Topics in arithmetic combinatorics

Tom Sanders
Department of Pure Mathematics
and Mathematical Statistics

A dissertation submitted for
the degree of Doctor of Philosophy
at the University of Cambridge.

To Mum & Dad

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration except where specifically indicated in the text.

Abstract

This thesis is chiefly concerned with a classical conjecture of Littlewood's regarding the L^1-norm of the Fourier transform, and the closely related idempotent theorem. The vast majority of the results regarding these problems are, in some sense, qualitative or at the very least infinitary and it has become increasingly apparent that a quantitative state of affairs is desirable.

Broadly speaking, the first part of the thesis develops three new tools for tackling the problems above: We prove a new structural theorem for the spectrum of functions in $A(G)$; we extend the notion of local Fourier analysis, pioneered by Bourgain, to a much more general structure, and localize Chang's classic structure theorem as well as our own spectral structure theorem; and we refine some aspects of Freĭman's celebrated theorem regarding the structure of sets with small doubling. These tools lead to improvements in a number of existing additive results which we indicate, but for us the main purpose is in application to the analytic problems mentioned above.

The second part of the thesis discusses a natural version of Littlewood's problem for finite abelian groups. Here the situation varies wildly with the underlying group and we pay special attention first to the finite field case (where we use Chang's Theorem) and then to the case of residues modulo a prime where we require our new local structure theorem for $A(G)$. We complete the consideration of Littlewood's problem for finite abelian groups by using the local version of Chang's Theorem we have developed. Finally we deploy the Freĭman tools along with the extended Fourier analytic techniques to yield a fully quantitative version of the idempotent theorem.

Acknowledgements

I should like to thank my supervisor Tim Gowers for his support and encouragement and Ben Green for functionally acting as a second supervisor despite no call of duty to do so. I should also like to thank the range of mathematicians with whom I have had many useful conversations over these last few years.

Tom Sanders
Cambridge
8th December 2006

Contents

Chapter 1

Introduction

In recent years it has become increasingly apparent that a lot of results from the harmonic analysis of the 70s and 80s have applications in additive combinatorics, and a number of the tools of additive combinatorics can be applied to yield quantitative version of analytic results from that period. It is this modern, quantitative, perspective on harmonic problems which guides our work.

The thesis is essentially a union of the papers [San06, San08c, San07a, San07b] and [GS08b], the last of these being coauthored with Ben Green. It has three main chapters. In the first two (Chapters 2 and 3) we develop some new tools; we believe this is the most interesting part of the thesis and provides the most scope for future applications. Chapter 4 applies the preceding results to the main questions addressed by the thesis.

The general objective in additive combinatorics is to understand additive structure in sets of integers. For example, if A is a finite set of integers we may well ask how many three term arithmetic progression or additive quadruples A contains. Recall that a three term arithmetic progression is a triple (x, y, z) such that $x + z = 2y$ and an additive quadruple is a quadruple (x, y, z, w) such that $x + y = z + w$. To do this we try to count the quantities

$$\sum_{x,y\in\mathbb{Z}} 1_A(x)1_A(y)1_A(2y-x) \text{ and } \sum_{x,y,z\in\mathbb{Z}} 1_A(x)1_A(y)1_A(z)1_A(x+y-z)$$

respectively. To see these expressions more clearly we introduce some notation. We write $\langle \cdot, \cdot \rangle$ for the usual inner product on $\ell^2(\mathbb{Z})$ and for functions $f, g \in \ell^1(\mathbb{Z})$ we define their convolution to be

$$f * g(x) := \sum_{y+z=x} f(y)g(z).$$

Using this the number of three term arithmetic progressions and additive quadruples in A are

$$\langle 1_A * 1_A, 1_{2A} \rangle \text{ and } \langle 1_A * 1_A, 1_A * 1_A \rangle$$

respectively.

A great strength of the operators $g \mapsto f * g$ is that they all commute and so are *simultaneously* diagonalizable. The basis we pick with respect to which they are all diagonal is called the Fourier basis and the Fourier transform describes the decomposition of a function in this basis; it maps $f \in \ell^1(\mathbb{Z})$ to $\widehat{f} \in L^\infty(\mathbb{T})$ defined by

$$\widehat{f}(\theta) := \sum_{z \in Z} f(z) \exp(-2\pi i z \theta).$$

The fact that the Fourier transform is a change of basis is encoded in the Fourier inversion theorem which tells us that

$$f(x) = \int_0^1 \widehat{f}(\theta) e(x\theta) d\theta \text{ for all } x \in \mathbb{Z}.$$

Moverover, the transform is in fact an orthogonal change of basis, a fact called Plancherel's theorem:

$$\langle f, g \rangle = \int_0^1 \widehat{f}(\theta) \overline{\widehat{g}(\theta)} d\theta \text{ for all } f, g \in \ell^2(\mathbb{Z}).$$

As we have said the Fourier transform maps convolution to multiplication so that the expressions for the number of three term arithmetic progressions and additive quadruples in A can be made even simpler: they become

$$\int_0^1 \widehat{1_A}(\theta)^2\overline{\widehat{1_{2A}}(\theta)}d\theta \text{ and } \int_0^1 |\widehat{1_A}(\theta)|^4 d\theta.$$

We restrict our attention to counting additive quadruples for the moment. A certainly can't have more than $|A|^3$ additive quadruples and if it has close to this number, in the sense of having at least $c|A|^3$ for some small $c > 0$, then counting them more precisely is fairly easy because we can restrict our attention in the Fourier expression above to those θ at which $\widehat{1_A}$ is large. Let

$$\mathfrak{M} := \{\theta \in \mathbb{T} : |\widehat{1_A}(\theta)| \geqslant \epsilon|A|\}.$$

We have

$$\begin{aligned}
\int_0^1 |\widehat{1_A}(\theta)|^4 d\theta &= \int_{\mathfrak{M}} |\widehat{1_A}(\theta)|^4 d\theta + \int_{\mathfrak{M}^c} |\widehat{1_A}(\theta)|^4 d\theta \\
&= \int_{\mathfrak{M}} |\widehat{1_A}(\theta)|^4 d\theta + O\left(\epsilon^2|A|^2 \int_{\mathfrak{M}^c} |\widehat{1_A}(\theta)|^2 d\theta\right) \\
&= \int_{\mathfrak{M}} |\widehat{1_A}(\theta)|^4 d\theta + O\left(\epsilon^2|A|^2 \int_0^1 |\widehat{1_A}(\theta)|^2 d\theta\right) \\
&= \int_{\mathfrak{M}} |\widehat{1_A}(\theta)|^4 d\theta + O(\epsilon^2|A|^3) \\
&= \int_{\mathfrak{M}} |\widehat{1_A}(\theta)|^4 d\theta + O\left(c^{-1}\epsilon^2 \int_0^1 |\widehat{1_A}(\theta)|^4 d\theta\right) \\
&= (1 + O(c^{-1}\epsilon^2)) \int_{\mathfrak{M}} |\widehat{1_A}(\theta)|^4 d\theta
\end{aligned}$$

by Hölder's inequality and Plancherel's theorem.

The reader unfamiliar with this derivation need not be overly concerned, the point is simply that calculating the number of additive quadruples in A has been reduced to understanding where the Fourier transform $\widehat{1_A}$ is 'large'.

By Plancherel's theorem we see that if $|A|$ is large then the Lebesgue measure of $\mathfrak{M}$ is small. In particular we have

$$(\epsilon|A|)^2\mu(\mathfrak{M}) \leqslant \int_0^1 |\widehat{1_A}(\theta)|^2 d\theta = |A|,$$

whence $\mu(\mathfrak{M}) \leqslant \epsilon^{-2}/|A|$. Very roughly this means that f, defined by $\widehat{f} := \widehat{1_A}|_{\mathfrak{M}}$, is a considerably 'lower complexity' object, and therefore easier to understand, than $\widehat{1_A}$. One the other hand, our calculation shows that for the purpose of counting additive quadruples f has roughly as good as 1_A!

While proximity of Fourier transforms in $L^4(\mathbb{T})$ does ensure that two functions have a similar number of additive quadruples it is harder to find other ways in which the functions are similar. Contrastingly if $\widehat{f}$ and $\widehat{1_A}$ are close in $L^2(\mathbb{T})$ then, by Plancherel's theorem, we have that f and 1_A are close in $\ell^2(\mathbb{Z})$ – they are *very* similar. Indeed, for almost any arithmetic way in which one may care to compare f and 1_A they will end up being very similar if $\|f - 1_A\|_{\ell^2(\mathbb{Z})}$ is small. It becomes natural then to ask when 1_A has a 'low complexity' approximation in $\ell^2(\mathbb{Z})$.

Suppose that $\|\widehat{1_A}\|_{L^1(\mathbb{T})} \leqslant M$. Then, by the same argument we used above, we have that f, defined by $\widehat{f} = \widehat{1_A}1_{\mathfrak{M}}$, has

$$\begin{aligned}\|f - 1_A\|^2_{\ell^2(\mathbb{Z})} &= \int_0^1 |\widehat{1_A}(\theta) - \widehat{f}(\theta)|^2 d\theta \\ &= \int_{\mathfrak{M}^c} |\widehat{1_A}(\theta)|^2 d\theta \leqslant \epsilon|A|M = \epsilon M\|1_A\|^2_{\ell^2(\mathbb{Z})}.\end{aligned}$$

In fact one could use any $L^p(\mathbb{T})$-norm of $\widehat{1_A}$ with $p < 2$; the choice of $p = 1$, however, ensures some useful algebraic properties. Indeed, the norm $\|\cdot\|_{A(\mathbb{Z})} := \|\widehat{\cdot}\|_{L^1(\mathbb{T})}$ is often called the algebra norm because of the algebra property

$$\|fg\|_{A(\mathbb{Z})} \leqslant \|f\|_{A(\mathbb{Z})}\|g\|_{A(\mathbb{Z})} \text{ for all } f, g \in \ell^1(\mathbb{Z}).$$

A natural question now arises as to which sets A actually have $\|1_A\|_{A(\mathbb{Z})} \leqslant M$. It was Littlewood in [HL48] who first asked this question, although he came from an entirely different starting point. The now proved Littlewood conjecture asserts that in fact one needs $|A|$ to be rather small for this to hold; specifically there is the following theorem.

Theorem. (Littlewood's conjecture, [Kon81, MPS81]) *Suppose that A is a finite set of integers with $\|1_A\|_{A(\mathbb{Z})} \leqslant M$. Then $|A| \leqslant \exp(O(M))$.*

In this thesis we are concerned first and foremost with understanding the above problems in abelian groups other than $\mathbb{Z}$ – it turns out to be a considerably richer problem in the general case because of the possibility of non-trivial compact subgroups. The Fourier transform has a totally natural generalization to locally compact abelian groups, the details of which are addressed in Chapter 2; they are not important for this discussion.

It is instructive to begin by considering the group $\mathbb{T}$. If $A \subset \mathbb{T}$ has $\|1_A\|_{A(\mathbb{T})} \leqslant M$ we cannot expect to show that A is finite: if A has measure zero then $\|1_A\|_{A(\mathbb{T})} = 0$ and if A has measure one then $\|1_A\|_{A(\mathbb{T})} = 1$. However, it turns out that these are all the exceptions: A must have either measure zero or one. A rigorous proof of this easy fact appears in Chapter 4 but for now we shall accept it and turn to regarding the torus as a good qualitative model for the groups $\mathbb{Z}/p\mathbb{Z}$ where p is a prime. The following discrete analogue of Littlewood's conjecture is one of our main results.

Theorem 1.1. (Theorem 4.8) *Suppose that $A \subset \mathbb{Z}/p\mathbb{Z}$ has density bounded away from 0 and 1, and $\|1_A\|_{A(\mathbb{Z}/p\mathbb{Z})} \leqslant M$. Then $|A| \leqslant \exp(O(M^{2+o(1)}))$.*

One might make the 'discrete Littlewood conjecture', by analogy with the Littlewood conjecture, that the $2 + o(1)$ can be replaced by 1, and, indeed, this may well be the case. However, while the formal similarity between the two problems is rather striking, the methods we require to prove our theorem are very different.

A key challenge in the result above is leveraging the fact that A is not close to being the whole of $\mathbb{Z}/p\mathbb{Z}$. If $A = \mathbb{Z}/p\mathbb{Z}$ then $\|1_A\|_{A(\mathbb{Z}/p\mathbb{Z})} = 1$ and more generally if $H \leqslant G$ then $\|1_H\|_{A(G)} \leqslant 1$, so while the only compact subgroup of $\mathbb{Z}$ is $\{0\}$, for more general groups we have other possibilities. A class of groups with a lot of subgroups are the dyadic groups $\mathbb{F}_2^n$. For these groups we prove the following theorem.

Theorem. (Theorem 4.1.2) *Suppose that $A \subset \mathbb{F}_2^n$ has density as close to $1/3$ as possible and $\|1_A\|_{A(\mathbb{F}_2^n)} \leqslant M$. Then $|A| \leqslant \exp(\exp(O(M)))$.*

The density condition essentially encodes the fact that A is not remotely close to being a subgroup, and it is the handling of the rich subgroup structure here which costs us in the form of a considerably weaker bound. The following is an equivalent, but arguably more attractive, formulation of the above.

Theorem. *Suppose that* $A \subset \mathbb{F}_2^\infty$ *has density* α *with* $|\alpha - 1/3| \leqslant \epsilon$*. Then* $\|1_A\|_{A(\mathbb{F}_2^\infty)} \gg \log\log \epsilon^{-1}$.

To understand the rôle which subgroups play in our work we return to the qualitative view point. The earlier argument for the torus has a considerable generalization to arbitrary locally compact abelian groups called Cohen's idempotent theorem [Coh60]. Cohen began by defining the coset ring. This is the collection of subsets of G which is closed under unions and intersections and which contains every coset of every open subgroup. It is easy to convince oneself using the triangle inequality and the algebra property of the norm $\|\cdot\|_{A(G)}$ that every set A in the coset ring has $\|1_A\|_{A(G)} < \infty$. Remarkably the converse is also true.

Theorem (Idempotent theorem)**.** *Suppose that* G *is a locally compact abelian group and* $A \subset G$ *has* $\|1_A\|_{A(G)} < \infty$*. Then* A *is in the coset ring of* G*.*

Concretely if a set is in the coset ring then there is some $L < \infty$ such that

$$1_A = \sum_{j=1}^{L} \sigma_j 1_{x_j + H_j}$$

where $\sigma_j \in \{-1, 1\}$, $x_j \in G$ and H_j is an open subgroup of G for each $j \in \{1, ..., L\}$. A main result of the thesis (which is joint with Ben Green) is a quantitative version of Cohen's idempotent theorem.

Theorem. (Theorem 4.12) *Suppose that* G *is a locally compact abelian group and* $A \subset G$ *has* $\|1_A\|_{A(G)} \leqslant M$*. Then there is an integer* $L \leqslant \exp(\exp(O(M^4)))$ *such that*

$$1_A = \sum_{j=1}^{L} \sigma_j 1_{x_j + H_j}$$

where $\sigma_j \in \{-1, 1\}$*,* $x_j \in G$ *and* H_j *is an open subgroup of* G *for each* $j \in \{1, ..., L\}$*.*

It is natural to conjecture that one may take $L \leqslant \exp(O(M))$, and a proof of this would not only yield the discrete Littlewood conjecture but also a new proof of Littlewood's conjecture and Cohen's idempotent theorem. Suffice to say it would be a very appealing result.

Before closing out this introduction it is worth mentioning a little bit about how we go about proving the above results. The main tools are developed in Chapters 2 & 3. In the first of these we develop some structural results for understanding the spectrum (essentially the set $\mathfrak{M}$ above) of functions in $A(G)$. This is a key ingredient which enables us to achieve the bound we do for the discrete Littlewood problem.

The second aspect of Chapter 2 is a framework, developed from work of Bourgain [Bou99], in which to conduct a sort of 'approximate group theory'. Basically a lot of our arguments would ideally involve passing to subgroups. Unfortunately most groups do not have a rich enough subgroup structure for this to be effective and we have to make do with a sort of 'approximate subgroup'. The details occupy a considerable portion of the chapter.

In Chapter 3 we develop some additive results and on the way improve a version of a famous result of Freĭman's regarding the additive structure of certain sets. The results there actually address more classical results from additive combinatorics although our purpose for them is in proving the results above.

Our modern outlook manifests itself particularly strongly in two ways: First, we shall work entirely with finite structures, principally concerning ourselves with specific bounds and dependencies. Secondly, we shall take advantage of the model setting of dyadic groups, popularized by Green in [Gre05], for exhibiting some of our methods. It turns out that arguments can very often be modelled in this setting in a way which vastly reduces their technical difficulty whilst retaining their conceptual content, thus making it an ideal illustrative environment.

Finally a word on notational conventions. We use both the Hardy-Littlewood big-O and Vinogradov notations in the normal way *viz.* $g = O(f)$ and $g \ll f$ both mean that there is an absolute constant $C > 0$ such that $|g(x)| \leqslant C|f(x)|$ for all $x > C$. We also write $f \asymp g$ when both $f \gg g$ and $f \ll g$ hold.

Chapter 2

Fourier analytic tools

We are interested in the Fourier transform on finite abelian groups and we begin by fixing the basic definitions and notation. It will often be useful, for the purpose of motivation, to have the transform available to us in the more general setting of locally compact abelian groups. However, presenting it in that setting seems to add undesirable technicalities so we shall restrict ourselves to supplementing our exposition of the finite case with rough indications of how results extend. A more detailed explanation can be found in Rudin [Rud90].

We start with some elementary function spaces. Suppose that X is a finite set. We write $M(X)$ for the space of complex valued measures on X endowed with the norm $\|\mu\| := \int d|\mu|$. Now suppose that μ is non-negative. For $p \in [1, \infty)$ we write $L^p(\mu)$ for the space of complex valued functions on X with norm

$$\|f\|_{L^p(\mu)} := \left(\int |f|^p d\mu \right)^{\frac{1}{p}},$$

and similarly $L^\infty(\mu)$ for the space of complex valued functions on X with norm

$$\|f\|_{L^\infty(\mu)} := \operatorname{esssup}_{x \in X} |f(x)| = \sup_{x \in \operatorname{supp} \mu} |f(x)|.$$

It will also be useful to use $\ell^p(X)$ to denote the space $L^p(\mu)$ in the specific case where μ is counting measure, that is, the measure ascribing mass 1 to each element of X.

We shall be working with finite abelian groups; suppose G is such. It will be useful for us to consider not just sums of elements, but also sums of sets of elements. Suppose A and B are subsets of G. Then we write $A + B$ for the set $\{a + b : a \in A, b \in B\}$. Similarly, if k and l are integers we write $kA - lB$ for the set

$$\{a_1 + ... + a_k - b_1 - ... - b_l : a_1, ..., a_k \in A, b_1, ..., b_l \in B\}.$$

The dual group of G is the finite abelian group of homomorphisms $\gamma : G \to S^1$, where $S^1 := \{z \in \mathbb{C} : |z| = 1\}$; we denote it $\widehat{G}$. Although the natural group operation on $\widehat{G}$ corresponds to pointwise multiplication of characters we shall denote it by '+' in alignment with contemporary work. We write μ_G for the unique translation invariant probability measure on G; μ_G assigns mass $|G|^{-1}$ to each $x \in G$.

The fact that G is a group and μ_G is translation invariant makes $L^1(\mu_G)$ into a normed algebra when combined with the operation of convolution. If $f, g \in L^1(\mu_G)$ we define the convolution of f and g to be

$$f * g(x) := \int f(x - y)g(y)d\mu_G(y).$$

Furthermore, the measure μ_G can be used to define the Fourier transform on $L^1(\mu_G)$: it is the map which takes $f \in L^1(\mu_G)$ to

$$\widehat{f} : \widehat{G} \to \mathbb{C}; \gamma \mapsto \int f\overline{\gamma}d\mu_G.$$

This transform has the crucial property of being an algebra homomorphism *viz.*

$$\widehat{f * g} = \widehat{f}\widehat{g} \text{ for all } f, g \in L^1(\mu_G).$$

We shall occasionally find ourselves taking the Fourier transform of a particularly complicated expression E in which case we shall use $(E)^\wedge$ to denote $\widehat{E}$.

Similar structure can be placed on $M(G)$. If $\mu, \nu \in M(G)$ then we define the convolution of μ and ν to be (the measure induced by)

$$f \mapsto \int f(x+y)d\mu(x)d\nu(y).$$

The Fourier(-Stieltjes) transform is the map which takes $\mu \in M(G)$ to

$$\widehat{\mu} : \widehat{G} \to \mathbb{C}; \gamma \mapsto \int \overline{\gamma} d\mu,$$

which, as before, is an algebra homomorphism. Convolution of measures with functions is defined in the obvious manner.

Having set up the machinery we can define one last function space of importance to us: $A(G)$ is the space of complex valued functions on G with norm

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

This norm is variously called the Wiener algebra norm or simply the algebra norm.

In the general case of G a locally compact abelian group it can be shown (see Halmos [Hal50]) that there is a unique (up to scalar multiplication) translation invariant measure on G. This measure takes the rôle of μ_G and can be used to define the Fourier transform in the same way as above. It is also necessary to restrict the various spaces we have defined to include only those functions for which the appropriate norm is finite. So, for example, $L^1(\mu_G)$ is the space of functions f such that $\|f\|_{L^1(\mu_G)} < \infty$.

It may be helpful to consider some concrete examples at this stage. We shall look at cyclic groups and the model dyadic groups. First, the characters on $\mathbb{Z}/N\mathbb{Z}$ are simply the maps $x \mapsto \exp(2\pi ixr/N)$ where $r \in \mathbb{Z}/N\mathbb{Z}$. Consequently we can identify $\widehat{\mathbb{Z}/N\mathbb{Z}}$ with $\mathbb{Z}/N\mathbb{Z}$ and if $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ then the Fourier transform is given by

$$\widehat{f}(r) := \frac{1}{N} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} f(x) \exp(2\pi ixr/N).$$

Secondly, if $x, y \in \mathbb{F}_2^n$ then we write $x.y$ for the sum $x_1y_1 + ... + x_ny_n$, and the characters on $\mathbb{F}_2^n$ are simply the maps $x \mapsto (-1)^{x.y}$ where $y \in \mathbb{F}_2^n$. These are sometimes called the Walsh functions in the literature. Consequently we can identify $\widehat{\mathbb{F}_2^n}$ with $\mathbb{F}_2^n$ and if $f : \mathbb{F}_2^n \to \mathbb{C}$ then the Fourier transform is given by

$$\widehat{f}(y) := \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{x.y}.$$

We begin the convention now, that unless otherwise stated, G is always assumed to be a finite abelian group.

With these definitions in place we are in a position to record two essential tools. Both results can be proved easily from the fact that the elements of $\widehat{G}$ form an orthonormal basis for the complex valued functions on G. This fact is, in turn, easy to prove directly in the case when G is finite.

Theorem (Fourier inversion formula)**.** *Suppose that* $f \in L^1(\mu_G) \cap A(G)$*. Then*

$$f = \sum_{\gamma \in \widehat{G}} \widehat{f}(\gamma)\gamma.$$

Theorem (Plancherel's Theorem)**.** *Suppose that* $f, g \in L^2(\mu_G)$*. Then*

$$\langle f, g \rangle_{L^2(\mu_G)} = \langle \widehat{f}, \widehat{g} \rangle_{\ell^2(\widehat{G})}.$$

Note that we shall often refer to Parseval's Theorem, which is just the special case of Plancherel's Theorem corresponding to $f = g$.

There are two ideas we shall find ourselves using repeatedly throughout this work. First we are often interested in some average behaviour of a function f, and very loosely speaking the Fourier inversion formula and Plancherel's theorem relate these to the large values of $\widehat{f}$. For example we may be interested in the inner produce of f with some other function g. In this case by Plancherel's Theorem we have

$$\langle f, g \rangle_{L^2(\mu_G)} = \widehat{f}(0_{\widehat{G}})\overline{\widehat{g}(0_{\widehat{G}})} + \sum_{\gamma \neq 0_{\widehat{G}}} \widehat{f}(\gamma)\overline{\widehat{g}(\gamma)}.$$

Here we have separated out the trivial mode (which is usually easy to compute), and we would hope to show that the remaining term is a small error. We certainly have

$$\langle f, g\rangle_{L^2(\mu_G)} = \widehat{f}(0_{\widehat{G}})\overline{\widehat{g}(0_{\widehat{G}})} + O(\|g\|_{A(G)} \sup_{\gamma \neq 0_{\widehat{G}}} |\widehat{f}(\gamma)|),$$

and to understand this, in §2.1, we establish some tools which describe the structure of the sets of characters at which $\widehat{f}$ is large in an appropriate sense. If we know where this happens then we can hope to understand the situations when the error term above is not guaranteed to be small, and hence know when we can have a good idea of what the average $\langle f, g\rangle_{L^2(\mu_G)}$ is.

The second idea is the iterative method: we shall often want to pass to a subgroup of G on which the behaviour of a given function is somehow better understood. Because there are many important groups (e.g. $\mathbb{Z}/p\mathbb{Z}$ for p a prime) with a paucity of subgroups we shall need to consider more general substructures, which behave in some approximate sense like groups. It turns out that so called Bohr sets are natural candidates and we develop this idea in §2.2. There we also extend some of the basic results of Fourier analysis on groups to approximate groups, a process which is often called localizing.

Naturally it will be useful to have the results of §2.1 not just for functions on groups but, more generally, for functions on these approximate groups. Proving these generalizations is the work of §2.3.

Finally, in §2.4, we formalize, as Bourgain systems, the aspects of Bohr sets which make them suitable for the rôle of approximate groups. Both Bohr sets and their more general counterparts have different uses in the thesis: The structure of Bohr sets is better understood than that of Bourgain systems and this extra information is sometimes useful (c.f. §4.3); on other occasions the generality of Bourgain systems is necessary (c.f. §4.4).

2.1 Spectral structures

A natural realization of the sets of characters at which $\widehat{f}$ is large is the sets

$$\{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geqslant \epsilon\|f\|_{L^1(\mu_G)}\} \text{ for } \epsilon \in (0, 1].$$

The study of these sets has been surveyed by Green in [Gre04] so we are brief and only recall the key facts. Write $\Gamma = \{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geqslant \epsilon \|f\|_{L^1(\mu_G)}\}$. Plancherel's Theorem (or really Bessel's inequality) yields

$$|\Gamma|\epsilon^2 \|f\|_{L^1(\mu_G)}^2 \leqslant \|\widehat{f}\|_{\ell^2(\widehat{G})}^2 \leqslant \|f\|_{L^2(\mu_G)}^2$$

which can be rearranged to give

$$|\Gamma| \leqslant \epsilon^{-2}(\|f\|_{L^2(\mu_G)}\|f\|_{L^1(\mu_G)}^{-1})^2. \tag{2.1.1}$$

Note that by nesting of norms we have $\|f\|_{L^2(\mu_G)}\|f\|_{L^1(\mu_G)}^{-1} \geqslant 1$. Now, there is a result of Chang from [Cha02] which refines (2.1.1) if $\|f\|_{L^2(\mu_G)}\|f\|_{L^1(\mu_G)}^{-1}$ is much larger than 1. We require some further notation to state this. If Λ is a set of characters on G and $m \in \mathbb{Z}^\Lambda$ then put

$$m.\Lambda := \sum_{\lambda \in \Lambda} m_\lambda.\lambda \text{ and } |m| := \sum_{\lambda \in \Lambda} |m_\lambda|,$$

where the second '.' in the first definition is the natural action of $\mathbb{Z}$ on $\widehat{G}$. Write $\langle \Lambda \rangle$ for the span of Λ, the set of all $\pm$-sums of elements of Λ, namely

$$\langle \Lambda \rangle := \left\{ m.\Lambda : m \in \{-1, 0, 1\}^\Lambda \right\}.$$

Theorem 2.1.1 (Chang's Theorem)**.** *Suppose that $f \in L^2(\mu_G)$ and $\epsilon \in (0, 1]$ is a parameter. Write $\Gamma := \{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geqslant \epsilon \|f\|_{L^1(\mu_G)}\}$. Then there is a set of characters Λ such that $\Gamma \subset \langle \Lambda \rangle$ and*

$$|\Lambda| \ll \epsilon^{-2}(1 + \log \|f\|_{L^2(\mu_G)}\|f\|_{L^1(\mu_G)}^{-1}).$$

To understand Chang's Theorem more fully it can be helpful to consider the case $f = 1_A$. Here the quantity $\|f\|_{L^2(\mu_G)}\|f\|_{L^1(\mu_G)}^{-1} = \alpha^{-1/2}$ where α is the density of A in G. The bound in (2.1.1) tells us that Γ, the set of large characters, is contained in a set of size $O(\epsilon^{-2}\alpha^{-1})$. Chang's Theorem tells us that it is contained in the span of a set of size $O(\epsilon^{-2} \log \alpha^{-1})$. In typical applications there is no difference between the large spectrum being contained in a small set and being contained in the span of a small set, so Chang's theorem provides an enormous strengthening when A is thin.

Later on we shall be in a situation where we want to examine the large spectrum of functions which we control in $A(G)$-norm rather than in $L^2(\mu_G)$-norm, so we develop an analogue of Chang's Theorem in this setting. Here it turns out that the natural realization of the sets of characters at which $\widehat{f}$ is large is the sets

$$\{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geqslant \epsilon \|f\|_{L^\infty(\mu_G)}\} \text{ for } \epsilon \in (0,1].$$

There is an easy analogue of (2.1.1): Write

$$\Gamma = \{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geqslant \epsilon \|f\|_{L^\infty(\mu_G)}\}.$$

Then

$$|\Gamma|\epsilon\|f\|_{L^\infty(\mu_G)} \leqslant \|\widehat{f}\|_{\ell^1(\widehat{G})} = \|f\|_{A(G)},$$

and so as before

$$|\Gamma| \leqslant \epsilon^{-1}\left(\|f\|_{A(G)}\|f\|_{L^\infty(\mu_G)}^{-1}\right). \tag{2.1.2}$$

A trivial instance of Hausdorff's inequality tells us that $\|f\|_{A(G)}\|f\|_{L^\infty(\mu_G)}^{-1} \geqslant 1$, and indeed the quantity $\|f\|_{A(G)}\|f\|_{L^\infty(\mu_G)}^{-1}$ plays the same rôle in $A(G)$ as the quantity $\|f\|_{L^2(\mu_G)}\|f\|_{L^1(\mu_G)}^{-1}$ does in $L^2(\mu_G)$. To complete the square, then, we shall prove the following.

Theorem 2.1.2. *Suppose that $f \in A(G)$ and $\epsilon \in (0,1]$ is a parameter. Write $\Gamma := \{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geqslant \epsilon\|f\|_{L^\infty(\mu_G)}\}$. Then there is a set of characters Λ such that $\Gamma \subset \langle\Lambda\rangle$ and*

$$|\Lambda| \ll \epsilon^{-1}(1 + \log \|f\|_{A(G)}\|f\|_{L^\infty(\mu_G)}^{-1}).$$

2.1.1 The proof of Theorem 2.1.2

We say that a set of characters Λ is dissociated if

$$m \in \{-1,0,1\}^\Lambda \text{ and } m.\Lambda = 0_{\widehat{G}} \text{ imply that } m \equiv 0.$$

We have the following simple lemma regarding dissociated sets.

Lemma 2.1.3. *Suppose that* Γ *is a set of characters on* G *and* Λ *is a maximal dissociated subset of* Γ*. Then* $\Gamma \subset \langle \Lambda \rangle$*.*

To prove this one supposes, for a contradiction, that there is a $\gamma \in \Gamma \setminus \langle \Lambda \rangle$. If one adds this γ to Λ it is easy to see that the resulting set is strictly larger and dissociated.

In view of this lemma Theorem 2.1.2 follows from:

Proposition 2.1.4. *Suppose that* $f \in A(G)$*, and* Λ *a dissociated subset of* $\{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geqslant \epsilon \|f\|_{L^\infty(\mu_G)}\}$ *for some* $\epsilon \in (0, 1]$*. Then*

$$|\Lambda| \ll \epsilon^{-1}(1 + \log \|f\|_{A(G)} \|f\|^{-1}_{L^\infty(\mu_G)}).$$

We prove this using a standard argument for which we require an auxiliary measure.

Proposition 2.1.5 (Auxiliary measure)**.** *Suppose that* Λ *is a dissociated set of characters on* G *and* $\omega \in \ell^\infty(\Lambda)$ *has* $\|\omega\|_{\ell^\infty(\Lambda)} \leqslant 1$*. Then for any* $\eta \in (0, 1]$ *there is a measure* $\mu_\eta \in M(G)$ *such that*

$$\widehat{\mu_\eta}|_\Lambda = \omega, \|\mu_\eta\| \ll (1 + \log \eta^{-1}) \text{ and } |\widehat{\mu_\eta}(\gamma)| \leqslant \eta \text{ for all } \gamma \notin \Lambda.$$

Constructing these measures is the heart of the argument, so before we do this we finish off Proposition 2.1.4.

Proof of Proposition 2.1.4. We define

$$\omega(\lambda) := \frac{\widehat{f}(\lambda)}{|\widehat{f}(\lambda)|} \text{ for all } \lambda \in \Lambda.$$

$\omega \in \ell^\infty(\Lambda)$ and $\|\omega\|_{\ell^\infty(\Lambda)} \leqslant 1$ so we may apply Proposition 2.1.5 to get the auxiliary measure μ_η corresponding to ω. We examine the inner product

$\langle f, \mu_\eta \rangle$.

$$\begin{aligned}
|\langle f, \mu_\eta \rangle| &= |\sum_{\gamma \in \widehat{G}} \widehat{f}(\gamma)\overline{\widehat{\mu_\eta}(\gamma)}| \text{ by Plancherel's Theorem,}\\
&= |\sum_{\lambda \in \Lambda} \widehat{f}(\lambda)\overline{\widehat{\mu_\eta}(\lambda)} + \sum_{\gamma \notin \Lambda} \widehat{f}(\gamma)\overline{\widehat{\mu_\eta}(\gamma)}|\\
&\geqslant |\sum_{\lambda \in \Lambda} \widehat{f}(\lambda)\overline{\widehat{\mu_\eta}(\lambda)}| - |\sum_{\gamma \notin \Lambda} \widehat{f}(\gamma)\overline{\widehat{\mu_\eta}(\gamma)}|\\
&\geqslant |\sum_{\lambda \in \Lambda} \widehat{f}(\lambda)\overline{\omega(\lambda)}| - \eta \sum_{\gamma \notin \Lambda} |\widehat{f}(\gamma)| \text{ from the properties of } \mu_\eta,\\
&\geqslant \sum_{\lambda \in \Lambda} |\widehat{f}(\lambda)| - \eta \|f\|_{A(G)}\\
&\geqslant |\Lambda|\epsilon \|f\|_{L^\infty(\mu_G)} - \eta \|f\|_{A(G)}.
\end{aligned}$$

However

$$|\langle f, \mu_\eta \rangle| \leqslant \|f\|_{L^\infty(\mu_G)} \|\mu_\eta\| \ll \|f\|_{L^\infty(\mu_G)}(1 + \log \eta^{-1}),$$

so that

$$\|f\|_{L^\infty(\mu_G)}(1 + \log \eta^{-1}) \gg |\Lambda|\epsilon \|f\|_{L^\infty(\mu_G)} - \eta \|f\|_{A(G)}.$$

Choosing $\eta^{-1} = \|f\|_{A(G)} \|f\|_{L^\infty(\mu_G)}^{-1}$ yields the result. □

2.1.2 Constructing the auxiliary measure

The construction of the auxiliary measure is best illustrated in the model setting of $\mathbb{F}_2^n$ where we benefit from two simplifications. Suppose that Λ is a set of characters on $\mathbb{F}_2^n$. Then

- $\langle \Lambda \rangle$ is simply the subspace of $\widehat{G}$ generated by Λ;
- Λ is dissociated if and only if it is linearly independent over $\widehat{\mathbb{F}_2^n}$.

The first of these is simply a convenience while the second represents the major obstacle in transferring the arguments of this subsection to the general setting. We shall prove the following result.

Proposition 2.1.6. *Suppose that* Λ *is a linearly independent set of characters on* $\mathbb{F}_2^n$ *and* $\omega : \Lambda \to [-1, 1]$. *Then for any* $\eta \in (0, 1]$ *there is a measure* $\mu_\eta \in M(\mathbb{F}_2^n)$ *such that*

$$\widehat{\mu_\eta}|_\Lambda = \omega, \|\mu_\eta\| \ll (1 + \log \eta^{-1}) \text{ and } |\widehat{\mu_\eta}(\gamma)| \leqslant \eta \text{ for all } \gamma \notin \Lambda.$$

In the next section we engage in the technical process of extending this argument to arbitrary finite abelian groups.

Riesz products are the building blocks of the measure; we record the basic definition now.

Riesz products

Suppose that Λ is a set of characters. If $\omega : \Lambda \to [-1, 1]$ then we define the product

$$p_\omega := \prod_{\lambda \in \Lambda} (1 + \omega(\lambda)\lambda). \tag{2.1.3}$$

Such a product is called a Riesz product, and although it has formally been defined as a function we think of it as a measure. It is easy to see that it is real and non-negative from which it follows that $\|p_\omega\| = \widehat{p_\omega}(0_{\widehat{G}})$. Further, expanding out the product reveals that $\operatorname{supp} \widehat{p_\omega} \subset \langle \Lambda \rangle$.

If Λ is linearly independent then we can easily compute the Fourier transform of a Riesz product. Suppose that $\gamma \in \langle \Lambda \rangle$. Then there is a unique $m : \Lambda \to \{0, 1\}$ such that $\gamma = m.\Lambda$ by the linear independence of Λ, so

$$\widehat{p_\omega}(\gamma) := \prod_{\substack{\lambda \in \Lambda \\ m_\lambda \neq 0}} \omega(\lambda).$$

This leads to the observation that $\|p_\omega\| = \widehat{p_\omega}(0_{\widehat{G}}) = 1$ and $\widehat{p_\omega}|_\Lambda = \omega$. Moreover if $t \in [-1, 1]$ then

$$\widehat{p_{t\omega}}(m.\Lambda) := t^{|m|}\widehat{p_\omega}(m.\Lambda) \text{ where, as before, } |m| = \sum_{\lambda \in \Lambda} |m_\lambda|.$$

So, if $|m| > 1$ then

$$|\widehat{p_{t\omega}}(m.\Lambda)| \leqslant |t|^2 |\widehat{p_\omega}(m.\Lambda)| \leqslant |t|^2 \|p_\omega\| = |t|^2$$

It follows that a lot of the Fourier coefficients of $p_{t\omega}$ are already small if $|t|$ is small. By taking $\mu_\eta := \eta^{-1} p_{\eta\omega}$ we get a well known primitive version of the auxiliary measure of Proposition 2.1.5.

Proposition 2.1.7 (Primitive auxiliary measure)**.** *Suppose that Λ is a linearly independent set of characters on $\mathbb{F}_2^n$ and $\omega : \Lambda \to [-1, 1]$. Then for any $\eta \in (0, 1]$ there is a measure $\mu_\eta \in M(\mathbb{F}_2^n)$ such that*

$$\widehat{\mu_\eta}|_\Lambda = \omega, \|\mu_\eta\| \ll \eta^{-1} \text{ and } |\widehat{\mu_\eta}(\gamma)| \leqslant \eta \text{ for all } \gamma \notin \Lambda \cup \{0_{\widehat{G}}\}.$$

The basic idea for improving the measure of Proposition 2.1.7 rests on the observation that if $|m|$ is large then $|\widehat{p_{t\omega}}(m.\Lambda)|$ is in fact guaranteed to be *very* small. To construct a better measure we take linear combinations of Riesz products so that their Fourier transforms cancel on the characters $m.\Lambda$ where $|m|$ is small (except of course for $|m| = 1$). Begin by considering

$$\nu_t := \frac{1}{2}(p_{t\omega} - p_{-t\omega}).$$

Then

$$\widehat{\nu_t}|_\Lambda = t\omega, \|\nu_t\| \leqslant 1, |\widehat{\nu_t}(m.\Lambda)| \leqslant t^{|m|}$$

and

$$\widehat{\nu_t}(m.\Lambda) = 0 \text{ if } |m| \equiv 0 \pmod 2.$$

It follows that

$$\widehat{\nu_t}|_\Lambda = t\omega, \|\nu_t\| \leqslant 1 \text{ and } |\widehat{\nu_t}(\gamma)| \leqslant t^3 \text{ for all } \gamma \notin \Lambda.$$

If we put $\mu_\eta = \nu_{\sqrt{\eta}}$ then we have a version of Proposition 2.1.6 with $\|\mu_\eta\| \ll \eta^{-1/2}$ instead of $\|\mu_\eta\| \ll (1 + \log \eta^{-1})$.

More generally we consider a measure τ on $[-1,1]$ and put

$$\nu_\tau := \int p_{t\omega} d\tau(t).$$

Then

$$\|\nu_\tau\| \leqslant \sup_{t\in[-1,1]} \|p_{t\omega}\|.\|\tau\| = \|\tau\| \text{ and } \widehat{\nu_\tau}(m.\Lambda) = \int t^{|m|} d\tau(t)\widehat{p_\omega}(m.\Lambda).$$

Following the idea of trying to get the Fourier transforms of the Riesz products in ν_τ to cancel on $\{m.\Lambda : |m| = r\}$, we should like a measure τ_l with $\|\tau_l\|$ minimal subject to

$$\int t^k d\tau_l(t) = 0 \text{ for } 1 < k \leqslant l, \int d\tau_l(t) = 0, \text{ and } \int t d\tau_l(t) = 1.$$

Méla, in [Mél82], already had this idea, and moreover for the purpose of constructing essentially the auxiliary measure we want. To produce τ_l he constructs a measure σ_l with the following properties:

Lemma 2.1.8. ([Mél82, Lemma 4, §7]) *Suppose that $l > 1$ is an integer. Then there is a measure σ_l on $[0,1]$ such that*

$$\int s^{2k-1} d\sigma_l(s) = 0 \textit{ for } 2 \leqslant k \leqslant l, \int s d\sigma_l(s) = 1 \textit{ and } \|\sigma_l\| = 2l - 1.$$

He chooses σ_l to be (the measure induced by) the polynomial

$$s + ((-1)^l/(2l-1))P_{2l-1}(s)$$

where P_{2l-1} is the Chebychev polynomial of order $2l-1$. Once this is known it is not hard to verify the properties of σ_l.

We take τ_{2l} to be the odd measure on $[-1,1]$ which extends $2\sigma_l(2s)$ on $[0,1/2]$, and the null measure on $[1/2,1]$. It is easy, then, to verify the following.

