

On Roth’s theorem on progressions

By TOM SANDERS

Abstract

We show that if $A \subset \{1, \dots, N\}$ contains no nontrivial three-term arithmetic progressions then $|A| = O(N/\log^{1-o(1)} N)$.

1. Introduction

In this paper we prove the following version of Roth’s theorem on arithmetic progressions [Rot52], [Rot53].

THEOREM 1.1. *Suppose that $A \subset \{1, \dots, N\}$ contains no nontrivial three-term arithmetic progressions. Then*

$$|A| = O\left(\frac{N(\log \log N)^5}{\log N}\right).$$

There are numerous detailed expositions and proofs of Roth’s theorem and the many related results, so we shall not address ourselves to a comprehensive history here. Briefly, the first nontrivial upper bound on the size of such sets was given by Roth [Rot52], [Rot53], and there then followed refinements by Heath-Brown [HB87] and Szemerédi [Sze90], and later Bourgain [Bou99], culminating in the above with the power $1/2$ in place of 1 (up to doubly logarithmic factors).

Bourgain then introduced a new sampling technique in [Bou08] which was refined in [San10] to give the previous best bound which had a power of $3/4$ (again up to doubly logarithmic factors) in place of 1 . The methods of this paper, however, are largely unrelated to these last developments. We do still use the Bohr set technology of Bourgain [Bou99], but couple this with two new tools: the first is motivated by the arguments of Katz and Koester in [KK10] and is a sort of variant of the Dyson e -transform; the second is a result on the L^p -invariance of convolutions due to Croot and Sisask [CS10a].

For comparison with these upper bounds, Salem and Spencer [SS42] showed that the surface of high-dimensional convex bodies can be embedded in the integers to construct sets of size $N^{1-o(1)}$ containing no three-term progressions, and Behrend [Beh46] noticed that spheres are a particularly good choice. Recently Elkin [Elk10] tweaked this further by thickening the spheres to produce

the largest known progression-free sets, and his argument was then considerably simplified by Green and Wolf in the very short and readable note [GW10].

2. Notation

Suppose that G is a finite abelian group. We write $M(G)$ for the space of measures on G , and given a measure $\mu \in M(G)$ and a function $f \in L^1(\mu)$ we write $f d\mu$ for the measure induced by

$$C(G) \rightarrow C(G); g \mapsto \int g(x)f(x)d\mu(x).$$

There is a privileged measure $\mu_G \in M(G)$ called Haar probability measure, defined to be the measure assigning mass $|G|^{-1}$ to each element of G .

The significance of this measure is that it is the unique (up to scaling) translation invariant measure on G : for $x \in G$ and $\mu \in M(G)$ we define $\tau_x(\mu)$ to be the measure induced by

$$C(G) \rightarrow C(G); f \mapsto \int f(y)d\mu(y+x),$$

and it is easy to see that $\tau_x(\mu_G) = \mu_G$ for all $x \in G$.

Translation can be usefully averaged by convolution: given two measures $\mu, \nu \in M(G)$ define their convolution $\mu * \nu$ to be the measure induced by

$$C(G) \rightarrow C(G); f \mapsto \int f(x+y)d\mu(x)d\nu(y).$$

We use Haar measure to pass between the notion of function $f \in L^1(\mu_G)$ and measure $\mu \in M(G)$. Indeed, since G is finite we shall often identify μ with $d\mu/d\mu_G$, the Radon-Nikodym derivate of μ with respect to μ_G . In light of this we can easily extend the notion of translation and convolution to $L^1(\mu_G)$: given $f \in L^1(\mu_G)$ and $x \in G$ we define the translation of f by x point-wise by

$$\tau_x(f)(y) := \frac{d(\tau_x(fd\mu_G))}{d\mu_G}(y) = f(x+y) \text{ for all } y \in G;$$

given $f, g \in L^1(\mu_G)$ we define convolution of f and g point-wise by

$$f * g(x) := \frac{d((fd\mu_G) * (gd\mu_G))}{d\mu_G}(x) = \int f(y)g(x-y)d\mu_G(y)$$

and similarly for the convolution of $f \in L^1(\mu_G)$ with $\mu \in M(G)$.

Convolution operators can be written in a particularly simple form with respect to the Fourier basis which we now recall. We write \widehat{G} for the dual group, that is the finite Abelian group of homomorphisms $\gamma : G \rightarrow S^1$, where $S^1 := \{z \in \mathbb{C} : |z| = 1\}$. Given $\mu \in M(G)$ we define $\widehat{\mu} \in \ell^\infty(\widehat{G})$ by

$$\widehat{\mu}(\gamma) := \int \bar{\gamma} d\mu \text{ for all } \gamma \in \widehat{G},$$

and extend this to $f \in L^1(G)$ by $\widehat{f} := \widehat{fd\mu_G}$. It is easy to check that $\widehat{\mu * \nu} = \widehat{\mu} \cdot \widehat{\nu}$ for all $\mu, \nu \in M(G)$ and $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$ for all $f, g \in L^1(\mu_G)$.

Throughout the paper C 's will denote absolute, effective, but unspecified constants of size greater than 1 and c s will denote the same of size at most 1. Typically the constants will be subscripted according to the result from which they come and superscripted within arguments.

3. Fourier analysis on Bohr sets

Fourier analysis on Bohr sets was introduced to additive combinatorics by Bourgain in [Bou99] and has since become a fundamental tool. The material is standard so we shall import the results we require from [San10] without comment; for a more detailed discussion the reader may wish to consult the book [TV06] of Tao and Vu.

A set B is called a *Bohr set* with *frequency set* $\Gamma \subset \widehat{G}$ and *width function* $\delta \in (0, 2]^\Gamma$ if

$$B = \{x \in G : |1 - \gamma(x)| \leq \delta_\gamma \text{ for all } \gamma \in \Gamma\}.$$

The size of the set Γ is called the *rank* of B and is denoted $\text{rk}(B)$.

There is a natural way of dilating Bohr sets which will be of particular use to us. Given such a B and $\rho \in \mathbb{R}^+$ we shall write B_ρ for the Bohr set with frequency set Γ and width function¹ $\rho\delta$ so that, in particular, $B = B_1$.

With these dilates we say that a Bohr set B' is a *sub-Bohr set* of another Bohr set B and write $B' \leq B$, if

$$B' \subset B_\rho \text{ for all } \rho \in \mathbb{R}^+.$$

Finally, we write β_ρ for the probability measure induced on B_ρ by μ_G , and β for β_1 .

3.1. *Size and regularity of Bohr sets.* The rank of a Bohr set is closely related to its dimension: a Bohr set B is said to be *d-dimensional* if

$$\mu_G(B_{2\rho}) \leq 2^d \mu_G(B_\rho) \text{ for all } \rho \in (0, 1],$$

and we have the following standard averaging argument; see [TV06, Lemma 4.20].

