Discrete Mathematics 311 (2011) 423–430

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

A Furstenberg–Katznelson–Weiss type theorem on $(d+1)$-point configurations in sets of positive density in finite field geometries

David Covert [a,1], Derrick Hart [b,2], Alex Iosevich [c,3], Steven Senger [a,4], Ignacio Uriarte-Tuero [d,5]

[a] Mathematics Department, 202 Mathematical Sciences Bldg, University of Missouri, Columbia, MO 65211, USA
[b] Department of Mathematics, Rutgers University, Hill Center - Busch Campus, 110 Frelinghuysen Road, Piscataway, NJ 08854-8019, USA
[c] UR Mathematics, 915 Hylan Building, University of Rochester, RC Box 270138, Rochester, NY 14627, USA
[d] Department of Mathematics, Michigan State University, East Lansing, MI 48824, USA

ARTICLE INFO

Article history:
Received 2 June 2009
Received in revised form 22 September 2010
Accepted 14 October 2010
Available online 28 December 2010

Keywords:
Vector spaces over finite fields
Furstenberg–Katznelson–Weiss
Distance sets

ABSTRACT

We show that if $E \subset \mathbb{F}_q^d$, the d-dimensional vector space over the finite field with q elements, and $|E| \geq \rho q^d$, where $q^{-\frac{1}{2}} \ll \rho \leq 1$, then E contains an isometric copy of at least $c\rho^{d-1}q^{\binom{d+1}{2}}$ distinct $(d+1)$-point configurations.

1. Background

A classical result due to Furstenberg et al. ([4]; 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. An example due to Bourgain shows that if the three point configuration in question is an arithmetic progression, then taking a δ-neighborhood is in fact necessary and the result is not otherwise true. However, it seems reasonable to conjecture that if the three point configuration is non-degenerate in the sense that the three points do not lie on the same line, then a set of positive density contains a sufficiently large dilate of this configuration.

When the size of the point set is smaller than the dimension of the ambient Euclidean space, taking a δ-neighborhood is not necessary, as shown by Bourgain [2]. He proves that if $E \subset \mathbb{R}^d$ has positive upper density and Δ_k is a k-simplex (a set of $k+1$ points which spans a k-dimensional subspace) with $k < d$, then E contains a rotated and translated image of every large dilate of Δ_k. The cases $k = d$ and $k = d+1$ remain open. See also, for example, [1,3,7,12,17] 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 Magyar in [10,11]. In particular, he proves [11] that if $d > 2k+4$ and $E \subset \mathbb{Z}^d$ has positive upper density, then all large (depending on the 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.

E-mail addresses: DavidCovert@mizzou.edu (D. Covert), DNHart@math.rutgers.edu (D. Hart), Iosevich@math.rochester.edu (A. Iosevich), Senger@math.missouri.edu (S. Senger), Ignacio@math.msu.edu (I. Uriarte-Tuero).

[1] Tel.: +1 573 884 7894; fax: +1 573 882 1869.
[2] Tel.: +1 732 445 2390x6030; fax: +1 732 445 5530.
[3] Tel.: +1 585 275 9419; fax: +1 585 273 4655.
[4] Tel.: +1 573 884 7895; fax: +1 573 882 1869.
[5] Tel.: +1 517 353 4672; fax: +517 432 1562.

0012-365X/$ – see front matter
doi:10.1016/j.disc.2010.10.009

We aim to investigate an analog of this question in finite field geometries. A step in this direction was taken [5] by the second and third listed authors. They prove that if $E \subset \mathbb{F}_q^d$, the d-dimensional vector space over the finite field with q elements, has $|E| \gtrsim q^{d\frac{k}{k+1}+\frac{k}{2}}$ and Δ is a k-simplex determined by (with vertices lying in) E, then there exists $\tau \in \mathbb{F}_q^d$ and $O \in O_d(\mathbb{F}_q)$ such that $\tau + O(\Delta) \subset E$. The result is only non-trivial in the range $d \geq \binom{k+1}{2}$ as larger simplices are out of range of the methods used.

