

# Generalized incidence theorems, homogeneous forms and sum-product estimates in finite fields

David Covert, Derrick Hart, Alex Iosevich, Doowon Koh, and Misha Rudnev

June 14, 2011

## Abstract

In recent years, sum-product estimates in Euclidean space and finite fields have been studied using a variety of combinatorial, number theoretic and analytic methods. Erdos type problems involving the distribution of distances, areas and volumes have also received much attention. In this paper we prove a relatively straightforward function version of an incidence results for points and planes previously established in [10] and [12]. As a consequence of our methods, we obtain sharp or near sharp results on the distribution of volumes determined by subsets of vector spaces over finite fields and the associated arithmetic expressions.

In particular, our machinery enables us to prove that if  $E \subset \mathbb{F}_q^d$ ,  $d \geq 4$ , the  $d$ -dimensional vector space over a finite field  $\mathbb{F}_q$ , of size much greater than  $q^{\frac{d}{2}}$ , and if  $E$  is a product set, then the set of volumes of  $d$ -dimensional parallelepipeds determined by  $E$  covers  $\mathbb{F}_q$ . This result is sharp as can be seen by taking  $E$  to equal to  $A \times A \times \cdots \times A$ , where  $A$  is a sub-field of  $\mathbb{F}_q$  of size  $\sqrt{q}$ . In three dimensions we establish the same result if  $|E| \gtrsim q^{\frac{15}{8}}$ . We prove in three dimensions that the set of volumes covers a positive proportion of  $\mathbb{F}_q$  if  $|E| \geq Cq^{\frac{3}{2}}$ . Finally we show that in three dimensions the set of volumes covers a positive proportion of  $\mathbb{F}_q$  if  $|E| \geq Cq^2$ , without any further assumptions on  $E$ , which is again sharp as taking  $E$  to be a 2-plane through the origin shows.

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Focus of this paper	4
1.2	Acknowledgements:	5
<b>2</b>	<b>Statement of results</b>	<b>6</b>
2.1	Generalized geometric incidence estimates:	6
2.2	Distribution of volumes and applications to sums and products	6
<b>3</b>	<b>Proof of the generalized geometric incidence estimate (Theorem 2.1)</b>	<b>7</b>

<b>4</b>	<b>Proof of the volume estimates (Theorem 2.6 and Theorem 2.10)</b>	<b>9</b>
4.1	Elimination of the origin . . . . .	9
4.2	Proof of Theorem 2.10: . . . . .	10
4.3	Proof of Theorem 2.6 . . . . .	11
<b>5</b>	<b>Proof of the key estimate (Lemma 4.2)</b>	<b>12</b>
5.0.1	Proof of Lemma 5.1 and Lemma 5.2: . . . . .	12
5.1	The conclusion of the proof of Lemma 4.2 and Lemma 4.1: . . . . .	13
5.2	Estimation of $I$ : . . . . .	13
5.3	Estimation of $II$ : . . . . .	14
<b>6</b>	<b>Proof of Theorem 2.7 and 2.8</b>	<b>14</b>

# 1 Introduction

The classical Erdős-Szemerédi sum-product problem asks for the smallest possible value of

$$\max\{|A + A|, |A \cdot A|\},$$

where  $A$  is a finite subset of a given ring and  $|\cdot|$  denotes the cardinality of a finite set.

$$A + A = \{a + a' : a, a' \in A\},$$

and

$$A \cdot A = \{a \cdot a' : a, a' \in A\}.$$

In this case when the ring is real numbers, Erdős and Szemerédi conjectured that

$$\max\{|A + A|, |A \cdot A|\} \gtrsim |A|^2,$$

where here and throughout the paper,  $X \lesssim Y$  means that there exists  $C > 0$  such that  $X \leq CY$ . Similarly,  $X \gtrsim Y$ , with respect to the parameter  $N$  means that for every  $\epsilon > 0$  there exists  $C_\epsilon > 0$  such that  $X \leq C_\epsilon N^\epsilon Y$ .

The best known result, in the setting of real numbers,

$$\max\{|A + A|, |A \cdot A|\} \gtrsim |A|^{\frac{14}{11}}$$

is due to Solymosi ([17]), following up on a result due to Elekes ([2]).