LEMMA 3.2 (Dimension of Bohr sets). *Suppose that B is a rank k Bohr set. Then it is $O(k)$ -dimensional.*

¹Technically, width function $\gamma \mapsto \min\{\rho\delta_\gamma, 2\}$.

A key observation of [Bou99] was that some Bohr sets behave better than others: a d -dimensional Bohr set is said to be C -regular if

$$\frac{1}{1 + Cd|\eta|} \leq \frac{\mu_G(B_{1+\eta})}{\mu_G(B_1)} \leq 1 + Cd|\eta| \text{ for all } \eta \text{ with } |\eta| \leq 1/Cd.$$

Crucially, regular Bohr sets are plentiful:

LEMMA 3.3 (Regular Bohr sets). *There is an absolute constant $C_{\mathcal{R}}$ such that whenever B is a Bohr set, there is some $\lambda \in [1/2, 1)$ such that B_λ is $C_{\mathcal{R}}$ -regular.*

The result is proved by a covering argument due to Bourgain [Bou99]; for details one may also consult [TV06, Lemma 4.25]. For the remainder of the paper we shall say *regular* for $C_{\mathcal{R}}$ -regular.

3.4. *The large spectrum.* Given a probability measure μ , a function $f \in L^1(\mu)$ and a parameter $\varepsilon \in (0, 1]$ we define the ε -spectrum of f with respect to μ to be the set

$$\text{Spec}_\varepsilon(f, \mu) := \{\gamma \in \widehat{G} : |(fd\mu)^\wedge(\gamma)| \geq \varepsilon \|f\|_{L^1(\mu)}\}.$$

This definition extends the usual one from the case $\mu = \mu_G$. We shall need a local version of a result of Chang [Cha02] for estimating the ‘complexity’ or ‘entropy’ of the large spectrum.

Conceptually the next definition is inspired by the discussion of quadratic rank Gowers and Wolf give in [GW10]. The (K, μ) -relative entropy of a set Γ is the size of the largest subset $\Lambda \subset \Gamma$ such that

$$\int \prod_{\lambda \in \Lambda} (1 + \text{Re } \omega(\lambda)\lambda) d\mu \leq \exp(K) \text{ for all } \omega : \Lambda \rightarrow D,$$

where $D := \{z \in \mathbb{C} : |z| \leq 1\}$. The definition is essentially relativising the notion of being dissociated (if $\mu = \mu_G$ and $K = 0$, it is precisely this), but the reader does not need to have a deep understanding for the purposes of this paper, as it is only used to couple the next two results from [San10] into Lemma 3.8.

LEMMA 3.5 (The Chang bound, [San10, Lemma 4.6]). *Suppose that $0 \neq f \in L^2(\mu)$. Then $\text{Spec}_\varepsilon(f, \mu)$ has $(1, \mu)$ -relative entropy*

$$O(\varepsilon^{-2} \log 2 \|f\|_{L^2(\mu)} \|f\|_{L^1(\mu)}^{-1}).$$

Low entropy sets of characters are majorised by large Bohr sets, a fact encoded in the following lemma.

LEMMA 3.6 ([San10, Cor. 6.4]). *Suppose that B is a regular d -dimensional Bohr set and Δ is a set of characters with (η, β) -relative entropy k . Then there*

is a Bohr set $B' \leq B$ with

$$\text{rk}(B') \leq \text{rk}(B) + k \text{ and } \mu_B(B') \geq (\eta/2dk)^{O(d)}(1/2k)^{O(k)}$$

such that $|1 - \gamma(x)| \leq 1/2$ for all $x \in B'$ and $\gamma \in \Delta$.

3.7. *The energy increment method.* The final lemma of the section encodes the Heath-Brown-Szemerédi energy increment technique from [HB87], [Sze90] which shows how to get a density increment on a Bohr set from large energy on a large spectrum.

LEMMA 3.8. *Suppose that B is a regular d -dimensional Bohr set, $A \subset B$ has density $\alpha > 0$, $B' \subset B_{\rho'}$ is a regular rank k Bohr set, $T \subset B'$ has relative density τ and*

$$\sum_{\gamma \in \text{Spec}_\eta(1_T, \beta')} |((1_A - \alpha)1_B)^\wedge(\gamma)|^2 \geq \nu\alpha^2\mu_G(B).$$

Then there is a regular Bohr set B'' with

$$\text{rk}(B'') \leq k + O(\eta^{-2} \log 2\tau^{-1}) \text{ and } \mu_{B'}(B'') \geq \left(\frac{\eta}{2k \log 2\tau^{-1}}\right)^{O(k + \eta^{-2} \log 2\tau^{-1})}$$

such that $\|1_A * \beta''\|_{L^\infty(\mu_G)} \geq \alpha(1 + \Omega(\nu))$ provided $\rho' \leq c_{3.8}\nu\alpha/d$.

Proof. By Lemma 3.5 the set $\text{Spec}_\eta(1_T, \beta')$ has $(1, \beta')$ -relative entropy $O(\eta^{-2} \log 2\tau^{-1})$. The dimension of B' is $O(k)$ so it follows by Lemma 3.6 that there is a Bohr set $B'' \leq B'$ with

$$\text{rk}(B'') \leq k + O(\eta^{-2} \log 2\tau^{-1}) \text{ and } \mu_{B'}(B'') \geq \left(\frac{\eta}{2k \log 2\tau^{-1}}\right)^{O(k + \eta^{-2} \log 2\tau^{-1})}$$

such that

$$\text{Spec}_\eta(1_T, \beta') \subset \{\gamma : |1 - \gamma(x)| \leq 1/2 \text{ for all } x \in B''\}.$$

By the triangle inequality and Parseval's theorem it follows that

$$\begin{aligned} \Omega(\nu\alpha^2\mu_G(B)) &= \sum_{\gamma \in \widehat{G}} |((1_A - \alpha)1_B)^\wedge(\gamma)|^2 |\widehat{\beta''}(\gamma)|^2 \\ &= \|(1_A - \alpha)1_B * \beta''\|_{L^2(\mu_G)}^2. \end{aligned}$$

Since $B'' \leq B' \subset B_{\rho'}$ and B is regular, we have that

$$\|(1_A - \alpha)1_B * \beta''\|_{L^2(\mu_G)}^2 = \|1_A * \beta''\|_{L^2(\mu_G)}^2 - \alpha^2\mu_G(B) + O(\alpha\rho'd\mu_G(B)).$$

It follows that if ρ' is sufficiently small, then

$$\|1_A * \beta''\|_{L^2(\mu_G)}^2 \geq \alpha^2(1 + \Omega(\nu))\mu_G(B),$$

and we get the result by Hölder's inequality. □

4. Katz-Koester and the Dyson e -transform

In [KK10] Katz and Koester introduced a new way of transforming sumsets. This method has seen impressive applications in, for example, [Sch11] and [SS11], and is particularly ripe for iteration. The arguments of this section evolved from these Katz-Koester techniques but in their final form may be seen to have more in common with the Dyson e -transform (see e.g. [TV06, §5.1]). In any case, from our perspective what is important is that it provides a sort of density increment without the cost of passing to an approximate subgroup.

