Some properties of lower level-sets of convolutions

Ernie Croot *

August 10, 2011

Abstract

In the present paper we prove a certain lemma about the structure of "lower level-sets of convolutions", which are sets of the form $\{x \in \mathbb{Z}_N : 1_A * 1_A(x) \leq \gamma N\}$ or of the form $\{x \in \mathbb{Z}_N : 1_A * 1_A(x) < \gamma N\}$, where A is a subset of $\mathbb{Z}_N$. One result we prove using this lemma is that if $|A| = \theta N$ and $|A + A| \leq (1 - \varepsilon)N$, $0 < \varepsilon < 1$, then this level-set contains an arithmetic progression of length at least N^c, $c = c(\theta, \varepsilon, \gamma) > 0$. For various reasons (discussed in the paper) one might think, wrongly, that such a result would only be possible for level-sets involving triple and higher convolutions.

AMS Subject Classification: 11B30

1 Introduction

There are many conditions that one can give on a subset $A \subseteq G$, where G is a finite additive abelian group, guaranteeing that $A + A = \{a + b : a, b \in G\} = G$ or that $A + A$ is *nearly* all of G (e.g. if $|A| > |G|/2$ or if the non-trivial Fourier coefficients of the indicator function 1_A are all "small"). And one might wonder whether there are some simple conditions on the set $A + A$ *itself* guaranteeing that it is all of G, or at least a substantial proportion of G; for example, is there a particular small set S such that if we know that $A + A$ contains

*Supported by NSF grant DMS-1001111

S and $|A| > |G|/\log|G|$, say, then $A+A$ must essentially be all of G? In the present paper we develop some related results. The key idea behind most of them is a lemma (actually, Corollary 3) on the structure of level-sets of convolutions given in a later section.

In order to discuss some of these results, we will need some notation: suppose that G is a finite group and that $g : G \to \mathbb{C}$. We define the expectation operator

$$\mathbb{E}g \ = \ \mathbb{E}_x g \ := \ |G|^{-1} \sum_{x \in G} g(x);$$

we define for an additive abelian groups G the (unnormalized) convolution $f * g$ of two functions $f, g : G \to \mathbb{C}$ to be

$$f * g(x) \ := \sum_{\substack{a+b=x \\ a,b \in G}} f(a)g(b) \ = \ |G| \cdot \mathbb{E}_{a \in G} f(a)g(x-a);$$

given $f : G \to \mathbb{C}$ we define the (unnormalized) Fourier transform at $\chi \in \hat{G}$ to be

$$\hat{f}(\chi) \ := \ \sum_{x \in G} f(x)\chi(x) \ = \ |G| \cdot \mathbb{E}_x f(x)\chi(x);$$

and lastly, we say that a function $f : G \to \mathbb{C}$ is α-uniform if

$$\max_{\chi \in \hat{G}} |\hat{f}(\chi)| \ \leq \ \alpha |G|.$$

An easy consequence of the triangle inequality and the linearity of the Fourier transform is that if $f_1, ..., f_k$ are $\alpha_1, ..., \alpha_k$-uniform, respectively, then their sum $f_1 + \cdots + f_k$ is $\alpha_1 + \cdots + \alpha_k$-uniform.

Our first result is along the lines of what we described above, except that we replace the condition that $A+A$ contains S with the condition that $1_A * 1_A(s)$ is "large" for all $s \in S$ – such a condition is often easier and more natural to work with than having $A + A$ contain S:

Theorem 1 *Suppose G is an additive abelian group with $|G| = N$, and suppose that $A \subseteq G$, $|A| = \theta N$. Then, for every $\delta, \varepsilon > 0$ there exists a set $S \subseteq G$ satisfying*

$$|S| \ \ll \ \varepsilon^{-1}\delta^{-6}\theta^{-10}(\log N - \log(\delta\theta\varepsilon)),$$

such that if $1_A * 1_A(x) > \delta\theta^2 N$ for every $x \in S$, then $|A+A| \geq (1-\varepsilon)N$.

Note: The expected value of $1_A * 1_A$ is $\theta^2 N$; so, the condition $1_A * 1_A(x) > \delta\theta^2 N$ is just requiring that the convolution be more than δ times as big as this expected value.

This theorem is not far from best-possible in that $|S|$ needs to be $\Omega(\log N)$ in order for the conclusion of the theorem to hold, as the following result demonstrates for $\theta \geq 1/3$:

Theorem 2 *For every sufficiently large prime N, and every set $S \subseteq \mathbb{Z}_N$ of size at most $(\log N)/2$, there exists a set $A \subseteq \mathbb{Z}_N$ of size $|A| \geq N/3$ such that $|A + A| < 2N/3$ and such that $1_A * 1_A(x) > N/6$ for every $x \in S$.*

Not only is it possible to show that *there exists* a set S having the requisite properties given in Theorem 1, but, in fact, if we allow $|S|$ to be somewhat larger than Theorem 1 requires then we can show that *any* set S whose non-trivial Fourier coefficients are sufficiently "small" (indicated below) will do.

Theorem 3 *Suppose that G is an additive abelian group satisfying $|G| = N$, and suppose that $\delta, \varepsilon, \theta > 0$ are parameters that we allow to depend on N. Let $S \subseteq G$ be a set such that*

$$\max_{\substack{\chi \in \hat{G} \\ \chi \neq \chi_0}} |\hat{1}_S(\chi)| \ < \ (\delta^3 \theta^{4.5} \sqrt{\varepsilon}/512\pi)^{512\delta^{-6}\theta^{-12}\varepsilon^{-1}+1}|S|,$$

where χ_0 denotes the principal character. Then, if $A \subseteq G$ satisfies $|A| \geq \theta N$ and $1_A * 1_A(x) > \delta\theta^2 N$ for every $x \in S$, we will have that $|A + A| \geq (1 - \varepsilon)N$.

See [1] for some explicit constructions of small sets S, all of whose non-trivial Fourier coefficients are small.

