Some constructions in the inverse spectral theory of cyclic groups[1]

Ben Green[2]

Abstract

The results of this paper concern the "large spectra" of sets, by which we mean the set of points in $\mathbf{F}_p^\times$ at which the Fourier transform of a characteristic function χ_A, $A \subseteq \mathbf{F}_p$, can be large. We show that a recent result of Chang concerning the structure of the large spectrum is best possible. Chang's result has already found a number of applications in combinatorial number theory.

We also show that if $|A| = \lfloor p/2 \rfloor$, and if R is the set of points r for which $|\hat{\chi}_A(r)| \geq \alpha p$, then almost nothing can be said about R other than that $|R| \ll \alpha^{-2}$, a trivial consequence of Parseval's theorem.

1 Introduction.

We begin by introducing a small amount of notation which is necessary to state our results. Throughout this paper N will be a large prime number and we will write $\mathbf{Z}_N$ for the set of residues modulo N. If $\Lambda = \{\lambda_1, \ldots, \lambda_L\} \subseteq \mathbf{Z}_N$ we write $\mathrm{Span}(\Lambda)$ for the set of all sums $s(\epsilon) = \sum_j \epsilon_j \lambda_j$ with $\epsilon_j \in \{-1, 0, 1\}$. We will write $\omega_N^x = e^{2\pi i x/N}$. Often the subscript N will be suppressed, as the value of N will be clear from the context. If $f : \mathbf{Z}_N \to \mathbf{C}$ is a function and $r \in \mathbf{Z}_N$ then we define the Fourier transform of f at r by

$$\hat{f}(r) \ = \ \sum_x f(x)\omega^{rx}.$$

We will adopt the convenient notational practice of identifying sets with their characteristic functions.

In a recent preprint [**?**] of Chang the following result is stated.

Theorem 1 (Chang's structure theorem) *Let $\rho, \alpha \in [0,1]$, Let $A \subseteq \mathbf{Z}_N$ be a set of size αN and suppose that $|\hat{A}(r)| \geq \rho|A|$ for all $r \in R$. Then there is a set $\Lambda \subseteq \mathbf{Z}_N$ with $|\Lambda| \leq 60\rho^{-2}\log\left(\frac{1}{\alpha}\right)$ such that $R \subseteq \mathrm{Span}(\Lambda)$.*

It is convenient to give a name to the situation covered by this theorem. Thus if $A, R \subseteq \mathbf{Z}_N$ and if $\rho \in (0,1)$ then we say that A is ρ-large at R if $|\hat{A}(r)| \geq \rho|A|$ for all $r \in R$.

Now Parseval's Theorem implies that the set R has size at most $\rho^{-2}\alpha^{-1}$, but for small α

[1]2000 Mathematics Subject Classification: 11L99.

[2]Supported by a Fellowship at Trinity College, Cambridge, and a grant from the Engineering and Physical Sciences Research Council (EPSRC) of the United Kingdom.

this is much bigger than the size of Λ guaranteed by Chang's result. Theorem 1 may thus be viewed as saying that the "large spectrum" of a small set is very highly structured. A result such as this is extremely valuable, being a strong structural statement valid in a highly general setting. It has already found two combinatorial applications: to Freiman's theorem [**?**] and to the location of arithmetic progressions in sumsets [**?**]. The reader may find a detailed discussion and proof of Theorem 1 together with an overview of these applications in the article [**?**] and in the lecture notes [1].

In §4 we will give an example which rules out potential improvements to Chang's theorem. Specifically, we will prove the following.

Theorem 2 (Chang's theorem is sharp) *Let α, ρ be positive real numbers satisfying $\alpha \leq 1/8$, $\rho \leq 1/32$ and*

$$\rho^{-2} \log(1/\alpha) \ \leq \ \frac{\log N}{\log \log N}. \tag{1}$$

Then there is a set $A \subseteq \mathbf{Z}_N$ with $|A| = \lfloor \alpha N \rfloor$ which is ρ-large at R, where R is not contained in Span(Λ) *for any set Λ with $|\Lambda| \leq 2^{-12}\rho^{-2}\log(1/\alpha)$.*

Observe that Chang's theorem gives nothing more than Parseval's theorem when $\alpha = 1/2$. It is therefore extremely natural to ask whether anything more can be said about the set of points at which A is ρ-large, where $|A| = \lfloor N/2 \rfloor$. We show in §5 that, at least in a certain sense, the answer is no. In fact we will show

Theorem 3 *There is a (small) absolute constant c with the following property. Let ρ be a real number satisfying $c \geq \rho \geq c^{-1}N^{-1/2}$, and let $R \subseteq \mathbf{Z}_N$ be an arbitrary set of size $c\rho^{-2}$. Then there is a set $A \subseteq \mathbf{Z}_N$, $|A| = \lfloor N/2 \rfloor$, which is ρ-large at at least 90 percent of the points in R.*

There is nothing particularly special about 90 percent, except that it feels like a good notion of "most". Annoyingly we have not been able to prove this result for 100 percent of R.

