GAFA Geometric And Functional Analysis

BOOLEAN FUNCTIONS WITH SMALL SPECTRAL NORM

BEN GREEN AND TOM SANDERS

Abstract. Let $f : \mathbb{F}_2^n \to \{0, 1\}$ be a boolean function, and suppose that the *spectral norm* $\|f\|_A := \sum_r |\widehat{f}(r)|$ of f is at most M. Then

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

where $L \leqslant 2^{2^{CM^4}}$ and each H_j is a subgroup of $\mathbb{F}_2^n$.

This result may be regarded as a quantitative analogue of the Cohen–Helson–Rudin structure theorem for idempotent measures in locally compact abelian groups.

1 Introduction

Let $G = \mathbb{F}_2^n$ be the n-dimensional cube, and let $f : G \to \{0, 1\}$ be a boolean function, or more generally a function from G to $\mathbb{R}$. In many works, particularly in theoretical computer science, the Fourier transform

$$\widehat{f}(r) := \mathbb{E}_{x \in G} f(x)(-1)^{r^T x} = \frac{1}{|G|} \sum_{x \in G} f(x)(-1)^{r^T x}$$

is considered. Here, r lies in the dual group $\widehat{G}$ which we have identified with G by choosing the scalar product $u^T v$.

It is natural to consider the ℓ^p-norms

$$\|\widehat{f}\|_p := \Big(\sum_{r \in \widehat{G}} |\widehat{f}(r)|^p \Big)^{1/p},$$

for $1 \leqslant p < \infty$, as well as the ℓ^∞-norm $\|\widehat{f}\|_\infty := \sup_r |\widehat{f}(r)|$.

There are many tools available for analysing these norms when $p \geqslant 2$, particularly when p is ∞ or an even integer. When $1 \leqslant p < 2$, however, the situation is in many ways rather mysterious. Of these cases, a very natural one is the endpoint $p = 1$. In this case the norm $\|\widehat{f}\|_1$ is called the *algebra norm*, *Wiener norm* or *spectral norm*; we shall denote it by $\|f\|_A$. It is quite easy to show, using an instance of Young's inequality for convolutions, that

$$\|fg\|_A \leqslant \|f\|_A \|g\|_A$$

for any two functions $f, g : G \to \mathbb{R}$. This explains the term *algebra norm*.

A basic question is the following.

QUESTION 1.1. Let M be a fixed positive real number and let $f : G \to \{0, 1\}$ be a boolean function. When is $\|f\|_A \leqslant M$?

A partial answer to this question will be the main business of this paper. By far the most important feature of the problem is that we are asking it for *boolean functions*, which take only the values 0 or 1. There is a ready supply of functions f with $\|f\|_A$ small: Take for instance any pair $g, h : G \to \mathbb{R}$. Then $f := g * h$ has

$$\|f\|_A = \|g * h\|_A = \|\widehat{g}\widehat{h}\|_1 \leqslant \|\widehat{g}\|_2 \|\widehat{h}\|_2 = \|g\|_2 \|h\|_2 \,,$$

which is small if g and h are small in L^2. It is rather hard, however, to construct a large supply of such functions which take only the values 0 and 1.

To get a feel for the question, we prove a simple folklore result concerning the case $M = 1$. In fact, by choosing a suitable argument from among the many available, one can cover the case $M < 3/2$.

PROPOSITION 1.2 (Boolean functions with tiny spectral norm). *Let $f : G \to \{0, 1\}$ be a boolean function which does not vanish identically. Then either $f = 1_{t+H}$, where $t + H$ is a coset of a subgroup of G, in which case $\|f\|_A = 1$, or else $\|f\|_A \geqslant 3/2$.*

Proof. First note that since f is not identically zero we have $\|f\|_\infty \geqslant 1$, and so $\|f\|_A \geqslant \|f\|_\infty \geqslant 1$, by the simplest instance of the Hausdorff–Young inequality.

Now suppose that $H \leqslant G$. The Fourier transform of 1_{t+H} is supported on $H^\perp := \{r \in \widehat{G} : r^T x = 0 \text{ for all } x \in H\}$, and it has modulus $\|1_H\|_1$ there. It follows from this and the fact that $|H||H^\perp| = |G|$ that $\|f\|_A = 1$ when $f = 1_{t+H}$.

To get the stronger statement claimed, we note that if f is not (the characteristic function of) a coset of a subgroup then there are four distinct

points $x, x+h, x+k, x+h+k$ forming a parallelogram in G such that $f(x) = f(x+h) = f(x+k) = 1$ but $f(x+h+k) = 0$ (this is actually an if and only if statement – we leave the proof of both directions to the reader). Let

$$\phi := \delta_x + \delta_{x+h} + \delta_{x+k} - \delta_{x+h+k}\,,$$

thus $\phi(x) = \phi(x+h) = \phi(x+k) = |G|$, $\phi(x+h+k) = -|G|$ and $\phi(y) = 0$ for all other y. Now we can compute that

$$\langle f, \phi \rangle := \mathbb{E}_{x \in G} f(x)\phi(x) = 3 \text{ and } \|\widehat{\phi}\|_\infty = 2\,,$$

and so it follows from Plancherel's theorem that

$$3 = \langle f, \phi \rangle = \langle \widehat{f}, \widehat{\phi} \rangle \leqslant \|\widehat{f}\|_1 \|\widehat{\phi}\|_\infty \leqslant 2\|f\|_A\,,$$

which proves the result. $\square$

REMARKS. We leave it to the reader to confirm that the constant $3/2$ is best possible. The result (and proof) are inspired by two papers of Saeki [S1,2] in which the same question is addressed over all locally compact abelian groups G. In that more general setting the constant $3/2$ should be reduced to $\frac{1}{2}(1 + \sqrt{2})$, and equality can occur in any group G with an element of order 4.

Returning to our main question, let us recall that $\|\cdot\|_A$ is an algebra norm. Thus if $f_1, f_2 : G \to \{0,1\}$ are functions for which $\|f_1\|_A$ and $\|f_2\|_A$ are small then the functions $f_1 \vee f_2$, $f_1 \wedge f_2, 1 - f_1$ and $1 - f_2$ also have this property. Loosely speaking, we refer to functions which can be obtained by a small number of operations of this kind from the basic functions 1_{t+H} as belonging to the *coset ring* of G. In fact, it is easy to see (ignoring quantitative issues for the time being) that all elements of the coset ring are in fact of the form

$$\sum_{j=1}^{L} \pm 1_{H_j}\,, \tag{1.1}$$

for subgroups $H_j \leqslant G$ and some "small" L.

One trivially has the bound

$$\left\| \sum_{j=1}^{L} \pm 1_{H_j} \right\|_A \leqslant L\,,$$

and so it is rather natural to ask whether something like the converse is true; this is the main result of our paper.

