Forum of Mathematics, Sigma (2016), Vol. 4, e5, 28 pages
doi:10.1017/fms.2016.2

ROTH'S THEOREM FOR FOUR VARIABLES AND ADDITIVE STRUCTURES IN SUMS OF SPARSE SETS

TOMASZ SCHOEN[1] and OLOF SISASK[2]

[1] Faculty of Mathematics and Computer Science, Adam Mickiewicz University,
Umultowska 87, 61-614 Poznań, Poland;
email: schoen@amu.edu.pl

[2] Department of Mathematics, KTH, 100 44 Stockholm, Sweden;
email: sisask@kth.se

Received 21 November 2014; accepted 15 October 2015

Abstract

We show that if $A \subseteq \{1, \ldots, N\}$ does not contain any nontrivial solutions to the equation $x + y + z = 3w$, then

$$|A| \leqslant \frac{N}{\exp(c(\log N)^{1/7})},$$

where $c > 0$ is some absolute constant. In view of Behrend's construction, this bound is of the right shape: the exponent $1/7$ cannot be replaced by any constant larger than $1/2$. We also establish a related result, which says that sumsets $A + A + A$ contain long arithmetic progressions if $A \subseteq \{1, \ldots, N\}$, or high-dimensional affine subspaces if $A \subseteq \mathbb{F}_q^n$, even if A has density of the shape above.

2010 Mathematics Subject Classification: 11B30 (primary); 11B25, 11K70 (secondary)

1. Introduction

This paper is concerned with two types of problems in additive combinatorics, namely solving linear equations in subsets of abelian groups and finding additive structures in sumsets, with a focus on being able to deal with relatively sparse sets. We discuss these in turn, focusing on the historically most important case of sets of integers.

Roth-type results. Roth's well-known theorem on arithmetic progressions says that if a set $A \subseteq [N] := \{1, \ldots, N\}$ does not contain any nontrivial three-term arithmetic progressions, that is solutions to the equation $x + z = 2y$ with x, y, z not equal, then $|A|$ cannot be very large:

THEOREM 1.1 (Roth's theorem [20]). *Let $r_3(N)$ denote the largest size of a subset of $[N]$ with no nontrivial three-term progressions. Then, for N large enough,*

$$r_3(N) \leqslant \frac{CN}{\log\log N}.$$

(Here and throughout the paper, we use the letters C and c to denote positive absolute constants whose values need not be the same at different occurrences.) This theorem has been central to additive combinatorics, and improving the above bound has been the object of much research and has led to a wealth of interesting techniques being developed; see for example [4–6, 18, 23, 24, 27], to which we also refer for more history on the problem. However, it is not yet known whether $r_3(N) \leqslant CN/\log N$ for some constant C; the current best upper bounds, due to Sanders [23] and Bloom [4], are of the form

$$r_3(N) \leqslant \frac{C(\log\log N)^C}{\log N} N.$$

By contrast, the best lower bounds on $r_3(N)$, coming from constructions of large subsets of $[N]$ with no nontrivial progressions, give

$$r_3(N) \geqslant \frac{N}{\exp(C(\log N)^{1/2})},$$

as proved by Behrend [2] (but see also [12, 17]).

Now, most proofs of Roth's theorem easily extend to provide similar upper bounds for any translation invariant equation

$$c_1x_1 + \cdots + c_kx_k = 0 \quad \text{where } k \geqslant 3, c_j \in \mathbb{Z} \setminus \{0\}, \text{ and } c_1 + \cdots + c_k = 0, \tag{1.1}$$

the last condition being the translation invariance property. Behrend's argument also extends directly to any such equation with one negative coefficient and the rest positive, that is of the form $a_1x_1 + \cdots + a_lx_l = by$ with the a_j positive integers summing to b. Furthermore, a somewhat folklore philosophy was that whatever techniques worked for additive combinatorial problems involving three variables would also work for those involving four or more, and vice versa, with the bounds being similar. The work [25] of Sanders led to this being questioned in the context of sumsets, however, and the first-named author and Shkredov [26] subsequently

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

showed that much stronger bounds than those given above for $r_3(N)$ hold for equations in six or more variables. A representative example:

THEOREM 1.2 [26]. *Suppose $A \subseteq [N]$ does not contain any solutions to $x_1 + \cdots + x_5 = 5y$ in distinct integers. Then*

$$|A| \leqslant \frac{N}{\exp(c(\log N)^{1/7})}.$$

Here, one has an almost matching lower bound: Behrend's construction gives sets A of size at least $\exp(-C(\log N)^{1/2})N$ that do not contain any solutions to this equation.

Around the same time, Bloom [3] established improved bounds for four- and five-variable equations, inspired by Sanders's technique from [23]:

THEOREM 1.3 [3]. *Suppose $A \subseteq [N]$ does not contain any nontrivial solutions to the equation in (1.1). Then*

$$|A| \leqslant \frac{N}{(\log N)^{k-2-o_{\mathbf{c}}(1)}}.$$

(A solution $(x_1, \ldots, x_k)$ to (1.1) is called trivial if one can partition the index set $[k]$ into parts on which the variables x_j are constant and the coefficients c_j sum to 0. For example $(x, \ldots, x)$. See the next section for a definition of the little-$o()$ notation.) There thus remained an almost exponential gap between the lower and upper bounds for four- and five-variable equations. In this paper, we show that one indeed has Behrend-shape upper bounds for these. For example:

THEOREM 1.4. *Suppose $A \subseteq [N]$ does not contain any nontrivial solutions to the equation $x + y + z = 3w$. Then*

$$|A| \leqslant \frac{N}{\exp(c(\log N)^{1/7})}.$$

In the much-studied finite field setting, where $[N]$ is replaced by a vector space over a finite field, we establish the following slightly stronger result.

THEOREM 1.5. *Let q be a prime power and let $A \subseteq \mathbb{F}_q^n$ be a set of size αq^n. If A does not contain any nontrivial solutions to $x + y + z = 3w$, then*

$$\alpha \leqslant \exp(-c(n^{1/5})).$$

By contrast, the best bound known for three-term progressions in this setting comes from the intricate work of Bateman and Katz [1], who showed that if $A \subseteq \mathbb{F}_3^n$ is free of nontrivial three-term progressions, then $|A| \leqslant 3^n/n^{1+\epsilon}$, where ϵ is some strictly positive constant.

Before we move on, let us make a quick remark about our arguments. These are somewhat different to those of [26], which used the bounds of Sanders [25] for a result known as the Bogolyubov–Ruzsa lemma. However, the proof of this lemma used in turn an almost-periodicity result of Croot and the second-named author [10], and this will together with an insight from [25] be of key importance in our proofs. This is actually part of the motivation behind this paper: while one aim is to prove strong bounds for as close a problem as possible to Roth's theorem, another is to attempt to illustrate the natural limitations of the ideas of [10, 25]. We thus give two different proofs of Theorem 1.5 that demonstrate different aspects of the results; see Section 3.

Structures in sumsets. Another big direction of additive combinatorics is to study the structure of sumsets $A + B = \{a + b : a \in A, b \in B\}$ for various types of sets A and B in an abelian group. Here we focus on the case of three-fold sumsets $3A := A + A + A$, where A is a large subset of $[N]$ or a finite abelian group G, as was first tackled by Freiman, Halberstam and Ruzsa [13]. Suppose $A \subseteq [N]$ has size at least αN, $\alpha > 0$. The following lower bounds for the length of a longest arithmetic progression in $3A$ are known.

Density range	Length of AP in $3A$	
$\alpha \geqslant (\log N)^{-1/3+o(1)}$	$N^{c\alpha^3}$	F–H–R [13]
$\alpha \geqslant (\log N)^{-1/2+o(1)}$	$N^{c\alpha^{2+o(1)}}$	Green [14]
$\alpha \geqslant (\log N)^{-1/2+o(1)}$	$N^{c\alpha}$	Sanders [21]
$\alpha \geqslant (\log N)^{-1+o(1)}$	$N^{c\alpha^{1+o(1)}}$	Henriot [19]
$\alpha \geqslant (\log N)^{-2+o(1)}$	$\exp((\alpha^{1/2+o(1)} \log N)^{1/2})$	Henriot [19]

Henriot [19] gives a useful and clear summary of the history of the problem, and we refer there for more information. Let us also mention that Henriot's results are actually more powerful in the asymmetric case of sumsets $A + B + C$: in this set-up [19] allows B and C to be much sparser, namely of densities around $\exp(-C(\log N)^c)$, as long as the density of A is more or less as above.

Here we prove the following, which is nontrivial in the range

$$\alpha \geqslant \exp(-c(\log N)^{1/5}).$$

THEOREM 1.6. *Let $A \subseteq [N]$ have size at least αN. Then $3A$ contains an arithmetic progression of length at least*

$$\alpha \exp\left(\left(\frac{c \log N}{\log^3(2/\alpha)}\right)^{1/2}\right).$$

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

The length of the progression here is of course much smaller than in previous results for large densities, being on par with what is known for just $A + A$ in this case, but when α gets small enough this theorem applies whereas those above do not. However, let us mention that there is a combinatorial argument due to Croot, Ruzsa and the first-named author [8] that guarantees arithmetic progressions in $2A := A + A$ of length around $c \log N/\log(2/\alpha)$, which certainly extends the nontrivial density range further albeit with fairly short progressions. We thus know of quite different behaviours for different densities, but a lack of examples pervades. The best example we know of comes from [13]: there it is shown that, for any $\alpha < c$, there is a set $A \subseteq [N]$ of size at least αN for which $3A$ does not contain an arithmetic progression of length

$$N^{2/\log(1/\alpha)}. \tag{1.2}$$

Theorem 1.6 thus gives an answer of the right shape $\exp((\log N)^c)$ for $\alpha = \exp(-(\log N)^c)$, but with a gap in the exponent on the $\log N$ compared to (1.2).

