Orthogonal systems in vector spaces over finite rings

Pham Van Thang

Faculty of Mathematics, Mechanics and Informatics
Hanoi University of Science
Vietnam National University, Hanoi
phmanhthang@gmail.com

Le Anh Vinh*

University of Education
Vietnam National University, Hanoi
vinhla@vnu.edu.vn

Submitted: Mar 19, 2012; Accepted: Jun 21, 2012; Published: Jun 28, 2012
Mathematics Subject Classification: 05C35, 05C38

Abstract

We prove that if a subset of the d-dimensional vector space over the ring of integers modulo p^r is large enough, then the number of k-tuples of mutually orthogonal vectors in this set is close to its expected value.

1 Introduction

The classical Erdős distance problem asks for the minimal number of distinct distances determined by a finite point set in $\mathbb{R}^l$, $l \geqslant 2$. This problem in the Euclidean plane has recently been solved by Guth and Katz ([8]). They showed that a set of N points in $\mathbb{R}^2$ has at least $cN/\log N$ distinct distances. For the latest developments on the Erdős distance problem in higher dimensions, see [11, 15], and the references contained therein. Let $\mathbb{F}_q$ denote a finite field with q elements, where q, a power of an odd prime, is viewed as an asymptotic parameter. For $\mathcal{E} \subset \mathbb{F}_q^l$ ($l \geqslant 2$), the finite analogue of the classical Erdős distance problem is to determine the smallest possible cardinality of the set

$$\Delta(\mathcal{E}) = \{\|\boldsymbol{x} - \boldsymbol{y}\| = (x_1 - y_1)^2 + \ldots + (x_l - y_l)^2 : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}\} \subset \mathbb{F}_q.$$

The first non-trivial result on the Erdős distance problem in vector spaces over finite fields is due to Bourgain, Katz, and Tao ([2]), who showed that if q is a prime, $q \equiv 3$ (mod

*The research is supported by University of Education, Vietnam National University, Hanoi, Grant No. QS.12.04

4), then for every $\varepsilon > 0$ and $\mathcal{E} \subset \mathbb{F}_q^2$ with $|\mathcal{E}| \leqslant C_\varepsilon q^{2-\epsilon}$, there exists $\delta > 0$ such that $|\Delta(\mathcal{E})| \geqslant C_\delta |\mathcal{E}|^{\frac{1}{2}+\delta}$ for some constants C_ε, C_δ. The relationship between ϵ and δ in their arguments, however, is difficult to determine. In addition, it is quite subtle to go up to higher dimensional cases with these arguments. Iosevich and Rudnev ([10]) used Fourier analytic methods to show that there are absolute constants $c_1, c_2 > 0$ such that for any odd prime power q and any set $\mathcal{E} \subset \mathbb{F}_l^d$ of cardinality $|\mathcal{E}| \geqslant c_1 q^{l/2}$, we have

$$|\Delta(\mathcal{E})| \geqslant c_2 \min\left\{q, q^{\frac{l-1}{2}}|\mathcal{E}|\right\}. \tag{1}$$

In [22], Van Vu gave another proof of (1) using the graph theoretic method (see also [16] for a similar proof). Iosevich and Rudnev reformulated the question in analogy with the Falconer distance problem: how large does $\mathcal{E} \subset \mathbb{F}_q^l$, $l \geqslant 2$, needed to be ensure that $\Delta(\mathcal{E})$ contains a positive proportion of the elements of $\mathbb{F}_q$. The above result implies that if $|\mathcal{E}| \geqslant 2q^{\frac{l+1}{2}}$ then $\Delta(\mathcal{E}) = \mathbb{F}_q$ directly in line with Falconer's result in Euclidean setting that for a set $\mathcal{E}$ with Hausdorff dimension greater than $(l+1)/2$, the distance set is of positive measure. At first, it seems reasonable that the exponent $(l+1)/2$ may be improvable, in line with the Falconer distance conjecture described above. However, Hart, Iosevich, Koh and Rudnev discovered in [6] that the arithmetic of the problem makes the exponent $(l+1)/2$ best possible in odd dimensions, at least in general fields. In even dimensions, it is still possible that the correct exponent is $l/2$, in analogy with the Euclidean case. In [3], Chapman et al. took a first step in this direction by showing that if $\mathcal{E} \subset \mathbb{F}_q^2$ satisfies $|\mathcal{E}| \geqslant q^{4/3}$ then $|\Delta(\mathcal{E})| \geqslant cq$. This is in line with Wolff's result for the Falconer conjecture in the plane which says that the Lebesgue measure of the set of distances determined by a subset of the plane of Hausdorff dimension greater than $4/3$ is positive.

