

ANALYSIS & PDE

Volume 5

No. 3

2012

TOM SANDERS

ON THE BOGOLYUBOV-RUZSA LEMMA

ON THE BOGOLYUBOV–RUZSA LEMMA

TOM SANDERS

Our main result is that if A is a finite subset of an abelian group with $|A + A| \leq K|A|$, then $2A - 2A$ contains an $O(\log^{O(1)} 2K)$ -dimensional coset progression M of size at least $\exp(-O(\log^{O(1)} 2K))|A|$.

1. Introduction

Croot and Sisask [2010] introduced a fundamental new method to additive combinatorics and, although they have already given a number of applications, our present purpose is to give another. Specifically, we shall prove the following.

Theorem 1.1 (Bogolyubov–Ruzsa lemma for abelian groups). *Suppose that G is an (discrete) abelian group and $A, S \subset G$ are finite nonempty sets such that $|A + S| \leq K \min\{|A|, |S|\}$. Then $(A - A) + (S - S)$ contains a proper symmetric $d(K)$ -dimensional coset progression M of size $\exp(-h(K))|A + S|$. Moreover, we may take $d(K) = O(\log^6 2K)$ and $h(K) = O(\log^6 2K \log 2 \log 2K)$.*

We should take a moment to justify the name, which is slightly nonstandard. Bogolyubov’s lemma (the idea for which originates in [Bogolyubov 1939]) is usually stated for sets of large density in the ambient group, rather than small doubling, and asserts that the fourfold sumset of a thick set contains a large Bohr set.

Ruzsa [1994], on his way to proving Freĭman’s theorem, showed that a set with small doubling could be sensibly embedded into a group where it is thick. He then applied Bogolyubov’s lemma and proceeded to show that a Bohr set contains a large generalised arithmetic progression which could then be pulled back. In doing all this he implicitly proved the first version of Theorem 1.1 in \mathbb{Z} —although, with different bounds—and this motivates the name.

This result has many variants (although the form given above seems to be a fairly useful one) and in light of this the history is not completely transparent. Certainly most proofs of Freĭman’s theorem broadly following the model of [Ruzsa 1994] will implicitly prove a result of this shape. With this in mind the extension from \mathbb{Z} to arbitrary abelian groups is due to Green and Ruzsa [2007], and the first good bounds to Schoen [2011] for certain classes of groups.

There are many applications of results of this type, particularly since their popularisation by Gowers [1998], and we shall deal with a number of these in Section 11 at the end of the paper. To help explain the main ideas we include a discursive sketch of the paper after the next section, which simply sets some notation.

MSC2010: 11L07.

Keywords: Freiman, Fourier analysis, sumsets, generalised arithmetic progressions, coset progressions, small doubling.

2. Notation

The main tool used in the paper is Fourier analysis on groups for which the classic reference is [Rudin 1990]. We deal almost exclusively with finite groups in the paper, but to be complete we shall need slightly more generality.

Suppose that G is a locally compact topological group. We write $C(G)$ for the space of continuous complex-valued functions on G . More generally if $R \subset \mathbb{C}$ we write $C(G, R)$ for the continuous R -valued functions on G .

The group structure on G induces an action of G on $C(G)$ called translation. In particular if $x \in G$ and $f \in C(G)$ then we write

$$\rho_x(f)(y) := f(yx) \quad \text{for all } y \in G. \quad (2-1)$$

We also write $M(G)$ for the space of regular Borel measures on G and can extend ρ to these in the natural way: for $x \in G$ and $\mu \in M(G)$, $\rho_x(\mu)$ is the measure induced by

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

The group structure on G is reflected in $M(G)$ in a fairly natural way and we define the convolution of two measures $\mu, \nu \in M(G)$ to be the measure $\mu * \nu$ induced by

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

There is a family of privileged measures on G called Haar measures. These are the translation-invariant measures on G : $\mu \in M(G)$ is a Haar measure on G if $\rho_x(\mu) = \mu$ for all $x \in G$.

Given a Haar measure μ on G we can extend ρ in the obvious way from (2-1) to define the right regular representation $\rho : G \rightarrow \text{Aut}(L^2(\mu))$. More than this we can define the convolution of two functions $f, g \in L^1(\mu)$ by

$$f * g(x) := \int f(y)g(y^{-1}x) d\mu(y) \quad \text{for all } x \in G.$$

There are two particularly useful instances of Haar measure depending on the topology on G : if G is compact we write μ_G for the Haar probability measure on G , while if G is discrete we write δ_G for the Haar counting measure on G , which assigns mass 1 to each element of G .

Of course, if G is finite it is both discrete and compact so one has both probability measure and counting measure to choose from. The measures are multiples of each other as μ_G is just the measure assigning mass $|G|^{-1}$ to each element of G . More generally given a finite set X we write μ_X for the measure assigning mass $|X|^{-1}$ to each $x \in X$.

When it is relevant we shall indicate whether we are taking a finite group G to be compact or discrete by declaring the group either compact, so that μ_G is to be used, or discrete so that δ_G is to be used. The reader should be aware that this has the effect of changing the normalisations in convolutions.

The above all works for general finite groups G , but when G is also abelian 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

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

and extend this to $f \in L^1(\mu_G)$ by $\widehat{f} := \widehat{f d\mu_G}$. 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 $f, g \in L^1(\mu_G)$.

3. A sketch of the argument

Assuming the hypotheses of Theorem 1.1 our objective will be to show that there is a large, low-dimensional coset progression M correlated with $A + S$, meaning such that

$$\|1_{A+S} * \mu_M\|_{\ell^\infty(G)} > 1 - o(1).$$

This is essentially the statement of Theorem 10.1 later, and Theorem 1.1 can be derived from it by a simple pigeonholing argument.

A simplified argument: the case of good modelling. We shall assume that we have good modelling in the sense of [Green and Ruzsa 2007], meaning that we shall assume that the sets A and S have density $K^{-O(1)}$ in the ambient group. This can actually be arranged in the two cases of greatest interest: \mathbb{F}_2^n and \mathbb{Z} and facilitates considerable simplifications.

A very useful observation in [López and Ross 1975] is that because the support of $\mu_A * \mu_S$ is contained in $A + S$ we have the identity

$$\langle 1_{A+S} * \mu_{-S}, \mu_A \rangle = 1.$$

Now, suppose we had a coset progression M over which $1_{A+S} * \mu_{-S}$ was in some sense invariant, meaning

$$\|1_{A+S} * \mu_{-S} * \mu_M - 1_{A+S} * \mu_{-S}\|_{\ell^p(G)} \leq \epsilon \|1_{A+S}\|_{\ell^p(G)}. \tag{3-1}$$

Then Hölder’s inequality and the López–Ross identity tell us that

$$|\langle 1_{A+S} * \mu_{-S} * \mu_M, \mu_A \rangle - 1| \leq \epsilon \|1_{A+S}\|_{\ell^p(G)} \|\mu_A\|_{\ell^{p/(p-1)}(G)} \leq \epsilon K^{1/p},$$

and it follows by averaging that $A + S$ is correlated with M provided that $\epsilon \sim K^{-1/p}$.

The traditional Fourier analytic approach to finding an M such that (3-1) holds is not particularly efficient, but recently Croot and Sisask showed that there is, at least, a set Z such that we have (3-1) with Z in place of M and

$$\mu_G(Z) \geq \exp(-O(\epsilon^{-2} p \log K)) \mu_G(A).$$

Moreover, they noted by the triangle inequality that one can endow Z with the structure of a k -fold sumset, so that we have (3-1) with kX in place of M and

$$\mu_G(X) \geq \exp(-O(k^2 \epsilon^{-2} p \log K)) \mu_G(A) = \exp(-O(k^2 \log^2 K)) \mu_G(A), \quad (3-2)$$

where the third term is by optimising the choice of $p \sim \log K$ given that $\epsilon \sim K^{-1/p}$.

What we actually end up with after all this is a set X with density as described in (3-2) such that

$$\langle 1_{A+S} * \mu_{-S} * \mu_X^{(k)}, \mu_A \rangle > 1 - o(1). \quad (3-3)$$

Now, by the usual sorts of applications of Plancherel's theorem and Cauchy-Schwarz we find that most of the Fourier mass of the inner product is concentrated on those characters in $\text{Spec}_{1/2}(1_X)$ provided $2^k \sim K$, and so we choose $k \sim \log K$.

With most of the Fourier mass supported on $\text{Spec}_{1/2}(1_X)$, it follows that the integrand in (3-3) correlates with any set which approximately annihilates $\text{Spec}_{1/2}(1_X)$. It remains to show that the approximate annihilator of $\text{Spec}_{1/2}(1_X)$ — that is the Bohr set B with $\text{Spec}_{1/2}(1_X)$ as its frequency set — contains a large coset progression.

We can now apply Chang's theorem to get that B is low-dimensional and then the usual geometry of numbers argument tells us that this Bohr set contains a large coset progression, and the result is proved.

Extending the argument: the case of bad modelling. We now drop the assumption of good modelling, and the argument proceeds in essentially the same way up until the application of Chang's theorem above.

In this case Chang's theorem does not provide good bounds. Instead what we do is note that the set X satisfies a relative polynomial growth condition

$$|nX| \leq n^{O(\log^4 K)} |X| \quad \text{for all } n \geq 1.$$

This lets us produce a Bohr set containing X which behaves enough like a group for a relative version of Chang's theorem to hold, whilst at the same time X is much denser in the Bohr set than it would be in the modelling group.

Since we are not using modelling what we have just done does not actually give us a Bohr set of low dimension, but rather a Bohr set of size comparable to X which has a lower order of polynomial growth on a certain range. It turns out that the usual argument that shows a low-dimensional Bohr set contains a large coset progression can be adapted relatively easily to this more general setting and this gives us our final ingredient.

These arguments are spread over the paper as follows. The simplified argument up to (3-3) is essentially contained in Section 4. Then, in Section 5, we record the basic properties of Bohr sets we need before Section 6, which has the relative version of Chang's theorem, and Section 7, which puts the material together to take a set satisfying a relative polynomial growth condition and produce a large Bohr superset.

After the material on Bohr sets we have Section 8 which records some standard covering lemmas and then Section 9 where we show how to find a large coset progression in a Bohr set with relative polynomial growth. Finally the argument is all put together in Section 10.

4. Freĭman-type theorems in arbitrary groups

In this section we are interested in Freĭman-type theorems in arbitrary, possibly nonabelian, groups. There has been considerable work towards such results, although often with restrictions on the type of nonabelian groups considered, or rather weak bounds. We direct the reader to [Green 2009] for a survey, but our interest is narrower, lying with a crucial result of Tao [2010, Proposition C.3] which inspires the following.

Proposition 4.1. *Suppose that G is a (discrete) group, $A, S \subset G$ are finite nonempty sets such that $|AS| \leq K \min\{|A|, |S|\}$, and $k \in \mathbb{N}$ is a parameter. Then $A^{-1}ASS^{-1}$ contains X^k where X is a symmetric neighbourhood of the identity with size $\delta(k, K)|AS|$. Moreover, we may take $\delta(k, K) \geq \exp(-O(k^2 \log^2 2K))$.*

Note that this result is a very weak version of Theorem 1.1 but for any group, not just abelian groups, and despite its weaknesses, its generality makes it useful in some situations.

Proposition 4.1 was essentially proved in [Croot and Sisask 2010, Theorem 1.6] with weaker K -dependence in the bound, using the $p = 2$ version of their Lemma 4.3 below. It turns out that we shall be able to show the above bound by coupling the large p case of their result with the López–Ross identity.

The key proposition of this section, then, is the following.

Proposition 4.2. *Suppose that G is (discrete) a group, $A, S, T \subset G$ are finite nonempty sets such that $|AS| \leq K|A|$ and $|TS| \leq L|S|$, and $k \in \mathbb{N}$ and $\epsilon \in (0, 1]$ are a pair of parameters. Then there is a symmetric neighbourhood of the identity $X \subset G$ with*

$$|X| \geq \exp(-O(\epsilon^{-2}k^2 \log 2K \log 2L))|T|$$

such that

$$|\mu_{A^{-1}} * 1_{AS} * \mu_{S^{-1}}(x) - 1| \leq \epsilon \text{ for all } x \in X^k.$$

The main ingredient in the proof of this is the following result, which is essentially due to Croot and Sisask [2010, Proposition 3.3]. To prove it they introduced the idea of sampling from physical space rather than Fourier space — sampling in Fourier space can be seen as the main idea in Chang’s theorem. Not only does this work in settings where the Fourier transform is less well behaved, but it also runs much more efficiently, which leads to the superior bounds.

