Applicable Analysis and Discrete Mathematics
available online at http://pefmath.etf.rs

Appl. Anal. Discrete Math. **7** (2013), 106–118. doi:10.2298/AADM121212026V

ON THE SUM OF THE SQUARED MULTIPLICITIES OF THE DISTANCES IN A POINT SET OVER FINITE SPACES

Le Anh Vinh

We study a finite analog of a conjecture of Erdős on the sum of the squared multiplicities of the distances determined by an n-element point set. Our result is based on an estimate of the number of hinges in spectral graphs.

1. INTRODUCTION

Let $\mathbb{F}_q$ denote the finite field with q elements where $q \gg 1$ is an odd prime power. Here, and throughout the paper, the implied constants in the symbols $O, o, \lesssim$ and $\ll$ may depend on integer parameter d. Recall that the notations $U = O(V)$ and $U \lesssim V$ are equivalent to the assertion that the inequality $|U| \leq cV$ holds for some constant $c > 0$. The notation $U = o(V)$ is equivalent to the assertion that $U = O(V)$ but $V \neq O(U)$, and the notation $U \ll V$ is equivalent to the assertion that $U = o(V)$. For any $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^d$, the distance between $\boldsymbol{x}, \boldsymbol{y}$ is defined as $||\boldsymbol{x} - \boldsymbol{y}|| = (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2$. Let $\mathcal{E} \subset \mathbb{F}_q^d$, $d \geq 2$. Then the finite analog of the classical Erdős distance problem is to determine the smallest possible cardinality of the set

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

viewed as a subset of $\mathbb{F}_q$. The first non-trivial result on the Erdős distance problem in vector spaces over finite fields is obtained by Bourgain, Katz, and Tao ([**3**]), who showed that if q is a prime, $q \equiv 3 \pmod 4$, then for every $\varepsilon > 0$ and $\mathcal{E} \subset \mathbb{F}_q^2$ with $|\mathcal{E}| \leq C_\varepsilon q^2$, there exists $\delta > 0$ such that $|\Delta(\mathcal{E})| \geq C_\delta |\mathcal{E}|^{\frac{1}{2}+\delta}$ for some constants C_ε, C_δ. The relationship between ε and δ in their arguments, however, is difficult to

2010 Mathematics Subject Classification. 05C15, 05C80.
Keywords and Phrases. Finite Euclidean graphs, pseudo-random graphs.

determine. In addition, it is quite subtle to go up to higher dimensional cases with these arguments. Iosevich and Rudnev ([**12**]) used Fourier analytic methods to show that there exist absolute constants $c_1, c_2 > 0$ such that for any odd prime power q and any set $\mathcal{E} \subset \mathbb{F}_q^d$ of cardinality $|\mathcal{E}| \geq c_1 q^{d/2}$, we have

$$|\Delta(\mathcal{E})| \geq c \min\left\{q, q^{\frac{d-1}{2}} |\mathcal{E}|\right\}. \tag{1.1}$$

Iosevich and Rudnev reformulated the question in analogy with the Falconer distance problem: how large does $\mathcal{E} \subset \mathbb{F}_q^d$, $d \geq 2$ need to be, to ensure that $\Delta(\mathcal{E})$ contains a positive proportion of the elements of $\mathbb{F}_q$. The above result implies that if $|\mathcal{E}| \geq 2q^{\frac{d+1}{2}}$, 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 $(d+1)/2$ the distance set is of positive measure. At first, it seems reasonable that the exponent $(d+1)/2$ may be improvable, in line with the Falconer distance conjecture described above. However, Hart, Iosevich, Koh and Rudnev discovered in [**10**] that the arithmetic of the problem makes the exponent $(d+1)/2$ best possible in odd dimensions, at least in general fields. In even dimensions, it is still possible that the correct exponent is $d/2$, in analogy with the Euclidean case. In [**5**], Chapman et al. took a first step in this direction by showing that if $\mathcal{E} \subset \mathbb{F}_q^2$ satisfies $|\mathcal{E}| \geq q^{4/3}$ then $|\Delta(\mathcal{E})| \geq cq$. 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.

In [**7**], Covert, Iosevich, and Pakianathan extended (1.1) to the setting of finite cyclic rings $\mathbb{Z}_{p^\ell} = \mathbb{Z}/p^\ell\mathbb{Z}$, where p is a fixed odd prime and $\ell \geq 2$. 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 answers in $\mathbb{R}^d$. By scale invariance of these questions, the problem of obtaining sharp bounds for the relationship between $|\Delta(\mathcal{E})|$ and $|\mathcal{E}|$ for a subset $\mathcal{E}$ of $\mathbb{Q}^d$ would be the same as for subsets of $\mathbb{Z}^d$. In [**7**], Covert, Iosevich, and Pakianathan 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

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

then

$$\mathbb{Z}_q^\times \subset \Delta(\mathcal{E}), \tag{1.2}$$

where $\mathbb{Z}_q^\times$ denote the set of units of $\mathbb{Z}_q$.

In [**22, 29**], the author gives other proofs of these results using the graph theoretic method. 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.