Lemma 2.1.9. *Suppose that $l > 1$ is an integer. Then the measure τ_{2l} on*

$[-1,1]$ *has* $\|\tau_{2l}\| \leqslant 2(2l-1)$,

$$\int t^k d\tau_{2l}(t) = \begin{cases} 0 \text{ if } k \leqslant 2l \text{ and } k \neq 1 \\ 1 \text{ if } k = 1 \end{cases}$$

and $|\int t^k d\tau_{2l}(t)| \leqslant 2^{1-k}$ *for all* k.

Proposition 2.1.6 follows from this by writing $l = \lceil 2^{-1} \log_2 \eta^{-1} \rceil$ and then letting $\mu_\eta = \nu_{\tau_{2l}}$.

2.1.3 The general construction of the auxiliary measure

To construct the measure in the general case we also requires Riesz products. Here, however, they are slightly more complicated.

Riesz products

Suppose that Λ is a finite set of characters. We say that $\omega \in \ell^\infty(\Lambda \cup -\Lambda)$ is hermitian if

$$\omega(\lambda^{-1}) = \overline{\omega(\lambda)} \text{ for all } \lambda \in \Lambda;$$

if ω also satisfies $\|\omega\|_{\ell^\infty(\Lambda\cup-\Lambda)} \leqslant 1$ then we define the product

$$p_\omega := \prod_{\lambda \in \Lambda} \left(1 + \frac{\omega(\lambda)\lambda + \omega(\lambda^{-1})\lambda^{-1}}{2}\right). \tag{2.1.4}$$

As before such a product is called a Riesz product and is regarded as a measure. Again it is easy to see that it is real and non-negative from which it follows that $\|p_\omega\| = \widehat{p_\omega}(0_{\widehat{G}})$. Further expanding out the product reveals that $\operatorname{supp} \widehat{p_\omega} \subset \langle \Lambda \rangle$.

We had an easy time computing the Fourier transform of Riesz products in $\mathbb{F}_2^n$. In general it is more complicated. We can expand out the product in

(2.1.4) to see that:

$$\widehat{p_\omega}(\gamma) = \sum_{m \in \{-1,0,1\}^\Lambda : m.\Lambda = \gamma} \prod_{\substack{\lambda \in \Lambda: \\ m_\lambda \neq 0}} \frac{\omega(\lambda^{m_\lambda})}{2}. \tag{2.1.5}$$

To keep track of this we say that $\widetilde{p}$, defined on $\{-1, 0, 1\}^\Lambda$, is a formal Fourier transform[1] for $p \in M(G)$ if

$$\widehat{p}(\gamma) = \sum_{m : m.\Lambda = \gamma} \widetilde{p}(m) \text{ for all } \gamma \in \widehat{G}. \tag{2.1.6}$$

The measures which we are interested in are of the form

$$p := \int p_{t\omega} d\tau(t),$$

for $\omega \in \ell^\infty(\Lambda \cup -\Lambda)$ hermitian with $\|\omega\|_{\ell^\infty(\Lambda \cup -\Lambda)} \leqslant 1$, and τ a real measure on $[-1, 1]$. It follows from (2.1.5) and linearity of the Fourier transform that $\widetilde{p}$ defined by

$$\widetilde{p}(m) := \int t^{|m|} d\tau(t). \prod_{\substack{\lambda \in \Lambda: \\ m_\lambda \neq 0}} \frac{\omega(\lambda^{m_\lambda})}{2} \text{ for all } m \in \{-1, 0, 1\}^\Lambda, \tag{2.1.7}$$

is a formal Fourier transform for p.

If Λ is dissociated then when $\gamma = 0_{\widehat{G}}$ there is only one summand in the expression for $\widehat{p_\omega}(\gamma)$ given in (2.1.5) and that has a value of 1, so

$$\|p_\omega\| = \widehat{p_\omega}(0_{\widehat{G}}) = 1. \tag{2.1.8}$$

Dissociativity makes computing the Fourier transform easy for $\gamma = 0_{\widehat{G}}$ by restricting the number of non-zero summands in (2.1.5); a lemma of Rider's [Rid66] provides a result for more general γ:

Lemma 2.1.10. *Suppose that Λ is a dissociated set of characters on G.*

[1] Formal Fourier transforms are not in general unique.

Then for all $\gamma \in \widehat{G}$

$$|\{m \in \{-1,0,1\}^\Lambda : |m| = r, m.\Lambda = \gamma\}| \leqslant 2^r.$$

Proof. Let ω be the hermitian function which takes Λ to 1. For this choice of ω (2.1.5) is

$$\widehat{p_\omega}(\gamma) = \sum_{r \geqslant 0} 2^{-r} |\{m \in \{-1,0,1\}^\Lambda : |m| = r, m.\Lambda = \gamma\}|$$

But $|\widehat{p_\omega}(\gamma)| \leqslant \|p_\omega\| = 1$ since Λ is dissociated which yields the conclusion. □

Proposition 2.1.11. *Suppose that* Λ *is a dissociated set of characters on* G *with no elements of order 2 and* $\omega \in \ell^\infty(\Lambda \cup -\Lambda)$ *is hermitian and has* $\|\omega\|_{\ell^\infty(\Lambda \cup -\Lambda)} \leqslant 1$*. Then for any* $\eta \in (0,1]$ *there is a measure* $\nu_\eta \in M(G)$ *such that*

$$\widehat{\nu_\eta}|_{\Lambda \cup -\Lambda} = \omega, \|\nu_\eta\|_1 \ll (1 + \log \eta^{-1}) \text{ and } |\widehat{\nu_\eta}(\gamma)| \leqslant \eta \text{ for all } \gamma \notin \Lambda \cup -\Lambda.$$

Proof. Fix an integer $l > 1$ to be optimized later and let τ_{2l} be the measure yielded by Lemma 2.1.9. Define

$$p := \int p_{t\omega} d\tau_{2l}(t),$$

and let $\widetilde{p}$ be the formal Fourier transform for p defined by (2.1.7). $\widetilde{p}(m) = 0$ if $|m| = 0$ by definition of τ_{2l} and $\widetilde{p}$, so

$$\begin{aligned}
\left| \widehat{p}(\gamma) - \sum_{\substack{|m|=1 \\ m.\Lambda=\gamma}} \widetilde{p}(m) \right| &\leqslant \sum_{r \geqslant 2} \sum_{\substack{|m|=r \\ m.\Lambda=\gamma}} |\widetilde{p}(m)| \text{ by definition (2.1.6),} \\
&\leqslant \sum_{r > 2l} \sum_{\substack{|m|=r \\ m.\Lambda=\gamma}} |\widetilde{p}(m)| \text{ since } \int t^r d\tau_{2l}(t) = 0 \text{ for } r \leqslant 2l, \\
&\leqslant \sum_{r > 2l} \sup_{\substack{|m|=r \\ m.\Lambda=\gamma}} |\widetilde{p}(m)| |\{m : |m| = r, m.\Lambda = \gamma\}|.
\end{aligned}$$

Now Λ is dissociated, so Lemma 2.1.10 applies to give

$$\begin{aligned}\left|\widehat{p}(\gamma) - \sum_{\substack{|m|=1\\ m.\Lambda=\gamma}} \widetilde{p}(m)\right| &\leqslant \sum_{r>2l} 2^r \sup_{\substack{|m|=r\\ m.\Lambda=\gamma}} |\widetilde{p}(m)|,\\ &\leqslant \sum_{r>2l} 2^r \int t^r d\tau_{2l}(t)(2^{-1}\|\omega\|_{\ell^\infty(\Lambda\cup-\Lambda)})^r\\ &\leqslant \sum_{r>2l} 2(2^{-1}\|\omega\|_{\ell^\infty(\Lambda\cup-\Lambda)})^r \text{ since } |\int t^r d\tau_{2l}(t)| \leqslant 2^{1-r},\\ &\leqslant 2^{1-2l}\|\omega\|_{\ell^\infty(\Lambda\cup-\Lambda)}. \qquad (2.1.9)\end{aligned}$$

Now let l be such that $2^{3-2l} \leqslant \eta$ but $l \ll (1 + \log\eta^{-1})$ and put $\nu_\eta^{(1)} := 2p$. Then

(i). If $\gamma \in \Lambda \cup -\Lambda$ then

$$\sum_{\substack{|m|=1\\ m.\Lambda=\gamma}} \widetilde{p}(m) = \int t d\tau_{2l}(t)\frac{\omega(\gamma)}{2} = \frac{\omega(\gamma)}{2}$$

since Λ has no elements of order 2. Hence by (2.1.9)

$$|\widehat{\nu_\eta^{(1)}}(\gamma) - \omega(\gamma)| \leqslant 2^{2-2l}\|\omega\|_{\ell^\infty(\Lambda\cup-\Lambda)} \leqslant 2^{-1}\|\omega\|_{\ell^\infty(\Lambda\cup-\Lambda)}. \qquad (2.1.10)$$

(ii). If $\gamma \notin \Lambda \cup -\Lambda$ then

$$\sum_{\substack{|m|=1\\ m.\Lambda=\gamma}} \widetilde{p}(m) = 0,$$

so by (2.1.9)

$$|\widehat{\nu_\eta^{(1)}}(\gamma)| \leqslant 2^{-1}\eta\|\omega\|_{\ell^\infty(\Lambda\cup-\Lambda)}. \qquad (2.1.11)$$

(iii). $\|\nu_\eta^{(1)}\| \leqslant 2\|\tau_{2l}\|$ by p and the triangle inequality.

(iv). $\widehat{\nu_\eta^{(1)}}|_{\Lambda\cup-\Lambda}$ is hermitian since τ_{2l} is real.

We can apply the foregoing recursively to the hermitian functions ω, $2(\omega -$

$\nu_\eta^{(1)})|_{\Lambda\cup-\Lambda}$, $2(2(\omega-\nu_\eta^{(1)})-\nu_\eta^{(2)})|_{\Lambda\cup-\Lambda}$,... to get a sequence of measures $\nu_\eta^{(1)}$, $\nu_\eta^{(2)}$, $\nu_\eta^{(3)}$,... such that:

(i). If $\gamma\in\Lambda\cup-\Lambda$ then

$$|\sum_{k=1}^{n}2^{-(k-1)}\widehat{\nu_\eta^{(k)}}(\gamma)-\omega(\gamma)|\leqslant 2^{-n}.$$

(ii). If $\gamma\not\in\Lambda\cup-\Lambda$ then

$$|\sum_{k=1}^{n}2^{-(k-1)}\widehat{\nu_\eta^{(k)}}(\gamma)|\leqslant\sum_{k=1}^{n}2^{-(k-1)}.\frac{\eta}{2}\leqslant\eta.$$

(iii).

$$\|\sum_{k=1}^{n}2^{-(k-1)}\nu_\eta^{(k)}\|\leqslant\sum_{k=1}^{n}2^{-(k-1)}\|\nu_\eta^{(k)}\|\leqslant 2^2\|\tau_{2l}\|$$

The sum $\sum_{k=1}^{n}2^{-(k-1)}\nu_\eta^{(k)}$ converges to a measure $\nu_\eta\in M(G)$ with the required properties since $\|\tau_{2l}\|\ll l\ll(1+\log\eta^{-1})$. □

Finally we modify the above proposition so that the Fourier transform is small on $-\Lambda\setminus\Lambda$.

Proof of Proposition 2.1.5. Note that the three element set $H:=\{z\in\mathbb{C}:z^3=1\}$ is a subgroup of S^1 under multiplication. Let $G':=G\times H$ and identify its dual with $\widehat{G}\times(\mathbb{Z}/3\mathbb{Z})$. Let $\Lambda'=\Lambda\times\{1+3\mathbb{Z}\}$, which is dissociated since Λ is dissociated, and has no elements of order 2 since $1+3\mathbb{Z}$ is not of order 2 in $\mathbb{Z}/3\mathbb{Z}$. Let ω' be the hermitian map on $\Lambda'\cup-\Lambda'$ induced by $\omega'(\lambda,1+3\mathbb{Z}):=\omega(\lambda)$. Apply Proposition 2.1.11 to G', Λ' and ω' to get the measure $\nu_\eta\in M(G')$. Let μ_η be the measure induced by

$$f\mapsto\int_{(x,z)\in G'}f(x)\overline{z}d\nu_\eta(x,z).$$

If $\gamma \in \widehat{G}$ then

$$\widehat{\mu_\eta}(\gamma) = \int_{(x,z)\in G'} \overline{\gamma}(x)\overline{z}d\nu_\eta(x,z) = \widehat{\nu_\eta}(\gamma, 1+3\mathbb{Z}).$$

We verify the three properties of μ_η from the corresponding properties of ν_η:

(i). If $\lambda \in \Lambda$ then $\widehat{\mu_\eta}(\lambda) = \widehat{\nu_\eta}(\lambda, 1+3\mathbb{Z}) = \omega'(\lambda, 1+3\mathbb{Z}) = \omega(\lambda)$.

(ii).

$$\|\mu_\eta\| = \sup_{f:\|f\|_{L^\infty(\mu_G)}\leqslant 1} \left| \int_{(x,z)\in G'} f(x)\overline{z}d\nu_\eta(x,z)\right| \leqslant \|\nu_\eta\| \ll (1+\log \eta^{-1}).$$

(iii). If $\gamma \notin \Lambda$ then $(\gamma, 1+3\mathbb{Z}) \notin \Lambda' \cup -\Lambda'$ so $|\widehat{\mu_\eta}(\gamma)| \leqslant \eta$.

□

2.1.4 Remarks on Theorem 2.1.2

The technique of applying Lemma 2.1.3 to reduce Theorem 2.1.2 to Proposition 2.1.4 is used by Chang, [Cha02], in the proof of Theorem 2.1.1. The analogue of Proposition 2.1.4 in that case is proved using the dual formulation of Rudin's Inequality, which states that if Λ is a dissociated set of characters on G and $f \in L^2(\mu_G)$ then

$$\|\widehat{f}|_\Lambda\|_2 \ll \sqrt{\frac{p}{p-1}}\|f\|_p \text{ for } 1 < p \leqslant 2.$$

Halász, [Hal81], uses the inner product technique of Proposition 2.1.4 to prove a non-Fourier result in discrepancy theory and employs a Riesz product (for a different Hilbert space) as the auxiliary measure. An exposition of his result may be found in Chazelle [Cha00] and this was the original motivation for our result.

Green pointed out the fact that Méla, in [Mél82], had already used the method of linear combinations of Riesz products to construct the auxiliary measure we require. Méla uses it as an example to show that a result of his regarding ϵ-idempotent measures is essentially best possible. In fact it follows from Méla's work that essentially no better auxiliary measure than the one we have constructed exists.

2.2 Fourier analysis on Bohr sets

Our attention now turns to developing the 'approximate groups' which were mentioned at the start of the chapter, and Fourier analysis 'local' to them.

If Γ is a set of characters then we define the annihilator of Γ to be

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

The annihilator is a subgroup of G. It is easy to localize the Fourier transform to $x' + \Gamma^\perp$: The local transform is the map

$$L^1(x' + \mu_{\Gamma^\perp}) \to \ell^\infty(\widehat{G}); f \mapsto (fd(x' + \mu_{\Gamma^\perp}))^\wedge,$$

where we recall the measure $x' + \mu_{\Gamma^\perp}$ denotes the measure $\mu_{\Gamma^\perp}$ translated by x'. Note that the right hand side is constant on cosets of $\Gamma^{\perp\perp}$ (defined in the obvious manner) and so can be thought of as an element of $\ell^\infty(\widehat{G}/\Gamma^{\perp\perp})$.

Bourgain, in [Bou99], observed that one can localize the Fourier transform to translates of typical 'approximate' annihilators and retain approximate versions of a number of the standard results for the Fourier transform on finite abelian groups. Since his original work various expositions and extensions have appeared most notably in the various papers of Green and Tao. Indeed all the results of this section can be found in [GT08], for example.

Throughout the remainder of the section Γ is a set of characters on G and $\delta \in (0, 1]$. We can define a natural valuation on S^1, namely

$$\|z\| := \frac{1}{2\pi} \inf_{n \in \mathbb{Z}} |2\pi n + \arg z|,$$

which can be used to measure how far $\gamma(x)$ is from 1. Consequently we define a prototype for an approximate annihilator:

$$B(\Gamma, \delta) := \{x \in G : \|\gamma(x)\| \leqslant \delta \text{ for all } \gamma \in \Gamma\},$$

called a Bohr set. A translate of such a set is called a Bohr neighborhood. We adopt the convention that if $B(\Gamma, \delta)$ is a Bohr set then the size of Γ is denoted by d.

The following simple averaging argument will be very useful. We include the proof, which appears in many places, but in particular in [TV06], for completeness.

Lemma 2.2.1. *Suppose that $B(\Gamma, \delta)$ is a Bohr set. Then $\mu_G(B(\Gamma, \delta)) \geqslant \delta^d$ where, as our convention states, $d := |\Gamma|$.*

Proof. For each $\theta \in \mathbb{T}^\Gamma$ define the set

$$B_\theta := \{x \in G : \|\gamma(x) - \exp(2\pi i \theta_\gamma)\| \leqslant \delta/2 \text{ for all } \gamma \in \Gamma\}.$$

If $x' \in B_\theta$ then the map $x \mapsto x - x'$ is an injection from B_θ to $B(\Gamma, \delta)$, whence $\mu_G(B_\theta) \leqslant \mu_G(B(\Gamma, \delta))$.

If we pix θ uniformly at random, then for a fixed $x \in G$ it is easy to see that $\mathbb{P}(x \in B_\theta) = \delta^d$. It follows by linearity of expectation that $\mathbb{E}\mu_G(B_\theta) = \delta^d$ from which the bound follows. □

Hence we write $\beta_{\Gamma,\delta}$ for the measure induced on $B(\Gamma, \delta)$ by μ_G, normalised so that $\|\beta_{\Gamma,\delta}\| = 1$. This is sometimes referred to as the normalised Bohr cutoff.

Annihilators are subgroups of G, a property which, at least in an approximate form, we would like to recover. Suppose that $\eta \in (0, 1]$. Then $B(\Gamma, \delta) + B(\Gamma, \eta\delta) \subset B(\Gamma, (1 + \eta)\delta)$. If $B(\Gamma, (1 + \eta)\delta)$ is not much bigger than $B(\Gamma, \delta)$ then we have a sort of approximate additive closure in the sense that $B(\Gamma, \delta) + B(\Gamma, \eta\delta) \approx B(\Gamma, (1 + \eta)\delta)$. Not all Bohr sets have this property, however, Bourgain showed that typically they do. For our purposes we have the following proposition.

Proposition 2.2.2. *Suppose that* Γ *a set of* d *characters on* G *and* $\delta \in (0,1]$. *There is an absolute constant* $c_{\mathcal{R}} > 0$ *and a* $\delta' \in [\delta/2, \delta)$ *such that*

$$\frac{\mu_G(B(\Gamma,(1+\kappa)\delta'))}{\mu_G(B(\Gamma,\delta'))} = 1 + O(|\kappa|d)$$

whenever $|\kappa|d \leqslant c_{\mathcal{R}}$.

This result is not as easy as the rest of the section. It uses a covering argument; a nice proof can be found in [GT08], but see also the proof of Proposition 2.4.5. We say that δ' is regular for Γ or that $B(\Gamma,\delta')$ is regular if

$$\frac{\mu_G(B(\Gamma,(1+\kappa)\delta'))}{\mu_G(B(\Gamma,\delta'))} = 1 + O(|\kappa|d) \text{ whenever } |\kappa|d \leqslant c_{\mathcal{R}}.$$

It is regular Bohr sets to which we localize the Fourier transform and we begin by observing that regular Bohr cutoffs are approximately translation invariant and so function as normalised approximate Haar measures.

Lemma 2.2.3. *Suppose that* $B(\Gamma,\delta)$ *is a regular Bohr set. If* $y \in B(\Gamma,\delta')$ *then* $\|(y+\beta_{\Gamma,\delta}) - \beta_{\Gamma,\delta}\| \ll d\delta'\delta^{-1}$ *where we recall that* $y+\beta_{\Gamma,\delta}$ *denotes the measure* $\beta_{\Gamma,\delta}$ *translated by* y.

Proof. Note that $\operatorname{supp}((y+\beta_{\Gamma,\delta}) - \beta_{\Gamma,\delta}) \subset B(\Gamma,\delta+\delta') \setminus B(\Gamma,\delta-\delta')$ whence

$$\|(y+\beta_{\Gamma,\delta}) - \beta_{\Gamma,\delta}\| \leqslant \frac{\mu_G(B(\Gamma,\delta+\delta') \setminus B(\Gamma,\delta-\delta'))}{\mu_G(B(\Gamma,\delta))} \ll d\delta'\delta^{-1}$$

by regularity. □

In applications the following two simple corollaries will be useful but they should be ignored until they are used.

Corollary 2.2.4. *Suppose that* $B(\Gamma,\delta)$ *is a regular Bohr set. If* $\mu \in M(G)$ *has* $\operatorname{supp}\mu \subset B(\Gamma,\delta')$ *then* $\|\beta_{\Gamma,\delta} * \mu - \beta_{\Gamma,\delta}\int d\mu\| \ll \|\mu\| d\delta'\delta^{-1}$.

Proof. The measures $\beta_{\Gamma,\delta}*\mu$ and $\beta_{\Gamma,\delta}\int d\mu$ agree inside $B(\Gamma,\delta-\delta')$ and outside $B(\Gamma,\delta+\delta')$, furthermore $\|\beta_{\Gamma,\delta}*\mu\| \leqslant \|\mu\|$ and $\|\beta_{\Gamma,\delta}\int d\mu\| \leqslant \|\mu\|$, whence

$$\|\beta_{\Gamma,\delta} * \mu - \beta_{\Gamma,\delta}\int d\mu\| \ll \|\mu\| \frac{\mu_G(B(\Gamma,\delta+\delta') \setminus B(\Gamma,\delta-\delta'))}{\mu_G(B(\Gamma,\delta))} \ll \|\mu\| d\delta'\delta^{-1}$$

by regularity. □

Corollary 2.2.5. *Suppose that $B(\Gamma,\delta)$ is a regular Bohr set. If $f \in L^\infty(\mu_G)$ then*

$$\sup_{x \in G} \|f * \beta_{\Gamma,\delta} - f * \beta_{\Gamma,\delta}(x)\|_{L^\infty(x+\beta_{\Gamma,\delta'})} \ll \|f\|_{L^\infty(\mu_G)} d\delta'\delta^{-1}.$$

Proof. Note that

$$\begin{aligned} |f * \beta_{\Gamma,\delta}(x+y) - f * \beta_{\Gamma,\delta}(x)| &= |f * ((-y+\beta_{\Gamma,\delta}) - \beta_{\Gamma,\delta})(x)| \\ &\leqslant \|f\|_{L^\infty(\mu_G)} \|(-y+\beta_{\Gamma,\delta}) - \beta_{\Gamma,\delta}\|. \end{aligned}$$

The result follows by Lemma 2.2.3. □

With an approximate Haar measure we are in a position to define the local Fourier transform: Suppose that $x' + B(\Gamma,\delta)$ is a regular Bohr neighborhood (defined in the obvious way). Then we define the Fourier transform local to $x' + B(\Gamma,\delta)$ by

$$L^1(x' + \beta_{\Gamma,\delta}) \to \ell^\infty(\widehat{G}); f \mapsto (fd(x' + \beta_{\Gamma,\delta}))^\wedge.$$

The translation of the Bohr set by x' simply twists the Fourier transform and is unimportant for the most part so we tend to restrict ourselves to the case when $x' = 0_G$.

$\widehat{fd\mu_{\Gamma^\perp}}$ was constant on cosets of $\Gamma^{\perp\perp}$. In the approximate setting we have an approximate analogue on which $\widehat{fd\beta_{\Gamma,\delta}}$ does not vary too much. There are a number of possibilities:

$$\begin{aligned} &\{\gamma : |1 - \gamma(x)| \leqslant \epsilon \text{ for all } x \in B(\Gamma,\delta)\} && \text{for } \epsilon \in (0,1] \\ &\{\gamma : |1 - \widehat{\beta_{\Gamma,\delta}}(\gamma)| \leqslant \epsilon\} && \text{for } \epsilon \in (0,1] \\ &\{\gamma : |\widehat{\beta_{\Gamma,\delta}}(\gamma)| \geqslant \epsilon\} && \text{for } \epsilon \in (0,1]. \end{aligned}$$

In applications each of these classes of sets is useful and so we should like all of them to be approximately equivalent. There is a clear chain of inclusions between the classes, where the first is contained in the second is contained in the third for all $\epsilon \in (0,1]$. For a small cost in the width of the Bohr set we can ensure that the sets in the third class are contained in those in the first.

Lemma 2.2.6. *Suppose that $B(\Gamma,\delta)$ is a regular Bohr set. Suppose that $\eta_1,\eta_2 > 0$. Then there is a $\delta' \gg \eta_1\eta_2\delta/d$ such that*

$$\{\gamma : |\widehat{\beta_{\Gamma,\delta}}(\gamma)| \geqslant \eta_1\} \subset \{\gamma : |1-\gamma(x)| \leqslant \eta_2 \text{ for all } x \in B(\Gamma,\delta')\}.$$

Proof. If $x \in B(\Gamma,\delta')$ then we have

$$\eta_1|1-\gamma(x)| \leqslant |\widehat{\beta_{\Gamma,\delta}}(\gamma)||1-\overline{\gamma(x)}| = |((x+\widehat{\beta_{\Gamma,\delta})-\beta_{\Gamma,\delta}})(\gamma)| \ll d\delta'\delta^{-1}$$

by Lemma 2.2.3. It follows that we may pick $\delta' \gg \eta_1\eta_2\delta/d$ such that $|1-\gamma(x)| \leqslant \eta_2$ for all $x \in B(\Gamma,\delta')$. □

2.3 Local spectral structures

In §2.1 we recorded four different results regarding the structure of collections of characters supporting large values of the Fourier transform; in this section we prove local versions of these.

In [GT08] Green and Tao localized (2.1.1) when they proved the following proposition.

Proposition 2.3.1 (Localized (2.1.1))**.** *Suppose that $B(\Gamma,\delta)$ is a regular Bohr set. Suppose that $f \in L^2(\beta_{\Gamma,\delta})$ and $\epsilon,\eta \in (0,1]$. Write L_f for the quantity $\|f\|_{L^2(\beta_{\Gamma,\delta})}\|f\|_{L^1(\beta_{\Gamma,\delta})}^{-1}$. Then there is a set Λ of characters and a $\delta' \in (0,1]$ with*

$$|\Lambda| \ll \epsilon^{-2}L_f^2 \text{ and } \delta' \gg \epsilon^2\eta\delta/dL_f^2,$$

such that

$$\{\gamma \in \widehat{G} : |\widehat{fd\beta_{\Gamma,\delta}}(\gamma)| \geqslant \epsilon\|f\|_{L^1(\beta_{\Gamma,\delta})}\}$$

is contained in

$$\{\gamma \in \widehat{G} : |1-\gamma(x)| \leqslant \eta \text{ for all } x \in B(\Gamma\cup\Lambda,\delta')\}.$$

To see how this is a localization of (2.1.1) consider the case when $B(\Gamma, \delta) = G$. In this instance once can essentially ignore δ' and we have the conclusion that the characters supporting the large values of $\widehat{f}$, that is the set $\Delta := \{\gamma : |\widehat{f}(\gamma)| \geqslant \epsilon \|f\|_{L^1(\mu_G)}\}$, are contained in the set

$$\{\gamma : \gamma(x) \approx 1 \text{ for all } x \text{ for which } \lambda(x) \approx 1 \text{ for all } \lambda \in \Lambda\}$$

where Λ is a set of size $O(\epsilon^{-2}\|f\|_{L^2(\mu_G)}^2 \|f\|_{L^1(\mu_G)}^{-2})$. Now this set is in fact much larger than Λ since it contains all smaller linear combinations of elements of Λ. However, as we have mentioned before, this does not turn out to be an important difference.

As it happens, it is even easier to prove a local version of (2.1.2):[2]

Proposition 2.3.2 (Localized (2.1.2))**.** *Suppose that $B(\Gamma, \delta)$ is a regular Bohr set. Suppose that $f \in A(G)$ and $\epsilon, \eta \in (0, 1]$. Write A_f for the quantity $\|f\|_{A(G)}\|f\|_{L^\infty(\beta_{\Gamma,\delta})}^{-1}$. Then there is a set Λ of characters and a $\delta' \in (0, 1]$ with*

$$|\Lambda| \ll \epsilon^{-1} A_f \text{ and } \delta' \gg \epsilon\eta\delta/dA_f,$$

such that

$$\{\gamma \in \widehat{G} : |\widehat{fd\beta}(\gamma)| \geqslant \epsilon \|f\|_{L^\infty(\beta_{\Gamma,\delta})}\}$$

is contained in

$$\{\gamma \in \widehat{G} : |1 - \gamma(x)| \leqslant \eta \text{ for all } x \in B(\Gamma \cup \Lambda, \delta')\}.$$

We shall not concern ourselves with the proof of Proposition 2.3.2 because it is simpler than the proof of Proposition 2.3.1 and will in any case follow from the forthcoming local version of Theorem 2.1.2.

The objective of this section, then, is to prove local versions of Chang's Theorem (Theorem 2.1.1) and Theorem 2.1.2. Specifically we shall prove the following two results.

[2]In actual fact one might argue that a local version of (2.1.2) would have A_f equal to $\|f1_{B(\Gamma,\delta)}\|_{A(G)}\|f\|_{L^\infty(\beta_{\Gamma,\delta})}^{-1}$, however it is most useful for our work to work with the version of A_f which we have chosen.

Proposition 2.3.3 (Localized Chang's Theorem). *Suppose that* $B(\Gamma,\delta)$ *is a regular Bohr set. Suppose that* $f \in L^2(\beta_{\Gamma,\delta})$ *and* $\epsilon,\eta \in (0,1]$. *Write* L_f *for the quantity* $\|f\|_{L^2(\beta_{\Gamma,\delta})}\|f\|_{L^1(\beta_{\Gamma,\delta})}^{-1}$. *Then there is a set of characters* Λ *and a* $\delta' \in (0,1]$ *with*

$$|\Lambda| \ll \epsilon^{-2}(1+\log L_f) \text{ and } \delta' \gg \delta\eta\epsilon^2/d^2(1+\log L_f),$$

such that

$$\{\gamma \in \widehat{G} : |\widehat{f d\beta_{\Gamma,\delta}}(\gamma)| \geqslant \epsilon\|f\|_{L^1(\beta_{\Gamma,\delta})}\}$$

is contained in

$$\{\gamma \in \widehat{G} : |1-\gamma(x)| \leqslant \eta \text{ for all } x \in B(\Gamma\cup\Lambda,\delta')\}.$$

Proposition 2.3.4 (Localized Theorem 2.1.2). *Suppose that* $B(\Gamma,\delta)$ *a regular Bohr set. Suppose that* $f \in A(G)$ *and* $\epsilon,\eta \in (0,1]$. *Write* A_f *for the quantity* $\|f\|_{A(G)}\|f\|_{L^\infty(\beta_{\Gamma,\delta})}^{-1}$. *Then there is a set of characters* Λ *and a* $\delta' \in (0,1]$ *with*

$$|\Lambda| \ll \epsilon^{-1}(1+\log A_f) \text{ and } \delta' \gg \epsilon^2\eta\delta/d^2(1+\log A_f),$$

such that

$$\{\gamma \in \widehat{G} : |\widehat{f d\beta_{\Gamma,\delta}}(\gamma)| \geqslant \epsilon\|f\|_{L^\infty(\beta_{\Gamma,\delta})}\}$$

is contained in

$$\{\gamma \in \widehat{G} : |1-\gamma(x)| \leqslant \eta \text{ for all } x \in B(\Gamma\cup\Lambda,\delta')\}.$$

A key tool in the proof of Chang's Theorem and Theorem 2.1.2 is that of dissociativity; in the local setting we use the following variant. If S is a non-empty symmetric neighborhood of $0_{\widehat{G}}$ then we say that Λ is S-dissociated if

$$m \in \{-1,0,1\}^\Lambda \text{ and } m.\Lambda \in S \text{ implies that } m \equiv 0.$$

Vanilla dissociativity corresponds to taking $S = \{0_{\widehat{G}}\}$, and typically in the local setting S will be a set of characters at which $\widehat{\beta_{\Gamma,\delta}}$ is large for some Bohr set $B(\Gamma, \delta)$.

We require the following local version of Lemma 2.1.3.

Lemma 2.3.5. *Suppose that $B(\Gamma, \delta)$ is a regular Bohr set. Suppose that $\eta', \eta \in (0, 1]$ and Δ is a set of characters on G. If Λ is a maximal $\{\gamma : |\widehat{\beta_{\Gamma,\delta}}(\gamma)| \geqslant \eta'\}$-dissociated subset of Δ then there is a $\delta' \gg \min\{\eta/|\Lambda|, \eta'\eta\delta/d\}$ such that*

$$\Delta \subset \{\gamma : |1 - \gamma(x)| \leqslant \eta \text{ for all } x \in B(\Gamma \cup \Lambda, \delta')\}.$$

Then Proposition 2.3.3 and Proposition 2.3.4 follow from this lemma and the next two lemmas respectively.

Lemma 2.3.6. *Suppose that $B(\Gamma, \delta)$ is a regular Bohr set. Suppose that $f \in L^2(\beta_{\Gamma,\delta})$ and $\epsilon, \eta \in (0, 1]$. Write L_f for the quantity $\|f\|_{L^2(\beta_{\Gamma,\delta})}\|f\|^{-1}_{L^1(\beta_{\Gamma,\delta})}$. Then there is a $\delta' \gg \epsilon^2\delta/d(1 + \log L_f)$ regular for Γ such that if Λ is a $\{\gamma : |\widehat{\beta_{\Gamma,\delta'}}(\gamma)| \geqslant 1/3\}$-dissociated subset of $\{\gamma \in \widehat{G} : |\widehat{fd\beta_{\Gamma,\delta}}(\gamma)| \geqslant \epsilon\|f\|_{L^1(\beta_{\Gamma,\delta})}\}$ then*

$$|\Lambda| \ll \epsilon^{-2}(1 + \log L_f).$$

Lemma 2.3.7. *Suppose that $B(\Gamma, \delta)$ is a regular Bohr set. Suppose that $f \in A(G)$ and $\epsilon, \eta \in (0, 1]$. Write A_f for the quantity $\|f\|_{A(G)}\|f\|^{-1}_{L^\infty(\beta_{\Gamma,\delta})}$. Then there is a $\delta' \gg \epsilon^2\delta/d(1 + \log A_f)$ regular for Γ such that if Λ is a $\{\gamma : |\widehat{\beta_{\Gamma,\delta'}}(\gamma)| \geqslant 1/3\}$-dissociated subset of $\{\gamma \in \widehat{G} : |\widehat{fd\beta_{\Gamma,\delta}}(\gamma)| \geqslant \epsilon\|f\|_{L^\infty(\beta_{\Gamma,\delta})}\}$ then*

$$|\Lambda| \ll \epsilon^{-1}(1 + \log A_f).$$

2.3.1 The proof of Lemma 2.3.5

Lemma 2.1.3 corresponds to the case $S = \{0_{\widehat{G}}\}$ of the following.

Lemma 2.3.8. *Suppose that S is a non-empty symmetric neighborhood of $0_{\widehat{G}}$. Suppose that Δ is a set of characters on G and Λ is a maximal S-dissociated subset of Δ. Then $\Delta \subset \langle\Lambda\rangle + S$.*

Proof. If $\lambda_0 \in \Delta \setminus (\langle\Lambda\rangle + S)$ then we put $\Lambda' := \Lambda \cup \{\lambda_0\}$, which is a strict superset of Λ, and a subset of Δ. It turns out that Λ' is also S-dissociated which contradicts the maximality of Λ. Suppose that $m : \Lambda' \to \{-1, 0, 1\}$ and $m.\Lambda' \in S$. Then we have three possibilities for the value of m_{λ_0}:

(i). $m.\Lambda' = \lambda_0 + m|_\Lambda.\Lambda$, in which case $\lambda_0 \in -m|_\Lambda.\Lambda + S \subset \langle\Lambda\rangle + S$ - a contradiction;

(ii). $m.\Lambda' = -\lambda_0 + m|_\Lambda.\Lambda$, in which case $\lambda_0 \in m|_\Lambda.\Lambda - S \subset \langle\Lambda\rangle + S$ - a contradiction;

(iii). $m.\Lambda' = m|_\Lambda.\Lambda$, in which case $m|_\Lambda \equiv 0$ since Λ is S-dissociated and hence $m \equiv 0$.

It follows that $m.\Lambda' \in S \Rightarrow m \equiv 0$ i.e. Λ' is S-dissociated as claimed. $\square$

Lemma 2.3.5 then follows from the above and the next lemma.

Lemma 2.3.9. *Suppose that $B(\Gamma, \delta)$ is a regular Bohr set. Suppose that $\eta', \eta \in (0, 1]$ and Λ is a set of characters on G. Then there is a $\delta' \gg \min\{\eta/|\Lambda|, \eta'\eta\delta/d\}$ such that*

$$\langle\Lambda\rangle + \{\gamma : |\widehat{\beta_{\Gamma,\delta}}(\gamma)| \geqslant \eta'\} \subset \{\gamma : |1 - \gamma(x)| \leqslant \eta \textit{ for all } x \in B(\Gamma \cup \Lambda, \delta')\}.$$

Proof. The lemma has two parts.

(i). If $\lambda \in \langle\Lambda\rangle$ then

$$|1 - \lambda(x)| \leqslant \sum_{\lambda' \in \Lambda} |1 - \lambda'(x)|,$$

so there is a $\delta'' \gg \eta/|\Lambda|$ such that

$$\langle\Lambda\rangle \subset \{\gamma : |1 - \gamma(x)| \leqslant \eta/2 \text{ for all } x \in B(\Lambda, \delta'')\}.$$

(ii). By Lemma 2.2.6 there is a $\delta''' \gg \eta\eta'\delta/d$ such that

$$\{\gamma : |\widehat{\beta}(\gamma)| \geqslant \eta'\} \subset \{\gamma : |1 - \gamma(x)| \leqslant \eta/2 \text{ for all } x \in B(\Gamma, \delta''')\}.$$

Taking $\delta' = \min\{\delta'', \delta'''\}$ we have the result by the triangle inequality. $\square$

2.3.2 The proof of Lemma 2.3.7

In both the proof of Lemma 2.3.7 and Lemma 2.3.6 we introduce some smoothed measures. They are slightly different in each case so for this section only we make the following definition.

Suppose that $B(\Gamma,\delta)$ is a regular Bohr set. For $L \in \mathbb{N}$ and $\kappa \in (0,1]$ we write

$$\tilde{\beta}^{L,\kappa}_{\Gamma,\delta} := \beta_{\Gamma,(1-\kappa)\delta} * \beta^{L}_{\Gamma,\kappa\delta/L},$$

where $\beta^{L}_{\Gamma,\kappa\delta/L}$ denotes the convolution of $\beta_{\Gamma,\kappa\delta/L}$ with itself L times. $\tilde{\beta}^{L,\kappa}_{\Gamma,\delta}$ is a good approximation to $\beta_{\Gamma,\delta}$ in $M(G)$:

$$\|\tilde{\beta}^{L,\kappa}_{\Gamma,\delta} - \beta_{\Gamma,\delta}\| \leqslant \|\beta_{\Gamma,\delta(1-\kappa)} * \mu - \beta_{\Gamma,\delta(1-\kappa)}\| + \|\beta_{\Gamma,\delta(1-\kappa)} - \beta_{\Gamma,\delta}\|$$

where $\mu = \beta^{L}_{\Gamma,\kappa\delta/L}$, the convolution of $\beta_{\Gamma,\kappa\delta/L}$ with itself L times. We deal with the first term using Corollary 2.2.4 which yields

$$\|\beta_{\Gamma,\delta(1-\kappa)} * \mu - \beta_{\Gamma,\delta(1-\kappa)}\| \ll \kappa d,$$

since $\operatorname{supp}\mu \subset B(\Gamma,\kappa\delta)$. For the second term we have

$$\begin{aligned}
\|\beta_{\Gamma,\delta(1-\kappa)} - \beta_{\Gamma,\delta}\| &\leqslant \|\beta_{\Gamma,\delta(1-\kappa)} - \beta_{\Gamma,\delta}|_{B(\Gamma,\delta(1-\kappa))}\| + \|\beta_{\Gamma,\delta}|_{B(\Gamma,\delta)\setminus B(\Gamma,\delta(1-\kappa))}\| \\
&= \left(1 - \frac{\mu_G(B(\Gamma,\delta(1-\kappa)))}{\mu_G(B(\Gamma,\delta))}\right) + \|\beta_{\Gamma,\delta}|_{B(\Gamma,\delta)\setminus B(\Gamma,\delta(1-\kappa))}\| \\
&= O(\kappa d) + \|\beta_{\Gamma,\delta}|_{B(\Gamma,\delta)\setminus B(\Gamma,\delta(1-\kappa))}\| \text{ by regularity,} \\
&= O(\kappa d) + \left(\frac{\mu_G(B(\Gamma,\delta)) - \mu_G(B(\Gamma,\delta(1-\kappa)))}{\mu_G(B(\Gamma,\delta))}\right) \\
&= O(\kappa d) \text{ by regularity.}
\end{aligned}$$

It follows that $\|\tilde{\beta}^{L,\kappa}_{\Gamma,\delta} - \beta_{\Gamma,\delta}\| = O(\kappa d)$ and hence if $f \in L^\infty(\beta_{\Gamma,\delta})$ we have

$$|\widehat{fd\tilde{\beta}^{L,\kappa}_{\Gamma,\delta}}(\gamma) - \widehat{fd\beta_{\Gamma,\delta}}(\gamma)| \ll \|f\|_{L^\infty(\beta_{\Gamma,\delta})}\kappa d. \tag{2.3.1}$$

The proof now follows the proof of Proposition 2.1.4 with this additional ingredient.

Proof of Lemma 2.3.7. We begin by fixing κ and L in the smoothed measure $\tilde{\beta}^{L,\kappa}_{\Gamma,\delta}$ so that we may dispense with the superscripts and subscripts and simply write $\tilde{\beta}$. Take $L = 2R$, where R will be chosen later and $\kappa \gg \epsilon/d$ so that

$$|\widehat{fd\tilde{\beta}^{L,\kappa}_{\Gamma,\delta}}(\gamma) - \widehat{fd\beta_{\Gamma,\delta}}(\gamma)| \leqslant 2^{-1}\epsilon\|f\|_{L^\infty(\beta_{\Gamma,\delta})},$$

which we may certainly do by (2.3.1), and also so that $\delta' := \kappa\delta/L$ is regular for Γ. As usual this last requirement is possible by Proposition 2.2.2. It follows that

$$|\widehat{fd\beta_{\Gamma,\delta}}(\gamma)| \geqslant \epsilon\|f\|_{L^\infty(\beta_{\Gamma,\delta})} \Rightarrow |\widehat{fd\tilde{\beta}}(\gamma)| \geqslant 2^{-1}\epsilon\|f\|_{L^\infty(\beta_{\Gamma,\delta})}.$$

Henceforth write β for $\beta_{\Gamma,\delta}$ and β' for $\beta_{\Gamma,\delta'}$.