We include the proof since it is the pivotal ingredient of this paper, and we frame it in such a way as to emphasise the parallels with Chang’s theorem.

Lemma 4.3 (Croot–Sisask). *Suppose that G is a (discrete) group, $f \in \ell^p(G)$ for $p \geq 2$ and $S, T \subset G$ are nonempty with $|ST| \leq K|S|$. Then there is a $t \in T$ and a set $X \subset Tt^{-1}$ with $|X| \geq (2K)^{-O(\epsilon^{-2}p)}|T|$ such that*

$$\|\rho_x(f * \mu_S) - f * \mu_S\|_{\ell^p(G)} \leq \epsilon \|f\|_{\ell^p(G)} \quad \text{for all } x \in X.$$

Proof. Let z_1, \dots, z_k be independent uniformly distributed S -valued random variables, and for each $y \in G$ define $Z_i(y) := \rho_{z_i^{-1}}(f)(y) - f * \mu_S(y)$. For fixed y , the variables $Z_i(y)$ are independent and

have mean zero, so it follows by the Marcinkiewicz–Zygmund inequality and Hölder’s inequality that

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

Summing over y and interchanging the order of summation we get

$$\sum_{y \in G} \left\| \sum_{i=1}^k Z_i(y) \right\|_{L^p(\mu_S^k)}^p \leq O(p)^{p/2} k^{p/2-1} \int \sum_{i=1}^k \sum_{y \in G} |Z_i(y)|^p d\mu_S^k. \tag{4-1}$$

On the other hand,

$$\left(\sum_{y \in G} |Z_i(y)|^p \right)^{1/p} = \|Z_i\|_{\ell^p(G)} \leq \|\rho_{z_i^{-1}}(f)\|_{\ell^p(G)} + \|f * \mu_S\|_{\ell^p(G)} \leq 2\|f\|_{\ell^p(G)}$$

by the triangle inequality. Dividing (4-1) by k^p and inserting the above and the expression for the Z_i s we get

$$\int \sum_{y \in G} \left| \frac{1}{k} \sum_{i=1}^k \rho_{z_i^{-1}}(f)(y) - f * \mu_S(y) \right|^p d\mu_S^k(z) = O(pk^{-1} \|f\|_{\ell^p(G)}^2)^{p/2}.$$

Pick $k = O(\epsilon^{-2} p)$ such that the right-hand side is at most $(\epsilon \|f\|_{\ell^p(G)} / 4)^p$ and write L for the set of $x \in S \times \dots \times S$ (where the Cartesian product is k -fold) for which the integrand above is at most $(\epsilon \|f\|_{\ell^p(G)} / 2)^p$; by averaging $\mu_S^k(L^c) \leq 2^{-p}$ and so $\mu_S^k(L) \geq 1 - 2^{-p} \geq \frac{1}{2}$.

Now, $\Delta := \{(t, \dots, t) : t \in T\}$ has $L\Delta \subset ST \times \dots \times ST$, whence $|L\Delta| \leq 2K^k |L|$ and so

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

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

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

Thus for each $x \in X$ there is some $z(x) \in L$ and $y(x) \in L$ such that $y(x)_i = z(x)_i x$. But then by the triangle inequality we get

$$\begin{aligned} & \|\rho_{x^{-1}}(f * \mu_S) - f * \mu_S\|_{\ell^p(G)} \\ & \leq \left\| \rho_{x^{-1}} \left(\frac{1}{k} \sum_{i=1}^k \rho_{z(x)_i^{-1}}(f) \right) - f * \mu_S \right\|_{\ell^p(G)} + \left\| \rho_{x^{-1}} \left(\frac{1}{k} \sum_{i=1}^k \rho_{z(x)_i^{-1}}(f) - f * \mu_S \right) \right\|_{\ell^p(G)}. \end{aligned}$$

However, since ρ_x is isometric on $\ell^p(G)$ we see that

$$\left\| \rho_x(f * \mu_S) - f * \mu_S \right\|_{\ell^p(G)} \leq \left\| \frac{1}{k} \sum_{i=1}^k \rho_{y(x)_i^{-1}}(f) - f * \mu_S \right\|_{\ell^p(G)} + \left\| \frac{1}{k} \sum_{i=1}^k \rho_{z(x)_i^{-1}}(f) - f * \mu_S \right\|_{\ell^p(G)},$$

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

The important thing to note about the Croot–Sisask lemma is that the p -dependence of the size of the set X is very good. The natural Fourier analytic analogue (essentially given in [Bourgain 1990], and clearly exposted in [Sisask 2009]) gives an exponentially worse bound. To make use of this strength we use the aforementioned López–Ross identity.

Proof of Proposition 4.2. We apply Lemma 4.3 to the function $f := 1_{AS}$ and with the set S^{-1} (so that $|S^{-1}T^{-1}| \leq L|S^{-1}|$) to get a set X with $|X| \geq (2L)^{O(\epsilon^{-2}k^2p)}|T|$ such that

$$\|\rho_x(1_{AS} * \mu_{S^{-1}}) - 1_{AS} * \mu_{S^{-1}}\|_{\ell^p(G)} \leq \frac{\epsilon \|1_{AS}\|_{\ell^p(G)}}{ek} \quad \text{for all } x \in X.$$

Since ρ is isometric on $\ell^p(G)$ and ρ_{1_G} is the identity we may certainly assume that X is a symmetric neighbourhood of the identity. Furthermore, by the triangle inequality we have

$$\|\rho_x(1_{AS} * \mu_{S^{-1}}) - 1_{AS} * \mu_{S^{-1}}\|_{\ell^p(G)} \leq \epsilon e^{-1} \|1_{AS}\|_{\ell^p(G)} \quad \text{for all } x \in X^k.$$

Now for any (real) function g we have

$$\mu_{A^{-1}} * g(x) - \mu_{A^{-1}} * g(1_G) = \mu_{A^{-1}} * (\rho_x(g) - g)(1_G) = \langle \mu_A, \rho_x(g) - g \rangle.$$

Thus by Hölder’s inequality we have

$$|\mu_{A^{-1}} * g(x) - \mu_{A^{-1}} * g(1_G)| \leq \|\mu_A\|_{\ell^{p'}(G)} \|\rho_x(g) - g\|_{\ell^p(G)}.$$

Putting $g = 1_{AS} * \mu_{S^{-1}}$ we conclude that

$$\begin{aligned} |\mu_{A^{-1}} * 1_{AS} * \mu_{S^{-1}}(x) - \mu_{A^{-1}} * 1_{AS} * \mu_{S^{-1}}(1_G)| &\leq \frac{\epsilon \|\mu_A\|_{\ell^{p'}(G)} \|1_{AS}\|_{\ell^p(G)}}{e} \\ &\leq \frac{\epsilon |A|^{1/p'} |AS|^{1/p}}{e|A|} \leq \frac{\epsilon K^{1/p}}{e} \end{aligned}$$

for all $x \in X^k$. Putting $p := 2 + \log K$ we get the conclusion. □

Proof of Proposition 4.1. We simply take $T = A$, $L = K$ and $\epsilon = \frac{1}{2}$ in Proposition 4.2. □

5. Basic properties of Bohr sets

Following [Bourgain 2008] we use a slight generalisation of the traditional notion of Bohr set, letting the width parameter vary according to the character. The advantage of this definition is that the meet of two Bohr sets in the lattice of Bohr sets is then just their intersection.

Throughout the section we let G be a finite (compact) abelian group. A set B is called a *Bohr set* if there is a *frequency set* Γ of characters on G , and a *width function* $\delta \in (0, 2]^\Gamma$ such that

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

Technically the same Bohr set can be defined by different frequency sets and width functions; we make the standard abuse that when we introduce a Bohr set we are implicitly fixing a frequency set and width function.

There is a natural way of dilating Bohr sets which will be of particular use to us. For a Bohr set B and $\rho \in \mathbb{R}^+$ we denote by B_ρ the Bohr set with frequency set Γ and width function¹ $\rho\delta$ so that, in particular, $B = B_1$ and more generally $(B_\rho)_{\rho'} = B_{\rho\rho'}$.

Given two Bohr sets B and B' we define their *intersection* to be the Bohr set with frequency set $\Gamma \cup \Gamma'$ and width function $\delta \wedge \delta'$. A simple averaging argument (see [Tao and Vu 2006, Lemma 4.20] but also the end of Lemma 4.3) can be used to see that the intersection of several Bohr sets is large.

Lemma 5.1 (intersections of Bohr sets). *Suppose that $(B^{(i)})_{i=1}^k$ is a sequence of Bohr sets. Then*

$$\mu_G(\bigwedge_{i=1}^k B^{(i)}) \geq \prod_{i=1}^k \mu_G(B_{1/2}^{(i)}).$$

Proof. Let $\Delta := \{(x, \dots, x) \in G^k : x \in G\}$ and $S := B_{1/2}^{(1)} \times \dots \times B_{1/2}^{(k)}$. Then

$$\int 1_\Delta * 1_{-\Delta} 1_S * 1_{-S} d\mu_{G^k} = \int (1_\Delta * 1_S)^2 d\mu_{G^k} \geq \mu_{G^k}(\Delta)^2 \mu_{G^k}(S)^2 \quad (5-1)$$

by Cauchy–Schwarz. The integrand on the left-hand side is at most $\mu_{G^k}(\Delta)\mu_{G^k}(S)$ and it is supported on the set of $x \in \Delta - \Delta = \Delta$ such that $1_S * 1_{-S}(x) > 0$. But if $1_S * 1_{-S}(y, \dots, y) > 0$ then

$$y \in \bigcap_{i=1}^k (B_{1/2}^{(i)} - B_{1/2}^{(i)}) \subset \bigcap_{i=1}^k B_1^{(i)} = (\bigwedge_{i=1}^k B^{(i)})_1.$$

Hence

$$\mu_{G^k}(\text{supp } 1_\Delta * 1_{-\Delta} 1_S * 1_{-S}) \leq \mu_G((\bigwedge_{i=1}^k B^{(i)})_1) \mu_{G^k}(\Delta),$$

and inserting this in (5-1) we get

$$\mu_G((\bigwedge_{i=1}^k B^{(i)})_1) \mu_{G^k}(\Delta)^2 \mu_{G^k}(S)^2 \geq \mu_{G^k}(\Delta)^2 \mu_{G^k}(S)^2.$$

The result follows after some cancelation and noting that $\mu_{G^k}(S)$ is just the right-hand side of the inequality in the statement of the lemma. \square

Note that if B is a Bohr set whose frequency set has one element, and whose width function is the constant function 2 then there is an easy lower bound for $\mu_G(B_\eta)$ as the length of a certain arc on a circle:

$$\mu_G(B_\eta) \geq \frac{1}{\pi} \arccos(1 - 2\eta^2) \geq \frac{1}{\pi} \min\{\eta, 2\}. \quad (5-2)$$

From this we immediately recover the usual lower bound on the size of a Bohr set with a larger frequency set from this and the preceding lemma.²

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

²To recover the bound in [Tao and Vu 2006, Lemma 4.20] some adjustments need to be made as our definition of a Bohr set is in terms of $\gamma(x)$ being close to 1 rather than $\arg \gamma(x)$ being close to 0.

Bourgain [1999] developed the idea of Bohr sets as approximate substitutes for groups, and since then his techniques have become an essential tool in additive combinatorics. To begin with we define the *entropy* of a Bohr set B to be

$$h(B) := \log \frac{\mu_G(B_2)}{\mu_G(B_{1/2})}.$$

A trivial covering argument shows that B_2 can be covered by $\exp(h(B))$ translates of B , and if B is actually a subgroup then $h(B) = 0$. It is often desirable to have a uniform bound on $h(B_\delta)$ for all $\delta \in (0, 2]$, and such a bound is called the dimension of B in other work. Here, however, it is crucial that we do not insist on this.

We shall be particularly interested in Bohr sets which grow in a reasonably regular way because they will function well as approximate groups. In light of the definition of entropy (which encodes growth over a fixed range) we say that a Bohr set B is *C-regular* if

$$\frac{1}{1 + Ch(B)|\eta|} \leq \frac{\mu_G(B_{1+\eta})}{\mu_G(B)} \leq 1 + Ch(B)|\eta|$$

for all η with $|\eta| \leq 1/Ch(B)$. Crucially such Bohr sets are commonplace.

Lemma 5.2. *There is an absolute constant $C_{\mathcal{R}}$ such that if B is a Bohr set then there is some $\lambda \in [1, 2]$ such that B_λ is $C_{\mathcal{R}}$ -regular.*

The proof is by a covering argument and follows [Tao and Vu 2006, Lemma 4.24], for example. From now on we say that a Bohr set B is *regular* if it is $C_{\mathcal{R}}$ -regular.