In finite fields the problem takes on a flavor of its own due to arithmetic considerations. The first non-trivial result was obtained by Bourgain, Katz and Tao in [4]. For arbitrary fields the best known results to date are

$$\max\{|A + A|, |A \cdot A|\} \gtrsim \min\{|A|^{\frac{1}{2}}q^{\frac{1}{2}}, |A|^2q^{-\frac{1}{2}}\}$$

due to Garaev ([6]). See also [7], [14], [15], [16], [18].

A related problem is to determine how large  $A \subset \mathbb{F}_q$ , the finite field with  $q$  elements needs to be in order to assure that

$$\mathbb{F}_q^* \subset dA^2 = A \cdot A + A \cdot A + \cdots + A \cdot A, \quad (1.1)$$

where  $\mathbb{F}_q^*$  denotes the multiplicative group of  $\mathbb{F}_q$ . Bourgain ([1]) proved that (1.1) holds if  $d = 3$  and

$$|A| \geq Cq^{\frac{3}{4}}.$$

See also [3], [5], [8], [9], and the references contained therein for related results.

The second and the third listed authors developed a combination of geometric and Fourier analytic machinery ([10]) to establish the following result. See also [12], [11] and [13] where this and related machinery is developed in a variety of contexts.

**Theorem 1.1.** *Let  $A \subset \mathbb{F}_q$ , where  $\mathbb{F}_q$  is an arbitrary finite field with  $q$  elements, such that  $|A| > q^{\frac{1}{2} + \frac{1}{2d}}$ . Then*

$$\mathbb{F}_q^* \subset dA^2. \quad (1.2)$$

Moreover, suppose that for some constant  $C_{size}^{\frac{1}{d}}$ ,

$$|A| \geq C_{size}^{\frac{1}{d}} q^{\frac{1}{2} + \frac{1}{2(2d-1)}}.$$

Then

$$|dA^2| \geq q \cdot \frac{C_{size}^{2-\frac{1}{d}}}{C_{size}^{2-\frac{1}{d}} + 1}. \quad (1.3)$$

It follows immediately from Theorem 1.1 that in the case  $d = 2$ ,

$$\mathbb{F}_q^* \subset 2A^2 \text{ if } |A| > q^{\frac{3}{4}},$$

and

$$|2A^2| \geq q \cdot \frac{C_{size}^{\frac{3}{2}}}{C_{size}^{\frac{3}{2}} + 1} \text{ if } |A| \geq C_{size}^{\frac{1}{2}} q^{\frac{2}{3}}.$$

This result was proved as a corollary of the following geometric statement.

**Theorem 1.2.** *Let  $E \subset \mathbb{F}_q^d$  such that  $|E| > q^{\frac{d+1}{2}}$ . Then*

$$\mathbb{F}_q^* \subset \{x \cdot y : x, y \in E\}.$$

Suppose that  $E \subset \mathbb{F}_q^d$  such that  $|E| \geq C_{size}^d q^{\frac{d}{2} + \frac{d}{2(2d-1)}}$ . Suppose, in addition, that  $E$  is a product set. Then

$$|\{x \cdot y : x, y \in E\}| \geq q \frac{C_{size}^{2-\frac{1}{d}}}{1 + C_{size}^{2-\frac{1}{d}}}.$$

The main tool used to establish this result is the following geometric incidence theorem.

**Theorem 1.3.** *Let  $E \subset \mathbb{F}_q^d$  that does not contain the origin. Let*

$$\nu(t) = \sum_{x \cdot y = t} E(x)E(y),$$

where here and throughout the paper,  $E(x)$  denotes the characteristic function of  $E$ . Then

$$\nu(t) = |E|^2 q^{-1} + R(t),$$

where

$$|R(t)| \leq |E| q^{\frac{d-1}{2}}, \text{ if } t \neq 0,$$

and

$$|R(0)| \leq |E| q^{\frac{d}{2}}.$$

Moreover,

$$\begin{aligned} \sum_t \nu^2(t) &\leq |E|^4 q^{-1} \\ &+ |E| q^{2d-1} \sum_k |\widehat{E}(k)|^2 |E \cap l_k|, \end{aligned}$$

where

$$l_k = \{tk : t \in \mathbb{F}_q^*\}.$$

## 1.1 Focus of this paper

The purpose of this paper is to develop the geometric incidence machinery to study the distribution of volumes and to apply the resulting estimates to the sum-product type estimates. More precisely, define  $\text{vol}(x^1, \dots, x^d)$  to be the determinant of the matrix whose rows are  $x^j$ s. Recall that

