

Invariant Equations in Many Variables

Tomasz Kościuszko

Submitted: Jun 14, 2023; Accepted: Jun 16, 2025; Published: Aug 8, 2025

© The author. Released under the CC BY license (International 4.0).

Abstract

We show that if a set does not contain any non-trivial solutions to an invariant equation of length $k \geq 4 \cdot 3^m + 2$ for some positive integer m , then its size is at most $\exp(-c \log^{1/(6+\gamma_m)} N)N$, where $\gamma_m = 2^{-m}$. We prove a lower bound of $\exp(-C \log^7(2/\alpha))N^{k-1}$ to the number of solutions of an invariant equation in $k \geq 4$ variables, contained in a set of density α . To compliment that result in the case of convex equations, we give a Behrend-type construction for the same problem with the number of solutions of a convex equation bounded above by $\exp(-c \log^2(2/\alpha))N^{k-1}$.

Mathematics Subject Classifications: 11B30, 11K70

1 Introduction

Finding structure in dense sets of integers has been a challenge to mathematical research since Van der Waerden proved his theorem on arithmetic progressions in 1927 [19]. Of particular interests have been quantitative results. We would like to have an upper-bound to the size of a set, which does not contain a certain structure. In the case of Roth's Theorem [12], we consider a set $A \subseteq \{1, 2, \dots, N\}$ which contains no non-trivial solutions to the equation

$$x + y = 2z.$$

Roth proved that for a large constant C we have

$$|A| \leq C \frac{N}{\log \log N}.$$

After many improvements over the years, a sensational result of Kelley and Meka [9] showed a near-optimal bound

$$|A| \leq \exp(-c \log^{1/12} N)N,$$

Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Umultowska 87, 61-614 Poznan, Poland (tomasz.kosciuszko@amu.edu.pl).

where c is a sufficiently small positive constant. The exponent was later improved to $1/9$ by Bloom and Sisask ([4], [5]). Other variations of this problem have been considered, for example, since Schoen and Shkredov [15] and the subsequent work of Schoen and Sisask [16] we know that longer equations like

$$x_1 + x_2 + x_3 = 3y$$

avoiding non-trivial solutions also restrict the size of the subset and even better bounds than the one from Kelley and Meka are known, namely

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

In this paper we show that the exponent $1/7$ here can be increased for similar equations with at least 14 variables, for example in the equation

$$x_1 + x_2 + \cdots + x_{13} = 13x_{14}$$

we get the exponent $2/13$. Below is a formulation of our result. By a trivial solution there, we mean one where all variables are equal.

Theorem 1. *Let $m \geq 1$, $k \geq 4 \cdot 3^m + 2$ and $A \subseteq \{1, 2, \dots, N\}$ be a set which contains no non-trivial solutions to the equation*

$$x_1 + x_2 + \cdots + x_{k-1} = (k-1)x_k.$$

Then $|A| \leq \exp(-c \log^{1/(6+\gamma_m)} N) N$, where $\gamma_m = 2^{-m}$. Here c is a small constant that depends only on the equation.

For the sake of readability, we state Theorem 1 for a specific equation of length k . Our proof can be generalized to any invariant equation, in a similar way as in Theorem 3. We say that a linear equation

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = 0$$

with coefficients $a_i \in \mathbb{Z}$ is invariant when $a_1 + a_2 + \cdots + a_k = 0$.

Bloom [3] considered the counting version of the above problem. By using his result it is possible to find an upper-bound not only if there are no non-trivial solutions, but also if their count is abnormally small.

Theorem 2. *(Bloom) Let $A \subseteq \{1, 2, \dots, N\}$ be such that $|A| = \alpha N$ and let $a_1x_1 + a_2x_2 + \cdots + a_kx_k = 0$ be an invariant equation in $k \geq 3$ variables. Then for some large constant C , which depends on the coefficients of the equation, there are at least*

$$\exp(-C\alpha^{-1/(k-2)} \log^4(2/\alpha)) N^{k-1}$$

solutions to the equation.

Theorem 2 is still the best published bound for 3-term equations, however Kelly and Meka [9] recently showed a much more efficient way of counting solutions to equations of length 3. They gave a lower bound of

$$\exp(-C \log^{12}(2/\alpha))N^2.$$

We shall also establish counting results for equations in at least four variables, for which Schoen and Sisask [16] (Theorem 1.4) only established density results. That this is possible was noted by Sanders and Prendiville [11], but the details were not provided. Here we prove such a counting result in full generality; more precisely, we prove the following theorem.

Theorem 3. *Let $k \geq 4$, $A \subseteq \{1, 2, \dots, N\}$ be a set of size αN and let $a_1x_1 + a_2x_2 + \dots + a_kx_k = 0$ be an invariant equation in k variables. Then there are at least*

$$\exp(-C \log^7(2/\alpha))N^{k-1}$$

solutions to the equation, that is tuples $(x_1, x_2, \dots, x_k) \in A^k$, for which $a_1x_1 + a_2x_2 + \dots + a_kx_k = 0$. Here C is a large constant that depends only on the coefficients of the equation.

The new bound can be used to boost results taking advantage of the Fourier Transference Principle [10]. For example, it could be applied to the result by Prendiville on solving equations in dense Sidon sets [11]. It was noted by Prendiville that a counting version of the result of Schoen and Sisask [16] yields improved bounds in his theorem. More details are given in the “Applications” section.

Finally, we give a construction which complements our Theorem 3. By generalizing [18] (Proposition 1.3) to the case of more variables, we show a lower bound similar to a well-known Behrend’s construction [1], where a set has high density, but contains only a few solutions to an invariant equation.

Theorem 4. *Let $k \geq 4$ and let c be a sufficiently small constant depending only on k . Let $\alpha \leq \exp(-1/c)$. There exist infinitely many integers $N \geq 1$ and sets $A \subseteq \{1, 2, \dots, N\}$ with $|A| \geq \alpha N$, such that A contains no more than*

$$\exp(-c \log^2(2/\alpha))N^{k-1}$$

solutions to the equation $x_1 + \dots + x_{k-1} = (k-1)x_k$.

We will prove Theorems 1 and 3 by treating A as a subset of the group $\mathbb{Z}/p\mathbb{Z}$, with p prime, instead of the interval $\{1, 2, \dots, N\}$. If we choose p (by Bertrand’s postulate) to satisfy

$$2(|a_1| + |a_2| + \dots + |a_k|)N > p > (|a_1| + |a_2| + \dots + |a_k|)N,$$

then no solutions in the integer case imply no solutions in the $\mathbb{Z}/p\mathbb{Z}$ case and therefore one version implies the other. Clearly the density of A changes by the factor of $|a_1| + |a_2| + \dots + |a_k|$ between these two setting, which can be neglected if we allow C and c to depend on the coefficients of the equation.

2 Notation

Let us fix some notation and recall a couple of well-known definitions. By c and C we mean real, positive constants, where c is sufficiently small and C is sufficiently large for all of our uses. If we wanted to be really precise, we would have to call the constants c_1, c_2, \dots and C_1, C_2, \dots in various parts of different proofs, however for simplicity we omit the indices. In the Theorems 1, 3 and 4 constants in the statements depend on the coefficients of the equation a_1, a_2, \dots, a_k , as well as the number k . It can be assumed that the constants c and C appearing in the proofs are all chosen for a fixed equation.

We work in the group $\mathbb{Z}/p\mathbb{Z}$, however most of the definitions are given for a general, finite, abelian group G of size N and then applied to $\mathbb{Z}/p\mathbb{Z}$. Let A be a subset of G . Define a normalized indicator function to be

$$\mu_A = 1_A \cdot \frac{1}{|A|},$$

where $1_A(x)$ is the function that gives 1 when $x \in A$ and 0 otherwise. Write $\mu_A(X)$ for the sum $\sum_{x \in X} \mu_A(x)$.

By the convolution of two functions $f, g : G \rightarrow \mathbb{R}$ we mean

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

We sometimes write $f^{(k)}(x)$ to mean multiple convolutions, that is

$$f^{(k)}(x) = f * f * \dots * f(x) \text{ where } f \text{ appears } k \text{ times.}$$

Let $1 \leq p < \infty$, the L_p norm of a function $f : G \rightarrow \mathbb{R}$ is defined as

$$\|f\|_p = \left(\sum_{x \in G} |f(x)|^p \right)^{1/p},$$

when $p = \infty$ we always mean $\|f\|_\infty = \max_{x \in G} |f(x)|$. For a function $f : G \rightarrow \mathbb{R}$ we define expectation as

$$\mathbb{E}_{x \in G} f(x) = \frac{1}{|G|} \sum_{x \in G} f(x).$$

Denote the group of all characters (homomorphisms) $\gamma : G \rightarrow \mathbb{C}$ as \widehat{G} . Given a function $f : G \rightarrow \mathbb{R}$ we define a Fourier coefficient at $\gamma \in \widehat{G}$ as

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

We call the function \widehat{f} the Fourier Transform of f .

3 Tools for finding Almost-Periods

A common technique in Additive Combinatorics is solving a problem in the group \mathbb{F}_p^n , before stating it for a general group or an interval of integers. The advantage of \mathbb{F}_p^n is that we can make use of subspaces, which are not found in all groups. Fortunately, Bohr sets act as approximate subspaces in any finite abelian group G . Translating the ideas from the language of subspaces to the language of Bohr sets is usually possible, although quite technical. In our work we immediately present the reasoning by using Bohr sets. The paper by Schoen and Sisask [16] contains simpler proofs of their result in the case of \mathbb{F}_p^n as well as the general proofs. A reader unfamiliar with Bohr sets, could consider reading that paper as an introduction.

