Solution of the Erdős-Falconer distance conjecture for subsets of the sphere and sum-product theory in vector spaces over finite fields

Derrick Hart, Alex Iosevich, Doowon Koh and Misha Rudnev

July 5, 2007

Abstract

We prove a point-wise and average bound for the number of incidences between points and hyper-planes in vector spaces over finite fields. While our estimates are, in general, sharp, we observe an improvement for product sets and sets contained in a sphere. We use these incidence bounds to obtain significant improvements on the arithmetic problem of covering $\mathbb{F}^q$, the finite field with q elements, by $A \cdot A + \cdots + A \cdot A$, where A is a subset $\mathbb{F}_q$ of sufficiently large size. We use similar machinery to prove the Erdős-Falconer distance conjecture for subsets of the unit sphere.

Contents

1 Introduction

Let $A \subset \mathbb{F}_q$. How large does A need to be to make sure that

$$dA^2 = A^2 + A^2 + \cdots + A^2 = \mathbb{F}_q,$$

where

$$A^2 = \{a \cdot a' : a, a' \in A\}.$$

It is known (see e.g. [9]) that if $d = 3$ and q is prime, this conclusion is assured if $|A| \geq Cq^{\frac{3}{4}}$, with a sufficiently large constant $C > 0$. It is reasonable to conjecture that if $|A| \geq C_\epsilon q^{\frac{1}{2}+\epsilon}$, then $2A^2 = \mathbb{F}_q$. This result cannot hold, especially in the setting of general finite fields if $|A| = \sqrt{q}$ because A may in fact be a subfield. See also [1], [3], [8], [7], [11], [13], [16], [17] and the references contained therein on recent progress related to this problem and its analogs.

For example, it is proved in [8] that

$$8X \cdot Y = \mathbb{Z}_p,$$

p prime, provided that $|X||Y| > p$ and either $Y = -Y$ or $Y \cap (-Y) = \emptyset$. In [9] the author proves that if A is subgroup of $\mathbb{Z}_p^*$, and $|A| > p^\delta$, $\delta > 0$, then

$$NA = \mathbb{Z}_p$$

with

$$N \leq C4^{\frac{1}{\delta}}.$$

The purpose of this paper is to use the geometry of $\mathbb{F}_q^d$, where q is not necessarily a prime number, to deduce a good lower bound on the size of A that guarantees that $dA^2 = \mathbb{F}_q$, with the possible exception of 0.

A seemingly different problem is the following question that we shall henceforth refer to as the The Erdős distance conjecture which says that if A is a finite subset of $\mathbb{R}^d$, $d \geq 2$, then $|\Delta(A)| \geq C_\epsilon |A|^{\frac{2}{d}-\epsilon}$, where $\Delta(A) = \{|x-y| : x, y \in A\}$, $|\cdot|$ denotes the standard Euclidean metric, and $|A|$ denotes the number of elements in A. This problem is far from resolution in any dimension in spite of much excellent work over the past 60 years. See, for example, a beautiful monograph by Matousek ([14]) and the references contained therein.

The Falconer distance conjecture says that if $E \subset \mathbb{R}^d$, $d \geq 2$, has Hausdorff dimension $> \frac{d}{2}$, then $\Delta(E) = \{|x-y|, x, y \in E\}$, has positive Lebesgue measure. See [4] for the latest progress and description of techniques. For the connections between this problem and its discrete predecessor, the Erdős distance conjecture, see, for example, [6].

In the finite field setting the question turns out to have features of both the Erdős and Falconer distance problems. The first non-trivial result was obtained by Bourgain, Katz and Tao, using combinatorial methods.

Theorem 1.1. *Suppose $E \subset \mathbb{F}_q^2$, $q \equiv 3 \mod 4$, q a prime, and $|E| \lesssim q^{2-\epsilon}$. Then there exists $\delta = \delta(\epsilon)$ such that*

$$|\Delta(E)| \gtrsim |E|^{\frac{1}{2}+\delta}.$$

Here

$$\Delta(E) = \{(x_1-y_1)^2 + (x_2-y_2)^2 : x, y \in E\}.$$

It is interesting to observe that while the quantity we are using is not a distance, in the traditional sense, it is still a natural object in that it is invariant under the action of orthogonal matrices.

