

# A STATISTICAL APPROACH TO COVERING LEMMAS

TOM SANDERS

**ABSTRACT.** We discuss a statistical variant of Ruzsa's covering lemma and use it to show that if  $G$  is an Abelian group of bounded exponent and  $A \subset G$  has  $|A + A| \leq K|A|$  then the subgroup generated by  $A$  has size at most  $\exp(O(K \log^2 2K))|A|$ , where the constant in the big- $O$  depends on the exponent of the group only.

## 1. INTRODUCTION

In this note we are concerned with the paper [Ruz99] of Ruzsa in which he proved what is now called the Ruzsa covering lemma, and where he went on to give its prototypical application to the Freĭman-Ruzsa theorem. In this note we shall examine a statistical variant of Ruzsa's covering lemma and show how to use it to improve that same application.

**Theorem 1.1** (Freĭman-Ruzsa theorem for Abelian groups of bounded exponent). *Suppose that  $G$  is an Abelian group of exponent<sup>1</sup>  $r$  and  $\emptyset \neq A \subset G$  has  $|A + A| \leq K|A|$ . Then there is a function  $F$  depending only on  $r$  and  $K$  such that  $\langle A \rangle$ , the group generated by  $A$ , has size at most  $F(r, K)|A|$ .*

We shall take  $F(r, K)$  to be the point-wise smallest function such that the conclusion of this theorem holds.

Ruzsa proved that  $F(r, K) \leq r^{O(K^4)}$  (in [Ruz99]) and noted by considering sets of independent elements that  $F(r, K) \geq r^{\Omega(K)}$ ; he further conjectured that this was close to optimal in particular suggesting that  $F(r, K) \leq r^{O(K)}$ .

We shall return to Ruzsa's conjecture and the cases in which it is known shortly, but first we shall take a brief look at the proof of Theorem 1.1 from [Ruz99]. The argument has two parts: first, note that if  $X \subset G$  has

$$(1.1) \quad A + A \subset X + A,$$

then by induction  $\langle A \rangle \subset \langle X \rangle + A$  and so

$$|\langle A \rangle| \leq |\langle X \rangle||A| \leq r^{|X|}|A|.$$

All we need to do now is find a set  $X$  satisfying (1.1) that is as small as possible – this will be the second part of the argument.

Unfortunately, if  $G$  is finite (but large) and  $A$  is chosen uniformly at random from subsets of  $G$  of size  $|G|/K$  then  $|A + A| \leq K|A|$  and with high probability all  $X$ s satisfying (1.1) have  $|X| = \Omega(K \log |G|)$ .

---

<sup>1</sup>Recall that an Abelian group has **exponent**  $r$  if  $r$  is the minimal natural number such that  $rx = 0_G$  for every  $x \in G$ .

One can eliminate the problem presented by random sets by considering not  $A$ , but instead  $A - A$  *i.e.* finding a set  $X$  such that

$$(1.2) \quad (A - A) + (A - A) \subset X + (A - A).$$

It is now possible to find a set  $X$  whose size depends only on  $K$  – this is what we now call Ruzsa’s Covering Lemma (see [TV06, Lemma 2.14]). Dealing with  $A - A$  comes at a price because the set  $X$  in (1.2) may need to be as large as  $K^3$ ; this is what has (do date) prevented us from establishing Ruzsa’s conjecture by this route.

Instead of working with  $A - A$  we shall continue to work with  $A$ , but (necessarily) relax (1.1) to a statistical statement of ‘almost covering’<sup>2</sup>. This too comes at a price, because the inductive consequence of (1.1) need no longer hold. Nevertheless, for considerably more work, we are able to handle this and prove the following version of Theorem 1.1.

**Theorem 1.2** (Freĭman-Ruzsa theorem for Abelian groups of bounded exponent). *Suppose that  $G$  is an Abelian group of exponent  $r$  and  $\emptyset \neq A \subset G$  has  $|A + A| \leq K|A|$ . Then the group generated by  $A$  has size at most  $\exp(O_r(K \log^2 2K))|A|$ .*

Finally, before proceeding to the proof we should like to make a few remarks about this result.

- (i) The dependence on  $r$  is poor with the proof giving

$$F(r, K) \leq \exp(O(K(\log 2K)((\log 2K)(\log r) + r^2))).$$

This is far from Ruzsa’s conjecture, and means that unless  $r$  is smaller than about  $\log 2K$  there are better results available *e.g.* those of Konyagin in (ii).

- (ii) The improvement on what was already known is very minor in two respects. First, Schoen showed in [Sch11] that

$$F(r, K) \leq \exp(O_r(K^{1+o(1)})),$$

and arguments of Konyagin [Kon11] can be used to show that

$$F(r, K) \leq \exp(O_r(K \log^{3+o(1)} 2K)),$$

so we are only saving a power of  $\log 2K$ , and less than that unless  $r$  is constant.

Secondly, in the case when the exponent is a prime *much* more precise estimates are known. Indeed,  $F(2, K)$  has been completely determined by Zohar [EZ12] using the compression techniques introduced by Green and Tao [GT09], and Zohar’s argument was extended by Lovett and Zohar in [LEZ14] to show that

$$F(r, K) \leq \frac{r^{2K-1}}{2K-1}$$

when  $K \geq 8$  and  $r$  is a prime, which is essentially tight.

- (iii) Although our results are slight, the conjecture itself is nowhere near as significant as the second conjecture mentioned in [Ruz99] – Marton’s conjecture, also called the Polynomial Freĭman-Ruzsa conjecture. This has many applications and the

---

<sup>2</sup>The reader interested primarily in this may skip directly to §2.

arguments of both Konyagin and Schoen mentioned earlier both bear on this much more important conjecture.

## 2. A STATISTICAL COVERING LEMMA

Our starting point, then, is Ruzsa's covering lemma which is proved in [Ruz99] although is not explicitly separated out there and appears as a distinct result in [TV06, Lemma 2.14].

**Lemma 2.1** (Ruzsa's covering lemma). *Suppose that  $|A + B| \leq K|B|$ . Then there is a set  $X \subset B$  of size at most  $K$  such that*

$$A \subset X + (B - B).$$

The classic proof of this is to let  $X$  be a maximal  $B$ -separated subset of  $A$ , meaning let  $X \subset A$  be maximal such that  $(x + B) \cap (x' + B) = \emptyset$  for all  $x \neq x' \in X$ . A short argument then yields the lemma.

The statistical covering lemma we shall use follows below using essentially the same argument; to the extent that it is different the additional ideas can be seen in the Green-Ruzsa covering lemma [GR06, Lemma 2.1].

**Lemma 2.2** (Statistical covering lemma). *Suppose that  $|A + B| \leq K|B|$  and  $\delta \in (0, 1]$  is a parameter. Then there is a set  $X \subset A$  of size at most  $\delta^{-1}(K - 1) + 1$  such that*

$$|(x + B) \cap (X + B)| \geq (1 - \delta)|B| \text{ for all } x \in A.$$

*Proof.* We construct sets  $X_0, \dots, X_k$  iteratively; let  $x_0 \in A$  and  $X_0 := \{x_0\}$ . Suppose we have constructed  $X_i \subset A$ . If there is some  $x_{i+1} \in A$  such that

$$|(x_{i+1} + B) \cap (X_i + B)| < (1 - \delta)|B|$$

then let  $X_{i+1} := X_i \cup \{x_{i+1}\}$ ; if there is no such  $x_{i+1}$  then terminate with  $X := X_i$ . It follows by induction that  $|X_i| \leq i + 1$ . Moreover, if there is a suitable  $x_{i+1}$  then

$$\begin{aligned} |(x_{i+1} + B) \setminus (X_i + B)| &\geq |x_{i+1} + B| - |(x_{i+1} + B) \cap (X_i + B)| \\ &> |B| - (1 - \delta)|B| = \delta|B|. \end{aligned}$$

