Mathematika 62 (2016) 587–613 © 2016 University College London
doi:10.1112/S002557931500039X

ARITHMETIC PROGRESSIONS IN SETS OF SMALL DOUBLING

KEVIN HENRIOT

Abstract. We show that if a finite, large enough subset A of an arbitrary abelian group G satisfies the small doubling condition $|A + A| \leqslant (\log |A|)^{1-\varepsilon}|A|$, then A must contain a three-term arithmetic progression whose terms are not all equal, and $A + A$ must contain an arithmetic progression or a coset of a subgroup, either of which is of size at least $\exp[c(\log |A|)^{\delta}]$. This extends analogous results obtained by Sanders, and by Croot, Łaba and Sisask in the case where $G = \mathbb{Z}$.

§1. *Introduction.* Our aim in this work is to generalize two types of results of additive combinatorics that are usually stated for dense subsets of the integers (namely, Roth's theorem [16] and Bourgain's theorem on long arithmetic progressions in sumsets [2]), to the case where the sets only have small doubling and live in an arbitrary abelian group. As in previous work of this nature [17, 19, 26, 27], our motivation is to provide a link between two types of additive structure: small doubling, on the one hand, and containment of arithmetic progressions in the set or its sumset, on the other hand. Since the result we seek is known qualitatively by the modelling methods of Green and Ruzsa [7], we focus on the quantitative bounds that may be obtained for it.

Concerning the first topic of Roth's theorem, we start by recalling the state-of-the-art bounds, which we state in the setting of a cyclic group. Here a k-term arithmetic progression in an abelian group is defined as a tuple $(x_1, \dots, x_k)$, where $x_1, \dots, x_k$ are group elements such that $x_2 - x_1 = \cdots = x_k - x_{k-1}$, and we say that it is trivial when $x_1, \dots, x_k$ are all equal, and proper when they are all distinct; note that, when the group has odd order, every non-trivial three-term arithmetic progression is proper. The breakthrough work of Sanders [21], that built on earlier work of Bourgain [3], has established that, given a large enough odd integer N, every subset of $\mathbb{Z}/N\mathbb{Z}$ of density at least $(\log N)^{-1+o(1)}$ contains a proper three-term arithmetic progression. Under a density hypothesis, the generalization to finite abelian groups is not very challenging: indeed, it can be, essentially, read from [21] that any set of density at least $(\log |G|)^{-1+o(1)}$ in a finite abelian group G of odd order contains a proper three-term arithmetic progression.

However, the situation is more complex when we only assume that the set in question, say A, has small doubling in the sense that $|A + A| \leqslant K|A|$. Since subsets of density α of a finite abelian group have doubling at most

Received 4 January 2015, published online 17 February 2016.
MSC (2010): 11B13, 11B30 (primary).

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

$K = \alpha^{-1}$, this includes the previous situation. We would then like to show that $K \leqslant (\log |A|)^{1-o(1)}$ forces A to contain a proper three-term arithmetic progression, which would truly generalize the dense case. However, this is not obvious even in the case where A is a set of integers. Indeed, the direct approach, which proceeds by combining the standard Ruzsa modelling lemma [17] with the bounds for Roth's theorem from [21], only yields an admissible range of $K \leqslant (\log |A|)^{1/4-o(1)}$. This is precisely what led Sanders [19] to design a more subtle approach which, for sets of integers, yields the range we seek.

THEOREM 1.1 (Sanders). *There exists an absolute constant $c > 0$ such that the following holds. Suppose that A is a finite set of integers such that*†

$$|A + A| \leqslant c(\log |A|)(\log \log |A|)^{-8} \cdot |A|.$$

Then A contains a proper three-term arithmetic progression.

This does not appear explicitly in the literature, but follows more or less directly from inserting Ruzsa's modelling bound [17] into the argument of [19], taking also into account the latest bounds for Roth's theorem [21]; we describe this in more detail at the end of the paper. By this procedure, one can actually obtain a version of Theorem 1.1 for any group with good modelling, in the sense of [7]. In the general abelian case, where available modelling arguments are, by necessity, much weaker [7], Sanders [19] also improves substantially on the bounds that would follow from a direct modelling approach.

THEOREM 1.2 (Sanders). *There exists an absolute constant $c > 0$ such that the following holds. Suppose that A is a finite subset of an abelian group such that*

$$|A + A| \leqslant c(\log |A|)^{1/3}(\log \log |A|)^{-1} \cdot |A|.$$

Then A contains a non-trivial three-term arithmetic progression.

Note that the conclusion changed to yield a non-trivial arithmetic progression only; we say more on this later. The loss in the exponent of $\log |A|$ in comparison with the previous case is due to a limitation of the results of modelling; indeed via [7], it is only possible to Freiman-embed a set A of doubling K into a finite abelian group where its image has density $\exp[-CK^2 \log K]$. A construction by Green and Ruzsa [7] further shows that any modelling result of this type will feature an exponential loss in $\sqrt{K}$, at least, if we insist on embedding the whole set. Fortunately, in a recent major advance on the polynomial Freiman–Ruzsa conjecture, Sanders [23] managed to sidestep this issue and obtained a correlation result which may be viewed as another form of modelling. This result may be applied to our situation to recover a range of doubling that matches the current bounds for Roth's theorem, for arbitrary abelian groups; this is the first observation of this paper.

† Throughout this introduction, we make the tacit assumption that all quantities appearing inside a double logarithm are at least e^e in size.

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

THEOREM 1.3. *There exists an absolute constant $c > 0$ such that the following holds. Suppose that A is a finite subset of an abelian group such that*

$$|A + A| \leqslant c(\log |A|)(\log\log |A|)^{-7} \cdot |A|.$$

Then A contains a non-trivial three-term arithmetic progression.

Here we say more on the issue of 2-torsion, which was already discussed by Sanders in [19]. In general, a set A contains a non-trivial degenerate arithmetic progression (x, y, x) if and only if $A - A$ contains an element of order two; therefore in that case, Theorems 1.2 and 1.3 give only trivial information. Obtaining proper progressions in every case where it is possible (this excludes groups such as $\mathbb{F}_2^n$) is a thorny issue that has been successfully addressed only in the work of Lev [13] and Sanders [18], in cases where the group rank is not too large; here we do not consider this issue.

The second topic we consider is that of long arithmetic progressions in sumsets, initiated by Bourgain [2] and further developed by Green [6]. Basing their work on a fundamental new technique introduced by Croot and Sisask [5], these two last authors, together with Łaba [4], obtained a remarkable extension of Green's result, which, furthermore, already works under a small doubling hypothesis.

THEOREM 1.4 (Croot, Łaba, Sisask). *There exists an absolute constant $c > 0$ such that the following holds. Let $K, L \geqslant 1$ be parameters, and suppose that A, B are finite sets of integers such that $|A + B| \leqslant K|A|$ and $|A + B| \leqslant L|B|$. Then $A + B$ contains an arithmetic progression of length at least*

$$\exp\left[c\left(\frac{\log |A + B|}{K(\log L)^3}\right)^{1/2}\right] \quad \textit{provided } K \log^5(L \log |A|) \leqslant c \log |A + B|.$$

From the methods of [4], one can easily deduce that an analogous result holds for subsets A and B of density α and β of a finite abelian group, with α^{-1} and β^{-1} in place of K and L. Therefore, we focus again on the case of small doubling in an arbitrary abelian group, to which the argument of [4] does not extend as it relies on a two-sets version of Ruzsa modelling [17]. The coveted generalization of Theorem 1.4 may however be recovered, again by using the Bogolyubov–Ruzsa lemma from [23], and establishing this is the second aim of this paper. Note that, in the general abelian setting, we need to adapt the type of structure that we seek to allow for both cosets of subgroups and arithmetic progressions.

THEOREM 1.5. *There exists an absolute constant $c > 0$ such that the following holds. Let $K \geqslant 1$ be a parameter and suppose that A is a finite subset of an abelian group such that $|A + A| \leqslant K|A|$. Then $A + A$ contains a set, which is either a proper arithmetic progression or a coset of a subgroup, of size at least*

$$\exp\left[c\left(\frac{\log |A|}{K(\log K)^3}\right)^{1/2}\right] \quad \textit{provided } K \leqslant \frac{c \log |A|}{(\log\log |A|)^5}.$$

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

This recovers Theorem 1.4 in the symmetric case $A = B$, since, in $\mathbb{Z}$, every non-trivial subgroup is infinite. We restrict our work to the symmetric case for simplicity; it seems feasible to obtain an asymmetric result of the shape of Theorem 1.4 from the methods of this paper, but we do not pursue this here. One drawback of Theorem 1.5 is that it does not recover the best-known estimate [**4**, **20**] in the case where A is a subset of density α of $\mathbb{F}_2^n$, which is that $A + A$ contains a subspace of size at least $\exp(c\alpha n)$. The reason for this discrepancy is that, in the finite field setting, one can work exclusively with subspaces, whereas in the general abelian setting, one is forced to work with an approximate analogue, namely, with Bourgain systems (defined in §4).

Finally, we mention an application of results on arithmetic progressions in sets of small doubling, to the asymptotic size of restricted sumsets. This application was first observed independently by Schoen [**25**] and Hegyvári *et al* [**10**] in the setting of integers, and later quantitatively strengthened by Sanders [**19**] in the more general setting of abelian groups. We write $A \mathbin{\widehat{+}} A$ for the set of sums of distinct elements of A below.

COROLLARY 1.6. *Suppose that A is a finite non-empty subset of an abelian group. Then*

$$|A \mathbin{\widehat{+}} A| \geqslant (1 - (\log |A|)^{-1+o(1)})|A + A|.$$

This improves upon the exponent $-1/3$ on the logarithm obtained by Sanders [**19**] via Theorem 1.2, since Theorem 1.3 is used instead. Note that, by Behrend's construction [**14**], the restricted sumset may have size as low as $(1 - \mathrm{e}^{-c\sqrt{\log |A|}})|A + A|$, and therefore the bounds for this problem match those for Roth's theorem closely.

Finally, we remark that, by the finite modelling argument of Green and Ruzsa [**7**, Lemma 2.1], it suffices to prove all our results in the case where the group is finite abelian, and therefore we work under that hypothesis for the rest of the paper. This concludes our introduction and we discuss the structure of this paper in the next section.

§2. *Overview.* In this section we sketch the argument behind our results and outline the structure of this paper. We use the symbols $\approx$ and $\gtrsim$ to indicate statements that hold true up to certain negligible factors.

The first logical step in the proof of Theorem 1.3 consists of applying the correlation version of Sanders' Bogolyubov–Ruzsa lemma [**23**] (Proposition 7.1) to deduce that a set A of doubling K has density $\asymp 1/K$ in (a translate of) a large Bourgain system B, which is a group-like object whose properties are recalled in §4. The second step is to obtain an efficient local version of Roth's theorem (Proposition 6.1), which, roughly speaking, asserts that a set A of density $\alpha \gtrsim (\log |B|)^{-1}$ in a large Bourgain system B contains many arithmetic progressions, and therefore a non-trivial one. This may be applied to the previous system B, for which $|B| \approx |A|$ and $\alpha \asymp 1/K$, under the condition $K \lesssim \log |A|$, thereby establishing Theorem 1.3. The local Roth theorem is developed in §6, drawing

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

on analytic tools from §5, and it is combined in the preceding fashion with the correlation Bogolyubov–Ruzsa lemma in §7.