Suppose that Λ is a $\{\gamma : |\widehat{\beta'}(\gamma)| \geqslant 1/3\}$-dissociated subset of $\{\gamma \in \widehat{G} : |\widehat{fd\beta}\gamma)| \geqslant \epsilon\|f\|_{L^\infty(\beta)}\}$ and that $\Lambda' \subset \Lambda$ has size at most R. Λ' is certainly still $\{\gamma : |\widehat{\beta'}(\gamma)| \geqslant 1/3\}$-dissociated. We define

$$\omega(\lambda) := \frac{\widehat{fd\tilde{\beta}}(\lambda)}{|\widehat{fd\tilde{\beta}}(\lambda)|} \text{ for all } \lambda \in \Lambda'.$$

$\omega \in \ell^\infty(\Lambda')$, $\|\omega\|_{\ell^\infty(\Lambda')} \leqslant 1$ and Λ' is dissociated (since it is $\{\gamma : |\widehat{\beta'}(\gamma)| \geqslant 1/3\}$-dissociated) so we may apply Proposition 2.1.5 to get the auxiliary measure μ_η. To leverage the stronger dissociativity condition we introduce a Riesz product:

$$q := \prod_{\lambda \in \Lambda'} \left(1 + \frac{\lambda + \overline{\lambda}}{2}\right).$$

Recall (from §2.1.3 if necessary) that q is non-negative and since Λ' is certainly dissociated, $\|q\| = 1$.

Plancherel's Theorem gives

$$\langle fd\tilde{\beta}, \mu_\eta * q\rangle = \sum_{\gamma \in \widehat{G}} \widehat{fd\tilde{\beta}}(\gamma)\overline{\widehat{q}(\gamma)\widehat{\mu_\eta}(\gamma)}.$$

We begin by bounding the right hand side from below using the bound on

$|\widehat{\mu_\eta}(\lambda)|$ for $\lambda \notin \widehat{G}$.

$$
\begin{aligned}
|\sum_{\gamma\in\widehat{G}} \widehat{fd\tilde{\beta}}(\gamma)\overline{\widehat{q}(\gamma)\widehat{\mu_\eta}(\gamma)}| &= |\sum_{\lambda\in\Lambda'} \widehat{fd\tilde{\beta}}(\lambda)\overline{\widehat{q}(\lambda)\widehat{\mu_\eta}(\lambda)} + \sum_{\lambda\notin\Lambda'} \widehat{fd\tilde{\beta}}(\lambda)\overline{\widehat{q}(\lambda)\widehat{\mu_\eta}(\lambda)}| \\
&\geqslant |\sum_{\lambda\in\Lambda'} \widehat{fd\tilde{\beta}}(\lambda)\overline{\widehat{q}(\lambda)\widehat{\mu_\eta}(\lambda)}| - |\sum_{\lambda\notin\Lambda'} \widehat{fd\tilde{\beta}}(\lambda)\overline{\widehat{q}(\lambda)\widehat{\mu_\eta}(\lambda)}| \\
&\geqslant |\sum_{\lambda\in\Lambda'} \widehat{fd\tilde{\beta}}(\lambda)\overline{\widehat{q}(\lambda)\omega(\lambda)}| - \eta\sum_{\lambda\in\widehat{G}} |\widehat{q}(\lambda)||\widehat{fd\tilde{\beta}}(\lambda)|.
\end{aligned}
$$

Now $\widehat{q}(\lambda) \geqslant 1/2$ if $\lambda \in \Lambda'$, so

$$
\begin{aligned}
|\sum_{\gamma\in\widehat{G}} \widehat{fd\tilde{\beta}}(\gamma)\overline{\widehat{q}(\gamma)\widehat{\mu_\eta}(\gamma)}| &\geqslant 2^{-1}\sum_{\lambda\in\Lambda'} |\widehat{fd\tilde{\beta}}(\lambda)| \\
&\quad -\eta\sum_{\lambda\in\widehat{G}}\sum_{\gamma\in\widehat{G}} |\widehat{q}(\lambda)||\widehat{f}(\gamma)\widehat{\tilde{\beta}}(\lambda-\gamma)| \\
&\geqslant 2^{-1}\sum_{\lambda\in\Lambda'} |\widehat{fd\tilde{\beta}}(\lambda)| \\
&\quad -\eta\|f\|_{A(G)}\sup_{\gamma\in\widehat{G}}\sum_{\lambda\in\widehat{G}} |\widehat{q}(\lambda)||\widehat{\tilde{\beta}}(\lambda-\gamma)|.
\end{aligned}
$$

For any $\gamma \in \widehat{G}$ we can estimate the last sum in a manner independent of γ by using a positivity argument:

$$
\begin{aligned}
\sum_{\lambda\in\widehat{G}} |\widehat{q}(\lambda)||\widehat{\tilde{\beta}}(\lambda-\gamma)| &= \sum_{\lambda\in\widehat{G}} |\widehat{q}(\gamma-\lambda)||\widehat{\tilde{\beta}}(\lambda)| \text{ by symmetry of } \widehat{\tilde{\beta}}, \\
&= \sum_{\lambda\in\widehat{G}} |\widehat{q}(\gamma-\lambda)||\widehat{\beta}(\lambda)\widehat{\beta'}(\lambda)^L| \text{ by definition of } \widehat{\tilde{\beta}}, \\
&\leqslant \sum_{\lambda\in\widehat{G}} |\widehat{q}(\gamma-\lambda)||\widehat{\beta'}(\lambda)|^L \text{ since } |\widehat{\beta}(\lambda)| \leqslant \|\beta\| = 1, \\
&= \widehat{qd\beta'^L}(\gamma) \text{ since } L \text{ is even and } \widehat{q} \geqslant 0, \\
&\leqslant \|qd\beta'^L\| \\
&= \widehat{qd\beta'^L}(0_{\widehat{G}}) \text{ by non-negativity of } qd\beta'^L, \\
&= \sum_{\lambda\in\widehat{G}} \widehat{q}(\lambda)|\widehat{\beta'}(\lambda)|^L \text{ by symmetry of } \widehat{q}.
\end{aligned}
$$

We estimate this by splitting the range of summation into two parts:

$$\sum_{\lambda \in \widehat{G}} \widehat{q}(\lambda)|\widehat{\beta'}(\lambda)|^L \leqslant \sum_{\lambda:|\widehat{\beta'}(\lambda)|\geqslant 1/3} \widehat{q}(\lambda)|\widehat{\beta'}(\lambda)|^L + \sum_{\lambda:|\widehat{\beta'}(\lambda)|\leqslant 1/3} \widehat{q}(\lambda)|\widehat{\beta'}(\lambda)|^L. \quad (2.3.2)$$

(i). For the first sum: $|\widehat{q}(\lambda)| \leqslant \|q\|_1 = 1$ and $|\widehat{\beta'}(\lambda)^L| \leqslant \|\beta'^L\| = 1$ so that each summand is at most 1, furthermore $\operatorname{supp} \widehat{q} \subset \langle \Lambda' \rangle$ so

$$\sum_{\lambda:|\widehat{\beta'}(\lambda)|\geqslant 1/3} \widehat{q}(\lambda)|\widehat{\beta'}(\lambda)|^L \leqslant \sum_{\lambda \in \langle \Lambda' \rangle : |\widehat{\beta'}(\lambda)|\geqslant 1/3} 1.$$

This range of summation contains at most 1 element by $\{\gamma : |\widehat{\beta'}(\gamma)| \geqslant 1/3\}$-dissociativity of Λ', and hence the sum is bounded above by 1.

(ii). For the second sum: $|\widehat{q}(\lambda)| \leqslant \|q\|_1 = 1$ and $|\widehat{\beta'}(\lambda)^L| \leqslant 3^{-L}$ for λ in the range of summation so that each summand is at most $9^{-|\Lambda'|}$, however $\operatorname{supp} \widehat{q} \subset \langle \Lambda' \rangle$ and $|\langle \Lambda' \rangle| \leqslant 3^{|\Lambda'|}$ so

$$\sum_{\lambda:|\widehat{\beta'}(\lambda)|\leqslant 1/3} \widehat{q}(\lambda)|\widehat{\beta'}(\lambda)|^L \leqslant \sum_{\lambda \in \langle \Lambda' \rangle} 9^{-|\Lambda'|} \leqslant 1.$$

It follows that the right hand side of (2.3.2) is bounded above by 2, and working backwards these estimates combine to show that

$$\sum_{\lambda \in \widehat{G}} |\widehat{q}(\lambda)||\widehat{\tilde{\beta}}(\lambda - \gamma)| \leqslant 2 \text{ for all } \gamma \in \widehat{G},$$

and hence that

$$|\langle f d\tilde{\beta}, \mu_\eta * q \rangle| \geqslant 2^{-1} \sum_{\lambda \in \Lambda'} |\widehat{f d\tilde{\beta}}(\lambda)| - 2\eta \|f\|_{A(G)}. \quad (2.3.3)$$

To estimate the inner product from above we have:

$$|\langle f d\tilde{\beta}, \mu_\eta * q \rangle| \leqslant \|f\|_{L^\infty(\beta)} \|\tilde{\beta}\| \|\mu_\eta\| \|q\|_1 \ll \|f\|_{L^\infty(\beta)} (1 + \log \eta^{-1})$$

by the estimate for $\|\mu_\eta\|$ given in Proposition 2.1.5. Combining this with our lower bound for the inner product in (2.3.3) and the fact that if $\lambda \in \Lambda'$ then $|\widehat{fd\tilde{\beta}}(\lambda)| \geqslant 2^{-1}\epsilon\|f\|_{L^\infty(\beta)}$ gives

$$\|f\|_{L^\infty(\beta)}(1+\log\eta^{-1}) + \eta\|f\|_{A(G)} \gg |\Lambda'|\epsilon\|f\|_{L^\infty(\beta)}.$$

Choosing $\eta^{-1} = \|f\|_{A(G)}\|f\|_{L^\infty(\beta)}^{-1}$ yields that

$$|\Lambda'| \ll \epsilon^{-1}(1+\log A_f).$$

Let C be the absolute constant implicit in the notation on the right so that $|\Lambda'| \leqslant C\epsilon^{-1}(1+\log A_f)$ is always true, and set $R := \lceil C\epsilon^{-1}(1+\log A_f)\rceil + 1$. If $|\Lambda|$ is a $\{\gamma : |\widehat{\beta'}(\gamma)| \geqslant 1/3\}$-dissociated set of size greater than R, then let Λ' be a subset of Λ of size R, which is automatically $\{\gamma : |\widehat{\beta'}(\gamma)| \geqslant 1/3\}$-dissociated because Λ is $\{\gamma : |\widehat{\beta'}(\gamma)| \geqslant 1/3\}$-dissociated. By the above

$$C\epsilon^{-1}(1+\log A_f) < \lceil C\epsilon^{-1}(1+\log A_f)\rceil + 1 = R = |\Lambda'| \leqslant C\epsilon^{-1}(1+\log A_f),$$

which is a contradiction and hence if Λ is $\{\gamma : |\widehat{\beta'}(\gamma)| \geqslant 1/3\}$-dissociated then $|\Lambda| < R \ll \epsilon^{-1}(1+\log A_f)$ as required. □

2.3.3 Proof of Lemma 2.3.6

The proof has three main ingredients. The first is Rudin's inequality, which is the analogue of Proposition 2.1.5 for Chang's Theorem.

Proposition 2.3.10 (Rudin's Inequality)**.** *Suppose that Λ is a dissociated set of characters on G. Then*

$$\|\widehat{f}\|_{\ell^2(\Lambda)} \ll \sqrt{p}\|f\|_{L^{p'}(\mu_G)} \textit{ for all } f \in L^{p'}(\mu_G)$$

and all conjugate exponents p and p' with $p' \in (1,2]$.

For a proof of this see, for example, Chapter 5 of Rudin [Rud90].

The second ingredient in an almost-orthogonality lemma introduced by Green and Tao to prove Proposition 2.3.1.

Lemma 2.3.11 (Cotlar's almost-orthogonality lemma)**.** *Suppose that v and (w_j) are elements of a complex inner product space. Then*

$$\sum_j |\langle v, w_j\rangle|^2 \leqslant \langle v, v\rangle \max_j \sum_i |\langle w_i, w_j\rangle|.$$

For a proof of this see, for example, Chapter VII of Stein [Ste93].

Finally we require some smoothed measures. This time they are a little simpler.

Suppose that $B(\Gamma, \delta)$ is a regular Bohr set. We produce a range of smoothed alternatives to the measure $\beta_{\Gamma,\delta}$; specifically suppose that $L \in \mathbb{N}$ and $\kappa \in (0, 1]$. Then we may define

$$\tilde{\beta}^{L,\kappa}_{\Gamma,\delta} := \beta_{\Gamma,(1+\kappa)\delta} * \beta^{L}_{\Gamma,\kappa\delta/L},$$

where $\beta^{L}_{\Gamma,\kappa\delta/L}$ denotes the convolution of $\beta_{\Gamma,\kappa\delta/L}$ with itself L times. This measure has the property that it is supported on $B(\Gamma, (1+2\kappa)\delta)$ and uniform on $B(\Gamma, \delta)$, indeed

$$\tilde{\beta}^{L,\kappa}_{\Gamma,\delta}|_{B(\Gamma,\delta)} = \frac{\mu_G|_{B(\Gamma,\delta)}}{\mu_G(B(\Gamma, (1 + \kappa)\delta))} = \frac{\mu_G(B(\Gamma, \delta))}{\mu_G(B(\Gamma, (1 + \kappa)\delta))}.\beta_{\Gamma,\delta}. \tag{2.3.4}$$

It follows that every $f \in L^1(\beta_{\Gamma,\delta})$ has $\widehat{fd\beta_{\Gamma,\delta}}$ well approximated by $\widehat{fd\tilde{\beta}^{L,\kappa}_{\Gamma,\delta}}$. Specifically

$$\widehat{fd\tilde{\beta}^{L,\kappa}_{\Gamma,\delta}}(\gamma) = (1 + O(\kappa d))\widehat{fd\beta_{\Gamma,\delta}}(\gamma) \tag{2.3.5}$$

by regularity of $B(\Gamma, \delta)$.

We use almost-orthogonality and the smoothed measures to show the following localization of Rudin's Inequality. The proof of the lemma to which this section is devoted then follows the usual proof of Chang's Theorem.

Lemma 2.3.12. *Suppose that $B(\Gamma, \delta)$ is a regular Bohr set and R is a natural number. Then there is a $\delta' \gg \delta/dR$ regular for Γ such that if Λ is a $\{\gamma : |\widehat{\beta_{\Gamma,\delta'}}(\gamma)| \geqslant 1/3\}$-dissociated set of size at most R then*

$$\|\widehat{fd\beta_{\Gamma,\delta}}\|_{\ell^2(\Lambda)} \ll \sqrt{p}\|f\|_{L^{p'}(\beta_{\Gamma,\delta})} \textit{ for all } f \in L^{p'}(\beta_{\Gamma,\delta})$$

and all conjugate exponents p and p' with $p' \in (1,2]$.

Proof. Begin by fixing the level of smoothing (i.e. the parameters κ and L of $\tilde{\beta}^{L,\kappa}_{\Gamma,\delta}$) that we require and write $\tilde{\beta}$ for $\tilde{\beta}^{L,\kappa}_{\Gamma,\delta}$. Set $L := 2R$ and recall (2.3.5):

$$\widehat{gd\tilde{\beta}}(\gamma) = (1 + O(\kappa d))\widehat{gd\beta_{\Gamma,\delta}}(\gamma) \text{ for all } g \in L^1(\beta_{\Gamma,\delta});$$

so we can pick $\kappa' \gg d^{-1}$ such that for all $\kappa \leqslant \kappa'$

$$\frac{1}{2}|\widehat{gd\beta_{\Gamma,\delta}}(\gamma)| \leqslant |\widehat{gd\tilde{\beta}}(\gamma)| \leqslant \frac{3}{2}|\widehat{gd\beta_{\Gamma,\delta}}(\gamma)| \text{ for all } g \in L^1(\beta_{\Gamma,\delta}).$$

By Proposition 2.2.2, we can take κ with $\kappa' \geqslant \kappa \gg d^{-1}$ such that $\delta' := \kappa\delta/L$ is regular. Henceforth write β for $\beta_{\Gamma,\delta}$ and β' for $\beta_{\Gamma,\delta'}$.

Define the Riesz product

$$q(x) := \prod_{\lambda \in \Lambda} \left(1 + \frac{\lambda(x) + \overline{\lambda}(x)}{2}\right).$$

Recall (from §2.1.3 if necessary) that q is non-negative and that we can compute the Fourier transform of q:

$$\widehat{q}(\gamma) = \sum_{m : m.\Lambda = \gamma} 2^{-|m|}. \tag{2.3.6}$$

Since Λ is $\{\gamma : |\widehat{\beta'}(\gamma)| \geqslant 1/3\}$-dissociated, it is certainly dissociated and hence $\widehat{q}(0_{\widehat{G}}) = 1$ and so, by non-negativity of q, $\|q\| = 1$.

Use q to define the map

$$T : L^1(\beta) \to L^1(G); g \mapsto (gd\beta) * q,$$

and note that

$$\|Tg\|_{L^1(\mu_G)} = \|(gd\beta) * q\|_{L^1(\mu_G)} \leqslant \|g\|_{L^1(\beta)}\|q\| = \|g\|_{L^1(\beta)}$$

by the triangle inequality. The following claim, which we defer proof of, is a corresponding result for $\|Tg\|_{L^2(\mu_G)}$.

Claim. *If* $g \in L^2(\beta)$ *then* $\|Tg\|_{L^2(\mu_G)} \ll \|g\|_{L^2(\beta)}$.

Assuming this claim, by the Riesz-Thorin interpolation theorem we have

$$\|Tg\|_{L^{p'}(\mu_G)} \ll \|g\|_{L^{p'}(\beta)} \text{ for any } p' \in [1,2]. \tag{2.3.7}$$

Hence, if $f \in L^{p'}(\beta)$ then

$$\begin{aligned} \frac{1}{2}\|\widehat{fd\beta}\|_{\ell^2(\Lambda)} &\leqslant \|\widehat{fd\beta}\widehat{q}\|_{\ell^2(\Lambda)} \text{ since } \widehat{q}(\lambda) \geqslant 1/2 \text{ for all } \lambda \in \Lambda, \\ &= \|\widehat{Tf}\|_{\ell^2(\Lambda)} \text{ by the definition of } T, \\ &\ll \sqrt{p}\|Tf\|_{L^{p'}(\mu_G)} \text{ by Rudin's Inequality}, \\ &\ll \sqrt{p}\|f\|_{L^{p'}(\beta)} \text{ by (2.3.7).} \end{aligned}$$

The lemma follows. It remains to prove the claim.

Proof of Claim. Begin by noting the following consequence of (2.3.4).

$$\|Tg\|^2_{L^2(\mu_G)} = \left(\frac{\mu_G(B(\Gamma,\delta(1+\kappa)))}{\mu_G(B(\Gamma,\delta))}\right)^2 \|(gd\tilde{\beta}) * q\|^2_{L^2(\mu_G)}. \tag{2.3.8}$$

By Plancherel's Theorem

$$\|(gd\tilde{\beta}) * q\|^2_{L^2(\mu_G)} = \sum_{\gamma \in \widehat{G}} |\widehat{(gd\tilde{\beta})}(\gamma)\widehat{q}(\gamma)|^2 = \sum_{\gamma \in \widehat{G}} |\langle g, \widehat{q}(\gamma)\gamma\rangle_{L^2(\tilde{\beta})}|^2.$$

Cotlar's almost-orthogonality lemma applied to the second sum gives

$$\begin{aligned} \|(gd\tilde{\beta}) * q\|^2_{L^2(\mu_G)} &\leqslant \langle g, g\rangle_{L^2(d\tilde{\beta})} \max_{\gamma} \sum_{\gamma'} |\langle \widehat{q}(\gamma)\gamma, \widehat{q}(\gamma')\gamma'\rangle_{L^2(\tilde{\beta})}| \\ &\leqslant \|g\|^2_{L^2(d\tilde{\beta})} \max_{\gamma} \sum_{\gamma'} \widehat{q}(\gamma')|\widehat{\tilde{\beta}}(\gamma - \gamma')|. \end{aligned}$$

For any $\gamma \in \widehat{G}$ we can estimate the last sum in a manner independent of γ

by using a positivity argument:

$$\begin{aligned}
\sum_{\gamma'\in\widehat{G}}\widehat{q}(\gamma')|\widehat{\tilde{\beta}}(\gamma-\gamma')| &= \sum_{\gamma'\in\widehat{G}}\widehat{q}(\gamma-\gamma')|\widehat{\beta}(\gamma')\widehat{\beta'}(\gamma')^L| \text{ by definition of } \tilde{\beta},\\
&\leqslant \sum_{\gamma'\in\widehat{G}}\widehat{q}(\gamma-\gamma')|\widehat{\beta'}(\gamma')|^L\\
&\quad \text{since } |\widehat{\beta}(\gamma')| \leqslant \|\beta\| = 1 \text{ and } \widehat{q} \geqslant 0,\\
&= \widehat{qd\beta'^L}(\gamma) \text{ since } L \text{ is even and } \widehat{q}\geqslant 0,\\
&\leqslant \|q\|_{L^1(\beta'^L)}\\
&= \widehat{qd\beta'^L}(0_{\widehat{G}}) \text{ by non-negativity of } qd\beta'^L,\\
&= \sum_{\gamma'\in\widehat{G}}\widehat{q}(\gamma')|\widehat{\beta'}(\gamma')|^L \text{ by symmetry of } \widehat{q}.
\end{aligned}$$

We estimate this in turn by splitting the range of summation into two parts:

$$\sum_{\gamma'\in\widehat{G}}\widehat{q}(\gamma')|\widehat{\beta'}(\gamma')|^L \leqslant \sum_{\gamma':|\widehat{\beta'}(\gamma')|\geqslant 1/3}\widehat{q}(\gamma')|\widehat{\beta'}(\gamma')|^L + \sum_{\gamma':|\widehat{\beta'}(\lambda)|\leqslant 1/3}\widehat{q}(\gamma')|\widehat{\beta'}(\gamma')|^L. \tag{2.3.9}$$

(i). For the first sum: $|\widehat{q}(\gamma')| \leqslant \|q\|_1 = 1$ and $|\widehat{\beta'}(\gamma')^L| \leqslant \|\beta'^L\| = 1$ so that each summand is at most 1, furthermore $\operatorname{supp}\widehat{q} \subset \langle\Lambda\rangle$ so

$$\sum_{\gamma':|\widehat{\beta'}(\gamma')|\geqslant 1/3}\widehat{q}(\gamma')|\widehat{\beta'}(\gamma')|^L \leqslant \sum_{\gamma'\in\langle\Lambda\rangle:|\widehat{\beta'}(\gamma')|\geqslant 1/3} 1.$$

This range of summation contains at most 1 element by $\{\gamma : |\widehat{\beta'}(\gamma)| \geqslant 1/3\}$-dissociativity of Λ, and hence the sum is bounded above by 1.

(ii). For the second sum: $|\widehat{q}(\gamma')| \leqslant \|q\|_1 = 1$ and $|\widehat{\beta'}(\gamma')^L| \leqslant 3^{-L}$ for γ' in the range of summation so that each summand is at most $9^{-|\Lambda|}$, however $\operatorname{supp}\widehat{q} \subset \langle\Lambda\rangle$ and $|\langle\Lambda\rangle| \leqslant 3^{|\Lambda|}$ so

$$\sum_{\gamma':|\widehat{\beta'}(\gamma')|\leqslant 1/3}\widehat{q}(\gamma')|\widehat{\beta'}(\gamma')|^L \leqslant \sum_{\gamma'\in\langle\Lambda\rangle} 9^{-|\Lambda|} \leqslant 1.$$

It follows that the right hand side of (2.3.9) is bounded above by 2 and hence that

$$\|(gd\tilde{\beta}) * q\|_{L^2(\mu_G)}^2 \leqslant 2\|g\|_{L^2(\tilde{\beta})}^2.$$

This, (2.3.8) and (2.3.4) yield

$$\|Tg\|_{L^2(\mu_G)}^2 \leqslant 2\frac{\mu_G(B(\Gamma,\delta(1+\kappa)))}{\mu_G(B(\Gamma,\delta))}\|g\|_{L^2(\beta)}^2,$$

from which the claim follows by regularity. □

□

Proof of Lemma 2.3.6. Fix R to be optimized later and suppose that $\Lambda' \subset \Lambda$ has $|\Lambda'| \leqslant R$. By Lemma 2.3.12, for any $p' \in (1,2]$ we have

$$|\Lambda'|.\epsilon^2\|f\|_{L^1(\beta_{\Gamma,\delta})}^2 \leqslant \sum_{\lambda\in\Lambda'} |\widehat{fd\beta_{\Gamma,\delta}}(\lambda)|^2 = \|\widehat{fd\beta_{\Gamma,\delta}}\|_{\ell^2(\Lambda')}^2 \ll p\|f\|_{L^{p'}(\beta_{\Gamma,\delta})}^2,$$

where p is the conjugate exponent of p'. The log-convexity of $\|.\|_{L^{p'}(\beta_{\Gamma,\delta})}$ gives

$$|\Lambda'| \ll \epsilon^{-2}p\left(\frac{\|f\|_{L^2(\beta_{\Gamma,\delta})}}{\|f\|_{L^1(\beta_{\Gamma,\delta})}}\right)^{\frac{4}{p}}.$$

Setting $p = 1+\log L_f$ yields $|\Lambda'| \ll \epsilon^{-2}(1+\log L_f)$. Let $C > 0$ be the absolute constant implicit in this expression, so $|\Lambda'| \leqslant C\epsilon^{-2}(1+\log L_f)$. Set $R = \lceil C\epsilon^{-2}(1+\log L_f)\rceil + 1$. If $|\Lambda| > R$ then let Λ' be a subset of Λ of size R. We then conclude that

$$R \leqslant C\epsilon^{-2}(1+\log L_f) \leqslant R-1.$$

This contradiction ensures that $|\Lambda| \leqslant R$ and the lemma is proved. □

2.3.4 Remarks on the Proofs

The proofs Lemmas 2.3.7 and 2.3.6 are rather similar and one might expect to be able to use the same smoothed measures for both. As it happens one can use the simpler measures of Lemma 2.3.6 for Lemma 2.3.7. However, there is some loss. One has to be willing to accept a version of Proposition 2.3.4 with

$\|f1_{B(\Gamma,\delta)}\|_{A(G)}$ rather than $\|f\|_{A(G)}$ in the expression for A_f. Unfortunately in applications we only have control over $\|f\|_{A(G)}$, and $\|f1_{B(\Gamma,\delta)}\|_{A(G)}$ may still be large while this is small (consider, for example, $G = \mathbb{Z}/p\mathbb{Z}$ for p a large prime, $f = 1_G$ and $B(\Gamma, \delta)$ a centred interval around the origin of length $(p-1)/2$).

Rather than convolving with the Riesz product q, as we did in the proof of Lemma 2.3.7 (and the proof of Lemma 2.3.6), one can construct a local version of the auxiliary measure (respectively, Rudin's Inequality) directly. However, doing so seems only to serve to obfuscate the underlying constructions with technical details.

2.4 Fourier analysis on Bourgain systems

In an exposition of Bourgain's paper [Bou99], Tao (in work now summarized in [TV06]) showed how to further relax the properties Bourgain required of Bohr sets for their use as 'approximate groups'. In view of this an abstract formulation of 'approximate groups' is now possible. Indeed it is possible to carry out a number (although not all) of the main results of this paper with Bourgain systems in place of Bohr sets. This leads to technically slightly weaker statements (Bohr sets have more structure than Bourgain systems) although for most practical purposes they seem equivalent. The work of this section is from the joint paper [GS08b] of Green and the author where these structures were first formalized.

Before making a formal definition we shall try to understand the notion of 'approximate group' or, more properly, 'approximate subgroup' a little more clearly. A subgroup of an abelian group G is a symmetric neighborhood of 0_G which is closed under addition. Bourgain noticed that in a number of cases there are symmetric neighborhoods of 0_G which are in some sense nearly closed under addition and, furthermore, for many problems these structures can replace subgroups. Suppose that B is a subset of $\mathbb{Z}^d$. Generically $B+B$ will need $|B|$ translates of B to cover it; however, if B is the $\ell^\infty(\mathbb{Z}^d)$ unit cube, for example, then $B+B$ is covered by 2^d translates of B so is 'approximately closed'. Bourgain effectively restricted his attention to the balls we have just described. However, Freĭman's Theorem (which we will discuss in Chapter 3) has, as a consequence, that *any* symmetric neighborhood B of $0_G$with $B+B \subset T+B$ for some set T with $|T|$ small enough looks a lot like the unit cube of a suitable lattice. In view of this we make the following definition.

Definition (Bourgain systems)**.** A Bourgain system $\mathcal{B}$ of dimension d is a collection $(B_\rho)_{\rho \in (0,4]}$ of subsets of G such that the following axioms are satisfied:

BS1 (Nesting) If $\rho' \leqslant \rho$ we have $B_{\rho'} \subseteq B_\rho$;

BS2 (Zero) $0_G \in B_0$;

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

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

BS5 (Doubling) If $\rho \leqslant 1$ then there is a set T of size at most 2^d such that $B_{2\rho} \subset \bigcup_{t \in T} t + B_\rho$.

We refer to $\mu_G(B_1)$ as the density of the system $\mathcal{B}$, and write $\mu_G(\mathcal{B})$ for this quantity.

Note that if $\mathcal{B}$ is a Bourgain system of dimension d then it is also a Bourgain system of dimension d' for any $d' \geqslant d$. This apparent ambiguity will not be a problem in practice.

We define the analogue of normalized Bohr cutoffs for Bourgain systems: Write β_ρ for the probability measure induced on B_ρ by μ_G.

If $\mathcal{B} = (B_\rho)_\rho$ is a Bourgain system, then, for any $\lambda \in (0,1]$, so is the dilated Bourgain system $\lambda\mathcal{B} := (B_{\lambda\rho})_\rho$.

The following easy averaging argument (c.f. the proof of Lemma 2.2.1) concerning dilated Bourgain systems will be useful in the sequel.

Lemma 2.4.1. *Suppose that $\mathcal{B}$ is a Bourgain system of dimension d, and suppose that $\lambda \in (0,1]$. Then $\lambda\mathcal{B}$ is a Bourgain system of dimension d and $\mu_G(\lambda\mathcal{B}) \geqslant (\lambda/2)^d \mu_G(\mathcal{B})$.*

The first important example of a Bourgain system is a system of Bohr sets.

Lemma 2.4.2. *Suppose that* Γ *is a set of characters and* $\delta \in (0,1]$*. Then* $(B(\Gamma,\delta))_\delta$ *is a Bourgain system of dimension at most* $2|\Gamma|$ *and density at least* $\delta^{|\Gamma|}$*.*

Proof. All the properties are immediate except BS5. As with Lemma 2.2.1, for each $\theta \in \mathbb{T}^\Gamma$ define the set

$$B_\theta := \{x \in G : \|\gamma(x) - \exp(2\pi i \theta_\gamma)\| \leqslant \delta/2 \text{ for all } \gamma \in \Gamma\}.$$

If $x' \in B_\theta$ then the map $x \mapsto x - x'$ is an injection from B_θ to $B(\Gamma,\delta)$.

Putting

$$\Theta = \prod_{\gamma \in \Gamma} \{-3\delta/2, -\delta/2, \delta/2, 3\delta/2\}$$

we have that $\{B_\theta : \theta \in \Theta\}$ is a cover of $B(\Gamma, 2\delta)$ from which BS5 follows. □

We now proceed to develop the basic theory of Bourgain systems, which for the most part parallels the theory of Bohr sets developed earlier.

Lemma 2.4.3. *Suppose that* $\rho \leqslant 1$*. The group* G *may be covered by at most* $(4/\rho)^d \mu_G(\mathcal{B})^{-1}$ *translates of* B_ρ*.*

Proof. Pick $T \subset G$ maximal such that the sets $t + B_{\rho/2}$ are all disjoint. It follows that each $x \in G$ has $x + B_{\rho/2} \cap T + B_{\rho/2} \neq \emptyset$, whence

$$G \subset T + B_{\rho/2} - B_{\rho/2} \subset T + B_\rho.$$

Moreover

$$|T| \leqslant \frac{1}{\mu_G(B_{\rho/2})} \leqslant (4/\rho)^d \mu_G(\mathcal{B})^{-1},$$

yielding the result. □

The intersection of two Bohr sets is (essentially) another Bohr set; the following lemma addresses this fact in general.

Lemma 2.4.4 (Intersections of Bourgain systems)**.** *Suppose that* $\mathcal{B}^{(1)}, \ldots \mathcal{B}^{(k)}$ *are Bourgan systems with dimension* $d_1, \ldots, d_k$ *respectively. Then* $\mathcal{B}^{(1)} \cap \cdots \cap \mathcal{B}^{(k)}$ *is a Bourgain system of dimension* $2(d_1 + \cdots + d_k)$ *with*

$$\mu_G(\mathcal{B}^{(1)} \cap \cdots \cap \mathcal{B}^{(k)}) \geqslant 2^{-3(d_1+\cdots+d_k)} \mu_G(\mathcal{B}^{(1)}) \ldots \mu_G(\mathcal{B}^{(k)}).$$

Proof. It is trivial to verify properties BS1–BS4. To show BS5 suppose that $\rho \leqslant 1$. For each i there is a set T_i with $|T_i| \leqslant 2^{2d_i}$ such that $B^{(i)}_{2\rho} \subset T_i + B^{(i)}_{\rho/2}$. It follows that

$$B^{(1)}_{2\rho} \cap \cdots \cap B^{(k)}_{2\rho} \subset (T_1 + B_{\rho/2}(1)) \cap \cdots \cap (T_k + B^{(k)}_{\rho/2}).$$

Suppose that $x \in (t_1 + B^{(1)}_{\rho/2}) \cap \cdots \cap (t_k + B^{(k)}_{\rho/2})$. Then the map $x' \mapsto x' - x$ is an injection from this set into $B^{(1)}_{\rho} \cap \cdots \cap B^{(k)}_{\rho}$. It follows that we have BS5 with a set of size at most $|T_1| \ldots |T_k|$ and the claimed bound follows.

It remains to obtain a lower bound for the density of this system. To do this we apply Lemma 2.4.3 to cover G by at most $8^{d_i}\mu_G(\mathcal{B}^{(i)})^{-1}$ translates of $B^{(i)}_{1/2}$. It follows by averaging that there are elements $t_1, \ldots, t_k$ such that

$$\mu_G((t_1 + B^{(1)}_{1/2}) \cap \cdots \cap (t_k + B^{(k)}_{1/2})) \geqslant 8^{-(d_1+\cdots+d_k)} \mu_G(\mathcal{B}^{(1)}) \ldots \mu_G(\mathcal{B}^{(k)}).$$

To compete the estimate we note that for fixed $x \in (t_1 + B^{(1)}_{1/2}) \cap \cdots \cap (t_k + B^{(k)}_{1/2})$ the map $x' \mapsto x' - x$ is an injection into $B^{(1)}_1 \cap \cdots \cap B^{(k)}_1$. □

If $\mathcal{B}$ and $\mathcal{B}'$ are Bourgain systems and $B_\rho \subset B'_\rho$ for all ρ then we say that $\mathcal{B}$ is a Bourgain subsystem of $\mathcal{B}'$. Clearly $\mathcal{B} \cap \mathcal{B}'$ is always a subsystem of $\mathcal{B}$ and $\mathcal{B}'$.

As with Bohr sets not all Bourgain systems behave as well as we might like. However, the following analogue of Proposition 2.2.2 basically asserts that typically they do.

Proposition 2.4.5. *Suppose* $\mathcal{B}$ *is a Bourgain system. There is an absolute constant* $c_{\mathcal{R}} > 0$ *and a* $\lambda \in [1/2, 1)$ *such that*

$$\frac{\mu_G(B_{\lambda(1+\kappa)})}{\mu_G(B_\lambda)} = 1 + O(d|\kappa|)$$

whenever $d|\kappa| \leqslant c_{\mathcal{R}}$.

Proof. Let $f : [0,1] \to \mathbb{R}$ be the function $f(a) := \frac{1}{d}\log_2 \mu_G(B_{2^a})$. Observe that f is non-decreasing 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 $\int_{I(a)} df > \int_I 3dx$. These intervals cover $[\frac{1}{6}, \frac{5}{6}]$, which has total length $\frac{2}{3}$. A simple covering lemma [GK09, Lemma 3.4] then allows us to pass to a disjoint subcollection $I_1 \cup \ldots \cup I_n$ of these intervals with total length at least $\frac{1}{3}$. However we now have

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

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

$$\exp(-5d\kappa) \leqslant \frac{\mu_G(B_{(1+\kappa)\lambda})}{\mu_G(B_\lambda)} \leqslant \exp(5d\kappa)$$

whenever $d|\kappa| \leqslant 1/10$. Since $1 - 2|x| \leqslant \exp(x) \leqslant 1 + 2|x|$ when $|x| \leqslant 1$. The result follows with $c_{\mathcal{R}} = 1/10$. □

We say that $\mathcal{B}$ is regular if

$$\frac{\mu_G(B_{1+\kappa})}{\mu_G(B_1)} = 1 + O(d|\kappa|)$$

whenever $d|\kappa| \leqslant c_{\mathcal{R}}$.

As with Bohr sets it is *regular* Bourgain systems to which we localize Fourier analysis.

Lemma 2.4.6. *Suppose that $\mathcal{B}$ is a regular Bourgain system of dimension d. If $y \in B_\kappa$ then $\|(y+\beta_1) - \beta_1\| \ll d\kappa$, where we recall that $y + \beta_1$ denotes the measure β_1 composed with translation by y.*

Proof. Same as Lemma 2.2.3. □

In applications the following simple corollary will be useful but it should be ignored until it is used.

Corollary 2.4.7. *Suppose that $\mathcal{B}$ is a regular Bourgain system. If $f \in L^\infty(\mu_G)$ then*

$$\sup_{x \in G} \|f * \beta_1 - f * \beta_1(x)\|_{L^\infty(x+\beta_\kappa)} \ll \|f\|_{L^\infty(\mu_G)} d\kappa.$$

Proof. Same as Corollary 2.2.5. □

Finally the following lemma ensures that the various candidates for the dual of a Bourgain system are essentially equivalent.

Lemma 2.4.8. *Suppose that $\mathcal{B}$ is a regular Bourgain system of dimension d and that $\eta_1, \eta_2 > 0$. Then there is a $\kappa \gg \eta_1\eta_2/d$ such that*

$$\{\gamma : |\widehat{\beta_1}(\gamma)| \geqslant \eta_1\} \subset \{\gamma : |1 - \gamma(x)| \leqslant \eta_2 \textit{ for all } x \in B_\kappa\}.$$

Proof. Same as Lemma 2.2.6. □

Chapter 3

Additive structure and Freĭman's Theorem

Sumsets are a fundamental object of interest in additive combinatorics and one of the first questions which arises is a question of Freĭman's regarding their structure. We say that a set A has doubling K if $|A + A| \leqslant K|A|$; Freĭman asked which sets have small doubling. In [Fre73] (see [Bil99] for an exposition) he famously described the structure of the finite sets of integers with small doubling. To state his result we require the following definition. P is a multidimensional progression of dimension d if

$$P = \{x_0 + l_1.x_1 + ... + l_d.x_d : 0 \leqslant l_i \leqslant L_i\}$$

for some integers $x_0, ..., x_d$ and natural numbers $L_1, ..., L_d$.

Theorem 3.1 (Freĭman's Theorem)**.** *Suppose that $A \subset \mathbb{Z}$ is finite with $|A + A| \leqslant K|A|$. Then A is contained in a $d(K)$-dimensional progression of size at most $f(K)|A|$.*

Here, of course, d and f are dependent only on K. Qualitatively this is a complete description of such sets, insofar as if A is contained in a multidimensional progression P of dimension d and size $f|A|$. Then

$$|A + A| \leqslant |P + P| \leqslant 2^d|P| \leqslant f2^d|A|.$$

Quantitatively, however, Freĭman's Theorem gives little information. In the 90s Ruzsa ([Ruz94]) provided a strong new proof of Freĭman's Theorem which was then refined by Chang in [Cha02].

Theorem 3.2 (Chang's quantitative version of the Freĭman-Ruzsa Theorem)**.** *Suppose that* $A \subset \mathbb{Z}$ *is finite with* $|A+A| \leqslant K|A|$. *Then* A *is contained in a* $O(K^2 \log^2(1+K))$*-dimensional progression of size at most* $\exp(O(K^2 \log^2(1+K)))|A|$.

In fact Chang also showed how to improve the dimension to essentially the optimal one for very little cost in the size but this is not important to us.

In the paper [Ruz99] Ruzsa considers Freĭman's Theorem for torsion groups. These groups are at the other end of the spectrum from $\mathbb{Z}$ which has no torsion. In this case, although multidimensional progressions make sense, bounding their dimension is not possible as the case $A = G = \mathbb{F}_2^n$ clearly demonstrates. Here A has doubling 1, however it is not contained in a multidimensional progression of dimension less than n. However, A *is* contained in a coset of a subgroup (namely G itself) and replacing multidimensional progressions with cosets turns out to be the appropriate idea. Ruzsa proved the following result.

Theorem 3.3 (Freĭman's Theorem for torsion groups)**.** *Suppose that* G *is an abelian group in which every element has order at most* r. *Suppose that* $A \subset G$ *is finite with* $|A+A| \leqslant K|A|$. *Then* A *is contained in a coset of a subgroup of size at most* $K^2 r^{K^4}|A|$.

Finally in [GR07] Green and Ruzsa combine this work with Chang's quantitative version of Freĭman's Theorem to prove Freĭman's Theorem in arbitrary abelian groups. To do this a slightly more general notion of progression is required combining cosets with multidimensional progressions: P is a multidimensional coset progression of dimension d if

$$P = H + \{x_0 + l_1.x_1 + ... + l_d.x_d : 0 \leqslant l_i \leqslant L_i\}$$

for some elements $x_0, ..., x_d \in G$, natural numbers $L_1, ..., L_d$ and a subgroup H.

Theorem 3.4 (Freĭman's Theorem in arbitrary abelian groups). *Suppose that G is an abelian group and $A \subset G$ is finite with $|A+A| \leqslant K|A|$. Then A is contained in a $O(K^4 \log(1+K))$-dimensional coset progression of size at most* $\exp(O(K^4 \log^2(1+K)))|A|$.

