ISRAEL JOURNAL OF MATHEMATICS xxx (2014), 1–22
DOI: 10.1007/s11856_000000000000000

ROTH'S THEOREM IN MANY VARIABLES

BY

Tomasz Schoen*

Faculty of Mathematics and Computer Science
Adam Mickiewicz University, Umultowska 87, 61-614 Poznań, Poland
e-mail: schoen@amu.edu.pl

AND

Ilya D. Shkredov**

Division of Algebra and Number Theory, Steklov Mathematical Institute
ul. Gubkina, 8, Moscow, Russia, 119991
and
Delone Laboratory of Discrete and Computational Geometry
Yaroslavl State University, Sovetskaya str. 14, Yaroslavl, Russia, 150000
and
IITP RAS, Bolshoy Karetny per. 19, Moscow, Russia, 127994
e-mail: ilya.shkredov@gmail.com

ABSTRACT

We prove that if $A \subseteq \{1, \dots, N\}$ has no nontrivial solution to the equation $x_1 + x_2 + x_3 + x_4 + x_5 = 5y$, then $|A| \ll Ne^{-c(\log N)^{1/7}}$, $c > 0$. In view of the well-known Behrend construction, this estimate is close to best possible.

* The author is partly supported by MNSW grant N N201 543538.
** The author is supported by grant RFFI NN 11-01-00759, Russian Government project 11.G34.31.0053, Federal Program "Scientific and scientific–pedagogical staff of innovative Russia" 2009–2013, grant mol_a_ved 12-01-33080 and grant Leading Scientific Schools N 2519.02012.1.

Received October 25, 2011 and in revised form October 30, 2012

1. Introduction

The celebrated theorem of Roth [15] asserts that every subset of $\{1,\dots,N\}$ that does not contain any three-term arithmetic progression has size $O(N/\log\log N)$. There are numerous refinements of Roth's result [2, 3, 9, 27]. Currently, the best known upper bound $O(N/(\log N)^{1-o(1)})$ is due to Sanders [23]. A comprehensive history of the subject can be found in [28].

It turns out that Roth's method gives a similar upper bound for the size of sets having no nontrivial solutions to a invariant linear equation, namely an equation of the form

$$a_1x_1+\dots+a_kx_k=0, \tag{1}$$

with $a_1+\dots+a_k=0$, $k\geqslant 3$ (three-term arithmetic progressions correspond to the equation $x+y=2z$). On the other hand, the well-known construction of Behrend [1, 7, 10, 13, 14, 18, 19] provides large sets having no solution to a certain kind of invariant equations. He showed that there are subsets of $\{1,\dots,N\}$ of size $Ne^{(-C_{b,k}\sqrt{\log N})}$ without solution to the invariant equation

$$a_1x_1+\dots+a_kx_k=by, \tag{2}$$

where $a_1+\dots+a_k=b,\ a_i>0$.

The aim of this paper is to establish a new upper bound for subsets of $\{1,\dots,N\}$ having no solution to an invariant equation in at least 6 variables.

THEOREM 1.1: *Let N and $k\geqslant 6$ be positive integers. Let $A\subseteq\{1,\dots,N\}$ be a set having no solution to equation* (1)*, where all $x_1,\dots,x_k$ are distinct integers. Then*

$$|A|\ll \exp\Big(-c\Big(\log N\Big)^{1/7}\Big)N, \tag{3}$$

where $c=c(a_1,\dots,a_k)$.

Observe that Theorem 1.1 together with Behrend's example give a reasonable estimate for all equations of the type (2). Let us also formulate an immediate corollary to Theorem 1.1 for the equation

$$x_1+x_2+x_3+x_4+x_5=5y \tag{4}$$

which is very close to the most intriguing case $x+y=2z$.

COROLLARY 1.2: *Suppose that $A \subseteq \{1,\dots,N\}$ has no solution to equation* (4) *with distinct integers. Then there exists a constant $c>0$ such that*

$$|A| \ll \exp\Big(-c\Big(\log N\Big)^{1/7}\Big)N.$$

Our argument also uses the density increment method introduced by Roth, however in a different way. The density increment is not deduced from the existence of a large Fourier coefficient of a set A, $|A|=\alpha N$, having no solution to an equation (1) (which is always the case). We will be rather interested in finding a translation of a large Bohr set in $a_1\cdot A+a_2\cdot A+a_3\cdot A+a_4\cdot A$. Recent work of Sanders [22] (see also [24]) on the Polynomial Freiman–Ruzsa Conjecture guarantees the existence of such a Bohr set (actually we need a local version of Sanders theorem, which is proved in Section 5). Then, we show that A has a large density increment, by a constant factor, on a translation of some large Bohr set. By Sanders' theorem the dimension of the Bohr set increases by $O(\log^4(1/\alpha))$ in each iteration step, which makes the argument very effective.

The paper is organized as follows. We start with proving analogues of Theorem 1.1 and Corollary 1.2 for finite fields in Section 3. The argument is especially simple and clear in this case. Theorem 1.1 is proved in the next three sections. In Section 4 we recall some basic properties of Bohr sets in abelian groups. In Section 5 we prove a local version of Sanders' result. The next section contains the proof of Theorem 1.1. We conclude the paper with a discussion concerning consequences of a version of the Polynomial Bogolyubov Conjecture for sets having no solutions to an invariant linear equation with distinct integers.

2. Notation

Let $\mathbf{G}=(\mathbf{G},+)$ be a finite Abelian group with additive group operation $+$, and let $N=|\mathbf{G}|$. By $\widehat{\mathbf{G}}$ we denote the Pontryagin dual of $\mathbf{G}$, i.e., the space of homomorphisms γ from $\mathbf{G}$ to S^1. It is well known that $\widehat{\mathbf{G}}$ is an additive group which is isomorphic to $\mathbf{G}$. The Fourier coefficients of $f:\mathbf{G}\to\mathbb{C}$ are defined by

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

By the convolution of two function $f,g:\mathbf{G}\to\mathbb{C}$ we mean

$$(f*g)(x)=\sum_{y\in\mathbf{G}} f(y)g(x-y).$$

It is easy to see that $\widehat{f*g}(\gamma)=\widehat{f}(\gamma)\widehat{g}(\gamma)$. If X is a nonempty set, then by μ_X we denote the uniform probability measure on X and let

$$\mathrm{Spec}_{\epsilon}(\mu_X):=\{\gamma\in\widehat{\mathbf{G}}\ :\ |\widehat{\mu}_X(\gamma)|\geqslant\epsilon\}.$$

Let $\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}$, and $\mathbb{F}_p^*=\mathbb{Z}_p\setminus\{0\}$. If A is a set, then we write $A(x)$ for its characteristic function, i.e., $A(x)=1$ if $x\in A$ and $A(x)=0$ otherwise. All logarithms are to base 2. The signs $\ll$ and $\gg$ are usual Vinogradov's symbols.

3. Finite fields model

In this section we present proofs of Corollary 1.2 and Theorem 1.1 in a finite fields setting. Here we assume that $a_1,\dots,a_k\in\mathbb{F}_p^*$. The case of $\mathbb{F}_p^n$, in view of its linear space structure over $\mathbb{F}_p$, is considerably simpler than the case of $\mathbb{Z}$. Even the simplest version of Roth's argument yields the estimate $O_p(p^n/n^{k-2})$ for the size of sets free of the solution to (1) (see [12, 11], [20], [21]).

