Ubiquity of simplices in subsets of vector spaces over finite fields

Derrick Hart and Alex Iosevich

June 12, 2007

Abstract

We prove that a sufficiently large subset of the d-dimensional vector space over a finite field with q elements, $\mathbb{F}_q^d$, contains a copy of every k-simplex. Fourier analytic methods, Kloosterman sums, and bootstrapping play an important role.

Contents

1 Introduction

Many problems in combinatorial geometry ask, in one form or another, whether a certain structure must be present in a set of sufficiently large size. Perhaps the most celebrated result of this type is Szemeredi's theorem ([10]) which says that if a subset of the integers has positive density, then it contains an arbitrary large arithmetic progression. The conclusion has recently been extended to the subsets of prime numbers by Green and Tao ([4]). In Euclidean space, a result due to Katznelson and Weiss ([3]) says that a subset of Euclidean space of positive Lebesgue upper density contains every sufficiently large distance. A

subsequent result by Bourgain ([1]), says that a subset of $\mathbb{R}^k$ of positive Lebesgue upper density contains an isometric copy of all large dilates of a set of k points spanning a $(k-1)$-dimensional hyperplane. Ergodic theory has been used to show that positive upper density implies that the set contains a copy of a sufficiently large dilate of every convex polygon with finitely many sides. See, for example, a recent survey by Bryna Kra ([7]).

Let $\mathbb{F}_q^d$ be a d-dimensional vector space over a finite field $\mathbb{F}_q$. A plausible analogy to Bourgain's result ([1]) in this context would be to consider whether a subset of positive density contains a isometric copy of a set of k points spanning a $(k-1)$-dimensional hyperplane. It turns out however, that the positive density condition is much too strong in the context of vector spaces over finite fields and the same conclusion follows from a much weaker assumption on the size of the underlying set.

Definition 1.1. Let a k-simplex be a set of $k+1$ points in general position, which means that no $n+1$ of these points, $n \leq k$, lie in a $(n-1)$-dimensional sub-space of $\mathbb{F}_q^d$.

Definition 1.2. We say that a linear transformation T on $\mathbb{F}_q^d$ is an isometry if

$$||Tx|| = ||x||,$$

where

$$||x|| = x_1^2 + x_2^2 + \cdots + x_d^2,$$

an element of $\mathbb{F}_q$.

The question we ask in this paper is how large does $E \subset \mathbb{F}_q^d$ needs to be in order to be sure that it contains a copy of every k-simplex. Our main result is the following.

Theorem 1.3. Let $E \subset \mathbb{F}_q^d$, $d > \binom{k+1}{2}$, such that $|E| \geq Cq^{\frac{k}{k+1}d}q^{\frac{k}{2}}$ with a sufficiently large constant $C > 0$. Then E contains an isometric copy of every k-simplex.

Note that we obtain non-trivial results only when $k << \sqrt{d}$. Nevertheless, in that range we are able to dip considerably below the positive density condition on the underlying set E.

The method of proof relies on the fact that orthogonal transformations on $\mathbb{F}_q^d$ are isometries. A "distance representation" of a simplex is then used to reduce Theorem 1.3 to an appropriate weighted incidence theorem for spheres and points. Weyl's estimate ([11]) for classical Kloosterman sums is used to control the size of the Fourier transform of spheres of non-zero radius. The key idea in the proof is to show at each step of an inductive argument that a collection of distances among vertices of a given simplex can not only be realized, but actually occur a "statistically correct" number of times.

2   Preliminaries and Definitions

Let $\mathbb{F}_q^d$ be the d-dimensional vector space over the finite field $\mathbb{F}_q$. The Fourier transform of a function

$$f : \mathbb{F}_q^d \to \mathbb{C}$$

is given by

$$\widehat{f}(m) := q^{-d} \sum_{x \in \mathbb{F}_q^d} g(x)\chi(-x \cdot m),$$

where χ is an additive character on $\mathbb{F}_q$.

The orthogonality property of the Fourier Transform says that

$$q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(-x \cdot m) = 1$$

for $m = (0, \dots, 0)$ and 0 otherwise yields many standard properties of the Fourier Transform.

We summarize some of the properties of the Fourier Transform as follows.

Lemma 2.1 (The Fourier Transform). *Let*

$$f, g : \mathbb{F}_q^d \to \mathbb{C}.$$

$$\hat{f}(0, \dots, 0) = q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x),$$

$$(Plancherel) \ q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x)\overline{g(x)} = \sum_{m \in \mathbb{F}_q^d} \hat{f}(m)\overline{\hat{g}(m)},$$

$$(Inversion) \quad f(x) = \sum_{m \in \mathbb{F}_q^d} \hat{f}(m)\chi(x \cdot m).$$

2.1   Notation

Throughout the paper $X \lesssim Y$ means that there exists $C > 0$ such that $X \leq CY$, $X \gtrsim Y$ means $Y \lesssim X$, and $X \approx Y$ if both $X \lesssim Y$ and $X \gtrsim Y$. Along the same lines, $X \ll Y$ means that $\frac{X}{Y} \to 0$, as $q \to \infty$ $X \gg Y$ means $Y \ll X$, and $X \sim Y$ if $\frac{X}{Y} \to 1$ as $q \to \infty$.

