INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus

Mathématique

Doowon Koh and Thang Pham

A point-sphere incidence bound in odd dimensions and applications

Volume 360 (2022), p. 687-698

<https://doi.org/10.5802/crmath.333>

Comptes Rendus
Mathématique
2022, 360, p. 687-698
https://doi.org/10.5802/crmath.333

Combinatorics / *Combinatoire*

A point-sphere incidence bound in odd dimensions and applications

Doowon Koh [a] **and Thang Pham** [*, b]

[a] Department of Mathematics, Chungbuk National University, Korea

[b] University of Science, Vietnam National University, Hanoi, Vietnam

E-mails: koh131@chungbuk.ac.kr, thangpham.math@vnu.edu.vn

Abstract. In this paper, we prove a new point-sphere incidence bound in vector spaces over finite fields. More precisely, let P be a set of points and S be a set of spheres in $\mathbb{F}_q^d$. Suppose that $|P|, |S| \le N$, we prove that the number of incidences between P and S satisfies

$$I(P,S) \le N^2 q^{-1} + q^{\frac{d-1}{2}} N,$$

under some conditions on d, q, and radii. This improves the known upper bound $N^2 q^{-1} + q^{\frac{d}{2}} N$ in the literature. As an application, we show that for $A \subset \mathbb{F}_q$ with $q^{1/2} \ll |A| \ll q^{\frac{d^2+1}{2d^2}}$, one has

$$\max\left\{|A+A|,\ |dA^2|\right\} \gg \frac{|A|^d}{q^{\frac{d-1}{2}}}.$$

This improves earlier results on this sum-product type problem over arbitrary finite fields.

Funding. D. Koh was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MIST) (No. NRF-2018R1D1A1B07044469). T. Pham was supported by Swiss National Science Foundation grant P4P4P2- 191067.

Manuscript received 17th September 2021, revised 28th December 2021, accepted 19th January 2022.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of order q, where q is a prime power. A sphere centered at $(c_1, \ldots, c_d) \in \mathbb{F}_q^d$ of radius r is defined by the equation

$$(x_1 - c_1)^2 + \cdots + (x_d - c_d)^2 = r.$$

Let P be a set of points in $\mathbb{F}_q^d$ and S be a set of spheres with arbitrary radii in $\mathbb{F}_q^d$. Let $I(P,S)$ be the number of incidences between P and S, namely,

$$I(P,S) = \#\left\{(p,s) :\ p \in s, p \in P, s \in S\right\}.$$

The following point-sphere incidence bound was obtained by Cilleruelo, Iosevich, Lund, Roche-Newton, and Rudnev [2], and independently by Phuong, Pham, and Vinh [13].

[*] Corresponding author.

ISSN (electronic) : 1778-3569

Theorem 1. *Let P be a set of points in $\mathbb{F}_q^d$ and S be a set of spheres with arbitrary radii in $\mathbb{F}_q^d$. We have*

$$\left| I(P,S) - \frac{|P||S|}{q} \right| \leq q^{\frac{d}{2}} (|P||S|)^{1/2}. \tag{1}$$

It follows from this theorem that if $|P||S| > q^{d+2}$, then the set of point-sphere incidences between P and S is non-empty. Using this incidence bound, Cilleruelo et al. [2] proved a Beck type theorem that for any set $P \subset \mathbb{F}_q^2$, if $|P| > 5q$, then the number of distinct circles determined by points of P is at least $\frac{4q^3}{9}$. We refer the reader to [2, 13] for other applications.

Throughout this paper, we use the following notations: $X \ll Y$ means that there exists some absolute constant $C_1 > 0$ such that $X \leq C_1 Y$, and $X \sim Y$ means $Y \ll X \ll Y$.

The main purpose of this paper is to improve the upper bound of Theorem 1. More precisely, we study the following question:

Question 2. *Let P be a set of points and S be a set of spheres in $\mathbb{F}_q^d$. Under what conditions on d, q, and the sets will we be able to improve the bound $\frac{|P||S|}{q} + q^{\frac{d}{2}}\sqrt{|P||S|}$?*

We first start with some observations.

Observation 1. If $d \equiv 3 \bmod 4$ and $q \equiv 1 \bmod 4$, or $d \equiv 1 \bmod 4$, then the term $q^{\frac{d}{2}}(|P||S|)^{1/2}$ in (1) cannot be improved to $q^{\frac{d}{2}-\epsilon}(|P||S|)^{1/2}$ for any $\epsilon > 0$ for arbitrary sets P and S. Otherwise, one could follow the proof of [2, Corollary 1] to show that for any $E \subset \mathbb{F}_q^d$ with $|E| \gg q^{\frac{d+1}{2}-\epsilon'}$, for some $\epsilon' > 0$, we have the set of distances determined by pairs of points in E satisfies $|\Delta(E)| \gg q$. This would contradict a construction in [3, Theorem 2.7] that states that the exponent $\frac{d+1}{2}$ for the distance problem is sharp in those dimensions even one wishes to cover a positive proportion of all distances. Note that in the proof of [2, Corollary 1], the size of S is much larger than the number of points in P. We refer the reader to [2, 3] for more explanations.