To derive Theorem 1.5, we need to obtain, instead, a local version of an almost-periodicity lemma of Croot *et al* [**4**] (Proposition 8.4), drawing again on the tools of §5. This process, carried out in §8, requires a somewhat simpler version of Sanders' Bogolyubov–Ruzsa lemma (Proposition 8.1) which deduces containment of a large Bourgain system in the sumset $2A - 2A$ from the hypothesis that A has small doubling; the rest of the argument follows the strategy of [**4**].

Finally, to illustrate some of the above ideas, we showcase the proof of Theorem 1.3 in the model setting of $\mathbb{F}_3^n$, where the proof of Sanders' Bogolyubov–Ruzsa lemma [**23**] simplifies substantially. As an added benefit, the formidable bounds of Bateman and Katz [**1**], for caps in $\mathbb{F}_3^n$, yield a larger admissible range of doubling in this setting. The notation used in the proof is introduced in §3.

THEOREM 2.1. *There exist positive absolute constants c and ε such that the following holds. Suppose that A is a subset of $\mathbb{F}_3^n$ such that*

$$|A + A| \leqslant c(\log |A|)^{1+\varepsilon} \cdot |A|.$$

Then A contains a proper three-term arithmetic progression.

Proof. Write $K = |A + A|/|A|$, so that we are assuming that $K \leqslant c(\log |A|)^{1+\varepsilon}$. The proof of [**7**, Proposition 6.1] readily adapts to $\mathbb{F}_3^n$, and shows that A is Freiman-isomorphic to a subset of doubling K and density at least K^{-4} of another vector space $\mathbb{F}_3^m$, which we denote by A from now on. By examining the proof of [**23**, Theorem A.1], which works equally well in $\mathbb{F}_3^m$, one may deduce that there exist a measure μ and a subspace V of $\mathbb{F}_3^m$ of codimension at most $C(\log K)^4$ such that

$$\langle 1_A * \mu_V * \mu_{A+A} * \mu, \mu_A \rangle_{L^2} \geqslant \tfrac{1}{2}\mu_G(A)/\mu_G(A + A).$$

By the definition of K, and upon applying Hölder's and Young's inequalities, we obtain

$$\begin{aligned} \frac{1}{2K} &\leqslant \langle 1_A * \mu_V * \mu_{A+A} * \mu, \mu_A \rangle_{L^2} \\ &\leqslant \|1_A * \mu_V * \mu_{A+A} * \mu\|_\infty \|\mu_A\|_{L^1} \\ &\leqslant \|1_A * \mu_V\|_\infty. \end{aligned}$$

Therefore we may find x such that $A' = (A - x) \cap V$ has density at least $1/2K$ in V. Since V has codimension at most $C(\log K)^4$, it has size at least $|G|^{1/2}$ in our range of K. Applying [**1**, Theorem 1.1] to A', ensures that we find a proper three-term arithmetic progression in A' provided

$$\frac{1}{2K} \geqslant C(\log |V|)^{-(1+\varepsilon)},$$

and this concludes the proof since $\log |V| \asymp \log |A|$. □

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

§3. *Notation.* In this section, we introduce the notation used throughout the paper.

Ambient group. We let G denote a fixed, finite abelian group. The arguments of later sections all take place in this group unless otherwise stated.

$\mathbb{Z}$-actions. The group G is naturally equipped with a structure of $\mathbb{Z}$-module, and we let $k \cdot x$ denote the action of a scalar $k \in \mathbb{Z}$ on an element $x \in G$. For a subset X of G and a subset I of $\mathbb{Z}$, we further write

$$k \cdot X = \{k \cdot x : x \in X\} \quad \text{and} \quad I \cdot x = \{k \cdot x : k \in I\}.$$

Note that $\cdot$ is also used in other places for the regular multiplication of complex numbers. However, it should be clear from the context which one is meant.

Functions. We define the averaging operator over a subset X of G, which acts on the space of functions $f : G \to \mathbb{C}$, by $\mathbb{E}_X f = |X|^{-1} \sum_{x \in X} f(x)$, and we write $\mathbb{E}_{x \in X} f(x)$ when we want to keep the variable explicit. It is also convenient to introduce the operator of translation on a function f defined by $\tau_x f(u) = f(x+u)$ for all $x, u \in G$. We, furthermore, define the support of f as $\mathrm{Supp}(f) = \{x \in G : f(x) \neq 0\}$. On the physical space, we use the normalized counting measure so that, for functions $f, g : G \to \mathbb{C}$, we let

$$\begin{aligned}
&(L^p\text{-norm}) && \|f\|_{L^p} = (\mathbb{E}_G |f|^p)^{1/p},\\
&(\text{scalar product}) && \langle f, g\rangle_{L^2} = \mathbb{E}_G f\bar{g},\\
&(\text{convolution}) && f * g(x) = \mathbb{E}_{y \in G} f(y) g(x-y) \text{ for all } x \in G.
\end{aligned}$$

We occasionally write $\|f\|_p$ for $\|f\|_{L^p}$, and we let $f^{(\ell)}$ denote the convolution of f with itself ℓ times.

Measures. We identify measures μ on G with functions $\mu : G \to \mathbb{R}_+$ via the identity $\mu(\{x\}) = |G|^{-1}\mu(x)$, so that $\mu(E) = \langle 1_E, \mu\rangle_{L^2}$ for every subset E of G. We only consider probability measures: in other words, we always assume that $\|\mu\|_{L^1} = 1$. We write μ_A for the measure defined by $\mu_A(E) = |E \cap A|/|A|$ for every set E, which, under our identification, corresponds to the function $\mu_A = \mu_G(A)^{-1} 1_A$.

Fourier transform. The Fourier transform over finite abelian groups is now a standard tool of additive combinatorics. It is very well explained, for example in [9], and here we recall its main properties only.

Write $\mathbb{U}$ for the unit circle. Then the dual group $\widehat{G}$ is defined as the set of morphisms from G to $\mathbb{U}$, called characters, and the Fourier transform of a function $f : G \to \mathbb{C}$ is defined by $\widehat{f}(\gamma) = \langle f, \gamma\rangle_{L^2}$ at every character γ. We write $(f)^\wedge$ for the Fourier transform of f when f has a complicated expression.

We define the summation operator over a subset Δ of $\widehat{G}$, which acts on the space of functions $F : \widehat{G} \to \mathbb{C}$, by $\sum_\Delta F = \sum_{\gamma \in \Delta} F(\gamma)$. On the Fourier space,

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

we use the counting measure so that, for functions $F, G : \widehat{G} \to \mathbb{C}$, we let

$$\text{(ℓ^p-norm)} \qquad \|F\|_{\ell^p} = \left(\sum_{\widehat{G}} |F|^p\right)^{1/p},$$

$$\text{(scalar product)} \qquad \langle F, G\rangle_{\ell^2} = \sum_{\widehat{G}} F\,\overline{G}.$$

The three classic formulæ of harmonic analysis then read as

$$\text{(Fourier inversion)} \qquad f = \sum_{\widehat{G}} \widehat{f}(\gamma)\gamma,$$

$$\text{(Parseval formula)} \qquad \langle f, g\rangle_{L^2} = \langle \widehat{f}, \widehat{g}\rangle_{\ell^2},$$

$$\text{(convolution identity)} \qquad (f * g)^{\wedge} = \widehat{f}\cdot\widehat{g}\,.$$

Other. We let c and C denote absolute positive constants, which may take different values at each occurrence. Given non-negative functions f and g, we let $f = O(g)$ or $f \ll g$ indicate the fact that there exists a constant C such that $f \leqslant Cg$, and we let $f = \Theta(g)$ or $f \asymp g$ indicate that $f \ll g$ and $g \ll f$ hold simultaneously. We also write $\ell(x) = \log(e/x)$ for $x \geqslant 1$, since this quantity arises often in our computations. Finally, note that, in many occurrences of logarithms throughout the paper, one should replace $\log x$ by $\log ex$ for the results to be formally correct in all ranges of parameters; we leave this as a mental task for the reader to alleviate the notation. Other notation used in this paper is introduced in the relevant section, as needed.

§4. *Bourgain systems.* In this section, we recall the theory of Bourgain systems, which was introduced by Green and Sanders [8] as a generalization of the Bohr set technology of Bourgain [3]. In a sense, these systems are the most general class of sets for which the strategy of density increment on Bohr sets, pioneered by Bourgain [3], may be carried out. What is needed for such an undertaking is for the set to behave, approximately, like a d-dimensional ball with respect to dilation, as axiomatized in the following definition.

Definition 4.1 (Bourgain system). A Bourgain system of dimension d is a family of sets $\mathcal{B} = (B_\rho)_{\rho>0}$, where B_ρ are subsets of G such that, for all positive ρ and ρ',

$$\text{(containment of 0)} \qquad 0 \in B_\rho$$

$$\text{(symmetry)} \qquad -B_\rho = B_\rho$$

$$\text{(nesting)} \qquad B_\rho \subset B_{\rho'} \quad \text{if } \rho \leqslant \rho'$$

$$\text{(additive closure)} \qquad B_\rho + B_{\rho'} \subset B_{\rho+\rho'}$$

$$\text{(2^d-covering)} \qquad \text{there exists } X_\rho : B_{2\rho} \subset X_\rho + B_\rho \quad \text{and} \quad |X_\rho| \leqslant 2^d.$$

We write $B = B_1$, and we define the density of $\mathcal{B}$ as $b = |B|/|G|$.

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

We let the sets B_ρ, and sometimes also the dimension d and the density b, be defined implicitly whenever we introduce a Bourgain system $\mathcal{B}$. We now describe two important classes of Bourgain systems: Bohr sets and coset progressions. To define the former, we consider the multiplicative analogue $\|\cdot\|_{\mathbb{U}}$ on the unit circle of the usual pseudo-norm $\|\cdot\|_{\mathbb{T}} = d(\cdot, \mathbb{Z})$ on the torus, defined by $\|e(\theta)\|_{\mathbb{U}} = \|\theta\|_{\mathbb{T}}$ for every $\theta \in \mathbb{T}$.

Definition 4.2 (Bohr set). Suppose that $\Gamma \subset \widehat{G}$ and $\delta > 0$. The Bohr set of frequency set Γ and radius δ is

$$B = B(\Gamma, \delta) = \{x \in G : \|\gamma(x)\|_{\mathbb{U}} \leqslant \delta\}.$$

The dimension of B is $d = |\Gamma|$. We define the dilate of B by $\rho > 0$ as the set $B_\rho = B(\Gamma, \rho\delta)$, and the Bohr system induced by B as the system $\mathcal{B} = (B_\rho)_{\rho>0}$.

The usual bounds for the size and growth of a Bohr set allow us to quickly estimate the dimension and density of the Bourgain system it induces.

