An application of the sum-product phenomenon to sets avoiding several linear equations

I.D. Shkredov

Abstract. Using the theory of sum-products we prove that for an arbitrary $\kappa \leq 1/3$ any subset of $\mathbb{F}_p$ avoiding $t$ linear equations with three variables has size less than $O(p/t^\kappa)$.

Bibliography: 26 titles.

Keywords: additive combinatorics, sum-product, Fourier transform.

§ 1. Introduction

Let $p$ be a prime number, let $\mathbb{F}_p$ be a finite field and let $A \subseteq \mathbb{F}_p$ be a set. Consider a linear equation

$$c_1 x_1 + \cdots + c_k x_k = b,$$  \hfill (1.1)

where $k \geq 3$ and $c_1, \ldots, c_k \neq 0$. We say that our set $A$ avoids equation (1.1) if there are no tuples $(x_1, \ldots, x_k) \in A^k$ satisfying (1.1). Sets avoiding linear equations is a well-known topic in Additive Combinatorics and Number Theory; see, for example, the classical papers [13] and [14] on this question. It is known that if $b = 0$ and $c_1 + \cdots + c_k = 0$, then $|A| = o(p)$ as $p \to \infty$ but in the other cases it is easy to construct a set of positive density avoiding (1.1). In this paper we only deal with the case $k = 3$ but instead of one equation we look at several at once, say, $t$ equations. Such problems are considered in the articles [14] and [4], for example. For us the basic question is the following: is it true that $|A| = o_t(p)$ as $t \to \infty$ (and $p \to \infty$ of course)? Notice that we do not require $b = 0$ or $c_1 + c_2 + c_3 = 0$. We now formulate the first preliminary result in this direction.

Theorem 1. Let $A \subseteq \mathbb{F}_p$ be a set. Suppose that $A$ avoids $t$ equations of the form

$$x_1 + a_j x_2 + b_j x_3 = d_j,$$  \hfill (1.2)

where all the $a_j$ and $b_j$ are nonzero and each point $(a_j, b_j)$ has either a unique abscissa or ordinate. Then

$$|A| \ll \frac{p}{t^{1/3}}.$$  

Theorem 1 has a straightforward application. Namely, in [15] and [18] the authors studied a family of subsets of $\mathbb{Z}$ which generalize arithmetic progressions of length
An application of the sum-product phenomenon to sets

three. Recall the definition. Let \( t \geq 1 \) be a fixed integer. A finite set \( A \subset \mathbb{Z} \) is called **nonaveraging of order** \( t \), if for every \( 1 \leq m, n \leq t \) the equation

\[
mX_1 + nX_2 = (m + n)X_3
\]

only has trivial solutions: \( X_1 = X_2 = X_3 \). For example, if \( t = 1 \), then \( A \) is nonaveraging of order 1 if and only if \( A \) has no arithmetic progressions of length three. The best upper bound for the size of a subset of \( \{1, \ldots, N\} \) having no arithmetic progressions, and also the history of the problem can be found in [3]. Developing Sanders’ method [16], Bloom proved that

\[
|A| \ll \frac{N(\log \log N)^4}{\log N}.
\]

Here we obtain a new upper bound for the size of a non-averaging set of order \( t \) in \( \mathbb{F}_p \). It is known that the modular version of the problem of the density of arithmetic progressions is equivalent to the integer case. In particular, inequality (1.4) holds with \( N = p \) for sets \( A \subseteq \mathbb{F}_p \) that contain no solutions of \( x + y \equiv 2z \pmod{p} \).

**Theorem 2.** Let \( A \subseteq \mathbb{F}_p \) be a non-averaging set of order \( t \), \( t < \sqrt{p} \). Then

\[
|A| \ll \frac{p}{t^{2/3}}.
\]

Thus, taking any \( C > 3/2 \) and \( t \) such that \( t \geq (\log p)^C \), we see that bound (1.5) is better than (1.4) in this case.

The proof of Theorem 1 only needs Parseval’s identity and the Cauchy-Schwarz inequality but applying the technique of the so-called sum-product phenomenon (see, for instance, [25]) the above result can be improved. Now we formulate a special but useful case of the main theorem in this paper (see Theorem 9 below).

**Theorem 3.** Let \( A \subseteq \mathbb{F}_p \) be a set, \( |A| \gg p^{39/47} \). Suppose that \( A \) avoids \( t \) equations of the form (1.2), where all the \( a_j \) and \( b_j \) are nonzero and each point \( (a_j, b_j) \) has either a unique abscissa or a unique ordinate. Then for any \( \kappa < 3/10 \)

\[
|A| = O\left(\frac{p}{t^{\kappa}}\right).
\]

On the other hand, the following theorem gives a lower bound in this problem.

**Theorem 4.** There is a set \( A \subseteq \mathbb{F}_p \) avoiding \( t \) linear equations of the form (1.2) such that

\[
|A| \gg \frac{p}{t^{1/2}}.
\]

Actually, we prove that \( \kappa \) in Theorem 3 can be improved in many cases; see §5. Nevertheless, we think that our 0.3 can be improved slightly but a bound of the form \( |A| = O(p/t^{\kappa}) \) with \( 1/3 < \kappa \leq 1/2 \) requires completely new ideas and would imply considerable progress in the area. It seems unattainable at the moment (see Example 3 in §3 and the discussion after Remark 5).

The method of the proof of Theorem 3 is based on precise estimates of the number of incidences in [11] and some applications of these results given in [1], [9].
Usually, theorems of this type deal with small subsets of \( \mathbb{F}_p \). Considering a certain dual set, that is, the spectrum of a set or, in other words, the set of large exponential sums (see §4), we show that these results are sometimes applicable to large subsets of \( \mathbb{F}_p \), and this is what we are interested in (see (1.6) and (1.7)). In particular, we prove the following fact, which is interesting in its own right: the spectrum always has small multiplicative energy (see Theorem 5 below). This statement is at the heart of our proof.

The paper is organized as follows. In §2 we give a list of the definitions we need. In §3 we consider some examples of families of sets avoiding several equations and prove the lower bound (1.7). Section 4 is devoted to the spectrum of a set. Here we prove, in particular, that the spectrum has small multiplicative energy and contains a large subset with even smaller multiplicative energy. In §5 we obtain Theorem 1 and our main Theorem 9, which implies Theorem 3. Section 6 contains further applications of the main result. Finally, in §7 we give the proofs of several simple technical lemmas.

§2. Definitions

Let \( p \) be a prime number, let \( \mathbb{F}_p \) be a finite field and denote the set \( \mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\} \) by \( \mathbb{F}_p^* \). The field \( \mathbb{F}_p \) is the main subject of our paper but we consider a slightly more general context which we use at times.

Let \( \mathbf{G} \) be an abelian group. If \( \mathbf{G} \) is finite, then denote the cardinality of \( \mathbf{G} \) by \( N \). It is well known [10] that the dual group \( \hat{\mathbf{G}} \) is isomorphic to \( \mathbf{G} \) in this case. Let \( f \) be a function from \( \mathbf{G} \) to \( \mathbb{C} \). We denote the Fourier transform of \( f \) by \( \hat{f} \),

\[
\hat{f}(\xi) = \sum_{x \in \mathbf{G}} f(x) e(-\xi(x)),
\]  

(2.1)

where \( e(x) = e^{2\pi i x} \) and \( \xi \) is a homomorphism from \( \hat{\mathbf{G}} \) to \( \mathbb{R}/\mathbb{Z} \). We recall the following basic identities

\[
\sum_{x \in \mathbf{G}} |f(x)|^2 = \frac{1}{N} \sum_{\xi \in \hat{\mathbf{G}}} |\hat{f}(\xi)|^2,
\]  

(2.2)

\[
\sum_{y \in \mathbf{G}} \left| \sum_{x \in \mathbf{G}} f(x) g(y - x) \right|^2 = \frac{1}{N} \sum_{\xi \in \hat{\mathbf{G}}} |\hat{f}(\xi)|^2 |\hat{g}(\xi)|^2
\]  

(2.3)

and

\[
f(x) = \frac{1}{N} \sum_{\xi \in \hat{\mathbf{G}}} \hat{f}(\xi) e(\xi(x)).
\]  

(2.4)

If

\[
(f \ast g)(x) := \sum_{y \in \mathbf{G}} f(y) g(x - y) \quad \text{and} \quad (f \circ g)(x) := \sum_{y \in \mathbf{G}} f(y) g(y + x),
\]

then

\[
\hat{f} \ast \hat{g} = \hat{f} \hat{g} \quad \text{and} \quad \hat{f} \circ \hat{g} = \hat{f} \hat{g} = \hat{f} \hat{g},
\]  

(2.5)
where for a function $f: G \to \mathbb{C}$ we set $f^c(x) := f(-x)$. Clearly, $(f \ast g)(x) = (g \ast f)(x)$ and $(f \circ g)(x) = (g \circ f)(-x)$, $x \in G$. In the same way we use the multiplicative convolution of two functions $f, g: \mathbb{F}_p \to \mathbb{C}$ which we denote by

$$(f \otimes g)(x) := \sum_{y \in \mathbb{F}_p^*} f(y)g(xy^{-1}).$$

For any function $f: G \to \mathbb{C}$ we write

$$\|f\|'_\infty := \max_{x \neq 0} |f(x)|.$$

Given a set $S \subseteq G$ we will use the same letter to denote its characteristic function $S: G \to \{0, 1\}$. Write $E^+(A, B)$ for the additive energy of two sets $A, B \subseteq G$ (for example, see [25]), that is,

$$E^+(A, B) = |\{a_1 + b_1 = a_2 + b_2: a_1, a_2 \in A, b_1, b_2 \in B\}|.$$

If $A = B$, we simply write $E^+(A)$ instead of $E^+(A, A)$. In the same way we can define the multiplicative energy of two sets $A, B \subseteq \mathbb{F}_p$ by

$$E^\times(A, B) = |\{a_1b_1 = a_2b_2: a_1, a_2 \in A, b_1, b_2 \in B\}|.$$

Further, clearly,

$$E^+(A, B) = \sum_x (A \ast B)(x)^2 = \sum_x (A \circ B)(x)^2 = \sum_x (A \circ A)(x)(B \circ B)(x), \quad (2.6)$$

and by (2.3),

$$E^+(A, B) = \frac{1}{N} \sum_\xi |\hat{A}(\xi)|^2 |\hat{B}(\xi)|^2. \quad (2.7)$$

We also set

$$E^\times_+(A) = \frac{1}{N} \sum_{\xi \neq 0} |\hat{A}(\xi)|^4 = E^+(A) - \frac{|A|^4}{N}.$$

Let

$$\sigma_k^+(A) := |\{a_1 + \cdots + a_k = 0: a_1, \ldots, a_k \in A\}|.$$

Notice that for a symmetric set $A$, that is, a set such that $A = -A$, we have $\sigma_2(A) = |A|$ and $\sigma_{2k}^+(A) = T_k^+(A)$. Given a set $P$ we write $\sigma_P^+(A) := \sum_{x \in P} (A \circ A)(x)$ and $E_P^+(A, B) := \sum_{x \in P} (A \circ A)(x)(B \circ B)(x)$.