These questions are also studied for subsets of vector spaces $\mathbb{F}_q^n$ over finite fields $\mathbb{F}_q$, where q is considered fixed, but in this setting one generally looks at the dimensions of (affine) subspaces found in sumsets rather than lengths of arithmetic progressions, for obvious reasons. See for example [7, 15, 21, 22] for more background. From the perspective of the present paper it is illuminating to consider what is known in this setting for $2A$, $3A$ and $4A$, for which the best bounds known for large densities are all due to Sanders. For $2A$, it is shown in [22] that $2A$ contains an affine subspace of dimension at least $c\alpha n$ for $\alpha \geqslant C/n$. Sumsets $3A$ are known [21] to contain affine subspaces of dimension at least $n - C/\alpha$, and sumsets $4A$ are known [25] to contain affine subspaces of dimension at least $n - C\log^4(2/\alpha)$. Here we prove a result somewhat intermediate between the latter two:

THEOREM 1.7. *Let $A \subseteq \mathbb{F}_5^n$ be a set of size at least $\alpha \cdot 5^n$. Then $3A$ contains an affine subspace of dimension at least $cn/\log(2/\alpha)^3 - \log(1/\alpha)$.*

We actually show somewhat more, namely that these three-fold sumsets contain lots of translates of the respective arithmetic progression or subspace; see Section 8 for further statements, and see also Section 9 for some further comparisons of $2A$, $3A$ and $4A$.

The rest of this paper is structured as follows. In the next section, we set up some notation and describe some preliminaries on density increments, convolutions and almost-periodicity. In Section 3, we prove Theorem 1.5; indeed, we give two proofs as already mentioned. We then proceed to a proof of the

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

general case, starting with a review of Bohr sets in Section 4 and the development of the appropriate almost-periodicity results in Section 5, and wrapping up with the density increment and iterative arguments in Sections 6 and 7. We then turn to structures in $3A$ in Section 8, and conclude with some remarks in Section 9.

2. Notation and preliminaries

If A is a subset of a finite set X, we refer to $\mu(A) := \mu_X(A) := |A|/|X|$ as the *density* of A (in X).

The density increment strategy. In proving the Roth-type theorems outlined above, we shall employ a so-called *density increment* strategy, as have most proofs of Roth's theorem resulting in good bounds. This operates roughly as follows. Let G be $[N]$ or $\mathbb{F}_q^n$. If $A \subseteq G$ has density α but contains no nontrivial solutions to $x + y + z = 3w$, then one shows that A has increased density $(1 + c(\alpha))\alpha$ on a translate of some 'large substructure' V of G – say a long progression in the case of $[N]$ or a large subspace in the case of $\mathbb{F}_q^n$. Thus $|A\cap(x+V)| \geqslant (1+c)\alpha|V|$. One then looks at $(A-x)\cap V$, which is still solution-free by translation invariance, and tries to repeat the argument. One thus produces denser and denser solution-free sets on smaller and smaller substructures, but since a density can never increase beyond 1, the iteration must at some point terminate (provided the function $c(\alpha)$ is nice enough). Generally this means that the substructures on which one is iterating must have become trivial, so as long as the original density is large enough for the increased densities to reach 1 before the substructures become trivial, one has shown that the set must contain a solution to the equation.

Of course, all this is saying roughly that we shall prove the result by induction; the whole game is to find arguments to make the substructures V and the increments $c(\alpha)$ as large as possible, while keeping V nice enough to iterate. For many proofs of Roth's theorem, the substructures on which one increments are directly related to the large Fourier coefficients of A; for us this is not quite the case, the substructures being uncovered instead by the probabilistic almost-periodicity results of [10]. To state one of these results in detail, let us introduce some further notation.

Normalizations, L^p-norms, convolutions. Now, we have talked about densities above, and it is relatively standard practice in additive combinatorics these days to work with these rather than cardinalities of sets. An associated trend has been to furthermore use normalized convolutions and L^p norms. In this paper, we shall find it useful to work with both densities and cardinalities, as we shall operate relatively 'locally' later on. We thus speak of densities, but write, for an abelian group G, a subset $X \subseteq G$, a function $f : G \to \mathbb{C}$ and a real number $p \geqslant 1$,

$$\mu_X := 1_X/|X|, \quad \|f\|_p^p := \sum_{x\in G} |f(x)|^p, \quad f * g(x) := \sum_{y\in G} f(y)g(x-y).$$

Here and throughout, 1_X denotes the *indicator function* of X, taking the value 1 if its input lies in X and 0 otherwise.

Convolutions really are central objects for us when pursuing a density increment strategy as outlined above. Indeed, the quantity $1_A * \mu_V(x)$ is precisely $|A \cap (x-V)|/|V|$, which is the relative density of A on $x - V$, and the number of solutions to our equation is precisely $1_A * 1_A * 1_A * 1_{-3\cdot A}(0)$. Crucially, however, we shall not prove our results by studying this function directly, as did most previous proofs, but we shall nevertheless deal with similar convolutions, and for this the key tools will be certain almost-periodicity results.

Almost-periodicity. Our main tool for showing properties of convolutions is the following L^p-almost-periodicity result, which is a version of the main theorem of [10], but with somewhat less detailed moment estimates in the probabilistic arguments; see for example [7, 25] for a proof.

THEOREM 2.1. *Let $p \geqslant 2$, $\epsilon \in (0,1)$ and $k \in \mathbb{N}$ be parameters. Let A, L, S be finite subsets of an abelian group. Suppose $|A+S| \leqslant K|A|$. Then there is a set $T \subseteq S$ with $|T| \geqslant 0.99K^{-Cpk^2/\epsilon^2}|S|$ such that*

$$\|1_A * 1_L(\cdot + t) - 1_A * 1_L\|_p \leqslant \epsilon|A||L|^{1/p} \quad \textit{for all } t \in kT - kT.$$

The result thus says that, for two sets A and L, provided A is structured in the sense of not growing much under addition with some set S, one can find lots of L^p-almost-periods of the convolution $1_A * 1_L$, these being elements t for which this function does not change by much (in L^p) upon translation by t.

We shall bootstrap this to other variants later on. In the model setting, we can simply quote such a bootstrapped result; we turn to this in the next section, after one further note on notation.

Asymptotic notation. For a real-valued function g defined on a subset of the reals, we use the notation $o(g)$ to refer to a function f for which $f(x)/g(x) \to 0$ either as $x \to \infty$ or as $x \to 0$, the context determining which of these is the case. Thus, an example of a function that is $(\log N)^{1-o(1)}$ as $N \to \infty$ is $\log N/\log\log N$, and an example of one that is $\alpha^{1+o(1)}$ as $\alpha \to 0$ is $\alpha/\log(1/\alpha)$. A subscript on the o refers to a parameter on which the function may depend. If f is another real-valued function similarly defined, then we write $f \ll g$ to mean that there is some constant C for which $|f(x)| \leqslant C|g(x)|$ for all x, and $f \gg g$ to mean that $g \ll f$.

3. Two proofs in the finite field setting

Here we shall prove Theorem 1.5, which said that if a subset $A \subseteq \mathbb{F}_q^n$ of density α does not contain any nontrivial solutions to the equation

$$x + y + z = 3w \tag{3.1}$$

then $\alpha \leqslant \exp(-cn^{1/5})$. Note that, for this equation, a solution is trivial if and only if $x = y = z = w$, and that the result is trivial if q is divisible by 2 or 3, so we assume throughout that it is not. We shall actually give two different proofs of this result, one more analytic and one more combinatorial – but both following the density increment strategy outlined in the previous section. It turns out that the former proof extends more easily to the setting of more general finite abelian groups, from which one can deduce Theorem 1.4, whereas the latter serves as inspiration for the later proofs finding structures in sumsets.

In both proofs, we shall use the following bootstrapped version of Theorem 2.1, which is a specialization of [7, Theorem 7.4].

THEOREM 3.1. *Let $p \geqslant 2$ and $\epsilon \in (0, 1)$. Let $G = \mathbb{F}_q^n$ be a vector space over a finite field and suppose $A, L \subseteq G$ have $\mu(A) \geqslant \alpha$. Then there is a subspace V of codimension*

$$d \leqslant Cp\epsilon^{-2} \log(2/\epsilon\alpha)^2 \log(2/\alpha)$$

such that, for each $t \in V$,

$$\|1_A * 1_L(\cdot + t) - 1_A * 1_L\|_{L^p} \leqslant \epsilon |A||L|^{1/p}.$$

First proof: via L^∞-almost-periodicity of three-fold convolutions. This proof is based on the fact that if A does not contain any nontrivial solutions to (3.1), then $1_{-3\cdot A} * 1_A * 1_{A+A}(0) = |A|$, which is very small. Three-fold convolutions like this are, however, fairly continuous functions: we shall deduce from a certain almost-periodicity result that $1_{-3\cdot A} * 1_A * 1_{A+A} * \mu_V(0)$ is then also small for some large subspace V. If $|A + A|$ is large, a simple averaging then implies that A has a density increment on a translate of V. If, on the other hand, $|A + A|$ is small, then one is done by a similar, if slightly simpler, argument.