A classical result due to Furstenberg, Katznelson and Weiss ([7]) states that if $\mathcal{E} \subset \mathbb{R}^2$ of positive upper Lebesgue density, then for any $\delta > 0$, the δ-neighborhood of $\mathcal{E}$ contains a congruent copy of a sufficiently large dilate of every three-point configuration. An example of Bourgain ([1]) showed that it is not possible to replace the thickened set $\mathcal{E}_\delta$ by $\mathcal{E}$ for arbitrary three-point configurations. In the case of k-simplex, that is the $k+1$ points spanning a k-dimensional subspace, Bourgain ([1]), using Fourier analytic techniques, showed that a set $\mathcal{E}$ of positive upper Lebesgue density always contains a sufficiently large dilate of every non-degenerate k-point configuration where $k < l$. In the case $k = l$, the problem still remains open. Using Fourier analytic methods, Akos Magyar ([13, 14]) considered this problem over the integer lattice $\mathbb{Z}^l$. He showed that a set of positive density will contain a congruent copy of every large dilate of a non-degenerate k-simplex where $l > 2k + 4$.

Hart and Iosevich ([9]) made the first investigation in an analog of this question in finite field geometries. Let P_k denote a k-simplex. Given another k-simplex P_k', we say $P_k \sim P_k'$ if there exist $\tau \in \mathbb{F}_q^l$, and $O \in SO_l(\mathbb{F}_q)$, the set of l-by-l orthogonal matrices over $\mathbb{F}_q$, such that $P_k' = O(P_k) + \tau$. Under this equivalent relation, Hart and Iosevich ([9]) observed that one may specify a simplex by the distances determined by its vertices. They showed that if $\mathcal{E} \subset \mathbb{F}_q^l$ ($l \geqslant \binom{k+1}{2}$) of cardinality $|\mathcal{E}| \gtrsim q^{\frac{kl}{k+1}+\frac{k}{2}}$ then $\mathcal{E}$ contains a congruent copy of every k-simplex (with the exception of simplices with zero distances).

Using graph theoretic methods, the second listed author ([19]) showed that the same result holds for $l \geqslant 2k$ and $|\mathcal{E}| \gg q^{\frac{l-1}{2}+k}$. Here and throughout, $X \gtrsim Y$ means that $X \geqslant CY$ for some large constant C and $X \gg Y$ means that $Y = o(X)$, where X, Y are viewed as functions of the parameter q. In [18], the author studied the triangles in three-dimensional vector spaces over finite fields. Using a combination of graph theory methods and Fourier analytic techniques, the second listed author showed that if $\mathcal{E} \subset \mathbb{F}_q^l$ ($l \geqslant 3$) of cardinality $|\mathcal{E}| \gtrsim q^{\frac{l+2}{2}}$, the set of triangles, up to congruence, has density greater than c. Using Fourier analytic techniques, Chapman et al ([3]) extended this result to higher dimensional cases. More precisely, they showed that if $|\mathcal{E}| \gtrsim q^{\frac{l+k}{2}}$ ($l \geqslant k$) then the set of k-simplices, up to congruence, has density greater than c. They also obtained a stronger result when $\mathcal{E}$ is a subset of the l-dimensional unit sphere $S^l = \{\boldsymbol{x} \in \mathbb{F}_q^l : \|\boldsymbol{x}\| = 1\}$. In particular, it was proven ([3, Theorem 2.15]) that if $\mathcal{E} \subset S^l$ of cardinality $|\mathcal{E}| \gtrsim q^{\frac{l+k-1}{2}}$ then $\mathcal{E}$ contains a congruent copy of a positive proportion of all k-simplices (see also [19] for a different proof of these results using graph-theoretic methods).

In [4], Iosevich and Senger showed that a sufficiently large subset of $\mathbb{F}_q^d$, the d-dimensional vector space over the finite field with q elements, contains many k-tuple of mutually orthogonal vectors. Using geometric and character sum machinery, they proved the following result.

Theorem 1 ([4, Theorem 1.1]) *Let $E \subset \mathbb{F}_q^d$, such that*

$$|E| \gtrsim q^{d\frac{k-1}{k}+\frac{k-1}{2}+\frac{1}{k}}, \tag{2}$$

where $0 < \binom{k}{2} < d$. Then the number of k-tuples of k mutually orthogonal vectors in E is

$$(1+o(1))\frac{|E|^k}{k!}q^{-\binom{k}{2}}. \tag{3}$$

In [17], the second listed author obtained a stronger result using graph theoretic methods.

Theorem 2 ([17, Theorem 1.2]) *Let $E \subset \mathbb{F}_q^d$, such that*

$$|E| \gg q^{\frac{d}{2}+k-1}, \tag{4}$$

where $d > 2(k-1)$. Then the number of k-tuples of k mutually orthogonal vectors in E is

$$(1+o(1))\frac{|E|^k}{k!}q^{-\binom{k}{2}}. \tag{5}$$

Note that Theorem 1 only works in the range $d > \binom{k}{2}$ (as larger tuples of mutually orthogonal vectors are out of range of the methods used) while Theorem 2 works in a wider range $d > 2(k-1)$. Moreover, Theorem 2 is stronger than Theorem 1 in the same range. It is also interesting to note that the exponent $\frac{d}{2}+1$ cannot be improved in the case

$k = 2$. In [4], Iosevich and Senger constructed a set $E \subset \mathbb{F}_q^d$ such that $|E| \geqslant cq^{\frac{d+1}{2}+1}$, for some $c > 0$, but no pair of its vectors are orthogonal (see Lemma 3.2 in [4]). Their basic idea is to construct $E = E_1 \oplus E_2$ where $E_1 \subset \mathbb{F}_q^2$ and $E_2 \subset \mathbb{F}_q^{d-2}$, such that $|E_1| \approx q^{1/2}$, $|E_2| \approx q^{\frac{d-1}{2}}$ and the sum set of their respective dot product sets does not contain 0.

