Uncertainty for convolutions of sets

I.D. Shkredov

Annotation.

The paper obtains the optimal form of the uncertainty principle in the special case of convolution of sets.

1 Introduction

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

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

A number of uncertainty principles on $\mathbf{G}$ assert, roughly, that a function on $\mathbf{G}$ and its Fourier transform cannot be simultaneously highly concentrated. This topic is quite popular see, e.g., papers [1], [2], [7], [10]. The most basic example is an inequality which connects the sizes of the supports of f and $\widehat{f}$ to the size of the finite group $\mathbf{G}$, namely,

$$|\mathsf{supp} f| \cdot |\mathsf{supp} \widehat{f}| \geqslant |\mathbf{G}| \,, \tag{2}$$

and, of course, it is worth mentioning the classical Heisenberg inequality for $\mathbf{G} = \mathbb{R}$, which states that for any $a, b \in \mathbb{R}$ one has

$$\int_{\mathbb{R}} (x-a)^2 |f(x)|^2 \, dx \cdot \int_{\mathbb{R}} (\xi - b)^2 |\widehat{f}(\xi)|^2 \, d\xi \geqslant \frac{\|f\|_2^4}{16\pi^2} \,. \tag{3}$$

For more background on the Fourier transform on abelian groups and the uncertainty principle we refer to [11] and the excellent surveys [3] and [12].

This paper considers the case when the function f has a special form, namely, f is the convolution of the characteristic function of a set $A \subseteq \mathbf{G}$ (all required definitions can be found in Section 2). This allows us to obtain a new optimal form of the uncertainty principle in terms of the difference set $A - A$ (we also consider the asymmetric case, see Theorem 4 below). Given two sets $A, B \subseteq \mathbf{G}$, define the *sumset* of A and B as

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

In a similar way we define the *difference sets* and the *higher sumsets*, e.g., $2A - A$ is $A + A - A$. Consider two quantities

$$\rho(A) := \max_{x \neq 0} |A \cap (A + x)|\,, \tag{4}$$

and

$$M(A) := \max_{\xi \neq 0} |\widehat{A}(\xi)|\,, \tag{5}$$

where we use the same capital letter to denote a set $A \subseteq \mathbf{G}$ and its characteristic function $A : \mathbf{G} \to \{0, 1\}$.

Theorem 1 *Let* $\mathbf{G}$ *be a finite abelian group,* $A \subseteq \mathbf{G}$*,* $|A| = \delta|\mathbf{G}|$*, and let* $|A - A| = K|A|$*. Suppose that* $|A| \to \infty$*,* $\log^2 K = o(\log |A|)$ *and*

$$K^2 \delta = o(1)\,. \tag{6}$$

Then

$$M^2(A)\rho(A) \geqslant \frac{|A|^3}{K} \cdot (1 - o(1))\,. \tag{7}$$

In other words, if f is the convolution of the characteristic function of a set $A \subseteq \mathbf{G}$, then

$$\max_{x \neq 0} |f(x)| \cdot \max_{\xi \neq 0} |\widehat{f}(\xi)| \geqslant \frac{|A|^3}{K} \cdot (1 - o(1))\,. \tag{8}$$

It is easy to see that bound (7) is tight (also, see Remark 6 below). Indeed, take $\mathbf{G} = \mathbb{F}_2^n$, let H be a proper subspace of $\mathbf{G}$ and let $A \subseteq H$ be a random set of positive density. Then with high probability

$$K|A| := |A - A| = |H|(1 - o(1)), \qquad \rho(A) \leqslant \frac{|A|}{K} \cdot (1 - o(1))$$

and $\mathsf{E}(A, H) = |A|^2|H|$. The last identity implies $M(A) = |A|(1 - o(1))$ and the same asymptotic formula follows from our bound (7). As for condition (6), we definitely need that $K\delta = o(1)$ (consider the case of a random set A). Finally, note that in our proof we make extensive use of the form of the function f (for example, we widely use of the concept of higher sumsets/higher energies, see [8]) and it seems like any reasonable analogue of (8) for general f fails, see Remark 5 below.

We thank Vsevolod F. Lev for useful discussions and valuable comments.

