Some remarks on combinatorial geometry in vector spaces over finite fields

Alex Iosevich

University of Missouri

April 9, 2008

Topics covered in this talks

- **The Erdős-Falconer distance problem:** How large does $E \subset \mathbb{F}_q^d$ need to be to ensure that

$$|\Delta(E)| = |\{||x-y|| \equiv (x_1-y_1)^2 + \cdots + (x_d-y_d)^2 : x, y \in E\}| \gtrsim q.$$

Topics covered in this talks

- **The Erdős-Falconer distance problem:** How large does $E \subset \mathbb{F}_q^d$ need to be to ensure that

$$|\Delta(E)| = |\{||x-y|| \equiv (x_1-y_1)^2 + \cdots + (x_d-y_d)^2 : x, y \in E\}| \gtrsim q.$$

- **The dot product problem:** How large does $E \subset \mathbb{F}_q^d$ need to be to ensure that

$$|\Pi(E)| = |\{x \cdot y : x, y \in E\}| \gtrsim q.$$

Topics covered in this talks

- **The Erdős-Falconer distance problem:** How large does $E \subset \mathbb{F}_q^d$ need to be to ensure that

$$|\Delta(E)| = |\{||x-y|| \equiv (x_1-y_1)^2 + \cdots + (x_d-y_d)^2 : x, y \in E\}| \gtrsim q.$$

- **The dot product problem:** How large does $E \subset \mathbb{F}_q^d$ need to be to ensure that

$$|\Pi(E)| = |\{x \cdot y : x, y \in E\}| \gtrsim q.$$

- **The k-point configuration problem:** How large does $E \subset \mathbb{F}_q^d$ need to be to ensure that a congruent copy of every non-degenerate k-point configuration is contained in E?

The Erdős-Falconer distance problem-basic obstructions

- Let $E = \mathbb{F}_q^d$. Then $\Delta(E) = \mathbb{F}_q$, so, in general,

$$|\Delta(E)| \leq |E|^{\frac{1}{d}}.$$

The Erdős-Falconer distance problem-basic obstructions

- Let $E = \mathbb{F}_q^d$. Then $\Delta(E) = \mathbb{F}_q$, so, in general,

$$|\Delta(E)| \leq |E|^{\frac{1}{d}}.$$

- Suppose that $d = 2$, $\sqrt{-1} \in \mathbb{F}_q$ and consider

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

Then $|E| = q$ and $\Delta(E) = \{0\}$.

The Erdős-Falconer distance problem-basic obstructions

- Let $E = \mathbb{F}_q^d$. Then $\Delta(E) = \mathbb{F}_q$, so, in general,

$$|\Delta(E)| \leq |E|^{\frac{1}{d}}.$$

- Suppose that $d = 2$, $\sqrt{-1} \in \mathbb{F}_q$ and consider

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

  Then $|E| = q$ and $\Delta(E) = \{0\}$.

- At least in even dimensions this shows that a set of size $q^{\frac{d}{2}}$ can have a distance set consisting of a single point.

A theorem of Bourgain, Katz and Tao

- Bourgain, Katz and Tao (2004) proved the following result as a corollary of their version of the Szemeredi-Trotter incidence theorem in two-dimensional vector spaces over finite fields:

A theorem of Bourgain, Katz and Tao

- Bourgain, Katz and Tao (2004) proved the following result as a corollary of their version of the Szemeredi-Trotter incidence theorem in two-dimensional vector spaces over finite fields:

Theorem

Let $q \equiv 3 \mod (4)$, q a prime. Let $E \subset \mathbb{F}_q^2$ such that

$$|E| \lesssim q^{2-\epsilon}.$$

Then there exists $\delta(\epsilon) > 0$ such that

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

Falconer's exponent

- The following is an analog of Falconer's $\frac{d+1}{2}$ exponent in vector spaces over finite fields:

Theorem

(A.I. and M. Rudnev (2007)) Let $E \subset \mathbb{F}_q^d$, $d \geq 2$, *such that* $|E| > 2q^{\frac{d+1}{2}}$. *Then*

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

Falconer's exponent

- The following is an analog of Falconer's $\frac{d+1}{2}$ exponent in vector spaces over finite fields:

Theorem

(A.I. and M. Rudnev (2007)) Let $E \subset \mathbb{F}_q^d$, $d \geq 2$, such that $|E| > 2q^{\frac{d+1}{2}}$. Then

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

- The proof proceeds by showing that if $t \neq 0$,

$$|\{(x,y) \in E \times E : ||x-y|| = t\}| = |E|^2 q^{-1} + O(|E| q^{\frac{d-1}{2}}),$$

where the error estimate is obtained by using Weil's (Salie's) bound for Kloosterman sums.