The remarkable results of Bourgain, Katz and Tao [**3**] on sum-product problem and its application in Erdős distance problem over finite fields have stimulated a series of studies of finite field analogues of classical discrete geometry problems, see [**5, 7, 10, 11, 12, 13, 14, 15, 20, 22, 23, 24, 25, 26, 27, 28, 29**] and references therein. In this paper, we use the same method to study a finite analog of a related conjecture of Erdős.

Let $\deg_S(\boldsymbol{p}, r)$ denote the number of points in $S \subset \mathbb{R}^2$ at distance r from a point $\boldsymbol{p} \in \mathbb{R}^2$. A conjecture of of Erdős [**9**] on the sum of the squared multiplicities of the distances determined by an n-element point set states that

$$\sum_{r>0}\left(\sum_{\boldsymbol{p}\in S}\deg_S(\boldsymbol{p}, r)^2\right) \leq O\big(n^3(\log n)^\alpha\big),$$

for some $\alpha > 0$. For this function, Akutsu et al. [**1**] obtained the upper bound $O(n^{3.2})$, improving an earlier result of Lefmann and Thiele ([**16**]). If no three points are collinear, Lefmann and Thiele give the better bound $O(n^3)$. This bound is sharp by the regular n-gons ([**16**]). Nothing is known about this function over higher dimensional spaces. The purpose of this paper is to study this function in the finite spaces $\mathbb{F}_q^d$ and $\mathbb{Z}_q^d$. The main results of this paper are the following theorems.

Theorem 1.1. *Let $\mathcal{E}$ be a subset of $\mathbb{F}_q^d$. For any point $\boldsymbol{p} \in \mathcal{E}$ and a distance $r \in \mathbb{F}_q - \{0\}$. Let $\deg_{\mathcal{E}}(\boldsymbol{p}, r)$ denote the number of points in $\mathcal{E}$ at distance r from $\boldsymbol{p}$. Let $f(\mathcal{E})$ denote the sum of the squared multiplicities of the distances determined by E :*

$$f(\mathcal{E}) = \sum_{r\in\mathbb{F}_q^*}\left(\sum_{\boldsymbol{p}\in\mathcal{E}}\deg_{\mathcal{E}}(\boldsymbol{p}, r)^2\right).$$

a) *Suppose that $|\mathcal{E}| \gtrsim q^{\frac{d+1}{2}}$ then $f(\mathcal{E}) = \Theta(|\mathcal{E}|^3/q)$.*

b) *Suppose that $|\mathcal{E}| \lesssim q^{\frac{d+1}{2}}$ then $|\mathcal{E}|^3/q \lesssim f(\mathcal{E} \lesssim |\mathcal{E}|q^d$.*

Note that the above theorem can be obtained by results about hinges of a given type in [**6**]. Our graph theoretic approach, however, works transparently in the finite cyclic rings.

Theorem 1.2. *Let $\mathcal{E}$ be a subset of $\mathbb{Z}_q^d$. For any point $\boldsymbol{p} \in \mathcal{E}$ and a distance $r \in \mathbb{Z}_q^\times$. Let $\deg_{\mathcal{E}}(\boldsymbol{p}, r)$ denote the number of points in $\mathcal{E}$ at distance r from $\boldsymbol{p}$. Let $f(\mathcal{E})$ denote the sum of the squared multiplicities of the distances determined by E :*

$$f(\mathcal{E}) = \sum_{r\in\mathbb{Z}_q^\times}\left(\sum_{\boldsymbol{p}\in\mathcal{E}}\deg_{\mathcal{E}}(\boldsymbol{p}, r)^2\right).$$

a) *Suppose that $|\mathcal{E}| \geq \Omega\big(q^{\frac{d+1}{2}}\big)$ then $f(\mathcal{E}) = \Theta(|\mathcal{E}|^3/q)$.*

b) *Suppose that $|\mathcal{E}| \leq O\big(q^{\frac{d+1}{2}}\big)$ then $\Omega(|\mathcal{E}|^3/q) \leq f(\mathcal{E}) \leq O(|\mathcal{E}|q^d)$.*

The rest of this paper is organized as follows. In Section 2, we establish an estimate about the number of hinges (i.e. ordered paths of length two) in spectral graphs. Using this estimate, we give proofs of Theorem 1.1 and Theorem 1.2 in Section 3 and Section 4, respectively.

2. NUMBER OF HINGES IN AN (n, d, λ)-GRAPH

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 $G_{n,d/n}$. Precisely, we have the following result (cf. Theorem 9.2.4 in [**2**]).

Theorem 2.1 ([**2**]). *Let G be an (n, d, λ)-graph. For a vertex $v \in V$ and a subset B of V denote by $N(v)$ the set of all neighbors of v in G, and let $N_B(v) = N(v) \cap B$ denote the set of all neighbors of v in B. Then for every subset B of V :*

$$\sum_{v\in V}\left(|N_B(v)| - \frac{d}{n}|B|\right)^2 \le \frac{\lambda^2}{n}|B|(n - |B|). \tag{2.1}$$

The following result is an easy corollary of Theorem 2.1.

Theorem 2.2 (cf. Corollary 9.2.5 in [**2**]). *Let G be an (n, d, λ)-graph. For each two sets of vertices B and C of G, we have*

$$|e(B, C) - \frac{d}{n}|B||C|| \le \lambda\sqrt{|B||C|}, \tag{2.2}$$

where $e(B, C)$ is the number of edges in the induced bipartite subgraph of G on (B, C) (i.e. the number of ordered pairs (u, v) where $u \in B$, $v \in C$ and uv is an edge of G).