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, we put

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

Also, let $\Delta_k(x) := \Delta_k(\{x\})$, $x \in \mathbf{G}$. Now we have

$$A - A := \{a - b \ : \ a, b \in A\} = \{s \in \mathbf{G} \ : \ A \cap (A + s) \neq \emptyset\} . \tag{9}$$

A natural generalization of the last formula in (9) is the set

$$\{(x_1, \dots, x_k) \in \mathbf{G}^k \ : \ A \cap (A + x_1) \cap \dots \cap (A + x_k) \neq \emptyset\} = A^k - \Delta_k(A) , \tag{10}$$

which is called the *higher difference set* (see [8]). Given a positive integer k, we put as in [6]

$$R_A^{(k+1)}(x_1, \dots, x_k) = |A \cap (A + x_1) \cap \dots \cap (A + x_k)| , \qquad x_1, \dots, x_k \in \mathbf{G} .$$

Thus, $(x_1, \dots, x_k) \in A^k - \Delta_k(A)$ iff $R_A^{(k+1)}(x_1, \dots, x_k) > 0$. 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 $\mathsf{E}(A, A)$. Similarly,

$$\mathsf{T}_k(A) := |\{(a_1, \dots, a_k, a'_1, \dots, a'_k) \in A^{2k} \ : \ a_1 + \dots + a_k = a'_1 + \dots + a'_k\}| . \tag{11}$$

Also, one can define the *higher energy* (see [8])

$$\mathsf{E}_k(A) = \sum_x (A \circ A)^k(x) = \sum_{x_1, \dots, x_{k-1}} R^{(k)}(x_1, \dots, x_{k-1})^2 := \mathsf{E}_{k,2}(A) . \tag{12}$$

It is known and easy to check (see, e.g., [6, proof of Theorem 4]) that $\mathsf{E}_{k,l}(A) = \mathsf{E}_{l,k}(A)$ for any integers $k, l > 1$. Note that the first formula in (12) can be thought of as the definition of $\mathsf{E}_k(A)$ for any real $k > 1$.

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

$$N \sum_{g \in \mathbf{G}} |f(g)|^2 = \sum_{\xi \in \widehat{\mathbf{G}}} \big|\widehat{f}(\xi)\big|^2 . \tag{13}$$

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

$$\widehat{f * g} = \widehat{f} \widehat{g} . \tag{14}$$

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, $A^{(4)}(0) = \mathsf{E}(A)$. Also, let $\mathsf{T}_k(f) = \sum_x (f^{(k)}(x))^2$.

We need a particular case of Corollary 1 from [9].

Lemma 2 *Let $k \geqslant 2$ be an even integer, $l \geqslant 2$ be any integer and $A \subseteq \mathbf{G}$ be a set. Then*

$$\sum_x (A^{(k)}(x))^l = \mathsf{T}_{k/2}(R_A^{(l)})\,. \tag{15}$$

Also, we need the generalized triangle inequality [8, Theorem 7].

Lemma 3 *Let k_1, k_2 be positive integers, $W \subseteq \mathbf{G}^{k_1}$, $Y \subseteq \mathbf{G}^{k_2}$ and $X, Z \subseteq \mathbf{G}$. Then*

$$|W \times X||Y - \Delta_{k_2}(Z)| \leqslant |W \times Y \times Z - \Delta_{k_1+k_2+1}(X)|\,. \tag{16}$$

We have defined the quantity $\rho(A)$ and $M(A)$ in formulae (4), (5) above. More generally, consider

$$\rho^{(k)}(A) := \max_{x \neq 0} A^{(k)}(x)\,.$$

Thus $A^{(2)}(x) = (A \circ A)(x) = |A \cap (A + x)|$. Similarly to formula (4) we put for any positive integer $l > 1$

$$\rho_l(A) := \max_{|X|=l} |A_X|\,,$$

where $A_X := (A + x_1) \cap (A + x_2) \cap \cdots \cap (A + x_l)$ and $X = \{x_1, \dots, x_l\}$ is a set of the cardinality l. Thus $\rho_2(A) = \rho(A)$. If $X = \{0, x\}$, where $x \in \mathbf{G}$, then we write $A_{\{0,x\}} = A_x = A \cap (A + x)$. The inclusion of Katz–Koester [4] is

$$B + A_x \subseteq (A + B)_x\,. \tag{17}$$

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

3 The proof of the main result

We are ready to obtain our first main result, which implies Theorem 1 from the introduction.