Let us introduce a few further pieces of notation. Let k be a positive integer and let $\Lambda = \{\lambda_1, \ldots, \lambda_L\}$ be a subset of $\mathbf{Z}_N$. We say that Λ is k-dissociated if the only solution to the equation

$$\eta_1\lambda_1 + \ldots + \eta_L\lambda_L \ = \ 0$$

with $|\eta_j| \leq k$ is the trivial solution $\eta_1 = \ldots = \eta_L = 0$.

Finally we will write $c_N(x) = \cos(2\pi x/N)$ and $s_N(x) = \sin(2\pi x/N)$. Once again the subscript N will often be suppressed: observe, to clarify this notation, that $c(x) = \frac{1}{2}(\omega^x + \omega^{-x})$.

2 Applications of Spencer's linear forms theorem.

The following result is a trivial deduction from Theorem 8 in [**?**], the only difference being that the statement here applies to complex linear forms but has a slightly worse constant.

Theorem 4 (Spencer, Beck) *Let n be sufficiently large and suppose that we have n linear forms*

$$L_i(x_1, \ldots, x_n) \ = \ a_{i1}x_1 + \ldots + a_{in}x_n,$$

where the a_{ij} are complex numbers with $|a_{ij}| \leq 1$. Suppose also that we have n real numbers $p_j \in [0,1]$. Then there are choices of $\epsilon_j \in \{0,1\}$ such that

$$|L_i(\epsilon_1, \ldots, \epsilon_n) - L_i(p_1, \ldots, p_n)| \ \leq \ 10\sqrt{n}$$

for all $1 \leq i \leq n$.

Corollary 1 *Let $f : \mathbf{Z}_N \rightarrow [0,1]$. Then there is a subset $S \subseteq \mathbf{Z}_N$ with $|S| = \lfloor \sum_x f(x) \rfloor$ and $|\hat{S}(r) - \hat{f}(r)| \leq 20\sqrt{N}$ for all $r \in \mathbf{Z}_N^\times$.*

Proof. The existence of a set S_0 with $|\hat{S}_0(r) - \hat{f}(r)| \leq 10\sqrt{N}$ for *all* $r \in \mathbf{Z}_N$ is immediate from Theorem 4. By adding or deleting at most $10\sqrt{N}$ elements we may form a set S with size exactly $\lfloor \sum_x f(x) \rfloor$. This will satisfy the conclusion of the corollary by the triangle inequality. □

Lemma 1 (Size change lemma) *Let $R \subseteq \mathbf{Z}_N$ and let $\alpha, \rho \in [0,1]$. Suppose that $\rho\alpha \geq 80N^{-1/2}$ and that there exists a set $A \subseteq \mathbf{Z}_N$, $|A| = \alpha N$, which is ρ-large at R. Then there exists a set $B \subseteq \mathbf{Z}_N$, $|B| = \lfloor N/2 \rfloor$, which is $\rho\alpha/2$-large at R.*

Proof. We divide into the two cases $\alpha < 1/2$ and $\alpha \geq 1/2$. We deal with the former, more difficult, case first. Suppose then that $\alpha < 1/2$ and define $f : \mathbf{Z}_N \rightarrow [0,1]$ by

$$f(x) \ = \ \begin{cases} 1 & (x \in A) \\ \frac{1-2\alpha}{2-2\alpha} & (x \notin A). \end{cases}$$

Let B be a set satisfying the conclusions of Corollary 1 for this function f, so that $|B| = \lfloor N/2 \rfloor$. For any $r \neq 0$ we have

$$\hat{f}(r) \ = \ \frac{1}{2-2\alpha}\hat{A}(r),$$

and so we see that for $r \in R$

$$\begin{aligned} |\hat{B}(r)| \ &\geq \ \frac{1}{2-2\alpha}|\hat{A}(r)| - 20\sqrt{N} \\ &\geq \ \rho\alpha|B| - 20\sqrt{N} \\ &\geq \ \rho\alpha|B|/2 \end{aligned}$$

if N satisfies the hypotheses of the corollary.