Observation 2. If $d \equiv 2 \bmod 4$ and $q \equiv 1 \bmod 4$, or $d \equiv 0 \bmod 4$, then there exists a set $E \subset \mathbb{F}_q^d$ with $|E| = q^{\frac{d}{2}}$ such that $x \cdot y = x \cdot x = 0$ for all $x, y \in E$, see [3, Lemma 5.1]. Hence, we can set $P = E$ and S being the set of spheres centered at points in E of radius 0. It is clear that $I(P,S) = |P||S| = q^{\frac{d}{2}}\sqrt{|P||S|}$. Thus, the upper bound of (1) is sharp for this case.

Observation 3. If all spheres in S have the same radius, then a stronger result follows directly from a theorem of Iosevich and Rudnev in [6]:

$$\left| I(P,S) - \frac{|P||S|}{q} \right| < 2q^{\frac{d-1}{2}} (|P||S|)^{1/2}. \tag{2}$$

In a recent paper [7], Koh, Pham, and Lee introduced an approach of using results from the restriction problem for cones to study this incidence topic. As a consequence, they obtained the following improvement.

Theorem 3. *Let P be a set of points in $\mathbb{F}_q^d$ and S be a set of spheres in $\mathbb{F}_q^d$.*

(1) *If $d \equiv 2 \bmod 4$, $q \equiv 3 \bmod 4$, and $|S| \leq q^{\frac{d}{2}}$, then we have*

$$\left| I(P,S) - q^{-1}|P||S| \right| \ll q^{\frac{d-1}{2}} |P|^{\frac{1}{2}} |S|^{\frac{1}{2}}.$$

(2) *If d is even and $q \equiv 1 \bmod 4$, or $d \equiv 0 \bmod 4$, then the same conclusion holds under the condition $|S| \leq q^{\frac{d-2}{2}}$.*

(3) *If $d \geq 3$ is odd, then the same conclusion holds under the condition $|S| \leq q^{\frac{d-1}{2}}$.*

In comparison, in its ranges, Theorem 3 improves Theorem 1 in both lower and upper bounds. Theorem 3 is sharp in the sense that one can construct sets P and S with $|S|$ arbitrary small and $|P||S| \leq q^{d+1}$ such that $I(P,S) = 0$.

In the first result we provide an improvement in odd dimensions when $|P| \sim |S|$.

Theorem 4. *Let P be a set of points and S be a set of spheres of* square *radii in $\mathbb{F}_q^d$. Suppose that $d \equiv 3 \bmod 4$ and $q \equiv 3 \bmod 4$. If $|P|, |S| \le N$, then we have*

$$I(P,S) \ll q^{-1}N^2 + q^{\frac{d-1}{2}}N.$$

It is worth noting that one cannot expect to prove the same upper bound in even dimensions ($d \equiv 2 \bmod 4$ and $q \equiv 1 \bmod 4$, or $d \equiv 0 \bmod 4$). This follows from the second observation above, but it is not known whether or not the same upper bound can be achieved if we assume that the spheres have non-zero radii.

The proof of Theorem 4 is based on a careful analysis of spectrum of graphs defined by cone equations. In particular, let C_k be the cone in $\mathbb{F}_q^k$ defined by

$$C_k := \left\{x \in \mathbb{F}_q^k \colon Q(x) = -x_1^2 + x_2^2 + \cdots + x_k^2 = 0\right\}. \tag{3}$$

Let $G_{Q,k}$ be the Cayley graph with the vertex set $\mathbb{F}_q^k$, there is an edge between two vertices x and y if and only if $x - y \in C_k$. It is clear that $G_{Q,k}$ is a regular graph of order $|C_k|$. In the following theorem, we show that when $k \equiv 0 \bmod 4$ and $q \equiv 3 \bmod 4$, the unique positive and non-trivial eigenvalue of this graph is much smaller than the absolute value of others. This observation plays the main role in the proof of Theorem 4.

Theorem 5. *Let $\{\lambda_m\}_{m \in \mathbb{F}_q^k}$ be the eigenvalues of $G_{Q,k}$. If $k \equiv 0 \bmod 4$ and $q \equiv 3 \bmod 4$, then we have*

$$\lambda_m = q^k \cdot \begin{cases} q^{-1}\delta_0(m) - q^{-\frac{k}{2}} + q^{-\frac{(k+2)}{2}} & \text{if } m \in C_k \\ q^{-\frac{(k+2)}{2}} & \text{if } m \notin C_k. \end{cases}$$

Here, and throughout the paper, we define $\delta_0(m) = 1$ if $m = (0,\ldots,0)$, and $\delta_0(m) = 0$ otherwise.

Our next improvement is for spheres of non-square radii in dimensions $d \equiv 1 \bmod 4$.