Theorem 1.3 (Main theorem). *Suppose that $f : G \to \{0,1\}$ has $\|f\|_A \leqslant M$. Then we may write*

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

where the H_j are subgroups of G and $L \leqslant 2^{2^{CM^4}}$ for some absolute constant C.

REMARKS.   The bound may seem unimpressive, and indeed in a sense it is. However it depends only on M, a feature which we believe is new to this paper. We do not dare to venture a guess as to the correct bound, and it seems to us that it would be difficult to use our method to reduce the number of exponentials below two. It may be possible to reduce the power 4 somewhat, although we have not attempted to do this.

The reader may wonder why we bothered to introduce the coset ring at all, when only the very natural functions (1.1) are involved in our theorem. The answer is that the description of the coset ring in the form (1.1) is specific to the case $G = \mathbb{F}_2^n$, and the phenomenon described by Theorem 1.3 is, in a sense, more general.

Indeed our entire approach was motivated by Cohen's celebrated idempotent theorem [Co]. Suppose that G is a locally compact abelian group, and that $M(G)$ is the Banach algebra of finite measures on G under convolution (see [R2, App. E] for details). We say that a measure $\mu \in M(G)$ is *idempotent* if $\mu * \mu = \mu$. Cohen's theorem is that μ is idempotent if and only if $\widehat{\mu}$ lies in the coset ring of $\Gamma = \widehat{G}$.

In our setting, Cohen's result implies that if $f : G \rightarrow \{0,1\}$ has $\|f\|_A < \infty$ then there is a decomposition of the form of (1.1) with L finite. This is, of course, a vacuous result. It was, however, natural to start with Cohen's argument (as described in Rudin [R2]) and try to make it effective. A naïve attempt along these lines fails at several points and there are even "softer" proofs of Cohen's theorem that we have not managed to interpret in a finite setting at all, cf. [HMP]. Nevertheless access to these classical results was crucial to our understanding and we could not have written this paper without them.

We also import some "modern" ingredients from additive combinatorics such as the Balog–Szemerédi theorem and Ruzsa's analogue of Freiman's theorem. It seems to the authors that it may be worth revisiting a number of classical results in the light of these developments.

It is possible that our methods, in combination with the ideas in [Co], could lead to a fully quantitative proof of Cohen's idempotent theorem. We intend to pursue this direction in future work.

We conclude the introduction by remarking that the spectral norm of boolean functions is discussed in the computer science literature, but not in a great deal of detail. The papers [B], [M] show that functions which can

be computed using a small binary decision tree have small spectral norm. Such functions are, however, rather special elements of the coset ring.

2   Notation

Much of the notation we will use is implicit in the introduction, but it may be helpful to clarify things here. When working with functions on G, we will always use Haar probability measure. Integration with respect to this measure will be denoted by $\mathbb{E}_{x \in G}$, or sometimes just $\mathbb{E}$. If $f : G \to \mathbb{R}$ is a function and $1 \leqslant p < \infty$ then we define

$$\|f\|_p := \left(\mathbb{E}_{x \in G} |f(x)|^p \right)^{1/p}.$$

We also define $\|f\|_\infty := \sup_x |f(x)|$ as usual. If $f_1, f_2 : G \to \mathbb{R}$ are two functions then we set

$$\langle f_1, f_2 \rangle := \mathbb{E}_{x \in G} f_1(x) f_2(x)$$

and

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

When working with the Fourier transforms of functions we will use counting measure. Integration with respect to this measure will be denoted by $\sum$ as usual. We defined the ℓ^p norms in the introduction. Note also Plancherel's identity, which implies that

$$\langle f_1, f_2 \rangle = \langle \widehat{f_1}, \widehat{f_2} \rangle := \sum_r \widehat{f_1}(r) \widehat{f_2}(r) \,.$$

We will occasionally write, e.g. $E^\wedge$, when taking the Fourier transform of a particularly complicated expression E.

Finally, a word concerning absolute constants. The letter C will always denote an absolute constant, but the exact value of this constant may change from expression to expression. If in doubt, the reader should recall that all instances of C could, if desired, be replaced by specific constants in such a way that all our proofs are correct.

3   Almost Integer-Valued Functions and Almost Homomorphisms

A key feature of this paper is that we cannot work entirely within the "category" of boolean functions. We must also consider more general functions which are close to being integer valued.

DEFINITION 3.1 (Almost integer-valued functions). Let $\epsilon \in (0, 1/2)$. We say that a function $f : G \to \mathbb{R}$ is ϵ-almost integer valued if there is a function $f_\mathbb{Z} : G \to \mathbb{Z}$ such that $\|f - f_\mathbb{Z}\|_\infty \leqslant \epsilon$.

We will need to study the behaviour of almost integer-valued functions under a certain class of map. Let H be a subgroup of G. For any function $f : G \to \mathbb{R}$, we define $\psi_H f$ by

$$(\psi_H f)(x) := \mathbb{E}_{y \in x + H} f(y) = f * \mu_H(x) \,,$$

where μ_H denotes the Haar probability measure on H. Equivalently, one may define ψ_H in terms of its Fourier transform by

$$(\psi_H f)^\wedge(r) := \widehat{f}(r) 1_{H^\perp}(r) \,,$$

where the subgroup $H^\perp \leqslant \widehat{G}$ is the annihilator of H, defined by

$$H^\perp := \{ r \in \widehat{G} : r^T x = 0 \quad \text{for all } x \in H \} \,.$$

The following simple properties of ψ_H follow immediately from the above definitions.

LEMMA 3.2 (Simple properties of ψ_H).   *The norm of ψ_H is at most 1 in both the operator norm induced by the spectral norm and in that induced by the L^∞-norm. That is to say*

$$\|\psi_H f\|_A \leqslant \|f\|_A \quad \text{and} \quad \|\psi_H f\|_\infty \leqslant \|f\|_\infty \quad \text{for all} \ \ f : G \to \mathbb{R} \,.$$

DEFINITION 3.3 (Spectral support).   *Let $\eta > 0$ be a parameter, let $f : G \to \mathbb{R}$ be a function, and suppose that $H \leqslant G$. Then we say that f is η-spectrally supported on H if*

$$\sup_{r \notin H^\perp} \sum_{r' \in r + H^\perp} |\widehat{f}(r')| \leqslant \eta \,.$$

Note that we do *not* assume that $\widehat{f}$ has substantial mass on $H^\perp$ itself.

LEMMA 3.4 (Finding the spectral support).   *Let $H \leqslant G$ be any subgroup, let $\eta > 0$ be any parameter, and let $f : G \to \mathbb{R}$ be a function with $\|f\|_A \leqslant M$. Then there is a subgroup $H' \leqslant H$ with*

$$\mathrm{codim}(H : H') \leqslant M/\eta$$

such that f is η-spectrally supported on H'.

