Orthogonal systems in vector spaces over finite fields

Alex Iosevich and Steven Senger*

Department of Mathematics
University of Missouri, Columbia, MO 65211-4100
iosevich@math.missouri.edu, senger@math.missouri.edu

Submitted: Jul 24, 2008; Accepted: Dec 2, 2008; Published: Dec 9, 2008
Mathematics Subject Classifications: 11T23, 05B15

Abstract

We prove that if a subset of the d-dimensional vector space over a finite field is large enough, then it contains many k-tuples of mutually orthogonal vectors.

Contents

1 Introduction **1**

1.1 Graph theoretic interpretation 3

1.2 Hyperplane discrepancy problem 3

1.3 Acknowledgements 3

2 Proof of Theorem 1.1 **3**

3 Sharpness examples **8**

1 Introduction

A classical set of problems in combinatorial geometry deals with the question of whether a sufficiently large subset of $\mathbb{R}^d$, $\mathbb{Z}^d$, or $\mathbb{F}_q^d$ contains a given geometric configuration. For example, a classical result due to Furstenberg, Katznelson and Weiss ([5]; see also [2]) says that if $E \subset \mathbb{R}^2$ has positive upper Lebesgue density, then for any $\delta > 0$, the δ-neighborhood of E contains a congruent copy of a sufficiently large dilate of every three point configuration.

When the size of the point set is smaller than the dimension of ambient Euclidean space, taking a δ-neighborhood is not necessary, as shown by Bourgain in [2]. He proves

*A. Iosevich was supported by the NSF Grant DMS04-56306 and S. Senger was supported by the NSF Grant DMS07-04216

that if $E \subset \mathbb{R}^d$ has positive upper density and Δ is a k-simplex with $k < d$, then E contains a rotated and translated image of every large dilate of Δ. The case $k = d$ and $k = d+1$ remain open, however. See also, for example, [3], [4], [9], [14] and [16] on related problems and their connections with discrete analogs.

In the geometry of the integer lattice $\mathbb{Z}^d$, related problems have been recently investigated by Akos Magyar in [12] and [13]. In particular, he proves in [13] that if $d > 2k+4$ and $E \subset \mathbb{Z}^d$ has positive upper density, then all large (depending on density of E) dilates of a k-simplex in $\mathbb{Z}^d$ can be embedded in E. Once again, serious difficulties arise when the size of the simplex is sufficiently large with respect to the ambient dimension.

In finite field geometries, a step in this direction was taken by the listed authors in [6]. They prove that if $E \subset \mathbb{F}_q^d$, the d-dimensional vector space over the finite field with q elements with $|E| \geq Cq^{d\frac{k-1}{k}+\frac{k-1}{2}}$ and Δ is a k-dimensional simplex, then there exists $\tau \in \mathbb{F}_q^d$ and $O \in SO_d(\mathbb{F}_q)$ such that $\tau + O(\Delta) \subset E$. The result is only non-trivial in the range $d \geq \binom{k}{2}$ as larger simplexes are out of range of the methods used. See also [8] for a detailed graph theoretic analysis of a more general problem.

In this paper, we ask whether a sufficiently large subset of $\mathbb{F}_q^d$, the d-dimensional vector space over the finite field with q elements, contains a k-tuple of mutually orthogonal vectors. Similar questions, at least in the context of pairs of orthogonal vectors, are studied in [1]. This problem does not have a direct analog in Euclidean or integer geometries because placing the set strictly inside $\{x \in \mathbb{R}^d : x_j > 0\}$ immediately guarantees that no orthogonal vectors are present. However, the arithmetic of finite fields allows for a richer orthogonal structure. Our main result is the following.

Theorem 1.1. *Let $E \subset \mathbb{F}_q^d$, such that*

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

with a sufficiently large constant $C > 0$, where

$$0 < \binom{k}{2} < d.$$

Let λ_k be the number of k-tuples of k mutually orthogonal vectors in E. Then

$$\lambda_k = (1 + o(1))|E|^k q^{-\binom{k}{2}}.$$

Soon after we presented our result, Le Anh Vinh, in [15], showed a way to gain in the case $k > 2$ by employing graph theoretic techniques that can be found in [1] and [10]. The threshold obtained therein is $|E| \gtrsim q^{\frac{d}{2}+k-1}$, which admits a wider effective range for k in dimensions greater than 2. However, there were no counterexamples to show how sharp either method was. Here, we present two counterexamples. The first shows that both results are tight for $k = d = 2$. We then extend this intuitive construction, and utilize elementary algebraic techniques to show sharpness at $k = 2$ for all dimensions.

