On Fourier Coefficients of Sets with Small Doubling

Ilya D. Shkredov[a]

Submitted: Dec 20, 2024; Accepted: May 28, 2025; Published: Aug 8, 2025

Abstract

Let A be a subset of a finite abelian group such that A has a small difference set $A - A$ and the density of A is small. We prove that, counter–intuitively, the smallness (in terms of $|A - A|$) of the Fourier coefficients of A guarantees that A is correlated with a large Bohr set. Our bounds on the size and the dimension of the resulting Bohr set are close to exact.

Mathematics Subject Classifications: 11B13, 11B75

1 Introduction

Let $\mathbf{G}$ be a finite abelian group and $\widehat{\mathbf{G}}$ its dual group. For any function $f : \mathbf{G} \to \mathbb{C}$ and $\chi \in \widehat{\mathbf{G}}$ define the Fourier transform of f at χ by the formula

$$\widehat{f}(\chi) = \sum_{g \in \mathbf{G}} f(g)\overline{\chi(g)}\,. \tag{1}$$

This paper considers the case when the function f has a special form, namely, f the characteristic function of a set $A \subseteq \mathbf{G}$ and we want to study the quantity

$$\mathcal{M}(A) := \max_{\chi \neq \chi_0} |\widehat{A}(\chi)|\,, \tag{2}$$

where by χ_0 we have denoted the principal character of $\widehat{\mathbf{G}}$ and we use the same capital letter to denote a set $A \subseteq \mathbf{G}$ and its characteristic function $A : \mathbf{G} \to \{0, 1\}$. It is well–known that $\mathsf{M}(A)$ is directly related to the uniform distribution properties of the set A (see, e.g., [13], [28]). Moreover, we impose an additional property on the set A, namely, that it is a set with small *doubling*, i.e. we consider sets A for which the ratio $|A-A|/|A|$ is small. Recall that given two sets $A, B \subseteq \mathbf{G}$ the *sumset* of A and B is defined as

$$A + B := \{a + b \ : \ a \in A,\, b \in B\}\,.$$

[a]Department of Mathematics, Purdue University, 150 N. University Street, West Lafayette, IN 47907–2067, U.S.A. (ishkredo@purdue.edu).

 https://doi.org/10.37236/13691

In a similar way we define the *difference sets* $A-A$ and the *iterated sumsets*, e.g., $2A-A$ is $A+A-A$. In terms of the difference sets $|A-A| := K|A|$ it is easy to see that

$$\mathsf{M}^2(A) \geqslant (1-o(1)) \cdot \frac{|A|^2}{K} \tag{3}$$

and estimate (3) gives us a simple lower bound for the quantity $\mathsf{M}(A)$. In general, bound (3) is tight, but the situation changes dramatically depending on the *density* $\delta := |A|/|\mathbf{G}|$ of A. For example, in [11, Lemma 4.1] (also, see [24] and [22, Propostion 6.1]) it was proved that

$$\mathsf{M}^2(A) \geqslant (1-o(1)) \cdot |A|^2 \,, \tag{4}$$

provided $\delta = \exp(-\Omega(K))$. Thus, if the density is exponentially small relative to K, then $\mathsf{M}(A)$ is close to its maximum value $|A|$ (choosing a random set A, it is easy to see that in order to have (4), the constraint $\delta = \exp(-\Omega(K))$ is close to tight). On the other hand, we always have $\delta \leqslant K^{-1}$ and for a random set $A \subseteq \mathbf{G}$ one has $\delta \gg K^{-1}$. Therefore, one of the reasonable questions here is the following. Assume that $\delta \sim K^{-d}$, where $d > 1$, that is, the dependence of δ on K is polynomial. What non–trivial properties do the Fourier coefficients of set A have in this case? Such a problem arises naturally in connection with the famous Freiman $3k-4$ theorem in $\mathbb{F}_p$, see, e.g., [7], [17], [18]. In particular, in [18, Theorem 6] it was proved that if $\delta \ll K^{-3}$, then

$$\mathsf{M}^2(A) \geqslant \frac{|A|^2}{K}(1+\kappa_0) \,, \tag{5}$$

where $\kappa_0 > 0$ is an absolute constant. Thus, a non-trivial lower bound for $\mathsf{M}(A)$ exists in any abelian group, and hence the Fourier coefficients of sets with small doubling have some interesting properties. Other results on the quantity $\mathsf{M}(A)$ and its relation to sets A_x (see Section 2 below) were obtained in [27]. The main result of this paper (all required definitions can be found in Sections 2, 4) concerns an even broader regime $\delta \ll K^{-2}$ and gives us a new structural property of sets with small doubling and small Fourier coefficients.

Theorem 1. *Let* $\mathbf{G}$ *be a finite abelian group,* $A \subseteq \mathbf{G}$ *be a set,* $|A| = \delta|\mathbf{G}|$, $|A-A| = K|A|$, *and* $1 \leqslant M \leqslant K$ *be a parameter. Suppose that*

$$100K^2\delta \leqslant 1 \,. \tag{6}$$

Then either there is $x \neq 0$ *such that*

$$|\widehat{A}(x)|^2 > \frac{M|A|^2}{K} \,, \tag{7}$$

or for any $B \subseteq A$, $|B| \gg |A| = \delta|\mathbf{G}|$ *there exists a regular Bohr set* $\mathcal{B}_*$ *and* $z \in \mathbf{G}$ *such that*

$$|B \cap (\mathcal{B}_* + z)| \geqslant \frac{|\mathcal{B}_*|}{8M} \,, \tag{8}$$

and

$$\dim(\mathcal{B}_*) \ll M^2 \left(\log(\delta^{-1}K) + \log^2 M\right) , \tag{9}$$

as well as

$$|\mathcal{B}_*| \gg |\mathbf{G}| \cdot \exp(-O(\dim(\mathcal{B}_*) \log(M \dim(\mathcal{B}_*)))) . \tag{10}$$

Let us make a few remarks regarding Theorem 1. First of all, the bounds (8)—(10) hold for *any* dense subset of our set A, which means that A has a very rigid structure (for example, see the second part of Corollary 9 below). Secondly, the dependencies on parameters in (8)—(10) have polynomial nature, which distinguishes them from the best modern results on the structure of sets with small doubling, see [22], [23]. Also, it appears that Theorem 1 does not depend on the recent breakthrough progress concerning Polynomial Freiman–Ruzsa Conjecture [9], [8]. Thirdly, the inversion of bound (7) guarantees the existence of a large intersection of A and a translation of a Bohr set $\mathcal{B}_*$, see inequality (8). This is quite surprising, because usually we have the opposite picture: small Fourier coefficients help *to avoid* such structural objects as Bohr sets. Finally, our proof drastically differs from the arguments of [11], [24], [22], which give us inequality (4). Instead of using almost periodicity of multiple convolutions [6] and the polynomial growth of sumsets, we apply some observations from the higher energies method, see papers [25], [27]. In particular, our structural subset of $A-A$ has a different nature (it resembles some steps of the proof of [9], [8] and even older constructions of Schoen, see [26, Examples 5,6]). Let us consider the following motivating example (see, e.g., [26, Example 5]).