Proof. Set $H_0 := H$. We define a descending sequence $H_0 \geqslant H_1 \geqslant \ldots$ of subgroups with $\mathrm{codim}(H_i : H_{i+1}) = 1$.

If, at some stage, f is η-spectrally supported on H_i then we stop. If not, there is some $r_i \notin H_i^\perp$ such that

$$\sum_{r' \in r_i + H_i^\perp} |\widehat{f}(r')| > \eta \,.$$

Define $H_{i+1}^\perp$ to be the subgroup of G generated by r_i and $H_i^\perp$. It is clear that for any j we have

$$\|f\|_A \geqslant \sum_{i=0}^{j} \sum_{r' \in r_i + H_i^\perp} |\widehat{f}(r')| \,,$$

and so this inductive process must terminate after no more than M/η steps.   □

The purpose of Definition 3.3 and Lemma 3.4 is to allow us to use the following approximate homomorphism property.

LEMMA 3.5 (ψ_H is an approximate homomorphism).   *Suppose that $f, g : G \to \mathbb{R}$ are two functions, and that f is η-spectrally supported on H. Then*

$$\left\|\psi_H(fg) - \psi_H(f)\psi_H(g)\right\|_A \leqslant \eta\|g\|_A \,.$$

Proof. We have

$$\left\|\psi_H(fg) - \psi_H(f)\psi_H(g)\right\|_A = \sum_r \left|\widehat{f} * \widehat{g}(r)1_{H^\perp}(r) - \widehat{f}1_{H^\perp} * \widehat{g}1_{H^\perp}(r)\right| \,.$$

However

$$\widehat{f} * \widehat{g}(r)1_{H^\perp}(r) = \sum_s \widehat{f}(r-s)\widehat{g}(s)1_{H^\perp}(r)$$

$$= \sum_s \widehat{f}(r-s)\widehat{g}(s)1_{H^\perp}(r-s)1_{H^\perp}(s) + \sum_{s \notin H^\perp} \widehat{f}(r-s)\widehat{g}(s)1_{H^\perp}(r)$$

$$= \widehat{f}1_{H^\perp} * \widehat{g}1_{H^\perp}(r) + \sum_{s \notin H^\perp} \widehat{f}(r-s)\widehat{g}(s)1_{H^\perp}(r) \,.$$

Now simply note that

$$\sum_r \left| \sum_{s \notin H^\perp} \widehat{f}(r-s)\widehat{g}(s)1_{H^\perp}(r) \right| \leqslant \sum_{s \notin H^\perp} \sum_{r \in H^\perp} \left|\widehat{f}(r-s)\right|\left|\widehat{g}(s)\right|$$

$$\leqslant \sum_s \left|\widehat{g}(s)\right| \sup_{s \notin H^\perp} \sum_{r \in H^\perp} \left|\widehat{f}(r-s)\right|$$

$$\leqslant \eta\|g\|_A \,.$$

This completes the proof.   □

Our aim is to show that, provided the parameter η is suitably small, the map ψ_H preserves almost integer-valued functions.

LEMMA 3.6.   *Let $d \geqslant 0$ be an integer, and write $P_d(X) := 4^d(2d)!^{-1}\prod_{j=-d}^{d}(X - j)$. Let $\epsilon, \delta \leqslant 1/2$ be positive real parameters. Let $f : G \to \mathbb{R}$ be a function.*

(1) *If f is ϵ-almost integer valued and $\|f\|_\infty \leqslant d$ then $\|P_d(f)\|_\infty \leqslant \epsilon 4^d$.*
(2) *If $\|P_d(f)\|_\infty \leqslant \delta$ then f is δ-almost integer valued.*

Proof. To prove the first statement, simply note that

$$\left\|P_d(f)\right\|_\infty \leqslant 4^d(2d)!^{-1} \cdot (2d)! \sup_x \inf_j \left|f(x) - j\right| \leqslant \epsilon 4^d.$$

To prove the second, observe that

$$\left|P_d(t)\right| \geqslant \left|P_d(\overline{t})\right|$$

for all $t \in \mathbb{R}$, where $\overline{t} \equiv t \,(\mathrm{mod}\,1)$ and lies in the interval $(-1/2, 1/2]$. Furthermore one may easily confirm that

$$\left|P_d(\overline{t})\right| \geqslant \frac{|\overline{t}| \cdot 4^d d! \prod_{j=0}^{d-1}\left(j + \frac{1}{2}\right)}{(2d)!} \geqslant |\overline{t}|\,,$$

for all t. It follows that for all x the distance from $f(x)$ to the nearest integer is no more than δ. $\square$

REMARK.   We have normalised the polynomials P_d slightly arbitrarily, so that no factors were lost in (2). This makes no essential difference to the argument.

To apply this, we combine it with the rest of the results of this section to obtain the following corollary.

PROPOSITION 3.7 (ψ_H preserves almost integer-valued functions).   *Suppose that $f : G \to \mathbb{R}$ is ϵ-almost integer valued, and that $\|f\|_A \leqslant M$ for some $M \geqslant 1/2$. Suppose that $\eta \leqslant 2^{-CM(1+\log M)}\epsilon$ for some suitably large C and that f is η-spectrally supported on H. Then both $\psi_H f$ and $f - \psi_H f$ are $(2^{CM}\epsilon)$-almost integer valued.*

Proof. It clearly suffices to prove the result for $\psi_H f$, as the sum or difference of two almost integer-valued functions is almost integer valued. Set $d := \lceil M \rceil$. Since $\|f\|_\infty \leqslant \|f\|_A \leqslant M$, Lemma 3.6 (1) implies that

$$\left\|P_d(f)\right\|_\infty \leqslant 2^{CM}\epsilon\,.$$

From Lemma 3.2 it follows that

$$\left\|\psi_H(P_d(f))\right\|_\infty \leqslant 2^{CM}\epsilon\,. \tag{3.1}$$

Now an easy induction based on Lemma 3.5 (and Lemma 3.2) confirms that

$$\left\|\psi_H(f^n) - (\psi_H f)^n\right\|_A \leqslant \eta(n-1)M^{n-1}\,,$$

for any positive integer n. It follows from this that

$$\left\|\psi_H(P_d(f)) - P_d(\psi_H f)\right\|_A \leqslant 2^{CM(1+\log M)}\eta \leqslant 2^{CM}\epsilon\,,$$

and hence in view of (3.1) that

$$\left\|P_d(\psi_H f)\right\|_\infty \leqslant 2^{CM}\epsilon\,.$$

The result is now an immediate consequence of Lemma 3.6 (2). $\square$

4   Ruzsa's Analogue of Freiman's Theorem

In the next two sections we use variants of a well-known sequence of arguments in additive combinatorics. The objective is to prove Proposition 5.1,

which roughly speaking states that a function with small $A(G)$-norm concentrates on a subspace. We will supply original references for the results we use, but would also recommend the book [TV] as a general resource for this subject.

