A NEW BOUND FOR $A(A + A)$ FOR LARGE SETS

ALIAKSEI SEMCHANKAU

Abstract. For $p$ being a large prime number, and $A \subseteq \mathbb{F}_p$ we prove the following:

1. $|A(A + A)| < p^{3/4} \log^{3/4} p$.
2. $|A| < p^{3/4} \log^{3/4} p$.
3. $|A(A + A)| < p^{3/4} \log^{3/4} p$. 

Here the constants $1/8$, $1/9$, and $2$ are the best possible. The proof involves wrappers, subsets of the finite abelian group $G$, with which we ‘wrap’ popular values in convolutions $A * B$ for dense sets $A, B \subseteq G$. These objects carry some special structural features, making them capable of addressing both additive-combinatorial and enumerative problems.

1. Introduction

Szemerédi’s Regularity Lemma [19] is a key result in structural Graph Theory, having numerous applications in and outside the scope of Graph Theory. We quote it as in [9].

Let $G = (V, E)$ be a graph and let $A, B$ be disjoint subsets of $V$. Define the density $d(A, B)$ to be the proportion of elements $(x, y) \in A \times B$ such that $xy \in E$. If $\epsilon > 0$, we say that a pair $(A, B)$ is $\epsilon$-uniform if $|d(A', B') - d(A, B)| \leq \epsilon$ whenever $A' \subseteq A$ and $B' \subseteq B$ satisfy $|A'| > \epsilon|A|$ and $|B'| > \epsilon|B|$.

Szemerédi’s Regularity Lemma. Let $\epsilon > 0$. There exists $M = M(\epsilon)$ such that the vertex set $V$ of any graph $G$ can be partitioned into $1/\epsilon < m < M$ sets $V_1, \ldots, V_m$ with sizes differing by at most 1, such that at least $(1 - \epsilon)m^2$ of the pairs $(V_i, V_j)$ are $\epsilon$-uniform.

This has the following structural corollary, history of which is discussed in [9]:

Triangle Removal Lemma. Let $G$ be a graph on $n$ vertices, and suppose that $G$ contains $o(n^3)$ triangles. Then we may remove $o(n^2)$ edges from $G$ so as to leave a graph which is triangle-free.

In particular, this implies the Roth-Varnavides Theorem: if a subset $A \subseteq \{1, 2, \ldots, N\}$ has $o(N^2)$ arithmetic progressions of length 3, then $|A| = o(N)$.

In 2005, Green demonstrated (see Theorem 1.5 in [9] and also the further development of these ideas in [11]), that a similar structural result takes place in finite abelian groups, giving the following. Let $G$ be an abelian group of size $N$:

Theorem (Green, 2005). Let $k \geq 3$ be a fixed integer, and suppose that $A_1, A_2, \ldots, A_k$ are subsets of $G$ such that there are $o(N^{k-1})$ solutions to the equation $a_1 + \ldots + a_k = 0$. Then we may remove $o(N)$ elements from each $A_i$, so as to leave sets $A'_i$ such that there are no solutions to $a'_1 + \ldots + a'_k = 0$ with $a'_i \in A'_i$ for all $i$.

This allowed answering in positive the following question of Bergelson, Host, and Kra:

Question: Suppose that $\alpha, \epsilon > 0$. Is it true, that there is $N_0(\alpha, \epsilon)$ such that if $N > N_0(\alpha, \epsilon)$ and $A \subset \{1, 2, \ldots, N\}$ has size $\alpha N$, then there is some $d \neq 0$ such that $A$ has at least $(\alpha^3 - \epsilon) N$ three-term arithmetic progressions of length $d$?

In this paper we prove the following result, which resembles Triangle Removal Lemma and Green’s Theorem:

Main Lemma. Let $A_1, A_2, \ldots, A_k \subseteq \mathbb{F}_p$ be such that $|A_i| \gg p$ for all $i$. Assume that $(A_1 * A_2 * \ldots * A_k)(a) = o(p^{k-1})$ for some $a \in \mathbb{F}_p$. Then there exist $Y_1, \ldots, Y_k, W_1, \ldots, W_k \subseteq \mathbb{F}_p$, such that:
we call its granularity density (or, more precisely, for density of order at least $1/\varepsilon$, see Proposition 6). A wrapping of $A$ is an $\varepsilon$-d-width of at least $1/\varepsilon$. However, we may approximate our set $A$ with $A^*$, which is a Wiener norm.

Remark: Point (1) implies $|W_1| + |W_2| + \ldots + |W_k| < p + o(p)$, see Proposition 6.4.

Remark: Point (3) implies $|cW_i + e| \cap (dW_j + f)| = (1 + o(1))|W_i||W_j|/p$ for all $i, j$ and $c, d, e, f \in \mathbb{F}_p, cd \neq 0$, see Property 9.

This result allows us to give the precise answers to the following questions, which we briefly mention here, see the history and the discussion in Section 5.

**Question:** Let $A \subset \mathbb{F}_p$ and assume $A(A + A)$ does not cover all nonzero values, how large can $A$ be?

**Question:** What is the largest possible size of $A \subset \mathbb{F}_p$, such that it both sum-free and $A = A^*$?

**Question:** Let $A \subset \mathbb{F}_p$ be of size $\alpha p$, what is the smallest possible size of the set $A + A^*$?

As we have seen, our new structural Main Lemma allows us to obtain optimal (up to an $o(p)$-term) results, and we deduce it with the help of a new conception of wrappers (see Section 5.1), and subsets of an abelian group $G$, approximating level-sets of sumsets $A + B$, and, more generally, level-sets of any function $f$, having a small Wiener norm. A wrapper comes with two parameters: $\varepsilon \in (0, 1)$, which we call its granularity, and positive integer $d$, which we call its dimension. We write $\varepsilon$-d-width for short. Granularity and dimension of wrappers are exploited in Properties 2 and 3 in Section 4 below.

Szemerédi Regularity Lemma and Green’s Theorem proofs rely on an energy increment argument, which gives tower-like dependencies, which makes results only applicable for graphs/sets of positive density (or, more precisely, for density of order at least $1/\log^* |G|$, where $G$ is a graph/group, and $\log^*$ is a number of times one has to logarithmize the argument to obtain a value below 2). However, at the cost of succinctness in the statement, we can prove the following quantitative result (at the further cost of symmetry, one can also obtain Technical Lemma below), which is applicable for sets of density $1/(\log |G|)^c$, $c > 0$. We defer both proofs of Main and Supplementary Lemma to Section 5.

**Supplementary Lemma.** Let $G$ be a finite abelian group, and let $\alpha, \beta \in (0, 1)$. Let $A, B \subset G$, and assume $|A| \geq \alpha |G|, |B| \geq \beta |G|$. Let $\eta_1, \eta_2 \in \mathbb{R}, \delta, \xi \in \mathbb{R}^+$. Let

$$X := \{x : \eta_1 |G| \leq (A * B)(x) \leq \eta_2 |G|\}, \quad X^+ := \{x : (\eta_1 - \delta) |G| < (A * B)(x) < (\eta_2 + \delta) |G|\}.$$ 

Then there exists a wrapper $W$ of granularity $\varepsilon = \varepsilon(\alpha, \beta) \gg \min \left(\frac{\alpha \beta}{\sqrt{\frac{1}{\delta^2}}}, 1\right)$ and dimension $d = d(\alpha, \beta, \xi) \ll \max \left(\frac{\alpha \beta}{\sqrt{\frac{1}{\delta^2}}}, 1\right) \log \left(\frac{1}{\varepsilon}\right)$, and set $Y, |Y| \leq \xi p$, satisfying inclusions $X \setminus Y \subseteq W$ and $W \setminus Y \subseteq X^+$, which we call wrapping.

The rest of the paper is structured as follows.

