Some examples of sets of large exponential sums *

Shkredov I.D.

Annotation.

Let A be a subset of $\mathbb{Z}/N\mathbb{Z}$ and let $\mathcal{R}$ be the set of large Fourier coefficients of A. Properties of $\mathcal{R}$ have been studied in works of M.–C. Chang, B. Green and the author. In the paper we obtain some new results on sets of large exponential sums.

1. Introduction.

Let N be a positive integer. By $\mathbb{Z}_N$ denote the set $\mathbb{Z}/N\mathbb{Z}$. Let $f : \mathbb{Z}_N \to \mathbb{C}$ be an arbitrary function. Denote by $\widehat{f}$ the Fourier transform of f

$$\widehat{f}(r) = \sum_{n\in\mathbb{Z}_N} f(n)e(-nr)\,, \qquad (1)$$

where $e(x) = e^{-2\pi ix/N}$.

Let δ, α be real numbers, $0 < \alpha \leq \delta \leq 1$ and let A be a subset of $\mathbb{Z}_N$ of cardinality δN. It is very convenient to write $A(x)$ for such a function. Thus $A(x) = 1$ if $x \in A$ and $A(x) = 0$ otherwise. Consider the set $\mathcal{R}_\alpha$ of large exponential sums of the set A

$$\mathcal{R}_\alpha = \mathcal{R}_\alpha(A) = \{\ r \in \mathbb{Z}_N\ :\ |\widehat{A}(r)| \geq \alpha N\ \}\,. \qquad (2)$$

In many problems of combinatorial number theory is important to know the structure of the set $\mathcal{R}_\alpha$ (see [1]). In other words what kind of properties $\mathcal{R}_\alpha$ has?

In 2002 M.–C. Chang proved the following result [3].

Theorem 1.1 (Chang) *Let δ, α be real numbers, $0 < \alpha \leq \delta \leq 1$, A be a subset of $\mathbb{Z}_N$, $|A| = \delta N$. Then there exists a set $\Lambda = \{\lambda_1, \ldots, \lambda_{|\Lambda|}\} \subseteq \mathbb{Z}_N$, $|\Lambda| \leq 2(\delta/\alpha)^2 \log(1/\delta)$ such that for any $r \in \mathcal{R}_\alpha$ we have*

$$r = \sum_{i=1}^{|\Lambda|} \varepsilon_i\lambda_i \pmod N\,, \qquad (3)$$

where $\varepsilon_i \in \{-1, 0, 1\}$.

Using approach of paper [4] (see also [5]) Chang applied her result to prove the famous Freiman's theorem [6] on sets with small doubling. Another applications of Theorem 1.1 were obtained by B. Green in [7], and by T. Schoen in [13]. If the parameter α is close to δ then the structural properties of the set $\mathcal{R}_\alpha$ was studied in papers [15, 16, 17], see also survey [18].

*This work was supported by RFFI grant no. 06-01-00383, President's of Russian Federation grant N 1726.2006.1 and INTAS (grant no. 03–51–5-70).

In paper [8] Green showed that Chang's theorem is sharp in a certain sense. Let $E = \{e_1, \dots, e_{|E|}\} \subseteq \mathbb{Z}_N$ be an arbitrary set. By $\mathrm{Span}(E)$ denote the set of all sums $\sum_{i=1}^{|E|} \varepsilon_i e_i$, where $\varepsilon_i \in \{-1, 0, 1\}$.

Theorem 1.2 (Green) *Let δ, α be real numbers, $\delta \le 1/8$, $0 < \alpha \le \delta/32$. Suppose that*

$$\left(\frac{\delta}{\alpha}\right)^2 \log(1/\delta) \le \frac{\log N}{\log\log N}\,. \tag{4}$$

Then there exists a set $A \subseteq \mathbb{Z}_N$, $|A| = [\delta N]$ such that the set $\mathcal{R}_\alpha$ does not contain in $\mathrm{Span}(\Lambda)$ for any set Λ of cardinality $2^{-12}(\delta/\alpha)^2 \log(1/\delta)$.

In papers [31, 32] further results on sets of large exponential sums were obtained. In particular the author proved the following theorem

Theorem 1.3 *Let δ, α be real numbers, $0 < \alpha \le \delta$, A be a subset of $\mathbb{Z}_N$, $|A| = \delta N$, and $k \ge 2$ be a positive integer. Let also $B \subseteq \mathcal{R}_\alpha \setminus \{0\}$ be an arbitrary set. Then the number*

$$T_k(B) := |\{\ (r_1, \dots, r_k, r'_1, \dots, r'_k) \in B^{2k}\ :\ r_1 + \dots + r_k = r'_1 + \dots + r'_k\ \}| \tag{5}$$

is at least

$$\frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}}|B|^{2k}\,. \tag{6}$$

In article [32] was showed that Theorem 1.3 and an inequality of W. Rudin [22] imply M.–C. Chang's theorem. Moreover in [32] the following improvement of Theorem 1.1 was obtained.

Theorem 1.4 *Let N be a positive integer, $(N, 6) = 1$, δ, α be real numbers, $0 < \alpha \le \delta \le 1/16$, and A be a subset of $\mathbb{Z}_N$, $|A| = \delta N$. Then there exists a set $\Lambda^* \subseteq \mathbb{Z}_N$,*

$$|\Lambda^*| \le \min\left(\max(\,2^{30}(\delta/\alpha)^2\log(1/\delta), 2^{4(\log\log(1/\delta))^2+2}\,),\ 2^{20}(\delta/\alpha)^2\log^{13/7}(1/\delta)\,\right) \tag{7}$$

such that for any $r \in \mathcal{R}_\alpha$ there exists a tuple $\lambda^*_1, \dots, \lambda^*_M \in \Lambda^*$, $M \le s8\log(1/\delta)$ such that

$$r = \sum_{i=1}^{M} \varepsilon_i \lambda^*_i \pmod N\,, \tag{8}$$

where $\varepsilon_i \in \{-1, 0, 1\}$.

Besides there exists a set $\tilde\Lambda \subseteq \mathbb{Z}_N$,

$$|\tilde\Lambda| \le 2^{20}(\delta/\alpha)^2\log^{5/3}(1/\delta)\log\log(1/\delta) \tag{9}$$

such that for any residual $r \in \mathcal{R}_\alpha$ there exists a tuple $\tilde\lambda_1, \dots, \tilde\lambda_M \in \tilde\Lambda$, $M \le 8\log(1/\delta)$ such that (8) holds.

The paper is organized as follows.

In section 2 we show that Theorem 1.3 is sharp in a certain sense. In our proof we construct concrete sets $A \subseteq \mathbb{Z}_N$ with required properties. Besides in the section we obtain a result which is an inverse to Chang's theorem in some sense (see Theorem 2.8).

In §3 we obtain the following improvement of Theorem 1.4 (we consider the case when N is a prime number).

Theorem 1.5 *Let N, d be positive integers, δ, α be real numbers, $0 < \alpha \le \delta \le 2^{-8}$, $\varphi = (\sqrt{73}-5)/2$, and A be a subset of $\mathbb{Z}_N$, $|A| = \delta N$. Then there exists a set $\Lambda^* \subseteq \mathbb{Z}_N$,*

$$\min\left(\max(\, 2^{30+8d(\log(1/\delta))^{-1}} \cdot (\delta/\alpha)^2 \log(1/\delta), 2^{(\log\log(1/\delta))^2+3}\,),\ 2^{20+8d(\log(1/\delta))^{-1}}(\delta/\alpha)^2 \log^{\varphi}(1/\delta)\,\right) \tag{10}$$

such that for any residual $r \in \mathcal{R}_\alpha \setminus \{0\}$ there exists a matrix $M = (m_{ij})_{i\in[d], j\in[|\Lambda^*|]}$ of rank d such that for any $i \in [d]$ we have $\sum_{j=1}^{|\Lambda^*|} |m_{ij}| \le 4\log(1/\delta)$ and for all $i \in [d]$

$$r = \sum_{j=1}^{|\Lambda^*|} m_{ij}\lambda_j^* \pmod N\,. \tag{11}$$

Certainly, our question on the structure of $\mathcal{R}_\alpha$ (as any question of combinatorial number theory) can be asked for any finite Abelian group G not only for $\mathbb{Z}_N$. It turns out that (see [11, 30] and, especially, a wonderful survey [12]) many problems of combinatorial number theory are considerably easier in groups $\mathbb{Z}_p^n$, where p is a small prime number (for example $p = 2, 3$ or 5).

In section 4 we obtain some analogs of results of section 2 for groups $\mathbb{Z}_p^n$. Main ideas of the proofs are easier in the groups then in $\mathbb{Z}_N$, and all technical details are simplified.

Finally note that the statements of Theorems 1.1, 1.4, and 1.5 are trivial if the parameter δ does not tends to zero as $N \to \infty$. In the case there are not non–trivial restrictions on structure of the set $\mathcal{R}_\alpha$ (see papers [19, 20, 21]).

In our forthcoming papers we are going to obtain further results on sets of large exponential sums.

The author is grateful to Professor N.G. Moshchevitin for constant attention to this work.

2. Some examples of sets of large exponential sums.

Let N be a positive integer. It is very convenient to write $[N]$ for $\{1, 2, \dots, N\}$. Let also $f : \mathbb{Z}_N \to \mathbb{C}$ be an arbitrary function. By Parseval's identity

$$\sum_{r\in\mathbb{Z}_N} |\widehat{f}(r)|^2 = N \sum_{n\in\mathbb{Z}_N} |f(n)|^2\,. \tag{12}$$

Let δ, α be real numbers, $0 < \alpha \le \delta \le 1$ and let A be a subset of $\mathbb{Z}_N$, $|A| = \delta N$. It is easy to see that $0 \in \mathcal{R}_\alpha$ and $\mathcal{R}_\alpha = -\mathcal{R}_\alpha$. Further, using (12), we obtain $|\mathcal{R}_\alpha| \le \delta/\alpha^2$.

In the section we give some examples of sets of large exponential sums. First of all note that any "small" subset of $\mathbb{Z}_N$ is a set of large exponential sums. To be precise, we have the following proposition.

Proposition 2.1 *Let $\delta, \alpha \in (0, 1]$ be real numbers, $\delta \le 1/2$, $20N^{-1/2} < \alpha \le \delta/2$, and $S \subseteq \mathbb{Z}_N$ be an arbitrary set such that $0 \in S$, $S = -S$ and $|S| \le \delta/(2\alpha)$. Then there exists a set $A \subseteq \mathbb{Z}_N$, $|A| = [\delta N]$ such that $\mathcal{R}_\alpha(A) = S$.*

To prove Proposition 2.1 we need in the following well–known lemma (see [24] and [8]).

Lemma 2.2 *Let $f : \mathbb{Z}_N \to [0, 1]$ be a function. Then there exists a set $C \subseteq \mathbb{Z}_N$, $|C| = [\sum_{x\in\mathbb{Z}_N} f(x)]$ such that for all $r \in \mathbb{Z}_N \setminus \{0\}$, we have $|\widehat{C}(r) - \widehat{f}(r)| \le 20\sqrt{N}$.*

Proof of Proposition 2.1. Let $S^* = S \setminus \{0\}$. Consider the function $f(x) = \delta + 2\alpha \sum_{r\in S^*} e(rx)$. Since $S = -S$, it follows that $f(x)$ is a real function. We have $|S| \le \delta/(2\alpha)$ and $\delta \le 1/2$. Hence for all $x \in \mathbb{Z}_N$, we get $0 \le f(x) \le 1$. Besides $\sum_{x\in\mathbb{Z}_N} f(x) = \delta N$ and for any $r \in \mathbb{Z}_N \setminus \{0\}$, we have $\widehat{f}(r) = 2\alpha S^*(r)N$. Using Lemma 2.2, we obtain the set A such

that $|A| = [\sum_{x\in\mathbb{Z}_N} f(x)] = [\delta N]$ and for all $r \in \mathbb{Z}_N \setminus \{0\}$

$$|\widehat{A}(r) - \widehat{f}(r)| = |\widehat{A}(r) - 2\alpha S^*(r)N| \le 20\sqrt{N}\,.$$

Since $\alpha > 20N^{-1/2}$ it follows that for any $r \in S^*$ the following inequality holds $|\widehat{A}(r)| \ge 2\alpha N - 20\sqrt{N} \ge \alpha N$. Hence $S \subseteq \mathcal{R}_\alpha(A)$. Using the inequality $\alpha > 20N^{-1/2}$ again, we obtain $|\widehat{A}(r)| < \alpha N$ for all $r \notin S^*$, $r \ne 0$. Whence $\mathcal{R}_\alpha(A) = S$. This completes the proof.

So any small symmetrical subset of $\mathbb{Z}_N$ is a set of large exponential sums. What is the structure of the large sets $\mathcal{R}_\alpha$? This question is not easy but clearly, these sets have special properties. For example any set $\mathcal{R}_\alpha$ has large quantity $T_k(\mathcal{R}_\alpha)$ (see Theorem 1.3).

Chang's theorem is another example which is demonstrating that our sets have really specific properties. This theorem can be reformulate as follows : any set of large exponential sums has small dissociated subset. We say that a set $\mathcal{D} = \{d_1, \dots, d_{|\mathcal{D}|}\} \subseteq \mathbb{Z}_N$ is *dissociated* if the equality

$$\sum_{i=1}^{|\mathcal{D}|} \varepsilon_i d_i = 0 \pmod N\,, \qquad (13)$$

where $\varepsilon_i \in \{-1, 0, 1\}$ implies that all ε_i are equal to zero. Actually Chang proved that *any* dissociated subset of $\mathcal{R}_\alpha(A)$ has cardinality less than $2(\delta/\alpha)^2\log(1/\delta)$. Now if we let Λ be a maximal dissociated subset of $\mathcal{R}_\alpha(A)$ then it is easy to see that for any $r \in \mathcal{R}_\alpha$ we have (3) (see details in [3] or in [10]).

In the section we obtain a result which is an inverse to Chang's theorem in some sense. We show that any not very big dissociated subset of $\mathbb{Z}_N$ is a set of large exponential sums. We extensively use approach of B. Green (see [8]) in our prove. His method is connected with "niveau sets" of I. Ruzsa (see [14]).

Let us introduce a few further pieces of notation. We say that a set $\mathcal{D} \subseteq \mathbb{Z}_N$ is k—*dissociated* if the equality (13), where $|\varepsilon_i| \le k$ implies that all ε_i are equal to zero. Using this definition we can reformulate Theorem 1.2 as follows.

Theorem 2.3 (Green) *Let δ, α be real numbers, $\delta \le 1/8$, $20N^{-1/2} < \alpha \le \delta/32$, and Λ be a $6|\Lambda|$—dissociated set, $|\Lambda| \le 2^{-11}(\delta/\alpha)^2\log(1/\delta)$. Then there exists a set $A \subseteq \mathbb{Z}_N$, $|A| = [\delta N]$ such that $\mathcal{R}_\alpha(A) = \{0\} \bigsqcup \Lambda \bigsqcup -\Lambda$.*

Note 2.4 If Λ is a $6|\Lambda|$ — dissociated set then we have $|\Lambda| \ll \log N/\log\log N$. Thus Theorem 2.3 is not useful for sets of cardinality $\gg \log N/\log\log N$.

We do not prove Theorem 2.3 here and obtain a slightly stronger result. To formulate this result we need in the following definition (see [29] and [31, 32]).

Definition 2.5 Let k, s be positive integers. Consider the family $\Lambda(k,s)$ of subsets of $\mathbb{Z}_N$. A set $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ belongs to the family $\Lambda(k,s)$ if the equality

$$\sum_{i=1}^{|\Lambda|} \lambda_i s_i = 0 \pmod N\,, \quad \lambda_i \in \Lambda\,, \quad s_i \in \mathbb{Z}\,, \quad |s_i| \le s\,, \quad \sum_{i=1}^{|\Lambda|} |s_i| \le k\,, \qquad (14)$$

implies that s_i are equal to zero.