$$\text{vol}(x^1, \dots, x^d) = x^1 \cdot (x^2 \wedge x^3 \wedge \dots \wedge x^d),$$

where the dot product is defined by the usual formula

$$u \cdot v = u_1 v_1 + u_2 v_2 + \dots + u_d v_d,$$

and the generalized cross product, sometimes called the wedge product, is given by the identity

$$u^2 \wedge \dots \wedge u^d = \det \begin{pmatrix} i \\ u^2 \\ \dots \\ u^d \end{pmatrix},$$

where

$$i = (i_1, i_2, \dots, i_d),$$

indicating the coordinate directions in  $\mathbb{F}_q^d$ . Similarly define

$$\text{vol}(E) = \{\text{vol}(x^1, \dots, x^d) : x^j \in E\}.$$

The question we ask is, under a variety of natural structural assumptions, how large does  $E$  need to be to ensure that  $\mathbb{F}_q^* \subset \text{vol}(E)$ , or, more modestly, that  $\text{vol}(E)$  contains a positive proportion of the elements of  $\mathbb{F}_q$ .

Taking  $E = A \times A \times \dots \times A$ , a product set, will allow us to study some special cases of the following general arithmetic problem. Let

$$\Lambda : (\mathbb{F}_q^d)^D = \mathbb{F}_q^d \times \dots \times \mathbb{F}_q^d \rightarrow \mathbb{F}_q$$

be a multi-homogeneous form in the sense that if  $t_j \in \mathbb{F}_q$ , then

$$\Lambda(t_1 x^1, t_2 x^2, \dots, t_D x^D) = t_1^{k_1} t_2^{k_2} \dots t_D^{k_D} \Lambda(x^1, \dots, x^D).$$

The question we ask is, large does  $A \subset \mathbb{F}_q$  need to be so that

$$\Lambda(A) = \{\Lambda(x^1, \dots, x^D) : x^j \in A \times \dots \times A\} \tag{1.4}$$

contains the whole  $\mathbb{F}_q$ , or at least a positive proportion?

If  $D = 2$  and

$$\Lambda(x^1, x^2) = x^1 \cdot x^2,$$

we are in the realm of Theorem 1.1. If

$$\Lambda(x^1, x^2, \dots, x^d) = x_1^1 \dots x_1^D + \dots + x_d^1 \dots x_d^D,$$

we would be looking at  $DA^d$ , the problem recently studied in [9]. In this paper we illustrate our method by studying the case

$$\Lambda(x^1, \dots, x^d) = \det(x^1, \dots, x^d), \tag{1.5}$$

the determinant of the  $d$  by  $d$  matrix with columns given by  $x^j$ s, though it will be clear that the method applies to a large variety of multi-homogeneous forms.

## 1.2 Acknowledgements:

The third listed author wishes to thank Boris Bukh, Alexei Glibichuk, Sergei Konyagin, Ilya Shkredov, and Jozsef Solymosi for a number of very useful conversations related to the topics covered by this paper during his visit to the Institute for Advanced Study in November, 2007.

## 2 Statement of results

### 2.1 Generalized geometric incidence estimates:

The main tool in our investigation is the following generalized geometric incidence theorem which can be viewed as a functional version of Theorem 1.3.

**Theorem 2.1.** *Let*

$$\nu(t) = \sum_{x \cdot y = t} f(x)g(y),$$

where  $f, g$  are non-negative functions on  $\mathbb{F}_q^d$ . Then

$$\nu(t) = \|f\|_1 \|g\|_1 q^{-1} + R(t), \quad (2.1)$$

where

$$|R(t)| \leq \|f\|_2 \|g\|_2 q^{\frac{d-1}{2}} \text{ if } t \neq 0.$$

Moreover, if  $(0, \dots, 0) \notin \text{support}(f) \equiv E$ , then

$$\begin{aligned} \sum_t \nu^2(t) &\leq \|f\|_2^2 \cdot |E| \cdot \|g\|_1^2 \cdot q^{-1} \\ &+ \|f\|_2^2 \cdot q^{2d-1} \sum_{k \neq (0, \dots, 0)} |\widehat{g}(k)|^2 |E \cap l_k|, \end{aligned} \quad (2.2)$$

where, as before,

$$l_k = \{tk : t \in \mathbb{F}_q^*\}.$$

*Remark 2.2.* The proof of Theorem 2.1 goes through without any essential changes if the dot product  $x \cdot y$  is replaced by any non-degenerate bi-linear form  $B(x, y)$ .