Covert, Iosevich, and Pakianathan ([5]) extended (1) to the setting of finite cyclic rings $\mathbb{Z}_{p^l} = \mathbb{Z}/p^l\mathbb{Z}$, where p is a fixed odd prime and $l \geqslant 2$. One reason for considering this situation is that if one is interested in answering questions about sets $\mathcal{E} \subset \mathbb{Q}^d$ of rational points, one can ask questions about distance sets for such sets and how they compare to the current results in $\mathbb{R}^d$. By scale invariance of these questions, the problem of obtaining sharp bounds for the relationship of $|\Delta(\mathcal{E})|$ and $|\mathcal{E}|$ for a subset $\mathcal{E}$ of $\mathbb{Q}^d$ would be the same as for subsets of $\mathbb{Z}^d$. Covert, Iosevich, and Pakianathan ([5]) obtained a nearly sharp bound for the distance problem in vector spaces over finite ring $\mathbb{Z}_q$. More precisely, they proved that if $\mathcal{E} \subset \mathbb{Z}_q^d$ of cardinality

$$|\mathcal{E}| \gg r(r+1)q^{\frac{(2r-1)d}{2r}+\frac{1}{2r}},$$

then

$$\mathbb{Z}_q^\times \subset \Delta(\mathcal{E}),$$

where $\mathbb{Z}_q^\times$ is the set of units of $\mathbb{Z}_q$. In [21], the second listed author reproved this result using graph-theoretic methods. Furthermore, the author showed that if $\mathcal{E}$ is sufficiently large then there exists a very large subset of $\mathcal{E}$ such that every point in this subset determines almost all possible distances to the set $\mathcal{E}$. The main purpose of this paper to extend Theorem 1 and Theorem 2 in the setting of finite cyclic rings $\mathbb{Z}_{p^l} = \mathbb{Z}/p^l\mathbb{Z}$. Note that, the arithmetic of finite rings allows for a richer orthogonal structure. More precisely, we have the following theorem.

Theorem 3 *Let $q = p^r$ be an odd prime power and $E \subset \mathbb{Z}_q^d$. Suppose that*

$$|E| \gg p^{r(d+k-2)+\left(1-\frac{d}{2}\right)},$$

where $d \geqslant 2r - 2$. Then the number of k-tuples of k mutually orthogonal vectors in E is

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

Note that Theorem 3 only works in the range $d/2 > r(k-2)+1$ (as larger tuples of mutually orthogonal vectors are out of range of the methods used). Recall that Iosevich and Senger ([4, Lemma 3.2]) constructed a subset $E \subset \mathbb{F}_p^d$ such that $|E| \gtrsim p^{\frac{d+1}{2}}$ but no pair of its vectors are orthogonal. Under the projection homomorphism $\pi : \mathbb{Z}_q^d \to \mathbb{Z}_p^d$, let $L = \pi^{-1}(E)$. Then

$$|L| = p^{(r-1)d}|E| \gtrsim p^{rd+\frac{1}{2}-\frac{d}{2}}$$

and $\boldsymbol{u} \cdot \boldsymbol{v} \neq 0$ for any $\boldsymbol{u}, \boldsymbol{v} \in L$. Hence, Theorem 3 is best possible up to a factor of $p^{1/2}$ in the case $k = 2$. The authors believe that the above example can be generalized to obtain results about how large a set in $\mathbb{Z}_{p^r}^d$ can be without containing orthogonal k-tuples for $k > 2$.

2 Zero-product graphs

We call a graph $G = (V, E)$ (n, l, λ)-graph if G is a l-regular graph on n vertices with the absolute values of each of its eigenvalues but the largest one is at most λ. It is well-known that if $\lambda \ll l$ then an (n, l, λ)-graph behaves similarly to a random graph $G(n, l/n)$, in which every possible edge occurs independently with probability l/n. Let H be a fixed graph of order v with e edges and with automorphism group $\mathrm{Aut}(H)$. Using the second moment method, it is not difficult to show that for every constant p, the random graph $G(n, p)$ contains

$$(1 + o(1))p^e(1 - p)^{\binom{v}{2}-e}\frac{n^v}{|\operatorname{Aut}(H)|} \tag{6}$$

induced copies of H. Alon extended this result to (n, l, λ)-graphs. He proved that every large subset of the set of vertices of an (n, l, λ)-graph contains the "correct" number of copies of any fixed small subgraph (Theorem 4.10 in [12]).