Le Anh Vinh has also investigated k-point configurations in $\mathbb{F}_q^d$. He showed in [14] that if $E \subset \mathbb{F}_q^d$, $|E| \gtrsim q^{\frac{d-1}{2}+k}$, and $d \geq 2k$ then E contains an isometric copy of every k-simplex. Also, he showed [15] that if an arbitrary set $E \subset \mathbb{F}_q^d$ has size $E \gtrsim q^{\frac{d+2}{2}}$ (for $d \geq 3$), then it determines a positive proportion of all triangles. Based on an earlier draft of this paper, Vinh proved [13] the 2-dimensional version of our main theorem (see Theorem 1.1 below) using graph-theoretic methods. Namely, if $E \subset \mathbb{F}_q^2$ has size $|E| \geq \rho q^2$ for some $q^{-\frac{1}{2}} \ll \rho \leq 1$, then the set of triangles determined by E has size $\geq c\rho q^3$.

The purpose of this paper is to address the case of d-simplices. As before we let Δ_k denote a k-simplex, i.e. a set of $k+1$ points which span a k-dimensional subspace. Given $E \subset \mathbb{F}_q^d$, let the set of k-simplices determined by E up to congruence be denoted by

$$T_k(E) = \{\Delta_k \in E^{k+1}\}/\sim$$

where two k-simplices are equivalent if one is a rotated, shifted, reflected copy of the other.

Note that $T_k(E)$ is a natural subset of $\mathbb{F}_q^{\binom{k+1}{2}}$ (see Lemma 2.1 below). Our main result is the following.

Theorem 1.1. *Let $E \subset \mathbb{F}_q^d$ with $|E| \geq \rho q^d$ for $q^{-1/2} \ll \rho \leq 1$. Then, there exists $c > 0$ so that*

$$|T_d(E)| \geq c\rho^{d-1} q^{\binom{d+1}{2}}.$$

Remark 1.2. The viable range for ρ in Theorem 1.1 is $q^{-(d-\alpha)} \ll \rho \leq 1$, where α is the threshold so that

$$\sum_{x,x^1,\ldots,x^d} E(x)E(x^1)\ldots E(x^d)S(x-x^1)\ldots S(x-x^d) = \frac{|E|^{d+1}}{q^d}(1+o(1)),$$

whenever $|E| \gg q^{\alpha}$. Theorem 2.2 gives $\alpha = q^{d-\frac{1}{2}}$, although it is reasonable to expect $\alpha = q^{\frac{d+1}{2}}$.

Remark 1.3. We deal only with finite fields $\mathbb{F}_q$ with characteristic $p > 2$. We also assume q is much larger than the dimension d. Also, note that the error terms appearing in Theorems 3.2 and 3.1 are always of lower order in the effective range of Theorem 1.1 for $d \geq 2$.

Remark 1.4. The assumption that $|E| \geq \rho q^d$ implies that the number of $(d+1)$-point configurations determined by E (up to congruence) is at least

$$\frac{|E|^{d+1}}{\rho q^d \cdot q^{\binom{d}{2}}} \geq \rho^d q^{\binom{d+1}{2}},$$

since the size of the subset of the translation group that maps points in E to a set of size $|E|$ is no larger than ρq^d and the rotation group is of size $\approx q^{\binom{d}{2}}$. Our result shaves off a power of ρ from this trivial estimate.

2. Proof of the main result (Theorem 1.1)

Here, we roughly state the argument. We prove Theorem 1.1 by first making a reduction to a statistical statement about hinges (defined below). Having made this reduction, we next show, using a pigeonholing argument that for some $x \in E$, the hinge is large. To finish the argument, we realize a dichotomy. If the number of transformations mapping the hinge to itself is small, then a purely probabilistic argument gives the number of distinct (incongruent) $(d+1)$-point configurations is what we claim. If the number of transformations mapping the hinge to itself is large, then a purely combinatorial argument gives the result.

We start with the statistical reduction. We observe that if $|E| \geq \rho q^d$, for ρ as above, then it suffices to show that this implies that

$$\left|\left\{(a_{i,j})_{1\leq i<j\leq d+1} \in \mathbb{F}_q^{\binom{d+1}{2}} : |R_a(E)| > 0\right\}\right| \geq c\rho^{d-1} q^{\binom{d+1}{2}}, \tag{2.1}$$

where

$$R_a(E) = \{(y^1,\ldots,y^{d+1}) \in E \times \cdots \times E : \|y^i - y^j\| = a_{i,j}\},$$

and

$$\|x\| = \sum_{j=1}^{d} x_j^2.$$

This follows immediately from the following simple linear algebra lemma. The proof of this lemma will appear in Section 4 for completeness.