In Section 8 we introduce the basic notation and recall useful facts on Discrete Fourier Transform.

In Section 4 we provide some further discussion on wrappers.

In Section 5 we state Theorems 5.1, 5.2, 5.3.

In Section 6 we provide some auxiliary results on sumsets.

In Section 7 we apply Main and Supplementary Lemmas to obtain the Theorems from 5.

In Sections 8 we introduce wrappers, which serve to prove Main and Supplementary Lemmas in Section 9.

2. Acknowledgements

This work was supported by the Russian Science Foundation under grant no.19-11-00001, [https://rscf.ru/en/project/19-11-00001/](https://rscf.ru/en/project/19-11-00001/) The author is very grateful to Ilya Shkredov for suggesting the problem on size of $A(A + A)$ as a project, and his constant attention to this work.
3. Notation

Throughout the paper, the standard notation \( \ll, \gg \), and respectively \( O \) and \( \Omega \) is applied to positive quantities in the usual way. That is, \( X \ll Y, Y \gg X, X = O(Y) \) and \( Y = \Omega(X) \) all mean that \( Y \geq cX \), for some absolute constant \( c > 0 \).

\( G \) always means a finite abelian group, and \( p \) always means a large prime number.

For \( A \subseteq G \) denote by \( A \) its characteristic function \( A : G \to \mathbb{C} \). For \( A \subseteq \mathbb{F}_p \) we denote by \( A^* \) the set \( \{1/a \mod p \mid a \neq 0\} \).

Given \( A, B \subseteq G \), define their sumset by \( A + B := \{a + b \mid a \in A, b \in B\} \). Given also \( \epsilon > 0 \), define their partial sumset by \( A + \epsilon B := \{x \in A + B : (A + B)(x) \geq \epsilon |G|\} \). Denote by \( \overline{A} \) the set \( G \setminus A \). We write \( A \neq B \) if \( A \cap B = \emptyset \). Clearly, \( A \neq \overline{A} \) for any \( A \notin \{\emptyset, G\} \).

For given \( G \) we write \( \hat{G} = \{\gamma : G \to \mathbb{S} \mid \gamma \) a homomorphism\( \} \), where \( \mathbb{S} = \{z \in \mathbb{C} : |z| = 1\} \). This \( \hat{G} \) is called a dual group of \( G \). Note that for \( G = \mathbb{Z}_N \) the dual group \( \hat{\mathbb{Z}}_N \) consists of the functions \( \gamma_r(x) := e^{2 \pi i r x/N} \) for \( r \in \mathbb{Z}_N \).

Given functions \( f, g : G \to \mathbb{C} \), define the convolution \( f \ast g : G \to \mathbb{C} \) by \( (f \ast g)(x) := \sum_{a,b:a+b=x} f(a)g(b) \).

We define the Fourier transform \( \hat{f} : \hat{G} \to \mathbb{C} \) by \( \hat{f}(\gamma) := \sum_{x \in G} f(x) \gamma(x) \). We assume the following properties to be well-known:

\[
\sum_{\gamma \in \hat{G}} \frac{1}{|G|} \hat{f}(\gamma) \gamma(x) = \sum_{x \in G} f(x) \gamma(x) = \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \hat{f}(\gamma) \gamma(x), \quad \hat{f} \ast \hat{g} = \hat{f}(\gamma) \hat{g}(\gamma),
\]

which are the Inverse Fourier Transform, Parseval Identity, and Convolution Identity, respectively. Denote by \( ||f||_\omega \) the Wiener norm: \( ||f||_\omega := \frac{1}{|G|} \sum_{\gamma \in \hat{G}} |\hat{f}(\gamma)| \).

4. Discussion on Wrappers

Here are the useful properties of the wrappers to be used in applications. Their proofs are deferred to Section \( \S \).

Property 1. Let \( W \subseteq G \) be an \( \epsilon \)-d-wrapper. Then its complement \( \overline{W} \) is an \( \epsilon \)-d-wrapper, too.

Property 2. Let \( W \subseteq \mathbb{F}_p \) be an \( \epsilon \)-d-wrapper. Then \( |W|_\omega \leq (C \log p/\epsilon)^d \), where \( C > 0 \) is absolute.

Property 3. Let \( W_1, W_2 \subseteq \mathbb{F}_p \) be of Wiener norms \( \omega_1, \omega_2 \), respectively. Then

\[
|W_1 \cap W_2^*| = \frac{|W_1||W_2|}{p} + O(\omega_1 \omega_2 \sqrt{p}).
\]

Let us mention the connection between wrappers and graph containers. Graph Container theorems were independently introduced by Saxton, Thomason (see [16]) and Balogh, Morris and Samotij (see [4]), and had a remarkable impact on extremal combinatorics in recent years.

Let \( \mathcal{H} \) be a 3-uniform hypergraph. Denote by \( V(\mathcal{H}) \) the set of vertices, and by \( E(\mathcal{H}) \) the set of edges. For any \( V' \subset V \) denote by \( \mathcal{H}[V'] \) the subgraph induced by \( V' \). Define by \( d(\mathcal{H}) \) the average vertex degree in \( \mathcal{H} \), and by \( \Delta_2(\mathcal{H}) \) the maximal number of edges two particular vertices might belong to.

Then, Corollary 3.6 [16] gives roughly the following:

3-Uniform Graph Container Theorem. Let \( \mathcal{H} = (V, E) \) be a 3-uniform hypergraph on \( n \) vertices. Let \( \epsilon, \tau \) be sufficiently small positive constants. Suppose that \( \Delta_2(\mathcal{H}) \ll \epsilon \tau d(\mathcal{H}) \). Then there exists a set \( \mathcal{C} \) of subsets in \( V \) such that

1. If \( A \subset V \) is an independent set, then \( A \subset C \) for some \( C \in \mathcal{C} \),
2. \( |E(\mathcal{H}[C])| \leq \epsilon |E(\mathcal{H})| \) for any \( C \in \mathcal{C} \),
3. \( \log |\mathcal{C}| \ll n \tau \log \left(\frac{1}{\epsilon}\right) \log \left(\frac{1}{\tau}\right) \).
The set \( C \) above is referred to as a set of containers, and a set \( C \subset C \) is itself a container.

One can notice from the proof of Supplementary Lemma, that there are just \( O(2^{1/3} p^d) \) wrappers with given parameters \( \epsilon, d \), which makes us able to formulate the result of the following form:

**Container Form of Supplementary Lemma.** Let \( \kappa(p) := p/(\log p)^c \), where \( c > 0 \) is some absolute constant, which we do not state here. Given \( \chi > 0 \), there exists \( F_\chi \subset 2^p \) with \( \log |F_\chi| \ll \kappa(p) \) such that the following holds.

Let \( A, B, C \subset \mathbb{F}_p \), \( |A|, |B|, |C| \geq \chi p \) be such that \( A \neq B + C \). Then there exists \( X_A, X_B, X_C \subset F_\chi \) such that \( A \subset X_A, B \subset X_B, C \subset X_C \) and \( |X_A| + |X_B| + |X_C| \leq p + O(\kappa(p)) \).

Using a similar observation, we find a correct estimate for a number of triples \( A, B, C \subset 2^G \) such that \( A \neq B + C \) in [17]. We are planning to exploit this idea further in a follow-up paper.

5. Results

5.1. **Covering** \( \mathbb{F}_p^* \) by \( A(A + A) \). The first problem we are interested in is to determine a size of the set \( A(A + A) = \{x(y + z), x, y, z \in A\} \) for \( A \subset \mathbb{F}_p^* \). This sort of problems belongs to a range of expanding polynomials and sum-product problems. In the literature, they are usually discussed in the sparse-set regime; for instance, Roche-Newton, Rudnev, and Shkredov [15], Yazici, Murphy, Rudnev, and Shkredov [22] proved that in the regime \( |A| \ll p^{2/3} \) one has \( \min(|A + AA|, |A(A + A)|) \gg |A|^{3/2} \) (see also [18]). This implies, in particular, that as soon as \( |A| \gg p^{2/3} \) both sets \( A(A + A) \) and \( A + AA \) occupy a positive proportion of \( \mathbb{F}_p^* \).