Finally, we write β_ρ for the probability measure induced on B_ρ by μ_G , and β for β_1 . These measures function as approximate analogues for Haar measure, and the following useful lemma of Green and Konyagin [2009] shows how they can be used to describe a sensible version of the annihilator of a Bohr set.

Lemma 5.3. *Suppose that B is a regular Bohr set. Then*

$$\{\gamma : |\hat{\beta}(\gamma)| \geq \kappa\} \subset \{\gamma : |1 - \gamma(x)| = O(h(B)\kappa^{-1}\rho) \text{ for all } x \in B_\rho\}.$$

Proof. First, suppose that $|\hat{\beta}(\gamma)| \geq \kappa$ and $y \in B_\rho$. Then

$$|1 - \gamma(y)|\kappa \leq \left| \int \gamma(x) d\beta(x) - \int \gamma(x+y) d\beta(x) \right| \leq \frac{\mu_G(B_{1+\rho} \setminus B_{1-\rho})}{\mu_G(B_1)} = O(h(B)\rho)$$

provided $\rho \leq 1/C_{\mathcal{R}}h(B)$. The result is proved. □

6. The large spectrum and Chang’s theorem

Given a probability measure μ , a function $f \in L^1(\mu)$ and a parameter $\epsilon \in (0, 1]$ we define the ϵ -*spectrum* of f w.r.t. μ to be the set

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

This definition extends the usual one from the case $\mu = \mu_G$. We shall need a local version of a result of Chang [2002] for estimating the “complexity” or “entropy” of the large spectrum.

Given a set of characters Λ and a function $\omega : \Lambda \rightarrow D := \{z \in \mathbb{C} : |z| \leq 1\}$ we define

$$p_{\omega, \Lambda} := \prod_{\lambda \in \Lambda} (1 + \operatorname{Re} \omega(\lambda)\lambda),$$

and call such a function a *Riesz product* for Λ . It is easy to see that all Riesz products are real nonnegative functions. They are at their most useful when they also have mass close to 1: the set Λ is said to be *K-dissociated* w.r.t. μ if

$$\int p_{\omega, \Lambda} d\mu \leq \exp(K) \quad \text{for all } \omega : \Lambda \rightarrow D.$$

In particular, being 0-dissociated w.r.t. μ_G is the usual definition of being dissociated. This relativised version of dissociativity has a useful monotonicity property.

Lemma 6.1 (monotonicity of dissociativity). *Suppose that μ' is another probability measure, Λ is K -dissociated w.r.t. μ , $\Lambda' \subset \Lambda$ and $K' \geq K$. Then Λ' is K' -dissociated w.r.t. $\mu' * \mu$.*

Conceptually the next definition is inspired by the discussion of quadratic rank Gowers and Wolf give in [Gowers and Wolf 2011]. The (K, μ) -relative entropy of a set Γ is the size of the largest subset $\Lambda \subset \Gamma$ such that Λ is K -dissociated w.r.t. μ .

Lemma 6.2 (Chang bound [Sanders 2012, Lemma 4.6]). *Suppose that $0 \neq f \in L^2(\mu)$ and write $L_f := \|f\|_{L^2(\mu)} \|f\|_{L^1(\mu)}^{-1}$. Then the set $\operatorname{Spec}_\epsilon(f, \mu)$ has $(1, \mu)$ -relative entropy $O(\epsilon^{-2} \log 2L_f)$.*

The proof of this goes by a Chernoff-type estimate, the argument for which follows [Green and Ruzsa 2007, Proposition 3.4], and then the usual argument from [Chang 2002].

Although Chang's theorem cannot be significantly improved (see [Green 2003; 2004] for a discussion), there are some small refinements and discussions of their limitations in [Shkredov 2006; 2007; 2008].

Low entropy sets of characters are majorised by large Bohr sets, a fact encoded in the following lemma. The proof is a minor variant of [Sanders 2012, Lemma 6.3].

Lemma 6.3 (annihilating dissociated sets). *Suppose that B is a regular Bohr set and Δ is a set of characters with (η, β) -relative entropy k . Then there is a set Λ of size at most k and some*

$$\rho = \Omega(\eta/(1 + h(B))(k + \log 2\eta^{-1}))$$

such that for all $\gamma \in \Delta$ we have

$$|1 - \gamma(x)| = O(kv + \rho' \rho^{-1} h(B_\rho)) \quad \text{for all } x \in B_{\rho'} \wedge B'_v, \rho', v \in \mathbb{R}^+$$

where B' is the Bohr set with constant width function 2 and frequency set Λ .

Proof. Let $L := \lceil \log_2 3^k 2(k + 1)\eta^{-1} \rceil$, the reason for which choice will become apparent, and define

$$\beta^+ := \beta_{1+L\rho} * \beta_\rho * \cdots * \beta_\rho,$$

where β_ρ occurs L times in the expression. By regularity (of B) we can pick $\rho \in (\Omega(\eta/(1 + h(B))L), 1]$

such that B_ρ is regular and we have the pointwise inequality

$$\beta \leq \frac{\mu_G(B_{1+L\rho})}{\mu_G(B)}\beta^+ \leq (1 + \eta/3)\beta^+.$$

It follows that if Λ is $\eta/2$ -dissociated w.r.t. β^+ then Λ is η -dissociated w.r.t. β , and hence Λ has size at most k . From now on all dissociativity will be w.r.t. β^+ .

We put $\eta_i := i\eta/2(k + 1)$ and begin by defining a sequence of sets $\Lambda_0, \Lambda_1, \dots$ iteratively such that Λ_i is η_i -dissociated. We let $\Lambda_0 := \emptyset$ which is easily seen to be 0-dissociated. Now, suppose that we have defined Λ_i as required. If there is some $\gamma \in \Delta \setminus \Lambda_i$ such that $\Lambda_i \cup \{\gamma\}$ is η_{i+1} -dissociated then let $\Lambda_{i+1} := \Lambda_i \cup \{\gamma\}$. Otherwise, terminate the iteration.

Note that for all $i \leq k + 1$, if the set Λ_i is defined then it is certainly $\eta/2$ -dissociated and so $|\Lambda_i| \leq k$. However, if the iteration had continued for $k + 1$ steps then $|\Lambda_{k+1}| > k$. This contradiction means that there is some $i \leq k$ such that $\Lambda := \Lambda_i$ is η_i -dissociated and $\Lambda_i \cup \{\gamma\}$ is not η_{i+1} -dissociated for any $\gamma \in \Delta \setminus \Lambda_i$.

It follows that we have a set Λ of at most k characters such that for all $\gamma \in \Delta \setminus \Lambda$ there is a function $\omega : \Lambda \rightarrow D$ and $\nu \in D$ such that

$$\int p_{\omega, \Lambda}(1 + \operatorname{Re} \nu\gamma) d\beta^+ > \exp(\eta_{i+1}).$$

Now, suppose that $\gamma \in \Delta$. If $\gamma \in \Lambda$ then the conclusion is immediate, so we may assume that $\gamma \in \Delta \setminus \Lambda$. Then, since Λ is η_i -dissociated, we see that

$$\left| \int p_{\omega, \Lambda} \bar{\gamma} d\beta^+ \right| > \exp(\eta_{i+1}) - \exp(\eta_i) \geq \frac{\eta}{2(k + 1)}.$$

Applying Plancherel’s theorem we get

$$\frac{\eta}{2(k + 1)} \leq \left| \sum_{\lambda \in \operatorname{Span}(\Lambda)} \widehat{p_{\omega, \Lambda}}(\lambda) \widehat{\beta}^+(\gamma - \lambda) \right| \leq 3^k \sup_{\lambda \in \operatorname{Span}(\Lambda)} |\widehat{\beta}_\rho(\gamma - \lambda)|^L.$$

Given the choice of L there is some $\lambda \in \operatorname{Span}(\Lambda)$ such that $|\widehat{\beta}_\rho(\gamma - \lambda)| \geq \frac{1}{2}$. By Lemma 5.3 we see that

$$\gamma - \lambda \in \{\gamma' : |1 - \gamma'(x)| = O(\rho''h(B_\rho)) \text{ for all } x \in (B_\rho)_{\rho''}\}.$$

On the other hand, by the triangle inequality if $\lambda \in \operatorname{Span}(\Lambda)$ then

$$\lambda \in \{\gamma' : |1 - \gamma'(x)| \leq k\nu \text{ for all } x \in B'_\nu\},$$

and the result follows from a final application of the triangle inequality. □

7. Containment in a Bohr set

The object of this section is to show the following result.

Proposition 7.1. *Suppose that G is a finite (compact) abelian group, $d \geq 1$ and X is a finite subset of G with $\mu_G(nX) \leq n^d \mu_G(X)$ for all $n \geq 1$ and $\kappa \in (0, 1]$ is a parameter. Then there is a regular Bohr set B such that*

$$X - X \subset B_\kappa \text{ and } \mu_G(B_2) \leq \exp(O(d \log 2d\kappa^{-1}))\mu_G(X).$$

What is important here is that given a set of relative polynomial growth we have produced a Bohr set which contains the original set, and which has controlled growth over a fixed range of dilations. Extending this range down to zero can be done but involves considerable additional work as well as being unnecessary for our arguments.

The next lemma is the key ingredient that provides us with an appropriate Bohr set. The idea originates with [Green and Ruzsa 2007, Lemma 2.3], but the lemma we record is more obviously related to [Tao and Vu 2006, Proposition 4.39].

Lemma 7.2. *Suppose that G is a finite (compact) abelian group, $A, S \subset G$ have*

$$\mu_G(A + S) \leq K\mu_G(A) \text{ and } |\widehat{1_{A+S}}(\gamma)| \geq (1 - \epsilon)\mu_G(A + S).$$

Then $|1 - \gamma(s)| \leq \sqrt{2^3 K\epsilon}$ for all $s \in S - S$.

Proof. By hypothesis there is a phase $\omega \in S^1$ such that

$$\int 1_{A+S}\omega\gamma d\mu_G = |\widehat{1_{A+S}}(\gamma)| \geq (1 - \epsilon)\mu_G(A + S).$$

It follows that

$$\int 1_{A+S}|1 - \omega\gamma|^2 d\mu_G = 2 \int 1_{A+S}(1 - \omega\gamma) d\mu_G \leq 2\epsilon\mu_G(A + S),$$

and so if $y_0, y_1 \in S$ then

$$\int 1_A|1 - \omega\gamma(y_i)\gamma|^2 d\mu_G \leq \int 1_{A+S}|1 - \omega\gamma|^2 d\mu_G \leq 2\epsilon\mu_G(A + S).$$

However, the Cauchy–Schwarz inequality tells us that

$$|1 - \gamma(y_0 - y_1)|^2 \leq 2(|1 - \omega\gamma(y_0)\gamma(x)|^2 + |1 - \omega\gamma(y_1)\gamma(x)|^2)$$

for all $x \in G$, whence

$$\int 1_A|1 - \gamma(y_0 - y_1)|^2 d\mu_G \leq 2^3\epsilon\mu_G(A + S),$$

and the result follows. □

To prove the proposition we use an idea from [Schoen 2003], first introduced to Freĭman-type problems in [Green and Ruzsa 2007]. The essence is that if we have sub-exponential growth of a set then we can apply the Cauchy–Schwarz inequality and Parseval’s theorem in a standard way to get a Fourier coefficient of very close to maximal value.

Proof of Proposition 7.1. By the pigeonhole principle there is some $l = O(d \log 2d)$ such that $\mu_G(lX) \leq 2\mu_G((l-1)X)$. We let B' be the Bohr set with width function the constant function $\frac{1}{2}$ and frequency set $\Gamma := \text{Spec}_{1-\epsilon}(1_{lX})$ where we pick $\epsilon := 2^{-10} \kappa^2$.

It follows by Lemma 7.2 applied to $A = (l-1)X$ and $S = X$ that

$$|1 - \gamma(x)| \leq \sqrt{2^3 \cdot 2 \cdot \epsilon} = \kappa/8 \quad \text{for all } x \in X - X \text{ and } \gamma \in \text{Spec}_{1-\epsilon}(1_{lX}),$$

and hence that $X - X \subset B'_{\kappa/4}$.