Our main tool is the following finite fields version of Sanders' theorem [22]. The interested reader will find all details of the proof in Section 5.

LEMMA 3.1: *Let K,L be real numbers. Suppose that $A,S,T\subseteq\mathbb{F}_p^n$ are finite non-empty sets such that $|A+S|\leqslant K|A|$, $|S+T|\leqslant L|S|$. Then $A-A+S-S$ contains a subspace V of codimension at most $O_p(\log^3 K\log L+\log(2\mu_{\mathbb{F}_p^n}^{-1/2}(T)))$.*

The proof of the next theorem illustrates the main idea of our approach.

THEOREM 3.2: *Suppose that $A\subseteq\mathbb{F}_p^n$, $p\neq 5$, and A has no nontrivial solution to (4) with $x_i\neq y$ for some i. Then*

$$|A|\leqslant p^n\cdot\exp(-c_p(\log p^n)^{1/5})$$

for some positive constant c_p.

Proof. Suppose that $A\subseteq\mathbb{F}_p^n$ has density α and contains no solution to (4). We split A into two disjoint sets A_1,A_2 of sizes that differ by at most one. Assuming the cardinality of A is large enough, we have

$$\sum_z|A_1\cap(z-A_2)|=|A_1||A_2|\geqslant|A|^2/16\gg\alpha^2p^{2n},$$

thus there exists $z\in\mathbb{F}_p^n$ such that

$$|A_1\cap(z-A_2)|\gg\alpha^2p^n.$$

Putting $B = A_1 \cap (z - A_2)$, we have $|B| \gg \alpha^2 p^n$, and thus $|B + B| \leqslant p^n \ll \alpha^{-2}|B|$.

By Lemma 3.1 applied with $A = S = T = B$, there exists a subspace V of codimension at most $O_p(\log^4(1/\alpha))$ such that $V \subseteq 2B - 2B$, so that

$$2z + V \subseteq 2A_1 + 2A_2.$$

Therefore, in view of $A_1 \cap A_2 = \emptyset$, we have $5y - x \notin 2z + V$ for all $x, y \in A$, hence for each w, if $A \cap (V + w) \neq \emptyset$ then $5 \cdot A \cap (V + w + 2z) = \emptyset$. Similarly, if $5 \cdot A \cap (V + w + 2z) \neq \emptyset$ then $A \cap (V + w) = \emptyset$. Hence

$$\begin{aligned} 2\alpha p^n = 2|A| &= \sum_{w \in V^\perp} (|A \cap (V + w)| + |5 \cdot A \cap (V + w + 2z)|) \\ &\leqslant |V|^{-1} p^n \max_v |A \cap (v + V)|, \end{aligned}$$

which implies

$$|A \cap (v + V)| \geqslant 2\alpha |V|,$$

for some v. Thus, $(A - v) \cap V$ is free of solutions to (4) and has density at least 2α on V. After t iterations we obtain a subspace of codimension at most $O_p(t \cdot \log^4(1/\alpha))$ such that

$$|(A - v_t) \cap V_t| \geqslant 2^t \alpha |V_t|,$$

for some v_t. Since the density is always at most one we can iterate this procedure at most $\log(1/\alpha) + 1$ times. Hence

$$(\log(1/\alpha) + 1) \cdot \log^4(1/\alpha) \gg_p n,$$

so that

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

for some positive constant ∎

LEMMA 3.3: *Let $A_1, \dots, A_k \subseteq \mathbb{F}_p^n$ be sets of density at least α. Then $A_1 - A_1 + \cdots + A_k - A_k$ contains a subspace V of codimension at most $O_p(k^{-3} \log^4(1/\alpha))$.*

Proof. We have

$$|A_1| \leqslant |A_1 + A_2| \leqslant \cdots \leqslant |A_1 + \cdots + A_k| \leqslant \alpha^{-1}|A_1|,$$

so that there exists $2 \leqslant i \leqslant k$ such that

$$|A_1 + \cdots + A_i| \leqslant \alpha^{-1/(k-1)} |A_1 + \cdots + A_{i-1}|.$$

Thus, setting $A = A_1 + \dots + A_{i-1}$, $S = T = A_i$, we have $|A+S| \leqslant \alpha^{-1/(k-1)}|A|$, $|S+T| \leqslant \alpha^{-1}|S|$, and $|T| \geqslant \alpha p^n$. Then applying Lemma 3.1, we infer that there is a subspace V of codimension

$$O_p(\log^3(\alpha^{-1/(k-1)}) \cdot \log(1/\alpha)) = O_p(k^{-3}\log^4(1/\alpha))$$

such that

$$v + V \subseteq A_1 - A_1 + \dots + A_i - A_i \subseteq A_1 - A_1 + \dots + A_k - A_k,$$

and the assertion follows. ∎

THEOREM 3.4: *Suppose that $A \subseteq \mathbb{F}_p^n$ has no solution with distinct elements to an invariant equation*

$$a_1x_1 + \dots + a_kx_k = 0, \tag{5}$$

where $a_1, \dots, a_k \in \mathbb{F}_p^*$ and $k \geqslant 6$. Then

$$|A| \leqslant kp^n \cdot \exp(-c_p(k^3 \log p^n)^{1/5})$$

for a positive constant c_p.

Proof. Suppose $A \subseteq \mathbb{F}_p^n$ has no solution with distinct elements to (5) and $|A| = \alpha p^n$. Let $A_1, \dots, A_{2l}$, $l = \lfloor (k-2)/2 \rfloor$ be arbitrary disjoint subsets of A of size $\lfloor |A|/(5k) \rfloor$ and put $A' = A \setminus \bigcup A_i$. As in (3) for any $i \in [l]$, we have

$$\sum_{z_i} |(a_{2i-1} \cdot A_{2i-1}) \cap (z_i - a_{2i} \cdot A_{2i})| = |A_{2i-1}||A_{2i}| \gg (\alpha/k)^2 p^{2n}$$

and, clearly, there are $z_1, \dots, z_l$ such that

$$|(a_{2i-1} \cdot A_{2i-1}) \cap (z_i - a_{2i} \cdot A_{2i})| \gg (\alpha/k)^2 p^n,$$

and let B_i, $1 \leqslant i \leqslant l$, be the sets on the left-hand side in the above inequalities, respectively. By Lemma 3.3, applied for $B_1, \dots, B_l$ and $K = O((k/\alpha)^2)$, there is a subspace V of codimension $d = O_p(k^{-3}\log^4(k/\alpha))$ such that

$$V \subseteq B_1 - B_1 + \dots + B_l - B_l,$$

so that

$$v + V \subseteq a_1 \cdot A_1 + \dots + a_{k-2} \cdot A_{k-2}$$

for some v. Since A does not contain any solution to (5) with distinct elements it follows that

$$a_{k-1}x + a_k y \notin v + V,$$

for all $x, y \in A'$, $x \neq y$. Hence, if for some w the coset $w + V$ contains at least 2 elements of A', then $-a_k^{-1}(a_{k-1}w - v) + V$ is disjoint from A'. The number of cosets of V sharing exactly 1 element with A is trivially at most p^d. Thus, there exists w' such that