The last set of results we prove are rather different from the ones listed above and pertain to the existence of long arithmetic progressions and other structures in level-sets of the convolution $1_A * 1_A(x)$. By *level-set* here we mean a set having the form $\{x \in G \ : \ 1_A * 1_A(x) \leq \gamma|G|\}$ or having the form $\{x \in G \ : \ 1_A * 1_A(x) < \gamma|G|\}$. As these results make use of Bohr neighborhoods, now is a good time to define them:

Definition. Suppose that $\Lambda := \{\chi_1, ..., \chi_k\} \subseteq \hat{G}$ and that $\varepsilon > 0$. Then, the Bohr neighborhood of radius ε determined by Λ is defined to be the set

$$\mathcal{B}(\Lambda, \varepsilon) \ := \ \{x \in G \ : \ \text{for} \ \ i = 1, ..., k, \ |1 - \chi_i(x)| \leq \varepsilon\}.$$

The *dimension* of a Bohr neighborhood is the least number of places χ_i needed to define the set; so, this $\mathcal{B}(\Lambda, \varepsilon)$ we wrote down has dimension at most k.

Our first result along these lines is stated as follows:

Theorem 4 *Suppose that G is an additive abelian group satisfying $|G| = N$; suppose that $A \subseteq G$, $|A| = \theta N$; and suppose that for $\delta > 0$,*

$$|\{x \in G \ : \ 1_A * 1_A(x) < \delta^3\theta^6 N/128\}| \ \geq \ \varepsilon N. \qquad (1)$$

Then, we have that the level-set

$$\{x \in G \ : \ 1_A * 1_A(x) < \delta\theta^2 N\} \qquad (2)$$

contains a translate of a Bohr neighborhood of dimension at most $512\delta^{-6}\theta^{-12}\varepsilon^{-1} + 1$ and radius $\delta^3\theta^{4.5}\sqrt{\varepsilon}/128$.

Furthermore, if $G = \mathbb{Z}_N$, where N is prime, then using the fact that large Bohr neighborhoods always contain long arithmetic progressions, we have in this case that (2) contains an arithmetic progression of length at least N^c, where $c = c(\theta, \varepsilon, \delta)$.

It is relatively straightforward to use standard Fourier arguments to deduce that the level-set (2) contains *most* of a translate of a Bohr neighborhood; and, using ideas due originally to Bogolyubov [5] one can deduce that the triple-convolution analogue of (2) – e.g. $\{x \in G : 1_A * 1_A * 1_A(x) < \delta\theta^3 N^2\}$ – contains a complete shifted Bohr neighborhood (see also [10] and [15]).

By replacing the condition (1) with simply an upper bound for $|A + A|$ we arrive at the following corollary:

Corollary 1 *Suppose that $A \subseteq G$, $|A| = \theta N$, and $|A + A| \leq (1 - \varepsilon)N$. Then, we deduce that the set (2) contains the same translate of the Bohr neighborhood indicated by Theorem 4 (and the associated arithmetic progression of length at least N^c in the case $G = \mathbb{Z}_N$, N prime).*

Interestingly, a consequence of a construction of Ruzsa [14] is that there exist sets A for which the complement of this level-set cannot contain progressions of length larger than $\exp((\log N)^{2/3+\varepsilon})$. So, there is something seemingly paradoxical going on: the "lower level sets" $\{x \in \mathbb{Z}_N : 1_A * 1_A(x) \leq \delta\theta^2 N\}$ *always* contain power-of-N-length arithmetic progressions provided $|A+A|$ isn't too large, whilst the "upper level sets" $\{x \in \mathbb{Z}_N : 1_A * 1_A(x) \geq \delta\theta^2 N\}$ *sometimes* do not.

From (the contrapositive of) Corollary 1 one can immediately deduce the following additional corollary, which gives another way to think about the result:

Corollary 2 *Suppose that $A \subseteq \mathbb{Z}_N$ satisfies $|A| = \theta N$, where N is prime. Furthermore, suppose that for every $x \in \mathbb{Z}_N$ satisfying $1_A * 1_A(x) \geq \delta\theta^2 N$ and for every $d \in \mathbb{Z}_N$, $d \neq 0$, we have that there exists $0 < t \leq N^c$, $c = c(\theta, \varepsilon, \delta) > 0$, such that $1_A * 1_A(x + dt) \geq \delta\theta^2 N$. (In other words, the gaps along APs of common difference $d = 1, ..., N-1$ where $1_A * 1_A(x)$ is "large", are all bounded from above by N^c.) Then, $|A + A| \geq (1 - \varepsilon)N$.*

The remainder of the paper is organized as follows: in section 2 we list some conjectures that, if true, would give much stronger structural information about lower level-sets than Theorem 4 provides; in section 3 we list out two technical lemmas used throughout the rest of the paper; in section 4 we state and prove the main lemma of the paper, and discuss some immediate consequences of it; in section 5 we prove Theorems 1, 2, 3, 4; finally, the remaining sections are devoted to acknowledgements and the bibliography.

2 Future directions

In this section we list some conjectures motivated by Theorem 4 that would be natural "next steps" for where to continue this work.

We begin by noting that Theorem 4 shows that certain level-sets always contain long arithmetic progressions (when the group is $G = \mathbb{Z}_N$, N prime), and one might wonder wether *complements* of sumsets always contain such long arithmetic progressions (which is itself the level-set $\{x : 1_A * 1_A(x) = 0\}$); in other words, in order to get the long-progressions conclusion in Theorem 4, must one necessarily work with level-sets of the form $\{x : 1_A * 1_A(x) < \delta\theta^2 N\}$, where $\delta > 0$? This motivates the following conjecture:

Conjecture 1. For every sufficiently large prime N there exists a set $A \subseteq \mathbb{Z}_N$, $|A| > N/4$, say, such that $|A+A| \leq 99N/100$ (say), and such that the longest arithmetic progression in the complement of $A + A$ has length at most $N^{o(1)}$.

Perhaps something like Ruzsa's construction [14] can be made to prove this conjecture; however, the author has not yet been able to do so.