Example 2. ($H + \Lambda$ sets). Let $\mathbf{G} = \mathbb{F}_2^n$, $H \leqslant \mathbf{G}$ be the space spanned by the first $k < n$ coordinate vectors, $\Lambda \subseteq H^\perp$ be a basis, $|\Lambda| = 2K$, $K \to \infty$, and $A := H + \Lambda$. In particular, $|A| = |H||\Lambda|$ and $|A - A| = |H||\Lambda - \Lambda| = 2^{-1}|\Lambda||H|(|\Lambda| + O(1)) = (1 + o(1)) \cdot K|A|$. Further for $s \in H$ one has $A_s = A$, but it is easy to check that for $s \in (A - A) \setminus H$ each A_s is a disjoint union of two shifts of H. Hence

$$\mathsf{E}(A) \sim |A|^3/K \sim \sum_{s \in H} |A_s|^2 \sim \sum_{s \in (A-A)\setminus H} |A_s|^2$$

(the existence of two "dual" subsets of $A - A$ where $\mathsf{E}(A)$ is achieved is in fact a general result, see [2] and also [26]), but for $k > 2$ the higher energies are supported on the set of measure zero (namely, H) in the sense that

$$\mathsf{E}_k(A) := \sum_s |A_s|^k = (1 + o_k(1)) \cdot \sum_{s \in H} |A_s|^k . \tag{11}$$

Moreover if one considers the function $\varphi_k(s) = |A_s|^k$, then it is easy to see that

$$\widehat{\varphi}_k(\chi) := \sum_s |A_s|^k \chi(s) = (1 + o_k(1)) \cdot \sum_{s \in H} |A_s|^k \chi(s) = (1 + o_k(1)) \cdot |A|^k \widehat{H}(\chi) ,$$

where χ is an arbitrary additive character on $\mathbf{G}$. Thus, as k goes to infinity, the Fourier transform $\widehat{\varphi}_k(\chi)$ becomes very regular, and this gives us a new way to extract the structure piece from sets with small doubling.

Roughly speaking, the same Example 2 shows that Theorem 1 is tight (also, see more rigorous Example 20 below). Indeed, it is easy to see that $\widehat{A} = \widehat{H} \cdot \widehat{\Lambda}$ and assuming that Λ is a sufficiently small set and $\mathsf{M}^2(\Lambda) \ll |\Lambda| \ll K$, we get $\mathsf{M}^2(A) = |H|^2 \mathsf{M}^2(\Lambda) \ll |A|^2/K$. Thus all conditions of Theorem 1 hold but the obvious subspace in $A - A$ is of course H and we have $\operatorname{codim}(H) = \log(\delta^{-1}K)$, which coincides with (9) up to multiple constants.

2 Definitions and notation

Let $\mathbf{G}$ be a finite abelian group and we denote the cardinality of $\mathbf{G}$ by N. Given a set $A \subseteq \mathbf{G}$ and a positive integer k, let us put

$$\Delta_k(A) := \{(a, a, \dots, a) \ : \ a \in A\} \subseteq \mathbf{G}^k \,.$$

Now we have

$$A - A := \{a - b \ : \ a, b \in A\} = \{x \in \mathbf{G} \ : \ A \cap (A - x) \neq \emptyset\} \,, \tag{12}$$

and for $x \in A - A$ we denote by A_x the intersection $A \cap (A + x)$. The useful inclusion of Katz–Koester [14] is the following

$$B + A_x \subseteq (A + B)_x \,. \tag{13}$$

A natural generalization of the last formula in (12) is the set

$$\{(x_1, \dots, x_k) \in \mathbf{G}^k \ : \ A \cap (A - x_1) \cap \dots \cap (A - x_k) \neq \emptyset\} = A^k - \Delta_k(A) \,, \tag{14}$$

which is called the *higher difference set* (see [25]). For any two sets $A, B \subseteq \mathbf{G}$ the *additive energy* of A and B is defined by

$$\mathsf{E}(A, B) = \mathsf{E}(A, B) = |\{(a_1, a_2, b_1, b_2) \in A \times A \times B \times B \ : \ a_1 - b_1 = a_2 - b_2\}| \,.$$

If $A = B$, then we simply write $\mathsf{E}(A)$ for $\mathsf{E}(A, A)$. Also, one can define the *higher energy* (see [25] and another formula (18) below)

$$\mathsf{E}_k(A) = |\{(a_1, \dots, a_k, a'_1, \dots, a'_k) \in A^{2k} \ : \ a_1 - a'_1 = \dots = a_k - a'_k\}| \,. \tag{15}$$

Let $\widehat{\mathbf{G}}$ be the dual group of $\mathbf{G}$. For any function $f : \mathbf{G} \to \mathbb{C}$ and $\chi \in \widehat{\mathbf{G}}$ we define its Fourier transform using the formula (1). The Parseval identity is

$$N \sum_{g \in \mathbf{G}} |f(g)|^2 = \sum_{\chi \in \widehat{\mathbf{G}}} \left| \widehat{f}(\chi) \right|^2 . \tag{16}$$

By *measure* we mean any non–negative function μ on $\mathbf{G}$ such that $\sum_{g \in \mathbf{G}} \mu(g) = 1$. If $f, g : \mathbf{G} \to \mathbb{C}$ are some functions, then

$$(f * g)(x) := \sum_{y \in \mathbf{G}} f(y) g(x - y) \quad \text{ and } \quad (f \circ g)(x) := \sum_{y \in \mathbf{G}} f(y) g(y + x) \,.$$

One has

$$\widehat{f*g} = \widehat{f}\cdot\widehat{g} \qquad \text{and} \qquad (\widehat{fg})(x) = \frac{1}{N}(\widehat{f}*\widehat{g})(x)\,. \tag{17}$$

Having a function $f : \mathbf{G} \to \mathbb{C}$ and a positive integer $k > 1$, we write $f^{(k)}(x) = (f \circ f \circ \dots \circ f)(x)$, where the convolution $\circ$ is taken $k-1$ times. For example, $A^{(4)}(0) = \mathsf{E}(A)$ and for $k \geqslant 2$ one has

$$\mathsf{E}_k(A) = \sum_x (A \circ A)^k(x) = \sum_{x_1,\dots,x_{k-1}} (A^{k-1} \circ \Delta_{k-1}(A))^2(x_1,\dots,x_{k-1})\,. \tag{18}$$

A finite set $\Lambda \subseteq \mathbf{G}$ is called *dissociated* if any equality of the form

$$\sum_{\lambda\in\Lambda} \varepsilon_\lambda \lambda = 0\,, \qquad \text{where} \qquad \varepsilon_\lambda \in \{0, \pm 1\}\,, \qquad \forall \lambda \in \Lambda$$

implies $\varepsilon_\lambda = 0$ for all $\lambda \in \Lambda$. Let $\dim(A)$ be the size of the largest dissociated subset of A and we call $\dim(A)$ the *additive dimension* of A. Let us denote all combinations of the form $\{\sum_{\lambda\in\Lambda} \varepsilon_\lambda\lambda\}_{\varepsilon_\lambda\in\{0,\pm1\}}$ as $\mathrm{Span}\,(\Lambda)$. If $\mathbf{G} = \mathbb{F}_2^n$, then $\mathrm{Span}\,(\Lambda)$ is just the minimal subspace, containing Λ.

Given a function f and $\varepsilon \in (0, 1]$ define the *spectrum* of f as

$$\mathrm{Spec}_{\,\varepsilon}(f) = \{\chi \in \widehat{\mathbf{G}} \;:\; |\widehat{f}(\chi)| \geqslant \varepsilon \|f\|_1\}\,. \tag{19}$$

We need Chang's lemma [5].

Lemma 3. *Let $f : \mathbf{G} \to \mathbb{C}$ be a function and $\varepsilon \in (0, 1]$ be a parameter. Then*

$$\dim(\mathrm{Spec}_{\,\varepsilon}(f)) \ll \varepsilon^{-2} \log \frac{\|f\|_2^2 N}{\|f\|_1^2}\,.$$

Also, we need the generalized triangle inequality [25, Theorem 7].