The first section of this chapter is a refinement of Freĭman's theorem for vector spaces over $\mathbb{F}_2$. It is principally of interest as a method and was recently used by Bourgain [Bou08] (see [San08b] to improve the bounds in Freĭman's Theorem for $\mathbb{Z}$, specifically the bounds on the dimension and size of the progression in Theorem 3.2 are improved to $O(K^{7/4} \log^3(1+K))$ and $\exp(O(K^{7/4} \log^3(1+K)))|A|$ respectively.

Although of interest in its own right, Freĭman's Theorem has found a number of applications (see, for example, [BC03, Bou03, GS08a, SSV05]) following the work of Gowers [Gow98] who introduced a fundamental proof method which employs it. As a tool we can often find ourselves interested not so much in containing A in a coset progression but rather simply something which behaves like an 'approximate group'.

In proving his theorem Freĭman introduced the fundamental concept of Freĭman homomorphisms. If G and G' are two abelian groups containing the sets A and A' respectively then we say that $\phi : A \to A'$ is a Freĭman s-homomorphism if whenever $a_1, ..., a_s, b_1, ..., b_s \in A$ satisfy

$$a_1 + ... + a_s = b_1 + ... + b_s$$

we have

$$\phi(a_1) + ... + \phi(a_s) = \phi(b_1) + ... + \phi(b_s).$$

If ϕ has an inverse which is also an s-homomorphism then we say that ϕ is a Freĭman s-isomorphism.

We naturally want the Freĭman homomorphic image of an 'approximate group' to be an approximate group and Bohr sets are insufficient for this purpose. This precipitated the introduction of Bourgain systems in [GS08b] whose structure *is* preserved under Freĭman homomorphisms. In the second section of this chapter, building on work of Green and Tao [GT09b], we prove what might be called a partially polynomial version of Freĭman's Theorem local to Bourgain systems. A more detailed discussion may be found there.

3.1 Freĭman's Theorem in finite fields

In this section we shall improve the bounds in Theorem 3.3 in the special case of $r = 2$. While finite field models are an important tool for understanding problems in general abelian groups, this result has independent significance in coding theory and has been pursued by a number of authors. We do not attempt a comprehensive survey here, but mention a few papers which are important from our standpoint.

The first improvements on this was in the paper [DHP04] of Deshouillers, Hennecart and Plagne. There, the authors present a relatively simple argument which shows that one may take the coset in which A is contained to be of size at most $K2^{\lfloor K^3\rfloor-1}|A|$. The bulk of their paper concerns refined estimates for the case when K is small; by contrast our interest lies in the asymptotics.

In a recent paper, [GR07], Green and Ruzsa improve the bound from [DHP04] when they show that one may take a size bound of $K^2 2^{\lfloor 2K^2-2\rfloor}|A|$. Our result, then, gives a size bound of $2^{O(K^{3/2}\log(1+K))}|A|$. Specifically we prove the following theorem.

Theorem 3.1.1 (Freĭman's Theorem in finite fields)**.** *Suppose that G is a vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ is a finite set with $|A+A| \leqslant K|A|$. Then A is contained in a coset of size at most $2^{O(K^{3/2}\log(1+K))}|A|$.*

For comparison we record the following well known example which shows that one cannot have a size bound better than $2^{2K+o(K)}|A|$. Let H be a finite subgroup of G and $g_1 + H, ..., g_{2K-1} + H$ be $2K - 1$ linearly independent cosets of H in the quotient space G/H. Let A be the union of H and the representatives $g_1, ..., g_{2K-1}$. Then $|A| = |H| + 2K - 1 \sim |H|$ and

$$|A + A| \leqslant K(|H| + K) \sim K|H| \lesssim K|A|.$$

However A contains a linearly independent set of size $\dim H + 2K - 1$ and so A is not contained in a coset of dimension less than $\dim H + 2K - 2$ hence if H' is a coset containing A then

$$|H'| \geqslant 2^{\dim H + 2K - 2} = 2^{2K-2}|H| \gtrsim 2^{2K-2}|A|.$$

Very recently in [GT09a], Green and Tao have improved Theorem 3.1.1 further and showed that the above example is essentially extremal; specifically they have proved a size bound of $2^{2K+o(K)}|A|$.

3.1.1 Proof of Theorem 3.1.1

Our proof is really a refinement of Green and Ruzsa's proof of Freĭman's Theorem for arbitrary abelian groups.

Their method becomes significantly simpler in the vector space setting, and would immediately give us the following weak version of the main theorem.

Theorem 3.1.2. *Suppose that G is a vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ is a finite set with $|A + A| \leqslant K|A|$. Then A is contained in a coset of size at most $2^{O(K^2 \log(1+K))}|A|$.*

The proof involves three main step.

- *(Finding a good model)* First we use the fact that $|A + A| \leqslant K|A|$ to show that A can be embedded as a *dense* subset of $\mathbb{F}_2^n$ in a way which preserves much of its additive structure.

- *(Bogolioùboff's argument)* Next we show that if A is a dense subset of $\mathbb{F}_2^n$ and A has small doubling then $2A - 2A$ contains a large subspace.

- *(Pullback and covering)* Finally we use our embedding to pull back this subspace to a coset in the original setting. A covering argument then gives us the result.

Our refinement of this argument occurs at the second stage.

Finding a good model

A simple but elegant argument establishes the existence of a small vector space into which we can embed our set via a Freĭman isomorphism.

Proposition 3.1.3. ([GR07, Proposition 6.1]) *Suppose that A is a subset of a vector space over $\mathbb{F}_2$. Suppose that $|A+A| \leqslant K|A|$. Then there is a vector space G' over $\mathbb{F}_2$ with $|G'| \leqslant K^{2s}|A|$ with a set $A' \subset G'$, and a Freĭman s-isomorphism $\phi : A \to A'$.*

Bogolioùboff's argument

Originally (in [Ruz96]) Ruzsa employed an argument of Bogolioùboff (see [Bog39]) for this stage. In [Cha02] Chang refined this further when she proved the following.[1]

Proposition 3.1.4. *Suppose that $G = \mathbb{F}_2^n$. Suppose that $A \subset G$ has density α and $\mu_G(A+A) \leqslant K\mu_G(A)$. Then $2A-2A$ contains a subspace of codimension $O(K \log \alpha^{-1})$.*

We prove the following refinement of this.

Proposition 3.1.5. *Suppose that $G = \mathbb{F}_2^n$. Suppose that $A \subset G$ has density α and $\mu_G(A+A) \leqslant K\mu_G(A)$. Then $2A-2A$ contains a subspace of codimension $O(K^{1/2} \log \alpha^{-1})$.*

To prove this we require the following *pure density* version of the proposition.

Proposition 3.1.6. ([San08a, Theorem 2.4]) *Suppose that G is a finite vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ has density α. Then $2A-2A$ contains a subspace of codimension $O(\alpha^{-1/2})$.*

The proof in [San08a] is for general finite abelian groups and becomes significantly simpler in the vector space setting; the basic technique is iterative.

[1] Although in [Cha02] it is stated for $G = \mathbb{Z}/N\mathbb{Z}$, the same proof applies to any finite abelian group and in particular to $\mathbb{F}_2^n$.

Lemma 3.1.7 (Iteration lemma). *Suppose that G is a finite vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ has density α. Then at least one of the following is true.*

(i). $2A - 2A$ *contains all of* G.

(ii). *There is a 1 dimensional subspace V of $\widehat{G}$, an element $x \in G$ and a set $A' \subset V^{\perp}$ with the following properties.*

- $x + A' \subset A$;
- $\mu_{V^{\perp}}(A') \geqslant \alpha(1 + 2^{-1}\alpha^{1/2})$.

Proof. As usual with problems of this type studying the sumset $2A - 2A$ is difficult so we turn instead to $g := 1_A * 1_A * 1_{-A} * 1_{-A}$ which has support equal to $2A - 2A$. One can easily compute the Fourier transform of g in terms of that of 1_A:

$$\widehat{g}(\gamma) = |\widehat{1_A}(\gamma)|^4 \text{ for all } \gamma \in \widehat{G},$$

from which it follows that g is very smooth. Specifically $\widehat{g} \in \ell^{\frac{1}{2}}(\widehat{G})$ since

$$\sum_{\gamma \in \widehat{G}} |\widehat{g}(\gamma)|^{\frac{1}{2}} = \sum_{\gamma \in \widehat{G}} |\widehat{1_A}(\gamma)|^2 = \alpha \tag{3.1.1}$$

by Parseval's Theorem. We may assume that $\mu_G(2A - 2A) < 1$ since otherwise we are in the first case of the lemma, so $S := (2A - 2A)^c$ has positive density, say σ. Plancherel's Theorem gives

$$0 = \langle 1_S, g \rangle = \sum_{\gamma \in \widehat{G}} \overline{\widehat{1_S}(\gamma)} \widehat{g}(\gamma) \Rightarrow |\widehat{1_S}(0_{\widehat{G}})\widehat{g}(0_{\widehat{G}})| \leqslant \sum_{\gamma \neq 0_{\widehat{G}}} |\widehat{1_S}(\gamma)\widehat{g}(\gamma)|.$$

$\widehat{g}(0_{\widehat{G}}) = \alpha^4$, $\widehat{1_S}(0_{\widehat{G}}) = \sigma$ and $|\widehat{1_S}(\gamma)| \leqslant \|1_S\|_{L^1(\mu_G)} = \sigma$, so the above yields

$$\sigma\alpha^4 \leqslant \sigma \sum_{\gamma \neq 0_{\widehat{G}}} |\widehat{g}(\gamma)| \Rightarrow \alpha^4 \leqslant \sum_{\gamma \neq 0_{\widehat{G}}} |\widehat{g}(\gamma)| \text{ since } \sigma > 0.$$

Finding a non-trivial character at which $\widehat{g}$ is large is now simple since $\widehat{g} \in$

$\ell^{\frac{1}{2}}(\widehat{G})$.

$$\alpha^4 \leqslant \sup_{\gamma \neq 0_{\widehat{G}}} |\widehat{g}(\gamma)|^{\frac{1}{2}} \left(\sum_{\gamma \in \widehat{G}} |\widehat{g}(\gamma)|^{\frac{1}{2}} \right) \leqslant \sup_{\gamma \neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)|^2.\alpha$$

by (3.1.1). Rearranging this we have

$$\sup_{\gamma \neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)| \geqslant \alpha^{\frac{3}{2}}.$$

We pick a character, γ, which attains this maximum and proceed with a standard L^∞-density-increment argument. Let $V := \{0_{\widehat{G}}, \gamma\}$ and $f := 1_A - \alpha$. Then

$$\int f * \mu_{V^\perp} d\mu_G = 0 \text{ and } \|f * \mu_{V^\perp}\|_{L^1(\mu_G)} \geqslant \|\widehat{f}\widehat{\mu_{V^\perp}}\|_{\ell^\infty(\widehat{G})} = |\widehat{1_A}(\gamma)|.$$

Adding these we conclude that

$$\begin{aligned} |\widehat{1_A}(\gamma)| &\leqslant 2\int (f * \mu_{V^\perp})_+ d\mu_G \\ &= 2\int (1_A * \mu_{V^\perp} - \alpha)_+ d\mu_G \\ &\leqslant 2(\|1_A * \mu_{V^\perp}\|_{L^\infty(\mu_G)} - \alpha). \end{aligned}$$

Here, of course, $(f * \mu_{V^\perp})_+$ denotes the function $\max\{f * \mu_{V^\perp}(x), 0\}$.

Hence there is some $x \in G$ with

$$1_A * \mu_{V^\perp}(x) = \|1_A * \mu_{V^\perp}\|_{L^\infty(\mu_G)} \geqslant \alpha(1 + 2^{-1}\alpha^{1/2}).$$

The result follows on taking $A' = x + A$. □

Proof of Proposition 3.1.6. We define a nested sequence of subspaces $V_0 \leqslant V_1 \leqslant ... \leqslant \widehat{G}$, elements $x_k \in V_k^\perp$ and subsets A_k of $V_k^\perp$ with density α_k, such that $x_k + A_k \subset A_{k-1}$. We begin the iteration with $V_0 := \{0_{\widehat{G}}\}$, $A_0 := A$ and $x_0 = 0_G$.

Suppose that we are at stage k of the iteration. If $\mu_{V_k^\perp}(2A_k - 2A_k) < 1$ then we apply Lemma 3.1.7 to A_k considered as a subset of $V_k^\perp$. We get a vector space V_{k+1} with $\dim V_{k+1} = 1 + \dim V_k$, an element $x_{k+1} \in G$ and a set A_{k+1} such that

$$x_{k+1} + A_{k+1} \subset A_k \text{ and } \alpha_{k+1} \geqslant \alpha_k(1 + 2^{-1}\alpha_k^{1/2}).$$

It follows from the density increment that if $m_k = 2\alpha_k^{-1/2}$ then $\alpha_{k+m_k} \geqslant 2\alpha_k$. Define the sequence $(N_l)_l$ recursively by $N_0 = 0$ and $N_{l+1} = m_{N_l} + N_l$. The density α_{N_l} is easily estimated:

$$\alpha_{N_l} \geqslant 2^l\alpha \text{ and } N_l \leqslant \sum_{s=0}^{l} 2\alpha_{N_s}^{-1/2} \leqslant 2\alpha^{-1/2}\sum_{s=0}^{l} 2^{-s/2} = O(\alpha^{-1/2}).$$

Since density cannot be greater than 1 there is some stage k with $k = O(\alpha^{-1/2})$ when the iteration cannot proceed i.e. for which $2A_k - 2A_k$ contains all of $V_k^{\perp}$. By construction of the A_ks there is a translate of A_k which is contained in $A_0 = A$ and hence $2A_k - 2A_k$ is contained in $2A - 2A$. It follows that $2A - 2A$ contains a subspace of G of codimension $k = O(\alpha^{-1/2})$. □

The key ingredient in the proof of Proposition 3.1.5 is the following iteration lemma, which has a number of similarities with Lemma 3.1.8.

Lemma 3.1.8. *Suppose that $G = \mathbb{F}_2^n$. Suppose that $A, B \subset G$ have $\mu_G(A + B) \leqslant K\mu_G(B)$. Write α for the density of A. Then at least one of the following is true.*

(i). B contains a subspace of codimension $O(K^{1/2})$.

(ii). There is a 1 dimensional subspace V of $\widehat{G}$, elements $x, y \in G$ and sets $A', B' \subset V^{\perp}$ with the following properties.

- *$x + A' \subset A$ and $y + B' \subset B$;*
- *$\mu_{V^{\perp}}(A') \geqslant \alpha(1 + 2^{-3/2}K^{-1/2})$;*
- *$\mu_{V^{\perp}}(A' + B') \leqslant K\mu_{V^{\perp}}(B')$.*

Proof. If $\mu_G(B) \geqslant (2K)^{-1}$ then we apply Proposition 3.1.6 to get that B contains a subspace of codimension $O(K^{1/2})$ and we are in the first case of the lemma. Hence we assume that $\mu_G(B) \leqslant (2K)^{-1}$.

Write β for the density of B. We have

$$\begin{aligned}(\alpha\beta)^2 &= \left(\int 1_A * 1_B d\mu_G\right)^2\\ &\leqslant \mu_G(A+B)\int (1_A * 1_B)^2 d\mu_G \text{ by Cauchy-Schwarz,}\\ &\leqslant K\beta \int (1_A * 1_B)^2 d\mu_G \text{ by hypothesis,}\\ &= K\beta \sum_{\gamma\in\widehat{G}} |\widehat{1_A}(\gamma)|^2|\widehat{1_B}(\gamma)|^2 \text{ by Parseval's Theorem.} \qquad (3.1.2)\end{aligned}$$

The main term in the sum on the right is the contribution from the trivial character, in particular

$$|\widehat{1_A}(0_{\widehat{G}})|^2|\widehat{1_B}(0_{\widehat{G}})|^2 = \alpha^2\beta^2,$$

while

$$\begin{aligned}\sum_{\gamma\neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)|^2|\widehat{1_B}(\gamma)|^2 &\leqslant \sup_{\gamma\neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)|^2 \sum_{\gamma\in\widehat{G}} |\widehat{1_B}(\gamma)|^2\\ &= \beta \sup_{\gamma\neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)|^2\end{aligned}$$

by Parseval's Theorem for 1_B. Putting these last two observations in (3.1.2) gives

$$\alpha^2\beta^2 \leqslant K\beta^3\alpha^2 + K\beta^2 \sup_{\gamma\neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)|^2.$$

Since $K\beta \leqslant 2^{-1}$ we can rearrange this to conclude that

$$\sup_{\gamma\neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)| \geqslant (2K)^{-1/2}\alpha.$$

As before we may pick a character γ which attains this maximum and proceed with a standard L^∞-density-increment argument. Let $V := \{0_{\widehat{G}}, \gamma\}$ and $f := 1_A - \alpha$. Then

$$\int f * \mu_{V^\perp} d\mu_G = 0 \text{ and } \|f * \mu_{V^\perp}\|_{L^1(\mu_G)} \geqslant \|\widehat{f}\widehat{\mu_{V^\perp}}\|_{\ell^\infty(\widehat{G})} = |\widehat{1_A}(\gamma)|.$$

Adding these we conclude that

$$\begin{aligned}|\widehat{1_A}(\gamma)| &\leqslant 2\int (f * \mu_{V^\perp})_+ d\mu_G\\ &= 2\int (1_A * \mu_{V^\perp} - \alpha)_+ d\mu_G\\ &\leqslant 2(\|1_A * \mu_{V^\perp}\|_{L^\infty(\mu_G)} - \alpha).\end{aligned}$$

It follows that there is some x for which

$$1_A * \mu_{V^\perp}(x) \geqslant \alpha(1 + 2^{-3/2}K^{-1/2}).$$

Let $x' + V^\perp := G \setminus (x + V^\perp)$ be the *other* coset of $V^\perp$ in G. Write $A_1 = A \cap (x + V^\perp)$, $B_1 = B \cap (x + V^\perp)$ and $B_2 = B \cap (x' + V^\perp)$. Now $A_1 \subset A$ so

$$(A_1 + B_1) \cup (A_1 + B_2) \subset A + B_1 \cup B_2,$$

and $A_1 + B_1 \subset V^\perp$ while $A_1 + B_2 \subset x + x' + V^\perp$ so these two sets are disjoint and we conclude that

$$\begin{aligned}\mu_G(A_1 + B_1) + \mu_G(A_1 + B_2) &= \mu_G((A_1 + B_1) \cup (A_1 + B_2))\\ &\leqslant \mu_G(A + B_1 \cup B_2)\\ &\leqslant K\mu_G(B_1 \cup B_2) \text{ by hypothesis}\\ &\leqslant K(\mu_G(B_1) + \mu_G(B_2)).\end{aligned}$$

Hence, by averaging, there is some i such that

$$\mu_G(A_1 + B_i) \leqslant K\mu_G(B_i).$$

We take $A' = x + A_1$ and, if $i = 1$, $B' = x + B_1$ and $y = x$, while if $i = 2$, $B' = x' + B_2$ and $y = x'$. The result follows. □

Proof of Proposition 3.1.5. We define a nested sequence of subspaces $V_0 \leqslant V_1 \leqslant ... \leqslant \widehat{G}$, elements $x_k, y_k \in V_k^\perp$, and subsets A_k and B_k of $V_k^\perp$ such that $A_k + x_k \subset A_{k-1}$ and $B_k + y_k \subset B_{k-1}$ and $\mu_{V_k^\perp}(A_k + B_k) \leqslant K\mu_{V_k^\perp}(B_k)$. We write α_k for the density of A_k in $V_k^\perp$. Begin the iteration with $V_0 := \{0_{\widehat{G}}\}$, $B_0 = A_0 := A$ and $x_0 = y_0 = 0_G$.

Suppose that we are at stage k of the iteration. We apply Lemma 3.1.8 to A_k and B_k inside $V_k^\perp$ (which we can do since $\mu_{V_k^\perp}(A_k + B_k) \leqslant K\mu_{V_k^\perp}(B_k)$). It follows that either $2B_k - 2B_k$ contains a subspace of codimension $O(K^{1/2})$ in $V_k^\perp$ or we get a subspace $V_{k+1} \leqslant \widehat{V_k}$ with $\dim V_{k+1} = 1 + \dim V_k$, elements $x_{k+1}, y_{k+1} \in V_k^\perp$ and sets A_{k+1} and B_{k+1} with the following properties.

- $x_{k+1} + A_{k+1} \subset A_k$ and $y_{k+1} + B_{k+1} \subset B_k$;
- $\mu_{V^\perp}(A_{k+1}) \geqslant \alpha_k(1 + 2^{-3/2}K^{-1/2})$;
- $\mu_{V^\perp}(A_{k+1} + B_{k+1}) \leqslant K\mu_{V^\perp}(B_{k+1})$.

It follows from the density increment that if $m = 2^{3/2}K^{1/2}$ then $\alpha_{k+m} \geqslant 2\alpha_k$, and hence the iteration must terminate (because density can be at most 1) at some stage k with $k = O(K^{1/2}\log\alpha^{-1})$. The iteration terminates if $2B_k - 2B_k$ contains a subspace of codimension $O(K^{1/2})$ in $V_k^\perp$, from which it follows that $2A - 2A \supset 2B_k - 2B_k$ contains a subspace of codimension $k + O(K^{1/2}) = O(K^{1/2}\log\alpha^{-1})$. □

Pullback and covering

We now complete the proof of the main theorem using a covering argument.

We are given $A \subset G$ finite with $|A + A| \leqslant K|A|$. By Proposition 3.1.3 there is a finite vector space (over $\mathbb{F}_2$) G' with $|G'| \leqslant K^{16}|A|$ and a subset A' with A' Freĭman 8-isomorphic to A. It follows that

$$\mu_{G'}(A') \geqslant K^{-16} \text{ and } \mu_{G'}(A' + A') \leqslant K\mu_{G'}(A').$$

We apply Proposition 3.1.5 to conclude that $2A' - 2A'$ contains a subspace of codimension $O(K^{1/2}\log(1+K))$. However, A is 8-isomorphic to A' so $2A - 2A$ is 2-isomorphic to $2A' - 2A'$ and it is easy to check that the 2-isomorphic pullback of a subspace is a coset so $2A - 2A$ contains a coset of size

$$2^{-O(K^{1/2}\log(1+K))}|G'| \geqslant 2^{-O(K^{1/2}\log(1+K))}|A|.$$

The following covering result of Chang [Cha02] converts this large coset contained in $2A-2A$ into a small coset containing A. It is true in more generality than we state; we only require the version below.

Proposition 3.1.9. *Suppose that G is a vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ is a finite set with $|A+A| \leqslant K|A|$. Suppose that $2A-2A$ contains a coset of size $\eta|A|$. Then A is contained in a coset of size at most $2^{O(K\log K\eta^{-1})}|A|$.*

Theorem 3.1.1 follows immediately from this proposition and the argument preceding it.

3.2 A weak Freĭman theorem

The example at the start of the previous section can be adapted to show that one cannot hope to improve the size bound on the progression in Theorem 3.2 to have sub-exponential dependence on the doubling. Often we would like polynomial dependence, and sometimes it is sufficient to have a large progression which intersects A in a *polynomially* large proportion of itself. Such a result was originally proved by Green and Tao in [GT09b]; our proof is from the joint paper [GS08b] of Green and the author and uses a method similar to the previous section.

There is a second direction in which the main result of the section differs from standard Freĭman theorems: it is stated relative to Bourgain systems. Here, the crucial property of Bourgain systems is that they are preserved by Freĭman homomorphisms:

Lemma 3.2.1. *Suppose that $\mathcal{B} = (B_\rho)_\rho$ is a Bourgain system and that $\phi : B_4 \to G'$ is some Freĭman 2-isomorphism such that $\phi(0) = 0$. Then $\phi(\mathcal{B}) := (\phi(B_\rho))_\rho$ is a Bourgain system of the same dimension and size.*

We are now in a position to state the key result.

Proposition 3.2.2. *Suppose that G is a finite abelian group, and that $A \subset G$ is a finite set with $|A+A| \leqslant K|A|$. Then there is a regular Bourgain system*

$\mathcal{B} = (B_\rho)_\rho$ of dimension at most $O(K^{O(1)})$ and with

$$\mu_G(\mathcal{B}) \geqslant \exp(-O(K^{O(1)}))\mu_G(A) \text{ and } \|1_A * \beta_1\|_{L^\infty(\mu_G)} \gg K^{-1}.$$

We begin as in the previous section.

Finding a good model

Proposition 3.2.3. (Good Models, [GR07, Proposition 1.2]) *Suppose that G is an abelian group and $A \subset G$ is finite with $|A + A| \leqslant K|A|$. Suppose that $s \geqslant 2$ is an integer. Then there is an abelian group G' with $|G'| \leqslant (10sK)^{10K^2}|A|$ such that A is Freĭman s-isomorphic to a subset of G'.*

Bogolioùboff's argument

This is very close to the variant of Bogolioùboff's argument due to Chang which we alluded to in the previous section (see Proposition 3.1.4).

Proposition 3.2.4. *Suppose that G is a finite abelian group, and that $A \subset G$ has density α and $|A+A| \leqslant K|A|$. Then there is a regular Bourgain system $\mathcal{B}$ of dimension $d = O(K \log \alpha^{-1})$ and with*

$$\mu_G(\mathcal{B}) \geqslant \exp(-O(d \log(1 + d))) \text{ and } \|1_A * \beta_1\|_{L^\infty(\mu_G)} \gg K^{-1},$$

such that $B_4 \subset 2A - 2A$.

Proof. Set

$$\Gamma := \{\gamma \in \widehat{G} : |\widehat{1_A}(\gamma)| \geqslant \frac{\alpha}{2\sqrt{K}}\}$$

and apply Chang's Theorem to get a set of characters Λ with $|\Lambda| \ll K(1 + \log \alpha^{-1})$ and $\Gamma \subset \langle \Lambda \rangle$. Now if $\gamma \in \Gamma$ then $\gamma = m.\Lambda$ for some $m : \Lambda \to \{-1, 0, 1\}$. Thus by the triangle inequality we have

$$|1 - \gamma(x)| \leqslant \sum_{\lambda \in \Lambda} |1 - \lambda(x)|.$$

Now if $x \in B(\Lambda, 1/10\pi|\Lambda|)$ and $\gamma \in \Gamma$ then

$$\begin{aligned} |1-\gamma(x)| &\leqslant |\Lambda| \sup_{\lambda\in\Lambda} |1-\lambda(x)| \\ &= |\Lambda| \sup_{\lambda\in\Lambda} \sqrt{2(1-\cos(4\pi\|\lambda(x)\|))} \\ &\leqslant 2/5. \end{aligned} \tag{3.2.1}$$

Now by the inversion formula we have

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

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

$$\|\widehat{1}_A\|^4_{\ell^4(\widehat{G})} = \|1_A * 1_A\|^2_{L^2(\mu_G)} \geqslant \alpha^3/K. \tag{3.2.2}$$

It follows that

$$\|\widehat{1}_A\|^4_{\ell^4(\widehat{G})} - 1_A * 1_A * 1_{-A} * 1_{-A}(x) \leqslant \left(\frac{2}{5}+\frac{1}{2}\right)\|\widehat{1}_A\|^4_{\ell^4(\widehat{G})} < \|\widehat{1}_A\|^4_{\ell^4(\widehat{G})},$$

and hence $1_A * 1_A * 1_{-A} * 1_{-A}(x) > 0$, so $x \in 2A - 2A$. It follows that $B(\Lambda, 1/10\pi|\Lambda|) \subset 2A - 2A$.

Take

$$\mathcal{B} = (B_\rho)_\rho \text{ where } B_\rho = B(\Gamma, \rho/40\pi|\Lambda|).$$

The previous argument ensures that $B_4 \subset 2A - 2A$. Moreover by Lemma 2.4.2 we conclude that $\mathcal{B}$ is a Bourgain system with dimension $d = 2|\Lambda| =$

$O(K\log\alpha^{-1})$ and density at least $\exp(-O(d\log(1+d)))$.

It remains to show that $\|1_A * \beta_1\|_{L^\infty(\mu_G)} \gg K^{-1}$. By (3.2.1), if $x \in B_1$ and $\gamma \in \Gamma$ then $|1-\gamma(x)| \leqslant 2/5$. It follows that $|1-\widehat{\beta_1}(\gamma)| \leqslant 2/5$ and hence

$$\|\widehat{1_A * \beta_1}\|_{\ell^4(\widehat{G})} \geqslant (3/5)^4 \sum_{\gamma\in\Gamma} |\widehat{1_A}(\gamma)|^4 \gg \|\widehat{1_A * \beta_1}\|_{\ell^4(\widehat{G})}.$$

It follows from (3.2.2) that

$$\begin{aligned}\alpha^3/K \ll \|\widehat{1_A * \beta_1}\|_{\ell^4(\widehat{G})} &= \|1_A * \beta_1 * 1_A * \beta_1\|^2_{L^2(\mu_G)}\\ &\leqslant \|1_A * \beta_1\|_{L^\infty(\mu_G)}\alpha^3.\end{aligned}$$

This yields the result. □

Pullback

The different goal of this result means that we are no longer concerned with the covering aspect of the 'Pullback and covering' part of the last section. Moreover, Lemma 3.2.1 lets us pullback the Bourgain system to another Bourgain system directly.

Proof of Proposition 3.2.2. By Proposition 3.2.3 there is an abelian group G', $|G'| \leqslant \exp(O(K^2\log(1+K)))|A|$, and a subset $A' \subset G'$ such that A' is 14-isomorphic to A. We apply Proposition 3.2.4 to this set A', the density of which we denote by α. Noting that $\alpha \gg \exp(-O(K^2\log(1+K)))$, we obtain a Bourgain system $\mathcal{B}' = (B'_\rho)_\rho$ with dimension $O(K^{O(1)})$,

$$|B'_1| \gg \exp(-O(K^{O(1)}))|A'| \text{ and } \|1_A * \beta'_1\|_{L^\infty(\mu_G)} \gg K^{-1},$$

and $B'_4 \subseteq 2A' - 2A'$. Write $\phi : A' \to A$ for the Freĭman 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' Freĭman 14-isomorphism $\phi_0(x) := \phi(x) - \phi(0)$.

Define $\mathcal{B} := \phi_0(\mathcal{B}')$. Since $B'_4 \subseteq 2A' - 2A'$, ϕ_0 is a Freĭman 2-isomorphism on B_4' with $\phi_0(0) = 0$. Therefore $\mathcal{B}$ is indeed a Bourgain system, with the same dimension as $\mathcal{B}'$ and $|B_1| = |B_1'|$.

It remains to check that $\|1_A * \beta_1\|_{L^\infty(\mu_G)} \gg K^{-1}$. The fact that $\|1_{A'} * \beta_1'\|_{L^\infty(\mu_G)} \gg K^{-1}$ means that there is x such that $|1_{A'} * \beta_1'(x)| \gg K^{-1}$. Since $\operatorname{supp} \beta_1' \subset B_1' \subset B_4' \subseteq 2A' - 2A'$, 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

$$x = a' - t_1' + t_2', \text{ with } a' \in A', t_i' \in B_1',$$

is the same as the number of solutions to

$$\phi_0(x) = \phi_0(a') - \phi_0(t_1') + \phi_0(t_2'), \text{ with } a' \in A', t_i' \in B_1'.$$

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 $7A' - 7A'$. $\square$

Chapter 4

Littlewood's conjecture and the idempotent theorem

It is a long standing question of Littlewood's (see [HL48]) to determine the smallest possible value of $\|1_A\|_{A(\mathbb{Z})}$ when A is a set of size N. It may be useful to recall that

$$\|1_A\|_{A(\mathbb{Z})} = \int_0^1 |\sum_{a\in A} \exp(2\pi a\theta)| d\theta.$$

The quantity $\|1_A\|_{A(\mathbb{Z})}$ is a sort of measure of the complexity of the set A: if $\|1_A\|_{A(\mathbb{Z})}$ is small then most of the Fourier mass is supported on a few modes so it is a 'low complexity' object, conversely if it is large then the Fourier mass is spread out and it is a 'high complexity' object. In view of this it becomes interesting to ask how 'simple' a set can be; it is natural to consider the case when A is an arithmetic progression. Here

$$\|1_A\|_{A(\mathbb{Z})} = \frac{4}{\pi^2}\log N + O(1),$$

a result which may be found in, for example, Zygmund [Zyg02, Section II.12], although in any case it is not hard to convince oneself that $\|1_A\|_{A(\mathbb{Z})} \gg \log N$. The problem then becomes one of trying to show that this is best possible. A lot of work was done before this was proved, independently, in the early 1980s by Konyagin [Kon81] and McGehee, Pigno and Smith [MPS81].

Theorem 4.1 (Littlewood conjecture)**.** *Suppose that A is a finite set of N*

integers. Then $\|1_A\|_{A(\mathbb{Z})} \gg \log N$.

This, however, did not completely finish the problem and there is still the question of the *strong* Littlewood conjecture.

Conjecture 4.2 (Strong Littlewood conjecture)**.** *Suppose that A is a finite set of N integers. Then*

$$\|1_A\|_{A(\mathbb{Z})} \geqslant \frac{4}{\pi^2} \log N + O(1).$$

In a different direction it is rather natural to consider the problem for other abelian groups. Here, however, a difficulty arises. Suppose that G is a finite abelian group. Cosets of subgroups of G have characteristic functions with very small algebra norm. Suppose that $V \leqslant \widehat{G}$ and $A = x + V^{\perp}$. Then a simple calculation gives

$$\widehat{1_A}(\gamma) = \begin{cases} \gamma(x)|V|^{-1} & \text{if } \gamma \in V \\ 0 & \text{otherwise.} \end{cases}$$

It follows that $\|1_A\|_{A(G)} = 1$, and hence (since $\|.\|_{A(G)}$ is an algebra norm) that any small combination of unions and intersections of cosets will also have small norm.

In the more general setting of a locally compact abelian group G we define the coset ring to be the smallest family of subsets of G containing all open subgroups of G and which is closed under complements, unions and intersections. It is a remarkable result of Cohen [Coh60], that this includes all the subsets of G with characteristic functions in $A(G)$.

Theorem 4.3 (Idempotent theorem)**.** *Suppose that G is a locally compact abelian group. Suppose that $A \subset G$ has $1_A \in A(G)$. Then A is in the coset ring of G.*

In words, what the theorem says is that if $1_A \in A(G)$, i.e. its algebra norm is finite, then it can be written as a finite $\pm$-sum of indicator functions of cosets. For example, suppose that $K \leqslant H \leqslant G$ are open subgroups of G

and $A = H \setminus K$. Then $1_A \in A(G)$ and, moreover,

$$1_A = 1_H - 1_K.$$

The converse is trivially true: any finite $\pm$-sum of indicator functions of cosets is in $A(G)$, so the theorem provides an exact characterization of those sets whose indicator functions are in $A(G)$.

In the finite setting Cohen's result has no content, but there are two obvious ways in which one might go about making it quantitative and so effective in the finite setting. First note the following immediate consequence of the idempotent theorem for which there is also an easy and direct proof. If x is a real then we write $\{x\}$ for the fractional part of x.

Proposition 4.4. *Suppose that G is a compact abelian group. Suppose that $A \subset G$ has density α and for all finite $V \leqslant \widehat{G}$ we have $\{\alpha|V|\}(1-\{\alpha|V|\}) > 0$. Then $1_A \notin A(G)$.*

We have written the hypothesis on α in a slightly peculiar fashion to make clear the connection to the quantitative version of the result. All the condition really says is that $\alpha \neq n\mu_G(H)$ for any integer n and open subgroup H; this sort of condition is fairly natural in the light of the idempotent theorem. We shall prove a theorem of the following form to make Proposition 4.4 quantitative.

Theorem 4.5. *Suppose that G is a finite abelian group. Suppose that $A \subset G$ has density α and for all $V \leqslant \widehat{G}$ with $|V| \leqslant M$ we have $\{\alpha|V|\}(1-\{\alpha|V|\}) \gg 1$. Then*

$$\|1_A\|_{A(G)} \gg f(M)$$

for some function f for which $f(M) \to \infty$ as $M \to \infty$.

It turns out that different groups require very different methods, with the dyadic groups at one end of the spectrum and the arithmetic groups at the other. We begin with the dyadic groups and in §4.1 prove the following theorem.

Theorem 4.6. *Suppose that $G = \mathbb{F}_2^n$. Suppose that $A \subset G$ has density α and for all $V \leqslant \widehat{G}$ with $|V| \leqslant M$ we have $\{\alpha|V|\}(1 - \{\alpha|V|\}) \gg 1$. Then*

$$\|1_A\|_{A(G)} \gg \log\log M.$$

Possibly the most interesting case, and one which captures the essence of the problem is when α is roughly $1/3$. Specifically if $|\alpha - 1/3| \leqslant 1/2M$, then the hypotheses of the theorem are satisfied. This example is discussed in more detail in §4.1, but the idea is that if A is a set with a density which can't be easily written as a $\pm$-sum of powers of 2, then 1_A cannot be written as a $\pm$-sum of a small number of cosets.

In that section we present a simple example to show that nothing better than the following conjecture can be true.

Conjecture 4.7. *Suppose that $G = \mathbb{F}_2^n$. Suppose that $A \subset G$ has density α and for all $V \leqslant \widehat{G}$ with $|V| \leqslant M$ we have $\{\alpha|V|\}(1 - \{\alpha|V|\}) \gg 1$. Then*

$$\|1_A\|_{A(G)} \gg \log M.$$

In §4.2 we consider the arithmetic groups and prove the following (although it is stated in a slightly different manner).

Theorem 4.8. *Suppose that $G = \mathbb{Z}/p\mathbb{Z}$ for some prime p. Suppose that $A \subset G$ has density α and for all $V \leqslant \widehat{G}$ with $|V| \leqslant M$ we have $\{\alpha|V|\}(1 - \{\alpha|V|\}) \gg 1$. Then*

$$\|1_A\|_{A(G)} \gg \left(\frac{\log M}{(\log\log M)^3}\right)^{1/2}.$$

Note that in this result the density condition collapses to α being bounded away from 0 and 1, and M may be taken as large as $p - 1$ (provided it is at least 1!). Analogy with the Littlewood conjecture leads one to the following.

Conjecture 4.9. *Suppose that $G = \mathbb{Z}/p\mathbb{Z}$ for some prime p. Suppose that $A \subset G$ has density α and for all $V \leqslant \widehat{G}$ with $|V| \leqslant M$ we have $\{\alpha|V|\}(1 - \{\alpha|V|\}) \gg 1$. Then*

$$\|1_A\|_{A(G)} \gg \log M.$$

Finally in §4.3 we combine the rather different methods of §4.1 and §4.2 to prove the following general result. The combination is a little more tricky than one might hope which is why we get a rather weak bound.

Theorem 4.10. *Suppose that G is a finite abelian group. Suppose that $A \subset G$ has density α and for all $V \leqslant \widehat{G}$ with $|V| \leqslant M$ we have $\{\alpha|V|\}(1 - \{\alpha|V|\}) \gg 1$. Then*

$$\|1_A\|_{A(G)} \gg \log\log\log M.$$

One might make the following conjecture.

Conjecture 4.11. *Suppose that G is a finite abelian group. Suppose that $A \subset G$ has density α and for all $V \leqslant \widehat{G}$ with $|V| \leqslant M$ we have $\{\alpha|V|\}(1 - \{\alpha|V|\}) \gg 1$. Then*

$$\|1_A\|_{A(G)} \gg \log M.$$

The alternative approach to the above is to try to make the idempotent theorem quantitative directly *viz.* if A has $\|1_A\|_{A(G)} \leqslant M$ then A can be made out of not too many cosets in G using not too many complements, intersections and unions. 'Too many' here is of course a function of M. Realizing this objective is the content of §4.4 where we prove the following theorem.

Theorem 4.12. *Suppose that G is a finite abelian group. Suppose that $A \subset G$ has $\|1_A\|_{A(G)} \leqslant M$. Then there is an integer $L \leqslant \exp(\exp(O(M^4)))$ such that*

$$1_A = \sum_{j=1}^{L} \sigma_j 1_{x_j + H_j}$$

where $\sigma_j \in \{-1, 1\}$, $x_j \in G$ and $H_j \leqslant G$ for each $j \in \{1, ..., L\}$.

This result actually implies (weaker) bounds for all the stated theorems as well as Littlewood's original problem; we shall discuss this in the concluding remarks in §4.4.6.

Finally it is worth remarking that fairly straightforward limiting arguments allow us to extend a number of these results to slightly wider classes of groups. In particular, Theorem 4.6 is extended to all compact vector spaces over $\mathbb{F}_2$ in [San07a], Theorem 4.10 is extended to all compact abelian groups in [San06], and Theorem 4.12 to all locally compact abelian groups in [GS08b]. In some sense this is attractive because it includes the motivating qualitative results, however the resulting analysis tends to obscure the underlying ideas so we do not include these arguments here.

4.1 Dyadic groups

Before beginning the proof of Theorem 4.6 it is instructive to mention the following special case which nevertheless captures the essence of the result. Suppose that G is a compact vector space over $\mathbb{F}_2$. Since finite subgroups of $\widehat{G}$ all have size a power of 2, if $A \subset G$ has density $\alpha = 1/3$ then

$$\{\alpha|V|\}(1 - \{\alpha|V|\}) \geqslant 1/9 \text{ for all finite } V \leqslant \widehat{G},$$

whence Proposition 4.4 specializes to the following.

Proposition 4.1.1. *Suppose that G is a compact vector space over $\mathbb{F}_2$ and $A \subset G$ has density $1/3$. Then $1_A \notin A(G)$.*

The next result is the corresponding consequence of Theorem 4.6.

Theorem 4.1.2. *Suppose that $G = \mathbb{F}_2^n$ and $A \subset G$ has density α with $|\alpha - 1/3| \leqslant \epsilon$. Then*

$$\|1_A\|_{A(G)} \gg \log\log \epsilon^{-1}.$$

The section now splits into five subsections. §4.1.1 provides some examples which complement our results and are worth bearing in mind when following the proof. §4.1.2 is the central iterative argument; in this section we prove a result with the conclusion of Theorem 4.6 but with a more cumbersome hypothesis on A. §4.1.3 then provides some physical space estimates to show that sets of density close to 1/3 (or, indeed, satisfying the more general hypothesis of Theorem 4.6) are included in the range of sets covered in the previous section. Finally, §4.1.4 combines the preceding work to prove a result which immediately implies Theorem 4.6. It then concludes with a discussion of the limitations of our methods.

For the remainder of this section $G = \mathbb{F}_2^n$.

4.1.1 Sets with small $A(G)$-norm

We address the question of how to construct subsets of G of a prescribed density whose characteristic function has small $A(G)$-norm.

Every coset in G has density 2^{-d} for some integer d; to produce a set with a density not of this form we take unions of cosets.

