New York Journal of Mathematics

New York J. Math. **29** (2023) 1032–1037.

Large spectral gaps and small sumsets

Tomasz Schoen

ABSTRACT. Let N be a prime number and α satisfies $\alpha_0 \geq \alpha \geq N^{-1/4}$. We construct a set $A \subseteq \mathbb{Z}/N\mathbb{Z}$, such that $|A| = (1+o(1))\alpha N$, $\max_{r\neq 0} |\widehat{1}_A(r)| \ll \alpha^{1/2}\log^{3/2}(1/\alpha)|A|$ and $|A+A| \leq N/2$. This result is essentially optimal.

CONTENTS

1. Introduction

The Fourier analysis is a well established method in additive combinatorics. Suppose that $A \subseteq \mathbb{Z}/N\mathbb{Z}$, where N is a prime number, and denote by

$$\widehat{1}_A(r) = \sum_{a\in A} e^{-2\pi i r a/N},$$

$r \in \mathbb{Z}/N\mathbb{Z}$, the Fourier coefficients of the characteristic function of the set A. It is well known that a sufficiently large spectral gap of $\widehat{1}_A$ implies that $A+A$ is very large. More precisely, if $\max_{r\neq 0} |\widehat{1}_A(r)| \leq \varepsilon\alpha^{1/2}|A|$, where $\alpha = |A|/N$, then $A+A$ fill out $1-\varepsilon^2$ proportion of the whole group. Let $E(A)$ be the additive energy of the set A, i.e. the number of solutions to the equation $a+b=c+d$ with $a,b,c,d \in A$. Then by the Fourier inversion formula and the Parseval identity, it is implied that

$$E(A) = \frac{1}{N}\sum_r |\widehat{1}_A(r)|^4 \leq \alpha|A|^3 + \varepsilon^2\alpha|A|^2\sum_{r\neq 0}|\widehat{1}_A(r)|^2 = (1+\varepsilon^2)\alpha|A|^3\,.$$

Thus, by the Cauchy-Schwarz inequality, we have

$$|A+A| \geq \frac{|A|^4}{E(A)} \geq \frac{1}{1+\varepsilon^2}N \geq (1-\varepsilon^2)N\,.$$

A more general result was obtained in [CS09]. Namely, a similar conclusion holds for sets having large spectral gap after at most $\log_2 N$ largest Fourier coefficients of 1_A [CS09]. Therefore, there arises a natural question asked in [CS09]:

Received December 3, 2022.
2010 *Mathematics Subject Classification.* 11B30, 11L03, 11P99, 41A16.
Key words and phrases. large spectrum, sumsets.

ISSN 1076-9803/2023

what is the minimal spectral gap that guaranties that a sumset covers almost whole group? We show that the assumption on the spectral gap of order $\alpha^{1/2}|A|$ is essentially optimal. Our purpose is to establish the following result.

Theorem 1.1. *There is an absolute constant $\alpha_0 \in (0,1]$ with the following property. Let $N \geq N_0$ be a prime number and let $\alpha_0 \geq \alpha \geq N^{-1/4}$. Then there exists a set $A \subseteq \mathbb{Z}/N\mathbb{Z}$ of size $|A| = (1+o(1))\alpha N$ such that* $\max_{r\neq 0} |\widehat{1}_A(r)| \leq 100\alpha^{1/2}\log(1/\alpha)^{3/2}|A|$ *and*

$$|A+A| \leq N/2\,.$$

The proof of our result relies on the construction of a function which is roughly the convolution of a sparse random set R and a dense structural set S. It is well known that a dense set has only few large Fourier coefficients (the large spectrum must be small). Therefore, using properties of the Fourier transform, to guarantee that the convolution of those sets has a large spectral gap it is enough to control the Fourier coefficients of R only on a suitable large spectrum of S. On the other hand, the support of $1_R * 1_S$ is the sumset $R+S$, so its sumset is not too large with appropriate choice of sizes of R and S. The proof is concluded by a construction of a set with the required properties using the constructed function, which is derived by a probabilistic argument.

1.1. Notation. Given functions $f, g : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, the convolution of f and g is defined by

$$(f*g)(x) = \sum_{t\in\mathbb{Z}/N\mathbb{Z}} f(t)g(x-t).$$

The Fourier coefficients of f are defined by

$$\widehat{f}(r) = \sum_{x\in\mathbb{Z}/N\mathbb{Z}} f(x)e^{-2\pi i r x/N},$$

where $r \in \mathbb{Z}/N\mathbb{Z}$. Parseval's formula states

$$\sum_{r=0}^{N-1} |\widehat{f}(r)|^2 = N\sum_{x=0}^{N-1} |f(x)|^2\,,$$

applied in particular for the indicator function of a set A gives

$$\sum_{r=0}^{N-1} |\widehat{1}_A(r)|^2 = |A|N\,.$$

Another important property that we will use is

$$\widehat{(f*g)}(r) = \widehat{f}(r)\widehat{g}(r)\,.$$

For $\beta \in \mathbb{R}$, we denote by $\|\beta\| = \min_{y\in\mathbb{Z}} |\beta - y|$ the distance of β from the nearest integer. Observe that for any $r \in \mathbb{Z}/N\mathbb{Z}$ and any integer $x \equiv r \pmod N$, the value of x/N modulo 1 is unique, hence we can define $\|r/N\| = \|x/N\|$.