$$|A' \cap (w' + V)| \geqslant \frac{(4/5)\alpha p^n - p^d}{p^d/2}|V|,$$

which is at least $(3/2)\alpha|V|$, provided that

$$p^{n-d} \gg \alpha^{-1}. \tag{6}$$

After t iterates of this argument we obtain a subspace V_t of codimension $O_p(tk^{-3}\log^4(k/\alpha))$ such that

$$|(A - v_t) \cap V_t| \geqslant (3/2)^t\alpha|V_t|.$$

Since $(3/2)^t\alpha \leqslant 1$ it follows that $t \leqslant 2\log(1/\alpha)$. Thus (6) must be violated after at most $2\log(1/\alpha)$ steps, in particular $p^{n-2\log(1/\alpha)d} \ll \alpha^{-1}$, so that

$$k^{-3}\log(1/\alpha)\log^4(k/\alpha) \gg_p n/2.$$

Hence $\alpha \leqslant k\exp(-c_p(k^3 \log p^n)^{1/5})$. ∎

4. Basic properties of Bohr sets

Bohr sets were introduced to additive number theory by Ruzsa [16]. Bourgain [2] was the first to use Fourier analysis on Bohr sets to improve the estimate in Roth's theorem. Sanders [22] further developed the theory of Bohr sets proving many important theorems; see, for example, Lemma 5.4 below.

Let Γ be a subset of $\widehat{\mathbf{G}}$, $|\Gamma| = d$, and $\varepsilon = (\varepsilon_1, \dots, \varepsilon_d) \in (0, 1]^d$.

Definition 4.1: Define the Bohr set $B = B(\Gamma, \varepsilon)$ setting

$$B(\Gamma, \varepsilon) = \{n \in \mathbf{G} \ : \ \|\gamma_j(n)\| < \varepsilon_j \text{ for all } \gamma_j \in \Gamma\},$$

where $\|x\| = |\arg x|/2\pi$.

The number d is called the **dimension** of B and is denoted by $\dim B$. If $M = B + n$, $n \in \mathbf{G}$ is a translation of a Bohr set B, we put $\dim M = \dim B$. The **intersection** $B \wedge B'$ of two Bohr sets $B = B(\Gamma, \varepsilon)$ and $B' = B(\Gamma', \varepsilon')$ is the Bohr set with the generating set $\Gamma \cup \Gamma'$ and a new vector $\tilde{\varepsilon}$ with $\tilde{\varepsilon}_j = \min\{\varepsilon_j, \varepsilon'_j\}$ if $\gamma_j \in \Gamma \cap \Gamma'$; further, $\tilde{\varepsilon}_j = \varepsilon_j$, $\gamma_j \in \Gamma \setminus \Gamma'$ and $\tilde{\varepsilon}_j = \varepsilon'_j$, $\gamma_j \in \Gamma' \setminus \Gamma$. We write $B' \leqslant B$ for two Bohr sets $B = B(\Gamma, \varepsilon)$, $B' = B(\Gamma', \varepsilon')$ if $\Gamma \subseteq \Gamma'$ and $\varepsilon'_j \leqslant \varepsilon_j$,

$j \in [\dim B]$. Thus $B' \leqslant B$ implies that $B' \subseteq B$ and always $B \wedge B' \leqslant B, B'$. Furthermore, if $B = B(\Gamma, \varepsilon)$ and $\rho > 0$, then by B_ρ we mean $B(\Gamma, \rho\varepsilon)$.

Definition 4.2: A Bohr set $B = B(\Gamma, \varepsilon)$ is called **regular**, if for every η, $d|\eta| \leqslant 1/100$ we have

$$(1 - 100d|\eta|)|B_1| < |B_{1+\eta}| < (1 + 100d|\eta|)|B_1|. \tag{7}$$

We formulate a sequence of basic properties of Bohr (see [2]), which will be used later.

LEMMA 4.3: *Let $B(\Gamma, \varepsilon)$ be a Bohr set. Then there exists ε_1 such that $\varepsilon/2 < \varepsilon_1 < \varepsilon$ and $B(\Gamma, \varepsilon_1)$ is regular.*

LEMMA 4.4: *Let $B(\Gamma, \varepsilon)$ be a Bohr set. Then*

$$|B(\Gamma, \varepsilon)| \geqslant \frac{N}{2} \prod_{j=1}^{d} \varepsilon_j.$$

LEMMA 4.5: *Let $B(\Gamma, \varepsilon)$ be a Bohr set. Then*

$$|B(\Gamma, \varepsilon)| \leqslant 8^{|\Gamma|+1} |B(\Gamma, \varepsilon/2)|.$$

LEMMA 4.6: *Suppose that $B^{(1)}, \dots, B^{(k)}$ is a sequence of Bohr sets. Then*

$$\mu_{\mathbf{G}}\Big(\bigwedge_{i=1}^{k} B^{(i)} \Big) \geqslant \prod_{i=1}^{k} \mu_{\mathbf{G}}(B^{(i)}_{1/2}).$$

The next lemma is due to Bourgain [2]. It shows the fundamental property of regular Bohr sets. We recall his argument for the sake of completeness.

LEMMA 4.7: *$B = B(\Gamma, \varepsilon)$ be a regular Bohr set. Then for every Bohr set $B' \leqslant B(\Gamma, \varepsilon')$ such that $\varepsilon' \leqslant \kappa\varepsilon/(100d)$ we have:*

1. *the number of n's such that $(B * B')(n) > 0$ does not exceed $|B|(1+\kappa)$;*
2. *the number of n's such that $(B * B')(n) = |B'|$ is greater than $|B|(1-\kappa)$ and*

$$\|\mu_B * \mu_{B'} - \mu_B\|_1 < 2\kappa. \tag{8}$$

Proof. If $(B * B^{'})(n) > 0$, then there exists m such that for any $\gamma_j \in \Gamma$ we have

$$\|\gamma_j \cdot m\| < \frac{\kappa}{100d}\varepsilon_j, \quad \|\gamma_j \cdot (n - m)\| < \varepsilon_j,$$

so that

$$\|\gamma_j \cdot n\| < \Big(1 + \frac{\kappa}{100d}\Big)\varepsilon_j,$$

for all $\gamma_j \in \Gamma$. Therefore $n \in B^+ := B\left(\Gamma, \left(1 + \frac{\kappa}{100d}\right)\varepsilon\right)$ and since B is regular by (7) we have $|B^+| \leqslant (1+\kappa)|B|$. This proves (1).

To prove (2) observe that if

$$n \in B^- := B\left(\Gamma, \left(1 - \frac{\kappa}{100d}\right)\varepsilon\right),$$

then $(B * B^{'})(n) = |B'|$. By (7) we have $|B^-| \geqslant (1-\kappa)|B|$.

To prove (8) note that

$$\|\mu_B * \mu_{B'} - \mu_B\|_1 = \|\mu_B * \mu_{B'} - \mu_B\|_{l^1(B^+ \setminus B^-)} \leqslant \frac{|B^+| - |B^-|}{|B|} < 2\kappa,$$

as required. ∎

Corollary 4.8: *With the assumptions of Lemma 4.7 we have* $|B| \leqslant |B+B'| \leqslant |B^+| \leqslant (1+\kappa)|B|$.

Another useful corollary is the following.