It remains to show that the Bohr set is not too large. Begin by noting that

$$\int (1_{lX}^{(k)})^2 d\mu_G \geq \frac{1}{\mu_G(k(lX))} \left(\int 1_{lX}^{(k)} d\mu_G \right)^2 \geq \frac{\mu_G(lX)^{2k-1}}{(kl)^d}, \tag{7-1}$$

where $1_{lX}^{(k)}$ denotes the k -fold convolution of 1_{lX} with itself, and the inequality is Cauchy–Schwarz and then the hypothesis. On the other hand, by Parseval’s theorem

$$\begin{aligned} \sum_{\gamma \notin \text{Spec}_{1-\epsilon}(1_{lX})} |\widehat{1_{lX}}(\gamma)|^{2k} &\leq ((1-\epsilon)\mu_G(lX))^{2k-2} \sum_{\gamma \in \widehat{G}} |\widehat{1_{lX}}(\gamma)|^2 \\ &\leq \exp(-\Omega(k\kappa)) \mu_G(lX)^{2k-1} \leq \frac{\mu_G(lX)^{2k-1}}{2(kl)^d} \end{aligned}$$

for some $k = O(d\kappa^{-1} \log 2d\kappa^{-1})$. In particular, from (7-1) we have

$$\sum_{\gamma \notin \text{Spec}_{1-\epsilon}(1_{lX})} |\widehat{1_{lX}}(\gamma)|^{2k} \leq \frac{1}{2} \int (1_{lX}^{(k)})^2 d\mu_G.$$

It then follows from Parseval’s theorem and the triangle inequality that

$$\begin{aligned} \sum_{\gamma \in \text{Spec}_{1-\epsilon}(1_{lX})} |\widehat{1_{lX}}(\gamma)|^{2k} &= \sum_{\gamma \in \widehat{G}} |\widehat{1_{lX}}(\gamma)|^{2k} - \sum_{\gamma \notin \text{Spec}_{1-\epsilon}(1_{lX})} |\widehat{1_{lX}}(\gamma)|^{2k} \\ &\geq \int (1_{lX}^{(k)})^2 d\mu_G - \frac{1}{2} \int (1_{lX}^{(k)})^2 d\mu_G = \frac{1}{2} \int (1_{lX}^{(k)})^2 d\mu_G. \end{aligned}$$

On the other hand by the triangle inequality $|\widehat{\beta}'(\gamma)| \geq \frac{1}{2}$ if $\gamma \in \Gamma$ since $\delta \leq \frac{1}{2}$, whence

$$\sum_{\gamma \in \widehat{G}} |\widehat{1_{lX}}(\gamma)|^{2k} |\widehat{\beta}'(\gamma)|^2 \geq \frac{1}{4} \sum_{\gamma \in \text{Spec}_{1-\epsilon}(1_{lX})} |\widehat{1_{lX}}(\gamma)|^{2k} \geq \frac{\mu_G(lX)^{2k-1}}{8(kl)^d}.$$

But, by Parseval’s theorem and Hölder’s inequality we have

$$\begin{aligned} \sum |\widehat{1_{lX}}(\gamma)|^{2k} |\widehat{\beta}'(\gamma)|^2 &= \int (1_{lX}^{(k)} * \beta')^2 d\mu_G \\ &\leq \|1_{lX}^{(k)} * 1_{-lX}^{(k)}\|_{L^1(G)} \|\beta' * \beta'\|_{L^\infty(G)} = \frac{\mu_G(lX)^{2k}}{\mu_G(B')}, \end{aligned}$$

and so

$$\mu_G(B') \leq (kl)^d \mu_G(lX) \leq \exp(O(d \log 2d\kappa^{-1})) \mu_G(X).$$

Finally we apply Lemma 5.2 to get a regular Bohr set B with $B_2 \subset B'_1$ and $B_\kappa \supset B'_{\kappa/4}$ so the result is proved. \square

8. Covering and growth in abelian groups

Covering lemmas are a major tool in additive combinatorics and have been since their development in [Ruzsa 1999]. This was further extended in [Green and Ruzsa 2006], and such lemmas play a pivotal role in the nonabelian theory as was highlighted by Tao [2008a], where we do not have many other techniques.

While the most basic form of covering lemmas do work in the nonabelian setting, there is a refined argument due to Chang [2002] that does not port over so easily.

Lemma 8.1 (Chang's covering lemma [Tao and Vu 2006, Lemma 5.31]). *Suppose that G is an (discrete) abelian group and $A, S \subset G$ are finite sets with $|nA| \leq K^n|A|$ for all $n \geq 1$ and $|A + S| \leq L|S|$. Then there is a set T with $|T| = O(K \log 2KL)$ such that³*

$$A \subset \text{Span}(T) + S - S.$$

We shall also need the following slight variant which provides a way in abelian groups to pass from relative polynomial growth on one scale to all scales.

Lemma 8.2 (variant of Chang's covering lemma). *Suppose that G is an (discrete) abelian group and $A, S \subset G$ are finite sets with $|kA + S| < 2^k|S|$. Then there is a set $T \subset A$ with $|T| < k$ such that $A \subset \text{Span}(T) + S - S$.*

Proof. Let T be a maximal S -dissociated subset of A , that is a maximal subset of A such that

$$(\sigma.T + S) \cap (\sigma'.T + S) = \emptyset \quad \text{for all } \sigma \neq \sigma' \in \{0, 1\}^T.$$

Now suppose that $x' \in A \setminus T$ and write $T' := T \cup \{x'\}$. By the maximality of T there are elements σ, σ' in $\{0, 1\}^{T'}$ such that $(\sigma.T' + S) \cap (\sigma'.T' + S) \neq \emptyset$. Now if $\sigma_{x'} = \sigma'_{x'}$, then $(\sigma|_T.T + S) \cap (\sigma'|_T.T + S) \neq \emptyset$, contradicting the fact that T is S -dissociated. Hence, without loss of generality, $\sigma_{x'} = 1$ and $\sigma'_{x'} = 0$, whence

$$x' \in \sigma'|_T.T - \sigma|_T.T + S - S \subset \text{Span}(T) + S - S.$$

We are done unless $|T| \geq k$; assume it is and let $T' \subset T$ be a set of size k . Denote $\{\sigma.T' : \sigma \in \{0, 1\}^{T'}\}$ by P and note that $P \subset kA$, whence

$$2^k|S| = |P + S| \leq |kA + S| < 2^k|S|.$$

This contradiction completes the proof. \square

³Recall that $\text{Span}(T) := \{\sum_{t \in T} \sigma_t.t : \sigma \in \{-1, 0, 1\}^T\}$.

Although this is a result in abelian groups, it has many parallels with Milnor’s proof [1968] establishing the dichotomy between polynomial growth and exponential growth in solvable groups.

The above lemma is particularly useful for controlling the order of relative polynomial growth through the next result, an idea introduced in [Green and Ruzsa 2006].

Lemma 8.3. *Suppose that G is an (discrete) abelian group, $X \subset G$ and $2X - X \subset \text{Span}(T) + X - X$ for some set T of size k . Then*

$$|(n + 1)X - X| \leq (2n + 1)^k |X - X| \quad \text{for all } n \geq 1.$$

Proof. By induction it is immediate that

$$(n + 1)X - X \subset n \text{Span}(T) + X - X,$$

and it is easy to see that $|n \text{Span}(T)| \leq (2n + 1)^k$ from which the result follows. \square

9. Lattices and coset progressions

The geometry of numbers seems to play a pivotal role in proofs of Freĭman-type theorems, and we direct the reader to [Tao and Vu 2006, Chapter 3.5] or [Green 2002b] for a much more comprehensive discussion.

Recall that Λ is a *lattice* in \mathbb{R}^k if there are linearly independent vectors v_1, \dots, v_k such that $\Lambda = v_1\mathbb{Z} + \dots + v_k\mathbb{Z}$; we call v_1, \dots, v_k a *basis* for Λ . Furthermore, a set K in \mathbb{R}^k is called a *convex body* if it is convex, open, nonempty and bounded.

We require the following application of John’s theorem and Minkowski’s second theorem, which provides us with a way of producing a generalised arithmetic progression from some sort of “convex progression”.⁴

Lemma 9.1 [Tao and Vu 2006, Lemma 3.33]. *Suppose that K is a symmetric convex body and Λ is a lattice, both in \mathbb{R}^d . Then there is a proper d -dimensional progression P in $K \cap \Lambda$ such that $|P| \geq \exp(-O(d \log 2d)) |K \cap \Lambda|$.*

The $\exp(-O(d \log d))$ factor should not come as a surprise: consider packing a d -dimensional cube (playing the role of the generalised progression) inside a d -dimensional sphere.

The question remains of how to find a “convex progression”, and to do this Ruzsa [1994] introduced an important embedding. Suppose that G is a (discrete) finite abelian group and $\Gamma \subset \widehat{G}$. Then we define a map

$$R_\Gamma : G \rightarrow C(\Gamma, \mathbb{R})$$

$$x \mapsto R_\Gamma(x) : \Gamma \rightarrow \mathbb{R}; \gamma \mapsto \frac{1}{2\pi} \arg(\gamma(x)),$$

⁴A more formal notion of convex progression is introduced by Green [2002b], where a detailed discussion and literature survey may be found.

where the argument is taken to lie in $(-\pi, \pi]$. Note that R_Γ preserves inverses, meaning that $R_\Gamma(-x) = -R_\Gamma(x)$, and furthermore if⁵

$$\|R_\Gamma(x_1)\|_{C(\Gamma, \mathbb{R})} + \cdots + \|R_\Gamma(x_d)\|_{C(\Gamma, \mathbb{R})} < \frac{1}{2},$$

then

$$R_\Gamma(x_1 + \cdots + x_d) = R_\Gamma(x_1) + \cdots + R_\Gamma(x_d).$$

This essentially encodes the idea that R_Γ behaves like a Freïman morphism.⁶ We shall use this embedding to establish the following proposition.

Proposition 9.2. *Suppose that G is a finite abelian group, $d \in \mathbb{N}$ and B is a Bohr set such that*

$$\mu_G(B_{(3d+1)\delta}) < 2^d \mu_G(B_\delta) \text{ for some } \delta < \frac{1}{4}(3d+1).$$

Then B_δ contains a proper coset progression M of dimension at most d satisfying the estimate $\beta_\delta(M) = \exp(-O(d \log 2d))$.

Proof. We write Γ for the frequency set of B and note that we may assume that $L := \bigcap \{\ker \gamma : \gamma \in \Gamma\}$ is trivial. Indeed, if it is nontrivial we may quotient out by it without impacting the hypotheses of the proposition; we call the quotiented Bohr set B' and note that $B_\delta = B'_\delta + L$ from which the result follows.

To start with note that if $x \in B_\eta$ then

$$\|R_\Gamma(x)\|_{C(\Gamma, \mathbb{R})} \leq \frac{1}{2\pi} \arccos(1 - \eta^2/2) \leq 2\eta,$$

and so since $2(3d+1)\delta < \frac{1}{2}$ we have that if $x_1, \dots, x_{3d+1} \in B_\delta$ then

$$R_\Gamma(x_1 + \cdots + x_{3d+1}) = R_\Gamma(x_1) + \cdots + R_\Gamma(x_{3d+1}). \tag{9-1}$$

By hypothesis we then have

$$\begin{aligned} |(3d+1)R_\Gamma(B_\delta)| &= |R_\Gamma((3d+1)B_\delta)| \leq |(3d+1)B_\delta| \\ &\leq |B_{(3d+1)\delta}| < 2^d |B_\delta| = 2^d |R_\Gamma(B_\delta)|. \end{aligned}$$

Apply the variant of Chang's covering lemma in Lemma 8.2 to the set $R_\Gamma(B_\delta)$ (which is symmetric since R_Γ preserves inverses and B_δ is symmetric) to get a set $X \subset R_\Gamma(B_\delta)$ with $|X| \leq d$ such that

$$3R_\Gamma(B_\delta) \subset \text{Span}(X) + 2R_\Gamma(B_\delta).$$

Writing V for the real subspace of $C(\Gamma, \mathbb{R})$ generated by X we see that $\dim V \leq d$ and (by induction) that

$$nR_\Gamma(B_\delta) \subset V + 2R_\Gamma(B_\delta)$$

for all n . Now, suppose that $v \in 2R_\Gamma(B_\delta)$. It follows that

$$n.v \in 2nR_\Gamma(B_\delta) \subset V + 2R_\Gamma(B_\delta).$$

⁵Recall that if X is a normed space then $\|\cdot\|_X$ denotes the norm on that space, so that $\|f\|_{C(\Gamma, \mathbb{R})} = \|f\|_{L^\infty(\Gamma)}$.

⁶We direct the unfamiliar reader to [Tao and Vu 2006, Chapter 5.3].

for all naturals n . Since $2R_\Gamma(B_\delta)$ is finite we see that there are two distinct naturals n and n' and some element $w \in 2R_\Gamma(B_\delta)$ such that $n.v, n'.v \in V + w$. It follows that $(n - n').v \in V$ whence $v \in V$ since V is a vector space and $n \neq n'$. We conclude that $R_\Gamma(B_\delta) \subset V$.

