The number of occurrences of a fixed spread among n directions in vector spaces over finite fields

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

February 9, 2014

Abstract

We study a finite analog of a problem of Erdos, Hickerson and Pach on the maximum number of occurrences of a fixed angle among n directions in three-dimensional spaces.

1 Introduction

The Erdos Distance Problem is perhaps the best known problem in combinatorial geometry. How often can the same distance occur among n points in the plane? Although this problem has received considerable attention, we are still far from the solution. Let $u(n)$ denote the maximum number of occurrences of the same distance among n points in the plane. Erdös initial upper bound [7], $u(n) \leqslant O(n^{2/3})$, follows from an extremal graph theory result. This bound was improved in several steps to $O(n^{4/3})$. There are several different proofs for this bound in which, perhaps, the most elegant proof, due to Székely [16], is based on a general lower bound for the crossing number of graphs (see Chapter 5 in [5] for a comprehensive survey on the progress and open problems in this area). Let $\mathbb{F}_q$ denote the finite field with q elements where $q \gg 1$ is an odd prime power. For any $x, y \in \mathbb{F}_q^d$, the distant between x, y is defined as $\|x-y\| = (x_1-y_1)^2 + \ldots + (x_d-y_d)^2$. Let $E \subset \mathbb{F}_q^d$, $d \geqslant 2$. Then the finite analogof the classical Erdos distance problem is to determine the smallest possible cardinality of the set

$$\Delta(E) = \{\|x-y\| : x, y \in E\}, \tag{1.1}$$

viewed as a subset of $\mathbb{F}_q$. Bourgain, Katz and Tao ([4]), showed, using intricate incidence geometry, that for every $\varepsilon > 0$, there exists $\delta > 0$, such that if $E \in \mathbb{F}_q^2$ and $C_\varepsilon^1 q^\varepsilon \leqslant |E| \leqslant$

$C_\varepsilon^2 q^{2-\varepsilon}$, then $|\Delta(E)| \geqslant C_\delta |E|^{\frac{1}{2}+\delta}$ for some constants $C_\varepsilon^1, C_\varepsilon^2$ and C_δ. The relationship between ε and δ in their argument is difficult to determine. Going up to higher dimension using arguments of Bourgain, Katz and Tao is quite subtle. Iosevich and Rudnev [14] establish the following result using Fourier analytic method.

Theorem 1.1 *([14]) Let $E \subset \mathbb{F}_q^d$ such that $|E| \gtrsim Cq^{d/2}$ for C sufficiently large. Then*

$$|\Delta(E)| \gtrsim \min\left\{q, \frac{|E|}{q^{(d-1)/2}}\right\}. \tag{1.2}$$

Iosevich and his collaborators investigated several related results using this method in a series of papers [6, 10, 11, 12, 13, 14, 15]. Using graph theoretic method, the author reproved some of these resutls in [19, 20, 21, 22, 23]. The advantages of the graph theoretic method are twofold. First, we can reprove and sometimes improve several known results in vector spaces over finite fields. Second, our approach works transparently in the non-Euclidean setting. In this note, we use the graph theoretic method to study a finite analog of a related problem of Erdos, Hickerson and Pach [9].

Problem 1.2 *([9]) Give a good asymptotic bounds for the maximum number of occurrences of a fixed angle γ among n unit vectors in three-dimensional spaces.*

If $\gamma = \pi/2$, the maximum number of orthogonal pairs is known to be $\Theta(n^{4/3})$ as this problem is equivalent to bounding the number of point-line incidences in the plane (see [5] for a detailed discussion). For any other angle $\gamma \neq \pi/2$, we are far from haveing good estimates for the maximum number of occurrences of γ. The only known upper bound is still $O(n^{4/3})$. the same as for orthogonal pairs. For the lower bound, Swanepoel and Valtr [17] established the bound $\Omega(n \log n)$, improving an earlier result of Erdos, Hickerson and Pach [9]. It is, however, widely believed that the $\Omega(n \log n)$ lower bound can be much improved.

The purpose of this note is to study an analog of this problem in the three-dimension space over finite fields. In vector spaces over finite fields, however, the separation of lines is not measured by the transcendental notion of angle. A remarkable approach of Wildberger [24, 25] by recasting metrical geometry in a purely algebraic setting, eliminate the difficulties in defining an angle by using instead the notion of spread - in Euclidean geometry the square of the sine of the angle between two rays lying on those lines (the notation of spread will be defined precisely in Section 2). Using this notation, we now can state the main result of this note.

