Annals of Mathematics, **168** (2008), 1025–1054

A quantitative version of the idempotent theorem in harmonic analysis

By Ben Green* and Tom Sanders

Abstract

Suppose that G is a locally compact abelian group, and write $\mathbf{M}(G)$ for the algebra of bounded, regular, complex-valued measures under convolution. A measure $\mu \in \mathbf{M}(G)$ is said to be *idempotent* if $\mu * \mu = \mu$, or alternatively if $\widehat{\mu}$ takes only the values 0 and 1. The Cohen-Helson-Rudin idempotent theorem states that a measure μ is idempotent if and only if the set $\{\gamma \in \widehat{G} : \widehat{\mu}(\gamma) = 1\}$ belongs to the *coset ring* of $\widehat{G}$, that is to say we may write

$$\widehat{\mu} = \sum_{j=1}^{L} \pm 1_{\gamma_j + \Gamma_j}$$

where the Γ_j are open subgroups of $\widehat{G}$.

In this paper we show that L can be bounded in terms of the norm $\|\mu\|$, and in fact one may take $L \leqslant \exp\exp(C\|\mu\|^4)$. In particular our result is nontrivial even for finite groups.

1. Introduction

Let us begin by stating the idempotent theorem. Let G be a locally compact abelian group with dual group $\widehat{G}$. Let $\mathbf{M}(G)$ denote the *measure algebra* of G, that is to say the algebra of bounded, regular, complex-valued measures on G. We will not dwell on the precise definitions here since our paper will be chiefly concerned with the case G finite, in which case $\mathbf{M}(G) = L^1(G)$. For those parts of our paper concerning groups which are not finite, the book [19] may be consulted. A discussion of the basic properties of $\mathbf{M}(G)$ may be found in Appendix E of that book.

If $\mu \in \mathbf{M}(G)$ satisfies $\mu * \mu = \mu$, we say that μ is *idempotent*. Equivalently, the Fourier-Stieltjes transform $\widehat{\mu}$ satisfies $\widehat{\mu}^2 = \widehat{\mu}$ and is thus $0, 1$-valued.

*The first author is a Clay Research Fellow, and is pleased to acknowledge the support of the Clay Mathematics Institute.

THEOREM 1.1 (Cohen's idempotent theorem). *μ is idempotent if and only if $\{\gamma \in \widehat{G} : \widehat{\mu}(\gamma) = 1\}$ lies in the coset ring of $\widehat{G}$, that is to say*

$$\widehat{\mu} = \sum_{j=1}^{L} \pm 1_{\gamma_j + \Gamma_j},$$

where the Γ_j are open subgroups of $\widehat{G}$.

This result was proved by Paul Cohen [4]. Earlier results had been obtained in the case $G = \mathbb{T}$ by Helson [15] and $G = \mathbb{T}^d$ by Rudin [20]. See [19, Ch. 3] for a complete discussion of the theorem.

When G is finite the idempotent theorem gives us no information, since $\mathbf{M}(G)$ consists of *all* functions on G, as does the coset ring. The purpose of this paper is to prove a quantitative version of the idempotent theorem which does have nontrivial content for finite groups.

THEOREM 1.2 (Quantitative idempotent theorem). *Suppose that $\mu \in \mathbf{M}(G)$ is idempotent. Then we may write*

$$\widehat{\mu} = \sum_{j=1}^{L} \pm 1_{\gamma_j + \Gamma_j},$$

where $\gamma_j \in \widehat{G}$, each Γ_j is an open subgroup of $\widehat{G}$ and $L \leqslant e^{e^{C\|\mu\|^4}}$ for some absolute constant C. The number of distinct subgroups Γ_j may be bounded above by $\|\mu\| + \frac{1}{100}$.

Remark. In this theorem (and in Theorem 1.3 below) the bound of $\|\mu\| + \frac{1}{100}$ on the number of different subgroups Γ_j (resp. H_j) could be improved to $\|\mu\| + \delta$, for any fixed positive δ. We have not bothered to state this improvement because obtaining the correct dependence on δ would add unnecessary complication to an already technical argument. Furthermore the improvement is only of any relevance at all when $\|\mu\|$ is a tiny bit less than an integer.

To apply Theorem 1.2 to finite groups it is natural to switch the rôles of G and $\widehat{G}$. One might also write $\widehat{\mu} = f$, in which case the idempotence of μ is equivalent to asking that f be $0,1$-valued, or the characteristic function of a set $A \subseteq G$. It turns out to be just as easy to deal with functions which are $\mathbb{Z}$-valued. The norm $\|\mu\|$ is the ℓ^1-norm of the Fourier transform of f, also known as the *algebra norm* $\|f\|_A$ or sometimes, in the computer science literature, as the *spectral norm*. We will define all of these terms properly in the next section.

THEOREM 1.3 (Main theorem, finite version). *Suppose that G is a finite abelian group and that $f : G \to \mathbb{Z}$ is a function with $\|f\|_A \leqslant M$. Then*

$$f = \sum_{j=1}^{L} \pm 1_{x_j + H_j},$$

where $x_j \in G$, each $H_j \leqslant G$ is a subgroup and $L \leqslant e^{e^{CM^4}}$. Furthermore the number of distinct subgroups H_j may be bounded above by $M + \frac{1}{100}$.

Theorem 1.3 is really the main result of this paper. Theorem 1.2 is actually deduced from it (and the "qualititative" version of the idempotent theorem). This reduction is contained in Appendix A. The rest of the paper is entirely finite in nature and may be read independently of Appendix A.

2. Notation and conventions

Background for much of the material in this paper may be found in the book of Tao and Vu [25]. We shall often give appropriate references to that book as well as the original references. Part of the reason for this is that we hope the *notation* of [25] will become standard.

Constants. Throughout the paper the letters c, C will denote absolute constants which could be specified explicitly if desired. These constants will generally satisfy $0 < c \ll 1 \ll C$. Different instances of the notation, even on the same line, will typically denote different constants. Occasionally we will want to fix a constant for the duration of an argument; such constants will be subscripted as C_0, C_1 and so on.

Measures on groups. Except in Appendix A we will be working with functions defined on finite abelian groups G. As usual we write $\widehat{G}$ for the group of characters $\gamma : G \to \mathbb{C}^\times$ on G. We shall always use the *normalised counting measure* on G which attaches weight $1/|G|$ to each point $x \in G$, and *counting measure* on $\widehat{G}$ which attaches weight one to each character $\gamma \in \widehat{G}$. Integration with respect to these measures will be denoted by $\mathbb{E}_{x \in G}$ and $\sum_{\gamma \in \widehat{G}}$ respectively. Thus if $f : G \to \mathbb{C}$ is a function we define the L^p-norm

$$\|f\|_p := \big(\mathbb{E}_{x \in G} |f(x)|^p\big)^{1/p} = \big(\frac{1}{|G|} \sum_{x \in G} |f(x)|^p\big)^{1/p},$$

whilst the ℓ^p-norm of a function $g : \widehat{G} \to \mathbb{C}$ is defined by

$$\|g\|_p := \big(\sum_{\gamma \in \widehat{G}} |g(\gamma)|^p\big)^{1/p}.$$

The group on which any given function is defined will always be clear from context, and so this notation should be unambiguous.

Fourier analysis. If $f : G \to \mathbb{C}$ is a function and $\gamma \in \widehat{G}$ we define the Fourier transform $\widehat{f}(\gamma)$ by

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

We shall sometimes write this as $(f)^\wedge(\gamma)$ when f is given by a complicated expression. If $f_1, f_2 : G \to \mathbb{C}$ are two functions we define their convolution by

$$f_1 * f_2(t) := \mathbb{E}_{x\in G} f_1(x) f_2(t-x).$$

We note the basic formulæ of Fourier analysis:

(i) (Plancherel) $\langle f_1, f_2\rangle := \mathbb{E}_{x\in G} f_1(x)\overline{f_2(x)} = \sum_{\gamma\in\widehat{G}} \widehat{f_1}(\gamma)\overline{\widehat{f_2}(\gamma)} = \langle \widehat{f_1}, \widehat{f_2}\rangle$;

(ii) (Inversion) $f(x) = \sum_{\gamma\in\widehat{G}} \widehat{f}(\gamma)\gamma(x)$;

(iii) (Convolution) $(f_1 * f_2)^\wedge = \widehat{f_1}\widehat{f_2}$.

In this paper we shall be particularly concerned with the algebra norm

$$\|f\|_A := \|\widehat{f}\|_1 = \sum_{\gamma\in\widehat{G}} |\widehat{f}(\gamma)|.$$

The name comes from the fact that it satisfies $\|f_1 f_2\|_1 \leqslant \|f_1\|_A \|f_2\|_A$ for any $f_1, f_2 : G \to \mathbb{C}$.

If $f : G \to \mathbb{C}$ is a function then we have $\|\widehat{f}\|_\infty \leqslant \|f\|_1$ (a simple instance of the Hausdorff-Young inequality). If $\rho \in [0,1]$ is a parameter we define

$$\mathrm{Spec}_\rho(f) := \{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geqslant \rho\|f\|_1\}.$$

Freiman isomorphism. Suppose that $A \subseteq G$ and $A' \subseteq G'$ are subsets of abelian groups, and that $s \geqslant 2$ is an integer. We say that a map $\phi : A \to A'$ is a Freiman s-homomorphism if $a_1 + \cdots + a_s = a_{s+1} + \cdots + a_{2s}$ implies that $\phi(a_1) + \cdots + \phi(a_s) = \phi(a_{s+1}) + \cdots + \phi(a_{2s})$. If ϕ has an inverse which is also a Freiman s-homomorphism then we say that ϕ is a Freiman s-isomorphism and write $A \cong_s A'$.

3. The main argument

In this section we derive Theorem 1.3 from Lemma 3.1 below. The proof of this lemma forms the heart of the paper and will occupy the next five sections.

Our argument essentially proceeds by induction on $\|f\|_A$, splitting f into a sum $f_1 + f_2$ of two functions and then handling those using the inductive hypothesis. As in our earlier paper [12], it is not possible to effect such a procedure entirely within the "category" of $\mathbb{Z}$-valued functions. One must consider, more generally, functions which are ε-almost $\mathbb{Z}$-valued, that is to say take values in $\mathbb{Z} + [-\varepsilon, \varepsilon]$. If a function has this property we will write $d(f, \mathbb{Z}) < \varepsilon$. In our argument we will always have $\varepsilon < 1/2$, in which case we may unambiguously define $f_{\mathbb{Z}}$ to be the integer-valued function which most closely approximates f.

LEMMA 3.1 (Inductive Step). *Suppose that $f : G \to \mathbb{R}$ has $\|f\|_A \leqslant M$, where $M \geqslant 1$, and that $d(f, \mathbb{Z}) \leqslant e^{-C_1 M^4}$. Set $\varepsilon := e^{-C_0 M^4}$, for some constant C_0. Then $f = f_1 + f_2$, where*

(i) *either $\|f_1\|_A \leqslant \|f\|_A - 1/2$ or else $(f_1)_{\mathbb{Z}}$ may be written as $\sum_{j=1}^{L} \pm 1_{x_j+H}$, where H is a subgroup of G and $L \leqslant e^{e^{C'(C_0)M^4}}$;*

(ii) *$\|f_2\|_A \leqslant \|f\|_A - \frac{1}{2}$ and*

(iii) *$d(f_1, \mathbb{Z}) \leqslant d(f, \mathbb{Z}) + \varepsilon$ and $d(f_2, \mathbb{Z}) \leqslant 2d(f, \mathbb{Z}) + \varepsilon$.*

Proof of Theorem 1.3 *assuming Lemma* 3.1. We apply Lemma 3.1 iteratively, starting with the observation that if $f : G \to \mathbb{Z}$ is a function then $d(f, \mathbb{Z}) = 0$. Let $\varepsilon = e^{-C_0 M^4}$ be a small parameter, where C_0 is much larger than the constant C_1 appearing in the statement of Lemma 3.1. Split

$$f = f_1 + f_2$$

according to Lemma 3.1 in such a way that $d(f_1, \mathbb{Z}), d(f_2, \mathbb{Z}) \leqslant \varepsilon$. Each $(f_i)_{\mathbb{Z}}$ is a sum of at most $e^{e^{CM^4}}$ functions of the form $\pm 1_{x_j+H_i}$ (in which case we say it is *finished*), or else we have $\|f_i\|_A \leqslant \|f\|_A - \frac{1}{2}$.