A set $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ belongs to the family $\Lambda(k,\infty)$ if the equality

$$\sum_{i=1}^{|\Lambda|} \lambda_i s_i = 0 \pmod N\,, \quad \lambda_i \in \Lambda\,, \quad s_i \in \mathbb{Z}\,, \qquad \sum_{i=1}^{|\Lambda|} |s_i| \le k\,, \qquad (15)$$

implies that all s_i are equal to zero.

Note that for any $\Lambda \in \Lambda(k,s)$, where s is a positive integer or ∞, we have $0 \notin \Lambda$ and $\Lambda \cap -\Lambda = \emptyset$.

We need in a more delicate definition.

Definition 2.6 Let k, p be positive integers and s be a positive integer or ∞. Consider the family $\Lambda(k,s,p)$ of subsets of $\mathbb{Z}_N$. A set $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ belongs to the family $\Lambda(k,s,p)$ if there exists a partition of Λ into p subsets $\Lambda_1 = \{\lambda_1^{(1)}, \dots, \lambda_{|\Lambda_1|}^{(1)}\}, \dots, \Lambda_p = \{\lambda_1^{(p)}, \dots, \lambda_{|\Lambda_p|}^{(p)}\}$, such that the cardinalities of any two subsets Λ_i, Λ_j differ by at most two times, and the equality

$$\sum_{i=1}^{|\Lambda_1|} \lambda_i^{(1)} s_i^{(1)} + \dots + \sum_{i=1}^{|\Lambda_p|} \lambda_i^{(p)} s_i^{(p)} = 0 \pmod N, \quad \text{where} \tag{16}$$

$$\lambda_j^{(i)} \in \Lambda_i, \quad s_j^{(i)} \in \mathbb{Z}, \quad |s_j^{(i)}| \le s, \qquad \sum_{j=1}^{|\Lambda_i|} |s_j^{(i)}| \le k, \quad i = 1, \dots, p \tag{17}$$

imply that all $s_j^{(i)}$, $i = 1, \dots, p$, $j = 1, \dots, |\Lambda_i|$ are equal to zero.

Example 2.7 Let k, s, p be positive integers. Then any set $\Lambda \in \Lambda(kp, s)$, $|\Lambda| \ge p$ belongs to the family $\Lambda(k,s,p)$.

Theorem 2.8 *Let δ, α be real numbers, $\delta \le 1/8$, $640N^{-1/2} < \alpha \le 2^{-27}\delta$, and Λ be a subset of the family $\Lambda((\delta/\alpha)^2, (\delta/\alpha)^2, [\log(1/\delta)])$, $|\Lambda| \le 2^{-12}(\delta/\alpha)^2 \log(1/\delta)$. Then there exists a set $A \subseteq \mathbb{Z}_N$, $|A| = [\delta N]$ such that $\mathcal{R}_\alpha(A) = \{0\} \bigsqcup \Lambda \bigsqcup -\Lambda$.*

To prove Theorem 2.8 we need in the following auxiliary result.

Statement 2.9 *Let $\delta, \alpha \in (0,1]$ be real numbers, $640N^{-1/2} < \alpha \le 2^{-10}\delta$, and Λ be any 2—dissociated set of the cardinality at most $\frac{\delta}{3\alpha}\log(1/\delta)$. Then there exists a set $A \subseteq \mathbb{Z}_N$, $|A| = [\delta N]$ such that $\mathcal{R}_\alpha(A) = \{0\} \bigsqcup \Lambda \bigsqcup -\Lambda$.*

Thus Statement 2.9 tells us that any 2—dissociated set of the cardinality rather more then δ/α is a set of large exponential sums.

Proof of Statement 2.9. Let $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ be a dissociated set, $|\Lambda| \le \frac{\delta}{3\alpha}\log(1/\delta)$. Let also $m = |\Lambda|$ and $c = (3\ln 2)/2$. Consider the function

$$f(x) = \delta \prod_{j=1}^{m} (1 + \frac{2c\alpha}{\delta}\cos(\lambda_j x)) = \delta \prod_{j=1}^{m} (1 + \frac{c\alpha}{\delta}(e(\lambda_j x) + e(-\lambda_j x))). \tag{18}$$

Clearly, $f(x) \ge 0$ and $\sum_{x \in \mathbb{Z}_N} f(x) = \delta N$. By assumption $m \le \frac{\delta}{3\alpha}\log(1/\delta)$. Hence $f(x) \le \delta(1 + \frac{2c\alpha}{\delta})^m \le 1$. Let

$$\nu_m(n) = |\{r_1, \dots, r_m \in \Lambda \ : \ n = \pm r_1 \pm \dots \pm r_m\}|, \dots,$$

$$\nu_2(n) = |\{r_1, r_2 \in \Lambda \ : \ n = \pm r_1 \pm r_2\}|, \quad \nu_1(n) = |\{r_1 \in \Lambda \ : \ n = \pm r_1\}|.$$

So the quantity $\nu_s(n)$ is the number of the solutions of the equation $n = \sum_{i=1}^{s} \varepsilon_i r_i$, where $\varepsilon_i = \pm 1$, and $r_i \in \Lambda$. Using (18), we get

$$f(x) = \delta + \delta\frac{c\alpha}{\delta}\sum_n \nu_1(n)e(nx) + \delta\left(\frac{c\alpha}{\delta}\right)^2 \sum_n \nu_2(n)e(nx) + \dots + \delta\left(\frac{c\alpha}{\delta}\right)^m \sum_n \nu_m(n)e(nx). \tag{19}$$

In other words

$$f(x) = \delta + c\alpha\widehat{\nu}_1(-x) + \delta\left(\frac{c\alpha}{\delta}\right)^2 \widehat{\nu}_2(-x) + \dots + \delta\left(\frac{c\alpha}{\delta}\right)^m \widehat{\nu}_m(-x). \tag{20}$$

Hence

$$\widehat{f}(r) = \begin{cases} \delta N\,, & \text{if } r = 0, \\ N(c\alpha \cdot \nu_1(r) + \delta \left(\frac{c\alpha}{\delta}\right)^2 \nu_2(r) + \cdots + \delta \left(\frac{c\alpha}{\delta}\right)^m \nu_m(r))\,, & \text{otherwise.} \end{cases}$$

By assumption Λ is a 2—dissociated set. It follows that for all $i \geq 1$, we have $\nu_i(n) \leq 1$. If $r \in \Lambda$ or $r \in -\Lambda$ then

$$|\widehat{f}(r)| \geq c\alpha N - N\left(\delta\left(\frac{c\alpha}{\delta}\right)^2 + \delta\left(\frac{c\alpha}{\delta}\right)^3 + \cdots + \delta\left(\frac{c\alpha}{\delta}\right)^m\right) \geq (1 + 2^{-5})\alpha N\,. \tag{21}$$

Similarly if $r \notin \Lambda \bigsqcup -\Lambda$ then

$$|\widehat{f}(r)| \leq N\left(\delta\left(\frac{c\alpha}{\delta}\right)^2 + \delta\left(\frac{c\alpha}{\delta}\right)^3 + \cdots + \delta\left(\frac{c\alpha}{\delta}\right)^m\right) \leq \frac{1}{2}\alpha N\,. \tag{22}$$

Using Lemma 2.2, we find a set A such that $|A| = [\sum_{x\in\mathbb{Z}_N} f(x)] = [\delta N]$ and for all $r \in \mathbb{Z}_N \setminus \{0\}$, we have $|\widehat{A}(r) - \widehat{f}(r)| \leq 20\sqrt{N}$. Combining (21), (22) and $\alpha > 640N^{-1/2}$, we get $\mathcal{R}_\alpha(A) = \{0\} \bigsqcup \Lambda \bigsqcup -\Lambda$. This completes the proof of Statement 2.9.

Let us return to the proof of Theorem 2.8.

We need in a lemma from [8].

Lemma 2.10 *Let k be a positive integer, and*

$$p_k(x) = 2 + x\sum_{j=0}^{k} \frac{(-1)^j x^{2j}}{2^{4j} j!}\,. \tag{23}$$

Then for all x such that $|x| \leq \sqrt{k}$, we have $0 \leq p_k(x) \leq 4$.

Proof of Theorem 2.8. Let $k = s = (\delta/\alpha)^2$, $p = [\log(1/\delta)]$. Let also $k_i = |\Lambda_i|$ and $\Lambda_i = \{\lambda_1^{(i)}, \ldots, \lambda_{k_i}^{(i)}\}$, $i = 1, 2, \ldots, p$. By definition of the family $\Lambda(k, k, p)$, we get

$$\frac{|\Lambda|}{2p} \leq k_i \leq \frac{2|\Lambda|}{p}\,. \tag{24}$$

We can assume that

$$|\Lambda| > \frac{\delta}{3\alpha}\log(1/\delta) > 2\log(1/\delta)\,. \tag{25}$$

Indeed if $|\Lambda| \leq \delta/(3\alpha) \cdot \log(1/\delta)$ then for all $i \in [p]$, we have $2k_i + 1 \leq 8\delta/\alpha \leq k$. Besides $s \geq 2$. Hence Λ is a 2—dissociated set, and using Statement 2.9, we obtain the required set A.

Let

$$g(x) = 4^{-p}\prod_{i=1}^{p} p_{k_i}\left(\frac{\cos(2\pi\lambda_1^{(i)}x/N) + \cdots + \cos(2\pi\lambda_{k_i}^{(i)}x/N)}{\sqrt{k_i}}\right)\,. \tag{26}$$

Using Lemma 2.10, we get for all $x \in \mathbb{Z}_N$ the following inequality holds $0 \leq g(x) \leq 1$. Consider the i–th term of product (26). By formula $\cos(2\pi x/N) = (e(x) + e(-x))/2$, we obtain

$$p_{k_i}\left(\frac{\cos(2\pi\lambda_1^{(i)}x/N) + \cdots + \cos(2\pi\lambda_{k_i}^{(i)}x/N)}{\sqrt{k_i}}\right) =$$

$$2+\frac{1}{2\sqrt{k_i}}\sum_{j=0}^{k_i}\frac{(-1)^j}{(64k_i)^j j!}\left(e(\lambda_1^{(i)}x)+e(-\lambda_1^{(i)}x)+\cdots+e(\lambda_{k_i}^{(i)}x)+e(-\lambda_{k_i}^{(i)}x)\right)^{2j+1}. \qquad (27)$$

Thus

$$g(x)=\sum_{\sum_{l=1}^{k_1}|s_l^{(1)}|\le 2k_1+1}\cdots\sum_{\sum_{l=1}^{k_p}|s_l^{(p)}|\le 2k_p+1}$$

$$Q(s_1^{(1)},\dots,s_{k_1}^{(1)},\dots,s_1^{(p)},\dots,s_{k_p}^{(p)})e((s_1^{(1)}\lambda_1^{(1)}+\cdots+s_{k_1}^{(1)}\lambda_{k_1}^{(1)}+\cdots+s_1^{(p)}\lambda_1^{(p)}+\cdots+s_{k_p}^{(p)}\lambda_{k_p}^{(p)})x)\,, \qquad (28)$$

where $Q(s_1^{(1)},\dots,s_{k_1}^{(1)},\dots,s_1^{(p)},\dots,s_{k_p}^{(p)})$ is a coefficient which attached to $e((s_1^{(1)}\lambda_1^{(1)}+\cdots+s_{k_1}^{(1)}\lambda_{k_1}^{(1)}+\cdots+s_1^{(p)}\lambda_1^{(p)}+\cdots+s_{k_p}^{(p)}\lambda_{k_p}^{(p)})x)$. Similar

$$p_{k_i}\left(\frac{\cos(2\pi\lambda_1^{(i)}x/N)+\cdots+\cos(2\pi\lambda_{k_i}^{(i)}x/N)}{\sqrt{k_i}}\right)=$$

$$=\sum_{\sum_{l=1}^{k_i}|s_l^{(i)}|\le 2k_i+1}Q(s_1^{(i)},\dots,s_{k_i}^{(i)})e((s_1^{(i)}\lambda_1^{(i)}+\cdots+s_{k_i}^{(i)}\lambda_{k_i}^{(i)})x) \qquad (29)$$

Clearly, $Q(s_1^{(1)},\dots,s_{k_1}^{(1)},\dots,s_1^{(p)},\dots,s_{k_p}^{(p)})=4^{-p}\prod_{i=1}^{p}Q(s_1^{(i)},\dots,s_{k_i}^{(i)})$. By assumption Λ belongs to $\Lambda(k,k,p)$. This implies that all the sums $s_1^{(1)}\lambda_1^{(1)}+\cdots+s_{k_1}^{(1)}\lambda_{k_1}^{(1)}+\cdots+s_1^{(p)}\lambda_1^{(p)}+\cdots+s_{k_p}^{(p)}\lambda_{k_p}^{(p)}$ are distinct. In particular

$$\sum_{x\in\mathbb{Z}_N}g(x)=2^{-p}N\,. \qquad (30)$$

Using formula (28), we obtain that any non–zero Fourier coefficient of the function $g(x)$ must have the following form $s_1^{(1)}\lambda_1^{(1)}+\cdots+s_{k_1}^{(1)}\lambda_{k_1}^{(1)}+\cdots+s_1^{(p)}\lambda_1^{(p)}+\cdots+s_{k_p}^{(p)}\lambda_{k_p}^{(p)}$, where $\sum_{l=1}^{k_i}|s_l^{(i)}|\le 2k_i+1$, $i\in[p]$. Moreover, any Fourier coefficient of $g(x)$ of the form $s_1^{(1)}\lambda_1^{(1)}+\cdots+s_{k_1}^{(1)}\lambda_{k_1}^{(1)}+\cdots+s_1^{(p)}\lambda_1^{(p)}+\cdots+s_{k_p}^{(p)}\lambda_{k_p}^{(p)}$ is equal to $N\cdot Q(s_1^{(1)},\dots,s_{k_1}^{(1)},\dots,s_1^{(p)},\dots,s_{k_p}^{(p)})$. Let us prove that for all $i\in[p]$, $j\in[k_i]$, we have

$$|\widehat{g}(\lambda_j^{(i)})|=|\widehat{g}(-\lambda_j^{(i)})|\ge 2^{-p}\frac{N}{8\sqrt{k_i}}\,. \qquad (31)$$

Clearly, it suffices to deal with the case $i=j=1$. In other words we need to find the coefficient $Q(1,0,\dots,0)$. We have

$$p_{k_1}\left(\frac{\cos(2\pi\lambda_1^{(1)}x/N)+\cdots+\cos(2\pi\lambda_{k_1}^{(1)}x/N)}{\sqrt{k_1}}\right)=$$

$$=2+\frac{1}{2\sqrt{k_1}}\sum_{j=0}^{k_1}\frac{(-1)^j}{(64k_1)^j j!}\left(e(\lambda_1^{(1)}x)+e(-\lambda_1^{(1)}x)+\cdots+e(\lambda_{k_1}^{(1)}x)+e(-\lambda_{k_1}^{(1)}x)\right)^{2j+1}=$$

$$=\sum_{\sum_{l=1}^{k_1}|s_l^{(1)}|\le 2k_1+1}Q(s_1^{(1)},\dots,s_{k_1}^{(1)})e((s_1^{(1)}\lambda_1^{(1)}+\cdots+s_{k_1}^{(1)}\lambda_{k_1}^{(1)})x)\,. \qquad (32)$$

The coefficient attached to $e(\lambda_1^{(1)})$ in (32) from $j=0$ equals $1/(2\sqrt{k_1})$. Let us prove that the sum of the coefficients attached to $e(\lambda_1^{(1)})$ from $j\ge 1$ at most $1/(4\sqrt{k_1})$.