1.1 Graph theoretic interpretation

Define a hyper-graph $G_k(q,d)$ by taking its vertices to be the elements of $\mathbb{F}_q^d$ and connect k vertices by a hyper-edge if they are mutually orthogonal. Theorem 1.1 above implies that any subgraph of $G_k(q,d)$ with more than $Cq^{d\frac{k-1}{k}+\frac{k-1}{2}+\frac{1}{k}}$ vertices contains $(1+o(1))|E|^k q^{-\binom{k}{2}}$ hyper-edges, which is the statistically expected number.

Alternatively, we can think of Theorem 1.1 as saying that any sub-graph of $G_2(q,d)$ of size greater than $Cq^{d\frac{k-1}{k}+\frac{k-1}{2}+\frac{1}{k}}$ contains $(1+o(1))|E|^k q^{-\binom{k}{2}}$ complete sub-graph on k vertices, once again a statistically expected number.

See [8], and the references contained therein, for a systematic description of the properties of related graphs.

1.2 Hyperplane discrepancy problem

One of the key features of the proof of this result is the analysis of the following discrepancy problem. Let

$$H_{x^1,x^2,\dots,x^k} = \{y \in \mathbb{F}_q^d : y \cdot x^j = 0,\ j = 1,2\dots,k\}.$$

Define the discrepancy function r_k by the equation

$$|E \cap H_{x^1,\dots,x^k}| = |E|q^{-k} + r_k(x^1,\dots,x^k),$$

where the first term should be viewed as the "expected" size of the intersection. In Lemma 2.1 below we show that on average,

$$|r_k(x^1,\dots,x^k)| \lesssim \sqrt{|E|q^{-k}},$$

where here, and throughout the paper, $X \lesssim Y$ means that there exists $C > 0$, independent of q, such that $X \leq CY$.

1.3 Acknowledgements

The authors wish to thank Boris Bukh, Seva Lev and Michael Krivelevich for interesting comments and conversations pertaining to this paper.

2 Proof of Theorem 1.1

Observe that

$$r_{k-1}\left(x^1,\dots,x^{k-1}\right) = q^{-(k-1)} \sum_{\substack{s_i \in \mathbb{F}_q^* \\ i=1,2,\dots,k-1}} \sum_{x^k \in \mathbb{F}_q^d} E(x^k) \prod_{i=1}^{k-1} \chi(-s_i x^i \cdot x^k).$$

Lemma 2.1. $\|r_{k-1}\|_{L^2} \lesssim |E|^{\frac{1}{2}} q^{\frac{(d-1)(k-1)+1}{2}}$.

Assuming Lemma 2.1 for now, we prove the main result, Theorem 1.1.

Proof. Define $\mathcal{D}_k := \{(x^1, ..., x^k) \in E^k : x^i \cdot x^j = 0, \forall 1 \le i < j \le k\}$, where E^k means $\underbrace{E \times E \times ... \times E}_{k \text{ times}}$. Also, let $\mathcal{D}_k(x^1, ..., x^k)$ and $E(x)$ be the indicator functions for the set $\mathcal{D}_k$ and E, respectively. Clearly $|\mathcal{D}_k| = \lambda_k$. Our goal is to get an expression for λ_k in terms of λ_{k-1}. In order for that to do us any good, we will need an expression for λ_2. We will show the direct calculation of λ_2, as well as the size condition on E for two vectors. This will help to illustrate the ideas employed in the same calculations for general k.