Now we focus on a case when \( A \) already occupies a positive proportion of \( \mathbb{F}_p^* \). Let \( \alpha = |A|/p \), and we suppose \( \alpha \) is bounded below by a positive constant when \( p \) tends to infinity. Bienvenu, Hennecart, and Shkredov [5] proved that in such a regime \( A(A + A) \) contains all but a finite number of elements. That is, when \( A \subset \mathbb{F}_p^*, |A| = \alpha p, 0 < \alpha < 1 \text{ one has } |A(A + A)| > p - 1 - \alpha^{-3}(1-\alpha)^2 + o(1) \). Besides that, they proved that this finite number of elements may be strictly larger than 1, unless \( \alpha \) is large enough. In particular, for any \( k > 0 \) there exists \( A \subset \mathbb{F}_p^*, |A| = (1/8k + o(1))p \), and \( |A(A + A)| \leq p - 1 - k \). In contrary, they demonstrated the following:

**Theorem (Bienvenu-Hennecart-Shkredov, 2019).** Let \( A \subset \mathbb{F}_p \) be such that \( A(A + A) \) does not cover all nonzero residues. Then \( |A| < 0.3051p + o(p) \).

We improve it as following:

**Theorem 5.1.** Let \( A \subset \mathbb{F}_p \) be such that \( A(A + A) \) does not cover all the nonzero residues. Then \( |A| \leq p/8 + o(p) \).

Remark. Consider sets \( P = \{x : 0 < x < p/4\} \) and \( Q = \{x : p/2 < x < p\} \). Set \( A := P \cap Q^* \). Clearly, \( |A| = p/8 + o(p) \). Now observe \( (A + A) \cap A^* = \emptyset \), and therefore \( 1 \not\in A(A + A) \), which implies that threshold \( \alpha = 1/8 \) is indeed optimal.

5.2. On size of a sum-free \( A \) with \( A = A^* \). \( A \subset \mathbb{F}_p \) is called sum-free if \( A \) does not intersect its sumset \( A + A \). From Cauchy-Davenport inequality size of such \( A \) cannot exceed \( (p + 1)/3 \), with equality when \( A \) is (some dilation of) a segment \( \{x : p/3 < x < 2p/3\} \). As a generalization of this fact, it was shown in [3] that the structure of a sum-free set \( A \) with size close to \( p/3 \) looks like a segment of length \( p/3 \); namely, if \( |A| > 0.318p \), then \( A \) belongs to (some dilation of) the segment \( \{|A|, \ldots, p - |A|\} \).

This gives an idea that the structure of a sum-free \( A \) should be ‘arithmetical’ in nature. It was conjectured by Benjamin in [2] that events ‘\( A \) is sum-free’ and ‘\( A = A^* \)’ should be independent in a sense that size of a sum-free \( A \) with \( A = A^* \) does not exceed \( p/9 + o(p) \).

Bound in [2] shows already that size of such \( A \) does not exceed 0.3051p. Furthermore, the following was proved in [2, Theorem 1.1]:
Theorem (Benjamin, 2020). There is an absolute constant $c > 0$ so that if $A \subseteq \mathbb{F}_p$ is sum-free and closed under inverses then $|A| < (0.25 - c)p + o(p)$.

One can deduce from the proof, that the value $c = 1/4000000$ is admissible. We prove the following:

**Theorem 5.2.** If $A \subseteq \mathbb{F}_p$ is sum-free and closed under inverses, then $|A| < p/9 + o(p)$.

**Remark.** Let $P := \{x : p/3 < x < 2p/3\}$ Set $A := P \cap P^*$. Clearly, $|A| = p/9 + o(p)$, $A$ is sum-free, and $A = A^*$. Therefore, inequality $|A| \leq p/9 + o(p)$ is indeed optimal.

5.3. **On size of the set $A + A^*$.** The third problem we are interested in is to study the cardinality of the set $A + A^*$, $A \subseteq \mathbb{F}_p^*$, where $A^*$ means the set of inverted elements of $A$, and $p$ is a large enough prime number.

Let $P := \{x : 0 < x < \alpha p\}, A := P \cap P^*$. Clearly, $|A| = (1 + o(1))\alpha^2 p$ and $|A + A^*| = (1 + o(1))\min(2\alpha p, p)$, which suggests the following:

**Conjecture.** There exists $\epsilon > 0$, such that for any $A \subseteq \mathbb{F}_p^*, |A| \gg p^{1-\epsilon}$

$|A + A^*| > (1 - o(1))\min(2\sqrt{|A|p, p})$.

Best estimates for $A + A^*$ in different regimes of size of $|A| \sim p^k$:

| $\lambda \in [0, \frac{15}{31}]$ | $|A + A^*| \gg |A|^{31/31}$ |
|-------------------|----------------------------------|
| $\lambda \in [\frac{15}{31}, \frac{4}{5}]$ | $|A + A^*| > (1/2 - o(1))|A|^2/\sqrt{p}$ |
| $\lambda \in [\frac{4}{5}, 1]$ | $|A + A^*| > (1 - o(1))\sqrt{p}|A|$ |

Yazici, Murphy, Rudnev, Shkredov (Prop. 14, [22])

Balog, Broughan, Shparlinski (Thm 7, [3])

We prove Conjecture above in case when $A$ is dense.

**Theorem 5.3.** Let $A \subseteq \mathbb{F}_p^*, |A| = \alpha p, \alpha \gg \kappa(p)$, where $\kappa(p) := \frac{\log \log p}{\sqrt{\log p}}$. Let $\delta$ be such that $\alpha^{3/2} \gg \delta \gg \alpha^{1/2} \kappa(p)$. Then $|A + \delta A^*| \geq \min(2\sqrt{|A|p, p}) - O(\sqrt{\delta p})$.

6. **Auxiliary Lemmas**

Recall the Cauchy-Davenport Inequality. See [13], Theorem 2.2 for a proof.

**Proposition 6.1.** Let $A, B$ be subsets of $\mathbb{F}_p$. Then $|A + B| \geq \min(p, |A| + |B| - 1)$.

It has a following generalization, which might be deduced from the result of Pollard (see Equation 3 in [14]) combined with the argument of Tao (see Corollary 1.2 in [20]).

**Proposition 6.2.** Let $A, B$ be subsets of $\mathbb{F}_p$. Let $0 < \epsilon < \min(\alpha^2, \beta^2)$. Then $|A + \epsilon B| \geq \min(p, |A| + |B| - (2 + o(1))\sqrt{\epsilon p})$.

If $A, B, C \subseteq G$ are arbitrary nonempty sets and $A \neq B + C$, then $B \neq A - C$. This has a following generalization:

**Proposition 6.3.** Let $A, B, C \subseteq G$ be nonempty sets, $|A| = \alpha |G|, |C| = \gamma |G|$, and $\delta \in (0, 1)$. Suppose that $A \neq B + \delta C$, then for any $T > 1$ there exists $E$, $|E| \leq |C|/T$, such that $C \setminus E \neq A - \alpha \delta T/\gamma B$.

**Proof.** Let $E := C \cap (A - \eta B), \eta := \alpha \delta T/\gamma$. Clearly, $|E| \eta |G| \leq \# \{(a, b, c) \in A \times B \times C : a = b + c\} \leq |A| \delta |G|$. This implies $|E| \leq |C|/T$, which completes the proof.