A proof of the $\frac{d+1}{2}$ exponent

- We have

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

A proof of the $\frac{d+1}{2}$ exponent

- We have

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

- $$= \sum_{x,y} E(x)E(y)S_t(x-y) = q^{2d} \sum_{m} |\widehat{E}(m)|^2 \widehat{S}_t(m)$$

A proof of the $\frac{d+1}{2}$ exponent

- We have
$$|\{(x,y) \in E \times E : ||x-y|| = t\}$$
- $$= \sum_{x,y} E(x)E(y)S_t(x-y) = q^{2d} \sum_{m} |\widehat{E}(m)|^2 \widehat{S}_t(m)$$
- $$= |E|^2 q^{-1} + q^{2d} \sum_{m \neq (0,\dots,0)} |\widehat{E}(m)|^2 \widehat{S}_t(m)$$

A proof of the $\frac{d+1}{2}$ exponent

- We have
$$|\{(x,y) \in E \times E : ||x-y|| = t\}|$$
-
$$= \sum_{x,y} E(x)E(y)S_t(x-y) = q^{2d} \sum_m |\widehat{E}(m)|^2 \widehat{S}_t(m)$$
-
$$= |E|^2 q^{-1} + q^{2d} \sum_{m \neq (0,\dots,0)} |\widehat{E}(m)|^2 \widehat{S}_t(m)$$
-
$$= |E|^2 q^{-1} + O(|E| q^{\frac{d-1}{2}})$$

  since
$$|\widehat{S}_t(m)| \leq 2q^{-\frac{d+1}{2}}$$
  using bound for Gauss and twisted Kloosterman sums.

Sharpness of exponents

- Moreover, the exponent $\frac{d+1}{2}$ is, in general, sharp in odd dimensions, as recently shown by D. Hart, A.I., D. Koh and M. Rudnev. The sharpness example relies on the existence of a large number of **mutually orthogonal vectors of length zero**, which explains why the corresponding exponents are better in the Euclidean space.

Sharpness of exponents

- Moreover, the exponent $\frac{d+1}{2}$ is, in general, sharp in odd dimensions, as recently shown by D. Hart, A.I., D. Koh and M. Rudnev. The sharpness example relies on the existence of a large number of **mutually orthogonal vectors of length zero**, which explains why the corresponding exponents are better in the Euclidean space.
- It seems quite likely that for Cartesian products the exponent can go down all the way to $\frac{d}{2}$. This is where we now turn our attention.

Improved estimates for Cartesian products

- While the exponent $\frac{d+1}{2}$ is sharp in general, at least in odd dimensions, we obtain a better exponent for product sets.

Theorem

(D. Hart and A.I. (2007)) Suppose that $E = A \times A \times \cdots \times A$ *and*

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

Then

$$|\Delta(E)| \gtrsim q.$$

Improved estimates for Cartesian products

- While the exponent $\frac{d+1}{2}$ is sharp in general, at least in odd dimensions, we obtain a better exponent for product sets.

Theorem

(D. Hart and A.I. (2007)) Suppose that $E = A \times A \times \cdots \times A$ *and*

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

Then

$$|\Delta(E)| \gtrsim q.$$

- This matches the Euclidean exponent in two dimensions (Wolff (1999)) and beats it slightly in higher dimensions (Erdogan (2005)). Note that these Euclidean results hold for general sets.

Dot products: a geometric viewpoint

- The following is our main result on dot products:

Theorem

(D. Hart and A.I. (2007)) Let $E \subset \mathbb{F}_q^d$. Then

$$\mathbb{F}_q^* \subset \Pi(E) \text{ if } |E| > q^{\frac{d+1}{2}},$$

and if E is a Cartesian product, then

$$|\Pi(E)| \geq q \frac{C^{2-\frac{1}{d}}}{1 + C^{2-\frac{1}{d}}} \text{ if } |E| \geq Cq^{\frac{d}{2} + \frac{d}{2(2d-1)}}.$$

Dot products: a geometric viewpoint

- The following is our main result on dot products:

Theorem

(D. Hart and A.I. (2007)) Let $E \subset \mathbb{F}_q^d$. Then

$$\mathbb{F}_q^* \subset \Pi(E) \text{ if } |E| > q^{\frac{d+1}{2}},$$

and if E is a Cartesian product, then

$$|\Pi(E)| \geq q \frac{C^{2-\frac{1}{d}}}{1 + C^{2-\frac{1}{d}}} \text{ if } |E| \geq Cq^{\frac{d}{2} + \frac{d}{2(2d-1)}}.$$

- The exponent $\frac{d+1}{2}$ is, in general, sharp. The sharpness example requires $q = p^2$ and we do not know if an improvement is possible in $\mathbb{Z}_p^d$.