If $\alpha \geq 1/2$ the proof goes along similar lines but is much easier. Take $f(x) = A(x)/2\alpha$. □

3 Chang's theorem is sharp.

In this section we proof Theorem 2, which rules out any substantial improvement of Chang's theorem. Our argument is inspired by two papers of Ruzsa [**?**, **?**] in which so-called niveau sets are constructed. Although our paper is self-contained it might be helpful for motivational purposes to recall Ruzsa's construction, and to outline our modification of it.

In [**?**], for example, Ruzsa takes k residues $a_1, \ldots, a_k \subseteq \mathbf{Z}_N$ and defines A by

$$A \;=\; \left\{ x \in \mathbf{Z}_N \;\left|\; \sum_{j=1}^{k} c(a_j x) \;>\; \delta\sqrt{k} \right.\right\} \tag{2}$$

for some $\delta > 0$. The point of this construction is that, for a suitable choice of $a_1, \ldots, a_k$, such a set A will have the property that $|A| \geq (\frac{1}{2} - \delta)N$ but that $A + A$ does not contain an arithmetic progression of length $e^{(\log N)^{2/3+\delta}}$. This shows that a result of Bourgain [**?**] is almost sharp (see also [**?**]).

The construction of this section might be called a *smoothed intersection of niveau sets*. We define polynomials p_k by truncating the power series of $f(x) = \frac{1}{2} + \frac{1}{4}xe^{-x^2/16}$, which itself acts as a kind of smooth approximation to the characteristic function $\chi_{[0,\infty)}$. We then modify Ruzsa's construction by setting $\delta = 0$ and using an appropriate p_k in place of $\chi_{[0,\infty)}$ (which is implicit in (2)). The smoothing makes it *much* easier to calculate the Fourier coefficients of the resulting set.

Lemma 2 *Let k be a positive integer, and write $p_k(x)$ for the polynomial*

$$\frac{1}{2} + \frac{x}{4} \sum_{j=0}^{k} \frac{(-1)^j x^{2j}}{2^{4j} j!}.$$

Then for $|x| \leq \sqrt{k}$ we have

$$0 \;\leq\; p_k(x) \;\leq\; 1.$$

Proof. The key to this lemma is the observation that the infinite series

$$\sum_{j=0}^{\infty} \frac{(-1)^j x^{2j}}{2^{4j} j!}$$

converges to the function $e^{-x^2/16}$ for all real x. Furthermore if $j > k$ and $|x| \leq \sqrt{k}$ then

$$\begin{aligned} \frac{|x|^{2j}}{2^{4j} j!} \;&\leq\; \left(\frac{e}{16}\right)^j \left(\frac{x^2}{j}\right)^j \\ &\leq\; 2^{-2j}. \end{aligned}$$

Thus

$$\begin{aligned}\left|p_k(x) - \frac{1}{2} - \frac{x}{4}e^{-x^2/16}\right| &\leq \frac{k^{1/2}}{4}\sum_{j>k} 2^{-2j} \\ &\leq 1/16.\end{aligned}$$

But a simple calculus exercise shows that $|xe^{-x^2/16}| \leq (8/e)^{1/2}$ for all real x, and the lemma follows immediately. □

Now let k, t be positive integers to be chosen later, let $m = kt$, and choose a $6m$-dissociated sequence (a_{ij}), $1 \leq i \leq t$, $1 \leq j \leq k$ of m elements from $\mathbf{Z}_N$. This is certainly possible if N is sufficiently large and $m \leq \log N/2\log\log N$, for in that case we could take $(a_{ij}) = \{1, 13m, (13m)^2, \ldots, (13m)^{m-1}\}$. Define a function $g : \mathbf{Z}_N \to \mathbf{R}$ by

$$g(x) \;=\; \prod_{j=1}^{t} p_k\left(\frac{c(a_{j,1}x) + \ldots + c(a_{j,k}x)}{\sqrt{k}}\right). \tag{3}$$

By Lemma 2 this function satisfies $0 \leq g(x) \leq 1$ for all x. It is to a closely related function that we will apply Lemma 1. In order to do this we need an understanding of g and some of its Fourier coefficients.

Lemma 3 (i) $\sum_x g(x) \;=\; 2^{-t}N$;

(ii) $|\hat{g}(a_{u,v})| \geq 2^{-t}N/8\sqrt{k}$ *for all* $1 \leq u \leq t, 1 \leq v \leq k$.