We record a couple of auxiliary definitions and propositions concerning the properties of Bohr sets. For more background on Bohr sets we recommend to the reader a book by Tao and Vu [17].

Let $0 < \rho \leq 2$ and let $\Gamma \subseteq \widehat{G}$ for some finite abelian group G . The Bohr set $B = \text{Bohr}(\Gamma, \rho)$ is defined as

$$B = \{x \in G : |1 - \gamma(x)| \leq \rho \text{ for all } \gamma \in \Gamma\}.$$

We refer to ρ as the width and to $|\Gamma|$ as the rank of B . We will only consider Bohr sets of rank at least 1, in order to avoid special cases of the propositions below. This does not restrict us in any way as the whole group can be trivially represented as $G = \text{Bohr}(\{1\}, 2)$, where by 1 we mean the constant character. Note that often B does not uniquely determine Γ or ρ .

If $\delta > 0$ and $B = \text{Bohr}(\Gamma, \rho)$ we write B_δ for $B = \text{Bohr}(\Gamma, \rho\delta)$ and call it a dilate of B . A Bohr set B with rank $d > 0$ is called regular when

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

for every $|\delta| \leq 1/12d$.

Proposition 5. *Let B be a regular Bohr set of rank $d > 0$ and let $B' \subseteq B_\delta$ where $\delta \leq \epsilon/24d$, then we have*

$$\|\mu_B * \mu_{B'} - \mu_B\|_1 \leq \epsilon.$$

Proof. Using the triangle inequality we notice that

$$\|\mu_B * \mu_{B'} - \mu_B\|_1 = \frac{1}{|B|} \|1_B * \mu_{B'} - 1_B\|_1 \leq \frac{1}{|B|} (\|1_B * \mu_{B'} - 1_{B+B'}\|_1 + \|1_{B+B'} - 1_B\|_1).$$

Now, by regularity of B we obtain

$$\|1_{B+B'} - 1_B\|_1 = |(B + B') \setminus B| \leq \epsilon|B|/2.$$

Again by regularity of B we have

$$\|1_B * \mu_{B'} - 1_{B+B'}\|_1 = \sum_{x \in B+B'} 1 - \frac{1}{|B'|} 1_B * 1_{B'}(x) = |B + B'| - |B| =$$

$$= |(B + B') \setminus B| \leq \epsilon |B|/2,$$

which ends the proof. \square

We will make also use of the following three properties, for the proofs see the book by Tao and Vu [17]. Another accessible source are the lecture notes by Thomas Bloom [2].

Proposition 6. *Let B be a Bohr set. There exists $\delta \in [\frac{1}{2}, 1]$, such that B_δ is regular.*

Proposition 7. *Let B be a Bohr set of rank d and let $\delta \in [0, 1]$. Then we have*

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

Proposition 8. *Let B be a Bohr set of rank d and width ρ contained in a group G . Then we have*

$$|B| \geq (\rho/2\pi)^d |G|.$$

Here is a basic lemma, where we choose a translate of a Bohr set, on which A has high density.

Lemma 9. *Let $A \subseteq B$ with $|A| = \alpha |B|$, where B is a regular Bohr set of rank $d > 0$ and radius ρ . Let δ be a positive constant with $\delta \leq \frac{\alpha}{240d}$. There exists $x \in G$ such that $|A \cap (x + B_\delta)| \geq 0.9\alpha |B_\delta|$.*

Proof. Applying Proposition 5 to B_δ we have

$$\|\mu_B * \mu_{B_\delta} - \mu_B\|_1 \leq \alpha/10,$$

and by the triangle inequality we get

$$\begin{aligned} \alpha = \mu_B(A) &\leq \|\mu_B 1_A - (\mu_B * \mu_{B_\delta}) 1_A\|_1 + \|(\mu_B * \mu_{B_\delta}) 1_A\|_1 \\ &\leq \alpha/10 + \frac{1}{|B|} \sum_{x \in B} \mu_{B_\delta} * 1_A(x). \end{aligned}$$

Thus for some $x \in B$ we have

$$\mu_{B_\delta} * 1_A(x) \geq 0.9\alpha$$

as required. \square

We now generalize Lemma 9 to allow multiple factors δ_i and multiple coefficients a_i , for which we consider $a_i \cdot A := \{a_i \cdot a : a \in A\}$. This will be crucial in working with many variables. In this lemma we have to assume that our group is $\mathbb{Z}/p\mathbb{Z}$ for p prime. The reason is that we want to define the operation of multiplying a Bohr set by an element of the group. Let $B = \text{Bohr}(\Gamma, \rho)$ and $a \in \mathbb{Z}/p\mathbb{Z}$ be a non-zero element, we define

$$a \cdot B := \{x \in \mathbb{Z}/p\mathbb{Z} : |1 - \gamma(a^{-1}x)| \leq \rho \text{ for all } \gamma \in \Gamma\}.$$

So if $B = \text{Bohr}(\{\gamma_1, \dots, \gamma_d\}, \rho)$, then $a \cdot B = \text{Bohr}(\{\gamma_1^{a^{-1}}, \dots, \gamma_d^{a^{-1}}\}, \rho)$. This way if $x \in B$ then $ax \in a \cdot B$ and $a \cdot B$ is a Bohr set of the same rank and radius as B .

Lemma 10. Let $B \subseteq \mathbb{Z}/p\mathbb{Z}$, with p prime, be a regular Bohr set of rank $d > 0$ and radius ρ . Let $A \subseteq B$ be its subset of size $\alpha|B|$. Let a_1, a_2, \dots, a_k be integers non-divisible by p . Then there is a regular Bohr set B' , such that, for any $\delta_1, \delta_2, \dots, \delta_k \in (0, 1]$ there are sets $A_1, A_2, \dots, A_k \subseteq A - x$, where x is a translate, $a_i \cdot A_i \subseteq B'_{\delta_i}$ and either

$$|(a_i \cdot A_i) \cap B'_{\delta_i}| \geq \frac{7}{8}\alpha|B'_{\delta_i}| \text{ for all } i$$

or

$$|(a_i \cdot A_i) \cap B'_{\delta_i}| \geq (1 + 1/16k)\alpha|B'_{\delta_i}| \text{ for some } i.$$

Moreover, B' can be chosen so that its rank is d and its radius is $\rho_2 \geq \rho \frac{c\alpha}{kd}$, where c is a small constant that depends on a_1, a_2, \dots, a_k .

Proof. Let $\epsilon := \frac{1}{16k}\alpha(\Pi_j|a_j|)^{-1}/24d$, $B^i := (\Pi_{j \neq i} a_j) \cdot B_{\epsilon, \delta_i}$ and $B' := (\Pi_j a_j) \cdot B_\epsilon$. Clearly B' satisfies the conditions on the rank and the radius. Notice that it is chosen independently of the widths δ_i .

B' does not need to be regular, but by Proposition 6 there is some $\delta \in [\frac{1}{2}, 1]$ for which B'_δ is regular. Thus in the Lemma we could consider $\delta\delta_1, \delta\delta_2, \dots, \delta\delta_k$ instead of $\delta_1, \delta_2, \dots, \delta_k$ to obtain a necessarily regular Bohr set B'_δ . Because of this without loss of generality we assume that $\delta = 1$ and so B' is regular.

If we Notice, that from Proposition 1 we have

$$\|\mu_B * \mu_{B^i} - \mu_B\|_1 \leq \frac{1}{16k}\alpha.$$

Since $\mu_B(A) = \alpha$ and by the application of the triangle inequality we get

$$\begin{aligned} k\alpha &\leq \sum_{i=1}^k \mu_B(A) \leq \sum_{i=1}^k \|\mu_B 1_A - (\mu_B * \mu_{B^i}) 1_A\|_1 + \sum_{i=1}^k \|(\mu_B * \mu_{B^i}) 1_A\|_1 \\ &\leq \frac{1}{16}\alpha + \frac{1}{|B|} \sum_{i=1}^k \sum_{x \in B} \mu_{B^i} * 1_A(x). \end{aligned}$$

Thus, for some $x \in B$ the sum is at least equal to the average, so

$$\sum_{i=1}^k \mu_{B^i} * 1_A(x) \geq (k - 1/16)\alpha.$$

Set $A_i = (A - x) \cap B^i$. We clearly have $a_i \cdot A_i \subseteq a_i \cdot B^i = B'_{\delta_i}$ for all i . If $\mu_{B^i} * 1_A(x) \geq (1 + 1/16k)\alpha$ for some x , then the second conclusion holds immediately. On the other hand if $\|\mu_{B^i} * 1_A\|_\infty < (1 + 1/16k)\alpha$, then

$$\begin{aligned} \mu_{B^i} * 1_A(x) &\geq (k - 1/16)\alpha - \sum_{j \neq i} \mu_{B^j} * 1_A(x) \\ &\geq (k - 1/16)\alpha - (k - 1)(1 + 1/16k)\alpha \\ &\geq \left(1 - \frac{2}{16} + \frac{1}{16k}\right)\alpha \\ &\geq \frac{7}{8}\alpha \end{aligned}$$

and the first conclusion holds. \square

All results which use Lemma 10 will be also stated for the group $\mathbb{Z}/p\mathbb{Z}$.
Going further, one of our main tools is the Croot-Sisask lemma, here is one of its versions, coming from the paper of Schoen and Sisask [16](Theorem 2.1).