Now split any unfinished functions using Lemma 3.1 again, and so on (we will discuss the admissibility of this shortly). After at most $2M - 1$ steps all functions will be finished. Thus we will have a decomposition

$$f = \sum_{k=1}^{L} f_k,$$

where

(a) $L \leqslant 2^{2M-1}$;

(b) for each k, $(f_k)_{\mathbb{Z}}$ may be written as the sum of at most $e^{e^{CM^4}}$ functions of the form $\pm 1_{x_{j,k}+H_k}$, where $H_k \leqslant G$ is a subgroup, and

(c) $d(f_k, \mathbb{Z}) \leqslant 2^{2M}\varepsilon$ for all k.

The last fact follows by an easy induction, where we note carefully the factor of 2 in (iii) of Lemma 3.1. Note that as a consequence of this, and the fact that $C_0 \ggg C_1$, our repeated applications of Lemma 3.1 were indeed valid.

Now we clearly have

$$\|f - \sum_{k=1}^{L} (f_k)_{\mathbb{Z}}\|_\infty \leqslant 2^{4M-1}\varepsilon < 1.$$

Since f is $\mathbb{Z}$-valued we are forced to conclude that in fact

$$f = \sum_{k=1}^{L} (f_k)_{\mathbb{Z}}.$$

It remains to establish the claim that $L \leqslant M + \frac{1}{100}$. By construction we have

$$\|f\|_A = \sum_{k=1}^{L} \|f_k\|_A.$$

If $(f_k)_{\mathbb{Z}}$ is not identically 0 then, since ε is so small, we have from (c) above that

$$\|f_k\|_A \geqslant \|f_k\|_\infty \geqslant \|(f_k)_{\mathbb{Z}}\|_\infty - 2^{2M}\varepsilon \geqslant \frac{M}{M + \frac{1}{100}}.$$

It follows that $(f_k)_{\mathbb{Z}} = 0$ for all but at most $M + \frac{1}{100}$ values of k, as desired. □

4. Bourgain systems

We now begin assembling the tools required to prove Lemma 3.1.

Many theorems in additive combinatorics can be stated for an arbitrary abelian group G, but are much easier to prove in certain *finite field models*, that is to say groups $G = \mathbb{F}_p^n$ where p is a small fixed prime. This phenomenon is discussed in detail in the survey [7]. The basic reason for it is that the groups $\mathbb{F}_p^n$ have a very rich subgroup structure, whereas arbitrary groups need not: indeed the group $\mathbb{Z}/N\mathbb{Z}$, N a prime, has no nontrivial subgroups at all.

In his work on 3-term arithmetic progressions Bourgain [1] showed that *Bohr sets* may be made to play the rôle of "approximate subgroups" in many arguments. A definition of Bohr sets will be given later. Since his work, similar ideas have been used in several places [8], [10], [13], [21], [22], [23].

In this paper we need a notion of approximate subgroup which includes that of Bourgain but is somewhat more general. In particular we need a notion which is invariant under Freiman isomorphism. A close examination of Bourgain's arguments reveals that the particular structure of Bohr sets is only relevant in one place, where it is necessary to classify the set of points at which the Fourier transform of a Bohr set is large. In an exposition of Bourgain's work, Tao [24] showed how to do without this information, and as a result of this it is possible to proceed in more abstract terms.

Definition 4.1 (Bourgain systems). Let G be a finite abelian group and let $d \geqslant 1$ be an integer. A Bourgain system $\mathcal{S}$ of dimension d is a collection $(X_\rho)_{\rho\in[0,4]}$ of subsets of G indexed by the nonnegative real numbers such that the following axioms are satisfied:

BS1 (*Nesting*) If $\rho' \leqslant \rho$, then $X_{\rho'} \subseteq X_\rho$;

BS2 (*Zero*) $0 \in X_0$;

BS3 (*Symmetry*) If $x \in X_\rho$ then $-x \in X_\rho$;

BS4 (*Addition*) For all ρ, ρ' such that $\rho + \rho' \leqslant 4$ we have $X_\rho + X_{\rho'} \subseteq X_{\rho+\rho'}$;

BS5 (*Doubling*) If $\rho \leqslant 1$, then $|X_{2\rho}| \leqslant 2^d |X_\rho|$.

We refer to $|X_1|$ as the *size* of the system $\mathcal{S}$, and write $|\mathcal{S}|$ for this quantity.

Remarks. If a Bourgain system has dimension at most d, then it also has dimension at most d' for any $d' \geqslant d$. It is convenient, however, to attach a fixed dimension to each system. Note that the definition is largely independent of the group G, a feature which enables one to think of the basic properties of Bourgain systems without paying much attention to the underlying group.

Definition 4.2 (Measures on a Bourgain system). Suppose that $\mathcal{S} = (X_\rho)_{\rho\in[0,4]}$ is a Bourgain system contained in a group G. We associate to $\mathcal{S}$ a system $(\beta_\rho)_{\rho\in[0,2]}$ of probability measures on the group G. These are defined by setting

$$\beta_\rho := \frac{1_{X_\rho}}{|X_\rho|} * \frac{1_{X_\rho}}{|X_\rho|}.$$

Note that β_ρ is supported on $X_{2\rho}$.

Definition 4.3 (Density). We define $\mu(\mathcal{S}) = |\mathcal{S}|/|G|$ to be the *density* of $\mathcal{S}$ relative to G.

Remarks. Note that everything in these two definitions *is* rather dependent on the underlying group G. The reason for defining our measures in this way is that the Fourier transform $\widehat{\beta_\rho}$ is real and nonnegative. This positivity property will be very useful to us later. The idea of achieving this by convolving an indicator function with itself goes back, of course, to Fejér. For a similar use of this device see [8, especially Lemma 7.2].

The first example of a Bourgain system is a rather trivial one.

Example (Subgroup systems). Suppose that $H \leqslant G$ is a subgroup. Then the collection $(X_\rho)_{\rho\in[0,4]}$ in which each X_ρ is equal to H is a Bourgain system of dimension 0.

The second example is important only in the sense that later on it will help us economise on notation.

Example (Dilated systems). Suppose that $\mathcal{S} = (X_\rho)_{\rho\in[0,4]}$ is a Bourgain system of dimension d. Then, for any $\lambda \in (0,1]$, so is the collection $\lambda\mathcal{S} := (X_{\lambda\rho})_{\rho\in[0,4]}$.

The following simple lemma concerning dilated Bourgain systems will be useful in the sequel.

LEMMA 4.4. *Let $\mathcal{S}$ be a Bourgain system of dimension d, and suppose that $\lambda \in (0,1]$. Then* $\dim(\lambda\mathcal{S}) = d$ *and* $|\lambda\mathcal{S}| \geqslant (\lambda/2)^d|\mathcal{S}|$. □

Definition 4.5 (Bohr systems). The first substantial example of a Bourgain system is the one contained in the original paper [1]. Let $\Gamma = \{\gamma_1,\dots,\gamma_k\} \subseteq \widehat{G}$ be a collection of characters, let $\kappa_1,\dots,\kappa_k > 0$, and define

the system $\mathrm{Bohr}_{\kappa_1,\dots,\kappa_k}(\Gamma)$ by taking

$$X_\rho := \{x \in G : |1 - \gamma_j(x)| \leqslant \kappa_j \rho\}.$$

When all the κ_i are the same we write $\mathrm{Bohr}_\kappa(\Gamma) = \mathrm{Bohr}_{\kappa_1,\dots,\kappa_k}(\Gamma)$ for short. The properties BS1,BS2 and BS3 are rather obvious. Property BS4 is a consequence of the triangle inequality and the fact that $|\gamma(x)-\gamma(x')| = |1-\gamma(x-x')|$. Property BS5 and a lower bound on the density of Bohr systems are documented in the next lemma, a proof of which may be found in any of [8], [10], [13].

LEMMA 4.6. *Suppose that* $\mathcal{S} = \mathrm{Bohr}_{\kappa_1,\dots,\kappa_k}(\Gamma)$ *is a Bohr system. Then* $\dim(\mathcal{S}) \leqslant 3k$ *and* $|\mathcal{S}| \geqslant 8^{-k}\kappa_1 \dots \kappa_k |G|$. □

The notion of a Bourgain system is invariant under Freiman isomorphisms.

Example (Freiman isomorphs). Suppose that $\mathcal{S} = (X_\rho)_{\rho\in[0,4]}$ is a Bourgain system and that $\phi : X_4 \to G'$ is some Freiman isomorphism such that $\phi(0) = 0$. Then $\phi(\mathcal{S}) := (\phi(X_\rho))_{\rho\in[0,4]}$ is a Bourgain system of the same dimension and size.

The next example is of no real importance over and above those already given, but it does serve to set the definition of Bourgain system in a somewhat different light.

Example (Translation-invariant pseudometrics). Suppose that $d : G\times G \to \mathbb{R}_{\geqslant 0}$ is a translation-invariant pseudometric. That is, d satisfies the usual axioms of a metric space except that it is possible for $d(x, y)$ to equal zero when $x \neq y$ and we insist that $d(x + z, y + z) = d(x, y)$ for any x, y, z. Write X_ρ for the ball

$$X_\rho := \{x \in G : d(x, 0) \leqslant \rho\}.$$

Then $(X_\rho)_{\rho\in[0,4]}$ is a Bourgain system precisely if d is *doubling*; cf. [14, Ch. 1].

Remark. It might seem more elegant to try and define a Bourgain system to be the same thing as a doubling, translation invariant pseudometric. There is a slight issue, however, which is that such Bourgain systems satisfy BS1–BS5 for all $\rho \in [0, \infty)$. It is not in general possible to extend a Bourgain system defined for $\rho \in [0, 4]$ to one defined for all nonnegative ρ, as one cannot keep control of the dimension condition BS5. Consider for example the (rather trivial) Bourgain system in which $X_\rho = \{0\}$ for $\rho < 4$ and X_4 is a symmetric set of K "dissociated" points.

We now proceed to develop the basic theory of Bourgain systems. For the most part this parallels the theory of Bohr sets as given in several of the papers cited earlier. The following lemmas all concern a Bourgain system $\mathcal{S}$ with dimension d.

We begin with simple covering and metric entropy estimates. The following covering lemma could easily be generalized somewhat, but we give here just the result we shall need later on.