Proof. It is possible to write all the cosines in (3) using exponentials (so $c(x)$ becomes $\frac{1}{2}(\omega^x + \omega^{-x})$) and then expand out the product. Doing this in a purely formal way gives an expression of the form

$$\sum_{|\lambda_{u,v}| \leq 2k+1 \;\forall u,v} Q\left(\lambda_{1,1}, \ldots, \lambda_{t,k}\right) \omega^{\left(\lambda_{1,1}a_{1,1} + \ldots + \lambda_{t,k}a_{t,k}\right)x}. \tag{4}$$

Recall, however, that (a_{ij}) is $6m$-dissociated and hence, *a fortiori*, $(4k+2)$-dissociated. This implies that all the sums

$$\lambda_{1,1}a_{1,1} + \ldots + \lambda_{t,k}a_{t,k}$$

appearing in (4) are distinct. The "formal" expansion (4) therefore has rather more meaning than one might at first sight think, and in fact it is precisely the Fourier expansion of g. In particular we see that

$$\sum_x g(x) \;=\; Q(0, 0, \ldots, 0)N$$

and that

$$\hat{g}(a_{u,v}) \;=\; Q(0, 0, \ldots, 1, \ldots, 0)N,$$

where $Q(0,0,\ldots,1,\ldots,0)$ is the coefficient attached to $\omega^{a_{u,v}x}$. It is easy to work out the constant term $Q(0,0,\ldots,0)$. Observing that

$$p_k(x) \;=\; \frac{1}{2} + \text{odd powers of } x$$

we see that the only contribution to the constant term of g comes from taking the $1/2$ from each term of the product (3). This constant term is therefore 2^{-t}. In considering $Q(0,0,\ldots,1,\ldots,0)$ it clearly suffices to deal with the case $(u,v)=(1,1)$, and we observe that to obtain such an exponential we must take the constant $1/2$ from each term of the product (3) except the first. Now this first term is

$$p_k\left(\frac{c(a_{1,1}x)+\ldots+c(a_{1,k}x)}{\sqrt{k}}\right) = \\ \frac{1}{2} + \frac{1}{8\sqrt{k}}\sum_{j=0}^{k}\frac{(-1)^j}{(64k)^j j!}\left(\omega^{a_{1,1}x}+\omega^{-a_{1,1}x}+\ldots+\omega^{a_{1,k}x}+\omega^{-a_{1,k}x}\right)^{2j+1}.$$

The coefficient of $\omega^{a_{1,1}x}$ from the first term, $j=0$, is $1/8\sqrt{k}$. We shall show that this is larger than the contribution from all of the remaining terms. Let us look at the contribution from the term $j=l$, which is essentially a product of $2l+1$ "brackets". Every term contributing to the coefficient of $\omega^{a_{1,1}x}$ arises in the following way. First of all choose $\omega^{a_{1,1}x}$ from some bracket ($2l+1$ choices). Look at the first bracket from which we have not selected an exponential and choose something from it, say $\omega^{a_{1,u}x}$. This can be done in $2k$ ways. Now this must be balanced by choosing $\omega^{-a_{1,u}x}$ from some other bracket. There are at most $(2l-1)$ ways of doing this. Now look at the first bracket from which we have still not chosen an exponential, and continue. In this way we see that the coefficient of $\omega^{a_{1,1}x}$ from $j=l$ is at most $1/8\sqrt{k}$ times

$$\frac{1}{(64k)^l l!}\times(2l+1)\times k\times(2l-1)\times k\times(2l-3)\times\ldots\times k\times 1 \\ \leq\; \frac{2l+1}{2^{5l}}.$$

Summing over all j, we see that the coefficient of $\omega^{a_{1,1}x}$ arising from the first term of the product (3) is positive and at least

$$\frac{1}{8\sqrt{k}}\left(1-\sum_{j=1}^{\infty}\frac{2j+1}{2^{5j}}\right) \;\geq\; \frac{1}{16\sqrt{k}}.$$

Thus the coefficient of $\omega^{a_{1,1}x}$ when g is expanded is at least $2^{-t}/8\sqrt{k}$. This completes the proof of the lemma. □

In what follows we will suppose that α, ρ are positive reals satisfying $\alpha \leq 1/8$, $\rho \leq 1/32$ and

$$\rho^{-2} \log\left(\tfrac{1}{\alpha}\right) \ \leq \ \frac{\log N}{\log\log N}. \tag{5}$$

Take $t = \lfloor \log(1/\alpha) \rfloor$ and $k = \lfloor 2^{-9}\rho^{-2} \rfloor$. It is easy to check that $m = tk$ satisfies the inequality $m \leq \log N/2 \log\log N$ required for the construction we have been discussing. Set $f = \gamma g$, where $\gamma \in [\frac{1}{2}, 1]$ is such that $\sum_x f(x) = \alpha N$. The existence of such a γ is of course a trivial consequence of Lemma 3, which also implies that

$$|\hat{f}(a_{u,v})| \ \geq \ 2\alpha\rho N$$

for all u, v. Now take a set S as in Corollary 1. This set will have cardinality $\lfloor \alpha N \rfloor$ and we will have

$$|\hat{S}(a_{u,v})| \ \geq \ 2\alpha\rho N - 20\sqrt{N}.$$

A slightly tedious calculation shows that this is larger than $\alpha\rho N$, at least for N greater than some absolute constant.