Lemma 2.1. *Let V be a simplex with vertices $V_i \in \mathbb{F}_q^d$, where $i = 0, \ldots, k$. Let W be another simplex with vertices $W_i \in \mathbb{F}_q^d$ for $i = 0, \ldots, k$. Suppose that*

$$\|V_i - V_j\| = \|W_i - W_j\| \tag{2.2}$$

for all i, j. Then $V \sim W$ in the sense of $T_k(E)$.

Our main estimate is the following:

Theorem 2.2. *Suppose that $\alpha_i \in \mathbb{F}_q \setminus \{0\}$ for $i = 1, \ldots, d$, and let $E \subset \mathbb{F}_q^d$. Then,*

$$|\{(x, x^1, \ldots, x^d) \in E \times \cdots \times E : \|x - x^i\| = \alpha_i\}| = \frac{|E|^{d+1}}{q^d}(1 + o(1))$$

whenever $|E| \gg q^{d-\frac{1}{2}}$.

This implies that there exists $x \in E$ so that

$$|\{(x^1, \ldots, x^d) \in E \times \cdots \times E : \|x - x^i\| = \alpha_i\}| \geq \frac{|E|^d}{q^d}(1 + o(1)). \tag{2.3}$$

Fix a d-tuple $\alpha = (\alpha_i)_{i=1}^d$, with $\alpha_i \in \mathbb{F}_q \setminus \{0\}$, for $i = 1, \ldots, d$. Define a *hinge* $h_{x,\alpha}$ to be the set $\{(x^1, \ldots, x^d) \in E \times \cdots \times E : \|x - x^i\| = \alpha_i\}$. Let $M_{x,\alpha} \subset O_d(\mathbb{F}_q)$ denote the set of orthogonal matrices which maps the hinge $h_{x,\alpha}$ to itself. We next turn our attention to the following dichotomy:

Suppose that $|M_{x,\alpha}| \leq \rho q^{\binom{d}{2}}$. By (2.3), the number of distinct d-point configurations between the d sets $\{x^i \in E : \|x - x^i\| = \alpha_i\}$ is at least

$$\frac{|h_{x,\alpha}|}{|M_{x,\alpha}|} \geq \frac{|E|^d q^{-d}(1 + o(1))}{\rho q^{\binom{d}{2}}} \geq c\rho^{d-1} q^{\binom{d}{2}}. \tag{2.4}$$

We are left only to deal with the case when $|M_{x,\alpha}| > \rho q^{\binom{d}{2}}$. We put $A_i = \{x^i \in E : \|x - x^i\| = \alpha_i\}$. It is worthwhile to point out the possibility that $A_i = A_j$. Also, although the sets A_i are not themselves spheres, they are subsets of spheres and therefore inherit some of their intersection properties. When dealing with the case $|M_{x,\alpha}| > \rho q^{\binom{d}{2}}$ we are faced with two possibilities. First, suppose that for some $i \in \{1, \ldots, d\}$ we have that $|A_i| \leq \rho q^{d-1}$. In this case we utilize the orbit-stabilizer theorem from elementary group theory:

Proposition 2.3 ([8]). *Let a group G act on a set S. Let $Gs = \{gs : g \in G\}$ be the orbit of $s \in S$, and $G_s = \{g : gs = s\}$ the isotropy group of $s \in S$. Then there is a bijection between Gs and G/G_s. Consequently,*

$$|Gs| = (G : G_s) = |G|/|G_s|.$$

We let the group $O_d(\mathbb{F}_q)$ act on $\mathbb{F}_q^d$. Recalling that $|O_d(\mathbb{F}_q)| \approx q^{\binom{d}{2}}$, and since orthogonal maps preserve the length of a certain vector, we get that the size of the orbit of any point is exactly q^{d-1}. Hence, picking some z from the previously mentioned set A_i, we get that the size of the stabilizer group of this element z is

$$|G_z| = \frac{|G|}{|Gz|} \approx \frac{q^{\binom{d}{2}}}{q^{d-1}}.$$

The final element here is to notice that

$$|M_{x,\alpha}| \leq |G_z||A_i| \leq \frac{q^{\binom{d}{2}}}{q^{d-1}} \cdot \rho q^{d-1} = \rho q^{\binom{d}{2}},$$

since the number of hinge-preserving orthogonal matrices is no more than the number of orthogonal transformations which fix a given vector $z \in A_i$, times the number of choices for that vector z, which is a contradiction. We may therefore assume