Specifically, our aim is to transform the set A in Roth's theorem into two sets L and S where L is thick, S is not too thin, and $L + S \subset A - 2A$. This dovetails with the regime of strength of the results in the next section.

The main idea is to construct such sets L and S iteratively using the Katz-Koester transformation. Suppose that L, S, A and A' are sets of density λ, σ, α and α' respectively and $L + S \subset A + A'$. Unless A is 'quite structured' one expects there to be very few x for which

$$1_L * 1_{-A}(x) \geq \alpha/2;$$

on the other hand, by averaging, there are many $x \in G$ such that

$$1_{-S} * 1_{A'}(x) \geq \sigma\alpha'/2.$$

It follows that unless A is 'quite structured,' one may find an $x \in G$ such that

$$1_L * 1_{-A}(x) \leq \alpha/2 \text{ and } 1_{-S} * 1_{A'}(x) \geq \sigma\alpha'/2.$$

Now, if we put

$$L' := L \cup (x + A) \text{ and } S' := S \cap (A' - x),$$

then we have

$$\mu_G(L') \geq \mu_G(L) + \mu_G(x + A) - 1_L * 1_{-A}(x) \geq \lambda + \alpha/2 \text{ and } \mu_G(S') \geq \alpha'\sigma/2$$

and also

$$L' + S' \subset (L + S') \cup ((x + A) + S') \subset (L + S) \cup (x + A + A' - x) \subset A + A'.$$

We see that unless A is quite structured, we have a new pair (L', S') whose sumset is contained in $A + A'$, but for which L' is somewhat larger (than L) while S' is not too much smaller (than S).

The actual result we require is the following relativised and weighted version of the above.

PROPOSITION 4.1. *Suppose that B is a regular d -dimensional Bohr set, B' is a regular rank k Bohr set with $B' \subset B_{\rho'}$, $B'' \subset B'_{\rho''}$, $A \subset B$ has relative density α and $A' \subset B'$ has relative density α' . Then either*

- (i) there is a regular Bohr set B''' of rank at most $k + O(\alpha^{-1} \log 2\alpha'^{-1})$ with

$$\mu_{B'}(B''') \geq \left(\frac{\alpha}{2k \log 2\alpha'^{-1}} \right)^{O(k + \alpha^{-1} \log 2\alpha'^{-1})}$$

and $\|1_A * \beta'''\|_{L^\infty(\mu_G)} \geq \alpha(1 + \Omega(1))$,

- (ii) or there are sets $L \subset B$ and $S \subset B''$ with $\beta(L) = \Omega(1)$ and $\beta''(S) \geq (\alpha'/2)^{O(\alpha^{-1})}$ such that

$$1_L * (1_S d\beta'')(x) \leq C_{4.1} \alpha^{-1} \mu_{B'}(B'')^{-1} 1_A * (1_{A'} d\beta')(x)$$

for all $x \in G$,

provided $\rho' \leq c_{4.2} \alpha/d$ and $\rho'' \leq c_{4.2} \alpha'/k$.

The proof is an iteration of the following lemma.

LEMMA 4.2. Suppose that B is a regular d -dimensional Bohr set, B' is a regular rank k Bohr set with $B' \subset B_{\rho'}$, $B'' \subset B'_{\rho''}$, $A \subset B$ has relative density α and $A' \subset B'$ has relative density α' .

If, additionally, there is a set $L \subset B$ of relative density λ and $S \subset B''$ of relative density σ , then either

- (i) there is a regular Bohr set B''' of rank at most $k + O(\alpha^{-1} \log 2\alpha'^{-1})$ with

$$\mu_{B'}(B''') \geq \left(\frac{\alpha}{2k \log 2\alpha'^{-1}} \right)^{O(k + \alpha^{-1} \log 2\alpha'^{-1})}$$

and $\|1_A * \beta'''\|_{L^\infty(\mu_G)} \geq \alpha(1 + \Omega(1))$,

- (ii) or there are sets $L' \subset B$ and $S' \subset B''$ with $\beta(L') \geq \lambda + \alpha/4$ and $\beta''(S') \geq \alpha'\sigma/2$ such that

$$1_{L'} * (1_{S'} d\beta'')(x) \leq 1_L * (1_S d\beta'')(x) + \mu_{B'}(B'')^{-1} 1_A * (1_{A'} d\beta')(x)$$

for all $x \in G$,

provided $\lambda \leq c_{4.2}$, $\rho' \leq c_{4.2} \alpha/d$ and $\rho'' \leq c_{4.2} \alpha'/k$.

Proof. We put

$$\mathcal{L} := \{x \in B' : 1_{-L} * (1_A d\beta)(-x) \geq \alpha/2\}$$

and split into two cases. First, when $\beta'(\mathcal{L})$ is large we shall show that A has a density increment on a Bohr set; secondly, when it is small we shall proceed as per the heuristic at the start of the section.

CASE. $\beta'(\mathcal{L}) \geq \alpha'/8$.

Proof. This is a textbook translation of a physical space condition into a density increment via the Fourier transform. We consider the inner product

$$\alpha \beta'(\mathcal{L})/2 \leq \langle 1_{-L} * (1_A d\beta), 1_{-\mathcal{L}} \rangle_{L^2(\beta')}.$$

By regularity we have that if ρ' is sufficiently small then

$$|\langle 1_{-L} * \beta, 1_{-\mathcal{L}} \rangle_{L^2(\beta')} - \lambda \beta'(\mathcal{L})| \leq \beta'(\mathcal{L})/4.$$

It follows by the triangle inequality that

$$|\langle 1_{-L} * ((1_A - \alpha)d\beta), 1_{-\mathcal{L}} \rangle_{L^2(\beta')}| \geq \alpha \beta'(\mathcal{L})(1/4 - \lambda) \geq \alpha \beta'(\mathcal{L})/8$$

if λ is sufficiently small. By Fourier inversion and rescaling we then have

$$\left| \sum_{\gamma \in \widehat{G}} \widehat{1_{-L}}(\gamma) (1_A - \alpha 1_B)^\wedge(\gamma) \overline{\widehat{1_{-\mathcal{L}}d\beta'}(\gamma)} \right| \geq \alpha \beta'(\mathcal{L}) \mu_G(B)/8.$$