Suppose that we are given $\alpha \in [0,1]$, a terminating binary number. Write

$$\alpha = \sum_{i=1}^{k} 2^{-d_i},$$

where the d_i are strictly increasing. If we can find a sequence of disjoint cosets $A_1, ..., A_k$ such that $\mu_G(A_i) = 2^{-d_i}$, then their union $A := \bigcup_{i=1}^{k} A_i$ has

$$\|1_A\|_{A(G)} = \| \sum_{i=1}^{k} 1_{A_i} \|_{A(G)} \leqslant \sum_{i=1}^{k} \|1_{A_i}\|_{A(G)} = k \tag{4.1.1}$$

by the triangle inequality, and density

$$\mu_G(A) = \sum_{i=1}^{k} \mu_G(A_i) = \sum_{i=1}^{k} 2^{-d_i} = \alpha$$

since the elements of the union are disjoint. To produce such cosets we take $\{0_{\widehat{G}}\} = \Lambda_0 < \Lambda_1 < ... < \Lambda_k \leqslant \widehat{G}$, a nested sequence of subspaces with $\dim \Lambda_i = d_i$. Choose a sequence of vectors $\{\gamma_i : 1 \leqslant i \leqslant k\}$ such that $\gamma_i \in \Lambda_i \setminus \Lambda_{i-1}$ for $1 \leqslant i \leqslant k$. It is easy to see that this sequence must be linearly independent so we may take a sequence $\{x_i : 1 \leqslant i \leqslant k-1\}$ such that

$$\gamma_j(x_i) = \begin{cases} 1 & \text{if } j \neq i \\ -1 & \text{if } j = i \end{cases} \tag{4.1.2}$$

for all $1 \leqslant i \leqslant k-1$. Put

$$A_i = x_1 + ... + x_{i-1} + \Lambda_i^{\perp}.$$

First we note that $\mu_G(A_i) = 2^{-d_i}$ and second that the sets A_i are pairwise disjoint: Suppose $j > i$ and $x \in A_j$ then $x = x_1 + ... + x_{j-1} + x'$ where $x' \in \Lambda_j^\perp$ so that

$$\gamma_i(x) = \gamma_i(x_1)...\gamma_i(x_{j-1}).\gamma_i(x').$$

Now $j > i$, so $\Lambda_j > \Lambda_i$ from which it follows that $\gamma_i(x') = 1$. Consequently $\gamma_i(x) = \gamma_i(x_i) = -1$ by (4.1.2). However if $x \in A_i$ then by a similar calculation $\gamma_i(x) = 1$.

It follows that $A_1, ..., A_k$ are disjoint cosets of the appropriate size and hence their union, $A := \bigcup_{i=1}^k A_i$, has density α and $\|1_A\|_{A(G)} \leqslant k$.

We shall apply this construction to two different densities. The first is

$$\alpha = \frac{1}{4} + \frac{1}{16} + ... + \frac{1}{4^k};$$

the second will come in §4.1.4 to illustrate the limitations of our method.

The set A we produce has density α and the following two properties.

(i). A satisfies the hypotheses of Theorem 4.6 with $M = 4^k - 1$: If $V \leqslant \widehat{G}$ and $|V| \leqslant M$ then $|V| = 2^d$ for some $d < k$ and

$$\frac{2}{3} \geqslant \sum_{i=\lfloor d/2 \rfloor + 1}^{k} 2^d.4^{-i} = \{\alpha 2^d\} \geqslant \frac{2^d}{4^{\lfloor d/2 \rfloor + 1}} \geqslant \frac{1}{4},$$

and hence $\{\alpha|V|\}(1 - \{\alpha|V|\}) \geqslant 1/12$.

(ii). $\|1_A\|_{A(G)} \asymp k$: $\|1_A\|_{A(G)} \leqslant k$ follows by construction; $\|1_A\|_{A(G)} \gg k$ is slightly more involved:

$$\widehat{1_{A_i}}(\gamma) = \begin{cases} 4^{-i}\gamma(x_1)...\gamma(x_{i-1}) & \text{if } \gamma \in \Lambda_i \\ 0 & \text{otherwise.} \end{cases}$$

Hence we can bound $|\widehat{1_A}(\gamma)|$ from below using the linearity of the Fourier transform.

$$|\widehat{1_A}(\gamma)| \geqslant 4^{-i} - \sum_{j=i+1}^{k} 4^{-j} \geqslant \frac{2}{3}.4^{-i} \text{ if } \gamma \in \Lambda_i \setminus \Lambda_{i-1},$$

and so

$$\|1_A\|_{A(G)} \geqslant \sum_{i=1}^{k} \frac{2}{3}4^{-i}.|\Lambda_i \setminus \Lambda_{i-1}| \geqslant \sum_{i=1}^{k} \frac{2}{3}4^{-i}.\frac{3}{4}4^{i} = \frac{k}{2}.$$

Now, the conclusion of Theorem 4.6 implies that $\|1_A\|_{A(G)} \gg \log k$ which should be compared with the fact that actually $\|1_A\|_{A(G)} \asymp k$.

4.1.2 An iteration argument in Fourier space

Throughout this section $A \subset G$ has density α.

A trivial lower bound

Suppose that $\alpha > 0$. It is natural to try to bound $\|1_A\|_{A(G)}$ by a combination of Hölder's inequality and Plancherel's Theorem:

$$\|1_A\|_{A(G)}\|\widehat{1_A}\|_{\ell^\infty(\widehat{G})} \geqslant \|\widehat{1_A}\|^2_{\ell^2(\widehat{G})} = \|1_A\|^2_{L^2(\mu_G)}; \tag{4.1.3}$$

non-negativity of 1_A means that $\widehat{1_A}(0_{\widehat{G}}) = \|1_A\|_{L^1(\mu_G)}$ so

$$\|1_A\|_{L^1(\mu_G)} \geqslant \|\widehat{1_A}\|_{L^\infty(\mu_G)} \geqslant \widehat{1_A}(0_{\widehat{G}}) = \|1_A\|_{L^1(\mu_G)}$$

which implies that

$$\|\widehat{1_A}\|_{L^\infty(\mu_G)} = \|1_A\|_{L^1(\mu_G)}. \tag{4.1.4}$$

$1_A \equiv 1_A^2$ so $\|1_A\|^2_{L^2(\mu_G)} = \|1_A\|_{L^1(\mu_G)} = \alpha$, which is positive, and hence (4.1.3) tells us that

$$\|1_A\|_{A(G)} \geqslant 1. \tag{4.1.5}$$

Taking $A = G$ shows that in general we can do no better.

A weak iteration lemma

A weakness in the above deduction is that we have no good upper bound for $\|\widehat{1_A}\|_{\ell^\infty(\widehat{G})}$. In fact, as we saw, $\|\widehat{1_A}\|_{\ell^\infty(\widehat{G})}$ is necessarily large because $\widehat{1_A}$ is large at the trivial character. However, we know nothing about how large $\widehat{1_A}$ is at any other character, a fact which we shall now exploit.

Write f for the balanced function of 1_A i.e. $f = 1_A - \alpha$. Then

$$\widehat{f}(\gamma) = \begin{cases} 0 & \text{if } \gamma = 0_{\widehat{G}} \\ \widehat{1_A}(\gamma) & \text{otherwise.} \end{cases}$$

Applying Hölder's inequality and Plancherel's Theorem in the same way as before we have

$$\|1_A\|_{A(G)}\|\widehat{f}\|_{\ell^\infty(\widehat{G})} \geqslant \langle \widehat{1_A}, \widehat{f}\rangle = \langle 1_A, f\rangle = \alpha - \alpha^2. \qquad (4.1.6)$$

Now, fix $\epsilon > 0$ to be optimized later. If α is bounded away from 0 and 1 by an absolute constant then either $\|1_A\|_{A(G)} \gg \epsilon^{-1}$ or $\|\widehat{f}\|_{\ell^\infty(\widehat{G})} \gg \epsilon$. In the former case we are done (since $\|1_A\|_{A(G)}$ is large) and in the latter we have a non-trivial character at which $\widehat{1_A}$ is large; we should like to start building up a collection of such characters.

Suppose that $\Gamma \subset \widehat{G}$ is a collection of characters on which we know $\widehat{1_A}$ has large ℓ^1-mass. We want to produce a superset Γ' of Γ by adding some more characters which support a significant ℓ^1-mass of $\widehat{1_A}$. To find characters outside Γ on which $\widehat{1_A}$ has large ℓ^1-mass we might replace f with a function f_Γ (by analogy with the earlier replacement of 1_A by f) defined by inversion:

$$\widehat{f_\Gamma}(\gamma) = \begin{cases} 0 & \text{if } \gamma \in \Gamma \\ \widehat{1_A}(\gamma) & \text{otherwise.} \end{cases} \qquad (4.1.7)$$

The problem with this is that for general Γ we can say very little about f_Γ. If $V \leqslant \widehat{G}$, however, then f_V has a particularly simple form:

$$f_V = \sum_{\gamma \in \widehat{G}} \widehat{1_A}(\gamma)(1 - \widehat{\mu_{V^\perp}}(\gamma))\gamma = 1_A * (\delta - \mu_{V^\perp}) = 1_A - 1_A * \mu_{V^\perp}.$$

Now suppose that $\Gamma = V \leqslant \widehat{G}$. We want to try to add characters to V to get a superspace $V' \leqslant \widehat{G}$ with $\sum_{\gamma \in V'} |\widehat{1_A}(\gamma)|$ 'significantly larger' than

$\sum_{\gamma\in V}|\widehat{1_A}(\gamma)|$. We can use the idea in (4.1.6) to do this; replace f by f_V in that argument:

$$\|1_A\|_{A(G)}\|\widehat{f_V}\|_{\ell^\infty(\widehat{G})} \geqslant \langle\widehat{1_A},\widehat{f_V}\rangle = \langle 1_A, f_V\rangle. \tag{4.1.8}$$

Before, an easy calculation gave us $\langle 1_A, f\rangle = \alpha(1-\alpha)$. To compute $\langle 1_A, f_V\rangle$ we have a slightly more involved calculation.

Lemma 4.1.3.

$$\|f_V\|_{L^1(\mu_G)} = 2\langle 1_A, f_V\rangle. \tag{4.1.9}$$

Proof. $\mu_{V^\perp}$ is a probability measure so $0 \leqslant 1_A * \mu_{V^\perp}(x) \leqslant 1$. Hence, $f_V(x) \leqslant 0$ for all $x \notin A$ and $f_V(x) \geqslant 0$ for all $x \in A$; consequently

$$\|f_V\|_{L^1(\mu_G)} = \int 1_A f_V d\mu_G + \int (1-1_A)(-f_V)d\mu_G = 2\langle 1_A, f_V\rangle - \int f_V d\mu_G.$$

But $\int f_V d\mu_G = 0$ since $\int 1_A d\mu_G = \int 1_A * \mu_{V^\perp} d\mu_G$, so we are done. □

It follows that

$$\|1_A\|_{A(G)}\|\widehat{f_V}\|_{\ell^\infty(\widehat{G})} \geqslant \frac{\|f_V\|_{L^1(\mu_G)}}{2}. \tag{4.1.10}$$

So either $\|1_A\|_{A(G)} \geqslant \epsilon^{-1}$ or there is a character γ such that $|\widehat{f_V}(\gamma)| \geqslant \epsilon\|f_V\|_{L^1(\mu_G)}/2$. By construction of f_V we have $\widehat{f_V}(\gamma') = 0$ if $\gamma' \in V$ so that $\gamma \notin V$ – γ is a genuinely new character. Letting V' be the space generated by γ and V, we have our first iteration lemma:

Lemma 4.1.4 (Weak iteration lemma)**.** *Suppose that $V \leqslant \widehat{G}$ and $A \subset G$. Suppose that $\epsilon \in (0,1]$. Then either $\|1_A\|_{A(G)} \geqslant \epsilon^{-1}$ or there is a superspace V' of V with* $\dim V' = \dim V + 1$ *for which*

$$\sum_{\gamma\in V'}|\widehat{1_A}(\gamma)| \geqslant \frac{\epsilon\|f_V\|_{L^1(\mu_G)}}{2} + \sum_{\gamma\in V}|\widehat{1_A}(\gamma)|.$$

Iterating this lemma leads to the following proposition.

Proposition 4.1.5. *Suppose that $A \subset G$ is such that for all $V \leqslant \widehat{G}$ with $|V| \leqslant M$ we have $\|f_V\|_{L^1(\mu_G)} \gg 1$, where $f_V = 1_A - 1_A * \mu_{V^\perp}$. Then*

$$\|1_A\|_{A(G)} \gg \sqrt{\log M}.$$

We omit the proof (it is not difficult and all the ideas are contained in the proof of Proposition 4.1.7) since the hypotheses the proposition assumes on A are prohibitively strong; nevertheless we can make use of these ideas.

A stronger iteration lemma

The main weakness of the above approach is that each time we apply the weak iteration lemma to find characters supporting more ℓ^1-mass of $\widehat{1_A}$ (assuming we are not in the case when $\|1_A\|_{A(G)}$ is automatically large) we do not find very much ℓ^1-mass, in fact we find mass in proportion to $\|f_V\|_{L^1(\mu_G)}$ which consequently has to be assumed large. We can improve this by adding to V not just one character at which $\widehat{f_V}$ is large but all such characters. This idea would not work but for two essential facts.

(i). There are a lot of characters at which $\widehat{f_V}$ is large, in the sense that the characters at which $\widehat{f_V}$ is large actually support a large amount of the sum $\langle \widehat{1_A}, \widehat{f_V} \rangle$.

(ii). Chang's Theorem ensures that the characters at which $\widehat{f_V}$ is large are contained in a subspace of relatively small dimension.

We are in a position to show:

Lemma 4.1.6. *Suppose that $V \leqslant \widehat{G}$, $A \subset G$ and $\|f_V\|_{L^1(\mu_G)} > 0$, where $f_V = 1_A - 1_A * \mu_{V^\perp}$. Then there is a non-negative integer s and a superspace V' of V such that*

$$\sum_{\gamma \in V'} |\widehat{1_A}(\gamma)| - \sum_{\gamma \in V} |\widehat{1_A}(\gamma)| \gg \left(\frac{4}{3}\right)^s$$

and

$$\dim V' - \dim V \ll 4^s(1 + \log \|f_V\|_{L^1(\mu_G)}^{-1}).$$

Proof. By Plancherel's Theorem and Lemma 4.1.3 we have

$$\sum_{\gamma\in\widehat{G}} \widehat{1_A}(\gamma)\overline{\widehat{f_V}(\gamma)} = \langle 1_A, f_V\rangle = \frac{1}{2}\|f_V\|_{L^1(\mu_G)}.$$

To make use of this we apply the triangle inequality to the left hand side and get the driving inequality of the lemma

$$\frac{1}{2}\|f_V\|_{L^1(\mu_G)} \leqslant \sum_{\gamma\in\widehat{G}} |\widehat{1_A}(\gamma)||\widehat{f_V}(\gamma)|. \tag{4.1.11}$$

Write $\mathcal{L}$ for the set of characters at which $\widehat{f_V}$ is non-zero. Partition $\mathcal{L}$ by a dyadic decomposition of the range of values of $|\widehat{f_V}|$. Specifically, for each non-negative integer s, let

$$\Gamma_s := \{\gamma \in \widehat{G} : 2^{-s}\|f_V\|_{L^1(\mu_G)} \geqslant |\widehat{f_V}(\gamma)| > 2^{-(s+1)}\|f_V\|_{L^1(\mu_G)}\}.$$

For all characters γ we have $|\widehat{f_V}(\gamma)| \leqslant \|f_V\|_{L^1(\mu_G)}$ and if $\gamma \in \mathcal{L}$ then $|\widehat{f_V}(\gamma)| > 0$ so certainly the Γ_ss cover $\mathcal{L}$; they are clearly disjoint and hence form a partition of $\mathcal{L}$. Write L_s for the ℓ^1-norm of $\widehat{1_A}$ supported on Γ_s:

$$L_s := \sum_{\gamma\in\Gamma_s} |\widehat{1_A}(\gamma)|.$$

The right hand side of (4.1.11) can now be rewritten using these definitions:

$$\begin{aligned}
\sum_{\gamma\in\widehat{G}} |\widehat{1_A}(\gamma)||\widehat{f_V}(\gamma)| &= \sum_{\gamma\in\mathcal{L}} |\widehat{1_A}(\gamma)||\widehat{f_V}(\gamma)| \text{ by the definition of } \mathcal{L} \\
&= \sum_{s=0}^{\infty}\sum_{\gamma\in\Gamma_s} |\widehat{1_A}(\gamma)||\widehat{f_V}(\gamma)| \\
&\quad \text{since } \{\Gamma_s\}_{s\geqslant 0} \text{ is a partition of } \mathcal{L}, \\
&\leqslant \sum_{s=0}^{\infty}\sum_{\gamma\in\Gamma_s} |\widehat{1_A}(\gamma)|.2^{-s}\|f_V\|_{L^1(\mu_G)} \\
&\quad \text{by the definition of } \Gamma_s, \\
&= \sum_{s=0}^{\infty} L_s 2^{-s}\|f_V\|_{L^1(\mu_G)} \text{ by the definition of } L_s.
\end{aligned}$$

Combining this with (4.1.11) and dividing by $\|f_V\|_{L^1(\mu_G)}$ (which is possible since $\|f_V\|_{L^1(\mu_G)} > 0$) we get

$$\frac{1}{2} \leqslant \sum_{s=0}^{\infty} 2^{-s} L_s. \tag{4.1.12}$$

Now, if for every non-negative integer s we have

$$L_s < \frac{1}{6}\left(\frac{4}{3}\right)^s,$$

then

$$\sum_{s=0}^{\infty} 2^{-s} L_s < \sum_{s=0}^{\infty} 2^{-s}\frac{1}{6}\left(\frac{4}{3}\right)^s = \frac{1}{6}\sum_{s=0}^{\infty}\left(\frac{2}{3}\right)^s = \frac{1}{2},$$

which contradicts (4.1.12). Hence there is a non-negative integer s such that

$$L_s \geqslant \frac{1}{6}\left(\frac{4}{3}\right)^s.$$

Chang's Theorem gives a space W for which

$$\Gamma_s \subset \{\gamma \in \widehat{G} : |\widehat{f_V}(\gamma)| \geqslant 2^{-(s+1)}\|f_V\|_{L^1(\mu_G)}\} \subset W$$

and

$$\dim W \ll 2^{2s}(1+\log(\|f_V\|_{L^2(\mu_G)}\|f_V\|_{L^1(\mu_G)}^{-1})).$$

To tidy this up we note that $f_V = 1_A - 1_A * \mu_{V^\perp}$ and $1_A(x), 1_A * \mu_{V^\perp}(x) \in [0,1]$, so $f_V(x) \in [-1,1]$ for $x \in G$ and hence $\|f_V\|_{L^2(\mu_G)} \leqslant 1$, from which it follows that

$$\dim W \ll 4^s(1+\log \|f_V\|_{L^1(\mu_G)}^{-1}).$$

Let V' be the space generated by V and W. Then

$$\dim V' - \dim V \ll 4^s(1+\log \|f_V\|_{L^1(\mu_G)}^{-1}).$$

Finally we note that $\Gamma_s \cap V = \emptyset$ since $\widehat{f_V}(\gamma) = 0$ if $\gamma \in V$ (recall $\widehat{f_V}$ from (4.1.7)) and $|\widehat{f_V}(\gamma)| > 2^{s+1}\|f_V\|_1 \geqslant 0$ if $\gamma \in \Gamma_s$. Hence

$$\sum_{\gamma \in V'} |\widehat{1_A}(\gamma)| \geqslant \sum_{\gamma \in \Gamma_s} |\widehat{1_A}(\gamma)| + \sum_{\gamma \in V} |\widehat{1_A}(\gamma)| \geqslant \frac{1}{6}\left(\frac{4}{3}\right)^s + \sum_{\gamma \in V} |\widehat{1_A}(\gamma)|.$$

This gives the result. □

By iterating this lemma we prove the following result.

Proposition 4.1.7. *Suppose that $A \subset G$ is such that for all $V \leqslant \widehat{G}$ with $|V| \leqslant M$ we have $\log \|f_V\|_1^{-1} \ll \log |V|$. Then*

$$\|1_A\|_{A(G)} \gg \log\log M.$$

Proof. Fix $\epsilon \in (0,1]$ to be optimized later. We construct a sequence $V_0 \leqslant V_1 \leqslant ... \leqslant \widehat{G}$ iteratively, writing $d_i := \dim V_i$ and

$$L_i = \sum_{\gamma \in V_i} |\widehat{1_A}(\gamma)|.$$

We start the construction by letting $V_0 := \{0_{\widehat{G}}\}$. Suppose that we are given V_k. If $|V_k| \leqslant M$ then apply the iteration lemma to V_k and A to get an integer

s_{k+1} and vector space V_{k+1} with

$$d_{k+1} - d_k \ll 4^{s_{k+1}}(1 + \log \|f_{V_k}\|_1^{-1}) \text{ and } L_{k+1} - L_k \gg \left(\frac{4}{3}\right)^{s_{k+1}}. \quad (4.1.13)$$

First we note that the iteration terminates since certainly $L_k \gg k$, but also $L_k \leqslant \|1_A\|_{A(G)} < \infty$.

Since $\log \|f_{V_k}\|_1^{-1} \ll \log |V_k| \ll d_k$ it follows from (4.1.13) that

$$d_{k+1} \ll 4^{s_{k+1}} d_k, \quad (4.1.14)$$

from which, in turn, we get

$$L_k \gg \sum_{l=0}^{k} \left(\frac{4}{3}\right)^{s_l} \gg \sum_{l=0}^{k} s_l \gg \log d_k. \quad (4.1.15)$$

Let K be the stage of the iteration at which it terminates i.e. $|V_K| > M$. We have two possibilities.

(i). $d_{K-1} \equiv \log_2 |V_{K-1}| \leqslant \sqrt{\log M}$: in which case $d_K \geqslant \sqrt{\log M}.d_{K-1}$. (4.1.14) then tells us that $4^{s_K} \gg \sqrt{\log M}$. However the first inequality in (4.1.15) tells us that $\|1_A\|_{A(G)} \geqslant L_K \gg (4/3)^{S_K}$ and so certainly $\|1_A\|_{A(G)} \gg \log\log M$.

(ii). Alternatively $d_{K-1} \equiv \log_2 |V_{K-1}| \geqslant \sqrt{\log M}$: in which case by (4.1.15) we have $L_{K-1} \gg \log d_{K-1} \gg \log\log M$ and so certainly $\|1_A\|_{A(G)} \gg \log\log M$.

In either case the proof is complete. □

4.1.3 Physical space estimates

To realize the hypothesis of Proposition 4.1.7 regarding f_V as a density condition we have the following lemma:

Lemma 4.1.8. *Suppose that $V \leqslant \widehat{G}$ and $A \subset G$ has density α. Then*

$$\|f_V\|_{L^1(\mu_G)} = \|1_A - 1_A * \mu_{V^\perp}\|_{L^1(\mu_G)} \geqslant 2|V|^{-1}\{\alpha|V|\}(1 - \{\alpha|V|\}).$$

We need the following technical lemma:

Lemma 4.1.9. *Let* $\delta_1, ..., \delta_m \in [0,1]$ *and put* $\gamma = \{\sum_{i=1}^m \delta_i\}$. *Then*

$$\sum_{i=1}^{m} (\delta_i - \delta_i^2) \geqslant \gamma(1-\gamma). \tag{4.1.16}$$

Proof. We may assume that $0 < \gamma < 1$. Suppose that we have $i \neq j$ such that $0 < \delta_i, \delta_j < 1$. Put $\delta = \delta_i + \delta_j \leqslant 2$ and we have two cases:

(i). $\delta \leqslant 1$: In this case we may replace δ_i and δ_j by δ and 0. This preserves γ and since

$$\delta_i - \delta_i^2 + \delta_j - \delta_j^2 \geqslant (\delta_i + \delta_j) - (\delta_i + \delta_j)^2 + 0 - 0^2,$$

it does not increase the sum in (4.1.16).

(ii). $2 \geqslant \delta > 1$: In this case we may replace δ_i and δ_j by 1 and $\delta - 1$. This preserves γ and since

$$\begin{aligned}
& (\delta_i - 1)(\delta_j - 1) && \geqslant 0 \\
\Rightarrow \quad & 0 && \geqslant -2\delta_i\delta_j + 2(\delta_i + \delta_j) - 2 \\
\Rightarrow \quad & \delta_i - \delta_i^2 + \delta_j - \delta_j^2 && \geqslant \delta_i - \delta_i^2 + \delta_j - \delta_j^2 - 2\delta_i\delta_j + 2(\delta_i + \delta_j) - 2 \\
\Rightarrow \quad & \delta_i - \delta_i^2 + \delta_j - \delta_j^2 && \geqslant (\delta_i + \delta_j - 1) - (\delta_i + \delta_j - 1)^2 + 1 - 1^2,
\end{aligned}$$

it does not increase the sum in (4.1.16).

In both cases we can reduce the number of is for which $0 < \delta_i < 1$ without increasing the sum in (4.1.16), so we may assume that there is only one j such that $0 < \delta_j < 1$. Then

$$\delta_j + \sum_{i \neq j} \delta_i = \gamma + \lfloor \sum_{i=1}^{m} \delta_i \rfloor \Rightarrow \delta_j - \gamma = \lfloor \sum_{i=1}^{m} \delta_i \rfloor - \sum_{i \neq j} \delta_i,$$

but the right hand side is an integer and $-1 < \delta_j - \gamma < 1$ so $\delta_j = \gamma$ and (4.1.16) follows. $\square$

Proof of Lemma 4.1.8. Lemma 4.1.3 states that $\|f_V\|_{L^1(\mu_G)} = 2\langle 1_A, f_V\rangle$ so

$$\begin{aligned}\|f_V\|_{L^1(\mu_G)} &= 2\int 1_A(1_A - 1_A * \mu_{V^\perp})d\mu_G \\ &= 2\int_{x\in G}\int 1_A(1_A - 1_A * \mu_{V^\perp})d\mu_{x+V^\perp}d\mu_G(x),\end{aligned}$$

(this is just conditional expectation). $1_A * \mu_{V^\perp}$ is constant on cosets of $V^\perp$ and $1_A^2 \equiv 1_A$ so that

$$\begin{aligned}\|f_V\|_1 &= 2\int_{x\in G}\int 1_A d\mu_{x+V^\perp}(1 - 1_A * \mu_{V^\perp}(x))d\mu_G(x) \\ &= 2\int_{x\in G} 1_A * \mu_{V^\perp}(x)(1 - 1_A * \mu_{V^\perp}(x))d\mu_G(x).\end{aligned}$$

There are $|V|$ cosets of $V^\perp$ in G, and $1_A * \mu_{V^\perp}$ is constant on cosets of $V^\perp$ so this integral is really a finite sum with $|V|$ terms in it. Let $\mathcal{C}$ be a set of coset representatives for $V^\perp$ in G then $|\mathcal{C}| = |V|$ and

$$\|f_V\|_1 = \frac{2}{|\mathcal{C}|}\sum_{x'\in\mathcal{C}} 1_A * \mu_{V^\perp}(x')(1 - 1_A * \mu_{V^\perp}(x')).$$

We can now apply Lemma 4.1.9 to the quantities $1_A * \mu_{V^\perp}(x')$ with $m = |\mathcal{C}|$. This gives

$$\|f_V\|_{L^1(\mu_G)} \geqslant \frac{2}{|\mathcal{C}|}\beta(1-\beta) = \frac{2}{|V|}\beta(1-\beta)$$

where

$$\beta = \left\{\sum_{x'\in\mathcal{C}} 1_A * \mu_{V^\perp}(x')\right\} = \left\{|\mathcal{C}|\int_{x\in G} 1_A * \mu_{V^\perp}(x)d\mu_G(x)\right\} = \{|V|\alpha\}.$$

□

Nothing better than Lemma 4.1.8 can be true: Let A be the union of $\lfloor\alpha|V|\rfloor$ cosets of $V^\perp$ and a subset of a coset of $V^\perp$ of relative density $\{\alpha|V|\}$. Equality is attained in Lemma 4.1.8 for this set.

4.1.4 The result, remarks and examples

As an easy corollary of Proposition 4.1.7 and Lemma 4.1.8 we have:

Theorem 4.1.10. *Suppose that* $G = \mathbb{F}_2^n$. *Suppose that* $A \subset G$ *has density* α *and for all* $V \leqslant \widehat{G}$ *with* $|V| \leqslant M$ *we have* $\{\alpha|V|\}(1 - \{\alpha|V|\}) \gg |V|^{-1}$. *Then*

$$\|1_A\|_{A(G)} \gg \log\log M.$$

Theorem 4.6 is simply a weaker version of this result.

There are strong similarities between this work and the work of Bourgain in [Bou02]. In particular a slight variation on the calculation in Lemma 4.1.3 is in his work and he proves a result using Beckner's Inequality (which is essentially equivalent to Chang's Theorem) which shows that if $A \subset \mathbb{F}_2^n$ has density α with $\alpha(1-\alpha) \gg 1$ then either $\widehat{1_A}$ is large at a non-trivial character or there is significant ℓ^2-mass in the tail of the Fourier transform.

Theorem 4.1.10 is sharp up to the constant and hence demonstrates a limitation of our method as regards improving Theorem 4.6. Let

$$\alpha = \frac{1}{2^{2^0}} + \frac{1}{2^{2^1}} + ... + \frac{1}{2^{2^{k-1}}}.$$

We showed in §4.1.1 that there is a set A of density α with $\|1_A\|_{A(G)} \leqslant k$. However A also satisfies the hypotheses of Theorem 4.1.10 with $M = 2^{2^{k-1}} - 1$: If $V \leqslant \widehat{G}$ has $|V| \leqslant M$ then $|V| = 2^d$ for some $d < 2^{k-1}$,

$$\begin{aligned}\{\alpha|V|\} = \sum_{\min\{0,\log_2 d\} < m \leqslant k-1} 2^d.2^{-2^m} &\leqslant \sum_{\min\{0,\log_2 d\} < m \leqslant k-1} 2^{-2^{m-1}} \\ &\leqslant \sum_{m=0}^{\infty} 2^{-2^m} \leqslant \frac{7}{8},\end{aligned}$$

and

$$\{\alpha|V|\} = \sum_{\min\{0,\log_2 d\} < m \leqslant k-1} 2^d.2^{-2^m} \geqslant 2^d.2^{-2^{\lfloor \log_2 d \rfloor + 1}} \geqslant 2^{-d} = |V|^{-1}.$$

Hence

$$\{\alpha|V|\}(1 - \{\alpha|V|\}) \gg |V|^{-1}.$$

Theorem 4.1.10 applied to A tells us that $\|1_A\|_{A(G)} \gg k$.

4.2 Arithmetic groups

In this section we consider groups at the arithmetic, rather than algebraic, end of the spectrum, namely $G = \mathbb{Z}/p\mathbb{Z}$ for p a prime. Again there is an attractive qualitative analogue that can be concluded from Cohen's theorem. We shall discuss a direct proof shortly.

Proposition 4.2.1. *Suppose that $A \subset \mathbb{T}$ has density α with $0 < \alpha < 1$. Then $1_A \notin A(\mathbb{T})$.*

A quantitative version of this was first proved by Green and Konyagin in [GK09]. They proved the following result.

Theorem 4.2.2. *Suppose that p is a prime number and $A \subset \mathbb{Z}/p\mathbb{Z}$ has density bounded away from 0 and 1 by an absolute constant. Then*

$$\|1_A\|_{A(\mathbb{Z}/p\mathbb{Z})} \gg \left(\frac{\log p}{\log\log p}\right)^{1/3}.$$

By analogy with the original problem of Littlewood they observe that more is probably true, indeed one might make the following conjecture.

Conjecture 4.2.3 (Green-Konyagin-Littlewood conjecture)**.** *Suppose that p is a prime number and $A \subset \mathbb{Z}/p\mathbb{Z}$ has density bounded away from 0 and 1 by an absolute constant. Then*

$$\|1_A\|_{A(\mathbb{Z}/p\mathbb{Z})} \gg \log p.$$

Certainly no more than this is true as any arithmetic progression of density bounded away from 0 and 1 shows. Consider, for example a symmetric interval I. It is well known that its Fourier transform is just the Dirichlet kernel:

$$\widehat{1_I}(r) = \frac{\sin(\pi r|I|/p)}{p\sin(\pi r/p)}.$$

Thus, since $|\sin x| \leqslant |x|$, we have

$$\|1_I\|_{A(G)} \geqslant \sum_{r=1}^{p-1} \frac{|\sin(\pi r|I|/p)|}{\pi r}.$$

Now suppose, for example, that $|I|/p \approx 1/2$. Then $|\sin(\pi r|I|/p)| \gg 1$ whenever r is odd so that

$$\|1_I\|_{A(G)} \gg \sum_{r'=1}^{(p-1)/2} \frac{1}{r'} \gg \log p.$$

A similar argument works for any $|I|$ with $1 \ll (|I|/p)(1 - (|I|/p))$.

In this section we improve Theorem 4.2.2, increasing the exponent of $\log p$ from $1/3 - \varepsilon$ to $1/2 - \varepsilon$. Specifically we show the following.

Theorem 4.2.4. *Suppose that p is a prime number and $A \subset \mathbb{Z}/p\mathbb{Z}$ has density bounded away from 0 and 1 by an absolute constant. Then*

$$\|1_A\|_{A(\mathbb{Z}/p\mathbb{Z})} \gg \left(\frac{\log p}{(\log\log p)^3}\right)^{1/2}.$$

It is easy to see that this is equivalent to Theorem 4.8.

4.2.1 A qualitative argument

It is instructive to begin considering the problem by looking at a proof of Proposition 4.2.1. The proof proceeds in three stages, the first two of which are naturally set in an arbitrary compact abelian group G.

(i). *(Fourier inversion)* First, if $f \in A(G)$ then we may define the function

$$\widetilde{f}(x) := \sum_{\gamma \in \widehat{G}} \widehat{f}(\gamma)\gamma(x),$$

which is continuous since it is the uniform limit of continuous functions. The Fourier inversion theorem tells us that $\|\widetilde{f} - f\|_{L^\infty(\mu_G)} = 0$.

(ii). *(Averaging)* Secondly, by averaging there are elements $x_0, x_1 \in G$ such that

$$\widetilde{f}(x_0) \leqslant \int f d\mu_G \leqslant \widetilde{f}(x_1),$$

since $\int f d\mu_G = \int \widetilde{f} d\mu_G$.

(iii). *(Intermediate value theorem)* Finally we suppose (for a contradiction) that $1_A \in A(\mathbb{T})$ so that by the intermediate value theorem there is some $x \in \mathbb{T}$ such that $\widetilde{1_A}(x) = \alpha$. Continuity ensures that there is an open ball $x + B$ on which $\widetilde{1_A}$ is very close to α, and in particular, since $\alpha \in (0, 1)$, on which $\widetilde{1_A}$ only takes values in $(0, 1)$. Since $\|1_A - \widetilde{1_A}\|_{L^\infty(G)} = 0$ and $\mu(x + B) > 0$ it follows that 1_A equals $\widetilde{1_A}$ for some point in $x + B$, but this contradicts the fact that 1_A can only take the values 0 or 1.

If we try to transfer this argument to $G = \mathbb{Z}/p\mathbb{Z}$ it breaks down at the third stage when we apply the intermediate value theorem. It is easy enough to remedy this and prove a sensible discrete analogue of the intermediate value theorem; the following, for example, is in [GK09]. It is also a corollary of the more general Lemma 4.3.3 which is proved later.

Proposition 4.2.5 (Discrete intermediate value theorem)**.** *Suppose that p is prime number. Suppose that $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{R}$ and that there is some non-zero $y \in \mathbb{Z}/p\mathbb{Z}$ such that*

$$|f(x + y) - f(x)| \leqslant \epsilon \|f\|_{L^\infty(\mu_G)} \text{ for all } x \in \mathbb{Z}/p\mathbb{Z}.$$

Then there is some $x \in \mathbb{Z}/p\mathbb{Z}$ such that

$$|f(x) - \int f d\mu_{\mathbb{Z}/p\mathbb{Z}}| \leqslant 2^{-1}\epsilon \|f\|_{L^\infty(\mu_G)}.$$

Of course this has only moved the difficulty: to use this result we need to replace the continuity in the first stage of our argument with the sort of *quantitative continuity* used in this proposition.

It turns out that we already have a ready supply of functions which are continuous in this new sense: Suppose that $f \in L^\infty(\mu_G)$ and $B(\Gamma,\delta)$ is a regular Bohr set. Then, by Lemma 2.2.5, we may pick $\delta' \gg \epsilon\delta/d$ such that

$$\|f * \beta_{\Gamma,\delta} - f * \beta_{\Gamma,\delta}(x)\|_{L^\infty(x+\beta_{\Gamma,\delta})} \leqslant \epsilon\|f\|_{L^\infty(\mu_G)}.$$

Now if $\mu_G(B(\Gamma,\delta')) > p^{-1}$ then $B(\Gamma,\delta')$ has a non-identity element and hence the discrete intermediate value theorem applies.

Essentially the same argument which shows that if $f \in A(G)$ then $\|f - \widetilde{f}\|_{L^\infty(\mu_G)} = 0$ for some continuous function $\widetilde{f}$, can be made quantitative to show that there is a regular Bohr set $B(\Gamma,\delta)$ such that $\|f - f*\beta_{\Gamma,\delta}\|_{L^\infty(\mu_G)}$ is small and, by our previous observations, $f*\beta_{\Gamma,\delta}$ is quantitatively continuous.

To be concrete suppose that G is a compact abelian group, $f \in A(G)$ and write $A_f := \|f\|_{A(G)}\|f\|^{-1}_{L^\infty(\mu_G)}$. Then there is a finite set of characters Γ such that

$$\sum_{\gamma\notin\Gamma} |\widehat{f}(\gamma)| \leqslant \epsilon A_f^{-1}\|f\|_{A(G)}.$$

Pick $\delta \gg \epsilon A_f^{-1}$ such that

$$B(\Gamma,\delta) \subset \{x \in G : |1-\gamma(x)| \leqslant \epsilon A_f^{-1} \text{ for all } \gamma \in \Gamma\},$$

and such that δ is regular for Γ by Proposition 2.2.2. It is easy to see that

$$|1-\widehat{\beta_{\Gamma,\delta}}(\gamma)| \leqslant \epsilon A_f^{-1} \text{ if } \gamma \in \Gamma,$$

and it follows that

$$\begin{aligned}
\|f - f*\beta_{\Gamma,\delta}\|_{L^\infty(\mu_G)} &\leqslant \sum_{\gamma\in\widehat{G}} |1-\widehat{\beta_{\Gamma,\delta}}(\gamma)||\widehat{f}(\gamma)| \\
&\leqslant \sum_{\gamma\in\Gamma} |1-\widehat{\beta_{\Gamma,\delta}}(\gamma)||\widehat{f}(\gamma)| + \sum_{\gamma\notin\Gamma} |1-\widehat{\beta_{\Gamma,\delta}}(\gamma)||\widehat{f}(\gamma)| \\
&\leqslant \epsilon A_f^{-1}\sum_{\gamma\in\widehat{G}} |\widehat{f}(\gamma)| + 2\sum_{\gamma\notin\Gamma} |\widehat{f}(\gamma)| \\
&\leqslant 3\epsilon A_f^{-1}\|f\|_{A(G)} \leqslant 3\epsilon\|f\|_{L^\infty(\mu_G)}.
\end{aligned}$$

In slightly formal language this has proved the following qualitative result.

Theorem 4.2.6. *Suppose that G is a compact abelian group, $f \in A(G)$ and $\epsilon \in (0,1]$. Write $A_f := \|f\|_{A(G)}\|f\|_{L^\infty(\mu_G)}^{-1}$. Then there is a Bohr set $B(\Gamma,\delta)$ with*

$$d < \infty \text{ and } \delta^{-1} \ll \epsilon^{-1}A_f,$$

and a narrower Bohr set $B(\Gamma,\delta')$ with $\delta' \gg \epsilon\delta/d$ such that

$$\sup_{x\in G} \|f * \beta_{\Gamma,\delta} - f * \beta_{\Gamma,\delta}(x)\|_{L^\infty(x+\beta_{\Gamma,\delta'})} \leqslant \epsilon\|f\|_{L^\infty(\mu_G)}$$

and

$$\sup_{x\in G} \|f - f * \beta_{\Gamma,\delta}\|_{L^\infty(x+\beta_{\Gamma,\delta'})} \leqslant \epsilon\|f\|_{L^\infty(\mu_G)}.$$

Of course, as we observed before, this is only useful to us if $B(\Gamma,\delta')$ contains a non-zero element. We can use Lemma 2.2.1 to estimate its size: If $G = \mathbb{Z}/p\mathbb{Z}$, then $B(\Gamma,\delta')$ contains a non-zero element if

$$(c\epsilon^2A_f^{-1}/d)^d > p^{-1} \text{ for some absolute } c > 0.$$

Unfortunately, because we have no control over d, we have no way of ensuring this inequality. The content of this section can be seen as an effort to make this method work by getting control of d; the main result is the following quantitative version of Theorem 4.2.6.

Theorem 4.2.7. *Suppose that G is a finite abelian group, $f \in A(G)$ and $\epsilon \in (0,1]$. Write $A_f := \|f\|_{A(G)}\|f\|_{L^\infty(\mu_G)}^{-1}$. Then there is a Bohr set $B(\Gamma,\delta)$ with*

$$d \ll \epsilon^{-2}A_f \log A_f \log \epsilon^{-1}A_f \text{ and } \log\delta^{-1} \ll \epsilon^{-2}A_f(\log\epsilon^{-1}A_f)^2,$$

and a narrower Bohr set $B(\Gamma,\delta')$ with $\delta' \gg \epsilon\delta/d$ such that

$$\sup_{x\in G} \|f * \beta_{\Gamma,\delta} - f * \beta_{\Gamma,\delta}(x)\|_{L^\infty(x+\beta_{\Gamma,\delta'})} \leqslant \epsilon\|f\|_{L^\infty(\mu_G)}$$

and

$$\sup_{x\in G}\|f - f * \beta_{\Gamma,\delta}\|_{L^2(x+\beta_{\Gamma,\delta'})} \leqslant \epsilon\|f\|_{L^\infty(\mu_G)}.$$

Note that to gain control of d we have had to sacrifice some control of δ and of the error in approximating f by $f * \beta_{\Gamma,\delta}$.

There are now three remaining subsections to the section.

- §4.2.2 details our arguments in the model setting of $G = \mathbb{F}_2^n$.
- §4.2.3 proves Theorem 4.2.7 following the outline of §4.2.2.
- Finally §4.2.4 completes the proof of Theorem 4.2.4 and concludes with some remarks and a conjecture.