Given two sets $Q, R \subseteq G$ and a real number $t \geq 1$, we define

$$\text{Sym}_t^+(Q, R) := \{x: |Q \cap (x - R)| \geq t\}.$$

and we define similarly $\text{Sym}_t^\times(Q, R)$.

For a positive integer $n$, we set $[n] = \{1, \ldots, n\}$. All logarithms are to the base 2. The signs $\ll$ and $\gg$ are the usual Vinogradov symbols, that is, $a \ll b$ means that $a = O(b)$ and $a \gg b$ means that $b = O(a)$. For a fixed set $A$ we will write $a \lesssim b$ or $b \gtrsim a$ if $a = O(b \cdot (\log |A|)^c)$, where $c > 0$ is an absolute constant. The notation $a \sim b$ means that $a \lessgtr b$ and, simultaneously, $b \lessgtr a$. We denote the disjoint union of two sets $A$ and $B$ by $A \cup B$. 
§ 3. Examples of sets avoiding several linear equations

First of all, recall the definitions. Let $\mathcal{E}$ be a finite family of equations of the form
\[ a_j x + b_j y + c_j z = d_j, \] (3.1)
where all $a_j, b_j$ and $c_j$ are nonzero and such that if two triples $(a_j, b_j, c_j)$ and $(a_j', b_j', c_j')$ correspond to some equations in $\mathcal{E}$ then they are not proportional. Thus the family $\mathcal{E}$ corresponds to a subset of the two-dimensional projective plane. We denote this set by $S(\mathcal{E})$. We write $|\mathcal{E}|$ for the cardinality of $S(\mathcal{E})$. Also notice that we do not require that $d_j = 0$ or $a_j + b_j + c_j = 0$ and hence we are looking at so-called non-affine equations (see [13] and [14]) as well. We say that a set $A$ avoids the family $\mathcal{E}$ if there are no $j \in ||\mathcal{E}||$ and $x, y, z \in A$ such that $a_j x + b_j y + c_j z = d_j$.

In other words, the set $A$ does not satisfy any of the equations in $\mathcal{E}$. Sometimes a rather more general setting is required. Let $A_1, A_2, A_3 \subseteq \mathbb{F}_p$ be three sets. We say that the triple $(A_1, A_2, A_3)$ avoids the family $\mathcal{E}$ if for any $j \in ||\mathcal{E}||$ and all $x \in A_1, y \in A_2$ and $z \in A_3$ we have $a_j x + b_j y + c_j z \neq d_j$.

Example 1. If some coefficients $a_j, b_j, c_j$ are zero, then we can construct large sets $A$ avoiding all equations (3.1). For example, let $A$ be the set of all quadratic residues and consider equations $x - ay = 0$, where $a$ runs over all quadratic non-residues. Then $A$ has size $|A| \gg p$ and avoids this family. Further let $A = \{0, p/4\}$ and consider the system $x + y - z = d$, where $d \in (p/2, 3p/4)$. Then, again, $|A| \gg p$ and $A$ avoids this family. The last example shows that the condition that all quadruples $(a_j, b_j, c_j, d_j)$ are not proportional does not guarantee any bounds for the size of $A$.

We thank the referee who pointed out these examples to us.

Of course, the size of a set $A$ avoiding equations (3.1) depends on the geometry of the set $\mathcal{E}$ or, equivalently, on the set $S(\mathcal{E})$. We consider several rather rough characteristics of the set $\mathcal{E}$ and study them.

Definition 1. Take the intersection of $S(\mathcal{E})$ with the plane $\{c = 1\}$, namely, $S(\mathcal{E}) \cap \{c = 1\} = \{(a, b, 1): (a, b, 1) \in S(\mathcal{E})\}$. Let $\mathcal{F}(\mathcal{E})$ denote the size of the maximal subset in this intersection with the property that any point $(a_j, b_j)$ in it has either a unique abscissa or a unique ordinate.

We can obtain a simple lower bound for the quantity $\mathcal{F}(\mathcal{E})$ (see the proof in § 7).

Lemma 1. We have $\mathcal{F}(\mathcal{E}) \geq |\mathcal{E}|^{1/2}$.

Remark 1. Let $\Gamma$ be a subgroup of $\mathbb{F}_p^*$ and let $S(\mathcal{E}) = (\Gamma \times \Gamma \times \Gamma)/\sim$, where $\sim$ is the standard equivalence. Then in view of $\Gamma/\Gamma = \Gamma$ we have $|\mathcal{E}| = |\Gamma|^2$ and it is easy to see that $\mathcal{F}(\mathcal{E}) = |\Gamma| = |\mathcal{E}|^{1/2}$. It follows that the bound of Lemma 1 is sharp.

We can give a simpler proof of Lemma 1 with a cruder bound of the form $\mathcal{F}(\mathcal{E}) \gg |\mathcal{E}|^{1/2}$ justly noting that for triples $(a, b, c) \in S(\mathcal{E})$ particular ratios $a/b, a/c$ and $b/c$ appear at most $\sqrt{|\mathcal{E}|}$ times because otherwise there is nothing to prove. This implies the lower bound $\mathcal{F}(\mathcal{E}) \geq |\mathcal{E}|/(3\sqrt{|\mathcal{E}|}) = \sqrt{|\mathcal{E}|}/3$. (We thank the referee who pointed this out to us.)

Now we consider another characteristic of the set $S(\mathcal{E})$.

Definition 2. Take the intersection of $S(\mathcal{E})$ with the plane $\{c = 1\}$. We obtain points $(a_j, b_j, 1) \in S(\mathcal{E})$. Then let $\mathcal{F}_4(\mathcal{E})$ denote the size of a maximal subset $J$
of \(|\mathcal{E}|\) such that for any \(j \in J\) either \(a_j \neq a_i\) for all \(i \in J, i \neq j\), or \(b_j \neq b_i\) for all \(i \in J, i \neq j\), or \(a_jb_j^{-1} \neq a_ib_i^{-1}\) for all \(i \in J, i \neq j\). In other words, each point \((a_j, b_j)\) has either a unique abscissa or a unique ordinate or their ratio is unique.

Thus \(\mathcal{I}_*(\mathcal{E}) \leq |\mathcal{E}|\) and the bound it attained if, say, \(S(\mathcal{E}) = \{1\} \times \{1\} \times |\mathcal{E}|\).

There is a similar lower bound for the quantity \(\mathcal{I}_*(\mathcal{E})\) (see § 7).

Lemma 2. We have \(\mathcal{I}_*(\mathcal{E}) \geq 2|\mathcal{E}|^{1/2} - 1\).

Remark 2. Let \(\Gamma\) be a multiplicative subgroup of \(\mathbb{F}_p^*\) and let \(S(\mathcal{E}) = (\Gamma \times \Gamma \times \Gamma) / \sim\).
Then we have \(\Gamma / \Gamma = \Gamma\) and hence \(\mathcal{I}_*(\mathcal{E}) \leq 3|\Gamma| = 3|\mathcal{E}|^{1/2}\). It follows that the bound of Lemma 2 is sharp up to constants.

We say that \(S(\mathcal{E})\) forms a Cartesian product if \(S(\mathcal{E})\) is equivalent to the Cartesian product \(A \times B \times \{1\}\) for some sets \(A\) and \(B\). With some abuse of the notation we sometimes write \(S(\mathcal{E}) = A \times B\) in this case. Note that \(\mathcal{I}_*(\mathcal{E})\) always satisfies
\[
\mathcal{I}_*(\mathcal{E}) \geq \left\{ \frac{x}{y} : (x, y, 1) \in S(\mathcal{E}) \right\}.
\] (3.2)

In particular, if \(S(\mathcal{E}) = A \times B\), then \(\mathcal{I}_*(\mathcal{E}) \geq |A/B|\) but it is easy to see that \(\mathcal{I}(\mathcal{E}) = \max\{|A|, |B|\}\). Thus the quantities \(\mathcal{I}(\mathcal{E})\) and \(\mathcal{I}_*(\mathcal{E})\) cannot be compared in general although, of course, we have the trivial inequality \(\mathcal{I}(\mathcal{E}) \leq \mathcal{I}_*(\mathcal{E})\).

Now we consider several examples of concrete systems of equations (3.1).

Example 2. Let \(\Gamma \subseteq \mathbb{F}_p^*\) be a multiplicative subgroup. The basis properties of \(\Gamma\), that is, the question of when \(\Gamma + \Gamma\) contains \(\mathbb{F}_p^*\) is a classical problem in number theory (see [26], for example). If \(\Gamma + \Gamma\) does not contain \(\mathbb{F}_p^*\), then it is easy to see that for some nonzero \(\xi\) one has \((\Gamma + \Gamma) \cap \xi \Gamma = \emptyset\). This means that, taking any \(a, b \in \Gamma\) the equation \(ax + by - \xi z = 0\) has no solutions in \(\Gamma\). Thus \(S(\mathcal{E})\) is a Cartesian product in this case.

Similarly, consider sets \(A\) with \((A + A) \cap \Gamma = \emptyset\), where \(A\) is not necessarily \(\Gamma\)-invariant. Here the equation \(\gamma x + \gamma y - z = 0, x, y \in A, z \in \Gamma\), has no solutions for any \(\gamma \in \Gamma\) and thus \(S(\mathcal{E}) = \{(\gamma, \gamma, -1) : \gamma \in \Gamma\}\) for the corresponding triple \((A, A, \Gamma)\).

The proposition below shows that we cannot replace the constant \(\kappa\) in Theorem 3 by anything greater than \(1/2\).