### 2.2 Distribution of volumes and applications to sums and products

Before stating our main results, we need the following definitions.

**Definition 2.3.** We say that  $E \subset \mathbb{F}_q^d$  is *product-like* if given any  $n$ -dimensional sub-space  $H_n \subset \mathbb{F}_q^d$ ,

$$|E \cap H_n| \lesssim |E|^{\frac{n}{d}}.$$

**Definition 2.4.** We say that  $E \subset \mathbb{F}_q^d$  is in *general position* if given any  $n$ -dimensional sub-space  $H_n \subset \mathbb{F}_q^d$ , there exist  $d - n$  linearly independent vectors of  $E$  whose span does not intersect  $H_n$ .

*Remark 2.5.* The meaning of the general position condition is that if  $E \cap H_n$  determines a positive proportion of all the  $n$ -dimensional volumes, then by elementary geometry,  $E$  determines a positive proportion of all the  $d$ -dimensional volumes.

Our main results are the following:

**Theorem 2.6.** *Suppose that  $E \subset \mathbb{F}_q^3$  is product-like. Then*

$$\mathbb{F}_q^* \subset \text{vol}(E) \text{ if } |E| \geq Cq^{\frac{15}{8}} \quad (2.3)$$

with a sufficiently large constant  $C > 0$ .

**Theorem 2.7.** *Suppose that  $E = A \times A \times A$  and  $|A| > \sqrt{q}$ . Then*

$$|\text{vol}(E)| > \frac{q}{2}.$$

**Theorem 2.8.** *Suppose that  $E = A \times A \times A \times A$  and  $|A| > \sqrt{q}$ . Then*

$$\text{vol}(E) = \mathbb{F}_q.$$

*Remark 2.9.* Observe that Theorem 2.7 and Theorem 2.8 are in general sharp. To see this we can simply take  $A$  to be a sub-field. For sharpness examples in the case of prime fields, see [8].

**Theorem 2.10.** *Suppose that  $E \subset \mathbb{F}_q^3$  is in general position and  $|E| \geq Cq^2$  with a sufficiently large constant  $C > 0$ . Then there exists  $c > 0$  such that*

$$|\text{vol}(E)| \geq cq.$$

*Remark 2.11.* The *general position* assumption in Theorem 2.10 is easily removed since any set  $E$  with  $|E| > q^2$  is in general position. The assumption  $|E| \geq Cq^2$  is sharp since a two-dimensional plane that passes through the origin determines exactly one volume- the zero volume.

### 3 Proof of the generalized geometric incidence estimate (Theorem 2.1)

We have

$$\begin{aligned} \nu(t) &= \sum_{x \cdot y = t} f(x)g(y) \\ &= \sum_{x,y} q^{-1} \sum_s \chi(s(x \cdot y - t))f(x)g(y) \end{aligned}$$

$$\begin{aligned}
&= \|f\|_1 \|g\|_1 q^{-1} + q^{-1} \sum_{x,y} \sum_{s \neq 0} \chi(s(x \cdot y - t)) f(x) g(y) \\
&= \|f\|_1 \|g\|_1 q^{-1} + R(t).
\end{aligned}$$

Using the Cauchy-Schwartz inequality,

$$\begin{aligned}
R^2(t) &\leq \|f\|_2^2 \cdot q^{-2} \sum_x \sum_{y,y'} \sum_{s,s' \neq 0} g(y) g(y') \chi(x \cdot (sy - s'y')) \chi(t(s' - s)) \\
&= q^{d-2} \|f\|_2^2 \cdot \sum_{sy=s'y':s,s' \neq 0} g(y) g(y') \chi(t(s' - s)) \\
&= q^{d-2} \|f\|_2^2 \cdot \sum_{s \neq 0} \sum_y g^2(y) + q^{d-2} \|f\|_2^2 \cdot \sum_{sy=s'y';s \neq s';s,s' \neq 0} g(y) g(y') \chi(t(s' - s)) \\
&= q^{d-2} (q-1) \|f\|_2^2 \|g\|_2^2 + q^{d-2} \|f\|_2^2 \cdot \sum_{sy=s'y';s \neq s';s,s' \neq 0} g(y) g(y') \chi(t(s' - s)) \\
&= q^{d-2} (q-1) \|f\|_2^2 \|g\|_2^2 + q^{d-2} \|f\|_2^2 \cdot \sum_{a \neq 0,1} \sum_{b \neq 0} \sum_y g(y) g(ay) \chi(tb(1-a)) \\
&= \|f\|_2^2 \|g\|_2^2 q^{d-2} (q-1) - q^{d-2} \|f\|_2^2 \cdot \sum_{a \neq 0,1} \sum_y g(y) g(ay),
\end{aligned}$$

and the result follows.

