1 tells us that we have a new subgroup $H_{i+1} \leqslant H_i$, and a family $\mathcal{A}_{i+1}$ on H_{i+1} with

$$\alpha_{i+1} \geqslant \alpha_i(1 + (L_i/4K_i)\alpha^{-1}) \quad \text{and} \quad \Lambda(\mathcal{A}_{i+1}) \geqslant 2^{-4}\Lambda(\mathcal{A}_i);$$

this has the desired property for the iteration.

In view of the lower bound on α_i we see that the density doubles in

$$F(\alpha) = O(\alpha^{-1} \log^{-1/6} \alpha^{-1} \log\log^{5/3} \alpha^{-1})$$

steps, whence the iteration must terminate in at most $F(\alpha) + F(2\alpha) + F(2^2\alpha) + \cdots$ steps. Of course $F(2\alpha') \leqslant F(\alpha')/\sqrt{2}$ whenever $\alpha' \in (0, c_0]$ for some absolute constant c_0. Thus, on summing the geometric progression we see that the iteration terminates in $O(F(\alpha))$ steps. It follows that at the time of termination we have

$$\Lambda(A) \geqslant \exp\bigl(-O(\alpha^{-1} \log^{-1/6} \alpha^{-1} \log\log^{5/3} \alpha^{-1})\bigr)\Lambda(\mathcal{A}_i),$$

and we get the result. □

12. Concluding remarks

No doubt some improvement could be squeezed out of our arguments by more judicious averaging, but there is a natural limit placed on the method by Corollary 8.2, and it seems that to move the $1/6$ in Theorem 3.4 past 1 would require a new idea. This, however, is a little frustrating for the following reason.

The well-known Erdős–Turán conjecture is essentially equivalent to asking for Roth's theorem in $\mathbb{Z}/N\mathbb{Z}$ for any set of density $\delta(N)$, where $\delta(N)$ is a function with $\sum_N N^{-1}\delta(N) = \infty$. In particular, $\delta(N) = 1/\log N \log\log N \log\log\log N$ satisfies this hypothesis and so to have the analogue of the Erdős–Turán conjecture in $\mathbb{Z}_4^n$ we would need to push the constant $1/6$ past 1.

In light of the heuristic in Section 4 one might reasonably conjecture the following much stronger result.

Conjecture 12.1. *Suppose that $G = \mathbb{Z}_4^n$ and $A \subset G$ contains no proper three-term arithmetic progressions. Then $|A| = O\big(|G|/\log^{3/2}|G|\big)$.*

Of course much more may be true. We were able to find the following lower bound; as with $\mathbb{Z}_3^n$, where the best lower bound is due to Edel [2004] (see also [Lin and Wolf 2009]), its density is of power shape.

Proposition 12.2. *Suppose that $G = \mathbb{Z}_4^n$. Then there is a set $A \subset G$ with no proper three-term arithmetic progressions and $|A| = \Omega(|G|^{2/3})$.*

Proof. The set

$$A_0 = \big\{ \begin{array}{l} (0,0,0),\ (0,0,1),\ (0,1,0),\ (0,1,2),\ (0,2,1),\ (0,2,2),\ (1,0,0),\ (1,0,2), \\ (1,2,0),\ (1,2,2),\ (2,0,1),\ (2,0,2),\ (2,1,0),\ (2,1,2),\ (2,2,0),\ (2,2,1) \end{array} \big\}$$

in $\mathbb{Z}_4^3$ has size 16 and contains no proper three-term arithmetic progressions. The result now follows on noting that the product of two sets not containing any proper three-term arithmetic progressions does, itself, not contain any proper three-term arithmetic progressions:

Suppose that B and C are such sets and $(x_0, x_1), (y_0, y_1), (z_0, z_1) \in B \times C$ have $x + y = 2z$. Then $x_i + y_i = 2z_i$ for $i \in \{0, 1\}$. However since B and C do not contain any proper progressions we have $x_i = y_i$ for all $i \in \{0, 1\}$ whence $x = y$ and so the progression is not proper. □

We are unaware of any serious search for better choices of A_0, though they may exist. Indeed, recently Elsholtz observed that a more general construction designed for Moser's cube problem can be used.