$$\begin{aligned}
\lambda_2 &= \sum_{x^1, x^2 \in \mathbb{F}_q^d : x^1 \cdot x^2 = 0} E(x^1)E(x^2) \\
&= q^{-1} \sum_{x^1, x^2 \in \mathbb{F}_q^d} E(x^1)E(x^2) \sum_{s \in \mathbb{F}_q} \chi(-sx^1 \cdot x^2) \\
&= q^{-1} \sum_{s \in \mathbb{F}_q} \sum_{x^1, x^2 \in \mathbb{F}_q^d} E(x^1)E(x^2)\chi(-sx^1 \cdot x^2) \\
&= I_2 + II_2,
\end{aligned}$$

where I_2 is the sum over $s = 0$, and II_2 is the same sum, but over $s \neq 0$. We will show that I_2 dominates the other term when $|E|$ satisfies the size condition, and is therefore the number of sets of 2 mutually orthogonal vectors present in E, modulo a constant.

$$\begin{aligned}
I_2 &= \sum_{x^1, x^2 \in \mathbb{F}_q^d} E(x^1)E(x^2)q^{-1} \\
&= q^{-1} \sum_{x^1 \in \mathbb{F}_q^d} E(x^1) \sum_{x^2 \in \mathbb{F}_q^d} E(x^2) \\
&= |E|^2 q^{-1}
\end{aligned}$$

If I_2 indeed dominates the other two terms, we'll have

$$\lambda_2 = |E|^2 q^{-1}.$$

So now we will have to compute II_2. First we will separate the factors into the indicator function of E and the discrepancy function. Then we will use Cauchy-Schwarz so we can deal with the L_2 norm of the discrepancy.

$$\begin{aligned}
II_2 &= q^{-1} \sum_{s \in \mathbb{F}_q^*} \sum_{x^1, x^2 \in \mathbb{F}_q^d} E(x^1)E(x^2)\chi(-sx^1 \cdot x^2) \\
&= \sum_{x^1, x^2 \in \mathbb{F}_q^d} E(x^1) q^{-1} \sum_{s \in \mathbb{F}_q^*} \sum_{x^2 \in \mathbb{F}_q^d} E(x^2)\chi(-sx^1 \cdot x^2) \\
&\le |E|^{\frac{1}{2}} (\sum_{x^1, ..., x^{k-1}} r_1^2)^{\frac{1}{2}} \approx |E|^{\frac{1}{2}} \|r_1\|_{L^2}.
\end{aligned}$$

Applying Lemma 2.1 gives us

$$\|r_1\|_{L^2} \lesssim |E|^{\frac{1}{2}} q^{\frac{d}{2}}.$$

So we can estimate II_2 from above by $|E|q^{\frac{d}{2}}$. Now we compare the sizes of I_2 and II_2. Recall that we want our "main term", I_2, to dominate, so we get the expected number of orthogonal pairs of vectors.

$$\begin{aligned} I_2 &> II_2 \\ |E|^2 q^{-1} &> |E| q^{\frac{(d-1)+1}{2}} \\ |E| &> q^{\frac{d}{2}+1} = q^{d\frac{2-1}{2}+\frac{2-1}{2}+\frac{1}{2}}, \end{aligned}$$

as claimed. The same ideas work for higher k. In the general case, one must operate with $\mathcal{D}_{k-1}$ instead of the indicator function of E, and there is a product of several additive characters present here, as opposed to only one. These and other details are handled below.

$$\begin{aligned} \lambda_k &= \sum_{\substack{x^j \in \mathbb{F}_q^d : x^j \cdot x^k = 0 \\ j=1,2,\ldots,k-1}} \mathcal{D}_{k-1}(x^1, \ldots, x^{k-1}) E(x^k) \\ &= q^{-(k-1)} \sum_{\substack{x^j \in \mathbb{F}_q^d \\ j=1,2,\ldots,k}} \mathcal{D}_{k-1}(x^1, \ldots, x^{k-1}) E(x^k) \sum_{\substack{s_i \in \mathbb{F}_q \\ i=1,2,\ldots,k-1}} \prod_{i=1}^{k-1} \chi(-s_i x^i \cdot x^k) \\ &= q^{-(k-1)} \sum_{\substack{s_i \in \mathbb{F}_q \\ i=1,2,\ldots,k-1}} \sum_{\substack{x^j \in \mathbb{F}_q^d \\ j=1,2,\ldots,k}} \mathcal{D}_{k-1}(x^1, \ldots, x^{k-1}) E(x^k) \prod_{i=1}^{k-1} \chi(-s_i x^i \cdot x^k) \\ &= I + II + III, \end{aligned}$$

where we separate the sum into three parts depending on the s_i's. I is the sum when all of the s_i's are zero. II is the sum when none of the s_i's are equal to zero. III is the sum when some of the s_i's are equal to zero, and some are not. We treat these three cases separately. As before, we will show that I dominates the other terms when $|E|$ satisfies the size condition, and is a constant times the number of k-tuples mutually orthogonal vectors contained in E.