We note that the conclusion of Theorem 1.1 with the exponent $\frac{1}{2}$ follows from the argument due to Erdős ([5]). The condition $|E| \lesssim q^{2-\epsilon}$ addresses the fact that if $E = \mathbb{F}_q^2$, then $\Delta(E) = \mathbb{F}_q$ and so $|\Delta(E)| = \sqrt{|E|}$ and no better. The condition $q \equiv 3 \mod 4$ addresses an even nastier fact that if $q \equiv 1 \mod 4$, the field $\mathbb{F}_q$ contains $\sqrt{-1}$, the number i such that $i^2 = -1$. This would allow one to take

$$E = \{(t, it) : t \in \mathbb{F}_q\}$$

and it is straightforward to check that while $|E| = q$, $|\Delta(E)| = 1$ as all the distances between the elements of the set are identically 0.

In view of the examples cited in the previous paragraph, the second and the third author ([12]) formulated the Erdős-Falconer conjecture as follows.

Conjecture 1.2. *Let $E \subset \mathbb{F}_q^d$ such that $|E| \geq C_\epsilon q^{\frac{d}{2}+\epsilon}$. Then there exists $c > 0$ such that*

$$|\Delta(E)| \geq cq.$$

They also established a Fourier analytic approach to this problem and proved the following result.

Theorem 1.3. *Suppose that $E \subset \mathbb{F}_q^d$ and $|E| \geq 4q^{\frac{d+1}{2}}$. Then $\Delta(E) = \mathbb{F}_q$.*

In the regime when $q << |E| << q^2$, this provides a quantitatively explicit result which, moreover, holds in higher dimensions, guarantees all distances in some ranges of

exponents, and is not limited to fields with prime base. The key tool in the proof is Weil's bound ([18]) for Kloosterman sums,

$$\left|\sum_{t\neq 0}\chi(at+t^{-1})\right| \leq 2\sqrt{q},$$

where χ is a non-trivial additive character.

In this paper we prove Conjecture 1.2 for subsets of the sphere

$$S = \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2 = 1\}.$$

Our proofs are based on the same incidence technology (see Theorem 2.1 below) that we use to obtain the arithmetic results mentioned above.

2 Statement of results

2.1 Key incidence estimate

Our main tool is the following incidence theorem. See [10] for an earlier version.

Theorem 2.1. *Let $E \subset \mathbb{F}_q^d$ and define*

$$\nu(t) = \{(x,y) \in E \times E : x \cdot y = t\}.$$

Then

$$\sum_t \nu^2(t) \leq |E|^4 q^{-1} + |E| q^{2d-1} \sum_{k \in \mathbb{F}_q^d} |E \cap l_k| \left|\widehat{E}(k)\right|^2 - q^{d-1}|E|^2 E(0,\ldots,0), \tag{2.1}$$

where

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

Moreover,

$$\nu(t) = |E|^2 q^{-1} + R(t), \tag{2.2}$$

with

$$|R(t)| \leq |E| q^{\frac{d-1}{2}}.$$

Note that by a common abuse of notation, $E(x)$ denotes the characteristic function of E, so $E(0,\ldots,0) = 1$ if the origin is in E and 0 otherwise. Also note that in many of the applications below it is legitimate to assume, without loss of generality, that E does not in fact contain the origin.

Remark 2.2. There are parallels here that are worth pointing out. In the study of the Euclidean Falconer conjecture, the L^2 norm of the distance measure is dominated by the Mattila integral, discovered by P. Mattila,

$$\int_1^\infty \left(\int_{S^{d-1}} |\widehat{\mu}(t\omega)|^2 d\omega \right)^2 t^{d-1} dt,$$

where μ is a Borel measure on the set E whose distance set is being examined. It is reasonable to view the expression

$$\sum_{k \in \mathbb{F}_q^d} |E \cap l_k| |\widehat{E}(k)|^2$$

as the Mattila integral for the dot product problem, a direct analog of the Mattila integral for the distance set problem in the Euclidean space.