Theorem 4 *Let $\mathbf{G}$ be a finite abelian group, $A, B \subseteq \mathbf{G}$, $|A| = \delta N$, $\delta \in (0, 1]$, further $|B| = \zeta |A|$, $|A - A| = K|A|$, $|B - B| = K_*|B|$, and let $|A + B| = \omega |A - A|$, where $\zeta, \omega \in \mathbb{R}^+$. Suppose that $|A| \geqslant (2K \cdot \max\{1, \omega\})^8$. Then*

$$M^2(B)\rho(A) \geqslant \frac{|A|^2|B|^2}{|A+B|} \cdot \left(1 - \frac{6 \log K \cdot \log(\zeta K K^*)}{\log |A|} - (\omega K)^2 \delta\right)\,, \tag{18}$$

and, similarly,

$$M(A - A)\rho^2(A) \geqslant \frac{|A|^3}{K} \cdot \left(1 - \frac{16 \log^2(2K)}{\log |A|} - K^3 \delta\right)\,. \tag{19}$$

P r o o f. Let $\rho = \rho(A)$, $M = M(B)$, $D = A - A$, $S = A + B$, $|D| = K|A|$, $|S| = \omega|D|$, and $\kappa := K\delta\omega \leqslant 1$. By the usual triangle inequality for sets (take $k_1 = k_2 = 1$ in Lemma 3), we have $|A||B - B| \leqslant |A + B|^2$ and hence

$$\zeta K_* \leqslant \omega^2 K^2 . \tag{20}$$

Also, let $n \geqslant 2$ be a positive integer and put

$$|A^{n-1} - \Delta_{n-1}(A)| = \varepsilon_{n-1} |D|^{n-1} , \tag{21}$$

where

$$K^{-n} \leqslant \varepsilon_n \leqslant 1 . \tag{22}$$

Then by the Cauchy–Schwarz inequality and the second equality in (12) one has

$$|A|^{2n} \leqslant |A^{n-1} - \Delta_{n-1}(A)| \mathsf{E}_n(A) \leqslant \varepsilon_{n-1} |D|^{n-1} (\rho^{n-1} |A|^2 + |A|^n) \tag{23}$$

$$= \varepsilon_{n-1} |D|^{n-1} \rho^{n-1} |A|^2 + \varepsilon_{n-1} K^{n-1} |A|^{2n-1} . \tag{24}$$

Thus, we get

$$\rho \geqslant \varepsilon_{n-1}^{-\frac{1}{n-1}} \cdot \frac{|A|}{K} \left(1 - \frac{\varepsilon_{n-1} K^{n-1}}{|A|} \right)^{1/(n-1)} > \varepsilon_{n-1}^{-\frac{1}{n-1}} \cdot \frac{|A|}{K} \left(1 - \frac{2\varepsilon_{n-1} K^{n-1}}{(n-1)|A|} \right) , \tag{25}$$

provided $n \leqslant 2^{-1} \log_K |A|$. Now using Lemma 3, we obtain for an arbitrary set $M \subseteq \mathbf{G}$ and any positive integer m

$$\varepsilon_{m-1} |M||D|^{m-1} = |M||A^{m-1} - \Delta_{m-1}(A)| \leqslant |A^m - \Delta_m(M)| \leqslant |A - M|^m ,$$

and thus replacing M to $(-M)$, we derive

$$|A + M| \geqslant \varepsilon_{m-1}^{1/m} \cdot \left(\frac{|M|}{|D|} \right)^{1/m} |D| . \tag{26}$$