LEMMA 4.3. *The system $\mathcal{B}$, induced by a Bohr set of dimension d and radius $\delta \leqslant 1$, is a Bourgain system $\mathcal{B}$ of dimension at most $6d$ and density at least δ^d.*

Proof. The first four properties of a Bourgain system are easy to check. Further, by three applications of [**28**, Lemma 4.20] we obtain $|B_{4\rho}| \leqslant 2^{6d}|B_{\rho/2}|$, and therefore, by Ruzsa's covering lemma, we may find a set X_ρ such that

$$B_{2\rho} \subset X_\rho + B_{\rho/2} - B_{\rho/2} \subset X_\rho + B_\rho$$

and $|X_\rho| \leqslant |B_{2\rho} + B_{\rho/2}|/|B_{\rho/2}| \leqslant 2^{6d}$. Working through the argument in that reference, one could extract a better bound 2^{2d}, but this would not affect our end results much. The bound on the density may be read directly from [**28**, Lemma 4.20]. An alternate reference for these estimates is [**11**, §5]. □

In our definition of a coset progression, we write $[x, y]_{\mathbb{Z}} = \{n \in \mathbb{Z} : x \leqslant n \leqslant y\}$ for reals $x \leqslant y$.

Definition 4.4 (Coset progression). Let $L \in \mathbb{R}_+^d$ and $\omega \in G^d$ where $d \geqslant 1$, and let H be a subgroup of G. The coset progression of dimension d determined by L, ω, H is

$$M = M(L, \omega, H) = [-L_1, L_1]_{\mathbb{Z}} \cdot \omega_1 + \cdots + [-L_d, L_d]_{\mathbb{Z}} \cdot \omega_d + H.$$

We define the dilate of M by $\rho > 0$ as $M_\rho = M(\rho L, \omega, H)$, and the coset progression system induced by M as the system $\mathcal{M} = (M_\rho)_{\rho>0}$.

The dimension of the Bourgain system induced by a coset progression may be estimated by a simple covering argument.

LEMMA 4.5. *The system $\mathcal{M}$ induced by a d-dimensional coset progression M is a Bourgain system of dimension at most $3d$.*

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

Proof. It is again rather simple to derive the first four properties of a Bourgain system for $\mathcal{M}$, and we now concern ourselves with the fifth. The dilate of M by $\rho > 0$ is

$$M_\rho = [-\rho L_1, \rho L_1]_{\mathbb{Z}} \cdot \omega_1 + \cdots + [-\rho L_d, \rho L_d]_{\mathbb{Z}} \cdot \omega_d + H.$$

To obtain the covering property, first observe that, for any $k \in \mathbb{N}_{\geqslant 0}$, one may cover the interval $[-k, k]_{\mathbb{Z}}$ by three translates of $[-k/2, k/2]_{\mathbb{Z}}$ (this is sharp for k odd), and that this still holds for any real $k \geqslant 0$. Therefore, for every $1 \leqslant i \leqslant d$, we may find a set T_i with $|T_i| \leqslant 3$ such that $[-2\rho L_i, 2\rho L_i]_{\mathbb{Z}} \subset T_i + [-\rho L_i, \rho L_i]_{\mathbb{Z}}$. Consequently, for any $\rho > 0$, we have a covering

$$M_{2\rho} \subset \bigcup_{t \in T_1 \times \cdots \times T_d} (t_1 \cdot \omega_1 + \cdots + t_d \cdot \omega_d + M_\rho) = X_\rho + M_\rho$$

for a certain set X_ρ of size at most $|T_1| \cdots |T_d| \leqslant 3^d$. □

With these examples covered, we now work exclusively within the framework of Bourgain systems. We start by defining a few basic operations on these systems.

LEMMA 4.6 (Dilation). *Suppose that $\lambda \in (0, 1]$ and that $\mathcal{B}$ is a Bourgain system of dimension d and density b. Then the dilated system $\mathcal{B}_\lambda = (B_{\lambda\rho})_{\rho>0}$ is a Bourgain system of dimension at most d and density at least $(\lambda/2)^d \cdot b$.*

Proof. Let $\lambda \in (0, 1]$, and choose $k \geqslant 0$ such that $2^{-(k+1)} < \lambda \leqslant 2^{-k}$. By the covering property of Definition 4.1, we have $|B_\rho| \leqslant 2^d |B_{\rho/2}|$ for every $\rho > 0$, from which it follows, by iteration, that $|B| \leqslant 2^{(k+1)d} |B_{1/2^{k+1}}| \leqslant (2/\lambda)^d |B_\lambda|$. That $\mathcal{B}_\lambda$ is a d-dimensional Bourgain system is obvious, and the bound on the density follows from the previous computation. □

Definition 4.7 (Sub-Bourgain systems). Suppose that $\mathcal{B}$ and $\mathcal{B}'$ are two Bourgain systems. We say that $\mathcal{B}$ is a sub-Bourgain system of $\mathcal{B}'$, and we write $\mathcal{B} \leqslant \mathcal{B}'$ when $B_\rho \subset B'_\rho$ for all $\rho > 0$. For $\lambda \in (0, 1]$, we also write $\mathcal{B} \leqslant_\lambda \mathcal{B}'$ when $\mathcal{B} \leqslant \mathcal{B}'_\lambda$.

The properties of an intersection of Bourgain systems were derived in [19, Lemma 3.4], and we reproduce the proof here, for completeness.

LEMMA 4.8 (Intersection). *Suppose that $\mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(k)}$ are Bourgain systems of dimensions $d_1, \ldots, d_k$ and densities $b_1, \ldots, b_k$. Then the intersection system*

$$\mathcal{B}_1 \wedge \cdots \wedge \mathcal{B}_k = (B_\rho^{(1)} \cap \cdots \cap B_\rho^{(k)})_{\rho>0}$$

is a Bourgain system of dimension at most $2(d_1 + \cdots + d_k)$ and of density at least $4^{-(d_1+\cdots+d_k)} b_1 \cdots b_k$.

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

Proof. The first four properties of a Bourgain system are again easy to check, and we now consider the covering property. Let $\rho > 0$. For each $1 \leqslant i \leqslant k$, apply the covering property of $\mathcal{B}^{(i)}$ twice to obtain a set T_i of size at most 4^{d_i} such that $B^{(i)}_{2\rho} \subset T_i + B^{(i)}_{\rho/2}$. Distributing intersection over union gives

$$\bigcap_{1\leqslant i\leqslant d} B^{(i)}_{2\rho} = \bigcup_{(t_1,\dots,t_k)\in T_1\times\cdots\times T_k} \bigcap_{1\leqslant i\leqslant k} (t_i + B^{(i)}_{\rho/2}).$$

Now pick an element $x(t)$ in each non-empty intersection $\bigcap_i (t_i + B^{(i)}_{\rho/2})$. Then, for each element x of $\bigcap_i B^{(i)}_{2\rho}$, we may find an element $t \in \prod_i T_i$ such that

$$x - x(t) \in \bigcap_i (B^{(i)}_{\rho/2} - B^{(i)}_{\rho/2}) \subset \bigcap_i B^{(i)}_{\rho}.$$

This yields the desired covering with X_ρ defined as the set of all $x(t)$.

To estimate the density of the intersection, first apply Ruzsa's covering lemma for each $1 \leqslant i \leqslant k$ to obtain a covering of the form

$$G \subset T_i + B^{(i)}_{1/4} - B^{(i)}_{1/4} \subset T_i + B^{(i)}_{1/2},$$

where T_i is a set of size $|T_i| \leqslant 4^{d_i} b_i^{-1}$. From $G \subset \bigcap_i (T_i + B^{(i)}_{1/2})$, it follows that

$$G = \bigcup_{(t_1,\dots,t_k)\in T_1\times\cdots\times T_k} \bigcap_{1\leqslant i\leqslant k} (t_i + B^{(i)}_{1/2}) = \bigcup_{t\in T_1\times\cdots\times T_k} A(t),$$

where $A(t)$ are sets satisfying $A(t) - A(t) \subset \bigcap_i B^{(i)}$. By the pigeonhole principle, we may also find a point t such that

$$|A(t)| \geqslant \frac{|G|}{|T_1|\cdots|T_k|} \geqslant 4^{-(d_1+\cdots+d_k)} b_1 \cdots b_k |G|,$$

which yields the desired density estimate, since $|A(t) - A(t)| \geqslant |A(t)|$. □

We consider one last operation on Bourgain systems; since it is so simple we leave it as an exercise for the reader.

LEMMA 4.9 (Homomorphic image). *Suppose that $\mathcal{B}$ is a Bourgain system of dimension d, and ϕ is an endomorphism of G. Then the image system $\phi(\mathcal{B}) = (\phi(B_\rho))_{\rho>0}$ is a Bourgain system of dimension at most d.*

Finally, we recall the essential notion of regularity introduced by Bourgain [3] for Bohr sets, and which has a natural analogue for Bourgain systems. We let† $C_0 = 2^5$ and $C_1 = 2^6$ in what follows, for definiteness, although the exact values are unimportant.

† These precise constants, featured in subsequent lemmas, are derived in [11, §6].

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

Definition 4.10 (Regular Bourgain system). We say that a Bourgain system $\mathcal{B}$ of dimension d is regular when, for every $|\rho| \leqslant 1/C_0 d$,

$$1 - C_0|\rho|d \leqslant \frac{|B_{1+\rho}|}{|B|} \leqslant 1 + C_0|\rho|d.$$

In practice, one can always afford to work with regular Bourgain systems, as is the case with Bohr sets, via [19, Proposition 3.5], which we now quote.

LEMMA 4.11. *Suppose that $\mathcal{B}$ is a Bourgain system. Then there exists $\lambda \in [1/2, 1]$ such that $\mathcal{B}_\lambda$ is regular.*

The regularity computations in subsequent sections rely on the following L^1 estimate.

LEMMA 4.12. *Suppose that $\mathcal{B}$ is a regular Bourgain system of dimension d and μ is a measure on G with support in B_ρ, where $0 < \rho \leqslant 1/C_1 d$. Then*

$$\|\mu_B * \mu - \mu_B\|_{L^1} \leqslant C_1 \rho d.$$

Proof. For every $y \in B_\rho$, the function $\mu_{y+B} - \mu_B$ has support in $B_{1+\rho} \setminus B_{1-\rho}$, so that

$$\|\mu_{y+B} - \mu_B\|_{L^1} \leqslant \frac{|B_{1+\rho}| - |B_{1-\rho}|}{|B|} \leqslant 2C_0\rho d.$$

Averaging over $y \in G$ with weights $\mu(y)$, and using the triangle inequality, we recover the desired estimate. □

§5. *Spectral analysis on Bourgain systems.* This section is concerned with collecting all the analytic information we need about the large spectrum of the indicator functions of certain sets. The main task is to obtain a large structured set on which all characters of the large spectrum take values close to one, since such a set may be later used for purposes of a density-increment-based iteration, or to locate long arithmetic progressions.

When considering indicator functions of subsets of Bohr sets, the information we seek is provided by the spectral analysis developed by Sanders [22], and the aim of this section is, therefore, to obtain a similar analysis for Bourgain systems. Note that such a process has already been carried out in the earlier paper [19]. However, we benefit here from the more efficient analysis of the local spectrum from [22]. To be specific, there is now a local analogue of Chang's bound [22, Lemma 4.6] which supersedes the earlier local analogue of Bessel's inequality [19, Proposition 4.4]. We now give the precise statements and, in that regard, it is useful to recall the following definitions.