Theorem 6. *Let P be a set of points and S be a set of spheres of* non-square *radii in $\mathbb{F}_q^d$. Suppose that $d \equiv 1 \bmod 4$ and $q \equiv 3 \bmod 4$. If $|P|, |S| \le N$, then we have*

$$I(P,S) \ll q^{-1}N^2 + q^{\frac{d-1}{2}}N.$$

Unlike Theorem 4, we do not have any construction to show that the upper bound $q^{-1}N^2 + q^{\frac{d-1}{2}}N$ is impossible for even dimensions.

Theorem 6 is proved by the same approach as for Theorem 4. The main difference is that we use the Cayley graph defined by the zero-norm equation. In particular, let S_0^{k-1} be the sphere centered at the origin of radius zero in $\mathbb{F}_q^k$ defined by

$$S_0^{k-1} := \left\{x \in \mathbb{F}_q^k \colon \|x\| := x_1^2 + x_2^2 + \cdots + x_k^2 = 0\right\}. \tag{4}$$

Let $G_{\|\cdot\|,k}$ be the Cayley graph with the vertex set $\mathbb{F}_q^k$, there is an edge between two vertices x and y if and only if $x - y \in S_0^{k-1}$. It is clear that $G_{\|\cdot\|,k}$ is a regular graph of order $|S_0^{k-1}|$. As in the graph $G_{Q,k}$, in the following theorem, we show that when $k \equiv 2 \bmod 4$ and $q \equiv 3 \bmod 4$, the unique positive and non-trivial eigenvalue of this graph is much smaller than the absolute value of others.

Theorem 7. *Let $\{\lambda_m\}_{m \in \mathbb{F}_q^k}$ be the eigenvalues of $G_{\|\cdot\|,k}$. If $k \equiv 2 \bmod 4$ and $q \equiv 3 \bmod 4$, then we have*

$$\lambda_m = q^k \cdot \begin{cases} q^{-1}\delta_0(m) - q^{-\frac{k}{2}} + q^{-\frac{k+2}{2}} & \text{if } \|m\| = 0 \\ q^{-\frac{(k+2)}{2}} & \text{if } \|m\| \neq 0. \end{cases}$$

In graph theoretic point of view, we believe that Theorems 5 and 7 have a potential for applications to other topics.

Sharpness of Theorems 4 and 6. Both Theorems 4 and 6 cannot be improved when $N > q^{\frac{d+1}{2}}$. The simplest example is to take S being a set of spheres with the same radius, then Observation 3 would tell us that $I(P,S) \sim N^2/q$. When $N > q^{\frac{d+2}{2}}$, Theorem 1 also tells us that the number of incidences is at least $(1-o(1))N^2/q$.

We now provide some applications.

Erdős–Falconer distance problem. For any two points x and y in $\mathbb{F}_q^d$, we define its distance function by $\|x-y\| = (x_1-y_1)^2+\cdots+(x_d-y_d)^2$. For $E \subset \mathbb{F}_q^d$ and $t \neq 0$, let $U(t)$ be the number of pairs of points in E of distance t. Iosevich and Rudnev [6], using the Kloosterman sum, proved that

$$\frac{|E|^2}{q} - 2q^{\frac{d-1}{2}}|E| \le U(t) \le \frac{|E|^2}{q} + 2q^{\frac{d-1}{2}}|E| \tag{5}$$

As a consequence of Theorem 4, we can see that the upper bound of (5) can be recovered when t is a square. The same holds when t is a non-square by Theorem 6. The most interesting aspect of this observation is that we are able to use Gauss sums instead of Kloosterman sum in the proof. It is still an open question whether or not one can prove the lower bound of (5) without the Kloosterman sum.

A sum-product type estimate. For $A \subset \mathbb{F}_q$, we define

$$A+A := \{a+b\colon a,b \in A\},\ A^2 := \{a^2\colon a \in A\},\ nA^2 = \left\{a_1+\cdots+a_n\colon a_i \in A^2\right\}.$$

As a consequence of Theorem 4, we obtain the following sum-product type estimate.

Theorem 8. *Let A be a set in $\mathbb{F}_q$ with $q \equiv 3 \bmod 4$ and $|A| \gg q^{1/2}$. For $d \ge 3$ odd, we have at least one of two following statements:*

(1) $|A+A| \ge \min\left\{q^{\frac{d+1}{2d}}, |A|^{\frac{d+1}{d}}\right\}$.

(2) $|dA^2| \gg \frac{|A|^d}{q^{\frac{d-1}{2}}}$.