From Theorem 2.1 and Theorem 2.2, we can derive the following estimate about the number of hinges in an (n, d, λ)-graph.

Theorem 2.3. *Let G be an (n, d, λ)-graph. For every set S of vertices of G, we have*

$$p_2(S) \le |S|\left(\frac{d|S|}{n} + \lambda\right)^2, \tag{2.3}$$

where $p_2(S)$ is the number of ordered paths of length two in S (i.e. the number of ordered triples $(u, v, w) \in S \times S \times S$ with uv, vw are edges of G).

Proof. For a vertex $v \in V$ let $N_S(v)$ denote the set of all neighbors of v in S. From Theorem 2.1, we have

$$\sum_{v\in S}\left(|N_S(v)| - \frac{d}{n}|S|\right)^2 \le \sum_{v\in V}\left(|N_S(v)| - \frac{d}{n}|S|\right)^2 \le \frac{\lambda^2}{n}|S|(n - |S|). \tag{2.4}$$

This implies that

$$\sum_{v\in S} N_S^2(v) + \left(\frac{d}{n}\right)^2 |S|^3 - 2\frac{d}{n}|S|\sum_{v\in S} N_S(v) \leq \frac{\lambda^2}{n}|S|(n-|S|) \tag{2.5}$$

From Theorem 2.2, we have

$$\sum_{v\in S} N_S(v) \leq \frac{d}{n}|S|^2 + \lambda|S|. \tag{2.6}$$

Putting (2.5) and (2.6) together, we have

$$\begin{aligned}\sum_{v\in S} N_S^2(v) &\leq \left(\frac{d}{n}\right)^2 |S|^3 + 2\frac{\lambda d}{n}|S|^2 + \frac{\lambda^2}{n}|S|(n-|S|)\\ &< \left(\frac{d}{n}\right)^2 |S|^3 + 2\frac{\lambda d}{n}|S|^2 + \lambda^2|S| = |S|\left(\frac{d|S|}{n}+\lambda\right)^2,\end{aligned}$$

completing the proof of the theorem.

3. EUCLIDEAN GRAPHS OVER FINITE FIELDS

Let $\mathbb{F}_q$ denote the finite field with q elements where $q \gg 1$ is an odd prime power. For a fixed $a \in \mathbb{F}_q^* = \mathbb{F}_q - \{0\}$, the finite Euclidean graph $G_q(d,a)$ in $\mathbb{F}_q^d$ is defined as the graph with vertex set $V(G_q(d,a)) = \mathbb{F}_q^d$ and the edge set

$$E(G_q(d,a)) = \{(x,y) \in \mathbb{F}_q^d \times \mathbb{F}_q^d \mid x \neq y, ||x-y|| = a\},$$

where $||.||$ is the analogue of Euclidean distance $||x|| = x_1^2 + \ldots + x_d^2$. In [**17**], Medrano et al. studied the spectrum of these graphs and showed that these graphs are asymptotically Ramanujan graphs. They proved the following result.

Theorem 3.1 ([**17**])**.** *The finite Euclidean graph $G_q(d,a)$ is regular of valency $(1+o(1))q^{d-1}$ for any $a \in \mathbb{F}_q^*$. Let λ be any eigenvalue of the graph $G_q(d,a)$ with λ is less than the valency of the graph then*

$$|\lambda| \leq 2q^{\frac{d-1}{2}}. \tag{3.1}$$

Proof of Theorem 1.1. Let $\mathcal{E}$ be a subset of $\mathbb{F}_q^d$. We have that the number of ordered triple $(u,v,w) \in \mathcal{E}\times\mathcal{E}\times\mathcal{E}$ with uv and vw are edges of $G_q(d,a)$ is $\sum_{\boldsymbol{p}\in\mathcal{E}} \deg_{\mathcal{E}}(\boldsymbol{p},a)^2$. From Theorem 2.3 and Theorem 3.1, we have

$$f(\mathcal{E}) \leq \sum_{a\in\mathbb{F}_q^*} |\mathcal{E}|\Big((1+o(1))\frac{|\mathcal{E}|}{q}+2q^{\frac{d-1}{2}}\Big)^2 \leq (q-1)|\mathcal{E}|\Big((1+o(1))\frac{|\mathcal{E}|}{q}+2q^{\frac{d-1}{2}}\Big)^2. \tag{3.2}$$

Thus, if $|\mathcal{E}| \gtrsim q^{\frac{d+1}{2}}$ then

$$f(\mathcal{E}) \lesssim |\mathcal{E}|^3/q, \tag{3.3}$$

and if $|\mathcal{E}| \lesssim q^{\frac{d+1}{2}}$ then

$$f(\mathcal{E}) \lesssim |\mathcal{E}|q^d. \tag{3.4}$$

We now give a lower bound for $f(\mathcal{E})$. We have

$$\begin{aligned} f(\mathcal{E}) &= \sum_{r\in\mathbb{F}_q^*}\left(\sum_{\boldsymbol{p}\in\mathcal{E}}\deg_{\mathcal{E}}(\boldsymbol{p},r)^2\right) \geq \sum_{r\in\mathbb{F}_q^*}\frac{1}{|\mathcal{E}|}\left(\sum_{\boldsymbol{p}\in\mathcal{E}}\deg_{\mathcal{E}}(\boldsymbol{p},r)\right)^2 \\ &\geq \frac{1}{(q-1)|\mathcal{E}|}\left(\sum_{r\in\mathbb{F}_q^*}\sum_{\boldsymbol{p}\in\mathcal{E}}\deg_{\mathcal{E}}(\boldsymbol{p},r)\right)^2 \geq \frac{|\mathcal{E}|(|\mathcal{E}|-1)^2}{(q-1)}. \end{aligned} \tag{3.5}$$

Theorem 1.1 follows immediately from (3.3), (3.4) and (3.5).