**Proposition 6.4.** Let $\eta > 0$ and $X_1, \ldots, X_k \subseteq \mathbb{F}_p$ be such that $|X_i| \gg \eta p$, and $|X_1| + \ldots + |X_k| \geq p + \eta p$. Then $(X_1 * \ldots * X_k)(0) \gg \eta^{2k-3}p^{k-1}$. 

Proof. Let $\beta$ be a smallest density among sets $X_1, \ldots, X_k$ and let $\epsilon := \min(0.1 \beta^2, \eta^2/16k^2)$. Let us set $V_1 := X_1$, and $V_i := V_{i-1} + X_i$ for $i = 2, \ldots, k-1$. By an induction argument, this is clear that $|V_i| \geq |X_1| + \ldots + |X_i| - 3i \sqrt{\epsilon} p \geq \beta p$. Indeed, this holds for $i = 1$, and for larger $i$ we have $|V_i| \geq |V_{i-1}| + |X_i| - (2 + o(1)) \sqrt{\epsilon} p$ by Proposition 6.2. This is clear that
\[(X_1 \ast X_2 \ast \ldots \ast X_k)(0) = (V_1 \ast X_2 \ast \ldots \ast X_k)(0) \geq (\epsilon p)(V_2 \ast \ldots \ast X_k)(0) \geq \ldots \geq (\epsilon p)^{k-2}(V_{k-1} \ast X_k)(0) \geq (\epsilon p)^{k-2}(|V_{k-1}| + |X_k| - p) \geq (\epsilon p)^{k-2}(|X_1| + \ldots + |X_k| - p - 3k \sqrt{\epsilon} p) \geq \epsilon^{k-3/2} p^{k-1},\]
which completes the proof. \hfill \Box

7. Main and Supplementary Lemma Applications

7.1. Proof of Theorem 5.1

Proof. Without loss of generality we assume that $|A| \gg p$ and $1 \notin A(A + A)$, hence $A^* \neq A + A$, and therefore the equation $x + y + z = 0$ has no solutions in $(x, y, z) \in -A^* \times A \times A$. Main Lemma application gives sets $W_i, Y_i$, such that $A^* \setminus Y_i \subseteq W_i, A \setminus Y_i \subseteq W, A \setminus Y_2 \subseteq W_2, A \setminus Y_3 \subseteq W_3$. Denote densities of $W_i$ by $\omega_i$. Then $\omega_1 + \omega_2 + \omega_3 < 1 + o(1)$. From $A \setminus (Y_1^* \cup Y_2) \subseteq W_1 \cap W_2$ we obtain
\[|A| - |Y_1| - |Y_2| \leq |W_1^* \cap W_2| = (\omega_1 \omega_2 + o(1))p,
\]
which gives $(1 - o(1)) \alpha \leq \omega_1 \omega_2 + o(1)$. Similarly, $\alpha \leq \omega_1 \omega_3 + o(1)$, from where
\[\alpha \leq \omega_1 \frac{\omega_2 + \omega_3}{2} + o(1) \leq \frac{1 - \omega_1}{2} + o(1) \leq \frac{1}{8} + o(1).
\]
\hfill \Box

7.2. Proof of Theorem 5.2

Since $A$ is sum-free, the equation $x + y + z = 0$ has no solutions in $(x, y, z) \in -A \times A \times A$. Main Lemma application gives $W_i, Y_i$ such that $A \setminus Y_i \subseteq W_i$ for $i = 1, 2, 3$, and densities $\omega_i$ satisfy $\omega_1 + \omega_2 + \omega_3 < 1 + o(1)$. By pigeonhole principle, some density (say, $\omega_3$) is at most $1/3 + o(1)$. From $A = A^*$ it follows that $A \setminus (Y_3^* \cup Y_3) \subseteq W_3 \cap W_3^*$, which results in $\alpha \leq \omega_3^2 + o(1) \leq 1/9 + o(1)$.

7.3. Proof of Theorem 5.3 (qualitative version). Let $B := \overline{A + A}$ and $\beta := |B|/p$. We need to prove $\beta \leq 1 - 2 \sqrt{\alpha} + o(1)$. Clearly, equation $x + y + z = 0$ has no solutions in $(x, y, z) \in A \times A^* \times -B$. Main Lemma application gives $W_i, Y_i$ such that $A \setminus Y_i \subseteq W_i, A^* \setminus Y_i \subseteq W_i, B \setminus Y_i \subseteq W_i$, and densities $\omega_i$ satisfy $\omega_1 + \omega_2 + \omega_3 < 1 + o(1)$. From $A \setminus (Y_1 \cup Y_2^* \cup Y_3) \subseteq W_1 \cap W_2 \cap W_3$ we obtain $\alpha(1 - o(1)) \leq \omega_1 \omega_2 + o(1)$, which implies $\sqrt{\alpha} + o(1) \leq \sqrt{\omega_1 \omega_2}$. Therefore, $\beta \leq \omega_3 + o(1) \leq 1 - \omega_1 - \omega_2 + o(1) \leq 1 - 2 \sqrt{\omega_1 \omega_2} + o(1) \leq 1 - 2 \sqrt{\alpha} + o(1)$.

7.4. Proof of Theorem 5.3 (quantitative version).

Technical Lemma. Let $X_1, X_2, X_3$ be sets in $\mathbb{F}_p$ of densities $\theta_1, \theta_2, \theta_3$, such that the equation $x + y + z = 0$ has no solutions in $(x, y, z) \in X_1 \times X_2 \times X_3$. Let $T \gg 1$ and $\delta \in (0, 1)$ be some parameters. Assume that for some absolute constant $C > 0$ inequalities $\theta_1, \theta_2, \theta_3, 1/\delta, \delta > (\log p)^{-C}$ hold. Then there exists $\epsilon_1$-$d_1$-wrapper $W_1$, $\epsilon_2$-$d_2$-wrapper $W_2$, sets $E_1, E_2$, such that
\[X_i \setminus E_i \subseteq W_i, \quad |E_i| < |X_i|/T, \quad \log (1/\epsilon_i) \ll \log \log p,
\]
\[d_1 \ll \max\left(\frac{\theta_2 \theta_3}{\delta^2}, 1\right) \log \log p, \quad d_2 \ll \max\left(\frac{\theta_1 \theta_3}{\eta^2}, 1\right) \log \log p,
\]
and $-(W_2 \setminus E_2) \neq (W_1 \setminus E_1) \cup \eta X_3$, where $w_1 := |W_1|/p$, and $\eta = \Theta(w_1 \delta T/\theta_2)$. All the $\ll$ signs assume dependence on $C$.

Proof. Clearly, $-X_1 \neq X_2 + \delta X_3$. Let $\xi := (\log p)^{-10C}$. Clearly, $\xi$ is much lesser than $1/T$. Supplementary Lemma application (with $\delta$ in place of both $\delta, \eta$) gives $\epsilon_1$-$d_1$-wrapper $W_1$ and set $Y_1$ such that
\[X_1 \setminus Y_1 \subseteq W_1, \quad -(W_1 \setminus Y_1) \neq X_2 + 2\delta X_3, \quad |Y_1| \leq \xi p,
\]
Let $|W_1| = w_1 p$. By the Proposition [5.3] there exists $E, |E| \leq |X_2|/2T$, such that $-(X_2 \setminus E) \neq (W_1 \setminus E_1) + \eta X_3$, where $\eta = 4w_1 \delta T/\theta_2$. Another application of Supplementary Lemma gives $\varepsilon_2$-$d_2$-wrapper $W_2$ and set $Y_2$ such that

$$X_2 \setminus (E \cup Y_2) \subseteq W_2, \quad -(W_2 \setminus E_2) \neq (W_1 \setminus E_1) + \eta X_3, \quad |E \cup Y_2| \leq |X_2|/2T + \xi p < |X_2|/T,$$