Corollary 9. *Let A be a set in $\mathbb{F}_q$ with $q \equiv 3 \bmod 4$ and $q^{1/2} \ll |A| \ll q^{\frac{d^2+1}{2d^2}}$. For $d \ge 3$ odd, we have*

$$\max\left\{|A+A|, \left|dA^2\right|\right\} \gg \frac{|A|^d}{q^{\frac{d-1}{2}}}.$$

In particular, for $d = 3$, one has

$$\max\left\{|A+A|, \left|A^2+A^2+A^2\right|\right\} \gg \frac{|A|^3}{q}.$$

The lower bound $|A|^d q^{-\frac{d-1}{2}}$ improves earlier results in the literature, for instance, $|A|^{\frac{3d-5}{d-1}} q^{\frac{2-d}{d-1}}$ in [12]. We refer the reader to [12] for discussions on this sum-product type problem, and to [11, 14] and references therein for results on other types.

The rest of this paper is organized as follows. In the next section, we recall some notations from discrete Fourier analysis, and proofs of Theorems 5 and 7 are given in Sections 3 and 4, respectively. In Section 5, we provide proofs of Theorems 4 and 6. In Section 6, a proof of Theorem 8 is presented. In the last section, we address some open questions.

2. Preliminaries

We first recall some notations and lemmas from discrete Fourier analysis. Let f be a complex valued function on $\mathbb{F}_q^k$. The Fourier transform $\widehat{f}$ of f is defined by

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

where χ denotes the principal additive character of $\mathbb{F}_q$. The Fourier inversion theorem states that

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

The orthogonality of the additive character χ says that

$$\sum_{\alpha\in\mathbb{F}_q^k} \chi(\beta\cdot\alpha) = \begin{cases} 0 & \text{if } \beta \neq (0,\ldots,0),\\ q^k & \text{if } \beta = (0,\ldots,0). \end{cases}$$

As a direct application of the orthogonality of χ, we obtain

$$\sum_{m\in\mathbb{F}_q^k} \left|\widehat{f}(m)\right|^2 = q^{-k}\sum_{x\in\mathbb{F}_q^k} |f(x)|^2,$$

which is known as the Plancherel theorem.

For example, it follows from the Plancherel theorem that for any set E in $\mathbb{F}_q^k$,

$$\sum_{m\in\mathbb{F}_q^k} |\widehat{E}(m)|^2 = q^{-k}|E|.$$

Here, and throughout this note, we identify a set E with the indicator function 1_E on E.

Throughout this paper, let η be the quadratic character of $\mathbb{F}_q$, namely, for $s \neq 0$, $\eta(s) = 1$ if s is a square, and $\eta(s) = -1$ if s is a non-square. We also use the convention that $\eta(0) = 0$.

For $a \in \mathbb{F}_q^*$, the Gauss sum $\mathcal{G}_a$ is defined by

$$\mathcal{G}_a := \sum_{s\in\mathbb{F}_q^*} \eta(s)\chi(as), \tag{6}$$

which can be written as

$$\mathcal{G}_a = \sum_{s\in\mathbb{F}_q} \chi(as^2) = \eta(a)\mathcal{G}_1.$$

The absolute value of the Gauss sum $\mathcal{G}_a$ is exactly $q^{1/2}$. Moreover, the explicit form of the Gauss sum $\mathcal{G}_1$ is provided in the next lemma.

Lemma 10 ([10, Theorem 5.15]). *Let $\mathbb{F}_q$ be a finite field with $q = p^\ell$, where p is an odd prime and $\ell \in \mathbb{N}$. Then we have*

$$\mathcal{G}_1 = \begin{cases} (-1)^{\ell-1} q^{\frac{1}{2}} & \text{if} \quad p \equiv 1 \mod 4\\ (-1)^{\ell-1} i^\ell q^{\frac{1}{2}} & \text{if} \quad p \equiv 3 \mod 4. \end{cases}$$

Notice that $q = p^l \equiv 3 \bmod 4$ if and only if $p \equiv 3 \bmod 4$ and l is an odd positive integer.

The following formula will be used in our proof of Theorem 5. For $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$,

$$\sum_{s\in\mathbb{F}_q} \chi(as^2 + bs) = \eta(a)\mathcal{G}_1\chi\left(\frac{b^2}{-4a}\right). \tag{7}$$

This can be proved easily by completing the square and using a change of variables.

Let X be a multi-set in $\mathbb{F}_q^\ell \times \mathbb{F}_q$, $\ell \geq 1$. We denote by $\overline{X}$ the set of distinct elements in the multi-set X. The cardinality of X, denoted by $|X|$, is $\sum_{x\in\bar{X}} m_X(x)$, where $m_X(x)$ is the multiplicity of $\mathbf{x}$ in X. For multi-sets $\mathcal{A},\mathcal{B} \subset \mathbb{F}_q^{\ell+1}$, let $N(\mathcal{A},\mathcal{B})$ be the number of pairs $\big((\alpha,a),(\beta,b)\big) \in \mathcal{A}\times\mathcal{B} \subset \left(\mathbb{F}_q^\ell \times \mathbb{F}_q\right)^2$ such that $\alpha\cdot\beta = a + b$. We have the following lemma on an upper bound of $N(\mathcal{A},\mathcal{B})$.