A closely related problem: sums-products

- The following can be deduced from a recent result due to Bourgain:

Theorem

(Bourgain (2006)) Suppose that $A \subset \mathbb{F}_q$ with

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

Then

$$dA^2 = \mathbb{F}_q.$$

A closely related problem: sums-products

- The following can be deduced from a recent result due to Bourgain:

Theorem

(Bourgain (2006)) Suppose that $A \subset \mathbb{F}_q$ with

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

Then

$$dA^2 = \mathbb{F}_q.$$

- When d is sufficiently large, things get better:

Theorem

(Glibichuk with an improvement by Rudnev (2008)) Suppose that $|A| > q^{\frac{1}{2}}$. Then

$$|6A^2| > \frac{q}{2} \text{ and } 12A^2 = \mathbb{F}_q.$$

A corollary of the dot product estimates

- The dot product result mentioned above has the following immediate consequence:

A corollary of the dot product estimates

- The dot product result mentioned above has the following immediate consequence:

Corollary

(D. Hart and A.I. (2007)) Let $A \subset \mathbb{F}_q$. *If* $|A| > q^{\frac{1}{2}+\frac{1}{2d}}$, *then* $\mathbb{F}_q^* \subset dA^2$. *Moreover, if*

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

then

$$|dA^2| \geq q \frac{C^{2-\frac{1}{d}}}{1 + C^{2-\frac{1}{d}}}.$$

A corollary of the dot product estimates

- The dot product result mentioned above has the following immediate consequence:

Corollary

(D. Hart and A.I. (2007)) Let $A \subset \mathbb{F}_q$. *If* $|A| > q^{\frac{1}{2}+\frac{1}{2d}}$, *then* $\mathbb{F}_q^* \subset dA^2$. *Moreover, if*

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

then

$$|dA^2| \geq q \frac{C^{2-\frac{1}{d}}}{1+C^{2-\frac{1}{d}}}.$$

- Attempts to improve the second exponent above lead to a rather interesting problem and this is where we now turn our attention.

Incidence theory behind the dot product estimate

- Using the Radon transform, we establish the following incidence estimates: Let $\nu(t) = |\{(x, y) \in E \times E : x \cdot y = t\}|$. Then

Incidence theory behind the dot product estimate

- Using the Radon transform, we establish the following incidence estimates: Let $\nu(t) = |\{(x, y) \in E \times E : x \cdot y = t\}|$. Then
-
$$\nu(t) = |E|^2 q^{-1} + R(t), \quad \text{where } |R(t)| \le |E| q^{\frac{d-1}{2}},$$

Incidence theory behind the dot product estimate

- Using the Radon transform, we establish the following incidence estimates: Let $\nu(t) = |\{(x, y) \in E \times E : x \cdot y = t\}|$. Then

- $$\nu(t) = |E|^2 q^{-1} + R(t), \text{ where } |R(t)| \le |E| q^{\frac{d-1}{2}},$$

- and

$$\sum_t \nu^2(t) \le |E|^4 q^{-1} + |E| q^{2d-1} \sum_{k \neq (0,\dots,0)} |\widehat{E}(k)|^2 |E \cap l_k|,$$

Incidence theory behind the dot product estimate

- Using the Radon transform, we establish the following incidence estimates: Let $\nu(t) = |\{(x,y) \in E \times E : x \cdot y = t\}|$. Then
- $$\nu(t) = |E|^2 q^{-1} + R(t), \quad \text{where } |R(t)| \le |E| q^{\frac{d-1}{2}},$$
- and
$$\sum_t \nu^2(t) \le |E|^4 q^{-1} + |E| q^{2d-1} \sum_{k \neq (0,\dots,0)} |\widehat{E}(k)|^2 |E \cap l_k|,$$
- where
$$l_k = \{tk : t \in \mathbb{F}_q\}, \text{ the line generated by } k.$$

Multiplicative sub-groups are difficult to handle

- The L^2 estimate on the incidence function gives us a better exponent for the arithmetic problem because it allows us to use the estimate

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

Multiplicative sub-groups are difficult to handle

- The L^2 estimate on the incidence function gives us a better exponent for the arithmetic problem because it allows us to use the estimate

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

- Even the latter estimate is incredibly unlikely to be sharp **unless** A has much multiplicative structure.

Multiplicative sub-groups are difficult to handle

- The L^2 estimate on the incidence function gives us a better exponent for the arithmetic problem because it allows us to use the estimate

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

- Even the latter estimate is incredibly unlikely to be sharp **unless** A has much multiplicative structure.