The set S is an example of a small set whose Fourier transform is large at a dissociated set (a_{ij}) of points. This is in fact already an example demonstrating the optimality of Chang's theorem, as the following lemma allows us to conclude.

Lemma 4 *The set (a_{ij}) is not contained in* $\mathrm{Span}(\Lambda)$ *for any $\Lambda \subseteq \mathbf{Z}_N$ with size at most $m/2$.*

Proof. Suppose that there was such a set Λ. Let its elements be $\lambda_1, \ldots, \lambda_L$ where $L \leq m/2$, and let $\epsilon_{ijl} \in \{-1, 0, 1\}$ be such that

$$\sum_{l=1}^{L} \epsilon_{ijl}\lambda_l \ = \ a_{ij}$$

for all $1 \leq i \leq k, 1 \leq j \leq t$. The ϵ_{ijl} constitute a set of m vectors $v_{ij} \in \mathbf{Z}^L$ with $\|v_{ij}\|_\infty \leq 1$. Consider the set of all vectors of the form $\sum d_{ij}v_{ij}$ with $|d_{ij}| \leq m$. There are at least $(2m)^m$ such vectors, and they all lie in the box $[-m^2, m^2]^L \subseteq \mathbf{Z}^L$. It follows that some two of these vectors must be the same, say $\sum_{ij} d_{ij}v_{ij} = \sum_{ij} d'_{ij}v_{ij}$. Subtracting, we get integers $|r_{ij}| \leq 2m$, not all zero, such that $\sum_{ij} r_{ij}\epsilon_{ijl} = 0$ for all l. It follows immediately that $\sum_{ij} r_{ij}a_{ij} = 0$, which is contrary to our assumption that (a_{ij}) is $2m$-dissociated. □

It remains only to observe that our conditions on α and ρ ensure that $m \geq 2^{-11}\rho^2 \log(1/\alpha)$. Theorem 2 follows immediately. □

4 Sets with size $\lfloor N/2 \rfloor$.

Let $A \subseteq \mathbf{Z}_N$ be a set of size $\lfloor N/2 \rfloor$, let $\rho > 0$ be a real number, and suppose that A is ρ-large at R. As we observed in the introduction Chang's theorem gives no more information about this case than Parseval's theorem, which tells us that $|R| \ll \rho^{-2}$. In this section we show that essentially nothing more can be shown by proving Theorem 3. The following lemma constitutes the heart of the argument:

Lemma 5 *Suppose that $2^{-12} \geq \rho \geq 50N^{-1/2}$ and let S be a subset of $\mathbf{Z}_N$ of size $2^{-10}\rho^{-2}$. Then there is a subset $R \subseteq S$ with $|R| \geq |S|/12$ and a set $A \subseteq \mathbf{Z}_N$ of size $\lfloor N/2 \rfloor$ which is ρ-large at R.*

Proof. The construction goes as follows. Pass to a subset $\{s_1, \ldots, s_k\} \subseteq S$ of size $k = 2^{-11}\rho^{-2}$ such that $s_i \neq -s_j$ for any i, j. Let $\underline{\epsilon} = (\epsilon_j)$ and $\underline{\eta} = (\eta_j)$, $1 \leq j \leq k$, be vectors of real numbers. Define

$$A \;=\; A(\underline{\epsilon}, \underline{\eta}) \;=\; \left\{ x \in \mathbf{Z}_N \;\left|\; \sum_{j=1}^{k} \epsilon_j c(s_j x) + \eta_j s(s_j x) \;\geq\; 0 \right.\right\}. \tag{6}$$

We will choose the ϵ_j, η_j randomly as independent $N(0,1)$ random variables and show that with positive probability A satisfies Theorem 3 after an application of the size change lemma. The sets constructed in this way I call *gaussian randomized niveau sets*.

An important rôle will be played by the following rather general lemma.