2. The proof of Theorem 1

Over the course of the proof of Theorem 1.1, we will use repeatedly the classical Bernstein's inequality [B27].

Lemma 2.1 (Bernstein)**.** *Let $X_1, \dots, X_N$ be independent random variables and suppose that $|X_k - \mathbb{E}(X_k)| \leq M$ for every $1 \leq k \leq N$. Then, for all positive t*

$$\mathbb{P}\big(|\sum_{k=1}^{N} X_k - \sum_{k=1}^{N} \mathbb{E}(X_k)| \geq t\big) \leq 2\exp\Big(-\frac{\frac{1}{2}t^2}{\sum_{k=1}^{N} \mathrm{Var}(X_k) + \frac{1}{3}tM}\Big).$$

Lemma 2.2. *Let $\Gamma \subseteq \mathbb{Z}/N\mathbb{Z}$ be any set. Then for every $n \geq \log|\Gamma| \geq n_0$ and $l \leq N/n$ there exists a set R such that $3n/4 \leq |R| \leq 5n/4$,*

$$\max_{r \in \Gamma\setminus\{0\}} |\widehat{1}_R(r)| \leq 8\sqrt{|R|\log|\Gamma|} \tag{1}$$

and

$$|R \cap \{a, a+1, \dots, a+l-1\}| \leq 10\log(N/l) \tag{2}$$

for every $a \in \mathbb{Z}/N\mathbb{Z}$.

Proof. Let R be a random subset chosen by picking each element of $\mathbb{Z}/N\mathbb{Z}$ independently with probability $p = n/N$. Since n is large enough, by Lemma 2.1 applied for indicator random variables, we have

$$\mathbb{P}\big(3n/4 \leq |R| \leq 5n/4\big) \geq 9/10\,. \tag{3}$$

Let us observe that for every $r \in \mathbb{Z}/N\mathbb{Z}, r \neq 0$

$$\mathbb{E}\big(\widehat{1}_R(r)\big) = \sum_{k=0}^{N-1} pe^{2\pi irk/N} = 0,$$

and that

$$\mathbb{P}\big(|\widehat{1}_R(r)| \geq \sqrt{2}t\big) \leq \mathbb{P}\big(|\Re\widehat{1}_R(r)| \geq t\big) + \mathbb{P}\big(|\Im\widehat{1}_R(r)| \geq t\big). \tag{4}$$

Let $r \neq 0$ be fixed. We define independent random variables $X_k, 0 \leq k \leq N-1$, by

$$X_k = \begin{cases} \cos(2\pi kr/N), & \text{if } k \in R \\ 0, & \text{if } k \notin R \end{cases} \tag{5}$$

Clearly, we have $|X_k - \mathbb{E}(X_k)| \leq 1$ and $\mathrm{Var}(X_k) \leq p$. Thus, by Lemma 2.1 applied with $t = 4\sqrt{pN\log|\Gamma|} = 4\sqrt{n\log|\Gamma|}$, we have

$$\begin{aligned} \mathbb{P}\big(|\Re\widehat{1}_R(r)| \geq t\big) &\leq 2\exp\Big(-\frac{\frac{1}{2}t^2}{pN + \frac{1}{3}t}\Big) \\ &\leq 2\exp\Big(-\frac{24}{7}\log|\Gamma|\Big) \\ &< \frac{1}{20|\Gamma|} \end{aligned}$$

and the same upper bound holds for $\mathbb{P}(|\Im\widehat{1}_R(r)| \geq t)$. Hence by (4), we have

$$\mathbb{P}\big(|\widehat{1}_R(r)| \geq 4\sqrt{2pN\log|\Gamma|}\big) \leq \frac{1}{10|\Gamma|},$$

so

$$\mathbb{P}\big(\max_{r\in\Gamma\setminus\{0\}} |\widehat{1}_R(r)| \leq 4\sqrt{2pN\log|\Gamma|}\big) \geq 9/10. \tag{6}$$