Theorem 11. (*Croot-Sisask*) Fix constants $\epsilon \in (0, 1)$, $k \in \mathbb{N}$ and $p \geq 2$. Let A, L, S be subsets of a finite abelian group and suppose that $|A + S| \leq K|A|$. There exists a set $T \subseteq S$ of size at least $|T| \geq 0.99K^{-Cpk^2/\epsilon^2}|S|$, such that for every $t \in kT - kT$ we have

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

The set $kT - kT$ is referred to as Almost Periods of $1_A * 1_L$, because this function does not change by much when shifted by any one element of $kT - kT$.
Next, we show a corollary to the Croot-Sisask Lemma that will enable us to consider multiple sets instead of just two. In the proof we take advantage of Young's inequality, which we state here.

Theorem 12. (*Young's convolution inequality - special case*) Let $f, g : G \rightarrow \mathbb{R}$ be functions and let $q \geq 1$, then we have

$$\|f * g\|_q \leq \|f\|_q \|g\|_1.$$

Corollary 13. Fix constants $\epsilon \in (0, 1)$ and $k \in \mathbb{N}$. Let $A_1, A_2, \dots, A_n, M, L, S$ be subsets of a finite abelian group. Suppose that $|A_1 + S| \leq K|A_1|$ and that $\eta = |M|/|L| \leq 1$. Then we can find a set $T \subseteq S$ such that

$$|T| \geq \exp(-Ck^2\epsilon^{-2} \log(2/\eta) \log(2K))|S|$$

and for every $t \in kT - kT$

$$\|1_{A_1} * \dots * 1_{A_n} * 1_M * 1_L(\cdot + t) - 1_{A_1} * \dots * 1_{A_n} * 1_M * 1_L\|_\infty \leq \epsilon |A_1| \dots |A_n| |M|.$$

Proof. Let $f = 1_{A_2} * 1_{A_3} * \dots * 1_{A_n}$. By writing the definition of convolution and using Holder's inequality we see that for any $t \in G$ and for any $p, q \geq 1$ such that $\frac{1}{p} + \frac{1}{q} = 1$ we have

$$\|1_{A_1} * 1_M * f * 1_L(\cdot + t) - 1_{A_1} * 1_M * f * 1_L\|_\infty \leq \|1_{A_1} * 1_M(\cdot + t) - 1_{A_1} * 1_M\|_q \|f * 1_L\|_p.$$

Let us set $p = \log(2/\eta)$. Using Theorem 11 with $\epsilon/3$ we get a set T of desired size such that for any $t \in T$ there is

$$\begin{aligned} \|1_{A_1} * 1_M(\cdot + t) - 1_{A_1} * 1_M\|_q \|f * 1_L\|_p &\leq \frac{1}{3} \epsilon |A_1| |M|^{1/q} \|f * 1_L\|_p \\ &\leq \frac{1}{3} \epsilon |A_1| |A_2| \dots |A_n| |M|^{1/q} |L|^{1/p} \\ &= \frac{1}{3} \epsilon |A_1| |A_2| \dots |A_n| |M| (|L|/|M|)^{1/p}, \end{aligned}$$

where the second inequality follows by applying Theorem 12. The Corollary is proved because for our choice of p we have

$$\frac{1}{3}(|L|/|M|)^{1/p} = \frac{1}{3}(1/\eta)^{1/\log(2/\eta)} \leq 1.$$

□

Let us now state the version of the Croot-Sisask lemma that will allow us to find almost periods which form a large Bohr set. This is a corollary of Theorem 5.4 from the paper of Schoen and Sisask [16] with arbitrary number of sets.

Theorem 14. *Fix $\epsilon \in (0, 1)$. Let $A_1, A_2, \dots, A_n, M, L$ be subsets of G . Let B be a regular Bohr set of rank $d > 0$ and width ρ . Suppose that there exists $S \subseteq B$, such that $|A_1 + S| \leq K|A_1|$. Denote the density of S in B as σ . Moreover, suppose that $\sigma > 0$ and $\eta = |M|/|L| \leq 1$. Then there exists a regular Bohr set $B' \subset B$ with the property that for every $t \in B'$ we have*

$$\|1_{A_1} * \dots * 1_{A_n} * 1_L * 1_M(\cdot + t) - 1_{A_1} * \dots * 1_{A_n} * 1_L * 1_M\|_\infty \leq \epsilon |A_1| \dots |A_n| |M|.$$

Furthermore, B' can be taken to have width at least $\rho \epsilon \eta^{1/2} / (d^2 d')$ and rank at most $d + d'$ where

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

Proof. We apply Theorem 5.4 from [16] to the sets A_1, M, L to obtain a regular Bohr set B' with appropriate rank and width, such that for every $t \in B'$ we have

$$\|1_{A_1} * 1_L * 1_M(\cdot + t) - 1_{A_1} * 1_L * 1_M\|_\infty \leq \epsilon |A_1| |M|.$$

From here we can easily deduce the desired inequality because the left-hand side can be rewritten as

$$\begin{aligned} & \| (1_{A_1} * 1_L * 1_M(\cdot + t) - 1_{A_1} * 1_L * 1_M(\cdot)) * 1_{A_2} * \dots * 1_{A_n} \|_\infty \\ & \leq \|1_{A_1} * 1_L * 1_M(\cdot + t) - 1_{A_1} * 1_L * 1_M\|_\infty |A_2| \dots |A_n|. \end{aligned}$$

□

4 Improving the bound for many variables

Theorem 3 and the analogous result of Schoen and Sisask [16] give the relevant constant 7 in the bound (for example $e^{-C \log^7(2/\alpha)} N^{k-1}$ in Theorem 3). The Behrend-type construction in Theorem 4 shows that this cannot be improved to less than 2 in the case of convex equations. In this section we show how to bring the constant down almost to 6, provided the considered equation is long enough. By the end of this section this is summed up as the proof of Theorem 1. The main idea is Theorem 15 below, which allows us to find a large Bohr set within $wA - wA$ for some w . That could be looked at as a variation of the Bogolyubov-Ruzsa lemma. After that a density increment can be obtained quite easily. The approach builds on an idea by Konyagin. To our knowledge it was not published,

but is mentioned by Sanders in his survey [14].

He observed that when applying Theorem 14 one can save on the K constant by choosing S well: suppose that for some sets A and X and a positive integer k we have $|A + kX| \leq K|A|$. Then by the pigeonhole principle there exists $l < k$ for which $|A + lX| \leq K^{1/k}|A|$. Below we attempt to exploit this observation as much as possible. We apply Theorem 14 multiple times, which allows us to decrease the set of almost periods with each step gently instead of getting a set of almost periods in one step and decreasing it dramatically.

Theorem 15. *Let $A \subseteq B$ with $|A| = \alpha|B|$ where B is a regular Bohr set of rank $d > 0$ and width ρ contained in a finite abelian group G . Let $m \geq 1$. There exists a Bohr set $\tilde{B} \subseteq 2 \cdot 3^m A - 2 \cdot 3^m A$ of rank $d + d'$ and width $\rho_{\tilde{B}}$. Moreover, \tilde{B} can be chosen so that*

$$d' \leq C \log^{3+\gamma}(2/\alpha) + Cm \log^3(2/\alpha),$$

where $\gamma = 2^{-m}$ and

$$\rho_{\tilde{B}} \geq \rho \frac{c\alpha^{7/2}}{\log(2/\alpha)md^5d'}.$$

Proof. The plan is to apply Theorem 14 on inductively constructed sets A'_m and T_m . The resulting Bohr set will have significantly smaller rank than the one we get by naively applying Theorem 14 to the set A .

Without loss of generality assume $0 \in A$. Define constants $k_0, k_1, k_2, \dots, k_m$ to be

$$k_i := \lceil \log^{1-2^{-i}}(2/\alpha) \rceil,$$

for $0 \leq i \leq m$. Notice that $k_0 = 1$. Let $k = 2(k_0 + k_1 + \dots + k_m)$, then $k \ll m \log(2/\alpha)$. We choose $\frac{\alpha}{480d} \leq \delta \leq \frac{\alpha}{240d}$ to get regular Bohr set B_δ such that $|B_{1+2\delta}| \leq \frac{3}{2}|B|$. By Lemma 9 there exists x such that $A'_0 := A \cap (x + B_\delta)$ has density at least 0.9α within $x + B_\delta$. Similarly, we choose $\frac{\alpha^2}{Ckd^2} \leq \frac{\alpha\delta}{480kd} \leq \nu \leq \frac{\alpha\delta}{240kd}$ to get regular Bohr set $B_{\delta\nu}$ such that $|B_{\delta(1+2k\nu)}| \leq \frac{3}{2}|B_\delta|$. This implies $1 + \delta(1 + k\nu) \leq 1 + 2\delta$, which we use later for proving (6). Again, by Lemma 9 there exists x' such that $T_0 := A \cap (x' + B_{\delta\nu})$ has density at least 0.9α within $x' + B_{\delta\nu}$. We see that

$$|A + A'_0| \leq |B + (x + B_\delta)| \leq |B_{1+\delta}| \leq \frac{3}{2}|B| \leq \frac{2}{\alpha}|A|$$

and so

$$\eta := |A + A'_0|/|A| \leq \frac{2}{\alpha}.$$

Similarly we have

$$|A'_0 + T_0 - T_0| \leq |B_{\delta(1+2\nu)}| \leq \frac{3}{2}|B_\delta| \leq \frac{3}{2 \cdot 0.9 \cdot \alpha}|A'_0| \leq \frac{2}{\alpha}|A'_0|.$$