which completes the proof. \hfill $\square$

**Proof.** Let $B := A + A^*$. Let $\beta := |B|/p$. Suppose that $\beta > 1 - 2\sqrt{\alpha}$, since otherwise there is nothing to prove. Clearly, equation $x + y + z = 0$ has no solutions in $x \in A, y \in A^*, z \in -B$. Therefore, the Technical Lemma is applicable with $X_1 := A, X_2 := A^*, X_3 := -B$. Let $T := c^\delta (\alpha^{3/\delta^2} / \log p)^{\delta}$, where $c > 0$ is sufficiently small. Clearly, inequality $T \gg 1$ is satisfied. We obtain $\varepsilon_1$-$d_1$-wrapper $W_1$, $\varepsilon_2$-$d_2$-wrapper $W_2$, and $E_1, E_2$, such that $A \setminus E_1 \subseteq W_1, \quad A^* \setminus E_2 \subseteq W_2, \quad |E_1| < |A|/T$, $\log (1/\varepsilon_1) \ll \log \log p$ for $i \in \{1, 2\}, and

$$d_1 \ll \max \left(1 - \frac{\alpha}{\delta^2}, 1\right) \log \log p, \quad d_2 \ll \max \left(w_1 \frac{\theta_3}{\eta^2}, 1\right) \log \log p,$$

and $-(W_2 \setminus E_2) \neq (W_1 \setminus E_1) + \eta X_3$, where $\eta = \Theta(w_1 \delta T/\alpha)$, $w_1 := |W_1|/p$. Let us assume first that $w_1 \gg \sqrt{\alpha}$.

To enforce $W_1, W_2$ to have Wiener norms at most $p^{0.001}$, we need $d_1 \ll \log p/\log \log p$ (which is satisfied by $\delta \gg \kappa(p) \sqrt{\alpha}$), and $d_2 \ll \log p/\log \log p$ (which is satisfied by the fact that $\omega_1 \gg \sqrt{\alpha}$ and $T^4 \gg \delta^2 (\log p)^{\delta} \gg \delta^2 \gg \log \kappa(p)$).

Since Wiener norms are small, $A \setminus (E_1 \cup E_2^*) \subseteq W_1 \cap W_2^*$ implies the inequality $\alpha(1 - 2/T) \leq w_1 w_2 (1 + O(p^{-c}))$.

To make Proposition [6.2] applicable to $(W_1 \setminus E_1) + \eta B$, we want to enforce $\eta \ll \min(w_1^2, \beta^2)$. This is satisfied by the fact $T^2 \ll \alpha^3/\delta^2$. Thus,

$$|W_2 \setminus E_2| < p - |(W_1 \setminus E_1) + \eta B| < p - |W_1 \setminus E_1| - |B| + 2\sqrt{\eta}p,$$

from where $\beta + w_1 + w_2 < 1 + O(\sqrt{\eta}) + O(\alpha/T)$. We can assume that both $O(\sqrt{\eta})$ and $O(\alpha/T)$ are sufficiently smaller than $w_1$, and so $w_1 + w_2 \ll 1 - \beta \ll \sqrt{\alpha}$ by the assumption made in the beginning.

Therefore from now on we can assume $w_1 \ll \sqrt{\alpha}$, and $\eta \ll \omega_1 \delta T/\alpha \ll \delta T/\sqrt{\alpha}$.

Writing same inequality again, we obtain

$$\beta < 1 - w_1 - w_2 + O(\sqrt{\eta}) + O(\alpha/T) < 1 - w_1 - w_2 + O(\sqrt{\delta T/\sqrt{\alpha}}) + O(\alpha/T) < 1 - 2\sqrt{\omega_1 \omega_2} + O(\sqrt{\delta T/\sqrt{\alpha}}) + O(\alpha/T) < 1 - 2\sqrt{\alpha} + O(\sqrt{\alpha/T}) + O(\sqrt{\delta T/\sqrt{\alpha}}).$$

The choice $T = c^\delta (\alpha^{3/\delta^2})$ gives error-term $O(\delta^{1/3})$, as declared.

Now let us comment on why we could have assumed $w_1 \gg \sqrt{\alpha}$. One can apply Technical Lemma with $X_1 := A, X_2 := A^*, X_3 := B$ to obtain $\varepsilon_1$-$d_1$-wrapper $W_1$ to wrap $A$, or with $X_1 := A^*, X_2 := A, X_3 := B$ to obtain $\varepsilon_1$-$d_1$-wrapper $W_1^*$ to wrap $A^*$. Let us denote their densities by $w_1, w_1^*$, respectively. Then, since $d_1, d_1^* \ll \alpha/\delta^2 \ll \log p/\log p^2$, Wiener norms of $W_1, W_1^*$ can be considered polynomially small, and therefore $A \setminus (E_1 \cup E_1^*) \subseteq W_1 \cap W_1^*$ implies $\alpha \ll w_1 w_1^*$. We assume without loss of generality that $w_1 \gg \sqrt{\alpha}$, which completes the proof. \hfill $\square$

8. Wrappers

8.1. Definition and main result on wrappers. Let $\varepsilon \in (0, 1/2)$ be such that $K := 1/\varepsilon$ is a positive integer, and let $\gamma_1, \ldots, \gamma_d : G \to S$ be some homomorphisms (not necessarily different). Split circle $S$ into $K$ equal arcs: $S_1, \ldots, S_K$. 

Definition 8.1. An $\epsilon$-$d$-block is a set of the form
\[ \left\{ g \in G : \gamma_1(g) \in S_{i_1}, \ldots, \gamma_d(g) \in S_{i_d} \right\} \]
for some $1 \leq i_1, \ldots, i_d \leq K$.

Definition 8.2. Assume a set of $d$ homomorphisms $\gamma_1, \ldots, \gamma_d$ to be fixed. We define $\epsilon$-$d$-wrapper to be a union of some $\epsilon$-$d$-blocks.

Clearly, distinct $\epsilon$-$d$-blocks are disjoint and their union constitutes the whole $G$. This proves, that complement of a wrapper is a wrapper, too.

The following statement is the main result on wrappers, with which one can ‘approximate’ level-sets of functions by $\epsilon$-$d$-blocks with a certain precision.

Wrapper Theorem. Let $f : G \to \mathbb{C}$ be a function with Wiener norm $\omega$. Let $\xi \in (0, 1/100)$ be some parameter. Let $\delta \leq \omega$ be some positive real number. Then there exist $\epsilon \in (0, 1/2)$, positive integer $d$, and a decomposition
\[ f = g + h + k, \]
such that:
- $\|h\|_{\infty} \leq \delta/10$.
- $|\text{supp} k| \leq \xi |G|$.
- There is a disjoint union of $G = \cup B_i$ into $\epsilon$-$d$-blocks, such that $g$ is constant on each block $B_i$.
- $\epsilon \gg \delta/\omega$, $d \ll \frac{\omega^2}{\xi} \log \frac{1}{\xi}$.

Proof. This is a Corollary 3.6 from [7].

Croot-Laba-Sisask Lemma. Let $G$ be a finite abelian group and let $\epsilon \in (0, 1)$ and $q > 2$ be parameters. For any nonzero function $f : G \to \mathbb{C}$ of Wiener norm $\omega$ there are characters $\gamma_1, \gamma_2, \ldots, \gamma_d \in \hat{G}$ with $d \leq Cq/\epsilon^2$ and coefficients $c_1, \ldots, c_d \in \mathbb{C}$ with $|c_j| \leq 1$ such that
\[ \|f/\omega - \frac{1}{d}(c_1 \gamma_1 + \ldots + c_d \gamma_d)\|_{L^q} \leq \epsilon. \]

As usual, $L_q$-norm of function $f : G \to \mathbb{C}$ is defined by $\|f\|_{L_q} := \left(\frac{1}{|G|} \sum_x |f(x)|^q\right)^{1/q}$.