Next, we show that (2) is satisfied with high probability. We split $\mathbb{Z}/N\mathbb{Z}$ into $m = \lceil N/l\rceil$ intervals $I_1, \dots, I_m$ such that $|I_j| = l$, for every $1 \leq j \leq \lfloor N/l\rfloor$, and $|I_m| \leq l$. Again by Lemma 2.1 applied for indicator random variables, for any j we have

$$\begin{aligned}
\mathbb{P}\big(|R\cap I_j| \geq pl + 2\log(N/l)\big) &\leq \mathbb{P}\big(|R\cap I_j| \geq p|I_j| + 2\log(N/l)\big)\\
&\leq 2\exp\Big(-\frac{2\log^2(N/l)}{p|I_j| + \frac{1}{3}\log(N/l)}\Big)\\
&\leq 2\exp\Big(-\frac{2\log^2(N/l)}{1 + \frac{1}{3}\log(N/l)}\Big)\\
&\leq 2\Big(\frac{l}{N}\Big)^3
\end{aligned}$$

and therefore,

$$\mathbb{P}\big(\text{for some } j \text{ we have } |R\cap I_j| \geq pl + 2\log(N/l)\big) \leq 2m\Big(\frac{l}{N}\Big)^3 \leq \frac{1}{10}.$$

Hence, there exists a set R of size $3n/4 \leq |R| \leq 5n/4$ that satisfies (1) and

$$|R\cap I_j| \leq pl + 2\log(N/l) \leq 3\log(N/l)$$

for every j. Since each interval of length l intersects with at most three intervals among $I_1, \dots, I_m$ it follows that for each a

$$|R\cap\{a, a+1, \dots, a+l-1\}| \leq 10\log(N/l).$$

which concludes the proof. □

Proof of Theorem 1. Let N_0 and $\alpha_0 \leq n_0/(30\log n_0)$ (n_0 is a positive constant given by Lemma 2.2) be positive constants chosen in such a way that all asymptotic inequalities used below hold. Let α be such that $\alpha_0 \geq \alpha \geq N^{-1/4}$ and let $\delta \in (0,1]$ be such that $\alpha = (20\log(1/\delta))^{-1}\delta$, so $\delta_0 \geq \delta \gg N^{-1/4}\log N$. We apply Lemma 2.2 with $n = \lceil 1/(3\delta)\rceil$, $l = \lceil\delta^2 N\rceil$ and

$$\Gamma = \{-\lceil\delta^{-5/2}\rceil, \dots, -1, 1, \dots, \lceil\delta^{-5/2}\rceil\}.$$

Let us check for such choice of parameters that the assumptions of Lemma 2.2 are satisfied. Notice that the following inequalities hold provided that $\delta_0 \geq \delta \gg N^{-1/4}\log N$ and $N \geq N_0$

$$l = \lceil\delta^2 N\rceil \leq N/\lceil 1/(3\delta)\rceil = N/n$$

and

$$n \geq 1/(3\delta) \geq \log(2\lceil \delta^{-5/2} \rceil) = \log |\Gamma| \geq n_0 .$$

Thus, we can apply Lemma 2.2 to obtain a set R of size $3n/4 \leq |R| \leq 5n/4$ fulfilling (1) and (2). Put $S = \{1, \ldots, l\}$ and define $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}_{\geq 0}$ by

$$f(x) = 1_R * 1_S(x).$$

Since $1_R * 1_S(x) = |R \cap (x - S)|$, by (2), it follows that for all x

$$f(x) \leq 10 \log(N/\lceil \delta^2 N \rceil) \leq 20 \log(1/\delta).$$

We use the function $g(x) = (20 \log(1/\delta))^{-1} f(x)$ to construct the required set. Note that

$$|\widehat{1}_S(r)| = \Big| \sum_{x=0}^{l-1} e^{-2\pi x r/N} \Big| = \frac{|1 - e^{-2\pi l r/N}|}{|1 - e^{-2\pi r/N}|} \leq \frac{1}{|\sin \pi r/N|} \leq \frac{1}{2\|r/N\|} ,$$

hence if $r \notin \Gamma$

$$|\widehat{1}_S(r)| \leq \delta^{1/2}|S|,$$

so

$$|\widehat{g}(r)| = (20 \log(1/\delta))^{-1} |\widehat{1}_R(r) \widehat{1}_S(r)| \leq (20 \log(1/\delta))^{-1} \delta^{1/2} |R||S| .$$