4.2.2 The argument in a model setting

We shall prove the following model version of Theorem 4.2.7.

Theorem 4.2.8. *Suppose that $G = \mathbb{F}_2^n$. Suppose that $f \in A(G)$ and $\epsilon \in (0, 1]$. Write $A_f := \|f\|_{A(G)}\|f\|^{-1}_{L^\infty(\mu_G)}$. Then there is a subspace V of G with*

$$\operatorname{codim} V \ll \epsilon^{-2}A_f(1 + \log A_f)(1 + \log \epsilon^{-1}A_f),$$

and

$$\sup_{x\in G}\|f - f * \mu_V\|_{L^2(x+\mu_V)} < \epsilon\|f\|_{L^\infty(\mu_G)}.$$

The first part of the conclusion of Theorem 4.2.7 is unnecessary since $f * \mu_V$ is constant on cosets of V and hence

$$\sup_{x\in G}\|f * \mu_V - f * \mu_V(x)\|_{L^\infty(x+\mu_V)} = 0.$$

The basic quantitative argument

We begin with an argument which proves the following weak version of Theorem 4.2.8; the argument will form the basis of our proof of that theorem.

Theorem 4.2.9. *Suppose that* $G = \mathbb{F}_2^n$. *Suppose that* $f \in A(G)$ *and* $\epsilon \in (0,1]$. *Write* $A_f := \|f\|_{A(G)}\|f\|_{L^\infty(\mu_G)}^{-1}$. *Then there is a subspace* V *of* G *with*

$$\operatorname{codim} V \leqslant 2^3\epsilon^{-4}A_f^3,$$

and

$$\sup_{x\in G}\|f - f*\mu_V\|_{L^2(x+\mu_V)} < \epsilon\|f\|_{L^\infty(\mu_G)}.$$

The technique is iterative, with the driving component being the following lemma.

Lemma 4.2.10 (Iteration lemma 1)**.** *Suppose that* $G = \mathbb{F}_2^n$ *and* $\Gamma^\perp$ *is an annihilator in* G. *Suppose that* $f \in A(G)$ *and* $\epsilon \in (0,1]$. *Write* $A_f := \|f\|_{A(G)}\|f\|_{L^\infty(\mu_G)}^{-1}$. *Then at least one of the following is true.*

(i). (f is close to a continuous function)

$$\sup_{x\in G}\|f - f*\mu_{\Gamma^\perp}\|_{L^2(x+\mu_{\Gamma^\perp})} < \epsilon\|f\|_{L^\infty(\mu_G)}.$$

(ii). There is a set of characters Λ *with* $|\Lambda| \leqslant 2\epsilon^{-2}A_f^2$ *such that*

$$\sum_{\gamma\in(\Gamma\cup\Lambda)^{\perp\perp}}|\widehat{f}(\gamma)| - \sum_{\gamma\in\Gamma^{\perp\perp}}|\widehat{f}(\gamma)| \geqslant 2^{-2}\epsilon^2\|f\|_{L^\infty(\mu_G)}.$$

Essentially this says that if f does not satisfy the conclusion of Theorem 4.2.9 for some annihilator $\Gamma^\perp$ then there is a smaller (but not too much smaller) annihilator $\Gamma'^\perp$ which supports more $A(G)$-norm of f.

To control the size of $\Gamma'^\perp$ we we use Proposition 2.3.2; in $\mathbb{F}_2^n$ its statement is particularly simple:

Proposition 4.2.11. (Model analogue of Proposition 2.3.2) *Suppose that* $G = \mathbb{F}_2^n$ *and* $\Gamma^\perp$ *is an annihilator in* G. *Suppose that* $f \in A(G)$ *and* $\epsilon \in (0,1]$. *Then there is a set* Λ *of characters with*

$$|\Lambda| \leqslant \epsilon^{-1}\|f\|_{A(G)}\|f\|_{L^\infty(\mu_\Gamma^\perp)}^{-1}$$

such that

$$\{\gamma \in \widehat{G} : |\widehat{fd\mu_{\Gamma^\perp}}(\gamma)| \geqslant \epsilon \|f\|_{L^\infty(\mu_{\Gamma^\perp})}\} \subset (\Gamma \cup \Lambda)^{\perp\perp}.$$

Proof of Lemma 4.2.10. Suppose that

$$\sup_{x \in G} \|f - f * \mu_{\Gamma^\perp}\|_{L^2(x+\mu_{\Gamma^\perp})} \geqslant \epsilon \|f\|_{L^\infty(\mu_G)}.$$

Since G is finite there is some $x' \in G$ which, without loss of generality, is equal to 0_G such that

$$\|f - f * \mu_{\Gamma^\perp}\|_{L^2(x'+\mu_{\Gamma^\perp})} \geqslant \epsilon \|f\|_{L^\infty(\mu_G)}. \tag{4.2.1}$$

For ease of notation write $g = f - f * \mu_{\Gamma^\perp}$, and observe that g satisfies the inequalities

$$\|g\|_{A(G)} \leqslant \|f\|_{A(G)} \text{ and } \|g\|_{L^\infty(\mu_{\Gamma^\perp})} \leqslant 2\|f\|_{L^\infty(\mu_G)}. \tag{4.2.2}$$

To see the first of these note that

$$\|g\|_{A(G)} = \sum_{\gamma \in \widehat{G}} |1 - \widehat{\mu_{\Gamma^\perp}}(\gamma)||\widehat{f}(\gamma)| \leqslant \sup_{\gamma \in \widehat{G}} |1 - \widehat{\mu_{\Gamma^\perp}}(\gamma)|\|f\|_{A(G)} \leqslant \|f\|_{A(G)},$$

and for the second

$$\|g\|_{L^\infty(\mu_{\Gamma^\perp})} \leqslant \|g\|_{L^\infty(\mu_G)} \leqslant \|f\|_{L^\infty(\mu_G)} + \|f * \mu_{\Gamma^\perp}\|_{L^\infty(\mu_G)} \leqslant 2\|f\|_{L^\infty(\mu_G)}.$$

Returning to (4.2.1) we may apply Plancherel's Theorem and then the triangle inequality to give us a Fourier statement:

$$\sum_{\gamma \in \widehat{G}} |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)||\widehat{g}(\gamma)| \geqslant \epsilon^2 \|f\|^2_{L^\infty(\mu_G)}. \tag{4.2.3}$$

The characters supporting large values of $\widehat{gd\mu_{\Gamma^\perp}}$ make the principal contribution to this sum. Specifically put

$$\mathcal{C} := \{\gamma \in \widehat{G} : |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)| > \epsilon' \|g\|_{L^\infty(\mu_{\Gamma^\perp})}\},$$

where

$$\epsilon' := 2^{-1}\epsilon^2 A_f^{-1} \|f\|_{L^\infty(G)} \|g\|^{-1}_{L^\infty(\mu_{\Gamma^\perp})}.$$

Then

$$\begin{aligned}\sum_{\gamma \notin \mathcal{C}} |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)||\widehat{g}(\gamma)| &\leqslant 2^{-1}\epsilon^2 A_f^{-1} \|f\|_{L^\infty(\mu_G)} \sum_{\gamma \notin \mathcal{C}} |\widehat{g}(\gamma)| \\ &\leqslant 2^{-1}\epsilon^2 A_f^{-1} \|f\|_{L^\infty(\mu_G)} \|g\|_{A(G)} \\ &\leqslant 2^{-1}\epsilon^2 \|f\|^2_{L^\infty(\mu_G)} \text{ since } \|g\|_{A(G)} \leqslant \|f\|_{A(G)}.\end{aligned}$$

Substituting this into (4.2.3) we conclude that

$$\sum_{\gamma \in \mathcal{C}} |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)||\widehat{g}(\gamma)| \geqslant 2^{-1}\epsilon^2 \|f\|^2_{L^\infty(\mu_G)}. \tag{4.2.4}$$

Now certainly $|\widehat{gd\mu_{\Gamma^\perp}}(\gamma)| \leqslant 2\|f\|_{L^\infty(\mu_G)}$ so that

$$2^{-2}\epsilon^2 \|f\|_{L^\infty(\mu_G)} \leqslant \sum_{\gamma \in \mathcal{C}} |\widehat{g}(\gamma)|.$$

We now apply Proposition 4.2.11 to $\mathcal{C}$ to get a set of characters Λ with

$$\begin{aligned}|\Lambda| &< (\epsilon')^{-1} \|g\|_{A(G)} \|g\|^{-1}_{L^\infty(\mu_{\Gamma^\perp})} \\ &\leqslant 2\epsilon^{-2} A_f^2,\end{aligned}$$

such that $\mathcal{C} \subset (\Gamma \cup \Lambda)^{\perp\perp}$. The lemma follows. □

We are now in a position to iterate this and prove Theorem 4.2.9.

Proof of Theorem 4.2.9. We construct a sequence of annihilators $\Gamma_k^\perp$ iteratively. Write

$$L_k := \sum_{\gamma \in \Gamma_k^{\perp\perp}} |\widehat{f}(\gamma)|,$$

and initiate the iteration with $\Gamma_0 := \{0_{\widehat{G}}\}$.

Suppose that we are at stage k of the iteration. Apply the iteration lemma (Lemma 4.2.10). If we are in the first case of the lemma then put $V = \Gamma_k^{\perp}$ and terminate; if not then we get a set of characters Λ and put $\Gamma_{k+1} = \Gamma_k \cup \Lambda$. It follows from the properties of Λ that

$$|\Gamma_{k+1}| \leqslant |\Gamma_k| + 2\epsilon^{-2}A_f^2 \text{ and } L_{k+1} - L_k \geqslant 2^{-2}\epsilon^2\|f\|_{L^\infty(\mu_G)}.$$

By induction we have that after k iterations

$$|\Gamma_k| \leqslant k.2\epsilon^{-2}A_f^2 \text{ and } L_k \geqslant k.2^{-2}\epsilon^2\|f\|_{L^\infty(\mu_G)}.$$

Since $L_k \leqslant \|f\|_{A(G)}$ we conclude that the iteration terminates and

$$|\Gamma_k| \leqslant 2^3\epsilon^{-4}A_f^3.$$

The theorem follows. □

Refining the basic argument: the proof of Theorem 4.2.8

To achieve the result in Theorem 4.2.8 we make two important improvements to the iteration lemma (Lemma 4.2.10) of the previous argument.

- *(Dyadic decomposition)* Our first improvement is the observation that having derived

  $$\sum_{\gamma \in \mathcal{C}} |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)||\widehat{g}(\gamma)| \geqslant 2^{-1}\epsilon^2\|f\|_{L^\infty(\mu_G)}^2 \text{ (4.2.4)},$$

  we can do something better than simply adding all the characters in $\mathcal{C}$ to Γ. Partition the characters in $\mathcal{C}$ by dyadically decomposing the range of values of $|\widehat{gd\mu_{\Gamma^\perp}}|$ and pick the characters in a dyadic class contributing maximal mass to (4.2.4). The $A(G)$-norm of f supported on this class is more closely related to the size of $\mathcal{C}$ which yields an improvement.

- *(Structure theorem for the Fourier spectrum)* The second improvement replaces the application of Proposition 4.2.11 with the stronger Proposition 2.3.4, which in the model setting has the following simpler statement.

Proposition 4.2.12. (Model analogue of Proposition 2.3.4) *Suppose that $G = \mathbb{F}_2^n$ and $\Gamma^\perp$ is an annihilator in G. Suppose that $f \in A(G)$ and $\epsilon \in (0,1]$. Write $A_f := \|f\|_{A(G)}\|f\|_{L^\infty(\mu_{\Gamma^\perp})}^{-1}$. Then there is a set Λ of characters with $|\Lambda| \ll \epsilon^{-1}\log A_f$ such that*

$$\{\gamma \in \widehat{G} : |\widehat{fd\mu_{\Gamma^\perp}}(\gamma)| \geqslant \epsilon\|f\|_{L^\infty(\mu_{\Gamma^\perp})}\} \subset (\Gamma \cup \Lambda)^{\perp\perp}.$$

By implementing these two refinements we prove the following iteration lemma.

Lemma 4.2.13 (Iteration lemma 2)**.** *Suppose that $G = \mathbb{F}_2^n$ and $\Gamma^\perp$ is an annihilator in G. Suppose that $f \in A(G)$ and $\epsilon \in (0,1]$. Write $A_f := \|f\|_{A(G)}\|f\|_{L^\infty(G)}^{-1}$. Then at least one of the following is true.*

(i). (f is close to a continuous function)

$$\sup_{x\in G}\|f - f * \mu_{\Gamma^\perp}\|_{L^2(x+\mu_{\Gamma^\perp})} < \epsilon\|f\|_{L^\infty(\mu_G)}.$$

(ii). There is a set of characters Λ and a non-negative integer s with $|\Lambda| \ll 2^s(1 + \log A_f)$ such that

$$\sum_{\gamma\in(\Gamma\cup\Lambda)^{\perp\perp}} |\widehat{f}(\gamma)| - \sum_{\gamma\in\Gamma^{\perp\perp}} |\widehat{f}(\gamma)| \gg \frac{2^s\epsilon^2\|f\|_{L^\infty(\mu_G)}}{1 + \log \epsilon^{-1}A_f}.$$

Proof. We proceed as in the proof of Lemma 4.2.10 up to the point where we conclude that

$$\sum_{\gamma\in\mathcal{C}} |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)||\widehat{g}(\gamma)| \geqslant 2^{-1}\epsilon^2\|f\|_{L^\infty(\mu_G)}^2 \text{ (4.2.4)}.$$

Write $I_s := (2^{-s}\|f\|_{L^\infty(\mu_G)}, 2^{-(s-1)}\|f\|_{L^\infty(\mu_G)}]$ and partition $\mathcal{C}$ into the sets

$$\mathcal{C}_s := \{\gamma \in \mathcal{C} : |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)| \in I_s\} \text{ for } 0 \leqslant s \leqslant 1 + \log_2 \epsilon^{-2} A_f.$$

Note that $\{\mathcal{C}_s : 0 \leqslant s \leqslant 1 + \log_2 \epsilon^{-2} A_f\}$ covers $\mathcal{C}$ since

$$\sup_{\gamma \in \mathcal{C}} |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)| \leqslant \sup_{\gamma \in \widehat{G}} |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)| \leqslant \|g\|_{L^\infty(\mu_{\Gamma^\perp})} \leqslant 2\|f\|_{L^\infty(\mu_G)}$$

and

$$\inf_{\gamma \in \mathcal{C}} |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)| > 2^{-1}\epsilon^2 A_f^{-1}\|f\|_{L^\infty(\mu_G)},$$

so that (4.2.4) may be rewritten to yield

$$\sum_{s=0}^{1+\log_2 \epsilon^{-2} A_f} \sum_{\gamma \in \mathcal{C}_s} |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)||\widehat{g}(\gamma)| \geqslant 2^{-1}\epsilon^2\|f\|^2_{L^\infty(\mu_G)}.$$

It follows by the pigeonhole principle that there is some s for which

$$\sum_{\gamma \in \mathcal{C}_s} |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)||\widehat{g}(\gamma)| \gg \frac{\epsilon^2\|f\|^2_{L^\infty(\mu_G)}}{1 + \log \epsilon^{-1} A_f},$$

and since $|\widehat{gd\mu_{\Gamma^\perp}}(\gamma)| \leqslant 2^{-(s-1)}\|f\|_{L^\infty(\mu_G)}$ if $\gamma \in \mathcal{C}_s$ we get

$$\sum_{\gamma \in \mathcal{C}_s} |\widehat{g}(\gamma)| \gg \frac{2^s\epsilon^2\|f\|_{L^\infty(\mu_G)}}{1 + \log \epsilon^{-1} A_f}.$$

Now

$$\mathcal{C}_s \subset \{\gamma : |\widehat{gd\mu_{\Gamma^\perp}}(\gamma)| > (2^{-s}\|f\|_{L^\infty(\mu_G)}\|g\|^{-1}_{L^\infty(\mu_{\Gamma^\perp})})\|g\|_{L^\infty(\mu_{\Gamma^\perp})}\},$$

and since $\|g\|_{A(G)} \leqslant \|f\|_{A(G)}$ we may apply Proposition 4.2.12 to get a set of characters Λ such that $\mathcal{C}_s \subset (\Gamma \cup \Lambda)^{\perp\perp}$. Moreover $|\Lambda|$ satisfies

$$\begin{aligned} |\Lambda| &\ll 2^s \|f\|_{L^\infty(\mu_G)}^{-1} \|g\|_{L^\infty(\mu_{\Gamma^\perp})}(1 + \log \|g\|_{A(G)} \|g\|_{L^\infty(\mu_{\Gamma^\perp})}^{-1}) \\ &\ll 2^s(1 + \log \|g\|_{A(G)} \|f\|_{L^\infty(\mu_G)}^{-1}) \text{ since } \|g\|_{L^\infty(\mu_{\Gamma^\perp})} \leqslant 2\|f\|_{L^\infty(\mu_G)} \\ &\ll 2^s(1 + \log A_f) \text{ since } \|g\|_{A(G)} \leqslant \|f\|_{A(G)}. \end{aligned}$$

The lemma follows. □

Iterating this in the same way as before yields Theorem 4.2.8.

4.2.3 The proof of Theorem 4.2.7

We begin by extending the second iteration lemma (Lemma 4.2.13) from the model setting to that of general finite abelian groups.

Lemma 4.2.14. *Suppose that G is a finite abelian group and $B(\Gamma, \delta)$ a regular Bohr set. Suppose that $f \in A(G)$ and $\epsilon \in (0, 1]$. Write A_f for the quantity $\|f\|_{A(G)} \|f\|_{L^\infty(\mu_G)}^{-1}$. Then at least one of the following is true.*

(i). (f is close to a continuous function) *There is a Bohr set $B(\Gamma, \delta')$ with $\delta' \gg \epsilon\delta/d$ such that*

$$\sup_{x \in G} \|f * \beta - f * \beta(x)\|_{L^\infty(x + \beta_{\Gamma,\delta'})} \leqslant \epsilon \|f\|_{L^\infty(\mu_G)}$$

and

$$\sup_{x \in G} \|f - f * \beta_{\Gamma,\delta}\|_{L^2(x + \beta_{\Gamma,\delta'})} \leqslant \epsilon \|f\|_{L^\infty(\mu_G)}.$$

(ii). For all $\eta \in (0, 1]$ there is a set of characters Λ, a $\delta'' \in (0, 1]$ and a non-negative integer s with

$$|\Lambda| \ll 2^s(1 + \log A_f) \text{ and } \delta'' \gg \epsilon^5 A_f^{-4} \eta\delta/d^3,$$

such that

$$\sum_{\gamma \in \mathcal{L}} |1 - \widehat{\beta_{\Gamma,\delta}}(\gamma)||\widehat{f}(\gamma)| \gg \frac{2^s \epsilon^2 \|f\|_{L^\infty(\mu_G)}}{\min\{2^s, 1 + \log \epsilon^{-1} A_f\}}$$

where

$$\mathcal{L} := \{\gamma : |1-\gamma(x)| \leqslant \eta \text{ for all } x \in B(\Gamma \cup \Lambda, \delta'')\}.$$

Proof. Choosing δ' is easy: By Corollary 2.2.5 and Proposition 2.2.2 there is a $\delta' \gg \delta\epsilon/d$ regular for Γ such that

$$\sup_{x\in G} \|f * \beta_{\Gamma,\delta} - f * \beta_{\Gamma,\delta}(x)\|_{L^\infty(x+\beta_{\Gamma,\delta'})} \leqslant \epsilon \|f\|_{L^\infty(\mu_G)}.$$

Now, suppose that

$$\sup_{x\in G} \|f - f * \beta_{\Gamma,\delta}\|_{L^2(x+\beta_{\Gamma,\delta'})} > \epsilon \|f\|_{L^\infty(\mu_G)}.$$

It follows that there is some $x' \in G$ which, without loss of generality, is equal to 0_G such that

$$\|f - f * \beta_{\Gamma,\delta}\|_{L^2(x'+\beta_{\Gamma,\delta'})} \geqslant \epsilon \|f\|_{L^\infty(\mu_G)}. \tag{4.2.5}$$

For ease of notation write $g = f - f * \beta_{\Gamma,\delta}$, and observe that g satisfies the inequalities

$$\|g\|_{A(G)} \leqslant 2\|f\|_{A(G)} \text{ and } \|g\|_{L^\infty(\beta_{\Gamma,\delta'})} \leqslant 2\|f\|_{L^\infty(\mu_G)}.$$

To see the first of these note that

$$\|g\|_{A(G)} = \sum_{\gamma\in\widehat{G}} |1 - \widehat{\beta_{\Gamma,\delta}}(\gamma)||\widehat{f}(\gamma)| \leqslant \sup_{\gamma\in\widehat{G}} |1 - \widehat{\beta_{\Gamma,\delta}}(\gamma)| \|f\|_{A(G)} \leqslant 2\|f\|_{A(G)},$$

and for the second

$$\|g\|_{L^\infty(\beta_{\Gamma,\delta'})} \leqslant \|g\|_{L^\infty(\mu_G)} \leqslant \|f\|_{L^\infty(\mu_G)} + \|f * \beta_{\Gamma,\delta}\|_{L^\infty(\mu_G)} \leqslant 2\|f\|_{L^\infty(\mu_G)}.$$

Returning to (4.2.5) we may apply Plancherel's Theorem and then the triangle inequality to give us a Fourier statement:

$$\sum_{\gamma \in \widehat{G}} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)||\widehat{g}(\gamma)| \geqslant \epsilon^2 \|f\|_{L^\infty(\mu_G)}^2. \tag{4.2.6}$$

The characters supporting large values of $\widehat{gd\beta_{\Gamma,\delta'}}$ make the principal contribution to this sum. Specifically put

$$\mathcal{C} := \{\gamma \in \widehat{G} : |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)| > \epsilon' \|g\|_{L^\infty(\beta_{\Gamma,\delta'})}\},$$

where

$$\epsilon' := 2^{-2}\epsilon^2 A_f^{-1}\|f\|_{L^\infty(\mu_G)}\|g\|_{L^\infty(\beta_{\Gamma,\delta'})}^{-1}.$$

Then

$$\begin{aligned}
\sum_{\gamma \notin \mathcal{C}} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)||\widehat{g}(\gamma)| &\leqslant 2^{-2}\epsilon^2 A_f^{-1}\|f\|_{L^\infty(\mu_G)} \sum_{\gamma \notin \mathcal{C}} |\widehat{g}(\gamma)| \\
&\leqslant 2^{-2}\epsilon^2 A_f^{-1}\|f\|_{L^\infty(\mu_G)}\|g\|_{A(G)} \\
&\leqslant 2^{-1}\epsilon^2\|f\|_{L^\infty(\mu_G)}^2 \text{ since } \|g\|_{A(G)} \leqslant 2\|f\|_{A(G)}.
\end{aligned}$$

Substituting this into (4.2.6) we conclude that

$$\sum_{\gamma \in \mathcal{C}} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)||\widehat{g}(\gamma)| \geqslant 2^{-1}\epsilon^2 \|f\|_{L^\infty(\mu_G)}^2. \tag{4.2.7}$$

Write $I_s := (2^{-s}\|f\|_{L^\infty(\mu_G)}, 2^{-(s-1)}\|f\|_{L^\infty(\mu_G)}]$ and partition $\mathcal{C}$ into the sets

$$\mathcal{C}_s := \{\gamma \in \mathcal{C} : |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)| \in I_s\} \text{ for } 0 \leqslant s \leqslant 3 + \log_2 \epsilon^{-2} A_f.$$

Notice that $\{\mathcal{C}_s : 0 \leqslant s \leqslant 3 + \log_2 \epsilon^{-2} A_f\}$ covers $\mathcal{C}$ since

$$\sup_{\gamma \in \mathcal{C}} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)| \leqslant \sup_{\gamma \in \widehat{G}} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)| \leqslant \|g\|_{L^\infty(\beta_{\Gamma,\delta'})} \leqslant 2\|f\|_{L^\infty(\mu_G)}$$

and

$$\inf_{\gamma \in \mathcal{C}} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)| > 2^{-2}\epsilon^2 A_f^{-1}\|f\|_{L^\infty(\mu_G)},$$

so that (4.2.7) may be rewritten to yield

$$\sum_{s=0}^{3+\log_2 \epsilon^{-2}A_f} \sum_{\gamma \in \mathcal{C}_s} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)||\widehat{g}(\gamma)| \geqslant 2^{-1}\epsilon^2\|f\|_{L^\infty(\mu_G)}^2.$$

Writing $S' := \{s \in \mathbb{N}_0 : 2^s \leqslant 3 + \log_2 \epsilon^{-2}A_f\}$ and $S'' := \{s \in \mathbb{N}_0 : 2^s > 3 + \log_2 \epsilon^{-2}A_f\}$ it follows that either

$$\sum_{s \in S'} 2^{-s}.2^s \sum_{\gamma \in \mathcal{C}_s} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)||\widehat{g}(\gamma)| \geqslant 2^{-2}\epsilon^2\|f\|_{L^\infty(\mu_G)}^2$$

or

$$\sum_{s \in S''} \sum_{\gamma \in \mathcal{C}_s} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)||\widehat{g}(\gamma)| \geqslant 2^{-2}\epsilon^2\|f\|_{L^\infty(\mu_G)}^2.$$

By the pigeonhole principle there is some s for which

$$\sum_{\gamma \in \mathcal{C}_s} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)||\widehat{g}(\gamma)| \gg \frac{\epsilon^2\|f\|_{L^\infty(\mu_G)}^2}{1 + \log \epsilon^{-1}A_f} \text{ if } 2^s > 3 + \log_2 \epsilon^{-2}A_f$$

and

$$\sum_{\gamma \in \mathcal{C}_s} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)||\widehat{g}(\gamma)| \gg \frac{\epsilon^2\|f\|_{L^\infty(\mu_G)}^2}{2^s} \text{ if } 2^s \leqslant 3 + \log_2 \epsilon^{-2}A_f.$$

i.e. there is some s such that

$$\sum_{\gamma \in \mathcal{C}_s} |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)||\widehat{g}(\gamma)| \gg \frac{\epsilon^2\|f\|_{L^\infty(\mu_G)}^2}{\min\{2^s, 1 + \log \epsilon^{-1}A_f\}}.$$

Since $|\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)| \leqslant 2^{-(s-1)}\|f\|_{L^\infty(\mu_G)}$ if $\gamma \in \mathcal{C}_s$ we get

$$\sum_{\gamma \in \mathcal{C}_s} |\widehat{g}(\gamma)| \gg \frac{2^s\epsilon^2\|f\|_{L^\infty(\mu_G)}}{\min\{2^s, 1 + \log \epsilon^{-1}A_f\}}.$$

Now

$$\mathcal{C}_s \subset \{\gamma : |\widehat{gd\beta_{\Gamma,\delta'}}(\gamma)| \geqslant (2^{-s}\|f\|_{L^\infty(\mu_G)}\|g\|_{L^\infty(\beta_{\Gamma,\delta'})}^{-1})\|g\|_{L^\infty(\beta_{\Gamma,\delta'})}\},$$

and $g \in A(G)$ so we may apply Proposition 2.3.4 to get a set of characters Λ and a δ'' regular for $\Gamma \cup \Lambda$ such that

$$\mathcal{C}_s \subset \{\gamma : |1 - \gamma(x)| \leqslant \eta \text{ for all } x \in B(\Gamma \cup \Lambda, \delta'')\}.$$

Moreover $|\Lambda|$ satisfies

$$\begin{aligned} |\Lambda| &\ll 2^s \|f\|_{L^\infty(\mu_G)}^{-1} \|g\|_{L^\infty(\beta_{\Gamma,\delta'})} (1 + \log \|g\|_{A(G)} \|g\|_{L^\infty(\beta_{\Gamma,\delta'})}^{-1}) \\ &\ll 2^s \|f\|_{L^\infty(\mu_G)}^{-1} \|g\|_{L^\infty(\beta_{\Gamma,\delta'})} (1 + \log 2\|f\|_{A(G)} \|g\|_{L^\infty(\beta_{\Gamma,\delta'})}^{-1}) \end{aligned}$$

since $\|g\|_{A(G)} \leqslant 2\|f\|_{A(G)}$, so

$$|\Lambda| \ll 2^s \|f\|_{L^\infty(\mu_G)}^{-1} \|g\|_{L^\infty(\beta_{\Gamma,\delta'})} (1 + \log 2A_f \|f\|_{L^\infty(\mu_G)} \|g\|_{L^\infty(\beta_{\Gamma,\delta'})}^{-1}).$$

So, writing X for $\|f\|_{L^\infty(\mu_G)}^{-1} \|g\|_{L^\infty(\beta_{\Gamma,\delta'})}$ we have

$$|\Lambda| \ll 2^s X (1 + \log 2A_f X^{-1}),$$

but $\|g\|_{L^\infty(\beta_{\Gamma,\delta'})} \leqslant 2\|f\|_{L^\infty(\mu_G)}$ so $X \leqslant 2$ and therefore

$$|\Lambda| \ll 2^s \sup_{X' \in (0,2]} X'(1 + \log 2A_f X'^{-1}) \ll 2^s (1 + \log A_f).$$

Furthermore δ'' satisfies

$$\begin{aligned} \delta'' &\gg 2^{-2s} \|f\|_{L^\infty(\mu_G)}^2 \|g\|_{L^\infty(\beta_{\Gamma,\delta'})}^{-2} \eta\delta'/d^2 (1 + \log \|g\|_{A(G)} \|g\|_{L^\infty(\beta_{\Gamma,\delta'})}^{-1}) \\ &\gg 2^{-2s} \|f\|_{L^\infty(\mu_G)}^2 \eta\delta'/d^2 \|g\|_{A(G)}^2 \\ &\gg \epsilon^4 A_f^{-2} \|f\|_{L^\infty(\mu_G)}^2 \eta\delta'/d^2 \|g\|_{A(G)}^2 \text{ since } 2^{2s} \leqslant 2^4 \epsilon^{-4} A_f^2 \\ &\gg \epsilon^4 A_f^{-4} \eta\delta'/d^2 \text{ since } \|g\|_{A(G)} \leqslant 2\|f\|_{A(G)}. \end{aligned}$$

The lemma follows. □

We are now in a position to iterate this lemma.

Proof of Theorem 4.2.7. Fix η to be optimized at the end of the argument. We construct a sequence of regular Bohr sets $B(\Gamma_k, \delta_k)$ iteratively using

Lemma 4.2.14. Put

$$\mathcal{L}_k := \{\gamma : |1-\gamma(x)| \leqslant \eta \text{ for all } x \in B(\Gamma_k, \delta_k)\}$$

and

$$d_k := |\Gamma_k| \text{ and } L_k := \sum_{\gamma \in \mathcal{L}_k} |\widehat{f}(\gamma)|.$$

We initialize the iteration with $\Gamma_0 := \{0_{\widehat{G}}\}$ and $\delta_0 \gg 1$ regular for Γ_0, chosen so by Proposition 2.2.2.

Suppose that we are at stage k. Apply the iteration lemma (Lemma 4.2.14) to f and the regular Bohr set $B(\Gamma_k, \delta_k)$. If we are in the first case terminate with the desired conclusion; if not then we get a set of characters Λ, a $\delta'' \in (0,1]$ and an integer s. Let $\Gamma_{k+1} = \Gamma_k \cup \Lambda$, pick $\delta_{k+1} \in (\delta''/2, \delta'']$ regular for Γ_{k+1} by Proposition 2.2.2, and let $s_{k+1} = s$. We are given that

$$d_{k+1} - d_k \ll 2^{s_{k+1}}(1+\log A_f) \text{ and } \delta_{k+1} \gg \epsilon^5 A_f^{-4}\eta\delta_k/d_k^3,$$

and furthermore

$$2(L_{k+1} - L_k) + \eta L_k \gg \frac{2^{s_{k+1}}\epsilon^2\|f\|_{L^\infty(\mu_G)}}{\min\{2^{s_{k+1}}, 1+\log \epsilon^{-1}A_f\}}.$$

Since $L_k \leqslant \|f\|_{A(G)}$ and $s_k \geqslant 0$ it follows that we can pick $\eta \gg \epsilon^3 A_f^{-2}$ (independently of k) such that

$$L_{k+1} - L_k \gg \frac{2^{s_{k+1}}\epsilon^2\|f\|_{L^\infty(\mu_G)}}{\min\{2^{s_{k+1}}, 1+\log \epsilon^{-1}A_f\}}.$$

Hence by induction we have

$$L_k \gg \epsilon^2\|f\|_{L^\infty(\mu_G)} \sum_{l=1}^{k} \frac{2^{s_l}}{\min\{2^{s_l}, 1+\log \epsilon^{-1}A_f\}} \text{ and } d_k \ll \sum_{l=1}^{k} 2^{s_l}(1+\log A_f).$$

Again since $s_k \geqslant 0$ it follows that the iteration terminates. Hence we have

$$\sum_{l=1}^{k} 2^{s_l} \ll L_k \epsilon^{-2} \|f\|_{L^\infty(\mu_G)}^{-1} (1 + \log \epsilon^{-1} A_f) \ll \epsilon^{-2} A_f (1 + \log \epsilon^{-1} A_f),$$

since $\|f\|_{A(G)} \geqslant L_k$. It follows that

$$d_k \ll \epsilon^{-2} A_f (1 + \log A_f)(1 + \log \epsilon^{-1} A_f).$$

The bound on η and d_k gives us

$$\delta_{k+1} \gg \epsilon^{17} A_f^{-15} \delta_k,$$

and hence

$$\begin{aligned} \log \delta_k^{-1} &\ll k(1 + \log \epsilon^{-1} A_f) \\ &\ll \sum_{l=1}^{k} \frac{2^{s_k}}{\min\{2^{s_k}, 1 + \log \epsilon^{-1} A_f\}} (1 + \log \epsilon^{-1} A_f) \\ &\ll \epsilon^{-2} A_f (1 + \log \epsilon^{-1} A_f). \end{aligned}$$

The result follows. □

4.2.4 The proof of Theorem 3.1.1 and concluding remarks

Having proved Theorem 4.2.7 it is essentially a formality to carry out the rest of the argument detailed in §4.2.1.

Proof of Theorem 3.1.1. Write G for $\mathbb{Z}/p\mathbb{Z}$ and $\alpha := \mu_G(A) = |A|/p$. We apply Theorem 4.2.7 to $f = 1_A$ with $\epsilon = 2^{-2}\alpha(1-\alpha)$. This gives a Bohr set $B(\Gamma, \delta)$ with

$$d \ll_\alpha \|1_A\|_{A(G)} (1 + \log \|1_A\|_{A(G)})^2$$

and

$$\log \delta^{-1} \ll_\alpha \|1_A\|_{A(G)} (1 + \log \|1_A\|_{A(G)}),$$

and a narrower Bohr set $B(\Gamma,\delta')$ with $\delta' \gg_\alpha \delta/d$ such that

$$\sup_{x\in G}\|1_A*\beta_{\Gamma,\delta}-1_A*\beta_{\Gamma,\delta}(x)\|_{L^\infty(x+\beta_{\Gamma,\delta'})}\leqslant 2^{-2}\alpha(1-\alpha)$$

and

$$\sup_{x\in G}\|1_A-1_A*\beta_{\Gamma,\delta}\|_{L^2(x+\beta_{\Gamma,\delta'})}\leqslant 2^{-2}\alpha(1-\alpha). \qquad (4.2.8)$$

Suppose that $\mu_G(\beta_{\Gamma,\delta'})>p^{-1}$. Then there is a non-zero $y\in B(\Gamma,\delta')$, and such a y has the property that $|1_A*\beta_{\Gamma,\delta}(x+y)-1_A*\beta_{\Gamma,\delta}(x)|\leqslant 2^{-2}\alpha(1-\alpha)$ for all $x\in G$. It follows that we may apply the discrete intermediate value theorem (Proposition 4.2.5) to $1_A*\beta_{\Gamma,\delta}$ and conclude that there is some $x\in G$ such that

$$|1_A*\beta_{\Gamma,\delta}(x)-\alpha|\leqslant 2^{-3}\alpha(1-\alpha).$$

Furthermore (4.2.8) ensures that there is some $x'\in x+B(\Gamma,\delta')$ such that

$$|1_A(x')-1_A*\beta_{\Gamma,\delta}(x')|\leqslant 2^{-2}\alpha(1-\alpha).$$

Since $|1_A(x')-\alpha|$ is at most

$$|1_A(x')-1_A*\beta_{\Gamma,\delta}(x')|+|1_A*\beta_{\Gamma,\delta}(x')-1_A*\beta_{\Gamma,\delta}(x)|+|1_A*\beta_{\Gamma,\delta}(x)-\alpha|$$

by the triangle inequality, we conclude that it is at most $\alpha(1-\alpha)$. This contradicts the fact that $1_A(x')\in\{0,1\}$, and hence $\mu_G(B(\Gamma,\delta'))\leqslant p^{-1}$. Lemma 2.2.1 then lets us infer that $d(1+\log\delta'^{-1})\gg\log p$ from which, on inserting the bounds on d and δ', the result follows. □

In [GK09] Green and Konyagin essentially prove a version of Theorem 4.2.7 with different bounds:

Theorem 4.2.15. *Suppose that G is a finite abelian group, $f\in A(G)$ and $\epsilon\in(0,1]$. Write A_f for the quantity $\|f\|_{A(G)}\|f\|^{-1}_{L^\infty(\mu_G)}$. Then there is a Bohr set $B(\Gamma,\delta)$ with*

$$|\Gamma|\ll\epsilon^{-2}A_f^2 \text{ and } \log\delta^{-1}\ll\epsilon^{-1}A_f(1+\log\epsilon^{-1}A_f),$$

and a narrower Bohr set $B(\Gamma,\delta')$ *with* $\delta' \gg \epsilon\delta/d$ *such that*

$$\sup_{x\in G}\|f*\beta_{\Gamma,\delta}-f*\beta_{\Gamma,\delta}(x)\|_{L^\infty(x+\beta_{\Gamma,\delta'})}\leqslant\epsilon\|f\|_{L^\infty(\mu_G)}$$

and

$$\sup_{x\in G}\|f-f*\beta_{\Gamma,\delta}\|_{L^2(x+\beta_{\Gamma,\delta'})}\leqslant\epsilon\|f\|_{L^\infty(\mu_G)}.$$

The crucial difference between our proof of Theorem 4.2.7 and their proof of Theorem 4.2.15 is that in their iteration lemma they find only a few characters at which $\widehat{f}$ is large, whereas we find all characters at which $\widehat{f}$ is large. Their approach leads to superior bounds in the basic version of their argument, however it prevents them from using a tool such as Proposition 2.3.4, which is where our argument gains its edge.

In both our argument and the argument of Green and Konyagin the width of the Bohr set which one eventually finds narrows exponentially with the number of times one has to use the (appropriate) iteration lemma. Green and Konyagin employ a neat trick to reduce this – the natural version of their argument has $\log\delta^{-1}\ll\epsilon^{-2}A_f^2(1+\log\epsilon^{-1}A_f)$ – which leads to the superior ϵ-dependence for $\log\delta^{-1}$ in Theorem 4.2.15. It is possible to add their trick to our argument and hence improve the ϵ-dependence of $\log\delta^{-1}$ in Theorem 4.2.7 too, however this would have no effect on our application.

Finally it would be interesting to know what the true bounds in Theorem 4.2.7 should be. As far as the model analogue, Theorem 4.2.8, is concerned it would probably be surprising if one could beat the following.

Conjecture 4.2.16. *Suppose that* $G=\mathbb{F}_2^n$, $f\in A(G)$ *and* $\epsilon\in(0,1]$. *Write* A_f *for the quantity* $\|f\|_{A(G)}\|f\|_{L^\infty(\mu_G)}^{-1}$. *Then there is a subspace* V *of* G *with*

$$\operatorname{codim}V\ll\epsilon^{-2}A_f,$$

and

$$\sup_{x'\in G}\|f-f(x')\|_{L^2(x'+\mu_V)}\leqslant\epsilon\|f\|_{L^\infty(\mu_G)}.$$

It is, however, not clear what an argument giving this might provide in the general setting. If the argument is iterative in the style of this paper then to provide an improvement in the exponent of $\log p$ in Theorem 3.1.1 one would require some way of cutting down the number of times we iterate.

4.3 Finite abelian groups

In this section we prove Theorem 4.10 which we recall now for convenience.

Theorem (Theorem 4.10)**.** *Suppose that G is a finite abelian group. Suppose that $A \subset G$ has density α and for all $V \leqslant \widehat{G}$ with $|V| \leqslant M$ we have $\{\alpha|V|\}(1 - \{\alpha|V|\}) \gg 1$. Then*

$$\|1_A\|_{A(G)} \gg \log\log\log M.$$

The proof is a combination of the work of the previous two sections with an extra ingredient. In §4.3.1 we prove the main Fourier argument and then in §4.3.2 establish some appropriate physical space estimates. These are analogues of the discrete intermediate value theorem (Proposition 4.2.5) and Lemma 4.1.8 for arbitrary finite abelian groups. However, some extra work needs to be done to ensure the stronger conditions we require in §4.3.1. This work involves a pigeonhole argument and some structural information from the geometry of numbers. In §4.3.3 we complete the proof of Theorem 4.10.

4.3.1 An iteration argument in Fourier space

The main result of this section takes physical space information about a set $A \subset G$ and converts it into Fourier information. The lemma is a sort of 'local' version of Lemma 4.1.6 with two main modifications:

- We have to assume the comparability of the local L^2-norm squared and local L^1-norm; ensuring this hypothesis is the principal extra complication of §4.3.2.

- We are less careful in our analysis because the physical space estimates available to us in the general setting are sufficiently weak as to render any more care irrelevant.

Lemma 4.3.1 (Iteration lemma)**.** *Suppose that G is a finite abelian group, $B(\Gamma,\delta)$ is a Bohr set and $B(\Gamma,\delta')$ is a regular Bohr set. Suppose that $A \subset G$ and write $f := 1_A - 1_A * \beta_{\Gamma,\delta}$. Suppose, additionally, that*

$$\|f\|_{L^2(\beta_{\Gamma,\delta'})}^2 \asymp \|f\|_{L^1(\beta_{\Gamma,\delta'})} \text{ and } \|f\|_{L^2(\beta_{\Gamma,\delta'})}^2 > 0.$$

Suppose that $\epsilon \in (0,1]$ is a parameter. Then either $\|1_A\|_{A(G)} \gg \epsilon^{-1}$ or there is a set of characters Λ and a regular Bohr set $B(\Gamma \cup \Lambda, \delta'')$ such that

$$|\Lambda| \ll \epsilon^{-2}(1 + \log \|f\|_{L^2(\beta_{\Gamma,\delta'})})^{-1} \text{ and } \delta'' \gg \delta'\epsilon^3/d^2(1 + \log \|f\|_{L^2(\beta_{\Gamma,\delta'})}^{-1}),$$

where, as usual, $d := |\Gamma|$, and

$$\sum_{\gamma \in \mathcal{N} \setminus \mathcal{O}} |\widehat{1_A}(\gamma)| \gg 1,$$

where $\mathcal{O} := \{\gamma : |1-\gamma(x)| \leqslant \epsilon \text{ for all } x \in B(\Gamma,\delta)\}$ and $\mathcal{N} := \{\gamma : |1-\gamma(x)| \leqslant \epsilon \text{ for all } x \in B(\Gamma \cup \Lambda, \delta'')\}$.