Definition 5.1 (Annihilation). Let $\nu \in (0, 2]$ be a parameter, and suppose that T is a subset of G and Δ is a subset of $\widehat{G}$. We say that Δ is ν-annihilated by T when

$$|1 - \gamma(t)| \leqslant \nu \quad \text{for all } t \in T \text{ and } \gamma \in \Delta.$$

When $\mathcal{B}$ is a Bourgain system, we say that it ν-annihilates Δ when B does.

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

The quantity we seek to annihilate is then the following.

Definition 5.2 (Large spectrum). Suppose that $\eta \in (0, 1]$ is a parameter and $f : G \to \mathbb{C}$ is a function. The η-large spectrum of f is the level set of $\widehat{G}$ defined by

$$\mathrm{Spec}_\eta(f) = \{|\widehat{f}| \geqslant \eta \|f\|_{L^1}\}.$$

We also need to recall one piece of terminology from [22, §4], which is only used in this section. Write $\mathbb{D}$ for the unit disk, and let μ be any measure on G. Given a parameter $\theta \in (0, 1]$, we say that a set Λ of characters is (θ, μ)-dissociated when, for every function $\omega : \Lambda \to \mathbb{D}$,

$$\int \prod_{\lambda \in \Lambda} (1 + \mathrm{Re}[\omega(\lambda)\lambda])\, d\mu \leqslant \mathrm{e}^\theta,$$

and, when $\theta = 1$, we simply say that Λ is μ-dissociated. We may now quote two lemmas of local spectral analysis from [22], with minor tweaks in both cases.

LEMMA 5.3 (Local Chang bound). *Let $\eta \in (0, 1]$ be a parameter, and suppose that B is a subset of G and X is a subset of B of relative density τ. Then every μ_B-dissociated subset of $\mathrm{Spec}_\eta(\mu_X)$ has size at most $C\eta^{-2}\log\tau^{-1}$.*

Proof. This is [22, Lemma 4.6], specialized to the case where $f = \mu_X$ and $\mu = \mu_B$, so that, with the notation from this lemma, $L_{\mu_X,\mu_B} = \tau^{-1/2}$. □

LEMMA 5.4 (Annihilating locally dissociated sets). *Let $\nu \in (0, 1]$ be a parameter. Suppose that $\mathcal{B}$ is a regular Bourgain system, Δ is a set of characters and m is the size of the largest μ_B-dissociated subset of Δ. Then there exists a Bohr set $\widetilde{B}$ of dimension at most m and radius equal to c/m such that Δ is ν-annihilated by $B_{c\nu/d^2m} \cap \widetilde{B}_\nu$.*

Proof. This is [22, Lemma 6.3] with $\eta = 1$ and $m = k$, and two minor tweaks: $\mathcal{B}$ is a Bourgain system instead of a Bohr set and a few changes of variables have been effected. Since the proof requires only a regularity estimate of the type of Lemma 4.12, the generalization to Bourgain systems is immediate. □

As usual these two ingredients combine to show that the large spectrum of a dense subset of a Bourgain system may be efficiently annihilated. Before carrying this out, we introduce a last definition which serves to simplify our technical statements.

Definition 5.5. Let $m \geqslant 1$ be a parameter and suppose that $\mathcal{B}$ is a Bourgain system. We say that $\mathcal{B}$ is m-controlled when it has dimension at most m and density at least $\exp[-Cm\log m]$.

We are now ready to introduce the main technical tool of this paper. Recall that $\ell(x)$ stands for $\log(e/x)$ here and throughout the paper.

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

PROPOSITION 5.6 (Local spectrum annihilation). *Let* $\eta, \nu \in (0,1]$ *be parameters. Suppose that* $\mathcal{B}$ *is a regular Bourgain system and* X *is a subset of* B *of relative density* τ. *Then* $\mathrm{Spec}_\eta(\mu_X)$ *is* ν*-annihilated by a regular Bourgain system of the form*

$$\mathcal{B}_{c\nu/d^2m} \wedge \widetilde{\mathcal{B}}_\nu \quad \text{where } m \leqslant C\eta^{-2}\ell(\tau)$$

and $\widetilde{\mathcal{B}}$ *is an* m*-controlled Bourgain system.*

Proof. Let m denote the size of the largest μ_B-dissociated subset of $\mathrm{Spec}_\eta(\mu_X)$, or equal one when there is no such set. By Lemma 5.3, we have $m \leqslant C\eta^{-2}\ell(\tau)$. By Lemma 5.4, we also know that $\mathrm{Spec}_\eta(\mu_X)$ is ν-annihilated by a regular Bourgain system $\overline{\mathcal{B}} := \mathcal{B}_{c\nu/d^2m} \wedge \widetilde{\mathcal{B}}_\nu$, where $\widetilde{\mathcal{B}}$ is the Bourgain system induced by a Bohr set of dimension $d \leqslant m$ and radius $\delta = c/m$. By Lemma 4.11, we may further ensure that $\overline{\mathcal{B}}$ is regular up to dilating it by a factor $\asymp 1$, which does not affect the shape of the above intersection, except in the value of the constants. By Lemma 4.3, we also see that $\widetilde{\mathcal{B}}$ has dimension at most $6m$ and density at least $\exp[-Cm\log m]$, so that the result follows by replacing $6m$ with m and adapting the constants. □

§6. *Roth's theorem for Bourgain systems.* This section is concerned with a local version of Roth's theorem [16], first considered by Sanders [19], which applies to dense subsets of a Bourgain system. Since the pioneering work of Bourgain [3], modern proofs of Roth's theorem [21, 22] all share the same global structure and proceed by an iteration on subsets of Bohr sets. An important observation, made in [19], is that this iteration may be initialized inside a certain Bohr set instead of the whole group and, further, that one may perform the same iteration on Bourgain systems in place of Bohr sets.

However, the quantitative estimates obtained in [19] correspond roughly in strength to a range of $\alpha \gtrsim (\log N)^{-1/3}$ in Roth's theorem, while the best-known range, also by Sanders [21], is now $\alpha \gtrsim (\log N)^{-1}$. Conceptually, there is no obstacle in obtaining this better quantitative dependency with Bourgain systems, and for the same local initialization. However, on a technical level, it is not entirely straightforward as most density-increment statements then take a different shape. We carry out this process in this section; since it is not the right place here to present the whole argument of [21], we include only the main structural results we need from it and indicate the changes that need to be made to others. Unfortunately, this means that the reader needs either to be conversant with [21], or to read this section conditionally on Proposition 6.4 below. What we obtain, eventually, is the following quantitative improvement of [19, Theorem 5.1].

PROPOSITION 6.1 (Local Sanders–Roth theorem). *Suppose that* $\mathcal{B}$ *is a regular Bourgain system and* A *is a subset of* B *of relative density* α *such that*

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

$A - A$ contains no element of order two. Then†

$$\langle 1_A * 1_A, 1_{2\cdot A}\rangle_{L^2} \geqslant \exp[-C(\alpha^{-1}+d)\ell(\alpha)^6\ell(\alpha/d)]\cdot b^2.$$

We make a brief comment here on the shape of the above proposition. The three-term arithmetic progressions contained in a set A are precisely the triples (x, y, z) of A^3 such that $x + z = 2 \cdot y$. The assumption on A shows that the change of variables $y \mapsto 2 \cdot y$ is injective on A, from which we see that the total number of such progressions is equal to $\langle 1_A * 1_A, 1_{2\cdot A}\rangle_{L^2} \cdot |G|^2$. We invite the reader to keep this observation in mind, as it is used implicitly in later arguments.

We now present our modified version of the argument of [**21**]. To begin with, we reconstitute the L^2 density-increment strategy entirely as it takes a different form for Bourgain systems, which determines the shape of iterative statements. The following lemma is the usual argument that allows one to pass from large energy of the Fourier transform over a character set to a density increment on any set that annihilates those characters.

LEMMA 6.2. *Let $\rho, \kappa \in (0, 1]$ be parameters. Suppose that $\mathcal{B}$ is a regular Bourgain system, A is a subset of B of relative density α, T is a subset of B_ρ and Δ is a set of characters. Assume, also, that $\rho \leqslant c\kappa\alpha/d$ and write $f_A = 1_A - \alpha 1_B$. Then if*

$$\sum_{\Delta} |\widehat{f_A}|^2 \geqslant \kappa\alpha^2 b \quad \textit{and } \Delta \textit{ is } \tfrac{1}{2}\textit{-annihilated by } T,$$

then $\|1_A * \mu_T\|_\infty \geqslant (1 + 2^{-3}\kappa)\alpha$.

Proof. For every character $\gamma \in \Delta$ we know that $|1 - \gamma| \leqslant \frac{1}{2}$ on T, and therefore $|\widehat{\mu_T}(\gamma) - 1| \leqslant \mathbb{E}_T|1 - \gamma| \leqslant \frac{1}{2}$ and $|\widehat{\mu_T}(\gamma)| \geqslant \frac{1}{2}$. Inserting this into the energy lower bound, we have, via Parseval,

$$\begin{aligned}\tfrac{1}{4}\kappa\alpha^2 b &\leqslant \sum_{\widehat{G}} |\widehat{f_A}|^2|\widehat{\mu_T}|^2\\ &= \langle f_A * \mu_T, f_A * \mu_T\rangle_{L^2}.\end{aligned}$$

Expanding this scalar product, and with the help of Lemma 4.12, we obtain

$$\begin{aligned}\tfrac{1}{4}\kappa\alpha^2 b &\leqslant \|1_A * \mu_T\|_2^2 - 2\alpha\,\langle 1_A * \mu_T, 1_B * \mu_T\rangle_{L^2} + \alpha^2\,\langle 1_B * \mu_T, 1_B * \mu_T\rangle_{L^2}\\ &= \|1_A * \mu_T\|_2^2 - 2\alpha b\,\langle 1_A, \mu_B * \mu_T * \mu_{-T}\rangle_{L^2}\\ &\quad + \alpha^2 b\,\langle 1_B, \mu_B * \mu_T * \mu_{-T}\rangle_{L^2}\\ &= \|1_A * \mu_T\|_2^2 - \left(1 + O\left(\frac{\rho d}{\alpha}\right)\right)\alpha^2 b.\end{aligned}$$

† It is possible to lower the powers of $\ell(\alpha) = 1 + \log\alpha^{-1}$ in this proposition. However, we do not pursue this direction here, as it would not produce a significant improvement of the final bounds in Theorem 1.3, due to the use of Proposition 7.1 in §7.

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

Since we assumed that $\rho \leqslant c\kappa\alpha/d$,

$$\begin{aligned}(1+2^{-3}\kappa)\alpha^2 b &\leqslant \|1_A * \mu_T\|_2^2\\ &\leqslant \|1_A * \mu_T\|_\infty \|1_A * \mu_T\|_1\\ &= \|1_A * \mu_T\|_\infty \cdot \alpha b.\end{aligned}$$

Dividing both sides by αb concludes the proof. □

As usual, this may be combined with a statement on the local annihilation of the large spectrum, such as Proposition 5.6, to recover an L^2-density increment lemma.