Corollary 4.9: *Let* $f : \mathbf{G} \to \mathbb{C}$ *be a function such that* $|f(x)| \leqslant 1$ *for every* $x \in \mathbf{G}$. *With the assumptions of Lemma 4.7, we have*

$$\|\mu_B \cdot f - \mu_B * \mu_{B'} \cdot f\|_1 < 2\kappa. \tag{9}$$

Proof. Indeed, we have

$$\begin{aligned}\|\mu_B \cdot f - \mu_B * \mu_{B'} \cdot f\|_1 =& \Big|\sum_x (\mu_B - \mu_B * \mu_{B'})(x) f(x)\Big| \\ \leqslant& \sum_x |(\mu_B - \mu_B * \mu_{B'})(x)| \\ =& \|\mu_B - \mu_B * \mu_{B'}\|_1 < 2\kappa,\end{aligned}$$

as required. ∎

Inequality (9) holds if we replace

$$\|\mu_B \cdot f - \mu_B * \mu_{B'} \cdot f\|_1$$

by

$$\|\mu_B * f - \mu_B * \mu_{B'} * f\|_\infty.$$

We do not need the fact in our proof.

Notice that for every $\gamma \in \mathbb{Z}_p^*$ and a Bohr set $B(\Gamma, \varepsilon) \subseteq \mathbb{Z}_p$ we have $\gamma \cdot B(\Gamma, \varepsilon) = B(\gamma^{-1} \cdot \Gamma, \varepsilon)$. Thus, if $B(\Gamma, \varepsilon)$ is regular, then $\gamma \cdot B(\Gamma, \varepsilon)$ is regular as well.

5. A variant of Sanders' theorem

Recall that an arithmetic progression of dimension d and size L is a set of the form

$$P = \{a_0 + a_1 x_1 + \dots + a_d x_d \ : \ 0 \leqslant x_j < l_j\}, \tag{10}$$

where $L = l_1 \dots l_d$; P is said to be **proper** if all of the sums in (10) are distinct. By a **proper coset progression** of dimension d we will mean a subset of $\mathbf{G}$ of the form $P + H$, where $H \subseteq \mathbf{G}$ is a subgroup, P is a proper progression of dimension d and the sum is direct in the sense that $p + h = p' + h'$ if and only if $h = h'$ and $p = p'$. By the size of a proper coset progression we mean simply its cardinality.

Very recently Sanders [22] proved the following remarkable result.

THEOREM 5.1: *Suppose that* $\mathbf{G}$ *is an abelian group and* $A, S \subseteq \mathbf{G}$ *are finite non-empty sets such that* $|A + S| \leqslant K \min\{|A|, |S|\}$. *Then* $(A - A) + (S - S)$ *contains a proper symmetric* $d(K)$*-dimensional coset progression* M *of size* $\exp(-h(K))|A + S|$. *Moreover, we may take* $d(K) = O(\log^6 K)$, *and* $h(K) = O(\log^6 K \log\log K)$.

The aim of this section is to show the following modification of Sanders' theorem which is crucial for our argument.

THEOREM 5.2: *Let* $\varepsilon, \delta \in (0, 1]$ *be real numbers. Let* A, A' *be subsets of a regular Bohr set* B *and let* S, S' *be subsets of a regular Bohr set* B_ε, *where* $\varepsilon \leqslant 1/(100d)$ *and* $d = \dim B$. *Suppose that* $\mu_B(A), \mu_B(A'), \mu_{B_\varepsilon}(S), \mu_{B_\varepsilon}(S') \geqslant \alpha$. *Then the set* $(A - A') + (S - S')$ *contains a translation of a regular Bohr set* $z + \tilde{B}$ *such that* $\dim \tilde{B} = d + O(\log^4(1/\alpha))$ *and*

$$|\tilde{B}| \geqslant \exp(-O(d\log d + d\log(1/\varepsilon) + \log^4(1/\alpha)\log d + \log^5(1/\alpha) + d\log(1/\alpha)))|B|. \tag{11}$$

Observe that the statement above with $O(d^4 + \log^4(1/\alpha))$ instead of $d + O(\log^4(1/\alpha))$ is a direct consequence of Theorem 5.1 (see the beginning of the proof of Theorem 5.2).

Next we formulate two results, which will be used in the course of the proof of Theorem 5.2. The first lemma coincides with Proposition 3.2 from Sanders' paper [22] and is a version of the Croot–Sisask theorem [6].

LEMMA 5.3: *Suppose that* $\mathbf{G}$ *is a group,* $A, S, T \subseteq \mathbf{G}$ *are finite non-empty sets such that* $|A+S| \leqslant K|A|$ *and* $|T+S| \leqslant L|S|$. *Let* $\epsilon \in (0,1]$ *and let* h *be a positive integer. Then there is* $t \in T$ *and a set* $X \subseteq T-t$ *with*

$$|X| \geqslant \exp(-O(\epsilon^{-2}h^2 \log K \log L))|T|$$

such that

$$|\mu_{-A} * (A+S) * \mu_{-S}(x) - 1| \leqslant \epsilon \quad \text{for all } x \in hX.$$

The next lemma is a special case of Lemma 5.3 from [22]. This is a local version of Chang's spectral lemma [5], which is another important result recently proved in additive combinatorics.

LEMMA 5.4: *Let* ϵ, ν, ρ *be positive real numbers. Suppose that* B *is a regular Bohr set and let* $X \subseteq B$. *Then there is a set* Λ *of size* $O(\epsilon^{-2}\log(2\mu_B^{-1/2}(X)))$ *such that for any* $\gamma \in \operatorname{Spec}_\epsilon(\mu_X)$ *we have*

$$|1-\gamma(x)| = O(|\Lambda|(\nu + \rho \dim^2(B))) \quad \text{for all } x \in B_\rho \wedge B'_\nu,$$

where $B' = B(\Lambda, 1/2)$.

Proof of Theorem 5.2. Let $T = B_\delta$, $\delta = \varepsilon/100d$ and $K = L = O(1/\alpha)$. In the notation of section 4, we have $A+S \subseteq B+B_\varepsilon \subseteq B^+$, and $S+T \subseteq B_\varepsilon + B_\delta \subseteq B_\varepsilon^+$, whence $|A+S| \leqslant K|A|$, $|S+T| \leqslant L|S|$ by the regularity of B and B_ε. Applying Lemma 5.3 with A, S and T, we see that there exist $t \in T$ and $X \subseteq B_\delta - t$ satisfying

$$|X| \geqslant \exp(-O(\epsilon^{-2}h^2 \log^2 K))|B_\delta|, \tag{12}$$

and

$$|\mu_{-A} * (A+S) * \mu_{-S}(x) - 1| \leqslant \epsilon/3 \quad \text{for all } x \in hX. \tag{13}$$

By Lemma 4.3 we may assume that B_δ is regular.

Let ϵ be a small positive constant to be specified later. Put $h = \lceil \log(K/\epsilon) \rceil$ and $l = O(\epsilon^{-4}h^2 \log^2 K)$. Applying Lemma 5.4 for $X+t \subseteq B_\delta$ with parameters $\nu = O(\epsilon/(lK^{1/2}))$, $\rho = O(\epsilon/(ld^2K^{1/2}))$, we obtain

$$|1-\gamma(x)| \leqslant \epsilon/(3K^{1/2}) \quad \text{for all } x \in B_{\delta\rho} \wedge B'_\nu \text{ and } \gamma \in \operatorname{Spec}_\epsilon(\mu_X). \tag{14}$$

Recall that $B' = B(\Lambda, 1/2)$, and $|\Lambda| = l$. We have $\dim(B_{\delta\rho} \wedge B'_\nu) = d + O(\log^4(1/\alpha))$.