$$\begin{aligned} I &= \sum_{\substack{x^j \in \mathbb{F}_q^d \\ j=1,2,\ldots,k}} \mathcal{D}_{k-1}(x^1, \ldots, x^{k-1}) E(x^k) q^{-(k-1)} \\ &= \sum_{\substack{x^j \in \mathbb{F}_q^d \\ j=1,2,\ldots,k-1}} \mathcal{D}_{k-1}(x^1, \ldots, x^{k-1}) |E| q^{-(k-1)} \\ &= |E| q^{-(k-1)} \sum_{\substack{x^j \in \mathbb{F}_q^d \\ j=1,2,\ldots,k-1}} \mathcal{D}_{k-1}(x^1, \ldots, x^{k-1}) \\ &= |E| q^{-(k-1)} \lambda_{k-1} \end{aligned}$$

If I indeed dominates the other two terms, we'll have

$$\frac{\lambda_k}{\lambda_{k-1}} = |E| q^{-(k-1)}.$$

To get an expression for λ_k, we recall the computation for $k = 2$ first: $\lambda_2 = |E|^2 q^{-1}$. Then notice the following collapsing product.

$$\lambda_k = \frac{\lambda_k}{\lambda_{k-1}} \cdot \frac{\lambda_{k-1}}{\lambda_{k-2}} \cdot \cdots \cdot \frac{\lambda_3}{\lambda_2} \cdot \lambda_2.$$

Substituting each in ratio, as computed above, yields

$$\lambda_k = \frac{|E|^k}{q^{\binom{k}{2}}}.$$

Now we need to compute II, the biggest error term. Now we recall the definition of the discrepancy function.

$$r_{k-1}\left(x^1, ..., x^{k-1}\right) = q^{-(k-1)} \sum_{\substack{s_i \in \mathbb{F}_q^* \\ i=1,2,...,k-1}} \sum_{x^k \in \mathbb{F}_q^d} E(x^k) \prod_{i=1}^{k-1} \chi(-s_i x^i \cdot x^k)$$

First, we separate the factors, then we apply Cauchy-Schwarz to the sum over the first $(k-1)$ vectors x^j. Again, we have an estimate in terms of the norm of the discrepancy.

$$II = q^{-(k-1)} \sum_{\substack{s_i \in \mathbb{F}_q^* \\ i=1,2,...,k-1}} \sum_{\substack{x^j \in \mathbb{F}_q^d \\ j=1,2,...,k}} \mathcal{D}_{k-1}(x^1, ..., x^{k-1}) E(x^k) \prod_{i=1}^{k-1} \chi(-s_i x^i \cdot x^k)$$

$$\leq \sum_{\substack{x^j \in \mathbb{F}_q^d \\ j=1,...,k-1}} \mathcal{D}_{k-1}(x^1, ..., x^{k-1}) q^{-(k-1)} \sum_{\substack{s_i \in \mathbb{F}_q^* \\ i=1,...,k-1}} \sum_{x^k \in \mathbb{F}_q^d} E(x^k) \prod_{i=1}^{k-1} \chi(-s_i x^i \cdot x^k)$$

$$\leq \lambda_{k-1}^{\frac{1}{2}} \Big(\sum_{x^1,...,x^{k-1}} r_{k-1}^2 \Big)^{\frac{1}{2}} \approx |E|^{\frac{k-1}{2}} q^{\frac{-\binom{k-1}{2}}{2}} \|r_{k-1}\|_{L^2}.$$

So we use Lemma 2.1 to get a handle on $\|r_{k-1}\|_{L^2}$. Now we are guaranteed that

$$\begin{aligned} II &\lesssim |E|^{\frac{k-1}{2}} q^{\frac{-\binom{k-1}{2}}{2}} |E|^{\frac{1}{2}} q^{\frac{(d-1)(k-1)+1}{2}} \\ &= |E|^{\frac{k}{2}} q^{\frac{(d-1)(k-1)+1-\binom{k-1}{2}}{2}}. \end{aligned}$$