Let $l = 1,2,\dots,k_1$, and consider the product of $(2l+1)$ brackets $\Bigl(e(\lambda_1^{(1)}x)+e(-\lambda_1^{(1)}x)+\dots+e(\lambda_{k_1}^{(1)}x)+e(-\lambda_{k_1}^{(1)}x)\Bigr)^{2l+1}$. Every term contributing to the coefficient of $e(\lambda_1^{(1)}x)$ arises in the following way. First of all choose $e(\lambda_1^{(1)}x)$ from some bracket. It can be done in $(2l+1)$ ways. Secondly we choose $e(\lambda_u^{(1)}x)$ u from some other bracket. This can be done in $2k_1$ ways. Clearly, it must be balanced by choosing $e(-\lambda_u^{(1)}x)$ from some other bracket. There are at most $(2l-1)$ ways of doing this. And so on. Thus the coefficient of $e(\lambda_1^{(1)}x)$ from $j=l$ does not exceed

$$\frac{1}{2\sqrt{k_1}}\cdot\frac{1}{(64k_1)^l l!}\times(2l+1)\times 2k_1\times(2l-1)\times 2k_1\times(2l-3)\times\dots\times 2k_1\times 1\le\frac{1}{2\sqrt{k_1}}\frac{2l+1}{2^{4l}}\,.$$

Hence

$$\frac{1}{4\sqrt{k_1}}\le\frac{1}{2\sqrt{k_1}}\left(1-\sum_{j=1}^{\infty}\frac{2j+1}{2^{4j}}\right)\le Q(1,0,\dots,0)\le\frac{1}{2\sqrt{k_1}}\left(1+\sum_{j=1}^{\infty}\frac{2j+1}{2^{4j}}\right)\le\frac{1}{\sqrt{k_1}}\qquad(33)$$

and inequality (31) is proved. Rather more accurate calculation shows that

$$Q(1,0,\dots,0)\le\frac{1}{2\sqrt{k_1}}\,.\qquad(34)$$

Indeed the term from $j=1$ in (32) is negative, and its absolute value is equal to

$$\frac{1}{2\sqrt{k_1}}\cdot\frac{1}{64k_1}(3(2k_1-2)+3)\ge\frac{1}{2\sqrt{k_1}}\cdot\frac{1}{16}\,.$$

Whence

$$Q(1,0,\dots,0)\le\frac{1}{2\sqrt{k_1}}\left(1-\frac{1}{16}+\sum_{j=2}^{\infty}\frac{2j+1}{2^{4j}}\right)\le\frac{1}{2\sqrt{k_1}}$$

and inequality (34) is proved.

It easy to see that there exists $\gamma\in[1/2,1]$ such that $\sum_x f(x)=\delta N$, where $f(x)=\gamma g(x)$. By assumption $|\Lambda|\le 2^{-12}(\delta/\alpha)^2\log(1/\delta)$. Since $f=\gamma g$, it follows that $i\in[p]$, and for any $j\in[k_i]$, we have

$$|\widehat{f}(\lambda_j^{(i)})|=|\widehat{f}(-\lambda_j^{(i)})|\ge 2\alpha N\qquad(35)$$

(here we have made use (24) and (33)). Now take A as in Lemma 2.2. Then $|A|=[\sum_{x\in\mathbb{Z}_N}f(x)]=[\delta N]$, and for all $r\in\mathbb{Z}_N\setminus\{0\}$, we have

$$|\widehat{A}(r)-\widehat{f}(r)|\le 20\sqrt{N}\,.\qquad(36)$$

Using (35) and $\alpha>40N^{-1/2}$, we get $\{0\}\bigsqcup\Lambda\bigsqcup-\Lambda\subseteq\mathcal{R}_\alpha(A)$.

Let $r\notin\{0\}\bigsqcup\Lambda\bigsqcup-\Lambda$. Prove that $r\notin\mathcal{R}_\alpha(A)$. As was noted above it suffices to consider residuals r such that $r=s_1^{(1)}\lambda_1^{(1)}+\dots+s_{k_1}^{(1)}\lambda_{k_1}^{(1)}+\dots+s_1^{(p)}\lambda_1^{(p)}+\dots+s_{k_p}^{(p)}\lambda_{k_p}^{(p)}$, where for all $i\in[p]$ the following inequalities hold $\sum_{l=1}^{k_i}|s_l^{(i)}|\le 2k_i+1$. Since $r\notin\{0\}\bigsqcup\Lambda\bigsqcup-\Lambda$, it follows that $\sum_{i=1}^{p}\sum_{l=1}^{k_i}|s_l^{(i)}|\ge 2$. Let $\sigma_i=\sum_{l=1}^{k_i}|s_l^{(i)}|$. Then $\sum_{i=1}^{p}\sigma_i\ge 2$ and either there exists $i\in[p]$ such that $\sigma_i\ge 2$ or there exist $i,j\in[p]$, $i\ne j$ such that $\sigma_i,\sigma_j\ge 1$.

Let us prove that for all $i \in [p]$, we have

$$|Q_i(s_1^{(i)}, \dots, s_{k_i}^{(i)})| \le \begin{cases} 2\,, & \text{if } \sigma_i = 0, \\ \frac{1}{2\sqrt{k_i}}\,, & \text{if } \sigma_i = 1, \\ \frac{2}{k_i\sqrt{k_i}}\,, & \text{otherwise.} \end{cases}$$

Clearly it suffices to deal with the case $i = 1$. Let $\sigma = \sigma_1$. If $\sigma = 0$ then we have the upper bound for Q_1. If $\sigma = 1$ then (34) implies that $Q_1 \le \frac{1}{2\sqrt{k_i}}$. Let $\sigma \ge 2$. Suppose that j_0 is the minimal positive integer $j_0 \in [k_1]$ such that $2j_0 + 1 \ge \sigma$ (if there is not such j_0 then $Q_1 = 0$ and we are done). It is easy to see that it is unnecessary to deal with all terms in (32) such that $j < j_0$. Suppose that σ is an odd number. Then $\sigma = 2r + 1$, $r \ge 1$. The absolute value of the coefficient from $j = l \ge j_0$ in (32) does not exceed

$$\frac{1}{2\sqrt{k_1}} \cdot \frac{1}{(64k_1)^l l!} \times \frac{(2l+1)!}{|s_1^{(1)}|! \dots |s_{k_1}^{(1)}|! \cdot (2l+1-\sigma)!} \times$$

$$\times 2k_1 \times (2l+1-\sigma-1) \times 2k_1 \times (2l+1-\sigma-3) \times \dots \times 2k_1 \times 1 := \rho\,. \qquad (37)$$

Indeed firstly if $s_1^{(1)} \ge 0$ then choose $|s_1^{(1)}|$ elements $e(\lambda_1^{(1)}x)$ from (32), if $s_1^{(1)} < 0$ then choose $|s_1^{(1)}|$ elements $e(-\lambda_1^{(1)}x)$. Further if $s_2^{(1)} \ge 0$ then choose $|s_2^{(1)}|$ elements $e(\lambda_2^{(1)}x)$ from (32) and if $s_2^{(1)} < 0$ then choose $|s_2^{(1)}|$ elements $e(-\lambda_2^{(1)}x)$. And so on. This can be done in $(2l+1)!/(|s_1^{(1)}|! \dots |s_{k_1}^{(1)}|! \cdot (2l+1-\sigma)!)$ ways. Secondly we choose $e(\lambda_u^{(1)}x)$ from some other bracket. This can be done in $2k_1$ ways. Clearly, it must be balanced by choosing $e(-\lambda_u^{(1)}x)$ from some other bracket. There are at most $(2l+1-\sigma-1)$ ways of doing this. And so one. Finally we have the inequality (37). Note that if σ is an even number, $\sigma \ge 2$ then the number $Q_1(s_1^{(1)}, \dots, s_{k_1}^{(1)})$ equals zero. Using $\sigma \le 2l + 1$, we get

$$\rho \le \frac{1}{2\sqrt{k_1}} \cdot \frac{k_1^{l-r}}{k_1^l 2^{5l}} \cdot \frac{(2l+1)(2l)(2l-1)\dots(2l+1-\sigma+1)(2l+1-\sigma-1)(2l+1-\sigma-3)\dots 1}{l!}$$

$$\le \frac{1}{2\sqrt{k_1}} k_1^{-r} (2l)^r \frac{2l+1}{2^{4l}} \le \frac{1}{2k_1\sqrt{k_1}} \frac{(2l+1)2l}{2^{4l}}\,.$$

Hence

$$|Q_1(s_1^{(1)}, \dots, s_{k_1}^{(1)})| \le \frac{1}{k_1\sqrt{k_1}} \sum_{l=1}^{\infty} \frac{(2l+1)2l}{2^{4l}} \le \frac{2}{k_1\sqrt{k_1}}$$

and we obtain the required upper bound for Q_1.

If there exists $i \in [p]$ such that $\sigma_i \ge 2$ then we get $|\widehat{g}(r)| \le 2^{-p}N/(k')^{3/2}$, where $k' = \min\{k_i \,:\, i \in [p]\}$. Combining (24), (25) and (33), we obtain $|\widehat{g}(r)| \le \alpha N/4$. If there exist three $\sigma_i = 1$, then using (24), (25) and (33) again, we get $|\widehat{g}(r)| \le \alpha N/4$. Finally, let there are exactly two $\sigma_i = 1$. Combining (24), (25) and (34), we have

$$|\widehat{g}(r)| \le \frac{2^{-p}N}{16k'} \le \frac{\delta p N}{4|\Lambda|} < \frac{3\alpha N}{4}\,.$$

Anyway for all $r \notin \{0\} \bigsqcup \Lambda \bigsqcup -\Lambda$, we get $|\widehat{f}(r)| \le |\widehat{g}(r)| < 3\alpha N/4$. Using (36), we obtain $|\widehat{A}(r)| < \alpha N$ for any $r \notin \{0\} \bigsqcup \Lambda \bigsqcup -\Lambda$. Hence $\mathcal{R}_\alpha(A) = \{0\} \bigsqcup \Lambda \bigsqcup -\Lambda$. This completes the proof.

The following result shows that our Theorem 1.3 is sharp.

Theorem 2.11 *Suppose that $\delta, \alpha \in (0,1]$ are real numbers , N is a prime number, k is a positive integer, $2 \le k \le 2^{-1}\log(1/\delta)$, $32\delta^2 \le \alpha \le \delta/4$ and*

$$2k \max\left\{\log\left(\frac{2^6\delta k}{\alpha^2}\right), \log\left(\frac{2^6\delta^2}{\alpha^3}\right)\right\} \le \log N\,. \tag{38}$$

Then there exists a set $A \subseteq \mathbb{Z}_N$ such that $\delta N \le |A| \le 3\delta N$, $|\mathcal{R}_\alpha(A)| \ge \frac{\delta}{64\alpha^2}$ and for all k, satisfying (38), we have $T_k(\mathcal{R}_\alpha(A)) \le \frac{2^{14k}\delta}{\alpha^{2k}}$.

Note 2.12 We prove in Theorem 2.11 that $|\mathcal{R}_\alpha(A)| \ge \frac{\delta}{64\alpha^2}$. Certainly this lower bound for $|\mathcal{R}_\alpha(A)|$ is absolutely indispensable because Theorem 2.11 is trivial otherwise.

To prove Theorem 2.11 we need in the following definition and lemma.

Definition 2.13 Let k, s be positive integers. Consider the family $\tilde{\Lambda}(k,s)$ of subsets of $\mathbb{Z}_N$. A set $\tilde{\Lambda} = \{\tilde{\lambda}_1, \dots, \tilde{\lambda}_{|\tilde{\Lambda}|}\}$ belongs to the family $\tilde{\Lambda}(k,s)$ if the equality

$$\sum_{i=1}^{|\tilde{\Lambda}|} \tilde{\lambda}_i s_i = 0 \pmod N\,, \quad \tilde{\lambda}_i \in \Lambda\,, \quad s_i \in \mathbb{Z}\,, \quad |s_i| \le s\,, \text{ the number of } s_i \ne 0 \text{ at most } k\,, \tag{39}$$

implies that all s_i are equal to zero.

Clearly $\Lambda(ks,s) \subseteq \tilde{\Lambda}(k,s) \subseteq \Lambda(k,s)$.

Lemma 2.14 *Let N, t, k, s be positive integers, $k \le t$ and $N > \binom{t}{k}(2s+1)^k$. Then $\tilde{\Lambda}(k,s)$ contains a set of the cardinality t.*

Proof. Consider all tuples $(a_1, \dots, a_t)$, where $a_i \in \mathbb{Z}_N$. Obviously that there exist N^t of this tuples. Further there are at most $\binom{t}{k}(2s+1)^k$ of equations (39) with coefficients $s_1, \dots, s_t$. The number of solutions of any non–trivial equation (39) does not exceed $N^{k-1}N^{t-k} = N^{t-1}$. Besides

$$N^{t-1}\binom{t}{k}(2s+1)^k < N^t\,.$$

Whence there exists a tuple $(a_1, \dots, a_t)$, satisfying the trivial equation only. It is easy to see that all residuals in $(a_1, \dots, a_t)$ are different. Hence the set $\tilde{\Lambda} = \{a_1, \dots, a_t\}$ belongs to the family $\tilde{\Lambda}(k,s)$. This completes the proof of the lemma.

Proof of Theorem 2.11. Let $k_1 = 2k$, $t = [\delta/\alpha]$, $\varepsilon = \delta/t$, $m = \max\{t, k_1\}$, $s = \lceil 8m/\varepsilon \rceil$. By assumption $2k\log(\frac{2^6\delta^2}{\alpha^3}) \le \log N$ and $2k\log(\frac{2^6\delta k}{\alpha^2}) \le \log N$. Hence $N > \binom{t}{k_1}(2s+1)^{k_1}$. Using Lemma 2.14, we find a set $\Lambda = \{\lambda_1, \dots, \lambda_t\}$ such that Λ belongs to the family $\tilde{\Lambda}(k_1, s)$.