It follows that

$$\begin{aligned} |X_i + B| &\geq |(X_i + B) \setminus (X_{i-1} + B)| + |(X_{i-1} + B) \setminus (X_{i-2} + B)| \\ &\quad + \dots + |(X_1 + B) \setminus (X_0 + B)| + |X_0 + B| \\ &\geq |(x_i + B) \setminus (X_{i-1} + B)| + |(x_{i-1} + B) \setminus (X_{i-2} + B)| \\ &\quad + \dots + |(x_1 + B) \setminus (X_0 + B)| + |x_0 + B| \\ &> \delta|B|.i + |B|. \end{aligned}$$

On the other hand  $X_i \subset A$  and so  $|X_i + B| \leq K|B|$ , and hence the iteration terminates for some  $i < \delta^{-1}(K - 1)$ , and which point we have

$$|(x + B) \cap (X_i + B)| \geq (1 - \delta)|B| \text{ for all } x \in A.$$

The bound follows since  $X = X_i$  and  $|X_i| \leq i + 1 < \delta^{-1}(K - 1) + 1$  as required.  $\square$

The case  $\delta = 1$  is essentially the argument for Ruzsa's covering lemma since

$$|(x + B) \cap (X + B)| > 0 \text{ if and only if } x \in X + B - B.$$

In this note, however, we are interested in the case of small  $\delta$  and  $A = B$ , and for convenience we shall wrap up the conclusion of the lemma in the case  $A = B$  in a definition. We say that  $A$  is  $(1 - \delta)$ -**covered by**  $X$  if

$$|(x + A) \cap (X + A)| \geq (1 - \delta)|A| \text{ for all } x \in A.$$

Thus  $A$  is 1-covered by  $X$  if and only if  $A + A \subset X + A$ , and the Statistical covering lemma tells us that if  $|A + A| \leq K|A|$  then  $A$  is  $(1 - \delta)$ -covered by a set  $X$  of size  $O(\delta^{-1}K)$ .

To use this definition it will be useful to relate it to convolution. Define the translation operator on  $\ell_p(G)$  for  $p \in [1, \infty]$  in the usual way *viz.*

$$\tau_x : \ell_p(G) \rightarrow \ell_p(G); f \mapsto (y \mapsto f(x + y)).$$

Given two functions  $f, g \in \ell_2(G)$  we then define their **convolution** point-wise by

$$f * g(x) := \langle \tau_{-x}(f), g \rangle_{\ell_2(G)} = \sum_{y+z=x} f(y)g(z) \text{ for all } x \in G.$$

Now, if  $A$  is  $(1 - \delta)$ -covered by  $X$  then it is possible to show (when  $\delta = 0$  this is essentially the induction we discussed in the introduction) that

$$(2.1) \quad \langle \overbrace{1_A * \dots * 1_A}^{(k+1) \text{ times}}, 1_{kX+A} \rangle_{\ell_2(G)} \geq (1 - \delta)^k |A|^{k+1}.$$

This already captures a great deal about  $A$ , in particular that  $A$  has a lot of *very* large Fourier coefficients.

Inequalities of the form (2.1) are not quite enough for us though, and to see what we need re-write the left hand side as a sum over  $A^k$ :

$$\langle \overbrace{1_A * \dots * 1_A}^{(k+1) \text{ times}}, 1_{kX+A} \rangle_{\ell_2(G)} = \sum_{x \in A^k} \langle \tau_{-(x_1 + \dots + x_k)}(1_A), 1_{kX+A} \rangle_{\ell_2(G)}.$$

We shall want lower bounds on sums over sets that are slightly more general than the product set  $A^k$ ; the definition of these is our next task.

**2.3. Generalised product sets.** We think of  $A^k$  as a product of uniform probability spaces, so that it is itself endowed with the uniform probability measure. A set  $\mathcal{A} \subset A^k$  is said to **contain a  $\nu$ -large generalised sub-product of  $A^k$**  for some  $\nu \in (0, 1]^k$  if there are sets  $(\mathcal{A}_i)_{i=0}^k$  such that

- [GP1] (Start and end)  $\mathcal{A}_0 = \{()\}$  and  $\mathcal{A}_k \subset \mathcal{A}$ ;
- [GP2] (Powers) whenever  $1 \leq i \leq k$  we have  $\mathcal{A}_i \subset A^i$ ;
- [GP3] (Sub-martingale) whenever  $1 \leq i \leq k$  we have the point-wise inequality

$$\mathbb{E}_{a_i} 1_{\mathcal{A}_i}(a_1, \dots, a_i) \geq \nu_i 1_{\mathcal{A}_{i-1}}(a_1, \dots, a_{i-1}).$$

In many cases we shall have  $\nu$  a constant vector: if  $\epsilon \in (0, 1]$  then we say that  $\mathcal{A}$  contains an  $\epsilon$ -large generalised sub-product of  $A^k$  if it contains a  $\nu$ -large generalised sub-product of  $A^k$  for  $\nu = \nu(\epsilon) \in (0, 1]^k$  defined by  $\nu_i = \epsilon$  for  $1 \leq i \leq k$ .

To explain the heading for GP3 write  $X_i := 1_{\mathcal{A}_i \times A^{k-i}}$  considered as random variables on  $A^k$ , and  $Y_k, \dots, Y_1$  for the coordinate projection maps  $A^k \rightarrow A; a \mapsto a_i$  considered as random elements. GP3 is simply the statement that  $((\prod_{j=1}^i \nu_j) X_i)_{i=0}^k$  a (finite) submartingale with respect to  $(Y_i)_{i=1}^k$ . That being said we shall make no use of any theory of martingales, and the reader not familiar with this may safely ignore this remark.

**Example 2.4** (Sub-products). If  $A_1, \dots, A_k \subset A$  have size at least  $\nu_1|A|, \dots, \nu_k|A|$  respectively then  $\mathcal{A} := A_1 \times \dots \times A_k$  contains a  $\nu$ -large generalised sub-product of  $A^k$ . To see this define

$$\mathcal{A}_i := A_1 \times \dots \times A_i \text{ for } 0 \leq i \leq k.$$

We certainly have GP1 (with the convention that the empty product is just the set containing the empty tuple) and GP2; it remains to check that

$$\mathbb{E}_{a_i} 1_{\mathcal{A}_i}(a_1, \dots, a_i) = \mathbb{E}_{a_i} 1_{\mathcal{A}_{i-1}}(a_1, \dots, a_{i-1}) 1_{A_i}(a_i) \geq \nu_i 1_{\mathcal{A}_{i-1}}(a_1, \dots, a_{i-1})$$

whenever  $1 \leq i \leq k$  which gives GP3 as required.

There are two properties of sub-products which are useful to us and which extend to generalised sub-products. The first is that it is easy to compute the size of sub-products; we do this for generalised sub-products in Lemma 2.5. The second is that we can apply the inclusion-exclusion principle fibre-wise. To see why this is useful consider the example when  $A_1, \dots, A_k, A'_1, \dots, A'_k \subset A$  all have size at least  $(1 - \eta)|A|$ . Then

$$|(A_1 \times \dots \times A_k) \cap (A'_1 \times \dots \times A'_k)| \geq (1 - 2\eta)^k |A|^k$$

by the inclusion-exclusion principle applied in each fibre. But if  $1/k \ll \eta \ll 1$  this is much better than the bound we get from applying the inclusion-exclusion principle directly, ignoring the product structure, in which case we get

$$|(A_1 \times \dots \times A_k) \cap (A'_1 \times \dots \times A'_k)| \geq (2(1 - \eta)^k - 1) |A|^k.$$

We address this issue in Lemma 2.6.