Remark 3.2. From the above proof, we can derive the result (1.1) as follows.

$$\frac{1}{|\Delta(\mathcal{E})||\mathcal{E}|}\left(|\mathcal{E}|(|\mathcal{E}|-1)\right)^2 \leq f(\mathcal{E}) \leq |\Delta(\mathcal{E})||\mathcal{E}|\Big((1+o(1))\frac{|\mathcal{E}|}{q}+2q^{\frac{d-1}{2}}\Big)^2.$$

This implies that

$$|\Delta(\mathcal{E})| \geq \frac{(1+o(1))q}{1+2\frac{q^{(d+1)/2}}{|\mathcal{E}|}},$$

and the equation (1.1) follows immediately. Note that q, a power of an odd prime, is viewed as an asymptotic parameter.

4. FINITE EUCLIDEAN GRAPHS OVER RINGS

We first recall some properties of finite Euclidean graphs over rings. We follows the presentation in [**18**]. Given $a \in \mathbb{Z}_q$, define the Euclidean graph $X_q(d,a)$ as follows. The vertices are the vectors in $\mathbb{Z}_q^d$, and two vertices $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_q^d$ are adjacent if $d(\boldsymbol{x},\boldsymbol{y}) = a$.

A Cayley graph $X(G,S)$ for an additive group G and a symmetric edge set $S \subset G$ has the elements of G as vertices and edges between vertices x and $y = x+s$ for $x, y \in G$ and $s \in S$. The set S is symmetric if $s \in S$ then $-s \in S$. Let

$$S_q(n,a) = \big\{\boldsymbol{x} \in \mathbb{Z}_q^n \mid d(\boldsymbol{x},\boldsymbol{0}) = a\big\}. \tag{4.1}$$

The Euclidean graph $X_q(d,a)$ is a Cayley graph for the additive group of $\mathbb{Z}_q^d$ with edge set $S_q(d,a)$. The following theorem tells us about the valency of $X_q(d,a)$.

Theorem 4.1 ([**18**, Theorem 2.1])**.** *If $p \nmid a$, i.e. $a \in \mathbb{Z}_q^\times$ = the multiplicative group of units mod q, the degree of the Euclidean graph $X_{p^r}(d,a)$ is given by*

$$|S_{p^r}(d,a)| = p^{(d-1)(r-1)}|S_p(d,a)|,$$

where

$$|S_p(d,a)| = \begin{cases} p^{d-1} + \chi\big((-1)^{\frac{d-1}{2}}a\big)p^{\frac{d-1}{2}} & \textit{if } d \textit{ odd},\\ p^{d-1} - \chi\big((-1)^{\frac{d-1}{2}}\big)p^{\frac{d-2}{2}} & \textit{if } d \textit{ even}.\end{cases}$$

Here the Legendre symbol χ *is defined by*

$$\chi(b) = \begin{cases} 1 & p \nmid b, b \textit{ is a square mod } p,\\ -1 & p \nmid b, b \textit{ is not a square mod } p,\\ 0 & p \mid b.\end{cases}$$

It follows that

$$|S_{p^r}(d,a)| = (1+o(1))p^{(d-1)r}. \tag{4.2}$$

In [**18**], Medrano, Myers, Stark and Terras studied the spectrum of the adjacency operator A_a acting on functions $f : \mathbb{Z}_q^d \to \mathbb{C}$ by

$$A_a f(\boldsymbol{x}) = \sum_{d(\boldsymbol{x},\boldsymbol{y})=a} f(\boldsymbol{y}).$$

Define the exponentials

$$e(v) = e^{(r)}(v) = \exp(2\pi i v/p^r),\ v \in \mathbb{Z}_{p^r},$$

$$e_{\boldsymbol{b}}(\boldsymbol{u}) = e_{\boldsymbol{b}}^{(r)}(\boldsymbol{u}) = \exp(2\pi i\ {}^t\boldsymbol{b}\cdot\boldsymbol{u}/p^r),\ \boldsymbol{b},\boldsymbol{u} \in \mathbb{Z}_q^d,$$

Medrano, Myers, Stark and Terras showed that

Proposition 4.2 ([**18**, Proposition 2.2])**.** *The function* $e_{\boldsymbol{b}}$*, for* $\boldsymbol{b} \in \mathbb{Z}_q^d$*, is an eigenfunction of the adjacency operator* A_a *of* $X_{p^r}(d,a)$ *corresponding to the eigenvalue*

$$\lambda_{\boldsymbol{b}}^{(r)} = \sum_{d(\boldsymbol{s},\boldsymbol{0})=a} e_{\boldsymbol{b}}^{(r)}(\boldsymbol{s}).$$