Lemma 4. *Let k be a positive integer, $Y \subseteq \mathbf{G}^k$ and $X, Z \subseteq \mathbf{G}$. Then*

$$|X||Y - \Delta_k(Z)| \leqslant |Y \times Z - \Delta_{k+1}(X)|\,. \tag{20}$$

The signs $\ll$ and $\gg$ are the usual Vinogradov symbols. All logarithms are to base e.

3 The model case

In this section we follow the well–known logic (see [10]) and first consider the simplest case $\mathbf{G} = \mathbb{F}_2^n$, where the technical difficulties are minimal, and the case of general groups will be considered later.

We need a generalization of a result from [27, Remark 6] (also see the proof of [27, Theorem 4]). For the convenience of the reader, we recall our argument.

Lemma 5. *Let $A, B \subseteq \mathbf{G}$ be sets, $|A-A| = K|A|$ and $k \geqslant 2$ be an integer. Then*

$$\mathsf{E}_k(B)\mathsf{E}^k(A, A+B) \geqslant \frac{|A|^{2k+1}|B|^{2k}}{K}\,. \tag{21}$$

Proof. Let $S = A+B$. In view of inclusion (13), we have

$$\mathsf{E}(A,S) = \sum_x |A_x||S_x| \geqslant \sum_x |A_x||B+A_x|\,.$$

Let $\mathcal{D}_k := |B^{k-1} - \Delta_{k-1}(B)|$. Using Lemma 4 with $X = Z$, $Y = Z = B$, $k = k-1$, we see that for any $Z \subseteq \mathbf{G}$ the following holds

$$|Z|\mathcal{D}_k = |Z||B^{k-1} - \Delta_{k-1}(B)| \leqslant |B-Z|^k$$

and therefore by the Hölder inequality one has

$$\mathsf{E}(A,S) \geqslant \mathcal{D}_k^{1/k} \sum_x |A_x|^{1+1/k} \geqslant \mathcal{D}_k^{1/k} \left(\sum_x |A_x| \right)^{1+1/k} |A-A|^{-1/k}\,. \tag{22}$$

Thus

$$\mathsf{E}^k(A,S) \geqslant \mathcal{D}_k |A|^{2k+1} K^{-1}\,. \tag{23}$$

On the other hand, applying the Cauchy–Schwarz inequality and formula (18), we derive

$$|B|^{2k} = \left(\sum_{y \in \mathbf{G}^{k-1}} (B^{k-1} \circ \Delta_{k-1}(B)(y) \right)^2 \leqslant \mathcal{D}_k \sum_{y \in \mathbf{G}^{k-1}} (B^{k-1} \circ \Delta_{k-1}(B)^2(y) = \mathcal{D}_k \mathsf{E}_k(B)\,. \tag{24}$$

Combining (23) and (24), one obtains

$$\mathsf{E}_k(B)\mathsf{E}^k(A,S) \geqslant \mathsf{E}_k(B)\mathcal{D}_k|A|^{2k+1}K^{-1} \geqslant |B|^{2k}|A|^{2k+1}K^{-1} \tag{25}$$

as required. ☐

Now we are ready to prove our main technical proposition.

Proposition 6. *Let* $\mathbf{G} = \mathbb{F}_2^n$*,* $A, B \subseteq \mathbf{G}$ *be sets,* $|A| = \delta N$*,* $|B| = \omega|A|$*,* $|A+B| = K|A|$*,* $|A-A| = K'|A|$*, and* $0 < M \leqslant K$*,* $0 < M' \leqslant K'$*,* $\kappa > 0$*,* $\zeta \in (0,1)$*,* $1 < T \leqslant M'(M+\kappa)\omega^{-1}$ *be some parameters. Suppose that*

$$\mathsf{M}^2(A) \leqslant \frac{M|A|^2}{K}, \qquad \mathsf{E}(B) \leqslant \frac{M'|B|^3}{K'}\,, \tag{26}$$

and

$$|A+B|^2 \leqslant \kappa |A| N\,. \tag{27}$$

Then there is $\mathcal{L} \leqslant \mathbf{G}$ *(*$\mathcal{L}$ *depends on* B *only) and* $z \in \mathbf{G}$ *such that*

$$|B \cap (\mathcal{L}+z)| \geqslant \frac{(1-\zeta)\omega|\mathcal{L}|}{T(M+\kappa)}\,,$$

and

$$\mathrm{codim}(\mathcal{L}) \ll (\omega\zeta)^{-2} T^2 (M+\kappa)^2 \cdot \left(\log(\delta^{-1}K') + \log_T(M'(M+\kappa)\omega^{-1}) \cdot \log((M+\kappa)\omega^{-1})\right)\,.$$

Proof. Let $a = |A|$, $b = |B| = \beta N = \omega\delta N$, $S = A+B$ and $\mathsf{E}_k = \mathsf{E}_k(B)$. Thanks to the condition (27) and Parseval identity (16), we have

$$\mathsf{E}(A,S) \leqslant \frac{a^2|A+B|^2}{N} + Ma^3 \leqslant (M+\kappa)a^3\,.$$

Using Lemma 5, we obtain for all integers $k \geqslant 2$ that

$$\mathsf{E}_{k+1} \geqslant \frac{b^{2k+2}}{K'(M+\kappa)^{k+1}a^k} = \frac{b^{k+2}\omega^k}{K'(M+\kappa)^{k+1}}\,. \tag{28}$$

Suppose that for every $k \geqslant 2$ the following holds

$$\mathsf{E}_{k+1} \leqslant \frac{b\mathsf{E}_k}{M_*}\,,$$

where $M_* \geqslant 1$ is a parameter. Then thanks to (26), we derive

$$\mathsf{E}_{k+1} \leqslant \frac{b^{k-1}\mathsf{E}_2}{M_*^{k-1}} \leqslant \frac{M' b^{k+2}}{K' M_*^{k-1}}\,, \tag{29}$$

and using (28), we have

$$M'(M+\kappa)^{k+1} \geqslant \omega^k M_*^{k-1}\,.$$

Put $M_* = \omega^{-1}(M+\kappa)T$. It gives us

$$M'(M+\kappa)^2 \geqslant \omega T^{k-1}$$

and we obtain a contradiction if $k \geqslant k_0 := \lceil 10 \log_T (M'(M+\kappa)\omega^{-1}) \rceil + 10$, say. Thus there is $2 \leqslant k \leqslant k_0$ such that

$$\mathsf{E}_{k+1} \geqslant \frac{b\mathsf{E}_k}{M_*} . \tag{30}$$

Consider the function $\varphi(x) := |B_x|^k$ and $\psi(s) := |B_x|$. One can check that $\widehat{\psi} \geqslant 0$ and hence $\widehat{\varphi} \geqslant 0$ (use, for example, formula (17)). Also, $\|\varphi\|_1 = \mathsf{E}_k$ and $\|\varphi\|_2^2 = \sum_x |B_x|^{2k} \leqslant |B|^k \mathsf{E}_k(B)$. In terms of Fourier transform we can rewrite inequality (30) as

$$\mathsf{E}_{k+1} = \frac{1}{N} \sum_{\xi} |\widehat{B}(\xi)|^2 \widehat{\varphi}(\xi) \geqslant \frac{b\mathsf{E}_k}{M_*} = \frac{\omega b \mathsf{E}_k}{T(M+\kappa)} .$$

Now we use the parameter ζ and derive

$$\frac{1}{N} \sum_{\xi \in \mathrm{Spec}_{\zeta/M_*}(\varphi)} |\widehat{B}(\xi)|^2 \widehat{\varphi}(\xi) \geqslant \frac{(1-\zeta)\omega b \mathsf{E}_k}{T(M+\kappa)} . \tag{31}$$