Finally, we repeat the argument from [5]. Using (26), the inclusion (17) and the Hölder inequality, one obtains

$$\sigma := \sum_x |B_x||S_x| \geqslant \sum_x |B_x||A + B_x| \geqslant \varepsilon_{m-1}^{1/m} |D|^{1-1/m} \sum_x |B_x|^{1+1/m}$$

$$\geqslant \varepsilon_{m-1}^{1/m} K|A||B|^2 (\zeta K K_*)^{-1/m} . \tag{27}$$

Applying the Fourier transform, formula (14) and the Parseval identity (13), we get

$$\sigma = N^{-1} \sum_\xi |\widehat{B}(\xi)|^2 |\widehat{S}(\xi)|^2 \leqslant \frac{\omega^2 K^2 |B|^2 |A|^2}{N} + M^2 \cdot (\omega K|A| - \omega^2 K^2 |A|^2 / N)$$

$$< \omega\kappa K|A||B|^2 + \omega K M^2 |A| . \tag{28}$$

Combining the last two bounds, we have

$$\omega M^2 > \left(\varepsilon_{m-1}^{1/m}(\zeta K K_*)^{-1/m} - \omega\kappa\right)|B|^2 \,. \tag{29}$$

Taking $m = n = [2^{-1}\log_K |A|] \geqslant 2$ and multiplying (25), (29), we obtain in view of estimates (20), (22) that

$$\begin{aligned}
\omega M^2 \rho &\geqslant \frac{|A||B|^2}{K} \cdot \left(1 - \frac{2\varepsilon_{n-1}K^{n-1}}{(n-1)|A|}\right)\left(\varepsilon_{n-1}^{-\frac{1}{n(n-1)}}(\zeta K K_*)^{-1/n} - \varepsilon_{n-1}^{-\frac{1}{n-1}}\omega\kappa\right) \\
&> \frac{|A||B|^2}{K} \cdot \left(1 - \frac{2}{\sqrt{|A|}}\right)\left(1 - \frac{\log(\zeta K K^*)}{n} - K\kappa\omega\right) \\
&\geqslant \frac{|A||B|^2}{K} \cdot \left(1 - \frac{2}{\sqrt{|A|}}\right)\left(1 - \frac{4\log K \cdot \log(\zeta K K^*)}{\log|A|} - K\kappa\omega\right) \\
&> \frac{|A||B|^2}{K} \cdot \left(1 - \frac{6\log K \cdot \log(\zeta K K^*)}{\log|A|} - K\kappa\omega\right)
\end{aligned} \tag{30}$$

as required.

It remains to obtain (19). In this case we use calculations similar to (27) (now $B = A$) and consider

$$\begin{aligned}
\sigma_* = \sum_{x\in D} |D_x| &\geqslant \sum_{x\in D} |A - A_x| \geqslant \varepsilon_{m-1}^{1/m}|D|^{1-1/m}\sum_{x\in D}|A_x|^{1/m} \\
&> \varepsilon_{m-1}^{1/m}K\rho^{-1}|A|^3(|D|/\rho)^{-1/m} - \varepsilon_{m-1}^{1/m}K\rho^{-1}|A|^2(|D|/\rho)^{-1/m} \,.
\end{aligned}$$

As in (28) putting $\kappa_* = \delta K^2\rho|A|^{-1} \leqslant \delta K^2$, we get

$$\begin{aligned}
\sigma_* = N^{-1}\sum_{\xi}\widehat{D}(\xi)|\widehat{D}(\xi)|^2 &\leqslant \frac{K^3|A|^3}{N} + M(D)\cdot(K|A| - K^2|A|^2/N) \\
&< \kappa_* K|A|^3\rho^{-1} + KM(D)|A| \,.
\end{aligned}$$

Combining the last two bounds, we derive

$$M(D)\rho > \left(\varepsilon_{m-1}^{1/m}(|D|/\rho)^{-1/m}(1-|A|^{-1}) - \kappa_*\right)|A|^2 \geqslant \left(\varepsilon_{m-1}^{1/m}(2K)^{-2/m}(1-|A|^{-1}) - \kappa_*\right)|A|^2 \,.$$

Here we have used the simple bound $\rho \geqslant |A|/(2K)$. Taking $m = n = [2^{-1}\log_K |A|] \geqslant 2$ and multiplying the last estimate by (25), we obtain the desired bound (19). This completes the proof. $\square$

Let us discuss obtained inequalities (7), (18). First of all, one can check that the both bounds are tight, see the construction after formula (8). Secondly, it is easy to make sure that our uncertainty principle does not hold for an arbitrary function.