Moreover, as $\boldsymbol{b}$ *runs through* $\mathbb{Z}_q^d$*, the* $e_{\boldsymbol{b}}(\boldsymbol{x})$ *form a complete orthogonal set of eigenfunctions of* A_a*. It follows that every eigenvalue of* $X_q(d,a)$ *has the form* $\lambda_{\boldsymbol{b}}$ *for some* $\boldsymbol{b} \in \mathbb{Z}_q^d$*.*

Using this formula, eigenvalues of $X_q(d,a)$ can be computed explicitly. Before beginning this discussion, we recall the Gauss sum. For $v \in \mathbb{Z}_q^\times$, define the Gauss sum

$$G_v^{(v)} = \sum_{y\in\mathbb{Z}_q} e(vy^2).$$

This is not the only kind of Gauss sum associated with rings. Another sort of Gauss sum over rings appears in Odoni [**19**].

Theorem 4.3 ([**18**, Theorem 2.9, Corollary 2.10])**.** *Suppose $p \nmid a$ and $q = p^r$. Then we have the following formula for the eigenvalue $\lambda_{2\boldsymbol{b}}^{(r)}$ of the Euclidean graph $X_q(d,a)$:*

$$q\lambda_{2\boldsymbol{b}}^{(r)} = S_1^{(r)} + S_2^{(r)}, \tag{4.3}$$

where

$$S_1^{(r)} = \begin{cases} 0 & \textit{if } p \nmid b_j \textit{ for some } j, \\ p^{r+d-1}\lambda_{2\boldsymbol{b}/p}^{(r-1)} & \textit{if } p \mid b_j \textit{ for all } j, \end{cases}$$

and

$$S_2^{(r)} = \sum_{v \in \mathbb{Z}_q^\times} (G_v^{(r)})^d e^{(r)}\left(-av - \frac{1}{v}\,{}^t\boldsymbol{b}\cdot\boldsymbol{b}\right).$$

The term S_2 can also be computed explicitly. Here χ denotes the Legendre symbol.

1. *If r is even,*

$$S_2^{(r)} = p^{\frac{rd}{2}} \begin{cases} 0 & \textit{if } a^t\boldsymbol{b}\cdot\boldsymbol{b} \neq \textit{square mod } q, \textit{ or if } p \mid a^t\boldsymbol{b}\cdot\boldsymbol{b}, \\ 2p^{r/2}\cos\dfrac{4\pi c}{p^r} & \textit{if } a^t\boldsymbol{b}\cdot\boldsymbol{b} = c^2, p \nmid c. \end{cases}$$

2. *If n is even and r is odd,*

$$S_2^{(r)} = 2p^{\frac{r(d+1)}{2}}\chi(c) \begin{cases} 0 & \textit{if } a^t\boldsymbol{b}\cdot\boldsymbol{b} \neq \textit{square mod } q, \textit{ or if } p \mid a^t\boldsymbol{b}\cdot\boldsymbol{b} \\ \cos\dfrac{4\pi c}{p^r} & \textit{if } a^t\boldsymbol{b}\cdot\boldsymbol{b} = c^2, p \nmid c, p \equiv 1(\textit{mod } 4), \\ (-1)^{\frac{d}{2}-1}\sin\dfrac{4\pi c}{p^r} & \textit{if } a^t\boldsymbol{b}\cdot\boldsymbol{b} = c^2, p \nmid c, p \equiv 3(\textit{mod } 4). \end{cases}$$

3. *If n is odd and r is odd,*

$$S_2^{(r)} = 2p^{\frac{r(d+1)}{2}}\chi(-\bar{a})\cos\frac{4\pi c}{p^r} \begin{cases} 0 & \textit{if } a^t\boldsymbol{b}\cdot\boldsymbol{b} \neq \textit{square mod } q, \textit{ or if } p \mid a^t\boldsymbol{b}\cdot\boldsymbol{b}, \\ 1 & \textit{if } a^t\boldsymbol{b}\cdot\boldsymbol{b} = c^2, p \nmid c, p \equiv 1(\textit{mod } 4), \\ (-1)^{\frac{d+1}{2}} & \textit{if } a^t\boldsymbol{b}\cdot\boldsymbol{b} = c^2, p \nmid c, p \equiv 3(\textit{mod } 4). \end{cases}$$

The later part of Theorem 4.3 implies that

$$|S_2^{(r)}| \leq 2p^{\frac{r(d+1)}{2}}. \tag{4.4}$$

It follows from (4.3) and (4.4) that

$$|\lambda_{2\boldsymbol{b}}^{(1)}| = |S_2^{(1)}|/p \leq 2p^{\frac{d-1}{2}}, \tag{4.5}$$

if $p \nmid b_j$ for some j. From (4.3), (4.4), and (4.5), we easily obtain using induction the following bound for spectrum of the Euclidean graph $X_q(d,a)$

$$|\lambda_{2\boldsymbol{b}}^{(r)}| \leq (2+o(1))p^{(d-1)(r-1)+\frac{d-1}{2}} = (2+o(1))q^{\frac{(d-1)(2r-1)}{2r}} \quad \text{if } \boldsymbol{b} \neq \boldsymbol{0}, p \nmid a. \tag{4.6}$$

Putting (4.2) and (4.6) together, we have the pseudo-randomness of the Euclidean graph $X_q(d,a)$.