If $r \in \Gamma \setminus \{0\}$ then by (1)

$$\begin{aligned} |\widehat{g}(r)| &= (20 \log(1/\delta))^{-1} |\widehat{f}(r)| = (20 \log(1/\delta))^{-1} |\widehat{1}_R(r)||\widehat{1}_S(r)| \\ &\leq 8(20 \log(1/\delta))^{-1} \sqrt{|R| \log |\Gamma|}|S| \leq 2\delta^{1/2}|R||S| , \end{aligned}$$

provided that $\delta \leq \delta_0$. Thus, for every $r \neq 0$ we have

$$|\widehat{g}(r)| \leq 2\delta^{1/2}|R||S|. \tag{7}$$

Next, we construct a set with required properties. We will proceed similarly as in the proof of Lemma 3. Let A be a random subset of $\mathbb{Z}/N\mathbb{Z}$ chosen by picking each element $x \in \mathbb{Z}/N\mathbb{Z}$ independently with probability $(20 \log(1/\delta))^{-1} 1_R * 1_S(x)$. Then the expected size of A equals

$$\sum_x (20 \log(1/\delta))^{-1} 1_R * 1_S(x) = (20 \log(1/\delta))^{-1} |R||S| .$$

By Lemma 2 for N large enough, we have

$$\mathbb{P}\Big(\big| |A| - \mathbb{E}(|A|) \big| \leq 2\sqrt{N \log N} \Big) \geq 1 - \frac{1}{N^{1/2}} . \tag{8}$$

For fixed $r \neq 0$, we define independent random variables $Y_x, 0 \leq x \leq N-1$ by

$$Y_x = \begin{cases} \cos(2\pi x r/N), & \text{if } x \in A \\ 0, & \text{if } x \notin A \end{cases}$$

Let us observe that for every $r \in \mathbb{Z}/N\mathbb{Z}, r \neq 0$

$$\mathbb{E}\big(\Re \widehat{1}_A(r)\big) = \sum_{x=0}^{N-1} \mathbb{E}(Y_x) = \Re \widehat{g}(r),$$

and that $|Y_x - \mathbb{E}(Y_x)| \le 1$ and $\mathrm{Var}(Y_x) \le 1$, so applying Bernstein's inequality once again we obtain that

$$\mathbb{P}\big(|\Re\widehat{1}_A(r) - \Re\widehat{g}(r)| \ge 2\sqrt{N\log N}\big) \le 2\exp\Big(-\frac{2N\log N}{N + \frac{2}{3}\sqrt{N\log N}}\Big) \le \frac{1}{N^{3/2}},$$

as $N \ge N_0$. Similarly, one can show that

$$\mathbb{P}\big(|\Im\widehat{1}_A(r) - \Im\widehat{g}(r)| \ge 2\sqrt{N\log N}\big) \le \frac{1}{N^{3/2}}$$

so

$$\mathbb{P}\big(\text{for all } r \ne 0 : |\widehat{1}_A(r) - \widehat{g}(r)| \le 2\sqrt{2}\sqrt{N\log N}\big) \ge 1 - \frac{2}{N^{1/2}}. \tag{9}$$

Thus, there exists a set A that satisfies the inequalities (8) and (9). Hence,

$$\begin{aligned} |A| &= (20\log(1/\delta))^{-1}\sum_x 1_R * 1_S(x) + O(\sqrt{N\log N}) \\ &= (20\log(1/\delta))^{-1}|R||S| + O(\sqrt{N\log N}) = (1+o(1))\alpha N \end{aligned}$$

and by (7) for $r \ne 0$,

$$\begin{aligned} |\widehat{1}_A(r)| &\le |\widehat{g}(r)| + 2\sqrt{N\log N} \\ &\le 2\delta^{1/2}|R||S| + 2\sqrt{N\log N} \\ &\le 40\log(1/\delta)\delta^{1/2}|A| + O(\sqrt{N\log N}) \\ &\le 100\alpha^{1/2}\log(1/\alpha)^{3/2}|A|. \end{aligned}$$

It remains to check that $A+A$ is not too large, but it follows easily from the fact that $A \subseteq R+S$. Let us recall that $|R| \le \frac{3}{2}\lceil 1/(3\delta)\rceil$ and $|S| = l = \lceil \delta^2 N\rceil$, hence

$$\begin{aligned} |A+A| &\le |(R+S)+(R+S)| \le |R+R||S+S| \\ &\le 2|R|^2|S| \le \frac{25}{8}\lceil 1/(3\delta)\rceil^2\lceil \delta^2 N\rceil \le N/2. \end{aligned}$$

□

References

[B27] Bernšteĭn, Sergeĭ N. Die Wahrscheinlichkeitsrechnung. (Russian). *Moskau-Leningrad: Staatsverlag (Lehrbücher für Hochschulen)*, 1927. viii, 363 S. JFM 53.0492.01. 1034

[CS09] Croot, Ernie; Schoen, Tomasz. On sumsets and spectral gaps. *Acta Arith.* **136** (2009), no. 1, 47–55. MR2469943, Zbl 1246.11023, arXiv:0708.0381, doi: 10.4064/aa136-1-4. 1032

(Tomasz Schoen) Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Uniwersytetu Poznańskiego 4, 61-614 Poznań, Poland
schoen@amu.edu.pl

This paper is available via http://nyjm.albany.edu/j/2023/29-40.html.