Let $\Lambda \subseteq \mathrm{Spec}_{\zeta/M_*}(\varphi)$ be a dissociated set such that $|\Lambda| = \dim(\mathrm{Spec}_{\zeta/M_*}(\varphi))$. Put $\mathcal{L}^\perp = \mathrm{Span}\,\Lambda$ (recall that in the case $\mathbf{G} = \mathbb{F}_2^n$ the set $\mathrm{Span}\,\Lambda$ concides with the minimal subspace, containing Λ). It is known that for an arbitrary $\mathcal{L} \leqslant \mathbf{G}$ one has $\widehat{\mathcal{L}}(x) = |\mathcal{L}|\mathcal{L}^\perp(x)$. Using the later formula and the Parseval identity, we get

$$\frac{(1-\zeta)\omega b\mathsf{E}_k}{T(M+\kappa)} \leqslant \frac{1}{N} \sum_{\xi \in \mathcal{L}^\perp} |\widehat{B}(\xi)|^2 \widehat{\varphi}(\xi) \leqslant \frac{\mathsf{E}_k}{N} \sum_{\xi \in \mathcal{L}^\perp} |\widehat{B}(\xi)|^2 = \frac{\mathsf{E}_k}{|\mathcal{L}|} \sum_x (B \circ B)(x) \mathcal{L}(x) . \tag{32}$$

By the pigeonhole principle there is $z \in B$ such that

$$|B \cap (\mathcal{L} + z)| \geqslant \frac{(1-\zeta)\omega |\mathcal{L}|}{T(M+\kappa)} . \tag{33}$$

Using the Chang Lemma 3, bound $\|\varphi\|_2^2 \leqslant b^k \mathsf{E}_k(B)$, and estimate (28), we derive

$$\mathrm{codim}(\mathcal{L}) \ll \zeta^{-2} M_*^2 \log\left(\frac{\|\varphi\|_2^2 N}{\|\varphi\|_1^2} \right) \ll (\omega\zeta)^{-2} T^2 (M+\kappa)^2 \log\left(\frac{b^k N}{\mathsf{E}_k} \right) \tag{34}$$

$$\ll (\omega\zeta)^{-2} T^2 (M+\kappa)^2 \log\left(\frac{K'(M+\kappa)^k}{\beta \omega^{k-1}} \right) . \tag{35}$$

Recalling that $k \leqslant k_0$, we finally obtain

$$\mathrm{codim}(\mathcal{L}) \ll (\omega\zeta)^{-2} T^2 (M+\kappa)^2 \cdot$$

$$\left(\log(\delta^{-1} K') + \log_T (M'(M+\kappa)\omega^{-1}) \cdot \log((M+\kappa)\omega^{-1}) \right) . \tag{36}$$

This completes the proof. □

Remark 7. Suppose that $A = B$. Then in terms of Proposition 6 one has

$$\mathsf{E}(A) \leqslant \frac{|A|^4}{N} + \mathsf{M}^2(A)|A| \leqslant \frac{|A|^4}{N} + \frac{M|A|^3}{K} \leqslant \frac{M|A|^3}{K}\left(1+\frac{\delta K}{M}\right) \leqslant \frac{M|A|^3}{K}\left(1+\frac{\kappa}{KM}\right).$$

Thus $M' \leqslant \left(1+\frac{\kappa}{KM}\right)M$.

We derive some consequences of Proposition 6. Let us start with the case when $\mathsf{M}(A)$ is really small, namely, $\mathsf{M}^2(A) \leqslant (2-\varepsilon)|A|^2/K$.

Corollary 8. *Let* $\mathbf{G} = \mathbb{F}_2^n$, $A \subseteq \mathbf{G}$ *be a set,* $|A| = \delta N$, $|A - A| = K|A|$, *and* $\varepsilon \in (0,1)$ *be a parameter. Suppose that*

$$100K^2\delta \leqslant \varepsilon\,.$$

Then either there is $x \neq 0$ *such that*

$$|\widehat{A}(x)|^2 \geqslant \frac{(2-\varepsilon)|A|^2}{K}\,,$$

or there exists $\mathcal{L} \leqslant \mathbf{G}$ *with* $\mathcal{L} \subseteq A - A$ *and*

$$\operatorname{codim}(\mathcal{L}) \ll \varepsilon^{-2}\log(\delta^{-1}K) + \varepsilon^{-3}\,.$$

Proof. We apply Proposition 6 with $B = -A$, $\omega = 1$, $M = 2-\varepsilon$, $M' = \left(1+\frac{\kappa}{KM}\right)M \leqslant M+\kappa$ (see Remark 7), $T = 1+\kappa$, and $\kappa = \zeta = \varepsilon/100$, say. Thus we find $\mathcal{L} \leqslant \mathbf{G}$ and $z \in \mathbf{G}$ such that

$$|A \cap (\mathcal{L}+z)| \geqslant \frac{(1-\zeta)|\mathcal{L}|}{T(M+\kappa)} \geqslant |\mathcal{L}|\left(\frac{1}{2}+\frac{\varepsilon}{8}\right)\,, \tag{37}$$

and

$$\operatorname{codim}(\mathcal{L}) \ll \zeta^{-2}T^2(M+\kappa)^2 \cdot \left(\log(\delta^{-1}K) + \log_T(M'(M+\kappa)) \cdot \log(M+\kappa)\right)$$
$$\ll \varepsilon^{-2}\log(\delta^{-1}K) + \varepsilon^{-2}\log_T 2 \ll \varepsilon^{-2}\log(\delta^{-1}K) + \varepsilon^{-3}\,.$$

The inequality (37) implies that $\mathcal{L} \subseteq A - A$. This completes the proof. □

Now we are ready to obtain our structural result for sets with small doubling and small $\mathsf{M}(A)$. Given two sets $A, B \subseteq \mathbf{G}$ we write $A \dot{+} B$ if $|A+B| = |A||B|$.

Corollary 9. *Let* $\mathbf{G} = \mathbb{F}_2^n$, $A \subseteq \mathbf{G}$ *be a set,* $|A| = \delta N$, $|A - A| = K|A|$, *and* $1 \leqslant M \leqslant K$ *be a parameter. Suppose that*

$$100K^2|A| \leqslant N\,.$$

Then either there is $x \neq 0$ *such that*

$$|\widehat{A}(x)|^2 > \frac{M|A|^2}{K}\,, \tag{38}$$

or for any $B \subseteq A$, $|B| = \beta N$ *there exist* $H \leqslant \mathbf{G}$, $z \in \mathbf{G}$ *with* $H \subseteq 3B + z$ *and*

$$\mathrm{codim}(H) \ll (\delta\beta^{-1}M)^2 \left(\log(\delta^{-1}K) + \log^2(\delta\beta^{-1}M)\right) .$$

In the last case one can find $\Lambda \subseteq \mathbf{G}/H$ *such that*

$$|A \cap (\Lambda \dotplus H)| \geqslant \frac{|A|}{16M} \qquad \textit{and} \qquad |\Lambda||H| \leqslant 16M|A| .$$

Proof. If $\mathsf{M}^2(A) > M|A|^2/K$, then there is nothing to prove. Otherwise, $\mathsf{M}^2(A) \leqslant M|A|^2/K$ and thanks to our assumption $100K^2|A| \leqslant N$ and $|A+B| = |A-B| \leqslant |A-A| = K|A|$, we get

$$|A+B|^2 \leqslant (K|A|)^2 = (K^2\delta)|A|N \leqslant 100^{-1}|A|N \leqslant |A||N| .$$