The author also cannot immediately see any reason why the results in Theorem 4 could not be made much stronger; perhaps, in fact, the following is true:

Conjecture 2. The following holds for certain absolute constants $0 < c_1, c_2, c_3, c_4 < 1$ and primes N sufficiently large: suppose that $A \subseteq \mathbb{Z}_N$, $|A| > N \exp(-(\log N)^{c_1})$ and $|A + A| \leq N(1 - \exp(-(\log N)^{c_2}))$. Then, the lower level-set $\{x \in \mathbb{Z}_N : 1_A * 1_A(x) < N \exp(-(\log N)^{c_3})\}$ contains an arithmetic progression of length at least $\exp((\log N)^{c_4})$.

An even stronger conjecture would be that, up to some small error, the level-set above is, in fact, *covered* by disjoint translates of some given large Bohr neighborhood. One formulation of such a conjecture is as follows:

Conjecture 3. The following holds for certain absolute constants $0 < c_1, c_2, c_3, c_4, c_5 < 1$ and primes N sufficiently large: suppose that $A \subseteq G$, where G is a finite abelian group of size N, where $|A| > N \exp(-(\log N)^{c_1})$ and $|A+A| \leq N(1-\exp(-(\log N)^{c_2}))$. Then, there exists a Bohr neighborhood $\mathcal{B}$ of dimension at most $(\log N)^{c_3}$ and size $|\mathcal{B}| \geq N \exp(-(\log N)^{c_4})$, and a set of translates $t_1, ..., t_k$ with $\mathcal{B} + t_i$ all disjoint, such that if we let

$$S := \cup_{i=1}^{k} (t_i + \mathcal{B}),$$

then the symmetric difference between S and the lower level-set $\{x \in \mathbb{Z}_N : 1_A * 1_A(x) < N \exp(-(\log N)^{c_5})\}$ has size at most $|S|/100$.

The sort of approach that *might* work here would be to combine ideas from the present paper with those from [6] and [15]; however, the author currently cannot see how to do this.

Besides being interesting problems in their own right, the two last conjectures above *could* perhaps be used to deduce good upper bounds

on the largest subset $A \subseteq \mathbb{Z}_N$ having no non-trivial solutions x, y, z to a given linear equations $a_1x + a_2y + a_3z \equiv 0 \pmod N$, where $a_1+a_2+a_3 \equiv 0 \pmod N$, thereby sharpening the already remarkable results of Sanders [16], to achieve a similar success for such problems as was recently done by Schoen and Shkredov in their sensational paper [17] for equations involving six or more variables (that produced upper bounds for $|A|$ of the general form of the Behrend [3] [8] [11] bound for particular choices of the a_i's) and by Bloom [4] for equations involving four variables and higher (in this paper he beautifully generalized Sanders's proof [16]). Both of these papers [4] and [17] make use of ideas from [7], [15] and [16].

There might also be a way to use a proof of Conjecture 3 to improve upon the breakthrough results of Bateman and Katz [2].

Here is a rough idea of exactly *how* the last two conjectures above might be applicable to problems about solutions to linear equations: it is easiest to describe this in the case where $G = \mathbb{Z}_3^n$, so let us make this assumption; and, let us suppose that $A \subseteq G$ has no solutions to $x+y-2z = 0$ – that is, no solutions to $x+y+z = 0$, since $-2 = 1$ in $\mathbb{Z}_3$. It follows that $-A$ is a subset of the level-set $\{x \in G : 1_A * 1_A(x) \leq 1\}$. If we knew that this level-set were approximately the disjoint union of translates of some large Bohr neighborhood $\mathcal{B}$, then one of those translates $t + \mathcal{B}$ should intersect $-A$ in many elements; indeed, one would expect that $(-A) \cap (t + \mathcal{B})$ has a higher density in $t + \mathcal{B}$ than $-A$ does in G. This is exactly what we need in order to implement a "density increment strategy" for showing that $|A|$ must be rather small, as was first done by Roth [13].

3 Some auxiliary lemmas

In this section we list some basic lemmas (and prove two of them) that we use in later sections in the proofs of our main theorems.

Lemma 1 *Suppose that G is an additive abelian group with $|G| = N$, and that $g, h : G \to [0, 1]$, $\mathbb{E}g = \theta$. Then, if $g - h$ is δ_1-uniform we will have*

$$\sum_{x \in G} |g * g(x) - h * h(x)|^2 \ \leq \ \delta_1^2(4\theta + \delta_1)N^3.$$

Proof of the Lemma. First note that since $g - h$ is δ_1-uniform and since $\mathbb{E}(g) = \theta$, we have that $\mathbb{E}(h) \leq \theta + \delta_1$; and so, since $g, h : \mathbb{Z}_N \to$

$[0,1]$ this implies that

$$\sum_{x\in G}(g+h)(x)^2 \;\leq\; (4\theta+\delta_1)N. \tag{3}$$

And now from Parseval's identity we then have:

$$\begin{aligned}\sum_{x\in G}|g*g(x)-h*h(x)|^2 &= \sum_{x\in G}|(g-h)*(g+h)(x)|^2\\ &= N^{-1}\sum_{\chi\in\hat{G}}|\widehat{(g-h)}(\chi)|^2|\widehat{(g+h)}(\chi)|^2\\ &\leq \delta_1^2 N\sum_{\chi\in\hat{G}}|\widehat{(g+h)}(\chi)|^2\\ &= \delta_1^2N^2\sum_{x\in G}(g+h)(x)^2,\end{aligned}$$

which, in combination with (3), proves the lemma. ■

Lemma 2 *Suppose that $h: G\to[0,1]$, where G is an additive abelian group satisfying $|G|=N$. Then, if we place the Fourier coefficients in order from largest to smallest,*

$$|\hat{h}(\chi_1)| \;\geq\; |\hat{h}(\chi_2)| \;\geq\; \cdots \;\geq\; |\hat{h}(\chi_N)|, \tag{4}$$

where $\{\chi_1,...,\chi_N\}=\hat{G}$, we will have that

$$|\hat{h}(\chi_k)| \;\leq\; N\sqrt{\mathbb{E}(h)/k}.$$

Note: Because we may have $|\hat{h}(\chi_i)|=|\hat{h}(\chi_{i+1})|$ for some $i=1,...,N$, the order of the χ_i's is not necessarily well-defined. However, the conclusion of the lemma does not depend on this choice; furthermore, for the applications of this lemma in later sections the choice of ordering of the χ_i's does not matter so long as they respect (4).