Theorem 4 ([12]) *Let H be a fixed graph with e edges, v vertices and maximum degree Δ, and let $G = (V, E)$ be an (n, l, λ)-graph, where, say, $l \leqslant 0.9n$. Let $m < n$ satisfy $m \gg \lambda \left(\frac{n}{l}\right)^{\Delta}$. Then, for every subset $U \subset V$ of cardinality m, the number of (not necessarily induced) copies of H in U is*

$$(1 + o(1))\frac{m^v}{|\operatorname{Aut}(H)|}\left(\frac{l}{n}\right)^e. \tag{7}$$

Note that the above theorem, proved for simple graphs in [12], remains true if we allow loops (i.e. edges that connects a vertex to itself) in the graph G. There is no different between the proof in [12] for simple graphs and the proof for graphs with loops.

Suppose that $q = p^r$ for some odd prime p and $r \geqslant 2$. We identify $\mathbb{Z}_q$ with $\{0, 1, ..., q-1\}$, then $p\mathbb{Z}_{p^{r-1}}$ is the set of nonunits in $\mathbb{Z}_q$. For any $d \geqslant 2$, the zero-product graph $\mathcal{ZP}_{q,d}$ is defined as follows. The vertex set of the zero-product graph $\mathcal{ZP}_{q,d}$ is the set $V(\mathcal{ZP}_{q,d}) = \mathbb{Z}_{p^r}^d \backslash (p\mathbb{Z}_{p^{r-1}})^d$. Two vertices $\boldsymbol{a}$ and $\boldsymbol{b} \in V(\mathcal{ZP}_{q,d})$ are connected by an edge, $(\boldsymbol{a}, \boldsymbol{b}) \in E(\mathcal{ZP}_{q,d})$, if and only if $\boldsymbol{a} \cdot \boldsymbol{b} = 0 \in \mathbb{Z}_q$. We have the following pseudo-randomness of the zero-product graph $\mathcal{ZP}_{q,d}$.

Theorem 5 *For any $d \geqslant 2$, the zero-product graph $\mathcal{ZP}_{q,d}$ is an*

$$\left(p^{rd} - p^{(r-1)d}, p^{r(d-1)} - p^{(r-1)(d-1)}, r\sqrt{p^{(2r-1)d-2r+2}}\right) - \textit{graph}.$$

Proof

It follows from the definition of the zero-product graph $\mathcal{ZP}_{q,d}$ that $V(\mathcal{ZP}_{q,d})$ is a graph of order $p^{rd} - p^{(r-1)d}$. The valency of the graph is also easy to compute. Given a vertex $\boldsymbol{x} \in V(\mathcal{ZP}_{q,d})$, there exists an index i such that $x_i \in \mathbb{Z}_q^\times$. We can assume that $x_1 \in \mathbb{Z}_q^\times$.If we choose $y_2, \ldots, y_d \in \mathbb{Z}_q$ not simultaneously nonunits arbitrarily, then y_1 is determined uniquely such that $\boldsymbol{x} \cdot \boldsymbol{y} = 0$ (note that, if $y_2, \ldots, y_d \in p\mathbb{Z}_{p^{r-1}}$ then so is y_1.) Hence, $\mathcal{ZP}_{q,d}$ is a regular graph of valency $p^{r(d-1)} - p^{(r-1)(d-1)}$.

It remains to estimate the eigenvalues of this multigraph (i.e. graph with loops). Note that, in order to bound the second largest eigenvalue of a matrix A, it is sometimes easier to work with A^2. For any $\boldsymbol{a} \neq \boldsymbol{b} \in \mathbb{Z}_{p^r}^d \backslash (p\mathbb{Z}_{p^{r-1}})^d$, we count the number of solutions of the following system

$$\boldsymbol{a} \cdot \boldsymbol{x} \equiv \boldsymbol{b} \cdot \boldsymbol{x} \equiv 0 \mod p^r, \ \boldsymbol{x} \in \mathbb{Z}_{p^r}^d \backslash (p\mathbb{Z}_{p^{r-1}})^d. \tag{8}$$

There exist uniquely $0 \leqslant \alpha \leqslant r-1$ and $\boldsymbol{b}_1 \in (\mathbb{Z}_{p^{r-\alpha}})^d \backslash (p\mathbb{Z}_{p^{r-1-\alpha}})^d$ such that $\boldsymbol{b} = \boldsymbol{a} + p^\alpha \boldsymbol{b}_1$. The system (8) above becomes

$$\boldsymbol{a} \cdot \boldsymbol{x} \equiv \ p^\alpha \boldsymbol{b}_1 \cdot \boldsymbol{x} \equiv 0 \mod p^r, \ \boldsymbol{x} \in (\mathbb{Z}_{p^r})^d \backslash (p\mathbb{Z}_{p^{r-1}})^d. \tag{9}$$