LEMMA 4.7 (Covering lemma). *For any $\rho \leqslant 1/2$, $X_{2\rho}$ may be covered by 2^{4d} translates of $X_{\rho/2}$.*

Proof. Let $Y = \{y_1, \dots, y_k\}$ be a maximal collection of elements of $X_{2\rho}$ with the property that the balls $y_j + X_{\rho/4}$ are all disjoint. If there is some point $y \in X_{2\rho}$ which does not lie in any $y_j + X_{\rho/2}$, then $y + X_{\rho/4}$ does not intersect $y_j + X_{\rho/4}$ for any j by BS4, contrary to the supposed maximality of Y. Now another application of BS4 implies that

$$\bigcup_{j=1}^{k} (y_j + X_{\rho/4}) \subseteq X_{9\rho/4}.$$

We therefore have

$$k \leqslant |X_{9\rho/4}|/|X_{\rho/4}| \leqslant |X_{4\rho}|/|X_{\rho/4}| \leqslant 2^{4d}.$$

The lemma follows. □

LEMMA 4.8 (Metric entropy lemma). *Let $\rho \leqslant 1$. The group G may be covered by at most $(4/\rho)^d \mu(\mathcal{S})^{-1}$ translates of X_ρ.*

Proof. This is a simple application fo the Ruzsa covering lemma (cf. [25, Ch. 2]) and the basic properties of Bourgain systems. Indeed the Ruzsa covering lemma provides a set $T \subseteq G$ such that $G = X_{\rho/2} - X_{\rho/2} + T$, where

$$|T| \leqslant \frac{|X_{\rho/2} + G|}{|X_{\rho/2}|} \leqslant \frac{|G|}{|X_{\rho/2}|}.$$

BS4 then tells us that $G = X_\rho + T$. To bound the size of T above, we observe from BS5 that $|X_{\rho/2}| \geqslant (\rho/4)^d |X_1|$. The result follows. □

In this paper we will often be doing a kind of Fourier analysis relative to Bourgain systems. In this regard it is useful to know what happens when an arbitrary Bourgain system $(X_\rho)_{\rho\in[0,4]}$ is joined with a system $(\mathrm{Bohr}(\Gamma, \varepsilon\rho))_{\rho\in[0,4]}$ of Bohr sets, where $\Gamma \subseteq \widehat{G}$ is a set of characters. It turns out not to be much harder to deal with the join of a pair of Bourgain systems in general.

Definition 4.9 (Joining of two Bourgain systems). Suppose that $\mathcal{S} = (X_\rho)_{\rho\in[0,4]}$ and $\mathcal{S}' = (X'_\rho)_{\rho\in[0,4]}$ are two Bourgain systems with dimensions at most d and d' respectively. Then we define the join of $\mathcal{S}$ and $\mathcal{S}'$, $\mathcal{S} \wedge \mathcal{S}'$, to be the collection $(X_\rho \cap X'_\rho)_{\rho\in[0,4]}$.

LEMMA 4.10 (Properties of joins). *Let $\mathcal{S}, \mathcal{S}'$ be as above. Then the join $\mathcal{S} \wedge \mathcal{S}'$ is also a Bourgain system. It has dimension at most $4(d+d')$ and its size satisfies the bound*

$$|\mathcal{S} \wedge \mathcal{S}'| \geqslant 2^{-3(d+d')}\mu(\mathcal{S}')|\mathcal{S}|.$$

Proof. It is trivial to verify properties BS1–BS4. To prove BS5, we apply Lemma 4.7 to both $\mathcal{S}$ and $\mathcal{S}'$. This enables us to cover $X_{2\rho} \cap X'_{2\rho}$ by $2^{4(d+d')}$ sets of the form $T = (y + X_{\rho/2}) \cap (y' + X'_{\rho/2})$. Now for any fixed $t_0 \in T$ the map $t \mapsto t - t_0$ is an injection from T to $X_\rho \cap X'_\rho$. It follows, of course, that $|T| \leqslant |X_\rho \cap X'_\rho|$ and hence that

$$|X_{2\rho} \cap X'_{2\rho}| \leqslant 2^{4(d+d')}|X_\rho \cap X'_\rho|.$$

This establishes the claimed bound on the dimension of $\mathcal{S} \wedge \mathcal{S}'$. It remains to obtain a lower bound for the density of this system. To do this, we apply Lemma 4.8 to cover G by at most $8^{d'}\mu(\mathcal{S}')^{-1}$ translates of $X'_{1/2}$. It follows that there is some x such that

$$|X_{1/2} \cap (x + X'_{1/2})| \geqslant 8^{-d'}\mu(\mathcal{S}')^{-1}|X_{1/2}| \geqslant 2^{-3(d+d')}\mu(\mathcal{S}')|X_1|.$$

Now for any fixed $x_0 \in X_{1/2} \cap (x + X'_{1/2})$ the map $x \mapsto x - x_0$ is an injection from $X_{1/2} \cap (x + X'_{1/2})$ to $X_1 \cap X'_1$. It follows that

$$|X_1 \cap X'_1| \geqslant 2^{-3(d+d')}\mu(\mathcal{S}')|X_1|,$$

which is equivalent to the lower bound on the size of $\mathcal{S} \wedge \mathcal{S}'$ that we claimed.□

We move on now to one of the more technical aspects of the theory of Bourgain systems, the notion of regularity.

Definition 4.11 (Regular Bourgain systems). Let $\mathcal{S} = (X_\rho)_{\rho \in [0,4]}$ be a Bourgain system of dimension d. We say that the system is *regular* if

$$1 - 10d\kappa \leqslant \frac{|X_1|}{|X_{1+\kappa}|} \leqslant 1 + 10d\kappa$$

whenever $|\kappa| \leqslant 1/10d$.

LEMMA 4.12 (Finding regular Bourgain systems). *Suppose $\mathcal{S}$ is a Bourgain system. Then there is some $\lambda \in [1/2, 1]$ such that the dilated system $\lambda\mathcal{S}$ is regular.*

Proof. Let $f : [0,1] \to \mathbb{R}$ be the function $f(a) := \frac{1}{d}\log_2 |X_{2^a}|$. Observe that f is nondecreasing in a and that $f(1) - f(0) \leqslant 1$. We claim that there is an $a \in [\frac{1}{6}, \frac{5}{6}]$ such that $|f(a+x) - f(a)| \leqslant 3|x|$ for all $|x| \leqslant \frac{1}{6}$. If no such a exists then for every $a \in [\frac{1}{6}, \frac{5}{6}]$ there is an interval $I(a)$ of length at most $\frac{1}{6}$ having one endpoint equal to a and with $\int_{I(a)} df > \int_{I(a)} 3dx$. These intervals

cover $[\frac{1}{6}, \frac{5}{6}]$, which has total length $\frac{2}{3}$. A simple covering lemma that has been discussed by Hallard Croft [5] (see also [10, Lemma 3.4]) then allows us to pass to a disjoint subcollection $I_1 \cup \cdots \cup I_n$ of these intervals with total length at least $\frac{1}{3}$. However, we now have

$$1 \geqslant \int_0^1 df \geqslant \sum_{i=1}^n \int_{I_i} df > \sum_{i=1}^n \int_{I_i} 3\,dx \geqslant \frac{1}{3} \cdot 3,$$

a contradiction. It follows that there is indeed an a such that $|f(a+x)-f(a)| \leqslant 3|x|$ for all $|x| \leqslant \frac{1}{6}$. Setting $\lambda := 2^a$, it is easy to see that

$$e^{-5d\kappa} \leqslant \frac{|X_\lambda|}{|X_{(1+\kappa)\lambda}|} \leqslant e^{5d\kappa}$$

whenever $|\kappa| \leqslant 1/10d$. Since $1 - 2|x| \leqslant e^x \leqslant 1 + 2|x|$ when $|x| \leqslant 1$, it follows that $\lambda\mathcal{S}$ is a regular Bourgain system. □

LEMMA 4.13. *Suppose that $\mathcal{S}$ is a regular Bourgain system of dimension d and let $\kappa \in (0,1)$. Suppose that $y \in X_\kappa$. Then*

$$\mathbb{E}_{x\in G}|\beta_1(x+y) - \beta_1(x)| \leqslant 20d\kappa.$$

Proof. For this lemma only, let us write $\mu_1 := 1_{X_1}/|X_1|$, so that $\beta_1 = \mu_1 * \mu_1$. We first claim that if $y \in X_\kappa$ then

$$\mathbb{E}_{x\in G}|\mu_1(x+y) - \mu_1(x)| \leqslant 20d\kappa.$$

The result is trivial if $\kappa > 1/10d$, so assume that $\kappa \leqslant 1/10d$. Observe that $|\mu_1(x+y) - \mu_1(x)| = 0$ unless $x \in X_{1+\kappa} \setminus X_{1-\kappa}$. Since $\mathcal{S}$ is regular, the size of this set is at most $20d\kappa|X_1|$, and the claim follows immediately.

To prove the lemma, note that

$$\begin{aligned}\mathbb{E}_{x\in G}|\beta_1(x+y) - \beta_1(x)| &= \mathbb{E}_{x\in G}|\mu_1 * \mu_1(x+y) - \mu_1 * \mu_1(x)| \\ &= \mathbb{E}_x\big|\mathbb{E}_z\mu_1(z)\mu_1(x+y-z) - \mathbb{E}_z\mu_1(z)\mu_1(x-z)\big| \\ &\leqslant \mathbb{E}_z\mu_1(z)\mathbb{E}_x|\mu_1(x+y-z) - \mu_1(x-z)| \\ &\leqslant 20d\kappa,\end{aligned}$$

the last inequality following from the claim. □

The operation of convolution by β_1 will play an important rôle in this paper, particularly in the next section.

Definition 4.14 (Convolution operator). Suppose that $\mathcal{S}$ is a Bourgain system. Then we associate to $\mathcal{S}$ the map $\psi_{\mathcal{S}} : L^\infty(G) \to L^\infty(G)$ defined by $\psi_{\mathcal{S}} f := f * \beta_1$, or equivalently by $(\psi_{\mathcal{S}} f)^\wedge := \widehat{f}\widehat{\beta}_1$.

We note in particular that, since $\widehat{\beta}_1$ is real and nonnegative,

$$\|f\|_A = \|\psi_{\mathcal{S}} f\|_A + \|f - \psi_{\mathcal{S}} f\|_A. \tag{4.1}$$

LEMMA 4.15 (Almost invariance). *Let $f : G \to \mathbb{C}$ be any function. Let $\mathcal{S}$ be a regular Bourgain system of dimension d, let $\kappa \in (0,1)$ and suppose that $y \in X_\kappa$. Then*

$$|\psi_{\mathcal{S}} f(x+y) - \psi_{\mathcal{S}} f(x)| \leqslant 20d\kappa \|f\|_\infty$$

for all $x \in G$.

Proof. The left-hand side, written out in full, is

$$|\mathbb{E}_t f(t)(\beta_\rho(t-x-y) - \beta_\rho(t-x))|.$$

The lemma follows immediately from Lemma 4.13 and the triangle inequality. □

LEMMA 4.16 (Structure of Spec). *Let $\delta \in (0,1]$. Suppose that $\mathcal{S}$ is a regular Bourgain system of dimension d and that $\gamma \in \mathrm{Spec}_\delta(\beta_1)$. Suppose that $\kappa \in (0,1)$. Then we have*

$$|1 - \gamma(y)| \leqslant 20\kappa d/\delta$$

for all $y \in X_\kappa$.

Proof. Suppose that $y \in X_\kappa$. Then we have

$$\begin{aligned}\delta|1-\gamma(y)| \leqslant |\widehat{\beta}_1(\gamma)||1-\gamma(y)| &= |\mathbb{E}_{x\in G}\beta_1(x)(\gamma(x)-\gamma(x+y))| \\ &= |\mathbb{E}_{x\in G}(\beta_1(x)-\beta_1(x-y))\gamma(x)|.\end{aligned}$$

This is bounded by $20d\kappa$ by Lemma 4.13. □

5. Averaging over a Bourgain system

Let $\mathcal{S} = (X_\rho)_{\rho\in[0,4]}$ be a Bourgain system of dimension d. Recall from the last section the definition of the operator $\psi_{\mathcal{S}} : L^\infty(G) \to L^\infty(G)$. From our earlier paper [12], one might use operators of this type to effect a decomposition

$$f = \psi_{\mathcal{S}} f + (f - \psi_{\mathcal{S}} f),$$

the aim being to prove Theorem 1.3 by induction on $\|f\|_A$. To make such a strategy work, a judicious choice of $\mathcal{S}$ must be made. First of all, one must ensure that both $\|\psi_{\mathcal{S}} f\|_A$ and $\|f - \psi_{\mathcal{S}} f\|_A$ are significantly less than $\|f\|_A$. In this regard (4.1) is of some importance, and this is why we defined the measures β_ρ in such a way that $\widehat{\beta}_\rho$ is always real and nonnegative. The actual accomplishment of this will be a task for the next section. In an ideal world, our second requirement would be that $\psi_{\mathcal{S}}$ preserves the property of being $\mathbb{Z}$-valued. As in our earlier paper this turns out not to be possible and one must expand the collection of functions under consideration to include those for which $d(f,\mathbb{Z}) \leqslant \varepsilon$. The reader may care to recall the definitions of $d(f,\mathbb{Z})$ and of $f_{\mathbb{Z}}$ at this point: they are given at the start of Section 3.