Corollary 2.3. *Let $E \subset \mathbb{F}_q^d$ such that $|E| > q^{\frac{d+1}{2}}$. Then*

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

Moreover, the result cannot in general be improved in the sense that for any $\epsilon > 0$ there exists $E \subset \mathbb{F}_q^d$ of size $\approx q^{\frac{d+1}{2}-\epsilon}$, such that $|\{x \cdot y : x, y \in E\}| = o(q)$. In particular, the set of dot products does not contain a positive proportion of the elements of $\mathbb{F}_q$.

Remark 2.4. As the reader shall see, our proof of the arithmetic and geometric results below is based, in large part, on the fact that Corollary 2.3 is improvable for sets possessing special structure, such as product sets or sets contained in a sphere. However, for general sets, the exponent $\frac{d+1}{2}$ is impassable.

2.2 Arithmetic results

Theorem 2.5. *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*

$$\mathbb{F}_q^* \subset dA^2. \tag{2.3}$$

Suppose that

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

Then

$$|dA^2| \geq q \cdot \frac{C_{size}^{2-\frac{1}{d}}}{C_{size}^{2-\frac{1}{d}} + 1}. \tag{2.4}$$

In particular, if $d = 2$,

$$\mathbb{F}_q^* \subset A^2 + A^2$$

if

$$|A| > q^{\frac{3}{4}},$$

and

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

if

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

Theorem 2.6. *Let $A \subset \mathbb{F}_q$, with $|A| \geq C_{size}^{\frac{1}{2}} q^{\frac{1}{2}}$, and suppose that*

$$|(A \times A) \cap t(A \times A)| \leq C_{uni} |A|^2 q^{-1} \tag{2.5}$$

for all $t \neq 1$.

Then

$$|2A^2| \geq q \cdot \frac{C_{size}}{2C_{size} + C_{uni}}.$$

2.3 Distance set results

Theorem 2.7. *Let $E \subset \mathbb{F}_q^d$, $d \geq 3$, be a subset of the sphere $S = \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2 = 1\}$. Suppose that $|E| \geq Cq^{\frac{d}{2}}$ with a sufficiently large constant C. Then there exists $c > 0$ such that*

$$|\Delta(E)| \geq cq.$$

We obtain a much stronger result under the assumption that E is suitably well-distributed.

Definition 2.8. Let $E \subset S = \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2 = 1\}$. Suppose that

$$|E \cap (S \cap H)| \leq C|E|q^{-1}$$

for every $(d-1)$-dimensional hyper-plane H passing through the origin. Then we say that E is uniformly distributed on the sphere.

Theorem 2.9. *Suppose that E is uniformly distributed on the sphere and that $|E| \geq Cq$. Then*

$$|\Delta(E)| \geq cq. \tag{2.6}$$

2.4 Acknowledgements:

The authors wish to thank Luca Brandolini, Leoardo Colzani, Giaccomo Gigante, Nets Katz, Sergei Konyagin, Seva Lev, Igor Shparlinsky and Ignacio Uriarte-Tuero for many helpful remarks about the content of this paper.