Apply Croot-Laba-Sisask Lemma with the parameters $f := f$, $\epsilon := \frac{\epsilon^2}{d}$ for sufficiently small $c > 0$ (say, $\sim 1/1000$), such that $1/\epsilon$ is an integer, and $q := \log \frac{1}{\xi}$. Clearly, conditions $\epsilon \in (0, 1)$ and $q > 2$ required by Croot-Laba-Sisask Lemma are satisfied.

This gives a function $g(x) := \frac{1}{d}(c_1 \gamma_1(x) + \ldots + c_d \gamma_d(x))$ with $|c_j| \leq 1$ and $\gamma_1, \ldots, \gamma_d$ being some elements in $\hat{G}$, such that $\|f/\omega - g\|_{L^q} \leq \epsilon$, and $d \leq Cq/\epsilon^2 \ll \frac{\epsilon^2}{\xi^2} \log \frac{1}{\xi}$. We now adapt $g$ to satisfy the conditions in Theorem’s statement.

Consider any $\epsilon$-$d$-block $B$ with respect to homomorphisms $\gamma_1, \ldots, \gamma_d$. It is rather trivial to check that $g$ varies by at most $O(\epsilon)$ on $B$. Indeed, if $x, y$ belong to the same block, we have
\[ |g(x) - g(y)| = \frac{1}{d} \sum_{i=1}^{d} c_i (\gamma_i(x) - \gamma_i(y)) \leq \frac{1}{d} \sum_{i=1}^{d} |c_i| \frac{2\pi}{K} \leq \frac{1}{d} \frac{2\pi d}{K} = 2\pi, \]
where $K := 1/\epsilon$. Let us now update values of $g$ by at most $2\pi\epsilon$, such that $g$ is now a constant on each block, and this constant belongs to $\epsilon\mathbb{Z}$. Clearly, now $\|f/\omega - g\|_{L^q} \leq (2\pi + 1)\epsilon < 10\epsilon$.

Define $h$ as $h := \omega(f/\omega - g)$. Let $Y$ be a set of those elements $y$ which do not satisfy $h(y) \leq 100\omega$. Since $\|h\|_{L^q} \leq 10\omega\epsilon$ we see that $|Y|(100\omega^2)^q \leq \sum_y h(y)^q \leq |G|(10\omega^2)^q$, which gives $|Y| \leq |G|/10^q < |G|/\epsilon^q = \xi |G|$.
Let $k$ be a functions equal $h$ on $Y$ and identically zero elsewhere. We update $h$ such that equality $f = \omega g + h + k$ still holds; clearly, $\|h\|_{\infty} \leq 100\omega \epsilon \leq \delta/10$ and $|\text{supp } k| = |Y| \leq \xi|G|$.

\[ \square \]

Remark. Note that this result is essentially equivalent to the Croot-Laba-Sisask Lemma.

Remark. If instead of applying Croot-Laba-Sisask Lemma we have directly considered the decomposition $f = \sum \gamma \hat{f}(\gamma) \gamma$, we then would still have a meaningful result, but with bound $d \ll \frac{\omega^2}{\sigma^2} \log \frac{1}{\xi}$.

### 8.2. Wrapping level-sets of functions.

**Corollary 1.** Let $f : G \to \mathbb{R}$ be a function of Wiener norm $\omega$. Let $\eta_1, \eta_2$ be arbitrary reals, and let $0 < \xi < 1/100$ and $\delta > 0$ be parameters. Then there exists $\epsilon$-$d$-wrapper $W$ and set $Y$ such that $|Y| \leq \xi|G|$, and all $x \notin Y$ satisfy the following:

1. If $l_1 \leq f(x) \leq l_2$, then $x \in W$,
2. If $f(x) \leq l_1 - \delta$ or $f(x) \geq l_2 - \delta$, then $x \notin W$.

Moreover, $\epsilon \gg \min\left(\frac{\delta}{\omega}, 1\right)$, $d \ll \max\left(\frac{\omega^2}{\sigma^2}, 1\right) \log \frac{1}{\xi}$.

**Proof.** If $\delta > \omega$, we replace it with $\delta := \omega$, since it does not affect the statement.

Application of the Wrapper Theorem with the parameters $f := f$, $\delta := \delta$ gives a decomposition $f = g + h + k$. Setting $Y := \text{supp } k$, one obtains $|Y| \leq \xi|G|$ . Now consider a set

\[ W := \{ x : l_1 - 0.5\delta \leq g(x) \leq l_2 + 0.5\delta \}. \]

Since $g$ is constant on each $\epsilon$-$d$-block, if one element of the block is in $W$, then the whole block is there. Thus it is clear that $W$ is a union of $\epsilon$-$d$-blocks, and therefore is an $\epsilon$-$d$-wrapper.

Let us demonstrate $W$ satisfies its declared properties.

Let us take some $x$ outside of the set $Y$. Clearly, $f(x) = g(x) + h(x)$ in this case, and therefore $|f(x) - g(x)| \leq 0.1\delta$.

If $x$ is such that $l_1 \leq f(x) \leq l_2$, then $l_1 - 0.1\delta \leq g(x) \leq l_2 + 0.1\delta$, and thus $x \in W$.

If $x$ is such that $f(x) \geq l_2 + \delta$, then $g(x) \geq l_2 + 0.9\delta$, and thus $x \notin W$. Same for $f(x) \leq l_1 - \delta$.

\[ \square \]

### 8.3. Properties.

Recall some facts on Wiener norm of sets and functions.

**Proposition 8.3.** Let $P$ be an arithmetic progression in $\mathbb{F}_p$. Then $\|P\|_{\omega} \ll \log p$.

**Proposition 8.4.** Let $X, Y$ be 2 subsets of $G$. Then $\|X \cap Y\|_{\omega} \leq \|X\|_{\omega} \|Y\|_{\omega}$.

**Proof.** It is easy to see that for any $\xi \in \hat{G}$ equality $\hat{X} \hat{Y}(\xi) = \frac{1}{|G|} \sum_{\eta \in \hat{G}} \hat{X}(\xi - \eta) \hat{Y}(\eta)$ takes place, from where it is easy to imply the Proposition’s statement.

\[ \square \]

**Definition 8.5.** For $X$ an arbitrary arc on $S$, and $\psi : G \to S$ an arbitrary homomorphism (possibly trivial) we set $\psi^{-1}(X)$ to be those elements $g \in G$, such that $\psi(g) \in X$. Denote

\[ w(G) := \max_{\psi \text{-homomorphism, } X \text{-arbitrary arc}} \|\psi^{-1}(X)\|_{\omega}. \]

Note that $w(Z_N) \ll \log N$, $w(Z^d_N) \ll p$. In general, $w(G) \ll \exp(\log^{1/2+o(1)} |G|)$.

The preimage of $S_i$ under any homomorphism has Wiener norm at most $w(G)$, and any $\epsilon$-$d$-block is an intersection of $d$ preimages. This implies Property 2.

**Proposition 8.6.** Let $B$ be an $\epsilon$-$d$-block in abelian group $G$. Then $\|B\|_{\omega} \leq \omega(G)^d$. 

To prove it, we just exploit Proposition 8.4.

**Proposition 8.7.** Let $W$ be an $\epsilon$-$d$-wrapper in abelian group $G$. Then $\|W\|_\omega \leq (\omega(G)/\epsilon)^d$.

To prove it, we just exploit the triangle inequality:

$$\|W\|_\omega \leq \sum_{B \subseteq W} \|B\|_\omega \leq \# \{ B \subseteq W, B \text{ is an } \epsilon$-d-block \} \omega(G)^d \leq (1/\epsilon)^d \omega(G)^d.$$ 

Thus, the Wiener norm of a wrapper is also bounded in terms of $\epsilon$, $d$, and $\omega(G)$.