Proof of the lemma. We have from Parseval's identity that

$$k|\hat{h}(\chi_k)|^2 \;\leq\; \sum_{\chi\in\hat{G}}|\hat{h}(\chi)|^2 \;\leq\; \mathbb{E}(h)N^2.$$

Solving for $|\hat{h}(\chi_k)|$, the lemma follows. ■

Finally, we will need the following lemma, which can be found in [18, sec. 4.4], that gives a lower bound on the cardinalities of certain Bohr neighborhoods:

Lemma 3 *Suppose G is an additive abelian group satisfying $|G| = N$. If $\Lambda \subseteq \hat{G}$, $|\Lambda| = d$, then for $r \in [0,2]$ we have $|\mathcal{B}(\Lambda, r)| \geq (r/2\pi)^d N$. Furthermore, if $G = \mathbb{Z}_N$ where N is prime then this Bohr neighborhood contains an arithmetic progression of size at least $rN^{1/d}/2\pi$.*

4 The key lemma and its proof

Before we can state the main lemma, we need to define the notion of a "generalized convolution" for finite groups: suppose that G is a finite group (possibly non-abelain) where the operation is written multiplicatively, and suppose that $T : G \times G \to G$. Then, for two functions $f, g : G \to \mathbb{C}$ we define the *T-convolution of f with g* to be

$$f *_T g(x) \;=\; \sum_{\substack{a,b \in G \\ T(a,b)=x}} f(a)g(b).$$

Associated with this generalized convolution, we define a parameter

$$\kappa = \kappa(T) \;:=\; \max(\kappa_1, \kappa_2),$$

where

$$\begin{aligned} \kappa_1 \;&:=\; \max_{x \in G} \max_{a \in G} |\{b \in G \;:\; T(a,b) = x\}|; \text{ and} \\ \kappa_2 \;&:=\; \max_{x \in G} \max_{a \in G} |\{b \in G \;:\; T(b,a) = x\}|. \end{aligned}$$

Note that in the case where $T(a,b) = ab$, the convolution $f *_T g(x)$ coincides with the usual group convolution $f * g(x) = \sum_{\substack{a,b \in G \\ ab=x}} f(a)g(b)$; furthermore, the parameter $\kappa = \kappa_1 = \kappa_2 = 1$ in this case.

Our main lemma is given as follows:

Lemma 4 *Suppose that $\|\cdot\|$ is a norm on the space of functions $f : G \to \mathbb{C}$, where G is a finite group (possibly non-abelian) of size N, and that $T : G \times G \to G$ has associated parameter κ as defined above. Further, suppose that $\delta_1, \delta_2 > 0$ are parameters we allow to depend on N, and that $A \subseteq G$ satisfies $|A| = \theta N \geq \delta_2 N > 0$. Then, there exists a function $f : G \to [0,1]$ satisfying $\|f - 1_A\| \leq \delta_1$ such that for every $B, C \subseteq G$ with $\|1_B - 1_A\|, \|1_C - 1_A\| \leq \delta_1$, we have that*

$$1_B *_T 1_C(x) \;\leq\; \delta_2^{-2} f *_T f(x) + 2\kappa\delta_2 N.$$

In order to make much use of this lemma, it seems that the choice of norm should somehow be related to the convolutions $1_B *_T 1_B$ and $f *_T f$. In the case where G is an additive abelian group and $T(a,b) = a+b$, Lemma 1 implies that there is a natural choice for the norm having this property, namely we can use $\|g\| = N^{-1}\max_{\chi\in\hat{G}}|\hat{g}(\chi)|$, $N = |G|$. This now brings us to the following immediate corollary of Lemma 4:

Corollary 3 *Suppose that G is an additive abelian group with $|G| = N$. Suppose that $\delta_1, \delta_2 > 0$ are parameters we allow to depend on N, and that $A \subseteq G$ satisfies $|A| = \theta N \geq \delta_2 N > 0$. Then, there exists a function $f : G \to [0,1]$ such that $f - 1_A$ is δ_1-uniform and such that for every $B, C \subseteq G$ having the properties that both $1_B - 1_A$ and $1_C - 1_A$ are δ_1-uniform, we have*

$$1_B * 1_C(x) \ \leq \ \delta_2^{-2} f * f(x) + 2\delta_2 N.$$

We now will try to give some idea of what Lemma 4 is saying by considering the special case of the above corollary with $G = \mathbb{Z}_N$: fix a subset $A \subseteq \mathbb{Z}_N$ of size θN and then consider all the other sets $B \subseteq \mathbb{Z}_N$ such that $1_B - 1_A$ is "highly uniform" – that is, $1_B - 1_A$ is δ_1-uniform, where $\delta_1 > 0$ is "small". Lemma 1 then implies that the convolutions $1_B * 1_B$ and $1_A * 1_A$ are "close" to one another in an L^2 sense; but they need not be close in an L^∞ sense, and in fact they cannot be in general. A good example to demonstrate the point is to consider the case where $N \equiv 3 \pmod 4$ is a prime number, and where $A = \{x^2 \pmod N \ : \ 1 \leq x \leq N-1\}$, which has size about $N/2$. This set has the property that $1_A * 1_A(0) = 0$, while $1_A * 1_A(x) \sim N/4$ for $x \neq 0$. Furthermore, all the non-zero Fourier coefficients of 1_A are "small"; indeed, for $a \not\equiv 0 \pmod N$ we have from Gauss sum estimates that $|\hat{1}_A(a)| \ll \sqrt{N}$. If we now define the set $A_t := A + t$ then we likewise will have that $1_{A_t} * 1_{A_t}(2t) = 0$, and that $|\hat{1}_{A_t}(a)| \ll \sqrt{N}$ for $a \not\equiv 0 \pmod N$. In particular, the level-sets $\{x \in \mathbb{Z}_N : 1_A * 1_A(x) < N/8\}$ and $\{x \in \mathbb{Z}_N : 1_{A_t} * 1_{A_t}(x) < N/8\}$, are disjoint for $t \not\equiv 0 \pmod N$ (the first level-set here is $\{0\}$, while the second is $\{2t\}$), even though $1_A - 1_{A_t}$ is $O(1/\sqrt{N})$-uniform; in addition,

$$\|1_A * 1_A - 1_{A_t} * 1_{A_t}\|_\infty \ = \ \max_{x\in\mathbb{Z}_N} |1_A * 1_A(x) - 1_{A_t} * 1_{A_t}(x)| \ \sim \ N/4,$$

which is rather large.