PROPOSITION 6.3 (L^2 density-increment). *Let $\kappa, \eta \in (0,1]$ be parameters. Suppose that $\mathcal{B}$, $\dot{\mathcal{B}}$ are Bourgain systems and $\mathcal{B}$ is regular, A is a subset of B of relative density α and X is a subset of $\dot{B}$ of relative density τ. Assume, also, that $\dot{\mathcal{B}} \leqslant_\rho \mathcal{B}$ with $\rho \leqslant c\kappa\alpha/d$ and write $f_A = 1_A - \alpha 1_B$. Then if*

$$\sum_{\mathrm{Spec}_\eta(\mu_X)} |\widehat{f_A}|^2 \geqslant \kappa\alpha^2 b,$$

there exists an m-controlled Bourgain system $\widetilde{\mathcal{B}}$ such that

$$\begin{aligned}\overline{\mathcal{B}} &= \dot{\mathcal{B}}_{c/\dot{d}^2 m} \wedge \widetilde{\mathcal{B}} \quad \text{is regular},\\ m &\leqslant C\eta^{-2}\ell(\tau),\\ \|1_A * \mu_{\overline{B}}\|_\infty &\geqslant (1+2^{-3}\kappa)\alpha.\end{aligned}$$

Proof. By Proposition 5.6, $\mathrm{Spec}_\eta(\mu_X)$ is $\frac{1}{2}$-annihilated by a regular Bourgain system of the form $\overline{\mathcal{B}} = \dot{\mathcal{B}}_{c\dot{d}^2/m} \wedge \widetilde{\mathcal{B}}$, where $\widetilde{\mathcal{B}} = \widetilde{\mathcal{B}}'_{1/2}$ and $\widetilde{\mathcal{B}}'$ is an m'-controlled Bourgain system with $m' \leqslant C\eta^{-2}\ell(\tau)$. Note that, by Lemma 4.6, $\widetilde{\mathcal{B}}$ is $O(m')$-controlled. Then applying Lemma 6.2 with $\Delta = \mathrm{Spec}_\eta(\mu_X)$ and $T = \overline{\mathcal{B}} \leqslant \dot{\mathcal{B}}$ concludes the proof. □

We now take a big step forward and claim that the following analogue of [21, Lemma 6.2] holds. This involves a careful examination of the argument of [21], and we regret imposing the double-checking process below on the reader. However, past this point, our argument is again self-contained.

PROPOSITION 6.4 (Iterative lemma on two scales). *Suppose that $\mathcal{B}$, $\mathcal{B}'$ are regular Bourgain systems, A is a subset of B of relative density α and A' is a subset of B' of relative density α'. Assume, also, that $\mathcal{B}' \leqslant_\rho \mathcal{B}$ with $\rho \leqslant c\alpha/d$. Then either:*

(i) *(many three-term arithmetic progressions)*

$$\langle 1_A * 1_{A'}, 1_{-A}\rangle_{L^2} \geqslant \exp[-C\alpha^{-1}\ell(\alpha') - Cd'\ell(\alpha'/d')]bb'; \text{ or}$$

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

(ii) *(density increment)*
there exists an m-controlled Bourgain system $\widetilde{\mathcal{B}}$ with

$$\overline{B} = \mathcal{B}'_{(\alpha\alpha'/2d')^C} \wedge \widetilde{\mathcal{B}} \quad \textit{regular},$$
$$m \leqslant C\alpha^{-1}\ell(\alpha)^3\ell(\alpha'),$$
$$\|1_A * \mu_{\overline{B}}\|_\infty \geqslant (1 + 2^{-13})\alpha.$$

Proof. This is obtained by replacing each occurrence of the energy-increment lemma [**21**, Lemma 3.8] for Bohr sets by its Bourgain system counterpart, viz. Proposition 6.3. Essentially, two types of L^2 density-increment appear in Sanders' argument, and we now describe them, using the notation of Proposition 6.3. In every application of [**21**, Lemma 3.8] the Bourgain system $\dot{\mathcal{B}}$ is (eventually) a dilate of the Bourgain system $\mathcal{B}$ by a factor $(\alpha\alpha'/2d')^{O(1)}$, and therefore we only need determine the parameters κ, η, τ.

The first type of L^2 density-increment appears in the proof of [**21**, Lemma 4.2, p. 626] with parameters $\kappa \asymp 1$, $\eta \asymp \alpha^{1/2}$, $\tau \gg \alpha'$, so that $m \leqslant C\alpha^{-1}\ell(\alpha')$ upon applying Proposition 6.3. The same density-increment is featured in [**21**, Proposition 4.1] which is just an iteration of the previous lemma.

A second type of density-increment arises in the proof of [**21**, Corollary 5.2, pp. 630–632] which involves certain densities σ and λ, and which features parameters $\kappa \asymp \lambda$, $\eta \asymp 1$,

$$\tau \geqslant \exp[-C\lambda^{-2}\ell(\sigma)\ell(\lambda\alpha)^2\ell(\alpha)] \quad \text{so that } m \leqslant C\lambda^{-2}\ell(\sigma)\ell(\lambda\alpha)^2\ell(\alpha)$$

upon applying Proposition 6.3. This is finally combined with [**21**, Proposition 4.1, p. 633] to obtain [**21**, Lemma 6.2], to the effect that we either have an L^2 density-increment of the first type, or of the second type with $\lambda \asymp 1$ and $\sigma \geqslant \exp[-C\alpha^{-1}\ell(\alpha')]$, and therefore such that $\kappa \asymp 1$ and $m \leqslant C\alpha^{-1}\ell(\alpha)^3\ell(\alpha')$ in the application of Proposition 6.3. Choosing $\mathcal{B}'' = \mathcal{B}'_{c\alpha'/d'}$ in (the Bourgain system version of) [**21**, Lemma 6.2] and using Lemma 4.6, we obtain an alternative case (i) of the desired shape.

Since, by Lemma 4.12, Bourgain systems satisfy the same regularity estimates as Bohr sets, we may replace the latter by the former and apply Proposition 6.3 everywhere as claimed, thereby obtaining the desired iterative lemma. Finally, the constant 2^{-13} may be extracted from [**21**] although its precise value is unimportant; it is just convenient to write down an explicit value for later computations. □

At this point, we recall a simple technique, originating in Bourgain's proof of Roth's theorem [**3**, (5.13)–(5.18)], which allows one to pass from two scales to one in iterative statements.

LEMMA 6.5. *Let $\theta \in (0, 1]$ be a parameter. Suppose that $\mathcal{B}$, $\mathcal{B}'$, $\mathcal{B}''$ are Bourgain systems, $\mathcal{B}$ is regular and A is a subset of B of relative density α.*

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

Assume, also, that $\mathcal{B}' \leqslant_\rho \mathcal{B}$ *and* $\mathcal{B}'' \leqslant_\rho \mathcal{B}$ *with* $\rho \leqslant c\theta\alpha/d$. *Then either*

$$\max(\|1_A * \mu_{B'}\|_\infty, \|1_A * \mu_{B''}\|_\infty) \geqslant \left(1 + \frac{\theta}{2}\right)\alpha$$

or there exists x *such that* $1_A * \mu_{B'}(x) \geqslant (1-\theta)\alpha$ *and* $1_A * \mu_{B''}(x) \geqslant (1-\theta)\alpha$.

Proof. A quick regularity computation via Lemma 4.12 yields

$$\begin{aligned}\mathbb{E}_B(1_A * \mu_{B'} + 1_A * \mu_{B''}) &= \langle 1_A, \mu_B * \mu_{B'}\rangle + \langle 1_A, \mu_B * \mu_{B''}\rangle \\ &= 2\alpha + O(\rho d) \\ &\geqslant \left(2 - \frac{\theta}{2}\right)\alpha\end{aligned}$$

provided that $\rho \leqslant c\theta\alpha/d$. By the pigeonhole principle, there exists $x \in G$ such that

$$1_A * \mu_{B'}(x) + 1_A * \mu_{B''}(x) \geqslant \left(2 - \frac{\theta}{2}\right)\alpha.$$

Assuming that we are not in the first case of the lemma,

$$1_A * \mu_{B'}(x) \geqslant \left(2 - \frac{\theta}{2}\right)\alpha - \left(1 + \frac{\theta}{2}\right)\alpha = (1-\theta)\alpha$$

and, similarly, for $1_A * \mu_{B''}(x)$. □

With this technique in hand, we may modify Proposition 6.4 so as to make the iteration easier to perform. Once this is done, Proposition 6.1 is derived by a standard, yet computationally intensive iterative process. For this argument to work, however, we need to make the assumption that the set A contains no degenerate arithmetic progressions at each step of the iteration.

PROPOSITION 6.6 (Final iterative lemma). *Suppose that* G *has odd order,* $\mathcal{B}$ *is a regular Bourgain system, and* A *is a subset of* B *of relative density* α *such that* $A - A$ *contains no element of order two. Then either:*

(i) *(many three-term arithmetic progressions)*

$$\langle 1_A * 1_A, 1_{2\cdot A}\rangle_{L^2} \geqslant \exp[-C\alpha^{-1}\ell(\alpha) - Cd\ell(\alpha/d)] \cdot b^2; \text{ or}$$

(ii) *(density increment)*
there exist Bourgain systems $\widehat{\mathcal{B}}$, $\widetilde{\mathcal{B}}$ *and an element* $u \in \{1, -2\}$ *such that*

$$\begin{aligned}&\overline{\mathcal{B}} = \widehat{\mathcal{B}} \wedge \widetilde{\mathcal{B}} \quad \text{is regular},\\ &\widehat{\mathcal{B}} = u \cdot \mathcal{B}_{(\alpha/2d)^C}, \qquad \widehat{b} \geqslant \exp[-Cd\ell(\alpha/d)] \cdot b,\\ &\widetilde{d} \leqslant C\alpha^{-1}\ell(\alpha)^4, \qquad \widetilde{b} \geqslant \exp[-C\alpha^{-1}\ell(\alpha)^5],\\ &\|1_A * \mu_{\overline{B}}\|_\infty \geqslant (1 + 2^{-16})\alpha.\end{aligned}$$

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

Proof. Let $\theta = 2^{-15}$ and define regular Bourgain systems $\mathcal{B}' = \mathcal{B}_{c\alpha/d}$ and $\mathcal{B}'' = \mathcal{B}'_{c'\alpha/d}$, with the help of Lemma 4.11. Now apply Lemma 6.5 to A and $\mathcal{B}, \mathcal{B}', \mathcal{B}''$: in the first case of that lemma, we are in the second case of the proposition, while in the second case we may find an element x such that $A' := (A - x) \cap B'$ has relative density $\alpha' \geqslant (1 - 2^{-15})\alpha$ in B', and $A'' := (A - x) \cap B''$ has relative density at least $\frac{1}{2}\alpha$ in B''; the latter weak bound suffices for our purposes.