For any $\lambda \in \mathbb{Z}_N$ consider one–dimensional Bohr set

$$B_\lambda = B_\lambda(\varepsilon) = \{x \in \mathbb{Z}_N \ : \ \left\|\frac{x\lambda}{N}\right\| \le \varepsilon\}\,, \tag{40}$$

(see [30] for example). Clearly, $B_\lambda(\varepsilon) = \{0, \pm\lambda^{-1}, \dots, \pm[\varepsilon N]\lambda^{-1}\}$. Hence $|B_\lambda(\varepsilon)| = 2[\varepsilon N] + 1$. By $B^s_\lambda = B^s_\lambda(\varepsilon)$ denote the set $B^s_\lambda = B_\lambda + s$. We shall construct a family of sets $B^{s_1}_{\lambda_1}, \dots, B^{s_t}_{\lambda_t}$, where $\lambda_i \in \Lambda$, $s_i \in \mathbb{Z}_N$. Let $s_1 = 0$ and we obtain the set $B^{s_1}_{\lambda_1}$. Suppose that we have the sets $B^{s_1}_{\lambda_1}, \dots, B^{s_d}_{\lambda_d}$. Let us construct a residual s_{d+1} and a set $B^{s_{d+1}}_{\lambda_{d+1}}$. Let $C_d = \bigcup_{i=1}^d B^{s_i}_{\lambda_i}$. Clearly, $|C_d| \le d(2[\varepsilon N]+1) \le t(2[\varepsilon N]+1) \le 3\delta N$. Let s_{d+1} be a residual such that

$$|B^{s_{d+1}}_{\lambda_{d+1}} \bigcap C_d| \le (2\varepsilon N + 1)^2 t \le 8\varepsilon\delta N\,. \tag{41}$$

Since

$$\sum_{s\in\mathbb{Z}_N}|C_d\cap B^s_{\lambda_{d+1}}|=|C_d||B_s|\,,$$

it follows that such a residual s_{d+1} exists. So we have the sets $B^{s_1}_{\lambda_1},\dots,B^{s_t}_{\lambda_t}$. Let $A=C_t=\bigcup_{i=1}^t B^{s_i}_{\lambda_i}$. Clearly, $|A|\le 3\delta N$. Prove that $|A|\ge\delta N$. Using (41), we get

$$|A|=|C_t|=|C_{t-1}|+|B^{s_t}_{\lambda_t}|-|C_{t-1}\cap B^{s_t}_{\lambda_t}|\ge|C_{t-1}|+(2[\varepsilon N]+1)-8\varepsilon\delta N\ge \qquad (42)$$

$$\ge|C_{t-2}|+2(2[\varepsilon N]+1)-2\cdot 8\varepsilon\delta N\ge\dots\ge t(2[\varepsilon N]+1)-t8\varepsilon\delta N\ge t\varepsilon N=\delta N\,. \qquad (43)$$

Let us prove that $|\mathcal{R}_\alpha(A)|\ge\frac{\delta}{64\alpha^2}$. Let $a\in\mathbb{Z}_N$. Assuming that a belongs to reduced residue system, we denote by $|a|$ the absolute value of a. We have $|a|\le N/2$ for all $a\in\mathbb{Z}_N$. Let $r\in\mathbb{Z}_N$, $r\ne 0$. Using the inequality $|1-e^{i\theta}|\ge 2|\theta|/\pi$, $\theta\in[-\pi,\pi]$, we get

$$|\widehat{B}_\lambda(r)|=\left|\sum_{l=-[\varepsilon N]}^{[\varepsilon N]}e(\lambda^{-1}lr)\right|=\left|2\frac{e(([\varepsilon N]+1)\lambda^{-1}r)-1}{e(\lambda^{-1}r)-1}-1\right|\le\frac{4}{|e(\lambda^{-1}r)-1|}\le\frac{N}{|\lambda^{-1}r|}\,. \qquad (44)$$

Let us obtain a lower bound for $\widehat{B}_\lambda(r)$. Let λ belongs to Λ and let

$$M_\lambda=\{\,x\in\mathbb{Z}_N\ :\ x=\lambda p\,,\quad |p|\le\frac{1}{16\varepsilon}\,\}\,. \qquad (45)$$

Observe that $|M_\lambda|=2[1/(16\varepsilon)]+1$. For all $r\in M_\lambda$, we have

$$\widehat{B}_\lambda(r)=2\sum_{l=0}^{[\varepsilon N]}\cos(2\pi\lambda^{-1}rl/N)-1\ge 2([\varepsilon N]+1)-1-([\varepsilon N]+1)/4\ge\frac{3}{2}\varepsilon N\,. \qquad (46)$$

Formulas (44) and (46) can be used to calculate Fourier coefficients of the sets $B_\lambda=B_\lambda(\varepsilon)$. Note that for any $s,r\in Z_N$, we have $|\widehat{B}^s_\lambda(r)|=|\widehat{B}_\lambda(r)|$. Thus (44), (46) can be used to find the absolute values of Fourier coefficients of the sets B^s_λ too.

It is easy to see that for all $i,j\in[t]$, $i\ne j$, we have $M_{\lambda_i}\cap M_{\lambda_j}=\{0\}$. Indeed, by assumption the set Λ belongs to the family $\tilde{\Lambda}(k_1,s)$ and $s\ge 1/(16\varepsilon)$. Hence the only solution of the equation $\lambda_ip_i=\lambda_jp_j$, $i\ne j$, $|p_i|,|p_j|\le 1/(16\varepsilon)$ is $p_i=p_j=0$. Prove that $\bigcup_{i=1}^t M_{\lambda_i}\subseteq\mathcal{R}_\alpha(A)$. Clearly, $0\in\mathcal{R}_\alpha(A)$. Let $i\in[t]$ be an arbitrary number, and r be a non–zero residual such that r belongs to some M_{λ_i}. We have

$$\widehat{A}(r)=\widehat{B}^{s_t}_{\lambda_t}(r)+\widehat{C}_{t-1}(r)+8\theta\varepsilon\delta N\,,$$

where $|\theta|\le 1$. By the same arguments as in (42) — (43), we get

$$\widehat{A}(r)=\sum_{l=1}^t\widehat{B}^{s_l}_{\lambda_l}(r)+8\tilde{\theta}\varepsilon\delta tN\,, \qquad (47)$$

where $|\tilde{\theta}|\le 1$. We have $r\in M_{\lambda_i}$. Using (46), we obtain $|\widehat{B}^{s_i}_{\lambda_i}(r)|\ge 3\varepsilon N/2$. Let $r=\lambda_ip_i$, $|p_i|\le 1/(16\varepsilon)$, and $j\in[t]$ be a number, $j\ne i$. Let $p:=\lambda_j^{-1}r=\lambda_j^{-1}\lambda_ip_i$. Then $\lambda_jp=\lambda_ip_i$. Since the set Λ belongs to the family $\tilde{\Lambda}(k_1,s)$, it follows that $|p|>s$. Using the last inequality and (44), we obtain

$$|\widehat{B}^{s_j}_{\lambda_j}(r)|\le\frac{N}{s}\,,\quad r\in M_{\lambda_i},\quad r\ne 0\,. \qquad (48)$$

Combining (48) and (47), we get

$$|\widehat{A}(r)| \geq \frac{3}{2}\varepsilon N - \sum_{j\neq i} |\widehat{B}^{s_j}_{\lambda_j}(r)| - 8\varepsilon\delta t N \geq \frac{3}{2}\varepsilon N - \frac{tN}{s} - 8\varepsilon\delta t N \geq \alpha N\,.$$

Hence $\bigcup_{i=1}^{t} M_{\lambda_i} \subseteq \mathcal{R}_\alpha(A)$ and $|\mathcal{R}_\alpha(A)| \geq \sum_{i=1}^{t} |M_{\lambda_i}| - t = 2t[1/(16\varepsilon)] \geq \frac{\delta}{64\alpha^2}$.

Finally, we shall show that for all k, $2 \leq k \leq 2^{-1}\log(1/\delta)$, we have $T_k(\mathcal{R}_\alpha(A)) \leq \frac{2^{14k}\delta}{\alpha^{2k}}$. Let g be a real number, λ belongs to the set Λ and let

$$L_\lambda(g) = \{\, x \in \mathbb{Z}_N \;:\; x = \lambda p\,, \quad |p| \leq g\,\}\,. \tag{49}$$

Let also $M'_\lambda = L_\lambda(8/\varepsilon)$. Then $|M'_\lambda| \leq 32/\varepsilon$. Let us prove that $\mathcal{R}_\alpha(A) \subseteq \bigcup_{\lambda\in\Lambda} M'_\lambda$. Assume the converse. Let $r \in \mathcal{R}_\alpha(A) \setminus \{0\}$ and $r \notin \bigcup_{\lambda\in\Lambda} M'_\lambda$. If $r \notin \bigcup_{\lambda\in\Lambda} L_\lambda(s)$ then using (47), we get

$$|\widehat{A}(r)| \leq \frac{tN}{s} + 8\varepsilon\delta t N \leq \frac{\varepsilon}{2}N < \alpha N$$

and $r \notin \mathcal{R}_\alpha(A)$. Let now $r \in \bigcup_{\lambda\in\Lambda} L_\lambda(s)$. We have $\Lambda \in \tilde{\Lambda}(k_1, s)$. Using this fact, we obtain that for all $\lambda_1, \lambda_2 \in \Lambda$, $\lambda_1 \neq \lambda_2$ the following holds $L_{\lambda_1}(s) \cap L_{\lambda_2}(s) = \{0\}$. Let $r \neq 0$. It is easy to see that there exists the only $i \in [t]$ such that $r \in L_{\lambda_i}(s)$. Using (47), we obtain

$$|\widehat{A}(r)| \leq |\widehat{B}^{s_i}_{\lambda_i}(r)| + \frac{tN}{s} + 8\varepsilon\delta t N\,. \tag{50}$$

We have $r \notin \bigcup_{\lambda\in\Lambda} M'_\lambda$. Using (44), we get $|\widehat{B}^{s_i}_{\lambda_i}(r)| \leq N/g \leq \varepsilon N/8$. Substituting the last inequality in (50), we obtain $|\widehat{A}(r)| \leq \varepsilon N/2 < \alpha N$ and $r \notin \mathcal{R}_\alpha(A)$. Whence $\mathcal{R}_\alpha(A) \subseteq \bigcup_{\lambda\in\Lambda} M'_\lambda$.

Consider the equation

$$r_1 + \cdots + r_k = r'_1 + \cdots + r'_k\,, \tag{51}$$

where all r_j, r'_j belong to $\mathcal{R}_\alpha(A)$. We have $\mathcal{R}_\alpha(A) \subseteq \bigcup_{i=1}^{t} M'_{\lambda_i}$. Hence any residual from (51) belongs to a set M'_{λ_i}.

Let z be a non–negative integer, and $s_1, \ldots, s_l$ be positive integers such that $s_1+\cdots+s_l+z = 2k$. Recall that for all $\lambda_1, \lambda_2 \in \Lambda$, $\lambda_1 \neq \lambda_2$, we have $L_{\lambda_1}(s) \cap L_{\lambda_2}(s) = \{0\}$. Hence for any $i, j \in [t]$, $i \neq j$, we get $M'_{\lambda_i} \cap M'_{\lambda_j} = \{0\}$. Let $M'_i = M'_{\lambda_i}$, $i \in [t]$, and $w = 2^5/\varepsilon$. Then for all $i \in [t]$, we have $|M'_i| \leq w$. By $E(s_1, \ldots, s_l, z)$ denote the set of all solutions $r_1, \ldots, r_k$, $r'_1, \ldots, r'_k$ of (51) such that among r_j, r'_j there exist exactly z of zeroes, there exist exactly s_1 non–zero residuals belong to a set M'_{j_1}, there exist exactly s_2 non–zero residuals belong to a set M'_{j_2}, …, there exist exactly s_l non–zero residuals belong to a set M'_{j_l} and at the same time all sets $M'_{j_1}, M'_{j_2}, \ldots, M'_{j_l}$ are different. Using $\Lambda \in \tilde{\Lambda}(k_1, s)$, we obtain

$$T_k(\mathcal{R}_\alpha(A)) = \sum_{l=1}^{2k}\sum_{z=0}^{2k} \sum_{s_1,\ldots,s_l,\; s_1+\cdots+s_l+z=2k} |E(s_1, \ldots, s_l, z)| \leq$$

$$\leq t w^{2k-1} + \sum_{l=2}^{2k}\sum_{z=0}^{2k} \sum_{s_1,\ldots,s_l,\; s_1+\cdots+s_l+z=2k} |E(s_1, \ldots, s_l, z)|\,. \tag{52}$$

Let us fixed $s_1, \ldots, s_l, z$ and consider the solutions of (51) belong to fixed subsets $M'_{j_1}, M'_{j_2}, \ldots, M'_{j_l}$. Denote by $E(s_1, \ldots, s_l, z)(M'_{j_1}, M'_{j_2}, \ldots, M'_{j_l})$ the set of all these solutions. Rewrite the equation (51) as

$$u_1 + \cdots + u_l = 0\,, \tag{53}$$

where $u_i \in M'_{j_i}$, $i \in [l]$. Since Λ belongs to $\tilde{\Lambda}(k_1, s)$, it follows that all residuals u_i equal zero. Hence, we have

$$|E(s_1, \dots, s_l, z)(M'_{j_1}, M'_{j_2}, \dots, M'_{j_l})| \le \frac{(2k)!}{s_1! \dots s_l! z!} w^{s_1 - 1} \times \dots \times w^{s_l - 1} \le \frac{(2k)!}{s_1! \dots s_l! z!} w^{2k-l}\,.$$

Whence

$$|E(s_1, \dots, s_l, z)| \le \binom{t}{l} \frac{(2k)!}{s_1! \dots s_l! z!} w^{2k-l} \le \frac{t^l}{l!} \cdot \frac{(2k)!}{s_1! \dots s_l! z!} w^{2k-l}\,. \tag{54}$$

Combining (54) and (52), we get

$$T_k(\mathcal{R}_\alpha(A)) \le t w^{2k-1} + \sum_{l=2}^{2k} \frac{t^l}{l!} w^{2k-l} \sum_{z=0}^{2k} \sum_{s_1, \dots, s_l,\ s_1 + \dots + s_l + z = 2k} \frac{(2k)!}{s_1! \dots s_l! z!} \le$$

$$\le t w^{2k-1} + \sum_{l=2}^{2k} \frac{t^l}{l!} w^{2k-l} (l+1)^{2k} = t w^{2k-1} + w^{2k} \sum_{l=2}^{2k} \left(\frac{t}{w}\right)^l \cdot (l+1)^{2k} \cdot \frac{1}{l!}\,. \tag{55}$$

Consider the function $f(l) = (t/w)^l (l+1)^{2k}$. It is easy to see that $f(l)$ has maximum at $l_0 = 2k/\ln(w/t) - 1$ and for all $l \ge l_0$ the function $f(l)$ is monotonically decreasing. By assumption $k \le 2^{-1}\log(1/\delta)$. Hence $l_0 \le 1$. It follows that

$$T_k(\mathcal{R}_\alpha(A)) \le t w^{2k-1} + 2^{2k} t w^{2k-1} \le 2^{2k+1} t w^{2k-1} \le \frac{2^{14k}\delta}{\alpha^{2k}}\,.$$

This completes the proof of the Theorem.

3. Proof of Theorem 1.5.

We assume in the section that N is a prime number.

Definition 3.1 Let k, s, d be positive integers. Let also $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\} \subseteq \mathbb{Z}_N$ be a set such that $\Lambda \cap -\Lambda = \emptyset$. Let $\vec{v}_1 = (v_1^{(1)}, \dots, v_1^{(d)}), \dots, \vec{v}_{|\Lambda|} = (v_{|\Lambda|}^{(1)}, \dots, v_{|\Lambda|}^{(d)})$ be vectors from $\mathbb{Z}^d$ such that for all $i \in [d]$, $j \in [|\Lambda|]$, we have $|\vec{v}_j^{(i)}| \le s$. Consider the equation

$$\lambda_1 \vec{v}_1 + \dots + \lambda_{|\Lambda|} \vec{v}_{|\Lambda|} = 0 \pmod N\,, \tag{56}$$

where $\lambda_i \in \Lambda$ and for any $i \in [d]$, we have $\sum_{j=1}^{|\Lambda|} |v_j^{(i)}| \le k$. Consider the family $\Lambda_d(k, s)$ of subsets of $\mathbb{Z}_N$. Our set Λ belongs to the family $\Lambda_d(k, s)$, if any equation (56) imply that the matrix

$$\begin{pmatrix} v_1^{(1)} & \dots & v_{|\Lambda|}^{(1)} \\ \dots & \dots & \dots \\ v_1^{(d)} & \dots & v_{|\Lambda|}^{(d)} \end{pmatrix}$$

has the rank at most $d-1$.

As was noted above the definition of $\Lambda_1(k, 1)$ can be found in [29], and the definition of $\Lambda_1(k, s)$ can be found in [32].

For an arbitrary $\Lambda \in \Lambda_d(k, s)$, we obtain the following upper bound for $T_k(\Lambda)$.

Statement 3.2 *Let N, k, s, d be positive integers, $s \ge 3$, $N \ge s+1$ be a prime number, and $\Lambda \subseteq \mathbb{Z}_N$ be a subset of the family $\Lambda_d(2k, s)$. Then*

$$T_k(\Lambda) \le 2^{9k} k^k |\Lambda|^k (s+1)^{2d} \cdot 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}}\,. \tag{57}$$

Example 3.3 Let $k \geq 2$, $\log|\Lambda| \geq \log^2 k$, and Λ be an arbitrary subset of the family $\Lambda_d(k,3)$. Using (57), we get $T_k(\Lambda) \leq 2^{20k+4d} k^k |\Lambda|^k$.