Recall Weil’s bound for Kloosterman sum [21]. For any $a, b \neq 0$, $\left| \sum_{\gamma \neq 0} e_p(a\gamma + bz) \right| \leq 2\sqrt{p}$. Using Weil bound, we derive the following:

**Proposition 8.8.** Let $X \subseteq \mathbb{F}_p^*$. Then inequality $\max_{\xi \neq 0} |\hat{X}^*(\xi)| \leq 2\sqrt{p} \|X\|_\omega$ holds.

**Proof.**

$$\hat{X}^*(\xi) = \sum_{x} X^*(x) e_p(-\xi x) = \sum_{x} X(x) e_p(-\xi x^*) = \frac{1}{p} \sum_{x} \left( \sum_{\eta} \hat{X}(\eta) e_p(\eta x) \right) e_p(-\xi x^*) = \frac{1}{p} \sum_{\eta} \hat{X}(h) \sum_{x} e_p(\eta x - \xi x^*),$$

which obviously does not exceed $2\sqrt{p} \|X\|_\omega.$ \hfill \qed

Now we prove Property 3.

**Proof.** By Fourier Transform properties,

$$|W_1 \cap W_2^*| = \sum_{x} W_1(x)W_2^*(x) = \frac{1}{p} \sum_{h} \hat{W}_1(h)\hat{W}_2^*(h) = \frac{|W_1||W_2|}{p} + \frac{1}{p} \sum_{h \neq 0} \hat{W}_1(h)\hat{W}_2^*(h).$$

Therefore,

$$\left| \frac{|W_1||W_2|}{p} - \frac{1}{p} \max_{h \neq 0} |\hat{W}_2^*(h)| \sum_{h \neq 0} |\hat{W}_1(h)| \right| \leq 2\sqrt{p} \omega_2 \omega_1. \hfill \qed$$

9. PROOF OF MAIN AND SUPPLEMENTARY LEMMAS

9.1. Proof of the Supplementary Lemma.

**Proof.** Let $A, B \subseteq G$, $|G| = N$, $|A| = \alpha' N$, $|B| = \beta' N$, $\alpha' \geq \alpha$, $\beta' \geq \beta$. Since

$$\|A \ast B\|_\omega \leq \frac{1}{p} \sum_{\gamma \in \mathbb{F}_p} |\hat{A}(\gamma)||\hat{B}(\gamma)| \leq \frac{1}{p} \left( \sum_{\gamma \in G} |\hat{A}(\gamma)|^2 \right) \left( \sum_{\gamma \in G} |\hat{B}(\gamma)|^2 \right) = |A||B|,$$

we obtain the inequality $\|A \ast B\|_\omega \leq \sqrt{\alpha' \beta' N}$. Applying Corollary 1 with $f = A \ast B$, $l_1 := \eta_1|G|$, $l_2 := \eta_2|G|$, and $\delta := \delta N$, we obtain the Supplementary Lemma. \hfill \qed

9.2. Proof of the Main Lemma. We can deduce the proof in a way similar to the one in the proof of Technical Lemma. However, this would involve tedious calculations, and we proceed with a cleaner one.

**Proof.** Without loss of generality, we assume that $(A_1 \ast \ldots \ast A_k)(0) = o(p^{k-1})$. 

Let us fix some positive integer $d$ and rearrange frequencies $\gamma_i$ such that $|\hat{A}_1(0)| > |\hat{A}_1(\gamma_i)| \geq |\hat{A}_1(\gamma_2)| \geq \ldots$. Clearly, since $\sum_{i} |\hat{A}_1(\gamma_i)|^2 = p|A| < p^2$, one has $|\hat{A}(\gamma_d)| < p/\sqrt{d}$ for any $d$. Now write
\[
\#(a_1, \ldots, a_k) \in A_1 \times \ldots \times A_k : a_1 + \ldots + a_k = 0 = \frac{1}{p} \sum_{i=1}^{d} \hat{A}_1(\gamma_i) \ldots \hat{A}_k(\gamma_i) + \frac{1}{p} \sum_{i>d} \hat{A}_1(\gamma_i) \ldots \hat{A}_k(\gamma_i).
\]
We estimate the second term as $\frac{1}{p} \max_{i>d} |\hat{A}_1(\gamma_i)| \sum_{i} |\hat{A}_2(\gamma_i)| \ldots |\hat{A}_k(\gamma_i)| \leq \frac{1}{p} p^{k-1} = p^{k-1}/\sqrt{d}$. Let us now introduce the parameter $\epsilon > 0$ such that $K := 1/\epsilon$ is a positive integer, and let split the unit circle $\{ z : |z| = 1 \}$ into $K$ equal arcs $S_1, S_2, \ldots, S_K$ such that $S_1$ is symmetric around $z = 1$. Let us introduce the Bohr set:
\[
\mathcal{B} := \{ x : \gamma_i(x) \in S_1, 1 \leq i \leq d \}.
\]
Clearly, for any $\gamma_i, 1 \leq i \leq d$, $\mathcal{B}(\gamma_i)/|\mathcal{B}| = 1 + O(\epsilon)$ holds.

Let $|\mathcal{B}| = \theta p$. It is well-known, that Bohr set satisfies the inequality $\theta \geq \epsilon^d p$.

Now we introduce functions $f_1, \ldots, f_k : \mathbb{F}_p \to \mathbb{C}$ defined by
\[
f_i(x) := \frac{(A_i * \mathcal{B})(x)}{|\mathcal{B}|} \text{ for } 1 \leq i \leq k.
\]
These functions are ‘smoothed’ versions of sets $A_1, \ldots, A_k$:
\[
(f_1 * \ldots * f_k)(0) = \frac{1}{p} \sum_{i} \hat{A}_1(\gamma_i) \ldots \hat{A}_k(\gamma_i) \overline{\mathcal{B}(\gamma_i)^k}/|\mathcal{B}|^k = \frac{1}{p} \sum_{i=1}^{d} \hat{A}_1(\gamma_i) \ldots \hat{A}_k(\gamma_i) + O(p^{k-1}/\sqrt{d}) + O(\epsilon p^{k-1}).
\]
To make both error terms equally small, we set $\epsilon \sim 1/\sqrt{d}$, so $(f_1 * f_2 * \ldots * f_k)(0) \ll \epsilon p^{k-1}$.

Let us work with level-sets of functions $f_i$. Take some particular $f_i$. Clearly, Wiener norm of the function $|\mathcal{B}| f_i = A_i * \mathcal{B}$ is at most $\sqrt{\epsilon} \theta p$. Let us choose some sufficiently small parameters $\chi_i, \xi_i$. We apply Corollary 1 with $\gamma := \delta := \chi_i \alpha_i \theta p$, which gives an $\epsilon_i \delta_i$-wrapper $W_i'$ and set $Y_i'$, such that all $x$ outside $Y_i'$ satisfy the following:

1. if $f_i(x) > 2\chi_i \alpha_i$, then $x \in W_i'$,
2. if $f_i(x) < \chi_i \alpha_i$, then $x \notin W_i'$.

Moreover, $\epsilon_i \gg \chi_i \sqrt{\alpha_i} \theta \delta_i \ll \chi_i \alpha_i \frac{1}{\alpha_i}, \quad |Y_i'| \ll \xi p$.