Let $\boldsymbol{a}_\alpha \in (\mathbb{Z}_{p^{r-\alpha}})^d \backslash (p\mathbb{Z}_{p^{r-1-\alpha}})^d \equiv \boldsymbol{a} \mod p^{r-\alpha}$ and $\boldsymbol{x}_\alpha \in (\mathbb{Z}_{p^{r-\alpha}})^d \backslash (p\mathbb{Z}_{p^{r-1-\alpha}})^d$, $\boldsymbol{x}_\alpha \equiv \boldsymbol{x} \mod p^{r-\alpha}$. To solve (9), we first solve the following system

$$\boldsymbol{a}_\alpha \cdot \boldsymbol{x}_\alpha \equiv \boldsymbol{b}_1 \cdot \boldsymbol{x}_\alpha \equiv 0 \mod p^{r-\alpha}, \ \boldsymbol{x}_\alpha \in (\mathbb{Z}_{p^{r-\alpha}})^d \backslash (p\mathbb{Z}_{p^{r-1-\alpha}})^d. \tag{10}$$

Let $\boldsymbol{a}_\alpha = (a_1, \ldots, a_d)$, $\boldsymbol{x}_\alpha = (x_1, \ldots, x_d)$ and $\boldsymbol{b}_1 = (b_1, \ldots, b_d)$. Since $\boldsymbol{a}_\alpha \in (\mathbb{Z}_{p^{r-\alpha}})^d \setminus (p\mathbb{Z}_{p^{r-1-\alpha}})^d$, there exists $a_i \in \mathbb{Z}_q^\times$. W.l.o.g., we can assume that $a_1 \in \mathbb{Z}_q^\times$. Let $k_1 = a_2x_2 + \ldots + a_dx_d$ and $k_2 = b_2x_2 + \ldots + b_dx_d$. System (10) is equivalent to the following system.

$$a_1x_1 + k_1 \equiv 0 \mod p^{r-\alpha}, \quad b_1x_1 + k_2 \equiv 0 \mod p^{r-\alpha}, \tag{11}$$

which implies that

$$a_1k_2 - b_1k_1 \equiv 0 \mod p^{r-\alpha}. \tag{12}$$

Therefore, if $\boldsymbol{x}_\alpha$ is a solution of (10) then $(x_2, \ldots, x_d)$ satisfies Eq. (12). We now count the number of solutions of this equation. Note that Eq. (12) can be written as

$$(a_1b_2 - a_2b_1)x_2 + \ldots + (a_1b_d - a_db_1)x_d \equiv 0 \mod p^{r-\alpha}. \tag{13}$$

Let p^β be the greatest common divisor of $a_1b_2 - a_2b_1, \ldots, a_1b_d - a_db_1$. Note that, Eq. (13) equivalent to $\boldsymbol{a}_\alpha \equiv t\boldsymbol{b}_1 \mod p^\beta$ for some $t \in \mathbb{Z}_{p^\beta}^\times$. Set $t_i = (a_1b_i - a_ib_1)/p^\beta$, then Eq. (13) becomes

$$p^\beta(t_2x_2 + \ldots t_dx_d) \equiv 0 \mod p^{r-\alpha}. \tag{14}$$

By the way of choosing β, there exists an index $t_i \notin p\mathbb{Z}_{p^{r-1-\alpha}}$. We can assume that $t_2 \notin p\mathbb{Z}_{p^{r-1-\alpha}}$. If we choose $x_3, \ldots, x_d \in \mathbb{Z}_{p^{r-\alpha}}$ not simultaneously nonunits arbitrarily, then x_2 is determined uniquely. (Note that, if $x_3, \ldots, x_d \in p\mathbb{Z}_{p^{r-1-\alpha}}$ then $x_2 \in p\mathbb{Z}_{p^{r-1-\alpha}}$. This also implies that $x_1 \in p\mathbb{Z}_{r-1-\alpha}$, which contradicts the definition of $\boldsymbol{x}$ in Eq. (10).) Hence, Eq. (14) has $p^{(r-\alpha)(d-1)} - p^{(r-\alpha-1)(d-1)}$ solutions if $\beta = r - \alpha$ and has $(p^{(r-\alpha)(d-2)} - p^{(r-\alpha-1)(d-2)})p^\beta$ solutions otherwise.

Since $a_1 \in \mathbb{Z}_q^\times$, we have a unique choice of x_1 for each solution $(x_2, .., x_d)$. Given a solution, $\boldsymbol{x}_\alpha$, of (10), upon putting everything back into the system

$$\boldsymbol{a} \cdot \boldsymbol{x} \equiv 0 \mod p^r, \ \boldsymbol{x} \equiv \boldsymbol{x}_\alpha \mod p^{r-\alpha}, \tag{15}$$

we get $p^{\alpha(d-1)}$ solutions of the system (9). Therefore, set

$$v_{\alpha,\beta} = (p^{(r-\alpha)(d-1)} - p^{(r-\alpha-1)(d-1)})p^{\alpha(d-1)} \text{ if } \beta = r - \alpha$$

and

$$v_{\alpha,\beta} = (p^{(r-\alpha)(d-2)} - p^{(r-\alpha-1)(d-2)})p^{\beta}p^{\alpha(d-1)} \text{ if } \beta < r-\alpha,$$

then the system (8) has $v_{\alpha,\beta}$ solutions.