Proof of Statement 3.2. Let $x \in \mathbb{Z}_N$ be a residual. By $N_k(x)$ define the number of vectors $(\lambda_1, \dots, \lambda_k)$ such that all λ_i belong to Λ and

$$\lambda_1 + \dots + \lambda_k = x\,. \tag{58}$$

Then $T_k(\Lambda) = \sum_{x \in \mathbb{Z}_N} N_k^2(x)$. Let $s_1, \dots, s_l$ be positive integers such that $s_1 + \dots + s_l = k$. By $E(s_1, \dots, s_l)(x)$ denote the set of all solutions $(\lambda_1, \dots, \lambda_k)$ of (58) such that among $\lambda_1, \dots, \lambda_k$ there exist exactly s_1 residuals equal $\tilde{\lambda}_1$, there exist exactly s_2 residuals equal $\tilde{\lambda}_2$, $\dots$, there exist exactly s_l residuals equal $\tilde{\lambda}_l$ such that $s_1\tilde{\lambda}_1 + \dots + s_l\tilde{\lambda}_l = x$ and all $\tilde{\lambda}_i$ are different. Let us denote the set $E(s_1, \dots, s_l)(x)$ by $E(\vec{s})(x)$ for simplicity. Recall that for $s_1, \dots, s_l$ in the definition of $E(\vec{s})(x) = E(s_1, \dots, s_l)(x)$ the following equality holds : $\sum_{i=1}^l s_i = k$. We have

$$N_k(x) = \sum_{\vec{s}} |E(\vec{s})(x)|\,.$$

Whence

$$\sigma = T_k(\Lambda) = \sum_{x \in \mathbb{Z}_N} (\sum_{\vec{s}} |E(\vec{s})(x)|)^2\,. \tag{59}$$

Let $\vec{s} = (s_1, \dots, s_l)$ and $G = G(\vec{s}) = \{i \ : \ s_i \leq s\}$, $B = B(\vec{s}) = \{i \ : \ s_i > s\}$. Then $|G(\vec{s})| + |B(\vec{s})| = l(\vec{s}) = l$. We have

$$l \leq k - s|B|\,. \tag{60}$$

Indeed

$$k = \sum_{i \in G} s_i + \sum_{i \in B} s_i \geq |G| + (s+1)|B| = l + s|B|\,. \tag{61}$$

Using (61), we obtain (60). Let also

$$l_j = l_j(\vec{s}) = |\,\{i \ : \ s_i = j,\ i \in [l]\}\,|\,, \qquad j = 1, 2, \dots, r = r(\vec{s})\,, \quad r \neq 0\,.$$

The next lemma was proved in [32].

Lemma 3.4 *For all $\vec{s}$, $\sum_{i=1}^l s_i = k$ the number of $x \in \mathbb{Z}_N$ such that $E(\vec{s})(x) \neq \emptyset$ does not exceed $|\Lambda|^l / l_1!$.*

We need in two lemmas.

Lemma 3.5 *Suppose that n, t, s are positive integers, $t \leq n$, $\vec{u}_1, \dots, \vec{u}_t \in \mathbb{Z}_N^n$ are linearly–independent vectors over $\mathbb{Z}_N$, and $N \geq s+1$. Let*

$$Q(s) := \{\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}_N^n \ : \ x_i \in \{0, 1, \dots, s\},\ \ i = 1, \dots, n\}$$

be a n–dimensional cube and $L = \{\vec{x} \in \mathbb{Z}_N^n \ : \ \vec{x} = \sum_{i=1}^t m_i \vec{u}_i,\ \ m_i \in \mathbb{Z}_N\}$. Then $|L \cap Q(s)| \leq (s+1)^t$.

Proof of Lemma 3.5. Let $\vec{u}_1 = (u_1^{(1)}, \dots, u_1^{(n)}), \dots, \vec{u}_t = (u_t^{(1)}, \dots, u_t^{(n)})$. Note that the cube $Q(s)$ is invariant under permutations of coordinates. So we can assume without loss of generality that the vectors $\vec{u}_1, \dots, \vec{u}_t$ have the form $\vec{u}_1 = (1, \dots, 0, 0, u_t^{(t+1)}, \dots, u_1^{(n)}), \vec{u}_2 = (0, 1, \dots, 0, u_t^{(t+1)}, \dots, u_2^{(n)}), \dots, \vec{u}_t = (0, \dots, 0, 1, u_t^{(t+1)}, \dots, u_t^{(n)})$. Let $\vec{x}$ be an arbitrary vector, $\vec{x} \in L \cap Q(s)$. Then there exist residuals $m_1, \dots, m_t$ such that $\vec{x} = \sum_{i=1}^t m_i \vec{u}_i$. Clearly,

$m_1 = x_1, \dots, m_t = x_t$. Since $\vec{x} \in Q(s)$, it follows that $m_i \in \{0, 1, \dots, s\}$, $i = 1, \dots, t$. Hence $|L \cap Q(s)| \le (s+1)^t$ as required.

Lemma 3.6 *For any $\vec{s}$, $\sum_{i=1}^{l} s_i = k$ and for any $x \in \mathbb{Z}_N$, we have*

$$|E(\vec{s})(x)| \le \frac{k!}{s_1! \dots s_l!} (s+1)^d |\Lambda|^{|B(\vec{s})|} . \qquad (62)$$

Proof of Lemma 3.6. Let $(\lambda^{(1)}, \dots, \lambda^{(k)}) \in E(\vec{s})(x)$. Then $\sum_{i=1}^{k} \lambda^{(i)} = \sum_{i=1}^{l} s_i \tilde{\lambda}^{(i)} = x$ and all residuals $\tilde{\lambda}^{(i)} \in \{\lambda^{(1)}, \dots, \lambda^{(k)}\}$ are different. Thus for any $(\lambda^{(1)}, \dots, \lambda^{(k)}) \in E(\vec{s})(x)$ there exists the only vector $(\tilde{\lambda}^{(1)}, \dots, \tilde{\lambda}^{(l)})$ such that all $\tilde{\lambda}^{(i)}$ are different. Let us fixed $\tilde{\lambda}^{(i)}$, $i \in B(\vec{s})$. We obtain the set $K = K(B(\vec{s}))$ of $(\lambda^{(1)}, \dots, \lambda^{(k)}) \in E(\vec{s})(x)$. Let us prove that the cardinality of K does not exceed $(s+1)^d \frac{k!}{s_1! \dots s_l!}$.

Let $(\lambda^{(1)}, \dots, \lambda^{(k)})$ be a vector from K. We have

$$\sum_{i \in G(\vec{s})} s_i \tilde{\lambda}^{(i)} = x - \sum_{i \in B(\vec{s})} s_i \tilde{\lambda}^{(i)} = x' . \qquad (63)$$

Since the elements $\tilde{\lambda}^{(i)}$, $i \in B(\vec{s})$ are fixed, it follows that the residual x' is the same for all $(\lambda^{(1)}, \dots, \lambda^{(k)}) \in K$.

Let the set $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ be ordered in an arbitrary way. To each $(\lambda^{(1)}, \dots, \lambda^{(k)}) \in K$ assign the vector $\vec{u} = (u_1, \dots, u_{|\Lambda|})$, where

$$u_j = \begin{cases} s_i , & \text{if for some } i \in G(\vec{s}) \text{ we have } \lambda_j = \tilde{\lambda}^{(i)}, \\ 0 , & \text{otherwise.} \end{cases}$$

Let $\vec{w} = (w_1, \dots, w_m)$, $\vec{w}' = (w'_1, \dots, w'_m)$ be two vectors from $\mathbb{Z}^m$. By $(\vec{w}, \vec{w}')$ denote the inner product of these vectors: $(\vec{w}, \vec{w}') = \sum_{j=1}^{m} w_j w'_j$. Rewrite (63) as

$$(\vec{u}, \vec{\lambda}) = x' , \qquad (64)$$

where $\vec{\lambda} = (\lambda_1, \dots, \lambda_{|\Lambda|})$. Let $\vec{u}_1, \dots, \vec{u}_t$ be a maximal system of vectors which are linearly–independent over $\mathbb{Z}_N$ and such that any of these vectors satisfies (64).

Suppose that $t \ge d+1$.

Since all vector $\vec{u}_i$, $i = 1, \dots, t$ satisfy (64), it follows that

$$\begin{cases} (\vec{u}_2 - \vec{u}_1, \vec{\lambda}) = 0 . \\ \dots\dots\dots\dots\dots \\ (\vec{u}_{d+1} - \vec{u}_1, \vec{\lambda}) = 0 . \end{cases}$$

Rewrite this system as $\lambda_1 \vec{v}_1 + \dots + \lambda_{|\Lambda|} \vec{v}_{|\Lambda|} = 0$, where $\vec{v}_i$ are vectors from $\mathbb{Z}^d$. Let $\vec{v}_1 = (v_1^{(1)}, \dots, v_1^{(d)}), \dots, \vec{v}_{|\Lambda|} = (v_{|\Lambda|}^{(1)}, \dots, v_{|\Lambda|}^{(d)})$. Since $\Lambda \cap -\Lambda = \emptyset$, it follows that $|\vec{v}_i^{(j)}| \le s$. It is easy to see that for any $i \in [d]$, we have $\sum_{j=1}^{|\Lambda|} |v_j^{(i)}| \le 2k$. Consider the matrix

$$M = \begin{pmatrix} v_1^{(1)} & \dots & v_{|\Lambda|}^{(1)} \\ \dots & \dots & \dots \\ v_1^{(d)} & \dots & v_{|\Lambda|}^{(d)} \end{pmatrix}$$

Let $\vec{p}_j = (v_1^{(j)}, \dots, v_{|\Lambda|}^{(j)})$, $j = 1, \dots, d$ be rows of M. Clearly, $\vec{p}_j = \vec{u}_{j+1} - \vec{u}_1$, $j = 1, \dots, d$. Since the vectors $\vec{u}_1, \dots, \vec{u}_{d+1}$ are linearly–independent, it follows that the vectors $\vec{p}_1, \dots, \vec{p}_d$ are also linearly–independent. Hence the rank of M is equal to d with contradiction to the definition of the family $\Lambda_d(2k, s)$.

Thus, we have $t \le d$. Let $\vec{u}$ be an arbitrary vector satisfies (64) By maximality of the system $\vec{u}_1, \dots, \vec{u}_t$, we get $\vec{u} = \sum_{i=1}^{t} m_i \vec{u}_i$, where $m_i \in \mathbb{Z}_N$. All coordinates of $\vec{u}$ belong to $\{0, 1, \dots, s\}$. Using Lemma 3.5, we obtain that the number of such $\vec{u}$ does not exceed $(s+1)^d$. Clearly, any vector $\vec{u}$ corresponds to the tuple $\{\tilde{\lambda}^{(i)}\}_{i \in G(\vec{s})}$. Besides we fixed residuals $\{\tilde{\lambda}^{(i)}\}_{i \in B(\vec{s})}$. Using the definition of the set $E(\vec{s})(x)$, we get that the number of permutations of the tuple $\{\tilde{\lambda}^{(i)}\}_{i \in G(\vec{s})} \bigsqcup \{\tilde{\lambda}^{(i)}\}_{i \in B(\vec{s})}$ equals $\frac{k!}{s_1! \dots s_l!}$. Hence the cardinality of the set K at most $(s+1)^d \frac{k!}{s_1! \dots s_l!}$ and the cardinality of $E(\vec{s})(x)$ at most $(s+1)^d \frac{k!}{s_1! \dots s_l!} |\Lambda|^{|B(\vec{s})|}$. This completes the proof of Lemma 3.6.

Let us return to the proof of Statement 3.2.

Let $t = (k \log k)/\log(k^{2s}|\Lambda|^{s-2})$. We can assume without loss of generality that

$$|\Lambda|^k \ge 2^{9k} k^k \,. \tag{65}$$

Using (65), we get $|\Lambda| \ge 2^9 k \ge k$. Let us estimate the sum σ.

$$\sigma \le 2 \left(\sum_{x \in \mathbb{Z}_N} \left(\sum_{\vec{s}: |B(\vec{s})| \le t} |E(\vec{s})(x)| \right)^2 + \sum_{x \in \mathbb{Z}_N} \left(\sum_{\vec{s}: |B(\vec{s})| > t} |E(\vec{s})(x)| \right)^2 \right) = 2\sigma_1 + 2\sigma_2 \,. \tag{66}$$

We have

$$\sigma_2 \le \sum_{\vec{s}_1, \vec{s}_2: |B(\vec{s}_1)| > t, |B(\vec{s}_2)| > t} \sum_x |E(\vec{s}_1)(x)| \cdot |E(\vec{s}_2)(x)| \tag{67}$$

If $|B(\vec{s}_1)| > |B(\vec{s}_2)|$ then put $\vec{s}^* = \vec{s}_1$. If $|B(\vec{s}_1)| \le |B(\vec{s}_2)|$ then set $\vec{s}^* = \vec{s}_2$. Let also $P_k(\vec{s}) = k!/(s_1! \dots s_l!)$. Using Lemma 3.6, we obtain $|E(\vec{s}_1)(x)| \le P_k(\vec{s}_1)(s+1)^d |\Lambda|^{|B(\vec{s}^*)|}$ and $|E(\vec{s}_2)(x)| \le P_k(\vec{s}_2)(s+1)^d |\Lambda|^{|B(\vec{s}^*)|}$. Further, using Lemma 3.4, we get

$$\sigma_2 \le (s+1)^{2d} \sum_{\vec{s}_1, \vec{s}_2: |B(\vec{s}_1)| > t, |B(\vec{s}_2)| > t} |\Lambda|^{l(\vec{s}^*)} |\Lambda|^{2|B(\vec{s}^*)|} P_k(\vec{s}_1) P_k(\vec{s}_2) \,. \tag{68}$$

Taking into account (60), we have

$$\sigma_2 \le (s+1)^{2d} \sum_{\vec{s}_1, \vec{s}_2: |B(\vec{s}_1)| > t, |B(\vec{s}_2)| > t} |\Lambda|^{k - s|B(\vec{s}^*)|} |\Lambda|^{2|B(\vec{s}^*)|} P_k(\vec{s}_1) P_k(\vec{s}_2) \le \tag{69}$$

$$\le (s+1)^{2d} |\Lambda|^k |\Lambda|^{-t(s-2)} \sum_{\vec{s}_1, \vec{s}_2} P_k(\vec{s}_1) P_k(\vec{s}_2) \le 2^4 (s+1)^{2d} |\Lambda|^k |\Lambda|^{-t(s-2)} (k^k)^2 \,. \tag{70}$$

Since $t = (k \log k)/\log(k^{2s}|\Lambda|^{s-2})$, it follows that

$$k^k |\Lambda|^{-t(s-2)} \le 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}} \,. \tag{71}$$

Hence

$$\sigma_2 \le 2^4 k^k |\Lambda|^k (s+1)^{2d} \cdot 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}} \,. \tag{72}$$

Let us estimate σ_1.

$$\sigma_1 \le 2\left(\sum_{x\in\mathbb{Z}_N}\left(\sum_{\vec{s}:|B(\vec{s})|\le t, l(\vec{s})\le k-st}|E(\vec{s})(x)|\right)^2+\sum_{x\in\mathbb{Z}_N}\left(\sum_{\vec{s}:|B(\vec{s})|\le t, l(\vec{s})>k-st}|E(\vec{s})(x)|\right)^2\right)=$$

$$=2\sigma_1^{'}+2\sigma_1^{''}\,. \tag{73}$$

We have

$$\sigma_1^{'}\le \sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|,|B(\vec{s}_2)|\le t,\ l(\vec{s}_1),l(\vec{s}_2)\le k-st}\ \sum_x |E(\vec{s}_1)(x)|\cdot|E(\vec{s}_2)(x)| \tag{74}$$