$|A_i| > \rho q^{d-1}$ for all $i = 1, \ldots, d$. Recall that we are working with the hinge $h_{x,\alpha} = \{(x^1, \ldots, x^d) \in E \times \cdots \times E : \|x - x^i\| = \alpha_i\}$, and we aim to show that the number of incongruent d-point configurations is bounded below by $c\rho^{d-1}q^{\binom{d}{2}}$.

We start by picking a point $a_1 \in A_1$. We want to know how many distinct distances occur between a_1 and points in the set A_2. To achieve this, we count how often a given distance may occur between a_1 and the points on A_2. This amounts to intersecting E with two spheres: one sphere of a given radius, centered at a_1, and the set A_2, which is, itself, a sphere intersected with E. The intersection must contain fewer than q^{d-2} possible points on the set A_2 which are at a given distance from a_1. Since $|A_2| > \rho q^{d-1}$, there must be at least $\rho q^{d-1}/q^{d-2} = \rho q$ different distances between a_1 and points on A_2, by pigeonholing.

For each of the ρq choices of a_2 which are different distances from a_1, we need to find the number of 3-point configurations that a_1 and a_2 can make with points on A_3. Now we are intersecting E with spheres of two (possibly the same) radii about a_1 and a_2 with the sphere containing S_3. There can be no more than q^{d-3} points in this intersection, which would each correspond to the same 3-point configuration. So there must be $\rho q^{d-1}/q^{d-3} = \rho q^2$ distinct 3-point configurations for each of the ρq different pairs we found before, which gives us a total of $\rho q \cdot \rho q^2 = \rho^2 q^3$ different 3-point configurations. Repeating this process, we see that we will pick up ρq^p different $(p-1)$-point configurations at each step. If we multiply all of these together, we will get a grand total of

$$\rho q \cdot \rho q^2 \cdot \ldots \cdot \rho q^{d-1} = \rho^{d-1} q^{\binom{d}{2}} \tag{2.5}$$

distinct d-point configurations.

From (2.4) and (2.5), we see that in any case, there exist no less than $c\rho^{d-1}q^{\binom{d}{2}}$ many distinct d-point configurations. Since this holds for any fixed vector $\alpha = (\alpha_i)_{i=1}^d$, and since there are $q-1$ choices for each $\alpha_i \in \mathbb{F}_q \setminus \{0\}$, then there are at least

$$c\rho^{d-1}q^{\binom{d}{2}}(q-1)^d \geq c\rho^{d-1}q^{\binom{d+1}{2}}$$

many distinct $(d+1)$-point configurations determined by E.

2.1. Fourier analysis

The Fourier transform of a function $f : \mathbb{F}_q^d \to \mathbb{C}$ is given by

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

where χ is a non-trivial additive character on $\mathbb{F}_q$. By orthogonality,

$$\sum_{x \in \mathbb{F}_q^d} \chi(-x \cdot m) = \begin{cases} q^d & m = (0, \ldots, 0) \\ 0 & m \neq (0, \ldots, 0). \end{cases}$$

Lemma 2.4. *Let $f, g : \mathbb{F}_q^d \to \mathbb{C}$. Then,*

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

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

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

3. Proof of Theorem 2.2

In order to prove Theorem 2.2 we will actually prove the more general following theorem.