**Lemma 2.5** (Generalised sub-products, size bound). *Suppose that  $\mathcal{A}$  contains a  $\nu$ -large generalised sub-product of  $A^k$ . Then  $|\mathcal{A}| \geq (\prod_{i=1}^k \nu_i) |A|^k$ .*

*Proof.* Start by noting that for  $1 \leq i \leq k$  we have, by GP3 and linearity of expectation that

$$\mathbb{E}_{a_1, \dots, a_i} 1_{\mathcal{A}_i}(a_1, \dots, a_i) \geq \nu_i \mathbb{E}_{a_1, \dots, a_{i-1}} 1_{\mathcal{A}_{i-1}}(a_1, \dots, a_{i-1}).$$

But then by induction and GP1 we have

$$\mathbb{E} 1_{\mathcal{A}} \geq \mathbb{E} 1_{\mathcal{A}_k} \geq \prod_{i=1}^k \nu_i \mathbb{E} 1_{\mathcal{A}_0} = \prod_{i=1}^k \nu_i,$$

and the result is proved.  $\square$

**Lemma 2.6** (Generalised sub-products, intersections). *Suppose that  $\eta, \eta' \in [0, 1]^k$  are such that  $\eta + \eta' \in [0, 1]^k$  and  $\mathcal{A}$  and  $\mathcal{A}'$  contain  $(1 - \eta)$ -large and  $(1 - \eta')$ -large generalised sub-products of  $A^k$  respectively. Then  $\mathcal{A} \cap \mathcal{A}'$  contains a  $(1 - (\eta + \eta'))$ -large generalised sub-product of  $A^k$ .*

*Proof.* We start by defining  $(\mathcal{A} \cap \mathcal{A}')_i := \mathcal{A}_i \cap \mathcal{A}'_i$  for  $0 \leq i \leq k$  so that GP1 and GP2 are satisfied for  $\mathcal{A} \cap \mathcal{A}'$ . With explanations of the passage from line to line in the following paragraph, it remains to note that

$$\begin{aligned}
\mathbb{E}_{a_i} 1_{(\mathcal{A} \cap \mathcal{A}')_i}(a_1, \dots, a_i) &= \mathbb{E}_{a_i} 1_{\mathcal{A}_i}(a_1, \dots, a_i) 1_{\mathcal{A}'_i}(a_1, \dots, a_i) \\
&\geq 1_{(\mathcal{A} \cap \mathcal{A}')_{i-1}}(a_1, \dots, a_{i-1}) \mathbb{E}_{a_i} 1_{\mathcal{A}_i}(a_1, \dots, a_i) 1_{\mathcal{A}'_i}(a_1, \dots, a_i) \\
&\geq 1_{(\mathcal{A} \cap \mathcal{A}')_{i-1}}(a_1, \dots, a_{i-1}) \\
&\quad \times \mathbb{E}_{a_i} (1_{\mathcal{A}_i}(a_1, \dots, a_i) + 1_{\mathcal{A}'_i}(a_1, \dots, a_i) - 1) \\
&\geq 1_{(\mathcal{A} \cap \mathcal{A}')_{i-1}}(a_1, \dots, a_{i-1}) \\
&\quad \times ((1 - \eta_i) 1_{\mathcal{A}_{i-1}}(a_1, \dots, a_{i-1}) + (1 - \eta'_i) 1_{\mathcal{A}'_{i-1}}(a_1, \dots, a_{i-1}) - 1) \\
&= 1_{(\mathcal{A} \cap \mathcal{A}')_{i-1}}(a_1, \dots, a_{i-1}) ((1 - \eta_i) + (1 - \eta'_i) - 1) \\
&= 1_{(\mathcal{A} \cap \mathcal{A}')_{i-1}}(a_1, \dots, a_{i-1}) (1 - (\eta_i + \eta'_i))
\end{aligned}$$

for  $1 \leq i \leq k$ . The passage from the first to the second line is because  $1_{(\mathcal{A} \cap \mathcal{A}')_{i-1}}$  is Boolean and the two expectations are non-negative; from the second to the third is that  $xy \geq x + y - 1$  whenever  $x, y \in \{0, 1\}$ ; from the third to the fourth uses linearity of expectation and GP3 for  $\mathcal{A}$  and  $\mathcal{A}'$ ; finally the fourth to the fifth uses the fact that  $1_{(\mathcal{A} \cap \mathcal{A}')_{i-1}} 1_{\mathcal{A}_{i-1}} = 1_{(\mathcal{A} \cap \mathcal{A}')_{i-1}}$  by definition and similarly for  $\mathcal{A}'$ . The result is proved.  $\square$

The next lemma captures how the notion of  $(1 - \delta)$ -covering (from the start of this section) is related to generalised sub-products. If  $A$  is 1-covered by a set  $X$  containing  $0_G$  then a short induction tells us that for any  $x \in A$  we have

$$\{a \in A^k : x + \sum_i a_i \in kX + A\} = A^k;$$

the set has a product structure. If it is almost 1-covered then it has a generalised sub-product structure. Although long-winded the proof below is straight-forward.

**Lemma 2.7.** *Suppose that  $A$  is  $(1 - \delta)$ -covered by  $X \ni 0_G$  for some  $\delta \in [0, 1]$ . Then for any  $x \in A$ ,  $k \in \mathbb{N}$  and  $S \subset [k]$ , the set*

$$\mathcal{A}^S := \{a \in A^k : x + \sum_{s \in S} a_s \in \overbrace{X + \dots + X}^{|S| \text{ times}} + A\}$$

*contains a  $\nu(S)$ -large generalised sub-product where  $\nu(S)_i = 1 - \delta 1_S(i)$ .*

*Proof.* For each  $S$  we shall construct sets  $(\mathcal{A}_i^S)_{i=0}^k$  satisfying GP1 (for  $\mathcal{A}^S$ ), GP2, and GP3 with  $\nu(S)$ . When  $S = \emptyset$  we have

$$\{a \in A^k : x + \sum_{s \in S} a_s \in \overbrace{X + \cdots + X}^{|S| \text{ times}} + A\} = \{a \in A^k : x \in A\} = A^k$$

since  $0_G \in X$  and  $x \in A$ , and so we have suitable sets  $(\mathcal{A}_i^S)_{i=0}^k$  from Example 2.4, namely  $\mathcal{A}_i^S = A^i$ .

Now, suppose that  $S$  is non-empty, that the largest element of  $S$  is  $j$ , and that we have constructed suitable sets  $(\mathcal{A}_i^{S'})_{i=0}^k$  for  $S' := S \setminus \{j\}$ . We shall construct the sets  $(\mathcal{A}_i^S)_{i=0}^k$  in three stages depending on the value of  $i$ , verifying GP2 and GP3 as we go, and GP1 at the end.

(i) ( $i < j$ ) Put

$$\mathcal{A}_i^S := \mathcal{A}_i^{S'} \text{ whenever } i < j$$

so that GP2 and GP3 are satisfied whenever  $i < j$  since  $\nu(S)_i = \nu(S')_i$  in that range.

(ii) ( $i = j$ ) Put

$$\mathcal{A}_j^S := \{(a_1, \dots, a_{j-1}, a) \in \mathcal{A}_{j-1}^S \times A : x + \sum_{s \in S'} a_s + a \in \overbrace{X + \cdots + X}^{|S| \text{ times}} + A\}$$

so that GP2 holds. It remains to verify GP3. If  $(a_1, \dots, a_{j-1}) \in \mathcal{A}_{j-1}^S$  then

$$\mathbb{E}_{a_j, \dots, a_k} 1_{\mathcal{A}_k^{S'}}(a_1, \dots, a_k) \geq \nu_k(S') \dots \nu_j(S') 1_{\mathcal{A}_{j-1}^{S'}}(a_1, \dots, a_{j-1}) = 1$$

by induction and since  $\nu_i(S') = 1$  for all  $j \leq i \leq k$  as  $j$  was the largest element of  $S$ . It follows that there is some  $a_j, \dots, a_k$  such that  $(a_1, \dots, a_k) \in \mathcal{A}_k^{S'} \subset \mathcal{A}_k^S$ . From the definition of  $\mathcal{A}^{S'}$  this means that

$$x + \sum_{s \in S'} a_s \in \overbrace{X + \cdots + X}^{|S'| \text{ times}} + A,$$

which we note does not depend on the particular choice of  $a_j, \dots, a_k$  since the largest element of  $S'$  is less than  $j$ . We conclude that there is some  $U(a_1, \dots, a_{j-1}) \in X + \cdots + X$  (where the sum is  $|S'|$ -fold) such that

$$-U(a_1, \dots, a_{j-1}) + x + \sum_{s \in S'} a_s \in A.$$

Since  $A$  is  $(1 - \delta)$ -covered by  $X$  there are at least  $(1 - \delta)|A|$  elements  $a \in A$  such that

$$-U(a_1, \dots, a_{j-1}) + x + \sum_{s \in S'} a_s + a \in X + A,$$

and so at least  $(1 - \delta)|A|$  elements  $a \in A$  such that

$$x + \sum_{s \in S'} a_s + a \in \overbrace{X + \cdots + X}^{|S| \text{ times}} + A;$$

written another way

$$\mathbb{E}_{a_j} 1_{\mathcal{A}_j^S}(a_1, \dots, a_j) \geq (1 - \delta) = \nu(S)_j$$

and so GP3 is satisfied.