Using Lemmas 3.4, 3.6 and (71), we obtain

$$\sigma_1^{'}\le (s+1)^{2d}\sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|,|B(\vec{s}_2)|\le t,\ l(\vec{s}_1),l(\vec{s}_2)\le k-st}|\Lambda|^{l(\vec{s}^*)}|\Lambda|^{2|B(\vec{s}^*)|}P_k(\vec{s}_1)P_k(\vec{s}_2)\le \tag{75}$$

$$\le 2^4(s+1)^{2d}|\Lambda|^k|\Lambda|^{-t(s-2)}(k^k)^2\le 2^4k^k|\Lambda|^k(s+1)^{2d}\cdot 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}}\,. \tag{76}$$

We need in an upper bound for $\sigma_1^{''}$. For any $\vec{s}=(s_1,\dots,s_l)$, $\sum_{i=1}^l s_i=k$, we have

$$l_1+\dots+l_r=l\quad\text{ and }\quad l_1+2l_2+\dots+rl_r=k\,. \tag{77}$$

Using (77), we get $l=k-(l_2+2l_3+\dots+(r-1)l_r)$. On the other hand $l\ge k-st$. It follows that $l_2+2l_3+\dots+(r-1)l_r\le st$. Further, $l_2+\dots+l_r\le l_2+2l_3+\dots+(r-1)l_r\le st$. Whence $l_1=l-(l_2+\dots+l_r)\ge l-st\ge k-2st$. Taking into account Lemmas 3.4, 3.6 and (60), we obtain

$$\sigma_1^{''}\le \sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|,|B(\vec{s}_2)|\le t, l(\vec{s}_1),l(\vec{s}_2)>k-st}\ \sum_x |E(\vec{s}_1)(x)|\cdot|E(\vec{s}_2)(x)|\le \tag{78}$$

$$\le (s+1)^{2d}\sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|,|B(\vec{s}_2)|\le t,\ l(\vec{s}_1),l(\vec{s}_2)>k-st}\frac{|\Lambda|^{l(\vec{s}^*)}|\Lambda|^{2|B(\vec{s}^*)|}}{l_1(\vec{s}^*)!}P_k(\vec{s}_1)P_k(\vec{s}_2)\le \tag{79}$$

$$\le (s+1)^{2d}\sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|,|B(\vec{s}_2)|\le t,\ l(\vec{s}_1),l(\vec{s}_2)>k-st}\frac{|\Lambda|^{k-s|B(\vec{s}^*)|}|\Lambda|^{2|B(\vec{s}^*)|}}{l_1(\vec{s}^*)!}P_k(\vec{s}_1)P_k(\vec{s}_2)\,. \tag{80}$$

Since $l_1=l_1(\vec{s}^*)\ge k-2st$, it follows that

$$\sigma_1^{''}\le (s+1)^{2d}\frac{|\Lambda|^k}{[k-2st]!}\sum_{\vec{s}_1,\vec{s}_2}P_k(\vec{s}_1)P_k(\vec{s}_2)\le 2^4(s+1)^{2d}\frac{|\Lambda|^k}{[k-2st]!}(k^k)^2\,. \tag{81}$$

We have $|\Lambda|\ge k$. Whence $t\le k/(3s-2)$. Using the last inequality, we get

$$[k-2st]!\ge [k-2st]^{[k-2st]}/e^k\ge k^{[k-2st]}/(8e)^k\,.$$

Since $t=(k\log k)/\log(k^{2s}|\Lambda|^{s-2})$, it follows that $k^{2st}\le 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}}$. Further,

$$[k-2st]!\ge k^k/(2^{5k}2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}})\,.$$

Hence

$$\sigma_1^{''} \le 2^4 2^{5k} k^k |\Lambda|^k (s+1)^{2d} \cdot 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}} . \tag{82}$$

Combining (72), (76) and (82), we finally obtain

$$\sigma = T_k(\Lambda) \le 2^{9k} k^k |\Lambda|^k (s+1)^{2d} \cdot 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}} . \tag{83}$$

This completes the proof of Statement 3.2.

Proof of Theorem 1.5 Let $k = [\log(1/\delta)]$. Since $0 \in \mathcal{R}_\alpha$ and $\mathcal{R}_\alpha = -\mathcal{R}_\alpha$, it follows that there exists a set $\mathcal{R}_\alpha^{(1)}$ such that $\mathcal{R}_\alpha = \mathcal{R}_\alpha^{(1)} \bigsqcup -\mathcal{R}_\alpha^{(1)} \bigsqcup \{0\}$ and $\mathcal{R}_\alpha^{(1)} \cap -\mathcal{R}_\alpha^{(1)} = \emptyset$. Let $s = 3$ and $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ be a maximal subset of $\mathcal{R}_\alpha^{(1)}$ such that Λ belongs to $\Lambda_d(2k, s)$. Let $\Lambda^* = (\bigcup_{j=1}^3 j^{-1}\Lambda) \bigcup (-\bigcup_{j=1}^3 j^{-1}\Lambda)$. Then $|\Lambda^*| \le 8|\Lambda|$.

Let us prove that for any $r \in \mathcal{R}_\alpha^{(1)}$ there exists a vector $\vec{u} = (u_1, \dots, u_d)$ and there exist vectors $\vec{v}_1 = (v_1^{(1)}, \dots, u_1^{(d)}), \dots, \vec{v}_1 = (v_{|\Lambda|}^{(1)}, \dots, u_{|\Lambda|}^{(d)})$ such that $|u_l| \le s$, $l = 1, \dots, d$, $|v_j^{(i)}| \le s$, $i = 1, \dots, d$, $j = 1, \dots, |\Lambda|$ and

$$r\vec{u} = \sum_{i=1}^{|\Lambda|} \lambda_i \vec{v}_i \, , \tag{84}$$

where for all $i \in [d]$ the following inequality holds $\sum_{j=1}^{|\Lambda|} |v_j^{(i)}| \le k$ and the rank of the matrix

$$M = \begin{pmatrix} v_1^{(1)} & \cdots & v_{|\Lambda|}^{(1)} \\ \cdots & \cdots & \cdots \\ v_1^{(d)} & \cdots & v_{|\Lambda|}^{(d)} \end{pmatrix}$$

equals d.

If such vectors exist then it is easy to see that (11) holds. Indeed since the set Λ belongs to $\Lambda_d(2k, s)$, it follows that the vector $\vec{u}$ does not equal zero. Hence it has non–zero component. Without loss of generality it can be assumed that the first component of $\vec{u}$ does not equal zero. For any i take i–th equation of system (84) such that $\vec{u}_i = 0$ and add the first equation of (84) to this equation. We obtain a new system

$$r\vec{u}' = \sum_{i=1}^{|\Lambda|} \lambda_i \vec{v}_i' \, , \tag{85}$$

where *all* components of a vector $\vec{u}'$ do not equal zero, for any $i \in [d]$ we have $\sum_{j=1}^{|\Lambda|} |(v_j')^{(i)}| \le 2k \le 4 \log 1/\delta$ and a matrix $M' = \{\vec{v}_1', \dots, \vec{v}_{|\Lambda|}'\}$ has the rank d. Clearly, it can be assumed that all components of $\vec{u}'$ belong to $[s]$. For any $i \in [|\Lambda|]$ and for any $j \in [s]$, we have $j^{-1}\lambda_i \in \Lambda^*$. Hence system (85) implies (11) for all $r \in \mathcal{R}_\alpha^{(1)}$. This obviously implies that equation (11) holds for all $r \in -\mathcal{R}_\alpha^{(1)}$.

Thus let r be an arbitrary element of $\mathcal{R}_\alpha^{(1)} \setminus \Lambda$. Let us consider all equations

$$\sum_{i=1}^{|\Lambda|} \tilde{\lambda}_i \vec{v}_i + r\vec{u} = \vec{0} \, , \tag{86}$$

such that $|v_j^{(i)}|, |u^{(i)}| \le s$ and for all $i \in [d]$, we have $\sum_{j=1}^{|\Lambda|} |v_j^{(i)}| + |u^{(i)}| \le k$. Consider all matrices

$$M_1 = \begin{pmatrix} v_1^{(1)} & \dots & v_{|\Lambda|}^{(1)} & u^{(1)} \\ \dots & \dots & \dots & \dots \\ v_1^{(d)} & \dots & v_{|\Lambda|}^{(d)} & u^{(d)} \end{pmatrix}$$

If all these matrices have the rank at most $d-1$ then we obtain a contradiction with maximality of Λ. It follows that there exists an equation (86) such that the rank of M_1 equals d. Let M be the $(d \times |\Lambda|)$ matrix composed of first $|\Lambda|$ columns of M_1. Using (86), we get that the rank of M is also equals d. As was noted above this implies (11).

Let us obtain the bound $|\Lambda^*| \le \max(\, 2^{30+8d(\log(1/\delta))^{-1}} \cdot (\delta/\alpha)^2 \log(1/\delta), 2^{(\log\log(1/\delta))^2+3}\,)$.

If $\log|\Lambda| < (\log k)^2$ then $|\Lambda| \le 2^{(\log\log(1/\delta))^2}$ and $|\Lambda^*| \le 2^{(\log\log(1/\delta))^2+3}$. Suppose that $\log|\Lambda| \ge (\log k)^2$. Using Statement 3.2, we get $T_k(\Lambda) \le 2^{20k+4d} k^k |\Lambda|^k$. On the other hand, using Theorem 1.3, we obtain $T_k(\Lambda) \ge \delta\alpha^{2k}|\Lambda|^{2k}/(2^{4k}\delta^{2k})$. Hence $|\Lambda| \le 2^{27+8d(\log(1/\delta))^{-1}}(\delta/\alpha)^2\log(1/\delta)$ and $|\Lambda^*| \le 2^{30+8d(\log(1/\delta))^{-1}} \cdot (\delta/\alpha)^2\log(1/\delta)$.

In any case, we have $|\Lambda^*| \le \max(\, 2^{30+8d(\log(1/\delta))^{-1}} \cdot (\delta/\alpha)^2 \log(1/\delta), 2^{(\log\log(1/\delta))^2+3}\,)$.

Let us prove that $|\Lambda^*| \le 2^{30}(\delta/\alpha)^2\log^{\varphi}(1/\delta)$. If $|\Lambda| < k^{\varphi}$ then $|\Lambda^*| \le 8|\Lambda| \le 8k^{\varphi}$ and we are done. If $|\Lambda| \ge k^{\varphi}$ then using Statement 3.2, we obtain

$$T_k(\Lambda) \le 2^{9k+4d} k^k |\Lambda|^k \cdot 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}} = 2^{9k+4d} k^k |\Lambda|^k \cdot 2^{\frac{6k(\log k)^2}{\log(k^6 k^{\varphi})}} = 2^{9k+4d} k^k |\Lambda|^k k^{\frac{6}{6+\varphi}}\,. \qquad (87)$$

On the other hand, using Theorem 1.3, we get $T_k(\Lambda) \ge \delta\alpha^{2k}|\Lambda|^{2k}/(2^{4k}\delta^{2k})$. Whence $|\Lambda| \le 2^{17+8d(\log(1/\delta))^{-1}}(\delta/\alpha)^2\log^{\varphi}(1/\delta)$ and $|\Lambda^*| \le 2^{20+8d(\log(1/\delta))^{-1}}(\delta/\alpha)^2\log^{\varphi}(1/\delta)$. This completes the proof.

4. Some examples of sets of large exponential sums in vectors spaces over finite field.

Let p be a prime number, n and N be positive integers, $N = p^n$. In the section we consider groups $\mathbb{Z}_p^n = (\mathbb{Z}/p\mathbb{Z})^n$, $|\mathbb{Z}_p^n| = N$. A finite Abelian group $\mathbb{Z}_p^n$ is a vector space with inner product

$$\vec{x}\cdot\vec{y} = <\vec{x},\vec{y}> = x_1y_1 + \dots + x_ny_n \pmod p\,.$$

Let $f : \mathbb{Z}_p^n \to \mathbb{C}$ be an arbitrary function. Denote by $\widehat{f}$ the Fourier transform of f

$$\widehat{f}(\vec{r}) = \sum_{\vec{x}\in\mathbb{Z}_p^n} f(\vec{x}) e(-(\vec{r}\cdot\vec{x}))\,,$$

where $e(x) = e^{2\pi i\frac{x}{p}}$, $x \in \mathbb{Z}_p$.

Let $\vec{v}_1, \dots, \vec{v}_k$ be linear–independent vectors and let $\varepsilon_1, \dots, \varepsilon_k$ be elements of $\mathbb{Z}_p$. Define the *affine subspace* P (of codimension k) by

$$P = P_{\varepsilon_1,\dots,\varepsilon_k} = \{\vec{x} \in \mathbb{Z}_p^n \ : <\vec{x},\vec{v}_1> = \varepsilon_1, \dots, <\vec{x},\vec{v}_k> = \varepsilon_k\}\,.$$

It is easy to calculate the the Fourier transform of P. Let L be the subspace of dimension k spanned by $\vec{v}_1, \dots, \vec{v}_k$. Suppose that $\vec{r} \in \mathbb{Z}_p^n$ is an arbitrary vector. We have $\vec{r} = \sum_{i=1}^k r_i\vec{v}_i + \vec{v}$, where $\vec{v} \in L^{\perp}$. Then

$$\widehat{P}(\vec{r}) = L(\vec{r})|P| \cdot e(-\sum_{i,j=1}^{k} \varepsilon_i r_j <\vec{v}_i,\vec{v}_j>)\,. \qquad (88)$$

Thus $|\widehat{P}(\vec{r})|$ either equals zero or equals $|P|$.

In this section we consider the case $p = 2$. At the case the Fourier transform of a function f, $f : \mathbb{Z}_2^n \to \mathbb{C}$ is equal to

$$\widehat{f}(\vec{r}) = \sum_{\vec{x} \in \mathbb{Z}_p^n} (-1)^{<\vec{r},\vec{x}>} f(\vec{x}) \,.$$

First of all let us prove an analog of Theorem 2.11 for $\mathbb{Z}_2^n$. It is very convenient to split our results into Theorem 4.1 and Theorem 4.3. Theorem 4.1 is simpler then Theorem 4.3 but we need in rigid condition (89) in our proof.

Theorem 4.1 *Let $\delta, \alpha \in (0,1]$ be real numbers, $\alpha \le \delta/2$, $\delta \le 2^{-5}$, and*

$$\frac{2\delta}{\alpha} \log \frac{1}{2\alpha} \le \log N \,. \qquad (89)$$

Then there exists a set $A \subseteq \mathbb{Z}_2^n$ such that $\delta N \le |A| \le 8\delta N$, $|\mathcal{R}_\alpha(A)| \ge \frac{\delta}{8\alpha^2}$ and for all k, $2 \le k \le 2^{-1}\log(1/8\delta)$, we have $T_k(\mathcal{R}_\alpha(A)) \le \frac{8\delta}{\alpha^{2k}}$.