The relevant almost-periodicity result is the following, but note that this will be superseded by a slightly more efficient and general version in Section 5.

THEOREM 3.2. *Let $\epsilon \in (0, 1)$ and let $A, M, L \subseteq \mathbb{F}_q^n$ have $\mu(A), \mu(M) \geqslant \alpha$. Then there is a subspace V of codimension at most $C\epsilon^{-2} \log(2/\epsilon\alpha)^2 \log(2/\alpha)^2$ such that*

$$|1_A * 1_M * 1_L(x + t) - 1_A * 1_M * 1_L(x)| \leqslant \epsilon |A||M|$$

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

for all $x \in G$ and $t \in V$. In particular,

$$|1_A * 1_M * 1_L(0) - 1_A * 1_M * 1_L * \mu_V(0)| \leqslant \epsilon |A||M|.$$

Proof. Apply Theorem 3.1 with $p = C \log(2/\alpha)$ and $\epsilon/2$ to get a subspace V of the required codimension such that

$$\|1_A * 1_L(\cdot + t) - 1_A * 1_L\|_p \leqslant \tfrac{1}{2}\epsilon |A||L|^{1/p}.$$

Then, for r with $1/r + 1/p = 1$, Hölder's inequality gives

$$\begin{aligned}\|1_A * 1_M * 1_L(\cdot + t) - 1_A * 1_M * 1_L\|_\infty &\leqslant \|1_M\|_r \|1_A * 1_L(\cdot + t) - 1_A * 1_L\|_p \\ &\leqslant \tfrac{1}{2}\epsilon |A||M|(|L|/|M|)^{1/p},\end{aligned}$$

whence the first claim is proved. The second follows from the triangle inequality. □

We now split into two cases, depending on whether the sumset $A + A$ is large or not.

Large sumset. In the large-sumset case, where $\mu(A + A) \geqslant \frac{1}{2}$, we shall make use of the fact that $1_{-3\cdot A} * 1_A * 1_{A+A}(0) = |A|$ if A is free from solutions to (3.1), which means that the convolution $1_{-3\cdot A} * 1_A * 1_{(A+A)^c}$ takes a really large value. Though perhaps not clear in this formulation, this argument was inspired by those of [9, 11].

PROPOSITION 3.3. *Let $A \subseteq \mathbb{F}_q^n$ have density α and size at least 8. Suppose $\mu(A + A) \geqslant \frac{1}{2}$ and that A does not contain any nontrivial solutions to (3.1). Then there is a subspace V of codimension at most $C \log(2/\alpha)^4$ such that $1_A * \mu_V(x) \geqslant \frac{3}{2}\alpha$ for some x.*

Recall that $1_A * \mu_V(x) = |A \cap (x - V)|/|V|$, and so the conclusion says that A has massively increased density on some affine subspace of low codimension.

Proof. Apply Theorem 3.2 with $M = -3 \cdot A$, $L = A + A$ and $\epsilon = 1/8$ to get a subspace V of the required codimension such that

$$1_{-3\cdot A} * 1_A * 1_{A+A} * \mu_V(0) \leqslant 1_{-3\cdot A} * 1_A * 1_{A+A}(0) + \tfrac{1}{8}|A|^2.$$

Since $1_{-3\cdot A} * 1_A * 1_{A+A}(0) = |A| \leqslant |A|^2/8$, we thus have

$$1_{-3\cdot A} * 1_A * 1_{A+A} * \mu_V(0) \leqslant \tfrac{1}{4}|A|^2,$$

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

and so

$$1_{-3\cdot A} * 1_A * 1_{(A+A)^c} * \mu_V(0) \geqslant \tfrac{3}{4}|A|^2.$$

The left-hand side here is at most $|A||(A+A)^c|\|1_A * \mu_V\|_\infty$, and so we are done. □

Small sumset. That one can obtain a good density increment for A when $A+A$ is small is well known, and a result almost sufficing for our purposes is contained in [25]; see, for example, Theorem 9.1 there. We shall however use the following.

PROPOSITION 3.4. *Suppose $A \subseteq \mathbb{F}_q^n$ has density α and $\mu(A+A) \leqslant \frac{1}{2}$. Then there is a subspace V of codimension at most $C(\log 2/\alpha)^4$ such that $1_A * \mu_V(x) \geqslant \frac{3}{2}\alpha$ for some x.*

Proof. Apply Theorem 3.2 with $M = A$, $L = -(A+A)$ and $\epsilon = 1/4$ to get a subspace V of the required codimension such that

$$|1_A * 1_A * 1_{-(A+A)}(0) - 1_A * 1_A * 1_{-(A+A)} * \mu_V(0)| \leqslant \tfrac{1}{4}|A|^2.$$

But $1_A * 1_A * 1_{-(A+A)}(0) = |A|^2$ since $1_A * 1_A$ is supported on $A+A$, and so

$$1_A * 1_A * 1_{-(A+A)} * \mu_V(0) \geqslant \tfrac{3}{4}|A|^2.$$

Since the left-hand side here is at most $|A||A+A|\|1_A * \mu_V\|_\infty$, the result follows. □

Note that we did not need to assume that A was free of solutions to any equations here.

Completing the proof: iterating. Combining these propositions, one immediately obtains the following corollary.

COROLLARY 3.5. *Let $A \subseteq \mathbb{F}_q^n$ have density α and size at least 8. Suppose A does not contain any nontrivial solutions to (3.1). Then there is a subspace of codimension at most $C\log(2/\alpha)^4$ such that $1_A * \mu_V(x) \geqslant \frac{3}{2}\alpha$ for some x.*

We now simply iterate this corollary to complete the proof.

Proof of Theorem 1.5. If $A \subseteq G := \mathbb{F}_q^n$ has density α, size at least 8 and is free of nontrivial solutions to (3.1), then Corollary 3.5 gives us a subspace $V \leqslant G$ of codimension at most $C\log(2/\alpha)^4$ and an element $x \in G$ for which

$$|(A-x) \cap V| \geqslant \tfrac{3}{2}\alpha|V|,$$

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

that is, a subspace in which $A - x$ has density at least $\frac{3}{2}\alpha$. Note that $A - x$ is still free of nontrivial solutions to (3.1) by translation invariance. We then repeat this argument with G replaced by V, and so on, obtaining solution-free sets of increasing densities α_j in spaces of lowering dimension n_j, with $\alpha_1 = \alpha$ and $n_1 = n$. Assuming $\alpha_j \geqslant 8q^{-n_j}$ at each stage, we thus have

$$n_{j+1} \geqslant n_j - C\log(2/\alpha)^4 \geqslant n - Cj\log(2/\alpha)^4,$$

and

$$\alpha_{j+1} \geqslant \tfrac{3}{2}\alpha_j \geqslant (\tfrac{3}{2})^j\alpha.$$

Since the density cannot increase beyond 1, this process must terminate with some $j \leqslant C\log(2/\alpha)$. If the claimed bound $\alpha \leqslant \exp(-cn^{1/5})$ does not hold then we have $n_j \geqslant n - Cj\log(2/\alpha)^4 \geqslant n/2$ by the time of termination, and so running out of dimensions is not a reason for the process to terminate. Thus, we must have $\alpha_j < 8q^{-n_j}$. But this is easily seen to imply the claimed bound anyway, and we are done. □

Before we go on to give our second proof, let us make a quick remark about the types of solutions we have considered.

REMARK 3.6. In the statement of Theorem 1.5, we forbade all nontrivial solutions to (3.1) in A, these being any nonconstant quadruples (x, y, z, w) for which $x + y + z = 3w$. This has the effect of forbidding A from containing solutions to certain other equations as well, such as nontrivial three-term arithmetic progressions – if x, y, z are distinct and lie in arithmetic progression, then the quadruple (x, y, z, y) solves our equation. Though we did not pursue this issue above for the sake of clarity of exposition, let us mention that incorporating a short additional argument in fact shows that the same bound holds if one only disallows solutions where all the variables are distinct, so that one is only disallowing solutions to this equation and not any 'subequations'.

Second proof: via properties of three-fold sumsets. The following property of three-fold sumsets encodes the key to this proof.

PROPOSITION 3.7. *Let $\eta \in (0, 1)$ and let $A, B \subseteq \mathbb{F}_q^n$ be sets of densities α, β respectively. Then there is a subspace V of codimension at most $C\log(2/\eta\beta)\log(2/\alpha)^3$ and a set $X \subseteq B$ with $|X| \geqslant 0.99|B|$ such that*

$$|(x + V) \cap (B + A - A)| \geqslant (1 - \eta)|V|$$

for every $x \in X$.

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

Another way of putting the conclusion is that $1_{B+A-A} * \mu_V(x) \geqslant 1-\eta$ for each $x \in X$.

Proof. Apply Theorem 3.1 with $p = C\log(2/\eta\beta)$, $\epsilon = 1/2$ and $L = B - A$ to get a subspace V of the required codimension such that

$$\|1_A * 1_{B-A}(\cdot + t) - 1_A * 1_{B-A}\|_p \leqslant \tfrac{1}{2}|A||B-A|^{1/p}$$

for each $t \in V$.