Lemma 6 *Let $X_1, \ldots, X_n$ be random variables with $\mathbf{E}X_j \geq a$ and $\mathbf{E}X_j^2 \leq Ca^2$. Then with positive probability at least $n/2C$ of the X_j are greater than or equal to $a/4$.*

Proof. Consider the sum

$$\Sigma \;=\; \sum_{j=1}^{n} 2CaX_j - X_j^2.$$

It is easy to see that $\mathbf{E}\Sigma \geq Ca^2 n$, and so with positive probability $\Sigma \geq Ca^2 n$. Suppose that the X_j are such that this is the case. Observing that $2CaX_j - X_j^2 \leq C^2a^2$ regardless of the value of X_j, we see that at least $n/2C$ values of j are such that $2CaX_j - X_j^2 \geq Ca^2/2$. For each of these values of j we clearly have $X_j \geq a/4$. □

Equally vital is the following lemma concerning dependent gaussians.

Lemma 7 *Let $\mathbf{a} = (a_1, \ldots, a_{2k})$ and $\mathbf{b} = (b_1, \ldots, b_{2k})$ be two vectors of real numbers with $|\mathbf{a}| = |\mathbf{b}| = k$ and $\mathbf{a}.\mathbf{b} = k\cos\theta$ where $\theta \in [0, \pi)$. Let $X_1, \ldots, X_{2k}$ be independent $N(0,1)$ random variables. Then*

$$\mathrm{Prob}\left(\left(\sum_i a_i X_i \geq 0 \right) \wedge \left(\sum_i b_i X_i \geq 0 \right) \right) \;=\; \frac{1}{2\pi}(\pi - \theta).$$

Proof. It is clear that the event in question is simply the probability that the gaussian random vector $X = (X_j) \in \mathbf{R}^{2k}$ lies in a region delineated by the two hyperplanes $\mathbf{a}.\mathbf{x} = 0$ and $\mathbf{b}.\mathbf{x} = 0$. The spherical symmetry of X renders the result obvious. □

We also recall a few slightly tedious properties of the gaussian distribution function Φ defined by

$$\Phi(x) \;=\; \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2}\, dt$$

and of the inverse cosine function.

Lemma 8 (i) *For all x we have* $\left|\Phi(x) - \frac{1}{2} + \frac{x}{\sqrt{2\pi}}\right| \leq |x|^2/8$.
(ii) *For all $x \in [-1,1]$ we have* $\left|\cos^{-1}(x) - \frac{\pi}{2} + x\right| \leq \left(\frac{\pi}{2} - 1\right)|x|^2$.

Remark. One way to prove (ii) is to develop $h(x) = \left(\frac{\pi}{2} - x - \cos^{-1}(x)\right)/x^2$ as a power series about $x = 0$. All of the coefficients are positive, and so h is increasing on $[0,1)$. It is clear that $h(-x) = -h(x)$.

Recall now the definition (6) of A. In what follows we will show that $\mathbf{E}|\hat{A}(s_j)| \gg \rho N$ and that $\mathbf{E}|\hat{A}(s_j)|^2 \ll \rho^2 N^2$. Theorem 3 will then follow quickly from Lemma 6 and the size change lemma.

It is almost certainly not possible to evaluate $\mathbf{E}|\hat{A}(s_j)|$ in any useful explicit form, so we will have to make do with an estimate. Suppose for the moment that $\epsilon_1 = \epsilon, \eta_1 = \eta$ are fixed but that ϵ_j, η_j, $j = 2, \ldots, k$, are i.i.d. $N(0,1)$ random variables. We have the formula

$$\mathrm{Prob}(x \in A) \;=\; \Phi\left(\frac{-\epsilon c(s_1 x) - \eta s(s_1 x)}{\sqrt{k-1}}\right)$$

for $k \geq 2$. This arises from the fact that

$$\sum_{j=2}^{k} \epsilon_j c(s_j x) + \eta_j s(s_j x)$$

is distributed as a normal random variable with variance $k-1$. Using Lemma 8 shows, after a little computation, that

$$\mathbf{E}\left(\hat{A}(s_1) \,\middle|\, \epsilon_1 = \epsilon, \eta_1 = \eta\right) \;=\; \left(\frac{\epsilon + i\eta}{2\sqrt{2\pi k}} + E_1\right) N,$$

where $|E_1| \leq (|\epsilon| + |\eta|)/k$.