By Cauchy-Schwarz and Parseval on the sum of $|\widehat{1_{-L}}(\gamma)|^2$ we get that

$$\sum_{\gamma \in \widehat{G}} |(1_A - \alpha 1_B)^\wedge(\gamma)|^2 |\widehat{1_{-\mathcal{L}}d\beta'}(\gamma)|^2 \geq \alpha^2 \beta'(\mathcal{L})^2 \mu_G(B)/64.$$

On the other hand, Parseval's theorem tells us that if $\eta := \sqrt{\alpha}/16$, then

$$\sum_{\gamma \notin \text{Spec}_\eta(1_{-\mathcal{L}}, \beta')} |(1_A - \alpha 1_B)^\wedge(\gamma)|^2 |\widehat{1_{-\mathcal{L}}d\beta'}(\gamma)|^2 \leq \alpha^2 \beta'(\mathcal{L})^2 \mu_G(B)/16^2.$$

Thus, by the triangle inequality and since $|\widehat{1_{-\mathcal{L}}d\beta'}(\gamma)| \leq \beta'(\mathcal{L})$, we get that

$$\sum_{\gamma \in \text{Spec}_\eta(1_{-\mathcal{L}}, \beta')} |(1_A - \alpha 1_B)^\wedge(\gamma)|^2 = \Omega(\alpha^2 \mu_G(B)).$$

It follows by Lemma 3.8 that we are in the first case of the lemma provided ρ' is sufficiently small. □

CASE. $\beta'(\mathcal{L}) \leq \alpha'/8$.

Proof. First we show that the set

$$\mathcal{S} := \{x \in B' : (1_{-S}d\beta'') * 1_{A'}(x) \geq \alpha' \sigma/2\}$$

is large by averaging. In particular,

$$\beta'(\mathcal{S})\sigma + \alpha' \sigma/2 \geq \int (1_{-S}d\beta'') * 1_{A'}d\beta' = \int 1_{A'}d((1_{-S}d\beta'') * \beta').$$

Of course, by regularity we have that

$$\|(1_{-S}d\beta'') * \beta' - \sigma \beta'\| = O(\sigma k \rho''),$$

whence

$$\beta'(\mathcal{S}) \geq \alpha'/2 - O(k \rho'') \geq \alpha'/4$$

provided ρ'' is sufficiently small. Now, since \mathcal{L} is assumed to be so small, there must be some $x \in \mathcal{S} \setminus \mathcal{L}$; we put

$$L' := L \cup ((x + A) \cap B) \text{ and } S' := S \cap (A' - x).$$

Now $L' \subset B$, and since $x \notin \mathcal{L}$, we have

$$\beta(L \cap (x + A)) = \beta((-L) \cap (-x - A)) = 1_{-L} * (1_A d\beta)(-x) \leq \alpha/2.$$

But then

$$\beta(L') \geq \lambda + \beta((x + A) \cap B) - \alpha/2 \geq \lambda + \alpha/2 - O(d\rho') \geq \lambda + \alpha/4$$

provided ρ' is sufficiently small. Additionally $S' \subset S \subset B''$ and

$$\beta''(S') = \beta''(S \cap (A' - x)) = (1_{-S} d\beta'') * 1_{A'}(x) \geq \alpha'\sigma/2,$$

and finally

$$\begin{aligned} 1_{L'} * (1_{S'} d\beta'') &\leq 1_L * (1_{S'} d\beta'') + 1_{x+A} * (1_{S'} d\beta'') \\ &\leq 1_L * (1_S d\beta'') + \mu_G(B'')^{-1} 1_{x+A} * 1_{A'-x} \\ &= 1_L * (1_S d\beta'') + \mu_{B'}(B'')^{-1} 1_A * (1_{A'} d\beta') \end{aligned} \quad \square$$

as required.

The completes the proof of Lemma 4.2. □

Proof of Proposition 4.1. We produce a sequence of sets $(L_i)_i$ and $(S_i)_i$ iteratively with $L_i \subset B$, $S_i \subset B''$, $\lambda_i := \beta(L_i)$ and $\sigma_i := \beta''(S_i)$ such that

$$(4.1) \quad \lambda_i \geq \alpha i/4 \text{ and } \sigma_i \geq (\alpha'/2)^{i+1}$$

and

$$(4.2) \quad 1_{L_i} * (1_{S_i} d\beta'') \leq i \mu_{B'}(B'')^{-1} 1_A * (1_{A'} d\beta').$$

To initialise the iteration we consider the inner product

$$\int 1_{A'} * \beta'' d\beta' = \alpha' + O(\rho''k).$$

Thus, if ρ'' is sufficiently small, then it follows that there is some $x \in B' \subset B$ such that

$$\beta''(B'' \cap (A' - x)) \geq \alpha'/2.$$

We put $L_0 := \emptyset$ and $S_0 := B'' \cap (A' - x)$ and note that this satisfies (4.1) and (4.2).

We now repeatedly apply Lemma 4.2. If at any point we are in the first case of that lemma, then we terminate in the first case here; otherwise we have the sequence as required. This process terminates after some $i_0 = O(\alpha^{-1})$ steps, when $\lambda_i > c_{4.2} = \Omega(1)$. We set $L := L_{i_0}$ and $S := S_{i_0}$ and the result is proved. □

5. A consequence of the Croot-Sisask lemma

In light of the previous section, rather than counting three-term progressions by examining the inner product $\langle 1_A * 1_A, 1_{2.A} \rangle_{L^2(\mu_G)}$, we shall be able to examine (a relativised version of) $\langle 1_L * 1_S, 1_{2.A} \rangle_{L^2(\mu_G)}$ where L has density $\Omega(1)$, and S , of density σ , is potentially thin but not too thin. To do this we shall find a Bohr set B such that

$$(5.1) \quad \|1_L * \mu_S * \beta - 1_L * \mu_S\|_{L^p(\mu_G)} \leq \varepsilon,$$

so that

$$|\langle 1_L * 1_S * \beta, 1_{2.A} \rangle_{L^2(\mu_G)} - \langle 1_L * 1_S, 1_{2.A} \rangle_{L^2(\mu_G)}| \leq \varepsilon \sigma \|1_{2.A}\|_{L^{p/(p-1)}(\mu_G)}.$$

If the error is small enough this will give rise to a density increment on B ; to get a sense of how small it needs to be we think of the second term on the left as being typically of size $\mu_G(L)\sigma\alpha = \Omega(\sigma\alpha)$. Now,

- (i) if $p = 2$ then $\|1_{2.A}\|_{L^{p/(p-1)}(\mu_G)} = \alpha^{1/2}$ and we would need $\varepsilon \sim \alpha^{1/2}$ for the error term not to swamp the main term;
- (ii) if $p \sim \log \alpha^{-1}$ then $\|1_{2.A}\|_{L^{p/(p-1)}(\mu_G)} \sim \alpha$ so we would only need $\varepsilon \sim 1$ for the error term not to swamp the main term.