Let X consist of all $x \in B$ such that $|(x+V) \cap (B+A-A)| \geqslant (1-\eta)|V|$, so that if $x \notin X$ then $1_A * 1_{B-A}(x+t) = 0$ for more than $\eta|V|$ elements $t \in V$. Then

$$\eta|V| \sum_{x \in B\setminus X} 1_A*1_{B-A}(x)^p < \sum_{t\in V}\|1_A*1_{B-A}(\cdot+t)-1_A*1_{B-A}\|_p^p \leqslant \tfrac{1}{2^p}|A|^p|B-A||V|.$$

But $1_A * 1_{B-A}(x) = |A|$ for each $x \in B$, and so this implies that

$$|B \setminus X| < \tfrac{1}{2^p}\eta^{-1}|B-A| \leqslant 0.01|B|,$$

which completes the proof. □

Corollary 3.8. *Let $\eta \in (0,1)$ and let $A, B, C \subseteq \mathbb{F}_q^n$ have $\mu(A), \mu(C) \geqslant \alpha$ and $\mu(B) \geqslant \beta$. Then there is a subspace V of codimension at most $C\log(2/\eta\beta)\log(2/\alpha)^3$, an element $t \in \mathbb{F}_q^n$ and a set $X \subseteq B+t$ with $|X| \geqslant 0.99|B|$ such that*

$$|(x+V) \cap (A+B+C)| \geqslant (1-\eta)|V|$$

for every $x \in X$.

Proof. Since $\sum_t 1_A * 1_C(t) = |A||C|$, there is some t such that $\mu(A \cap (t-C)) \geqslant \alpha^2$. Applying Proposition 3.7 with this intersection instead of A completes the proof. □

Using this, we give a second proof of Corollary 3.5, finding a good density increment.

Second proof of Corollary 3.5. Partition $A = A_1 \cup A_2$ with $|A_1| = \lceil \frac{4}{5}|A| \rceil$ and apply Corollary 3.8 with $\eta := \alpha/2$, $B := C := -A_1$ and $3 \cdot A_2$ in place of A. This gives us a subspace V of codimension at most $C\log(2/\alpha)^4$, an element t and a set $X \subseteq t - A$ with $|X| \geqslant \frac{3}{4}|A|$ such that

$$|(x+V) \cap (3\cdot A_2 - A_1 - A_1)| \geqslant (1-\eta)|V| \quad \text{for each } x \in X.$$

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

Since A does not contain any nontrivial solutions to (3.1), A and $3 \cdot A_2 - A_1 - A_1$ are disjoint, whence

$$|(x+V) \cap A| \leqslant \tfrac{1}{2}\alpha|V| \quad \text{for each } x \in X. \tag{3.2}$$

Since V is a subspace, this in fact holds for all $x \in X + V$. How large is this sumset? Well, if $1_X * \mu_V(x) \geqslant \frac{3}{2}\alpha$ for some x, then we would have a density increment of the kind we are after, so let us assume that $1_X * \mu_V(x) < \frac{3}{2}\alpha$ for all x. Then

$$|X| = \sum_{x \in X+V} 1_X * \mu_V(x) < \tfrac{3}{2}\alpha|X+V|,$$

and so (3.2) holds for at least $|X+V| \geqslant \frac{1}{2}|G|$ elements x. In other words, $1_A * \mu_V(x) \leqslant \frac{1}{2}\alpha$ for at least half of the elements of the group. Since the average of this function over the whole group is α, we must have $1_A * \mu_V(x) \geqslant \frac{3}{2}\alpha$ for some x, and so we are done. □

Since Theorem 1.5 followed directly from Corollary 3.5, this completes the proof.

Extending the arguments. Both of these proofs of Theorem 1.5 can be extended to handle the case of sets of integers using the machinery of regular Bohr sets pioneered by Bourgain [5], each with their own sets of difficulties. However, it turns out this process is more straightforward for the first proof, and so it is this that we shall present, starting in the next section with a review of the basic theory surrounding Bohr sets. The second proof is however very much related to the proofs we shall give for the results on structures in sums of sparse sets, as should become apparent.

4. Bohr sets and their elementary properties

When one wants to perform a density increment argument of the type we have just used in groups without a rich subgroup structure, it is by now a rather established practice to turn to Bohr sets as a natural substitute for subspaces. In an abelian group G, we define these in terms of the dual group $\widehat{G}$ of characters, consisting of homomorphisms from G to $\mathbb{C}^\times$ with the group operation given by pointwise multiplication.

DEFINITION 4.1. Let $\Gamma \subseteq \widehat{G}$ and let $\rho \geqslant 0$. We define the *Bohr set* on these data by

$$\mathrm{Bohr}(\Gamma, \rho) = \{x \in G : |\gamma(x) - 1| \leqslant \rho \text{ for all } \gamma \in \Gamma\}.$$

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

We refer to $|\Gamma|$ as the *rank* of the Bohr set, and ρ as its *radius*. (Note that these quantities are not well defined in terms of just the set itself, but we think of these data as being included in the definition of the Bohr set.) We say that $\mathrm{Bohr}(\Gamma', \rho') \leqslant \mathrm{Bohr}(\Gamma, \rho)$ is a *sub-Bohr set* if $\Gamma' \supseteq \Gamma$ and $\rho' \leqslant \rho$; note, in particular, that this implies containment as sets. We shall frequently need to scale the radii of our Bohr sets: if $B = \mathrm{Bohr}(\Gamma, \rho)$ and $\delta \geqslant 0$, then we write $B_\delta = \mathrm{Bohr}(\Gamma, \delta\rho)$.

We refer the reader to Section 4.4 in the book [28] of Tao and Vu for the proofs of the following lemmas and for more background. (The constants appearing here are somewhat different to those in [28], as we have defined Bohr sets in terms of quantities of the form $|z - 1|$ rather than $\arg(z)$.)

LEMMA 4.2. *Let $\Gamma \subseteq \widehat{G}$ be a set of d characters, let $\rho \in [0, 2]$, and let $B = \mathrm{Bohr}(\Gamma, \rho)$. Then we have the size estimate*

$$|B| \geqslant (\rho/2\pi)^d |G|,$$

the doubling estimate

$$|B_2| \leqslant 6^d |B|,$$

and, for $\delta \in [0, 1]$, the decay estimate

$$|B_\delta| \geqslant (\delta/2)^{3d} |B|.$$

In particular, $|B + B| \leqslant 6^d |B|$, since $B_\delta + B_\epsilon \subseteq B_{\delta+\epsilon}$ by the triangle inequality. Thus, Bohr sets have fairly small doubling if d is small. Subspaces, however, enjoy the stronger property that $|V + V| = |V|$ regardless of dimension, and this discrepancy in doubling constants reflects an underlying issue that means our argument becomes terribly inefficient if we simply try to replace subspaces with Bohr sets. In giving a proof of Roth's theorem with strong bounds, Bourgain [5] showed how to work around this issue, namely by working with pairs of Bohr sets (B, B_δ) with δ small, for which $|B + B_\delta| \leqslant |B_{1+\delta}|$. A priori this need not be close to $|B|$, but the following property ensures this.

DEFINITION 4.3 (Regularity). We say that a Bohr set B of rank d is regular if

$$1 - 12d|\delta| \leqslant \frac{|B_{1+\delta}|}{|B|} \leqslant 1 + 12d|\delta|$$

whenever $|\delta| \leqslant 1/12d$.

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

The constant 12 here is of course not particularly important, but we include it for definiteness. Now, not all Bohr sets are regular, but it is a consequence of the doubling estimate $|B| \leqslant 6^d|B_{1/2}|$ that growth must be somewhat limited around some slight rescaling of B:

LEMMA 4.4. *If B is a Bohr set, then there is a $\delta \in [\frac{1}{2}, 1]$ for which B_δ is regular.*

If B is regular of rank d we have the useful property that $|B + B_\delta| \leqslant 2|B|$ whenever $\delta \leqslant 1/12d$. We also have the following useful consequence of regularity, resting simply on an application of the triangle inequality.

LEMMA 4.5. *If B is a regular Bohr set of rank d and $B' \subseteq B_\delta$ with $\delta \leqslant \epsilon/24d$, then*

$$\|\mu_B * \mu_{B'} - \mu_B\|_{L^1(G)} \leqslant \epsilon.$$

We finally require an arithmetic property of Bohr sets, which follows from the size estimate in Lemma 4.2 and the inclusion $kB_{1/k} = B_{1/k} + \cdots + B_{1/k} \subseteq B$.

LEMMA 4.6. *Let N be a prime and let $B \subseteq \mathbb{Z}_N$ be a Bohr set of rank $d \geqslant 1$ and radius $\rho \in [0, 2]$. Then B contains an arithmetic progression of size at least $(1/2\pi)\rho N^{1/d}$.*

5. L^∞-almost-periodicity relative to Bohr sets

To carry out the strategy of Section 3 with Bohr sets in place of groups, the first thing we need to do is prove an appropriate analogue of Theorem 3.2. Of course, not only do we need to replace the subspace V in the conclusion with a Bohr set – which is entirely straightforward – but we are only allowed to assume density in a Bohr set rather than in a group. It turns out that this is also fairly straightforwardly achievable.

Almost-periodicity with dense sets. Recall Theorem 2.1, the L^p-almost-periodicity result for two-fold convolutions. From this we argue straightforwardly as with Theorem 3.2 to obtain the following L^∞-almost-periodicity result for three-fold convolutions.