Lemma 11. [1] *Let $\mathscr{A},\mathscr{B}$ be multi-sets in $\mathbb{F}_q^\ell \times \mathbb{F}_q$, $\ell \geq 1$. We have*

$$\left|N(\mathscr{A},\mathscr{B}) - \frac{|\mathscr{A}||\mathscr{B}|}{q}\right| \leq q^{\frac{\ell}{2}} \left(\sum_{(\alpha,a)\in\bar{\mathscr{A}}} m_{\mathscr{A}}((\alpha,a))^2 \sum_{(\beta,b)\in\bar{\mathscr{B}}} m_{\mathscr{B}}((\beta,b))^2 \right)^{1/2}.$$

Proof. We first have

$$N(\mathscr{A},\mathscr{B}) = \sum_{(\alpha,a)\in\bar{\mathscr{A}},(\beta,b)\in\bar{\mathscr{B}}} q^{-1} m_{\mathscr{A}}((\alpha,a)) m_{\mathscr{B}}((\beta,b)) \sum_{s\in\mathbb{F}_q} \chi(s(\alpha\cdot\beta - a - b)),$$

where χ is a non-trivial additive character on $\mathbb{F}_q$. This implies that

$$N(\mathscr{A},\mathscr{B}) = \frac{|\mathscr{A}||\mathscr{B}|}{q} + R,$$

where

$$R = \sum_{(\alpha,a)\in\bar{\mathscr{A}},(\beta,b)\in\bar{\mathscr{B}}} m_{\mathscr{A}}((\alpha,a)) m_{\mathscr{B}}((\beta,b)) q^{-1} \sum_{s\neq 0} \chi(s(\alpha\cdot\beta - a - b)).$$

If we view R as a sum in $(\alpha,a)\in\overline{\mathscr{A}}$, apply the Cauchy–Schwarz inequality, and dominate the sum in $(\alpha,a)\in\overline{\mathscr{A}}$ by the sum in $(\alpha,a)\in\mathbb{F}_q^{\ell+1}$, we have

$$\begin{aligned}
R^2 &\leq \sum_{(\alpha,a)\in\bar{\mathscr{A}}} m_{\mathscr{A}}((\alpha,a))^2 \sum_{(\alpha,a)\in\mathbb{F}_q^{\ell+1}} q^{-2} \sum_{s,s'\neq 0} \sum_{(\beta,b),(\beta',b')\in\bar{\mathscr{B}}} m_{\mathscr{B}}((\beta,b)) m_{\mathscr{B}}((\beta',b')) \\
&\quad \cdot \chi(s(\alpha\cdot\beta - a - b))\chi(s'(-\alpha\cdot\beta' + a + b')) \\
&= \sum_{(\alpha,a)\in\bar{\mathscr{A}}} m_{\mathscr{A}}((\alpha,a))^2 q^{-2} \sum_{\substack{(\alpha,a)\in\mathbb{F}_q^{\ell+1}\\ (\beta,b)\in\bar{\mathscr{B}}\\ (\beta',b')\in\bar{\mathscr{B}}\\ s,s'\neq 0}} m_{\mathscr{B}}((\beta,b)) m_{\mathscr{B}}((\beta',b'))\chi(\alpha\cdot(s\beta - s'\beta'))\chi(a(s'-s))\chi(s'b' - sb) \\
&= q^{\ell-1} \sum_{(\alpha,a)\in\bar{\mathscr{A}}} m_{\mathscr{A}}((\alpha,a))^2 \sum_{\substack{s\neq 0\\ (\beta,b)\in\bar{\mathscr{B}}\\ (\beta',b')\in\bar{\mathscr{B}}\\ \beta=\beta'}} m_{\mathscr{B}}((\beta,b)) m_{\mathscr{B}}((\beta',b'))\chi(s(b'-b)) = I + II,
\end{aligned}$$

where I is the sum over all pairs $(\beta,b),(\beta',b')$ with $b = b'$, and II is the sum over all pairs $(\beta,b),(\beta',b')$ with $b\neq b'$.

It is clear that if $b\neq b'$, then we have

$$\sum_{s\neq 0}\chi(s(b-b')) = -1,$$

which implies that $II < 0$.

On the other hand, it is easy to see that if $b = b'$, then

$$\sum_{s\neq 0}\chi(s(b-b')) = (q-1).$$

This give us

$$I \ll q^\ell \sum_{(\alpha,a)\in\bar{\mathscr{A}}} m_{\mathscr{A}}((\alpha,a))^2 \sum_{(\beta,b)\in\bar{\mathscr{B}}} m_{\mathscr{B}}((\beta,b))^2$$

In other words, we have proved that

$$R \ll q^{\frac{\ell}{2}} \left(\sum_{(\alpha,a)\in\bar{\mathscr{A}}} m_{\mathscr{A}}((\alpha,a))^2 \sum_{(\beta,b)\in\bar{\mathscr{B}}} m_{\mathscr{B}}((\beta,b))^2 \right)^{1/2}.$$

[1] This lemma was referred to as Lemma 8.1 in the early version of [8] but it was removed in the final version of [8]. Lemma 2.1 in [1] is a specific case of Lemma 11 when ℓ is even.