Moser asked for large subsets of $\{0, 1, 2\}^n$ not containing three points on a line; Komlós and Chvátal [Chvátal 1972] note that the sets

$$S_n := \big\{x \in \{0, 1, 2\}^n : x_i = 1 \text{ for } \lfloor n/3 \rfloor \text{ values of } i \in [n]\big\}$$

have size $\Omega(3^n/\sqrt{n})$ by Stirling's formula and satisfy Moser's requirement. Our set A_0 is equal to S_3. Embedding S_n in $\mathbb{Z}_4^n$ in the obvious way it may be checked that the lack of lines in S_n yields a set containing no proper three-term arithmetic progressions and hence the following theorem.

Theorem 12.3 [Elsholtz 2008, Theorem 3]. *Suppose that $G = \mathbb{Z}_4^n$. Then there is a set $A \subset G$ with no proper three-term arithmetic progressions and*

$$|A| = \Omega\big(|G|^{\log 3/\log 4}/\sqrt{\log|G|}\big).$$

The reader may wish to know that $\log 3/\log 4 = 0.792\ldots$. The details along with some other results and generalisations are supplied in Elsholtz's paper.

Acknowledgments

The author thanks Ernie Croot for a number of very useful conversations, Christian Elsholtz for supplying the preprint [Elsholtz 2008], Olof Sisask for writing a program to find the example in Proposition 12.2, Terry Tao for useful comments and two anonymous referees for useful comments and careful reading.

References

[Balog and Szemerédi 1994] A. Balog and E. Szemerédi, "A statistical theorem of set addition", *Combinatorica* **14**:3 (1994), 263–268. MR 95m:11019 Zbl 0812.11017

[Bourgain 1999] J. Bourgain, "On triples in arithmetic progression", *Geom. Funct. Anal.* **9**:5 (1999), 968–984. MR 2001h:11132 Zbl 0959.11004

[Bourgain 2008] J. Bourgain, "Roth's theorem on progressions revisited", *J. Anal. Math.* **104** (2008), 155–192. MR 2009g:11011 Zbl 1155.11011

[Brown and Buhler 1984] T. C. Brown and J. P. Buhler, "Lines imply spaces in density Ramsey theory", *J. Combin. Theory Ser. A* **36**:2 (1984), 214–220. MR 85d:05068 Zbl 0532.05002

[Chvátal 1972] V. Chvátal, "Remarks on a problem of Moser", *Canad. Math. Bull.* **15** (1972), 19–21. MR 47 #1642 Zbl 0232.05002

[Croot 2007] E. S. Croot, "On the decay of the Fourier transform and three term arithmetic progressions", *Online J. Anal. Comb.* **2** (2007), Art. 6, 10 pp. MR 2008h:11011 Zbl 1145.11015

[Croot 2008] E. S. Croot, "Subsets of $\mathbb{F}_p^n$ without three term arithmetic progressions have several large Fourier coefficients.", preprint, 2008.

[Croot and Lev 2007] E. S. Croot and V. F. Lev, "Open problems in additive combinatorics", pp. 207–233 in *Additive combinatorics*, edited by A. Granville et al., CRM Proc. Lecture Notes **43**, Amer. Math. Soc., Providence, RI, 2007. MR 2009d:11038 Zbl 05219607

[Edel 2004] Y. Edel, "Extensions of generalized product caps", *Des. Codes Cryptogr.* **31**:1 (2004), 5–14. MR 2004m:51021 Zbl 1057.51005

[Edel et al. 2007] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, and L. Rackham, "Zero-sum problems in finite abelian groups and affine caps", *Q. J. Math.* **58**:2 (2007), 159–186. MR 2008g:11017 Zbl 05190260

[Elsholtz 2008] C. Elsholtz, "Lower bounds for Roth's theorem in $\mathbb{Z}_4^n$", preprint, 2008.