3 Geometric estimates: Proof of Theorem 2.1 and Corollary 2.3

3.1 Proof of the L^2 estimate (2.1):

To this end let

$$\begin{aligned}\nu(t) &= \{(x,y) \in E^2 : x \cdot y = t\} \\ &= \sum_{x \cdot y = t} E(x)E(y).\end{aligned}$$

The Cauchy-Schwartz inequality applied to the sum in x yields

$$\sum_t \nu^2(t) \leq |E| \cdot \sum_t \sum_{x \cdot y = t} \sum_{x \cdot y' = t} E(x)E(y)E(y')$$

$$= |E| \sum_{(x-y)\cdot k = 0} E(x)E(y)E(k)$$

$$= |E| q^{-1} \sum_{x,y,k} \sum_s \chi(s((x-y)\cdot k))E(x)E(y)E(k)$$

$$= |E|^4 q^{-1} + |E| q^{2d-1} \sum_k \sum_{s \neq 0} E(sk) \left|\widehat{E}(k)\right|^2$$

$$= |E|^4 q^{-1} + |E| q^{2d-1} \sum_k |E \cap l_k| \left|\widehat{E}(k)\right|^2 - q^{d-1}|E|^2 E(0,\ldots,0),$$

where we go from third line to fourth by changing variables in k and then in s. This completes the proof of the estimate (2.1).

3.2 Proof of the point-wise estimate (2.2):

Let

$$\nu(t) = |\{(x,y) \in E \times E : x \cdot y = t\}|.$$

We have

$$\nu(t) = \sum_{x,y \in E} q^{-1} \sum_{s \in \mathbb{F}_q} \chi(s(x \cdot y - t)),$$

where χ is a non-trivial additive character on $\mathbb{F}_q$. It follows that

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

where

$$R = \sum_{x,y \in E} q^{-1} \sum_{s \neq 0} \chi(s(x \cdot y - t)).$$

Viewing R as a sum in x, applying the Cauchy-Schwartz inequality and dominating the sum over $x \in E$ by the sum over $x \in \mathbb{F}_q^d$, we see that

$$R^2 \leq |E| \sum_{x \in \mathbb{F}_q^d} q^{-2} \sum_{s,s' \neq 0} \sum_{y,y' \in E} \chi(sx \cdot y - s'x \cdot y')\chi(t(s' - s)).$$

Orthogonality in the x variable yields

$$= |E| q^{d-2} \sum_{\substack{sy = s'y' \\ s,s' \neq 0}} \chi(t(s' - s))E(y)E(y').$$

If $s \neq s'$ we may set $a = s/s', b = s'$ and obtain

$$|E| q^{d-2} \sum_{\substack{y \neq y' \\ ay = y' \\ a \neq 1, b}} \chi(tb(1-a))E(y)E(y')$$

$$= -|E| q^{d-2} \sum_{y \neq y', a \neq 1} E(y)E(ay),$$

and the absolute value of this quantity is

$$\leq |E| q^{d-2} \sum_{y \in E} |E \cap l_y|$$

$$\leq |E|^2 q^{d-1},$$

since

$$|E \cap l_y| \leq q$$

by the virtue of the fact that each line contains exactly q points.

If $s = s'$ we get

$$|E| q^{d-2} \sum_{s,y} E(y) = |E|^2 q^{d-1}.$$

It follows that

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

where

$$R^2(t) \leq -Q(t) + |E|^2 q^{d-1},$$

with

$$Q(t) \geq 0.$$

It follows that

$$R^2(t) \leq |E|^2 q^{d-1},$$

so

$$|R(t)| \leq |E| q^{\frac{d-1}{2}}. \tag{3.1}$$

We conclude that

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

with $|R(t)|$ bounded as in (2.2).

3.3 Proof of sharpness of Corollary 2.3

We now turn our attention to the Corollary 2.3. Let us consider the case $d = 2$ and $q = p^2$, where p is a power of an odd prime. The higher dimensional case follows similarly. Let a be a generator of the cyclic group $\mathbb{F}_q^*$. Then $a^{q-1} = 1$ and a^{p+1} is the generating element for $\mathbb{F}_q^*$ since $p + 1 = \frac{q-1}{p-1}$.