Proof. By Plancherel's Theorem we have

$$\sum_{\gamma \in \widehat{G}} \widehat{f}(\gamma)\overline{\widehat{fd\beta_{\Gamma,\delta'}}(\gamma)} = \|f\|_{L^2(\beta_{\Gamma,\delta'})}^2. \tag{4.3.1}$$

Write

$$\mathcal{L} := \{\gamma : |\widehat{fd\beta_{\Gamma,\delta'}}(\gamma)| \geqslant \epsilon\|f\|_{L^1(\beta_{\Gamma,\delta'})}\},$$

and suppose that

$$\sum_{\gamma \notin \mathcal{L}} \widehat{f}(\gamma)\overline{\widehat{fd\beta_{\Gamma,\delta'}}(\gamma)} \geqslant \|f\|_{L^2(\beta_{\Gamma,\delta'})}^2/2. \tag{4.3.2}$$

Note that

$$\|f\|_{A(G)} = \|1_A - 1_A * \beta_{\Gamma,\delta}\|_{A(G)} \leqslant \|1_A\|_{A(G)} + \|1_A * \beta_{\Gamma,\delta}\|_{A(G)} \leqslant 2\|1_A\|_{A(G)},$$

whence

$$\begin{aligned}\sum_{\gamma \notin \mathcal{L}} |\widehat{f}(\gamma)||\widehat{fd\beta_{\Gamma,\delta'}}(\gamma)| &\leqslant \epsilon\|f\|_{L^1(\beta_{\Gamma,\delta'})}\|f\|_{A(G)} \\ &\leqslant 2\epsilon\|1_A\|_{A(G)}\|f\|_{L^1(\beta_{\Gamma,\delta'})} \\ &\ll \epsilon\|1_A\|_{A(G)}\|f\|^2_{L^2(\beta_{\Gamma,\delta'})}.\end{aligned}$$

If (4.3.2) holds then the left hand side of this is at least $\|f\|^2_{L^2(\beta_{\Gamma,\delta'})}/2$ and so (dividing by $\|f\|^2_{L^2(\beta_{\Gamma,\delta'})}$) we conclude that $\|1_A\|_{A(G)} \gg \epsilon^{-1}$.

Thus we may suppose that (4.3.2) is not true and therefore, by (4.3.1), that

$$\sum_{\gamma \in \mathcal{L}} \widehat{f}(\gamma)\overline{\widehat{fd\beta_{\Gamma,\delta'}}(\gamma)} \geqslant \|f\|^2_{L^2(\beta_{\Gamma,\delta'})}/2.$$

By Proposition 2.3.3 there is a set of characters Λ and a δ'' (regular for $\Gamma \cup \Lambda$ by Proposition 2.2.2), with

$$|\Lambda| \ll \epsilon^{-2}(1 + \log\|f\|^{-2}_{L^1(\beta_{\Gamma,\delta'})}\|f\|^2_{L^2(\beta_{\Gamma,\delta'})}) \ll \epsilon^{-2}(1 + \log\|f\|^{-1}_{L^2(\beta_{\Gamma,\delta'})})$$

and

$$\delta'' \gg \delta'\epsilon^3/d^2(1 + \log\|f\|^{-2}_{L^1(\beta_{\Gamma,\delta'})}\|f\|^2_{L^2(\beta_{\Gamma,\delta'})}) \gg \delta'\epsilon^3/d^2(1 + \log\|f\|^{-1}_{L^2(\beta_{\Gamma,\delta'})}),$$

such that

$$\mathcal{L} \subset \{\gamma : |1 - \gamma(x)| \leqslant \epsilon \text{ for all } x \in B(\Gamma \cup \Lambda, \delta'')\} = \mathcal{N}.$$

Since $\mathcal{L} \subset \mathcal{N}$ we have

$$\sum_{\gamma \in \mathcal{N}} |\widehat{f}(\gamma)\widehat{fd\beta_{\Gamma,\delta'}}(\gamma)| \geqslant \|f\|^2_{L^2(\beta_{\Gamma,\delta'})}/2.$$

Now

$$|\widehat{fd\beta_{\Gamma,\delta'}}(\gamma)| \leqslant \|f\|_{L^1(\beta_{\Gamma,\delta'})} \ll \|f\|^2_{L^2(\beta_{\Gamma,\delta'})},$$

hence

$$\sum_{\gamma \in \mathcal{N}} |\widehat{f}(\gamma)| \gg 1. \tag{4.3.3}$$

Finally suppose that

$$\sum_{\gamma \in \mathcal{O}} |\widehat{f}(\gamma)| \geqslant \frac{1}{2} \sum_{\gamma \in \mathcal{N}} |\widehat{f}(\gamma)|. \tag{4.3.4}$$

By the definition of $\mathcal{O}$ we have

$$\begin{aligned} \sum_{\gamma \in \mathcal{O}} |\widehat{f}(\gamma)| &= \sum_{\gamma \in \mathcal{O}} |\widehat{1_A}(\gamma)|.|1 - \widehat{\beta_{\Gamma,\delta}}(\gamma)| \\ &\leqslant \|1_A\|_{A(G)} \sup_{\gamma \in \mathcal{O}} |1 - \widehat{\beta_{\Gamma,\delta}}(\gamma)| \leqslant \epsilon \|1_A\|_{A(G)}. \end{aligned}$$

It follows that if (4.3.4) holds then, in view of (4.3.3), $\|1_A\|_{A(G)} \gg \epsilon^{-1}$. Thus we may assume it does not and hence that

$$\sum_{\gamma \in \mathcal{N} \setminus \mathcal{O}} |\widehat{f}(\gamma)| \gg 1.$$

Noting that $|\widehat{f}(\gamma)| \leqslant 2|\widehat{1_A}(\gamma)|$ completes the proof. □

4.3.2 Physical space estimates

The objective of this section is to prove the following result.

Proposition 4.3.2. *Suppose that G is a finite abelian group and $B(\Gamma, \delta)$ is a regular Bohr set in G. Suppose that $A \subset G$ has density α and for all finite $V \leqslant \widehat{G}$ with $|V| \leqslant M$ we have $\{\alpha|V|\}(1 - \{\alpha|V|\}) \gg 1$. Then either*

$$\log M \ll d(\log \delta^{-1} + d \log d)$$

or there is an $x'' \in G$ and reals δ' and δ'', both regular for Γ, with $\delta' \leqslant \delta$,

$$\log \delta\delta'^{-1} \ll d \log d \text{ and } \log \delta''^{-1} \ll d(\log \delta^{-1} + d \log d)$$

such that

$$\|1_A - 1_A * \beta_{\Gamma,\delta'}\|^2_{L^2(x''+\beta_{\Gamma,\delta''})} \asymp \|1_A - 1_A * \beta_{\Gamma,\delta'}\|_{L^1(x''+\beta_{\Gamma,\delta''})} \tag{4.3.5}$$

and

$$\log \|1_A - 1_A * \beta_{\Gamma,\delta'}\|^{-2}_{L^2(x''+\beta_{\Gamma,\delta''})} \ll d(\log \delta^{-1} + d \log d). \tag{4.3.6}$$

Of the two parts (4.3.5) and (4.3.6) the second is the easiest to derive and comes essentially from a straightforward generalization of the physical space estimates of §4.1 and the discrete intermediate value theorem (Proposition 4.2.5). First we record an appropriate version of the intermediate value theorem.

Lemma 4.3.3 (Discrete intermediate value theorem)**.** *Suppose that G is a finite abelian group and that B is a subset of G. Suppose that $g : G \to \mathbb{R}$ has*

$$\sup_{x-y\in B} |g(x) - g(y)| \leqslant \eta. \tag{4.3.7}$$

Suppose that $x_0, x_1 \in G$ have $x_0 - x_1 \in B^{\perp\perp}$. Then for any $c \in [g(x_0), g(x_1)]$, there is an $x_2 \in G$ such that

$$|g(x_2) - c| \leqslant \frac{\eta}{2}.$$

Proof. We write H for the group, $B^{\perp\perp}$, generated by B and define

$$S^- := \{x \in x_0 + H : g(x) < c - \frac{\eta}{2}\}$$

and

$$S^+ := \{x \in x_0 + H : g(x) > c + \frac{\eta}{2}\}.$$

If the conclusion of the lemma is false then $\mathcal{S} := \{S^-, S^+\}$ is a partition of $x_0 + H$.

By the continuity hypothesis (4.3.7) we have that if $x \in S^-$ and $y \in B$

then
$$|g(x+y)-g(x)| \leqslant \eta \Rightarrow g(x+y) < c + \frac{\eta}{2}.$$
It follows that $x+y \notin S^+$ and since $\mathcal{S}$ is a partition of $x_0 + H$ we conclude that $x+y \in S^-$. We have shown that $S^- = S^- + H$.

Now $g(x_0) \leqslant c \leqslant g(x_1)$ and $\mathcal{S}$ is a partition of $x_0 + H$, whence $x_0 \in S^-$ and $x_1 \in S^+$. However $S^- = S^- + H$, whence $S^- = x_0 + H$ and so $x_1 \in S^-$. This contradicts the fact that S^- and S^+ are disjoint and so proves the lemma. □

The following is a slightly simpler proof of Lemma 4.1.8 in the general setting which gives worse (although functionally equivalent) bounds.

Lemma 4.3.4. *Suppose that G is a finite abelian group. Suppose that $f \in L^1(\mu_G)$ maps G into $[0,1]$ and that $V \leqslant \widehat{G}$ has*
$$\{\|f\|_{L^1(\mu_G)}|V|\}(1 - \{\|f\|_{L^1(\mu_G)}|V|\}) \gg 1.$$
Then there is a coset $x' + V^\perp$ with
$$f * \mu_{V^\perp}(x') \gg \mu_G(V^\perp) \text{ and } (1-f) * \mu_{V^\perp}(x') \gg \mu_G(V^\perp).$$

Proof. $f * \mu_{V^\perp}$ is constant on cosets of $V^\perp$ so we define
$$g(x) := \begin{cases} 1 & \text{if } f * \mu_{V^\perp}(x) \geqslant 1/2 \\ 0 & \text{otherwise.} \end{cases}$$
Since g is integral on cosets of $V^\perp$ there is some integer n such that
$$\int g d\mu_G = n\mu_G(V^\perp).$$

However

$$\begin{aligned} |n\mu_G(V^\perp) - \|f\|_{L^1(\mu_G)}| &= |\int g d\mu_G - \int f d\mu_G| \\ &= |\int g d\mu_G - \int f * \mu_{V^\perp} d\mu_G| \\ &\leqslant \int |g - f * \mu_{V^\perp}| d\mu_G \\ &\leqslant \sup_{x \in G} \min\{f * \mu_{V^\perp}(x), 1 - f * \mu_{V^\perp}(x)\} \\ &= \sup_{x \in G} \min\{f * \mu_{V^\perp}(x), (1-f) * \mu_{V^\perp}(x)\}. \end{aligned}$$

Now

$$\begin{aligned} |n\mu_G(V^\perp) - \|f\|_{L^1(\mu_G)}| &= \mu_G(V^\perp)|n - |V|\|f\|_{L^1(\mu_G)}| \\ &\geqslant \mu_G(V^\perp)\{\|f\|_{L^1(\mu_G)}|V|\}(1 - \{\|f\|_{L^1(\mu_G)}|V|\}) \\ &\gg \mu_G(V^\perp), \end{aligned}$$

and the conclusion of the lemma follows. □

The next lemma is the extra ingredient necessary for dealing with the general case.

Lemma 4.3.5. *Suppose that G is a finite abelian group and $B(\Gamma, \delta)$ is a Bohr set in G. Then there are reals δ' and δ'' both regular for Γ with $\delta' \leqslant \delta$,*

$$\log \delta\delta'^{-1} \ll d \log d \text{ and } \delta'' \gg \delta'/d$$

such that

$$B(\Gamma, \delta')^\perp = B(\Gamma, \delta'')^\perp$$

and

$$\|f * \beta_{\Gamma,\delta'} - f * \beta_{\Gamma,\delta'}(x)\|_{L^\infty(x+\beta_{\Gamma,\delta''})} \leqslant \|f\|_\infty/4$$

for all $x \in G$ and $f \in L^\infty(\mu_G)$.

Proof. We define a sequence $(\delta_i)_i$ iteratively and write

$$\beta_i := \beta_{\Gamma,\delta_i} \text{ and } H_i := B(\Gamma, \delta_i)^{\perp\perp}.$$

To begin with we apply Proposition 2.2.2 to get some δ_0 regular for Γ with $\delta \geqslant \delta_0 \gg \delta$. Now, if we have constructed δ_i for some $i \geqslant 0$, we apply Corollary 2.2.5 (and Proposition 2.2.2) to get a δ_{i+1} regular for Γ with $\delta_i \geqslant \delta_{i+1} \gg \delta_i/d$ and

$$\|f * \beta_i - f * \beta_i(x)\|_{L^\infty(x+\beta_{\Gamma,\delta_{i+1}})} \leqslant \|f\|_{L^\infty(\mu_G)}/4$$

for all $x \in G$ and $f \in L^\infty(\mu_G)$. We are done if we can show that there is some $i \leqslant d$ such that $H_i = H_{i+1}$. This follows by the pigeon-hole principle from the following claim.

Claim. *Suppose that $\kappa_0 \in (0,1]$. Then there is a sequence of elements $x_1, ..., x_d \in G$ such that for each $\kappa \in (\kappa_0, 1]$ there is some $0 \leqslant i \leqslant d$ such that*

$$B(\Gamma,\kappa)^{\perp\perp} = \{x_1, ..., x_i\}^{\perp\perp} + \bigcap_{\gamma\in\Gamma} \ker\gamma.$$

Proof. The proof of the claim is based on ideas from the geometry of numbers introduced to the area by Ruzsa in [Ruz96]; [GR07] contains a neat exposition. By quotienting we may assume that $\bigcap_{\gamma\in\Gamma}\ker\gamma = \{0_G\}$.

Let $\phi : G \to \mathbb{T}^d; x \mapsto (\gamma(x))_{\gamma\in\Gamma}$ and define the lattice $\mathcal{L} := \bigcup \phi(G) \leqslant \mathbb{R}^d$. Since $\bigcap_{\gamma\in\Gamma}\ker\gamma = \{0_G\}$ there is a natural homomorphism $\psi : \mathcal{L} \to G$ which takes $b \in \mathcal{L}$ to the unique $x \in G$ such that $\phi(x) = b + \mathbb{Z}^d$, with kernel $\mathbb{Z}^d$.

We write Q for the unit cube centered at the origin in $\mathbb{R}^d$ and note that $\psi(\kappa Q) = B(\Gamma,\kappa)$. We choose linearly independent vectors $b_1, ..., b_d \in \mathcal{L}$ inductively so that

$$\|b_i\|_\infty \leqslant \inf\{\lambda : \lambda Q \cap \mathcal{L} \text{ contains } i \text{ linearly independent vectors}\}.$$

Let $x_i = \psi(b_i)$. Since ψ is a homomorphism we have $B(\Gamma,\kappa)^{\perp\perp} = \psi((\kappa Q)^{\perp\perp})$, but to each $\kappa \in (0,1]$ there corresponds an $1 \leqslant i \leqslant d$ such that κQ contains at most i linearly independent vectors and κQ contains $b_1, ..., b_i$. Hence $(\kappa Q)^{\perp\perp} = \{b_1, ..., b_i\}^{\perp\perp}$. Again, the fact that ψ is a homomorphism gives the result. □

□

Proof of Proposition 4.3.2. Applying Lemma 4.3.5 we get reals $\delta' \leqslant \delta$ and δ''' both regular for Γ with

$$\log \delta\delta'^{-1} \ll d \log d \text{ and } \delta''' \gg \delta'/d$$

such that

$$B(\Gamma, \delta')^{\perp} = B(\Gamma, \delta''')^{\perp} =: V,$$

and

$$\|1_A * \beta_{\Gamma,\delta'} - 1_A * \beta_{\Gamma,\delta'}(x)\|_{L^{\infty}(x+\beta_{\Gamma,\delta'''})} \leqslant 1/4 \text{ for all } x \in G. \tag{4.3.8}$$

Now

$$|V|^{-1} = \mu_G(V^{\perp}) \geqslant \mu_G(B(\Gamma, \delta')) \geqslant (\delta')^d; \tag{4.3.9}$$

the last inequality by Lemma 2.2.1. If $M \leqslant |V|$ then we are in the first case of the lemma. Otherwise by hypothesis $\{\alpha|V|\}(1 - \{\alpha|V|\}) \gg 1$. If we put $f = 1_A * \beta_{\Gamma,\delta'}$ then $\|f\|_{L^1(\mu_G)} = \alpha$ and f maps G into $[0,1]$ whence, by Lemma 4.3.4, there is some $x''' \in G$ such that

$$1_A * \beta_{\Gamma,\delta'} * \mu_{V^{\perp}}(x''') \gg \mu_G(V^{\perp}) \text{ and } (1 - 1_A * \beta_{\Gamma,\delta'}) * \mu_{V^{\perp}}(x''') \gg \mu_G(V^{\perp}). \tag{4.3.10}$$

The argument now splits into three cases.

(i). *There are elements $x_0, x_1 \in x''' + V^{\perp}$ such that $1_A * \beta_{\Gamma,\delta'}(x_0) \geqslant 1/2$ and $1_A * \beta_{\Gamma,\delta'}(x_1) \leqslant 1/2$.* Here $x_0 - x_1 \in V^{\perp} = B(\Gamma, \delta''')^{\perp\perp}$, so by the discrete intermediate value theorem (Lemma 4.3.3) and (4.3.8) we conclude that there is some $x_2 \in x''' + V^{\perp}$ such that

$$\frac{3}{8} \leqslant 1_A * \beta_{\Gamma,\delta'}(x_2) \leqslant \frac{5}{8}.$$

Further by (4.3.8) we conclude that

$$\frac{1}{8} \leqslant 1_A * \beta_{\Gamma,\delta'}(x) \leqslant \frac{7}{8} \text{ for all } x \in x_2 + B(\Gamma, \delta''').$$

Since 1_A only takes values in $\{0,1\}$ it follows that $|1_A - 1_A * \beta_{\Gamma,\delta'}| \asymp 1$

on $x_2 + B(\Gamma, \delta''')$. Thus

$$\|1_A - 1_A * \beta_{\Gamma,\delta'}\|^2_{L^2(x_2+\beta_{\Gamma,\delta'''})} \asymp \mu_G(B(\Gamma, \delta''')),$$

and

$$\|1_A - 1_A * \beta_{\Gamma,\delta'}\|_{L^1(x_2+\beta_{\Gamma,\delta'''})} \asymp \mu_G(B(\Gamma, \delta''')).$$

The result follows on putting $\delta'' = \delta'''$; Lemma 2.2.1 then gives (4.3.6).

(ii). $1_A * \beta_{\Gamma,\delta'}(x) \leqslant 1/2$ *for all* $x \in x''' + V^\perp$. Suppose that $\delta'' \leqslant \delta'$. Then $B(\Gamma, \delta'') \subset B(\Gamma, \delta')$ so we have $B(\Gamma, \delta'')^{\perp\perp} \subset B(\Gamma, \delta')^{\perp\perp}$, whence $\beta'_{\Gamma,\delta'} * \mu_{V^\perp} = \mu_{V^\perp} = \beta_{\Gamma,\delta'} * \mu_{V^\perp}$. Thus we define

$$\alpha' := 1_A * \beta_{\Gamma,\delta'} * \mu_{V^\perp}(x''') = 1_A * \beta'_{\Gamma,\delta'} * \mu_{V^\perp}(x'''),$$

which has

$$\alpha' \gg \mu_G(V^\perp) \geqslant (\delta')^d)^d > 0$$

by (4.3.10) and (4.3.9). By Corollary 2.2.5 we can pick a δ'' (regular for Γ by Proposition 2.2.2) with $\delta' \geqslant \delta'' \gg \delta'\alpha'/d$ such that

$$\|1_A - 1_A * \beta_{\Gamma,\delta'}(x)\|_{L^\infty(x+\beta_{\Gamma,\delta''})} \leqslant \alpha' \text{ for all } x \in G. \qquad (4.3.11)$$

We write

$$L := \{x \in x''' + V^\perp : 1_A * \beta'_{\Gamma,\delta'}(x) \geqslant \alpha'/2\}$$

and note that

$$\int_{x \notin L} 1_A * \beta'_{\Gamma,\delta'}(x) d\mu_{V^\perp}(x''' - x) \leqslant \sup_{x \notin L} 1_A * \beta'_{\Gamma,\delta'}(x) \leqslant \alpha'/2,$$

so

$$\int_{x \in L} 1_A * \beta'_{\Gamma,\delta'}(x) d\mu_{V^\perp}(x''' - x) \geqslant \alpha'/2.$$

If $1_A * \beta'_{\Gamma,\delta'}(x) \neq 0$ then $1_A * \beta_{\Gamma,\delta'}(x) \neq 0$, whence

$$\begin{aligned} \alpha'/2 &\leqslant \int_{x \in L} 1_A * \beta_{\Gamma,\delta'}(x) \frac{1_A * \beta'_{\Gamma,\delta'}(x)}{1_A * \beta_{\Gamma,\delta'}(x)} d\mu_{V^\perp}(x''' - x) \\ &\leqslant \alpha' \sup_{x \in L} \frac{1_A * \beta'_{\Gamma,\delta'}(x)}{1_A * \beta_{\Gamma,\delta'}(x)}, \end{aligned}$$

Dividing by α' (which we have previously observed is positive) we conclude that there is some $x'' \in L$ such that

$$1_A * \beta'_{\Gamma,\delta'}(x'') \geqslant 1_A * \beta_{\Gamma,\delta'}(x'')/4.$$

If $x \in A \cap (x'' + B(\Gamma, \delta''))$ then $|1_A(x) - 1_A * \beta_{\Gamma,\delta'}(x)| \asymp 1$ since $1_A * \beta_{\Gamma,\delta'}(x) \leqslant 1/2$ by the hypothesis of this case. If $x \in A^c \cap (x'' + B(\Gamma, \delta''))$ then

$$|1_A(x) - 1_A * \beta_{\Gamma,\delta'}(x)| \leqslant |1_A * \beta_{\Gamma,\delta'}(x)| \leqslant 1_A * \beta_{\Gamma,\delta'}(x'') + O(\alpha') = O(\alpha'),$$

where the second inequality is a result of (4.3.11). It follows that

$$\|1_A - 1_A * \beta_{\Gamma,\delta'}\|_{L^1(x'' + \beta_{\Gamma,\delta''})} \gg 1_A * \beta_{\Gamma,\delta''}(x''),$$

and

$$\begin{aligned} \|1_A - 1_A * \beta_{\Gamma,\delta'}\|_{L^1(x'' + \beta_{\Gamma,\delta''})} &\leqslant O(1_A * \beta_{\Gamma,\delta''}(x'')) + O(\alpha') \\ &= O(1_A * \beta_{\Gamma,\delta''}(x'')) \end{aligned}$$

since $1_A * \beta_{\Gamma,\delta''}(x'') \gg \alpha'$ since $x'' \in L$. Similarly we have

$$\|1_A - 1_A * \beta_{\Gamma,\delta'}\|^2_{L^2(x'' + \beta_{\Gamma,\delta''})} \gg 1_A * \beta_{\Gamma,\delta''}(x''),$$

and

$$\begin{aligned} \|1_A - 1_A * \beta_{\Gamma,\delta'}\|^2_{L^2(x'' + \beta_{\Gamma,\delta''})} &\leqslant O(1_A * \beta_{\Gamma,\delta''}(x'')) + O(\alpha') \\ &= O(1_A * \beta_{\Gamma,\delta''}(x'')). \end{aligned}$$

It follows that

$$\|1_A - 1_A * \beta_{\Gamma,\delta'}\|_{L^1(x''+\beta_{\Gamma,\delta''})} \asymp \|1_A - 1_A * \beta_{\Gamma,\delta'}\|^2_{L^2(x''+\beta_{\Gamma,\delta''})},$$

and

$$\|1_A - 1_A * \beta_{\Gamma,\delta'}\|^2_{L^2(x''+\beta_{\Gamma,\delta''})} \gg \alpha'.$$

(iii). $1_A * \beta_{\Gamma,\delta'}(x) \geqslant 1/2$ *for all* $x \in x''' + V^\perp$. This follows by replacing A by A^c in the previous case.

The proof is complete. □

4.3.3 Proof of Theorem 4.10

Proof of Theorem 4.10. In what follows it is convenient to let $C > 0$ denote an absolute constant which may vary from instance to instance.

Fix $\epsilon \in (0, 1]$ to be optimized later. We define three sequences $(\delta_k)_k$, $(\delta'_k)_k$ and $(\delta''_k)_k$ of reals, one sequence $(x_k)_k$ of elements of G, and one sequence $(\Gamma_k)_k$ of sets of characters inductively. We write

$$\beta_k := \beta_{\Gamma_k,\delta_k},\ \beta'_k := \beta_{\Gamma_k,\delta'_k} \text{ and } \beta''_k := \beta_{\Gamma_k,\delta''_k},$$

as well as $d_k := |\Gamma_k|$ and

$$\mathcal{L}_k := \{\gamma : |1 - \gamma(x)| \leqslant \epsilon \text{ for all } x \in B(\Gamma_k, \delta_k)\}.$$

We shall ensure the following properties.

(i). $B(\Gamma_k, \delta_k)$, $B(\Gamma_k, \delta'_k)$ and $B(\Gamma_k, \delta''_k)$ are regular;

(ii).
$$\|1_A - 1_A * \beta_k\|^2_{L^2(x_k+\beta_{\Gamma_k,\delta'_k})} \asymp \|1_A - 1_A * \beta'_k\|_{L^1(x_k+\beta_{\Gamma_k,\delta''_k})};$$

(iii).
$$\|1_A - 1_A * \beta'_k\|^2_{L^2(x_k+\beta_{\Gamma_k,\delta''_k})} \gg \delta_k^{d_k}/(Cd_k)^{d_k^2};$$

(iv).
$$\delta_k \geqslant \delta'_k \gg \delta_k/(Cd_k)^{d_k} \text{ and } \delta_k \geqslant \delta''_k \gg \delta_k^{d_k+1}/(Cd_k)^{d_k^2+d_k+1};$$

(v).
$$d_{k+1} \ll \epsilon^{-2} d_k(\log \delta_k^{-1} + d_k \log d_k);$$

(vi).
$$\delta_k \geqslant \delta_{k+1} \gg \delta_k^{d_k+1}\epsilon^4/(Cd_k)^{d_k^2+d_k+6}\log \delta_k^{-1};$$

(vii).
$$\sum_{\gamma \in \mathcal{L}_{k+1}\setminus\mathcal{L}_k} |\widehat{1_A}(\gamma)| \gg 1.$$

We initialize the iteration with $\Gamma_0 = \{0_{\widehat{G}}\}$. Pick $\delta_0 \gg 1$ regular for Γ_0 by Proposition 2.2.2. Apply Proposition 4.3.2 (assuming that we have $\delta_0^{d_0}(Cd_0)^{d_0^2} < M$) to get x_0 δ'_0 and δ''_0 satisfying properties (i),(ii),(iii) and (iv). By translating A by $-x_0$, if necessary, we can apply Lemma 4.3.1 (assuming that we do not have $\|1_A\|_{A(G)} \gg \epsilon^{-1}$) to get Γ_1 and δ_1 such that properties (v), (vi) and (vii) are satisfied.

Given Γ_k and δ_k we can proceed as we just have (assuming that we have $\delta_k^{d_k}(Cd_k)^{d_k^2} < M$) to generate x_k, δ'_k, δ''_k, δ_{k+1} and Γ_{k+1}.

By property (vii) (and the leftmost inequality in (vi)) we have $\|1_A\|_{A(G)} \gg k$, so either $\|1_A\|_{A(G)} \gg \epsilon^{-1}$, or the iteration terminates with $k \ll \epsilon^{-1}$.

(v) and (vi) imply

$$d_{k+1} \ll \epsilon^{-2} d_k \log \delta_k^{-1} \text{ and } \log \delta_{k+1}^{-1} \ll d_k \log \delta_k^{-1} + \log \epsilon^{-1},$$

whence

$$d_{k+1} \ll \epsilon^{-2} d_k \log \delta_k^{-1} \text{ and } \epsilon^{-2} \log \delta_{k+1}^{-1} \ll \epsilon^{-2} d_k \log \delta_k^{-1}.$$

It follows that $d_{k+1} \ll d_k^2$ and so $d_k \leqslant 2^{2^{Ck}}$ and $\delta_k \geqslant 2^{2^{2^{Ck}}}$. For the iteration to terminate we must have $M \leqslant \delta_k^{d_k}(Cd_k)^{d_k^2}$; for this to happen for some $k \ll \epsilon^{-1}$ we need $\exp(\exp(\exp(C\epsilon^{-1}))) \geqslant M$. The result follows. □

4.4 A quantitative version of the idempotent theorem

In this section we shall prove Theorem 4.12 which we recall now for convenience. This work is from the joint paper [GS08b] of Green and the author.

Theorem (Theorem 4.12)**.** *Suppose that $A \subset G$. Then there is an integer $L \leqslant \exp(\exp(O(1 + \|1_A\|_{A(G)})^4))$ such that*

$$1_A = \sum_{j=1}^{L} \sigma_j 1_{x_j + H_j}$$

where $\sigma_j \in \{-1, 1\}$, $x_j \in G$ and $H_j \leqslant G$ for each $j \in \{1, ..., L\}$.

In our arguments we are, in fact, forced to work with a wider class of functions than simply boolean functions; we consider all functions which only take values close to integers. Suppose that $f : G \to \mathbb{R}$. We write $f_{\mathbb{Z}}$ for the function $G \to \mathbb{Z}$ defined by

$$f_{\mathbb{Z}}(x) := \begin{cases} \lceil f(x) \rceil & \text{if } \lceil f(x) \rceil - f(x) \leqslant 1/2 \\ \lfloor f(x) \rfloor & \text{otherwise.} \end{cases}$$

We say that f is ϵ-almost integer valued if $\|f - f_{\mathbb{Z}}\|_{L^\infty(\mu_G)} \leqslant \epsilon$. In words this just means that $f(x)$ is always within ϵ of an integer.

It turns out that what is important in Theorem 4.12 is that we can partition the codomain of 1_A into well separated sets. In general if we have a function $f \in A(G)$ which is ϵ-almost integer valued for sufficiently small ϵ, then we can describe the structure of the sets

$$L_z := \{x \in G : |f(x) - z| \leqslant \epsilon\} = \{x \in G : f_{\mathbb{Z}}(x) = z\}$$

for any $z \in \mathbb{Z}$. By and large they will be empty, but they will always be elements of the coset ring. The following theorem is a precise statement of this and yields Theorem 4.12 immediately.

Theorem 4.4.1. *There is an absolute constant $C > 0$ such that if $f \in A(G)$ has real range and is ϵ-almost integer valued for some $\epsilon \leqslant \exp(-C(1 + \|f\|_{A(G)})^4)$, then there is an integer $L \leqslant \exp(\exp(O(1+\|f\|_{A(G)})^4))$ such that*

$$f_{\mathbb{Z}} = \sum_{j=1}^{L} \sigma_j 1_{x_j+H_j},$$

where $\sigma_j \in \{-1, 1\}$, $x_j \in G$ and $H_j \leqslant G$ for each $j \in \{1, ..., L\}$.

The proof involves a number of the techniques which we have developed already. First, in §4.4.1, we introduce the notion of arithmetic connectedness and combine it with some of the work of §3.2 to show how arithmetic connectedness implies large inner product with a Bourgain system. In §4.4.2 we show how we can pass from information about the algebra norm to the arithmetic connectedness condition, before proving a quantitative continuity result in §4.4.3. We conclude by showing that combining these sections leads to concentration on a coset and hence prove the theorem inductively. §4.4.5 includes this proof and some concluding remarks are presented in §4.4.6.

4.4.1 Arithmetic connectedness

In his, by now, well-known work on Szemerédi's theorem Gowers ([Gow98]) introduced the following strong quantitative version of the Balog-Szemerédi theorem.

Proposition 4.4.2. (Balog-Szemerédi-Gowers Theorem [Gow98, Proposition 12]). *Suppose that A is a subset of G with at least $\delta|A|^3$ quadruples $(a_1, a_2, a_3, a_4) \in A^4$ such that $a_1 + a_2 = a_3 + a_4$. Then there is a set $A' \subset A$ with $|A'| \geqslant \delta^{O(1)}|A|$ such that $|A' + A'| \leqslant \delta^{O(1)}|A'|$.*

Combining this with Proposition 3.2.2 immediately yields the following result.

Proposition 4.4.3. *Suppose that A is a subset of G with at least $\delta|A|^3$ quadruples $(a_1, a_2, a_3, a_4) \in A^4$ such that $a_1 + a_2 = a_3 + a_4$. Then there is a* *regular Bourgain system* $\mathcal{B}$ *of dimension* $O(\delta^{-O(1)})$ *with*

$$|B_1| \geqslant \exp(-O(\delta^{-O(1)}))|A| \text{ and } \|1_A * \beta_1\|_{L^\infty(\mu_G)} \gg \delta^{O(1)}.$$

Recall that we call a quadruple $(x_1, x_2, x_3, x_4) \in G^4$ an additive quadruple if $x_1 + x_2 = x_3 + x_4$.

To leverage this result we have to convert control of the algebra norm into bounds on the number of additive quadruples; doing this involves the introduction of the concept of 'arithmetic connectedness'.

Definition (Arithmetic connectedness)**.** Suppose A is a subset of G with $0 \notin A$ and m is a natural number. We say that A is m-arithmetically connected if, for any set $A' \subset A$ with $|A'| = m$ we have either

(i). A' is not dissociated or

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

A typical example of an arithmetically connected set is a union of a few cosets. Indeed, the next proposition shows that if A is arithmetically connected then it intersects a large Bourgain system.

The reason for the definition, however, only becomes apparent in the proof of Proposition 4.4.6. Suppose that $A \subset G$ and $\|1_A\|_{A(G)} \leqslant M$. Then it is easy to deduce from Hölder's Inequality and Parseval's Theorem that A contains at least $|A|^3/M^2$ additive quadruples. Hence by Proposition 4.4.3 A intersects a large Bourgain system. However, as we have already noted we can't simply deal with sets, we have to deal with the more general almost integer valued functions. Doing so naturally leads to the concept of arithmetic connectedness in the proof of Proposition 4.4.6.

Proposition 4.4.4. *Suppose* A *is an* m*-arithmetically connected subset of* G *and* m *is a natural number. Then there is a regular Bourgain system* $\mathcal{B}$ *of dimension* $\exp(O(m))$ *and with*

$$\mu_G(\mathcal{B}) \geqslant \exp(-\exp(O(m)))\mu_G(A) \text{ and } \|1_A * \beta_1\|_{L^\infty(\mu_G)} \geqslant \exp(-O(m)).$$

Proof. By Proposition 4.4.3, it suffices to prove that an m-arithmetically connected set A has at least $\exp(-O(m))|A|^3$ additive quadruples. If $|A| < m^2$ this result is trivial, so we may assume 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 elements $a_1, ..., a_m$ are not dissociated, or else there is a further $a' \in A$ such that a' lies in the span of the a_is. In either situation there is some non-trivial 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

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

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

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

has at least $(6m^2)^{-1}3^{-m}|A|^{r_1+r_2-1} \geqslant \exp(-O(m))|A|^{r_1+r_2-1}$ solutions with $x_1, ..., x_{r_1}, y_1, ..., y_{r_2} \in A$.

We may deduce directly from this the claim that there are at least $\exp(-O(m))|A|^3$ additive quadruples in A. To do this observe that what we have shown may be recast in the form

$$1_A * ... * 1_A * 1_{-A} * ... * 1_{-A}(0) \geqslant \exp(-O(m))\|1_A\|_{L^1(\mu_G)}^{r_1+r_2-1},$$

where there are r_1 copies of 1_A and r_2 copies of 1_{-A}.

Applying the inversion formula gives

$$\|\widehat{1}_A\|_{\ell^{r_1+r_2}(\widehat{G})}^{r_1+r_2} \geqslant \sum_{\gamma\in\widehat{G}} \widehat{1}_A(\gamma)^{r_1}\widehat{1}_A(\overline{\gamma})^{r_2} \geqslant \exp(-O(m))\|1_A\|_{L^1(\mu_G)}^{r_1+r_2-1}.$$

By Hölder's inequality this implies that

$$\|\widehat{1}_A\|_{\ell^4(\widehat{G})}^{2}\|\widehat{1}_A\|_{\ell^{2r_1+2r_2-4}(\widehat{G})}^{r_1+r_2-2} \geqslant \exp(-O(m))\|1_A\|_{L^1(\mu_G)}^{r_1+r_2-1}. \tag{4.4.1}$$

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

$$\|\widehat{1}_A\|_{\ell^{2k}(\widehat{G})} \leqslant \|1_A\|_{L^1(\mu_G)}^{1-1/2k}.$$

Setting $k = r_1 + r_2 - 2$ and substituting into (4.4.1), we immediately obtain

$$\|\widehat{1}_A\|_{\ell^4(\widehat{G})}^{4} \geqslant \exp(-O(m))\|1_A\|_{L^1(\mu_G)}^{3},$$

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

4.4.2 Concentration on a Bourgain system

We now combine the previous two sections to produce a concentration of mass on a Bourgain system.

Proposition 4.4.5. *Suppose that $f \in A(G)$ is $\exp(-2^5(1+\|f\|_{A(G)})^4)$-almost integer valued and has real range. Then there is a regular Bourgain system $\mathcal{B}$ of dimension $\exp(O(1 + \|f\|_{A(G)})^4)$ with*

$$\mu_G(\mathcal{B}) \geqslant \exp(-\exp(O(1 + \|f\|_{A(G)})^4))\|f_{\mathbb{Z}}\|_{L^1(\mu_G)}$$

such that

$$\|f * \beta_1\|_{L^\infty(\mu_G)} \geqslant \exp(-O(1 + \|f\|_{A(G)})^4).$$

The proof of this splits into two parts. It is easier to prove the result with the additional assumption that f is non-negative, so to begin with we prove the following proposition. A technical lemma will then complete the argument.

Proposition 4.4.6. *Suppose that $f \in A(G)$ has $f \geqslant 0$ and $\|f - f_{\mathbb{Z}}\|_{L^\infty(\mu_G)} \leqslant \exp(-2^4(1+\|f\|_{A(G)})^2)$. Then there is a regular Bourgain system $\mathcal{B}$ of dimension $\exp(O(1+\|f\|_{A(G)})^2)$ with*

$$\mu_G(\mathcal{B}) \geqslant \exp(-\exp(O(1+\|f\|_{A(G)})^2))\|f_{\mathbb{Z}}\|_{L^1(\mu_G)}$$

and

$$\|f * \beta_1\|_{L^\infty(\mu_G)} \geqslant \exp(-O(1+\|f\|_{A(G)})^2).$$

Proof. Write $A := \operatorname{supp}(f_{\mathbb{Z}})$, and $m := \lceil 13(1+\|f\|_{A(G)})^2\rceil$. If $A = G$ we take $\mathcal{B}$ to be the regular Bourgain system with all balls equal to G and the result is trivial since

$$f(x) \geqslant 1 - \exp(-2^4) \geqslant 1/2 \text{ for all } x \in G.$$

Otherwise, by subjecting f to a suitable translation, we may assume that $0 \notin A$. We claim that A is m-arithmetically connected. If this is not the case then there are dissociated elements $a_1, ..., a_m \in A$ such that there is no further $x \in A$ lying in the span $\langle a_1, ..., a_m\rangle$. Consider the function $p(x)$ defined in terms of its Fourier transform by

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

Note that $\widehat{p}$ is a Riesz product and, recalling §2.1.3 if necessary, we see that $\|p\|_{A(G)} = 1$ and $\operatorname{supp} p \subset \langle a_1, ..., a_m\rangle$. Thus we have

$$\|fp\|_{A(G)} \leqslant \|f\|_{A(G)}\|p\|_{A(G)} = \|f\|_{A(G)}$$

and

$$\begin{aligned}\|(f-f_{\mathbb{Z}})p\|_{A(G)} &\leqslant \sum_{x\in\langle a_1,\ldots,a_m\rangle}\|(f-f_{\mathbb{Z}})p1_{\{x\}}\|_{A(G)}\\ &\leqslant 3^m\|f-f_{\mathbb{Z}}\|_{L^\infty(\mu_G)}\leqslant 1.\end{aligned}$$

It follows, by the triangle inequality, that $\|f_{\mathbb{Z}}p\|_{A(G)}\leqslant 1+\|f\|_{A(G)}$. Now since $A\cap\langle a_1,...,a_m\rangle=\langle a_1,...,a_m\rangle$ we have

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

Again recalling from §2.1.3 if necessary we have

$$p(a_i)=\sum_{m':m'.\{a_1,\ldots,a_m\}=a_i}2^{-|m'|}\geqslant\frac{1}{2},$$

so

$$\|\widehat{f_{\mathbb{Z}}p}\|^2_{\ell^2(\widehat{G})}=\|f_{\mathbb{Z}}p\|^2_{L^2(\mu_G)}\geqslant\frac{1}{4|G|}\sum_{i=1}^m|f_{\mathbb{Z}}(a_i)|^2\geqslant\frac{m}{4|G|}$$

and

$$\begin{aligned}\|\widehat{f_{\mathbb{Z}}p}\|^4_{\ell^4(\widehat{G})} &= \frac{1}{|G|^3}\sum_{\substack{i_1,i_2,i_3,i_4\\ a_{i_1}+a_{i_2}=a_{i_3}+a_{i_4}}}\prod_{j=1}^4 f_{\mathbb{Z}}(a_{i_j})p(a_{i_j})\\ &\leqslant \frac{3}{|G|^3}\big(\sum_{i=1}^m|f_{\mathbb{Z}}(a_i)p(a_i)|^2\big)^2\leqslant\frac{3}{|G|}\|\widehat{f_{\mathbb{Z}}p}\|^4_{\ell^2(\widehat{G})},\end{aligned}$$

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

$$\|f_{\mathbb{Z}}p\|_{A(G)}\geqslant\frac{\|\widehat{f_{\mathbb{Z}}p}\|^3_{\ell^2(\widehat{G})}}{\|\widehat{f_{\mathbb{Z}}p}\|^2_{\ell^4(\widehat{G})}}\geqslant\sqrt{\frac{|G|}{3}}\|\widehat{f_{\mathbb{Z}}p}\|_{\ell^2(\widehat{G})}\geqslant\sqrt{\frac{m}{12}}.$$

Recalling our choice of m, we see that this contradicts the upper bound

$\|f_{\mathbb{Z}}p\|_{A(G)} \leqslant 1 + \|f\|_{A(G)}$ we obtained earlier.