By the same argument applied for sets A', S' there are sets X', Λ' of cardinality l and a Bohr set B^*_ν that satisfy inequalities (12) and (14), respectively. Finally, we set

$$B'' = B_{\delta\rho} \wedge B'_\nu \wedge B^*_\nu.$$

Clearly, $d'' = \dim B'' = d + O(\log^4(1/\alpha))$ and by Lemma 4.4, Lemma 4.5, Lemma 4.6 and $\epsilon = \Omega(1)$ we have

(15)
$$|B''| \geqslant \exp(-O(d\log d + d\log(1/\varepsilon) + \log^4(1/\alpha)\log d + \log^5(1/\alpha) + d\log(1/\alpha)))|B|.$$

In view of the inequality

$$\sum_\gamma |\widehat{(A+S)}(\gamma)\widehat{\mu}_A(\gamma)\widehat{\mu}_S(\gamma)| \leqslant \frac{(|A+S||A|)^{1/2}}{|S|} \leqslant K^{1/2},$$

which follows from the Cauchy–Schwarz inequality and Parseval's formula, we may proceed in the same way as in the proof of Lemma 9.2 in [22] and conclude that for any probability measure μ supported on B'' we have

$$\|(A+S)*\mu\|_\infty \geqslant 1-\epsilon \quad \text{and} \quad \|(A'+S')*\mu\|_\infty \geqslant 1-\epsilon. \tag{16}$$

Let $\eta = 1/4d''$. We show that $(A-A')+(S-S')$ contains a translation of $\tilde{B} := B''_\eta$.

Indeed, note that

$$B''_{1/2} \subseteq B''_{1/2+\eta} \subseteq \cdots \subseteq B''_{1/2+2d''\eta} = B'',$$

so that by the pigeonhole principle, there is some $i \leqslant 2d''$ such that $|B''_{1/2+i\eta}| \leqslant \sqrt{2}|B''_{1/2+(i-1)\eta}|$. We apply (16) for

$$\mu = \frac{B''_{1/2+i\eta} + B''_{1/2+(i-1)\eta}}{|B''_{1/2+i\eta}| + |B''_{1/2+(i-1)\eta}|}.$$

Thus, there is x such that

$$|(x+A+S)\cap B''_{1/2+i\eta}| + |(x+A+S)\cap B''_{1/2+(i-1)\eta}| \geqslant (1-\epsilon)\left(|B''_{1/2+i\eta}| + |B''_{1/2+(i-1)\eta}|\right).$$

Taking ϵ sufficiently small (see [22] for details), we get

$$|(x+A+S)\cap B''_{1/2+i\eta}| \geqslant \frac{3}{4}|B''_{1/2+(i-1)\eta}|,$$
$$|(x+A+S)\cap B''_{1/2+(i-1)\eta}| \geqslant \frac{3}{4}|B''_{1/2+(i-1)\eta}|.$$

Analogously, for some y, we obtain

$$|(y+A'+S')\cap B''_{1/2+i\eta}| \geqslant \frac{3}{4}|B''_{1/2+(i-1)\eta}|,$$
$$|(y+A'+S')\cap B''_{1/2+(i-1)\eta}| \geqslant \frac{3}{4}|B''_{1/2+(i-1)\eta}|.$$

Hence for each $b\in \tilde{B}$, we have

$$\begin{aligned}(A+S)*(-A'-S')(b+y-x)&\\ =&(x+A+S)*(-y-A'-S')(b)\\ \geqslant&((x+A+S)\cap B''_{1/2+i\eta})*((-y-A-S)\cap B''_{1/2+(i-1)\eta})(b)\\ \geqslant&|(x+A+S)\cap B''_{1/2+i\eta}|+|(y+A+S)\cap B''_{1/2+(i-1)\eta}|\\ &-|((x+A+S)\cap B''_{1/2+i\eta})\cap((-y-A-S)\cap B''_{1/2+i\eta})|\\ \geqslant&\frac{3}{2}|B''_{1/2+(i-1)\eta}|-|B''_{1/2+i\eta}|>0.\end{aligned}$$

Therefore, $(A-A')+(S-S')$ contains a translation of $\tilde{B}$. Finally, by Lemma 4.3, there is $1/2\leqslant\sigma\leqslant 1$ such that $\tilde{B}_\sigma$ is regular. By (15) and Lemma 4.5, $\tilde{B}_\sigma$ also satisfies (11). This completes the proof. ∎

6. Proof of the main result

Let $A\subseteq\{1,\dots,N\}$ be a set having no solution to (1). As usual we embed A in $\mathbb{Z}_p$, where p is a prime between $(\sum|a_i|)N$ and $2(\sum|a_i|)N$, so A has no solution to (1) in $\mathbb{Z}_p$. All sets considered below are subsets of $\mathbb{Z}_p$. We start with the following simple observation.

LEMMA 6.1: *Let B be a regular Bohr set of dimension d and let $B'\leqslant B_\rho$, where $\rho\leqslant\alpha/(1600d)$. Suppose that $\mu_B(A),\mu_B(A')\geqslant\alpha$. Then there exists $x\in B$ such that*

$$(\mu_{B'}*A)(x),\ (\mu_{B'}*A')(-x)\geqslant\alpha/4 \tag{17}$$

or

$$\|\mu_{B'}*A\|_\infty\geqslant 1.5\alpha \text{ or } \|\mu_{B'}*A'\|_\infty\geqslant 1.5\alpha. \tag{18}$$

Proof. By Corollary 4.9 we have

$$\alpha \leqslant \sum_{x\in B}\mu_B(x)A(x) \leqslant \|\mu_B\cdot A-\mu_B*\mu_{B'}\cdot A\|_1+\sum_{x\in B}(\mu_B*\mu_{B'})(x)A(x)$$
$$\leqslant \frac{1}{8}\alpha+\frac{1}{|B|}\sum_{x\in B}(\mu_{B'}*A)(x),$$

and similarly

$$\alpha \leqslant \frac{1}{8}\alpha+\frac{1}{|B|}\sum_{x\in B}(\mu_{B'}*A')(x)=\frac{1}{8}\alpha+\frac{1}{|B|}\sum_{x\in B}(\mu_{B'}*A')(-x).$$

Hence

$$\sum_{x\in B}((\mu_{B'}*A)(x)+(\mu_{B'}*A')(-x)) \geqslant \frac{7}{4}\alpha|B|$$

and the result follows. ∎

Theorem 1.1 is a consequence of the next lemma.