Of course, which of these two ranges to use depends on how the size of the Bohr set found varies with p and ε . We shall use an argument of Croot and Sisask [CS10a] to show that we can take

$$(5.2) \quad \mu_G(B) \geq \exp(-O(\varepsilon^{-2} p \log \sigma^{-1}))$$

in (5.1), and so in particular case (ii) above leads to a much larger Bohr set.

This argument of Croot and Sisask is an important new approach for studying the L^p -invariance of convolutions. It relies on random sampling in physical space to approximate a convolution by a small number of translates and works for general groups, not just abelian ones.

We shall now record a version of their result which will be particularly useful to us. For completeness — and since it is simple — we include the proof of the result as well.

LEMMA 5.1 (Croot-Sisask). *Suppose that G is a finite abelian group, $f \in L^p(\mu_G)$ and $A, S \subset G$ have $\mu_G(S+A) \leq K\mu_G(A)$. Then there is an $s \in S$ and a set $T \subset S$ with $\mu_S(T) \geq (2K)^{-O(\varepsilon^{-2}p)}$ such that*

$$\|\tau_t(f * \mu_A) - f * \mu_A\|_{L^p(\mu_G)} \leq \varepsilon \|f\|_{L^p(\mu_G)} \text{ for all } t \in T - s.$$

Proof. Let z_1, \dots, z_k be independent uniformly distributed S -valued random variables, and for each $y \in G$ define $Z_i(y) := \tau_{-z_i}(f)(y) - f * \mu_A(y)$. For fixed y , the variables $Z_i(y)$ are independent and have mean zero, so it follows

by the Marcinkiewicz-Zygmund inequality, with constants due to Yao-Feng and Han-Ying [YFHY01, Th. 2], that

$$\left\| \sum_{i=1}^k Z_i(y) \right\|_{L^p(\mu_A^k)}^p \leq O(p)^{p/2} k^{p/2-1} \sum_{i=1}^k \int |Z_i(y)|^p d\mu_A^k.$$

Integrating over y and interchanging the order of summation we get
(5.3)

$$\int \left\| \sum_{i=1}^k Z_i(y) \right\|_{L^p(\mu_A^k)}^p d\mu_G(y) \leq O(p)^{p/2} k^{p/2-1} \int \sum_{i=1}^k \int |Z_i(y)|^p d\mu_G(y) d\mu_A^k.$$

On the other hand,

$$\begin{aligned} \left(\int |Z_i(y)|^p d\mu_G(y) \right)^{1/p} &= \|Z_i\|_{L^p(\mu_G)} \leq \|\tau_{-z_i}(f)\|_{L^p(\mu_G)}^p \\ &+ \|f * \mu_A\|_{L^p(\mu_G)} \leq 2\|f\|_{L^p(\mu_G)} \end{aligned}$$

by the triangle inequality. Dividing (5.3) by k^p and inserting the above and the expression for the Z_i s we get that

$$\int \int \left| \frac{1}{k} \sum_{i=1}^k \tau_{-z_i}(f)(y) - f * \mu_A(y) \right|^p d\mu_G(y) d\mu_A^k(z) = O(pk^{-1} \|f\|_{L^p(\mu_G)}^2)^{p/2}.$$

Pick $k = O(\varepsilon^{-2}p)$ such that the right-hand side is at most $(\varepsilon\|f\|_{\ell^p(G)}/4)^p$ and write L for the set of $x = (x_1, \dots, x_k) \in A^k$ for which the integrand above is at most $(\varepsilon\|f\|_{\ell^p(G)}/2)^p$; by averaging $\mu_A^k(L^c) \leq 2^{-p}$ and so $\mu_A^k(L) \geq 1 - 2^{-p} \geq 1/2$.

Now, $\Delta := \{(s, \dots, s) : s \in S\}$ has $L + \Delta \subset (A + S)^k$, whence $|L + \Delta| \leq 2K^k|L|$ and so

$$\langle 1_\Delta * 1_{-\Delta}, 1_{-L} * 1_L \rangle_{L^2(\mu_{G^k})} = \|1_L * 1_\Delta\|_{L^2(\mu_{G^k})}^2 \geq |\Delta|^2 |L| / 2K^k,$$

by the Cauchy-Schwarz inequality since the adjoint of $g \mapsto 1_L * g$ is $g \mapsto 1_{-L} * g$ and similarly for $g \mapsto g * 1_\Delta$.

By averaging it follows that at least $|\Delta|^2 / 2K^k$ pairs $(z, y) \in \Delta^2$ have $1_{-L} * 1_L(z - y) > 0$, and hence there is some $s \in S$ such that there is a set $T \subset S$ with $\mu_S(T) \geq 1/2K^k$ and $1_{-L} * 1_L(t, \dots, t) > 0$ for all $t \in T - s$.

Thus for each $t \in T - s$ there is some $z(t) \in L$ and $y(t) \in L$ such that $y(t)_i = z(t)_i + t$ for all i . But then by the triangle inequality we get that

$$\begin{aligned} \|\tau_{-t}(f * \mu_A) - f * \mu_A\|_{L^p(\mu_G)} &\leq \|\tau_{-t} \left(\frac{1}{k} \sum_{i=1}^k \tau_{-z(t)_i}(f) \right) - f * \mu_A\|_{L^p(\mu_G)} \\ &+ \|\tau_{-t} \left(\frac{1}{k} \sum_{i=1}^k \tau_{-z(t)_i}(f) - f * \mu_A \right)\|_{L^p(\mu_G)}. \end{aligned}$$

However, since τ_t is isometric on $L^p(\mu_G)$, we see that

$$\begin{aligned} \|\tau_t(f * \mu_A) - f * \mu_A\|_{L^p(\mu_G)} &\leq \left\| \frac{1}{k} \sum_{i=1}^k \tau_{-y(t)_i}(f) - f * \mu_A \right\|_{L^p(\mu_G)} \\ &\quad + \left\| \frac{1}{k} \sum_{i=1}^k \tau_{-z(t)_i}(f) - f * \mu_A \right\|_{L^p(\mu_G)}, \end{aligned}$$

and we are done since $z(t), y(t) \in L$. □

The quantitatively weaker arguments of [Bou90] and the usual Bogolyubov-Chang argument in the case $p = 2$ actually endow T with the structure of a Bohr set, while the set we found has, *a priori*, no structure. Croot and Sisask noted that this could, to some degree, be recovered by taking repeated sum-sets, and we shall couple this idea with Chang’s theorem to get the necessary strength in our corollary.