We let $\widehat{A}'' = -2 \cdot A''$ and $\widehat{\mathcal{B}}'' = -2 \cdot \mathcal{B}''$, so that, from the injectivity of $y \mapsto 2 \cdot y$ on A'' and the bound $|\widehat{B}''| \leqslant |B''|$, we deduce that $\widehat{A}''$ has density at least $\frac{1}{2}\alpha$ in $\widehat{B}''$. Furthermore, by Lemma 4.9, we see that $\widehat{\mathcal{B}}''$ is a Bourgain system of dimension at most d'' and, since $\widehat{B}''$ contains $\widehat{A}''$, of density at least $\frac{1}{2}\alpha b''$. Observe, finally, that with these choices of A' and $\widehat{A}''$,

$$\langle 1_A * 1_A, 1_{2\cdot A}\rangle_{L^2} = \langle 1_{A-x} * 1_{2x-2\cdot A}, 1_{x-A}\rangle_{L^2} \geqslant \langle 1_{A'} * 1_{\widehat{A}''}, 1_{-A'}\rangle_{L^2}. \quad (6.1)$$

We now apply Proposition 6.4 to the sets A' and $\widehat{A}''$, located, respectively, in B' and $\widehat{B}''$. In the first case of that proposition, it follows from equation (6.1) and Lemma 4.6 that we are in the first case of the proposition that we seek to prove. In the second case of Proposition 6.4, we obtain a regular Bourgain system $\overline{\mathcal{B}} = \widehat{\mathcal{B}} \wedge \widetilde{\mathcal{B}}$, where

$$\widehat{\mathcal{B}} = (-2 \cdot \mathcal{B}'')_{(\alpha/2d)^C} = -2 \cdot \mathcal{B}''_{(\alpha/2d)^C} = -2 \cdot \mathcal{B}_{(\alpha/2d)^{C'}}$$

and $\widetilde{\mathcal{B}}$ is $C\alpha^{-1}\ell(\alpha)^4$-controlled, and such that

$$\|1_A * \mu_{\overline{B}}\|_\infty \geqslant \|1_{A'} * \mu_{\overline{B}}\|_\infty \geqslant (1 + 2^{-13})\alpha' \geqslant (1 + 2^{-14})\alpha.$$

Applying Lemma 4.6 to $\widehat{\mathcal{B}} = \widehat{\mathcal{B}}''_{(\alpha/2d)^C}$, recalling that $\widehat{b}'' \geqslant \frac{1}{2}\alpha b''$ and via Definition 5.5, we conclude that we are in the second case of the proposition that we intend to prove. □

Proof of Proposition 6.1. We construct, iteratively, sequences of subsets A_i of regular Bourgain systems $\mathcal{B}^{(i)}$ of density α_i, such that A_i is contained in a translate of A. Since $A_i - A_i$ is a subset $A - A$, it does not contain any element of order two either. We initiate the iteration with $A_1 = A$ and $\mathcal{B}^{(1)} = \mathcal{B}$.

At each step, we apply Proposition 6.6 to the set A_i and, in the first case of that proposition, we stop the iteration, while, in the second case, we let $\mathcal{B}^{(i+1)} = \overline{\mathcal{B}}^{(i)}$ (with the notation from the proposition) and we pick x_i and $A_{i+1} = (A_i - x_i) \cap \overline{B}^{(i)}$ so that A_{i+1} has relative density $\alpha_{i+1} = \|1_{A_i} * \mu_{\overline{B}^{(i)}}\|_\infty$ in $\overline{B}^{(i)}$.

Since $\alpha_{i+1} \geqslant (1 + c)\alpha_i$ whenever A_{i+1} is defined, the iteration proceeds for a number of steps bounded by $C\ell(\alpha)$. At each step, we obtain Bourgain systems $\widehat{\mathcal{B}}^{(i)}$ and $\widetilde{\mathcal{B}}^{(i)}$ and an element $u_i \in \{1, -2\}$ such that

$$\mathcal{B}^{(i+1)} = \widehat{\mathcal{B}}^{(i)} \wedge \widetilde{\mathcal{B}}^{(i)} \quad \text{is regular}, \quad (6.2)$$

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

and, since $\alpha_i \geqslant \alpha$, such that

$$\widehat{\mathcal{B}}^{(i)} = u_i \cdot \mathcal{B}^{(i)}_{(\alpha_i/2d_i)^C}, \qquad \widehat{b}_i \geqslant \exp[-Cd_i\ell(\alpha/d_i)] \cdot b_i, \tag{6.3}$$

$$\widetilde{d}_i \leqslant C\alpha^{-1}\ell(\alpha)^4, \qquad \widetilde{b}_i \geqslant \exp[-C\alpha^{-1}\ell(\alpha)^5]. \tag{6.4}$$

Iterating $i-1$ times equation (6.2) and equation (6.3), we obtain a Bourgain system of the form

$$\mathcal{B}^{(i)} = \widetilde{\mathcal{B}}^{(i-1)} \wedge u_{i-1} \cdot (\dots u_2 \cdot (\widetilde{\mathcal{B}}^{(1)}_* \wedge u_1 \cdot \widetilde{\mathcal{B}}_*) \dots),$$

where the stars stand for certain dilations. This is not exactly an intersection of Bourgain systems, but the argument used in the proof of Lemma 4.8 is easily adapted to show that $\mathcal{B}^{(i)}$ has dimension at most

$$d_i \leqslant 2(d + \widetilde{d}_1 + \dots + \widetilde{d}_{i-1}).$$

By equation (6.4) and since $i \leqslant C\ell(\alpha)$, this yields $d_i \leqslant 2d + C\alpha^{-1}\ell(\alpha)^5$.

Applying Lemma 4.8 to the intersection (6.2), and with (6.3) and (6.4), we also obtain

$$\begin{aligned} b_{i+1} &\geqslant 4^{-(\widehat{d}_i+\widetilde{d}_i)} \cdot \widehat{b}_i \cdot \widetilde{b}_i \\ &\geqslant \exp[-C(\alpha^{-1}+d)\ell(\alpha)^5\ell(\alpha/d)] \cdot b_i. \end{aligned}$$

Iterating this at most $C\ell(\alpha)$ times, we obtain

$$b_i \geqslant \exp[-C(\alpha^{-1}+d)\ell(\alpha)^6\ell(\alpha/d)] \cdot b.$$

When the algorithm stops, we therefore have

$$\langle 1_{A_i} * 1_{A_i}, 1_{2\cdot A_i}\rangle_{L^2} \geqslant \exp[-C\alpha^{-1}\ell(\alpha) - Cd_i\ell(\alpha/d_i)] \cdot b_i^2.$$

Inserting the bounds on d_i and b_i in the above, and recalling that A_i is contained in a translate of A, this concludes the proof. □

§7. *From small doubling to three-term arithmetic progressions.* This section is concerned with the proof of Theorem 1.3 and the related Corollary 1.6. As mentioned before, an extremely important tool for us is the recent correlation-based Bogolyubov–Ruzsa lemma of Sanders [**23**]. In our situation, it serves to pass from a set of small doubling to one with high density in a coset progression, which is a particular type of Bourgain system. The local Sanders–Roth theorem of the previous section may then be applied to this new set, to show that it contains a non-trivial three-term arithmetic progression; this is the main observation of this paper. We now quote the main result of [**23**], with a minor tweak to ensure regularity.

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

PROPOSITION 7.1 (Correlation Bogolyubov–Ruzsa lemma [23]). *Let $K \geqslant 1$ be a parameter, and suppose that A is a subset of G such that $|A+A| \leqslant K|A|$. Then there exists a d-dimensional coset progression M inducing a regular Bourgain system and such that*

$$\begin{aligned} \|1_A * \mu_M\|_\infty &\geqslant \frac{1}{2K}, \\ d &\leqslant C(\log K)^6, \\ |M| &\geqslant \exp[-C(\log K)^6(\log\log K)] \cdot |A|. \end{aligned}$$

Proof. Without the regularity condition, this is [23, Theorem 10.1] with $A = S$ and $\varepsilon = \frac{1}{2}$. To obtain regularity, one may simply follow the proof in [23], stopping just before the application of [23, Lemma 10.2], and dilating by a certain constant factor the coset progression M obtained at this point. By Lemmas 4.6 and 4.11, one may choose this constant so that the dilated induced Bourgain system is regular, while losing at most a factor $e^{-C(\log K)^6}$ in size. The rest of the proof goes unchanged. □

It is crucial for our argument that this statement makes no assumption of density on the set A, whereas the earlier Bogolyubov–Chang-type lemma [19, Proposition 6.1] used by Sanders does. In terms of bounds, we could also allow for $d \leqslant K^{1+o(1)}$ and $|M| \geqslant e^{-CK^{1+o(1)}}|A|$ in Proposition 7.1, without affecting the quality of bounds in Theorem 1.3; however we do not know of any argument significantly simpler than that of [23] to obtain such estimates.

We now present the proof of Theorem 1.3, following the usual approach of estimating the total number of three-term arithmetic progressions, only to compare it later to the number of trivial ones. Corollary 1.6 then follows by inserting the bound of Theorem 1.3 into the argument of [19].

PROPOSITION 7.2. *Let $K \geqslant 1$ be a parameter. Suppose that A is a subset of G such that $|A+A| \leqslant K|A|$ and $A-A$ contains no element of order two. Then*

$$\langle 1_A * 1_A, 1_{2\cdot A}\rangle_{L^2} \geqslant \exp[-CK(\log K)^7] \cdot \mu_G(A)^2.$$

Proof. Let M be the coset progression given by Proposition 7.1, and write $\mathcal{M}$ for its induced regular Bourgain system. By the correlation conclusion, we may pick an element x such that $A' = (A-x) \cap M$ has relative density $1/2K$ in M. Then applying Proposition 6.1 to A' and $\mathcal{M}$, we obtain

$$\begin{aligned} \langle 1_A * 1_A, 1_{2\cdot A}\rangle_{L^2} &\geqslant \langle 1_{A'} * 1_{A'}, 1_{2\cdot A'}\rangle_{L^2} \\ &\geqslant \exp[-C(K+d)(\log K)^6(\log Kd)] \cdot \mu_G(M)^2. \end{aligned}$$

This yields the desired estimate upon inserting the bounds from Proposition 7.1. □

Proof of Theorem 1.3. Write $K = |A+A|/|A|$. If $A-A$ contains an element $x-y$ of order two, we readily find a non-trivial, degenerate arithmetic

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

progression (x, y, x) in A. Otherwise, Proposition 7.2 tells us that A possesses at least $e^{-CK(\log K)^7}|A|^2$ three-term arithmetic progressions, while the number of trivial ones is at most $|A|$. By the assumption on K, we are then ensured to find at least one non-trivial arithmetic progression in A. □

Proof of Corollary 1.6. It suffices to insert the bounds of Theorem 1.3 into the proof of [19, Theorem 1.5, pp. 230–231]. □

§8. *From small doubling to long arithmetic progressions.* In this section, we derive Theorem 1.5, basing our method on the approach of Croot *et al* [4], which divides roughly into three steps. In the first step, one produces a large, structured set of almost-periods of the convolution of the set A under consideration with itself. The second step is to show, by a packing argument, that the set $A + A$ necessarily contains a translated copy of any subset of this set of almost-periods of a certain size. The third step is to pick such a subset with basic additive structure, such as an arithmetic progression.

The original argument of [4] is based on Ruzsa's modelling lemma [17], which has no efficient equivalent for general abelian groups, and therefore we need to use again a modelling approach based on the Bogolyubov–Ruzsa lemma of Sanders. In contrast with the previous section, however, we now need a version of this lemma that provides us with a containment conclusion, and for this we quote [23, Theorem 1.1].