When we actually prove Proposition 5.1 we will find ourselves dealing with a set $A \subseteq G$ with *small doubling*, that is to say a set A with $\mathbb{E}1_{A+A} \leqslant K\mathbb{E}1_A$ for some "not too large" K. There is a beautiful theorem of Imre Ruzsa [Ru2] (see also [Sa]) which states that in this case A is contained in a subgroup $H \leqslant G$ with density at most $K^2 2^{K^4} \mathbb{E}1_A$. This certainly implies that

$$\mathbb{E}_{x \in A} 1_H(x) \geqslant 1 \quad \text{and} \quad \mathbb{E}_{x \in H} 1_A(x) \geqslant 2^{-CK^C}. \qquad (4.1)$$

One could use this result as it is, and obtain a bound in Theorem 1.3 with a three-fold iterated exponential. To reduce the number of exponentials to two, we need a different version of Ruzsa's result, in which we shall replace (4.1) with

$$\mathbb{E}_{x \in A} 1_H(x) \geqslant 2^{-CK^C} \quad \text{and} \quad \mathbb{E}_{x \in H} 1_A(x) \geqslant cK^{-C}.$$

A more precise version of the following proposition, which is the main result of the section, will be contained in a forthcoming paper of the first author and Terence Tao. The authors are grateful to the latter for useful discussions regarding this circle of ideas.

PROPOSITION 4.1 (Freiman in torsion groups, refined).   *Suppose that* $A \subseteq G$ *is a set with* $\mathbb{E}1_{A+A} \leqslant K\mathbb{E}1_A$. *Then there is a subgroup* $H \leqslant G$ *such that*

$$\mathbb{E}_{x \in A} 1_H(x) \geqslant 2^{-CK^C} \quad \text{and} \quad \mathbb{E}_{x \in H} 1_A(x) \geqslant cK^{-C}.$$

REMARK.   It is an important unsolved problem to decide whether or not one may replace 2^{-CK^C} by a polynomial in the first bound. This is known as the polynomial Freiman–Ruzsa conjecture (PFR); see for example [Gr2]. The truth of this conjecture, however, would not make an essential difference to the bound we obtain in Theorem 1.3.

To prove Proposition 4.1 we need to set up a little notation. Write $\alpha := \mathbb{E}1_A$ for the density of A in G. Put

$$\nu^{(4)}(x) := 1_A * 1_A * 1_A * 1_A(x),$$

and for any parameter $\eta > 0$ define

$$S_\eta := \left\{ x \in G : \nu^{(4)}(x) \geqslant \eta\alpha^3 \right\}.$$

For a parameter $\rho \in (0,1)$, we write (as is becoming standard)

$$\mathrm{Spec}_\rho(A) := \left\{ r \in \widehat{G} : |\widehat{1}_A(r)| \geqslant \rho\alpha \right\}.$$

We begin by recording a well-known argument of Bogolyubov [Bo] in this language.

LEMMA 4.2 (Bogolyubov's argument).   *Suppose that $A \subset G$. Let $\delta, \epsilon \in (0,1)$ be any parameters and set $\rho := (\epsilon/2)^{1/2}$ and $H := \mathrm{Spec}_\rho(A)^\perp$. Then*

$$S_\delta + H \subseteq S_{\delta - \epsilon}.$$

Proof. Suppose that $x \in S_\delta$ and that $h \in H$. Then we have

$$\nu^{(4)}(x+h) = \sum_{r \in \widehat{G}} \left|\widehat{1}_A(r)\right|^4 (-1)^{r^T(x+h)}$$

$$= \sum_{r \in \mathrm{Spec}_\rho(A)} \left|\widehat{1}_A(r)\right|^4 (-1)^{r^T x} + \sum_{r \notin \mathrm{Spec}_\rho(A)} \left|\widehat{1}_A(r)\right|^4 (-1)^{r^T(x+h)}$$

$$\geqslant \nu^{(4)}(x) - 2 \sum_{r \notin \mathrm{Spec}_\rho(A)} \left|\widehat{1}_A(r)\right|^4.$$

Thus we only need observe, using Parseval's identity and the definition of $\mathrm{Spec}_\rho(A)$, that

$$\sum_{r \notin \mathrm{Spec}_\rho(A)} \left|\widehat{1}_A(r)\right|^4 \leqslant \sup_{r \notin \mathrm{Spec}_\rho(A)} \left|\widehat{1}_A(r)\right|^2 \sum_{r \in G} \left|\widehat{1}_A(r)\right|^2 \leqslant (\rho\alpha)^2 \cdot \alpha = \epsilon\alpha^3/2. \quad \square$$

The next two lemmas are the vehicles by which we leverage the assumption that A has small doubling. The first states that A has large density on a translate of S_η, provided η is sufficiently small.

LEMMA 4.3.   *Suppose that $A \subseteq G$, that $\mathbb{E}1_{A+A} \leqslant K\mathbb{E}1_A$ and that $\eta \leqslant 1/2K^4$ is a parameter. Then $\mathbb{E}1_{S_\eta} \geqslant \alpha/2$ and*

$$\|1_A * 1_{S_\eta}\|_\infty \geqslant \eta\alpha/2.$$

Proof. Averaging $\nu^{(4)}$ over $x \in G$, we get

$$\alpha^4 = \mathbb{E}\nu^{(4)}$$

$$\leqslant \alpha^3 \mathbb{E}1_{S_\eta} + \eta\alpha^3 \mathbb{E}1_{4A}$$

$$\leqslant \alpha^3 \mathbb{E}1_{S_\eta} + \eta\alpha^4 K^4$$

$$\leqslant \alpha^3 \mathbb{E}1_{S_\eta} + \alpha^4/2,$$

where the second inequality follows from the Plünnecke–Ruzsa inequalities [Ru1], and the third from the condition on η. The first conclusion of the lemma follows immediately upon rearranging.