It would seem that this is pretty much all that one can say on the intersection of level-sets; but Corollary 3 says that if the lower

level-sets we are considering are all rather large (instead of just a single element as in the example involving the squares mod N), then in fact they all have large intersection. The following corollary of the Corollary 3 gives a quantitative version of this fact:

Corollary 4 *Suppose G is an additive abelian group satisfying $|G| = N$, and fix a subset $A \subseteq G$, $|A| = \theta N$. Then, letting $0 < \gamma \leq 1$ and letting*

$$I := \bigcap_{\substack{B \subseteq G \\ 1_A - 1_B \text{ is } \delta-\text{uniform}}} \{x \in G : 1_B * 1_B(x) \leq \gamma\theta^2 N\},$$

we have that

$$|I| \geq |\{x \in G : 1_A * 1_A(x) \leq \gamma^3\theta^6 N/128\}| - 2^{14}\gamma^{-6}\theta^{-12}\delta^2(4\theta+\delta)N.$$

If we furthermore suppose that $|A+A| \leq (1-\varepsilon)N$ then we immediately deduce from this corollary that

$$|I| \geq (\varepsilon - 2^{14}\gamma^{-6}\theta^{-12}\delta^2(4\theta+\delta))N.$$

For fixed $\theta, \varepsilon, \gamma > 0$, then, we see that if $\delta > 0$ is sufficiently small in terms of θ, ε and γ, we must have that $|I| \gg \varepsilon N$.

Proof of the Corollary. Let $\delta_1 = \delta$, $\delta_2 = \gamma\theta^2/4$, and then let $f : G \to [0,1]$ be the function given by our Corollary 3. We have then for every $x \in G$ such that $f * f(x) \leq \gamma^3\theta^6 N/64$ and for every set $B \subseteq G$ where $1_A - 1_B$ is δ-uniform,

$$1_B * 1_B(x) \leq \delta_2^{-2} f * f(x) + 2\delta_2 N \leq 3\gamma\theta^2 N/4.$$

Next we apply Lemma 1 using $g = 1_A$, $h = f$, and deduce that if we let S be the set of all $x \in G$ such that $1_A * 1_A(x) \leq \gamma^3\theta^6 N/128$, and $T \subseteq S$ be those $x \in S$ where $f * f(x) > \gamma^3\theta^6 N/64$, then

$$|T|(\gamma^3\theta^6 N/128)^2 \leq \delta_1^2(4\theta+\delta_1)N^3;$$

that is,

$$|T| \leq 2^{14}\gamma^{-6}\theta^{-12}\delta^2(4\theta+\delta)N,$$

which completes the proof of the Corollary. ∎

4.1 Proof of Lemma 4

The proof of this lemma iterates on single places $x \in G$ where some convolution $1_B *_T 1_C(x)$ is "large", which makes it somewhat like the Dyson e-transform and also the Katz-Koester Lemma [12].

We begin by constructing a sequence of functions $f_1, f_2, ...$ according to the following algorithm:

1. Set $f_1 := 1_A$, and set $j := 1$.
2. Suppose we have constructed f_j. If for every pair of sets $B, C \subseteq G$ such that $\|1_A - 1_B\|, \|1_A - 1_C\| \leq \delta_1$ we have that

$$1_B *_T 1_C(x) \ \leq \ f_j *_T f_j(x) + 2\kappa\delta_2 N \text{ for every } x \in G,$$

   then we STOP.
3. Otherwise, there exist sets $B, C \subseteq G$ for which $\|1_A - 1_B\|, \|1_A - 1_C\| \leq \delta_1$, and for which there exists $x \in \mathbb{Z}_N$ satisfying

$$1_B *_T 1_C(x) \ > \ f_j *_T f_j(x) + 2\kappa\delta_2 N.$$

   Given such sets B, C we either set $f_{j+1} := f_j + 1_B$ or $f_{j+1} := f_j + 1_C$, according to which of these two possibilities makes f_{j+1} have the larger support (if there is a tie in the size of the support, simply choose $f_{j+1} := f_j + 1_B$). Then, set $j \leftarrow j + 1$.
4. And then we loop back to the second step.

Let us see that this procedure must eventually terminate: first, we note that $1 \leq f_j(x) \leq j$ for all $x \in \text{supp}(f_j)$ and for all $j \geq 1$. Given f_j, if there exist sets $B, C \subseteq G$ as in the third step, we must have that there exists $x \in G$ satisfying

$$1_B *_T 1_C(x) \ > \ f_j *_T f_j(x) + 2\kappa\delta_2 N.$$

Thus, there are more than $f_j *_T f_j(x) + 2\kappa\delta_2 N$ pairs

$$(b, c) \ \in \ B \times C \text{ with } T(b, c) = x,$$

while there are at most $f_j *_T f_j(x)$ pairs

$$(b, c) \ \in \ \text{supp}(f_j) \times \text{supp}(f_j) \text{ with } T(b, c) = x.$$