Theorem 1.3 *Let E be a set of unit vectors in $\mathbb{F}_q^3$ with $q^{3/2} \ll |E| \ll q^2$. For any $\gamma \in \mathbb{F}_q$, let $f_\gamma(E)$ denote the number of occurrences of a fixed spread γ among E. Then $f_\gamma(E) = \Theta(|E|^2/q)$ if $1-\gamma$ is a square in $\mathbb{F}_q$ and $f_\gamma(E) = 0$ otherwise.*

The rest of this note is organized as follows. In Section 2, we follow Wildberger's construction of affine and projective rational trigonometry to define the notions of quadrance and spread. We then define the main tool of our proof, the finite Poincaré graphs. Using these graphs, we give a proof of Theorem 1.3 in Section 3.

2 Quadrance, Spread and finite Poincaré graphs

In this section, we follow Wildberger's construction of affine and projective rational trigonometry over finite fields. Interested readers can see [24, 25] for a detailed discussion.

2.1 Quadrance and Spread: affine rational geometry

We work in a three-dimensional vector space over a field F, not of characteristic two. Elements of the vector space are called points or vectors (these two terms are equivalent and will be used interchangeably) and are denoted by U, V, W and so on. The zero vector or point is denote O. The unique line l through distinct points U and V is denoted UV. For a non-zero point U the line OU is denoted $[U]$. Fix a symmetric bilinear form and represent it by $U \cdot V$. In terms of this form, the line UV is perpendicular to the line WZ precisely when $(V - U) \cdot (Z - W) = 0$. A point U is a null point or null vector when $U \cdot U = 0$. The origin O is always a null point, and there are others as well.

The distance (or so-called *quadrance* in Wildberger's construction) between the points U and V is the number

$$Q(U, V) = (V - U) \cdot (V - U). \tag{2.1}$$

The line UV is a null line precisely when $Q(U, V) = 0$, or equivalently when it is perpendicular to itself.

In Euclidean geometry, the separation of lines is traditionally measured by the transcendental notion of *angle*. The difficulities in defining an angle precisely, and in extending the concept over an arbitrarily field, are eliminated in rational trigonometry by using instead the notion of *spread* - in Euclidean geometry the square of the sine of the angle between two rays lying on those lines. Precisely, the *spread* between the non-null lines UW and VZ is the number

$$s(UW, VZ) = 1 - \frac{((W - U) \cdot (Z - V))^2}{Q(U, W)Q(V, Z)}. \tag{2.2}$$

This depends only on the two lines, not the choice of points lying on them. The spread between two non-null lines is 1 precisely when they are perpendicular. Given a large set E of unit vectors in $\mathbb{F}_q^3$, our aim is to study the number of occurences of a fixed spread $\gamma \in \mathbb{F}_q$ among E.

2.2 Finite Poincaré graphs: projective rational geometry

Fix a three-dimensional vector space over a field with a symmetric bilinear form $U \cdot V$ as in the previous subsection. A line though the origion O will now be called a projective point and denoted by a small letter such as u. The space of such projective points is called n dimensional projective space. If V is a non-zero vector in the vector space, then $v = [V]$ denote the projective point OV. A projective point is a null projective point when some non-zero null point lies on it. Two projective points $u = [U]$ and $v = [V]$ are perpendicular when they are perpendicular as lines.

The *projective quadrance* between the non-null projective points $u = [U]$ and $v = [V]$ is the number

$$q(u,v) = 1 - \frac{(U \cdot V)^2}{(U \cdot U)(V \cdot V)}. \tag{2.3}$$

This is the same as the spread $s(OU, OV)$, and has the value 1 precisely when the projective points are perpendicular.

The *projective spread* between the intersecting projective lines $wu = [W, U]$ and $wv = [W, V]$ is defined to be the spread between these intersecting planes:

$$S(wu,wv) = 1 - \frac{\left(\left(U - \frac{U\cdot W}{W\cdot W}W\right)\cdot\left(V - \frac{V\cdot W}{W\cdot W}W\right)\right)^2}{\left(\left(U - \frac{U\cdot W}{W\cdot W}W\right)\cdot\left(U - \frac{U\cdot W}{W\cdot W}W\right)\right)\left(\left(V - \frac{V\cdot W}{W\cdot W}W\right)\cdot\left(V - \frac{V\cdot W}{W\cdot W}W\right)\right)} \tag{2.4}$$

This approach is entirely algebraic and elementary which allows one to formulate two dimensional hyperbolic geometry as a projective theorey over a general field. Precisely, over the real numbers, the projective quadrance in the projective rational model is the negative of the square of the hyperbolic sine of the hyperbolic distance between the corresponding points in the Poincaré model, and the projective spread is the square of the sine of the angle between corresponding geodesics in the Poincaré model (see [25]).