For the second part we use the first to see that

$$\eta\alpha^4/2 \leqslant \eta\alpha^3 \mathbb{E}1_{S_\eta}$$

$$\leqslant \mathbb{E}(1_{S_\eta}\nu^{(4)})$$

$$= \langle 1_{S_\eta}, 1_A * 1_A * 1_A * 1_A \rangle$$

$$= \langle 1_A * 1_{S_\eta}, 1_A * 1_A * 1_A \rangle$$

$$\leqslant \|1_A * 1_{S_\eta}\|_\infty \mathbb{E}1_A * 1_A * 1_A \,.$$

The conclusion follows immediately since $\mathbb{E}1_A * 1_A * 1_A = \alpha^3$. $\square$

LEMMA 4.4.   *Suppose that $A \subseteq G$ has density $\alpha := \mathbb{E}1_A$ and that $\mathbb{E}1_{A+A} \leqslant K\mathbb{E}1_A$. Then there is a subgroup $H \leqslant G$ with $\mathbb{E}1_H \geqslant (\alpha/2)^{-CK^{12}}$ and some η with $1/4K^4 \leqslant \eta \leqslant 1/2K^4$, such that S_η is a union of cosets of H together with an exceptional set X satisfying $\mathbb{E}1_X \leqslant \alpha/16K^4$.*

Proof. Let $\eta_0 := 1/2K^4$ and set $\epsilon := 1/64K^{12}$. Consider the nested sequence

$$S_{\eta_0} \subseteq S_{\eta_0-\epsilon} \subseteq \cdots \subseteq S_{\eta_0-(L-1)\epsilon} \,,$$

where $L := 1/4K^4\epsilon$. By the Plünnecke–Ruzsa inequalities we have [Ru1]

$$\mathbb{E}1_{S_\eta} \leqslant \mathbb{E}1_{4A} \leqslant K^4\alpha$$

for any η, and therefore by the pigeonhole principle there is some j with $0 \leqslant j < L$ such that

$$\mathbb{E}1_{S_{\eta_0-(j+1)\epsilon}\backslash S_{\eta_0-j\epsilon}} \leqslant \alpha/16K^4.$$

Now we apply Lemma 4.2. Writing $H = \mathrm{Spec}_\rho(A)^\perp$ where $\rho := 1/16K^6$, we know from that lemma that

$$S_{\eta_0-j\epsilon} + H \subseteq S_{\eta_0-(j+1)\epsilon} \,.$$

Thus $S_{\eta_0-(j+1)\epsilon}$ can be written as a union of cosets of H together with an exceptional set X of density at most $\alpha/16K^4$.

It remains to establish the claimed lower bound on $\mathbb{E}1_H$. By a lemma of Chang [C, Lem. 3.1] (see also [Gr1, Lec. 14, Lem. 3] and [R1], [TV]) the set $\mathrm{Spec}_\rho(A)$ is contained in a subgroup of G with dimension $O(\rho^{-2}(1 + \log(1/\alpha))) = O(K^{12} \log \alpha^{-1})$. This concludes the proof. $\square$

Proof of Proposition 4.1.   It is sufficient to prove the proposition when $G = \langle A \rangle$ in which case, by Ruzsa's theorem [Ru2], we have $\alpha \geqslant K^{-2}2^{-K^4}$.

Apply Lemma 4.4 to get a subgroup H' with $\mathbb{E}1_{H'} \geqslant 2^{-CK^{16}}$ and some η with $1/4K^4 \leqslant \eta \leqslant 1/2K^4$, such that

$$S_\eta = X \cup \bigcup_{y \in Y} (y + H') \,,$$

where $\mathbb{E}1_X \leqslant \alpha/16K^4$. Writing $\mu_{H'} := 1_{H'}/\mathbb{E}1_{H'}$ for the Haar measure on H', we have for all $x \in G$ that

$$
\begin{aligned}
1_A * 1_{S_\eta} * \mu_{H'}(x) &\geqslant 1_A * 1_{S_\eta\backslash X} * \mu_{H'}(x) \\
&= 1_A * 1_{S_\eta\backslash X}(x) \\
&= 1_A * 1_{S_\eta}(x) - 1_A * 1_X(x) \\
&\geqslant 1_A * 1_{S_\eta}(x) - \mathbb{E}1_X \\
&\geqslant 1_A * 1_{S_\eta}(x) - \alpha/16K^4 \,.
\end{aligned}
$$

It follows from this, Lemma 4.3 and the assumption that $\eta \geqslant 1/4K^4$ that

$$\|1_A * 1_{S_\eta} * \mu_{H'}\|_\infty \geqslant \|1_A * 1_{S_\eta}\|_\infty - \alpha/16K^4 \geqslant \eta\alpha/2 - \alpha/16K^4 \geqslant \alpha/16K^4.$$
(4.2)

Furthermore by the Plünnecke–Ruzsa inequalities [Ru1] we have

$$\|1_A * 1_{S_\eta} * \mu_{H'}\|_\infty \leqslant \|1_A * \mu_{H'}\|_\infty \mathbb{E}1_{S_\eta} \leqslant \|1_A * \mu_{H'}\|_\infty \mathbb{E}1_{4A} \leqslant K^4\alpha\|1_A * \mu_{H'}\|_\infty.$$

Comparing with (4.2) leads immediately to

$$\|1_A * \mu_{H'}\|_\infty \geqslant 1/16K^8.$$

We have found a coset of H' on which the relative density of A is at least $1/16K^8$; by adjoining the zero element to H' if necessary, one obtains a subgroup H on which the relative density of A is at least $1/32K^8$, that is to say

$$\mathbb{E}_{x \in H}1_A(x) \geqslant 1/32K^8.$$

To complete the proof of Proposition 4.1 it remains to note that

$$\mathbb{E}_{x \in A}1_H(x) = \frac{\mathbb{E}1_H}{\mathbb{E}1_A} \cdot \mathbb{E}_{x \in H}1_A(x) \geqslant (\mathbb{E}1_H)\mathbb{E}_{x \in H}1_A(x) \geqslant 2^{-CK^{16}}. \qquad \square$$

5   Concentration on a Subgroup

PROPOSITION 5.1 (Concentration on a subgroup).   *Suppose that* $f : G \to \mathbb{R}$ *is an* ϵ*-integer-valued function with* $\|f\|_A \leqslant M$, *where* $M \geqslant 1/2$ *and* $\epsilon \leqslant 2^{-CM^4}$. *Then there is a subgroup* $H \leqslant G$ *with*

$$\mathbb{E}1_H \geqslant 2^{-2^{CM^4}}\|f_{\mathbb{Z}}\|_1$$

and

$$\sup_{x \in G}\left|\mathbb{E}_{y \in x+H}f(y)\right| = \|\psi_H f\|_\infty \geqslant 2^{-CM^4}.$$

DEFINITION 5.2 (Arithmetic connectedness).   Let m be a positive integer. Suppose that $A \subseteq G$ is a set with $0 \notin A$. Then we say that A is m-*arithmetically connected* if, for any choice of distinct $a_1, \ldots, a_m \in A$, one of the following alternatives holds:

(1) The vectors $a_1, \ldots, a_m$ are linearly dependent;
(2) The vectors $a_1, \ldots, a_m$ are linearly independent but there exists a further $a' \in A$ such that a' lies in the linear span of the a_i.

The next lemma imports the tools we developed in section 4. The result allows us to weaken the condition of small doubling in Proposition 4.1 to that of arithmetic connectedness.