Let A be a proper cyclic subgroup of $\mathbb{F}_q^*$ which properly contains $\mathbb{F}_p^*$. Let s a divisor of $p + 1$ and let the generating element of A be $\alpha = a^s$. Note that we are taking advantage of the fact that $\mathbb{F}_q^*$ is cyclic. Consider the unit circle

$$\{x \in \mathbb{F}_q^2 : x_1^2 + x_2^2 = 1\},$$

and its subset

$$C_p = \{x \in \mathbb{F}_p^2 : x_1^2 + x_2^2 = 1\}.$$

By elementary number theory, the cardinality of C_p is $p \pm 1$, depending on whether negative one is or is not a square in $\mathbb{F}_p^*$. By a direct calculation, for any $u, v \in C_p$, $u \cdot v \in \mathbb{F}_p^*$. Let

$$E = \{tu : t \in A, u \in C\}. \tag{3.2}$$

For any $x, y \in E$, the dot product $x \cdot y$, if nonzero, will lie in A. Indeed, if $x = tu$, $y = \tau v$, according to (3.2), then

$$x \cdot y = t\tau(u \cdot v) \in A \cup \{0\},$$

since A contains $\mathbb{F}_p^*$. The cardinality of E is

$$|E| = \frac{p \pm 1}{2}|A| = \frac{p \pm 1}{2} \cdot \frac{q-1}{s},$$

where s is a divisor of $p+1$. Taking $s=2$ works and shows that less than half the elements of $\mathbb{F}_q^*$ may be realized as dot products determined by a set of size $\geq \frac{1}{4} \cdot |E|^{\frac{3}{2}}$. In order to see that $\{x \cdot y : x, y \in E\}$ does not in general even contain a positive proportion of the elements of $\mathbb{F}_q$ if $|E| << q^{\frac{3}{2}}$, we need to produce a sequence of primes, or prime power, such that $p+1$ has large divisors. To do this, consider the family of prime powers

$$\{p^{2k+1} : k = 1, 2 \dots\}$$

and observe that

$$p+1 \mid p^{2k+1}+1.$$

This completes the proof.

4 Proof of the main arithmetic result (Theorem 2.5)

Let $E = A \times A \times \cdots \times A$. The proof of the first part of Theorem 2.5 follows instantly from the estimate (2.2). To prove the second part observe that

$$|E \cap l_y| \leq |A| = |E|^{\frac{1}{d}}$$

for every $y \in E$. Using this, the estimate (2.1) implies that

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

and, consequently, that

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

if

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

It follows that if

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

then

$$|dA^2| \geq q \cdot \frac{C_{size}^{2-\frac{1}{d}}}{C_{size}^{2-\frac{1}{d}}+1}$$

as desired. This completes the proof of Theorem 2.5.

5 Proof of the conditionally optimal arithmetic result (Theorem 2.6)

Let $E = A \times A$. Using (2.1) we see that

$$\sum_t \nu^2(t) \leq |E|^4 q^{-1} + q^3 |E| \sum_k |E \cap l_k| |\widehat{E}(k)|^2.$$

Now,

$$q^3|E| \sum_k |E \cap l_k| |\widehat{E}(k)|^2 = q^3|E| \cdot |E| \cdot |\widehat{E}(1,1)|^2$$

$$+q^3|E| \sum_{k \neq (1,1)} |E \cap l_k| |\widehat{E}(k)|^2$$

$$\leq |E|^4 q^{-1} + C_{uni}|E|^3.$$

It follows that

$$|2A^2| = |\{x \cdot y : x, y \in E\}|$$

$$\geq \frac{|E|^4}{|E|^4 q^{-1} + C_{uni}|E|^3} \geq q \cdot \frac{C_{size}}{2C_{size} + C_{uni}},$$

as desired.

6 Proof of the Erdős-Falconer distance conjecture for subsets of the sphere (Theorem 2.7)

Since $E \subset S$,

$$||x - y|| = (x - y) \cdot (x - y) = 2 - 2x \cdot y,$$

so counting distance on the sphere is the same as counting dot products.