Let Ω be the set of square-type non-isotropic 1-dimensional subspaces of $\mathbb{F}_q^3$ then $|\Omega| = q(q+1)/2$. For a fixed $\gamma \in \mathbb{F}_q$, the *finite Poincaré graph* $P_q(\gamma)$ has vertices as the points in Ω and edges between vertices $[Z], [W]$ if and only if $s(OZ, OW) = \gamma$. These graphs can be viewed as a companion of the well-known (and well studied) finite upper half plane graphs (see [18] for a survey on the finite upper half plane graphs). From the definition of the spread, the finite Poincaré graph $P_q(\gamma)$ is nonempty if and only if $1 - \lambda$ is a square in $\mathbb{F}_q$.

We have the orthogonal group $O_3(\mathbb{F}_q)$ acts transitively on Ω, and yields a symmetric association scheme $\Psi(O_3(\mathbb{F}_q), \Omega)$ of class $(q+1)/2$. The relations of $\Psi(O_3(\mathbb{F}_q), \Omega)$ are given by

$$\begin{aligned}
R_1 &= \{([U],[V]) \in \Omega \times \Omega \mid (U+V)\cdot(U+V) = 0\},\\
R_i &= \{([U],[V]) \in \Omega \times \Omega \mid (U+V)\cdot(U+V) = 2 + 2\nu^{-(i-1)}\}\ (2 \leqslant i \leqslant (q-1)/2)\\
R_{(q+1)/2} &= \{([U],[V]) \in \Omega \times \Omega \cdot (U+V)\cdot(U+V) = 2\},
\end{aligned}$$

where ν is a generator of the field $\mathbb{F}_q$ and we assume $U \cdot U = 1$ for all $[U] \in \Omega$ (see [2], Section 6). Note that $\Psi(O_3(\mathbb{F}_q), \Omega)$ is isomorphic to the association scheme $PGL(2,q)/D_{2(q-1)}$ where $D_{2(q-1)}$ is a dihedral sugroup of order $2(q-1)$. The graphs (Ω, R_i) are not Ramanujan in general, but fortunately, they are asymptotic Ramanujan for large q. The following theorem summaries the results from [3], Section 2 in a rough form.

Theorem 2.1 *([3]) The graphs (Ω, R_i) $(1 \leq i \leq (q+1)/2)$ are regular of valency $Cq(1 + o(1))$. Let λ be any eigenvalue of the graph (Ω, R_i) with $\lambda \neq$ valency of the graph then*

$$|\lambda| \leq c(1 + o(1))\sqrt{q},$$

for some $C, c > 0$ (In fact, we can show that $c = 1/2$).

Theorem 2.1 implies that the finite Poincaré graphs $P_q(\gamma)$ are asymptotic Ramanujan whenever $1-\gamma$ is a square in $\mathbb{F}_q$. Precisely, we have the following theorem.

Theorem 2.2 *a) If $1-\gamma$ is not a square in $\mathbb{F}_q$ then the finite Poincaré graph $P_q(\gamma)$ is empty.*

b) If $1-\gamma$ is a square in $\mathbb{F}_q$ then the finite Poincaré graph $P_q(\gamma)$ is regular of valency $Cq(1+o(1))$. Let λ be any eigenvalue of the graph $P_q(\gamma)$ with $\lambda \neq$ valency of the graph then

$$|\lambda| \leq c(1+o(1))\sqrt{q},$$

for some $C, c > 0$.

Proof a) Suppose that $[U], [V] \in \Omega$ and $s(OU, OV) = \gamma$ then

$$1-\gamma = \frac{(U \cdot V)^2}{(U \cdot U)(V \cdot V)}.$$

But U, V are square-type so $1-\gamma$ is a square in $\mathbb{F}_q$.

b) It is easy to see that the finite Poincaré graphs $P_q(1-\nu^{2-2i}) = (\Omega, R_i)$ for $1 \leq i \leq (q-1)/2$ and $P_q(1) = (\Omega, R_{(q+1)/2})$. The theorem follows immediately from Theorem 2.1. □

3 Proof of Theorem 1.3

We call a graph $G = (V, E)$ (n, d, λ)-regular if G is a d-regular graph on n vertices with the absolute value of each of its eigenvalues but the largest one is at most λ. It is well-known that if $\lambda \ll d$ then a (n, d, λ)-regular graph behaves similarly as a random graph $G_{n,d/n}$. Presicely, we have the following result (see Corollary 9.2.5 and Corollary 9.2.6 in [1]).

Theorem 3.1 *([1]) Let G be a (n, d, λ)-regular graph. For every set of vertices B of G, we have*

$$|e(B) - \frac{d}{2n}|B|^2| \leqslant \frac{1}{2}\lambda|B|, \tag{3.1}$$

where $e(B)$ is number of edges in the induced subgraph of G on B.