Proposition 1. For any \(k \geq 1\) there is a system \(\mathcal{E}\) with \(\mathcal{I}_*(\mathcal{E}) \gg |\mathcal{E}| \geq k\) such that for all sufficiently large \(p \geq p(k)\) there exists \(A \subseteq \mathbb{F}_p\) avoiding the family \(\mathcal{E}\) with
\[
|A| \gg \frac{p}{|\mathcal{E}|^{1/2}}.
\] (3.3)

Proof. Let \(q\) be an even parameter, with \(4k \leq q < \sqrt{p}\), and let
\[
A := \left\{ 1 \leq x < \frac{p}{q} : x \equiv 1 \pmod{2} \right\}.
\]

We have \(|A| \gg p/q\). Set \(q' = q/2\) and \(W = \{(i, j) \in [q'] : i, j \equiv 0 \pmod{2}\}\). The set \(W\) can be considered as a subset of \(\mathbb{N}^2\) rather than \(\mathbb{F}_p^2\). Clearly, \(q^2 \geq |W| \gg q^2\), so taking \(p\) and hence \(q\) sufficiently large we obtain \(|W| \geq k\). Finally, let \(\mathcal{E} =\)
would give better bounds. We have not performed such calculations. Form (3.1) by fixing the variables result we need about the structure of $A$. Let $A \subseteq \mathbb{F}_p$ be a set and $\varepsilon \in (0, 1]$ a real number. Define

$$\text{Spec}_\varepsilon(A) = \{ r \in \mathbb{F}_p : |\widehat{A}(r)| \geq \varepsilon |A| \}.$$
Clearly, $0 \in \text{Spec}_\varepsilon(A)$ and $\text{Spec}_\varepsilon(A) = -\text{Spec}_\varepsilon(A)$. In this section we denote the density of our set $A$ by $\delta$, that is, $\delta = |A|/p$. From Parseval’s identity (2.2), we have a simple upper bound for the size of the spectrum, namely,

$$|\text{Spec}_\varepsilon(A)| \leq \frac{p}{|A|^2} = \frac{1}{\delta^2}. \quad (4.1)$$

We need a result from [19] (sharper bounds are given in [20]) which shows that the spectrum has a rich additive structure.

**Lemma 3.** Let $A \subset \mathbb{F}_p$ be a set, $k \geq 2$ an integer and let $\varepsilon \in (0,1]$ be a real number. Then for any $B \subseteq \text{Spec}_\varepsilon(A)$

$$|\{ (b_1, \ldots, b_k, b'_1, \ldots, b'_k) \in B^k : b_1 + \cdots + b_k = b'_1 + \cdots + b'_k \} | \geq \varepsilon^{2k} |A||B|^{2k} / p. \quad (4.2)$$

We need Proposition 16 from [12] and a combinatorial lemma which is contained in the proof of this proposition. We give the proof of this lemma for completeness.

**Lemma 4.** Let $A \subseteq \mathbb{G}$ be a set and let $P \subseteq A - A$, $P = -P$. Then $A_* \subseteq A$ and a number $q$, $q \leq |A_*|$, can be found such that $(A * P)(x) \geq q$ for any $x \in A_*$ and $\sigma_P(A) \sim |A_*|^q$.

**Proof.** We have

$$\sigma := \sigma_P(A) = \sum_{x \in P} (A \circ A)(x) = \sum_{x \in A} (A * P)(x).$$

Using the pigeonhole principle, we find $A' \subseteq A$ such that the quantities $(A * P)(x)$ differ by a multiplicative factor of at most two on $A'$ and $\sigma \sim q'|A'|$, where $q' = \min_{x \in A'} (A * P)(x)$. If $q' \leq |A'|$, then set $A_* = A'$ and $q = q'$ and we are done. Suppose not. By assumption $P = -P$, and thus we get

$$\sigma \leq \sum_{x \in A'} (A * P)(x) = \sum_{x \in A} (A' * P)(x).$$

Applying the pigeonhole principle again, we find $A'' \subseteq A$ such that the quantities $(A' * P)(x)$ differ by a multiplicative factor of at most two on $A''$ and $\sigma \sim q''|A''|$, where $q'' = \min_{x \in A''}(A' * P)(x)$. Using the inequality $q' > |A'|$ and the trivial bound $q'' \leq |A'|$, we obtain

$$|A''| |A'| \geq |A''| q'' \sim \sigma \geq |A'| q' > q''|A'|$$

and hence $q'' \leq |A''|$. After that we put $A_* = A''$ and $q = q''$. This completes the proof.

We recall a sum-product type result (see Proposition 16 in [12]).

**Proposition 2.** Let $S \subseteq \mathbb{F}_p$ be a set, $|S|^6 \lesssim p^2 \mathbb{E}^x(S)$. Then there is a set $S_1 \subseteq S$, $|S_1|^2 \gtrsim \mathbb{E}^x(S)/|S|$, such that

$$\mathbb{E}^+(S_1)^2 \mathbb{E}^x(S)^3 \lesssim |S_1|^{11} |S|^3. \quad (4.3)$$

The same result holds if $+$ and $\times$ are interchanged.
Now we are ready to prove that a (large) subset of the spectrum always has small multiplicative energy. This is one of the main results in this section.

**Theorem 5.** Let $A \subseteq \mathbb{F}_p$ be a set, and let $\varepsilon \in (0, 1]$ be a real number. Then for any $B \subseteq \text{Spec}_\varepsilon(A)$ with $|B| < \delta^{-1/6} \varepsilon^{-2/3} \sqrt{p}$,

$$E^\times(B) \lesssim |B|^2 \delta^{-2/3} \varepsilon^{-8/3}.$$  \hspace{1cm} (4.4)

**Proof.** If $E^\times(B) \lesssim |B|^2 \delta^{-2/3} \varepsilon^{-8/3}$, then there is nothing to prove. Otherwise, in view of our assumption, we have $|B|^6 \lesssim p^2 E^\times(B)$. Applying Proposition 2 with $S = B$, we find $B_1 \subseteq B$ such that $|B_1|^2 \gtrsim E^\times(B)/|B|$ and

$$E^+(B_1)^2 E^\times(B)^3 \lesssim |B_1|^11 |B|^3.$$ 

Further, using Lemma 3 for $B = B_1$ and $k = 2$ we have $E^+(B_1) \gtrsim \delta \varepsilon^4 |B_1|^4$. Thus

$$E^\times(B)^3 \lesssim |B_1|^3 |B|^3 \delta^{-2} \varepsilon^{-8} \lesssim |B|^6 \delta^{-2} \varepsilon^{-8},$$

as required. The theorem is proved.

**Example 4.** Let $\varepsilon \gg 1$, $B = \text{Spec}_\varepsilon(A)$, $|A| \gg p^{2/5}$, and suppose that the size of $B$ is comparable with the upper bound which is given by (4.1), namely, $|B| \gg \delta^{-1}$. Then $E^\times(B) \lesssim |B|^8/3$. This means that we have a nontrivial estimate for the multiplicative energy of the spectrum in this case.

**Remark 4.** The proof of Theorem 5 shows that a similar statement about the energy holds for the wider class of so-called connected sets, that is, sets $S$ such that for any $S' \subseteq S$, $|S'| \gg |S|$, the energy comparison $E(S') \gg E(S)$ holds (see the rigorous definition in [21] say).

It is possible to increase the size of the set $S_1$ in Proposition 2, decreasing the upper estimate for the product of energies in (4.3). Our arguments mimic the proof of Corollary 22 in [6].

**Corollary 1.** Let $S \subseteq \mathbb{F}_p$ be a set, $|S|^6 \lesssim p^2 E^\times(S)$. Then there is a set $S' \subseteq S$, $|S'|^3 \gtrsim E^\times(S)$ such that

$$E^+(S')^2 E^\times(S)^3 \lesssim |S|^{14}. \hspace{1cm} (4.5)$$

The same result holds if $+$ and $\times$ are interchanged.

**Proof.** Our argument is a sort of algorithm. We construct a decreasing sequence of sets $U_1 = S \supseteq U_2 \supseteq \cdots \supseteq U_k$ and an increasing sequence of sets $V_0 = \emptyset \subseteq V_1 \subseteq \cdots \subseteq V_{k-1} \subseteq S$ such that for any $j = 1, 2, \ldots, k$ the sets $U_j$ and $V_{j-1}$ are disjoint and moreover $S = U_j \sqcup V_{j-1}$. If at some step $j$ we have $|V_j| > (E^\times(S))^{1/3}/2$, then we stop the algorithm by putting $S' = V_j$ and $k = j - 1$. Otherwise we have $|V_j| \leq (E^\times(S))^{1/3}/2$. Applying Proposition 2 to the set $U_j$ we find a subset $Y_j$ of $U_j$ such that $|Y_j|^2 \gtrsim E^\times(U_j)/|U_j|$ and

$$E^+(Y_j)^2 E^\times(U_j)^3 \lesssim |Y_j|^{11} |U_j|^3,$$

provided that $|U_j|^6 \lesssim p^2 E^\times(U_j)$. Now notice that the inequality $|V_j| \leq (E^\times(S))^{1/3}/2$ implies that $E^\times(V_j) \lesssim |V_j|^3 \lesssim E^\times(S)/8$ and hence $E^\times(U_j) \gg E^\times(S)$. In particular, $|Y_j|^2 \gtrsim E^\times(S)/|S|$ and, further,

$$|U_j|^6 \lesssim |S|^6 \lesssim p^2 E^\times(S) \ll p^2 E^\times(U_j),$$
and thus the condition $|U_j|^6 \lesssim p^2 E^x(U_j)$ is satisfied. Hence

$$E^+(Y_j) \lesssim |Y_j|^{11/2} |S|^{3/2} E^x(S)^{-3/2}.$$  

Next we put $U_{j+1} = U_j \setminus Y_j$ and $V_j = V_{j-1} \cup Y_j$ and repeat the procedure. Clearly, for each number $k$ we have $V_k = \bigcup_{j=1}^k Y_j$, and it is easy to see that our algorithm must stop at some finite step $k$. Put $S' = V_{k-1}$. It is known that $E^{1/4}(\cdot)$ is a norm (see [25] or [6], for example), and so

$$E^+(S') \leq \left(\sum_{j=1}^{k-1} E^+(Y_j)^{1/4}\right)^4 \lesssim |S|^{3/2} E^x(S)^{-3/2} \left(\sum_{j=1}^{k-1} |Y_j|^{11/8}\right)^4 \lesssim |S|^{3/2} E^x(S)^{-3/2} |S|^{11/2} = |S|^7 E^x(S)^{-3/2},$$

as required. The corollary is proved.

Using Corollary 1 above we can prove that any subset of the spectrum has a large subset with small multiplicative energy.