(iii) ( $i > j$ ) Put

$$\mathcal{A}_i^S := \mathcal{A}_j^S \times A^{k-j}$$

so that GP2 is satisfied. It remains to note that

$$\mathbb{E}_{a_i} 1_{\mathcal{A}_i^S}(a_1, \dots, a_i) = \mathbb{E}_{a_i} 1_{\mathcal{A}_{i-1}^S \times A}(a_1, \dots, a_i) = 1_{\mathcal{A}_{i-1}^S}(a_1, \dots, a_{i-1}),$$

and GP3 is satisfied.

Finally, note that  $\mathcal{A}_0^S = \{()\}$  and

$$\begin{aligned} \mathcal{A}^S &= \{a \in A^k : x + \sum_{s \in S} a_s \in \overbrace{X + \cdots + X}^{|S| \text{ times}} + A\} \\ &= \{a \in A^j : x + \sum_{s \in S} a_s \in \overbrace{X + \cdots + X}^{|S| \text{ times}} + A\} \times A^{k-j} \\ &\supset \{(a_1, \dots, a_{j-1}, a) \in \mathcal{A}_{j-1}^S \times A : x + \sum_{s \in S} a_s \in \overbrace{X + \cdots + X}^{|S| \text{ times}} + A\} \times A^{k-j} \\ &= \mathcal{A}_j^S \times A^{k-j} = \mathcal{A}_k^S. \end{aligned}$$

GP1 is proved and we have the result by induction on the largest element of  $S$ .  $\square$

The final result of this section packages up the previous lemma in a corollary that captures the aspects of (2.1) that we should like. It may be worth saying that it is useful for similar reason to [Tao10, Proposition C.2], although the link is a little obscure.

Before we state the corollary we record one final piece of notation, the precise reason for which will become clear in §3. Given a finite subset  $S$  of  $G$  we write  $\mu_S$  for the uniform probability measure supported on  $S$ , and for each  $a \in G^r$  we write

$$\mu_a := 2^{-r} *_{i=1}^r (\mu_{\{0_G\}} + \mu_{\{a_i\}}).$$

This behaves like an approximation to the uniform measure on the group generated by  $a_1, \dots, a_r$ . Indeed, if  $G$  has exponent 2 then  $\mu_a = \mu_{\langle a_1, \dots, a_r \rangle}$ .



**Corollary 2.8.** *Suppose that  $\delta, \eta \in [0, 1/2)$ , that  $A$  is  $(1 - \delta)$ -covered by  $X \ni 0_G$ ,  $k \in \mathbb{N}$ , and that  $\mathcal{A} \subset A^k$  contains a  $(1 - \eta)$ -large generalised sub-product. Then*

$$\sum_{a \in \mathcal{A}} \|1_A * \mu_a\|_{\ell_2(G)}^2 \geq \frac{(1 - \eta)^{2k} (1 - \delta)^{2k}}{|kX|} |A|^{k+1}$$

*Proof.* We apply Lemma 2.7 to get that for any  $x \in A$  and  $S \subset [k]$  the set  $\mathcal{A}^S$  contains a  $(1 - \delta)$ -large generalised product. By Lemma 2.6 it follows that  $\mathcal{A}^S \cap \mathcal{A}$  contains an  $\nu$ -large generalised product where  $\nu(S)_i = 1 - \eta - \delta 1_S(i)$ . Lemma 2.5 then tells us that

$$\begin{aligned} \sum_{a \in \mathcal{A}} 1_{kX+A}(x + \sum_{s \in S} a_s) &= |\{a \in \mathcal{A} : x + \sum_{s \in S} a_s \in kX + A\}| \\ &= |\mathcal{A}^S \cap \mathcal{A}| \\ &\geq \prod_{i=1}^k (1 - \eta - \delta 1_S(i)) |A|^k \\ &\geq (1 - \eta)^k (1 - 2\delta)^{|S|} |A|^k, \end{aligned}$$

since  $\eta, \delta < 1/2$ . Note that

$$1_{kX+A}(x + \sum_{s \in S} a_s) = \langle \mu_{\{x\}} * \mu_{\{a_s\}}, 1_{kX+A} \rangle_{\ell_2(G)}$$

Averaging over  $S \subset [k]$  we have that

$$\frac{1}{2^k} \sum_{S \subset [k]} 1_{kX+A}(x + \sum_{s \in S} a_s) = \langle \mu_{\{x\}} * \mu_a, 1_{kX+A} \rangle_{\ell_2(G)},$$

and hence

$$\begin{aligned} \sum_{a \in \mathcal{A}} \langle \mu_{\{x\}} * \mu_a, 1_{kX+A} \rangle_{\ell_2(G)} &\geq \frac{1}{2^k} \sum_{S \subset [k]} (1 - \eta)^k (1 - 2\delta)^{|S|} |A|^k \\ &= \frac{1}{2^k} (1 - \eta)^k |A|^k \sum_{S \subset [k]} (1 - 2\delta)^{|S|} \\ &= \frac{1}{2^k} (1 - \eta)^k |A|^k (1 + (1 - 2\delta))^k = (1 - \eta)^k (1 - \delta)^k |A|^k. \end{aligned}$$

Summing over  $x \in A$  then gives

$$\sum_{a \in \mathcal{A}} \langle 1_A * \mu_a, 1_{kX+A} \rangle_{\ell_2(G)} \geq (1 - \eta)^k (1 - \delta)^k |A|^{k+1}.$$

Finally, apply the Cauchy-Schwarz inequality to the inner product, and then to the outer sum to get that

$$\begin{aligned}
(1 - \eta)^k (1 - \delta)^k |A|^{k+1} &\leq \sum_{a \in \mathcal{A}} \langle 1_A * \mu_a, 1_{kX+A} \rangle_{\ell_2(G)} \\
&\leq \sum_{a \in \mathcal{A}} \|1_A * \mu_a\|_{\ell_2(G)} \|1_{kX+A}\|_{\ell_2(G)} \\
&= |kX + A|^{1/2} \sum_{a \in \mathcal{A}} \|1_A * \mu_a\|_{\ell_2(G)} \\
&\leq |kX + A|^{1/2} |\mathcal{A}|^{1/2} \left( \sum_{a \in \mathcal{A}} \|1_A * \mu_a\|_{\ell_2(G)}^2 \right)^{1/2} \\
&\leq |kX|^{1/2} |A|^{(k+1)/2} \left( \sum_{a \in \mathcal{A}} \|1_A * \mu_a\|_{\ell_2(G)}^2 \right)^{1/2}.
\end{aligned}$$

The result follows on rearrangement.  $\square$

### 3. CHANG'S LEMMA

In this section we capture an idea of Chang from [Cha02, §2] (recorded as Chang's covering lemma in [TV06, Lemma 5.31]), although the connection may not be immediately obvious. The lemma will be used in the case  $h = 1_A$  and combined with Corollary 2.8 from the previous section.