PROPOSITION 8.1 (Containment Bogolyubov–Ruzsa lemma [23]). *Let $K \geqslant 1$ be a parameter, and suppose that A is a subset of G such that $|A+A| \leqslant K|A|$. Then there exists a d-dimensional coset progression M contained in $2A - 2A$ and such that*

$$d \leqslant C(\log K)^6 \quad \text{and} \quad |M| \geqslant \exp[-C(\log K)^6(\log\log K)] \cdot |A|.$$

As noted in [23, §3], this version can be deduced from Proposition 7.1. The containment conclusion is sufficient in our situation, because the Croot–Sisask lemma works under a doubling hypothesis, whereas the iterative argument used in the proof of Roth's theorem requires an assumption of density instead. Our reason for emphasizing this point is that the containment version above is easier to obtain than the correlation one, and is explained in depth in a survey by Sanders [24]. Although the type of structure obtained there is different, consisting of a convex coset progression instead, this would not affect our argument much since this object is also a Bourgain system, as can be seen from [24, §4].

We now proceed to the proof, starting with the following lemma which serves to collect together certain computations from [4] on L^p and $L^{p/2}$ norms of convolutions.

LEMMA 8.2. *Let $p \geqslant 2$ and $K \geqslant 1$ be parameters. Suppose that A is a subset of G such that $|A + A| \leqslant K|A|$. Then*

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

$$\mu_G(A+A)^{1/p} \leqslant K^{1/2}\|1_A * \mu_A\|_{p/2}^{1/2}$$

and

$$\|1_A * \mu_A\|_{p/2}^{1/2} \leqslant K^{1/2}\|1_A * \mu_A\|_p.$$

Proof. By Hölder's inequality,

$$\mu_G(A) = \mathbb{E}_G 1_A * \mu_A \leqslant \mu_G(A+A)^{1-2/p}\|1_A * \mu_A\|_{p/2},$$

from which the first estimate follows upon rearranging and taking square roots. To obtain the second, apply Cauchy–Schwarz and the first estimate in

$$\begin{aligned}[\mathbb{E}_G (1_A * \mu_A)^{p/2}]^2 &\leqslant \mu_G(A+A)\|1_A * \mu_A\|_p^p \\ &\leqslant K^{p/2}\|1_A * \mu_A\|_{p/2}^{p/2}\|1_A * \mu_A\|_p^p.\end{aligned}$$

The result follows upon taking pth roots, then dividing both sides by $\|1_A * \mu_A\|_{p/2}^{1/2}$. □

An important tool from [4] is a version of the Croot–Sisask lemma [5] that serves to smooth the convolution of two sets by an iterated convolution factor. The precise statement we need is a standard consequence of [4, Theorem 6.1]; an exposition of it by the author may be found in [12, §7].

LEMMA 8.3 (Croot–Sisask L^p-smoothing). *Let $K, L \geqslant 1$, $\theta \in (0, K^{-1/2}]$, $p \in 2\mathbb{N}$, $\ell \in \mathbb{N}$ be parameters. Suppose that A, S, T are subsets of G such that $|A+S| \leqslant K|A|$ and $|S+T| \leqslant L|S|$. Then there exists a subset X of T of size $|X| \geqslant (2L)^{-Cp\ell^2/\theta^2}|T|$ such that*

$$\|1_A * \mu_S - 1_A * \mu_S * \lambda_X^{(\ell)}\|_p \leqslant \theta\|1_A * \mu_S\|_{p/2}^{1/2},$$

where $\lambda_X = \mu_X * \mu_{-X}$.

As anticipated, our first step is to produce a set of almost-periods of the convolution of a small doubling set with itself. Following [4], this is done by first smoothing this convolution by the iterated convolution of a certain set X, with the difference that this set is now localized to a Bourgain system, which is taken to be a coset progression later on. Via the Fourier transform, any set annihilating the large spectrum of X induces a set of almost-periods of the smoothed convolution and, via the results of §5, we may choose this annihilator to be a large Bourgain system. Here we make a small comment on notation: throughout this section, $a \sim b$ stands for $b/2 \leqslant a \leqslant 2b$.

PROPOSITION 8.4. *Let $K \geqslant 1$ and $p \in 2\mathbb{N}$ be parameters. Suppose that $\mathcal{B}$ is a regular Bourgain system and A is a subset of G such that $|A+A| \leqslant K|A|$ and $B \subset 2A - 2A$. Then there exist $m \geqslant 1$ and Bourgain systems $\overline{\mathcal{B}}, \widetilde{\mathcal{B}}$ such that $\widetilde{\mathcal{B}}$ is m-controlled and*

$$\begin{aligned}\overline{\mathcal{B}} &= \mathcal{B}_{c/(Kd^2m)} \wedge \widetilde{\mathcal{B}}_{c/K}, \\ m &\leqslant CpK(\log K)^3,\end{aligned}$$

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

and for every $x \in \overline{B}$,

$$\|1_A * \mu_A - \tau_x 1_A * \mu_A\|_p \leqslant \tfrac{1}{2}\|1_A * \mu_A\|_p.$$

Proof. First observe that, by the Plünnecke–Ruzsa–Petridis inequality [**15**],

$$|A + B| \leqslant |3A - 2A| \leqslant K^5|A|,$$

and therefore we may apply Lemma 8.3 with $(S, T) = (A, B)$ and $L = K^5$, for parameters θ and ℓ to be determined later. This yields a subset X of B of relative density τ such that

$$\tau \geqslant \exp[-Cp\ell^2\theta^{-2}\log K], \tag{8.1}$$

$$\|1_A * \mu_A - 1_A * \mu_A * \lambda_X^{(\ell)}\|_p \leqslant \theta\|1_A * \mu_A\|_{p/2}^{1/2}. \tag{8.2}$$

We write I for the identity operator on functions and, given $x \in G$, we define the function $\widehat{x} : \widehat{G} \to G$, which maps γ to $\gamma(x)$. Consider now an arbitrary element x of G. Then, by the triangle inequality and equation (8.2),

$$\begin{aligned}
&\|(I - \tau_x)1_A * \mu_A\|_p \\
&\quad\leqslant \|(I - \tau_x)(1_A * \mu_A - 1_A * \mu_A * \lambda_X^{(\ell)})\|_p \\
&\qquad + \|1_{(A+A)\cup(A+A-x)} \cdot (I - \tau_x)1_A * \mu_A * \lambda_X^{(\ell)}\|_p \\
&\quad\leqslant 2\theta\|1_A * \mu_A\|_{p/2}^{1/2} + 2\mu_G(A + A)^{1/p}\|(I - \tau_x)1_A * \mu_A * \lambda_X^{(\ell)}\|_\infty.
\end{aligned}$$

Also, by Parseval,

$$\begin{aligned}
\|(I - \tau_x)1_A * \mu_A\|_p &\leqslant 2\theta\|1_A * \mu_A\|_{p/2}^{1/2} \\
&\quad + 2\mu_G(A + A)^{1/p}\sum_{\widehat{G}} |\widehat{1}_A||\widehat{\mu}_A||\widehat{\mu}_X|^{2\ell}|1 - \widehat{x}|.
\end{aligned} \tag{8.3}$$

Now, invoking Proposition 5.6 with a parameter $\nu \in (0, 1]$, and recalling equation (8.1), we infer that $\mathrm{Spec}_{1/2}(\mu_X)$ is ν-annihilated by $\overline{\mathcal{B}} = \mathcal{B}_{c\nu/d^2m} \wedge \widetilde{\mathcal{B}}_\nu$, where $\widetilde{\mathcal{B}}$ is an m-controlled Bourgain system with $m \leqslant Cp\ell^2\theta^{-2}\log K$. From now on we restrict to $x \in \overline{B}$, so that, by considering separately the summation over $\mathrm{Spec}_{1/2}(\mu_X)$ in equation (8.3), we obtain

$$\begin{aligned}
\|(I - \tau_x)1_A * \mu_A\|_p &\leqslant 2\theta\,\|1_A * \mu_A\|_{p/2}^{1/2} \\
&\quad + 2(\nu + 2^{1-2\ell})\,\mu_G(A + A)^{1/p}\sum_{\widehat{G}} |\widehat{1}_A||\widehat{\mu}_A|.
\end{aligned}$$

By Parseval, we know that $\sum_{\widehat{G}} |\widehat{1}_A||\widehat{\mu}_A| = 1$. Finally, by applying Lemma 8.2, we obtain

$$\begin{aligned}
\|(I - \tau_x)1_A * \mu_A\|_p &\leqslant (2\theta + 2\nu K^{1/2} + 2^{2-2\ell}K^{1/2})\|1_A * \mu_A\|_{p/2}^{1/2} \\
&\leqslant (2\theta + 2\nu K^{1/2} + 2^{2-2\ell}K^{1/2})K^{1/2}\|1_A * \mu_A\|_p.
\end{aligned}$$

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

Choosing $\theta = K^{-1/2}/8$, $\nu = K^{-1}/16$ and $\ell \sim C \log K$, we obtain the desired L^p-estimate, and the bound on m follows by inserting the value of these parameters. □

Secondly, we need the following packing argument which may be extracted from the computations of [4], but we include the proof for completeness. In practice, we specialize f below to $1_A * \mu_A$, which has $A + A$ as support.

LEMMA 8.5. *Let $p \geqslant 2$ be a parameter. Suppose that $f : G \to \mathbb{C}$ and $R \subset G$ are such that, for all $t \in R$,*

$$\|(I - \tau_t) f\|_p \leqslant \tfrac{1}{2}\|f\|_p.$$

Then, for every subset T of R of size $|T| < 2^p$, there exists a translate $x \in G$ such that $x + T \subset \mathrm{Supp}(f)$.

Proof. Given a subset T of R, consider the quantity

$$I := \sum_{t \in T} \|f - \tau_t f\|_p^p,$$

so that, by the assumptions of the lemma, we have at once $I \leqslant |T| \cdot 2^{-p}\|f\|_p^p$.

Now assume, for contradiction, that, for every $x \in G$, the translate $x + T$ is not contained in $\mathrm{Supp}(f)$; then for every $x \in G$ we may find an element $t \in T$ such that $f(x + t) = 0$. Exchanging summations, this yields the lower bound

$$I = \mathbb{E}_G \sum_{t \in T} |f - \tau_t f|^p \geqslant \mathbb{E}_G |f|^p.$$

Combining both bounds on I, we obtain

$$\|f\|_p^p \leqslant |T| 2^{-p} \|f\|_p^p.$$

We obtain a contradiction if $|T| < 2^p$, and therefore,in that case, we find a translated copy of T in the support of f. □

Last, we need an analogue for Bourgain systems in abelian groups of the well-known fact, used in [4], that Bohr sets of $\mathbb{Z}_N$ of radius δ and dimension d contain arithmetic progressions of length $\delta N^{1/d}$.

LEMMA 8.6. *Suppose that $\mathcal{B}$ is a Bourgain system of dimension d and $h \geqslant d$, and assume that $|B| \geqslant 2^{6h}$. Then there exists a subset T of B, which is either a proper arithmetic progression or a subgroup, of size $\frac{1}{4}|B|^{1/4h} \leqslant |T| \leqslant |B|^{1/2h}$.*

Proof. Let $\eta = 2|B|^{-1/2h} \in (0, 2^{-2}]$ so that, by Lemma 4.6,

$$|B_\eta| \geqslant \exp\left[\log|B| - d \log \frac{2}{\eta}\right] \geqslant |B|^{1/2}.$$

Let $N = \lfloor \eta^{-1/2} \rfloor$, so that we have a sumset containment

$$N^2 B_\eta \subset B_{N^2\eta} \subset B. \tag{8.4}$$

Since $\eta^{-1/2} \geqslant 2$, we have also $\frac{1}{2}\eta^{-1/2} \leqslant N \leqslant \eta^{-1/2}$.