Proof. Let $\vec{e}_1 = (1,0,\dots,0)$, $\vec{e}_2 = (0,1,0,\dots,0), \dots, \vec{e}_n = (0,\dots,0,1)$ be the standard basis of $\mathbb{Z}_2^n$. Let also $k' = [\log 1/(2\alpha)]$, $t = \lceil \delta/\alpha \rceil$, $n = \log N$. Let $i \in [t]$ and let P_i be a affine subspace such that

$$P_i = \{\vec{x} \in \mathbb{Z}_2^n \ : < \vec{x}, \vec{e}_j >= 0 \,, \quad j = (i-1)k' + 1, \dots, ik'\} \,.$$

Since $tk' \le \frac{2\delta}{\alpha} \log \frac{1}{2\alpha} \le \log N = n$, it follows that all affine subspaces P_i are well defined. Let $A = \bigcup_{i=1}^t P_i$. Clearly, $|A| \le t2^{-k'}N \le 8\delta N$. Let us prove that $|A| \ge \delta N$. We have $|P_i| = N2^{-k'}$, $i \in [t]$. Besides for any $l \in [t]$ and for all *different* subspaces $P_{i_1}, \dots, P_{i_l}$ the following holds

$$|P_{i_1} \cap \dots \cap P_{i_l}| = N2^{-k'l} \,. \qquad (90)$$

Using the inequality $\delta \le 2^{-5}$, we get

$$|A| \ge \sum_{i=1}^t |P_i| - \sum_{i,j=1, i\ne j}^t |P_i \cap P_j| \ge t2^{-k'}N - t^2(2^{-k'})^2 N = t2^{-k'}N\left(1 - \frac{t}{2^{k'}}\right) \ge \delta N \,.$$

Let us prove now that $|\mathcal{R}_\alpha(A)| \ge \frac{\delta}{8\alpha^2}$. Let L_i be a subspace of $\mathbb{Z}_2^n$ of the dimension k' spanned by $\{\vec{e}_j\}_{,\ j=(i-1)k'+1,\dots,ik'}$. Suppose that $\vec{s} \in \mathbb{Z}_2^n$ is an arbitrary vector. Using (88), we obtain

$$\widehat{P}_i(\vec{s}) = |P_i| L_i(\vec{s}) \,. \qquad (91)$$

Whence $\mathcal{R}_\alpha(A) \subseteq \bigcup_{i=1}^t L_i$. Prove that $\bigcup_{i=1}^t L_i \subseteq \mathcal{R}_\alpha(A)$. Obviously, $\vec{0} \in \mathcal{R}_\alpha(A)$. Let $\vec{s}$ be a non–zero vector such that $\vec{s}$ belongs to some L_i. Clearly, for any $i, j \in [t]$, $i \ne j$, we have $L_i \cap L_j = \{\vec{0}\}$. Using this fact and (91), we get

$$\widehat{A}(\vec{s}) = \widehat{P}_i(\vec{s}) - \sum_{j=1}^t (P_i \cap P_j)\widehat{\ }(\vec{s}) + \sum_{j,l=1,\ j\ne l,\ j,l\ne i}^t (P_i \cap P_j \cap P_l)\widehat{\ }(\vec{s}) + \dots \qquad (92)$$

Using (90) and (92), we obtain

$$|\widehat{A}(\vec{s})| \ge 2^{-k'}N - 2^{-k'}N\left(\frac{t}{2^{k'}} + \frac{t^2}{(2^{k'})^2} + \dots\right) \ge 2^{-k'-1}N \ge \alpha N \,. \qquad (93)$$

Hence $\bigcup_{i=1}^t L_i \subseteq \mathcal{R}_\alpha(A)$ and $|\mathcal{R}_\alpha(A)| \ge \sum_{i=1}^t |L_i| - t \ge t2^{k'} - t \ge \frac{\delta}{8\alpha^2}$.

Finally, let us prove that for all $2 \le k \le 2^{-1}\log(1/8\delta)$, we have $T_k(\mathcal{R}_\alpha(A)) \le \frac{8\delta}{\alpha^{2k}}$. Consider the equation

$$r_1 + \cdots + r_k = r'_1 + \cdots + r'_k\,, \tag{94}$$

where all vectors r_j, r'_j belong to $\mathcal{R}_\alpha(A)$. As was noted above $\mathcal{R}_\alpha(A) \subseteq \bigcup_{i=1}^t L_i$. Hence any vector in (94) belongs to some subspace L_{i_j}. Let z be a non–negative integer, and $s_1, \ldots, s_l$ be positive integers such that $s_1 + \cdots + s_l + z = 2k$. By $E(s_1, \ldots, s_l, z)$ denote the set of all solutions $r_1, \ldots, r_k$, $r'_1, \ldots, r'_k$ of (94) such that among r_j, r'_j there exist exactly z of zeroes, there exist exactly s_1 non–zero residuals belong to a subspace L_{j_1}, there exist exactly s_2 non–zero residuals belong to a subspace L_{j_2}, $\ldots$, there exist exactly s_l non–zero residuals belong to a subspace L_{j_l} and at the same time all sets $L_{j_1}, L_{j_2}, \ldots, L_{j_l}$ are different. We have

$$T_k(\mathcal{R}_\alpha(A)) = \sum_{l=1}^{2k}\sum_{z=0}^{2k} \sum_{s_1,\ldots,s_l,\ s_1+\cdots+s_l+z=2k} |E(s_1, \ldots, s_l, z)| =$$

$$= t(2^{k'})^{2k-1} + \sum_{l=2}^{2k}\sum_{z=0}^{2k} \sum_{s_1,\ldots,s_l,\ s_1+\cdots+s_l+z=2k} |E(s_1, \ldots, s_l, z)|\,. \tag{95}$$

Let us fixed $s_1, \ldots, s_l, z$ and consider the solutions of (94) belong to fixed subspaces $L_{j_1}, \ldots, L_{j_l}$. Denote by $E(s_1, \ldots, s_l, z)(L_{j_1}, \ldots, L_{j_l})$ the set of all these solutions. Rewrite (94) as

$$\vec{u}_1 + \cdots + \vec{u}_l = \vec{0}\,, \tag{96}$$

where $\vec{u}_i \in L_{j_i}$, $i \in [l]$. For all $i, h \in [t]$, $i \ne h$, we have $L_{j_i} \cap L_{j_h} = \{\vec{0}\}$. Hence all vectors $\vec{u}_i$ equal $\vec{0}$. It follows that

$$|E(s_1, \ldots, s_l, z)(L_{j_1}, \ldots, L_{j_l})| \le \frac{(2k)!}{s_1!\ldots s_l! z!}(2^{k'})^{s_1-1} \times \ldots \times (2^{k'})^{s_l-1} \le \frac{(2k)!}{s_1!\ldots s_l! z!}(2^{k'})^{2k-l}\,.$$

Whence

$$|E(s_1, \ldots, s_l, z)| \le \binom{t}{l}\frac{(2k)!}{s_1!\ldots s_l! z!}(2^{k'})^{2k-l} \le \frac{t^l}{l!}\cdot\frac{(2k)!}{s_1!\ldots s_l! z!}(2^{k'})^{2k-l}\,. \tag{97}$$

Combining (97) and (95), we get

$$T_k(\mathcal{R}_\alpha(A)) \le t(2^{k'})^{2k-1} + \sum_{l=2}^{2k}\frac{t^l}{l!}(2^{k'})^{2k-l}\sum_{z=0}^{2k} \sum_{s_1,\ldots,s_l,\ s_1+\cdots+s_l+z=2k} \frac{(2k)!}{s_1!\ldots s_l! z!} \le$$

$$\le t(2^{k'})^{2k-1} + \sum_{l=2}^{2k}\frac{t^l}{l!}(2^{k'})^{2k-l}(l+1)^{2k} = t(2^{k'})^{2k-1} + (2^{k'})^{2k}\sum_{l=2}^{2k}\left(\frac{t}{2^{k'}}\right)^l \cdot (l+1)^{2k}\cdot\frac{1}{l!}\,. \tag{98}$$

Consider the function $f(l) = (t/2^{k'})^l(l+1)^{2k}$. It is easy to see that $f(l)$ has maximum at $l_0 = 2k/\ln(2^{k'}/t) - 1$ and for all $l \ge l_0$ the function $f(l)$ is monotonically decreasing. By assumption $k \le 2^{-1}\log(1/8\delta)$. Hence $l_0 \le 1$. It follows that

$$T_k(\mathcal{R}_\alpha(A)) \le t(2^{k'})^{2k-1} + 2^{2k}t(2^{k'})^{2k-1} \le 2^{2k+1}t(2^{k'})^{2k-1} \le 2^{2k+1}\cdot\frac{2\delta}{\alpha}\left(\frac{1}{2\alpha}\right)^{2k-1} = \frac{8\delta}{\alpha^{2k}}\,.$$

This completes the proof.

Note 4.2 In special cases of choosing δ and α we do not need in a bound $k \ll \log(1/\delta)$ of Theorem 4.1. For example, suppose that $\alpha \approx \delta$ and A is a subspace of $\mathbb{Z}_2^n$ of codimension k', $k' \approx \log(1/\delta)$. Then $\mathcal{R}_\alpha(A)$ is a subspace of dimension k' and it has the cardinality $\approx 1/\delta$. It is easy to see that for all $k \geq 2$, we have $T_k(\mathcal{R}_\alpha(A)) = (2^{k'})^{2k-1} \approx 1/\delta^{2k-1}$. This quantity coincides with lower bound (6).

We shall consider the simplest case of $k = 2$ in our next Theorem 4.3, i.e. we shall prove that the lower bound for $T_2(\mathcal{R}_\alpha(A))$ from Theorem 1.3 is best possible.

Theorem 4.3 *Let $\delta, \alpha \in (0,1]$ be real numbers, $32\delta^2 \leq \alpha \leq \delta/2$, $\alpha \geq N^{-2^{-300}}$, $\alpha \leq 2^{-30}$, and $\frac{\delta}{\alpha}\log\frac{1}{2\alpha} \geq 400\log N \cdot \log(8\log N)$. Then there exists a set $A \subseteq \mathbb{Z}_2^n$ such that $\delta N \leq |A| \leq 8\delta N$, $|\mathcal{R}_\alpha(A)| \geq \frac{\delta}{8\alpha^2}$ and $T_2(\mathcal{R}_\alpha(A)) \leq \frac{16\delta}{\alpha^4}$.*

To prove such result we need in a well–known large deviations inequality of Bernstein [25]. The following variant of this inequality can be found in [7].

Theorem 4.4 *Let $X_1, \dots, X_n$ be independent random variables with $\mathbb{E}X_j = 0$ and $\mathbb{E}|X_j|^2 = \sigma_j^2$. Let $\sigma^2 = \sigma_1^2 + \dots + \sigma_n^2$. Suppose that for all $j \in [n]$, we have $|X_j| \leq 1$. Let also t be a real number such that $\sigma^2 \geq 6nt$. Then*

$$\mathbb{P}\left(\left|\frac{X_1 + \dots + X_n}{n}\right| \geq t\right) \leq 4e^{-n^2t^2/8\sigma^2}\,.$$

Using Theorem 4.4, we prove a combinatorial lemma.

Lemma 4.5 *Let n, k, r, t be real numbers, $4 \leq r \leq k/2$, $2k \leq n$, and*

$$kt > 288n\ln(8n) \quad \text{and} \quad t^2 \cdot \frac{2^k\binom{n-k}{k-\lceil k/r\rceil}}{\binom{n}{k}} \leq 1/2\,. \tag{99}$$

Then there exist sets $A_1, \dots, A_t \subseteq [n]$, $|A_i| = k$, $i \in [t]$ such that
1) *For all $i, j \in [t]$, $i \neq j$, we have $|A_i \cap A_j| < k/r$.*
2) *For any $i \in [t]$ there exist at most $2tk^2/n$ sets A_j such that $A_j \cap A_i \neq \emptyset$.*

Proof. Let Ω be a family of all subsets of $[n]$ of the cardinality k, $|\Omega| = \binom{n}{k} = M$. Choose sets $A_1, \dots, A_t \in \Omega$ at random (uniformly and independently).

Let U_{ij}, $i, j \in [t]$, $i \neq j$ be a random event consists in $|A_i \cap A_j| \geq k/r$. Let also $U = \bigcup_{i,j\in[t],i\neq j} U_{ij}$. Let us fix a set A_i. It is easy to see that there are exactly

$$\sigma := \sum_{l=\lceil k/r\rceil}^{k} \binom{k}{l}\binom{n-k}{k-l}$$

sets $A_j \in \Omega$ such that $|A_j \cap A_i| \geq k/r$. Hence the probability of U_{ij} is equal to σ/M. Whence $\mathbb{P}(U) \leq t^2\sigma/M$.

Let $x \in [n]$ and $\xi_j^x(\omega)$, $\omega \in \Omega^t$, $j \in [t]$ be a random variable such that $\xi_j^x(\omega) = 1$ if $x \in \omega_j$ and $\xi_j^x(\omega) = 0$ otherwise. Clearly, $\xi^x(\omega) := \sum_{j=1}^t \xi_j^x(\omega)$ is the number of sets A_j such that $x \in A_j$. Further, for any x and j, we have $\mathbb{E}\xi_j^x = k/n$ and $\mathbb{D}\xi_j^x = k/n - (k/n)^2$. Let $x \in [n]$ and let V_x be the event such that x belongs to at least $7tk/(6n)$ the sets A_j. Let also $V = \bigcup_{x\in[n]} V_x$. Using Theorem 4.4, we get

$$\mathbb{P}(V_x) \leq \mathbb{P}\left(\omega \;:\; \left|\xi^x(\omega) - \frac{tk}{n}\right| > \frac{tk}{6n}\right) \leq 4e^{-kt/(288n)}\,.$$

Whence

$$\mathbb{P}(V) \le \sum_{x\in[n]} \mathbb{P}(V_x) \le 4ne^{-kt/(288n)}\,. \tag{100}$$

By assumption $kt > 288n\ln(8n)$. It follows that $4ne^{-kt/(288n)} < 1/2$. Besides $\sigma \le 2^k\binom{n-k}{k-\lceil k/r\rceil}$. Using condition (99) and inequality (100), we obtain

$$\mathbb{P}(U\cup V) \le \mathbb{P}(U)+\mathbb{P}(V) \le t^2\frac{\sigma}{M}+4ne^{-kt/(288n)} \le t^2\cdot\frac{2^k\binom{n-k}{k-\lceil k/r\rceil}}{\binom{n}{k}}+4ne^{-kt/(288n)} < 1/2+1/2 = 1\,.$$

Hence there exists a collection of sets $A_1,\dots,A_t\subseteq[n]$, $|A_j| = k$ such that 1) holds and such that any element $x\in[n]$ belongs to at most $7tk/(6n) \le 2tk/n$ of these sets. Using the last inequality, we get that for all $i\in[t]$ there are at most $2tk^2/n$ the sets A_j such that $A_i\cap A_j\neq\emptyset$. This concludes the proof.

Proof of Theorem 4.3. Let $\vec{e}_1 = (1,0,\dots,0)$, $\vec{e}_2 = (0,1,0,\dots,0),\dots,\vec{e}_n = (0,\dots,0,1)$ be the standard basis of $\mathbb{Z}_2^n$. Let also $r = 32$, $k = [\log 1/(2\alpha)]$, $t = \lceil\delta/\alpha\rceil$, $n = \log N$. By assumption $\frac{\delta}{\alpha}\log\frac{1}{2\alpha} \ge 400\log N\cdot\log(8\log N)$. Hence $kt > 288n\ln(8n)$. Besides $\alpha \ge N^{-2^{-300}}$. Whence

$$t^2\cdot\frac{2^k\binom{n-k}{k-\lceil k/32\rceil}}{\binom{n}{k}} \le t^2 2^k\frac{k^{k/32+1}}{(n-k)^{k/32}} \le kt^2 2^k\left(\frac{2k}{n}\right)^{k/32} \le 1/2\,.$$

Using Lemma 4.5, we find a collection of sets $A_1,\dots,A_t$ such that 1) and 2) hold.