**Lemma 3.1.** *Suppose that  $h \in \ell_2(G)$  and,  $\kappa \in (0, 1]$ ,  $\eta \in [0, 1)$  and  $k \in \mathbb{N}$  are parameters. Then either*

(i) *there is some  $0 \leq l < k$  and some  $a \in A^l$  such that the set of  $x \in A$  having*

$$\|h * \mu_a - \tau_x(h * \mu_a)\|_{\ell_2(G)}^2 < \kappa \|h * \mu_a\|_{\ell_2(G)}^2$$

*has size at least  $\eta|A|$ ;*

(ii) *or there is a  $(1 - \eta)$ -large generalised sub-product of  $A^k$ ,  $\mathcal{A}$ , such that*

$$\|h * \mu_a\|_{\ell_2(G)}^2 \leq (1 - \kappa/4)^k \|h\|_{\ell_2(G)}^2$$

*for all  $a \in \mathcal{A}$ .*

*Proof.* Put  $\mathcal{A}_0 := \{()\}$  and

$$\mathcal{A}_i := \{(a_1, \dots, a_i) \in \mathcal{A}_{i-1} \times A : \|h * \mu_{a_1, \dots, a_i}\|_{\ell_2(G)}^2 \leq (1 - \kappa/4) \|h * \mu_{a_1, \dots, a_{i-1}}\|_{\ell_2(G)}^2\}$$

for  $1 \leq i \leq k$  so that GP2 holds. Now, suppose  $1 \leq i \leq k$  and  $a \in \mathcal{A}_{i-1}$ . If the set of  $x \in A$  such that

$$\|h * \mu_a - \tau_x(h * \mu_a)\|_{\ell_2(G)}^2 < \kappa \|h * \mu_a\|_{\ell_2(G)}^2$$

has size at least  $\eta|A|$  then we terminate in the first case of the lemma with  $l = i - 1$ . Thus we may assume that there are at least  $(1 - \eta)|A|$  elements  $x \in A$  such that

$$\|h * \mu_a - \tau_x(h * \mu_a)\|_{\ell_2(G)}^2 \geq \kappa \|h * \mu_a\|_{\ell_2(G)}^2.$$

But then

$$\begin{aligned}
4\|h * \mu_{(a_1, \dots, a_{i-1}, x)}\|_{\ell_2(G)}^2 &= \|h * \mu_a + \tau_x(h * \mu_a)\|_{\ell_2(G)}^2 \\
&= 4\|h * \mu_a\|_{\ell_2(G)}^2 - \|h * \mu_a - \tau_x(h * \mu_a)\|_{\ell_2(G)}^2 \\
&\leq (4 - \kappa)\|h * \mu_a\|_{\ell_2(G)}^2,
\end{aligned}$$

and so  $(a_1, \dots, a_{i-1}, x) \in \mathcal{A}_i$ . It follows that

$$\mathbb{E}_{a_i} 1_{\mathcal{A}_i}(a_1, \dots, a_i) \geq (1 - \eta) = (1 - \eta) 1_{\mathcal{A}_{i-1}}(a_1, \dots, a_{i-1})$$

and we have GP3. Setting  $\mathcal{A} = \mathcal{A}_k$  we have GP1 for  $\mathcal{A}$ , and so  $\mathcal{A}$  is a  $(1 - \eta)$ -large generalised sub-product. Furthermore, if  $a \in \mathcal{A}$  then

$$\|h * \mu_{a_1, \dots, a_k}\|_{\ell_2(G)}^2 \leq (1 - \kappa/4)\|h * \mu_{a_1, \dots, a_{k-1}}\|_{\ell_2(G)}^2 \leq \dots \leq (1 - \kappa/4)^k \|h\|_{\ell_2(G)}^2$$

by induction and construction of the sets  $\mathcal{A}_i$ . We are then in the second case of the lemma and the result is proved.  $\square$

It may be worth saying that it is because this lemma outputs a generalised sub-product that we had to extend Corollary 2.8 to cover generalised sub-products; in other words, this lemma is the reason for the presence of generalised sub-products in this note.

#### 4. FOURIER ANALYSIS AND ALMOST-INVARIANT FUNCTIONS

Fourier analysis is inextricably linked with Freiman's theorem and while we have not needed it so far, the introduction of convolution earlier was a clear foreshadowing of things to come. We take a moment to record some basic definitions, but the reader may wish to refer to [TV06, §4] or [Rud90] for a more extensive discussion.

We shall regard  $G$  as a discrete group and write  $\hat{G}$  for the compact Abelian group of characters on  $G$ . Given  $f \in \ell_1(G)$ , the *Fourier transform* of  $f$  is defined to be the function

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

The group  $\hat{G}$  is naturally a compact group endowed with Haar probability measure which we shall denote  $d\gamma$ . While it may seem like there is some analysis here, we are only interested in finite subsets of groups with finite exponent and so we can freely take  $G$  to be finite and ignore any of this.

Following Green and Ruzsa [GR07] we shall analyse the subgroup  $\langle A \rangle$  in our problem by considering the annihilator of the large spectrum of  $A$ . To make sense of this we need a couple of definitions: given a set of characters  $\Gamma$ , we define the **annihilator** of  $\Gamma$  to be

$$\Gamma^\perp := \{x \in G : \gamma(x) = 1 \text{ for all } \gamma \in \Gamma\}.$$

Given  $f \in \ell_1(G)$  and  $\epsilon \in (0, 1]$  we define the  **$\epsilon$ -large spectrum** of  $f$  to be

$$\text{Spec}_\epsilon(f) := \{\gamma \in \hat{G} : |\hat{f}(\gamma)| \geq \epsilon \|f\|_{\ell_1(G)}\}.$$

The next lemma gives us a way to contain our set in the annihilator of a suitable large spectrum, and it is here that we make essential use of the fact that  $G$  has bounded exponent.

The first part of the proof is basically an argument of Green and Konyagin [GK09, Lemma 3.6].

**Lemma 4.1.** *Suppose that  $G$  is an Abelian group of exponent  $r$ ,  $g \in \ell_1(G)$  is not identically 0, and  $\epsilon \in (0, 1]$  is a parameter such that*

$$\|g - \tau_a(g)\|_{\ell_1(G)} \leq \epsilon \|g\|_{\ell_1(G)} \text{ for all } a \in A.$$

*Then  $A \subset \text{Spec}_{r\epsilon}(g)^\perp$ .*

*Proof.* Suppose that  $\gamma \in \text{Spec}_{r\epsilon}(g)$  and  $a \in A$ . Then

$$\begin{aligned} r\epsilon \|g\|_{\ell_1(G)} |1 - \gamma(a)| &\leq |1 - \gamma(a)| |\widehat{g}(\gamma)| \\ &= |\widehat{g}(\gamma) - \gamma(a) \widehat{g}(\gamma)| \\ &= |(g - \tau_a(g))^\wedge(\gamma)| \\ &\leq \|g - \tau_a(g)\|_{\ell_1(G)} \leq \epsilon \|g\|_{\ell_1(G)}, \end{aligned}$$

by the Hausdorff-Young inequality. Dividing by  $\epsilon \|g\|_{\ell_1(G)}$  (possible since  $g \neq 0$  and  $\epsilon > 0$ ) and rearranging we get that  $|1 - \gamma(a)| \leq 1/r$ . Of course since  $G$  is a group of exponent  $r$  it follows that  $\gamma(a)$  is an  $r$ th root of unity and hence if it is not equal to 1 then

$$|1 - \gamma(a)| \geq |1 - \exp(2\pi i/r)| \geq |\sin(2\pi/r)| \geq \frac{2}{\pi} \cdot \frac{2\pi}{r} = \frac{4}{r}.$$

It follows that  $\gamma(a) = 1$  and the result is proved.  $\square$

With the above lemma in hand we need a supply of suitable functions  $g$ . The hypothesis on  $g$  look somewhat like those in the first case of Lemma 3.1 so it should not be too surprising that we shall be combining the work of §2 and §3 to act as such a supply. The next proposition does just this and is the driving result of the whole note.