It follows that condition (27) of Proposition 6 takes place with $\kappa = 1$, say. We apply this proposition with $\kappa = 1$, $T = 2$, $\zeta = 1/8$, $|B| = \beta N := \omega|A|$ and $M' = 2M$ (see Remark 7) to find $\mathcal{L} \leqslant \mathbf{G}$ such that

$$\mathrm{codim}(\mathcal{L}) \ll (\omega\zeta)^{-2}T^2(M+\kappa)^2 \cdot \left(\log(\delta^{-1}K) + \log_T(M'(M+\kappa)\omega^{-1}) \cdot \log((M+\kappa)\omega^{-1})\right)$$

$$\ll (\delta\beta^{-1}M)^2 \left(\log(\delta^{-1}K) + \log^2(\delta\beta^{-1}M)\right) ,$$

and (see (32) or (37))

$$|B \cap (\mathcal{L} + z)| \geqslant \frac{(1-\zeta)|\mathcal{L}|}{T(M+\kappa)} \geqslant \frac{|\mathcal{L}|}{8M} . \qquad (39)$$

Put $B' = B \cap (\mathcal{L} + z)$. It remains to apply the Kelley–Meka bound (see [16, Corollary 1.12], also see [3, Theorem 3]) and find $H \leqslant \mathcal{L}$, $z \in \mathbf{G}$ such that $H \subseteq 3B' + z$ and

$$\mathrm{codim}(H) \leqslant \mathrm{codim}(\mathcal{L}) + O(\log^{O(1)} M) \ll (\delta\beta^{-1}M)^2 \left(\log(\delta^{-1}K) + \log^2(\delta\beta^{-1}M)\right) .$$

Returning to (32) with $B = A$, we see that

$$\sum_x (A \circ A)(x)\mathcal{L}(x) \geqslant \frac{|\mathcal{L}||A|}{8M} . \qquad (40)$$

Put $A = \bigsqcup_{\lambda \in \mathbf{G}/\mathcal{L}} (A \cap (\mathcal{L} + \lambda))$ and for any $\lambda \in \mathbf{G}/\mathcal{L}$ define $A_\lambda = A \cap (\mathcal{L} + \lambda)$. Thus $A(x) = \sum_\lambda A_\lambda(x)$. Then (40) is equivalent to

$$2 \sum_{\lambda \in \mathbf{G}/\mathcal{L} \,:\, |A_\lambda| \geqslant |\mathcal{L}|/16M} |A_\lambda|^2 \geqslant \sum_{\lambda \in \mathbf{G}/\mathcal{L}} |A_\lambda|^2 = \sum_{\lambda \in \mathbf{G}/\mathcal{L}} \sum_x A_\lambda(x)|A_x| = \sum_x A(x)|A_x| \geqslant \frac{|\mathcal{L}||A|}{8M} .$$

Let $\Lambda = \{\lambda \in \mathbf{G}/\mathcal{L} \;:\; |A_\lambda| \geqslant |\mathcal{L}|/16M\}$. Putting $A_* = A \cap (\Lambda \dotplus \mathcal{L})$, we see that $|A_*| \geqslant |A|/16M$ and $|\Lambda||\mathcal{L}| \leqslant 16M|A|$. This completes the proof. □

Suppose we have a set $A \subseteq \mathbf{G}$ with doubling constant $K[A] := |A-A|/|A|$ and density $\delta = |A|/|\mathbf{G}|$. The relation between K and δ can be arbitrary, but the following consequence of proposition 6 allows us to have a "regularization" of any set A in the sense that one can always find a large subset $\tilde{A}$ of A such that the density of $\tilde{A}$ depends on the doubling constant $\tilde{A}$ at least quadratically, see inequality (41) below.

Corollary 10. *Let $\mathbf{G} = \mathbb{F}_2^n$, $A \subseteq \mathbf{G}$ be a set, $|A| = \delta N$. Then there is $H \leqslant \mathbf{G}$ and $z \in \mathbf{G}$ such that*

$$\operatorname{codim}(H) \ll \delta^{-2} \log^3(1/\delta)\,.$$

and for $\tilde{A} = A \cap (H+z)$ one has $\tilde{\delta} = |\tilde{A}|/|H| \geqslant \delta$, $\tilde{K} = K[\tilde{A}]$ and

$$100\tilde{K}^2\tilde{\delta} > 1\,. \tag{41}$$

Proof. Let $K = K[A]$. If $100K^2\delta > 1$, then there is nothing to prove. Otherwise, we apply Proposition 6 with $B = -A$, $\omega = 1$, $\kappa = 1$, $T = 2$, $\zeta = 1/8$ and $M' = 2M$ as we did in the proof of Corollary 9. Here M is defined as $\mathsf{M}(A)^2 = M|A|^2/K$, where $K = K[A]$. Exactly as in (39) we find $H_1 \leqslant \mathbf{G}$ and $z_1 \in \mathbf{G}$ such that

$$|A \cap (H_1 + z_1)| \geqslant \frac{|H_1|}{8M}\,, \tag{42}$$

and

$$\operatorname{codim}(H_1) \ll M^2 \left(\log(\delta^{-1}K) + \log^2 M\right)\,.$$

Now suppose that $M \leqslant 1/(16\delta)$ and therefore $\operatorname{codim}(H_1) \ll \delta^{-2}\log^2(\delta^{-1})$. Then (42) shows that the A has density 2δ inside $H_1 + z_1$. On the other hand, if $M > 1/(16\delta)$ then there is $x \neq 0$ such that

$$|\widehat{A}(x)| \geqslant |A| \cdot (M/K)^{1/2} = 2^{-2}\delta|A|\,.$$

Here we have used the trivial fact that $K \leqslant \delta^{-1}$. In this case we can use classical density increment (see [19] or [28]) and find $H_1' \leqslant \mathbf{G}$, $\operatorname{codim}(H_1') = 1$, $z_1' \in \mathbf{G}$ such that

$$|A \cap (H_1' + z_1')| \geqslant \delta(1 + 2^{-3}\delta)|H_1'|\,. \tag{43}$$

After that, one can repeat our dichotomy for $A_1 := A \cap (H_1 + z_1)$ or $A_1' := A \cap (H_1' + z_1')$. Using (42) or (43), we see that the algorithm must stop after a finite number of steps and the resulting codimension is big–O of

$$\log(1/\delta) \cdot \delta^{-2}\log^2(\delta^{-1}) + \delta^{-1} = O(\delta^{-2}\log^3(1/\delta))\,.$$

This completes the proof. $\square$

4 General case

Now we are ready to consider the case of an arbitrary finite abelian group $\mathbf{G}$. The main tool here is the so–called *Bohr sets*, and we recall all the necessary definitions and properties of this object. Bohr sets were introduced to additive number theory by Ruzsa [20] and Bourgain [4] was the first who used Fourier analysis on Bohr sets to improve the estimate in Roth's theorem [19]. Sanders (see, e.g., [21], [22]) developed the theory of Bohr sets proving many important theorems, see for example Lemma 17 below.