This may sound like we cannot have gained anything over the usual multi-sum version of the Bogolyubov-Chang argument. However, we do get some extra strength from the fact that we are in some sense able to increase the number of summands without decreasing the (higher order) additive energy or having the individual summands become too thin. A similar sort of observation is exploited by Schoen in [Sch11] (see also [CS10b]) for the purpose of proving a remarkable Freiman-type theorem.

COROLLARY 5.2. *Suppose that B is a regular d -dimensional Bohr set, $B' \subset B_{\rho'}$ is a regular rank k Bohr set, $L, A \subset B$ have relative densities λ and α respectively, $S \subset B'$ has relative density σ . Then either*

(i) *(large inner product)*

$$\langle 1_L * (1_S d\beta'), 1_A \rangle_{L^2(\beta)} \geq \lambda\sigma\alpha/2,$$

(ii) *(density increment) or there is a regular Bohr set B''' and an*

$$m = O(\lambda^{-2}(\log 2\lambda^{-1}\alpha^{-1})^2(\log 2\alpha^{-1})(\log 2\sigma^{-1}))$$

with $\text{rk}(B''') \leq k + m$ and $\mu_{B'}(B''') \geq (1/2km)^{O(k+m)}$ such that

$$\|1_A * \beta'''\|_{L^\infty(\mu_G)} \geq \alpha(1 + \Omega(\lambda)),$$

provided $\rho' \leq c_{5.2}\lambda\alpha/d$.

Proof. We can certainly assume that all of λ, α and σ are positive, and to begin we set some parameters, the choices for which will become apparent later:

$$l := \lceil \log 2\lambda^{-1}\alpha^{-1} \rceil, p := 2 + \log \alpha^{-1} \text{ and } \varepsilon := \lambda/8el.$$

The Bohr set B' has dimension $O(k)$, whence we may pick $\rho'' = \Omega(1/k)$ such that $B'' := B'_{\rho''/2l}$ is regular and $\mu_G(B'' + B') \leq 2\mu_G(B')$. Then

$$|B'' + S| \leq |B'' + B'| \leq 2|B'| \leq 2\sigma^{-1}|S|,$$

and we apply Lemma 5.1 to the sets S , B'' and the function 1_L respectively² with parameters p and ε . We get that there is an $s \in B''$ and a set $T \subset B''$ with $\beta''(T) \geq (\sigma/2)^{O(p\varepsilon^{-2})}$ such that

$$\|\tau_t(1_L * (1_S d\beta')) - 1_L * (1_S d\beta')\|_{L^p(\mu_G)} \leq \varepsilon\sigma \|1_L\|_{L^p(\mu_G)} \text{ for all } t \in T - s.$$

Of course

$$\begin{aligned} & \|\tau_t(1_L * (1_S d\beta')) - 1_L * (1_S d\beta')\|_{L^p(\beta)}^p \\ & \leq \frac{1}{\mu_G(B)} \int |\tau_t(1_L * (1_S d\beta')) - 1_L * (1_S d\beta')|^p d\mu_G \leq \varepsilon^p \sigma^p \beta(L) \leq \varepsilon^p \sigma^p, \end{aligned}$$

whence

$$\|\tau_t(1_L * (1_S d\beta')) - 1_L * (1_S d\beta')\|_{L^p(\beta)} \leq \varepsilon\sigma \text{ for all } t \in T - s.$$

It follows by the triangle inequality that

$$\|\tau_t(1_L * (1_S d\beta')) - 1_L * (1_S d\beta')\|_{L^p(\beta)} \leq 2l\varepsilon\sigma \text{ for all } t \in l(T - T).$$

Integrating and applying the triangle inequality again, we get

$$\|1_L * (1_S d\beta') * f - 1_L * (1_S d\beta')\|_{L^p(\beta)} \leq 2l\varepsilon\sigma$$

where $f := \mu_T * \dots * \mu_T * \mu_{-T} * \dots * \mu_{-T}$, and there are l copies of μ_T and l copies of μ_{-T} . By Hölder's inequality we have

$$\begin{aligned} & |\langle 1_L * (1_S d\beta') * f, 1_A \rangle_{L^2(\beta)} - \langle 1_L * (1_S d\beta'), 1_A \rangle_{L^2(\beta)}| \\ & \leq 2l\varepsilon\sigma \|1_A\|_{L^{p/(p-1)}(\beta)} \leq \lambda\sigma\alpha/4. \end{aligned}$$

It follows that we are either in the first case of the corollary, or else

$$\langle f * (1_S d\beta') * 1_L, 1_A \rangle_{L^2(\beta)} \leq 3\lambda\sigma\alpha/4,$$

which we assume from hereon.

Now, $\text{supp } f \subset 2lB'' \subset B'_{\rho''} \subset B_{\rho'}$ so

$$\int 1_L * (1_S d\beta') * f d\beta = \lambda\sigma + O(\rho' d\sigma),$$

whence

$$|\langle 1_L * (1_S d\beta') * f, 1_A - \alpha \rangle_{L^2(\beta)}| \geq \lambda\sigma\alpha/8$$

²So that A is S , and S is B'' .

provided ρ' is sufficiently small. We now apply Fourier inversion to get that

$$\left| \sum_{\gamma \in \widehat{G}} |\widehat{\mu}_T(\gamma)|^{2l} \widehat{1_S d\beta'}(\gamma) \widehat{1_L}(\gamma) \overline{(1_A - \alpha 1_B)^\wedge(\gamma)} \right| \geq \lambda \sigma \alpha \mu_G(B) / 8.$$

By the Cauchy-Schwarz inequality and the Hausdorff-Young inequality (in the trivial case which ensures $|\widehat{1_S d\beta'}(\gamma)| \leq \sigma$) we see that

$$\sigma \left(\sum_{\gamma \in \widehat{G}} |\widehat{1_L}(\gamma)|^2 \right)^{1/2} \left(\sum_{\gamma \in \widehat{G}} |\widehat{\mu}_T(\gamma)|^{4l} |(1_A - \alpha 1_B)^\wedge(\gamma)|^2 \right)^{1/2} \geq \lambda \sigma \alpha \mu_G(B) / 8.$$

Parseval's theorem tells us that the first sum is $\lambda \mu_G(B)$ and so

$$\sum_{\gamma \in \widehat{G}} |\widehat{\mu}_T(\gamma)|^{4l} |(1_A - \alpha 1_B)^\wedge(\gamma)|^2 \geq \lambda \alpha^2 \mu_G(B) / 64.$$

We put $\eta := (\lambda \alpha)^{1/2l} / 16^{1/l} = \Omega(1)$ and since $\mu_T = 1_T d\beta''$ note, by the triangle inequality, that

$$\sum_{\gamma \in \text{Spec}_\eta(1_T, \beta'')} |(1_A - \alpha 1_B)^\wedge(\gamma)|^2 = \Omega(\lambda \alpha^2 \mu_G(B)).$$

The corollary is completed by Lemma 3.8 provided ρ' is sufficiently small. \square

6. Proof of the main theorem

We shall now prove the following theorem from which our main result follows by the usual Freĭman embedding.