[Frankl et al. 1987] P. Frankl, R. L. Graham, and V. Rödl, "On subsets of abelian groups with no 3-term arithmetic progression", *J. Combin. Theory Ser. A* **45**:1 (1987), 157–161. MR 88f:05018 Zbl 0613.10043

[Freĭman 1973] G. A. Freĭman, *Foundations of a structural theory of set addition*, Translations of Mathematical Monographs **37**, American Mathematical Society, Providence, R. I., 1973. MR 50 #12944 Zbl 0271.10044

[Gowers 1998] W. T. Gowers, "A new proof of Szemerédi's theorem for arithmetic progressions of length four", *Geom. Funct. Anal.* **8**:3 (1998), 529–551. MR 2000d:11019 Zbl 0907.11005

[Green 2005] B. Green, "Finite field models in additive combinatorics", pp. 1–27 in *Surveys in combinatorics 2005*, edited by B. S. Webb, London Math. Soc. Lecture Note Ser. **327**, Cambridge Univ. Press, 2005. MR 2006j:11030 Zbl 1155.11306

[Green and Tao 2009] B. Green and T. Tao, "A note on the Freiman and Balog–Szemerédi–Gowers theorems in finite fields", *J. Aust. Math. Soc.* **86**:1 (2009), 61–74. MR 2495998 Zbl 05550054

[Heath-Brown 1987] D. R. Heath-Brown, "Integer sets containing no arithmetic progressions", *J. London Math. Soc.* (2) **35**:3 (1987), 385–394. MR 88g:11005 Zbl 0589.10062

[Lev 2004] V. F. Lev, "Progression-free sets in finite abelian groups", *J. Number Theory* **104**:1 (2004), 162–169. MR 2004k:11023 Zbl 1043.11022

[Lin and Wolf 2009] Y. Lin and J. Wolf, "Subsets of $\mathbb{F}_q^n$ containing no k-term progressions", preprint, 2009.

[Meshulam 1995] R. Meshulam, "On subsets of finite abelian groups with no 3-term arithmetic progressions", *J. Combin. Theory Ser. A* **71**:1 (1995), 168–172. MR 96g:20033 Zbl 0832.11006

[Roth 1952] K. Roth, "Sur quelques ensembles d'entiers", *C. R. Acad. Sci. Paris* **234** (1952), 388–390. MR 13,724d Zbl 0046.04302

[Roth 1953] K. F. Roth, "On certain sets of integers", *J. London Math. Soc.* **28** (1953), 104–109. MR 14,536g Zbl 0050.04002

[Rudin 1962] W. Rudin, *Fourier analysis on groups*, Wiley, New York, 1962. Reprinted 1990 in the Wiley Classics Library. MR 27 #2808 Zbl 0107.096

[Ruzsa 1999] I. Z. Ruzsa, "An analog of Freiman's theorem in groups", pp. 323–326 in *Structure theory of set addition*, edited by J.-M. Deshouillers et al., Astérisque **258**, Soc. Math. de France, Paris, 1999. MR 2000h:11111 Zbl 0946.11007

[Szemerédi 1990] E. Szemerédi, "Integer sets containing no arithmetic progressions", *Acta Math. Hungar.* **56**:1-2 (1990), 155–158. MR 92c:11100 Zbl 0721.11007

[Tao 2008] T. Tao, *Structure and randomness: pages from year one of a mathematical blog*, American Mathematical Society, Providence, RI, 2008. MR 2459552

[Tao and Vu 2006] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics **105**, Cambridge University Press, 2006. MR 2008a:11002 Zbl 1127.11002

[Varnavides 1959] P. Varnavides, "On certain sets of positive density", *J. London Math. Soc.* **34** (1959), 358–360. MR 21 #5595 Zbl 0088.25702

[Yekhanin and Dumer 2004] S. Yekhanin and I. Dumer, "Long nonbinary codes exceeding the Gilbert–Varshamov bound for any fixed distance", *IEEE Trans. Inform. Theory* **50**:10 (2004), 2357–2362. MR 2097052

Received 14 Nov 2008. Revised 30 Mar 2009. Accepted 4 May 2009.

TOM SANDERS: t.sanders@dpmms.cam.ac.uk
Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Cambridge, CB3 0WA, United Kingdom
http://www.dpmms.cam.ac.uk/∼tws22/