3 Proof of the main result

Even though a finite field with q elements, $\mathbb{F}_q$, is not a metric space, we define the "distance" between two points x and y in $\mathbb{F}_q^d$ by the formula

$$||x - y|| = (x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_d - y_d)^2.$$

The same notion of "distance" was used by Bourgain, Katz and Tao([2]), and Iosevich and Rudnev([5]) in their study of the Erdős distance problem in vector spaces over finite fields. As we noted above, a geometric justification of this notion of distance is that an orthogonal transformation on $\mathbb{F}_q^d$, a matrix O such that $O^t \cdot O = I$, preserves this notion of a "distance". Represent a k-simplex in a subset $E \subset \mathbb{F}_q^d$ on $k+1$ points recursively by setting

$$\mathcal{T}_{l_k}^k = \{(x_0, \ldots, x_{k-1}, x_k) \in \mathcal{T}_{l_{k-1}}^{k-1} \times E : (||x_0 - x_k||, ||x_1 - x_k||, \ldots, ||x_{k-1} - x_k||) = l_k\},$$

for $l_k \in (\mathbb{F}_q^*)^k$, where

$$\mathcal{T}_{l_1}^1 = \{(x_0, x_1) \in E^2 : ||x_0 - x_1|| = l_1\}.$$

This representation does not, in general, always embody a simplex as $\mathcal{T}_{l_k}^k$ is not guaranteed to be in general position. However, as we show below, "legitimate" k-simplices are equivalent up to an orthogonal transformation.

Theorem 3.1. *Let $E \subset \mathbb{F}_q^d$, $d > \binom{k+1}{2}$, such that $|E| \geq Cq^{\frac{k}{k+1}d}q^{\frac{k}{2}}$, with a sufficiently large constant C. Then for every side length set $\{l_1, \ldots, l_k\}$, $l_k \in (\mathbb{F}_q^*)^k$ we have that $|\mathcal{T}_{l_k}^k| > 0$. Furthermore,*

$$|\mathcal{T}_{l_k}^k| \sim |E|^{k+1}q^{-\binom{k+1}{2}}.$$

Using this theorem we recover the main result of the paper using the following linear algebraic observation.

Lemma 3.2. *Let P be a simplex with vertices $V_0, V_1, \ldots, V_k$, $V_j \in \mathbb{F}_q^d$. Let P' be another simplex with vertices $V_0', V_1', \ldots, V_k'$. Suppose that*

$$||V_i - V_j|| = ||V_i' - V_j'|| \tag{3.1}$$

for all i, j. Then there exists an orthogonal transformation O on $\mathbb{F}_q^d$ such that $O(P) = P'$.

4

3.1 Proof of Theorem 3.1-the main result reformulated in terms of "distances"

The proof proceeds by induction. The first step is the case $k = 2$. For a set E we define the characteristic or indicator function to be $E(x)$. Now define the sphere of radius $l \in \mathbb{F}_q^*$ to be

$$S_l = \{x \in \mathbb{F}_q^d : ||x|| = l\},$$

then

$$|\mathcal{T}_{l_1}^1| = |\{(x_0, x_1) \in E \times E : ||x_0 - x_1|| = l_1\}|$$
$$= \sum_{x_0, x_1} E(x_0)E(x_1)S_l(x_0 - x_1).$$

In order to obtain information from this quantity the behavior of incidences of spheres and points in E will be critical. The following classical fact, whose proof will be given in a subsequent section, states that the the sphere has optimal Fourier decay away from the origin.

Lemma 3.3. *Let S_l, $l \in \mathbb{F}_q^*$ be defined as above. If $m \neq (0, \ldots, 0)$ then*

$$|\widehat{S}_l(m)| \lesssim q^{-\frac{d+1}{2}},$$

and

$$\widehat{S}_l(0, \ldots, 0) = q^{-d}|S_l| \approx q^{-1}.$$

Applying Fourier inversion to the sphere,

$$|\mathcal{T}_{l_1}^1| = q^{2d} \sum_{x_0, x_1} E(x_0)E(x_1) \sum_m \widehat{S}_l(m)\chi(m \cdot (x_0 - x_1))$$
$$= q^{2d} \sum_m |\widehat{E}(m)|^2 \widehat{S}_l(m)$$
$$= |E|^2 \cdot q^{-d} \cdot |S_l| + q^{2d} \sum_{m \neq (0, \ldots, 0)} |\widehat{E}(m)|^2 \widehat{S}_l(m)$$
$$= M + R.$$