Let E be the group generated by B_δ which is finite, and note that $H := R_\Gamma(E) + C(\Gamma, \mathbb{Z})$ is a closed discrete subgroup of $C(\Gamma, \mathbb{R})$, where $C(\Gamma, \mathbb{Z})$ is the group of \mathbb{Z} -valued functions on Γ . Since H is a closed discrete subgroup of $C(\Gamma, \mathbb{R})$ contained in V , it is also a closed discrete subgroup of V . Since V is certainly generated by $R_\Gamma(B_\delta)$ and $H \supset R_\Gamma(B_\delta)$ we see that $\Lambda := H \cap V$ has finite covolume and so is a lattice in V .

Let ρ be the unique solution to $|1 - \exp(2\pi i \rho)| = \eta$ in the range $[0, \frac{1}{2}]$, and write Q_ρ for the ρ -cube in $C(\Gamma, \mathbb{R})$, which is a symmetric convex body in $C(\Gamma, \mathbb{R})$, and so $K := V \cap Q_\rho$ is a symmetric convex body in V . Now, by Lemma 9.1 the set $K \cap \Lambda$ contains a proper d -dimensional progression P of size $\exp(-O(d \log 2d))|K \cap \Lambda|$.

To see this note that by (9-1), $R_\Gamma|_{B_\delta}$ is a Freĭman 2-homomorphism. Now, if $x_1, x_2, x_3, x_4 \in B_\delta$ satisfy

$$R_\Gamma(x_1) + R_\Gamma(x_2) = R_\Gamma(x_3) + R_\Gamma(x_4)$$

then

$$R_\Gamma(x_1 + x_2 - x_3 - x_4) = R_\Gamma(x_1) + R_\Gamma(x_2) + R_\Gamma(-x_3) + R_\Gamma(-x_4) = 0.$$

However, $R_\Gamma(x) = 0$ if and only if $\gamma(x) = 1$ for all $\gamma \in \Gamma$, which is to say if and only if $x \in L$. Since L is trivial we conclude that $x_1 + x_2 = x_3 + x_4$ and hence that R_Γ is injective on B_δ , and $R_\Gamma^{-1} : R_\Gamma(B_\delta) \rightarrow B_\delta$ is a Freĭman 2-homomorphism.

On the other hand, by (9-1) $R_\Gamma : B_\delta \rightarrow R_\Gamma(B_\delta)$ is a Freĭman 2-homomorphism, and therefore also a Freĭman 2-isomorphism; hence its inverse $R_\Gamma^{-1} : R_\Gamma(B_\delta) \rightarrow B_\delta$ is one as well.

Since $B_\delta = R_\Gamma^{-1}(K \cap \Lambda)$, we are done by, for example, [Tao and Vu 2006, Proposition 5.24], which simply says that the image of a proper coset progression under a Freĭman isomorphism of order at least 2 is a proper coset progression of the same size and dimension; in particular $R_\Gamma^{-1}(P)$ is a proper coset progression of size $\exp(-O(d \log 2d))|B_\delta|$ and dimension at most d . □

10. Proof of the main theorem

The result driving Theorem 1.1 is the following which brings together all the ingredients of the paper.

Theorem 10.1. *Suppose that G is a finite abelian group, $A, S \subset G$ have $|A + S| \leq K \min\{|A|, |S|\}$, and $\epsilon \in (0, 1]$ is a parameter. Then there is a proper coset progression M with*

$$\dim M = O(\epsilon^{-2} \log^6 2\epsilon^{-1} K) \text{ and } |M| \geq \left(\frac{\epsilon}{2 \log K}\right)^{O(\epsilon^{-2} \log^6 2\epsilon^{-1} K)} |A + S|,$$

such that for any probability measure μ supported on M we have

$$\|1_{A+S} * \mu\|_{\ell^\infty(G)} \geq 1 - \epsilon \text{ and } \|1_A * \mu\|_{\ell^\infty(G)} \geq (1 - \epsilon) \frac{|A|}{|A + S|}.$$

Proof. We start by thinking of G as discrete and using counting measure. By Plünnecke's inequality [Tao and Vu 2006, Corollary 6.28] there is a nonempty set $S' \subset S$ such that

$$|A + A + S'| \leq \left(\frac{K \min\{|A|, |S|\}}{|S|} \right)^2 |S'| \leq K^2 \frac{|A||S'|}{|S|} \leq K^2 |A|.$$

Note, in particular, that since $|A + A + S'| \geq |A|$ we have $|S'| \geq |S|/K^2$ from the second inequality. Applying the inequality again we get a nonempty set $A' \subset A$ such that

$$|A' + (A + S') + (A + S')| \leq K^4 |A'|,$$

and it follows that

$$|(A + S') + (A + S')| \leq K^4 |A + S'|. \quad (10-1)$$

Now we apply Proposition 4.2 with $T = A$ to get a symmetric neighbourhood of the identity X such that

$$|X| \geq \exp(-O(\epsilon^{-2} k^2 \log^2 2K)) |A + S|$$

since $|A| \geq |A + S|/K$, and

$$|\mu_{-A} * 1_{A+S'} * \mu_{-S'}(x) - 1| \leq \epsilon/4 \quad \text{for all } x \in kX. \quad (10-2)$$

In the first instance it follows that $kX \subset (A + S') - (A + S')$. On the other hand, by the Plünnecke–Ruzsa estimates [Tao and Vu 2006, Corollary 6.29] applied to (10-1) we have

$$|4l((A + S') - (A + S'))| \leq K^{32l} |A + S'| = \exp(O(l \log K + \epsilon^{-2} k^2 \log^2 K)) |X|,$$

and hence

$$|4lkX| \leq \exp(O(l \log 2K + \epsilon^{-2} k^2 \log^2 2K)) |X|.$$

We put $l = \lceil \epsilon^{-2} k^2 \log 2K \rceil$, so that

$$|(3kl + 1)X| \leq |4klX| \leq 2^{kl \cdot O(k^{-1} \log 2K)} |X|.$$

Hence we can pick k such that

$$1 + \log \epsilon^{-1} K \leq k = O(\log 2\epsilon^{-1} K) \text{ and } |(3kl + 1)X| < 2^{kl} |X|.$$

By the variant of Chang's covering lemma in Lemma 8.2 there is some set T of size at most $kl = O(\epsilon^{-2} \log^4 2\epsilon^{-1} K)$ such that $3X \subset \text{Span}(T) + 2X$, and hence (by Lemma 8.3)

$$|(n + 2)X| \leq n^{O(\epsilon^{-2} \log^4 2\epsilon^{-1} K)} |2X| \text{ for all } n \geq 1.$$

On the other hand $|2X| \leq 2^{kl} |X|$, and so (rescaling the measure to think of G as compact) we have

$$\mu_G(nX) \leq n^{O(\epsilon^{-2} \log^4 2\epsilon^{-1} K)} \mu_G(X) \text{ for all } n \geq 1.$$

Now, by Proposition 7.1 applied to the set X there is a $d = O(kl \log 2kl\kappa^{-1})$ (which we may also assume is at least 1) and a regular Bohr set B such that

$$X - X \subset B_{\kappa/2} \text{ and } \mu_G(B_2) \leq \exp(d) \mu_G(X).$$

Let c be the absolute constant in the following technical lemma and note that since X is a neighbourhood of the identity, $X \subset B$ and $\beta(X) \geq \exp(-d)$.

We apply Chang’s theorem relative to B to get that $\text{Spec}_c(1_X, \beta) = \text{Spec}_c(\mu_X)$ has $(1, \beta)$ -relative entropy

$$r = O(c^{-2} \log 2 \|1_X\|_{L^2(\beta)} \|1_X\|_{L^1(\beta)}^{-1}) = O(d).$$

It follows from Lemma 6.3 that there is a set of characters Λ of size r and a $\rho = \Omega(1/(1 + h(B))r)$ such that for all $\gamma \in \text{Spec}_c(\mu_X)$ we have

$$|1 - \gamma(x)| = O(vr + \rho'rh(B)h(B_\rho)) \quad \text{for all } x \in B_{\rho'} \wedge B'_v,$$

where B' is the Bohr set with width function the constant function 2 and frequency set Λ . Provided $\rho \geq \kappa$ we see that

$$\mu_G(X) \leq \mu_G(B_{\rho/2}) \leq \mu_G(B_{1/2}) \text{ and } \mu_G(B_{2\rho}) \leq \mu_G(B_2) \leq \exp(d)\mu_G(X),$$

and so it follows that $h(B), h(B_\rho) \leq d$. It follows that $\rho = \Omega(1/d^2)$ and

$$|1 - \gamma(x)| = O(vd + \rho'd^3) \quad \text{for all } x \in B_{\rho'} \wedge B'_v \text{ and } \gamma \in \text{Spec}_c(\mu_X).$$

Pick $\rho' = \Omega(\epsilon/d^3 K^2)$ and $v = \Omega(\epsilon/K^2 d)$ such that $B'' := B_{\rho'} \wedge B'_v$ has

$$|1 - \gamma(x)| \leq \epsilon/4K^2 \quad \text{for all } x \in B'' \text{ and } \gamma \in \text{Spec}_c(\mu_X).$$

In particular

$$\rho', v = \Omega(1/K^2 d^{O(1)}).$$

For each $\lambda \in \Lambda$ write $B^{(\lambda)}$ for the Bohr set with frequency set $\{\lambda\}$ and width function the constant function 2, thus $B'_v = \bigwedge_{\lambda \in \Lambda} B_v^{(\lambda)}$. By Lemma 5.1 we see that

$$\mu_G(B''_\eta) \geq \mu_G(B_{\eta\rho'/2}) \prod_{\lambda \in \Lambda} \mu_G(B_{\eta v/2}^{(\lambda)}).$$

On the other hand, since $B^{(\lambda)}$ has a frequency set of size 1 we see (from (5-2)) that

$$\mu_G(B_{\eta'}^{(\lambda)}) \geq \frac{1}{\pi} \min\{\eta', 2\}.$$

Now, if $\eta\rho'/2 \geq \kappa$ we have

$$\mu_G(B''_\eta) \geq (\eta v/2\pi)^r \mu_G(X),$$

and on the other we have $\mu_G(B) \leq \exp(d)\mu_G(X)$. Let $t \geq 1$ be a natural such that

$$(16\pi(3t + 1)v^{-1})^r \exp(d) < 2^t \text{ and } t = O(d \log 2dK).$$

Then if $\eta \in [\frac{1}{8}(3t + 1), \frac{1}{4}(3t + 1))$ we have

$$\mu_G(B''_{(3t+1)\eta}) < 2^t \mu_G(B''_\eta).$$

We now apply Proposition 9.2 to get that B''_η contains a proper coset progression M of dimension at most t and size $(2t)^{-O(t)}\mu_G(X)$. The result is proved on an application of the next lemma provided such a choice of η is possible. This can be done if κ can be chosen such that

$$\frac{\rho'}{8(3t+1)} > \kappa,$$

which can be done with $\kappa = \Omega(\epsilon^{O(1)}K^{-O(1)})$, and working this back gives that $t = O(\epsilon^{-2} \log^6 2\epsilon^{-1}K)$ and the result. \square

The next lemma is here simply to avoid interrupting the flow of the previous argument, and the hypotheses are set up purely for that setting. The proof is simply a series of standard Fourier manipulations.