This proves our claim that A is $\lceil 13(1 + \|f\|_{A(G)})^2 \rceil$ -arithmetically connected. It follows from Proposition 4.4.4 that there is a regular Bourgain system $\mathcal{B}$ of dimension $\exp(O(1 + \|f\|_{A(G)})^2)$ with

$$\mu_G(\mathcal{B}) \geqslant \exp(-\exp(O(1 + \|f\|_{A(G)})^2))\mu_G(A)$$

and

$$\|1_A * \beta_1\|_{L^\infty(\mu_G)} \geqslant \exp(-O(1 + \|f\|_{A(G)})^2).$$

Since $\|f\|_{L^\infty(\mu_G)} \leqslant \|f\|_{A(G)}$ and $A = \mathrm{supp}(f)_{\mathbb{Z}}$ we get

$$\mu_G(\mathcal{B}) \geqslant \exp(-\exp(O(1 + \|f\|_{A(G)})^2))\|f_{\mathbb{Z}}\|_{L^1(\mu_G)},$$

and non-negativity of f yields

$$\|f * \beta_1\|_{L^\infty(\mu_G)} \geqslant \exp(-O(1 + \|f\|_{A(G)})^2).$$

□

The following technical lemma is essentially a standard L^∞-density increment argument in disguise.

Lemma 4.4.7. *Suppose that $\mathcal{B}$ is a regular Bourgain system of dimension d and $f \in A(G)$ has $\|f\|_{L^2(\beta_1)} \geqslant \eta$. Then there is a regular Bourgain system $\mathcal{B}'$ of dimension $d' \leqslant 2d + 4$ with*

$$\mu_G(\mathcal{B}') \geqslant \left(\frac{\eta^2}{2(1 + \|f\|_{A(G)})}\right)^{O(d)} \mu_G(\mathcal{B})$$

and

$$\|f * \beta'_1\|_{L^\infty(\mu_G)} \gg \eta^2/\|f\|_{A(G)}.$$

Proof. We can apply Plancherel's Theorem to get

$$\sum_{\gamma \in \widehat{G}} \widehat{f}(\gamma)\overline{\widehat{fd\beta_1}(\gamma)} = \|f\|^2_{L^2(\beta_1)} = \eta^2.$$

The triangle inequality then tells us that

$$\sup_{\gamma \in \widehat{G}} \left| \int f(y)\gamma(y) d\beta_1(y) \right| = \sup_{\gamma \in \widehat{G}} |\widehat{fd\beta_1}(\gamma)| \geqslant \eta^2/\|f\|_{A(G)}.$$

Let $\gamma'' \in \widehat{G}$ be a character for which the leftmost maximum is attained. Now

$$|1-\gamma''(x)| \leqslant \sqrt{2(1-\cos(4\pi\gamma''(x)))} \leqslant 4\pi\|\gamma''(x)\|.$$

Thus if $\rho_0 = \eta^2/12\pi(1+\|f\|_{A(G)})^2$, then

$$|1-\gamma''(x)| \leqslant \eta^2/3(1+\|f\|_{A(G)})^2 \text{ for all } x \in B(\{\gamma''\}, \rho_0).$$

Pick ρ_1 with

$$\rho_1 \asymp \eta^2/d(1+\|f\|_{A(G)})^2,$$

so that

$$\|(x+\beta_1)-\beta_1\| \leqslant \eta^2/3(1+\|f\|_{A(G)})^2 \text{ for all } x \in B_{\rho_1},$$

by Lemma 2.4.6. Pick $\lambda \in [1/2, 1)$ such that $\mathcal{B}' = \lambda(\rho_1\mathcal{B} \cap (B(\{\gamma''\}, \rho_0\delta))_\delta)$ is regular by Proposition 2.4.5. Now

$$|1-\gamma''(x)| \leqslant \eta^2/3(1+\|f\|_{A(G)})^2 \text{ for all } x \in B_1',$$

and

$$\|\beta_1 * \beta_1' - \beta_1\| \leqslant \eta^2/3(1+\|f\|_{A(G)})^2,$$

by Lemma 2.4.6. In view of this last bound and the fact $\|f\|_{L^\infty(\mu_G)} \leqslant \|f\|_{A(G)}$ we have

$$\begin{aligned} \left| \int f(u+x)\gamma''(u)d\beta_1'(u)\gamma''(x)d\beta_1(x) \right| &= \left| \int f(y)\gamma''(y)d\beta_1 * \beta_1'(y) \right| \\ &\geqslant 2\eta^2/3\|f\|_{A(G)}, \end{aligned}$$

by the triangle inequality. The first (again with $\|f\|_{L^\infty(\mu_G)} \leqslant \|f\|_{A(G)}$) yields

$$|\int f(u+x)d\beta_1'(u)\gamma''(x)d\beta_1(x)| \geqslant \eta^2/3\|f\|_{A(G)}.$$

This leads to the conclusion of the lemma; Lemma 2.4.4 yields the appropriate bounds. □

Proof of Proposition 4.4.5. Note that $\|f^2\|_{A(G)} \leqslant \|f\|_{A(G)}^2$, and

$$\|f^2 - f_{\mathbb{Z}}^2\|_{L^\infty(\mu_G)} \leqslant (2\|f\|_{A(G)} + 1)\|f - f_{\mathbb{Z}}\|_{L^\infty(\mu_G)} \leqslant \exp(-2^4(1 + \|f^2\|_{A(G)})).$$

It follows that we may apply Proposition 4.4.6 to get a regular Bourgain system $\mathcal{B}'$ of dimension $\exp(O(1 + \|f\|_{A(G)})^4)$ such that

$$\mu_G(\mathcal{B}') \geqslant \exp(-\exp(O(1 + \|f\|_{A(G)})^4))\|f_{\mathbb{Z}}^2\|_{L^1(\mu_G)}$$

and

$$\|f^2 * \beta_1'\|_{L^\infty(\mu_G)} \geqslant \exp(-O(1 + \|f\|_{A(G)})^4).$$

Now by translation we way assume that the maximum on the left is attained at $x = 0_G$, and hence apply Lemma 4.4.7 to conclude that there is a regular Bourgain system with the required properties. □

4.4.3 Continuity relative to a Bourgain system

The main result of this section states that if we are given a Bourgain system $\mathcal{B}$ and a function f then we can refine it to a system $\mathcal{B}'$ on which f is 'quantitatively continuous' in the sense of §4.2. The specific dependencies of the result are rather unimportant and could be improved by including the techniques of §4.2.

Proposition 4.4.8. *Suppose that $\mathcal{B}$ is a regular Bourgain system of dimension d. Suppose that $f \in A(G)$ and $\epsilon \in (0, 1]$ is a parameter. Then there is a regular Bourgain system $\mathcal{B}'$ of dimension $d' \leqslant d + O(\epsilon^{-1}(1 + \|f\|_{A(G)}))^2$ with*

$$\mu_G(\mathcal{B}') \geqslant \exp(-O(\epsilon^{-5}(1 + \|f\|_{A(G)})^5 d\log(1 + d)))\mu_G(\mathcal{B})$$

and a $\rho \gg \epsilon/d(1+\|f\|_{A(G)})$ *such that*

$$\sup_{x\in G}\|f*\beta_1 - f*\beta_1(x)\|_{L^\infty(x+\beta_\rho)} \leqslant \epsilon$$

and

$$\sup_{x\in G}\|f - f*\beta_1\|_{L^2(x+\beta_\rho)} \leqslant \epsilon.$$

The proof is an iteration of the following lemma.

Lemma 4.4.9 (Iteration lemma)**.** *Suppose that* G *is a finite abelian group and* $\mathcal{B}$ *is a Bourgain system of dimension* d*. Suppose that* $f \in A(G)$ *and* $\epsilon \in (0,1]$ *is a parameter. Then at least one of the following is true.*

(i). (f is close to a continuous function) *There is a* $\rho \gg \epsilon/d(1+\|f\|_{A(G)})$ *such that*

$$\sup_{x\in G}\|f*\beta_1 - f*\beta_1(x)\|_{L^\infty(x+\beta_\rho)} \leqslant \epsilon$$

and

$$\sup_{x\in G}\|f - f*\beta_1\|_{L^2(x+\beta_\rho)} \leqslant \epsilon.$$

(ii). There is a $\rho' \gg \epsilon^5/d^2(1+\|f\|_{A(G)})^5$ *and a Bourgain system* $\mathcal{B}'$ *of dimension* 2 *with* $\mathcal{B}' \cap (\rho'\mathcal{B})$ *regular and*

$$\mu_G(\mathcal{B}') \gg \epsilon^2/(1+\|f\|_{A(G)})^2,$$

such that

$$\sum_{\gamma\in\mathcal{L}} |1-\widehat{\beta_1}(\gamma)||\widehat{f}(\gamma)| \geqslant \epsilon^2/4\|f\|_{A(G)}$$

where

$$\mathcal{L} := \{\gamma : |1-\gamma(x)| \leqslant \epsilon^2/8(1+\|f\|_{A(G)})^2 \textit{ for all } x \in B'_1 \cap B_{\rho'}\}.$$

Proof. Apply Corollary 2.4.7 and Proposition 2.4.5 to pick $\rho \gg \epsilon/d(1+\|f\|_{A(G)})$ so that $\rho\mathcal{B}$ is regular and

$$\sup_{x\in G}\|f*\beta_1 - f*\beta_1(x)\|_{L^\infty(x+\beta_\rho)} \leqslant \epsilon.$$

Either we are in the first case of the lemma or we may assume that there is some $x \in G$ (without loss of generality equal to 0_G) such that

$$\|f - f * \beta_1\|_{L^2(x+\beta_\rho)} > \epsilon.$$

Squaring both sides and applying Plancherel's Theorem we get

$$\begin{aligned}
\epsilon^2 &< \|f - f * \beta_1\|^2_{L^2(x+\beta_\rho)} \\
&= \sum_{\gamma \in \widehat{G}} (f - f * \beta_1)^\wedge(\gamma)\overline{((f - f * \beta_1)d\beta_\rho)^\wedge(\gamma)} \\
&\leqslant 2\|f\|_{A(G)} \sup_{\gamma \in \widehat{G}} |((f - f * \beta_1)d\beta_\rho)^\wedge(\gamma)|,
\end{aligned}$$

by the triangle inequality and the fact that

$$\|f - f * \beta_1\|_{A(G)} \leqslant \|f\|_{A(G)} + \|f * \beta_1\|_{A(G)} \leqslant 2\|f\|_{A(G)}.$$

Rearranging we get

$$\sup_{\gamma \in \widehat{G}} |((f - f * \beta_1)d\beta_\rho)^\wedge(\gamma)| \geqslant \epsilon^2/2\|f\|_{A(G)};$$

fix a γ'' for which this maximum is attained and we get

$$\sum_{\gamma' \in \widehat{G}} |(f - f * \beta_1)^\wedge(\gamma')||\widehat{\beta_\rho}(\gamma'' - \gamma')| \geqslant \epsilon^2/2\|f\|_{A(G)}.$$

Write $\mathcal{L}' := \{\gamma \in \widehat{G} : |\widehat{\beta_\rho}(\gamma)| \geqslant \epsilon^2/8\|f\|^2_{A(G)}\}$, and note by the triangle inequality that

$$\sum_{\gamma' \notin \gamma'' + \mathcal{L}'} |(f - f * \beta_1)^\wedge(\gamma')||\widehat{\beta_\rho}(\gamma'' - \gamma')| \leqslant \epsilon^2/4\|f\|_{A(G)}.$$

It follows that

$$\sum_{\gamma' \in \gamma'' + \mathcal{L}'} |(f - f * \beta_1)^\wedge(\gamma')| \geqslant \epsilon^2/4\|f\|_{A(G)}.$$

Set $\eta = \epsilon^2/8(1+\|f\|_{A(G)})^2$. Since

$$|1-\gamma(x)| = \sqrt{2(1-\cos(4\pi\|\gamma(x)\|))} \leqslant 4\pi\|\gamma(x)\|$$

we have

$$\{\gamma''\} \subset \{\gamma \in \widehat{G} : |1-\gamma(x)| \leqslant \eta/2 \text{ for all } x \in B(\{\gamma''\}, \eta/8\pi)\}.$$

Furthermore by Lemma 2.4.8 there is a $\kappa \gg \epsilon^2/d(1+\|f\|_{A(G)})^2$ such that

$$\mathcal{L}' \subset \{\gamma \in \widehat{G} : |1-\gamma(x)| \leqslant \eta/2 \text{ for all } x \in B_{\rho\kappa\eta}\}.$$

Pick $\lambda \in [1/2, 1)$ such that $\mathcal{B}'' := \lambda(\rho\kappa\eta\mathcal{B} \cap (B(\{\gamma''\}, \delta\eta/8\pi))_\delta)$ is regular. Now set $\rho' := \lambda\rho\kappa\eta$ and $\mathcal{B}' := (B(\{\gamma''\}, \lambda\delta\eta/8\pi))_\delta$. The result follows since $\mu_G((B(\{\gamma\}, \lambda\delta\eta/8\pi))_\delta) \gg \eta$ by Lemma 2.2.1. □

Proof of Proposition 4.4.8. We construct a sequence of regular Bourgain systems $\mathcal{B}^{(k)}$ iteratively. Write

$$\mathcal{L}_k := \{\gamma \in \widehat{G} : |1-\gamma(x)| \leqslant \epsilon^2/8(1+\|f\|_{A(G)})^2 \text{ for all } x \in B_1^{(k)}\},$$

and

$$L_k := \sum_{\gamma \in \mathcal{L}_k} |\widehat{f}(\gamma)|.$$

Initially set $\mathcal{B}^{(0)} = \mathcal{B}$. At stage k we apply the above iteration lemma, and either we are in the first case, in which case we are done, or we are in the second and get a regular Bourgain system $\mathcal{B}^{(k+1)} := \mathcal{B}'^{(k)} \cap (\rho'\mathcal{B}^{(k)})$ such that

$$\sum_{\gamma \in \mathcal{L}_{k+1}} |1-\widehat{\beta_1^{(k)}}(\gamma)||\widehat{f}(\gamma)| \geqslant \epsilon^2/4\|f\|_{A(G)}.$$

It follows by the triangle inequality that

$$2(L_{k+1}-L_k) + \epsilon^2/8(1+\|f\|_{A(G)}) \geqslant \epsilon^2/4\|f\|_{A(G)},$$

and so

$$L_k \geqslant \epsilon^2 k/2^4\|_{A(G)}$$

by induction. Since $L_k \leqslant \|f\|_{A(G)}$, the iteration must terminate in stage (i) after at most $2^4\|f\|_{A(G)}^2\epsilon^{-2}$ steps. If the iteration terminates at stage k then we set $\mathcal{B}' := \mathcal{B}^{(k)}$ and note that it satisfies the required dimension and density hypotheses by Lemma 2.4.4 as it is the intersection of $k+1$ Bourgain systems. □

4.4.4 Concentration on a subspace

In this section we prove the following proposition which combines all our previous work.

Proposition 4.4.10. *There is an absolute constant $C > 0$ such that the following holds. Suppose that $f \in A(G)$ has real range and is ϵ-almost integer valued for some $\epsilon \leqslant \exp(-C(1 + \|f\|_{A(G)})^4)$. Then there is a subgroup K of G with*

$$\mu_G(K) \geqslant \exp(-\epsilon^{-5}\exp(O(1 + \|f\|_{A(G)})^4))\|f_{\mathbb{Z}}\|_{L^1(\mu_G)}$$

and

$$\|f * \mu_K\|_{L^\infty(\mu_G)} \geqslant 1/2,$$

such that $f * \mu_K$ is 4ϵ-almost integer valued.

Proof. Let $C' > 0$ be the absolute constant implicit in the last estimate of Proposition 4.4.5. If

$$\epsilon \leqslant \exp(-(C' + 2^5)(1 + \|f\|_{A(G)})^4)$$

then we may apply Proposition 4.4.5 to get a regular Bourgain system $\mathcal{B}$ of dimension $\exp(O(1 + \|f\|_{A(G)})^4)$ with

$$\mu_G(\mathcal{B}) \geqslant \exp(-\exp(O(1 + \|f\|_{A(G)})^4))\|f_{\mathbb{Z}}\|_{L^1(\mu_G)}$$

and

$$\|f * \beta_1\|_{L^\infty(\mu_G)} \geqslant \exp(-C'(1 + \|f\|_{A(G)})^4).$$

Apply Corollary 2.4.6 and Proposition 2.4.5 to pick a regular Bourgain subsystem $\mathcal{B}'$ of $\mathcal{B}$ with

$$\mu_G(\mathcal{B}') \geqslant \exp(-\epsilon^{-1}\exp(O(1+\|f\|_{A(G)})^4))\|f_{\mathbb{Z}}\|_{L^1(\mu_G)}$$

such that

$$\|(y+\beta_1)-\beta_1\| \leqslant \epsilon \text{ for all } y \in B'_1.$$

Apply Proposition 4.4.8 to f and the Bourgain system $\mathcal{B}'$ with parameter ϵ to get a regular Bourgain subsystem $\mathcal{B}''$ of dimension $d'' \leqslant \epsilon^{-2}\exp(O(1+\|f\|_{A(G)})^4)$ with

$$\mu_G(\mathcal{B}'') \geqslant \exp(-\epsilon^{-5}\exp(O(1+\|f\|_{A(G)})^4))\|f_{\mathbb{Z}}\|_{L^1(\mu_G)}$$

and a $\rho \gg \epsilon\exp(-O(1+\|f\|_{A(G)})^4)$ such that

$$\sup_{x\in G}\|f*\beta''_1 - f*\beta''_1(x)\|_{L^\infty(x+\beta''_\rho)} \leqslant \epsilon$$

and

$$\sup_{x\in G}\|f - f*\beta''_1\|_{L^2(x+\beta''_\rho)} \leqslant \epsilon.$$

Let $K := (B''_\rho)^{\perp\perp}$. Then

$$\mu_G(K) \geqslant \rho^d\mu_G(\mathcal{B}'') \geqslant \exp(-\epsilon^{-5}\exp(O(1+\|f\|_{A(G)})^4))\|f_{\mathbb{Z}}\|_{L^1(\mu_G)}.$$

Now write $f'' := f*\beta''_1$ and note that

$$|f''_{\mathbb{Z}}(x) - f''(x)| = \inf_{z\in\mathbb{Z}}|z - f''(x)| \leqslant \|f_{\mathbb{Z}} - f''(x)\|_{L^2(x+\beta''_\rho)}$$

But this last expression is at most

$$\|f_{\mathbb{Z}} - f\|_{L^\infty(x+\beta''_\rho)} + \|f - f*\beta''_1\|_{L^2(x+\beta''_\rho)} + \|f*\beta''_1 - f*\beta''_1(x)\|_{L^\infty(x+\beta''_\rho)},$$

which, in turn, is at most 3ϵ.

Claim. *$f''_{\mathbb{Z}}$ is constant on cosets of K.*

Proof. Suppose that there are x_0 and x_1 with $x_0 - x_1 \in K$ and $f''_{\mathbb{Z}}(x_0) < f''_{\mathbb{Z}}(x_1)$. Since $\epsilon < 1/6$ there is a number $z + 1/2$ with z an integer and

$$f * \beta''_1(x_0) \leqslant f''_{\mathbb{Z}}(x_0) + 3\epsilon < z + 1/2 < f''_{\mathbb{Z}}(x_1) - 3\epsilon \leqslant f * \beta''_1(x_1).$$

It follows from Lemma 4.3.3 that there is an $x \in x_0 + K$ such that

$$|f * \beta''_1(x) - (z + 1/2)| \leqslant \epsilon/2.$$

But $f * \beta''_1(x)$ is within 3ϵ of an integer which is a contradiction since $\epsilon < 1/7$. The claim follows. □

Now

$$\begin{aligned} |f * \mu_K(x) - f''_{\mathbb{Z}} * \mu_K(x)| &\leqslant |f - f''_{\mathbb{Z}}| * \mu_K(x) \\ &= |f - f''_{\mathbb{Z}}| * \beta''_\rho * \mu_K(x) \\ &\leqslant \left(|f - f''_{\mathbb{Z}}|^2 * \beta''_\rho\right)^{\frac{1}{2}} * \mu_K(x) \end{aligned}$$

by the Cauchy-Schwarz inequality. Hence

$$\begin{aligned} |f * \mu_K(x) - f''_{\mathbb{Z}} * \mu_K(x)| &\leqslant \left(|f - f * \beta''_1|^2 * \beta''_\rho\right)^{\frac{1}{2}} * \mu_K(x) \\ &\quad + \left(|f * \beta''_1 - f''_{\mathbb{Z}}|^2 * \beta''_\rho\right)^{\frac{1}{2}} * \mu_K(x) \\ &\leqslant 4\epsilon. \end{aligned}$$

Since $f''_{\mathbb{Z}}$ is constant on coset of K we conclude that $f''_{\mathbb{Z}} * \mu_K(x) = f''_{\mathbb{Z}}(x)$ and hence that $f * \mu_K$ is 4ϵ-almost integer valued.

Finally since $\mathcal{B}''$ is a subsystem of $\mathcal{B}'$ we have

$$\|\beta_1 - \beta_1 * \beta''_1\| \leqslant \epsilon,$$

hence

$$\begin{aligned}\|(f*\mu_K)_{\mathbb{Z}}\|_{L^\infty(\mu_G)} &= \|f''_{\mathbb{Z}}\|_{L^\infty(\mu_G)}\\ &\geqslant \|f*\beta''_1\|_{L^\infty(\mu_G)} - 3\epsilon\\ &\geqslant \|f*\beta_1\|_{L^\infty(\mu_G)} - 4\epsilon.\end{aligned}$$

Since $4\epsilon < \exp(-C'(1+\|f\|_{A(G)})^4)$ we conclude that $\|(f*\mu_K)_{\mathbb{Z}}\|_{L^\infty(\mu_G)} > 0$ and hence, since it is an integer, $\|(f*\mu_K)_{\mathbb{Z}}\|_{L^\infty(\mu_G)} \geqslant 1$. The result follows since $f*\mu_K$ is 4ϵ-almost integer valued and $\epsilon < 1/8$. □

4.4.5 Proof of Theorem 4.12

We shall prove the result inductively using the following lemma.

Lemma 4.4.11 (Inductive Step)**.** *There is an absolute constant C such that if $f \in A(G)$ has real range and is ϵ-almost integer valued for some $\epsilon \leqslant \exp(-C(1+\|f\|_{A(G)})^4)$, then we may write $f = f_1 + f_2$, where*

(i). either $\|f_1\|_{A(G)} \leqslant \|f\|_{A(G)} - 1/2$ or else

$$(f_1)_{\mathbb{Z}} = \sum_{j=1}^{L} \pm 1_{x_j+K}$$

where $K \leqslant G$ and $L \leqslant \exp(\exp(O(1+\|f\|_{A(G)})^4))$;

(ii). $\|f_2\|_{A(G)} \leqslant \|f\|_{A(G)} - 1/2$ and

(iii). f_1 and f_2 are 5ϵ-almost integer valued.

Proof. Applying Proposition 4.4.10 to f, we obtain a subgroup K with

$$\mu_G(K) \geqslant \exp(-\epsilon^{-5}\exp(O(1+\|f\|_{A(G)})^4))\|f_{\mathbb{Z}}\|_{L^1(\mu_G)}$$

and

$$\|f*\mu_K\|_{L^\infty(\mu_G)} \geqslant 1/2.$$

We define $f_1 := f * \mu_K$ and $f_2 := f - f_1$, noting immediately that they are both 5ϵ-almost integer valued. It follows that $\|f_1\|_{A(G)} \geqslant \|f_1\|_{L^\infty(\mu_G)} \geqslant 1/2$, whence $\|f_2\|_{A(G)} \leqslant \|f\|_{A(G)} - 1/2$, since

$$\|f\|_{A(G)} = \|f * \mu_K\|_{A(G)} + \|f - f * \mu_K\|_{A(G)} = \|f_1\|_{A(G)} + \|f_2\|_{A(G)}.$$

It remains to deal with the possibility that $\|f_1\|_{A(G)} > \|f\|_{A(G)} - 1/2$. If this is so then $\|f_2\|_{A(G)} < 1/2$, and thus $\|f_2\|_{L^\infty(\mu_G)} < 1/2$. It follows that $(f_2)_{\mathbb{Z}} = 0$, and hence $f_{\mathbb{Z}} = (f_1)_{\mathbb{Z}}$, so we may write

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

for some $j = 1, ..., L$, where we may take $L \leqslant \|f_{\mathbb{Z}}\|_{L^1(\mu_G)}/\|1_K\|_{L^1(\mu_G)}$. The result follows. □

Proof of Theorem 4.4.1. Let C' be the absolute constant in Lemma 4.4.11. For each $k \geqslant 0$ let $\epsilon_k := 5^k\epsilon$. If $g : G \to \mathbb{C}$ then we say that g has property

- $P_0(g, k)$ if g is ϵ_k-almost integer valued;
- $P_1(g)$ if there is a subgroup $H_g \leqslant G$, an integer

  $$L_g \leqslant \exp(\epsilon^{-5} \exp(O(1 + \|f\|_{A(G)})^4))$$

  and for each j with $1 \leqslant j \leqslant L_g$ a sign $\sigma_j^{(g)} \in \{-1, 1\}$ and an element $x_j^{(g)} \in G$ such that

  $$(g)_{\mathbb{Z}} = \sum_{j=1}^{L_g} \sigma_j^{(g)} 1_{x_j^{(g)} + H_g};$$

- $P_2(g, k)$ if $\|g\|_{A(G)} \leqslant \|f\|_{A(G)} - k/2$.

We construct a sequence of collections of functions $(\mathcal{F}_k)_{k \geqslant 0}$ iteratively such that the following properties hold.

- $P_0(k)$: $f = \sum_{g \in \mathcal{F}_k} g$.

- $P_1(k)$: $|\mathcal{F}_k| \leqslant 2^k$.
- $P_2(k)$: If $g \in \mathcal{F}_k$ then $P_0(g,k)$ holds.
- $P_3(k)$: If $g \in \mathcal{F}_k$ then either $P_1(g)$ or $P_2(g,k)$ holds.

We initiate the iteration with $\mathcal{F}_0 = \{f\}$. In this case it is trivial to verify that $P_0(0), P_1(0), P_2(0)$ and $P_3(0)$ hold.

Suppose that for some $0 \leqslant k \leqslant \lceil 2\|f\|_{A(G)}\rceil + 2$ we have constructed $\mathcal{F}_k$ such that $P_0(k), P_1(k), P_2(k)$ and $P_3(k)$ hold. Suppose that $g \in \mathcal{F}_k$. We have two cases.

(i). $P_1(g)$ holds: Since $P_0(g,k)$ holds and $\epsilon_k \leqslant \epsilon_{k+1}$ we conclude that $P_0(g,k+1)$ holds. We add g into $\mathcal{F}_{k+1}$.

(ii). $P_2(g,k)$ holds: Since $k \leqslant \lceil 2\|f\|_{A(G)}\rceil + 2$ we conclude that

$$\epsilon_k \leqslant 2^{3.(2\|f\|_{A(G)}+3)}.\epsilon \leqslant \exp(-C'(1+\|f\|_{A(G)})^4),$$

so we may apply Lemma 4.4.11 to get $g = g_1 + g_2$, where for each $i \in \{1,2\}$ g_i is $2^3\epsilon_k = \epsilon_{k+1}$-almost integer valued and either $P_1(g_i)$ holds or $\|g_i\|_{A(G)} \leqslant \|g\|_{A(G)} - 1/2$; in the second case we combine this with the fact $P_2(g,k)$ holds to get that $P_2(g_i,k+1)$ holds. We add g_1 and g_2 into $\mathcal{F}_{k+1}$.

This construction ensures that $P_2(k+1)$ and $P_3(k+1)$ hold. Since $P_0(k)$ holds and for each $g \in \mathcal{F}_k$ we either added g or two functions summing to g into $\mathcal{F}_{k+1}$ we conclude that $P_0(k+1)$ holds. Finally since for each $g \in \mathcal{F}_k$ we added at most two functions to $\mathcal{F}_k$ we conclude that $|\mathcal{F}_{k+1}| \leqslant 2|\mathcal{F}_k|$. It then follows that since $P_1(k)$ holds, $P_1(k+1)$ holds.

If $K = \lceil 2\|f\|_{A(G)}\rceil + 1$ then $P_2(g,K)$ can never hold. It follows that for each $g \in \mathcal{F}_K$, $P_1(g)$ holds. Now

$$\begin{aligned}\|(f)_{\mathbb{Z}} - \sum_{g\in\mathcal{F}_K}(g)_{\mathbb{Z}}\|_{L^\infty(\mu_G)} &\leqslant \|f-(f)_{\mathbb{Z}}\|_{L^\infty(\mu_G)}\\ &\quad +|\mathcal{F}_K|\sup_{g\in\mathcal{F}_K}\|g-(g)_{\mathbb{Z}}\|_{L^\infty(\mu_G)}\\ &\leqslant \epsilon_0 + 2^K\epsilon_K \leqslant 2^{4K+1}\epsilon.\end{aligned}$$

The left hand side is integer valued and $2^{4K+1}\epsilon \leqslant 2^{-1}$ so we can conclude that

$$(f)_{\mathbb{Z}} = \sum_{g \in \mathcal{F}_K} (g)_{\mathbb{Z}}.$$

It remains to note that

$$\sum_{g \in \mathcal{F}_K} (g)_{\mathbb{Z}} = \sum_{g \in \mathcal{F}_K} \sum_{j=1}^{L_g} \sigma_j^{(g)} 1_{x_j^{(g)} + H_g}.$$

Now we may in fact assume that $\epsilon = \exp(-O(1 + \|f\|_{A(G)})^4)$ whereupon the result follows. □

4.4.6 Concluding remarks

As it stands, our argument 'loses an exponential' in two places. First of all the almost integer parameter must not be allowed to get too large during the iteration leading to the proof of Theorem 4.4.1. This requires it to be exponentially small in $1 + \|f\|_{A(G)}$ at the beginning of the argument. This parameter then gets exponentiated again in any application of Proposition 4.4.8. Méla's work, [Mél82], in fact shows that one cannot hope for a result which only asks for $\|f - f_{\mathbb{Z}}\|_{L^\infty(\mu_G)} \leqslant \exp(-o(1 + \|f\|_{A(G)}))$, essentially by considering the example of the auxiliary measures we constructed in §2.1.3, so our result is at most 'one exponential out'.

Write $L(M)$ for the smallest integer L such that for every finite abelian group G and subset A with $\|1_A\|_{A(G)} \leqslant M$ one can write 1_A as a $\pm$-sum of at most L indicator functions of cosets in G. Theorem 4.12 asserts that

$$L(M) = \exp(\exp(O(1 + M)^4)).$$

Limitations on how small $L(M)$ can be seem to be dependent on the underlying group. Consider the arithmetic group $\mathbb{Z}/p\mathbb{Z}$ where p is a prime. If $A \subset \mathbb{Z}/p\mathbb{Z}$ has density bounded away from 0 and 1 then 1_A cannot be written as a $\pm$-sum of $o(p)$ indicator functions of cosets in $\mathbb{Z}/p\mathbb{Z}$. It follows that

$$p \ll L(\|1_A\|_{A(\mathbb{Z}/p\mathbb{Z})}) = \exp(\exp(O(1+\|1_A\|_{A(\mathbb{Z}/p\mathbb{Z})})^4)).$$

Rearranging this implies that

$$\|1_A\|_{A(\mathbb{Z}/p\mathbb{Z})} \gg (\log\log p)^{1/4}.$$

Note that this is a very weak version of the result of §4.2. A straightforward calculation shows that if A is an arithmetic progression then $\|1_A\|_{A(\mathbb{Z}/p\mathbb{Z})} \ll \log p$ whence $\log L(M) \gg M$ and Theorem 4.12 is out by at most one exponential. Similarly, when Theorem 4.12 is extended to all locally compact abelian groups one can conclude a weak version of Littlewood's conjecture *viz.*

$$\|1_A\|_{A(\mathbb{Z})} \gg (\log\log |A|)^{1/4}.$$

Of course the example of an arithmetic progression does not exist in the model setting of $\mathbb{F}_2^n$, where it may be that $L(M)$ (restricted to cover only these model groups) can be taken to be polynomial in M. Note that a random set can be used to see that this polynomial must be at least quadratic. This case was treated first by Green and the author in [GS08a]; the arguments there are slightly different from those here but ultimately yield a bound of the same shape.

Because of the abundance of subgroups in the model setting the bound Theorem 4.12 implies for the results of the dyadic setting, §4.1, are far weaker than for the arithmetic setting. Suppose $A \subset \mathbb{F}_2^n$ is a set with density α such that $|\alpha - 1/3| \leqslant \epsilon$. Then a straightforward pigeon-hole argument shows that there is no decomposition of 1_A as the $\pm$-sum of $o(\log \epsilon^{-1})$ indicator functions of cosets. Thus, our quantitative idempotent theorem implies that

$$\log \epsilon^{-1} \ll L(\|1_A\|_{A(\mathbb{F}_2^n)}) \leqslant \exp(\exp(O(1+\|1_A\|_{A(\mathbb{F}_2^n)})^4)),$$

which gives the rather poor bound

$$\|1_A\|_{A(\mathbb{F}_2^n)} \gg (\log\log\log\epsilon^{-1})^{1/4}.$$

The same argument gives the same bound for the case of G any finite abelian group.

Finally, recall that $\|1_A\|_{A(G)} \geqslant 1$ for all nonempty subsets A of G. It seems natural, by analogy with Freĭman's Theorem, to consider in more detail what the structure of $A \subset G$ might be when $\|1_A\|_{A(G)}$ is close to 1; say less than 3/2. Some work on this problem has been done by Saeki see [Sae68a, Sae68b].

Bibliography

[BC03] J. Bourgain and M.-C. Chang, *On multiple sum and product sets of finite sets of integers*, C. R. Math. Acad. Sci. Paris **337** (2003), no. 8, 499–503. MR 2017126 (2004i:11013)

[Bil99] Y. Bilu, *Structure of sets with small sumset*, Astérisque (1999), no. 258, xi, 77–108, Structure theory of set addition. MR MR1701189 (2000h:11109)

[Bog39] N. Bogolioùboff, *Sur quelques propriétés arithmétiques des presque-périodes*, Ann. Chaire Phys. Math. Kiev **4** (1939), 185–205. MR MR0020164 (8,512b)

[Bou99] J. Bourgain, *On triples in arithmetic progression*, Geom. Funct. Anal. **9** (1999), no. 5, 968–984. MR MR1726234 (2001h:11132)

[Bou02] ———, *On the distributions of the Fourier spectrum of Boolean functions*, Israel J. Math. **131** (2002), 269–276. MR MR1942312 (2003j:43009)

[Bou03] ———, *On the Erdős-Volkmann and Katz-Tao ring conjectures*, Geom. Funct. Anal. **13** (2003), no. 2, 334–365. MR 1982147 (2004d:11070)

[Bou08] J Bourgain, *Roth's theorem on progressions revisited*, J. Anal. Math. **104** (2008), 155–192. MR 2403433 (2009g:11011)

[Cha00] B. Chazelle, *The discrepancy method*, Cambridge University Press, Cambridge, 2000, Randomness and complexity. MR MR1779341 (2002c:68002)

[Cha02] M.-C. Chang, *A polynomial bound in Freĭman's theorem*, Duke Math. J. **113** (2002), no. 3, 399–419. MR MR1909605 (2003d:11151)

[Coh60] P. J. Cohen, *On a conjecture of Littlewood and idempotent measures*, Amer. J. Math. **82** (1960), 191–212. MR MR0133397 (24 #A3231)

[DHP04] J.-M. Deshouillers, F. Hennecart, and A. Plagne, *On small sumsets in* $(\mathbb{Z}/2\mathbb{Z})^n$, Combinatorica **24** (2004), no. 1, 53–68. MR MR2057683 (2005f:11231)

[Fre73] G. A. Freĭman, *Foundations of a structural theory of set addition*, American Mathematical Society, Providence, R. I., 1973, Translated from the Russian, Translations of Mathematical Monographs, Vol 37. MR MR0360496 (50 #12944)

[GK09] B. J. Green and S. V. Konyagin, *On the Littlewood problem modulo a prime*, Canad. J. Math. **61** (2009), no. 1, 141–164. MR MR2488453

[Gow98] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal. **8** (1998), no. 3, 529–551. MR MR1631259 (2000d:11019)

[GR07] B. J. Green and I. Z. Ruzsa, *Freĭman's theorem in an arbitrary abelian group*, J. Lond. Math. Soc. (2) **75** (2007), no. 1, 163–175. MR MR2302736 (2007m:20087)

[Gre04] B. J. Green, *Spectral structure of sets of integers*, Fourier analysis and convexity, Appl. Numer. Harmon. Anal., Birkhäuser Boston, Boston, MA, 2004, pp. 83–96. MR MR2087239 (2005i:11015)

[Gre05] ———, *Finite field models in additive combinatorics*, Surveys in combinatorics 2005, London Math. Soc. Lecture Note Ser., vol. 327, Cambridge Univ. Press, Cambridge, 2005, pp. 1–27. MR MR2187732 (2006j:11030)

[GS08a] B. J. Green and T. Sanders, *Boolean functions with small spectral norm*, Geom. Funct. Anal. **18** (2008), no. 1, 144–162. MR 2399099

[GS08b] ______, *A quantitative version of the idempotent theorem in harmonic analysis*, Ann. of Math. (2) **168** (2008), no. 3, 1025–1054. MR 2456890

[GT08] B. J. Green and T. C. Tao, *An inverse theorem for the Gowers $U^3(G)$ norm*, Proc. Edinb. Math. Soc. (2) **51** (2008), no. 1, 73–153. MR MR2391635 (2009g:11012)

[GT09a] ______, *Freĭman's theorem in finite fields via extremal set theory*, Combin. Probab. Comput. **18** (2009), no. 3, 335–355. MR 2501431 (2010f:11176)

[GT09b] ______, *A note on the Freĭman and Balog-Szemerédi-Gowers theorems in finite fields*, J. Aust. Math. Soc. **86** (2009), no. 1, 61–74. MR MR2495998

[Hal50] P. R. Halmos, *Measure Theory*, D. Van Nostrand Company, Inc., New York, N. Y., 1950. MR MR0033869 (11,504d)

[Hal81] G. Halász, *On Roth's method in the theory of irregularities of point distributions*, Recent progress in analytic number theory, Vol. 2 (Durham, 1979), Academic Press, London, 1981, pp. 79–94. MR MR637361 (83e:10072)

[HL48] G. H. Hardy and J. E. Littlewood, *A new proof of a theorem on rearrangements*, J. London Math. Soc. **23** (1948), 163–168. MR 0028445 (10,448b)

[Kon81] S. V. Konyagin, *On the Littlewood problem*, Izv. Akad. Nauk SSSR Ser. Mat. **45** (1981), no. 2, 243–265, 463. MR MR616222 (83d:10045)

[Mél82] J.-F. Méla, *Mesures ε-idempotentes de norme bornée*, Studia Math. **72** (1982), no. 2, 131–149. MR MR665414 (84a:43007)

[MPS81] O. C. McGehee, L. Pigno, and B. Smith, *Hardy's inequality and the L^1 norm of exponential sums*, Ann. of Math. (2) **113** (1981), no. 3, 613–618. MR MR621019 (83c:43002b)

[Rid66] D. Rider, *Gap series on groups and spheres*, Canad. J. Math. **18** (1966), 389–398. MR MR0190635 (32 #8047)

[Rud90] W. Rudin, *Fourier analysis on groups*, Wiley Classics Library, John Wiley & Sons Inc., New York, 1990, Reprint of the 1962 original, A Wiley-Interscience Publication. MR MR1038803 (91b:43002)

[Ruz94] I. Z. Ruzsa, *Generalized arithmetical progressions and sumsets*, Acta Math. Hungar. **65** (1994), no. 4, 379–388. MR MR1281447 (95k:11011)

[Ruz96] ______, *Sums of finite sets*, Number theory (New York, 1991–1995), Springer, New York, 1996, pp. 281–293. MR MR1420216 (97i:11019)

[Ruz99] ______, *An analog of Freĭman's theorem in groups*, Astérisque (1999), no. 258, xv, 323–326, Structure theory of set addition. MR MR1701207 (2000h:11111)

[Sae68a] S. Saeki, *On norms of idempotent measures*, Proc. Amer. Math. Soc. **19** (1968), 600–602. MR MR0225102 (37 #697)

[Sae68b] ______, *On norms of idempotent measures. II*, Proc. Amer. Math. Soc. **19** (1968), 367–371. MR MR0228931 (37 #4510)

[San06] T. Sanders, *An application of a local version of Chang's theorem*, 2006.

[San07a] ______, *The ℓ^1-norm of the Fourier transform on compact vector spaces*, Bull. Lond. Math. Soc. **39** (2007), no. 3, 509–521. MR 2331582

[San07b] ______, *The Littlewood-Gowers problem*, J. Anal. Math. **101** (2007), 123–162. MR 2346542

[San08a] ______, *Additive structures in sumsets*, Math. Proc. Cambridge Philos. Soc. **144** (2008), no. 2, 289–316. MR 2405891

[San08b] ______, *Appendix to: "Roth's theorem on progressions revisited" [J. Anal. Math.* **104** *(2008), 155–192] by J. Bourgain*, J. Anal. Math. **104** (2008), 193–206. MR 2403434

[San08c] ______, *A note on Freĭman's theorem in vector spaces*, Combin. Probab. Comput. **17** (2008), no. 2, 297–305. MR 2396355

[SSV05] B. Sudakov, E. Szemerédi, and V. H. Vu, *On a question of Erdős and Moser*, Duke Math. J. **129** (2005), no. 1, 129–155. MR MR2155059 (2006c:11118)

[Ste93] E. M. Stein, *Harmonic analysis: real-variable methods, orthogonality, and oscillatory integrals*, Princeton Mathematical Series, vol. 43, Princeton University Press, Princeton, NJ, 1993, With the assistance of Timothy S. Murphy, Monographs in Harmonic Analysis, III. MR MR1232192 (95c:42002)

[TV06] T. C. Tao and H. V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006. MR MR2289012 (2008a:11002)

[Zyg02] A. Zygmund, *Trigonometric series. Vol. I, II*, third ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 2002, With a foreword by Robert A. Fefferman. MR 1963498 (2004h:01041)