For any $0 \leqslant \alpha \leqslant r-1, 0 \leqslant \beta \leqslant r-\alpha$, let $B_{E_{\alpha,\beta}}$ be a graph with the vertex set $V(B_{E_{\alpha,\beta}}) = V(\mathcal{ZP}_{q,d})$. For any two vertices $\boldsymbol{a}, \boldsymbol{b} \in (\mathbb{Z}_q)^d \backslash (p\mathbb{Z}_{p^{r-1}})^d$, $(\boldsymbol{a}, \boldsymbol{b})$ is an edge of $B_{E_{\alpha,\beta}}$ if and only if $\boldsymbol{b} = \boldsymbol{a} + p^{\alpha}\boldsymbol{b}_1$ for some $\boldsymbol{b}_1 \in (\mathbb{Z}_{p^{r-\alpha}})^d \backslash (\mathbb{Z}_{p^{r-1-\alpha}})^d$. Let $\boldsymbol{a}_\alpha \in (\mathbb{Z}_{p^{r-\alpha}})^d \backslash (p\mathbb{Z}_{p^{r-\alpha-1}})^d \equiv \boldsymbol{a} \mod p^{r-\alpha}$ then $\boldsymbol{a}_\alpha \equiv t\boldsymbol{b}_1 \mod p^{\beta}$ for some $t \in \mathbb{Z}_{p^\beta}^{\times}$. It is easy to see that $B_{E_{\alpha,\beta}}$ is a regular graph of valency

$$\phi(p^\beta)((p^{r-\alpha-\beta})^d - (p^r - \phi(p^{r-\alpha-\beta}))^d) < \phi(p^\beta)\left(p^{r-\alpha-\beta}\right)^d,$$

where ϕ is the Euler function. Let $E_{\alpha,\beta}$ be the adjacency matrix of $B_{E_{\alpha,\beta}}$ then absolute values of eigenvalues of $E_{\alpha,\beta}$ are bounded by $\phi(p^\beta)\left(p^{r-\alpha-\beta}\right)^d$.

Let A be the adjacency matrix of $\mathcal{ZP}_{q,d}$. It follows that

$$\begin{aligned} A^2 &= (p^{r(d-1)} - p^{(r-1)(d-1)})I + \sum_{\substack{0\leqslant\alpha\leqslant r-1\\ 0\leqslant\beta\leqslant r-\alpha}} v_{\alpha,\beta}E_{\alpha,\beta} \\ &= (p^{r(d-1)} - p^{(r-1)(d-1)} - v_{0,0})I + v_{0,0}J + \sum_{\substack{0\leqslant\alpha\leqslant r-1\\ 0\leqslant\beta\leqslant r-\alpha}} (v_{\alpha,\beta} - v_{0,0})E_{\alpha,\beta}, \end{aligned} \tag{16}$$

where I is the identity matrix and J is the all-one matrix. Note that, the assumption $\boldsymbol{a} \neq \boldsymbol{b}$ means that we are substracting the off-diagonal from the sum with $E_{\alpha,\beta}$ in the last part of Eq. (16).

Since $\mathcal{ZP}_{q,d}$ is a $p^{r(d-1)} - p^{(r-1)(d-1)}$-regular graph, $p^{r(d-1)} - p^{(r-1)(d-1)}$ is an eigenvalue of A with the all-one eigenvector $\mathbf{1}$. The graph $\mathcal{ZP}_{q,d}$ is connected, therefore the eigenvalue $p^{r(d-1)} - p^{(r-1)(d-1)}$ has multiplicity one. Since the graph $\mathcal{ZP}_{q,d}$ contains (many) triangles, it is not bipartite. Hence, for any other eigenvalue θ then $|\theta| < p^{r(d-1)} - p^{(r-1)(d-1)}$. Let $\boldsymbol{v}_\theta$ denote the corresponding eigenvector of θ. Note that $\boldsymbol{v}_\theta \in \mathbf{1}^\perp$, so $J\boldsymbol{v}_\theta = 0$. It follows from (16) that

$$(\theta^2 - p^{(d-1)r} + p^{(r-1)(d-1)} + v_{0,0})\boldsymbol{v}_\theta = \left(\sum_{\substack{0\leqslant\alpha\leqslant r-1\\ 0\leqslant\beta\leqslant r-\alpha}} (v_{\alpha,\beta} - v_{0,0})E_{\alpha,\beta}\right)\boldsymbol{v}_\theta.$$

Hence, $\boldsymbol{v}_\theta$ is also an eigenvector of

$$\sum_{\substack{0\leqslant\alpha\leqslant r-1\\ 0\leqslant\beta\leqslant r-\alpha}} (v_{\alpha,\beta} - v_{0,0})E_{\alpha,\beta}.$$