Remark 5 *Inequalities* (7), (18) *have no place for any function* f, *namely, the bounds*

$$\|\widehat{f}\|_\infty \cdot \|f\|_\infty \cdot |\mathsf{supp} f| \geqslant \|f\|_1^2\,, \tag{31}$$

$$\max_{\xi\neq 0} |\widehat{f}(\xi)| \cdot \max_{x\neq 0} |f(x)| \cdot |\mathsf{supp} f| \geqslant \|f\|_1^2\,, \tag{32}$$

fail. Indeed, let p *be a prime number,* $\mathbf{G} = \mathbb{Z}/p\mathbb{Z}$, *and* $f(x) = A(x) - |A|/p$ *be the balanced function of a random set* A *of size* $|A| > p^{2/3+\varepsilon}$, *where* $\varepsilon > 0$ *(one can even take the set of quadratic residues to get a constructive example). Then the right–hand side of* (31), (32) *is* $|A|^2$ *but the left–hand side of* (31), (32) *is* $O(\sqrt{|A|}p^{1+o(1)}) = o(|A|^2)$.

Remark 6 *It is easy to see that the argument of the proof of Theorem 4 gives us*

$$\mathsf{E}_k(A)\mathsf{E}^k(A,D) \geqslant \frac{|A|^{4k+1}}{K}\,, \tag{33}$$

and the last bound is tight up to constants. Indeed, let $\mathbf{G} = \mathbb{F}_2^n$ *and let* $A = H + \Lambda$, $|A| = |H||\Lambda|$, *where* $H \leqslant \mathbf{G}$ *and* $|\Lambda| = K$ *be a basis (for* $\mathbf{G} = \mathbb{Z}$ *a similar construction can be found in [6, Claim 1]). Then for* $x \in H$ *one has* $|A_x| = |A|$ *and for* $x \in D \setminus H$ *the following holds* $|A_x| = 2|A|/K$. *Thus* $\mathsf{E}(A,D) = O(|A|^3)$, $\mathsf{E}_k(A) = \frac{|A|^{k+1}}{K}(1 + o_K(1))$ *and* (33) *is sharp (up to constants).*

The example above shows (also, see [6, Claim 1]) that set of large A_x *has measure zero. Similarly,* $\widehat{A}(\xi) = |H|H^\perp(\xi)\widehat{\Lambda}(\xi)$ *and thus the set of large Fourier coefficients of* A *has measure zero as well. Therefore, inequality* (18) *is rather delicate and has place on a set of measure zero.*

Using the arguments similar to [6] (also, see [8]) we obtain an analogue of Theorem 4 for the quantity $\rho_l(A)$. Here and below, for simplicity, we consider the symmetric case $A = B$.

Theorem 7 *Let* $\mathbf{G}$ *be a finite abelian group,* $A \subseteq \mathbf{G}$, $|A| = \delta N$, $l > 1$ *be a positive integer, and let* $|A - A| = K|A|$. *Suppose that* $|A| \geqslant K^{8(l-1)}$, *and* $|A| > 4l^4$. *Then*

$$M^{2(l-1)}(A)\rho_l(A) \geqslant \frac{|A|^{2l-1}}{K^{l-1}} \cdot \left(1 - \frac{2l^2}{\sqrt{|A|}}\right)\left(1 - \frac{12(l-1)\log^2 K}{\log|A|} - K^2\delta\right)^{l-1}\,. \tag{34}$$