We will show how to inductively construct sets A'_i and T_i , for which the following conditions hold. As the base case we already have the sets A_0 and T_0 which satisfy (6) and (7) ($i = 1$ is the first step of induction).

$$T_i \subseteq T_{i-1} \subseteq B_{\delta\nu} \tag{4}$$

$$A'_{i-1} \subseteq A'_i \subseteq B_{\delta(1+k\nu)} \quad (5)$$

$$|A + A'_{i-1}| \leq \frac{2}{\alpha}|A| \quad (6)$$

$$|A'_{i-1} + T_{i-1} - T_{i-1}| \leq \left(\frac{2}{\alpha}\right)^{1/k_{i-1}} |A'_{i-1}| \quad (7)$$

$$|T_i| \geq \exp(-Ck_i^2/k_{i-1} \log^2(2/\alpha)) |T_{i-1}| \quad (8)$$

$$k_i T_i - k_i T_i \subseteq A + A'_{i-1} - A - A'_{i-1} \quad (9)$$

We apply Corollary 13 to the sets A'_{i-1} , A , $-(A + A'_{i-1})$ and T_{i-1} in place of (A_1, M, L, S) with $\epsilon = 1/2$ and the chosen k_i to obtain a set $T_i \subseteq T_{i-1}$ where condition (8) holds such that for every $t \in k_i T_i - k_i T_i$ we have

$$|1_A * 1_{A'_{i-1}} * 1_{-(A+A'_{i-1})}(t) - 1_A * 1_{A'_{i-1}} * 1_{-(A+A'_{i-1})}(0)| \leq \frac{1}{2} |A| |A'_{i-1}|.$$

Notice that $1_A * 1_{A'_{i-1}} * 1_{-(A+A'_{i-1})}(0) = |A| |A'_{i-1}|$, thus by the triangle inequality

$$1_A * 1_{A'_{i-1}} * 1_{-(A+A'_{i-1})}(t) \geq \frac{1}{2} |A| |A'_{i-1}| > 0$$

and so (9) holds. We also have by (4), (5) and the choice of ν that

$$\begin{aligned} |A'_{i-1} + k_i(T_i - T_i)| &\leq |B_{\delta(1+k\nu)} + k_i(T_0 - T_0)| \leq |B_{\delta(1+k\nu)} + B_{2k_i\delta\nu}| \\ &\leq |B_{\delta(1+2k\nu)}| \leq \frac{3}{2} |B_\delta| \leq \frac{2}{\alpha} |A_0| \leq \frac{2}{\alpha} |A'_{i-1}|. \end{aligned}$$

Here comes the insight by Konyagin. Since by k_i times adding $T_i - T_i$ we increase A'_{i-1} by the factor of at most $\frac{2}{\alpha}$, there must be an $0 \leq l_i < k_i$ such that

$$|A'_{i-1} + l_i(T_i - T_i) + (T_i - T_i)| \leq \left(\frac{2}{\alpha}\right)^{1/k_i} |A'_{i-1}| \leq \left(\frac{2}{\alpha}\right)^{1/k_i} |A'_{i-1} + l_i(T_i - T_i)|.$$

Define $A'_i := A'_{i-1} + l_i(T_i - T_i)$ so that (7) is satisfied. Moreover, the first part of (5) holds trivially and the second part is true because

$$A'_i = A'_0 + l_1(T_1 - T_1) + \dots + l_i(T_i - T_i) \subseteq A'_0 + k(T_0 - T_0) \subseteq B_{\delta(1+k\nu)}.$$

Let us also notice that

$$|A + A'_i| \leq |B_{1+\delta(1+k\nu)}| \leq |B_{1+2\delta}| \leq \frac{3}{2} |B| \leq \frac{2}{\alpha} |A|.$$

Therefore (6) holds and the inductive step is complete.

We now calculate the closed form of the recursive relation (9), making use of the fact that we defined A'_i so that

$$A'_i = A'_{i-1} + l_i(T_i - T_i) \subseteq A'_{i-1} + k_i(T_i - T_i) \subseteq 2A'_{i-1} + A - A - A'_{i-1}.$$

By simple induction we can show that $A'_i \subseteq 3^i A - (3^i - 1)A$. That is certainly true for $i = 0$ and if $i > 0$ then

$$\begin{aligned} A'_i &\subseteq 2A'_{i-1} + A - A - A'_{i-1} \\ &\subseteq 2 \cdot 3^{i-1}A - 2 \cdot (3^{i-1} - 1)A + A - A - 3^{i-1}A + (3^{i-1} - 1)A \\ &\subseteq 3^i A - (3^i - 1)A. \end{aligned}$$

Iterate the above inductive procedure m times to obtain the sets T_1, T_2, \dots, T_m . For every $i \geq 1$ we have

$$\begin{aligned} \frac{k_i^2}{k_{i-1}} &= \frac{[\log^{1-2^{-i}}(2/\alpha)]^2}{[\log^{1-2 \cdot 2^{-i}}(2/\alpha)]} \leq \frac{(\log^{1-2^{-i}}(2/\alpha) + 1)^2}{\log^{1-2 \cdot 2^{-i}}(2/\alpha)} \\ &= \log(2/\alpha) + 2 \log^{2^{-i}}(2/\alpha) + \log^{2 \cdot 2^{-i}-1}(2/\alpha) \\ &\leq 4 \log(2/\alpha). \end{aligned}$$

In the last inequality we assume that $\log(2/\alpha) \geq 1$. This is true if $\alpha \leq 1/2$. We can make that assumption because the theorem for larger values of α follows from the case $\alpha \leq 1/2$ by a change of a constant.

We can thus give the lower bound

$$\begin{aligned} |T_m| &\geq \exp((-k_1^2 - k_2^2/k_1 - k_3^2/k_2 - \dots - k_m^2/k_{m-1})(C \log^2(2/\alpha)))|T_0| \\ &\geq \exp(-Cm \log^3(2/\alpha))|T_0|. \end{aligned}$$

Let us apply Theorem 14 to sets $A'_m, A, -(A + A'_m), T_m, B_{\delta\nu}$ in place of (A_1, M, L, S, B) and with $\epsilon = 1/2$, making use of the properties (6) and (7). This way we find a Bohr set \tilde{B} such that for every $t \in \tilde{B}$ we have

$$|1_{A'_m} * 1_{-(A+A'_m)} * 1_A(t) - |A'_m||A|| \leq |A'_m||A|/2.$$

Here we just considered the convolution from Theorem 14 at points t and 0 . We deduce that the value of the convolution above can never be 0 and so $t \in A + A'_m - (A + A'_m)$. The set \tilde{B} thus satisfies the following properties.

$$\begin{aligned} \tilde{B} &\subseteq A + A'_m - (A + A'_m) \subseteq 2 \cdot 3^m A - 2 \cdot 3^m A, \\ \dim \tilde{B} = d + d' &\leq d + C \log^4(2/\alpha)/k_m + C \log(1/\sigma), \\ \sigma = |T_m|/|B_{\delta\nu}| &\geq \exp(-Cm \log^3(2/\alpha))|T_0|/|B_{\delta\nu}| \\ &\geq \exp(-Cm \log^3(2/\alpha)) \cdot 0.9\alpha. \end{aligned}$$

We notice that since $k_m \gg \log^{1-2^{-m}}(2/\alpha)$, by setting $\gamma = 2^{-m}$ we have

$$d' \ll \log^{3+\gamma}(2/\alpha) + m \log^3(2/\alpha),$$

moreover

$$\rho_{\tilde{B}} = \rho_{\delta\nu} \frac{(\alpha/2)^{1/2}}{2d^2 d'} \geq \rho \frac{c\alpha^{7/2}}{kd^5 d'} \geq \frac{c\alpha^{7/2}}{\log(2/\alpha)md^5 d'},$$

which are the desired bounds. □

Notice that Theorem 15 works also when A is contained in a translate of a Bohr set $g + B$, for some $g \in G$. To see that it is enough to consider $A - g \subseteq B$.

The corollary we prove next shows that a Bohr set can be found also in a translate of a sumset $t + (4 \cdot 3^m)A$ as well as in $2 \cdot 3^m A - 2 \cdot 3^m A$.

The strategy is simple and used frequently - for example a very similar argument is presented in [15]. If A was symmetric the conclusion of Corollary 16 would be trivial as $2 \cdot 3^m A + 2 \cdot 3^m A = 2 \cdot 3^m A - 2 \cdot 3^m A$.

We search for a subset of A , which is symmetric around some point x . Because x is not necessarily 0 there is a shift we have to take into account. We cannot quite maintain the density of α in the subset, but $\alpha^2/2$ is shown to be possible with an averaging argument. It is worth mentioning that if we wanted to deal with more general equations and not only $x_1 + x_2 + \dots + x_{k-1} = (k-1)x_k$ we could modify Corollary 16 to take into account coefficients other than 1 and -1 by considering the intersection $(x + a_1 \cdot A) \cap (x + a_2 \cdot A) \cap \dots \cap (x + a_k \cdot A)$ instead of $A \cap (A - x)$.