To prove the second part of Theorem 2.1, apply Cauchy-Schwartz once again to see that

$$\nu^2(t) \leq \|f\|_2^2 \cdot \sum_{x,y,y':x \cdot y = x \cdot y' = t} E(x) g(y) g(y'),$$

where  $E = \text{support}(f)$ .

It follows that

$$\begin{aligned}
\sum_t \nu^2(t) &\leq \|f\|_2^2 \cdot \sum_{x \cdot y = x \cdot y'} E(x) g(y) g(y') \\
&= \|f\|_2^2 q^{-1} \sum_{x,y,y'} \sum_s \chi(s(x \cdot y - x \cdot y')) E(x) g(y) g(y') \\
&= \|f\|_2^2 q^{-1} |E| \|g\|_1^2 + \|f\|_2^2 q^{2d-1} \sum_{s \neq 0} \sum_x |\widehat{g}(x)|^2 E(sx) \\
&= \|f\|_2^2 q^{-1} |E| \|g\|_1^2 + \|f\|_2^2 q^{2d-1} \sum_x |\widehat{g}(x)|^2 |E \cap l_x|,
\end{aligned}$$

as desired.



## 4 Proof of the volume estimates (Theorem 2.6 and Theorem 2.10)

Let  $f(x) = E(x)$  and define

$$g_0(x) = |\{(u^2, u^3) \in E \times E : u^2 \wedge u^3 = x\}|.$$

Observe that

$$\|f\|_1 = \|f\|_2^2 = |E|. \quad (4.1)$$

On the other hand,

$$\|g_0\|_1 = |E|^2. \quad (4.2)$$

Let

$$\nu(t) = |\{(x^1, x^2, x^3) \in E \times E \times E : \text{vol}(x^1, x^2, x^3) = t\}|$$

and observe that it equals

$$\sum_{x \cdot y = t} f(x)g_0(y),$$

where  $f$  and  $g_0$  are as above.

### 4.1 Elimination of the origin

Let  $g(x) = g_0(x)$  if  $x \neq (0, 0, 0)$  and 0 otherwise. The argument below is simplified considerably if we work with  $g$  instead of  $g_0$ . We may work with  $g$  provided that we show that

$$\sum g(x) \gtrsim |E|^2.$$

To do this, it suffices to show that

$$g_0(0, 0, 0) \leq c|E|^2$$

for some  $0 < c < 1$ . Indeed,

$$\begin{aligned} g_0(0, 0, 0) &= |\{(u^2, u^3) \in E \times E : u^2 \wedge u^3 = (0, 0, 0)\}| \\ &\leq |E| \cdot \max_{H_1} |E \cap H_1|, \end{aligned}$$

where the maximum is taken over all the 1-dimensional sub-spaces of  $\mathbb{F}_q^3$ . If  $E$  is product-like, then

$$|E \cap H_1| \lesssim |E|^{\frac{1}{3}}$$

and so

$$g_0(0, 0, 0) \lesssim |E|^{2-\frac{2}{3}} \ll |E|^2.$$

On the other hand, if

$$|E \cap H_n| \lesssim q^{\frac{n+1}{2}} \quad (4.3)$$

for every  $n$ -dimensional sub-space  $H_n$ , then

$$|E \cap H_1| \lesssim q,$$

so

$$g_0(0, 0, 0) \leq |E|q,$$

and this quantity is much smaller than  $|E|^2$  if  $|E|$  is much larger than  $q$ .

Throughout the argument below we shall either prove results about product-like sets, or sets where the condition (4.3) can be inductively assumed. Thus the origin has indeed been eliminated from the domain of  $g_0$  without any harm.

In the arguments below, we shall work with  $g_{H_n}$ , defined just like  $g$  with respect to sub-spaces  $H_n$ . We also define  $g_H$  to be 0 at the origin as we do not need to worry about the lower bound in this case.

## 4.2 Proof of Theorem 2.10:

We shall need the following estimate, proved in a subsequent section.