Lemma 10.2. *There is an absolute constant $c > 0$ such that if G is a finite abelian group, $A, S, X \subset G$ have $|A + S| \leq K \min\{|A|, |S|\}$, $S' \subset S$ has $|S'| \geq |S|/K^2$, $k \geq \log \epsilon^{-1}K$ is a natural number such that*

$$|\mu_{-A} * 1_{A+S'} * \mu_{-S'}(x) - 1| \leq \epsilon/4 \quad \text{for all } x \in kX,$$

and M is a set such that

$$|1 - \gamma(x)| \leq \epsilon/4K^2 \quad \text{for all } x \in M \text{ and } \gamma \in \text{Spec}_c(\mu_X), \tag{10-3}$$

then for any probability measure μ supported on M we have

$$\|1_{A+S} * \mu\|_{\ell^\infty(G)} \geq 1 - \epsilon \quad \text{and} \quad \|1_A * \mu\|_{\ell^\infty(G)} \geq (1 - \epsilon) \frac{|A|}{|A + S|}.$$

Proof. Integrating the first hypothesis we get

$$|\langle \mu_{-A} * 1_{A+S'} * \mu_{-S'}, \mu_X^{(k)} \rangle - 1| \leq \epsilon/4,$$

where $\mu_X^{(k)}$ denotes the k -fold convolution of μ_X with itself. By Fourier inversion we have

$$\left| \sum_{\gamma \in \widehat{G}} \widehat{1_{A+S'}}(\gamma) \overline{\widehat{\mu_A}(\gamma)} \widehat{\mu_{S'}}(\gamma) \widehat{\mu_X}(\gamma)^k - 1 \right| \leq \epsilon/4. \tag{10-4}$$

The triangle inequality, Cauchy–Schwarz and Parseval’s theorem in the usual way tell us that

$$\sum_{\gamma \in \widehat{G}} |\widehat{1_{A+S'}}(\gamma) \widehat{\mu_A}(\gamma) \widehat{\mu_{S'}}(\gamma)| \leq \mu_G(A + S') \|\widehat{\mu_A}\|_{\ell^2(\widehat{G})} \|\widehat{\mu_{S'}}\|_{\ell^2(\widehat{G})} = \frac{\mu_G(A + S')}{\sqrt{\mu_G(A)\mu_G(S')}} \leq K^2. \tag{10-5}$$

Then, by the triangle inequality, for any probability measure μ supported on M we have

$$|\widehat{\mu}(\gamma) - 1| \leq \epsilon/4K^2 \quad \text{for all } \gamma \in \text{Spec}_c(\mu_X). \tag{10-6}$$

We conclude that

$$E := \left| \langle 1_{A+S'} * \mu, \mu_A * \mu_{S'} * \mu_X^{(k)} * \mu \rangle - 1 \right| = \left| \sum_{\gamma \in \widehat{G}} \widehat{1_{A+S'}}(\gamma) \widehat{\mu}(\gamma) \overline{\widehat{\mu_A}(\gamma)} \widehat{\mu_{S'}}(\gamma) \widehat{\mu_X}(\gamma)^k \widehat{\mu}(\gamma) - 1 \right|$$

is at most $S_1 + S_2 + S_3$, where

$$\begin{aligned}
 S_1 &:= \left| \sum_{\gamma \notin \text{Spec}_c(\mu_X)} \widehat{1_{A+S'}(\gamma)} \overline{\widehat{\mu_A(\gamma)} \widehat{\mu_{S'}(\gamma)} \widehat{\mu_X(\gamma)}^k} (|\widehat{\mu}(\gamma)|^2 - 1) \right|, \\
 S_2 &:= \left| \sum_{\gamma \in \text{Spec}_c(\mu_X)} \widehat{1_{A+S'}(\gamma)} \overline{\widehat{\mu_A(\gamma)} \widehat{\mu_{S'}(\gamma)} \widehat{\mu_X(\gamma)}^k} (|\widehat{\mu}(\gamma)|^2 - 1) \right|, \\
 S_3 &:= \left| \sum_{\gamma \in \widehat{G}} \widehat{1_{A+S'}(\gamma)} \overline{\widehat{\mu_A(\gamma)} \widehat{\mu_{S'}(\gamma)} \widehat{\mu_X(\gamma)}^k} - 1 \right|.
 \end{aligned}$$

By the triangle inequality and (10-5) we see that

$$S_1 \leq \sup_{\gamma \notin \text{Spec}_c(\mu_X)} |\widehat{\mu_X(\gamma)}|^k \cdot \sum_{\gamma \in \widehat{G}} |\widehat{1_{A+S'}(\gamma)} \widehat{\mu_A(\gamma)} \widehat{\mu_{S'}(\gamma)}| \leq c^k K^2 \leq \epsilon/4$$

for a suitable choice of $c = \Omega(1)$, since $k \geq \log \epsilon^{-1} K$; by (10-5) and (10-6) we see that

$$S_2 \leq 2 \sup_{\gamma \in \text{Spec}_c(\mu_X)} |\widehat{\mu}(\gamma) - 1| \cdot \sum_{\gamma \in \widehat{G}} |\widehat{1_{A+S'}(\gamma)} \widehat{\mu_A(\gamma)} \widehat{\mu_{S'}(\gamma)}| \leq 2(\epsilon/4K^2)K^2 \leq \epsilon/2;$$

and finally by (10-4) we see that $S_3 \leq \epsilon/4$, so that $E \leq \epsilon$. It follows from this that

$$\langle 1_{A+S'} * \mu, \mu_A * \mu_{S'} * \mu_X^{(k)} * \mu \rangle \geq 1 - \epsilon,$$

and hence by averaging that

$$\|1_{A+S'} * \mu\|_{L^\infty(G)} \geq 1 - \epsilon \quad \text{and} \quad \|1_A * \mu\|_{L^\infty(G)} \geq (1 - \epsilon) \frac{\mu_G(A)}{\mu_G(A + S')}.$$

The lemma is proved. □

It is worth making a couple of remarks before continuing. First, Theorem 10.1 can be extended to infinite abelian groups by embedding the sets there in a finite group via a sufficiently large Freïman isomorphism. This is the finite modelling argument of [Green and Ruzsa 2007, Lemma 2.1], but we shall not pursue it here.

The expected ϵ -dependence in Theorem 10.1 may be less clear than the K -dependence. The argument we have given works equally well for the so-called popular difference set in place of 1_{A+S} , that is the set

$$D(A, S) := \{x \in G : 1_A * 1_S(x) \geq c\epsilon/K\}$$

for sufficiently small c . On the other hand Wolf [2010], developing the niveau set construction of Ruzsa [1987; 1991], showed that even finding a large sumset in such popular difference sets is hard, and it seems likely that her arguments can be adapted to cover the case of $D(A, S)$ containing a proportion $1 - \epsilon$ of a sumset.

Understanding this, even in the model setting of $G = \mathbb{F}_2^n$, would be of great interest since a better ϵ -dependence would probably yield better analysis of inner products of the form $\langle 1_A * 1_S, 1_T \rangle$ which are of importance in, for example, Roth's theorem [Roth 1953; 1952].

We are now in a position to prove Theorem 1.1 by an easy pigeonhole argument.

Proof of Theorem 1.1. Freiman 2-embed the sets A and S into a finite group (via, for example, the method of [Green and Ruzsa 2007, Lemma 2.1]); if we can prove the result there then it immediately pulls back.

Apply Theorem 10.1 with $\epsilon = \frac{1}{2}(1 + \sqrt{2})$ to get a proper d -dimensional coset progression M . Note that we may assume the progression is symmetric by translating it and possibly shrinking it by a factor of $\exp(d)$; this has no impact on the bounds. Thus we put

$$M = H + \{x_1.l_1 + \cdots + x_d.l_d : |l_i| \leq L_i \text{ for all } 1 \leq i \leq d\}$$

where $L_1, \dots, L_d \in \mathbb{N}$, $H \leq G$ and $x_1, \dots, x_d \in G$. Write

$$M_\eta := H + \{x_1.l_1 + \cdots + x_d.l_d : |l_i| \leq \eta L_i \text{ for all } 1 \leq i \leq d\},$$

and note that $|M_1| \leq \exp(O(d))|M_{1/2}|$. On the other hand if $j\eta \leq \frac{1}{2}$ we have

$$M_{1/2} \subset M_{1/2+\eta} \subset \cdots \subset M_{1/2+j\eta} = M_1,$$

so it follows that there is some $\eta = \Omega(1/d)$ and $i \leq j = O(d)$ such that $|M_{1/2+i\eta}| \leq 2^{1/2}|M_{1/2+(i-1)\eta}|$. Since $\eta = \Omega(1/d)$ we easily have that $|M_\eta| = \exp(-O(d \log d))|M_1|$. On the other hand if we apply the conclusion of Theorem 10.1 with

$$\mu = \frac{1_{M_{1/2+i\eta}} + 1_{M_{1/2+(i-1)\eta}}}{|M_{1/2+i\eta}| + |M_{1/2+(i-1)\eta}|}$$

we get an element x such that

$$|(x + A + S) \cap M_{1/2+i\eta}| + |(x + A + S) \cap M_{1/2+(i-1)\eta}|$$

is at least

$$(1 - \epsilon)(|M_{1/2+i\eta}| + |M_{1/2+(i-1)\eta}|).$$

But then if $z \in M_\eta$ we get

$$\begin{aligned} 1_{A+S} * 1_{-(A+S)}(z) &= 1_{x+A+S} * 1_{-(x+A+S)}(z) \\ &\geq 1_{(x+A+S) \cap M_{1/2+i\eta}} * 1_{-(x+A+S) \cap M_{1/2+(i-1)\eta}}(z) \\ &\geq |(x + A + S) \cap M_{1/2+i\eta}| + |z + ((x + A + S) \cap M_{1/2+(i-1)\eta})| \\ &\quad - |((x + A + S) \cap M_{1/2+i\eta}) \cup (z + ((x + A + S) \cap M_{1/2+(i-1)\eta}))| \\ &\geq |(x + A + S) \cap M_{1/2+i\eta}| + |(x + A + S) \cap M_{1/2+(i-1)\eta}| - |M_{1/2+i\eta}| \\ &\geq (1 - (1 + \sqrt{2})\epsilon)|M_{1/2+(i-1)\eta}| > 0, \end{aligned}$$

and it follows that $(A - A) + (S - S)$ contains M_η . Tracking through the bounds we get the result. \square

11. Concluding remarks and applications

To begin with we should remark that in the case when G has bounded exponent or is torsion-free, we can get slightly better bounds and the argument is much simpler because of the presence of a good modelling lemmas. In the first case we get the following result, a proof of which (in the case $G = \mathbb{F}_2^n$) is contained in the Appendix as it is so short.

Theorem 11.1 (Bogolyubov–Ruzsa lemma for bounded exponent abelian groups). *Suppose G is an abelian group of exponent r and $A, S \subset G$ are finite nonempty sets such that $|A + S| \leq K \min\{|A|, |S|\}$. Then $(A - A) + (S - S)$ contains a subspace V of size $\exp(-O_r(\log^4 2K))|A + S|$.*

In the second, the material of Sections 5–9 can be replaced by similar but more standard arguments because of the following modelling lemma.

Lemma 11.2 (modelling for torsion-free abelian groups [Ruzsa 2009, Theorem 3.5]). *Suppose that G is a torsion-free abelian group, $A \subset G$ is a finite nonempty set and $k \geq 2$ is a natural. Then for every $q \geq |kA - kA|$ there is a set $A' \subset A$ with $|A'| \geq |A|/k$ such that A' is Freĭman k -isomorphic to a subset of $\mathbb{Z}/q\mathbb{Z}$.*

Theorem 11.3 (Bogolyubov–Ruzsa lemma for torsion-free abelian groups). *Suppose that G is a torsion-free abelian group and $A, S \subset G$ are finite nonempty sets such that $|A + S| \leq K \min\{|A|, |S|\}$. Then $(A - A) + (S - S)$ contains a proper symmetric $d(K)$ -dimensional coset progression M of size*

$$\exp(-h(K))|A + S|.$$

Moreover, we may take $d(K) = O(\log^4 2K)$ and $h(K) = O(\log^4 2K \log 2 \log 2K)$.

Returning to Theorem 1.1 it is easy to see that we must have $d(K), h(K) = \Omega(\log K)$ by considering a union of \sqrt{K} coset progressions of dimension $\log_2 \sqrt{K}$, and even achieving this bound may be hard without refining the definition of a coset progression. (See the comments of Green in [Tao 2008b] for a discussion of this.)

The paper [Schoen 2011] was a major breakthrough in proving the first good bounds for (a slight variant of) Theorem 1.1; it was essentially shown that one could take

$$d(K), h(K) = O(\exp(O(\sqrt{\log K})))$$

for torsion-free or bounded-exponent abelian groups.

Indeed, it should be clear that while we do not use [Schoen 2011] directly in the proof of Theorem 1.1, it has had a considerable influence on the present work and the applications which now follow are from the end of that paper as well.

Freĭman’s theorem. As an immediate corollary of Theorem 1.1 and Chang’s covering lemma we have the following.

Theorem 11.4 (Freĭman’s theorem for abelian groups). *Suppose that G is an (discrete) abelian group and $A \subset G$ is finite with $|A \pm A| \leq K|A|$. Then A is contained in a $d(K)$ -dimensional coset progression M of size at most $\exp(h(K))|A|$. Moreover, we may take $d(K), h(K) = O(K \log^{O(1)} 2K)$.*

By considering a union of K dissociated translates of a coset progression it is easy to see that we must have $d(K), h(K) = \Omega(K)$, so the result is close to best possible.