We shall construct a family of affine subspaces $P_1,\dots,P_t$ of such form

$$P_i = P_i^{\vec{\varepsilon}} = \{\vec{x}\in\mathbb{Z}_2^n \ : <\vec{x},\vec{e}_j>=\varepsilon_i^{(j)}\,,\quad j\in A_i\}\,,$$

where $\vec{\varepsilon}_i = (\varepsilon_i^{(j)})$ be a vector from $\mathbb{Z}_2^k$. Thus to construct affine subspaces P_i, we need to choose vectors $\vec{\varepsilon}_1,\dots,\vec{\varepsilon}_t$. Let $\vec{\varepsilon}_1 = \vec{0}$ and we obtain P_1. Suppose that we have the affine subspaces $P_1,\dots,P_d$. Let us construct a vector $\vec{\varepsilon}_{d+1}$ and a affine subspace P_{d+1}. Let $C_d = \bigcup_{i=1}^d P_i$. Clearly, $|C_d| \le dN2^{-k} \le tN2^{-k} \le 8\delta N$. Let $\vec{\varepsilon}_{d+1}$ be a vector such that

$$|P_{d+1}^{\vec{\varepsilon}_{d+1}}\bigcap C_d| \le 2\delta\cdot 2^{-k}N\,. \tag{101}$$

Since

$$\sum_{\vec{\varepsilon}=(\varepsilon_i^{(j)})\,,\ j\in A_r} |C_d\cap P_{d+1}^{\vec{\varepsilon}}| = |C_d|\,,$$

it follows that such a vector $\vec{\varepsilon}_{d+1}$ exists. So we have the affine subspaces $P_1,\dots,P_t$. Let $A = C_t = \bigcup_{i=1}^t P_i$. Clearly, $|A| \le 8\delta N$. Let us prove that $|A| \ge \delta N$. We have $|P_i| = N2^{-k}$, $i\in[t]$. Using (101), we get

$$|A| = |C_t| = |C_{t-1}| + |P_t| - |C_{t-1}\cap P_t| \ge |C_{t-1}| + N2^{-k} - \frac{8\delta N}{2^k} \ge \tag{102}$$

$$\ge |C_{t-2}| + 2N2^{-k} - 2\frac{8\delta N}{2^k} \ge \dots \ge tN2^{-k} - t\frac{8\delta N}{2^k} = tN2^{-k}(1-8\delta) \ge \delta N\,. \tag{103}$$

Let us prove that $|\mathcal{R}_\alpha(A)| \ge \frac{\delta}{8\alpha^2}$. Let L_i be a subspace of $\mathbb{Z}_2^n$ of the dimension k spanned by $\{\vec{e}_j\}_{j\in A_i}$. Let also

$$M_i = \{\vec{x}\in L_i \ :\ \text{ the number of units in } \vec{x} \text{ at least } k/8\}\,.$$

Clearly, for all $i \in [t]$, we get $|M_i| \geq 2^{k-1}$. Since for any $i, j \in [t]$, $i \neq j$, we have $|A_i \cap A_j| < k/r < k/8$, it follows that for all $i, j \in [t]$, $i \neq j$, we obtain $M_i \cap L_j = \emptyset$. In particular, for any $i, j \in [t]$, $i \neq j$, we get $M_i \cap M_j = \emptyset$. Let $\vec{s} \in \mathbb{Z}_2^n$ be an arbitrary vector. Using (88), we get

$$\widehat{P}_i(\vec{s}) = e(-\sum_{j \in A_i} \varepsilon_i^{(j)} s_j)|P_i| L_i(r)\,. \tag{104}$$

Whence $\mathcal{R}_\alpha(A) \subseteq \bigcup_{i=1}^t L_i$. Prove that $\bigsqcup_{i=1}^t M_i \subseteq \mathcal{R}_\alpha(A)$. Let $i \in [t]$, and $\vec{s} \in M_i$ be a vector. We have

$$\widehat{A}(\vec{s}) = \widehat{P}_t(\vec{s}) + \widehat{C}_{t-1}(\vec{s}) + \theta \frac{8\delta N}{2^k}\,,$$

where $|\theta| \leq 1$. By the same arguments as in (102) — (103), we get

$$\widehat{A}(\vec{s}) = \sum_{l=1}^t \widehat{P}_l(\vec{s}) + \tilde{\theta} t \frac{8\delta N}{2^k}\,, \tag{105}$$

where $|\tilde{\theta}| \leq 1$. For all $i, j \in [t]$, $i \neq j$, we have $M_i \cap L_j = \emptyset$. Hence

$$|\sum_{l=1}^t \widehat{P}_l(\vec{s})| = |\widehat{P}_i(\vec{s})| = N 2^{-k}\,. \tag{106}$$

Using (105), (106) and $\alpha \geq 32\delta^2$, we obtain

$$|\widehat{A}(\vec{s})| \geq N2^{-k} - t\frac{8\delta N}{2^k} = \frac{N}{2^k}(1 - 8\delta t) \geq \alpha N\,.$$

Therefore $\bigsqcup_{i=1}^t M_i \subseteq \mathcal{R}_\alpha(A)$ and $|\mathcal{R}_\alpha(A)| \geq t2^{k-1} \geq \frac{\delta}{8\alpha^2}$.

Finally, we shall show that $T_2(\mathcal{R}_\alpha(A)) \leq \frac{16\delta}{\alpha^4}$. Consider the equation

$$\vec{r}_1 + \vec{r}_2 = \vec{r}_3 + \vec{r}_4\,, \tag{107}$$

where all $\vec{r}_l$, $l = 1, 2, 3, 4$ belong to $\mathcal{R}_\alpha(A)$. As was noted above $\mathcal{R}_\alpha(A) \subseteq \bigcup_{i=1}^t L_i$. It follows that any vector $\vec{r}_l$ belongs to some subspace L_{i_l}. Let $M = \bigsqcup_{i=1}^t M_i$, and $Q = (\bigcup_{i=1}^t) \setminus M$. For any $i \in [t]$, we have

$$|L_i \setminus M_i| = \sum_{l=1}^{[k/8]} \binom{k}{l} \leq \frac{k}{8}\binom{k}{[k/8]}\,. \tag{108}$$

Hence

$$|Q| \leq \sum_{i=1}^t |L_i \setminus M_i| \leq \frac{kt}{8}\binom{k}{[k/8]}\,. \tag{109}$$

Using Stirling's formula, (109) and $\alpha \geq 8\delta^2$, we obtain

$$T_2(Q) \leq |Q|^3 \leq \frac{k^3 t^3}{8^3}\binom{k}{[k/8]}^3 \leq \frac{t}{8}(2^k)^3\,. \tag{110}$$

The last inequality implies that

$$T_2(\mathcal{R}_\alpha(A)) \leq T_2(M \sqcup Q) = \frac{1}{N}\sum_{\vec{r} \in \mathbb{Z}_2^n} |\widehat{M}(r) + \widehat{Q}(r)|^4 \leq \frac{8}{N}\sum_{\vec{r} \in \mathbb{Z}_2^n} |\widehat{M}(r)|^4 + \frac{8}{N}\sum_{\vec{r} \in \mathbb{Z}_2^n} |\widehat{Q}(r)|^4 \leq$$

$$\le 8T_2(M) + 8T_2(Q) \le 8T_2(M) + t(2^k)^3\,. \qquad (111)$$

Thus to obtain an upper bound for $T_2(\mathcal{R}_\alpha(A))$ we need to compute $T_2(M)$.

So let $\vec{r}_l \in M_{i_l}$, $l \in [4]$. For all $i, j \in [t]$, $i \ne j$, we have $|A_i \cap A_j| < k/r$. Since $3k/r = 3k/32 < k/8$, it follows that all set M_{i_l}, $l = 1, 2, 3, 4$ cannot be different. Furthermore we have three cases :

1) $i_1 = i_2 = i_3 = i_4$,

2) $i_1 = i_3$, $i_2 = i_4$ and $i_1 \ne i_2$,

3) $i_1 = i_4$, $i_2 = i_3$ and $i_1 \ne i_2$.

In the first case the number of solutions of (107) does not exceed $t(2^k)^3$. Let us consider the case 2) (or 3)). Let us fixed i_1 and i_2, $i_1 \ne i_2$. Let $\vec{u} = \vec{r}_1 - \vec{r}_3 = \vec{r}_4 - \vec{r}_2$. Clearly, $\vec{u} \in L_{i_1} \cap L_{i_2}$. If $A_{i_1} \cap A_{i_2} = \emptyset$ then $\vec{u} = \vec{0}$ and $\vec{r}_1 = \vec{r}_3$, $\vec{r}_2 = \vec{r}_4$. Hence if $A_{i_1} \cap A_{i_2} = \emptyset$ then (107) has at most $(2^k)^2$ solutions. Suppose that $A_{i_1} \cap A_{i_2} \ne \emptyset$. Since $|A_{i_1} \cap A_{i_2}| < k/r$, it follows that the number of solutions of (107) does not exceed $(2^k)^2 \cdot 2^{k/r}$ in this case. Whence the number of solutions of (107) at most

$$\sum_{i_1=1}^{t} \sum_{i_2=1, i_2 \ne i_1, A_{i_1} \cap A_{i_2} = \emptyset}^{t} (2^k)^2 + \sum_{i_1=1}^{t} \sum_{i_2=1, i_2 \ne i_1, A_{i_1} \cap A_{i_2} \ne \emptyset}^{t} (2^k)^2 \cdot 2^{k/r} := \sigma_1\,.$$

Using property 2) of the collection of the sets $A_1, \dots, A_t$, we obtain that the number of $i_2 \ne i_1$ such that $A_{i_1} \cap A_{i_2} \ne \emptyset$ does not exceed $2tk^2/n$. Hence

$$\sigma_1 \le t^2(2^k)^2 + t\frac{2tk^2}{n}(2^k)^2 \cdot 2^{k/32}\,.$$

Using the last inequality and $\alpha \ge 32\delta^2$, we get $\sigma_1 \le t(2^k)^3 + t(2^k)^3 = 2t(2^k)^3$. Whence the *total* number of solutions of (107) at most

$$T_2(\mathcal{R}_\alpha(A)) \le 8(t(2^k)^3 + 2t(2^k)^3 + 2t(2^k)^3) + t(2^k)^3 = 41t(2^k)^3 \le 41\frac{2\delta}{\alpha}\frac{1}{(2\alpha)^3} \le \frac{16\delta}{\alpha^4}\,.$$

This completes the proof.

As was showed in Theorems 4.1, 4.3 an upper bound of Theorem 1.3 is best possible. It is easy to see that the number of elements λ_i^* in (8) of Theorem 1.4 is also best possible. Indeed, let $\alpha \approx \delta$ and let A be a subset of $\mathbb{Z}_2^n$ such that $|\mathcal{R}_\alpha(A)| \approx \delta/\alpha^2 \approx 1/\delta$. Certainly, such sets exist, for example one can take a subspace of $\mathbb{Z}_2^n$ of the cardinality δN. By Chang's Theorem there exists a set Λ^*, $|\Lambda^*| \ll \log(1/\delta)$ such that for any $\vec{r} \in \mathcal{R}_\alpha(A)$, we have (8). On the other hand since $|\mathcal{R}_\alpha(A)| \approx 1/\delta$, it follows that there exists a vector $\vec{r} \in \mathcal{R}_\alpha(A)$ such that we need in $k \gg \log(1/\delta)$ vectors of Λ^* to involve $\vec{r}$ in some equation (8). Indeed, we have at most $2^k\binom{|\Lambda^*|}{k}$ of linear combinations of k vectors from Λ^*. Hence the following inequality must be hold $2^k\binom{|\Lambda^*|}{k} \gg 1/\delta$. This implies that $k \gg \log(1/\delta)$.

References

[1] *Gowers W. T.* Rough structure and classification // Geom. Funct. Anal., Special Volume - GAFA2000 "Visions in Mathematics", Tel Aviv, (1999) Part I, 79–117.

[2] *Gowers W. T.* A new proof of Szemerédi's theorem // Geom. Funct. Anal. **11** (2001), 465–588.

[3] *Chang M.– C.,* A polynomial bound in Freiman's theorem // Duke Math. J. **113** (2002) no. 3, 399–419.

[4] *Ruzsa I.* Generalized arithmetic progressions and sumsets // Acta Math. Hungar., **65** (1994), 379–388.

[5] *Bilu Y.* Structure of sets with small sumset // Structure Theory of Sets Addition, Astérisque, Soc. Math. France, Montrouge, **258** (1999), 77–108.

[6] *Freiman G. A.* Foundations of a Structural Theory of Set Addition / Kazanskii Gos. Ped. Inst., Kazan, 1966. Translations of Mathimatical Monographs **37**, AMS, Providence, R.I., USA.

[7] *Green B.* Arithmetic Progressions in Sumsets // Geom. Funct. Anal., **12** (2002) no. 3, 584–597.

[8] *Green B.* Some constructions in the inverse spectral theory of cyclic groups // Comb. Prob. Comp. **12** (2003) no. 2, 127–138.

[9] *Green B.* Spectral structure of sets of integers // Fourier analysis and convexity (survey article, Milan 2001), Appl. Numer. Harmon. Anal., Birkhauser Boston, Boston, MA (2004), 83–96.

[10] *Green B.* Structure Theory of Set Addition // ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis, Edinburgh March 25 — April 5 2002.

[11] *Green B.* A Szemerédi–type regularity lemma in abelian groups // Geom. Funct. Anal. **15** (2005) no. 2, 340–376.

[12] *Green B.* Finite field model in additive combinatorics // Surveys in Combinatorics 2005, LMS Lecture Notes **329**, 1–29.

[13] *Schoen T.* Linear equations in $\mathbb{Z}_p$ // London Math. Soc., submitted.

[14] *Ruzsa I.* Arithmetic progressions in sumsets // Acta Arith. **60** (1991) no. 2, 191–202.

[15] *Yudin A. A.* On the measure of large values of a trigonametric sum // Number Theory (under the edition of G.A. Freiman, A.M. Rubinov, E.V. Novosyolov), Kalinin State Univ., Moscow (1973), 163–174.

[16] *Besser A.* Sets of integers with large trigonometric sums // Astérisque **258** (1999), 35–76.

[17] *Lev V. F.* Linear Equations over $\mathbb{F}_p$ and Moments of Exponential Sums // Duke Mathematical Journal **107** (2001), 239–263.

[18] *Konyagin S. V., Lev V. F.* On the distribution of exponential sums // Integers: Electronic Journal of Combinatorial Number Theory **0** # A01, (2000).

[19] *de Leeuw K., Katznelson Y., Kahane J. P.* Sur les coefficients de Fourier des fonctions continues // C. R. Acad. Sci. Paris Sér. A–B **285** (1977) no. 16, A1001–A1003.

[20] *Nazarov F. L.* The Bang solution of coefficient problem // Algebra i Analiz **9** (1997) no. 2, 272–287. English Transl. in St. Petersburg Math. J. **9** (1998) no. 2, 407–419.

[21] *Ball K.* Convex geometry and functional analysis // Handbook of the geometry of Banach spaces, vol. I, North–Holland, Amsterdam (2001), 161–194.

[22] *Rudin W.* Fourier analysis on groups / Wiley 1990 (reprint of the 1962 original).

[23] *Rudin W.* Trigonometric series with gaps // J. Math. Mech. **9** (1960), 203–227.

[24] *Spencer J.* Six Standard Deviations Suffice // Transactions of the American Mathematical Society **289** (1985), 679–706.

[25] *Bernstein S.* Sur une modification de l'inéqualité de Tchebichef // Annal. Sci. Inst. Sav. Ukr. Sect. Math. I (1924).

[26] *Vinogradov I. M.* The method of trigonometric sums in number theory / M.: Nauka, 1971.

[27] *Linnik Y. V.* On Weyl's sums. // Math. Sbornik **12** (1943) I, 28–39.

[28] *Nesterenko Y. V.* On I.M. Vinogradov's mean–value theorem // Trudi of Moscow Math. Soc. **48** (1985), 97–105.

[29] *Bajnok B., Ruzsa I.* The independence number of a subset of an abelian group // Integers: Electronic Journal of Combinatorial Number Theory **3** # A02, 2003.

[30] *Bourgain J.* On triples in arithmetic progression // Geom. Funct. Anal. **9** (1999), 968–984.

[31] *Shkredov I. D.* On sets of large exponential sums // Doklady of Russian Academy of Sciences, 411, N 4, 2006.

[32] *Shkredov I. D.* On sets of large exponential sums // Izvestiya of Russian Academy of Sciences, submitted.