**Lemma 4.1.** *Suppose that  $E \subset \mathbb{F}_q^3$  such that  $|E| \gtrsim q^2$  and  $|E \cap H_n| \lesssim q^{\frac{n+1}{2}}$  for every  $n$ -dimensional sub-space  $H_n$ . Then*

$$\|g\|_2^2 \lesssim |E|^2 q^2.$$

The result holds in two dimensions by Theorem 1.2. We may assume that for any sub-space  $H_n$ ,

$$|E \cap H_n| \lesssim q^{\frac{n+1}{2}}$$

for  $1 \leq n \leq 2$  for otherwise the induction hypothesis would imply that we recover a positive proportion of all the  $n$ -dimensional volumes and the definition of general position would then imply that we recover the positive proportion of all the  $d$ -dimensional volumes. Thus the assumptions of Lemma 4.1 are satisfied and we see using Cauchy-Schwartz that

$$|E|^6 = \left( \sum_t \nu(t) \right)^2 \leq |\text{vol}(E)| \cdot \sum_t \nu^2(t). \quad (4.4)$$

By Theorem 2.1, keeping in mind that  $E$  is not assumed to be product-like, followed by Lemma 4.1 we see that

$$\sum_t \nu^2(t) \lesssim |E|q^3 \|g\|_2^2$$

$$\lesssim |E|q^3 \cdot q^2|E|^2.$$

Inserting this back into (4.4) we see that

$$|\text{vol}(E)| \gtrsim \frac{|E|^6}{|E|^3q^5} = \frac{|E|^3}{q^5}.$$

This expression is  $\gtrsim q$  if

$$|E| \gtrsim q^2,$$

as desired. This completes the proof of Theorem 2.10.

### 4.3 Proof of Theorem 2.6

We shall need the following estimate proved in a subsequent section.

**Lemma 4.2.** *Suppose that  $E \subset \mathbb{F}_q^3$  is product-like. Then*

$$\|g\|_2^2 \lesssim |E|^{\frac{7}{3}}q.$$

Applying the estimate (2.1) of Theorem 2.1 we see that if  $t \neq 0$ , then

$$\nu(t) = |E|^3q^{-1} + R(t),$$

where

$$|R(t)| \leq q|E|^{\frac{1}{2}} \cdot \|g\|_2.$$

By Lemma 4.2,

$$|R(t)|^2 \lesssim q^3|E|^{3+\frac{1}{3}},$$

provided that

$$|E| \lesssim q^2.$$

It follows that  $\nu(t) > 0$  if

$$|E|^{\frac{8}{3}} \geq Cq^5$$

with a sufficiently large constant  $C > 0$ . It follows that  $\nu(t) > 0$  if

$$|E| \geq Cq^{\frac{15}{8}},$$

which completes the proof of the point-wise estimate.

## 5 Proof of the key estimate (Lemma 4.2)

We shall make use of the following calculations.

**Lemma 5.1.** *Let  $E \subset \mathbb{F}_q^3$  be product-like. Let  $H_2$  be a 2-dimensional subspace of  $\mathbb{F}_q^3$ . Then*

$$\sum_{H_2} |E \cap H_2|^2 \lesssim |E|^2 \quad (5.1)$$

provided that

$$|E| \gtrsim q^{\frac{3}{2}}.$$

**Lemma 5.2.** *Let  $E \subset \mathbb{F}_q^3$ . Let  $H_2$  be an 2-dimensional sub-space of  $\mathbb{F}_q^3$ . Then*

$$\sum_{H_2} |E \cap H_2|^2 \lesssim |E|^2 \quad (5.2)$$

provided that

$$|E| \gtrsim q^2.$$

### 5.0.1 Proof of Lemma 5.1 and Lemma 5.2:

To prove the estimate (5.1), observe that

$$\begin{aligned} \sum_{H_2} |E \cap H_2|^2 &= (q-1)^{-1} \sum_x \left( \sum_{x \cdot y=0} E(y) \right)^2 \\ &= (q-1)^{-1} \sum_{x \in \mathbb{F}_q^3} \prod_{j=1}^2 \sum_{x \cdot y^j=0} E(y^j). \end{aligned}$$

If  $E$  is product-like, then this expression is

$$\lesssim |E|^2 + q|E|^{\frac{4}{3}} \lesssim |E|^2 \quad (5.3)$$

if  $|E| \geq Cq^{\frac{3}{2}}$ , as claimed.