This completes the proof of the lemma. □

3. Proof of Theorem 5

In this section, we provide a proof of Theorem 5 and also for other dimensions.

Theorem 12. *Let $\{\lambda_m\}_{m\in\mathbb{F}_q^k}$ be the eigenvalues of $G_{Q,k}$.*

(1) *If $k = 4n$ for some $n \in \mathbb{N}$, and $q \equiv 3 \bmod 4$, then we have*

$$\lambda_m = q^k \cdot \begin{cases} q^{-1}\delta_0(m) - q^{-\frac{k}{2}} + q^{-\frac{(k+2)}{2}} & \text{if } m \in C_k \\ q^{-\frac{(k+2)}{2}} & \text{if } m \notin C_k. \end{cases}$$

(2) *If $k = 4n$ for some $n \in \mathbb{N}$ and $q \equiv 1 \bmod 4$, or $k = 4n+2$ for some $n \in \mathbb{N}$, then we have*

$$\lambda_m = q^k \cdot \begin{cases} q^{-1}\delta_0(m) + q^{-\frac{k}{2}} - q^{-\frac{(k+2)}{2}} & \text{if } m \in C_k \\ -q^{-\frac{(k+2)}{2}} & \text{if } m \notin C_k. \end{cases}$$

(3) *If $k \geq 3$ is odd, then we have*

$$\lambda_m = q^{k-1}\delta_0(m) + q^{-1}\eta(Q(m))\mathcal{G}_1^{k+1},$$

where $\mathcal{G}_1$ is the Gauss sum defined in (6)*, η is the quadratic character of $\mathbb{F}_q^*$, and we use the convention that $\eta(0) = 0$.*

As we observed in the introduction, when $k = 4n$ and $q \equiv 3 \bmod 4$, the unique positive and non-trivial eigenvalue of this graph is much smaller than the absolute value of others. This does not hold for other dimensions or $q \equiv 1 \bmod 4$.

Since $G_{Q,k}$ is a Cayley graph, it is well-known in the literature that its eigenvalues can be expressed in the form $q^k \cdot \widehat{C_k}(m)$. It is sufficient to prove the following lemma.

Lemma 13. *For any $m \in \mathbb{F}_q^k$, we have*

$$\widehat{C_k}(m) = q^{-1}\delta_0(m) + q^{-k-1}\eta(-1)\mathcal{G}_1^k \sum_{s\neq 0} \eta^k(s)\chi\left(\frac{Q(m)}{-4s}\right), \tag{8}$$

where $\delta_0(m) = 1$ if and only if $m = (0,\dots,0)$. In particular, we have the followings:

(1) *If $k = 4n$ for some $n \in \mathbb{N}$, and $q \equiv 3 \bmod 4$, then we have*

$$\widehat{C_k}(m) = \begin{cases} q^{-1}\delta_0(m) - q^{-\frac{k}{2}} + q^{-\frac{(k+2)}{2}} & \text{if } m \in C_k \\ q^{-\frac{(k+2)}{2}} & \text{if } m \notin C_k. \end{cases}$$

(2) *If $k = 4n$ for some $n \in \mathbb{N}$ and $q \equiv 1 \bmod 4$, or $k = 4n+2$ for some $n \in \mathbb{N}$, then we have*

$$\widehat{C_k}(m) = \begin{cases} q^{-1}\delta_0(m) + q^{-\frac{k}{2}} - q^{-\frac{(k+2)}{2}} & \text{if } m \in C_k \\ -q^{-\frac{(k+2)}{2}} & \text{if } m \notin C_k. \end{cases}$$

(3) *If $k \geq 3$ is odd, then we have*

$$\widehat{C_k}(m) = q^{-1}\delta_0(m) + q^{-k-1}\eta(Q(m))\mathcal{G}_1^{k+1},$$

where we use the convention that $\eta(0) = 0$.

We note that our proof of Lemma 13 is quite similar to that of [7, Proposition 2.4] with Q is defined by $Q(x) = -x_1 \cdot x_2 + x_3^2 + \cdots + x_k^2$.

Proof. By the definition and the orthogonality of χ, we have

$$\begin{aligned}\widehat{C_k}(m) &= q^{-k}\sum_{x\in C_k}\chi(-x\cdot m)\\ &= q^{-1}\delta_0(m)+q^{-k-1}\sum_{x\in\mathbb{F}_q^k}\sum_{s\neq 0}\chi\left(s(-x_1^2+x_2^2+\cdots+x_k^2)\right)\,\chi(-x\cdot m)\\ &= q^{-1}\delta_0(m)+q^{-k-1}\sum_{s\neq 0}\sum_{x_1\in\mathbb{F}_q}\chi(-sx_1^2-m_1x_1)\prod_{j=2}^{k}\sum_{x_j\in\mathbb{F}_q}\chi(sx_j^2-m_jx_j).\end{aligned}$$

By the complete square formula (7), we obtain (8) which states that

$$\widehat{C_k}(m)=q^{-1}\delta_0(m)+q^{-k-1}\eta(-1)\mathcal{G}_1^k\sum_{s\neq 0}\eta^k(s)\chi\left(\frac{Q(m)}{-4s}\right).$$

We now fall into three cases.