LEMMA 6.2: *Suppose that B is a regular Bohr set of dimension d and $A\subseteq B$, $\mu_B(A)\geqslant\alpha$ has no solution with distinct elements to (1). Assume that*

$$|B| \geqslant \exp(C(d\log d+\log^5(1/\alpha)+d\log(1/\alpha)+\log d\log^4(1/\alpha))), \tag{19}$$

where $C=C(k)>0$ is a large constant. Then there exists a regular Bohr set B' such that

$$\|\mu_{B'}*A\|_\infty \geqslant (1+1/(16k))\alpha, \tag{20}$$

$\dim B'=d+O(\log^4(1/\alpha))$, *and*

$$|B'| \geqslant \exp(-O(d\log d+\log^5(1/\alpha)+d\log(1/\alpha)+\log d\log^4(1/\alpha)))|B|. \tag{21}$$

Proof. Set $M=\prod|a_i|$ and choose a constant $1/64\leqslant c\leqslant 1/32$ in such a way that B_ε is a regular Bohr set, where $\varepsilon=c\alpha/(100Mdk)$. Furthermore, define $B^i=(\prod_{j\neq i}a_j)\cdot B_\varepsilon$. Observe that by Lemma 4.5 it follows that

$$|B_{\varepsilon/2}| \geqslant \exp(-O(d\log d+d\log(1/\alpha))|B|. \tag{22}$$

By Corollary 4.9 we have

$$\begin{aligned} k\alpha \leqslant & k\sum_{x\in B}\mu_B(x)A(x)\\ \leqslant & \sum_{i=1}^{k}\|\mu_B\cdot A-\mu_B*\mu_{B^i}\cdot A\|_1+\sum_{i=1}^{k}\sum_{x\in B}(\mu_B*\mu_{B^i})(x)A(x)\\ \leqslant & 200\varepsilon kdM+\frac{1}{|B|}\sum_{x\in B}\sum_{i=1}^{k}(\mu_{B^i}*A)(x), \end{aligned}$$

so that

$$\sum_{i=1}^{k}(\mu_{B^i}*A)(w)\geqslant (k-2c)\alpha\geqslant (k-1/16)\alpha$$

for some $w\in B$. Thus, for $\eta=1/(16k)$, either we have $\|\mu_{B^i}*A\|_\infty\geqslant(1+\eta)\alpha$ for some $1\leqslant i\leqslant k$, or

$$(\mu_{B^i}*A)(w)=\mu_{B^i}(A+w)=\mu_{B'}(a_i\cdot(A+w))\geqslant (k-1/16)\alpha-(k-1)(1+\eta)\alpha\geqslant\frac{7}{8}\alpha$$

for every i, where $B'=(\prod a_j)\cdot B_\varepsilon$. In the first case, in view of $\dim B'=d$ and (22), we are done because we achieve the required density increment on a large Bohr set, so we may assume that the last inequalities hold. Since (1) is an invariant equation we may translate our set and assume that $\mu_{B'}(a_i\cdot A)\geqslant 7\alpha/8$ for all $1\leqslant i\leqslant k$.

Let $B'_{\varepsilon/2}\subseteq B''\subseteq B'_\varepsilon$ and $B''_{\varepsilon/2}\subseteq B'''\subseteq B''_\varepsilon$ be regular Bohr sets. By regularity of B' and Lemma 6.1 applied for $A=a_1\cdot A$, $A'=a_2\cdot A$ and $B'=B''$, either (18) holds, and again we are done, or there exists $x\in B'$ with

$$\mu_{B''+x}(a_1\cdot A)\geqslant\alpha/8\quad\text{ and }\quad\mu_{B''-x}(a_2\cdot A)\geqslant\alpha/8. \tag{23}$$

We show that there are disjoint sets A_1,A_2 of A such that

$$\alpha/32\leqslant\mu_{B''+x}(a_1\cdot A_1)\leqslant\alpha/16\quad\text{ and }\quad\alpha/32\leqslant\mu_{B''-x}(a_2\cdot A_2)\leqslant\alpha/16. \tag{24}$$

Indeed, let

$$Q_1=\{q\in A\ :\ a_1\cdot q\in B''+x\},\quad Q_2=\{q\in A\ :\ a_2\cdot q\in B''-x\}.$$

By (23) we have $|Q_1|,|Q_2|\geqslant\alpha|B''|/8$. If $|Q_1\cap Q_2|>\alpha|B''|/16$, then split $Q_1\cap Q_2$ into two parts A_1, A_2 whose sizes differ by at most one. Otherwise, we put $A_1=Q_1\setminus Q_2$, $A_2=Q_2\setminus Q_1$ and delete unnecessary elements from the sets.

Put $A' = A \setminus (A_1 \cup A_2)$; then $\mu_{B'}(a_i \cdot A') \geqslant 3\alpha/4$ for $i \geqslant 3$. Again applying Lemma 6.1 for B''' and the arguments above, we find $y \in B'$ and disjoint sets $A_3, A_4 \subseteq A'$ such that

$$\alpha/32 \leqslant \mu_{B'''+y}(a_3 \cdot A_3) \leqslant \alpha/16 \quad \text{and} \quad \alpha/32 \leqslant \mu_{B'''-y}(a_4 \cdot A_4) \leqslant \alpha/16. \tag{25}$$

Assume that k is even and set $l = (k-6)/2$. Using very similar arguments as above (based on Lemma 6.1), one can find $y_1, \dots, y_l \in \mathbb{Z}_p$ and distinct elements $x_5, \dots, x_{k-2} \in A \setminus (A_1 \cup A_2 \cup A_3 \cup A_4)$ such that

$$a_5x_5, -a_6x_6 \in B'' + y_1, \dots, a_{k-3}x_{k-3}, -a_{k-2}x_{k-2} \in B'' + y_l. \tag{26}$$

Finally, by Theorem 5.2 applied with

$$a_1 \cdot A_1 - x \subseteq B'',\ -a_2 \cdot A_2 - x \subseteq B'',\ a_3 \cdot A_3 - y \subseteq B''',\ -a_4 \cdot A_4 - y \subseteq B''',$$

there exists a Bohr set $\tilde{B} \leqslant B''$ and z such that

$$\tilde{B} + z \subseteq a_1 \cdot A_1 + a_2 \cdot A_2 + a_3 \cdot A_3 + a_4 \cdot A_4 + \sum_{j=5}^{k-2} a_j x_j, \tag{27}$$

$\tilde{d} = \dim \tilde{B} = d + O(\log^4(1/\alpha))$ and

$$\begin{aligned} |\tilde{B}| &\geqslant \exp(-O(d\log d + d\log(1/\varepsilon) + \log^5(1/\alpha) \\ &\qquad + d\log(1/\alpha) + \log d \log^4(1/\alpha)))|B''| \\ &\geqslant \exp(-O(d\log d + \log^5(1/\alpha) + d\log(1/\alpha) + \log d \log^4(1/\alpha)))|B|. \end{aligned} \tag{28}$$

If the sum over j in (27) is empty, then we define it to be equal to zero. Notice that by (26), $z \in (k-4)B'' + 2B''' \subseteq kB''$. Since $A_1, \dots, A_4$ are disjoint and $x_5, \dots, x_{k-2} \in A \setminus (A_1 \cup A_2 \cup A_3 \cup A_4)$ are distinct, it follows that

$$a_{k-1}x_{k-1} + a_kx_k \notin \tilde{B} - z \tag{29}$$

for all distinct $x_{k-1}, x_k \in (A \setminus (A_1 \cup A_2 \cup A_3 \cup A_4)) \setminus \{x_5, \dots, x_{k-2}\}$.