THEOREM 5.1. *Let $\epsilon \in (0, 1)$ and $k \in \mathbb{N}$ be parameters. Let A, M, L, S be finite subsets of an abelian group. Suppose $|A+S| \leqslant K|A|$ and $\eta := |M|/|L| \leqslant 1$. Then there is a set $T \subseteq S$ with $|T| \geqslant \exp(-Ck^2\epsilon^{-2}\log(2/\eta)\log(2K))|S|$ such that*

$$\|1_A * 1_M * 1_L(\cdot + t) - 1_A * 1_M * 1_L\|_\infty \leqslant \epsilon|A||M| \quad \textit{for all } t \in kT - kT.$$

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

Proof. Apply Theorem 2.1 with parameters $\epsilon/2$ and p to be specified to obtain a set T of almost-periods for $1_A * 1_L$. By Hölder's inequality we then have, for $1/p + 1/q = 1$ and any $t \in kT - kT$,

$$\begin{aligned}\|1_A * 1_M * 1_L(\cdot + t) - 1_A * 1_M * 1_L\|_\infty &\leqslant \|1_M\|_q \|1_A * 1_L(\cdot + t) - 1_A * 1_L\|_p \\ &\leqslant \tfrac{1}{2}\epsilon |A||M|(|L|/|M|)^{1/p}.\end{aligned}$$

Picking $p = 3\log(2|L|/|M|)$ yields the result. □

REMARK 5.2. Note that the set T one obtains does not in fact depend on M but only on $|M|/|L|$. Also, since the methods of [10] worked for nonabelian groups, a version of the above result holds for arbitrary groups, and one could also replace 1_M and 1_L by functions more general than indicator functions, but we shall only apply it in the above case.

Finally, we shall bootstrap this to find not only a large set of translates, but a *structured* set: a Bohr set of translates. The price we shall pay is that we shall need to assume that the set A interacts nicely with a Bohr set and not just an arbitrary set S. The main idea of the proof is to couple Theorem 5.1 with Chang's theorem on the structure of large spectra, which was one of the main insights that led to the powerful results [25] of Sanders. To state this properly we shall need the Fourier transform; the results of the following subsection are the only ones in this paper that appeal to Fourier analysis.

Almost-periodicity with Bohr sets. For a function $f : G \to \mathbb{C}$ on a finite abelian group G, we define the Fourier transform $\widehat{f} : \widehat{G} \to \mathbb{C}$ on the dual group $\widehat{G}$ by

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

Writing $\mathbb{E}_{x \in X} = |X|^{-1}\sum_{x \in X}$, the Fourier inversion formula, Parseval's identity and the convolution identity then take the form

$$\begin{gathered} f(x) = \mathbb{E}_{\gamma \in \widehat{G}}\, \widehat{f}(\gamma)\gamma(x), \\ \textstyle\sum_{x \in G} |f(x)|^2 = \mathbb{E}_{\gamma \in \widehat{G}}\, |\widehat{f}(\gamma)|^2, \quad \text{and} \\ \widehat{f * g}(\gamma) = \widehat{f}(\gamma)\widehat{g}(\gamma). \end{gathered}$$

Finally, for a set $X \subseteq G$, write

$$\mathrm{Spec}_\delta(\mu_X) := \{\gamma \in \widehat{G} : |\widehat{\mu_X}(\gamma)| \geqslant \delta\}$$

for the δ-*large spectrum* of $\mu_X = 1_X/|X|$. See [28] for more on all of this.

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

Chang's theorem [28, Lemma 4.36] says that the large spectrum $\mathrm{Spec}_\delta(\mu_X)$ is 'low-dimensional': it is contained in the $\{-1, 0, 1\}$-span of a set of at most $C\delta^{-2}\log(1/\mu_G(X))$ characters. An immediate and useful consequence is that all the characters in $\mathrm{Spec}_\delta(\mu_X)$ can be approximately annihilated by a low-rank Bohr set if X is relatively dense in G. Sanders proved an efficient version of such a consequence when X is a dense subset of a Bohr set rather than the group; the following is [21, Proposition 4.2].

PROPOSITION 5.3 (Chang–Sanders). *Let $\delta, \nu \in (0, 1]$. Let G be a finite abelian group, let $B = \mathrm{Bohr}(\Gamma, \rho) \subseteq G$ be a regular Bohr set of rank d and let $X \subseteq B$. Then there is a set of characters $\Lambda \in \widehat{G}$ and a radius ρ' with*

$$|\Lambda| \ll \delta^{-2}\log(2/\mu_B(X)) \quad \textit{and} \quad \rho' \gg \rho\nu\delta^2/d^2\log(2/\mu_B(X))$$

such that

$$|1 - \gamma(t)| \leqslant \nu \quad \textit{for all } \gamma \in \mathrm{Spec}_\delta(\mu_X) \textit{ and } t \in \mathrm{Bohr}(\Gamma \cup \Lambda, \rho').$$

The aforementioned bootstrapping can now take place via a standard argument.

THEOREM 5.4 (L^∞-almost-periodicity with Bohr sets). *Let $\epsilon \in (0, 1)$. Let A, M, L be subsets of a finite abelian group G, and let $B \subseteq G$ be a regular Bohr set of rank d and radius ρ. Suppose $|A + S| \leqslant K|A|$ for a subset $S \subseteq B$ with $\mu_B(S) \geqslant \sigma > 0$, and assume $\eta := |M|/|L| \leqslant 1$. Then there is a regular Bohr set $B' \leqslant B$ of rank at most $d + d'$ and radius at least $\rho\epsilon\eta^{1/2}/d^2 d'$, where*

$$d' \ll \epsilon^{-2}\log^2(2/\epsilon\eta)\log(2/\eta)\log(2K) + \log(1/\sigma),$$

such that

$$\|1_A * 1_M * 1_L(\cdot + t) - 1_A * 1_M * 1_L\|_\infty \leqslant \epsilon|A||M| \quad \textit{for all } t \in B'.$$

In particular,

$$\|1_A * 1_M * 1_L * \mu_{B'} - 1_A * 1_M * 1_L\|_\infty \leqslant \epsilon|A||M|.$$

Proof. Begin by applying Theorem 5.1 to $1_A * 1_M * 1_L$ with parameters ϵ and $k := \lceil C\log(2/\epsilon\eta)\rceil$ to obtain a set $T \subseteq S$ with

$$\mu_B(T) \geqslant \exp(-C\epsilon^{-2}k^2\log(2/\eta)\log(2K))\sigma$$

such that

$$\|1_A * 1_M * 1_L(\cdot + t) - 1_A * 1_M * 1_L\|_\infty \leqslant \epsilon|A||M| \quad \text{for all } t \in kT - kT.$$

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

Fix some $z \in T$ and set $X = T - z$, so that the above inequality holds for all $t \in kX$. Thus, by the triangle inequality,

$$\|1_A * 1_M * 1_L * \mu_X^{(k)} - 1_A * 1_M * 1_L\|_\infty \leqslant \epsilon|A||M|,$$

where $\mu_X^{(k)} := \mu_X * \cdots * \mu_X$ with k copies of μ_X. It thus suffices to establish the theorem with $1_A * 1_M * 1_L * \mu_X^{(k)}$ in place of $1_A * 1_M * 1_L$, and so we switch now to this.

Noting that translating X does not affect the conclusion of Proposition 5.3, apply this proposition to $T = X + z$ with parameters $\delta = 1/2$ and $\nu = \epsilon\eta^{1/2}$ together with Lemma 4.4 to get a regular Bohr set $B' \leqslant B$ of the required rank and radius such that

$$|1 - \gamma(t)| \leqslant \epsilon\eta^{1/2} \quad \text{for all } \gamma \in \operatorname{Spec}_{1/2}(\mu_X) \text{ and } t \in B'.$$

For any $x \in G$ and $t \in B'$ we then have, by the Fourier inversion formula, triangle inequality and convolution identity,

$$\begin{aligned} &|1_A * 1_M * 1_L * \mu_X^{(k)}(x+t) - 1_A * 1_M * 1_L * \mu_X^{(k)}(x)| \\ &\quad \leqslant \mathbb{E}_{\gamma \in \widehat{G}} |\widehat{1_A}(\gamma)||\widehat{1_M}(\gamma)||\widehat{1_L}(\gamma)||\widehat{\mu_X}(\gamma)|^k|\gamma(t) - 1|. \end{aligned} \tag{5.1}$$

For each term in this average, consider whether $\gamma \in \operatorname{Spec}_{1/2}(\mu_X)$ or not. If $\gamma \in \operatorname{Spec}_{1/2}(\mu_X)$ we have $|\gamma(t) - 1| \leqslant \epsilon\eta^{1/2}$, and if not then $|\widehat{\mu_X}(\gamma)|^k \leqslant 1/2^k \leqslant \epsilon\eta^{1/2}$. Thus (5.1) is at most twice

$$\epsilon\eta^{1/2}\, \mathbb{E}_{\gamma \in \widehat{G}} |\widehat{1_A}(\gamma)||\widehat{1_M}(\gamma)||\widehat{1_L}(\gamma)|.$$

Using the trivial inequality $|\widehat{1_A}(\gamma)| \leqslant |A|$ and Cauchy–Schwarz plus Parseval à la

$$\mathbb{E}_{\gamma \in \widehat{G}} |\widehat{1_M}(\gamma)||\widehat{1_L}(\gamma)| \leqslant (\mathbb{E}_{\gamma \in \widehat{G}} |\widehat{1_M}(\gamma)|^2)^{1/2}(\mathbb{E}_{\gamma \in \widehat{G}} |\widehat{1_L}(\gamma)|^2)^{1/2} = |M|^{1/2}|L|^{1/2}$$

finishes the proof, after replacing ϵ with $\epsilon/4$. □

REMARK 5.5. The regime in which the above argument is set up to be efficient is one in which A is thought of as extremely small, but structured in the sense of not expanding much under addition to a Bohr set, M as being of 'medium' size and L as being large. The main utility of this result over previous Fourier-analytic ones of this sort, then, stems from the fact that the dependence on $|L|/|M|$ in the rank of B' is only polylogarithmic rather than polynomial.