Definition 11. Let Γ be a subset of $\widehat{\mathbf{G}}$, $|\Gamma| = d$, and $\varepsilon = (\varepsilon_1, \dots, \varepsilon_d) \in (0,1]^d$. Define the Bohr set $\mathcal{B} = \mathcal{B}(\Gamma, \varepsilon)$ by

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

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

The number $d = |\Gamma|$ is called *dimension* of $\mathcal{B}$ and is denoted by $\dim B$. If $M = \mathcal{B} + n$, $n \in \mathbf{G}$ is a translation of $\mathcal{B}$, then, by definition, put $\dim(M) = \dim(\mathcal{B})$. The *intersection* $\mathcal{B} \wedge \mathcal{B}'$ of two Bohr sets $\mathcal{B} = \mathcal{B}(\Gamma, \varepsilon)$ and $\mathcal{B}' = \mathcal{B}(\Gamma', \varepsilon')$ is the Bohr set with the generating set $\Gamma \cup \Gamma'$ and new vector $\tilde{\varepsilon}$ equals $\min\{\varepsilon_j, \varepsilon'_j\}$. Furthermore, if $\mathcal{B} = \mathcal{B}(\Gamma, \varepsilon)$ and $\rho > 0$ then by $\mathcal{B}_\rho$ we mean $\mathcal{B}(\Gamma, \rho\varepsilon)$.

Definition 12. A Bohr set $\mathcal{B} = \mathcal{B}(\Gamma, \varepsilon)$ is called *regular*, if for every η, $d|\eta| \leqslant 1/100$ we have

$$(1 - 100d|\eta|)|\mathcal{B}_1| < |\mathcal{B}_{1+\eta}| < (1 + 100d|\eta|)|\mathcal{B}_1|. \tag{44}$$

Let us recall a sequence of basic properties of Bohr sets that will be used in what follows. These properties are now well known (see [28]), historically they were proved by Bourgain in [4]: Lemmas 14, 15 are Lemma 2 of this paper, Lemma 13 is Lemma 3 and Lemma 16 is a simple consequence of definitions probably first obtained in [22, Lemma 4.1].

Lemma 13. *Let $\mathcal{B}(\Gamma, \varepsilon)$ be a Bohr set. Then there exists ε_1 such that $\frac{\varepsilon}{2} < \varepsilon_1 < \varepsilon$ and $\mathcal{B}(\Gamma, \varepsilon_1)$ is regular.*

Lemma 14. *Let $\mathcal{B}(\Gamma, \varepsilon)$ be a Bohr set. Then*

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

Lemma 15. *Let $\mathcal{B}(\Gamma, \varepsilon)$ be a Bohr set. Then*

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

Lemma 16. *Suppose that $\mathcal{B}^{(1)}, \dots, \mathcal{B}^{(k)}$ is a sequence of Bohr sets. Then*

$$|\bigwedge_{i=1}^k \mathcal{B}^{(i)}| \geqslant N \cdot \prod_{i=1}^k \frac{|\mathcal{B}^{(i)}_{1/2}|}{N}\,.$$

Recall a local version of Chang's lemma [5], see [22, Lemma 5.3] and [21, Lemmas 4.6, 6.3].

Lemma 17. *Let $\varepsilon, \nu, \rho \in (0,1]$ be positive real numbers. Suppose that $\mathcal{B}$ is a regular Bohr set and $f : \mathcal{B} \to \mathbb{C}$. Then there is a set Λ of size $O(\varepsilon^{-2} \log(\|f\|_2^2 |\mathcal{B}| / \|f\|_1^2))$ such that for any $\gamma \in \mathrm{Spec}_\varepsilon(f)$ we have*

$$|1-\gamma(x)| \ll |\Lambda|(\nu + \rho \dim^2(B)) \qquad \forall x \in \mathcal{B}_\rho \wedge \mathcal{B}'_\nu\,, \tag{45}$$

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

Now we are ready to obtain an analogue of Proposition 6.

Proposition 18. *Let $\mathbf{G}$ be a finite abelian group, $A, B \subseteq \mathbf{G}$ be sets, $|B| = \omega|A|$, $|A+B| = K|A|$, $|A-A| = K'|A|$, and $0 < M \leqslant K$, $0 < M' \leqslant K'$, $\kappa > 0$, $\zeta \in (0,1/2)$, $1 < T \leqslant M'(M+\kappa)\omega^{-1}$ be some parameters. Suppose that*

$$\mathsf{M}^2(A) \leqslant \frac{M|A|^2}{K}, \qquad \mathsf{E}(B) \leqslant \frac{M'|B|^3}{K'}\,, \tag{46}$$

and

$$|A+B|^2 \leqslant \kappa |A| N\,. \tag{47}$$

Then there is a regular Bohr set $\mathcal{B}_* = \mathcal{B}(\Gamma, \varepsilon)$ ($\mathcal{B}_*$ depends on B only) and $z \in \mathbf{G}$ such that

$$|B \cap (\mathcal{B}_* + z)| \geqslant \frac{(1-2\zeta)|\mathcal{B}_*|}{T(M+\kappa)}\,,$$

and

$$\dim(\mathcal{B}_*) \ll (\omega\zeta)^{-2} T^2 (M+\kappa)^2 \cdot \left(\log(\delta^{-1}K) + \log_T(M'(M+\kappa)\omega^{-1}) \cdot \log((M+\kappa)\omega^{-1})\right)\,, \tag{48}$$

as well as

$$|\mathcal{B}_*| \gg N \cdot \exp(-O(\dim(\mathcal{B}_*) \log((\omega\zeta)^{-1}(M+\kappa) T \dim(\mathcal{B}_*))))\,. \tag{49}$$

Proof. We use the same argument and the notation of the proof of Proposition 6. The argument before inequality (31) does not depend on a group, therefore we have

$$\frac{1}{N} \sum_{\xi \in \mathrm{Spec}_{\zeta/M_*}(\varphi)} |\widehat{B}(\xi)|^2 \widehat{\varphi}(\xi) \geqslant \frac{(1-\zeta)\omega b \mathsf{E}_k}{T(M+\kappa)}\,. \tag{50}$$

Applying Lemma 17 with $\mathcal{B} = \mathbf{G}$ (hence $\dim(\mathcal{B}) = 1$), $f = \varphi$, and $\rho = \nu = c\zeta/(M_*|\Lambda|)$, where $c > 0$ is a sufficiently small absolute constant, we see that for any $\xi \in \mathrm{Spec}_{\zeta/M_*}(\varphi)$ one has

$$\mathrm{Spec}_{\zeta/M_*}(\varphi)(\xi) \leqslant |\mathcal{B}_*|^{-2}|\widehat{\mathcal{B}_*}(\xi)|^2(1+\zeta)\,, \tag{51}$$

where $\mathcal{B}_* = \mathcal{B}_\rho \wedge \mathcal{B}'_\nu$. Indeed, we can assume that $\xi \in \mathrm{Spec}_{\zeta/M_*}(\varphi)(\xi)$ because otherwise there is nothing to prove. Then by estimate (45) of Lemma 17, we get (below $C > 0$ is an absolute constant)

$$|\widehat{\mathcal{B}_*}(\xi)| = |\mathcal{B}_*| - |\sum_{x\in\mathcal{B}_*}(1-\xi(x))| \geqslant |\mathcal{B}_*|\left(1 - \frac{2cC\zeta}{M_*}\right)\,,$$

as required. Thus bounds (50), (51) give us

$$\frac{1}{N}\sum_{\xi}|\widehat{B}(\xi)|^2|\widehat{\mathcal{B}_*}(\xi)|^2 \geqslant \frac{(1-2\zeta)\omega b|\mathcal{B}_*|^2}{T(M+\kappa)}\,.$$

This is equivalent to

$$\sum_x (B\circ B)(x)(\mathcal{B}_*\circ\mathcal{B}_*)(x) \geqslant \frac{(1-2\zeta)\omega b|\mathcal{B}_*|^2}{T(M+\kappa)}\,.$$

By the pigeonhole principle there is $z \in \mathbf{G}$ such that

$$|B\cap(\mathcal{B}_*+z)| \geqslant \frac{(1-2\zeta)\omega|\mathcal{B}_*|}{T(M+\kappa)}\,.$$

Now

$$\dim(\mathcal{B}_*) = |\Lambda| \ll (\omega\zeta)^{-2}T^2(M+\kappa)^2\cdot\big(\log(\delta^{-1}K) + \log_T(M'(M+\kappa)\omega^{-1})\cdot\log((M+\kappa)\omega^{-1})\big)\,,$$

see computations in (34)—(36). Applying Lemmas 14, 16, we see that

$$|\mathcal{B}_*| \gg N\cdot(\zeta/(M_*|\Lambda|))^{O(|\Lambda|)} \gg N\cdot\exp(-O(\dim(\mathcal{B}_*)\log((\omega\zeta)^{-1}(M+\kappa)T\dim(\mathcal{B}_*))))\,.$$

Finally, in view of Lemma 13 one can assume that $\mathcal{B}_*$ is a regular Bohr set. This completes the proof. □

Proposition 18 immediately implies an analogue of Corollary 9.

