On the number of orthogonal systems in vector spaces over finite fields

Le Anh Vinh
Mathematics Department
Harvard University
Cambridge, MA 02138, US
vinh@math.harvard.edu

Submitted: Jul 15, 2008; Accepted: Aug 13, 2008; Published: Aug 25, 2008
Mathematics Subject Classification: 05C50,05C35

Abstract

Iosevich and Senger (2008) showed 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. In this note, we provide a graph theoretic proof of this result.

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. In a recent paper [3], 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 (see [3] for the motivation of this result).

Theorem 1.1 *([3]) Let $E \subset \mathbb{F}_q^d$, such that*

$$|E| \geqslant Cq^{d\frac{k-1}{k}+\frac{k-1}{2}+\frac{1}{k}} \tag{1.1}$$

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

$$\lambda_k = (1 + o(1))\frac{|E|^k}{k!}q^{-\binom{k}{2}}. \tag{1.2}$$

In this note, we provide a different proof to this result using graph theoretic methods. The main result of this note is the following.

Theorem 1.2 *Let $E \subset \mathbb{F}_q^d$, such that*

$$|E| \gg q^{\frac{d}{2}+k-1}, \tag{1.3}$$

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

$$(1+o(1))\frac{|E|^k}{k!}q^{-\binom{k}{2}}. \tag{1.4}$$

Note that Theorem 1.1 only works in the range $d > \binom{k}{2}$ (as larger tuples of mutually orthogonal vectors are out of range of the methods uses) while Theorem 1.2 works in a wider range $d > 2(k-1)$. Moreover, Theorem 1.2 is stronger than Theorem 1.1 in the same range.

1.1 Sharpness of results

It is also interesting to note that the exponent $\frac{d}{2}+1$ cannot be improved in the case $k = 2$. In [3], Iosevich and Senger constructed a set $E \subset \mathbb{F}_q^d$ such that $|E| \geq cq^{\frac{d+1}{2}+1}$, for some $c > 0$, but no pair of its vectors are orthogonal (see Lemma 3.2 in [3]). 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 $|E_1| \approx q^{1/2}$ and $|E_2| \approx q^{\frac{d-1}{2}}$ with the sum set of their respective dot product sets does not contain 0. We hope to demonstrate in the future that the exponent $\frac{d}{2} + k - 1$ cannot, in general, be improved, for any $k > 2$.

2 Proof of Theorem 1.2

We call a graph $G = (V, E)$ (n, d, λ)-graph if G is a d-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 $\lambda \ll d$ then an (n, d, λ)-graph behaves similarly as a random graph $G_{n,d/n}$. Let H be a fixed graph of order s with r 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

$$(1+o(1))p^r(1-p)^{\binom{s}{2}-r}\frac{n^s}{|\mathrm{Aut}(H)|} \tag{2.1}$$

induced copies of H. Alon extended this result to (n, d, λ)-graphs. He proved that every large subset of the set of vertices of an (n, d, λ)-graph contains the "correct" number of copies of any fixed small subgraph (Theorem 4.10 in [2]).

Theorem 2.1 *([2]) Let H be a fixed graph with r edges, s vertices and maximum degree Δ, and let $G = (V, E)$ be an (n, d, λ)-graph, where, say, $d \leqslant 0.9n$. Let $m < n$ satisfies $m \gg \lambda\left(\frac{n}{d}\right)^{\Delta}$. Then, for every subset $U \subset V$ of cardinality m, the number of (not necessarily induced) copies of H in U is*

$$(1+o(1))\frac{m^s}{|\mathrm{Aut}(H)|}\left(\frac{d}{n}\right)^r. \tag{2.2}$$

Note that the above theorem, proved for simple graphs in [2], 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 [2] for simple graph and the proof for graph with loops.

We recall a well-known construction of Alon and Krivelevich [1]. Let $PG(q,d)$ denote the projective geometry of dimension $d-1$ over finite field $\mathbb{F}_q$. The vertices of $PG(q,d)$ correspond to the equivalence classes of the set of all non-zero vectors $x=(x_1,\dots,x_d)$ over $\mathbb{F}_q$, where two vectors are equivalent if one is a multiple of the other by an element of the field. Let $G_P(q,d)$ denote the graph whose vertices are the points of $PG(q,d)$ and two (not necessarily distinct) vertices x and y are adjacent if and only if $x_1y_1+\ldots+x_dy_d=0$. This construction is well known. In the case $d=2$, this graph is called the Erdős-Rényi graph. It is easy to see that the number of vertices of $G_P(q,d)$ is $n_{q,d}=(q^d-1)/(q-1)$ and that it is $d_{q,d}$-regular for $d_{q,d}=(q^{d-1}-1)/(q-1)$. The eigenvalues of G are easy to compute ([1]). Let A be the adjacency matrix of G. Then, by properties of $PG(q,d)$, $A^2=AA^T=\mu J+(d_{q,d}-\mu)I$, where $\mu=(q^{d-2}-1)/(q-1)$, J is the all one matrix and I is the identity matrix, both of size $n_{q,d}\times n_{q,d}$. Thus the largest eigenvalue of A is $d_{q,d}$ and the absolute value of all other eigenvalues is $\sqrt{d_{q,d}-\mu}=q^{(d-2)/2}$.