LEMMA 5.3.   *Suppose that* m *is a positive integer and that* $A \subseteq G$ *is a set with* $0 \notin A$. *Suppose that* A *is* m-*arithmetically connected. Then there is*

a subgroup $H \leqslant G$ such that

$$\mathbb{E}_{x \in A} 1_H(x) \geqslant 2^{-2^{Cm}} \quad \text{and} \quad \mathbb{E}_{x \in H} 1_A(x) \geqslant 2^{-Cm}.$$

Proof. If $|A| < m^2$ the result is trivial, so we stipulate that $|A| \geqslant m^2$. Pick any m-tuple $(a_1, \ldots, a_m)$ 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 $a_1, \ldots, a_m$ are linearly dependent, 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 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 $\mathbb{F}_2$ and, since $0 \notin A$ and the a_is 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 $|A|^m/2^{m+2}$ solutions with $x_1, \ldots, x_m, x' \in A$. Removing the zero coefficients, we may thus assert that there is some r, $3 \leqslant r \leqslant m+1$, such that the equation

$$x_1 + \cdots + x_r = 0$$

has at least $|A|^{r-1}/2^{m+2}$ solutions with $x_1, \ldots, x_r \in A$. Note that this is a strong structural statement about A, since the maximum possible number of solutions to such an equation is $|A|^{r-1}$.

We claim that there are at least $2^{-2m-4}|A|^3$ solutions to $x_1 + x_2 = x_3 + x_4$ with $x_i \in A$. To see this, write $R_l(x)$ for the number of l-tuples $(x_1, \ldots, x_l) \in A^l$ such that $x_1 + \cdots + x_l = x$, and note that

$$\sum_x R_2(x) R_{r-2}(x) = R_r(0) \geqslant |A|^{r-1}/2^{m+2}.$$

Noting that $R_{r-2}(x) \leqslant |A|^{r-3}$ for all x (here, of course, it is important that $r \geqslant 3$) we see from the Cauchy–Schwarz inequality that

$$\sum_x R_2(x)^2 \geqslant \frac{|A|^{2(r-1)}}{2^{2m+4} \left(\sum_x R_{r-2}(x)^2 \right)} \geqslant 2^{-2m-4}|A|^3,$$

confirming the claim.

It now follows from the Balog–Szemerédi–Gowers theorem [G, Prop. 12] that there is some set $A' \subseteq A$, $\mathbb{E}1_{A'} \geqslant 2^{-Cm} \mathbb{E}1_A$, such that $\mathbb{E}1_{A'+A'} \leqslant 2^{Cm} \mathbb{E}1_{A'}$. By Proposition 4.1 there is a subgroup $H \leqslant G$ with

$$\mathbb{E}_{x \in A'} 1_H(x) \geqslant 2^{-2^{Cm}} \quad \text{and} \quad \mathbb{E}_{x \in H} 1_{A'}(x) \geqslant 2^{-Cm}.$$

The result follows since $\mathbb{E}1_A \geqslant \mathbb{E}1_{A'} \geqslant 2^{-Cm} \mathbb{E}1_A$. $\qquad\qquad$ $\square$

Proof of Proposition 5.1.   We begin by decomposing f^2 as $g + h$ where $g = f_{\mathbb{Z}}^2$ and $h = f^2 - g$. We have
$$\|h\|_\infty = \|f^2 - f_{\mathbb{Z}}^2\|_\infty \leqslant \|f - f_{\mathbb{Z}}\|_\infty \|f + f_{\mathbb{Z}}\|_\infty \leqslant 4\epsilon M \,,$$
the latter inequality being a consequence of the fact that $\|f\|_\infty \leqslant \|f\|_A \leqslant M$ and that $\|f_{\mathbb{Z}}\|_\infty \leqslant \|f\|_\infty + \epsilon$.

Set $m = \lceil (2M)^4 \rceil$ and suppose that $V \leqslant G$ is a subgroup of dimension m. We have
$$\|f^2 1_V\|_A \leqslant \|f\|_A^2 \|1_V\|_A = \|f\|_A^2 \leqslant M^2.$$
In view of the trivial estimate
$$\|h 1_V\|_A \leqslant \sum_{x \in V} \left\|h(x) 1_x\right\|_A \leqslant 2^m \|h\|_\infty \leqslant 2^{m+2} \epsilon M \,,$$
it follows from the triangle inequality and the assumption on ϵ that
$$\|g 1_V\|_A \leqslant M^2 + 2^{m+2} \epsilon M \leqslant 2M^2. \tag{5.1}$$

Write $A := \operatorname{Supp}(g) = \operatorname{Supp}(f_{\mathbb{Z}})$. If A is all of G then the proposition follows trivially so we may assume that this is not the case. Hence by replacing $f(x)$ by $f(x + y)$ for some $y \notin A$, we may assume without loss of generality that $0 \notin A$. We claim that A is m-arithmetically connected in the sense of Definition 5.2. If this is not the case then there are elements $a_1, \ldots, a_m \in A$ such that the vectors $a_1, \ldots, a_m$ are linearly independent, and such that there is no $a' \in A$ with a' in the linear span of the a_i. Writing V for the subgroup of G spanned by the a_i, this means that the support of $g 1_V$ is precisely $\{a_1, \ldots, a_m\}$.

Thus we have
$$g 1_V(x) = \sum_{i=1}^{m} g(a_i) 1_{a_i}(x) \,.$$
Now we may compute that
$$\left\|(g 1_V)^{\wedge}\right\|_2^2 = \|g 1_V\|_2^2 = \frac{1}{|G|} \sum_{i=1}^{m} |g(a_i)|^2 \geqslant \frac{m}{|G|} \,,$$
and that
$$\left\|(g 1_V)^{\wedge}\right\|_4^4 = \frac{1}{|G|^3} \sum_{\substack{i_1, i_2, i_3, i_4 \\ a_{i_1} + a_{i_2} = a_{i_3} + a_{i_4}}} |g(a_i)|^4 \leqslant \frac{3}{|G|^3} \left(\sum_{i=1}^{m} |g(a_i)|^2 \right)^2$$
$$= \frac{3}{|G|} \left\|(g 1_V)^{\wedge}\right\|_2^4 \,,$$
the middle inequality following from the observation that $a_{i_1} + a_{i_2} = a_{i_3} + a_{i_4}$ only if $i_1 = i_2$ and $i_3 = i_4$, or $i_1 = i_3$ and $i_2 = i_4$, or $i_1 = i_4$ and $i_2 = i_3$. From Hölder's inequality we therefore obtain
$$\|g 1_V\|_A := \left\|(g 1_V)^{\wedge}\right\|_1 \geqslant \frac{\|(g 1_V)^{\wedge}\|_2^3}{\|(g 1_V)^{\wedge}\|_4^2} \geqslant \left(\frac{|G|}{3} \right)^{1/2} \left\|(g 1_V)^{\wedge}\right\|_2 \geqslant \sqrt{m/3} \,.$$

Since $m > 12M^4$, this is contrary to (5.1), and this proves the claim.