Under the assumptions of Lemma 5.2, this expression is

$$\lesssim |E|^2 + q^2 \cdot |E| \lesssim |E|^2 \quad (5.4)$$

if  $|E| \geq Cq^2$ , as desired.

In both (5.3) and (5.4) we use the fact that if  $y^1, y^2$  span the 1-dimensional sub-space,

$$|\{x : x \cdot y^j = 0; j = 1, 2\}| \approx q^2.$$

In order to establish (5.3) we also use the fact that the restriction of  $E$  to a 1-dimensional subspace has size  $\lesssim |E|^{\frac{1}{3}}$ , whereas in the general case we simply use the fact that the size of this intersection does not exceed  $q$ . This completes the proof of the estimate (5.1) and (5.2).

## 5.1 The conclusion of the proof of Lemma 4.2 and Lemma 4.1:

We have

$$\begin{aligned} \|g\|_2^2 &\lesssim \sum_j \sum_{H_2 \in G_0(2,3)} \nu_{H_2}^2(j) \\ &\lesssim \sum_{H_2} |E \cap H_2|^4 q^{-1} + II, \end{aligned} \quad (5.5)$$

where

$$I = \sum_{H_2} |E \cap H_2|^4 q^{-1}$$

and

$$II = II_{prod} \lesssim |E|^{\frac{1}{3}} \sum_{H_2} |E \cap H_2| q \|g_{H_2}\|_{L^2(H_2)}^2 \quad (5.6)$$

if  $E$  is product-like and

$$II = II_{generic} \lesssim q \sum_{H_2} |E \cap H_2| q \|g_{H_2}\|_{L^2(H_2)}^2 \quad (5.7)$$

if  $E$  is in general position.

## 5.2 Estimation of $I$ :

Suppose that  $E$  is product like and  $|E| \gtrsim q^{\frac{3}{2}}$ . Since

$$|E \cap H_2|^2 \lesssim |E|^{\frac{4}{3}}$$

due to the fact that  $E$  is a product set and  $H$  is a 2-dimensional plane, Lemma 5.1 gives us

$$\begin{aligned} I &\lesssim q^{-1} |E|^{\frac{4}{3}} \cdot |E|^2 \\ &\lesssim |E|^{\frac{7}{3}} q \end{aligned}$$

as long as

$$|E| \lesssim q^2$$

as desired.

If  $E$  is in general position,

$$|E \cap H_2|^2 \lesssim q^3,$$

so

$$I \lesssim q^{-1} q^3 |E|^2$$

by Lemma 5.2.

### 5.3 Estimation of $II$ :

Since  $g_{H_2}$  is simply the characteristic function of  $E \cap H_2$ , Lemma 5.1 implies that

$$\| \cdot \|_{\text{prod}} \lesssim q|E|^{\frac{7}{3}},$$

if  $|E| \gtrsim q^{\frac{3}{2}}$ , as desired.

Similarly, Lemma 5.2 implies that

$$II_{\text{generic}} \lesssim q^2|E|^2,$$

if  $|E| \gtrsim q^2$  and we are done.

## 6 Proof of Theorem 2.7 and 2.8

We shall use the following lemmata. See [4] and [8]

**Lemma 6.1.** *Suppose,  $A \subset \mathbb{F}_q^*$  is such that  $|A|^2 > q$ . Then there exist elements  $\alpha, \beta \in A - A$ , such that*

$$|\alpha A \pm \beta A| > \frac{q}{2}. \quad (6.1)$$

**Lemma 6.2.** *If  $C \subset \mathbb{F}_q$  is such that  $|C| > \frac{q}{2}$ , then  $C \pm C = \mathbb{F}_q$ .*

Using Lemma 6.1, we have the following.

**Lemma 6.3.** *Suppose,  $A \subset \mathbb{F}_q^*$  is such that  $|A|^2 > q$ . Let  $B = A - A$ . Then  $B^2 - B^2 = \mathbb{F}_q$ .*

*Proof.* The claim is that the set  $D$  of two by two determinants

$$\begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}$$

with elements in  $B$  cover  $\mathbb{F}_q$ . Let us fix  $x_1 = \alpha$ ,  $x_2 = \beta$ , from Lemma 6.1, which are determined by  $A$  only. Let  $y_1 = u_1 - v_1$ ,  $y_2 = u_2 - v_2$ , where  $u_1, v_1, u_2, v_2 \in A$ . Let  $C = \alpha A - \beta A$ . We have

$$D = C - C,$$

and the result follows from the fact that  $|C| > \frac{q}{2}$  by Lemma 6.1 and Lemma 6.2.