Theorem 4.4. *Suppose $p \nmid a$ and $q = p^r$. Then the Euclidean graph $X_q(d,a)$ is an*

$$(q^d, (1+o(1))q^{d-1}, (2+o(1))q^{(d-1)(2r-1)/2r}) - graph.$$

Proof of Theorem 1.2. Let $\mathcal{E}$ be a subset of $\mathbb{Z}_q^d$. We have that the number of ordered triple $(u,v,w) \in \mathcal{E} \times \mathcal{E} \times \mathcal{E}$ with uv and vw are edges of $X_q(d,a)$ is $\sum_{\boldsymbol{p} \in \mathcal{E}} \deg_{\mathcal{E}}(\boldsymbol{p}, a)^2$. From Theorem 2.3 and Theorem 4.4, we have

$$\begin{aligned} f(\mathcal{E}) &\leq \sum_{a \in \mathbb{Z}_q^\times} |\mathcal{E}| \left((1+o(1))\frac{|\mathcal{E}|}{q} + (2+o(1))q^{\frac{(d-1)(2r-1)}{2r}} \right)^2 \\ &\leq (1+o(1))q|\mathcal{E}| \left((1+o(1))\frac{|\mathcal{E}|}{q} + (2+o(1))q^{\frac{(d-1)(2r-1)}{2r}} \right)^2. \end{aligned} \tag{4.7}$$

Thus, if $|\mathcal{E}| \gtrsim q^{\frac{d(2r-1)+1}{2r}}$ then

$$f(\mathcal{E}) \lesssim |\mathcal{E}|^3/q, \tag{4.8}$$

and if $|\mathcal{E}| \lesssim q^{\frac{d(2r-1)+1}{2r}}$ then

$$f(\mathcal{E}) \lesssim |\mathcal{E}| q^{(d(2r-1)+1-r)/r}. \tag{4.9}$$

The lower bound for $f(\mathcal{E})$ is similar to the case of vector spaces over finite fields.

$$\begin{aligned} f(\mathcal{E}) &= \sum_{r \in \mathbb{F}_q^*} \left(\sum_{\boldsymbol{p} \in \mathcal{E}} \deg_{\mathcal{E}}(\boldsymbol{p}, r)^2 \right) \geq \sum_{r \in \mathbb{F}_q^*} \frac{1}{|\mathcal{E}|} \left(\sum_{\boldsymbol{p} \in \mathcal{E}} \deg_{\mathcal{E}}(\boldsymbol{p}, r) \right)^2 \\ &\geq \frac{1}{(q-1)|\mathcal{E}|} \left(\sum_{r \in \mathbb{F}_q^*} \sum_{\boldsymbol{p} \in \mathcal{E}} \deg_{\mathcal{E}}(\boldsymbol{p}, r) \right)^2 \geq \frac{|\mathcal{E}|(|\mathcal{E}|-1)^2}{(q-1)}. \end{aligned} \tag{4.10}$$

Theorem 1.2 follows immediately from (4.8), (4.9) and (4.10). Note that, from the above proof, we can derive the result (1.2) as follows:

$$\begin{aligned} \frac{1}{|\Delta(\mathcal{E})||\mathcal{E}|} (|\mathcal{E}|(|\mathcal{E}|-1))^2 &\leq f(\mathcal{E}) \\ &\leq |\Delta(\mathcal{E})||\mathcal{E}| \left((1+o(1))\frac{|\mathcal{E}|}{q} + (2+o(1))q^{\frac{(d-1)(2r-1)}{2r}} \right)^2. \end{aligned}$$

This implies that

$$|\Delta(\mathcal{E})| \geq \frac{(1+o(1))q}{1 + 2q^{\frac{d(2r-1)+1}{2r}}/|\mathcal{E}|},$$

and the equation (1.2) follows immediately. Note that q, a power of an odd prime, is viewed as an asymptotic parameter.

5. FURTHER REMARKS

The proofs in [**12**] show that the conclusion of (1.1) holds with the non-degenerate quadratic form Q is replaced by any function F with the property that the Fourier transform satisfies the decay estimates

$$|\hat{F}_t(m)| = \left| q^{-d} \sum_{x\in\mathbb{F}_q^d : F(x)=t} \chi(-x\cdot m) \right| \le Cq^{-(d+1)/2} \tag{5.1}$$

and

$$|\hat{F}_t(0,\dots,0)| = \left| q^{-d} \sum_{x\in\mathbb{F}_q^d : F(x)=t} \chi(-x\cdot (0,\dots,0)) \right| \le Cq^{-1}, \tag{5.2}$$

where $\chi(s) = e^{2\pi i \mathrm{Tr}(s)/q}$ and $m \ne (0,\dots,0) \in \mathbb{F}_q^d$ (recall that for $y \in \mathbb{F}_q$, where $q = p^r$ with p prime, the trace of y is defined as $\mathrm{Tr}(y) = y + y^p + \cdots + y^{p^{r-1}} \in \mathbb{F}_q$). The basic object in these proofs is the incidence function

$$\begin{aligned} I_{B,C}(j) = |B||C|v(j) &= |(x,y) \in B\times C : F(x-y) = j| \\ &= \sum_{x,y\in\mathbb{F}_q^d} B(x)C(y)F_j(x-y), \end{aligned}$$

where B, C, F_j denote the characteristic functions of the sets B, C and $\{x : F(x) = j\}$, respectively. Using the Fourier inversion, we have

$$I_{B,C}(j) = q^{2d} \sum_{m\in\mathbb{F}_q^d} \overline{\hat{B}(m)}\hat{C}(m)\hat{F}_j(m). \tag{5.3}$$