Since eigenvalues of the sum of the matrices are bounded by the sum of the largest eigenvalues of summands. We have

$$\begin{aligned}\theta^2 &\leqslant p^{r(d-1)} - p^{(r-1)(d-1)} - v_{0,0} + \sum_{\substack{1\leqslant\alpha\leqslant r-1\\ \beta=0}} (v_{\alpha,0}-v_{0,0})\phi(1)p^{(r-\alpha)d} \\ &\quad + \sum_{\substack{0\leqslant\alpha\leqslant r-1\\ \beta=r-\alpha}} (v_{\alpha,r-\alpha}-v_{0,0})\phi(p^{r-\alpha}) \\ &\quad + \sum_{\substack{0\leqslant\alpha\leqslant r-1\\ 1\leqslant\beta\leqslant r-\alpha-1}} (v_{\alpha,\beta}-v_{0,0})\phi(p^{\beta})p^{(r-\alpha-\beta)d}. \qquad (17)\end{aligned}$$

Next, we estimate each term of (17). We have

$$\begin{aligned}\sum_{\substack{1\leqslant\alpha\leqslant r-1\\ \beta=0}} (v_{\alpha,0}-v_{0,0})\phi(1)p^{(r-\alpha)d} &\leqslant \sum_{\substack{1\leqslant\alpha\leqslant r-1\\ \beta=0}} p^{(r-\alpha)d}p^{(r-\alpha)(d-2)}p^{\alpha(d-1)} \\ &< rp^{(2r-1)d-2r+1}. \qquad (18)\\ \sum_{\substack{0\leqslant\alpha\leqslant r-1\\ \beta=r-\alpha}} (v_{\alpha,r-\alpha}-v_{0,0})\phi(p^{r-\alpha}) &\leqslant \sum_{\substack{0\leqslant\alpha\leqslant r-1\\ \beta=r-\alpha}} p^{rd-\alpha} < rp^{rd}. \qquad (19)\\ \sum_{\substack{0\leqslant\alpha\leqslant r-1\\ 1\leqslant\beta\leqslant r-\alpha-1}} (v_{\alpha,\beta}-v_{0,0})\phi(p^{\beta})p^{(r-\alpha-\beta)d} &\leqslant \sum_{\substack{0\leqslant\alpha\leqslant r-1\\ 1\leqslant\beta\leqslant r-\alpha-1}} p^{(r-\alpha)(d-2)}p^{2\beta}p^{\alpha(d-1)}p^{(r-\alpha-\beta)d} \\ &< \sum_{\substack{0\leqslant\alpha\leqslant r-1\\ 1\leqslant\beta\leqslant r-\alpha-1}} p^{2rd-2r-\alpha(d-1)-\beta(d-2)} \\ &< r^2p^{(2r-1)d-2r+2}. \qquad (20)\end{aligned}$$

Putting (17), (18), (19), and (20) together, the theorem follows. □

3 Orthogonal systems

We are now ready to give a proof of Theorem 3. Let K_k be a complete graph with k vertices. Then K_k has $\binom{k}{2}$ edges and the degree of each vertex is $k-1$. Let $E \subset \mathbb{Z}_q^d$ such that $|E| \gg p^{r(d+k-2)+\left(1-\frac{d}{2}\right)}$. We consider E as a subset of the vertex set of $\mathcal{ZP}_{q,d}$. Then the number of k-tuples of k mutually orthogonal vectors in E is the number of copies of K_k in E. Set $E_1 = E\setminus(p\mathbb{Z}_{p^{r-1}})^d$, then we have $|E| - p^{(r-1)d} \leqslant |E_1| \leqslant |E|$. Note that

$$|E| \gg p^{r(d+k-2)+\left(1-\frac{d}{2}\right)} = p^{rd+r(k-2)+1-\frac{d}{2}} \gg p^{rd-d} = p^{(r-1)d},$$

which implies that $|E_1| = (1+o(1))|E|$. We have

$$|E_1| \geqslant |E| - p^{(r-1)d} \gg p^{r(d+k-2)+\left(1-\frac{d}{2}\right)} \gtrsim \left(rp^{\frac{(2r-1)d-2r+2}{2}}\right)\left(\frac{p^{rd}-p^{(r-1)d}}{p^{r(d-1)}-p^{(r-1)(d-1)}}\right)^{k-1}. \qquad (21)$$

From Theorem 4 and (21), the number of copies of K_k in E_1 is

$$(1+o(1))\frac{|E_1|^k}{k!}\left(\frac{p^{r(d-1)}-p^{(r-1)(d-1)}}{p^{rd}-p^{(r-1)d}}\right)^{\binom{k}{2}}=(1+o(1))\frac{|E|^k}{k!}q^{-\binom{k}{2}}. \tag{22}$$