Since

$$|E \cap l_k| \leq 2$$

due to the fact that E is a subset of the sphere, we conclude from Theorem 2.1 that

$$|E|q^{2d-1} \sum_{k \neq (0,\ldots,0)} |E \cap l_k| |\widehat{E}(k)|^2$$

$$\leq 2|E|q^{2d-1} \sum_k |\widehat{E}(k)|^2$$

$$= 2|E|q^{2d-1}q^{-d}\sum_x E^2(x) = 2|E|^2q^{d-1}. \tag{6.1}$$

We have

$$|E|^4 = \left(\sum_t \nu(t)\right)^2 \leq |\Delta(E)| \cdot \sum_t \nu^2(t), \tag{6.2}$$

and we conclude that

$$\Delta(E) \geq Cq$$

if $|E| \geq cq^{\frac{d}{2}}$ by plugging (6.1) into (6.2).

7 Proof of the optimal exponent for uniformly distributed subsets of the sphere (Theorem 2.9)

Once again we use the estimate (2.1) which tells us that

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

Now,

$$|E|q^{2d-1}\sum_k |E \cap l_k||\widehat{E}(k)|^2$$

$$\leq 2|E|q^{2d-1}\sum_{C(E)} |\widehat{E}(k)|^2,$$

where

$$C(E) = \cup_{t\in\mathbb{F}_q} tE.$$

Now,

$$|E|q^{2d-1}\sum_{C(E)} |\widehat{E}(k)|^2$$

$$|E|q^{2d-1}q^{-2d}\sum_{u,v\in E}\sum_{C(E)} \chi((u-v)\cdot k)$$

$$= |E|q^{-1}\sum_{u,v\in E}\sum_t\sum_{m\in E} \chi((u-v)\cdot tm)$$

$$= |E|^3 + |E|\sum_{(u-v)\cdot m=0; u\neq v} E(u)E(v)E(m). \tag{7.1}$$

Since E is assumed to be uniformly distributed,

$$\sum_{(u-v)\cdot m=0} E(m) \leq C|E|q^{-1},$$

plugging this into (7.1) we obtain $|E|^4 q^{-1}$. Using (6.2) once again we complete the proof. Observe that the assumption that $|E| \geq Cq$ is implicit in the uniform distributivity assumption.

References

[1] 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.

[2] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Func. Anal. **14** (2004) 27-57.

[3] E. Croot, *Sums of the Form* $1/x_1^k + \ldots 1/x_n^k$ *modulo a prime*, Integers **4** (2004).

[4] B. Erdoğan. *A bilinear Fourier extension theorem and applications to the distance set problem.* IMRN (accepted for publication) 2005.

[5] P. Erdös *On sets of distances of n points,* Amer. Math. Monthly. **53** (1946), 248–250.

[6] A. Iosevich, S. Hofmann, *Circular averages and Falconer/Erdős distance conjecture in the plane for random metrics*, Proc. Amer. Mat. Soc. 133 (2005), 133-143.

[7] M. Garaev, *The sum-product estimate for large subsets of prime fields*, (preprint), (2007).

[8] A. A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime and the Erds-Graham problem*, Mat. Zametki, **79** (2006), 384-395; translation in: Math. Notes **79** (2006), 356-365.

[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).

[10] D. Hart and A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*, (preprint), arxiv.org (2007).

[11] D. Hart, A. Iosevich and J. Solymosi, *Sums and products in finite fields via Kloosterman sums*, IMRN (to appear), (2007).

[12] A. Iosevich and M. Rudnev, *Erdös distance problem in vector spaces over finite fields*, TAMS, (to appear), (2007).

[13] Nets Hawk Katz and Chun-Yen Shen, *Garaev's Inequality in finite fields not of prime order*, (preprint), (2007).

[14] J. Matousek, *Lectures on Discrete Geometry,* Graduate Texts in Mathematics, Springer **202** (2002).

[15] E. Stein, *Harmonic Analysis*, Princeton University Press, (1993).

[16] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge University Press, (2006).

[17] V. Vu, *Sum-Product estimates via directed expanders*, (preprint), (2007).

[18] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34** (1948) 204-207.