Now we define the F-distance graph $G_F(q,d,j)$ with the vertex set $V = \mathbb{F}_q^d$ and the edge set

$$E(G_F(q,d,j)) = \{(x,y) \in V\times V | x \ne y, F(x-y) = j\}.$$

Then the exponentials (or characters of the additive group $\mathbb{F}_q^d$)

$$e_m(x) = \exp\left(\frac{2\pi i \mathrm{Tr}(x\cdot m)}{p}\right), \tag{5.4}$$

for $x, m \in \mathbb{F}_q^d$, are eigenfunctions of the adjacency operator for the F-distance graph $G_F(q,d,j)$ corresponding to the eigenvalue

$$\lambda_m = \sum_{F(x)=j} e_m(x) = q^d \hat{F}_j(-m). \tag{5.5}$$

Thus, the decay estimates (5.1) and (5.2) are equivalent to

$$\lambda_m \le Cq^{(d-1)/2}, \tag{5.6}$$

for $m \neq (0,\dots,0) \in \mathbb{F}_q^d$, and

$$\lambda_{(0,\dots,0)} \leq Cq^{d-1}. \tag{5.7}$$

Let A be the adjacency matrix of $G_F(q,d,j)$ with the orthonormal base $v_0,\dots,v_{q^d-1}$, corresponding to eigenvalues $\lambda_{(0,\dots,0)},\dots,\lambda_{(q-1,\dots,q-1)}$, where $v_0 = \bar{1}/\sqrt{n}$. For any two sets $B, C \subset \mathbb{F}_q^d$, let v_B and v_C be the eigenvectors of B and C. Let $v_B = \sum_i \beta_i v_i$ and $v_C = \sum_i \gamma_i v_i$ be their representations as linear combinations of $v_0,\dots,v_{q^d-1}$. We have

$$\begin{aligned} I_{B,C}(j) = e_{G_F(q,d,j)}(B,C) = v_B A v_C &= \Big(\sum_i \beta_i v_i\Big) A \Big(\sum_j \gamma_j v_j\Big) \\ &= \Big(\sum_i \beta_i v_i\Big)\Big(\sum_j \gamma_j \lambda_j v_j\Big) = \sum_i \lambda_i \beta_i \gamma_i. \end{aligned}$$

From (5.3), (5.5) and the above expression, we can see the similarity between our approach and those in [**12**] as follows. Given the decay estimates (5.1) and (5.2), we can bound the incidence function as in [**12**]

$$\begin{aligned} I_{B,C}(j) &\leq |B||C|\hat{F}_j(0,\dots,0) + q^{(d-1)/2} \sum_{m\neq(0,\dots,0)} q^d |\hat{B}(m)||\hat{C}(m)| \\ &\leq Cq^{-1}|B||C| + Cq^{(d-1)/2} q^d \Bigg(\sum_{m\neq(0,\dots,0)} |\hat{B}(m)|^2\Bigg)^{\frac{1}{2}} \Bigg(\sum_{m\neq(0,\dots,0)} |\hat{C}(m)|^2\Bigg)^{\frac{1}{2}} \\ &\leq Cq^{-1}|B||C| + Cq^{d-1} \Bigg(\sum_x |B(x)|^2\Bigg)^{\frac{1}{2}} \Bigg(\sum_x |C(x)|^2\Bigg)^{\frac{1}{2}} \\ &\leq Cq^{-1}|B||C| + Cq^{d-1}\sqrt{|B|}\sqrt{|C|}. \end{aligned}$$

Given the bounds from (5.6), (5.7) for eigenvalues of the F-distance graph $G_F(q,d,j)$, we obtain the same bound for the incidence function

$$\begin{aligned} I_{B,C}(j) &= \lambda_{(0,\dots,0)} \langle v_B, \bar{1}/\sqrt{q^d}\,\rangle \langle v_C, \bar{1}/\sqrt{q^d}\,\rangle + \sum_{m\neq(0,\dots,0)} \lambda_m \beta_m \gamma_m \\ &\leq Cq^{-1}|B||C| + Cq^{(d-1)/2} \sum_{m\neq(0,\dots,0)} |\beta_m||\gamma_m| \\ &\leq Cq^{-1}|B||C| + Cq^{(d-1)/2} \|\beta\|_2 \|\gamma\|_2 \\ &= Cq^{-1}|B||C| + Cq^{(d-1)/2}\sqrt{|B|}\sqrt{|C|}. \end{aligned}$$

Thus, our approach and the Fourier methods in [**12, 7**] are almost identical. Many results obtained from the Fourier method can be proved using our method and vice versa. However, both methods have their own advantages. On one hand, many results (obtained from the Fourier methods) are hard to derive from the graph theory method. On another hand, the graph theory method sometimes gives us many simple applications without invoking more advanced tools like the character sums or Fourier transform.