Let E be a set of m unit vectors in $\mathbb{F}_q^3$ then E can be viewed as a subset of Ω. The number of occurrences of a fixed spread γ among E can be realized as the number of edges in the induced subgraph of the finite Poincaré graph $P_q(\gamma)$ on the vertex set E. Thus, from Theorem 2.2, $f_\gamma(E) = 0$ if $1-\gamma$ is not a square in $\mathbb{F}_q$.

Suppose that $1-\gamma$ is a square in $\mathbb{F}_q$. From Theorem 2.2 and Theorem 3.1, we have

$$|f_\gamma(E) - \frac{Cq(1+o(1))}{q(q+1)/2}|E|^2| \leq \frac{1}{2}c(1+o(1))\sqrt{q}|E|. \tag{3.2}$$

Since $|E| \gg q^{3/2}$, we have $\frac{1}{2}c(1+o(1))\sqrt{q}|E| \ll \frac{Cq(1+o(1))}{q(q+1)/2}|E|^2$ and the theorem follows.

References

[1] N. Alon and J. H. Spencer, *The probabilistic method*, 2nd ed., Willey-Interscience, 2000.

[2] E. Bannai, S. Hao and S.-Y. Song, Character tables of the association schemes of finite orthogonal groups acting on the nonisotropic points, *Journal of Combinatorial Theory, Series A* **54** (1990), 164-170.

[3] E. Bannai, O. Shimabukuro and H. Tanaka, Finite analogues of non-Euclidean spaces and Ramanujan graphs, *European Journal of Combinatorics* **25** (2004), 243–259.

[4] J. Bourgain, N. Katz, T. Tao, A sum-product estimate in finite fields, and applications, *Geom. Funct. Anal.* **14** (2004), 27-57.

[5] P. Brass, W. Moser and J. Pach, *Research problems in discrete geometry*, Springer, 2005.

[6] D. Covert, D. Hart, A. Iosevich and I. Uriarte-Tuero, An analog of the Furstenberg-Katznelson-Weiss theorem on triangles in sets of positive density in finite field geometries, preprint (2008).

[7] P. Erdös, On sets of distances of n points, *Amer. Math. Monthly* **53** (1946) 248–250.

[8] P. Erdös, Some of my favorite unsolved problems, in: *A Tribute to Paul Erdös*, A. Baker et al., eds., Cambridge Univ. Press 1990, 467–478.

[9] P. Erdös, D. Hickerson and J. Pach, A problem of Leo Moser about repeated distances on the sphere, *Amer. Math. Monthly* **96** (1989) 569–575.

[10] D. Hart, A. Iosevich, J. Solymosi, Sum-product estimates in finite fields via Kloosterman sums, *International Mathematics Research Notices* (to appear).

[11] D. Hart, A. Iosevich, Sums and products in finite fields: an integral geometric viewpoint, preprint, 2007.

[12] D. Hart, A. Iosevich, D. Koh and M. Rudnev, Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdös-Falconer distance conjecture, preprint, 2007.

[13] A. Iosevich, D. Koh, Erdös-Falconer distance problem, exponential sums, and Fourier analytic approach to incidence theorems in vector spaces over finite fields, preprint.

[14] A. Iosevich, M. Rudnev, Erdös distance problem in vector spaces over finite fields, *Transactions of the American Mathematical Society* **359** (12) (2007), 6127-6142.

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

[16] L. A. Székely, Crossing numbers and hard Erdös problems in discrete geometry, *Comb. Probab. Comput.* **6** (1997), 353–358.

[17] K. J. Swanepoel and P. Valtr, The unit distance problem on spheres, in *Towards a Theory of Geometric Graphs*, J. Pach, ed., *Contemporary Mathematics* **342**, AMS 2004, 273–279.

[18] A. Terras, Survey of Spectra of Laplacians on Finite Symmetric Spaces, *Experimental Mathematics* (1996).

[19] L. A. Vinh, Explicit Ramsey graphs and Erdös distance problem over finite Euclidean and non-Euclidean spaces, *Electronic Journal of Combinatorics* **15** (2008), R5.

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

[21] L. A. Vinh, Szemerédi-Trotter type theorem and sum-product estimate in finite fields, *European Journal of Combinatorics*, to appear.

[22] L. A. Vinh, On a Furstenberg-Katznelson-Weiss type theorem over finite fields, preprint (2008).

[23] L. A. Vinh, On kaleidoscopic pseudo-randomness of finite Euclidean and non-Euclidean graphs, preprint (2008).

[24] N. J. Wildberger, *Divine Proportions: Rational Trigonometry to Universal Geometry*, Wild Egg Books, Sydney 2005.

[25] N. J. Wildberger, Affine and projective universal geometry, preprint, 2006. arXiv:math/0612499v1 [math.MG].