6. Obtaining density increments on Bohr sets

The following proposition drives the density increment argument.

PROPOSITION 6.1. *Let G be a finite abelian group of order not divisible by 3, let $B \subseteq G$ be a regular Bohr set of rank d and radius ρ, and let $A \subseteq B$ have relative density $\mu_B(A) \geqslant \alpha$. Assume that $|B| \geqslant (Cd/\alpha)^{3d}$. If A does not contain any nontrivial solutions to $x + y + z = 3w$, then A has relative density at least $\frac{5}{4}\alpha$ on a translate of a Bohr set $B' \leqslant B$ of rank at most $d + d'$ and radius at least $\rho\alpha^{3/2}/d^5 d'$, where $d' \ll \log(2/\alpha)^4$.*

As in the model case, we prove this differently in two cases depending on whether a particular sumset is large or not. In each case, we make the further assumption that our given set A is dense also in a narrower sub-Bohr set.

The large-sumset, solution-free case.

LEMMA 6.2. *Let G be a finite abelian group of order not divisible by 3, let $B \subseteq G$ be a regular Bohr set of rank d and radius ρ, and let $A \subseteq B$ have relative density $\mu_B(A) \geqslant \alpha$. Let $B' := B_\delta$ be a regular sub-Bohr set with $\delta := 1/Cd$ such that $|B_{1+3\delta}| \leqslant 1.01|B|$, and assume that $A' := A \cap B'$ satisfies $\mu_{B'}(A') \geqslant \alpha$ and $|A + A'| \geqslant |A|/2\alpha$. If $|A| \geqslant C$ and A does not contain any nontrivial solutions to $x + y + z = 3w$, then $\|1_A * \mu_T\|_\infty \geqslant 1.8\alpha$ for some Bohr set $T \leqslant B$ of rank at most $d + d'$ and radius at least $\rho\alpha^{1/2}/d^4 d'$, where $d' \ll \log^4(2/\alpha)$.*

Proof. Define $S := 3 \cdot B'_\nu$ where $\nu := 1/Cd$, so that (using the assumption on $|G|$) S is a Bohr set of rank d and radius at least ρ/Cd^2, and note that, by regularity,

$$|3 \cdot A' + S| \leqslant |B'_{(1+\nu)}| \leqslant 2|B'| \leqslant \tfrac{2}{\alpha}|3 \cdot A'|. \tag{6.1}$$

Apply Theorem 5.4 with $-3 \cdot A'$ in place of A, S as defined above in place of both B and S, $M := A$, $L := B_{1+3\delta} \setminus (A + A')$ and $\epsilon := \frac{1}{40}$. Our assumption $|A + A'| \geqslant |A|/2\alpha$ implies that

$$|L| \leqslant 1.01|B| - \frac{1}{2\alpha}|A| \leqslant \tfrac{0.501}{\alpha}|A|, \tag{6.2}$$

and so the parameter η of that theorem is certainly at least α. We may further take $K = 2/\alpha$ by (6.1), and so we get a Bohr set $T \leqslant S$ of rank at most $d + d'$ and radius at least $\rho\alpha^{1/2}/d^4 d'$, where $d' \leqslant C\log^4(2/\alpha)$, such that

$$\|1_{-3\cdot A'} * 1_A * 1_L * \mu_T - 1_{-3\cdot A'} * 1_A * 1_L\|_\infty \leqslant \tfrac{1}{40}|A'||A|.$$

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

Now, since A does not contain any nontrivial solutions to $x+y+z=3w$, we have

$$1_{-3\cdot A'} * 1_A * 1_{A+A'}(0) = |A'|.$$

Thus

$$\begin{aligned} 1_{-3\cdot A'} * 1_A * 1_L * \mu_T(0) &\geqslant 1_{-3\cdot A'} * 1_A * (1_{B_{1+3\delta}} - 1_{A+A'})(0) - \tfrac{1}{40}|A'||A| \\ &= \tfrac{39}{40}|A'||A| - |A'| \\ &\geqslant \tfrac{19}{20}|A'||A|, \end{aligned}$$

provided $|A| \geqslant 40$. By the pigeonhole principle, then, there must be some element x for which

$$1_A * \mu_T(x) \geqslant \tfrac{19}{20}|A|/|L| \geqslant 1.8\alpha,$$

by (6.2). □

The small-sumset case. Again, the case in which $A + A'$ is small can be handled in a slightly simpler fashion.

LEMMA 6.3. *Let $A \subseteq G$, let $B \subseteq G$ be a regular Bohr set of rank d and radius ρ, and let $A' \subseteq B$ have relative density $\mu_B(A') \geqslant \alpha$. If $|A + A'| \leqslant |A|/2\alpha$, then $\|1_A * \mu_T\|_\infty \geqslant 1.8\alpha$ for some Bohr set $T \leqslant B$ of rank at most $d + d'$ and radius at least $\rho\alpha^{1/2}/d^3 d'$, where $d' \ll \log^4(2/\alpha)$.*

Proof. Let $S = B_\nu$ where $\nu := 1/Cd$, so that

$$|A' + S| \leqslant |B_{1+\nu}| \leqslant \tfrac{2}{\alpha}|A'|.$$

Applying Theorem 5.4 with A' in place of A, this set S, $M := A$, $L := -A - A'$ and $\epsilon := \frac{1}{10}$, we may take $\eta \geqslant 2\alpha$ and $K = 2/\alpha$ to get a Bohr set $T \leqslant S$ of rank at most $d + d'$ and radius at least $\rho\alpha^{1/2}/d^3 d'$ where $d' \leqslant C\log^4(2/\alpha)$ such that

$$\|1_{A'} * 1_A * 1_{-A-A'} * \mu_T - 1_{A'} * 1_A * 1_{-A-A'}\|_\infty \leqslant \tfrac{1}{10}|A'||A|.$$

Now, $1_{A'} * 1_A * 1_{-A-A'}(0) = |A'||A|$ since $1_{A'} * 1_A$ is supported on $A' + A$, and so

$$1_{A'} * 1_A * 1_{-A-A'} * \mu_T(0) \geqslant \tfrac{9}{10}|A'||A|.$$

Pigeonholing and using the assumption on $|A+A'|$, there is thus some x for which

$$1_A * \mu_T(x) \geqslant \tfrac{9}{10}|A|/|A + A'| \geqslant 1.8\alpha.$$ □

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

Rescaling and putting the cases together. We need one final tool in order to put the previous two lemmas together to prove Proposition 6.1, namely a simple averaging argument due to Bourgain [5] that, in practice, allows us to assume that a dense subset A of a Bohr set B is also large on a sub-Bohr set B_δ for some not-too-small δ.

LEMMA 6.4. *Let B be a regular Bohr set of rank d, let $A \subseteq B$ have relative density α, and let $B', B'' \subseteq B_\delta$ where $\delta \leqslant \alpha/Cd$. Then either:*

(i) *there is an $x \in B$ such that $1_A * \mu_{B'}(x) \geqslant \frac{7}{10}\alpha$ and $1_A * \mu_{B''}(x) \geqslant \frac{7}{10}\alpha$; or*

(ii) $\|1_A * \mu_{B'}\|_\infty \geqslant \frac{5}{4}\alpha$ *or* $\|1_A * \mu_{B''}\|_\infty \geqslant \frac{5}{4}\alpha$.

Proof. Since B is regular, picking the constant C large enough yields

$$|1_A * \mu_B * \mu_{B'}(0) - 1_A * \mu_B(0)| \leqslant \|\mu_B * \mu_{B'} - \mu_B\|_1 \leqslant \tfrac{1}{40}\alpha$$

by Lemma 4.5, and similarly for B''. Since $1_A * \mu_B(0) = \mu_B(A) = \alpha$, this implies that

$$\mathbb{E}_{x \in B}\, (1_A * \mu_{B'}(x) + 1_A * \mu_{B''}(x)) \geqslant (2 - \tfrac{1}{20})\alpha,$$

and so there exists $x \in B$ such that $1_A * \mu_{B'}(x) + 1_A * \mu_{B''}(x) \geqslant (2 - \frac{1}{20})\alpha$. Fix such an x. If we are not in the second case of the conclusion, we then have

$$1_A * \mu_{B'}(x) \geqslant (2 - \tfrac{1}{20})\alpha - \tfrac{5}{4}\alpha = \tfrac{7}{10}\alpha,$$

and similarly for B'', and so we are done. □

Proof of Proposition 6.1. We start by rescaling our Bohr set so that A is large at two scales simultaneously: apply Lemma 6.4 with $\delta := \alpha/Cd$ picked so that $B' := B_\delta$ is regular, and with $B'' := B'_{\delta'}$ where $\delta' := 1/Cd$ is picked so that this is regular and $|B'_{1+3\delta'}| \leqslant 1.01|B'|$. If we are in the second case of the conclusion of that lemma, then we have a density increment on a translate of a Bohr set of rank d and radius at least $\rho\alpha/Cd^2$, in which case we are done. So assume instead that we get an element $x \in B$ such that

$$1_A * \mu_{B'}(x),\ 1_A * \mu_{B''}(x) \geqslant \tfrac{7}{10}\alpha,$$

and let $A' := (A - x) \cap B'$, $A'' := (A - x) \cap B''$; these sets thus have relative densities at least $\alpha' := \frac{7}{10}\alpha$ in their respective Bohr sets. Note by translation invariance that A' also does not contain any nontrivial solutions to our equation.