Corollary 16. *Let $A \subseteq B$ with $|A| = \alpha|B|$ where B is a regular Bohr set of rank $d > 0$ and width ρ contained in a finite abelian group G . Let $m \geq 1$ and $w \geq 2 \cdot 3^m$. There exists a Bohr set $\tilde{B} \subseteq (2w)A - wx$ of rank $d + d'$ and width $\rho_{\tilde{B}}$, where $x \in B_4$. Moreover, \tilde{B} can be chosen so that*

$$d' \leq C \log^{3+\gamma}(2/\alpha) + Cm \log^3(2/\alpha),$$

where $\gamma = 2^{-m}$ and

$$\rho_{\tilde{B}} \geq \rho \frac{c\alpha^7}{\log(2/\alpha)md^6d'}.$$

Proof. Let us choose $\frac{1}{Cd} < \delta < 1$, so that $|B_{1+\delta}| \leq 1.01|B|$. By an averaging argument, we find a translate of B_δ , in which A is dense. Specifically we write

$$\sum_{t \in B_{1+\delta}} |A \cap (t + B_\delta)| \geq |A||B_\delta|.$$

Thus for some $t \in B_{1+\delta}$ we have

$$|A \cap (t + B_\delta)| \geq \frac{|A|}{|B_{1+\delta}|} |B_\delta| \geq \frac{|A|}{1.01|B|} |B_\delta| \geq 0.99\alpha |B_\delta|.$$

Denote $A' := A \cap (t + B_\delta)$, then $A + A' \subseteq t + B_{1+\delta}$ and

$$\sum_{x \in t+B_{1+\delta}} 1_A * 1_{A'}(x) = \sum_{x \in A+A'} |A \cap (x - A')| = |A||A'|.$$

Thus we know that for some $x \in t + B_{1+\delta} \subseteq B_4$ we have

$$|A \cap (x - A')| \geq |A||A'|/|B_{1+\delta}| \geq \frac{1}{2}\alpha^2 |B_\delta|.$$

Define $A^* := A \cap (x - A')$, clearly $A^* \in x - t + B_\delta$, moreover

$$wA^* - wA^* \subseteq wA^* + wA' - wx.$$

By Theorem 15 applied to A^* and $x - t + B_\delta$ we find a Bohr set

$$T \subseteq wA^* - wA^* \subseteq (2w)A - wx$$

of the desired width and rank. Notice that width changes by additional factor of d comparing to Theorem 15 because of the factor δ and since relative density was α^2 , now the term α^7 appears. The rank changes only by a constant as the density is now $\frac{1}{2}\alpha^2$. \square

We now show how to use the Bohr set from Corollary 16 to obtain a density increment for solution free sets. The strategy is very similar to the one suggested by Schoen and Shkredov [15]: we observe that approximately half of the translates of the obtained Bohr set cannot intersect A , as this would lead to a non-trivial solution. By an averaging argument, A must have higher density in the remaining translates.

Lemma 17. *Let $m \geq 1$, $k \geq 4 \cdot 3^m + 2$ and p be a prime. Let $A \subseteq B \subseteq \mathbb{Z}/p\mathbb{Z}$, where $|A| = \alpha|B|$ and B is a Bohr set of rank $d > 0$ and width ρ with $|B| \geq \alpha^{-1} \left(\frac{Cd^2}{\alpha} \right)^{3d}$. Suppose that A does not contain any non-trivial solutions to the equation*

$$x_1 + x_2 + \cdots + x_{k-1} = (k-1)x_k.$$

Then, there is a Bohr set \tilde{B} of rank $d + d'$ and radius $\rho_{\tilde{B}}$, such that for some y we have $|\tilde{B} \cap (A - y)| \geq 1.01\alpha|\tilde{B}|$. It is possible to choose it in such a way that

$$d' \leq C \log^{3+2^{-m}}(2/\alpha)$$

and

$$\rho_{\tilde{B}} \geq \rho \frac{c\alpha^7}{\log(2/\alpha)d^6d'}.$$

Here the constants c and C depend on m .

Proof. Choose $\delta = \frac{1}{12 \cdot 100 \cdot 5k \cdot d} \geq \frac{1}{Cd}$. Then by the definition of regularity, any regular Bohr set B' of rank at most d satisfies

$$|B'_{1+5k\delta}| \leq 1.01|B'|.$$

We apply Lemma 10 to obtain a regular Bohr set B' of rank d and radius $\rho \geq \frac{c\alpha}{d}\rho$ and sets $D_1, D_2, D_3 \subseteq A - t$, such that $(k-1) \cdot D_1, D_2, D_3$ have densities at least $\frac{7}{8}\alpha$ inside B', B', B'_δ , or there is a density increment $1 + 1/48$ on one of these sets. We would like to have $D_1 \cup D_2$ disjoint from D_3 so we adjust the sets slightly. Let us select arbitrarily $A_3 \subseteq D_3$ so that the density of A_3 in B'_δ is between $\frac{\alpha}{100}$ and $\frac{\alpha}{200}$. Now defining $A_1 := D_1 \setminus A_3$ and $A_2 := D_2 \setminus A_3$ we have the desired property and moreover the densities of $(k-1) \cdot A_1$ and A_2 are still at least $\frac{69}{80}\alpha$ inside B' . Because our equation is translation-invariant and

$A_1, A_2, A_3 \subseteq A - t$ we have no solutions to our equation in the set $A_1 \cup A_2 \cup A_3$. We can require that $|A_3| \geq 1$ because by our assumption on the size of B we have

$$|A_3| \geq \frac{1}{200} \alpha |B_\delta| \geq \frac{7}{8} \alpha \left(\frac{\alpha}{Cd^2} \right)^{3d} |B| \geq 1.$$

Set $w = \left\lfloor \frac{k-2}{2} \right\rfloor$. This way we have $w \geq 2 \cdot 3^m$. We initially assume that k is even and the floor function is unnecessary, which gives $2w+1 = k-1$. By Corollary 16 we find a Bohr set T of the required width and rank, such that $T \subseteq (2w)A_3 - wx$ and $x \in B'_{5\delta}$ (notice that we allow C to depend on m).

Suppose that $b \in A_1$ and $a \in A_2$. Then we must crucially have

$$(2w+1)b - a \notin T + wx$$

as otherwise we would have $(2w+1)b - a \in (2w)A_3$ and that would mean a non-trivial solution to the equation

$$x_1 + x_2 + \cdots + x_{2w+1} = (2w+1)x_{2w+2},$$

where $x_1, x_2, \dots, x_{2w} \in A_3; x_{2w+1} = a$ and $x_{2w+2} = b$. Because $a, b \notin A_3$ we such solution is non-trivial.

Consider a larger Bohr set $B^* = B'_{1+2w\delta}$, we have $|B^*| \leq |B'_{1+2k\delta}| \leq 1.01|B'|$. Thus $(k-1) \cdot A_1, A_2$ have densities at least 0.8α inside $B^* - wx$ as it contains B' .

At this point let us remark what happens if k is odd. Let z be an arbitrary element of $A \cap B'_\delta$. Then instead of $(2w+1)b - a \notin T + wx$ we assert that $(2w+2)b - a \notin T + wx + z$, thus adding one extra variable to our equation, which we set immediately to z . If we choose $B^{**} = B'_{1+5w\delta}$, we still have $B' \subseteq B^{**} + (w+1)x$ and the rest of the argument remains the same (with B^{**} instead of B^*).

By the above observation about non-inclusion we notice that for any $y \in G$ either $(y - T_{1/2}) \cap A_2$ or $(y + T_{1/2} - wx) \cap ((k-1) \cdot A_1)$ must be empty. Otherwise we have found $b \in A_1, a \in A_2$ where

$$(2w+1)b - a = (k-1)b - a \in T + wx,$$

which is a contradiction. Summing over all $y \in B^*$ we have

$$1.6\alpha|B^*||T_{1/2}| \leq \sum_{y \in B^*} |(y - T_{1/2}) \cap A_2| + |(y + T_{1/2} + wx) \cap ((k-1) \cdot A_1)|,$$

because every element of $A_2 \cap B'$ and $((k-1) \cdot A_1) \cap B'$ appears exactly $|T_{1/2}|$ times. Indeed, because $T \subseteq (2w)A_3 + wx$ we have

$$y + T_{1/2} + wx \subseteq B' + T + wx \subseteq B' + (2w)A_3 \subseteq B'_{1+2w\delta} \subseteq B^*$$

and for the other term

$$y - T_{1/2} \subseteq B' + B'_{w\delta} \subseteq B'_{1+w\delta} \subseteq B^*.$$

Because one element in the sum is always equal to 0 we must have some $y \in B^*$ for which

$$1.6\alpha|T_{1/2}| \leq |(y - T_{1/2}) \cap A_2|$$

or

$$1.6\alpha|T_{1/2}| \leq |(y + T_{1/2} - wx) \cap ((k - 1) \cdot A_1)|.$$

That is a density increment on a translate of $T_{1/2}$. In the second case we have to multiply the set of characters of $T_{1/2}$ by $k - 1$ or -1 we obtain a density increment of 1.6 on the resulting Bohr set \tilde{B} . \square

We are now in position to prove Theorem 1.