By Lemma 3.3,

$$M \approx \frac{|E|^2}{q},$$

and using Lemma 3.3 once again,

$$|R| \lesssim q^{2d} \cdot q^{-\frac{d+1}{2}} \cdot \sum_m |\widehat{E}(m)|^2$$
$$= q^{\frac{d-1}{2}} \cdot |E|,$$

5

which is smaller than M if $|E| \geq Cq^{\frac{d+1}{2}}$ with a sufficiently large constant C and thus $\mathcal{T}_{l_1}^1$ is non-empty. Moreover, if $|E| \gg q^{\frac{d+1}{2}}$, we get the "statistically expected" number of distances,

$$|\mathcal{T}_{l_1}^1| \sim \frac{|E|^2}{q}.$$

Assuming the $(k-1)$st case, we count the number of k-simplices in E as an extension of the $(k-1)$-simplices in E.

$$|\mathcal{T}_{t_k}^k| = \sum_{x_0,\dots,x_k} \mathcal{T}_{l_{k-1}}^{k-1}(x_0,\dots,x_{k-1})E(x_k)S_{l_1}(x_0-x_k)\dots.S_{l_k}(x_{k-1}-x_k).$$

By Fourier inversion, the expression equals

$$\sum_{x_0,\dots,x_k} \sum_{m_0,\dots,m_{k-1}} \prod_{i=1}^{k-1} \chi((x_i-x_k)\cdot m_i)\widehat{S}_{l_i}(m_i)\mathcal{T}_{l_{k-1}}^{k-1}(x_0,\dots,x_{k-1})E(x_k)$$

$$= q^{kd} \sum_{m_0,\dots,m_{k-1}} \widehat{\mathcal{T}}_{l_{k-1}}^{k-1}(-m_0,\dots,-m_{k-1})\widehat{E}(m_0+\dots+m_{k-1})\widehat{S}_{l_1}(m_0)\dots\widehat{S}_{l_{k-1}}(m_{k-1}),$$

where the Fourier transform of $\mathcal{T}_{l_{k-1}}^{k-1}$ is actually the Fourier transform on $\mathbb{F}_q^d \times \dots \times \mathbb{F}_q^d$, k times.

Extracting the zero term and breaking the remaining sum into pieces on which we may apply Lemma 3.3, this expression equals

$$q^{(k+1)d} \cdot q^{-kd} \cdot |\mathcal{T}_{l_{k-1}}^{k-1}| \cdot |E| \cdot |S_{l_1}| \cdot q^{-d} \cdot \dots \cdot |S_{l_{k-1}}| \cdot q^{-d}$$

$$+q^{(k+1)d} \sum_{\substack{\mathcal{P}\cup\mathcal{P}'=\{m_i\}_1^{k-1} \\ 0=m_i\in\mathcal{P} \\ 0\neq m_i\in\mathcal{P}'}} \widehat{\mathcal{T}}_{l_{k-1}}^{k-1}(-m_0,\dots,-m_{k-1})\widehat{E}(m_0+\dots+m_{k-1})\widehat{S}_{l_1}(m_0)\dots\widehat{S}_{l_{k-1}}(m_{k-1})$$

$$= M + R,$$

where the sum defining R runs over all the partitions of $\{m_0,\dots,m_{k-1}\}$ with the case $\mathcal{P}'=\emptyset$ extracted and used as the main term M above.

By Lemma 3.3 and the induction hypothesis,

$$M \sim |E|^{k+1}q^{-\binom{k+1}{2}}.$$

By Lemma 3.3 and Cauchy-Schwartz,

$$|R|^2 \lesssim q^{2(k+1)d}q^{-|\mathcal{P}'|(k-1)(d+1)}q^{-2|\mathcal{P}|} \sum_{m_0,\dots,m_{k-1}} |\widehat{\mathcal{T}}_{l_{k-1}}^{k-1}(-m_0,\dots,-m_{k-1})|^2 \sum_{m_i\in\mathcal{P}'} \left|\widehat{E}\left(\sum_{m_i\in\mathcal{P}'} m_i\right)\right|^2.$$

6

Applying Plancherel and the induction hypothesis, we get

$$= q^{2(k+1)d} q^{-|\mathcal{P}'|(d+1)} q^{-2|\mathcal{P}|} q^{-kd} |\mathcal{T}_{l_{k-1}}^{k-1}| q^{|\mathcal{P}'|d} q^{-2d} |E|$$

$$\sim q^{kd} q^{-|\mathcal{P}'|} q^{-2|\mathcal{P}|} q^{-\binom{k}{2}} |E|^{k+1}.$$

The quantity above is maximized when $\mathcal{P} = \emptyset$. We conclude that

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

The term R is smaller than, say, $\frac{M}{2}$ if

$$q^{\frac{kd}{2}} q^{-\frac{k(k+1)}{4}} |E|^{\frac{k+1}{2}} \leq C |E|^{k+1} q^{-\binom{k+1}{2}},$$

with a sufficiently large constant C, which happens if

$$|E| \geq C' q^{\frac{k}{k+1}d} q^{\frac{k}{2}},$$

with a sufficiently large constant C' depending on the constants implicit in the estimates above. This completes the proof.