We are now ready to prove Theorem 2.8. Consider the determinants in the form

$$\begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ u_1 & u_2 & x_3 & x_4 \\ v_1 & v_2 & y_3 & y_4 \end{vmatrix} = \begin{vmatrix} x_1 - u_1 & x_2 - u_2 & 0 & 0 \\ y_1 - v_1 & y_2 - v_2 & 0 & 0 \\ u_1 & u_2 & x_3 & x_4 \\ v_1 & v_2 & y_3 & y_4 \end{vmatrix}$$

$$= (x_3y_4 - y_3x_4) \begin{vmatrix} x_1 - u_1 & x_2 - u_2 \\ y_1 - v_1 & y_2 - v_2 \end{vmatrix}.$$

The statement now follows from Lemma 6.3.

We now prove Theorem 2.7. Consider the determinants in the form

$$\begin{aligned} \begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ u_1 & u_2 & u_3 \end{vmatrix} &= \begin{vmatrix} x_1 - u_1 & x_2 - u_2 & 0 \\ y_1 & y_2 & y_3 \\ u_1 & u_2 & u_3 \end{vmatrix} \\ &= (x_1 - u_1)(y_2u_3 - y_3u_2) - (x_2 - u_2)(y_1u_3 - y_3u_1) \\ &= u_3[(x_1 - u_1)y_2 - (x_2 - u_2)y_1] - y_3[(x_1 - u_1)u_2 - (x_2 - u_2)u_1] \end{aligned}$$

Let  $(x_1 - u_1) = \alpha$ ,  $(x_2 - u_2) = \beta$  come from Lemma 6.1, having therefore fixed  $x_1, u_1, x_2, u_2$ . Now fix  $u_3 \neq 0$ , and some  $y_3$ . The statement now follows from Lemma 6.1.

## References

- [1] J. Bourgain, *Exponential sum estimate revisited*, JAMS **18** (2) (2005) 477-499. [3](#)
- [2] G. Elekes, On the number of sums and products. *Acta Arith.*, 81(4) 365-367, (1997). [2](#)
- [3] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) **73** (2006), 380-398. [3](#)
- [4] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Func. Anal. **14** (2004) 27-57. [2](#), [14](#)
- [5] E. Croot, *Sums of the Form  $1/x_1^k + \dots + 1/x_n^k$  modulo a prime*, Integers **4** (2004). [3](#)
- [6] M. Garaev, *An explicit sum-product estimate in  $\mathbb{F}_p$* , (preprint), (2007). [3](#)
- [7] M. Garaev, *The sum-product estimate for large subsets of prime fields*, (preprint), (2007). [3](#)
- [8] A. A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime and the Erdős-Graham problem*, Mat. Zametki, **79** (2006), 384-395; translation in: Math. Notes **79** (2006), 356-365. [3](#), [7](#), [14](#)
- [9] A. Glibichuk and S. Konyagin, *Additive properties of product sets in fields of prime order*, Centre de Recherches Mathematiques, Proceedings and Lecture Notes, (2006). [3](#), [5](#)
- [10] D. Hart and A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*, Contemporary Mathematics (to appear), (2007). [1](#), [3](#)
- [11] D. Hart, A. Iosevich, J. Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Notices (2007) Vol. 2007, article ID rmn007, 14 pages. [3](#)
- [12] D. Hart, A. Iosevich, D. Koh and M. Rudnev *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture*, submitted for publication (2007). [1](#), [3](#)
- [13] A. Iosevich and M. Rudnev. *Erdős distance problem in vector spaces over finite fields*. Trans. Amer. Math. Soc. (2007). [3](#)
- [14] N. Katz and C. Shen, *A Slight Improvement to Garaev's Sum Product Estimate*, (preprint), (2007). [3](#)



- [15] N. Katz and C. Shen, *Garaev's Inequality in finite fields not of prime order*, (preprint), (2007). [3](#)
- [16] I. Shparlinski, *On The Solvability of Bilinear Equations in Finite Fields*, (preprint), (2007) [3](#)
- [17] J. Solymosi, *On the number of sums and products*, Bull. London Math. Soc. **37** (2005) 491-494. [2](#)
- [18] V. Vu, *Sum-Product estimates via directed expanders*, (preprint), (2007). [3](#)