Theorem 3.1. *Let $r > 2$ be an integer, and let $H_{r,\alpha}$ represent the set of r-hinges, with distances $\alpha = \{\alpha_i\}_{i=1}^{r-1}$, which are present in E. That is,*

$$H_{r,\alpha} = \{(x, x^1, \ldots, x^{r-1}) \in E \times \cdots \times E : \|x - x^i\| = \alpha_i\},$$

where $\alpha_i \neq 0$ *for* $i = 1, \ldots, r-1$. *Then,*

$$|H_{r,\alpha}| = \frac{|E|^r}{q^{r-1}}(1+o(1)),$$

whenever $|E| \gg q^{\frac{2r-5}{2r-4}d+\frac{1}{2r-4}}$.

Setting $r = d+1$ in Theorem 3.1 gives Theorem 2.2.

We will need the following estimates whose proof we delay to the end of the paper.

Theorem 3.2. *Let* $S_t = \{x \in \mathbb{F}_q^d : \|x\| = t\}$. *Identify* S_t *with its characteristic function. For* $t \neq 0$,

$$|S_t| = q^{d-1}(1+o(1)) \tag{3.1}$$

and if also $m \neq (0, \ldots, 0)$,

$$|\widehat{S}_t(m)| \lesssim q^{-\frac{d+1}{2}}. \tag{3.2}$$

We will proceed by induction. Before we handle the case $r = 3$ we first observe the following estimate which originally appeared in [6].

Lemma 3.3. *Using the notation as above, we have* $|H_{2,\alpha}| = \frac{|E|^2}{q} + O(q^{\frac{d-1}{2}}|E|)$.

To see this, write

$$\begin{aligned}|H_{2,\alpha}| &= \sum_{x,y} E(x)E(y)S(x-y)\\ &= q^{2d}\sum_m \left|\widehat{E}(m)\right|^2 \widehat{S}(m)\\ &= q^{-d}|E|^2|S| + q^{2d}\sum_{m\neq 0}\left|\widehat{E}(m)\right|^2\widehat{S}(m)\end{aligned}$$

and

$$\begin{aligned}q^{2d}\left|\sum_{m\neq 0}\left|\widehat{E}(m)\right|^2\widehat{S}(m)\right| &\leq 2q^{2d}q^{-\frac{d+1}{2}}q^{-d}|E|\\ &= 2q^{\frac{d-1}{2}}|E|.\end{aligned}$$

We now illustrate the base step. First we write

$$|H_{3,\alpha}| = \sum_{x\in E}|E\cap(x-S)|^2.$$

Now,

$$\begin{aligned}|E\cap(x-S)| &= \sum_y E(y)S(x-y) = q^d\sum_m \widehat{E}(m)\widehat{S}(m)\chi(m\cdot x)\\ &= |E||S|q^{-d} + q^d\sum_{m\neq 0}\widehat{E}(m)\widehat{S}(m)\chi(m\cdot x),\end{aligned}$$

which gives

$$\begin{aligned}|H_{3,\alpha}| &= \sum_{x\in E}|E\cap(x-S)|^2\\ &= |E|^3|S|^2q^{-2d} + 2|E||S|q^d\sum_{m\neq 0}|\widehat{E}(m)|^2|\widehat{S}(m)| + q^{2d}\sum_x\left|\sum_{m\neq 0}\widehat{E}(m)\widehat{S}(m)\chi(m\cdot x)\right|^2\\ &= |E|^3|S|^2q^{-2d} + O\left(|E|^2|S|q^{-d}q^{(d-1)/2} + q^{3d}\sum_{m\neq 0}|\widehat{E}(m)|^2|\widehat{S}(m)|^2\right)\\ &= |E|^3|S|^2q^{-2d} + O\left(|E|^2|S|q^{-d}q^{(d-1)/2} + q^{d-1}|E|\right).\end{aligned}$$

If $|E| \gg q^{\frac{d+1}{2}}$ then

$$|H_{3,\alpha}| = |E|^3 q^{-2}(1+o(1)).$$

For the inductive step, assume that we are in the case $|H_{r,\alpha}| = \frac{|E|^r}{q^{r-1}}(1+o(1))$ for $|E| \gg q^{\frac{2r-5}{2r-4}d+\frac{1}{2r-4}}$. We begin by writing

$$\begin{aligned}
|H_{r+1,\alpha}| &= \sum_{x,x^1,\ldots,x^r} H_{r,\alpha}(x,x^1,\ldots,x^{r-1})E(x^r)S(x-x^r) \\
&= q^{(r+1)d}\sum_m \widehat{H}_{r,\alpha}(m,0,\ldots,0)\widehat{S}(m)\widehat{E}(m) \\
&= q^{-d}|E||S||H_{r,\alpha}| + q^{(r+1)d}\sum_{m\neq 0}\widehat{H}_{r,\alpha}(m,0,\ldots,0)\widehat{S}(m)\widehat{E}(m) \\
&= q^{-d}|E||S||H_{r,\alpha}| + R.
\end{aligned}$$