4 Proof of Lemma 3.2

To prove Lemma 3.2, let $\pi_r(x)$ denote the rth coordinate of x. There is no harm in assuming that $V_0 = (0, \ldots, 0)$. We may also assume that $V_1, \ldots, V_k$ are contained in $\mathbb{F}_q^k$. The condition (3.1) implies that

$$\sum_{r=1}^{k} \pi_r(V_i) \pi_r(V_j) = \sum_{r=1}^{k} \pi_r(W_i) \pi_r(W_j). \tag{4.1}$$

Let T be the linear transformation uniquely determined by the condition

$$T(V_i) = V_i'.$$

In order to prove that T is orthogonal, it suffices to show that

$$||Tx|| = ||x||$$

for any $x \neq (0, \ldots, 0)$.

Since V_js form a basis, by assumption, we have

$$x = \sum_i t_i V_i,$$

7

so it suffices to show that

$$||x|| = \sum_r \sum_{i,j} t_i t_j \pi_r(V_i) \pi_r(V_j)$$

$$= \sum_r \sum_{i,j} t_i t_j \pi_r(V_i') \pi_r(V_j') = ||Tx||,$$

which follows immediately from (4.1).

Observe that we used the fact that orthogonality of T, the condition that $T^t \cdot T = I$ is equivalent to the condition that $||Tx|| = ||x||$. To see this observe that to show that $T^t \cdot T = I$ it suffices to show that $T^t T x = x$ for all non-zero x. This, in turn, is equivalent to the statement that

$$< T^t T x, x >= ||x||,$$

where

$$< x, y >= \sum_{i=1}^k x_i y_i.$$

Now,

$$< T^t T x, x >=< Tx, Tx >$$

by definition of the transpose, so the stated equivalence is established. This completes the proof of Lemma 3.2.

5 Estimation of the Fourier transform of the sphere: proof of Lemma 3.3

The proof of Lemma 3.3 is fairly standard, but we outline the argument for reader's convenience. Let l be in $\mathbb{F}_q^*$ and ψ is a multiplicative character on $\mathbb{F}_q^*$ then observe that

$$\widehat{S_l}(m) = q^{-d} \sum_x \chi(-x \cdot m) S_l(x)$$

$$= q^{-1} \delta(m) + q^{-d-1} \sum_x \sum_{s \neq 0} \chi(-x \cdot m) \chi(s(|x|^2 - l))$$

$$= q^{-1} \delta(m) + q^{-\frac{d}{2}-1} \sum_{s \neq 0} \chi\left(\frac{|m|^2}{4s} - ls\right) \psi^d(s),$$

where $\delta(m) = 1$ for $m = (0, \ldots, 0)$ and zero otherwise. The conclusion now follows from the following classical estimate due to A. Weil.

8

Theorem 5.1. *Let*

$$K(a) = \sum_{s \neq 0} \chi(as + s^{-1})\psi(s),$$

where, once again, ψ is a multiplicative character on $\mathbb{F}_q^*$. Then

$$|K(a)| \leq 2\sqrt{q}$$

if $a \neq 0$.

References

[1] J. Bourgain, *A Szemerédi type theorem for sets of positive density in $\mathbb{R}^k$*. Isr. J. Math **54** (1986) 307-316.

[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] H. Furstenberg, Y. Katznelson, and B. Weiss, *Ergodic theory and configurations in sets of positive density.* In *Mathematics of Ramsey theory*, pages 184-198, Algorithms Combin., **5** , Springer, Berlin, (1990).

[4] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (to appear), (2007).

[5] A. Iosevich and M. Rudnev, *Erdos distance problem in vector spaces over finite fields*, Transactions of the AMS (accepted for publication) (2007).

[6] A. Magyar, *K-point configurations in sets of positive density of $\mathbb{Z}^n$*, preprint.

[7] B. Kra, *Ergodic methods in additive combinatorics*, Lecture notes from the Montreal Workshop on Additive Combinatorics (2006).

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

[9] L.A. Székely, *Remarks on the chromatic number of geometric graphs.* In *Graphs and other combinatorial topics (Prague, 1982)*, pages 312-315, Algorithms Combin., **59** , Teubner-Texte Math, Leipzig, 1983.

[10] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression.* Acta. Arith. **27** (1975) 199-245.

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