Point (2) implies an inequality $W_i'(x) \leq \frac{1}{\chi_i \alpha_i} f_i(x) + Y_i'(x) \quad \forall x \in \mathbb{F}_p$. Therefore,
\[
(W_i' * \ldots * W_k')(0) = \sum_{x_1+\ldots+x_k=0} W_i'(x_1) \ldots W_k'(x_k) \leq \sum_{x_1+\ldots+x_k=0} \prod_{i} \left( \frac{1}{\chi_i \alpha_i} f_i(x) + Y_i'(x) \right) \leq \frac{(f_1 * \ldots * f_k)(0)}{\chi_1 \ldots \chi_k \alpha_1 \ldots \alpha_k} + O(\ldots) \ll \frac{\epsilon \chi_1 \ldots \chi_k \alpha_1 \ldots \alpha_k}{\alpha_1} p^{k-1}.
\]

We suppressed the second error term, since it is negligibly small due to choice of parameters $\xi_i$.

To make this quantity equal $O(p^{k-1})$, we need $d$ to dominate the value of $1/\chi_1 \ldots \chi_k \alpha_1 \ldots \alpha_k$. To make Wiener norms of sets $W_i'$ to be at most $p^{0.001}$, we need inequalities $d_i \log 1/\epsilon_i \ll \log p$, or $(\chi_i)^{-2} \alpha_i^{-1} \theta^{-1} \log \xi_i^{-1} \ll \log p/\log \log p$. Since $\theta \gg \epsilon^d$, this would follow from $d \ll \log p/\log \log p$ and $\xi_i \gg 1/(\log p)^{100}$.

Now let us construct particular $W_i, Y_i$, required by the Lemma’s statement. There exists $b_i \in \mathcal{B}$, such that $f(a + b_i) \geq 2\chi_i \alpha_i$ for all but $2\chi_i |A_i|$ elements $a$ of $A_i$. Indeed,}
\[
|\mathcal{B}| \min_{b \in \mathcal{B}} \#\{ a \in A : f(a + b) < 2\chi_i \alpha_i \} \leq \sum_{b \in \mathcal{B}} \#\{ a \in A : f(a + b) < 2\chi_i \alpha_i \} = \sum_{x : f(x) < 2\chi_i \alpha_i} (A * \mathcal{B})(x) < p \cdot 2\chi_i \alpha_i |\mathcal{B}| = 2\chi_i |A| |\mathcal{B}|
\]

Let us denote this particular $b$ as $b_i$, and denote by $Y_i''$ those $a \in A$ which do not satisfy $f(a + b_i) \geq 2\chi_i \alpha_i$. Clearly, if $a \in A$ is not in $Y_i'$ and not in $Y_i'' - b_i$, then $f(a + b_i) > 2\chi_i \alpha_i$, and point (1) implies
If the Croot-Laba-Sisask result is applied towards the sums a + b ∈ W_i, or a ∈ W_i - b, Setting Y_i := E'_i \cup (E''_i - b_i) and W_i := W'_i - b_i gives the sets, required by the Main Lemma statement.

Point (1) of the Lemma statement is satisfied by the (W_1 \ast \ldots \ast W_k)(b_1 + \ldots + b_k) = o(p^{k-1}).

Point (2) is satisfied by |Y_i| ≪ |A| + xp = o(p).

Point (3) is satisfied by the fact that W_i has bounded dimension and granularity, which makes the argument of the Property 4 applicable. This completes the proof.

Remark. Inequalities, showing up in the course of the proof, show that one can make the statement lemma quantitative with densities of α_i being some small degrees of 1/log log p.

If the Croot-Laba-Sisask result is applied towards the sumset A_i \ast B, one can improve a small degree of 1/log log p to some small degree of 1/log p. However, ‘asymmetric’ results such as the Technical Lemma above appear to give better estimates in particular applications and, therefore, we do not prove a better quantitative symmetric result here.

References

[1] N. Alon, A. Granville, A. Ubis, “The number of sumsets in a finite field”, Bulletin of The London Mathematical Society - BULL LOND MATH SOC 42 (2010) http://www.cs.tau.ac.il/~nogaa/PDFS/sumfp7.pdf

[2] K. Benjamini, “Sum-free sets which are closed under multiplicative inverses”, arXiv: 2009.04322 https://arxiv.org/abs/2009.04322

[3] A. Balogh, K. A. Broughan, I. E. Shparlinski, “Sum-products estimates with several sets and applications”, Integers: electronic journal of combinatorial number theory 12:A27 (2012): 1–10 https://www.math.waikato.ac.nz/~kab/papers/MultiplSumProd7.pdf

[4] J. Balogh, R. Morris and W. Samotij, “The method of hypergraph containers”, Proceedings of the International Congress of Mathematicians—Rio de Janeiro 2018. Vol. IV. Invited lectures 3059-3092 (2018)

[5] P-Y. Bienvenu, F. Hennecart, I. Shkredov, “A note on the set A ∪ A^′″”, Combinatorics, Probability and Computing 22:3 (2013): 351–365 https://arxiv.org/abs/1103.6000

[6] J. M. Deshoulles, V. F. Lev, “A refined bound for sum-free sets in groups of prime order”, Bulletin of the London Mathematical Society 40:5 (2008): 863–875 https://arxiv.org/abs/0705.4536

[7] B. Green, “A Szemerédi-type regularity lemma in abelian groups”. Geometric and Functional Analysis. 15. 340-376 (2005). 10.1007/s00039-005-0509-8

[8] B. Green, I. Ružsa, “Counting sumsets and sum-free sets modulo a prime”, Studia Scientiarum Mathematicarum Hungarica 41 (2004): 285-293 https://arxiv.org/pdf/math/0307142.pdf

[9] B. Green, T. Tao, “An Arithmetic Regularity Lemma, An Associated Counting Lemma, and Applications”. An Irregular Mind. Bolyai Society Mathematical Studies, vol 21. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-14444-8_7

[10] V. F. Lev, “Distribution of points on arcs.”, Integers 5:2 (2005) https://www.emis.de/journals/INTEGERS/papers/allint2003/allint2003.pdf

[11] M. B. Nathanson, “Additive Number Theory: Inverse Problems and the Geometry of Sumsets” (1996).

[12] J. M. Pollard, “A Generalisation of the Theorem of Cauchy and Davenport”, Journal of the London Mathematical Society 2:2-3 (1974): 460-462 https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/jlms/s2-8.3.460

[13] O. Roche-Newton, M. Rudnev, I. D. Shkredov, “New sum-product type estimates over finite fields”, Advances in Mathematics 303 (2017): 589 - 605 https://arxiv.org/abs/1408.0542

[14] D. Saxton and A. Thomason, “Hypergraph containers”, Invent. Math. 201 (2015), no. 3, 925-992.

[15] A. Semchankau, D. Shabanov, I. Shkredov, “Number of A + B \neq C solutions in abelian groups and application to counting independent sets in hypergraphs”, arXiv: 2012.13433 https://arxiv.org/abs/2012.13433

[16] S. Stevens, F. Zeeuw, “An improved point-line incidence bound over arbitrary fields”, Bulletin of the London Mathematical Society 49 (2017) https://arxiv.org/abs/1609.06284

[17] E. Szemerédi, “Regular partitions of graphs, Probèmes combinatoires et th’eorie des graphes” (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976), pp. 399–401. Colloq. Internat. CNRS, 260, CNRS, Paris, 1978.

[18] T. Tao, “An inverse theorem for an inequality of Kneser”, Proceedings of the Steklov Institute of Mathematics 303 (2018): 193-219 https://arxiv.org/abs/1711.04337

[19] A. Weil, “On Some Exponential Sums”, Proceedings of the National Academy of Sciences 34:5 (1948): 204–207 https://www.pnas.org/content/34/5/204
[22] E. A. Yazici, B. Murphy, M. Rudnev, I. Shkredov, “Growth Estimates in Positive Characteristic via Collisions”, International Mathematics Research Notices 2017:23 (2016): 7148-7189 https://arxiv.org/abs/1512.06613

A. S. Semchankau,
Steklov Mathematical Institute of Russian Academy of Sciences,
8 Gubkina St., Moscow 119991, Russia
aliaksei.semchankau@gmail.com