Now, if $|A' + A''| \leqslant |A'|/2\alpha'$, then we apply Lemma 6.3 with (A', A'', B'') in place of (A, A', B) to get that

$$\|1_A * \mu_T\|_\infty \geqslant \|1_{A'} * \mu_T\|_\infty \geqslant 1.8\alpha' \geqslant \tfrac{5}{4}\alpha,$$

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

where T is a Bohr set of rank at most $d + d'$ and radius at least $\rho\alpha^{3/2}/d^5 d'$, with $d' \ll \log^4(2/\alpha)$, and so we are done.

If, on the other hand, $|A' + A''| \geqslant |A'|/2\alpha'$, then we apply Lemma 6.2 with (A', A'', B') in place of (A, A', B) to get precisely the same conclusion, provided that $|A'| \geqslant C$. A quick computation using Lemma 4.2 shows that this is ensured by our assumption that $|B| \geqslant (Cd/\alpha)^{3d}$, and so we are done. □

7. The iterative argument

We now iterate the density increment result of the preceding section to prove our theorem.

THEOREM 7.1. *Let G be a finite abelian group of order N not divisible by 3. If $A \subseteq G$ does not contain any nontrivial solutions to $x + y + z = 3w$, then*

$$|A| \leqslant \frac{N}{\exp(c(\log N)^{1/7})}.$$

Proof. Initialize $A_1 = A$, $B^{(1)} = \mathrm{Bohr}(\{1\}, 2) = G$, $d_1 = 1$, $\rho_1 = 2$ and $\alpha_1 = \alpha = |A|/|G|$. We run the following iterative scheme until the condition required for doing so fails.

If $|B^{(j)}| \geqslant (Cd_j/\alpha_j)^{3d_j}$, then we apply Proposition 6.1 to our sets and parameters to produce a new Bohr set $B^{(j+1)} \leqslant B^{(j)}$ of rank d_j and radius ρ_j satisfying

$$d_{j+1} \leqslant d_j + C\log^4(2/\alpha_j) \leqslant Cj\log^4(2/\alpha),$$
$$\rho_{j+1} \geqslant \rho_j\alpha_j^{3/2}/Cd_j^5 \log^4(2/\alpha)$$

and a set $A_{j+1} = (A_j - x_j) \cap B^{(j+1)} \subseteq B^{(j+1)}$ (for some x_j) of relative density

$$\alpha_{j+1} \geqslant \tfrac{5}{4}\alpha_j \geqslant (\tfrac{5}{4})^j\alpha.$$

Note that A_{j+1} has no nontrivial solutions to our equation by translation invariance.

Since the density of a set can never increase beyond 1, the growth of the α_j implies that we must no longer be able to iterate this process when $j = s$ for some $s \leqslant C\log(2/\alpha)$. Thus, we must have $|B^{(s)}| < (Cd_s/\alpha_s)^{3d_s}$. On the other hand, by Lemma 4.2 we have $|B^{(s)}| \geqslant (\rho_s/2\pi)^{d_s}|G|$. Putting these together we certainly have

$$|G| < (Cd_s/\rho_s\alpha_s)^{3d_s}.$$

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

Now $d_s \leqslant C\log^5(2/\alpha)$, $\rho_s \geqslant (c\alpha)^{Cs}$ and $\alpha_s \geqslant \alpha$; putting these bounds in gives

$$|G| < \exp(C\log^7(2/\alpha)),$$

which yields the bound of the theorem upon rearranging. □

REMARK 7.2. With minor modifications, one can of course also prove a version of this theorem with A simply being dense in a Bohr set rather than the full group; we omit the details.

8. Additive structures in sums of sparse sets

We turn now to the questions of structures in sumsets, proving Theorems 1.6 and 1.7. This will be somewhat easier work than in the previous few sections as the arguments are iteration-free and so do not require the machinery associated with regular Bohr sets. However, we do require the analogue of Theorem 3.1 for arbitrary finite abelian groups, this being another specialization of [7, Theorem 7.4]:

THEOREM 8.1. *Let $p \geqslant 2$ and $\epsilon \in (0,1)$. Let G be a finite abelian group and let $A, L \subseteq G$ be sets with $\mu(A) \geqslant \alpha$. Then there is a Bohr set T of rank at most*

$$d := Cp\epsilon^{-2}\log(2/\epsilon\alpha)^2\log(2/\alpha)$$

and radius at least $\epsilon\alpha^{1/2}/d$ such that, for each $t \in T$,

$$\|1_A * 1_L(\cdot + t) - 1_A * 1_L\|_p \leqslant \epsilon|A||L|^{1/p}.$$

Using this in place of Theorem 3.1, the following can be proved in precisely the same way as Corollary 3.8.

PROPOSITION 8.2. *Let $\eta \in (0,1)$ and let $A, B, C \subseteq G$ have densities α, β, γ respectively. Then there is a Bohr set $T \subseteq G$ of rank at most $d := C\log(2/\eta\beta)\log(2/\alpha\gamma)^3$ and radius at least $(\alpha\gamma)^{1/2}/d$, and an element $t \in G$, such that for any $V \subseteq T$ there is a set $X \subseteq B + t$ with $|X| \geqslant 0.99|B|$ such that*

$$|(x + V) \cap (A + B + C)| \geqslant (1-\eta)|V| \quad \textit{for every } x \in X.$$

Note that if $C = -A$ then we can reduce the radius to $\alpha^{1/2}/d$ and take $t = 0$.

PROPOSITION 8.3. *Let A, B, C be sets of densities α, β, γ respectively in a finite abelian group G, and let $p \geqslant 1$. Then there is a Bohr set $T \subseteq G$ of rank at*

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

most $d := Cp(\log 2/\alpha\gamma)^3$ and radius at least $(\alpha\gamma)^{1/2}/d$ such that, for any subset $V \subseteq T$ of size at most $\beta \cdot 2^p$, there is a set $X \subseteq B$ of size $|X| \geqslant 0.99|B|$ such that a translate of $X + V$ is contained in $A + B + C$.

Proof. This follows immediately from the preceding proposition on taking $\eta = 1/(\beta\, 2^{p+1})$, so that $(1-\eta)|V| > |V| - 1$. □

One can also prove this directly from Theorem 8.1 following the proof of [7, Theorem 1.4] but taking into account the very large 'higher energy' of $1_A * 1_{B-A}$; this is, of course, very much related to the proof of Proposition 3.7.

We now have some easy corollaries. Theorem 1.6 follows immediately from:

THEOREM 8.4. *Let $A, B, C \subseteq [N]$ be sets of densities α, β, γ. Then $A + B + C$ contains $X + P$ where $X \subseteq B$ has $|X| \geqslant 0.99|B|$ and P is an arithmetic progression of length at least*

$$\exp\left(c\left(\frac{\log N}{\log^3(2/\alpha\gamma)}\right)^{1/2} - \log(1/\alpha\beta\gamma)\right).$$

Proof. By the standard trick of embedding $[N]$ into $\mathbb{Z}_{N'}$ for N' a prime between $6N$ and $12N$, it suffices to prove the statement with $[N]$ replaced by $\mathbb{Z}_N$ for N a prime, so we assume this set-up instead.

Now, apply Proposition 8.3 with $p := C((\log N)/(\log^3(2/\alpha\gamma)))^{1/2}$ to obtain a set $X \subseteq B$ and a Bohr set T of rank $d \leqslant Cp\log^3(2/\alpha\gamma)$ and radius at least $c\alpha\gamma/d$ satisfying that theorem's conclusion. By Lemma 4.6, T contains an arithmetic progression of length at least $(c\alpha\gamma/d)N^{1/d}$. A quick calculation shows that the claimed arithmetic progression has length shorter than both this and $\beta \cdot 2^p$, whence we are done. □

Note that this result can be nontrivial for α and γ as small as $\exp(-c(\log N)^{1/5})$ and for β even as small as $\exp(-c(\log N)^{1/2})$. Also, since Bohr sets are extremely rich in additive structure, one can of course replace P in the conclusion by other kinds of sets, such as generalized arithmetic progressions, which can then be much larger. Just measuring the length of a single progression, as we have done above, is nevertheless a simple and useful measure of the strength of the method.

In the finite field world we obtain the following generalization of Theorem 1.7.

THEOREM 8.5. *Let $A, B, C \subseteq \mathbb{F}_q^n$ be sets of densities α, β, γ. Then $A + B + C$ contains $X + V$ where $X \subseteq B$ has $|X| \geqslant 0.99|B|$ and V is an affine subspace of*

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

dimension at least

$$\left(\frac{cn}{\log^3(2/\alpha\gamma)} - \log(1/\beta)\right)/\log q.$$

Proof. This follows just as before: applying Proposition 8.3 with $p := cn/\log^3(2/\alpha\gamma)$, we obtain a large set $X \subseteq B$ and a subspace $T \leqslant \mathbb{F}_q^n$ of dimension at least $n - Cp\log^3(2/\alpha\gamma)$ such that $A + B + C$ contains a translate of $X + V$ for any subset $V \subseteq T$ of size less than $\beta \cdot 2^p$. Noting that this is less than $|T|$ and letting V be a subspace of T of size between $\beta \cdot 2^p/q$ and $\beta \cdot 2^p$ then does the job. □

Note that if $q = 5$, say, this can be nontrivial for α, γ as small as $\exp(-cn^{1/3})$ and for β as small as 5^{-cn} – in other words, $|B|$ can be as small as a power of $|G|$ in this set-up. One can also reach such densities in the $[N]$ world; see the next section.