- In order to push the estimates further, it would be great to have a sharp lower bound on $|A + A|$ when A is a multiplicative subgroup.

Multiplicative sub-groups are difficult to handle

- The L^2 estimate on the incidence function gives us a better exponent for the arithmetic problem because it allows us to use the estimate

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

- Even the latter estimate is incredibly unlikely to be sharp **unless** A has much multiplicative structure.
- In order to push the estimates further, it would be great to have a sharp lower bound on $|A + A|$ when A is a multiplicative subgroup.
- However, the best result to date, due to Bourgain and Konyagin, says that

$$|A + A| \gtrsim \min\{|A|^{\frac{3}{2}}, q\}.$$

k-point configurations in $\mathbb{F}_q^d$

- We have the following finite field analog of the classical results by Bourgain, Furstenberg, Katznelson, Weiss and others.

k-point configurations in $\mathbb{F}_q^d$

- We have the following finite field analog of the classical results by Bourgain, Furstenberg, Katznelson, Weiss and others.

- We say that a k point set P_k is non-degenerate if elements of P_k are linearly independent and if $(P_k - P_k) \cap \{x \in \mathbb{F}_q^d : ||x|| = 0\} = \{(0, \dots, 0)\}$.

k-point configurations in $\mathbb{F}_q^d$

- We have the following finite field analog of the classical results by Bourgain, Furstenberg, Katznelson, Weiss and others.
- We say that a k point set P_k is non-degenerate if elements of P_k are linearly independent and if $(P_k - P_k) \cap \{x \in \mathbb{F}_q^d : ||x|| = 0\} = \{(0, \dots, 0)\}$.

Theorem

(D. Hart and A.I. (2007)) Let P_k be a non-degenerate set of k points in $\mathbb{F}_q^d$. Suppose that $E \subset \mathbb{F}_q^d$ such that

$$|E| \geq Cq^{d\frac{k-1}{k}+\frac{k-1}{2}}.$$

Then there exists $\tau \in \mathbb{F}_q^d$ and $O \in SO(d)$ such that

$$O(P_k) + \tau \subset E.$$

Reformulation in terms of distances

- Observe that this result has some meaning as long as

$$d \geq \binom{k}{2}.$$

Reformulation in terms of distances

- Observe that this result has some meaning as long as
$$d \geq \binom{k}{2}.$$
- The result we actually prove is the following:

Theorem

(D. Hart and A.I. (2007)) Let $\{t_{ij}\}_{1 \leq i \neq j \leq k} \in \mathbb{F}_q^*$. *Then*

$$|\{(x^1, \ldots, x^k) \in E \times \cdots \times E : ||x^i - x^j|| = t_{ij}\}| = |E|^k q^{-\binom{k}{2}} + R,$$

where

$$|R| \lesssim q^{\frac{kd}{2}} q^{-\frac{k(k+1)}{4}} |E|^{\frac{k+1}{2}}.$$

Reformulation in terms of distances

- Observe that this result has some meaning as long as

$$d \geq \binom{k}{2}.$$

- The result we actually prove is the following:

Theorem

(D. Hart and A.I. (2007)) Let $\{t_{ij}\}_{1 \leq i \neq j \leq k} \in \mathbb{F}_q^*$. *Then*

$$|\{(x^1, \dots, x^k) \in E \times \cdots \times E : ||x^i - x^j|| = t_{ij}\}| = |E|^k q^{-\binom{k}{2}} + R,$$

where

$$|R| \lesssim q^{\frac{kd}{2}} q^{-\frac{k(k+1)}{4}} |E|^{\frac{k+1}{2}}.$$

- Note that any two sets with the same pair-wise distances are equivalent up to a translation and an orthogonal transformation.

An improvement: arbitrary subgraphs

- The previous result may be interpreted as a statement about large complete subgraphs of the distance graph. The following result addresses the issue of arbitrary subgraphs:

An improvement: arbitrary subgraphs

- The previous result may be interpreted as a statement about large complete subgraphs of the distance graph. The following result addresses the issue of arbitrary subgraphs:

Theorem

(D. Hart, A.I., D. Koh and I. Uriarte-Tuero) (2007)) Let

$$J \subset \{1,2\dots,k\} \times \{1,2\dots,k\} \text{ with } |J| = n.$$

Then

$$|\{(x^1,\dots,x^k) \in E \times \cdots \times E : ||x^i - x^j|| = t_{ij}; (i,j) \in J\}|$$

$$= |E|^k q^{-n}(1+o(1))$$

if

$$|E| \geq Cq^{d\frac{k-1}{k}+\frac{n}{k}}.$$