**Theorem 6.** Let $A \subset \mathbb{F}_p$ be a set, and let $\varepsilon \in (0, 1]$ be a real number. Then for any $B \subseteq \text{Spec}_\varepsilon(A)$, $|B| < \delta^{1/3} \varepsilon^2 p$, there is a $B' \subseteq B$ such that $|B'|^3 \gtrsim \delta \varepsilon^4 |B|^4$ and

$$E^x(B') \lesssim |B| \delta^{-3/2} \varepsilon^{-6}. \quad (4.6)$$

**Proof.** Suppose that $|B|^6 \lesssim p^2 E^+(B)$. Then we use Corollary 1 replacing $+$ by $\times$. Thus, there is $B' \subseteq B$, $|B'|^3 \gtrsim E^+(B)$, such that

$$E^x(B')^2 E^+(B)^3 \lesssim |B|^{14}. \quad (4.7)$$

Applying Lemma 3 with $k = 2$, we see that $E^+(B) \geq \delta \varepsilon^4 |B|^4$. It gives us, first, $|B|^3 \gtrsim \varepsilon \delta^4 |B|^4$ and, second, from (4.7) it follows that

$$E^x(B')^2 \delta^3 \varepsilon^{12} |B|^{12} \lesssim |B|^{14},$$

as required. To check the inequality $|B|^6 \lesssim p^2 E^+(B)$ we recall that $E^+(B) \gtrsim \delta \varepsilon^4 |B|^4$. This completes the proof.

**Example 5.** Let $\varepsilon \gg 1$, let $B = \text{Spec}_\varepsilon(A)$, $|A| \gg p^{1/3}$ and suppose the size of $B$ is comparable with the upper bound (4.1), namely, $|B| \gg \delta^{-1}$. Then by Theorem 6 we can find a set $B' \subseteq B$ such that $E^x(B') \lesssim |B'|^{5/2}$ and $|B'| \gtrsim |B|$. It is interesting to note that a full analogue of the Szemerédi-Trotter Theorem for $\mathbb{R}$ (see [12], Proposition 16) would only give us $E^x(B') \lesssim |B'|^{3/2} \delta^{-1} \varepsilon^{-4} \sim |B'|^{5/2}$, that is, the same bound in this regime.

Theorem 6 immediately implies the following corollary.

**Corollary 2.** Let $A \subset \mathbb{F}_p$ be a set, and let $\varepsilon \in (0, 1]$ be a real number. Then for any $B := \text{Spec}_\varepsilon(A)$, $|B| < \delta^{1/2} \varepsilon^2 p$, there is $\widetilde{B} \subseteq B$ such that $|\widetilde{B}| \geq |B|/2$ and

$$E^x(\widetilde{B}) \lesssim \delta^{-17/6} \varepsilon^{-34/3} |B|^{-1/3} \lesssim \delta^{-5/2} \varepsilon^{-32/3}.$$
Proof. Applying Theorem 6 to the set $B$, we find $B' := B' \subseteq B$ such that (4.6) holds and $|B'||^3 \gtrsim \delta^4 |B|^4$. Consider $B \setminus B'$. If $|B \setminus B'| < |B|/2$, then we are done. If not, then apply the same arguments to this set, and so on. At the end we have constructed a sequence of disjoint subsets of $B$, namely, $B'_1, \ldots, B'_k$ such that the set $\widetilde{B} := \bigcup_{j=1}^k B'_j$ has size at least $|B|/2$. Clearly, $k \lesssim \delta^{-1/3} \varepsilon^{-4/3} |B|^{-1/3}$. Because $E^{1/4}()$ is a norm, in view of (4.6) and Parseval’s identity we obtain

$$E^x(\widetilde{B}) \leq k^4 |B| \delta^{-3/2} \varepsilon^{-6} = \delta^{-17/6} \varepsilon^{-34/3} |B|^{-1/3} \lesssim \delta^{-5/2} \varepsilon^{-32/3}.$$  

This completes the proof.

As in Example 5, if $\varepsilon \gg 1$, $B = \text{Spec}_\varepsilon(A)$, $|A| \gg p^{1/3}$ and $|B| \gg \delta^{-1}$, then we find a set $\widetilde{B} \subseteq B$ such that $E^x(\widetilde{B}) \lesssim |\tilde{B}|^{5/2}$ and $|\tilde{B}| \geq |B|/2$.

§ 5. The proof of the main result

First of all we give a plan of the proof of Theorem 3. Using Fourier analysis it is easy to see that equations (1.2) have no solutions if and only if

$$0 = \sum_r \hat{A}(r)\hat{A}(a_j r)\hat{A}(b_j r) = |A|^3 + \sum_{r \neq 0} \hat{A}(r)\hat{A}(a_j r)\hat{A}(b_j r).$$

In other words, for each $j$ we have $\sum_{r \neq 0} |\hat{A}(r)||\hat{A}(a_j r)||\hat{A}(b_j r)| \geq |A|^3$ and thus the sum is large. Further we can check that the sum in the last formula is only taken over large $\hat{A}(r)$, namely, all the three numbers $r, a_j r$ and $b_j r$ must belong to the spectrum $\text{Spec}_\varepsilon(A)$ with some $\varepsilon > 0$ effectively depending on the density of $A$. It means that for any $j$ the intersection

$$\text{Spec}_\varepsilon(A) \cap a_j^{-1} \text{Spec}_\varepsilon(A) \cap b_j^{-1} \text{Spec}_\varepsilon(A)$$

is large. This type of intersection can be large if $\text{Spec}_\varepsilon(A)$ behaves as a multiplicative subgroup, say. Nevertheless, by the results of the previous section the spectrum has a strong additive structure and by the sum-product phenomenon this implies that the multiplicative structure of $\text{Spec}_\varepsilon(A)$ must be poor. To obtain a contradiction with the sum-product phenomenon we need the $a_j$ and $b_j$ in formula (5.1) to be distinct. But this is guaranteed by our assumptions on the set $\varepsilon'$.

5.1. The proof of Theorem 1. The main result in this subsection is the following theorem.

Theorem 7. Let $\varepsilon$ be a finite family of equations of the form (3.1). Also let $A \subseteq \mathbb{F}_p$ be a set avoiding the family $\varepsilon$. Then

$$|A| \ll \frac{p}{(\mathcal{F}(\varepsilon))^{1/3}}.$$  

(5.2)

Proof. Let $|A| = \delta p$ and $t = \mathcal{F}(\varepsilon)$. By assumption the set $A$ avoids all equations in the family $\varepsilon$. Using the Fourier transform we see that this is equivalent to

$$0 = \sum_r \hat{A}(a_j r)\hat{A}(b_j r)\hat{A}(c_j r)e(-d_j r) = |A|^3 + \sum_{r \neq 0} \hat{A}(a_j r)\hat{A}(b_j r)\hat{A}(c_j r)e(-d_j r)$$

(5.3)
for all $j \in [t]$. Applying Parseval’s identity (2.2) three times, we have
\[
2^{-1}|A|^3 \leq \sum_{r \in (a_j^{-1}B) \cap (b_j^{-1}B) \cap (c_j^{-1}B)} |\hat{A}(a_j r)||\hat{A}(b_j r)||\hat{A}(c_j r)|,
\] (5.4)
where $B = \text{Spec}_e(A) \setminus \{0\}$, $\varepsilon = \delta/6$. Now,
\[
\sum_{r \notin c_j^{-1}B} |\hat{A}(a_j r)||\hat{A}(b_j r)||\hat{A}(c_j r)| \leq \varepsilon|A|\sum_r |\hat{A}(a_j r)||\hat{A}(b_j r)|
\]
\[
\leq \varepsilon|A|\left(\sum_r |\hat{A}(a_j r)|^2\right)^{1/2}\left(\sum_r |\hat{A}(b_j r)|^2\right)^{1/2} \leq \varepsilon|A|p = \frac{|A|^3}{6}
\]
and similarly for the other two terms. Here we have used the fact that $a_j$, $b_j$ and $c_j$ are nonzero numbers.

Let $S := \{s_1, \ldots, s_t\} \subseteq S(\mathcal{E})$ be such that, say, $s_j = (a_j, b_j, 1)$, where the $a_j$ and the $b_j$ are distinct. In other words, the $a_j$ and the $b_j$ belong to two sets $S_A$ and $S_B$, respectively, and $|S_A| = |S_B| = t$. Now we return to (5.4). Summing the last estimate over $S$, and using the Cauchy-Schwartz inequality and Parseval’s identity (2.2) we have
\[
t^2|A|^6 \ll \left(\sum_{r \in B} |\hat{A}(r)|\sum_{j=1}^t |\hat{A}(a_j r)||\hat{A}(b_j r)|B(a_j r)B(b_j r)\right)^2
\]
\[
\ll \sum_r |\hat{A}(r)|^2 \sum_{r \in B} \left(\sum_{j=1}^t |\hat{A}(a_j r)||\hat{A}(b_j r)|B(a_j r)B(b_j r)\right)^2
\]
\[
\ll |A|^p \sum_{r \in B} \left(\sum_{j=1}^t |\hat{A}(a_j r)||\hat{A}(b_j r)|B(a_j r)B(b_j r)\right)^2
\]
\[
\ll |A|^p \sum_{r \in B} \left(\sum_{j=1}^t |\hat{A}(a_j r)|^2\right)^{1/2}\left(\sum_{j=1}^t |\hat{A}(b_j r)|^2\right)^{1/2} \ll (|A|^3|B| \ll p^6,
\]
or, in other words, $\delta \ll t^{-1/3}$. The theorem is proved.

After this paper was written, Tomasz Schoen found a simpler proof of the above result and here we have followed his approach, which is more direct.

Remark 5. It is easy to see from the proof of Theorem 9 that the same arguments work for sets having, say, at most $|A|^3/(4p)$ or at least $2|A|^3/p$ solutions to equations (3.1). In other words, for our method we need the number of solutions to differ significantly from the expectation.

5.2. The proof of Theorem 3. In [1] (see also [9]) a sum-product type result was obtained which we will use below. For a more general view of these problems consult the paper [12].

Theorem 8. Suppose that $A, B, C \subseteq \mathbb{F}_p$ are sets with $|A||B||C| = O(p^2)$. Then
\[
|\{(a_1, a_2, b_1, b_2, c_1, c_2) \in A^2 \times B^2 \times C^2 : a_1(b_1 + c_1) = a_2(b_2 + c_2)\}|
\]
\[
\ll (|A||B||C|)^{3/2} + |A||B||C| \max\{|A|, |B|, |C|\}.
\]
Now we formulate the main technical proposition in this subsection.