By Lemma 4.3 we find $\alpha/(6400d) \leqslant \delta \leqslant \alpha/(3200d)$ such that $\tilde{B}_\delta$ is regular. Obviously $\tilde{B}_\delta$ satisfies (28). For $i = k-1$ and k, write

$$E_i := \{x \in B' \ :\ (\mu_{\tilde{B}_\delta} * (a_i \cdot A))(x) \geqslant k/|\tilde{B}_\delta|\}.$$

Observe that by (29), if $-z \in E_{k-1} + E_k$, then one can find a solution to (1) with distinct $x_1, \dots, x_k \in A$. Therefore $E_{k-1} \subseteq B' \setminus (-E_k - z)$, and since $z \in kB''$

and the Bohr set B' is regular, we have

$$\begin{aligned}|E_{k-1}| \leqslant &|B' \setminus (-E_k - z)| = |B'| - |B' \cap (E_k + z)| \\ \leqslant &|B'| - (|E_k| - |(B' + kB'') \setminus B'|) \\ \leqslant &|B'| - |E_k| + 100\varepsilon dk|B'|,\end{aligned}$$

whence

$$|E_{k-1}| + |E_k| \leqslant (4/3)|B'|,$$

so that $|E_i| \leqslant (2/3)|B'|$ for some $i \in \{k, k+1\}$. Thus, by Corollary 4.9

$$\begin{aligned}\frac{7}{8}\alpha \leqslant &\sum_{x\in B'} \mu_{B'}(x)(a_i \cdot A)(x) \\ \leqslant &\frac{1}{|B'|}\sum_{x\in B'} \mu_{\tilde{B}_\delta}(x)(a_i \cdot A)(x) + \|\mu_{B'} * \mu_{\tilde{B}_\delta} \cdot (a_i \cdot A) - \mu_{\tilde{B}_\delta} \cdot (a_i \cdot A)\|_1 \\ \leqslant &\mu_{B'}(E_i)\|\mu_{\tilde{B}_\delta} * (a_i \cdot A)\|_\infty + \frac{k}{|\tilde{B}_\delta|} + 200\delta d \\ \leqslant &\frac{2}{3}\|\mu_{\tilde{B}_\delta} * (a_i \cdot A)\|_\infty + \frac{k}{|\tilde{B}_\delta|} + \frac{1}{16}\alpha.\end{aligned}$$

By Lemma 4.5, (19) and (28), we have

$$\begin{aligned}|\tilde{B}_\delta| \geqslant &\exp(-O((d + \log^4(1/\alpha))(\log(1/\alpha) + \log d))|\tilde{B}| \\ \geqslant &\exp(-O(d\log d + \log^5(1/\alpha) + d\log(1/\alpha) + \log d \log^4(1/\alpha)))|B| \\ \geqslant &16k/\alpha,\end{aligned}$$

hence

$$\|\mu_{\tilde{B}_\delta} * (a_i \cdot A)\|_\infty \geqslant \frac{9}{8}\alpha.$$

Finally

$$\|\mu_{B^*} * A\|_\infty \geqslant \frac{9}{8}\alpha,$$

where $B^* = a_i^{-1} \cdot \tilde{B}_\delta$, and the assertion follows.

Now suppose that k is odd. Only the first part of the proof needs to be slightly modified. Certainly, we may assume that $a_5 = 1$. Proceeding exactly as before we find regular Bohr sets B', B'' and B''', and disjoint sets $A_1, A_2, A_3, A_4 \subseteq A$ such that $\mu_{B'}(a_i \cdot A) \geqslant 7\alpha/8$ and (24), (25) hold. Furthermore, for $l = (k-7)/2 \geqslant 0$, we find $y_1, \dots, y_l \in \mathbb{Z}_p$ and distinct elements $x_5, \dots, x_{k-2} \in A \setminus (A_1 \cup A_2 \cup A_3 \cup A_4)$ such that

$$x_5 \in B'',\ a_6x_6, -a_7x_7 \in B'' + y_1, \dots, a_{k-3}x_{k-3}, -a_{k-2}x_{k-2} \in B'' + y_l.$$

By Theorem 5.2 there exists a Bohr set $\tilde{B}$ satisfying (27)–(29). However, $x_5 \in B''$, so that again $z \in kB''$, which was the only thing we have to check. One can finish the proof in exactly the same way as before. ∎

Proof of Theorem 1.1. Let $A \subseteq B^0 = \mathbb{Z}_p, |A| \geqslant \alpha p$. We apply iteratively Lemma 6.2. After t steps we obtain a regular Bohr set B^t and $x_t \in \mathbb{Z}_p$ such that

$$|A \cap (B^t + x_t)| \geqslant (1 + 1/(16k))^t \alpha |B^t|,$$

$\dim B^t \ll t \log^4(1/\alpha)$, and

$$|B^t| \geqslant \exp(-O(t \log^5(1/\alpha)))|B^{t-1}|.$$

Since the density is always less than 1 we may apply Lemma 6.2 at most $O(\log(1/\alpha))$ times. Therefore, after $t = O(\log(1/\alpha))$ iterates, the assumptions of Lemma 6.2 are violated, so that

$$\exp(-O(\log^7(1/\alpha)))p \leqslant |B^t| \leqslant \exp(O(\log^6(1/\alpha))),$$

which yields

$$\alpha \ll \exp(-c(\log p/\log\log p)^{1/6}),$$

and the assertion follows. ∎

7. The Polynomial Bogolyubov Conjecture and linear equations

The Polynomial Bogolyubov Conjecture can be formulated as follows.

CONJECTURE 7.1: *Let $A \subseteq \mathbb{Z}_N, |A| = \alpha N$. Then there exists a Bohr set $B(\Gamma, \varepsilon) \subseteq 2A - 2A$ such that $|\Gamma| = d \ll \log(1/\alpha)$ and $\varepsilon \gg 1/\log(1/\alpha)$.*

It is known (see [8]) that the Polynomial Bogolyubov Conjecture implies the well known Polynomial Freiman–Ruzsa Conjecture.

For every Bohr set we have

$$|B(\Gamma, \varepsilon)| \geqslant \frac{1}{2}\varepsilon^d N,$$

so that Conjecture 7.1 would give a nontrivial result provided that $\alpha \gg N^{-c/\log\log N}$. However, it was proved in [25] and [26] that in Chang's lemma (which is an important ingredient of all results of this sort, see Section 5) one can take much larger ε. This gives a (little) support for the following version of the above conjecture for sparse sets.

CONJECTURE 7.2: *Let $A, A' \subseteq \mathbb{Z}_N, |A|, |A'| \geqslant N^{1-c}$. Then there exists a $\delta_c \log N$-dimensional Bohr set $B \subseteq A - A + A' - A'$ such that $|B| \gg N^{1-c'}$ and $\delta_c \to 0, c' \to 0$ with $c \to 0$. Furthermore, each $b \in B$ has $\gg |A|^2|A'|^2/N$ representations in the form $a - b + a' - b'$, $a, b \in A$, $a', b' \in A'$.*

We shall give here an application of Conjecture 7.2. First we recall some definitions from [17]. Let

$$a_1x_1 + \cdots + a_kx_k = 0 \tag{30}$$

be an invariant linear equation. We say that the solution $x_1, \ldots, x_k$ of (30) is trivial if there is a partition $\{1, \ldots, k\} = \mathcal{T}_1 \cup \cdots \cup \mathcal{T}_l$ into nonempty and disjoint sets $\mathcal{T}_j$ such that $x_u = x_v$ if and only if $u, v \in \mathcal{T}_j$ for some j and

$$\sum_{i \in \mathcal{T}_j} a_i = 0,$$

for every $1 \leqslant j \leqslant l$. The **genus** of (30) is the largest $\mathbf{g}$ such that there is a partition $\{1, \ldots, k\} = \mathcal{T}_1 \cup \cdots \cup \mathcal{T}_{\mathbf{g}}$ into nonempty and disjoint sets $\mathcal{T}_j$ such that

$$\sum_{i \in \mathcal{T}_j} a_i = 0,$$

for every $1 \leqslant j \leqslant \mathbf{g}$. Let $r(N)$ be the maximum size of a set $A \subseteq \{1, \ldots, N\}$ having no nontrivial solution to (30) with $x_i \in A$ and let $R(N)$ be the analogous maximum over sets such that equation (30) has no solution with distinct $x_i \in A$. It is not hard to prove that $r(N) \ll N^{1/\mathbf{g}}$. Much less is known about the behavior of $R(N)$. Bukh [4] showed that we always have $R(N) \ll N^{1/2-\varepsilon}$ for the symmetric equations

$$a_1x_1 + \cdots + a_lx_l = a_1y_1 + \cdots + a_ly_l.$$

Our result is the following.