To deal with III, break it up into sums that have the same number of non-zero s_j's.

$$\begin{aligned} III &= \sum_{\text{one } s_j=0} + \sum_{\text{two } s_j\text{'s}=0} + ... \\ &= d \sum_{s_1=0} + d(d-1) \sum_{s_1=s_2=0} + ... \end{aligned}$$

Now each of these sums will look like II, but with $(k-2)$ instead of $(k-1)$ for the first sum, and $(k-3)$ instead of $(k-1)$ in the second sum, and so on. This allows us to bound each sum in III as follows:

$$III \lesssim d|E|^{\frac{k-2}{2}} q^{\frac{\binom{k-2}{2}}{2}} \|r_{k-2}\|_{L^2} + d(d-1)|E|^{\frac{k-3}{2}} q^{\frac{\binom{k-3}{2}}{2}} \|r_{k-3}\|_{L^2} + \ldots$$

So III is dominated by II as long as $q > d$, which is guaranteed, as q grows arbirtarily large.

Now we only need to find appropriate conditions on E to ensure that $I > II$.

$$\begin{aligned} I &> II \\ |E|^k q^{-\binom{k}{2}} &> |E|^{\frac{k}{2}} q^{\frac{(d-1)(k-1)+1-\binom{k-1}{2}}{2}} \\ |E|^{\frac{k}{2}} &> q^{\frac{2(d-1)(k-1)+2-(k-1)(k-2)+2k(k-1)}{4}} \\ |E| &> q^{\left(\frac{k-1}{k}\right)d+\frac{k-1}{2}+\frac{1}{k}}. \end{aligned}$$

□

Now to prove the Lemma 2.1.

Proof. Recall the definition of $r_{k-1}\left(x^1, \ldots, x^{k-1}\right)$ and use orthogonality in $x^1, \ldots, x^{k-1}$.

$$\begin{aligned} \|r_{k-1}\|_{L^2}^2 &= q^{-2(k-1)} \sum_{x^1,\ldots,x^{k-1}} \sum_{\substack{s_1,s'_1,\ldots, \\ s_{k-1},s'_{k-1}}} \sum_{x^k,y^k\in E} \prod_{j=1}^{k-1} \chi((s_j x^k - s'_j y^k)\cdot x^j) \\ &= q^{d(k-1)} q^{-2(k-1)} \left(\sum_{s_j=s'_j} \sum_{\substack{x^k,y^k: \\ s_j x^k = s'_j y^k}} E(x^k)E(y^k) + \sum_{s_j\neq s'_j} \sum_{\substack{x^k,y^k: \\ s_j x^k = s'_j y^k}} E(x^k)E(y^k) \right) \\ &= q^{(d-2)(k-1)} \left(A+B\right). \end{aligned}$$

Let us approach A first. Since $s_1 = s'_1$, and $s_j x^k = s'_j y^k$ for all j, we know that it holds for $j=1$, and therefore $x^k = y^k$. This tells us that $s_j = s'_j$ for all j. So

$$A = \sum_{s_1,\ldots,s_{k-1}} \sum_{x^k} E(x^k)E(x^k) = q^{(k-1)} \sum_{x^k} E(x^k)E(x^k) = |E|q^{(k-1)}$$

Now we tackle the quantity B. Here we introduce a new variable, $\alpha = \frac{s_1}{s'_1}$. We know that $s'_j \neq 0$, as they are elements of $\mathbb{F}_q^*$. Also notice that the condition $s_j x^k = s'_j y^k$ implies $\alpha = \frac{s_j}{s'_j}$ for all j. So we did have to sum over $2(k-1)$ different variables, but now we know that these are completely determined by only $(k-1)$ of the originals. So we will have $(k-1)$ free variables. In light of this, with a simple change of variables we get

$$B = q^{(k-1)} \sum_{y^k=\alpha x^k} E(x^k)E(\alpha x^k) \leq q^{(k-1)} \sum_{x^k\in\mathbb{F}_q^d} |E\cap l_{x^k}| \leq |E|q^k$$

where $l_{x^k} := \left\{ tx^k \in \mathbb{F}_q^d : t \in \mathbb{F}_q \right\}$, which can only intersect E at most q times. With the estimates for A and B in tow,

$$\begin{aligned} \|r_{k-1}\|_{L^2}^2 &= q^{(d-2)(k-1)} \left(A + B\right) \\ &\lesssim q^{(d-2)(k-1)} \left(|E|q^{(k-1)} + |E|q^k\right) \\ &\approx |E|q^{(d-1)(k-1)+1}. \end{aligned}$$