P r o o f. We use the notation and the argument of the proof of Theorem 4. Let $\rho_l = \rho_l(A)$. Applying the Hölder inequality, we obtain an analogue of calculations in (23), (24) (see [6, proof of Theorem 4])

$$|A|^{ln} = \left(\sum_{x_1,\dots,x_{n-1}} R_A^{(n)}(x_1,\dots,x_{n-1})\right)^l \leqslant |A^{n-1} - \Delta_{n-1}(A)|^{l-1}\mathsf{E}_{l,n}(A)$$

$$\leqslant \varepsilon_{n-1}^{l-1}|D|^{(l-1)(n-1)}\mathsf{E}_{n,l}(A) \leqslant \varepsilon_{n-1}^{l-1}|D|^{(l-1)(n-1)}\left(\rho_l^{n-1}|A|^l + l^2|A|^{n+l-2}\right)$$

and hence

$$\rho_l \geqslant \varepsilon_{n-1}^{-\frac{l-1}{n-1}} \cdot \frac{|A|}{K^{l-1}} \left(1 - \frac{l^2 \varepsilon_{n-1}^{l-1} K^{(l-1)(n-1)}}{|A|}\right)^{1/(n-1)} \geqslant \varepsilon_{n-1}^{-\frac{l-1}{n-1}} \cdot \frac{|A|}{K^{l-1}} \left(1 - \frac{2l^2 \varepsilon_{n-1}^{l-1} K^{(l-1)(n-1)}}{(n-1)|A|}\right),$$

provided $(l-1)n \leqslant 2^{-1} \log_K |A|$. After that we repeat the proof of Theorem 4, namely, we put $m = n = [(2(l-1))^{-1} \log_K |A|] \geqslant 2$ and obtain

$$M^{2(l-1)} \rho_l \geqslant \frac{|A|^{2l-1}}{K^{l-1}} \cdot \left(1 - \frac{2l^2 \varepsilon_{n-1}^{l-1} K^{(l-1)(n-1)}}{(n-1)|A|}\right) \left(\varepsilon_{n-1}^{-\frac{1}{n(n-1)}} K^{-2/n} - \varepsilon_{n-1}^{-\frac{1}{n-1}} \kappa\right)^{l-1}$$

$$\geqslant \frac{|A|^{2l-1}}{K^{l-1}} \cdot \left(1 - \frac{2l^2}{\sqrt{|A|}}\right) \left(1 - \frac{12(l-1)\log^2 K}{\log |A|} - K\kappa\right)^{l-1},$$

where we have used inequality (29). This completes the proof. □

4 Further generalizations

Now we obtain an analogue of Theorem 4 for the quantity $\rho^{(k)}(A)$, $k > 2$. First of all, we give a trivial lower bound for $\rho^{(k)}(A)$. Let $k = 2s \geqslant 4$ for simplicity. Using the Cauchy–Schwartz inequality, one has

$$\frac{|A|^{k+2}}{|sA \pm A|} \leqslant \mathsf{T}_{s+1}(A) = \sum_x A^{(k)}(x) A^{(2)}(x) \leqslant \mathsf{T}_s(A)|A| + \rho^{(k)}(A)|A|^2 . \qquad (35)$$

Hence, if we ignore the first term in (35) (it is easy to see that it is negligible for small $|sA \pm A|$), then we derive

$$\rho^{(k)}(A) \geqslant \frac{|A|^k}{|sA \pm A|} \cdot (1 - o(1)) \qquad (36)$$

and this estimate can be considered as a trivial lower bound for the quantity $\rho^{(k)}(A)$.

Theorem 8 *Let $\mathbf{G}$ be a finite abelian group, $A \subseteq \mathbf{G}$ and let $k = 2s \geqslant 2$ be a positive integer. Also, let $|A| = \delta N$, $|sA \pm A| = K|A|$ and $|sA - sA| = K_*|A|$. Suppose that*

$$|A|^{nk-n+1} \geqslant K_*^8 \mathsf{T}_s^n(A),$$

and $|A| > 4$. Then

$$M^2(A) \rho^{(k)}(A) \geqslant \frac{|A|^{k+1}}{K} \cdot \left(1 - \frac{14 \log^2 K_*}{\log |A|} - \delta K K_*\right). \qquad (37)$$

Proof. We use the argument of the proof of Theorem 4. Let $\rho = \rho^{(k)}(A)$, $D = A - A$, $|sD| = K_* |A|$ and put

$$|s(A^{n-1} - \Delta_{n-1}(A))| = |(sA)^{n-1} - \Delta_{n-1}(sA)| := \varepsilon_{n-1} |sD|^{n-1} \,,$$

where

$$\frac{1}{K_*^n} \leqslant \frac{|sA|^n}{|sD|^n} \leqslant \varepsilon_n \leqslant 1 \,.$$