For any $1\leqslant s\leqslant k$, let K_{k-s} be the complete graph with $k-s$ vertices then K_{k-s} has $\binom{k-s}{2}$ edges and the degree of each vertex is $k-s-1$. It is clear that

$$\left(rp^{\frac{(2r-1)d-2r+2}{2}}\right)\left(\frac{p^{rd}-p^{(r-1)d}}{p^{r(d-1)}-p^{(r-1)(d-1)}}\right)^{k-1}\geqslant\left(rp^{\frac{(2r-1)d-2r+2}{2}}\right)\left(\frac{p^{rd}-p^{(r-1)d}}{p^{r(d-1)}-p^{(r-1)(d-1)}}\right)^{k-s-1}.$$

From Theorem 4 and (21), the number of copies of K_{k-s} in E_1 is

$$(1+o(1))\frac{|E_1|^{k-s}}{(k-s)!}\left(\frac{p^{r(d-1)}-p^{(r-1)(d-1)}}{p^{rd}-p^{(r-1)d}}\right)^{\binom{k-s}{2}}=(1+o(1))\frac{|E|^{k-s}}{(k-s)!}q^{-\binom{k-s}{2}}.$$

For any $1\leqslant s\leqslant k$, the number of s-element subsets of $E\backslash E_1$ is $\binom{p^{(r-1)d}}{s}\leqslant p^{ds(r-1)}$. Note that $d\geqslant 2r-2$ so

$$(1+o(1))\frac{|E|^{k-s}}{(k-s)!}q^{-\binom{k-s}{2}}p^{ds(r-1)}\ll\frac{|E|^k}{k!}q^{-\binom{k}{2}}.$$

Hence, the number of copies of K_k, in which s vertices in $E\backslash E_1$ and $k-s$ vertices in E_1, is dominated by $\frac{|E|^k}{k!}q^{-\binom{k}{2}}$. This implies that the number of k mutually orthogonal vectors in E is

$$(1+o(1))\frac{|E|^k}{k!}q^{-\binom{k}{2}},$$

completing the proof of Theorem 3.

References

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

[2] J. Bourgain, N. Katz, and T. Tao, A sum product estimate in finite fields and Applications, *Geom. Funct. Analysis*, **14** (2004), 27–57.

[3] J. Chapman, M. B. Erdoğan, Derrick Hart, Alex Iosevich, and Doowon Koh, Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates, *Mathematische Zeitschrift* (to appear).

[4] A. Iosevich and S. Senger, Orthogonal systems in vector spaces over finite fields, *Electronic J. Combin.*, **15** (2008), #R151.

[5] D. Covert, A. Iosevich, and J. Pakianathan, Geometric configurations in the ring of integers modulo p^l, *Indiana University Mathematics Journal* (to appear).

[6] 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, *Transactions of the AMS*, **363** (2011) 3255–3275.

[7] 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).

[8] L. Guth and N. Katz, On the Erdős distinct distances problem in the plane, (preprint) arXiv:1011.4105 (2010).

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

[10] A. Iosevich and M. Rudnev, Erdős distance problem in vector spaces over finite fields, *Trans. Amer. Math. Soc.*, **359** (2007), 6127–6142.

[11] N. H. Katz and G. Tardos, A new entropy inequality for the Erdős distance problem, *Contemp. Math.* **342**, Towards a theory of geometric graphs, 119–126, Amer. Math. Soc., Providence, RI (2004).

[12] M. Krivelevich and B. Sudakov, Pseudo-random graphs, *Conference on Finite and Infinite Sets Budapest*, Bolyai Society Mathematical Studies X, pp. 164.

[13] A. Magyar, On distance sets of large sets of integers points, *Israel J. Math.* **164** (2008), 251–263.

[14] A. Magyar, k-point configurations in sets of positive density of $\mathbb{Z}^n$, *Duke Math J.* (to appear) (2007).

[15] J. Solymosi and V. Vu, Near optimal bounds for the number of distinct distances in high dimensions, *Combinatorica*, (2005).

[16] L. A. Vinh, Explicit Ramsey graphs and Erdős distance problem over finite Euclidean and non-Euclidean spaces, *Electronic J. Combin.*, **15** (2008), #R5.

[17] L. A. Vinh, On orthogonal systems in vector spaces over finite fields, *The Electronic Journal of Combinatorics*, **15** (2008), N32.

[18] L. A. Vinh, Triangles in vector spaces over finite fields, *Online Journal of Analytic Combinatorics* (to appear).

[19] L. A. Vinh, The solvability of norm, bilinear and quadratic equations over finite fields via spectral of graphs, *Forum Mathematicum* (in press).

[20] L. A. Vinh, Product sets and distance sets of random point sets in vector spaces over finite rings, *Indiana University Mathematics Journal* (to appear).

[21] L. A. Vinh, Pinned distance sets and k-simplices in vector spaces over finite rings, preprint (2011).

[22] V. H. Vu, Sum-product estimates via directed expanders, *Math. Res. Lett.* **15** (2008), no. 2, 375–388.