Proof. Let us pick a prime $kN < p < 2kN$. Let $A^{(0)} = A$ and $B^{(0)} = \text{Bohr}(\{1\}, 2) = \mathbb{Z}/p\mathbb{Z}$. Define $\alpha := \frac{|A|}{p}$. We iterate Lemma 17 on these sets, obtaining $(A^{(1)}, B^{(1)})$, $(A^{(2)}, B^{(2)})$, \dots . For each $i \geq 1$ we have $A^{(i)} = (A^{(i-1)} + t_i) \cap B^{(i)}$, where t_i is some element of $\mathbb{Z}/p\mathbb{Z}$. As a crucial consequence of Lemma 17 the density increases by at least a factor of 1.01 with each step. We know that after, say, s steps it is no longer possible. That is because the density of $A^{(i)}$ cannot exceed 1. Clearly

$$s \leq C \log(2/\alpha),$$

where the constant C depends on m . We easily calculate that

$$d_s \leq C \log^{4+\gamma_m}(2/\alpha),$$

$$\rho_s \geq (c\alpha)^{Cs}.$$

The only reason for density increment not possible is that $|B^{(s)}| < \alpha^{-1} \left(\frac{Cd_s^2}{\alpha} \right)^{3d_s}$. On the other hand we can lower-bound the size of $B^{(s)}$ by Proposition 3. Comparing the lower-bound and the upper-bound we have

$$(\rho_s/4)^{3d_s} p \leq \alpha^{-1} \left(\frac{Cd_s^2}{\alpha} \right)^{3d_s},$$

which implies

$$\log(p) \leq 4d_s \log \left(\frac{Cd_s^2}{\alpha\rho_s} \right).$$

Substituting the bounds for d_s and ρ_s that is equivalent (again up to a constant) to

$$\log(p) \leq C \log^{6+\gamma_m}(2/\alpha).$$

Rearranging we obtain

$$\alpha \leq e^{-c \log^{1/(6+\gamma_m)} p}$$

and using the fact that $kN < p < 2kN$, where we treat $2k$ as a constant we have

$$|A| \leq e^{-c \log^{1/(6+\gamma_m)} N} N. \quad \square$$

5 Counting solutions to invariant equations

Our next result is Theorem 3 - a counting version of the Theorem of Schoen and Sisask [16]. In the proof of Theorem 3 we will follow a classical paradigm of finding density increments. The main tool is the Croot-Sisask lemma, more precisely its version for Bohr sets proved by means of the Chang-Sanders lemma. Similarly as in [16], we combine this powerful result with the fact, that for Bohr sets, almost-periods of convolutions and density increments are very closely related. That is depicted by the following lemma. In the applications β will be typically some multiple of $\frac{1}{\alpha}$, for example $\frac{3}{5\alpha}$ and B a Bohr set.

Lemma 18. *Let $\epsilon > 0$, $f : G \rightarrow \mathbb{R}$ and let $A \subseteq G$. Suppose that B is a set symmetric around 0, such that for every $t \in B$*

$$\|f * 1_A(\cdot + t) - f * 1_A\|_\infty \leq \epsilon \text{ holds.}$$

*Further assume that $\|f\|_1 \leq \beta$ where $\beta > 0$ and $f * 1_A(0) \geq 1 - \epsilon$. Then there exists a translate of A (say $x + A$), such that $B \cap (x + A)$ has density at least $\frac{1}{\beta}(1 - 2\epsilon)$ inside B .*

Proof. We notice that since $B = -B$, we have

$$\begin{aligned} \|f * 1_A * \mu_B - f * 1_A\|_\infty &= \left\| \sum_{t \in -B} \left(f * 1_A(\cdot - t) \right) \cdot \mu_B(t) - f * 1_A \right\|_\infty \\ &\leq \sum_{t \in B} \|f * 1_A(\cdot + t) - f * 1_A\|_\infty \cdot \mu_B(t) \\ &\leq \epsilon \end{aligned}$$

By the triangle inequality it follows that $f * 1_A * \mu_B(0) \geq 1 - 2\epsilon$. We now notice that

$$\beta \|1_A * \mu_B\|_\infty \geq \|f\|_1 \|1_A * \mu_B\|_\infty \geq f * 1_A * \mu_B(0) \geq 1 - 2\epsilon.$$

Therefore, for some x we have $1_A * \mu_B(x) \geq \frac{1}{\beta}(1 - 2\epsilon)$ and we have proved the result as $1_A * \mu_B(x) = \frac{1}{|B|} |(x + A) \cap B|$. \square

So far we have shown in Lemma 18, that a large Bohr set of almost periods lets us find a density increment inside of this Bohr set (upon translating the original set). We also know how to find such Bohr set using Theorem 14. It remains to show how to proceed so that the assumptions of Theorem 14 are satisfied. This will require some non-trivial manipulations on Bohr sets, Lemma 10 will be key to keeping our equation under control with more variables. In the next lemma we prove a density increment on a Bohr set with rank and width slightly smaller than the initial one. A new idea here is applying Theorem 14 to the set of Popular sums, as suggested by Sanders and Prendiville [11].

Lemma 19. *Let $B \subseteq \mathbb{Z}/p\mathbb{Z}$, with p prime, be a regular Bohr set of rank $d > 0$ and radius ρ and let $A \subseteq B$ be its subset of size $\alpha|B|$. Suppose that non-zero numbers a_1, a_2, \dots, a_k are such that the sum of their absolute values is smaller than p . Let*

$$a_1x_1 + a_2x_2 + \dots + a_kx_k = 0$$

be an invariant equation in $k \geq 4$ variables and suppose that the number of solutions to the equation in A does not exceed

$$\exp(-Cd(\log(d/\alpha)))|A|^{k-1}.$$

Then we can find a regular Bohr set B^* of rank $d + d'$ and radius ρ_2 , such that for some x we have $B^* \cap (A - x) \geq (1 + 1/16k)\alpha|B^*|$. Moreover, B^* can be chosen so that

$$d' \leq C \log^4(2/\alpha)$$

and

$$\rho_2 \geq c\rho\alpha^{3/2}/(d^5d'),$$

where the constants C and c depend on the equation.

Proof. We will set up the proof by using Lemma 10 with a_i - the coefficients of the equation. Let B' be the Bohr set defined at the beginning of the proof of the Lemma, explicitly $B' := (\Pi_j a_j) B_\epsilon$ for $\epsilon := \frac{1}{16k}\alpha(\Pi_j |a_j|)^{-1}/24d$. By Proposition 2 it is possible to choose $\frac{1}{Cd} \leq \delta \leq 1$ so that $|B'_{1+(k-3)\delta}| \leq 1.01|B'|$ and B'_δ is regular. We are ready to use Lemma 10, specifying $\delta_1 = \delta_3 = 1$ and $\delta_2 = \delta_4 = \delta_5 = \dots = \delta_k = \delta$. It gives us sets $A_1, A_2, \dots, A_k \subseteq A - x$ such that $a_i \cdot A_i \subseteq B'_{\delta_i}$ of appropriate density. The translate x does not matter as if A is free from solutions then $A - x$ is free from solutions as well. If the second conclusion of the is true, that is for some i there is $|(a_i \cdot A_i) \cap B'_{\delta_i}| \geq (1 + 1/16k)\alpha|B'_{\delta_i}|$ we immediately finish the proof, as we have the desired density increment with $B^* = B'_{\delta_i}$. Otherwise we continue the proof, keeping the first conclusion. We now define a set of Popular sums P . Consider the function

$$f(x) = 1_{a_3 \cdot A_3} * 1_{a_4 \cdot A_4} * \dots * 1_{a_k \cdot A_k}(x).$$

We see that

$$\text{supp } f = a_3 \cdot A_3 + a_4 \cdot A_4 + \dots + a_k \cdot A_k \subseteq B' + (k - 3)B'_\delta \subseteq B'_{1+(k-3)\delta}.$$

We fix a threshold to be

$$Q := \frac{\alpha}{8}|A_4||A_5| \dots |A_k|$$

and finally define $P \subseteq B'_{1+(k-3)\delta}$ as

$$P := \{x \in B'_{1+(k-3)\delta} : f(x) \geq Q\}.$$

Notice that in the definition of Q we do not have the $|A_3|$ term, because instead we wrote $\frac{\alpha}{8}$, which is proportional to the density of A_3 in $B'_{1+(k-3)\delta}$. We will consider two cases, depending on the size of P .

Case 1 ($|P| \geq |B'_{1+(k-3)\delta}|/2$): We will apply Theorem 14 to the sets, $M := a_1 \cdot A_1$, $A := a_2 \cdot A_2$ and $L = P^c = B'_{1+(k-3)\delta} \setminus P$. We define S to be $a_2 \cdot B'_{\delta_\nu}$ where $\nu := 1/Cd$, to

get a regular Bohr set with radius at least ρ/Cd^3 , such that $|B'_{\delta(1+\nu)}| \leq 2|B'_\delta|$. We have to verify the assumptions of Theorem 14, let us start by calculating

$$|a_2 \cdot A_2 + S| \leq |B'_{\delta(1+\nu)}| \leq 2|B'_\delta| \leq 2 \cdot \frac{8}{7\alpha} |A_2| = \frac{16}{7\alpha} |a_2 \cdot A_2|,$$

and so $K = \frac{16}{7\alpha}$ is sufficient. To calculate η , let us see that

$$|L| \leq (1 - 1/2)|B'_{1+(k-3)\delta}| \leq 1.01 \cdot |B'|/2 \leq 1.01 \cdot \frac{1}{2} \cdot \frac{8}{7\alpha} |a_1 \cdot A_1| \leq \frac{3}{5\alpha} |a_1 \cdot A_1|,$$

so $\eta \geq \alpha$.