It follows that there are more than $2\kappa\delta_2 N$ pairs $(b, c) \in B \times C$ with $T(b, c) = x$ for which either b or c fails to belong to $\text{supp}(f_j)$. Clearly,

then, there are either at least $\kappa\delta_2 N$ pairs $(b,c) \in B \times C$ for which $T(b,c) = x$ and $b \notin \mathrm{supp}(f_j)$; or, there are at least $\kappa\delta_2 N$ pairs $(b,c) \in B \times C$ for which $T(b,c) = x$ and $c \notin \mathrm{supp}(f_j)$. Suppose that the former holds; then, since for fixed b and x there can be at most κ choices for $c \in G$ with $T(b,c) = x$, it follows that there are at least $\delta_2 N$ elements $b \in B$ that do not belong to $\mathrm{supp}(f_j)$. And if the latter holds, then there are at least $\delta_2 N$ elements $c \in C$ that do not belong to $\mathrm{supp}(f_j)$. Clearly, then, the support of f_{j+1} is larger than the support of f_j by at least $\delta_2 N$ elements. Iterating this, and using the fact that

$$|A| \;=\; \mathrm{supp}(1_A) \;=\; \theta N \;\geq\; \delta_2 N,$$

we deduce that the support of f_j has size at least $j\delta_2 N$, which implies that the procedure must terminate with a function f_J where $J \leq \delta_2^{-1}$. We then just let $f := J^{-1} f_J$. And now, since

$$f_J *_T f_J(x) \;=\; J^2 f *_T f(x) \;\leq\; \delta_2^{-2} f *_T f(x) \text{ for every } x \in G,$$

and since at this last iteration that produced f_J we stopped at step 2 in the above algorithm, it follows that for every pair of sets $B, C \subseteq G$ such that $\|1_A - 1_B\|, \|1_A - 1_C\| \leq \delta_1$,

$$1_B *_T 1_C(x) \;\leq\; \delta_2^{-2} f *_T f(x) + 2\kappa\delta_2 N \text{ for every } x \in G.$$

It remains to show that $\|1_A - f\| \leq \delta_1$: we first note that $f = J^{-1}(1_{B_1} + \cdots + 1_{B_J})$, where $B_1, ..., B_J$ are the sets B or C arising at each iteration of step 3 in the above algorithm, and satisfy $\|1_{B_i} - 1_A\| \leq \delta_1$. Then, writing

$$f - 1_A \;=\; J^{-1}((1_{B_1} - 1_A) + \cdots + (1_{B_J} - 1_A))$$

the triangle inequality immediately gives us that $\|f - 1_A\| \leq \delta_1$, thereby completing the proof of the lemma.

5 Proof of main theorems

5.1 Proof of Theorem 1

Let $\delta_1 = \delta^3\theta^{5.5}\sqrt{\varepsilon}/128$, and let $k = \lfloor 4\delta_1^{-2}\theta \rfloor + 1$. For a given subset $A \subseteq G$, $|A| = \theta N$, associate a vector

$$v_A \;:=\; (\chi_1, ..., \chi_k, \Re\hat{1}_A(\chi_1), \Im\hat{1}_A(\chi_1), ..., \Re\hat{1}_A(\chi_k), \Im\hat{1}_A(\chi_k)),$$

where $\chi_1, ..., \chi_k$ are the places corresponding to the k largest Fourier coefficients of $h = 1_A$, as described in Lemma 2. From the conclusion of that same lemma we deduce that

$$|\hat{1}_A(\chi_k)| \ \leq \ \delta_1 N/2. \tag{5}$$

Next, round the last $2k$ coordinates of v_A to the nearest multiple of $\delta_1 N/2$. Let w_A denote the new vector that results. It is obvious that as we vary over subsets $A \subseteq G$ satisfying $|A| = \theta N$, the number of possibilities for w_A is bounded (crudely) from above by $N^k(\delta_1/4)^{-2k}$.

Furthermore, if two sets A and B, $|A| = |B| = \theta N$ share the same vector $w_A = w_B$ then the last $2k$ coordinates of v_A and v_B come within $\delta_1 N/2$ of one another; and, in light of (5), this implies that

$$\max_{\chi \in \hat{G}} |\hat{1}_A(\chi) - \hat{1}_B(\chi)| \ \leq \ \delta_1 N \ = \ \delta_1 N.$$

The possibilities for the vectors w_A give us a way of placing sets $A \subseteq G$ with $|A| = \theta N$ into equivalence classes. And now for any such non-empty equivalence class, we fix a set A that it contains, and we suppose that $f : G \to [0, 1]$ has the property that $f - 1_A$ is δ_1-uniform. Then, from Lemma 1, using $g = 1_A$ and $h = f$, we have that

$$\sum_{x \in \mathbb{Z}_N} |f * f(x) - 1_A * 1_A(x)|^2 \ \leq \ \delta_1^2(4\theta + \delta_1)N^3.$$

It follows that if we let T denote the set of all $x \in G$ where $1_A * 1_A(x) = 0$ and where $f * f(x) > \delta^3\theta^6 N/32$, then

$$|T|\delta^6\theta^{12}N^2/1024 \ \leq \ \delta_1^2(4\theta + \delta_1)N^3;$$

that is,

$$|T| \ \leq \ 1024\delta_1^2(4\theta + \delta_1)\delta^{-6}\theta^{-12}N.$$

If we now assume that $|A + A| \leq (1 - \varepsilon)N$ then it follows that there are at least $(\varepsilon - 1024\delta_1^2(4\theta + \delta_1)\delta^{-6}\theta^{-12})N$ places $x \in G$ for which $f * f(x) \leq \delta^3\theta^6 N/32$. Let U denote this set of places x, and note that from our choice for δ_1 we have that $|U| \geq \varepsilon N/2$.

Suppose that f satisfies the conclusion to Corollary 3 for our set A and for the above choice of δ_1 and for $\delta_2 = \delta\theta^2/4$. Then, for any set B where $1_A - 1_B$ is δ_1-uniform, we have that for each $x \in U$,

$$1_B * 1_B(x) \ \leq \ \delta_2^{-2} f * f(x) + 2\delta_2 N \ < \ \delta\theta^2 N.$$