The main result of this section states that if f is almost integer-valued then any Bourgain system $\mathcal{S}$ may be refined to a system $\mathcal{S}'$ so that $\psi_{\mathcal{S}'}f$ is almost integer-valued. A result of this type in the finite field setting, where $\mathcal{S}$ is just a subgroup system in $\mathbb{F}_2^n$, was obtained in [12]. The argument there, which was a combination of [12, Lemma 3.4] and [12, Prop. 3.7], was somewhat elaborate and involved polynomials which are small near small integers. The argument we give here is different and is close to the main argument in [10] (in fact, it is very close to the somewhat simpler argument, leading to a bound of $O(\log^{-1/4} p)$, sketched just after Lemma 4.1 of that paper). In the finite field setting it is simpler than that given in [12, Sec. 3] and provides a better bound. Due to losses elsewhere in the argument, however, it does not lead to an improvement in the overall bound in our earlier paper.

PROPOSITION 5.1. *Suppose that $f : G \to \mathbb{R}$ satisfies $\|f\|_A \leqslant M$, where $M \geqslant 1$, and also $d(f,\mathbb{Z}) < 1/4$. Let $\mathcal{S}$ be a regular Bourgain system of dimension $d \geqslant 2$, and let $\varepsilon \leqslant \frac{1}{4}$ be a positive real. Then there is a regular Bourgain system $\mathcal{S}'$ with dimension d' such that*

$$d' \leqslant 4d + \frac{64M^2}{\varepsilon^2}; \tag{5.1}$$

$$|\mathcal{S}'| \geqslant e^{-\frac{Cd M^4}{\varepsilon^4}\log(dM/\varepsilon)}|\mathcal{S}|; \tag{5.2}$$

$$\|\psi_{\mathcal{S}'}f\|_\infty \geqslant \|\psi_{\mathcal{S}}f\|_\infty - \varepsilon \tag{5.3}$$

and such that

$$d(\psi_{\mathcal{S}'}f,\mathbb{Z}) \leqslant d(f,\mathbb{Z}) + \varepsilon. \tag{5.4}$$

Remarks. The stipulation that $d \geqslant 2$ and that $M \geqslant 1$ is made for notational convenience in our bounds. These conditions may clearly be satisfied in any case by simply increasing d or M as necessary.

Proof. We shall actually find $\mathcal{S}'$ satisfying the following property:

$$\mathbb{E}_{x\in G}(f - \psi_{\mathcal{S}'}f)(x)^2\beta'_\rho(x - x_0) \leqslant \varepsilon^2/4 \tag{5.5}$$

for any $x_0 \in G$ and every $\rho \geqslant \varepsilon/160d'M$ such that $\rho\mathcal{S}'$ is regular. The truth of (5.5) implies (5.4). To see this, suppose that (5.4) is false. Then there is x_0 so that $\psi_{\mathcal{S}'}f(x_0)$ is not within $d(f,\mathbb{Z}) + \varepsilon$ of an integer. Noting that $\|f\|_\infty \leqslant \|f\|_A \leqslant M$, we see from Lemma 4.15 that $\psi_{\mathcal{S}'}f(x)$ is not within $d(f,\mathbb{Z}) + \varepsilon/2$ of an integer for any $x \in x_0 + X_{\varepsilon/40d'M}$. Choosing, according to Lemma 4.12, a value $\rho \in [\varepsilon/160d'M, \varepsilon/80d'M]$ for which $\rho\mathcal{S}'$ is regular, we have

$$\mathbb{E}_x(f - \psi_{\mathcal{S}'}f)(x)^2\beta'_\rho(x - x_0) > \varepsilon^2/4,$$

contrary to our assumption of (5.5).

It remains to find an $\mathcal{S}'$ such that (5.5) is satisfied for all $x_0 \in G$ and all $\rho \geqslant \varepsilon/160d'M$ such that $\rho\mathcal{S}'$ is regular. We shall define a nested sequence

$\mathcal{S}^{(j)} = (X_\rho^{(j)})_{\rho\in[0,4]}$, $j = 0, 1, 2, \dots$ of regular Bourgain systems with $d_j := \dim(\mathcal{S}^{(j)})$. We initialize this process by taking $\mathcal{S}^{(0)} := \mathcal{S}$.

Suppose that $\mathcal{S}^{(j)}$ does not satisfy (5.5), that is to say there is $y \in G$ and $\rho \geqslant \varepsilon/160d_jM$ such that $\rho\mathcal{S}^{(j)}$ is regular and

$$\mathbb{E}_{x\in G}(f - f * \beta_1^{(j)})(x)^2\beta_\rho^{(j)}(x-y) > \varepsilon^2/4.$$

Applying Plancherel, we obtain

$$\sum_{\gamma\in\widehat{G}} \big((f - f * \beta_1^{(j)})\beta_\rho^{(j)}(\cdot - y)\big)^\wedge(\gamma)(f - f * \beta_1^{(j)})^\wedge(\gamma) > \varepsilon^2/4.$$

This implies that

$$\|\big((f - f * \beta_1^{(j)})\beta_\rho^{(j)}(\cdot - y)\big)^\wedge\|_\infty > \varepsilon^2/8M,$$

which implies that there is some $\gamma_0^{(j+1)} \in \widehat{G}$ such that

$$\sum_\gamma |\widehat{f}(\gamma)||1 - \widehat{\beta}_1^{(j)}(\gamma)||\widehat{\beta}_\rho^{(j)}(\gamma_0^{(j+1)} - \gamma)| > \varepsilon^2/8M.$$

Removing the tails where either $|1-\widehat{\beta}_1^{(j)}(\gamma)| \leqslant \varepsilon^2/32M^2$ or $|\widehat{\beta}_\rho^{(j)}(\gamma_0^{(j+1)} - \gamma)| \leqslant \varepsilon^2/64M^2$, we see this implies

$$\sum_{\gamma\in\Gamma^{(j)}} |\widehat{f}(\gamma)| > \varepsilon^2/16M, \tag{5.6}$$

where the sum is over the set

$$\Gamma^{(j)} := \big(\gamma_0^{(j+1)} + \operatorname{Spec}_{\varepsilon^2/64M^2}(\beta_\rho^{(j)})\big) \setminus \operatorname{Spec}_{1-\varepsilon^2/32M^2}(\beta_1^{(j)}).$$

We shall choose a regular Bourgain system $\mathcal{S}^{(j+1)}$ in such a way that

$$\gamma_0^{(j+1)} + \operatorname{Spec}_{\varepsilon^2/64M^2}(\beta_\rho^{(j)}) \subseteq \operatorname{Spec}_{1-\varepsilon^2/32M^2}(\beta_1^{(j+1)}). \tag{5.7}$$

The sets $\Gamma^{(j)}$ are then disjoint, and it follows from (5.6) that the iteration must stop for some $j = J$, $J \leqslant 16M^2/\varepsilon^2$. We then define $\mathcal{S}' := \mathcal{S}^{(J)}$.

To satisfy (5.7) we take

$$\mathcal{S}^{(j+1)} := \lambda\big(\kappa\rho\mathcal{S}^{(j)} \wedge \operatorname{Bohr}_{\kappa'}(\{\gamma_0^{(j+1)}\})\big), \tag{5.8}$$

where $\kappa := 2^{-17}\epsilon^4/d_jM^4$, $\kappa' := \varepsilon^2/64M^2$, and $\lambda \in [1/2, 1]$ is chosen so that $\mathcal{S}^{(j+1)}$ is regular. Note that

$$\lambda\kappa\rho \geqslant \frac{\varepsilon^5}{2^{26}d_j^2M^5}. \tag{5.9}$$

Suppose that $\gamma \in \operatorname{Spec}_{\varepsilon^2/64M^2}(\beta_\rho^{(j)})$. Then in view of Lemma 4.16 and the fact that $\rho\mathcal{S}^{(j)}$ is regular we have

$$|1 - \gamma(x)| \leqslant \frac{1280\kappa d_jM^2}{\varepsilon^2} \leqslant \frac{\varepsilon^2}{64M^2}$$

whenever $x \in X_1^{(j+1)}$. Furthermore we also have

$$|1 - \gamma_0^{(j+1)}(x)| \leqslant \kappa' = \varepsilon^2/64M^2.$$

It follows that if $x \in X_1^{(j+1)}$ then

$$|1 - \gamma_0^{(j+1)}(x)\gamma(x)| \leqslant \varepsilon^2/32M^2,$$

and therefore $\gamma_0^{(j+1)} + \gamma \in \mathrm{Spec}_{1-\varepsilon^2/32M^2}(\beta_1^{(j+1)})$.

It remains to bound $\dim(\mathcal{S}^{(j)})$ and $|\mathcal{S}^{(j)}|$. To this end we note that by construction,

$$\mathcal{S}^{(j)} = \delta^{(j)}\mathcal{S}^{(0)} \wedge \mathrm{Bohr}_{\kappa_1,\dots,\kappa_j}(\{\gamma_0^{(1)},\dots,\gamma_0^{(j)}\}),$$

where each κ_i is at least $2^{-j}\epsilon^2/64M^2$ and, in view of (5.9),

$$\delta^{(j)} \geqslant (\varepsilon^5/2^{26}M^5)^j\big(\prod_{i\leqslant j} d_i\big)^{-2}.$$

It follows from Lemmas 4.6 and 4.10 that $d_j \leqslant 4(d+j)$ for all j, and in particular we obtain the claimed upper bound on $\dim(\mathcal{S}')$. It follows from the same two lemmas together with Lemma 4.4 and a short computation that $|\mathcal{S}'|$ is subject to the claimed lower bound. The lower bound we have given is, in fact, rather crude but has been favoured due to its simplicity of form.

It remains to establish (5.3). Noting that

$$f * \beta_1 = f * \beta_1 * \beta_1' - f * (\beta_1 * \beta_1' - \beta_1),$$

we obtain the bound

$$\|\psi_{\mathcal{S}} f\|_\infty \leqslant \|\psi_{\mathcal{S}'} f\|_\infty + \|f\|_\infty \|\beta_1 * \beta_1' - \beta_1\|_1.$$

If

$$\|\beta_1 * \beta_1' - \beta_1\|_1 \leqslant \varepsilon/M,$$

then the result will follow. We have, however, that

$$\|\beta_1 * \beta_1' - \beta_1\|_1 = \mathbb{E}_x\big|\mathbb{E}_y \beta_1'(y)(\beta_1(x-y) - \beta_1(x))\big|,$$

and from Lemma 4.13 it will follow that this is at most ε/M provided that $\mathrm{Supp}(\beta_1') \subseteq X_{\varepsilon/20dM}$. This, however, is more than guaranteed by the construction of the successive Bourgain systems as given in (5.8). Note that we may assume without loss of generality that the iteration does proceed for at least one step; even if (5.5) is satisfied by $\mathcal{S} = \mathcal{S}^{(0)}$, we may simply take an arbitrary $\gamma_0^{(1)} \in \widehat{G}$ and define $\mathcal{S}^{(1)}$ as in (5.8). □

6. A weak Freiman theorem

In our earlier work [12] we used (a refinement of) Ruzsa's analogue of Freiman's theorem, which gives a fairly strong characterisation of subsets $A \subseteq \mathbb{F}_2^n$ satisfying a small doubling condition $|A+A| \leqslant K|A|$. An analogue of this theorem for any abelian group was obtained in [11]. We could apply this theorem here, but as reward for setting up the notion of Bourgain systems in some generality we are able to make do with a weaker theorem of the following type, which we refer to as a "weak Freiman theorem".