□

3 Sharpness examples

The following lemmata are included to show how close Theorem 1.1 is to being sharp. While there are several possible notions of sharpness for this result, it is clearly interesting to consider how big a set can be without containing *any* orthogonal k-tuples. The first lemma is merely an intuitive construction used in the next lemma, both of which concern large sets with no orthogonal k-tuples.

Lemma 3.1. *There exists a set $E \subset \mathbb{F}_q^2$ such that $|E| \approx q^2$, but no pair of its vectors are orthogonal.*

Proof. This is done by taking the union of about $\frac{q}{2}$ lines through the origin, such that no two lines are perpendicular, and removing the union of their $\frac{q}{2}$ orthogonal complements, which are lines perpendicular to lines in the first union. Then our set E has about $\frac{q^2}{2}$ points, but no pair has a zero dot product. □

The next result is the main counterexample, which shows that it is possible to construct large subsets of $\mathbb{F}_q^d$ with no pairs of orthogonal vectors.

Lemma 3.2. *There exists a set $E \subset \mathbb{F}_q^d$ such that $|E| \geq cq^{\frac{d}{2}+1}$, for some $c > 0$, but no pair of its vectors are orthogonal.*

Proof. The basic idea is to construct two sets, $E_1 \subset \mathbb{F}_q^2$, and $E_2 \subset \mathbb{F}_q^{d-2}$, such that $|E_1| \approx q^{\frac{3}{2}}$ and $|E_2| \approx q^{\frac{d-1}{2}}$. If you pick q and build these sets carefully, you can guarantee that the sum set of their respective dot product sets does not contain 0. The following algorithm was inspired by [7].

Here we will indicate how to construct E_1. The construction of E_2 is similar. First, let $q = p^2$, where p is a power of a large prime. We also pick these such that $p + 1$ is of the form $4n$, where n is odd. This way we can be guaranteed a large, well-behaved multiplicative group of order $q - 1 = (p - 1)(p + 1)$, as well as a subfield of order p.

Let i denote the square root of -1, which is in $\mathbb{F}_q^*$, since q is congruent to 1 mod 4. Now let B be a cyclic subgroup of $\mathbb{F}_q^*$ of order $\frac{p+1}{4}(p-1) = n(p-1)$. Since n was odd, and p was congruent to 3 mod 4, we know that 4 does not divide the order of B. This means that B has no element of order 4, so it is clear that $i \notin B$. Let β denote the generator of B, as it is a subgroup of a cyclic group, and therefore cyclic. Since $p-1$ is even, we know that we can find another cyclic subgroup, A, generated by β^2. Let C_p be the elements of $\mathbb{F}_p^*$ that lie on the unit circle, that is,

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

From a lemma in [7], (or basic number theory) we know that $|C_p| = p - 1$, since -1 is not a square in a field of order congruent to 3 mod 4. We can be sure that for all $u, v \in C_p, u \cdot v \in \mathbb{F}_p$. Now let

$$E_1' := \{\tau u : \tau \in A, u \in C_p\}.$$

So, for all $x, y \in E_1'$, we can be sure that $x \cdot y \in A \cup \{0\}$. To see this, let $x = \sigma u$, and $y = \tau v$, where $\sigma, \tau \in A$ and $u, v \in C_p$. Then $x \cdot y = \sigma\tau(u \cdot v) \in A \cup \{0\}$, as any non-zero $u \cdot v \in \mathbb{F}_p^* \subset A$. Now, the cardinality of E_1' is

$$|E_1'| = |C_p||A| = (p-1)\left(\frac{p+1}{4}\frac{p-1}{2}\right) \approx q^{\frac{3}{2}}.$$

Now pick $\frac{q}{2}$ mutually non-orthogonal lines in E_1'. Call this collection of lines L. Let $L^\perp$ indicate the set of lines perpendicular to the lines in L. Now we need to prune E_1' so that it has no pairs of orthogonal vectors. One of the sets $E_1' \cap L$ or $E_1' \cap L^\perp$ has more points. Call the set with more points E_1. This means that no zero dot products can show up in E_1, in a similar manner to the construction in the proof of Lemma 3.1. Now we have $|E_1| \approx q^{\frac{3}{2}}$, and for any $x, y \in E_1$, we are guaranteed that $x \cdot y \in A$, which does not contain 0.