Green and Ruzsa [2007] provided the first bounds of $d(K), h(K) = O(K^{4+o(1)})$, and the peppering of their work throughout this paper should indicate the importance of their ideas.

Schoen [2011] improved the bounds to $O(K^{3+o(1)})$ and to $O(K^{1+o(1)})$ for certain classes of groups, and in [Cwalina and Schoen 2010] the structure is further elucidated with particular emphasis on getting good control on the dimension.

The U^3 -inverse theorem. Theorem 1.1 can be inserted into the various U^3 -inverse theorems of Tao and Green [2008] for finite abelian groups of odd order, and Samorodnitsky [2007] (see also [Wolf 2009]) for \mathbb{F}_2^n to improve the bounds there. In particular one gets the following.

Theorem 11.5 ($U^3(\mathbb{F}_2^n)$ -inverse theorem). *Suppose that $f \in L^\infty(\mathbb{F}_2^n)$ has $\|f\|_{U^3(\mathbb{F}_2^n)} \geq \delta \|f\|_{L^\infty(\mathbb{F}_2^n)}$. Then there is a quadratic polynomial $q : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that*

$$|\langle f, (-1)^q \rangle_{L^2(\mathbb{F}_2^n)}| \geq \exp(-O(\log^{O(1)} 2\delta^{-1})) \|f\|_{L^\infty(\mathbb{F}_2^n)}.$$

In fact the connection between good bounds in results of this type and good bounds in Freïman-type theorems is quite clearly developed by Green and Tao [2010] and Lovett [2010].

Long arithmetic progressions in sumsets. The question of finding long arithmetic progressions in sets of integers is one of central interest in additive combinatorics. The basic question has the following form: suppose that $A_1, \dots, A_k \subset \{1, \dots, N\}$ all have density at least α . How long an arithmetic progression can we guarantee that $A_1 + \dots + A_k$ contain?

For one set this is addressed by the notoriously difficult Szemerédi's theorem [1969; 1975], where the best quantitative work is that of Gowers [1998; 2001]; for two sets the longest progression is much longer with the state of the art due to Green [2002a]; for three sets or more the results get even stronger with the work of Freïman, Halberstam and Ruzsa [Freïman et al. 1992]; and finally for eight sets or more, longer again by the recent work of Schoen [2011].

Theorem 1.1 yields an immediate improvement for the case of four sets or more.

Theorem 11.6. *Suppose that $A_1, \dots, A_4 \subset \{1, \dots, N\}$ all have density at least α . Then $A_1 + \dots + A_4$ contains an arithmetic progression of length $N^{O(\log^{-O(1)} 2\alpha^{-1})}$.*

Proof. Since $|A_i + A_j| \leq 2\alpha^{-1}|A_i|$ for all i, j we have, by averaging, that there is a symmetric set A of density $\alpha^{O(1)}$ such that A_1, \dots, A_4 each contains a translate of A . In particular, the longest progression in $A - A + A - A$ is contained in a translate of $A_1 + A_2 + A_3 + A_4$.

Now, by Theorem 1.1 the set $A - A + A - A$ contains an $O(\log^{O(1)} \alpha^{-1})$ -dimensional coset progression M of size $\exp(-O(\log^{O(1)} \alpha^{-1}))N$. Since \mathbb{Z} is torsion-free the progression is just a generalised progression which certainly contains a 1-dimensional progression of length $|M|^{1/\dim M}$. The result is proved. \square

It is not clear that this result gives the best possible conclusion for k sets as k tends to infinity, but if one were interested in this no doubt some improvement could be squeezed out by delving into the main proof.

$\Lambda(4)$ -estimate for the squares. Inserting Theorem 1.1 into a result from [Chang 2004] (itself developed from an argument of Bourgain in [Johnson and Lindenstrauss 2001]) yields the following $\Lambda(4)$ -estimate for the squares.

Theorem 11.7. *Suppose that n_1, \dots, n_k are naturals. Then*

$$\int \left| \sum_{i=1}^k \exp(2\pi i n_i^2 \theta) \right|^4 d\theta = O(k^3 \exp(-\Omega(\log^{\Omega(1)} 2k))).$$

This is essentially equivalent to inserting Theorem 1.1 into the proof of [Schoen 2011, Theorem 8] and Gowers’ [1998] version of the Balog–Szemerédi lemma [1994]. In any case a conjecture of Rudin [1960] suggests that the bound $O(k^{2+o(1)})$ is likely to be true, and the above is not even a power-type improvement on the trivial upper bound of k^3 .

The Konyagin–Łaba theorem. Theorem 1.1 inserted into the argument at the end of [Schoen 2011] yields the following quantitative improvement to a result from [Konyagin and Łaba 2006].

Theorem 11.8 (Konyagin–Łaba theorem). *Suppose that A is a set of reals and $\alpha \in \mathbb{R}$ is transcendental. Then*

$$|A + \alpha \cdot A| = \exp(\Omega(\log^{\Omega(1)} 2|A|))|A|.$$

What is particularly interesting here is that there is a simple construction which shows that there are arbitrarily large sets A with $|A + \alpha \cdot A| = \exp(O(\sqrt{\log |A|}))|A|$.

Appendix: Proof of Theorem 11.1

Our objective in this appendix is to prove the following result.

Theorem A.1. *Suppose that $G := \mathbb{F}_2^n$, and $A \subset G$ has density $\alpha > 0$. Then there is a subspace $V \leq G$ with $\text{cod } V = O(\log^4 2\alpha^{-1})$ such that $V \subset 4A$.*

We have distilled this argument out because it is short and just uses the two ingredients of the Croot–Sisask lemma and Chang’s theorem. For the reader interested in a little more motivation the sketch after the introduction may be of more interest.

In the rather special setting of \mathbb{F}_2^n it is known from [Green and Ruzsa 2007, Proposition 6.1] that if $|A + A| \leq K|A|$ then A is Freĭman δ -isomorphic to a set A' of density $K^{-O(1)}$ in some \mathbb{F}_2^m , from which we get the following corollary of Theorem A.1.

Corollary A.2. *Suppose that $G := \mathbb{F}_2^n$, and $A \subset G$ has $|A + A| \leq K|A|$. Then there is a subspace $V \leq G$ with $|V| \geq \exp(-O(\log^4 2K))|A|$ such that $V \subset 4A$.*

In this setting the result of Croot and Sisask is the following.

Lemma A.3 (Croot–Sisask). *Suppose that $G := \mathbb{F}_2^n$, $f \in L^p(G)$ and $A \subset G$ has density $\alpha > 0$. Then there is an $a \in A$ and a set T with $\mu_G(T) \geq (\alpha/2)^{O(\epsilon^{-2p})}$ such that*

$$\|\rho_t(f * \mu_A) - f * \mu_A\|_{L^p(G)} \leq \epsilon \|f\|_{L^p(G)} \quad \text{for all } t \in T.$$

Additionally we have:

Lemma A.4 (Chang's theorem). *Suppose that $G := \mathbb{F}_2^n$ and $A \subset G$ has density $\alpha > 0$. Then*

$$\text{cod Spec}_\epsilon(\mu_A)^\perp = O(\epsilon^{-2} \log 2\alpha^{-1}).$$

Proof of Theorem A.1. We begin by noting that

$$\langle 1_{2A} * 1_A, 1_A \rangle = \langle 1_{2A}, 1_A * 1_A \rangle = \alpha^2. \quad (\text{A-1})$$

By the Croot–Sisask lemma applied with $f := 1_{2A}$ we get a set $T \subset G$ with $\mu_G(T) \geq (\alpha/2)^{O(k^2 p)}$ such that

$$\|\rho_t(1_{2A} * 1_A) - 1_{2A} * 1_A\|_{L^p(G)} \leq \alpha/4ke \quad \text{for all } t \in T.$$

By the triangle inequality this gives

$$\|\rho_t(1_{2A} * 1_A) - 1_{2A} * 1_A\|_{L^p(G)} \leq \alpha/4e \quad \text{for all } t \in kT,$$

and so on integrating (and applying the triangle inequality again) we have

$$\|1_{2A} * 1_A * \mu_T^{(k)} - 1_{2A} * 1_A\|_{L^p(G)} \leq \alpha/4e.$$

By Hölder's inequality we get

$$|\langle 1_{2A} * 1_A * \mu_T^{(k)}, 1_A \rangle - \langle 1_{2A} * 1_A, 1_A \rangle| \leq \alpha \alpha^{1+1/(p-1)}/4e.$$

Choosing $p = 1 + \log \alpha^{-1}$ and inserting (A-1) we have

$$|\langle 1_{2A} * 1_A * \mu_T^{(k)}, 1_A \rangle - \alpha^2| \leq \alpha^2/4,$$

and so by the triangle inequality

$$\langle 1_{2A} * 1_A * \mu_T^{(k)}, 1_A \rangle_{L^p(G)} \geq 3\alpha^2/4.$$

Now, put $V := \text{Spec}_{1/2}(\mu_T)^\perp$ and $g := 1_{2A} * 1_A * \mu_T^{(k)}$, so that

$$|\langle g, 1_A \rangle - \langle g * \mu_V, 1_A \rangle| = \left| \sum_{\gamma \notin V^\perp} \widehat{1_{2A}}(\gamma) |\widehat{1_A}(\gamma)|^2 \widehat{\mu_T}(\gamma)^k \right| \leq \alpha 2^{-k} \leq \alpha^2/8,$$

by Parseval's theorem, the definition of V and by taking $k = O(\log 2\alpha^{-1})$ a sufficiently large natural. It follows by the triangle inequality that

$$\langle 1_{2A} * 1_A * \mu_T^{(k)} * \mu_V, 1_A \rangle > \alpha^2/2,$$

and so, by averaging, that $\|1_{2A} * \mu_V\|_{L^\infty(G)} > \frac{1}{2}$. We conclude that $4A$ contains V by the pigeon-hole principle and the result is proved on applying Chang's theorem to see that

$$\text{cod } V = O(\log 2\mu_G(T)^{-1}) = O(\log^4 2\alpha^{-1}). \quad \square$$

Acknowledgement

The author should like to thank Julia Wolf for useful discussions surrounding the $U^3(\mathbb{F}_2^n)$ -inverse theorem, and an anonymous referee for a thorough reading of the paper and numerous useful suggestions.

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
- [Bogolyubov 1939] N. N. Bogolyubov, “On some arithmetic properties of quasi-periods”, *Zap. kaf. matem. fiz. Akad. Nauk Ukr. = Ann. Chaire Phys. Math. Acad. Sci. Ukraine (Kiev)* **4** (1939), 185–194 (in Ukrainian), 195–205 (in French). MR 8,512b JFM 65.0268.01
- [Bourgain 1990] J. Bourgain, “On arithmetic progressions in sums of sets of integers”, pp. 105–109 in *A tribute to Paul Erdős*, edited by A. Baker et al., Cambridge University Press, 1990. MR 92e:11011 Zbl 0715.11006
- [Bourgain 1999] J. Bourgain, “On triples in arithmetic progression”, *Geom. Funct. Anal.* **9**:5 (1999), 968–984. MR 2011h: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
- [Chang 2002] M.-C. Chang, “A polynomial bound in Freiman’s theorem”, *Duke Math. J.* **113**:3 (2002), 399–419. MR 2033d:11151 Zbl 1035.11048
- [Chang 2004] M.-C. Chang, “On problems of Erdős and Rudin”, *J. Funct. Anal.* **207**:2 (2004), 444–460. MR 2004j:11022 Zbl 1046.11012
- [Crook and Sisask 2010] E. Crook and O. Sisask, “A probabilistic technique for finding almost-periods of convolutions”, *Geom. Funct. Anal.* **20**:6 (2010), 1367–1396. MR 2012d:11019 Zbl 1234.11013
- [Cwalina and Schoen 2010] K. Cwalina and T. Schoen, “A linear bound on the dimension in Green–Ruzsa’s theorem”, preprint, 2010, available at <http://ssdm.mimuw.edu.pl/pliki/prace-studentow/karol-cwalina-1.pdf>.
- [Freĭman et al. 1992] G. A. Freĭman, H. Halberstam, and I. Z. Ruzsa, “Integer sum sets containing long arithmetic progressions”, *J. London Math. Soc.* (2) **46**:2 (1992), 193–201. MR 93j:11008 Zbl 0768.11005
- [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
- [Gowers 2001] W. T. Gowers, “A new proof of Szemerédi’s theorem”, *Geom. Funct. Anal.* **11**:3 (2001), 465–588. MR 2002k:11014 Zbl 1028.11005
- [Gowers and Wolf 2011] W. T. Gowers and J. Wolf, “Linear forms and quadratic uniformity for functions on \mathbb{Z}_N ”, *J. Anal. Math.* **115** (2011), 121–186. MR 2855036 arXiv 1002.2210
- [Green 2002a] B. J. Green, “Arithmetic progressions in sumsets”, *Geom. Funct. Anal.* **12**:3 (2002), 584–597. MR 2003i:11148 Zbl 1020.11009
- [Green 2002b] B. J. Green, “Structure theory of set addition: Edinburgh–MIT lecture notes on Freĭman’s theorem”, preprint, 2002, available at <http://www.dpmms.cam.ac.uk/~bjg23/papers/icmsnotes.pdf>.
- [Green 2003] B. J. Green, “Some constructions in the inverse spectral theory of cyclic groups”, *Combin. Probab. Comput.* **12**:2 (2003), 127–138. MR 2004b:11144 Zbl 1097.11051
- [Green 2004] B. J. Green, “Spectral structure of sets of integers”, pp. 83–96 in *Fourier analysis and convexity*, edited by L. Brandolini et al., Birkhäuser, Boston, 2004. MR 2005i:11015 Zbl 1093.11004
- [Green 2009] B. J. Green, “Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak”, preprint, 2009. arXiv 0911.3354
- [Green and Konyagin 2009] B. J. Green and S. Konyagin, “On the Littlewood problem modulo a prime”, *Canad. J. Math.* **61**:1 (2009), 141–164. MR 2010a:42001 Zbl 1232.11013