PROPOSITION 6.1 (Weak Freiman). *Suppose that G is a finite abelian group, and that $A \subseteq G$ is a finite set with $|A+A| \leqslant K|A|$. Then there is a regular Bourgain system $\mathcal{S} = (X_\rho)_{\rho\in[0,4]}$ such that*

$$\dim(\mathcal{S}) \leqslant CK^C; \qquad |\mathcal{S}| \geqslant e^{-CK^C}|A|$$

and

$$\|\psi_{\mathcal{S}} 1_A\|_\infty \geqslant cK^{-C}.$$

Remark. We note that, unlike the usual Freiman theorem, it is clear how one might formulate a weak Freiman theorem in arbitrary (non-abelian) groups. We are not able to prove such a statement, and there seem to be significant difficulties in doing so. For example, there is no analogue of [11, Prop. 1.2] in general groups. See [9] for more details.

We begin by proving a result similar to Proposition 6.1 in what appears to be a special case: when A is a dense subset of a group G. We will show later on that the general case can be reduced to this one.

PROPOSITION 6.2 (Bogolyubov-Chang argument). *Let G be a finite abelian group, and suppose that $A \subseteq G$ is a set with $|A| = \alpha|G|$ and $|A+A| \leqslant K|A|$. Then there is a regular Bourgain system $\mathcal{S}$ with*

$$\dim(\mathcal{S}) \leqslant CK\log(1/\alpha), \qquad \|\psi_{\mathcal{S}} 1_A\|_\infty \geqslant 1/2K,$$
$$|\mathcal{S}| \geqslant (CK\log(1/\alpha))^{-CK\log(1/\alpha)}|G|$$

and

$$X_4 \subseteq 2A - 2A.$$

Proof. The argument is a variant due to Chang [3] of an old argument of Bogolyubov [2]. It is by now described in several places, including the book [25].

Set

$$\Gamma := \mathrm{Spec}_{1/4\sqrt{K}}(A) := \{\gamma \in \widehat{G} : |\widehat{1}_A(\gamma)| \geqslant \frac{\alpha}{4\sqrt{K}}\},$$

and take

$$\tilde{\mathcal{S}} = (\tilde{X}_\rho)_{\rho\in[0,4]} := \mathrm{Bohr}_{1/20}(\Gamma),$$

a Bohr system as defined in Definition 4.5. We claim that $\tilde{X}_4 \subseteq 2A-2A$. Recall from the definition that $\tilde{X}_4$ consists of those $x \in G$ for which $|1-\gamma(x)| \leqslant \frac{1}{5}$ for all $\gamma \in \Gamma$. Suppose then that $x \in \tilde{X}_4$. By the inversion formula we have

$$\begin{aligned}\|\widehat{1}_A\|_4^4 - 1_A * 1_A * 1_{-A} * 1_{-A}(x) &= \sum_\gamma |\widehat{1}_A(\gamma)|^4(1-\gamma(x))\\ &\leqslant \sum_{\gamma\in\Gamma} |\widehat{1}_A(\gamma)|^4|1-\gamma(x)| + \sum_{\gamma\notin\Gamma} |\widehat{1}_A(\gamma)|^4|1-\gamma(x)|\\ &\leqslant \frac{1}{5}\|\widehat{1}_A\|_4^4 + \frac{\alpha^2}{8K}\|1_A\|_2^2\\ &= \frac{1}{5}\|\widehat{1}_A\|_4^4 + \frac{\alpha^3}{8K}.\end{aligned}$$

However the fact that $|A+A| \leqslant K|A|$ implies, from Cauchy-Schwarz, that

$$\|\widehat{1}_A\|_4^4 = \|1_A * 1_A\|_2^2 \geqslant \alpha^3/K. \tag{6.1}$$

It follows that

$$\|\widehat{1}_A\|_4^4 - 1_A * 1_A * 1_{-A} * 1_{-A}(x) \leqslant (\frac{1}{5}+\frac{1}{8})\|\widehat{1}_A\|_4^4 < \|\widehat{1}_A\|_4^4.$$

Therefore $1_A * 1_A * 1_{-A} * 1_{-A}(x) > 0$; that is to say $x \in 2A-2A$.

Now we only have the dimension bound $\dim(\tilde{\mathcal{S}}) \leqslant 48K/\alpha$, which comes from the fact (a consequence of Parseval's identity) that $|\Gamma| \leqslant 16K/\alpha$. This is substantially weaker than the bound $CK\log(1/\alpha)$ that we require. To obtain the superior bound we must refine $\tilde{\mathcal{S}}$ to a somewhat smaller system $\mathcal{S}$. To do this we apply a well-known lemma of Chang [3], which follows from an inequality of Rudin [19]. See also [11], [25] for complete, self-contained proofs of this result. In our case the lemma states that there is a set $\Lambda \subseteq \widehat{G}$, $|\Lambda| \leqslant 32K\log(1/\alpha)$, such that $\Gamma \subseteq \langle\Lambda\rangle$. Here,

$$\langle\Lambda\rangle := \{\lambda_1^{\varepsilon_1}\dots\lambda_k^{\varepsilon_k} : \varepsilon_i \in \{-1,0,1\}\},$$

where $\lambda_1,\dots,\lambda_k$ is a list of the characters in Λ.

Now by repeated applications of the triangle inequality we see that

$$\mathrm{Bohr}_{1/20k}(\Lambda) \subseteq \mathrm{Bohr}_{1/20}(\langle\Lambda\rangle) \subseteq \mathrm{Bohr}_{1/20}(\Gamma).$$

Thus if we set

$$\mathcal{S} = (X_\rho)_{\rho\in[0,4]} := \mathrm{Bohr}_{\lambda/20k}(\Lambda),$$

where $\lambda \in [1/2,1]$ is chosen so that $\mathcal{S}$ is regular, then $X_4 \subseteq \tilde{X}_4 \subseteq 2A-2A$. It follows from Lemma 4.5 that $\dim(\mathcal{S}) \leqslant 72K\log(1/\alpha)$ and that

$$|\mathcal{S}| \geqslant (1/320k)^k|G| \geqslant (CK\log(1/\alpha))^{-CK\log(1/\alpha)}|G|,$$

as required.

It remains to show that $\|\psi_{\mathcal{S}}1_A\|_\infty \geqslant 1/2K$. Let us begin by noting that if $\gamma \in \Gamma$ and $x \in \widetilde{X}_2$ then $|1-\gamma(x)| \leqslant \frac{1}{10}$, and so if $\gamma \in \Gamma$ then $|\widehat{\beta}_1(\gamma)| \geqslant \frac{9}{10}$. It follows that

$$\begin{aligned}\|1_A * 1_A * \beta_1\|_2^2 &= \mathbb{E}1_A * 1_A * \beta_1(x)^2\\ &= \sum_\gamma |\widehat{1}_A(\gamma)|^4 |\widehat{\beta}_1(\gamma)|^2\\ &\geqslant \sum_{\gamma\in\Gamma} |\widehat{1}_A(\gamma)|^4 |\widehat{\beta}_1(\gamma)|^2 - \frac{\alpha^3}{16K}\\ &\geqslant \frac{3}{4}\sum_{\gamma\in\Gamma} |\widehat{1}_A(\gamma)|^4 - \frac{\alpha^3}{16K}\\ &\geqslant \frac{3}{4}\big(\|\widehat{1}_A\|_4^4 - \frac{\alpha^3}{16K}\big) - \frac{\alpha^3}{16K}\\ &\geqslant \alpha^3/2K,\end{aligned}$$

the last step following from (6.1). Since $\|1_A * 1_A * \beta_1\|_1 = \alpha^2$, it follows that

$$\|1_A * 1_A * \beta_1\|_\infty \geqslant \alpha/2K,$$

and hence that

$$\|\psi_{\mathcal{S}}1_A\|_\infty = \|1_A * \beta_1\|_\infty \geqslant 1/2K,$$

as required. □

Proof of Theorem 6.1. By [11, Prop. 1.2] there is an abelian group G', $|G'| \leqslant (CK)^{CK^2}|A|$, and a subset $A' \subseteq G'$ such that $A' \cong_{14} A$. We apply Proposition 6.2 to this set A'. Noting that $\alpha \geqslant (CK)^{-CK^2}$, we obtain a Bourgain system $\mathcal{S}' = (X'_\rho)_{\rho\in[0,4]}$ for which

$$\dim(\mathcal{S}') \leqslant CK^C; \qquad |\mathcal{S}'| \geqslant e^{-CK^C}|A'|; \qquad \|\psi_{\mathcal{S}'}1_{A'}\|_\infty \geqslant cK^{-C}$$

and

$$X'_4 \subseteq 2A' - 2A'.$$

Write $\phi : A' \to A$ for the Freiman 14-isomorphism between A' and A. The map ϕ extends to a well-defined 1-1 map on $kA' - lA'$ for any k, l with $k+l \leqslant 14$. By abuse of notation we write ϕ for any such map. In particular $\phi(0)$ is well-defined and we may define a "centred" Freiman 14-isomorphism $\phi_0(x) := \phi(x) - \phi(0)$.

Define $\mathcal{S} := \phi_0(\mathcal{S}')$. Since $X'_4 \subseteq 2A' - 2A'$, ϕ_0 is a Freiman 2-isomorphism on X'_4 with $\phi_0(0) = 0$. Therefore $\mathcal{S}$ is indeed a Bourgain system, with the same dimension and size as $\mathcal{S}'$.

It remains to check that $\|\psi_{\mathcal{S}}1_A\|_\infty \geqslant cK^{-C}$. The fact that $\|\psi_{\mathcal{S}'}1_{A'}\|_\infty \geqslant cK^{-C}$ means that there is x such that $|1_{A'} * \beta'_1(x)| \geqslant cK^{-C}$. Since $\mathrm{Supp}(\beta'_1) \subseteq X'_2 \subseteq X'_4 \subseteq 2A' - 2A'$, we must have $x \in 3A' - 2A'$. We claim that $1_A * \beta_1(\phi(x)) = 1_{A'} * \beta'_1(x)$, which clearly suffices to prove the result. Recalling the

definition of β_1, β_1', we see that this amounts to showing that the number of solutions to

$$x = a' - t_1' + t_2', \quad a' \in A', t_i' \in X_1',$$

is the same as the number of solutions to

$$\phi_0(x) = \phi_0(a') - \phi_0(t_1') + \phi_0(t_2'), \quad a' \in A', t_i' \in X_1'.$$

All we need check is that if $y \in 7A' - 7A'$ then $\phi_0(y) = 0$ only if $y = 0$. But since $0 \in 7A' - 7A'$, this follows from the fact that ϕ_0 is 1-1 on $7A' - 7A'$.

To conclude the section we note that Proposition 6.1 may be strengthened by combining it with the Balog-Szemerédi-Gowers theorem [6, Prop. 12] to obtain the following result.

PROPOSITION 6.3 (Weak Balog-Szemerédi-Gowers-Freiman). *Let A be a subset of an abelian group G, and suppose that there are at least $\delta|A|^3$ additive quadruples (a_1, a_2, a_3, a_4) in A^4 with $a_1 + a_2 = a_3 + a_4$. Then there is a regular Bourgain system $\mathcal{S}$ satisfying*

$$\dim(\mathcal{S}) \leqslant C\delta^{-C}; \qquad |\mathcal{S}| \geqslant e^{-C\delta^{-C}}|A|$$

and

$$\|\psi_{\mathcal{S}} 1_A\|_\infty \geqslant c\delta^C.$$

It might be conjectured that the first of these bounds can be improved to $\dim(\mathcal{S}) \leqslant C\log(1/\delta)$ and the second to $|\mathcal{S}| \geqslant c\delta^C|A|$. This might be called a *Weak Polynomial Freiman-Ruzsa Conjecture* by analogy with [7].