Acknowledgments. This research was supported by Vietnam National Foundation for Science and Technology Development grant 101.01-2011.28.

REFERENCES

1. T. Akutsu, H. Tamaki, T. Tokuyama: *Distribution of distances and triangles in a point set and algorithms for computing the largest common point sets.* Discrete Comput. Geom., **20** (1998), 307–331.

2. N. Alon, J. H. Spencer: *The Probabilistic Method*, 2nd ed., Willey-Interscience, 2000.

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

4. P. Brass, W. Moser, J. Pach: *Research problems in discrete geometry*, Springer, 2005.

5. J. Chapman, M. B. Erdogan, D. Hart, A. Iosevich, D. Koh: *Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates.* Math. Z., (to appear).

6. D. Covert, D. Hart, A. Iosevich, S. Senger, I. Uriarte-Tuero: *A Furstenberg-Katznelson-Weiss type theorem on $(d+1)$-point configurations in sets of positive density in finite field geometries.* Discrete Math., **311** (2011), 423–430.

7. D. Covert, A. Iosevich, J. Pakianathan: *Geometric configurations in the ring of integers modulo p^ℓ.* Indiana Univ. Math. J., (to appear).

8. P. Erdős: *On sets of distances of n points.* Amer. Math. Monthly, **53** (1946), 248–250.

9. P. Erdős: *Some of my favorite unsolved problems.* In: A Tribute to Paul Erdös. A. Baker et al., eds., Cambridge Univ. Press 1990, 467–478.

10. D. Hart, A. Iosevich, D. Koh, M. Rudnev: *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture.* Trans. Amer. Math. Soc, **363** (2011), 3255–3275.

11. A. Iosevich, D. Koh: *Erdős-Falconer distance problem, exponential sums, and Fourier analytic approach to incidence theorem in vector spaces over finite fields.* SIAM J. Disc. Math., **23** (2008), 123–135.

12. A. Iosevich, M. Rudnev: *Erdős distance problem in vector spaces over finite fields.* Trans. Amer. Math. Soc., **359** (12) (2007), 6127–6142.

13. A. Iosevich, O. Roche-Newton, M. Rudnev: *On an application of Guth-Katz theorem.* Math. Res. Lett, **18** (4) (2011), 1–7.

14. A. Iosevich, I. E. Shparlinski, M. Xiong: *Sets with integral distances in finite fields.* Trans. Amer. Math. Soc., **362** (2010), 2189–2204.

15. A. Iosevich, S. Senger: *Orthogonal systems in vector spaces over finite fields.* Electron. J. Combin., **15** (2008), Article R151.

16. H. Lefmann, T. Thiele: *Point Sets with Distinct Distances.* Combinatorica, **15** (1995), 379–408.

17. A. Medrano, P. Myers, H. M. Stark, A. Terras: *Finite analogues of Euclidean space.* J. Comput. Appl. Math., **68** (1996), 221–238.

18. A. Medrano, P. Myers, H. M. Stark, A. Terras: *Finite Euclidean graphs over rings.* Proc. Amer. Math. Soc., **126** (3) (1998), 701–710.

19. R. W. K. Odoni: *On Gauss sums* $(mod\, p^n)$, $n \geq 2$. Bull. Lond. Math. Soc., **5** (1973), 325–327.

20. I. E. Shparlinski: *On Point Sets in Vector Spaces over Finite Fields that Determine only Acute Angle.* Bull. Aust. Math. Soc., **81** (2010), 114–120.

21. L. A. Székely: *Crossing numbers and hard Erdös problems in discrete geometry.* Combin. Probab. Comput., **6** (1997), 353–358.

22. L. A. Vinh: *Explicit Ramsey graphs and Erdős distance problem over finite Euclidean and non-Euclidean spaces.* Electron. J. Combin., **15** (2008), R5.

23. L. A. Vinh: *On the number of orthogonal systems in vector spaces over finite fields.* Electron. J. Combin., **15** (2008), N32.

24. L. A. Vinh: *Szemerédi-Trotter type theorem and sum-product estimate in finite fields.* Electron. J. Combin., **32** (8) (2011), 1177–1181.

25. L. A. Vinh: *On a Furstenberg-Katznelson-Weiss type theorem over finite fields.* Ann. Comb., **15** (2011), 541–547.

26. L. A. Vinh: *On k-simplexes in* $(2k-1)$*-dimensional vector spaces over finite fields.* Discrete Math. Theor. Comput. Sci. Proc., **AK** (2009), 871–880.

27. L. A. Vinh: *Singular matrices with restricted rows in vector spaces over finite fields.* Discrete Math., **312** (2) (2012), 413–418.

28. L. A. Vinh: *The sovability of norm, bilinear and quadratic equations over finite fields via spectra of graphs.* Forum Math., (to appear).

29. L. A. Vinh: *Pinned distance sets and k-simplices in vector spaces over finite rings.* (preprint) (2011).

University of Education,
Vietnam National University, Hanoi
Vietnam
E-mail: vinhla@vnu.edu.vn

(Received August 31, 2012)
(Revised December 10, 2012)