**Proposition 4.2.** *Suppose that  $G$  is an Abelian group of exponent  $r$ ,  $A \subset G$  has  $|A + A| \leq K|A|$ , and  $\epsilon \in (0, 1]$  is a parameter. Then there is a subgroup  $V$  generated by at most  $O(K\epsilon^{-2} \min\{\log r, \log 2\epsilon^{-1}\})$  elements, and a non-negative function  $f$  supported on  $A + V$  such that*

$$\|f - \tau_x(f)\|_{\ell_1(G)} \leq \epsilon \|f\|_{\ell_1(G)}$$

*for at least  $\Omega(\epsilon|A|)$  elements  $x \in A$ .*

*Proof.* Let  $\delta$  be a parameter to be chosen later (it will just be a constant multiple of  $\epsilon$ ). Apply the statistical covering lemma (Lemma 2.2) to the set  $A$  with parameter  $\delta$  to get a set  $Y$  of size at most  $\delta^{-1}K$  such that  $A$  is  $(1 - \delta)$ -covered by  $Y$ . Let  $X := Y \cup \{0_G\}$  so that  $A$  is  $(1 - \delta)$ -covered by  $X$  and  $|X| \leq \delta^{-1}K + 1$ .

Let  $k \geq \delta^{-1}K$  be a natural number to be optimised later and apply Lemma 3.1 with  $h = 1_A$ ,  $\kappa = \epsilon/4$  and  $\delta$  to get that either there is some  $0 \leq l < k$  and some  $a \in A^l$  such that the set of  $x \in A$  having

$$\|1_A * \mu_a - \tau_a(1_A * \mu_a)\|_{\ell_2(G)}^2 \leq \frac{\epsilon}{4} \|1_A * \mu_a\|_{\ell_2(G)}^2$$

has size at least  $\delta|A|$ , or else there is a  $(1 - \delta)$ -large generalised sub-product  $\mathcal{A}$  of  $A^k$  such that

$$(4.1) \quad \|1_A * \mu_a\|_{\ell_2(G)}^2 \leq (1 - \epsilon/16)^k |A| \text{ for all } a \in \mathcal{A}.$$

Now apply Corollary 2.8 with the set  $A$  ( $(1 - \delta)$ -covered by  $X$ ) to get that

$$(4.2) \quad \sum_{a \in \mathcal{A}} \|1_A * \mu_a\|_{\ell_2(G)}^2 \geq |kX|^{-1} (1 - \delta)^{4k} |A|^{k+1}.$$

Since  $G$  is an Abelian group of exponent  $r$  we have that  $|kX| \leq r^{|X|}$ . On the other hand if  $k$  is small compared with  $r$  then we have a better upper bound, from the fact that  $G$  is commutative, namely

$$\begin{aligned} |kX| &\leq \binom{k + |X| - 1}{|X| - 1} \leq \exp(O(|X|(1 + \log((k + |X|)/|X|)))) \\ &\leq \exp(O((K/\delta) \log 2(k\delta/K))), \end{aligned}$$

where we have used the fact that  $k \geq \delta^{-1}K \geq |X| - 1$  in the second inequality. It follows that

$$|kX|^{1/k} \leq \exp(O(K/\delta k) \min\{\log r, \log 2(k\delta/K)\}).$$

Combining (4.1) and (4.2), dividing by  $|A|^{k+1}$ , and taking  $k$ -th roots we conclude that

$$\exp(O(K/\delta k) \min\{\log r, \log 2(k\delta/K)\})(1 - \epsilon/16) \geq (1 - \delta)^4.$$

We can choose  $k = O(K\delta^{-2} \min\{\log r, \log 2\delta^{-1}\})$  such that the first term on the left is at most  $1 + \delta$ , and it follows that we can then take  $\delta = \Omega(\epsilon)$  to get a contradiction. This contradiction means that we must have been in the first case of Lemma 3.1 at some point *i.e.* there is some

$$l < k = O(K\delta^{-2} \min\{\log r, \log 2\delta^{-1}\}) = O(K\epsilon^{-2} \min\{\log r, \log 2\epsilon^{-1}\})$$

and some  $a \in A^l$  such that

$$\|1_A * \mu_a - \tau_x(1_A * \mu_a)\|_{\ell_2(G)}^2 \leq \frac{\epsilon}{4} \|1_A * \mu_{a'}\|_{\ell_2(G)}^2$$

for  $\Omega(\epsilon|A|)$  elements  $x \in A$ . We put  $V := \langle a_1, \dots, a_l \rangle$ , and see that  $V$  is generated by the claimed number of elements, and  $f := (1_A * \mu_a)^2$  so that  $f$  is supported on  $A + V$ . It remains to note that by the triangle inequality and the fact that  $\tau_x$  is an isometry we have

$$\begin{aligned} \|f - \tau_x(f)\|_{\ell_1(G)} &\leq |\langle 1_A * \mu_a, 1_A * \mu_a - \tau_x(1_A * \mu_a) \rangle| \\ &\quad + |\langle \tau_x(1_A * \mu_a), 1_A * \mu_a - \tau_x(1_A * \mu_a) \rangle| \\ &= 2\|1_A * \mu_a - \tau_x(1_A * \mu_a)\|_{\ell_2(G)}^2 \\ &\quad + 2\|1_A * \mu_a - \tau_{-x}(1_A * \mu_a)\|_{\ell_2(G)}^2 \\ &\leq 4 \cdot \frac{\epsilon}{4} \|1_A * \mu_a\|_{\ell_2(G)}^2 = \epsilon \|f\|_{\ell_1(G)}. \end{aligned}$$

The result is proved.  $\square$

Although the proposition makes use of the fact that  $G$  has bounded exponent this is not really essential and it can be recast as a useful statement in more general settings too.

Finally, while the proposition does provide functions satisfying the hypothesis of Lemma 4.1, they are only useful if we can also show that the annihilator of the large spectrum of these functions is small; the next lemma does this. Its basis is an idea introduced to Freiman-type problems by Green and Ruzsa in [GR07] in a way closely related to work of Schoen [Sch03].

**Lemma 4.3.** *Suppose that  $G$  is an Abelian group,  $\emptyset \neq A \subset G$  has  $|A + A| \leq K|A|$ ,  $\epsilon \in (0, 1/2]$  is a parameter, and  $0 \neq h \in \ell_1(G)$  is a non-negative function supported on  $A$  such that*

$$\|h - \tau_a(h)\|_{\ell_1(G)} \leq \epsilon \|h\|_{\ell_1(G)}$$

*for all  $a \in A'$ . Then for any non-negative  $0 \neq g \in \ell_1(G)$  supported on  $A'$  we have*

$$|\text{Spec}_{1/4K^{2\epsilon}}(g)^\perp| \leq 4K|A|.$$

*Proof.* Let  $k := \lfloor \epsilon^{-1}/2 \rfloor$  and note that by the triangle inequality and the fact that  $\tau_x$  is an isometry we have

$$\|h - \tau_{-x}(h)\|_{\ell_1(G)} = \|h - \tau_x(h)\|_{\ell_1(G)} \leq \frac{1}{2} \|h\|_{\ell_1(G)} \text{ for all } x \in kA'.$$

Since  $h$  is non-negative and the support of  $h$  is contained in  $A$  we have that

$$\begin{aligned} \|h\|_{\ell_1(G)}|A| &= \langle h, 1_{A+A} * 1_{-A} \rangle_{\ell_2(G)} \\ &= \langle \tau_{-x}(h), 1_{A+A} * 1_{-A} \rangle_{\ell_2(G)} + \langle (h - \tau_{-x}(h)), 1_{A+A} * 1_{-A} \rangle_{\ell_2(G)} \\ &\leq \langle \tau_{-x}(h), 1_{A+A} * 1_{-A} \rangle_{\ell_2(G)} + \frac{1}{2} \|h\|_{\ell_1(G)}|A| \end{aligned}$$

for any  $x \in kA'$ . Summing against  $\overbrace{g * \cdots * g}^{k \text{ times}}(x)$  (which has support on  $kA'$  and is non-negative), we get that

$$(4.3) \quad \langle h * \overbrace{g * \cdots * g}^{k \text{ times}}, 1_{A+A} * 1_{-A} \rangle_{\ell_2(G)} \geq \frac{1}{2} \|h\|_{\ell_1(G)}|A| \|g\|_{\ell_1(G)}^k.$$