The final result of this section is the one we shall actually use in the sequel. It has the same form as Proposition 6.3, but in place of the condition that there are many additive quadruples we impose a condition which may appear rather strange at first sight, but is designed specifically with the application we have in mind in the next section.

If $A = \{a_1, \dots, a_k\}$ is a subset of an abelian group G then we say that A is *dissociated* if the only solution to $\varepsilon_1 a_1 + \cdots + \varepsilon_k a_k = 0$ with $\varepsilon_i \in \{-1, 0, 1\}$ is the trivial solution in which $\varepsilon_i = 0$ for all i. Recall also that $\langle A \rangle$ denotes the set of all sums $\varepsilon_1 a_1 + \cdots + \varepsilon_k a_k$ with $\varepsilon_i \in \{-1, 0, 1\}$ for all i.

Definition 6.4 (Arithmetic connectedness). Suppose that $A \subseteq G$ is a set with $0 \notin A$ and that $m \geqslant 1$ is an integer. We say that A is *m-arithmetically connected* if, for any set $A' \subseteq A$ with $|A'| = m$ we have either

(i) A' is not dissociated or

(ii) A' is dissociated, and there is some $x \in A \setminus A'$ with $x \in \langle A' \rangle$.

PROPOSITION 6.5 (Arithmetic connectedness and Bourgain systems). *Suppose that $m \geqslant 1$ is an integer, and that a set A in some abelian group G*

is m-arithmetically connected. Suppose that $0 \notin A$. Then there is a regular Bourgain system $\mathcal{S}$ satisfying

$$\dim(\mathcal{S}) \leqslant e^{Cm}; \qquad |\mathcal{S}| \geqslant e^{-e^{Cm}}|A|$$

and

$$\|\psi_{\mathcal{S}} 1_A\|_\infty \geqslant e^{-Cm}.$$

Proof. By Proposition 6.3, it suffices to prove that an m-arithmetically connected set A has at least $e^{-Cm}|A|^3$ additive quadruples. If $|A| < m^2$ this result is trivial, so we stipulate that $|A| \geqslant m^2$. Pick any m-tuple $(a_1, ..., a_m)$ of distinct elements of A. With the stipulated lower bound on $|A|$, there are at least $|A|^m/2$ such m-tuples. We know that either the vectors $a_1, ..., a_m$ are not dissociated, or else there is a further $a' \in A$ such that a' lies in the linear span of the a_i. In either situation there is some nontrivial linear relation

$$\lambda_1 a_1 + \cdots + \lambda_m a_m + \lambda' a' = 0$$

where $\vec{\lambda} := (\lambda_1, \ldots, \lambda_m, \lambda')$ has elements in $\{-1, 0, 1\}$ and, since $0 \notin A$ and the a_is (and a') are distinct, at least three of the components of $\vec{\lambda}$ are nonzero. By the pigeonhole principle, it follows that there is some $\vec{\lambda}$ such that the linear equation

$$\lambda_1 x_1 + \cdots + \lambda_m x_m + \lambda' x' = 0$$

has at least $\frac{1}{2\cdot 3^{m+1}}|A|^m$ solutions with $x_1, ..., x_m, x' \in A$. Removing the zero coefficients, we may thus assert that there are some nonnegative integers r_1, r_2, $3 \leqslant r_1 + r_2 \leqslant m + 1$, such that the equation

$$x_1 + \cdots + x_{r_1} - y_1 - \cdots - y_{r_2} = 0$$

has at least $\frac{1}{6m^2 3^m}|A|^{r_1+r_2-1} \geqslant e^{-Cm}|A|^{r_1+r_2-1}$ solutions with $x_1, \ldots, x_{r_1}$, $y_1, \ldots, y_{r_2} \in A$. Note that this is a strong structural statement about A, since the maximum possible number of solutions to such an equation is $|A|^{r_1+r_2-1}$.

We may deduce directly from this the claim that there are at least $e^{-C'm}|A|^3$ additive quadruples in A. To do this observe that what we have shown may be recast in the form

$$1_A * \cdots * 1_A * 1_{-A} * \cdots * 1_{-A}(0) \geqslant e^{-Cm}\|1_A\|_1^{r_1+r_2-1},$$

where there are r_1 copies of 1_A and r_2 copies of 1_{-A}. Writing this in terms of the Fourier transform gives

$$\|\widehat{1}_A\|_{r_1+r_2}^{r_1+r_2} \geqslant \sum_\gamma \widehat{1}_A(\gamma)^{r_1}\widehat{1}_A(\overline{\gamma})^{r_2} \geqslant e^{-Cm}\|1_A\|_1^{r_1+r_2-1}.$$

By Hölder's inequality this implies that

$$\|\widehat{1}_A\|_4^2 \|\widehat{1}_A\|_{2r_1+2r_2-4}^{r_1+r_2-2} \geqslant e^{-Cm}\|1_A\|_1^{r_1+r_2-1}. \tag{6.2}$$

However if k is an integer then $\|\widehat{1}_A\|_{2k}^{2k}$ is $|G|^{1-2k}$ times the number of solutions to $a_1 + \cdots + a_k = a_1' + \cdots + a_k'$ with $a_i, a_i' \in A$, and this latter quantity is clearly at most $|A|^{2k-1}$. Thus

$$\|\widehat{1}_A\|_{2k} \leqslant \|1_A\|_1^{1-1/2k}.$$

(In fact, the same is true if $2k \geqslant 2$ is any real number, by the Hausdorff-Young inequality and the fact that f is bounded by 1.) Setting $k = r_1 + r_2 - 2$ and substituting into (6.2), we immediately obtain

$$\|\widehat{1}_A\|_4^4 \geqslant e^{-2Cm}\|1_A\|_1^3,$$

which is equivalent to the result we claimed about the number of additive quadruples in A. □

7. Concentration on a Bourgain system

PROPOSITION 7.1. *Suppose that $f : G \to \mathbb{R}$ has $\|f\|_A \leqslant M$, $M \geqslant 1/2$, and $d(f, \mathbb{Z}) \leqslant e^{-CM^4}$. Then there is a regular Bourgain system $\mathcal{S}$ with*

$$\dim(\mathcal{S}) \leqslant e^{CM^4}, \qquad \mu(\mathcal{S}) \geqslant e^{-e^{CM^4}}\|f_{\mathbb{Z}}\|_1$$

and

$$\|\psi_{\mathcal{S}} f\|_\infty \geqslant e^{-CM^4}.$$

Proof. We first obtain a similar result with $g := f^2$ replacing f. This function, of course, has the advantage of being nonnegative. Note that $\|g\|_A \leqslant M^2$, and also that

$$\|g - f_{\mathbb{Z}}^2\|_\infty \leqslant \|f - f_{\mathbb{Z}}\|_\infty \|f + f_{\mathbb{Z}}\|_\infty \leqslant d(f, \mathbb{Z})(2\|f\|_A + 1) \leqslant 4Md(f, \mathbb{Z}),$$

and so $d(g, \mathbb{Z}) \leqslant 4Md(f, \mathbb{Z})$.

Write $A := \mathrm{Supp}(g_{\mathbb{Z}})$, and $m := \lceil 50M^4 \rceil$. If $A = G$ the result is trivial; otherwise, by subjecting f to a suitable translation we may assume without loss of generality that $0 \notin A$. We claim that A is m-arithmetically connected. If this is not the case then there are dissociated elements $a_1, \ldots, a_m \in A$ such that there is no further $x \in A$ lying in the span $\langle a_1, \ldots, a_m \rangle$. Consider the function $p(x)$ defined using its Fourier transform by the Riesz product

$$\widehat{p}(\gamma) := \prod_{i=1}^m (1 + \frac{1}{2}(\gamma(a_i) + \overline{\gamma}(a_i))).$$

It is easy to check that p enjoys the standard properties of Riesz products, namely that $\widehat{p}$ is real and nonnegative and that $\|p\|_A = \sum_\gamma \widehat{p}(\gamma) = 1$, and that $\mathrm{Supp}(p) \subseteq \langle a_1, \ldots, a_m \rangle$.

Thus we have

$$\|gp\|_A \leqslant \|g\|_A \|p\|_A \leqslant M^2$$

and

$$\|(g-g_{\mathbb{Z}})p\|_A \leqslant \sum_{x\in\langle a_1,\dots,a_m\rangle} \|(g-g_{\mathbb{Z}})p1_x\|_A \leqslant 3^m\|g-g_{\mathbb{Z}}\|_\infty \leqslant 4M3^m d(f,\mathbb{Z}).$$

Now, since $d(f,\mathbb{Z})$ is so small, we have

$$\|g_{\mathbb{Z}}p\|_A \leqslant 2M^2.$$

Next, since $A\cap\langle a_1,\dots,a_m\rangle = \{a_1,\dots,a_m\}$,

$$g_{\mathbb{Z}}p(x) = \sum_{i=1}^m g_{\mathbb{Z}}(a_i)p(a_i)1_{a_i}(x).$$

Noting that

$$p(a_i) = \sum_{\vec{\varepsilon}:\varepsilon_1a_1+\cdots+\varepsilon_ma_m=a_i} 2^{-\sum_j|\varepsilon_j|} \geqslant \frac{1}{2},$$

we see that

$$\|\widehat{g_{\mathbb{Z}}p}\|_2^2 = \|g_{\mathbb{Z}}p\|_2^2 \geqslant \frac{1}{4|G|}\sum_{i=1}^m |g_{\mathbb{Z}}(a_i)|^2 \geqslant \frac{m}{4|G|}$$

and

$$\begin{aligned}\|\widehat{g_{\mathbb{Z}}p}\|_4^4 &= \frac{1}{|G|^3}\sum_{\substack{i_1,i_2,i_3,i_4\\ a_{i_1}+a_{i_2}=a_{i_3}+a_{i_4}}} |g_{\mathbb{Z}}(a_i)p(a_i)|^4\\ &\leqslant \frac{3}{|G|^3}\Big(\sum_{i=1}^m |g_{\mathbb{Z}}(a_i)p(a_i)|^2\Big)^2 \leqslant \frac{3}{|G|}\|\widehat{g_{\mathbb{Z}}p}\|_2^4,\end{aligned}$$

the middle inequality following from the fact that $a_{i_1}+a_{i_2}=a_{i_3}+a_{i_4}$ only if $i_1=i_3, i_2=i_4$ or $i_1=i_4, i_2=i_3$ or $i_1=i_2, i_3=i_4$. From Hölder's inequality we thus obtain

$$\|g_{\mathbb{Z}}p\|_A \geqslant \frac{\|\widehat{g_{\mathbb{Z}}p}\|_2^3}{\|\widehat{g_{\mathbb{Z}}p}\|_4^2} \geqslant \sqrt{\frac{|G|}{3}}\|\widehat{g_{\mathbb{Z}}p}\|_2 \geqslant \sqrt{\frac{m}{12}}.$$

Recalling our choice of m, we see that this contradicts the upper bound $\|g_{\mathbb{Z}}p\|_A \leqslant 2M^2$ we obtained earlier.

This proves our claim that $A=\mathrm{Supp}(g_{\mathbb{Z}})$ is $50M^4$-arithmetically connected. It follows from Proposition 6.5 that there is a regular Bourgain system $\mathcal{S}=(X_\rho)_{\rho\in[0,4]}$ with

$$\dim(\mathcal{S}) \leqslant e^{CM^4}, \qquad |\mathcal{S}| \geqslant e^{-e^{CM^4}}|A| \tag{7.1}$$

and

$$\|\psi_{\mathcal{S}}1_A\|_\infty \geqslant e^{-CM^4}.$$

Since $\|f\|_\infty \leqslant M$, the second of these implies that

$$\mu(\mathcal{S}) \geqslant e^{-e^{C'M^4}}\|f_{\mathbb{Z}}\|_1. \tag{7.2}$$

Since $g(x) \geqslant 1_A(x)/2$, the last of these implies that

$$\|\psi_{\mathcal{S}} g\|_\infty \geqslant e^{-CM^4}. \tag{7.3}$$

It remains to convert these facts about g to the required facts about f. The corresponding argument in [12] (which comes near the end of Proposition 5.1) is rather short, but in the setting of a general Bourgain system we must work a little harder.