THEOREM 7.3: *Assuming Conjecture 7.2 we have*

$$R(N) \ll N^{1-c},$$

for every invariant equation (30) *with* $a_1 = -a_2$, $a_3 = -a_4$, *where* $c = c(a_1, \ldots, a_k)$.

Proof. Suppose that A has no solution to an equation (30) with $a_1 = -a_2$, $a_3 = -a_4$, where $c = c(a_1, \ldots, a_k)$, and assume that $|A| \gg N^{1-c}$, $c > 0$. We embed A in $\mathbb{Z}_M$ with $M = SN$, where $S = \sum |a_i|$, so that any solution to (30)

in $\mathbb{Z}_M$ is a genuine solution in $\mathbb{Z}$. Let $A = A_1 \cup A_2$ be a partition of A into roughly equal parts. If Conjecture 7.2 holds, then there is a Bohr set

$$B \subseteq a_1 \cdot A_1 - a_1 \cdot A_1 + a_3 \cdot A_1 - a_3 \cdot A_1$$

of dimension at most $\delta_c \log N$ and size at least $\gg N^{1-c'}$. Put $B' = B_{1/S}$. We show that for every $t \in \mathbb{Z}_M$ we have

$$|(t + B') \cap A_2| \leqslant k - 4.$$

Indeed, if there are distinct $x_5, \dots, x_k \in (t + B') \cap A_2$, then

$$\sum_{i=5}^{k} a_i x_i \in \Big(\sum_{i=5}^{k} a_i t \Big) + B = B.$$

However, each element in B has at least $|A|^4/M$ representations in the form $a_1 x - a_1 y + a_3 z - a_3 w$, $x, y, z, w \in A_1$. This would give a solution to (30) with distinct integers. Hence

$$|B'||A_2| = \sum_t |(t + B') \cap A_2| \leqslant kM,$$

so

$$|A| \leqslant 2kSN/|B'|.$$

Now, by Lemma 4.5 it follows that $|B'| \gg S^{-4d}|B| \gg N^{1-c'-2\delta_c \log S}$. This leads to a contradiction, provided c is small enough. ∎

Acknowledgement. We wish to thank Tom Sanders for stimulating discussions.

References

[1] F. A. Behrend, *On sets of integers which contain no three terms in arithmetic progression,* Proceedings of the National Academy of Sciences of the United States of America **23** (1946), 331–332.

[2] J. Bourgain, *On triples in arithmetic progression,* Geometric and Functional Analysis **9** (1999), 968–984.

[3] J. Bourgain, *Roth's theorem on progressions revisited,* Journal d'Analyse Mathématique **104** (2008), 155–192.

[4] B. Bukh, *Non-trivial solutions to a linear equation in integers,* Acta Arithmetica **131** (2008), 51–55.

[5] M. C. Chang, *A polynomial bound in Freiman's theorem,* Duke Mathematical Journal **113** (2002), 399–419.

[6] E. Croot and O. Sisask, *A probabilistic technique for finding almost-periods of convolutions,* Geometric and Functional Analysis **20** (2010), 1367–1396.

[7] M. Elkin, *An improved construction of progression-free sets,* Israel Journal of Mathematics **184** (2011), 93–128.

[8] B. Green and T. Tao, *Freiman's theorem in finite fields via extremal set theory,* Combinatorics, Probability and Computing **18** (2009), 335–355.

[9] D. R. Heath-Brown, *Integer sets containing no arithmetic progressions,* Journal of the London Mathematical Society **35** (1987), 385–394.

[10] P. Koester, *An extension of Behrend's theorem,* Online Journal of Analytic Combinatorics **8** (2008), Art. 4, 8.

[11] Y. R. Liu and C. V. Spencer, *A generalization of Meshulam's theorem on subsets of finite abelian groups with no 3-term arithmetic progression,* Designs, Codes and Cryptography **52** (2009), 83–91.

[12] R. Meshulam, *On subsets of finite abelian groups with no 3-term arithmetic progressions,* Journal of Combinatorial Theory. Series A **71** (1995), 168–172.

[13] L. Moser, *On non-averaging sets of integers,* Canadian Journal of Mathematics **5** (1953), 245–252.

[14] R. A. Rankin, *Sets of integers containing not more than a given number of terms in arithmetic progression,* Proceedings of the Royal Society of Edinburgh **65** (1961), 332–344.

[15] K. F. Roth, *On certain sets of integers,* Journal of the London Mathematical Society **28** (1953), 104–109.

[16] I. Z. Ruzsa, *Generalized arithemtic progresions and sumsets,* Acta Mathematica Hungarica **65** (1994), 379–388.

[17] I. Z. Ruzsa, *Solving linear equations in sets of integers. I,* Acta Arithmetica **65** (1993), 259–282.

[18] R. Salem and D. C. Spencer, *On sets of integers which contain no three terms in arithmetical progression,* Proceedings of the National Academy of Sciences of the United States of America **28** (1942), 561–563.

[19] R. Salem and D. C. Spencer, *On sets which do not contain a given number of terms in arithmetical progression,* Nieuw Archief voor Wiskunde **23** (1950), 133–143.

[20] T. Sanders, *Roth's theorem in $\mathbb{Z}_4^n$,* Analysis & PDE **2** (2009), 211–234.

[21] T. Sanders, *Structure in sets with logarithmic doubling,* Canadian Mathematical Bulletin, to appear. doi : http://dx.doi.org/10.4153/CMB-2011-165-0.

[22] T. Sanders, *On the Bogolubov–Ruzsa Lemma,* Analysis & PDE **5** (2012), 627–655.

[23] T. Sanders, *On Roth's theorem on progressions,* Annals of Mathematics **174** (2011), 619–636.

[24] T. Schoen, *Near optimal bounds in Freiman's theorem,* Duke Mathematical Journal **158** (2011), 1–12.

[25] I. D. Shkredov, *On sets of large exponential sums,* Rossiĭskaya Akademiya Nauk. Izvestiya. Seriya Matematicheskaya **72** (2008), 161–182.

[26] I. D. Shkredov, *Some examples of sets of large exponential sums,* Rossiĭskaya Akademiya Nauk. Matematichesiĭ Sbornik **198** (2007), 105–140.

[27] E. Szemerédi, *On sets of integers containing no arithmetic progressions,* Acta Mathematica Hungarica **56** (1990), 155–158.

[28] T. Tao and V. Vu, *Additive Combinatorics,* Cambridge Studies in Advanced Mathematics, Vol. 105, Cambridge University Press, Cambridge, 2006.