Case 1. Suppose that $k=4n$ for some $n\in\mathbb{N}$, and $q\equiv 3 \bmod 4$. Then $\eta^k\equiv 1$ and $\eta(-1)=-1$. One can use Lemma 10 to see that $\mathcal{G}_1^k=q^{k/2}$ for $k\equiv 0 \bmod 4$. So, $\eta(-1)\mathcal{G}_1^k=-q^{k/2}$. This implies

$$\widehat{C_k}(m)=q^{-1}\delta_0(m)-q^{-k-1}q^{k/2}\sum_{s\neq 0}\chi\left(\frac{Q(m)}{-4s}\right).$$

Thus, the first part of the lemma follows by the orthogonality of χ.

Case 2. Assume that $k=4n$ for some $n\in\mathbb{N}$ and $q\equiv 1 \bmod 4$, or $k=4n+2$ for some $n\in\mathbb{N}$. Using the same argument as in the previous case, it suffices to show that

$$\eta(-1)\mathcal{G}_1^k=q^{k/2}.$$

We first assume that $k\equiv 0 \bmod 4$ and $q\equiv 1 \bmod 4$, then -1 is a square number, i.e., $\eta(-1)=1$, and $\mathcal{G}_1^k=q^{k/2}$ by Lemma 10. Hence, we get $\eta(-1)\mathcal{G}_1^k=q^{\frac{k}{2}}$, as required.

If $k\equiv 2 \bmod 4$, then $k-2\equiv 0 \bmod 4$, so $\mathcal{G}_1^{k-2}=q^{(k-2)/2}$. One can use Lemma 10 again to obtain that $\mathcal{G}_1^2=\eta(-1)q$. Hence, $\mathcal{G}_1^k=\eta(-1)q\mathcal{G}_1^{k-2}=\eta(-1)q^{k/2}$. In other words, we have proved that $\eta(-1)\mathcal{G}_1^k=q^{k/2}$.

Case 3. Suppose that $k\geq 3$ is an odd integer. Since $\eta^k=\eta$, it follows

$$\widehat{C_k}(m)=q^{-1}\delta_0(m)+q^{-k-1}\eta(-1)\mathcal{G}_1^k\sum_{s\neq 0}\eta(s)\chi\left(\frac{Q(m)}{-4s}\right).$$

If $Q(m)=0$, then we are done by the orthogonality of η. On the other hand, if $Q(m)\neq 0$, then the above summation over $s\neq 0$ is the same as the quantity $\eta(-1)\eta(Q(m))\mathcal{G}_1$, which follows by a change of variables by letting $t=\frac{Q(m)}{-4s}$. This completes the proof of the third part. □

Since eigenvalues of $G_{Q,k}$ are $q^k\cdot\widehat{C_k}(m)$ with $m\in\mathbb{F}_q^k$, Theorem 12 follows directly from Lemma 13.

4. Proof of Theorem 7

Eigenvalues of $G_{\|\cdot\|,k}$ are of the form $q^k\cdot\widehat{S_0^{k-1}}(m)$. Thus, Theorem 7 follows directly from [5, Lemma 2.2]. For the reader convenience, we recall it here.

Lemma 14. *Assume* $k=4n+2$ *for some* $n\in\mathbb{N}$*, and* $q\equiv 3 \bmod 4$*, then we have*

$$\widehat{S_0^{k-1}}(m)=q^{-1}\delta_0(m)-q^{-\frac{k+2}{2}}\sum_{r\neq 0}\chi(r\|m\|).$$

This lemma was deduced from the following general statement, which can be found in [5, Lemma 2.3] or [4, Lemma 4].

Lemma 15. *For $m \in \mathbb{F}_q^k$, we have*

$$\widehat{S_0^{k-1}} = q^{-1}\delta_0(m) + q^{-k-1}\eta^k(-1)\mathcal{G}_1^k \sum_{r\neq 0} \eta^k(r)\chi\left(\frac{\|m\|}{4r}\right).$$

When $k = 4n+2$ and $q \equiv 1 \bmod 4$, or $k = 4n$, one can compute from Lemma 15 that

$$\lambda_m = q^k \cdot \begin{cases} q^{-1}\delta_0(m) + q^{-\frac{k}{2}} - q^{-\frac{k+2}{2}} & \text{if } \|m\| = 0 \\ -q^{-\frac{k+2}{2}} & \text{if } \|m\| \neq 0. \end{cases}$$

When k is odd, we have

$$\lambda_m = q^{k-1}\delta_0(m) + q^{-1}\eta(-\|m\|)\mathcal{G}_1^{k+1}.$$

5. Proofs of Theorems 4 and 6

To prove the incidence bounds, we make use of the following lemma, which can be easily proved by following the proof of the Expander mixing lemma [9, Theorem 2.11] and using the fact that the only positive non-trivial eigenvalue of $G_{Q,k}$ is $q^{\frac{k-2}{2}}$ when $k \equiv 0 \bmod 4$ and $q \equiv 3 \bmod 4$. The interested reader can also find a similar proof in [8, Lemma 2.6].