We have proved (7.3), which implies the existence of an x such that

$$|\mathbb{E}_y f(y)^2 \beta_1(x-y)| = \delta,$$

for some $\delta \geqslant e^{-CM^4}$. Writing this in terms of the Fourier transform we have

$$|\sum_\gamma (f(\cdot)\beta_1(x-\cdot))^\wedge(\gamma)\widehat{f}(\gamma)| = \delta$$

which, since $\|f\|_A \leqslant M$, implies that there is a $\gamma \in \widehat{G}$ such that

$$|(f(\cdot)\beta_1(x-\cdot))^\wedge(\gamma)| \geqslant \delta/M,$$

or in other words

$$|\mathbb{E}_y f(y)\beta_1(y-x)\gamma(y)| \geqslant \delta/M. \tag{7.4}$$

Now define

$$\mathcal{S}' := \lambda\big(\frac{\delta}{80dM^2}\mathcal{S} \cap \mathrm{Bohr}_{\delta/8M^2}(\{\gamma\})\big),$$

where as usual $\lambda \in [1/2, 1]$ is chosen so that $\mathcal{S}'$ is regular. Now since $\mathrm{Supp}(\beta_1') \subseteq X_{\delta/40dM^2}$ we have from Lemma 4.13 that

$$\|\beta_1 * \beta_1' - \beta_1\|_1 = \mathbb{E}_x\big|\mathbb{E}_y \beta_1'(y)(\beta_1(x-y) - \beta_1(x))\big| \leqslant \delta/2M^2.$$

Since $\|f\|_\infty \leqslant \|f\|_A \leqslant M$ we may introduce an averaging over β_1' into (7.4), obtaining

$$|\mathbb{E}_y f(y)\gamma(y)\mathbb{E}_t \beta_1(y+t-x)\beta_1'(t)| \geqslant \delta/2M. \tag{7.5}$$

Now if $t \in \mathrm{Supp}(\beta_1')$ then by construction,

$$|1-\gamma(t)| \leqslant \delta/4M^2,$$

and so from (7.5) and the fact that $\|f\|_\infty \leqslant M$ we see that

$$|\mathbb{E}_y f(y)\gamma(y+t)\mathbb{E}_t \beta_1(y+t-x)\beta_1'(t)| \geqslant \delta/4M.$$

Changing variables by writing $z := y+t-x$ and noting that $|\gamma(x)| = 1$, we may write

$$|\mathbb{E}_z \beta_1(z)\gamma(z)\mathbb{E}_y f(y)\beta_1'(z+x-y)| \geqslant \delta/4M,$$

which immediately implies that

$$\|\psi_{\mathcal{S}'} f\|_\infty \geqslant \delta/4M \geqslant e^{-C'M^4}.$$

To conclude the argument we must show that $\mathcal{S}'$ is subject to the same bounds (7.1), (7.2) (possibly with different constants C). This follows easily from Lemma 4.10 and the bounds of Lemma 4.6. □

8. The inductive step

Our remaining task is to prove Lemma 3.1, the inductive step which drives the proof of Theorem 1.3. We recall the statement of that lemma now for the reader's convenience.

LEMMA 3.1 (Inductive Step). *Suppose that $f : G \to \mathbb{R}$ has $\|f\|_A \leqslant M$, where $M \geqslant 1$, and that $d(f,\mathbb{Z}) \leqslant e^{-C_1 M^4}$. Set $\varepsilon := e^{-C_0 M^4}$, for some constant C_0. Then $f = f_1 + f_2$, where*

(i) *either $\|f_1\|_A \leqslant \|f\|_A - 1/2$ or else $(f_1)_{\mathbb{Z}}$ may be written as $\sum_{j=1}^{L} \pm 1_{x_j+H}$, where H is a subgroup of G and $L \leqslant e^{e^{C'(C_0)M^4}}$;*

(ii) *$\|f_2\|_A \leqslant \|f\|_A - \frac{1}{2}$ and*

(iii) *$d(f_1,\mathbb{Z}) \leqslant d(f,\mathbb{Z}) + \varepsilon$ and $d(f_2,\mathbb{Z}) \leqslant 2d(f,\mathbb{Z}) + \varepsilon$.*

Remark. Note carefully the factor 2 in the bound for $d(f_2,\mathbb{Z})$; this is one important reason for the weakness of our bounds in Theorem 1.3.

Proof. Applying Proposition 7.1 to f we obtain a regular Bourgain system $\mathcal{S}$ with

$$d = \dim(\mathcal{S}) \leqslant e^{CM^4}, \qquad \mu(\mathcal{S}) \geqslant e^{-e^{CM^4}} \|f_{\mathbb{Z}}\|_1$$

and

$$\|\psi_{\mathcal{S}} f\|_\infty \geqslant 3e^{-CM^4}.$$

We were given that $\varepsilon = e^{-C_0 M^4}$ in the statement of the proposition. Without loss of generality (by increasing C_0) we may assume that C_0 is much larger than the constant C in the bounds just given.

Applying Proposition 5.1 with this value of ε we obtain a regular Bourgain system $\mathcal{S}' = (X'_\rho)_{\rho\in[0,4]}$ such that

$$\dim(\mathcal{S}') \leqslant e^{C'M^4}, \qquad \mu(\mathcal{S}') \geqslant e^{-e^{C'M^4}} \|f_{\mathbb{Z}}\|_1 \tag{8.1}$$

and

$$\|\psi_{\mathcal{S}'} f\|_\infty \geqslant \|\psi_{\mathcal{S}} f\|_\infty - \varepsilon > 2e^{-CM^4}, \tag{8.2}$$

and with the additional property that

$$d(\psi_{\mathcal{S}'} f, \mathbb{Z}) \leqslant d(f,\mathbb{Z}) + \varepsilon. \tag{8.3}$$

Here, $C' = C'(C_0)$ depends only on C_0. We define $f_1 := \psi_{\mathcal{S}'} f$ and $f_2 := f - \psi_{\mathcal{S}'} f$. Thus we immediately see that $d(f_1,\mathbb{Z}) \leqslant d(f,\mathbb{Z}) + \varepsilon$, which is one part of (iii), and the other inequality $d(f_2,\mathbb{Z}) \leqslant 2d(f,\mathbb{Z}) + \varepsilon$ follows immediately from this.

Note also that (8.2) and the fact that $d(f_1,\mathbb{Z}) \leqslant d(f,\mathbb{Z}) + \varepsilon < 2e^{-CM^4}$ implies that $(f_1)_{\mathbb{Z}}$ is not identically zero, and therefore $\|f_1\|_\infty \geqslant \|(f_1)_{\mathbb{Z}}\|_\infty - \varepsilon$

$> 1/2$, and hence $\|f_1\|_A \geqslant \frac{1}{2}$. It follows that $\|f_2\|_A \leqslant \|f\|_A - \frac{1}{2}$, as we were required to prove.

It remains to deal with the possibility that $\|f_1\|_A > \|f\|_A - \frac{1}{2}$. If this is so then $\|f_2\|_A < 1/2$, and thus $\|f_2\|_\infty < 1/2$. Now, $(f_2)_{\mathbb{Z}} = 0$, and hence $f_{\mathbb{Z}} = (\psi_{\mathcal{S}'} f)_{\mathbb{Z}}$.

Next, suppose that $x - x' \in X'_{\varepsilon/20dM}$. Then from Lemma 4.15 and (8.3) we see that

$$\begin{aligned}|f_{\mathbb{Z}}(x) - f_{\mathbb{Z}}(x')| &= |(\psi_{\mathcal{S}'} f)_{\mathbb{Z}}(x) - (\psi_{\mathcal{S}'} f)_{\mathbb{Z}}(x')| \\ &\leqslant |\psi_{\mathcal{S}'} f(x) - \psi_{\mathcal{S}'} f(x')| + 2(d(f,\mathbb{Z}) + \varepsilon) \leqslant 2d(f,\mathbb{Z}) + 3\varepsilon < 1/10.\end{aligned}$$

We are forced to conclude that $f_{\mathbb{Z}}(x) = f_{\mathbb{Z}}(x')$. It follows immediately that $f_{\mathbb{Z}}$ is constant on cosets of the subgroup $H := \langle X_{\varepsilon/20dM} \rangle$, and so

$$f_{\mathbb{Z}} = \sum_{j=1}^{L} \pm 1_{x_j + H}$$

for some $j = 1, \dots, L$, where we may take

$$L \leqslant M\|f_{\mathbb{Z}}\|_1 / \|1_H\|_1.$$

Let us note from property BS5 of Bourgain systems that

$$\|1_H\|_1 \geqslant \frac{|X_{\varepsilon/20dM}|}{|G|} \geqslant \big(\frac{\varepsilon}{40dM}\big)^d \mu(\mathcal{S}').$$

From this and (8.1) we have

$$L \leqslant e^{e^{C'' M^4}},$$

where $C'' = C''(C_0)$ depends only on C_0, as required. □

9. Possible improvements

As it stands, our argument "loses an exponential" in two places. First of all the "almost integer" parameter $d(f,\mathbb{Z})$ must not be allowed to blow up during the iteration leading to the proof of Theorem 1.3. This requires it to be exponentially small in M at the beginning of the argument. This parameter then gets exponentiated again in any application of Proposition 5.1.

We note that our proof in fact yields a version of Theorem 1.3 for functions f satisfying $d(f,\mathbb{Z}) \leqslant e^{-CM^4}$, rather than simply $d(f,\mathbb{Z}) = 0$. Such functions are within $d(f,\mathbb{Z})$ of a sum $\sum_{j=1}^{L} \pm 1_{x_j + H_j}$. Now an example of Méla [18] shows that, for such a theorem to hold, $d(f,\mathbb{Z})$ must be exponentially small in M. It seems then that, as long as our proof technique also establishes this more general result, the bound we can hope to obtain is seriously restricted.

The function $f := 1_{\{1,\dots,N\}}$ on the group $G = \mathbb{Z}$ has $\|f\|_A \sim \log N$, yet it cannot be written as the $\pm$-sum of fewer than N cosets in $\mathbb{Z}$. This shows

that the bound of Theorem 1.2 cannot be improved beyond $L \leqslant e^{C\|\mu\|}$ in general. It may be that this represents the correct bound. Note that this would immediately provide another proof of the Littlewood conjecture, to add to the famous papers of Konyagin[16] and McGehee, Pigno and Smith [17]. Recall that this conjecture was the following statement: if $A \subseteq \mathbb{Z}$ is a set of size N then

$$\int_0^1 \big|\sum_{a\in A} e^{2\pi i\theta a}\big|\, d\theta \gg \log N.$$

Our results imply the weaker inequality

$$\int_0^1 \big|\sum_{a\in A} e^{2\pi i\theta a}\big|\, d\theta \gg (\log\log N)^{1/4},$$

easily the weakest bound ever obtained in the direction of the Littlewood conjecture!

Appendix A. Reduction of Theorem 1.2 to the finite case

Throughout the section G will be a locally compact abelian group; here, we deduce Theorem 1.2 from Theorem 1.3. As we remarked, this section is independent of the rest of the paper. It is also not self-contained, and in particular we assume the (qualitative) idempotent theorem. The reader may safely think of the case $G = \mathbb{T}^d$, $\widehat{G} = \mathbb{Z}^d$, which captures the essence of the argument and may be thought of in quite concrete terms.

We begin by proving the following special case of Theorem 1.2.