Therefore from Theorem 14, we get a Bohr set B^* , such that for every $t \in B^*$ we have

$$\|1_{a_1 \cdot A_1} * 1_{a_2 \cdot A_2} * 1_L(\cdot + t) - 1_{a_1 \cdot A_1} * 1_{a_2 \cdot A_2} * 1_L\|_\infty \leq \epsilon |A_1| |A_2|.$$

Later we will see that $\epsilon = \frac{1}{8}$ suffices therefore the rank and the radius of B^* are appropriate. We now show that Lemma 18 can be used with $\beta = \frac{3}{5\alpha}$ to obtain a density increment. We easily see that

$$\|1_{a_2 \cdot A_2} * 1_L\|_1 = |A_2| |L| \leq \frac{3}{5\alpha} |A_1| |A_2|$$

and so we take our function to be $1_{a_2 \cdot A_2} * 1_L / |A_1| |A_2|$. To show that the remaining assumption is satisfied we need

$$1_{a_1 \cdot A_1} * 1_{a_2 \cdot A_2} * 1_L(0) \geq (1 - \epsilon) |A_1| |A_2|.$$

Let us use what we know about the number of solutions in A . Since our equation is invariant the number of solutions in $A - x$ is the same. We notice that

$$1_{a_1 \cdot A_1} * 1_{a_2 \cdot A_2} * 1_P(0) \cdot Q \leq \exp(-Cd \log(d/\alpha)) |A_1| |A_2| |A|^{k-3}. \quad (3)$$

By Proposition 3 we also see that

$$|A_i| \geq \frac{7\alpha}{8} |B'_\delta| \geq \left(c \frac{\alpha}{d^2}\right)^{3d} |B|$$

for $i > 2$. Simplifying the constants we get

$$|A_i| \geq \exp(-C'd \log(d^2/\alpha)) |A| \geq \exp(-Cd \log(d/\alpha)) |A|.$$

Applying this inequality multiple times to lower bound Q and then rearranging (3) gives

$$\begin{aligned} 1_{a_1 \cdot A_1} * 1_{a_2 \cdot A_2} * 1_P(0) \cdot \frac{\alpha}{8} |A|^{k-3} &\leq 1_{a_1 \cdot A_1} * 1_{a_2 \cdot A_2} * 1_P(0) \cdot Q \cdot \exp(C_2 d \log(d/\alpha)) \\ &\leq \frac{\alpha}{64} |A_1| |A_2| |A|^{k-3}, \end{aligned}$$

where the last inequality follows from the restriction on the number of solutions, provided the constant C has been chosen large enough. Thus we have

$$1_{a_1 \cdot A_1} * 1_{a_2 \cdot A_2} * 1_P(0) \leq \frac{1}{8} |A_1| |A_2|.$$

Because $1_L = 1_{B'_{1+(k-3)\delta}} - 1_P$ we have

$$1_{a_1 \cdot A_1} * 1_{a_2 \cdot A_2} * 1_L(0) \geq \left(1 - \frac{1}{8}\right) |A_1| |A_2| \geq \left(1 - \frac{1}{8}\right) |A_1| |A_2|.$$

Thus we can apply Lemma 18 with $\epsilon = \frac{1}{8}$ to finish the first case of the proof. Here the density increment was $\frac{5}{3}(1 - \frac{2}{8})\alpha = \frac{5}{4}\alpha$.

Case 2 ($|P| < |B'_{1+(k-3)\delta}|/2$): We will proceed in a similar fashion, however this time we will apply Theorem 14 to the sets $a_4 \cdot A_4, \dots, a_k \cdot A_k$, $M := a_3 \cdot A_3$ and $L := -1 \cdot P \subseteq \mathbb{Z}/p\mathbb{Z}$. The Bohr set will be $B^* = B'_{1+(k-3)\delta}$ as previously. We use almost the same S as in the previous case. We only swap $a_2 \cdot A_2$ for $a_4 \cdot A_4$, that is $S := a_4 \cdot B'_{\delta\nu}$. Arguing in exactly the same way we have

$$|a_4 \cdot A_4 + S| \leq \frac{16}{7\alpha} |a_4 \cdot A_4|.$$

This time we have $|L| \leq |B'_{1+(k-3)\delta}|/2 \leq \frac{3}{5\alpha} |a_3 \cdot A_3|$, again arguing in the same way, just swapping $a_1 \cdot A_1$ for $a_3 \cdot A_3$. We apply Theorem 14 with $\epsilon = \frac{1}{6}$ and so the rank and the radius of B^* are as needed. We also estimate the $\|\cdot\|_1$ norm, notice that

$$\begin{aligned} \|1_{a_4 \cdot A_4} * 1_{a_5 \cdot A_5} * \dots * 1_{a_k \cdot A_k} * 1_{-P}\|_1 &= |A_4| |A_5| \dots |A_k| |L| \\ &\leq \frac{3}{5\alpha} |A_3| |A_4| |A_5| \dots |A_k|. \end{aligned}$$

So this time our function in the application of Lemma 18 (again with $\beta = \frac{3}{5}$) will be

$$1_{a_4 \cdot A_4} * 1_{a_5 \cdot A_5} * \dots * 1_{a_k \cdot A_k} * 1_{-P} / |A_4| |A_5| \dots |A_k|$$

and the set will be $a_3 \cdot A_3$, sufficient ϵ will turn out to be $1/6$. It remains to estimate (using g defined above) $g * 1_{a_3 \cdot A_3}(0)$. We see that

$$g * 1_{a_3 \cdot A_3}(0) = \sum_{p \in P} 1_{a_3 \cdot A_3} * 1_{a_4 \cdot A_4} * \dots * 1_{a_k \cdot A_k}(p) = |A_3| |A_4| \dots |A_k| - \sum_{p \notin P} f(p),$$

however, by the definition of P , we have

$$\sum_{p \notin P} f(p) \leq \frac{\alpha}{8} |B'_{1+(k-3)\delta}| |A_4| |A_5| \dots |A_k| \leq \frac{1}{7} \cdot 1.01 \cdot |A_3| |A_4| \dots |A_k|,$$

where we use the fact that density of $a_3 \cdot A_3$ in B' is at least $\frac{7}{8}\alpha$. Combining the two previous lines we obtain

$$g * 1_{a_3 \cdot A_3}(0) \geq \left(1 - \frac{1}{6}\right) |A_3| |A_4| \dots |A_k|,$$

which finally lets us apply Lemma 18 with $\epsilon = \frac{1}{6}$. Here the density increment of A_3 on $(a_3)^{-1} B'_{1+(k-3)\delta}$ is $\frac{5}{3}(1 - \frac{2}{6})\alpha = \frac{10}{9}\alpha$.

We actually considered 3 possible cases, one being the second conclusion of Lemma 10. That one had by far the worst density increment, which we record in the current lemma. This finishes the proof. \square

We can finally prove Theorem 3.

Proof. As mentioned before, we pick

$$(|a_1| + |a_2| + \cdots + |a_n|)N < p < 2(|a_1| + |a_2| + \cdots + |a_n|)N.$$

Let $\alpha_2 = \frac{|A|}{p}$.

By Proposition 6 and Lemma 9 there exists a number $\delta \in [1/240, 1]$ such that there for some translate $x \in \mathbb{Z}/p\mathbb{Z}$ we have $B^{(0)} := \text{Bohr}(\{1\}, \delta)$ regular and

$$(A - x) \cap B^{(0)} \geq 0.9\alpha_2|B^{(0)}|.$$

Let $A^{(0)} = (A - x) \cap B^{(0)}$. We iterate Lemma 19 on the sets $A^{(0)}, B^{(0)}$, obtaining $(A^{(1)}, B^{(1)}), (A^{(2)}, B^{(2)}), \dots$. For each $i \geq 0$ we have $A^{(i)} = (A - t_i) \cap B^{(i)}$, where t_i is some translate. We know that after, say, s steps it is no longer possible. That is because the density of $A^{(i)}$ cannot exceed 1. Since Lemma 19 cannot be applied to $A^{(s)}$ and $B^{(s)}$ we know that $A^{(s)}$ contains at least $e^{-Cd_s \log(d_s/\alpha_2)}|A^{(s)}|^{k-1}$ solutions of $a_1x_1 + a_2x_2 + \cdots + a_kx_k = 0$, where C depends on the equation. We easily calculate that

$$\begin{aligned} s &\leq C \log(1/\alpha_2), \\ d_s &\leq C \log^5(2/\alpha_2), \\ \rho_s &\geq (c\alpha_2)^{Cs}. \end{aligned}$$

Clearly α_2 and α differ only by a constant depending on the equation, so do N and p . Therefore by Proposition 8 we have

$$|A^{(s)}| \geq \alpha_2|B^{(s)}| \geq \alpha_2(\rho_s/2\pi)^{d_s}p \geq e^{-C \log^7(2/\alpha)}N.$$

We also note that $\log(d_s/\alpha) \ll \log \log^5(2/\alpha) \ll \log(2/\alpha)$. Putting all of these bounds together with the estimate on the number of solutions in $A^{(s)}$ we have

$$e^{-Cd_s \log(d_s/\alpha)}|A^{(s)}|^{k-1} \geq e^{-C \log^7(2/\alpha)}N^{k-1}.$$

So A contains at least $e^{-C \log^7(2/\alpha)}N^{k-1}$ solutions to $a_1x_1 + a_2x_2 + \cdots + a_kx_k = 0$, since $A^{(s)} + t_s \subseteq A$ and the equation is invariant. \square

6 Behrend-type construction for the lower-bound

In this section we prove Theorem 4, which gives an analogous lower bound to what we have proved in the last section. We modify the argument of Tao ([18], Proposition 1.3) to show a Behrend-type bound for convex equations.