Now we are ready to give a proof of Theorem 1.2. Let $G(q,d)$ denote the graph whose vertices are the points of $\mathbb{F}_q^d-(0,\dots,0)$ and two (not necessarily distinct) vertices x and y are adjacent if and only if they are orthogonal, i.e. $x_1y_1+\ldots+x_dy_d=0$. Then $G(q,d)$ is just the product of $q-1$ copies of $G_P(q,d)$. Therefore, it is easy to see that the number of vertices of G is $N_{q,d}=(q-1)n_{q,d}=q^d-1$ and that it is $D_{q,d}$-regular for $D_{q,d}=(q-1)d_{q,d}=q^{d-1}-1$. The eigenvalues of $G(q,d)$ are also easy to compute. Let V be the adjacency matrix of $G(q,d)$. Then by the properties of $PG(q,d)$,

$$V^2=VV^T=\rho J_{N_{q,d}}+(D_{q,d}-\rho)\bigoplus_{n_{q,d}} J_{q-1}, \tag{2.3}$$

where $\rho=(q-1)\mu=q^{d-2}-1$, $J_{N_{q,d}}$ is the all one matrix of size $N_{q,d}\times N_{q,d}$ and J_{q-1} is the all one matrix of size $(q-1)\times(q-1)$. Thus, all eigenvalues of V^2 are all eigenvalues of $(q-1)\rho J_{n_{q,d}}+(q-1)(D_{q,d}-\rho)I_{n_{q,d}}$ and zeros (with $J_{n_{q,d}}$ is the all one matrix and $I_{n_{q,d}}$ is the identity matrix, both of size $n_{q,d}\times n_{q,d}$). Therefore, the largest eigenvalue of V is $D_{q,d}$ and the absolute values of all other eigenvalues are either $\sqrt{(q-1)(D_{q,d}-\rho)}=(q-1)q^{(d-2)/2}$ or 0. This implies that $G(q,d)$ is a $(q^d-1,q^{d-1}-1,(q-1)q^{(d-2)/2})$-graph.

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 $E\subset\mathbb{F}_q^d$, such that

$$|E|\gg q^{\frac{d}{2}+k-1}, \tag{2.4}$$

where $d\geqslant 2k-1$. We consider E as a subset of the vertex set of $G(q,d)$ then the number of k-tuples of k mutually orthogonal vectors in E is the number of copies of K_k in E. Set $E_1=E-\{0,\dots,0\}$ then we have $|E|-1\leq|E_1|\leq|E|$. We have

$$|E_1|\geq|E|-1\gg q^{\frac{d}{2}+k-1}\geq(q-1)q^{(d-2)/2}\left(\frac{q^d-1}{q^{d-1}-1}\right)^{k-1}. \tag{2.5}$$

From Theorem 2.1 and (2.5), the number of copies of K_k in E_1 is

$$(1+o(1))\frac{|E_1|^k}{k!}\left(\frac{q^{d-1}-1}{q^d-1}\right)^{\binom{k}{2}} = (1+o(1))\frac{|E|^k}{k!}q^{-\binom{k}{2}}. \tag{2.6}$$

Let K_{k-1} be a complete graph with $k-1$ vertices then K_{k-1} has $\binom{k-1}{2}$ edges and the degree of each vertex is $k-2$.

We have $(q-1)q^{(d-2)/2}\left(\frac{q^d-1}{q^{d-1}-1}\right)^{k-1} > (q-1)q^{(d-2)/2}\left(\frac{q^d-1}{q^{d-1}-1}\right)^{k-2}$. Thus, from Theorem 2.1 and (2.5), the number of copies of K_{k-1} in E_1 is

$$\begin{aligned}(1+o(1))\frac{|E_1|^{k-1}}{(k-1)!}\left(\frac{q^{d-1}-1}{q^d-1}\right)^{\binom{k-1}{2}} &= (1+o(1))\frac{|E|^{k-1}}{(k-1)!}q^{-\binom{k-1}{2}} && (2.7)\\ &\ll (1+o(1))\frac{|E|^k}{k!}q^{-\binom{k}{2}}, && (2.8)\end{aligned}$$

as $|E| \gg q^{\frac{d}{2}+k-1} \gg q^{k-1}$. From (2.6) and (2.8), the number of copies of K_k in E is

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

.

This implies that the number of the number of k-tuples of k mutually orthogonal vectors in E is also

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

completing the proof of Theorem 1.2.

Acknowledgments

The research is performed during the author's visit at the Erwin Schrödinger International Institute for Mathematical Physics. The author would like to thank the ESI for hospitality and financial support during his visit.

References

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

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

[3] A. Iosevich and S. Senger, Orthogonal systems in vector spaces over finite fields, preprint (2008), arXiv:0807.0592.