Applying Lemma 5.3 we obtain a subgroup H' such that

$$\mathbb{E}_{x \in A} 1_{H'}(x) \geqslant 2^{-2^{CM^4}} \quad \text{and} \quad \mathbb{E}_{x \in H'} 1_A(x) \geqslant 2^{-CM^4}.$$

Since $f^2 \geqslant 1_A/4$ we get $\mathbb{E}_{x \in H'} f^2(x) \geqslant 2^{-CM^4}$, but this does not quite imply Proposition 5.1. By Plancherel's theorem, however, we do have

$$\left\langle (f\mu_{H'})^\wedge, \widehat{f} \right\rangle = \langle f\mu_{H'}, f \rangle = \mathbb{E}_{x \in H'} f^2(x) \geqslant 2^{-CM^4},$$

which, since $\|f\|_A \leqslant M$, means that

$$\left\| (f\mu_{H'})^\wedge \right\|_\infty \geqslant 2^{-CM^4}/M \geqslant 2^{-C'M^4}.$$

By the definition of the Fourier transform this yields an r such that

$$\left| \mathbb{E}_{x \in H'} f(x)(-1)^{r^T x} \right| \geqslant 2^{-CM^4}.$$

Taking $H = H' \cap \{r\}^\perp$, it is clear that

$$\|\psi_H f\|_\infty \geqslant \sup_{x \in H'} \left| \mathbb{E}_{y \in x+H} f(y) \right| \geqslant 2^{-CM^4}.$$

Finally we note that

$$\mathbb{E} 1_H \geqslant \mathbb{E} 1_{H'}/2 \geqslant 2^{-2^{CM^4}} \mathbb{E} 1_A$$

and that

$$\mathbb{E} 1_A \geqslant \frac{\|f_{\mathbb{Z}}\|_1}{\|f_{\mathbb{Z}}\|_\infty} \geqslant \frac{\|f_{\mathbb{Z}}\|_1}{\|f\|_\infty + \epsilon} \geqslant \frac{\|f_{\mathbb{Z}}\|_1}{\|f\|_A + \epsilon} \geqslant \frac{\|f_{\mathbb{Z}}\|_1}{M + \epsilon} \geqslant \frac{\|f_{\mathbb{Z}}\|_1}{M + 1},$$

two estimates which together imply the claimed lower bound on $\mathbb{E} 1_H$. $\square$

6   The Main Argument

The basic strategy for proving Theorem 1.3 is that of an induction on M. Our first lemma provides the main inductive step. The most noteworthy feature of this lemma is that, in order to make the induction work, one cannot restrict attention to boolean functions $f : G \to \{0, 1\}$. It is necessary to consider almost integer-valued functions as well.

LEMMA 6.1 (Inductive step). *Suppose that $f : G \to \mathbb{R}$ is ϵ-almost integer valued with $\|f\|_A \leqslant M$, where $\epsilon \leqslant 2^{-CM^4}$. Then we may decompose f as $f_1 + f_2$, where each f_i is ϵ'-almost integer valued for some $\epsilon' \leqslant 2^{CM}\epsilon$, and for $i = 1, 2$ one of the following two alternatives holds:*

(1) $(f_i)_{\mathbb{Z}}$ *may be written as* $\sum_{j=1}^{L} \pm 1_{H_j}$, *where each H_j is a subgroup of G and*

$$L \leqslant 2^{2^{CM^4}/\epsilon};$$

(2) $\|f_i\|_A$ *is most $\|f\|_A - \frac{1}{2}$.*

Proof. If $M \leqslant 1/2$ then $f_{\mathbb{Z}} = 0$, and so option (1) vacuously holds. Assume, then, that $M \geqslant 1/2$. We begin by applying Proposition 5.1. This provides a subgroup $H \leqslant G$ such that

$$\mathbb{E}1_H \geqslant 2^{-2^{CM^4}} \|f_{\mathbb{Z}}\|_1 \quad \text{and} \quad \|\psi_H f\|_\infty \geqslant 2^{-CM^4}.$$

Set

$$\eta := 2^{-CM(1+\log M)}\epsilon$$

for some large C, this choice being dictated by a later application of Proposition 3.7.

By Lemma 3.4 we may find a subgroup $H' \leqslant H$ with

$$\mathrm{codim}(H : H') \leqslant M/\eta$$

such that f is η-spectrally supported on H'. By averaging we have

$$\|\psi_{H'} f\|_\infty \geqslant \|\psi_H f\|_\infty \geqslant 2^{-CM^4}; \tag{6.1}$$

we also have

$$\mathbb{E}1_{H'} \geqslant 2^{-M/\eta}\mathbb{E}1_H \geqslant 2^{-2^{CM^4}/\epsilon}\|f_{\mathbb{Z}}\|_1 \,.$$

Define $f_1 := \psi_{H'} f$ and $f_2 := f - \psi_{H'} f$. Since f is η-spectrally supported on H', it is an immediate consequence of Proposition 3.7 that both f_1 and f_2 are ϵ'-almost integer valued, for some $\epsilon' \leqslant 2^{CM}\epsilon$.

It turns out that for f_2 alternative (2) always holds, that is to say $\|f_2\|_A \leqslant \|f\|_A - \frac{1}{2}$. From the Fourier definition of $\psi_{H'}$ one sees that the supports of $\widehat{f_1}$ and $\widehat{f_2}$ are disjoint, and hence that

$$\|f\|_A = \|f_1\|_A + \|f_2\|_A \,.$$

Thus we need only show that $\|f_1\|_A \geqslant 1/2$. To see this, note that from (6.1) we have

$$\left\|(f_1)_{\mathbb{Z}}\right\|_\infty \geqslant \|f_1\|_\infty - \epsilon' \geqslant 2^{-CM^4} - \epsilon' > 0 \,.$$

Since $(f_1)_{\mathbb{Z}}$ is integer valued, this of course means that

$$\left\|(f_1)_{\mathbb{Z}}\right\|_\infty \geqslant 1 \,,$$

whence

$$\|f_1\|_A \geqslant \|f_1\|_\infty \geqslant 1 - \epsilon' \geqslant 1/2 \,.$$

To conclude the proof, then, we need only show that if $\|f_2\|_A < 1/2$ then $(f_1)_{\mathbb{Z}}$ may be written as a ± 1 sum of not too many cosets of H'. The hypothesis on $\|f_2\|_A$ then ensures that $\|f_2\|_\infty < \epsilon'$ which is certainly at most $1/10$. Also f is $1/10$-almost integer valued so

$$\|f_{\mathbb{Z}} - \psi_{H'} f\|_\infty \leqslant 1/10 + \|f - \psi_{H'} f\|_\infty \leqslant 1/5 \,.$$

Thus $f_{\mathbb{Z}}$ is within $1/5$ of a function which is constant on cosets of H'. Since $f_{\mathbb{Z}}$ is integer valued, this can only be the case if $f_{\mathbb{Z}}$ is itself constant on

cosets of H', that is to say

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

for some $x_1, \ldots, x_L$ which are distinct modulo H' and some non-zero integers c_j, $|c_j| \leqslant \|f_{\mathbb{Z}}\|_\infty \leqslant \|f\|_A + \epsilon \leqslant 2M$.