We can then apply Plancherel's theorem to see that

$$\int \widehat{h}(\gamma) \widehat{g}(\gamma)^k \overline{\widehat{1_{A+A}}(\gamma)} \widehat{1_A}(\gamma) d\gamma \geq \frac{1}{2} \|h\|_{\ell_1(G)}|A| \|g\|_{\ell_1(G)}^k.$$

Write  $S := \text{Spec}_{1/4K^{2\epsilon}}(g)$  and, with explanation of the passage between the lines in the following paragraph, we then have

$$\begin{aligned}
\int_{\widehat{G} \setminus S} |\widehat{h}(\gamma)| |\widehat{g}(\gamma)|^k |\widehat{1_{A+A}}(\gamma)| |\widehat{1_A}(\gamma)| d\gamma &\leq \left( \frac{\|g\|_{\ell_1(G)}}{4K^{2\epsilon}} \right)^k \int |\widehat{h}(\gamma)| |\widehat{1_{A+A}}(\gamma)| |\widehat{1_A}(\gamma)| d\gamma \\
&\leq \frac{\|g\|_{\ell_1(G)}^k}{4^k K^{2\epsilon k}} \|h\|_{\ell_1(G)} \int |\widehat{1_{A+A}}(\gamma)| |\widehat{1_A}(\gamma)| d\gamma \\
&\leq \frac{\|g\|_{\ell_1(G)}^k}{4^k K^{2\epsilon k}} \|h\|_{\ell_1(G)} \\
&\quad \times \left( \int |\widehat{1_{A+A}}(\gamma)|^2 d\gamma \right)^{1/2} \left( \int |\widehat{1_A}(\gamma)|^2 d\gamma \right)^{1/2} \\
&= \frac{\|g\|_{\ell_1(G)}^k}{4^k K^{2\epsilon k}} \|h\|_{\ell_1(G)} \sqrt{|A+A||A|} \\
&\leq \frac{1}{4} \|g\|_{\ell_1(G)}^k \|h\|_{\ell_1(G)} |A| K^{1/2-2\epsilon k} \\
(4.4) \quad &\leq \frac{1}{4} \|h\|_{\ell_1(G)} |A| \|g\|_{\ell_1(G)}^k.
\end{aligned}$$

The first inequality is the definition of  $S$ ; the second inequality is the Hausdorff-Young inequality applied to  $h$ ; the third inequality is the Cauchy-Schwarz inequality; the following equality is Parseval's theorem; and we then finish the chain by noting that  $4^{-k} \leq 4^{-1}$ ,  $|A+A| \leq K|A|$ , and  $1/2 - 2\epsilon k \leq 0$ .

It remains to note, again with explanations afterwards, that

$$\begin{aligned}
\|h\|_{\ell_1(G)} \|g\|_{\ell_1(G)}^k \int_S |\widehat{1_{A+A}}(\gamma)| |\widehat{1_A}(\gamma)| d\gamma &\geq \int_S |\widehat{h}(\gamma)| |\widehat{g}(\gamma)|^k \overline{|\widehat{1_{A+A}}(\gamma)|} |\widehat{1_A}(\gamma)| d\gamma \\
&\geq \left| \int_S \widehat{h}(\gamma) \widehat{g}(\gamma)^k \overline{|\widehat{1_{A+A}}(\gamma)|} \widehat{1_A}(\gamma) d\gamma \right| \\
&\geq \left| \int_S \widehat{h}(\gamma) \widehat{g}(\gamma)^k \overline{|\widehat{1_{A+A}}(\gamma)|} \widehat{1_A}(\gamma) d\gamma \right| \\
&\quad - \int_{\widehat{G} \setminus S} |\widehat{h}(\gamma)| |\widehat{g}(\gamma)|^k |\widehat{1_{A+A}}(\gamma)| |\widehat{1_A}(\gamma)| d\gamma \\
&\geq \frac{1}{2} \|h\|_{\ell_1(G)} |A| \|g\|_{\ell_1(G)}^k - \frac{1}{4} \|h\|_{\ell_1(G)} |A| \|g\|_{\ell_1(G)}^k \\
&= \frac{1}{4} \|h\|_{\ell_1(G)} |A| \|g\|_{\ell_1(G)}^k.
\end{aligned}$$

The first inequality is the Hausdorff-Young inequality in  $h$  and  $g$ ; the second is the integral triangle inequality; the third is the triangle inequality; and the final inequality then inserts (4.3) and (4.4).

Dividing out by  $\|h\|_{\ell_1(G)}$  and  $\|g\|_{\ell_1(G)}^k$  (both of which are non-zero since  $g$  and  $h$  are non-trivial) we see that

$$\int_S |\widehat{1_{A+A}}(\gamma)| |\widehat{1_A}(\gamma)| d\gamma \geq \frac{1}{4} |A|.$$

Let  $V$  be any finite subgroup of  $\text{Spec}_{1/4K^{2\epsilon}}(g)^\perp$  and note that  $\widehat{1_V}(\gamma) = |V|$  for all  $\gamma \in S$ . It follows that

$$\begin{aligned} \frac{1}{4} |A| |V|^2 &\leq \int_S |\widehat{1_{A+A}}(\gamma)| |\widehat{1_A}(\gamma)| |\widehat{1_V}(\gamma)|^2 d\gamma \\ &\leq \int_S |\widehat{1_{A+A}}(\gamma)| |\widehat{1_A}(\gamma)| |\widehat{1_V}(\gamma)|^2 d\gamma \leq |A| |A + A| |V| \end{aligned}$$

by the Hausdorff-Young inequality in  $1_{A+A}$  and  $1_A$ , and Parseval's theorem in  $1_V$ . We conclude that  $|V| \leq 4K|A|$ . It follows that  $\text{Spec}_{1/4K^\epsilon}(g)^\perp$  is finite and hence satisfies the required bound.  $\square$

## 5. PROOF OF THE MAIN THEOREM

Before proving our main result we need to record one more ingredient. In [Pet12] Petridis found a fantastic new proof of Plünnecke's inequality [Plü69] (see also [Ruz89]) which proceeded via the following lemma.

**Lemma 5.1** (Petridis' lemma [Pet12, Proposition 2.1]). *Suppose that  $A, B \subset G$  are finite sets with  $|A + B| \leq K|B|$ , and  $Z \subset B$  is non-empty with  $|A + Z|/|Z|$  minimal. Then*

$$|A + Z + C| \leq K|Z + C| \text{ for all finite } C \subset G.$$

We shall not discuss the proof of this here, although it inspired the proof of Lemma 2.2. Indeed, the genesis of this note centred around trying to use Petridis' arguments to give a proof of Ruzsa's conjecture. That approach failed, at least in part because Petridis' arguments actually work just as well for non-Abelian groups as they do for Abelian groups, and Ruzsa's conjecture is essentially Abelian.

Finally, then, we turn to our proof.