Proof. Let $N = M^{d+d'}$, where $d' \geq 0$ is an arbitrary integer (to construct infinitely many N) and M, d will be chosen later. Define a map $D : [N] \rightarrow [M]^d$ to be the mapping that sends a number to the vector of its last d digits in base M . To be precise, we define D as

$$D(n)_i = \left\lfloor \frac{n}{M^{i-1}} \right\rfloor \bmod M \text{ for } 1 \leq i \leq d.$$

To put it in yet another way, if $n = a_k M^k + a_{k-1} M^{k-1} + \cdots + a_1 M + a_0$ then $D(N) = (a_0, a_1, \dots, a_k)$. Define $T \subseteq [N]$ by including all n such that for all i one has $D(n)_i < \frac{M}{k}$. Clearly $|T| \geq N \cdot k^{-d}$. Among the numbers $1, 2, \dots, dM^2$ choose r such that the sphere $\|D(x)\|_2^2 = r$, which we call A , has at least $\frac{|T|}{dM^2} \geq \frac{1}{dk^d} M^{d'+d-2}$ points inside T . Suppose that $x_1, x_2, \dots, x_k \in A$ are such that $x_1 + \cdots + x_{k-1} = (k-1)x_k$. Since there is no carry-over in base M for the last d digits when adding elements of A up to k times, we have

$$D(x_1) + \cdots + D(x_{k-1}) = (k-1)D(x_k).$$

This however, can only be the case when $D(x_1) = \cdots = D(x_{k-1}) = D(x_k)$ by convexity, since all of the points belong to a sphere of radius r .

Let us now carefully count the total number of solutions. We pick x_1 to be an arbitrary element of A . As a consequence of the above observations x_2, x_3, \dots, x_{k-1} must have the same last d digits as x_1 . That leaves out d' digits to choose from for each of the $k-2$ variables. Since x_k is determined by the rest of the variables we conclude that there is at most $|A|M^{d'(k-2)}$ solutions to the equation $x_1 + \cdots + x_{k-1} = (k-1)x_k$ inside A . Now we choose $c = c(k) > 0$ to be a small constant, $c = \frac{1}{4+2\log k}$ suffices. We set $d := \lfloor c \log(2/\alpha) \rfloor$ and $M := \lfloor \alpha^{-c} \rfloor$, then we have

$$\begin{aligned} |A|/N &\geq \frac{M^{d'+d-2}}{Ndk^d} = \frac{1}{dk^d M^2} \\ &\geq \frac{1}{c \log(2/\alpha) k^{c \log(2/\alpha)} \alpha^{-2c}} \geq \alpha. \end{aligned}$$

The last inequality follows after simple rearranging. We also note that $d \geq 1$. That is because we assumed $\alpha \leq \exp(-1/c)$, thus we have $\log(2/\alpha) \geq 1/c$ and so

$$d = \lfloor c \log(2/\alpha) \rfloor \geq 1.$$

Further, bounding the size of A by N we have

$$\frac{|A|M^{d'(k-2)}}{N^{k-1}} \leq \frac{|A|}{M^{(k-1)d+d'}} \leq M^{d'+d-(k-1)d-d'} = M^{-(k-2)d} \leq e^{-c(k-2)\log^2(2/\alpha)},$$

which is the desired maximal number of solutions as $c(k-2)$ is a constant depending only on k . \square

7 Applications

Theorem 2 of Bloom has been used in a number of papers employing the Fourier Transference Principle. Examples of such results are papers from Prendiville [11], Chow [7],

Browning and Prendiville [6]. We think that substituting Theorem 2 by our Theorem 3 for equations of length 4 and more, could bring quantitative improvements. We briefly recall the first of the results [11] and state how the bound improves.

Let $S \subseteq \{1, 2, \dots, N\}$ and suppose that the only solutions to the equation

$$x_1 + y_1 = x_2 + y_2$$

for $x_1, x_2, y_1, y_2 \in S$ are trivial (by which we mean $x_1 = y_1$ and $x_2 = y_2$ or $x_1 = y_2$ and $x_2 = y_1$). Then S is called a Sidon set and it is known that $|S| \leq (1 + o(1))N^{1/2}$. The problem of finding solutions to invariant equations in Sidon sets was considered by Conlon, Fox, Sudakov and Zhao [8]. They give a weak upper bound of $|S| \leq o(N^{1/2})$, providing a comment about how to use their methods to obtain a stronger bound. Prendiville [11] used the method of Fourier Transference Principle to get an improvement on the work of Conlon, Fox, Sudakov and Zhao.

Theorem 20. (Prendiville) *If $N \geq 3$ and $S \subseteq \{1, 2, \dots, N\}$ is a Sidon set lacking solutions to an invariant equation $a_1x_1 + a_2x_2 + \dots + a_kx_k = 0$ in $k \geq 5$ variables, we have*

$$|S| \leq CN^{1/2}(\log \log N)^{-1}.$$

Prendiville already mentions that the result could be boosted by a counting version of the theorem of Schoen and Sisask [16]. Indeed, after we have proved Theorem 3, we can apply it in Prendiville's proof instead of Theorem 2. As a result, the following statement is obtained.

Theorem 21. *Let $S \subseteq \{1, 2, \dots, N\}$ be a Sidon set, which contains no non-trivial solutions to an invariant equation $a_1x_1 + a_2x_2 + \dots + a_kx_k = 0$ in $k \geq 5$ variables. Then we have*

$$|S| \leq N^{1/2} \exp(-C(\log \log N)^{1/7}),$$

where the constant C depends on the equation.

References

- [1] F. A. Behrend, On the sets of integers which contain no three in arithmetic progression. Proc. Nat. Acad. Sci., 23:331–332 (1946).
- [2] T. F. Bloom, Additive Combinatorics - part III lecture notes. <http://thomasbloom.org/teaching/AC2021.pdf>.
- [3] T. F. Bloom, Translation invariant equations and the method of Sanders. Bull. Lond. Math. Soc. 44 (2012), no. 5, 1050–1067.
- [4] T. F. Bloom, O. Sisask, The Kelley-Meka bounds for sets free of three-term arithmetic progressions. [arXiv:2302.07211](https://arxiv.org/abs/2302.07211).
- [5] T. F. Bloom, O. Sisask, An improvement to the Kelley-Meka bounds on three-term arithmetic progressions. [arXiv:2309.02353v1](https://arxiv.org/abs/2309.02353v1).

- [6] T. Browning, S. Prediville, A Transference Approach to a Roth-Type Theorem in the Squares. *International Mathematics Research Notices*, Volume 2017, Issue 7, April 2017, Pages 2219–2248 (2016).
- [7] S. Chow, Roth-Waring-Goldbach. *International Mathematics Research Notices*, Volume 2018, Issue 8, April 2018, Pages 2341–2374 (2017).
- [8] D. Conlon, J. Fox, B. Sudakov, Y. Zhao, The regularity method for graphs with few 4-cycles, *J. London Math. Soc.* 104; 2376–2401 (2021).
- [9] Z. Kelley and R. Meka, Strong bounds for 3-progressions. *IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*. Santa Cruz, CA, USA 2023, 933–973 (2023).
- [10] S. Prediville, Four variants of the Fourier-analytic transference principle. *Online Journal of Analytic Combinatorics* (2015).
- [11] S. Prediville, Solving equations in dense Sidon sets. *Math. Proc. Cambridge Philos. Soc.* 173 (2022), no. 1, 25–34.
- [12] K. F. Roth, On certain sets of integers. *J. London Math. Soc.* 28 (1953): 104–109. 1, 3.
- [13] T. Sanders, Additive structures in sumsets. *Math. Proc. Cambridge Philos. Soc.* 144 (2008), no. 2, 289–316.
- [14] T. Sanders, The structure theory of set addition revisited. *Bulletin of the American Mathematical Society* 50 (2012).
- [15] T. Schoen, I.D. Shkredov, Roth’s theorem in many variables, *Isr. J. Math.* 199 (2014) 287–308.
- [16] T. Schoen and O. Sisask, Roth’s theorem for four variables and additive structures in sums of sparse sets. *Forum Math. Sigma* 4 (2016) e5, 28.
- [17] T. Tao and V. H. Vu, *Additive Combinatorics*. Cambridge University Press (2006).
- [18] T. Tao, The ergodic and combinatorial approaches to Szemerédi’s theorem, [arXiv:math/0604456](https://arxiv.org/abs/math/0604456) (2006).
- [19] B. L. van der Waerden, Beweis einer Baudetschen Vermutung. *Nieuw Arch. Wisk.*, 15 (1927), pp. 212–216.