Corollary 19. *Let $\mathbf{G}$ be a finite abelian group, $A \subseteq \mathbf{G}$ be a set, $|A| = \delta N$, $|A-A| = K|A|$, and $1 \leqslant M \leqslant K$ be a parameter. Suppose that*

$$100K^2|A| \leqslant N\,. \tag{52}$$

Then either there is $x \neq 0$ such that

$$|\widehat{A}(x)|^2 > \frac{M|A|^2}{K}\,, \tag{53}$$

or for any $B \subseteq A$ *or* $B \subseteq -A$, $|B| = \beta N$ *there exists a regular Bohr set* $\mathcal{B}_* = \mathcal{B}(\Gamma, \varepsilon)$ *and* $z \in \mathbf{G}$ *such that*

$$|B \cap (\mathcal{B}_* + z)| \geqslant \frac{|\mathcal{B}_*|}{8M},$$

and the bounds

$$\dim(\mathcal{B}_*) \ll (\delta\beta^{-1}M)^2 \left(\log(\delta^{-1}K) + \log^2(\delta\beta^{-1}M)\right), \tag{54}$$

$$|\mathcal{B}_*| \gg N \cdot \exp(-O(\dim(\mathcal{B}_*) \log(\delta\beta^{-1}M \dim(\mathcal{B}_*)))) \tag{55}$$

take place.

Now we present a construction showing that the estimates in Corollary 19 are close to exact.

Example 20. Let p be a prime number, $d \geqslant 4$ be a positive integer, and $\mathbf{G}$ be the cyclic group $\mathbf{G} = \mathbb{F}^*_{p^d}$. Take an arbitrary g such that $\mathbf{G}$ coincides with $\{1, g, \dots, g^{|\mathbf{G}|} - 1\}$ and for any $x \in \mathbf{G}$ put $\mathrm{ind}(x) = j$ iff $x = g^j$. Now choose $A = \{\mathrm{ind}(g + j)\}_{j=0,1,\dots,p-1}$. Then by Katz's result (see [15, Theorem 1] and the proof of [1, Lemma 1]) all non–zero Fourier coefficients of A are bounded by $(d-1)\sqrt{p} = 3\sqrt{|A|}$. Clearly, $K = |A-A|/|A| \leqslant |A|$ and hence

$$\mathsf{M}^2(A) \leqslant (d-1)^2|A| \leqslant \frac{(d-1)^2|A|^2}{K} \ll \frac{|A|^2}{K}. \tag{56}$$

In other words, the set A has small Fourier coefficients. Also,

$$K^2\delta \leqslant |A|^3 p^{-d} = p^{3-d} = o(1)$$

and, therefore, condition (52) is satisfied for large $|\mathbf{G}| = N = p^d$. Now, if there exists a regular Bohr set $\mathcal{B} = \mathcal{B}(\Gamma, \varepsilon)$ and $z \in \mathbf{G}$ such that $|A \cap (\mathcal{B} + z)| \gg |\mathcal{B}|$, then $|\mathcal{B}| \ll |A| = p \ll |\mathbf{G}|^{1/d}$ (if one believes in GRH [13], then it is possible to obtain even better upper bounds for the cardinality of the intersection $A \cap (\mathcal{B} + z)$, see the argument of [12]). But then estimate (55) gives us

$$\dim(\mathcal{B}) \gg \frac{\log N}{\log\log N} \geqslant \frac{\log(\delta^{-1}K)}{\log\log(\delta^{-1}K)},$$

and this coincides with (54) up to double logarithm.

Similarly, it is easy to prove an analogue of Corollary 8 (and we leave the derivation of the analogue of Corollary 10 to the interested reader).

Corollary 21. *Let* $\mathbf{G}$ *be a finite abelian group,* $A \subseteq \mathbf{G}$ *be a set,* $|A| = \delta N$, $|A - A| = K|A|$, *and* $\varepsilon \in (0, 1)$ *be a parameter. Suppose that*

$$100K^2\delta \leqslant \varepsilon.$$

Then either there is $x \neq 0$ such that

$$|\widehat{A}(x)|^2 \geqslant \frac{(2-\varepsilon)|A|^2}{K}\,,$$

or there is a regular Bohr set $\mathcal{B}_* = \mathcal{B}(\Gamma, \varepsilon)$ and $z \in \mathbf{G}$ such that $\mathcal{B}_* \subseteq A - A$ and

$$\dim(\mathcal{B}_*) \ll \varepsilon^{-2} \log(\delta^{-1}K) + \varepsilon^{-3}\,, \tag{57}$$

as well as

$$|\mathcal{B}_*| \gg N \cdot \exp(-O(\dim(\mathcal{B}_*) \cdot \log(\varepsilon^{-1} \dim(\mathcal{B}_*))))\,. \tag{58}$$

Proof. We apply the argument of Proposition 18 with $B = -A$, $\omega = 1$, $M = 2 - \varepsilon$, $M' = \left(1 + \frac{\kappa}{KM}\right) M \leqslant M + \kappa$ (see Remark 7), $T = 1 + \kappa$, and $\kappa = \zeta = \varepsilon/200$, say. Thus we find a Bohr set $\mathcal{B}_* \subseteq \mathbf{G}$ and $z \in \mathbf{G}$ such that

$$(A * \mu)(z) \geqslant \frac{(1-2\zeta)|\mathcal{L}|}{T(M+\kappa)} \geqslant \left(\frac{1}{2} + \frac{\varepsilon}{8}\right)\,, \tag{59}$$

where μ is any measure on $\mathcal{B}_*$. Also, we have

$$d := \dim(\mathcal{B}_*) \ll \zeta^{-2} T^2 (M+\kappa)^2 \cdot \left(\log(\delta^{-1}K) + \log_T(M'(M+\kappa)) \cdot \log(M+\kappa)\right)$$
$$\ll \varepsilon^{-2} \log(\delta^{-1}K) + \varepsilon^{-3}\,,$$

and thanks to Lemmas 14, 16, one has

$$|\mathcal{B}_*| \gg N \cdot (\zeta/(M_*|\Lambda|))^{O(|\Lambda|)} \gg N \cdot \exp(-O(\dim(\mathcal{B}_*) \cdot \log(\varepsilon^{-1} \dim(\mathcal{B}_*))))\,.$$

Now we follow the argument of [22, Lemma 9.2]. Namely, put $t = \lceil 100\varepsilon^{-1} d \rceil$ and $\eta = 1/2t$ and consider the sequence of Bohr sets

$$(\mathcal{B}_*)_{1/2} \subseteq (\mathcal{B}_*)_{1/2+\eta} \subseteq \cdots \subseteq (\mathcal{B}_*)_{1/2+t\eta} = \mathcal{B}_*\,.$$