Construct $E_2 \subset \mathbb{F}_q^{d-2}$ in a similar manner, using spheres instead of circles. However, in the construction of E_2, it will not be necessary prune anything. Now we have $|E_2| \approx q^{\frac{d-1}{2}}$ and all of its dot products lie in $A \cup \{0\}$. Set $E = E_1 \times E_2$. Since E_1 has its dot product set contained in A, and E_2 has its dot product set contained in $A \cup \{0\}$, we know that any dot product of two elements in E is in the sum set $A + (A \cup \{0\})$.

Now we will show that 0 is not in the dot product set. If two elements did have a zero dot product, that would mean that we had $s, t \in A$, where s comes from the first two dimensions, or E_1, and t comes from the other $d - 2$ dimensions, or E_2, and we also have $s = -t$. (Note, even though t could conceivably be zero, s can not, so we would not have $s = -t$ if t were zero. Therefore t is necessarily an element of A.) Recall that s and t are squares of elements in B. Call them σ^2 and τ^2, respectively, for some $\sigma, \tau \in B$. Since B has multiplicative inverses, let $\alpha = \frac{\sigma}{\tau} \in B$. So we would need the following:

$$\sigma^2 = -\tau^2 \Rightarrow -1 = \frac{\sigma^2}{\tau^2} = \alpha^2.$$

But we constructed B so that it does not contain the square root of -1. Therefore there can be no two elements of E which have a zero dot product. $\square$

The authors believe that the preceeding example can be generalized to obtain results about how large a set can be without containing orthogonal k-tuples for $k > 2$.

References

[1] N. Alon and M. Krivelevich, *Constructive bounds for a Ramsey-type problem*, Graphs and Combinatorics **13** (1997), 217–225.

[2] J. Bourgain, *A Szemerédi type theorem for sets of positive density*, Israel J. Math. **54** (1986), no. 3, 307–331.

[3] V. Bergelson, *Ergodic Ramsey theory – an update*, Ergodic Theory of $\mathbb{Z}^d$ -Actions (Warwick, 1993 – 1994) (M. Pollicott and K. Schmidt, eds.), London Math. Soc. Lecture Note Ser., **228**, Cambridge Univ. Press, Cambridge, (1996).

[4] H. Furstenberg, *Recurrence in ergodic theory and combinatorial number theory*, M. B. Porter Lectures, Princeton Univ. Press, Princeton, NJ, (1981).

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

[6] D. Hart and A. Iosevich, *Ubiquity of simplices in subsets of vector spaces over finite fields*, Analysis Mathematika, **34**, (2007).

[7] 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).

[8] D. Hart, A. Iosevich, D. Koh. S. Senger and I. Uriarte-Tuero, *Distance graphs in vector spaces over finite fields, coloring and pseudo-randomness*, (submitted for publication), (2008).

[9] B. Kra, *Ergodic methods in additive combinatorics*, Centre de Recherches Mathematiques Proceedings and Lecture Notes (2007).

[10] M. Krivelevich and B. Sudakov, Pseudo-random graphs, *Conference on Finite and Infinite Sets Budapest*, Bolyai Society Mathematical Studies X, pp. 1–64.

[11] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, (1997).

[12] A. Magyar, *On distance sets of large sets of integers points*, Israel Math J. (to appear).

[13] A. Magyar, *k-point configurations in sets of positive density of $\mathbb{Z}^n$*, Duke Math J. (to appear).

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

[15] Le Anh Vinh, *On the number of orthogonal systems in vector spaces over finite fields*, Electronic Journal of Combinatorics, **15**(1) (2008) N32.

[16] T. Ziegler, *An application of ergodic theory to a problem in geometric Ramsey theory*, Israel Journal of Math. **114** (1999) 271–288.