Applying Cauchy–Schwarz gives

$$\begin{aligned}
R^2 &\leq q^{2d(r+1)}\sum_{m\neq 0}|\widehat{S}(m)|^2|\widehat{E}(m)|^2\sum_{m\neq 0}|\widehat{H}_{r,\alpha}(m,0,\ldots,0)|^2 \\
&\lesssim q^{2d(r+1)}q^{-d-1}q^{-d}|E|\sum_{m\neq 0}|\widehat{H}_{r,\alpha}(m,0,\ldots,0)|^2 \\
&\leq q^{2dr-1}|E|\sum_m|\widehat{H}_{r,\alpha}(m,0,\ldots,0)|^2.
\end{aligned}$$

Also, we have that

$$\begin{aligned}
\widehat{H}_{r,\alpha}(m,0,\ldots,0) &= q^{-rd}\sum_{x,x^1,\ldots,x^{r-1}}\chi(x\cdot m)E(x)E(x^1)\ldots E(x^{r-1})S(x-x^1)\ldots S(x-x^{r-1}) \\
&= q^{-rd+d}\widehat{f}(m)
\end{aligned}$$

where

$$f(x) = E(x)\sum E(x^1),\ldots,E(x^{r-1})S(x-x^1)\ldots S(x-x^{r-1}) = E(x)|E\cap(x-S)|^{r-1}.$$

Since $|E\cap(x-S)| \leq q^{d-1}$, it follows that

$$\begin{aligned}
A = \sum_m|\widehat{H}_{r,\alpha}(m,0,\ldots,0)|^2 &= q^{-2rd+2d}\sum_m|\widehat{f}(m)|^2 \\
&= q^{-2rd+d}\sum_x|f(x)|^2 \\
&\leq q^{-2rd+d}\left(q^{d-1}\right)^{2(r-2)}|H_{3,\alpha}|
\end{aligned}$$

and

$$A \lesssim q^{-2rd+d}\left(q^{d-1}\right)^{2(r-2)}|E|^3q^{-2}(1+o(1)).$$

Finally,

$$R^2 \lesssim q^{-3}q^d\left(q^{d-1}\right)^{2(r-2)}|E|^4(1+o(1)) \leq q^{(2r-3)d-2r+1}|E|^4(1+o(1)).$$

Therefore,

$$|H_{r+1,\alpha}| = q^{-d}|E||S||H_{r,\alpha}| + O(q^{d\frac{2r-3}{2}-r+\frac{1}{2}}|E|^2),$$

and we have that

$$|H_{r+1,\alpha}| = \frac{|E|^{r+1}}{q^r}(1+o(1)),$$

whenever

$$|E| \gg q^{\frac{2r-3}{2r-2}d+\frac{1}{2r-2}}.$$

4. Proof of Lemma 2.1

Let $\pi_r(x)$ denote the rth coordinate of x. By translating, we may assume that $V_0 = \vec{0}$. We may also assume that $V_1, \ldots, V_k$ are contained in $\mathbb{F}_q^k$. The condition that $\|V_i - V_j\| = \|W_i - W_j\|$ for all i, j 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 transformation uniquely defined by $T(V_i) = W_i$. To show that T is orthogonal it suffices to show that $\|Tx\| = \|x\|$ for all x. By assumption, the V_i's form a basis, so we have

$$x = \sum_i t_i V_i.$$

Thus, by (4.1), we have that

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

giving the result.