THEOREM 6.1. *Suppose that G is a group of odd order and $A \subset G$ has density $\alpha > 0$. Then*

$$\langle 1_A * 1_{-2.A}, 1_{-A} \rangle_{L^2(\mu_G)} = \exp(-O(\alpha^{-1} \log^5 2\alpha^{-1})).$$

There is some merit in trying to control the logarithmic term here. Indeed, while it seems likely that with care one could improve the 5 a bit, if one could replace it by $1 - \Omega(1)$, then one could use the W -trick (as popularised by Green [Gre05]) to deduce van der Corput's theorem pretty easily; if one could replace it by $-\Omega(1)$, then van der Corput's theorem would follow directly from the prime number theorem.

Even more ambitiously, the Erdős-Turán conjecture would follow (for progressions of length three) if one could replace the 5 by $-(1 + \Omega(1))$. However, despite the fact that such an improvement appears small it seems that a new idea would probably be required to prove such a result since it is not known even in the model setting of $G = (\mathbb{Z}/3\mathbb{Z})^n$. (The best result known there is the celebrated Roth-Meshulam theorem of Meshulam [Mes95].)

The proof of Theorem 6.1 is an iterative application of the following lemma.

LEMMA 6.2. *Suppose that B is a regular d -dimensional Bohr set, B' is a regular rank k Bohr set with $B' \subset B_{\rho'}$, $B'' \subset B_{\rho''}$, $A \subset B$ has relative density α and $A' \subset B'$ has relative density α' . Then either*

(i) (large inner product)

$$\langle 1_A * (1_{A'} d\beta'), 1_{-A} \rangle_{L^2(\beta)} \geq \mu_{B'}(B'')(\alpha'/2)^{O(\alpha^{-1})},$$

(ii) (density increment) or there is a regular Bohr set B''' with rank at most $k + O(\alpha^{-1}(\log^3 2\alpha^{-1})(\log 2\alpha'^{-1}))$ and

$$\mu_{B'}(B''') \geq \left(\frac{\alpha}{2k \log 2\alpha'^{-1}} \right)^{O(k + \alpha^{-1}(\log^3 2\alpha^{-1})(\log 2\alpha'^{-1}))}$$

and $\|1_A * \beta'''\|_{L^\infty(\mu_G)} \geq \alpha(1 + c_{6.2})$,

provided $\rho' \leq c_{6.2}\alpha/d$ and $\rho'' \leq c_{6.2}\alpha'/k$.

Proof. We apply Proposition 4.1 to see that (provided ρ' and ρ'' are not too large) either we are in the second case of the lemma, or else there are sets $L \subset B$ and $S \subset B''$ with $\beta(L) = \Omega(1)$ and $\beta''(S) \geq (\alpha'/2)^{O(\alpha^{-1})}$ such that

$$1_L * (1_S d\beta'') \leq C_{4.1}\alpha^{-1} \mu_{B'}(B'')^{-1} 1_A * (1_{A'} d\beta').$$

In this latter case we apply Corollary 5.2 (to the set $-A$ provided ρ' is not too large) to get that either we are in the second case of the lemma, or else

$$\langle 1_L * (1_S d\beta''), 1_{-A} \rangle_{L^2(\beta)} \geq \alpha\beta(L)\beta''(S)/2 \geq (\alpha'/2)^{O(\alpha^{-1})},$$

and we are in the first case of the lemma. □

Proof of Theorem 6.1. We construct a sequence of regular Bohr sets $B^{(i)}$ and sequences

$$k_i := \text{rk}(B^{(i)}), d_i = \dim B^{(i)} \text{ and } \alpha_i := \|1_A * \beta^{(i)}\|_{L^\infty(\mu_G)}.$$

We initialise with $B^{(0)} = G$ which is easily seen to be regular so that $\alpha_0 = \alpha$. Suppose that we are at stage i of the iteration.

We have $d_i = O(k_i)$, and so by regularity we have that

$$\|1_A * \beta^{(i)} * \beta_{\rho'}^{(i)} + 1_A * \beta^{(i)} * \beta_{\rho'\rho''}^{(i)} - 2(1_A * \beta^{(i)})\|_{L^\infty(\mu_G)} = O(\rho'k_i).$$

It follows that we can pick $\rho', \rho'' = \Omega(\alpha/k_i)$ such that $B^{(i)'} := B_{\rho'}^{(i)}$ is regular of dimension d_i , $B^{(i)''} := 2.B_{\rho'\rho''}^{(i)}$ is regular of rank k_i ,

$$B^{(i)''} \subset B_{c_{6.2}\alpha/2d_i}^{(i)'}$$

and

$$\|1_A * \beta^{(i)} * \beta^{(i)'} + 1_A * \beta^{(i)} * \beta_{\rho''}^{(i)'} - 2(1_A * \beta^{(i)})\|_{L^\infty(\mu_G)} \leq c_{6.2}\alpha/4.$$

If

$$\|1_A * \beta^{(i)'}\|_{L^\infty(\mu_G)} \geq \alpha_i(1 + c_{6.2}/4) \text{ or } \|1_A * \beta_{\rho''}^{(i)'}\|_{L^\infty(\mu_G)} \geq \alpha_i(1 + c_{6.2}/4),$$

then we let $B^{(i+1)}$ be $B^{(i)'}$ or $B_{\rho''}^{(i)'}$ respectively and see that

$$k_{i+1} = k_i, \mu_G(B^{(i+1)}) \geq \mu_G(B^{(i)})(\alpha/2k_i)^{O(k_i)} \text{ and } \alpha_{i+1} \geq \alpha_i(1 + c_{6.2}/4).$$

Otherwise, by averaging, there is some x_i such that

$$1_A * \beta^{(i)'}(x_i) \geq \alpha_i(1 - c_{6.2}/2) \text{ and } 1_A * \beta_{\rho''}^{(i)'}(x_i) \geq \alpha_i(1 - c_{6.2}/2).$$

Translating by x_i we get a set $A_1 := (A - x_i) \cap B^{(i)'}$ and $A_2 := (2x_i - 2.A) \cap B^{(i)''}$ such that

$$\beta^{(i)'}(A_1) \geq \alpha_i(1 - c_{6.2}/2) \text{ and } \beta^{(i)''}(A_2) \geq \alpha/2,$$

and

$$\langle 1_A * 1_{-2.A}, 1_{-A} \rangle \geq \mu_G(B^{(i)'})\mu_G(B^{(i)'})\langle 1_{A_1} * (1_{A_2}d\beta^{(i)''}), 1_{-A_1} \rangle_{L^2(\beta^{(i)'})}.$$