REMARK 8.6. In the case that A or C has very large density, the above results follow from those known for two-fold sumsets, with X being the whole of B even. The point here is thus that one can deal with much sparser sets, and the cost is only that one gets slightly fewer translates of the structure in $A + B + C$.

9. Concluding remarks

Other equations. We only dealt with the equation $x+y+z = 3w$ in this paper, but it should be clear that one can deal with a general translation invariant equation $c_1x + c_2y + c_3z + c_4w = 0$ in precisely the same way, at least in the finite field setting. In the more general setting, one needs to make some small alterations related to the radii of the Bohr sets involved, but as in the former case the main difficulty is notational. A similar remark applies to equations in five variables, where precisely the same bounds hold.

Lower bounds in finite fields. What is the largest size of a subset of $\mathbb{F}_5^n$ with no nontrivial solutions to $x + y + z = 3w$? Just as for three-term progressions, we do not know of a Behrend-type example in this setting; indeed the best we know of comes from taking products of examples for small n, resulting in sets of size around θ^n for some $\theta < 5$.

Small doubling instead of density. Clearly, one could work with small-sumset conditions instead of density conditions in many of the proofs in this paper, but there is not much incentive to do so in view of the nature of the bounds and

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

the presence of effective ‘modelling lemmas’ in the settings of interest; see for example [16, Section 6].

Lower densities for the $A+B+C$ problem in the integers. Theorem 8.4 found arithmetic progressions in $A+B+C$ where one of the sets could have density as low as $\exp(-c(\log N)^{1/2})$. To reach even lower densities, one can use the argument underlying [10, Theorem 1.9], again adding the idea of exploiting the higher energy of $1_A * 1_{B-A}$:

THEOREM 9.1. *Let $A, B, C \subseteq [N]$ be sets of densities α, β, γ. Then $A+B+C$ contains an arithmetic progression of length at least*

$$\exp\left(c\left(\frac{\log N}{\log(2/\alpha\gamma)}\right)^{1/4} - \log(1/\beta)\right).$$

This is worse than the bound in Theorem 8.4 for $\alpha=\beta=\gamma$, but for certain density combinations it actually wins out. For example, it allows one to take α and γ to be as small as N^{-c} provided β is a constant. (Note, however, that in this particular range one is guaranteed constant-length progressions already in $A+C$, as follows from [8].) An answer to the following question would thus be interesting.

QUESTION 9.2. Suppose $A, B \subseteq [N]$ have densities N^{-c} and $C \subseteq [N]$ has density $\exp(-C(\log N)^{2/3})$. Must $A+B+C$ contain an arithmetic progression of length tending to infinity with N?

Correlations for $2A$, $3A$ and $4A$. Following on from the discussion of subspaces in sumsets in the introduction, let us offer this perhaps illustrative comparison of results on correlations of $2A$, $3A$ and $4A$ with subspaces, where $A \subseteq \mathbb{F}_q^n$ has density α.

- $2A$ contains $1-\epsilon$ of an affine subspace of codimension at most $C\epsilon^{-2-o(1)}\log(1/\alpha)^4$.
- $3A$ contains $1-\epsilon$ of an affine subspace of codimension at most $C\log(1/\epsilon\alpha)\log(1/\alpha)^3$.
- $4A$ contains all of an affine subspace of codimension at most $C\log(1/\alpha)^4$.

The first and last bullets follow from Sanders’s work [25] (and directly from Theorem 3.2), and the middle one from Proposition 3.7. (Note also that the last bullet follows from either of the other two by inclusion–exclusion.) These results

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press

focus on the small density case: when α is large some prior results can offer better bounds; for example, for $\mathbb{F}_2^n$ Sanders showed in [21] that $2A$ contains $1-\epsilon$ of an affine subspace of codimension at most $C\alpha^{-2}\log(1/\epsilon)$, and codimension at most $C\alpha^{-1}\log(1/\epsilon)$ in [22].

However, it is far from clear where the truth lies for these results – not only in terms of the exponents on the logarithms but also in the qualitative differences between $3A$ and $4A$. It may very well be that the result for $4A$ actually holds for $3A$, as would have been expected prior to [25], and any proof of this is likely to be useful in proving Behrend-shape bounds for Roth's theorem itself. On the other hand, any demonstrations of a genuine difference between $3A$ and $4A$, or three- and four-variable equations, say, would also be very interesting.

Acknowledgements

T.S. was supported by NCN grant 2012/07/B/ST1/03556 and O.S. by The Swedish Research Council grant 2013-4896.

References

[1] M. Bateman and N. H. Katz, 'New bounds on cap sets', *J. Amer. Math. Soc.* **25**(2) (2012), 585–613. arXiv:1101.5851.

[2] F. A. Behrend, 'On sets of integers which contain no three terms in arithmetical progression', *Proc. Natl. Acad. Sci. USA* **32** (1946), 331–332.

[3] T. F. Bloom, 'Translation invariant equations and the method of Sanders', *Bull. Lond. Math. Soc.* **44**(5) (2012), 1050–1067. arXiv:1107.1110.

[4] T. F. Bloom, A quantitative improvement for Roth's theorem on arithmetic progressions, arXiv:1405.5800.

[5] J. Bourgain, 'On triples in arithmetic progression', *Geom. Funct. Anal.* **9**(5) (1999), 968–984.

[6] J. Bourgain, 'Roth's theorem on progressions revisited', *J. Anal. Math.* **104** (2008), 155–192.

[7] E. Croot, I. Łaba and O. Sisask, 'Arithmetic progressions in sumsets and L^p-almost-periodicity', *Combin. Probab. Comput.* **22**(3) (2013), 351–365. arXiv:1103.6000.

[8] E. Croot, I. Z. Ruzsa and T. Schoen, 'Arithmetic progressions in sparse sumsets', in *Combinatorial Number Theory* (de Gruyter, Berlin, 2007), 157–164.

[9] E. Croot and O. Sisask, 'A new proof of Roth's theorem on arithmetic progressions', *Proc. Amer. Math. Soc.* **137** (2009), 805–809. arXiv:0801.2577.

[10] E. Croot and O. Sisask, 'A probabilistic technique for finding almost-periods of convolutions', *Geom. Funct. Anal.* **20**(6) (2010), 1367–1396. arXiv:1003.2978.

[11] E. Croot and O. Sisask, Notes on proving Roth's theorem using Bogolyubov's method, http://people.math.gatech.edu/~ecroot/bogolyubov-roth2.pdf.

[12] M. Elkin, 'An improved construction of progression-free sets', *Israel J. Math.* **184** (2011), 93–128. arXiv:0801.4310.

[13] G. A. Freiman, H. Halberstam and I. Z. Ruzsa, 'Integer sum sets containing long arithmetic progressions', *J. Lond. Math. Soc.* **46**(2) (1992), 193–201.

[14] B. Green, 'Arithmetic progressions in sumsets', *Geom. Funct. Anal.* **12**(3) (2002), 584–597.

[15] B. Green, 'Finite field models in additive combinatorics', in *Surveys in Combinatorics 2005*, London Mathematical Society Lecture Note Series, 327 (Cambridge University Press, Cambridge, 2005), 1–27. arXiv:math/0409420.

[16] B. Green and I. Z. Ruzsa, 'Freiman's theorem in an arbitrary abelian group', *J. Lond. Math. Soc. (2)* **75**(1) (2007), 163–175. arXiv:math/0505198.

[17] B. Green and J. Wolf, 'A note on Elkin's improvement of Behrend's construction', in *Additive Number Theory* (Springer, New York, 2010), 141–144. arXiv:0810.0732.

[18] D. R. Heath-Brown, 'Integer sets containing no arithmetic progressions', *J. Lond. Math. Soc. (2)* **35**(3) (1987), 385–394.

[19] K. Henriot, 'On arithmetic progressions in $A + B + C$', *Int. Math. Res. Notices* **2014**(18) (2014), 5134–5164. arXiv:1211.4917.

[20] K. F. Roth, 'On certain sets of integers', *J. Lond. Math. Soc.* **28** (1953), 104–109.

[21] T. Sanders, 'Additive structures in sumsets', *Math. Proc. Cambridge Philos. Soc.* **144**(2) (2008), 289–316. arXiv:math/0605520.

[22] T. Sanders, 'Green's sumset problem at density one half', *Acta Arith.* **146**(1) (2011), 91–101. arXiv:1003.5649.

[23] T. Sanders, 'On Roth's theorem on progressions', *Ann. of Math. (2)* **174**(1) (2011), 619–636. arXiv:1011.0104.

[24] T. Sanders, 'On certain other sets of integers', *J. Anal. Math.* **116** (2012), 53–82. arXiv:1007.5444.

[25] T. Sanders, 'On the Bogolyubov-Ruzsa lemma', *Anal. PDE* **5**(3) (2012), 627–655. arXiv:1011.0107.

[26] T. Schoen and I. Shkredov, 'Roth's theorem in many variables', *Israel J. Math.* **199**(1) (2014), 287–308. arXiv:1106.1601.

[27] E. Szemerédi, 'Integer sets containing no arithmetic progressions', *Acta Math. Hungar.* **56**(1–2) (1990), 155–158.

[28] T. Tao and V. H. Vu, *Additive Combinatorics* (Cambridge University Press, Cambridge, 2006).

https://doi.org/10.1017/fms.2016.2 Published online by Cambridge University Press