Recall that the subgroup H' is such that $\mathbb{E}1_{H'} \geqslant 2^{-2^{CM^4}/\epsilon}\|f_{\mathbb{Z}}\|_1$, and since we obviously have

$$\|f_{\mathbb{Z}}\|_1 \geqslant L\mathbb{E}1_{H'}\,,$$

it follows immediately that $L \leqslant 2^{2^{CM^4}/\epsilon}$. The result follows upon noting that any coset in G is either a subgroup, or else its characteristic function can be expressed as $1_{H_1} - 1_{H_2}$ for two subgroups $H_1, H_2 \leqslant G$. $\square$

Proof of Theorem 1.3.   We apply Lemma 6.1 iteratively, starting with the observation that if $f : G \to \{0,1\}$ is a boolean function then f is 0-almost integer valued, and hence ϵ_0-almost integer valued for any $\epsilon_0 > 0$. An appropriate choice of ϵ_0 will be made later. Split

$$f = f_1 + f_2$$

according to Lemma 6.1. Each f_i is ϵ_1-almost integer valued, where

$$\epsilon_1 \leqslant 2^{CM}\epsilon_0\,,$$

and is such that either $(f_i)_{\mathbb{Z}}$ is a sum of at most $2^{2^{CM^4}/\epsilon}$ functions of the form $\pm 1_H$ (in which case we say it is *finished*), or else we have $\|f_i\|_A \leqslant M - \frac{1}{2}$.

Now split any unfinished functions f_i using Lemma 6.1 again, and so on (we will discuss the admissibility of this shortly). This procedure will result in the definition of parameters $\epsilon_0 \leqslant \epsilon_1 \leqslant \ldots$ satisfying

$$\epsilon_{j+1} \leqslant 2^{CM}\epsilon_j \tag{6.2}$$

for all j. After at most $2M - 1$ steps all functions will be either finished or will have $\|\cdot\|_A$-norm at most $1/2$, in which case they are finished for trivial reasons. Thus we have a decomposition

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

where $K \leqslant 2^{2M}$, each function f_k is ϵ_{2M}-almost integer valued and, for each k, $(f_k)_{\mathbb{Z}}$ may be written as a sum of at most $2^{2^{CM^4}/\epsilon_0}$ functions $\pm 1_H$. Now if ϵ_0 is chosen so that $\epsilon_{2M} \leqslant 2^{-2M}/5$ then

$$\left\| f - \sum_{k=1}^{K} (f_k)_{\mathbb{Z}} \right\|_\infty \leqslant 1/5\,.$$

However f only takes values in $\{0,1\}$ so it follows that

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

which means that f can be written as a sum of at most $2^{2^{CM^4}/\epsilon_0}$ functions $\pm 1_H$.

The condition $\epsilon_{2M} \leqslant 2^{-2M}/5$ is not the strongest condition that we require on ϵ_0. In the repeated applications of Lemma 6.1 we must ensure that $\epsilon \leqslant 2^{-CM^4}$ is always satisfied, and so we require

$$\epsilon_{2M} \leqslant 2^{-CM^4}.$$

In view of (6.2) it is clear, however, that we may choose $\epsilon_0 \geqslant 2^{-CM^4}$, for some suitably large C, so that this is indeed always satisfied. This concludes the proof of Theorem 1.3.   □

7   Concluding Remarks

Note that our proof of Theorem 1.3 actually proves the following slightly stronger result.

PROPOSITION 7.1. *Suppose that $f : G \to \mathbb{R}$ is a function with $\|f\|_A \leqslant M$, and which is ϵ-almost integer valued for some $\epsilon \leqslant 2^{-CM^4}$. Then the function $f_{\mathbb{Z}}$ can be written as a combination of at most $2^{2^{CM^4}}$ functions of the form $\pm 1_H$.*

In the same way that Theorem 1.3 can be seen as a quantitative version of Cohen's result, this proposition can be seen as a quantitative version of some results of Méla [HMP], [Me]. An example in Méla's work [HMP], [Me] shows that ϵ must be smaller than 2^{-cM} for such a theorem to hold.

References

[B]   M. BELLARE, A technique for upper bounding the spectral norm, in "Proceedings of the Fifth Annual Workshop on Computational Learning Theory", ACM (1992), 62–70.

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

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

[Co]   P.J. Cohen, On a conjecture of Littlewood and Idempotent measures, Amer. J. Math. 82:2 (1960), 191–212.

[G]   W.T. Gowers, A new proof of Szemerédi's theorem for progressions of length four, GAFA, Geom. funct. anal. 8:3 (1998), 529–551.

[Gr1]   B.J. Green, Restriction and Kakeya phenomena, http://www.maths.bris.ac.uk/~mabjg.

[Gr2]   B.J. Green, Finite field models in additive combinatorics, in "Surveys in Combinatorics 2005", London Mathematical Society Lecture Notes 327 (2005), 1–27.

[HMP]   B. Host, J.-F. Méla, F. Parreau, Analyse harmonique des mesures, Astérisque 135,136 (1986).

[M]   Y. Mansour, Learning Boolean functions via the Fourier transform, in "Theoretical Advances in Neural Computation and Learning" (V.P. Roychodhury, K.-Y. Siu, A. Orlitsky, eds.) (1994), 391–424.

[Me]   J.-F. Méla, Mesures ε-idempotentes de norme bornée, Studia Math. 72:2 (1982), 131–149.

[R1]   W. Rudin, Trigonometric series with gaps, J. Math. Mech. 9 (1960), 203–227.

[R2]   W. Rudin, Fourier analysis on groups, Interscience Tracts in Pure and Applied Mathematics 12, Interscience Publishers (a division of John Wiley and Sons), New York-London, 1962.

[Ru1]   I.Z. Ruzsa, Sums of finite sets, Number Theory (New York, 1991–1995), Springer, New York (1996), 281–293.

[Ru2]   I.Z. Ruzsa, An analog of Freiman's theorem in torsion groups, Structure theory of set addition, Astérisque 258 (1999), xv, 323–326.

[S1]   S. Saeki, On norms of idempotent measures, Proc. Amer. Math. Soc. 19 (1968), 600–602.

[S2]   S. Saeki, On norms of idempotent measures, II, Proc. Amer. Math. Soc. 19 (1968), 367–371.

[Sa]   T. Sanders, A note on Freiman's theorem in vector spaces, preprint.

[TV]   T.C. Tao, V.H. Vu, Additive Combinatorics, book to appear, CUP, 2006.

Ben Green, Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, England

b.j.green@dpmms.cam.ac.uk

Tom Sanders, Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, England

t.sanders@dpmms.cam.ac.uk