Then by the Cauchy–Schwarz inequality and Lemma 2 one has

$$|A|^{nk} \leqslant |(sA)^{n-1} - \Delta_{n-1}(sA)| \mathsf{T}_s(R_A^{(n)}) = \varepsilon_{n-1} |sD|^{n-1} \cdot \sum_x (A^{(k)}(x))^n \tag{38}$$

$$\leqslant \varepsilon_{n-1} |sD|^{n-1} (\rho^{n-1} |A|^k + \mathsf{T}_s^n(A)) \,, \tag{39}$$

and hence

$$\rho \geqslant \varepsilon_{n-1}^{-\frac{1}{n-1}} \cdot \frac{|A|^{k-1}}{K_*} \left(1 - \frac{\varepsilon_{n-1} K_*^{n-1} \mathsf{T}_s^n(A)}{|A|^{nk-n+1}} \right)^{1/(n-1)} \geqslant \varepsilon_{n-1}^{-\frac{1}{n-1}} \cdot \frac{|A|^{k-1}}{K_*} \left(1 - \frac{2\varepsilon_{n-1} K_*^{n-1} \mathsf{T}_s^n(A)}{(n-1)|A|^{nk-n+1}} \right) \,,$$

provided $n \leqslant 2^{-1} \log_{K_*} (|A|^{nk-n+1} \mathsf{T}_s^{-n}(A))$. Now let $Q = sA \pm A$, $|Q| = K|A|$. Then the inclusion of Katz–Koester (17) gives us $sA \pm A_x \subseteq Q_{\pm x}$. Hence as in the proof of Theorem 4, we get

$$\sigma := \sum_x |A_x| |Q_x| \geqslant \varepsilon_{m-1}^{1/m} |sD|^{1-1/m} \sum_x |A_x|^{1+1/m} \geqslant \varepsilon_{m-1}^{1/m} K_* |A|^3 K_*^{-2/m} \,.$$

On the other hand, there is the upper bound (28) for σ. Putting

$$m = n = [2^{-1} \log_{K_*} (|A|^{nk-n+1} \mathsf{T}_s^{-n}(A))] \geqslant 2$$

we can repeat the argument of the proof of Theorem 4. $\square$

Remark 9 *If $\mathbf{G} = \mathbb{Z}/p\mathbb{Z}$, where p is a prime number and $|sA - sA| \leqslant \min\{2(p+1)/3, |sA|^{1+o(1)}\}$, then it is possible to obtain another lower bound for the quantity $\rho^{(k)}(A)$, namely,*

$$\rho^{(k)}(A) \geqslant \frac{2|A|^k}{|sA - sA|} \cdot (1 - o(1)) \,. \tag{40}$$

Indeed, combine the estimate $|(sA)^{n-1} - \Delta_{n-1}(sA)| \leqslant (1/2 + o(1))^{n-1} |sD|^{n-1}$ from [6, Theorem 1, Proposition 1] and calculations in (38), (39) above. Estimate (40) shows that there are some irregularities in the distribution of the quantity $\rho^{(k)}(A)$ and may be of interest in itself.

In the last result, we make no assumptions about the size of $A \pm A$, but only use the additive energy of A. The resulting estimate (42) is not as accurate as in Theorems 4, 7, 8 but nevertheless it is optimal up to logarithms.

Theorem 10 *Let* $\mathbf{G}$ *be a finite abelian group,* $A \subseteq \mathbf{G}$*,* $|A| = \delta N$*, and* $\mathsf{E}(A) = |A|^3/K$*. Suppose that* $|A| \geqslant 8K^3$*, and*

$$\delta^3 L^{28} K^{25} \ll 1\,. \tag{41}$$

Then

$$\rho^7(A) M^4(A) \log^7 |A| \gg \frac{|A|^{11}}{K^7}\,. \tag{42}$$

Proof. Let $L = \log |A|$, $\rho = \rho(A)$ and $M = M(A)$. Also, let $\Delta > 0$ be a real number and $P = \{s \ :\ \Delta < |A_s| \leqslant 2\Delta\}$ be a set such that $\Delta^{10/7}|P| \gg \mathsf{E}_{10/7}(A)/L$. It is easy to see that the number Δ and the set P exist by the pigeonhole principle. Clearly, we have