Proposition A.1 (The finite case). *Suppose that G is compact, and that $\mu \in \mathbf{M}(G)$ satisfies $\|\mu\| \leqslant M$ and has the form*

$$\widehat{\mu} = \sum_{j=1}^{K} \pm 1_{\gamma_j}.$$

Then

$$\widehat{\mu} = \sum_{l=1}^{L} \pm 1_{\gamma_l' + \Gamma_l},$$

where $L \leqslant e^{e^{CM^4}}$, each Γ_l is a subgroup of $\widehat{G}$ and there are at most $\|\mu\| + \frac{1}{100M}$ different groups Γ_l.

Proof. We may suppose that $\widehat{G} = \langle \gamma_1, \dots, \gamma_K\rangle$. By the structure theorem for finitely-generated abelian groups, $\widehat{G}$ is isomorphic to $\widehat{H} \times \mathbb{Z}^d$, where H is finite. We may now explicitly describe the characters γ_j as

$$\gamma_j = (\omega^{(j)}, r_1^{(j)}, \dots, r_d^{(j)}),$$

where $\omega^{(j)} \in \widehat{H}$ and the $r_i^{(j)}$ are integers.

Let $N = N(K)$ be an enormous prime and define the measure $\widetilde{\mu}$ on $H \times (\mathbb{Z}/N\mathbb{Z})^d$ by

$$\widetilde{\mu}(h, x_1, \dots, x_d) := \sum_{j=1}^{K} \omega^{(j)}(h) e\big(\frac{r_1^{(j)} x_1 + \dots + r_d^{(j)} x_d}{N}\big).$$

It is clear that

$$\lim_{N\to\infty} \|\widetilde{\mu}\| = \lim_{N\to\infty} \mathbb{E}_{h\in H, x_1,\dots,x_d \in \mathbb{Z}/N\mathbb{Z}} \big| \sum_{j=1}^{K} \omega^{(j)}(h) e\big(\frac{r_1^{(j)} x_1 + \dots + r_d^{(j)} x_d}{N}\big)\big|$$

$$= \mathbb{E}_h \int_{\theta_1,\dots,\theta_d \in \mathbb{T}^d} \big| \sum_{j=1}^{K} \omega^{(j)}(h) e(r_1^{(j)}\theta_1 + \dots + r_d^{(j)}\theta_d)\big| \, d\theta_1 \dots d\theta_d = \|\mu\|.$$

Taking N large enough, we may assume that $\|\widetilde{\mu}\| \leqslant \|\mu\| + \frac{1}{200M}$.

Theorem 1.3 now applies[1] with $f := \widehat{\widetilde{\mu}}$ to show that

$$\widehat{\widetilde{\mu}} = \sum_{l=1}^{L} \pm 1_{\gamma_l' + \Gamma_l}, \tag{A.1}$$

where the Γ_l are subgroups of $\widehat{H} \times (\mathbb{Z}/N\mathbb{Z})^d$, $L \leqslant e^{e^{CM^4}}$, and we may assume the number of distinct Γ_l is at most

$$\|\widetilde{\mu}\| + \frac{1}{200M} \leqslant \|\mu\| + \frac{1}{100M}.$$

Let $\pi : \widehat{H} \times (\mathbb{Z}/N\mathbb{Z})^d \to \widehat{H}$ be the obvious projection, and for each group Γ_l appearing in the decomposition (A.1) consider the subgroup $\Gamma_l \cap \ker \pi$. Suppose without loss of generality that $|\Gamma_1 \cap \ker \pi| \geqslant |\Gamma_l \cap \ker \pi|$ for $l = 1, \dots, L$, and also that $\Gamma_1 \cap \ker \pi = \Gamma_l \cap \ker \pi$ precisely for $l = 1, \dots, m$.

We clearly have $|\Gamma_1 \cap \ker \pi| = N^{d'}$ for some d', $0 \leqslant d' \leqslant d$. Suppose that $d' \geqslant 1$. The portion $\sum_{l=1}^{m} \pm 1_{\gamma_l' + \Gamma_l}$ is constant on cosets of $\Gamma_1 \cap \ker \pi$. If this portion is zero then we may simply delete it from (A.1). Suppose, then, that it is not zero. We note that if $l \in \{1, \dots, m\}$ and $k \notin \{1, \dots, m\}$ then

$$|(\gamma_l' + \Gamma_l) \cap (\gamma_k' + \Gamma_k)| \leqslant |H| N^{d'-1}.$$

We therefore have the estimate

$$\|\sum_{l=1}^{L} \pm 1_{\gamma_l' + \Gamma_l}\|_1 \geqslant |\Gamma_1 \cap \ker \pi| - |H| N^{d'-1} m(L-m) \geqslant N^{d'} - |H| N^{d'-1} m(L-m).$$

[1] In fact, this is not quite true. Theorem 1.3 stated a weaker bound of $\|\widetilde{\mu}\| + \frac{1}{100}$ on the number of distinct Γ_j, but that was done only for clarity and it is clear that a trivial modification of the proof gives this somewhat stronger bound while preserving the upper bound on L.

If N is chosen large enough this gives us

$$\|\sum_{l=1}^{L} \pm 1_{\gamma_l' + \Gamma_l}\|_1 > K.$$

However by definition $\widehat{\widehat{\mu}}$ is the characteristic function of a set of K characters, and so we have a contradiction.

It follows that we may assume $d' = 0$, in which case all of the subgroups Γ_l appearing in (A.1) are simply subgroups of $\widehat{H}$. The decomposition (A.1) may then be regarded as a decomposition of $\widehat{\mu}$ as well, and we have proved our result. □

It remains to reduce to the finite case covered in this last proposition. Let $\mu \in \mathbf{M}(G)$ be an arbitrary idempotent measure, and write $M := \|\mu\|$. The idempotent theorem implies that $\widehat{\mu}$ may be written as a finite combination

$$\widehat{\mu} = \sum_{k \in E} \pm 1_{\gamma_k + \Gamma_k}.$$

We say that two open subgroups Γ_k, Γ_l are *commensurable* if $|\Gamma_k : \Gamma_k \cap \Gamma_l|, |\Gamma_l : \Gamma_k \cap \Gamma_l| < \infty$; this is an equivalence relation. Split E into a disjoint union $E_1 \cup \cdots \cup E_J$ of equivalence classes. We have

$$\widehat{\mu} = \sum_{k=1}^{K} \pm 1_{\gamma_k + \Gamma_k} = \sum_{j=1}^{J} \sum_{k \in E_j} \pm 1_{\gamma_k + \Gamma_k}.$$

Writing $\Omega_j := \bigcap_{k \in E_j} \Gamma_k$ and noting that $|\Gamma_k : \Omega_j| < \infty$ for $k \in E_j$, we obtain this in the form

$$\widehat{\mu} = \sum_{j=1}^{J} \sum_{k \in E_j'} \pm 1_{\gamma_k + \Omega_j},$$

where the index sets E_j' are still finite and the open subgroups Ω_j, $j = 1, \ldots, J$, are mutually incommensurable. It follows that

$$\mu = \sum_{j=1}^{J} \mu_j,$$

where

$$\mu_j(x) := \sum_{k \in E_j'} \pm \gamma_k(x) \mu_{H_j}(x).$$

Here, μ_{H_j} is the Haar measure on the compact group $H_j := \Omega_j^{\perp}$. The incommensurability of the H_j implies that

$$\|\mu\| = \sum_{j=1}^{J} \|\mu_j\|.$$

The measures μ_j need not be idempotent, but their Fourier-Stieltjes transforms are, by construction, integer-valued. We may of course suppose that no μ_j is zero, and hence we have the upper bound $J \leqslant \|\mu\| = M$.

We may now simply apply Proposition A.1 to μ_j which, when regarded as a measure on H_j, is of the form covered by that proposition.

Once this is done, we shall have written $\widehat{\mu}$ as a sum

$$\widehat{\mu} = \sum_{q=1}^{Q} \pm 1_{\gamma_q + \Gamma_q}$$

where

$$Q \leqslant Je^{e^{CM^4}} \leqslant e^{e^{C'M^4}}$$

and the number of distinct Γ_q is bounded by

$$\sum_{j=1}^{J} \big(\|\mu_j\| + \frac{1}{100M}\big) \leqslant \|\mu\| + \frac{1}{100}.$$

This concludes the proof of Theorem 1.2. □

Centre for Mathematical Sciences, Cambridge, England
E-mail addresses: b.j.green@dpmms.cam.ac.uk
t.sanders@dpmms.cam.ac.uk

References

[1] J. Bourgain, On triples in arithmetic progression, *Geom. Funct. Anal.* **9** (1999), 968–984.

[2] N. N. Bogolyubov, Sur quelques propriétés arithmétiques des presque-périodes, *Ann. Chaire Math. Phys. Kiev* **4** (1939), 185–194.

[3] M.-C. Chang, A polynomial bound in Freiman's theorem, *Duke Math. J.* **113** (2002), 399–419.

[4] P. J. Cohen, On a conjecture of Littlewood and idempotent measures, *Amer. J. Math.* **82**, (1960), 191–212.

[5] H. T. Croft, *Some Problems,* Eureka, Cambridge Univ. Cambridge, 1968.

[6] W. T. Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four, *Geom. Funct. Anal.* **8** (1998), 529–551.

[7] B. J. Green, Finite field models in additive combinatorics, in *Surveys in Combinatorics* 2005, *London Math. Soc. Lecture Notes* **327**, 1–27.

[8] ———, A Szemerédi-type regularity lemma in abelian groups, with applications, *Geom. Funct. Anal.* **15** (2005), 340–376.

[9] ———, On Freiman models, in preparation.

[10] B. J. Green and S. V. Konyagin, The Littlewood problem modulo a prime, *Canadian J. Math.*, to appear.

[11] B. J. Green and I. Z. Ruzsa, An analogue of Freiman's theorem in an arbitrary abelian group, *J. London Math. Soc.* **75** (2007), 163–175.

[12] B. J. Green and T. Sanders, Boolean functions with small spectral norm, *Geom. Funct. Anal.* **18** (2008), 144–162.

[13] B. J. Green and T. C. Tao, An inverse theorem for the Gowers U^3-norm, with applications, *Proc. Edinburgh Math. Soc.* **51** (2008), 73–153.

[14] J. Heinonen, *Lectures on Analysis on Metric Spaces*, Springer Universitext 2001.

[15] H. Helson, Note on harmonic functions, *Proc. Amer. Math. Soc.* **4** (1953), 686–691.

[16] S. V. Konyagin, On the Littlewood problem (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **45** (1981), 243–265, 463; English translation in *Math. USSR Izvestija* **18** (1982), 205–225.

[17] O. C. McGehee, L. Pigno, and B. Smith, Hardy's inequality and the L^1 norm of exponential sums, *Ann. of Math.* **113** (1981), 613–618.

[18] J. -F. Méla, Mesures ε-idempotentes de norme bornée, *Studia Math.* **72** (1982), 131–149.

[19] W. Rudin, *Fourier Analysis on Groups*, 2nd edition, John Wiley & Sons, New York, 1990.

[20] ———, Idempotent measures on abelian groups, *Pacific J. Math.* **9** (1959), 195–209.

[21] T. Sanders, An application of a local version of Chang's theorem, preprint; available at `http://www.arxiv.org/abs/math.CA/0607668`.

[22] ———, The Littlewood-Gowers problem, preprint, *J. Anal. Math.* **101** (2007), 123–162.

[23] I. D. Shkredov, On a generalization of Szemerédi's theorem, *Proc. London Math. Soc.* **93** (2006), 723–760.

[24] T. C. Tao, The Roth-Bourgain theorem, "Short story" available at `http://www.math.ucla.edu/~tao`.

[25] T. C. Tao and V. H. Vu, *Additive Combinatorics, Cambridge Studies in Adv. Math.* **105**, Cambridge Univ. Press, Cambridge, 2006.

(Received December 1, 2006)