*Proof of Theorem 1.2.* Let  $Z \subset A$  be such that  $|A + Z|/|Z|$  is minimal. In particular,  $|A + Z| \leq K|Z|$  and  $|Z + Z| \leq K|Z|$ . We apply Proposition 4.2 to  $Z$  with a parameter  $\epsilon$  (to be optimised later, ending up being  $\Omega(1/\log K)$ ) to get a subgroup  $V$  generated by at most  $O(K\epsilon^{-2} \min\{\log r, \log 2\epsilon^{-1}\})$  elements and a non-negative function  $f \not\equiv 0$  with support on  $Z + V$  such that

$$\|f - \tau_z(f)\|_{\ell_1(G)} \leq \epsilon \|f\|_{\ell_1(G)}$$

for at least  $\Omega(\epsilon|Z|)$  elements  $z \in Z$ ; call the set of such  $z$ s  $Z'$ . Thus

$$|Z' + Z'| \leq |Z + Z| \leq K|Z| = O(\epsilon^{-1}K|Z'|).$$

Now apply Proposition 4.2 again, but this time to the set  $Z'$  with a parameter  $\eta$  (again, to be optimised later, but this time it will end up being  $\Omega(1/r)$ ). This gives us a subgroup  $V'$  generated by at most  $O(K\epsilon^{-1}\eta^{-2} \min\{\log r, \log 2\eta^{-1}\})$  elements and a non-negative function



$g \not\equiv 0$  with support on  $Z' + V'$  such that

$$\|g - \tau_z(g)\|_{\ell_1(G)} \leq \eta \|g\|_{\ell_1(G)}$$

for at least  $\Omega(\eta|Z'|)$  elements  $z \in Z'$ ; call the set of such  $z$ s  $Z''$ . We shall return to  $Z''$  later, but now we turn to showing that  $g$  has large Fourier coefficients.

Let  $h := f * \mu_{V'}$  i.e.

$$h(x) := \int f(x - y) d\mu_{V'}(y) = \int \tau_{-y}(f)(x) d\mu_{V'}(y) \text{ for all } x \in G.$$

It follows immediately that  $h$  is invariant under translation by elements of  $V'$ . Suppose that  $z \in Z' + V'$ , so that  $z = z' + v'$  where  $z' \in Z'$  and  $v' \in V'$ . Then using the fact that  $h$  is invariant under translation by elements of  $V'$ ; linearity of  $\tau$ ; the integral Minkowski inequality; and finally the isometry of  $\tau$  we get that

$$\begin{aligned} \|h - \tau_z(h)\|_{\ell_1(G)} &= \|h - \tau_{z'}(\tau_{v'}(h))\|_{\ell_1(G)} \\ &= \|h - \tau_{z'}(h)\|_{\ell_1(G)} \\ &= \left\| \int \tau_{-y}(f) d\mu_{V'}(y) - \tau_{z'} \left( \int \tau_{-y}(f) d\mu_{V'}(y) \right) \right\|_{\ell_1(G)} \\ &= \left\| \int \tau_{-y}(f - \tau_{z'}(f)) d\mu_{V'}(y) \right\|_{\ell_1(G)} \\ &\leq \int \|\tau_{-y}(f - \tau_{z'}(f))\|_{\ell_1(G)} d\mu_{V'}(y) \\ &= \int \|f - \tau_{z'}f\|_{\ell_1(G)} d\mu_{V'}(y) \leq \epsilon \|f\|_{\ell_1(G)}. \end{aligned}$$

To summarise:

$$\|h - \tau_z(h)\|_{\ell_1(G)} \leq \epsilon \|f\|_{\ell_1(G)} \text{ for all } z \in Z' + V'$$

Additionally  $h$  is supported on  $Z + V + V'$ , and by Petridis' Lemma we have that

$$\begin{aligned} |(Z + V + V') + (Z + V + V')| &\leq |(A + V + V') + (Z + V + V')| \\ &= |A + Z + (V + V')| \leq K|Z + V + V'|. \end{aligned}$$

Take  $\epsilon = 1/4 \log 2K$  and apply Lemma 4.3 to the set  $Z + V + V'$  and the functions  $h$  and  $g$  to get that

$$\begin{aligned} |\text{Spec}_{1/4\sqrt{e}}(g)^\perp| &\leq 4K|Z + V + V'| \\ &\leq 4K|Z||V||V'| \\ &= \exp(O(K(\log 2K)((\log 2K)(\log r) + \eta^{-2})))|A|. \end{aligned}$$

Now, if we put  $\eta = 1/4r\sqrt{e}$  then by Lemma 4.1 we have that  $Z'' \subset \text{Spec}_{1/4r\sqrt{e}}(g)^\perp$ . On the other hand  $Z'' \subset Z' \subset Z$  and so

$$|A + Z''| \leq K|Z| = O(K\epsilon^{-1}\eta^{-1}|Z''|).$$

Let  $Z''' \subset Z''$  be such that  $|A+Z'''|/|Z'''|$  is minimal and put  $V''' := \langle Z''' \rangle \subset \langle Z'' \rangle \text{Spec}_{1/4r\sqrt{e}}(g)^\perp$  so that

$$|V'''| \leq \exp(O(K(\log 2K)((\log 2K) \log r + r^2)))|A|,$$

and note that by Petridis' lemma we have

$$\begin{aligned} |A + V'''| &= |A + Z''' + V'''| = O(K\epsilon^{-1}\eta^{-1}|Z''' + V'''|) \\ &= O(K\epsilon^{-1}\eta^{-1}|V'''|) = O(Kr(\log 2K)|V'''|). \end{aligned}$$

It follows that  $A + V'''$  contains at most  $O(Kr \log 2K)$  cosets of  $V'''$  and hence

$$|\langle A \rangle| \leq r^{O(Kr \log 2K)}|V'''| = \exp(O(K(\log 2K)((\log 2K)(\log r) + r^2)))|A|$$

as required.  $\square$

## REFERENCES

- [Cha02] M.-C. Chang. A polynomial bound in Freiman's theorem. *Duke Math. J.*, 113(3):399–419, 2002.
- [EZ12] C. Even-Zohar. On sums of generating sets in  $\mathbb{Z}_2^n$ . *Combin. Probab. Comput.*, 21(6):916–941, 2012.
- [GK09] B. J. Green and S. V. Konyagin. On the Littlewood problem modulo a prime. *Canad. J. Math.*, 61(1):141–164, 2009.
- [GR06] B. J. Green and I. Z. Ruzsa. Sets with small sumset and rectification. *Bull. London Math. Soc.*, 38(1):43–52, 2006.
- [GR07] B. J. Green and I. Z. Ruzsa. Freiman's theorem in an arbitrary abelian group. *J. Lond. Math. Soc. (2)*, 75(1):163–175, 2007.
- [GT09] B. J. Green and T. C. Tao. Freiman's theorem in finite fields via extremal set theory. *Combin. Probab. Comput.*, 18(3):335–355, 2009.
- [Kon11] S. V. Konyagin. On Freiman's theorem. Abstract at <http://atlas-conferences.com/c/b/d/g/67.htm>, 2011.
- [LEZ14] S. Lovett and C. Even-Zohar. The Freiman-Ruzsa theorem over finite fields. *J. Combin. Theory Ser. A*, 125:333–341, 2014.
- [Pet12] G. Petridis. New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica*, 32(6):721–733, 2012.
- [Plü69] H. Plünnecke. *Eigenschaften und Abschätzungen von Wirkungsfunktionen*. BMwF-GMD-22. Gesellschaft für Mathematik und Datenverarbeitung, Bonn, 1969.
- [Rud90] W. Rudin. *Fourier analysis on groups*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1990. Reprint of the 1962 original, A Wiley-Interscience Publication.
- [Ruz89] I. Z. Ruzsa. An application of graph theory to additive number theory. *Scientia, Ser. A.*, 3:97–109, 1989.
- [Ruz99] I. Z. Ruzsa. An analog of Freiman's theorem in groups. *Astérisque*, (258):xv, 323–326, 1999. Structure theory of set addition.
- [Sch03] T. Schoen. Multiple set addition in  $\mathbb{Z}_p$ . *Integers*, 3:A17, 6 pp. (electronic), 2003.
- [Sch11] T. Schoen. Near optimal bounds in Freiman's theorem. *Duke Math. J.*, 158:1–12, 2011.
- [Tao10] T. C. Tao. Freiman's theorem for solvable groups. *Contrib. Disc. Math.*, 5(2):137–184, 2010.
- [TV06] T. C. Tao and H. V. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

MATHEMATICAL INSTITUTE, UNIVERSITY OF OXFORD, RADCLIFFE OBSERVATORY QUARTER, WOOD-STOCK ROAD, OXFORD OX2 6GG, UNITED KINGDOM

*E-mail address:* tom.sanders@maths.ox.ac.uk