Let us now regard all of $\epsilon_1, \eta_1, \ldots, \epsilon_k, \eta_k$ as i.i.d. $N(0,1)$ random variables. It follows from the above that the random variable X_1 defined by

$$X_1 \;=\; \frac{\epsilon_1 - i\eta_1}{\sqrt{\epsilon_1^2 + \eta_1^2}} \hat{A}(s_1)$$

satisfies

$$\Re\mathbf{E}\left(X_1 \mid \epsilon_1 = \epsilon, \eta_1 = \eta\right) \;\geq\; N\sqrt{\epsilon^2+\eta^2}\left(\frac{1}{2\sqrt{2\pi k}} - \frac{2}{k}\right).$$

Thus

$$\begin{aligned}
\Re\mathbf{E}X_1 &\geq \frac{N}{2\pi}\left(\frac{1}{2\sqrt{2\pi k}} - \frac{2}{k}\right)\int \sqrt{\epsilon^2+\eta^2}e^{-(\epsilon^2+\eta^2)/2}\,d\epsilon d\eta \\
&= N\left(\frac{1}{2\sqrt{2\pi k}} - \frac{2}{k}\right)\int_0^\infty r^2 e^{-r^2/2}\,dr \\
&\geq N\left(\frac{1}{4\sqrt{k}} - \frac{3}{k}\right),
\end{aligned}$$

from which it follows that

$$\mathbf{E}|\hat{A}(s_1)| \;=\; \mathbf{E}|X_1| \;\geq\; |\mathbf{E}X_1| \;\geq\; \Re\mathbf{E}X_1 \;\geq\; N\left(\frac{1}{4\sqrt{k}} - \frac{3}{k}\right) \;\geq\; \frac{N}{\sqrt{24k}} \tag{7}$$

because $k \geq 2^{13}$. We may now turn our attention to $\mathbf{E}|\hat{A}(s_1)|^2$. There is a sense in which this is easier to handle, because

$$\mathbf{E}|\hat{A}(s_1)|^2 \;=\; \sum_{x,y\in\mathbf{Z}_N} \mathrm{Prob}(x\in A, y\in A)\omega^{s_1(x-y)}. \tag{8}$$

The estimation of $\mathrm{Prob}(x \in A, y \in A)$ is dealt with by Lemma 7, taking $\mathbf{a}$ to be the vector

$$(c(s_1x), s(s_1x), \ldots, c(s_kx), s(s_kx))$$

and $\mathbf{b}$ to be the corresponding vector with x replaced by y. It is clear that for this choice we have

$$\cos\theta \;=\; \frac{1}{k}\sum_{j=1}^{k} c\left(s_j(x-y)\right).$$

Invoking Lemma 8 (ii) and (8), and recalling that $s_j \neq -s_i$, we have that

$$\begin{aligned}
\mathbf{E}|\hat{A}(s_1)|^2 &= \frac{N}{2\pi k}\sum_{x\in\mathbf{Z}_N}\sum_{j=1}^{k} c(s_jx)\omega^{s_1x} + E \\
&= \frac{N^2}{4\pi k} + E,
\end{aligned}$$

where E, the error, can be bounded by

$$\begin{aligned}
|E| &\leq \frac{\left(\frac{\pi}{2}-1\right)N}{2\pi k^2}\sum_x \left|\sum_{j=1}^{k} c(s_jx)\right|^2 \\
&= \frac{\left(\frac{\pi}{2}-1\right)N^2}{4\pi k}.
\end{aligned}$$

It follows that

$$\mathbf{E}|\hat{A}(s_1)|^2 \ \leq \ \frac{N^2}{8k}. \tag{9}$$

Now the two main inequalities we have derived, namely (7) and (9), clearly hold with any s_j in place of s_1. Thus Lemma 6 tells us that with positive probability at least $k/6$ of the $\hat{A}(s_j)$ have magnitude at least $N/20\sqrt{k}$. Choose a specific A with this property.

We do not know anything about the size of A, but this does not matter because of the size change lemma. Let $|A| = \alpha N$ and apply the size change lemma with $\rho = (20\alpha\sqrt{k})^{-1}$. The conditions on ρ ensure that $k \leq 2^{-22}N$, so the lemma applies to give us a set A', $|A'| = \lfloor N/2 \rfloor$, for which

$$|\hat{A}'(s_j)| \ \geq \ \frac{|A'|}{40\sqrt{k}}$$

for at least $k/6$ values of j.

Recalling that $k = 2^{-11}\rho^{-2}$, we see that Lemma 5 holds. □

The deduction of Theorem 3 involves a repeated application of Lemma 5. This iteration is not as easy to carry out as one might think, and the key is the following lemma. In this lemma R is a fixed subset of $\mathbf{Z}_N$ of size $2^{-10}\rho^{-2}$.