5. Proof of Theorem 3.2

For any $l \in \mathbb{F}_q^d$, we have

$$\begin{aligned}\widehat{S_t}(l) &= q^{-d} \sum_{x \in \mathbb{F}_q^d} q^{-1} \sum_{j \in \mathbb{F}_q} \chi(j(\|x\| - t))\chi(-x \cdot l) \\ &= q^{-1}\delta(l) + q^{-d-1} \sum_{j \in \mathbb{F}_q^*} \chi(-jt) \sum_x \chi(j\|x\|)\chi(-x \cdot l),\end{aligned} \tag{5.1}$$

where the notation $\delta(l) = 1$ if $l = (0 \ldots, 0)$ and $\delta(l) = 0$ otherwise.

Now

$$\widehat{S_t}(l) = q^{-1}\delta(l) + Q^d q^{-\frac{d+2}{2}} \sum_{j \in \mathbb{F}_q^*} \chi\left(\frac{\|l\|}{4j} + jt\right) \eta^d(-j).$$

In the last line we have completed the square, changed j to $-j$, and used d times the Gauss sum equality

$$\sum_{c \in \mathbb{F}_q} \chi(jc^2) = \eta(j) \sum_{c \in \mathbb{F}_q} \eta(c)\chi(c) = \eta(j) \sum_{c \in \mathbb{F}_q^*} \eta(c)\chi(c) = Q\sqrt{q}\eta(j), \tag{5.2}$$

where the constant Q equals ± 1 or $\pm i$, depending on q, and η is the quadratic multiplicative character (or the Legendre symbol) of $\mathbb{F}_q^*$. (see, e.g. [9], for more information).

The conclusion to both parts of Theorem 3.2 now follows from the following classical estimate due to Weil [16].

Theorem 5.1. *Let*

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

where ψ is a multiplicative character on $\mathbb{F}_q \setminus \{0\}$. Then if $a \neq 0$,

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

References

[1] V. Bergelson, Ergodic Ramsey theory – an update, in: M. Pollicott, K. Schmidt (Eds.), Ergodic Theory of $\mathbb{Z}^d$- actions, in: London Math. Soc. Lecture Note Series, vol. 228, 1996, pp. 1–61.
[2] J. Bourgain, A Szemeredi type theorem for sets of positive density, Israel J. Math. 54 (3) (1986) 307–331.
[3] H. Furstenberg, Recurrence in ergodic theory and combinatorial number theory, in: M.B. Porter Lectures, Princeton Univ. Press, Princeton, NJ, 1981.
[4] H. Furstenberg, Y. Katznelson, B. Weiss, Ergodic theory and configurations in sets of positive density, in: Mathematics of Ramsey theory, in: Alg. Combin., vol. 5, Springer, Berlin, 1990, pp. 184–198.
[5] D. Hart, A. Iosevich, Ubiquity of simplices in subsets of vector spaces over finite fields, Anal. Math. 34 (1) (2008) (10 pages).
[6] A. Iosevich, M. Rudnev, Erdös distance problem in vector spaces over finite fields, Trans. Amer. Math. Soc. 359 (12) (2007) 6127–6142.
[7] B. Kra, Ergodic methods in additive combinatorics, in: Centre de Recherches Mathematiques Proceedings and Lecture Notes, 2007.
[8] S. Lang, Algebra, Addison-Wesley Publishing Company, Menlo Park, California, 1984.
[9] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, 1997.

[10] A. Magyar, On distance sets of large sets of integer points, Israel J. of Math. 164 (1) (2008) 251–263.
[11] A. Magyar, k-point configurations in sets of positive density of $\mathbb{Z}^n$, Duke Math. J. 146 (1) (2009) 1–34.
[12] T. Tao, V. Vu, Additive Combinatorics, Cambridge University Press, 2006.
[13] L.A. Vinh, On a Furstenberg–Katznelson–Weiss type theorem over finite fields, Ann. Comb. (2008) (in press).
[14] L.A. Vinh, On kaleidoscopic psuedo-randomness of finite Euclidean graphs, preprint, 2008.
[15] L.A. Vinh, Triangles in vector spaces over finite fields, Online J. Anal. Comb. (2008) (in press).
[16] A. Weil, On some exponential sums, Proc. Nat. Acad. Sci. USA 34 (1948) 204–207.
[17] T. Ziegler, An application of ergodic theory to a problem in geometric Ramsey theory, Israel J. Math. 114 (1999) 271–288.