Since, as we said, there are at most $N^k(\delta_1/4)^{-2k}$ possible vectors w_A, it follows that we have a collection of at most $N^k(\delta_1/4)^{-2k}$ sets U such that for every set $B \subseteq G$ satisfying $|B+B| \leq (1-\varepsilon)|B|$, the collection contains a set $U = U_B$, $|U| \geq \varepsilon N/2$, satisfying

$$1_B * 1_B(x) \ < \ \delta\theta^2 N, \text{ for every } x \in U.$$

We claim that if we choose a random set $S_0 \subseteq \mathbb{Z}_N$ of size

$$K \ := \ \lfloor (4k/\varepsilon)(\log N + 1 + \log(1/\delta_1) \rfloor \ \ll \ \varepsilon^{-1}\delta^{-6}\theta^{-10}(\log N - \log(\delta\varepsilon\theta)),$$

then with positive probability S_0 will have non-empty intersection with all these $< N^k(\delta_1/4)^{-2k}$ sets U. To see this, first note that the probability that S_0 fails to intersect any particular set U_B is at most

$$\frac{\binom{(1-\varepsilon/2)N}{K}}{\binom{N}{K}} \ \leq \ (1-\varepsilon/2)^K \ \leq \ \exp(-K\varepsilon/2) \ < \ N^{-k}(\delta_1/4)^{2k}.$$

So, by the union bound, the probability that S_0 intersects *every* one of our sets U_B is positive. It follows that there exists a set S of size K that intersects all the sets U_B; and therefore if $A \subseteq G$, $|A| \geq \theta N$, and if $1_A * 1_A(x) > \delta\theta^2 N$ for every $x \in S$, A could not be one of our sets satisfying $|A+A| \leq (1-\varepsilon)N$ – that is, we would have to have $|A+A| > (1-\varepsilon)N$, thereby completing the proof of the theorem.

5.2 Proof of Theorem 2

The proof of this theorem is not much more than the Dirichlet Box Principle. Before we state it, we introduce the notation $\|x\|$ to denote the least residue mod N in absolute value that is congruent to x mod N.

Lemma 5 *Suppose that $x_1, ..., x_k \in \mathbb{Z}_N$. Then, there exists an integer $n \not\equiv 0 \pmod N$ satisfying*

$$\|nx_1\|, \ \|nx_2\|, \ ..., \ \|nx_k\| \ \leq \ N^{1-1/(k+1)}.$$

Proof of the lemma. The proof of this lemma is standard: we consider the set of vectors

$$\{(jx_1, \ ..., \ jx_k) \pmod N \ : \ 0 \leq j \leq N^{1-1/(k+1)}\} \ \subseteq \ (\mathbb{R}/N\mathbb{Z})^k.$$

Around each point draw a k-dimensional box (so, the point $(jx_1, ..., jx_k)$ (mod N) is the center point of the box) having edge length $N^{1-1/(k+1)}$. The total volume consumed by all the boxes exceeds

$$N^{k-k/(k+1)}N^{1-1/(k+1)} \ = \ N.$$

So, at least two of those boxes must have a point in common; say these boxes correspond to $j = a$ and $j = b$, where $a < b$. It follows that for each $i = 1, ..., k$ the numbers ax_i and bx_i are at most $N^{1-1/(k+1)}$ apart when considered mod N. Letting $n = b - a$ it is easy to see that this then implies the lemma. ■

Given the set S, set $k = |S|$ and $\{x_1, ..., x_k\} = S$, and then let n be as in the lemma. We then let

$$A \ := \ n^{-1} * B \ \subseteq \ \mathbb{Z}_N, \text{ where } B \ := \ \{t \ : \ -N/6 < t < N/6\} \ \subseteq \ \mathbb{Z}_N,$$

where the notation $\lambda * B$ represents the set that results when we dilate the elements of B by λ.

It follows that for each $x \in S$ we have

$$1_A * 1_A(x) \ = \ 1_{n^{-1}*B} * 1_{n^{-1}*B}(x) \ = \ 1_B * 1_B(nx).$$

We have that if $k < (\log N)/2$ then $\|nx\| \lesssim N/e^2$ for $x \in S$, and then

$$1_A * 1_A(x) \ > \ 1_B * 1_B(\lfloor N/e^2 \rfloor + 1) \ \gtrsim \ N(1/3 - 1/e^2) \ > \ N/6.$$

This completes the proof of Theorem 2.

5.3 Proof of Theorem 3

To prove the theorem we will show that if $A \subseteq G$ is any set satisfying $|A + A| < (1 - \varepsilon)|A|$, where $|A| = \theta N$, then the level-set $\{x \in G \ : \ 1_A * 1_A(x) \leq \delta\theta^2 N\}$ must have non-trivial intersection with the set S. And, from Theorem 4 we furthermore have that to prove this conclusion it suffices to show that S intersects every translate of every Bohr neighborhood of radius $\delta^3\theta^{4.5}\sqrt{\varepsilon}/128$ and dimension at most $512\delta^{-6}\theta^{-12}\varepsilon^{-1} + 1$.

Letting $\mathcal{B}(\Lambda, \rho)$ be such a Bohr neighborhood, where $\rho = \delta^3\theta^{4.5}\sqrt{\varepsilon}/128$, we begin by letting $\mathcal{B}' = \mathcal{B}(\Lambda, \rho/2)$ and setting $g = 1_{\mathcal{B}'} * 1_{\mathcal{B}'}$. Since $\text{supp}(g) \subseteq \mathcal{B}(\Lambda, \rho)$, to prove our theorem it suffices to show that for every translate $t \in G$ we have

$$\sum_{x \in G} g(x + t)1_S(x) \ > \ 0. \tag{6}$$

In terms of Fourier coefficients this inequality is simply

$$\sum_{\chi\in\hat{G}} \chi(t)\hat{1}_{\mathcal{B}'}(\chi)^2\hat{1}_S(\chi^{-1}) \ > \ 0;$$

and to prove this it suffices to show that

$$\max_{\chi\neq\chi_0} |\hat{1}_S(\chi)| \sum_{\chi\neq\chi_0} |\hat{1}_{\mathcal{B}'}(\chi)|^2 \ < \ |\mathcal{B}'|^2|S|.$$

From Parseval's identity we have that this holds provided

$$\max_{\chi\neq\chi_0} |\hat{1}_S(\chi)|/|S| \ < \ |\mathcal{B}'|/N.$$

To finish our proof we apply Lemma 3 using $r = \rho/2$, and deduce that we have that (6) holds provided

$$\max_{\chi\neq\chi_0} |\hat{1}_S(\chi)|/|S| \ < \ (\delta^3\theta^{4.5}\sqrt{\varepsilon}/512\pi)^{512\delta^{-6}\theta^{-12}\varepsilon^{-1}+1},$$

which is one of our assumptions. The theorem now follows.