$$\mathsf{E}(A)\rho^{-4/7}L^{-1} \ll \mathsf{E}_{10/7}(A)L^{-1} \ll \Delta^{10/7}|P| \ll |A|^2\Delta^{3/7}\,,$$

and thus

$$\Delta \gg \frac{|A|^{7/3}}{(KL)^{7/3}\rho^{4/3}}\,. \tag{43}$$

Computing the eigenvalues of the operator $M(x,y) := P(x-y)A(x)A(y)$ (see, e.g., [8, Section 8] or [9, Theorem 6.3]), we have

$$(\Delta|P|)^8 \ll |A|^8 \mathsf{E}_4(A)\mathsf{E}(P)$$

and hence using the simple bound $\rho \geqslant |A|/(2K)$ as well as the assumption $|A| \geqslant 8K^3$, we obtain in view of (13), (14)

$$\Delta^{10}|P|^8 \ll |A|^8\mathsf{E}_4(A)\sum_x P^{(2)}(x)A^{(4)}(x) \leqslant |A|^8\left(|A|^4 + \rho^3|A|^2\right)\cdot N^{-1}\sum_{\xi}|\widehat{P}(\xi)|^2|\widehat{A}(\xi)|^4$$

$$\ll \rho^3|A|^{10}\cdot\left(N^{-1}|P|^2|A|^4 + M^4|P|\right) \tag{44}$$

If the second term in (44) dominates, then thanks to our choice of the set P, we get

$$\mathsf{E}^7(A)\rho^{-4}L^{-7} \ll \mathsf{E}^7_{10/7}(A)L^{-7} \ll \Delta^{10}|P|^7 \ll |A|^{10}\rho^3 M^4$$

and (42) follows. If the first term in (44) is the largest one, then we derive

$$\Delta^{10}|P|^6 \ll \delta\mathsf{E}_4(A)|A|^{11} \ll \delta|A|^{11}\rho^{18/7}\mathsf{E}_{10/7}(A)\,,$$

and therefore in view of (43)

$$\left(\frac{|A|^{7/3}}{(KL)^{7/3}\rho^{4/3}}\right)^{10/7}\mathsf{E}^5(A)\rho^{-20/7} \ll \Delta^{10/7}\mathsf{E}^5_{10/7}(A) \ll \delta|A|^{11}\rho^{18/7}L^6\,.$$

It follows that

$$\delta^3 L^{28} K^{25} \gg 1$$

and this is a contradiction with (41). This completes the proof. $\square$

References

[1] G. Alagic. *Uncertainty principles for compact groups*. University of Connecticut, 2008.

[2] A. Biró and V. F. Lev. Uncertainty in finite planes. *Journal of Functional Analysis*, 281(3):109026, 2021.

[3] G. B. Folland and A. Sitaram. The uncertainty principle: a mathematical survey. *Journal of Fourier analysis and applications*, 3:207–238, 1997.

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

[5] 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.

[6] V. F. Lev and I. D. Shkredov. The popularity gap. *Journal of Algebraic Combinatorics*, 58(4):1155–1172, 2023.

[7] R. Meshulam. An uncertainty inequality for finite abelian groups. *European Journal of Combinatorics*, 27(1):63–67, 2006.

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

[9] I. D. Shkredov. Some new inequalities in additive combinatorics. *Mosc. J. Comb. Number Theory*, 3(3-4):189–239, 2013.

[10] T. Tao. An uncertainty principle for cyclic groups of prime order. *Mathematical Research Letters*, 12(1):121–127, 2005.

[11] A. Terras. *Fourier analysis on finite groups and applications*, volume 43. Cambridge University Press, 1999.

[12] A. Wigderson and Y. Wigderson. The uncertainty principle: variations on a theme. *Bulletin of the American Mathematical Society*, 58(2):225–261, 2021.