**Proposition 3.** Let $A \subset \mathbb{F}_p$ be a set, let $\delta = |A|/p$, and let $\varepsilon \in (0,1]$ be a real number. For an arbitrary $B \subseteq \text{Spec}_\varepsilon(A)$ and any sets $C, D \subseteq \mathbb{F}_p$, $|C| \leq |D|$, assume that

$$|B| \leq \delta \varepsilon^4 |C|^3 |D|^2 \leq |B|^9$$  \hfill (5.5)

and

$$\delta^{-1/4} \varepsilon^{-1} |B|^{9/4} |D|^{-1/2} |C|^{5/4} < p^2.$$  \hfill (5.6)

Then

$$\sum_{x \in D} (B \otimes C)(x) \lesssim \delta^{-3/16} \varepsilon^{-3/4} |B|^{11/16} |D|^{1/8} |C|^{15/16}.$$  \hfill (5.7)

**Proof.** First, it is trivial that $\sigma \leq |B| |C|$, and hence we can suppose that

$$|B| |C| > \delta^{-3/16} \varepsilon^{-3/4} |B|^{11/16} |D|^{1/8} |C|^{15/16},$$

or, in other words,

$$|B|^5 |C| \varepsilon^{12} \delta^3 > |D|^2.$$  \hfill (5.8)

Finally, because of $B \subseteq \text{Spec}_\varepsilon(A)$, in view of (4.1) we have

$$|B| \leq \delta^{-1/4} \varepsilon^{-2}.$$  \hfill (5.9)

Now let $M \geq 1$ be a parameter which we will choose later. Our arguments are a sort of algorithm. We construct a decreasing sequence of sets $U_1 = B \supseteq U_2 \supseteq \cdots \supseteq U_k$ and an increasing sequence of sets $V_0 = \emptyset \subseteq V_1 \subseteq \cdots \subseteq V_{k-1} \subseteq B$ such that for any $j = 1, 2, \ldots, k$ the sets $U_j$ and $V_{j-1}$ are disjoint and moreover $B = U_j \cup V_{j-1}$. If at some step $j$ we have $E^+(U_j) \leq |B|^3 / M$, then we stop the algorithm by setting $U = U_j$, $V = V_{j-1}$ and $k = j - 1$. Otherwise we have $E^+(U_j) > |B|^3 / M$. Using the pigeonhole principle we find a set $P_j \subseteq U_j - U_{j-1}$ such that $E^+_{P_j}(U_j) \sim E^+(U_j)$ and a number $t = t_j$ with $t < (U_j \cap U_{j+1})(x) \leq 2t$ for all $x \in P_j$. Applying Lemma 4 to the sets $U_j$ and $P_j$ we get a subset $Y_j$ of $U_j$ such that $|Y_j| \geq |B|/M$, and a number $q_j \lesssim |Y_j|$ such that for any $x \in Y_j$ we have $(U_j \ast P_j)(x) \geq q_j$ and $\text{dist}_{P_j}(U_j) \sim |Y_j| q_j$. Then we set $U_{j+1} = U_j \setminus Y_j$, $V_j = V_{j-1} \cup Y_j$ and repeat the procedure. Clearly, $V_k = \bigcup_{j=1}^k Y_j$ and because of $|Y_j| \geq |B| / M$ we have $k \lesssim M$, so the number of steps is finite.

Consider $\sigma_j = \sum_{x \in D} (Y_j \otimes C)(x)$. By the Cauchy-Schwarz inequality and the fact that $(U_j \ast P_j)(x) \geq q_j$ on $Y_j$, we have

$$\sigma_j^2 \leq |D| E^x(Y_j, C) \lesssim q_j^{-2} |D| \cdot \max \{|U_j|, |P_j|, |C|\}. \hfill (5.10)$$

Applying Theorem 8 we obtain

$$\sigma_j^2 \ll q_j^{-2} |D| \cdot \max \{|U_j|, |P_j|, |C|\} \cdot \max \{|U_j|, |P_j|, |C|\}, \hfill (5.10)$$

provided that

$$|U_j|, |P_j|, |C| \ll p^2. \hfill (5.11)$$

We will check condition (5.11) later. In addition, we will assume that the first term in (5.10) dominates. Then using the fact that $q_j |Y_j| \sim t |P_j|$ we obtain

$$\sigma_j^2 \ll q_j^{-2} |D| \cdot \max \{|U_j|, |P_j|, |C|\} \ll |D| \cdot |C|^{3/2} |B|^{3/2} |Y_j|^{2t-2} |P_j|^{-1/2}.$$


Now recalling that \( \sigma_j \lesssim |Y_j| \) and observing that
\[
t|Y_j|^2 \gtrsim t q_j |Y_j| \approx t \sigma P_j(U_j) \sim t^2 |P_j| \sim E^+(U_j),
\]
from \( t|Y_j|^2 \gtrsim t^2 |P_j| \) and \( t|Y_j|^2 \gtrsim E^+(U_j) \) we obtain \( E^+(U_j)/|Y_j|^2 \lesssim t \lesssim |Y_j|^2/|P_j| \) and hence, in view of \( t^2 |P_j| \sim E^+(U_j) \), we derive
\[
|P_j| \lesssim \frac{|Y_j|^4}{E^+(U_j)};
\]
(5.12)
and therefore
\[
\sigma_j^2 \lesssim |D| |C|^{3/2} |B|^{3/2} |Y_j|^2 E^+(U_j)^{-1} |P_j|^{1/2} \lesssim |D| |C|^{3/2} |B|^{3/2} |Y_j|^4 E^+(U_j)^{-3/2} \\
\lesssim M^{3/2} |D| |C|^{3/2} |Y_j|^4 |B|^{-3/2}.
\]
Thus
\[
\sigma = \sum_{x \in D} (U \otimes C)(x) + \sum_{x \in D} (V \otimes C)(x) \leq \sum_{x \in D} (U \otimes C)(x) + \sum_{j=1}^k \sigma_j \\
\lesssim \sum_{x \in D} (U \otimes C)(x) + M^{3/4} |D|^{1/2} |C|^{3/4} |B|^{-3/2} \sum_{j=1}^l |Y_j|^2 \\
\lesssim \sum_{x \in D} (U \otimes C)(x) + M^{3/4} |D|^{1/2} |C|^{3/4} |B|^{1/2}.
\]
(5.13)
To estimate the first term in the last formula we recall that \( E^+(U) \leq |B|^3/M \) and \( U \subseteq B \subseteq \text{Spec}_\varepsilon(A) \). Using Lemma 3 we see that
\[
\delta^4 |U|^4 \leq E^+(U) \leq \frac{|B|^3}{M}.
\]
Hence
\[
|U| \leq \delta^{-1/4} \varepsilon^{-1} M^{-1/4} |B|^{3/4}
\]
(5.14)
and thus
\[
\sigma \lesssim \delta^{-1/4} \varepsilon^{-1} M^{-1/4} |B|^{3/4} \cdot \min\{|C|, |D|\} + M^{3/4} |D|^{1/2} |C|^{3/4} |B|^{1/2}.
\]
Recall that \( m := \min\{|C|, |D|\} = |C| \). The optimal choice of \( M \) is
\[
M = \delta^{-1/4} \varepsilon^{-1} |B|^{1/4} |D|^{-1/2} |C|^{-3/4} m = \delta^{-1/4} \varepsilon^{-1} |B|^{1/4} |D|^{-1/2} |C|^{1/4},
\]
and hence
\[
\sigma \lesssim \delta^{-3/16} \varepsilon^{-3/4} m^{3/4} |B|^{11/16} |D|^{1/8} |C|^{13/16} = \delta^{-3/16} \varepsilon^{-3/4} |B|^{11/16} |D|^{1/8} |C|^{15/16}.
\]
It is easy to see that the inequality \( M \geq 1 \) is equivalent to
\[
|B| |C| \geq \delta^4 |D|^2,
\]
but, in view of (5.8), this follows from

$$|B|^4 \leq \delta^{-4}\varepsilon^{-16}.$$  

The last inequality is a simple consequence of (5.9). Now we check condition (5.11). In view of the estimate (5.12) it is sufficient to have

$$|U_j||P_j||C| \lesssim \frac{|Y_j|^4|U_j||C|}{E^+(U_j)} \leq M|C||B|^2$$

$$= \delta^{-1/4}\varepsilon^{-1}|B|^{9/4}|D|^{-1/2}|C|^{5/4} \ll p^2.$$  

The last bound is our condition (5.6) (we ignore the signs $\ll$ and $\gg$ by increasing the constants in (5.7) where necessary).

It remains to consider the case when the second term in (5.10) dominates. We will show that in this situation we obtain an even better upper bound for $\sigma$. Put $\nu_j = \max\{|U_j|, |P_j||C|\})$. In view of formulae (5.10) and (5.13), and our choice of $q_j$, it is sufficient to check that

$$|D|^{1/2} \sum_j q_j^{-1}(|U_j||P_j||C|\nu_j)^{1/2} \lesssim |D|^{1/2} \sum_j t_j^{-1}|Y_j|(|U_j||P_j|^{-1}|C|\nu_j)^{1/2}$$

$$\lesssim M^{3/4}|D|^{1/2}|C|^{3/4}|B|^{1/2}.$$  

If $\nu_j = |P_j|$, then we obtain the following inequality to verify:

$$\sum_j |Y_j|t_j^{-1}|U_j|^{1/2} \lesssim M^{3/4}|C|^{1/4}|B|^{1/2}.$$  

Clearly, $|U_j| \leq |B|$, $t_j \geq |B|/M$ and $\sum_j |Y_j| \leq |B|$. Thus we need to check that $M \leq |C|,$

or, in other words,

$$|B| \leq |C|^3|D|^2\delta\varepsilon^4,$$

and this is the first part of condition (5.5). If $\nu_j = U_j$, then we have the bound

$$\sum_j |Y_j||U_j|((t_j^2|P_j|)^{-1/2} \lesssim \sum_j (E^+(B))^{-1/2}|Y_j||U_j|$$

$$\leq \left(\frac{|B|^3}{M}\right)^{-1/2} \sum_j |Y_j||U_j| \leq M^{1/2}|B|^{1/2}.$$  

Clearly, the last quantity is less than $M^{3/4}|C|^{1/4}|B|^{1/2}$. Finally, if $\nu_j = |C|$, then similarly we get

$$\sum_j |Y_j||U_j|^{1/2}|C|^{1/2}(t_j^2|P_j|)^{-1/2} \lesssim M^{1/2}|C|^{1/2}.$$  

To make this less than $M^{3/4}|C|^{1/4}|B|^{1/2}$ it is sufficient to have

$$|C| \leq M|B|^2.$$  

or

$$|C|^3|D|^2 \delta^4 \leq |B|^9.$$  

The last inequality coincides with the second part of (5.5). This completes the proof.