Lemma 9 *Let $\gamma, \eta \in [0,1]$ satisfy $\gamma \leq \rho$, $\gamma\eta \geq 2^{15}N^{-1/2}$ and $2^{-12}\eta^{1/2} \geq \rho \geq 50N^{-1/2}$. Suppose that there is a set $A \subseteq \mathbf{Z}_N$, $|A| = \lfloor N/2 \rfloor$ and a subset $S \subseteq R$, $|S| \geq (1-\eta)|R|$, such that A is γ-large at S. Then there is a set $A' \subseteq \mathbf{Z}_N$, $|A'| = \lfloor N/2 \rfloor$ and a subset $S' \subseteq R$, $|S'| \geq \left(1 - \frac{23}{24}\eta\right)|R|$, such that A' is $\gamma\eta/200$-large at S'.*

Proof. By Lemma 5 we may certainly pick a set $T \subseteq R \setminus S$, $|T| \geq \eta|R|/12$, and a set $B \subseteq \mathbf{Z}_N$, $|B| = \lfloor N/2 \rfloor$, such that B is $(\eta^{-1/2}\rho)$-large at T. It is easy to check that the conditions of the present lemma imply those of Lemma 5. Set $S_0 = S \cup T$. Pick $\mu \in [0, \gamma/2\rho]$ at random according to the uniform distribution and set $f(x) = A(x) + \mu B(x)$. We estimate, for a given $r \in S_0$, the probability p_r that $|\hat{f}(r)| < \eta\gamma N/192$. There are two cases to consider.

Case 1. $|\hat{B}(r)| \geq \rho N/2$. Then the measure of the set

$$\left\{ t \in \mathbf{R} \ \Big| \ \left|\hat{A}(r) + t\hat{B}(r)\right| \leq \eta\gamma N/192 \right\}$$

is at most $\eta\gamma/48\rho$. It follows that

$$p_r \ \leq \ \eta/24. \tag{10}$$

Case 2. $|\hat{B}(r)| < \rho N/2$. Then r is certainly not in T, and so $r \in S$. Hence $|\hat{A}(r)| \geq \gamma N/2$ and

$$|\hat{f}(r)| \ \geq \ \frac{\gamma N}{2} - \frac{|\mu|\rho N}{2} \ \geq \ \frac{\gamma N}{4} \ \geq \ \frac{\eta\gamma N}{192}$$

automatically, and so in this case $p_r = 0$.

It follows immediately that the expected number of $r \in S_0$ for which $|\hat{f}(r)| \geq \eta\gamma N/192$ is at least

$$\begin{aligned}\left(1 - \tfrac{1}{24}\eta\right)|S_0| &= \left(1 - \tfrac{1}{24}\eta\right)\left(1 - \tfrac{11}{12}\eta\right)|R| \\ &\geq \left(1 - \tfrac{23}{24}\eta\right)|R|.\end{aligned}$$

Pick a specific μ for which this inequality holds, let S' be the set of all r for which $|\hat{f}(r)| \geq \eta\gamma N/192$ and let $g(x) = f(x)/(1+\mu)$. Then $\sum_x g(x) = N/2$ and $|\hat{g}(r)| \geq \eta\gamma N/288$ for all $r \in S'$. Choose, as allowed by Lemma 1, our set A' to satisfy $|A'| = \lfloor N/2 \rfloor$ and $\|\hat{g} - \hat{A}\|_\infty \leq 20\sqrt{N}$. Then for all $r \in S'$ we have

$$\begin{aligned}|\hat{A}'(r)| &\geq \frac{\gamma\eta N}{288} - 20\sqrt{N} \\ &\geq \frac{\gamma\eta N}{400}\end{aligned}$$

provided that $\gamma\eta \geq 2^{15}N^{-1/2}$. □

Now apply Lemma 9 repeatedly. We may start with $\eta_0 = 1$ and $\gamma_0 = \rho$. At the jth step we may take $\gamma_j = 200^{-j}(23/24)^{j(j+1)/2}\rho$ and $\eta_j = (23/24)^j$. Taking $j = 55$ we can check that $\eta_j < 0.1$ whilst $\gamma_j > 2^{-515}\rho$. Such repeated applications of Lemma 9 are valid provided that $2^{-14} \geq \rho \geq 2^{534}N^{-1/2}$. A short calculation confirms that Theorem 3 holds, and in fact that we can take $c = 2^{-1060}$. □

5 Concluding remarks.

As remarked earlier it is rather irritating that we were unable to prove Theorem 3 with 100 percent in place of 90 percent. It might also be of interest to prove the theorem with a "reasonable" value of the constant c.

This paper seems to be the first place in which questions of this sort have been addressed. However we should like to draw the reader's attention to the paper [**?**] in which the issue of how often $|\hat{A}(r)|$ can be *very* large, namely at least $(1-\epsilon)|A|$, is addressed. This question and the techniques used to tackle it turn out, however, to be of a very different nature to those in this paper.

References

[1] Green, B.J. *Edinburgh lecture notes on Freiman's theorem*, available at `http://www.dpmms.cam.ac.uk/~bjg23`