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

We are now in one of two cases. In the first, there exists an element x in B_η of order N, and thus the arithmetic progression $T = [0, N-1]_{\mathbb{Z}} \cdot x$ is proper and, by (8.4), contained in B. Since $|T| = N$, we have also $\frac{1}{4}|B|^{1/4h} \leqslant |T| \leqslant |B|^{1/4h}$.

In the second case, every element of B_η has order at most N. Since $|B_\eta| \geqslant |B|^{1/2} \geqslant N$, we may pick $N-1$ distinct non-zero elements $x_1, \dots, x_{N-1} \in B_\eta$ and consider the subgroup T they generate, namely,

$$T = \langle x_1, \dots, x_{N-1} \rangle_{\mathbb{Z}} = [0, N-1]_{\mathbb{Z}} \cdot x_1 + \cdots + [0, N-1]_{\mathbb{Z}} \cdot x_{N-1}.$$

By equation (8.4), it follows again that T is contained in B, and the size of T satisfies

$$\tfrac{1}{4}|B|^{1/4h} \leqslant N \leqslant |T| \leqslant N^2 \leqslant |B|^{1/2h}. \qquad \square$$

We are now ready to combine the previous propositions into a proof of Theorem 1.5.

Proof of Theorem 1.5. By Proposition 8.1, we may find a d-dimensional coset progression $M \subset 2A - 2A$ such that

$$d \leqslant (\log K)^{O(1)} \quad \text{and} \quad |M| \geqslant \exp[-(\log K)^{O(1)}] \cdot |A|. \tag{8.5}$$

Up to dilating M by a constant factor, which preserves the above bounds by Lemma 4.6, we may assume, via Lemma 4.11, that M induces a regular Bourgain system $\mathcal{M}$. By Lemma 4.5, that system also satisfies the dimension bound equation (8.5).

Applying now Proposition 8.4 with $\mathcal{B} = \mathcal{M}$ and a parameter $p \in 2\mathbb{N}$ to be determined later, we obtain Bourgain systems $\overline{\mathcal{B}}$, $\widetilde{\mathcal{B}}$ such that

$$\overline{\mathcal{B}} = \mathcal{M}_{(1/2dpK)^{O(1)}} \wedge \widetilde{\mathcal{B}}_{c/K}, \tag{8.6}$$

$$\widetilde{d} \leqslant CpK(\log K)^3, \tag{8.7}$$

$$\widetilde{b} \geqslant \exp[-CpK(\log pK)(\log K)^3], \tag{8.8}$$

where we have unfolded Definition 5.5, and such that

$$\|(I - \tau_x)1_A * \mu_A\| \leqslant \tfrac{1}{2}\|1_A * \mu_A\|_p \quad \text{for all } x \in \overline{B}. \tag{8.9}$$

Applying Lemma 4.8 to the intersection (8.6), and considering (8.5) and (8.7), we obtain

$$\overline{d} \ll (\log K)^{O(1)} + pK(\log K)^3 \ll pK(\log K)^3$$

and we let $h = CpK(\log K)^3 \geqslant \overline{d}$. By Lemmas 4.6 and 4.8, we also obtain

$$\mu_G(\overline{B}) \geqslant \exp[-Cd(\log dpK)]\mu_G(M) \cdot \exp[-C\widetilde{d}\log K]\widetilde{b}$$

and therefore, by (8.5), (8.7) and (8.8),

$$|\overline{B}| \geqslant \exp[-CpK(\log pK)(\log K)^3] \cdot |A|.$$

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

Both the conditions $|\overline{B}| \geqslant |A|^{1/2}$ and $|\overline{B}| \geqslant 2^{6h}$ are satisfied provided

$$pK(\log pK)(\log K)^3 \leqslant c \log |A|. \tag{8.10}$$

Considering that $\overline{B} \subset M \subset 2A - 2A$, we thus have a rough estimate $|A|^{1/2} \leqslant |\overline{B}| \leqslant |A|^4$. By Lemma 8.6, we may therefore find a subset T of $\overline{B}$, which is either a proper arithmetic progression or a subgroup, of size bounded by

$$\tfrac{1}{4}|A|^{1/8h} \leqslant \tfrac{1}{4}|\overline{B}|^{1/4h} \leqslant |T| \leqslant |\overline{B}|^{1/2h} \leqslant |A|^{2/h}.$$

Recalling our choice $h = CpK(\log K)^3$ and (8.10), this shows that

$$|T| = \exp\left[\Theta\left(\frac{\log |A|}{pK(\log K)^3}\right)\right].$$

The condition $|T| < 2^p$ is therefore satisfied if we choose

$$p \sim C\left(\frac{\log |A|}{K(\log K)^3}\right)^{1/2}.$$

It remains to check the conditions $p \geqslant 2$ and (8.10); these are seen to be satisfied for

$$K \leqslant \frac{c \log |A|}{(\log \log |A|)^5}$$

after a tedious, yet elementary, computation. This yields the final size estimate

$$|T| = \exp\left[\Theta\left(\frac{\log |A|}{K(\log K)^3}\right)^{1/2}\right]$$

and, since we verified the conditions $|T| < 2^p$ and (8.9), an application of Lemma 8.5 with $f = 1_A * \mu_A$ and $R = \overline{B}$ concludes the proof. □

§9. *Remarks.* In this last section we explain how Theorem 1.1 follows from the results of the literature, as alluded to in the introduction. Consider a set of integers A of doubling K, then, for the purpose of finding arithmetic progressions in A, we may instead assume that A is a subset of a cyclic group of odd order of density $\gg K^{-4}$ and doubling K, via a partial Freiman isomorphy [**17**]. Applying [**19**, Proposition 6.1] to A, one obtains a regular Bohr set of dimension $d \ll K \log K$ and density $b \geqslant \exp[-CK(\log K)^2]$, on which a certain translate of A has density $\gg K^{-1}$. In that setting, Proposition 6.1 of this paper is just [**21**, Theorem 1.1], with the iterative argument from there initialized on a Bohr set instead of the whole group; there is no need to consider Bourgain systems or 2-torsion. Proposition 6.1, thus specialized, shows that A contains at least $\exp[-CK(\log K)^8] \cdot |A|^2$ three-term arithmetic progressions, and therefore at least one non-trivial progression for $K = |A + A|/|A|$ in the range specified by Theorem 1.1.

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press

Acknowledgements. This research was supported by a *contrat doctoral* from Université Paris 7 and by the ANR Caesar ANR-12-BS01-0011.

References

1. M. Bateman and N. H. Katz, New bounds on cap sets. *J. Amer. Math. Soc.* **25**(2) (2012), 585–613.
2. J. Bourgain, On arithmetic progressions in sums of sets of integers. In *A Tribute to Paul Erdős*, Cambridge University Press (Cambridge, 1990), 105–109.
3. J. Bourgain, On triples in arithmetic progression. *Geom. Funct. Anal.* **9**(5) (1999), 968–984.
4. E. Croot, I. Łaba and O. Sisask, Arithmetic progressions in sumsets and L^p-almost-periodicity. *Combin. Probab. Comput.* **22**(3) (2013), 351–365.
5. E. Croot and O. Sisask, A probabilistic technique for finding almost-periods of convolutions. *Geom. Funct. Anal.* **20**(6) (2010), 1367–1396.
6. B. Green, Arithmetic progressions in sumsets. *Geom. Funct. Anal.* **12**(3) (2002), 584–597.
7. B. Green and I. Z. Ruzsa, Freiman's theorem in an arbitrary abelian group. *J. Lond. Math. Soc.* (2) **75**(1) (2007), 163–175.
8. B. Green and T. Sanders, A quantitative version of the idempotent theorem in harmonic analysis. *Ann. of Math.* (2) **168**(3) (2008), 1025–1054.
9. H. Hatami, Fourier analysis of finite abelian groups. In *Lecture Notes*, 2011, http://cs.mcgill.ca/~hatami/comp760-2011/.
10. N. Hegyvári, F. Hennecart and A. Plagne, A proof of two Erdős' conjectures on restricted addition and further results. *J. Reine Angew. Math.* **560** (2003), 199–220.
11. K. Henriot, Bourgain's bounds for Roth's theorem. In *Expository Note*, 2013, http://www.math.ubc.ca/~khenriot/notes/bourgainroth.pdf.
12. K. Henriot, Notes on the Croot–Sisask lemma. In *Expository Note*, 2013, http://www.math.ubc.ca/~khenriot/notes/almostp.pdf.
13. V. F. Lev, Progression-free sets in finite abelian groups. *J. Number Theory* **104**(1) (2004), 162–169.
14. N. Lyall, Behrend's example. In *Expository Note*, 2005.
15. G. Petridis, New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica* **32**(6) (2012), 721–733.
16. K. F. Roth, On certain sets of integers. *J. Lond. Math. Soc.* **28**(1) (1953), 104–109.
17. I. Z. Ruzsa, Arithmetical progressions and the number of sums. *Period. Math. Hungar.* **25**(1) (1992), 105–111.
18. T. Sanders, Roth's theorem in $\mathbb{Z}_4^n$. *Anal. PDE* **2**(2) (2009), 211–234.
19. T. Sanders, Three-term arithmetic progressions and sumsets. *Proc. Edinb. Math. Soc.* (2) **52**(1) (2009), 211–233.
20. T. Sanders, Green's sumset problem at density one half. *Acta Arith.* **146**(1) (2011), 91–101.
21. T. Sanders, On Roth's theorem on progressions. *Ann. of Math.* (2) **174**(1) (2011), 619–636.
22. T. Sanders, On certain other sets of integers. *J. Anal. Math.* **116**(1) (2012), 53–82.
23. T. Sanders, On the Bogolyubov–Ruzsa lemma. *Anal. PDE* **5**(3) (2012), 627–655.
24. T. Sanders, The structure theory of set addition revisited. *Bull. Amer. Math. Soc. (N.S.)* **50**(1) (2013), 93–127.
25. T. Schoen, The cardinality of restricted sumsets. *J. Number Theory* **96**(1) (2002), 48–54.
26. J. Solymosi, Arithmetic progressions in sets with small sumsets. *Combin. Probab. Comput.* **15**(4) (2006), 597–603.
27. Y. V. Stanchescu, Planar sets containing no three collinear points and non-averaging sets of integers. *Discrete Math.* **256**(1–2) (2002), 387–395.
28. T. Tao and V. H. Vu, *Additive Combinatorics* (*Cambridge Studies in Advanced Mathematics* **105**), Cambridge University Press (Cambridge, 2010).

Kevin Henriot,
Department of Mathematics,
University of British Columbia,
Room 121,
1984 Mathematics Road,
Vancouver BC V6T 1Z2,
Canada
E-mail: khenriot@math.ubc.ca

https://doi.org/10.1112/S002557931500039X Published online by Cambridge University Press