**Theorem 9.** Let $\mathcal{E}$ be a finite family of equations of the form (3.1). Also, let $A \subseteq \mathbb{F}_p$ be a set avoiding the family $\mathcal{E}$ and $|A| \gg p^{39/47}$. Then for any $\kappa < 3/10$,

$$|A| \ll \frac{p}{\mathcal{T}(\mathcal{E})^{\kappa}}. \quad (5.15)$$

**Proof.** Put $t_* = \mathcal{T}(\mathcal{E})$ and let $S_* = \{s_1, \ldots, s_{t_*}\}$ be the set from the Definition 2. We use the notation and the calculations from Theorem 7. So, returning to (5.4) and changing the variables, for any $j \in [t_*]$ we have

$$2^{-1}|A|^3 \leq \sum_{r \in B \cap (B/s_j) \cap (B/s'_j)} |\hat{A}(s_j r)| \cdot |\hat{A}(s'_j r)| \cdot |\hat{A}(r)|.$$  

Here $s'_j = a_j$ if $s_j = b_j$, further $s'_j = b_j$ if $s_j = a_j$ and, finally, $s'_j = b_j^{-1}$ if $s_j = a_j/b_j$. Since $s'_j \neq 0$, by the Cauchy-Schwarz inequality and (2.2) we obtain

$$|A|^6 \ll |A|^p \sum_{r \in B \cap (B/s_j)} |\hat{A}(s_j r)|^2 |\hat{A}(r)|^2. \quad (5.16)$$

Thus, summing over $j \in [t_*]$ we get

$$|A|^{5t_*} \ll p \sum_{j=1}^{t_*} \sum_{r \in B \cap (B/s_j)} |\hat{A}(s_j r)|^2 |\hat{A}(r)|^2. \quad (5.17)$$

Using the pigeonholing principle twice we find two numbers $\Delta_1, \Delta_2 \leq |A|$ and two sets $W_1, W_2 \subseteq B$ such that $\Delta_1 \leq |\hat{A}(r)| \leq 2\Delta_1$ for $r \in W_1$ and $\Delta_2 \leq |\hat{A}(r)| \leq 2\Delta_2$ for $r \in W_2$ and

$$|A|^{5t_*} \lesssim p\Delta_1^2 \Delta_2^2 \sum_r W_2(r)(W_1 \otimes S_*^{-1})(r). \quad (5.18)$$

As above, we have $|W_1|, |W_2| \leq t_*$ because otherwise there is nothing to prove. Similarly, we can check that the conditions

$$\delta^{-1/4} \varepsilon_1^{-1} |W_1|^{9/4} t_*^{-1/2} |W_2|^{5/4} < p^2 \quad \text{and} \quad \delta^{-1/4} \varepsilon_2^{-1} |W_2|^{9/4} t_*^{-1/2} |W_1|^{5/4} < p^2$$

follow from the assumption that $|A| \gg p^{39/47}$. Here $\varepsilon_1 = \Delta_1/|A|$ and $\varepsilon_2 = \Delta_2/|A|$. Further, from (5.18) we obtain

$$t_* \delta |A|^4 \ll \Delta_1^2 \Delta_2^2 |W_1| |W_2|.$$  

Hence in view of Parseval’s identity we have

$$|W_1|, |W_2| \gg \delta^2 t_* \quad \text{and} \quad |W_1| |W_2| \gg \delta t_*.$$  

(5.19)
Suppose that $|W_2| \geq |W_1|$ for definiteness. We split the set $W_2$ into some $s$ sets $W_2^{(j)}$ whose sizes can only differ from one another by one, where $s$ is a parameter which we will choose later. For any $j$, the bounds (5.19) imply that

$$\delta \varepsilon_4 |W_2^{(j)}|^{3/4} t_*^2 \gg \delta^5 |W_2|^{3/4} t_*^{2s} - 3 \gg |W_1|$$

provided that $s \ll |W_2|^{2/3} \delta^{-5/3} |W_1|^{-1/3}$. Further,

$$\delta \varepsilon_4 |W_2^{(j)}|^{3/4} t_*^2 \ll \delta |W_2|^{3/4} t_*^{2s} - 3 \ll |W_1|^9$$

provided that $s \gg \delta^{1/3} |W_2|^{2/3} |W_1|^{-3}$. Setting $s = \delta^{1/3} |W_2|^{2/3} |W_1|^{-3}$ we can verify that $s \ll |W_2|^{2/3} \delta^{-5/3} |W_1|^{-1/3}$ because otherwise, in view of (5.19), we have

$$1 \gg |W_1|^{8/3} \delta^{4/3} \gg t_*^{8/3} \delta^{20/3}$$

or, in other words, $\delta \ll t_*^{-2/5}$ which is better than (5.15). Suppose, in addition, that $s \gg 1$. Thus all the conditions of the second part of Proposition 3 are satisfied. Using (5.19) and applying Proposition 3 with $\varepsilon = \varepsilon_1$, $B = W_1$, $C = (W_2^{(j)})^{-1}$ and $D = S_*$ and Parseval’s identity, we have

$$|A|^{7/8} \lesssim p \Delta_1^2 \Delta_2 \delta^{-3/16} \left( \frac{|A|}{\Delta_1} \right)^{3/4} |W_1|^{11/16} \left( \frac{|W_2|}{s} \right)^{15/16} s$$

$$= p |A|^{3/4} \Delta_1^{5/4} \Delta_2 \delta^{-3/16} |W_1|^{11/16} |W_2|^{15/16} s^{1/16}$$

$$\leq p |A|^{3/4} (p |A|)^{13/8} \delta^{-3/16} |W_1|^{1/16} |W_2|^{-1/16} s^{1/16}$$

$$= p^{21/8} |A|^{19/8} \delta^{-3/16} |W_1|^{1/16} |W_2|^{-1/16} s^{1/16}$$

$$\ll p^5 \delta^{35/16} \left( \delta^{1/3} t_*^{-3/2} |W_1|^{-2} \right)^{1/16} \ll p^5 \delta^{35/16} (\delta^{-11/3} t_*^{-4/3})^{1/16}. \quad (5.20)$$

This gives us

$$\delta \lesssim t_*^{-23/73} \quad (5.21)$$

which is better than (5.15). If $s \ll 1$ then from (5.20) and (5.19) we see that

$$\delta^5 t_*^{7/8} \lesssim \delta^{35/16} |W_1|^{1/16} |W_2|^{-1/16} \lesssim \delta^2 (\delta^2 t_*)^{-1/16} \gg \delta^{15/8} t_*^{-1/16}$$

or, in other words,

$$\delta \lesssim t_*^{-3/10}$$

which coincides with (5.15). Finally, we should note that in the case $s \ll 1$, in view of the inequality $|W_2| \geq |W_1|$ and the bound (5.19), we have

$$\delta \varepsilon_4 |W_2|^{3} t_*^2 \gg \delta^5 |W_1| |W_2|^2 t_*^2 \gg \delta^9 |W_1| t_*^4 \gg |W_1|,$$

because otherwise we obtain $\delta \lesssim t_*^{-4/9}$ which is much better than (5.15).

In view of Lemma 2, we obtain the following.

**Corollary 3.** Let $\mathcal{E}$ be a finite family of equations of the form (3.1). Also let $A \subseteq \mathbb{F}_p$ be a set avoiding the family $\mathcal{E}$, $|A| \gg p^{39/47}$. Then for any $\kappa < 5/31$

$$|A| \ll \frac{p}{|\mathcal{E}|^\kappa}.$$
§ 6. Further results

First, we prove Theorem 2 from § 1.

Proof of Theorem 2. By our assumption the set \( A \) avoids all equations from (1.3). In other words, \( X_1 + n/m \cdot X_2 = (1 + n/m)X_3 \), where \( X_1, X_2, X_3 \in A \) implies \( X_1 = X_2 = X_3 \). Thus, we have the corresponding system \( \mathcal{S} \) with the set \( S(\mathcal{S}) \) of cardinality \(|[t]/[t]|\). In a similar way

\[
\mathcal{S}(\mathcal{S}) = \left\{ \frac{n}{m} : n, m \in [t] \right\} = \left\lfloor \frac{[t]}{[t]} \right\rfloor.
\]

Considering square-free numbers, in view of the assumption that \( t < \sqrt{p} \), it is easy to see that \(|[t]/[t]| \gg t^2\) both in \( \mathbb{Z} \) and in \( \mathbb{F}_p \) (see the proof of Proposition 1). Although Theorem 9 was formulated just for sets having no solutions at all, it is easy to verify that the number of trivial solutions is \( |A| \). Thus, if \( |A|p \leq |A|^3/4 \), say, then the method of the proof works (see Remark 5). Of course, if \( |A|p > |A|^3/4 \), then \( |A| < 2\sqrt{p} \) and there is nothing to prove. Thus, applying the first part of Theorem 9 (and the arguments after Remark 5) we obtain the required result. Theorem 2 is proved.

Now we need the best bound for the number of incidences in \( \mathbb{F}_p \) currently available (see the paper [24] and also [7], Theorem 7).

Theorem 10. Let \( n \) be an integer and \( A, B \subset \mathbb{F}_p \) be two sets, \( |A||B|^2 \leq n^3 \) and \( |A|n \ll p^2 \). Then the number of incidences between the point set \( A \times B \) and any set of \( n \) lines in \( \mathbb{F}_p^2 \) is \( O(|A|^{3/4}|B|^{1/2}n^{3/4} + n + |A|^{2/3}|B|^{2/3}n^{2/3}) \).

We will obtain a consequence of Theorem 10 in the spirit of the paper [6].