Now we apply the preceding lemma to see that either

$$(6.1) \quad \langle 1_A * 1_{-2.A}, 1_{-A} \rangle \geq \mu_G(B^{(i)'})\mu_G(B_{c_{6.2}\alpha/2k_i}^{(i)'}) (\alpha/2)^{O(\alpha^{-1})},$$

or there is a Bohr set $B^{(i+1)}$ such that

$$k_{i+1} \leq k_i + O(\alpha_i^{-1} \log^4 2\alpha^{-1}),$$

$$\mu_G(B^{(i+1)}) \geq \mu_G(B^{(i)}) \left(\frac{\alpha}{2k_i} \right)^{O(k_i + \alpha_i^{-1} \log^4 2\alpha^{-1})},$$

and

$$\alpha_{i+1} \geq \alpha_i(1 + c_{6.2}/2).$$

Since α_i cannot exceed 1, the iteration described above must terminate after $i_0 = O(\log 2\alpha^{-1})$ steps with (6.1). By summing the geometric progression we see that

$$k_{i_0} = O(\alpha^{-1} \log^4 2\alpha^{-1}) \text{ and } \mu_G(B^{(i_0)}) \geq (\alpha/2)^{O(\alpha^{-1} \log^4 2\alpha^{-1})}.$$

Inserting this in (6.1) gives the required result. □

Acknowledgements. The author would like to thank an anonymous referee for useful comments and suggesting the connection of the material in Section 4 with the Dyson e -transform, Thomas Bloom for numerous corrections, Ben Green for encouragement, and Julia Wolf for many useful comments and encouragement.

References

- [Beh46] F. A. BEHREND, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U.S.A.* **32** (1946), 331–332. MR 0018694. Zbl 0060.10302.
- [Bou90] J. BOURGAIN, On arithmetic progressions in sums of sets of integers, in *A Tribute to Paul Erdős*, Cambridge Univ. Press, Cambridge, 1990, pp. 105–109. MR 1117007. Zbl 0715.11006.
- [Bou99] ———, On triples in arithmetic progression, *Geom. Funct. Anal.* **9** (1999), 968–984. MR 1726234. Zbl 0959.11004. doi: 10.1007/s000390050105.
- [Bou08] ———, Roth's theorem on progressions revisited, *J. Anal. Math.* **104** (2008), 155–192. MR 2403433. Zbl 1155.11011. doi: 10.1007/s11854-008-0020-x.
- [Cha02] M.-C. CHANG, A polynomial bound in Freiman's theorem, *Duke Math. J.* **113** (2002), 399–419. MR 1909605. Zbl 1035.11048. doi: 10.1215/S0012-7094-02-11331-3.
- [CS10a] E. CROOT and O. SISASK, A probabilistic technique for finding almost-periods of convolutions, *Geom. Funct. Anal.* **20** (2010), 1367–1396. MR 2738997. Zbl 05833796. doi: 10.1007/s00039-010-0101-8.
- [CS10b] K. CWALINA and T. SCHOEN, A linear bound on the dimension in Green-Ruzsa's theorem, 2010, preprint.
- [Elk10] M. ELKIN, An improved construction of progression-free sets, in *Symposium on Discrete Algorithms*, 2010, pp. 886–905.
- [GW10] W. T. GOWERS and J. WOLF, The true complexity of a system of linear equations, *Proc. Lond. Math. Soc.* **100** (2010), 155–176. MR 2578471. Zbl 05658776. doi: 10.1112/plms/pdp019.
- [Gre05] B. GREEN, Roth's theorem in the primes, *Ann. of Math.* **161** (2005), 1609–1636. MR 2180408. Zbl 1160.11307. doi: 10.4007/annals.2005.161.1609.
- [GW10] B. GREEN and J. WOLF, A note on Elkin's improvement of Behrend's construction, in *Additive Number Theory: Festschrift in Honor of the Sixtieth Birthday of Melvyn B. Nathanson*, Springer-Verlag, New York, 1st ed., 2010, pp. 141–144.
- [HB87] D. R. HEATH-BROWN, Integer sets containing no arithmetic progressions, *J. London Math. Soc.* **35** (1987), 385–394. MR 0889362. Zbl 0589.10062. doi: 10.1112/jlms/s2-35.3.385.
- [KK10] N. H. KATZ and P. KOESTER, On additive doubling and energy, *SIAM J. Discrete Math.* **24** (2010), 1684–1693. MR 2746716. doi: 10.1137/080717286.
- [Mes95] R. MESHULAM, On subsets of finite abelian groups with no 3-term arithmetic progressions, *J. Combin. Theory Ser. A* **71** (1995), 168–172. MR 1335785. Zbl 0832.11006. doi: 10.1016/0097-3165(95)90024-1.
- [Rot52] K. ROTH, Sur quelques ensembles d'entiers, *C. R. Acad. Sci. Paris* **234** (1952), 388–390. MR 0046374. Zbl 0046.04302.

- [Rot53] ———, On certain sets of integers, *J. London Math. Soc.* **28** (1953), 104–109. MR 0051853. Zbl 0050.04002. doi: 10.1112/jlms/s1-28.1.104.
- [SS42] R. SALEM and D. C. SPENCER, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U. S. A.* **28** (1942), 561–563. MR 0007405. Zbl 0060.10301.
- [San10] T. SANDERS, On certain other sets of integers, 2010, *J. Anal. Math.*, to appear. arXiv 1007.5444.
- [Sch11] T. SCHOEN, Near optimal bounds in Freiman’s theorem, *Duke Math. J.* **158** (2011), 1–12. doi: 10.1215/00127094-1276283.
- [SS11] T. SCHOEN and I. SHKREDOV, Additive properties of multiplicative subgroups in \mathbb{F}_p , 2011, *Quart. J. Math.*, to appear. doi: 10.1093/qmath/har002.
- [Sze90] E. SZEMERÉDI, Integer sets containing no arithmetic progressions, *Acta Math. Hungar.* **56** (1990), 155–158. MR 1100788. Zbl 0721.11007. doi: 10.1007/BF01903717.
- [TV06] T. TAO and V. VU, *Additive Combinatorics*, Cambridge Stud. Adv. Math. **105**, Cambridge Univ. Press, Cambridge, 2006. MR 2289012. Zbl 1127.11002. doi: 10.1017/CB09780511755149.
- [YFHY01] R. YAO-FENG and L. HAN-YING, On the best constant in Marcinkiewicz-Zygmund inequality, *Stat. Prob. Lett.* **53** (2001), 227–233. MR 1841623. Zbl 0991.60011. doi: 10.1016/S0167-7152(01)00015-3.

(Received: November 14, 2010)

UNIVERSITY OF CAMBRIDGE, CAMBRIDGE, ENGLAND
E-mail: t.sanders@dpmms.cam.ac.uk