Applying Lemma 15, we see that there is $j \in [t]$ such that

$$|\mathcal{B}''| := |(\mathcal{B}_*)_{1/2+j\eta}| \leqslant 8^{(d+1)/t} |(\mathcal{B}_*)_{1/2+(j-1)\eta}| \leqslant (1+\varepsilon/4)|(\mathcal{B}_*)_{1/2+(j-1)\eta}| := (1+\varepsilon/4)|\mathcal{B}'|\,. \tag{60}$$

Consider the measure $\mu(x) = \frac{\mathcal{B}'(x) + \mathcal{B}''(x)}{|\mathcal{B}'| + |\mathcal{B}''|}$, $\mathsf{supp}(\mu) \subseteq \mathcal{B}_*$. Then inequality (59) gives us

$$|A \cap (\mathcal{B}' + z)| + |A \cap (\mathcal{B}'' + z)| \geqslant \left(\frac{1}{2} + \frac{\varepsilon}{8}\right) \cdot (|\mathcal{B}'| + |\mathcal{B}''|)\,. \tag{61}$$

One the other hand, for any $x \in (\mathcal{B}_*)_\eta$, we have

$$(A \circ A)(x) \geqslant ((A \cap (\mathcal{B}' + z)) \circ (A \cap (\mathcal{B}'' + z)))(x)$$

$$\geqslant |A \cap (\mathcal{B}' + z)| + |A \cap (\mathcal{B}'' + z)| - |(A \cap (\mathcal{B}' + z + x)) \bigcup (A \cap (\mathcal{B}'' + z))|$$

$$\geqslant |A \cap (\mathcal{B}' + z)| + |A \cap (\mathcal{B}'' + z)| - |A \cap (\mathcal{B}'' + z)| \geqslant |A \cap (\mathcal{B}' + z)| + |A \cap (\mathcal{B}'' + z)| - |\mathcal{B}''| .$$

Using formulae (60), (61), we get

$$(A \circ A)(x) \geqslant \left(\frac{1}{2} + \frac{\varepsilon}{8}\right) \cdot (|\mathcal{B}'| + |\mathcal{B}''|) - |\mathcal{B}''| = \left(\frac{1}{2} + \frac{\varepsilon}{8}\right) |\mathcal{B}'| - \left(\frac{1}{2} - \frac{\varepsilon}{8}\right) \left(1 + \frac{\varepsilon}{4}\right) |\mathcal{B}'|$$

$$\geqslant \frac{\varepsilon |\mathcal{B}'|}{8} > 0 . \tag{62}$$

The inequality (62) implies that $(\mathcal{B}_*)_\eta \subseteq A - A$. We see that (57), (58) take place (use Lemmas 14, 16 again) and thanks to Lemma 13 one can assume that we have to deal with a regular Bohr set. This completes the proof. □

Problem 22. In Example 20 we constructed a set $A \subseteq \mathbf{G}$, $|A| = \delta |\mathbf{G}|$, $|A - A| = K|A|$ such that for $d > 1$ one has

$$K^{d-1} \delta \sim 1 , \tag{63}$$

and

$$\mathsf{M}^2(A) \leqslant \frac{(d-1)^2 |A|^2}{K} ,$$

see formula (56) of Example 56. On the other hand, we always have a universal lower bound (5), provided $d \geqslant 4$. Given $d > 1$ and a set A such that (63) takes place, what are the proper upper/lower bounds for $\mathsf{M}(A)$?

Acknowledgements

The author expresses deep gratitude to the reviewer for valuable comments and suggestions that significantly improved the presentation of the article.

References

[1] J. Andersson. On some power sum problems of Montgomery and Turán. *International mathematics research notices*, 2008:rnn015, 2008.

[2] M. Bateman and N. Katz. New bounds on cap sets. *Journal of the American Mathematical Society*, 25(2):585–613, 2012.

[3] T. F. Bloom and O. Sisask. The Kelley–Meka bounds for sets free of three-term arithmetic progressions. arXiv:2302.07211, 2023.

[4] J. Bourgain. On triples in arithmetic progression. *Geometric and Functional Analysis*, 9(5):968–984, 1999.

[5] M.-C. Chang. A polynomial bound in Freiman's theorem. *Duke Math. J.*, 113(3):399–419, 2002.

[6] E. Croot and O. Sisask. A probabilistic technique for finding almost-periods of convolutions. *Geometric and functional analysis*, 20:1367–1396, 2010.

[7] G. A. Freiman. Inverse problems in additive number theory. Addition of sets of residues modulo a prime. *Doklady Akademii Nauk*, 141(3):571–573, 1961.

[8] W. Gowers, B. Green, F. Manners, and T. Tao. Marton's Conjecture in abelian groups with bounded torsion. arXiv:2404.02244, 2024.

[9] W. Gowers, B. Green, F. Manners, and T. Tao. On a conjecture of Marton. *Annals of Mathematics*, 201(2):515–549, 2025.

[10] B. Green. Finite field models in additive combinatorics. *Bridget S. Webb (Ed.), Surveys in Combinatorics 2005*, pages 1–27, 2005.

[11] B. Green and I. Z. Ruzsa. Sets with small sumset and rectification. *Bulletin of the London Mathematical Society*, 38(1):43–52, 2006.

[12] B. Hanson. Character sums over Bohr sets. *Canadian Mathematical Bulletin*, 58(4):774–786, 2015.

[13] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53. American Mathematical Soc., 2021.

[14] N. H. Katz and P. Koester. On additive doubling and energy. *SIAM Journal on Discrete Mathematics*, 24(4):1684–1693, 2010.

[15] N. M. Katz. An estimate for character sums. *Journal of the American Mathematical Society*, 2(2):197–200, 1989.

[16] Z. Kelley and R. Meka. Strong Bounds for 3-Progressions. *IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 933–973, 2023.

[17] V. F. Lev and O. Serra Albó. Towards $3n-4$ in groups of prime order. *The Electronic Journal of Combinatorics*, 30: #P248, 2023.

[18] V. F. Lev and I. D. Shkredov. Small doubling in prime-order groups: from 2.4 to 2.6. *J. Number Theory*, 217:278–291, 2020.

[19] K. F. Roth. On certain sets of integers. *J. London Math. Soc*, 28(1):104–109, 1953.

[20] I. Z. Ruzsa. Generalized arithmetical progressions and sumsets. *Acta Mathematica Hungarica*, 65(4):379–388, 1994.

[21] T. Sanders. On certain other sets of integers. *Journal d'Analyse Mathématique*, 116(1):53, 2012.

[22] T. Sanders. On the Bogolyubov–Ruzsa lemma. *Analysis & PDE*, 5(3):627–655, 2012.

[23] T. Sanders. The structure theory of set addition revisited. *Bulletin of the American Mathematical Society*, 50(1):93–127, 2013.

[24] T. Schoen. Multiple set addition in $\mathbb{Z}_p$. *Integers: Electronic Journal of Combinatorial Number Theory*, 3(A17):2, 2003.

[25] T. Schoen and I. D. Shkredov. Higher moments of convolutions. *J. Number Theory*, 133(5):1693–1737, 2013.

[26] I. D. Shkredov. Structure theorems in additive combinatorics. *Uspekhi Mat. Nauk*, 70(1(421)):123–178, 2015.

[27] I. D. Shkredov. Uncertainty for convolutions of sets. arXiv:2404.12469, 2024.

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