Lemma 5. Let \( A \subset \mathbb{F}_p \) be a set such that \( A \subset \text{Sym}_t^+(P, Q) \), where \( P, Q \subset \mathbb{F}_p \) are two other sets, \( \max\{|P|, |Q|\} \geq |A| \). Then for any set \( B \), where \( |B||P||Q| \ll p^2 \),

\[
|\{ s : |A \cap Bs| \geq \tau \}| \ll \frac{|P||Q||B|^{3/2}}{(t\tau)^{2}}.
\]

Proof. Let \( S_\tau \) be the set on the left-hand side of (6.1). We have

\[
\tau|S_\tau| \leq \sum_{s \in S_\tau} |A \cap Bs| = |\{ a = bs : a \in A, b \in B, s \in S_\tau \}| := \sigma.
\]

Because \( A \subset \text{Sym}_t^+(P, Q) \), we obtain the following upper bound for the number of solutions \( \sigma \)

\[
\sigma \leq t^{-1}|\{ p + q = sb : p \in P, q \in Q, b \in B, s \in S_\tau \}|.
\]

(6.2)

Assume for definiteness that \( |P| \leq |Q| \). Thus \( |Q| \geq |A| \). First, we prove a trivial estimate for the size of \( S_\tau \). Namely, dropping the condition \( s \in S_\tau \) in (6.2) we obtain

\[
\tau|S_\tau|t \leq |P||Q||B|,
\]

and hence inequality (6.1) only has to be checked in the range

\[
t^{2/2} \gg |P||Q||B|,
\]

(6.3)
because otherwise

\[ |S_\tau| \leq \frac{|P| |Q| |B|}{t\tau} \ll \frac{(|P| |Q| |B|)^{3/2}}{(t\tau)^2}. \]

Further, consider the family \( \mathcal{L} \) of \(|B| |Q|\) lines \( l_{b,q} = \{(x, y) : y + q = bx\},\) \( q \in Q, \ b \in B, \) and the family of points \( \mathcal{P} = S_\tau \times P. \) Applying Theorem 10 to the pair \((\mathcal{P}, \mathcal{L})\) we obtain

\[
\sigma \leq t^{-1} \mathcal{I}(\mathcal{P}, \mathcal{L}) \ll t^{-1} \left( (|S_\tau|^{1/2} |P|^{3/4} |\mathcal{L}|^{3/4} + |\mathcal{L}| + |S_\tau|^{2/3} |P|^{2/3} |\mathcal{L}|^{2/3}) \right)
\ll t^{-1} \left( (|S_\tau|^{1/2} (|P| |Q| |B|)^{3/4} + |B| |Q| + (|S_\tau| |P| |Q| |B|)^{2/3}) \right)
\]

(6.4)

provided that \(|P||B||Q|\ll p^2\) and \(|P||S_\tau||B|\leq |B|^{3}|Q|^3\). The first inequality is our assumption. We will check the second. We have a trivial bound \(|S_\tau| \leq |A| |B|\) and hence, if \(|S_\tau|^2 |P| > |B|^{3}|Q|^3\), then

\[ |A|^2 |B|^2 |Q| \geq |A|^2 |B|^2 |P| \geq |S_\tau|^2 |P| > |B|^3 |Q|^3, \]

(6.5)

and we have arrived at a contradiction since \(|Q| \geq |A|\).

Now, if the first term in (6.4) dominates, then we obtain (6.1). Suppose that the required bound (6.1) does not hold. Then if the second term in (6.4) is the largest one, in view of (6.3) we obtain

\[ \frac{(|P| |Q| |B|)^{3/2}}{t\tau} \ll t\tau |S_\tau| \ll |\mathcal{L}| = |Q| |B|. \]

But clearly \( t \leq \min\{|P|, |Q|\} \) and \( \tau \leq \min\{|A|, |B|\}, \) thus

\[ |P|^{1/2} |Q|^{1/2} \ll \tau^{1/2}. \]

Recalling that \(|Q| \geq |A|\), we arrive at a contradiction. Finally, if the third term in (6.4) dominates, then in view of (6.3) we obtain

\[ |S_\tau| \ll \frac{(|P| |Q| |B|)^2}{(t\tau)^3} \ll \frac{(|P| |Q| |B|)^{3/2}}{(t\tau)^2}. \]

This completes the proof.

By simple summation we get an immediate consequence of the last lemma.

**Corollary 4.** Let \( A \subset \mathbb{F}_p \) be a set such that \( A \subset \text{Sym}_t^+(P, Q), \) where \( P, Q \subset \mathbb{F}_p \) are two other sets and \( \max\{|P|, |Q|\} \geq |A|. \) Then, for any set \( Y, |Y||P||Q| \ll p^2, \)

\[ \mathbb{E}^x(A, Y) \lesssim \frac{(|P| |Q| |Y|)^{3/2}}{t^2}. \]

Using the above results we formulate the main technical proposition in this section.

**Proposition 4.** Let \( A \subset \mathbb{F}_p \) be a set, let \( \delta = |A|/p, \) and let \( \varepsilon \in (0, 1) \) be a real number. Then, for an arbitrary \( B \subset \text{Spec}_\varepsilon(A) \) and any sets \( C, D \subset \mathbb{F}_p \) with

\[ |D||C|^2 |B|^9 \ll \delta \varepsilon^4 p^8, \]

(6.6)
the notation and calculations from there. In particular, we construct two sets $V$ and $B$ holds

$$
\sum_{x \in C} (B \otimes D)^2(x) \lesssim \delta^{-3/8} \varepsilon^{-3/2} |C|^{3/4} |B|^{11/8} |D|^{3/8}
$$

Proof. In our arguments we use the same algorithm as in Proposition 3 and we use the notation and calculations from there. In particular, we construct two sets $U$ and $V$, $U \cup V = B$ with $|U| \lesssim \delta^{-1/4} \varepsilon^{-1} M^{-1/4} |B|^{3/4}$. Using the Cauchy-Schwarz inequality, the norm property of the additive energy (see [25]) and our bound for the size of $U$ we obtain

$$
\sum_{x \in C} (B \otimes D)^2(x) = \sum_{x \in C} ((U \otimes D)(x) + (V \otimes C)(x))^2
$$

$$
\ll \sum_{x \in C} (U \otimes D)^2(x) + \sum_{x \in C} (V \otimes D)^2(x) \lesssim |U|^2 |C| + \left( \sum_{j=1}^{k} (E^\times(Y_j, D))^1/2 \right)^2
$$

$$
\lesssim \delta^{-1/2} \varepsilon^{-2} M^{-1/2} |B|^{3/2} |C| + \sigma^*.
$$

Here $M$ is a parameter which we will choose later. Our task is to find a good upper bound for $\sigma^*$, and to do this we need to bound $E^\times(Y_j, D)$ via Corollary 4 with $A = Y_j$, $Y = D$, $P = P_j$, $Q = U_j$ and $t = q_j$, provided that

$$
|U_j| |P_j| |D| \ll p^2.
$$

We will check this condition later. Notice that

$$
\max \{|U_j|, |P_j|\} \geq |U_j| \geq |Y_j|,
$$

because $Y_j$ is a subset of $U_j$. Thus, applying this corollary, formulae $q_j|Y_j| \sim t_j|P_j|$, $t_j^2|P_j| \sim E^+(U_j)$ and inequality (5.12) we obtain

$$
\sigma^* \lesssim |D|^{3/2} \left( \sum_{j=1}^{k} q_j^{-1} |P_j|^{3/4} |U_j|^{3/4} \right)^2 \lesssim |D|^{3/2} |B|^{3/2} \left( \sum_{j=1}^{k} Y_j^{1/4}(E^+(U_j))^{-1/2} \right)^2
$$

$$
\lesssim |D|^{3/2} |B|^{3/2} \left( \sum_{j=1}^{k} |Y_j|^{1/4}(E^+(U_j))^{-1/2} \right)^2
$$

$$
\lesssim |D|^{3/2} |B|^{3/2} \left( \sum_{j=1}^{k} |Y_j|^2(E^+(U_j))^{-3/4} \right)^2 \lesssim M^{3/2} |D|^{3/2} |B|.
$$

Thus

$$
\sum_{x \in C} (B \otimes D)^2(x) \lesssim \delta^{-1/2} \varepsilon^{-2} M^{-1/2} |B|^{3/2} |C| + M^{3/2} |D|^{3/2} |B|.
$$

The optimal choice of $M$ is

$$
M = |D|^{-3/4} |C|^{1/2} |B|^{1/4} \varepsilon^{-1} \delta^{-1/4},
$$
and hence
\[
\sum_{x \in C} (B \otimes D)^2(x) \lesssim \delta^{-3/8} \varepsilon^{-3/2} |C|^{3/4} |B|^{11/8} |D|^{3/8},
\]
as required.

It remains to check condition (6.8). Because \( |P_j| \lesssim |Y_j|^4 / E^+(U_j) \), we obtain
\[
|U_j||P_j||D| \lesssim |Y_j|^4 |U_j||D| / E^+(U_j) \leq M|D||B|^2
= \varepsilon^{-1} \delta^{-1/4} |D|^{1/4} |C|^{1/2} |B|^{9/4} \ll p^2,
\]
which coincides with (6.6). This completes the proof.

The bound (5.7) is stronger than (6.7) in the case when the size of \( D \) is large compared to \( B \) and \( C \). For very small \( D \) a direct application of Theorem 5 gives the best results.

Now we are ready to prove the second main result in this section.

**Theorem 11.** Let \( \mathcal{E} \) be a finite family of equations of the form (3.1). Also let \( A \subseteq \mathbb{F}_p \) be a set avoiding the family \( \mathcal{E} \) and suppose that \( \mathcal{T}_*(\mathcal{E}) \ll |A|^{38}/p^{30} \). Then, for an arbitrary \( \kappa < 13/58 \),
\[
|A| \ll \frac{p}{\mathcal{T}_*(\mathcal{E})^\kappa} \cdot \left( \frac{E^+(A)}{|A|^3} \right)^{4/29}.
\]  

**Proof.** We use the notation and calculations in Theorems 7 and 9. Returning to (5.17) and squaring we obtain
\[
|A|^{10} t_*^{12} \lesssim p^3 E^+_s(A) \Delta^4 \sum_{r \in B} (W \otimes S^{-1}_*)^2(r).
\]
Here \( \Delta := \varepsilon|A| \leq |A| \) and \( W \subseteq B \) comes from the pigeonhole principle.

Applying Proposition 4 with \( C = B, B = W, D = S^{-1}_*, \varepsilon = \Delta/|A| \) and Parseval’s identity we obtain
\[
|A|^{10} t_*^{13/8} \lesssim p^3 E^+_s(A) \Delta^4 \delta^{-3/8} \left( \frac{|A|}{\Delta} \right)^{3/2} |B|^{3/4} |W|^{11/8}
= p^3 E^+_s(A) |A|^{3/2} \Delta^{5/2} \delta^{-3/8} |B|^{3/4} |W|^{11/8}
\leq p^3 E^+_s(A) |A|^{3/2} (|A|^p)^{5/4} \delta^{-3/8} |B|^{3/4} |W|^{1/8}.
\]

Using the fact that \( |B|, |W| \ll \delta^{-3} \), we have
\[
\delta^{29/4} \lesssim \frac{E^+_s(A)}{|A|^3} \cdot t_*^{-13/8}
\]
or
\[
\delta \lesssim t_*^{-13/58} \cdot \left( \frac{E^+_s(A)}{|A|^3} \right)^{4/29},
\]
as required. We only need to check the condition in Proposition 4, namely,
\[
t_* |B|^2 |W|^{9} \ll \delta^{4} p^8.
\]
Suppose not. Then in view of $|B|, |W| \ll \delta^{-3}$ and $\varepsilon \gg \delta$, we obtain
\[ t_\ast \delta^{-33} \gg \delta^5 p^8, \]
and this contradicts our assumption $t_\ast \ll |A|^{38}/p^{30}$. This completes the proof.