- [Green and Ruzsa 2006] B. J. Green and I. Z. Ruzsa, “Sets with small sumset and rectification”, *Bull. London Math. Soc.* **38**:1 (2006), 43–52. MR 2006i:11027 Zbl 1155.11307
- [Green and Ruzsa 2007] B. J. Green and I. Z. Ruzsa, “Freiman’s theorem in an arbitrary abelian group”, *J. London Math. Soc.* (2) **75**:1 (2007), 163–175. MR 2007m:20087 Zbl 1133.11058
- [Green and Tao 2008] B. J. Green and T. Tao, “An inverse theorem for the Gowers $U^3(G)$ norm”, *Proc. Edinb. Math. Soc.* (2) **51**:1 (2008), 73–153. MR 2009g:11012 Zbl 1202.11013
- [Green and Tao 2010] B. J. Green and T. Tao, “An equivalence between inverse sumset theorems and inverse conjectures for the U^3 norm”, *Math. Proc. Cambridge Philos. Soc.* **149**:1 (2010), 1–19. MR 2011g:11019 Zbl 1229.11132
- [Johnson and Lindenstrauss 2001] W. B. Johnson and J. Lindenstrauss (editors), *Handbook of the geometry of Banach spaces, I*, North-Holland, Amsterdam, 2001. MR 2003a:46001 Zbl 0970.46001
- [Konyagin and Łaba 2006] S. Konyagin and I. Łaba, “Distance sets of well-distributed planar sets for polygonal norms”, *Israel J. Math.* **152** (2006), 157–179. MR 2006m:11032 Zbl 1127.52021
- [López and Ross 1975] J. M. López and K. A. Ross, *Sidon sets*, Lecture Notes in Pure and Applied Mathematics **13**, Marcel Dekker, New York, 1975. MR 55 #13173 Zbl 0351.43008
- [Lovett 2010] S. Lovett, “Equivalence of polynomial conjectures in additive combinatorics”, preprint, 2010. To appear in *Combinatorica*. arXiv 1001.3356
- [Milnor 1968] J. Milnor, “Growth of finitely generated solvable groups”, *J. Differential Geometry* **2** (1968), 447–449. MR 39 #6212 Zbl 0176.29803
- [Roth 1952] K. F. 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 1960] W. Rudin, “Trigonometric series with gaps”, *J. Math. Mech.* **9** (1960), 203–227. MR 22 #6972 Zbl 0091.05802
- [Rudin 1990] W. Rudin, *Fourier analysis on groups*, Wiley, New York, 1990. MR 91b:43002 Zbl 0698.43001
- [Ruzsa 1987] I. Z. Ruzsa, “Essential components”, *Proc. London Math. Soc.* (3) **54**:1 (1987), 38–56. Zbl 0609.10042
- [Ruzsa 1991] I. Z. Ruzsa, “Arithmetic progressions in sumsets”, *Acta Arith.* **60**:2 (1991), 191–202. MR 92k:11009 Zbl 0728.11009
- [Ruzsa 1994] I. Z. Ruzsa, “Generalized arithmetical progressions and sumsets”, *Acta Math. Hungar.* **65**:4 (1994), 379–388. MR 95k:11011 Zbl 0816.11008
- [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**, Société de Mathématique de France, Paris, 1999. MR 2000h:11111 Zbl 0946.11007
- [Ruzsa 2009] I. Z. Ruzsa, “Sumsets and structure”, pp. 87–210 in *Combinatorial number theory and additive group theory*, edited by A. Geroldinger and I. Z. Ruzsa, Birkhäuser, Basel, 2009. MR 2010m:11013 Zbl 1221.11026
- [Samorodnitsky 2007] A. Samorodnitsky, “Low-degree tests at large distances”, pp. 506–515 in *STOC’07: Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, edited by D. Johnson, ACM, New York, 2007. MR 2009f:68077 Zbl 1232.68175
- [Sanders 2012] T. Sanders, “On certain other sets of integers”, *J. Anal. Math.* **116** (2012), 53–82. MR 2892617
- [Schoen 2003] T. Schoen, “Multiple set addition in \mathbb{Z}_p ”, *Integers* **3** (2003), Paper #A17. MR 2004j:11012 Zbl 1089.11009
- [Schoen 2011] T. Schoen, “Near optimal bounds in Freiman’s theorem”, *Duke Math. J.* **158**:1 (2011), 1–12. MR 2012f:11018 Zbl 05904309
- [Shkredov 2006] I. D. Shkredov, “On sets of large exponential sums”, *Dokl. Akad. Nauk* **411**:4 (2006), 455–459. In Russian; translated in *Dokl. Math.* **74**:3 (2006), 860–864. MR 2009j:11130 Zbl 1211.11093 arXiv math/0605689
- [Shkredov 2007] I. D. Shkredov, “Some examples of sets of large trigonometric sums”, *Mat. Sb.* **198**:12 (2007), 105–140. In Russian; translated in *Sb. Math.* **198**:12 (2007), 1805–1838. MR 2009e:11150 Zbl 1176.11038
- [Shkredov 2008] I. D. Shkredov, “On sets of large trigonometric sums”, *Izv. Ross. Akad. Nauk Ser. Mat.* **72**:1 (2008), 161–182. In Russian; translated in *Izv. Math.* **72**:1 (2008), 149–168. MR 2009e:11151 Zbl 1148.11040

- [Sisask 2009] O. Sisask, “Bourgain’s proof of the existence of long arithmetic progressions in $A + B$ ”, preprint, 2009, available at <http://www.maths.qmul.ac.uk/~olof/files/dl/bourgain-APs.pdf>.
- [Szemerédi 1969] E. Szemerédi, “On sets of integers containing no four elements in arithmetic progression”, *Acta Math. Acad. Sci. Hungar.* **20** (1969), 89–104. MR 39 #6861 Zbl 0175.04301
- [Szemerédi 1975] E. Szemerédi, “On sets of integers containing no k elements in arithmetic progression”, *Acta Arith.* **27** (1975), 199–245. MR 51 #5547 Zbl 0303.10056
- [Tao 2008a] T. Tao, “Product set estimates for non-commutative groups”, *Combinatorica* **28**:5 (2008), 547–594. MR 2010b:11017 Zbl 05494691
- [Tao 2008b] T. Tao, *Structure and randomness: pages from year one of a mathematical blog*, American Mathematical Society, Providence, RI, 2008. MR 2010h:00002 Zbl 05380664
- [Tao 2010] T. Tao, “Freiman’s theorem for solvable groups”, *Contrib. Discrete Math.* **5**:2 (2010), 137–184. MR 2012e:05063
- [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
- [Wolf 2009] J. Wolf, “A local inverse theorem in \mathbb{F}_2^n ”, preprint, 2009.
- [Wolf 2010] J. Wolf, “The structure of popular difference sets”, *Israel J. Math.* **179** (2010), 253–278. MR 2011k:05043 Zbl 05823090

Received 4 Nov 2010. Revised 12 Sep 2011. Accepted 9 Oct 2011.

TOM SANDERS: t.sanders@dpmms.cam.ac.uk

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WB, United Kingdom

Analysis & PDE

msp.berkeley.edu/apde

EDITORS

EDITOR-IN-CHIEF

Maciej Zworski
University of California
Berkeley, USA

BOARD OF EDITORS

Michael Aizenman	Princeton University, USA aizenman@math.princeton.edu	Nicolas Burq	Université Paris-Sud 11, France nicolas.burq@math.u-psud.fr
Luis A. Caffarelli	University of Texas, USA caffarel@math.utexas.edu	Sun-Yung Alice Chang	Princeton University, USA chang@math.princeton.edu
Michael Christ	University of California, Berkeley, USA mchrist@math.berkeley.edu	Charles Fefferman	Princeton University, USA cf@math.princeton.edu
Ursula Hamenstaedt	Universität Bonn, Germany ursula@math.uni-bonn.de	Nigel Higson	Pennsylvania State University, USA higson@math.psu.edu
Vaughan Jones	University of California, Berkeley, USA vfr@math.berkeley.edu	Herbert Koch	Universität Bonn, Germany koch@math.uni-bonn.de
Izabella Laba	University of British Columbia, Canada ilaba@math.ubc.ca	Gilles Lebeau	Université de Nice Sophia Antipolis, France lebeau@unice.fr
László Lempert	Purdue University, USA lempert@math.purdue.edu	Richard B. Melrose	Massachusetts Institute of Technology, USA rbm@math.mit.edu
Frank Merle	Université de Cergy-Pontoise, France Frank.Merle@u-cergy.fr	William Minicozzi II	Johns Hopkins University, USA minicozz@math.jhu.edu
Werner Müller	Universität Bonn, Germany mueller@math.uni-bonn.de	Yuval Peres	University of California, Berkeley, USA peres@stat.berkeley.edu
Gilles Pisier	Texas A&M University, and Paris 6 pisier@math.tamu.edu	Tristan Rivière	ETH, Switzerland riviere@math.ethz.ch
Igor Rodnianski	Princeton University, USA irod@math.princeton.edu	Wilhelm Schlag	University of Chicago, USA schlag@math.uchicago.edu
Sylvia Serfaty	New York University, USA serfaty@cims.nyu.edu	Yum-Tong Siu	Harvard University, USA siu@math.harvard.edu
Terence Tao	University of California, Los Angeles, USA tao@math.ucla.edu	Michael E. Taylor	Univ. of North Carolina, Chapel Hill, USA met@math.unc.edu
Gunther Uhlmann	University of Washington, USA gunther@math.washington.edu	András Vasy	Stanford University, USA andras@math.stanford.edu
Dan Virgil Voiculescu	University of California, Berkeley, USA dvv@math.berkeley.edu	Steven Zelditch	Northwestern University, USA zelditch@math.northwestern.edu

PRODUCTION

contact@msp.org

Silvio Levy, Scientific Editor

Sheila Newbery, Senior Production Editor


See inside back cover or msp.berkeley.edu/apde for submission instructions.

The subscription price for 2012 is US \$140/year for the electronic version, and \$240/year for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Analysis & PDE, at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

APDE peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
<http://msp.org/>

A NON-PROFIT CORPORATION

Typeset in L^AT_EX

Copyright ©2012 by Mathematical Sciences Publishers

ANALYSIS & PDE

Volume 5 No. 3 2012

On some microlocal properties of the range of a pseudodifferential operator of principal type	423
JENS WITTSTEN	
Blow-up solutions on a sphere for the 3D quintic NLS in the energy space	475
JUSTIN HOLMER and SVETLANA ROUDENKO	
Sharp geometric upper bounds on resonances for surfaces with hyperbolic ends	513
DAVID BORTHWICK	
A vector field method approach to improved decay for solutions to the wave equation on a slowly rotating Kerr black hole	553
JONATHAN LUK	
On the Bogolyubov–Ruzsa lemma	627
TOM SANDERS	
Real analyticity away from the nucleus of pseudorelativistic Hartree–Fock orbitals	657
ANNA DALL’ACQUA, SØREN FOURNAIS, THOMAS ØSTERGAARD SØRENSEN and EDGARDO STOCKMEYER	
Semiclassical trace formulas and heat expansions	693
YVES COLIN DE VERDIÈRE	



2157-5045(2012)5:3;1-H