5.4 Proof of Theorem 4

Arrange the Fourier coefficients of $h = 1_A$ from largest to smallest in magnitude as in Lemma 2.

Let $\delta_1 = \delta^3\theta^{5.5}\sqrt{\varepsilon}/128$ and let $k = \lfloor 4\delta_1^{-2}\theta\rfloor + 1$. Letting $\chi_1, ..., \chi_N$ be as in (4), from Lemma 2 we will have from Parseval that $|\hat{1}_A(\chi_k)| \leq \delta_1 N/2$.

Next, we let $\mathcal{B}$ denote the Bohr neighborhood $\mathcal{B}(\chi_1, ..., \chi_k; \delta_1/\theta)$. Then, for each $t \in \mathcal{B}$ define the set $A_t := A + t$. Note that $1_{A+t}(x) = 1_A(x - t)$ and that $\hat{1}_{A_t}(\chi) = \chi(t)\hat{1}_A(\chi)$.

We have that for $i = 1, 2, ..., k$,

$$|\hat{1}_{A_t}(\chi_i) - \hat{1}_A(\chi_i)| \ \leq \ |1 - \chi_i(t)| \cdot |\hat{1}_A(\chi_i)| \ \leq \ \delta_1 N.$$

And for $k + 1 \leq i \leq N$ we have

$$|\hat{1}_{A_t}(\chi_i) - \hat{1}_A(\chi_i)| \ \leq \ |1 - \chi_i(t)| \cdot |\hat{1}_A(\chi_i)| \ \leq \ 2|\hat{1}_A(\chi_i)| \ \leq \ \delta_1 N.$$

In general, then, we have that for all $\chi \in \hat{G}$,

$$|\hat{1}_{A_t}(\chi) - \hat{1}_A(\chi)| \ \leq \ \delta_1 N,$$

which implies that $1_{A_t} - 1_A$ is δ_1-uniform.

We now apply Corollary 3 using $\delta_2 = \delta\theta^2/4$, and deduce the existence of a function $f : G \to [0,1]$ having the properties indicated by the Corollary. From the fact that $f - 1_A$ is δ_1-uniform we deduce from Lemma 1, using $g = 1_A$ and $h = f$, that

$$\sum_{x \in G} |1_A * 1_A(x) - f * f(x)|^2 \;=\; \delta_1^2(4\theta + \delta_1)N^3. \tag{7}$$

Letting T denote the set of all $x \in G$ such that $1_A * 1_A(x) < \delta^3\theta^6 N/128$, since we are given that $|T| \geq \varepsilon N$ we deduce from (7) that if for all such x we also had that $f * f(x) \geq \delta^3\theta^6 N/32$, then

$$9\delta^6\theta^{12}\varepsilon N^3/2^{14} \;\leq\; |T|(3\delta^3\theta^6 N/128)^2 \;\leq\; \delta_1^2(4\theta + \delta_1)N^3,$$

which is impossible. So, there exists $x \in G$ such that $f * f(x) < \delta^3\theta^6 N/32$. From Corollary 3, and the fact that $1_A - 1_{A_t}$ is δ_1-uniform (and that $1_A - 1_A = 0$ is also δ_1-uniform), we will have for this value x that

$$1_A * 1_A(x - t) \;=\; 1_A * 1_{A_t}(x) \;\leq\; \delta_2^{-2} f * f(x) + 2\delta_2 N \;<\; \delta\theta^2 N.$$

It follows that the level-set $\{y \;:\; 1_A * 1_A(y) < \delta\theta^2 N\}$ contains the set $x - \mathcal{B}$, which completes the proof of the theorem.

6 Acknowledgments

I would like to thank Olof Sisask and Thomas Bloom for their numerous comments and suggestions.

References

[1] M. Ajtai, H. Iwaniec, J. Komlós, J. Pintz, and E. Szemerédi, *Construction of a thin set with small Fourier coefficients*, Bull. London Math. Soc. **22** (1990), 583-590.

[2] M. Bateman and N. H. Katz, *New bounds on cap sets*, preprint arXiv:1101.5851

[3] F. A. Behrend, *On sets of integers which contain no three terms in arithmetic progression*, Proc. Nat. Acad. Sci. **23** (1946), 331-332.

[4] T. Bloom, *Translation invariant equations and the method of Sanders*, preprint arXiv:1107.1110

[5] N. Bogolioùboff, *Sur quelques propiétés arithmétiques des presque-périodes*, Ann. Chaire Phys. Math. Kiev **4** (1939), 185-205.

[6] E. Croot, I. Laba, and O. Sisask, *Arithmetic progressions in sumsets and L^p-almost-periodicity*, preprint arXiv:1103.6000

[7] E. Croot and O. Sisask, *A probabilistic technique for finding almost-periods of convolutions*, Geom. Funct. Anal. **20** (2010), no. 6, 1367-1396.

[8] M. Elkin, *An improved construction of progression-free sets* Israel Jour. of Math. **184** (2011), 93-128.

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

[10] B. Green, *Arithmetic progressions in sumsets*, Geom. Funct. Anal. **12** (2002), no. 3, 584-597.

[11] B. Green and J. Wolf, *A note on Elkin's improvement of Behrend's construction*, Additive Number Theory: Festschrift in Honor of the Sixtieth Birthday of Melvyn B. Nathanson, 2010, p. 141-144.

[12] N. H. Katz and P. Koester, *On additive doubling and energy*, SIAM J. Discrete Math. **24** (2010), 1684-1693.

[13] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104-109.

[14] I. Z. Ruzsa, *Arithmetic progressions in sumsets*, Acta Arith. **60** (1991), no. 2, 191-202.

[15] T. Sanders, *On the Bogolyubov-Ruzsa Lemma*, preprint arXiv:1011.0107

[16] ————, *On Roth's Theorem on progressions*, to appear in Ann. of Math.

[17] T. Schoen and I. Shkredov, *Roth's Theorem in many variables*, preprint arXiv:1106.1601

[18] T. Tao and V. Vu, *Additive Combinatorics*, 2006 Cambridge Univ. Press.