It is easy to see that $E^+(A) = o(|A|^3)$ implies that any set avoiding just one equation has size $o(p)$. Inequality (6.9) can be regarded as a generalization of this fact for several equations.

§ 7. Appendix

In this section we prove Lemmas 1 and 2. We begin with Lemma 1.

**Proof of Lemma 1.** Put $s = |S(\mathcal{E})| = |\mathcal{E}|$ and $t = \mathcal{T}(\mathcal{E})$. Take a maximal subset $J$ of $|\mathcal{E}|$ such that $\{(a_j, b_j, 1) \in \mathcal{E} \}$ and all elements $a_j$ and also all elements $b_j$ are distinct. Clearly, $t \geq |J|$. We set $R = \{(a_j, b_j)\}_{j \in J}$ and $S = \{(a_j, b_j)\}_{j \in [s]}$. By the maximality of $R$ we see that any point in $S$ has either the same abscissa or the same ordinate as a point in $R$. Thus we can split $S \setminus R$ into two sets $S_1$ and $S_2$ and split $R$ into sets $R_1$ and $R_2$ such that any point in $S_1$ and $S_2$ shares a common abscissa or a common ordinate (or both) with some point in $R_1$ and $R_2$, respectively. We split the points in $S \setminus R$ having both a common abscissa and a common ordinate with some points in $R$ in an arbitrary way. Let $r_1 = |R_1|$, $r_2 = |R_2|$, $s_1 = |S_1|$ and $s_2 = |S_2|$. Then, clearly, $r_1 + r_2 = |J|$ and $s_1 + s_2 + r_1 + r_2 = s$. Suppose that $r_1, r_2 > 0$. By averaging arguments there is some point $a_0$ such that the set $\{(a_0, b, 1): (a_0, b) \in S_1\}$ has size at least $s_1/r_1$. Similarly, there is some point $b_0$ such that the set $\{(a, b_0, 1): (a, b_0) \in S_2\}$ has size at least $s_2/r_2$. Without loss of generality, suppose that $s_2/r_2 \leq s_1/r_1$ By a well-known property of the median we have
\[ \frac{s_2}{r_2} \leq \frac{s_1 + s_2}{r_1 + r_2} = \frac{s}{|J|} - 1 \leq \frac{s_1}{r_1}. \]
Hence there is a set $Q$ of the form $Q = \{(a_0, q, 1) \in S\}$ of size $|Q| \geq s/|J| - 1 + 1 = s/|J|$ (we have added a point from $R_1$ to $Q$). If $r_1$ or $r_2$ vanishes then it is easy to see that proving the existence of such $Q$ follows similarly and is even simpler. Finally, the points $(a_0, q, 1)$ in $Q$ are equivalent to $|Q|$ points of the form $\{(a_0q^{-1}, 1, q^{-1})\}$ which have different coordinates in the plane $\{b = 1\}$. Thus, $t \geq s/|J|$. Obviously, $\max_{|J|} \{|J|, s/|J|\} \geq s^{1/2}$ and hence $t \geq s^{1/2}$. This completes the proof.

**Proof of Lemma 2.** Consider the intersection of $\mathcal{E}$ with any of the three planes $\{a = 1\}, \{b = 1\}$ or $\{c = 1\}$, say with $\{c = 1\}$, and put $s = |S(\mathcal{E})| = |\mathcal{E} \cap \{c = 1\}|$. So we can think about $S(\mathcal{E})$ as a subset of $\mathbb{F}_p^* \times \mathbb{F}_p^*$. Take minimal sets $A, B \subseteq \mathbb{F}_p^*$ such that $S(\mathcal{E}) \subseteq A \times B$. We have $s \leq |A||B|$. Clearly, there is an $a_\ast$ such that $\{|a = a_\ast\} \cap S(\mathcal{E})| \geq s/|A|$ and, similarly, there exists a $b_\ast$ with $\{|b = b_\ast\} \cap S(\mathcal{E})| \geq s/|B|$. Put $V = \{a = a_\ast\} \cap S(\mathcal{E})$ and $H = \{b = b_\ast\} \cap S(\mathcal{E})$. If $V \cap H = \emptyset$ then each point in $V \cup H$ either has a unique abscissa or a unique ordinate. Now suppose that $V \cap H = (a_\ast, b_\ast)$. Then it is easy to see that the point $(a_\ast, b_\ast)$ has a unique ratio $a_\ast/b_\ast$, distinct from the ratios for points in $V \cup H$. Thus any point in $V \cup H$ has either a unique abscissa or a unique ordinate or a unique ratio of these. This gives us $\mathcal{T}(\mathcal{E}) \geq s/|A| + s/|B| - 1$. Optimizing the expression $s/|A| + s/|B| - 1$ over $|A|$ and $|B|$ subject to $s \leq |A||B|$, we get $\mathcal{T}(\mathcal{E}) \geq 2|\mathcal{E}|^{1/2} - 1$ as required. The lemma is proved.
Acknowledgements. The author is grateful to Sergey Yekhanin, Tomasz Schoen, Anh Vinh Le and Misha Rudnev for useful discussions. He also thanks the referees for their valuable suggestions and remarks.

Bibliography

[1] E.A. Yazici, B. Murphy, M. Rudnev and I. Shkredov, “Growth estimates in positive characteristic via collisions”, International Mathematics Research Notices 2017:23 (2017), 7148–7189; arXiv:1512.06613v1.

[2] N. Alon and J. Bourgain, “Additive patterns in multiplicative subgroups”, Geom. Funct. Anal. 24:3 (2014), 721–739.

[3] T.F. Bloom, “A quantitative improvement for Roth’s theorem on arithmetic progressions”, J. Lond. Math. Soc. (2) 93:3 (2016), 643–663.

[4] P. Candela and O. Sisask, “On the asymptotic maximal density of a set avoiding solutions to linear equations modulo a prime”, Acta Math. Hungar. 132:3 (2011), 223–243.

[5] S.V. Konyagin and I.D. Shkredov, “On sum sets of sets having small product set”, Modern problems of mathematics, mechanics, and mathematical physics, Collected papers, Tr. Mat. Inst. Steklova, vol. 290, MAIK Nauka/Interperiodica, Moscow 2015, pp. 304–316; English transl. in Proc. Steklov Inst. Math. 290:1 (2015), 288–299.

[6] S.V. Konyagin and I.D. Shkredov, “New results on sum and products in $\mathbb{R}$”, Modern problems of mathematics, mechanics, and mathematical physics. II, Collected papers, Tr. Mat. Inst. Steklova, vol. 294, MAIK Nauka/Interperiodica, Moscow 2016, pp. 87–98; English transl. in Proc. Steklov Inst. Math. 294 (2016), 78–88.

[7] B. Murphy and G. Petridis, A second wave of expanders in finite fields, arXiv: 1701.01635v1.

[8] G. Petridis, Products of differences in prime order finite fields, arXiv: 1602.02142.

[9] O. Roche-Newton, M. Rudnev and I.D. Shkredov, “New sum-product type estimates over finite fields”, Adv. Math. 293 (2016), 589–605.

[10] W. Rudin, Fourier analysis on groups, Reprint of the 1962 original, Wiley Classics Lib., John Wiley & Sons, Inc., New York 1990, x+285 pp.

[11] M. Rudnev, “On the number of incidences between planes and points in three dimensions”, Combinatorica 38:1, 219–254; arXiv:1407.0426v3.

[12] M. Rudnev, I.D. Shkredov and S. Stevens, On the energy variant of the sum-product conjecture, arXiv: 1607.05053v2.

[13] I.Z. Ruzsa, “Solving a linear equation in a set of integers. I”, Acta Arith. 65:3 (1993), 259–282.

[14] I.Z. Ruzsa, “Solving a linear equation in a set of integers. II”, Acta Arith. 72:4 (1995), 385–397.

[15] I.Z. Ruzsa, “Arithmetical progressions and the number of sums”, Period. Math. Hungar. 25:1 (1992), 105–111.

[16] T. Sanders, “On Roth’s theorem on progressions”, Ann. of Math. (2) 174:1 (2011), 619–636.

[17] A. Sárközy, “On sums and products of residues modulo $p$”, Acta Arith. 118:4 (2005), 403–409.

[18] Y.V. Stanchescu, “Planar sets containing no three collinear points and non-averaging sets of integers”, Discrete Math. 256:1–2 (2002), 387–395.
I.D. Shkredov, “On sets of large trigonometric sums”, *Izv. Ross. Akad. Nauk Ser. Mat.* **72**:1 (2008), 161–182; English transl. in *Izv. Math.* **72**:1 (2008), 149–168.

I.D. Shkredov, “On sumsets of dissociated sets”, *Online J. Anal. Comb.*, 2009, no. 4, Art. 4, 26 pp.

I. Shkredov, “Energies and structure of additive sets”, *Electron. J. Combin.* **21**:3 (2014), P3.44, 53 pp.

I.D. Shkredov, “Difference sets are not multiplicatively closed”, *Discrete Anal.*, 2016, 17, 21 pp.

I.D. Shkredov and D. Zhelezov, “On additive bases of sets with small product set”, *International Mathematics Research Notices* **2018**:5, 1585–1599; arXiv: 1606.02320v1.

S. Stevens and F. de Zeeuw, “An improved point-line incidence bound over arbitrary fields”, *Bull. London Math. Soc.* **49** (2017), 842–858; arXiv: 1609.06284v2.

T. Tao and Van H. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., vol. 105, Cambridge Univ. Press, Cambridge 2006, xviii+512 pp.

S. Yekhanin, “A note on plane pointless curves”, *Finite Fields Appl.* **13**:2 (2007), 418–422.

**Ilya D. Shkredov**

Steklov Mathematical Institute of Russian Academy of Sciences, Moscow

E-mail: ilya.shkredov@gmail.com

Received 5/JAN/17 and 1/JUN/17

Translated by I. SHKREDOV