Lemma 16. *Suppose that $k \equiv 0 \bmod 4$ and $q \equiv 3 \bmod 4$. Let $Q(x) = -x_1^2 + \sum_{i=2}^k x_i^2$. Let W be a vertex set in $G_{Q,k}$ and $e(W,W)$ be the number of edges in W, then we have*

$$e(W,W) \leq \frac{|W|^2}{q} + q^{\frac{k-2}{2}}|W|.$$

We are ready to prove Theorem 4.

Proof of Theorem 4. Set $k = d+1$. We identify each point $p = (p_1,\ldots,p_d)$ in P with $(0,p) \in \mathbb{F}_q^k$ and each sphere s centered at $a \in \mathbb{F}_q^d$ of square radius r^2 with $(r,a) \in \mathbb{F}_q^d$. It is clear that there is an incidence between the point p and the sphere s if $(p_1-a_1)^2 + \cdots + (p_d-a_d)^2 = (r-0)^2$. This means that $(0,p)-(r,a) \in C_k$, i.e. an edge between $(0,p)$ and (r,a) in $G_{Q,k}$. Let P' and S' be the sets of corresponding points in $\mathbb{F}_q^k$. We have $I(P,S) = e(P',S')$. Set $W = P' \cup S'$. It is clear that $e(P',S') \leq e(W,W)$. Thus, the theorem follows from Lemma 16 and theorem's assumptions. □

Proof of Theorem 6. Set $k = d+1$. Notice that -1 is not a square since we have assumed that q is congruent to 3 mod 4. From the fact that the product of two non-squares is a square, we see that $-r$ is a squre number in $\mathbb{F}_q$ for any non-square r in $\mathbb{F}_q$. Hence, the argument is the same as what we did for Theorem 4, except that we use the graph $G_{\|\cdot\|,k}$ in place of $G_{Q,k}$. □

6. Proof of Theorem 8

To prove Theorem 8, we need to deal with two cases $d \equiv 3 \bmod 4$ and $d \equiv 1 \bmod 4$. However, the proofs for these two situations are almost identical, so we only present an argument for $d \equiv 3 \bmod 4$. In particular, we will show that

Theorem 17. *Let A be a set in $\mathbb{F}_q$ with $q \equiv 3 \bmod 4$ and $|A| \gg q^{1/2}$. For $d \equiv 3 \bmod 4$, we have at least one of two following statements:*

(1) $|A+A| \geq \min\left\{q^{\frac{d+1}{2d}}, |A|^{\frac{d+1}{d}}\right\}$.

(2) $|dA^2| \gg \frac{|A|^d}{q^{\frac{d-1}{2}}}$.

For a triple $(x, y, z) \in A \times A \times A$, we say that (x, y, z) is a *square triple* if $x^2 + y^2 + z^2$ is a square, otherwise, we say it is a *non-square triple*.

For $A \subset \mathbb{F}_q$, define $A^2 := \{x^2 \colon x \in A\}$. A tuple $(x_1, \dots, x_d) \in A^d$ is called *square-sum-type* if $x_1^2 + \cdots + x_d^2$ is a square in $\mathbb{F}_q$. The next lemma shows that a constant proportion of d-tuples in A^d is of square-sum-type.

Lemma 18. *Any set $A \subset \mathbb{F}_q$ with $|A| \gg q^{1/2}$ has at least $\gg |A|^d$ square-sum-type tuples.*

Proof. Let $SQ(\mathbb{F}_q)$ be the set of non-zero square elements in $\mathbb{F}_q$, and B be the multi-set defined by $B := \{x_1^2 + x_2^2 + \cdots + x_{d-1}^2 \colon x_i \in A\}$. We write $\overline{B}$ for the set of distinct elements in B and $\sum_{b \in \bar{B}} m(b)^2$, where $m(b)$ is the multiplicity of b, is the number of tuples

$$(x_1, \dots, x_{d-1}, y_1, \dots, y_{d-1}) \in A^{2(d-1)}$$

such that $x_1^2 + \cdots + x_{d-1}^2 = y_1^2 + \cdots + y_{d-1}^2$. We denote the number of these tuples by $E(B)$. One can check that $E(B) \ll |A|^{2d-3}$. We now consider the following equation

$$xy = a + b, \tag{9}$$

where $x, y \in SQ(\mathbb{F}_q), a \in A^2, b \in B$. Let M be the number of solutions of this equation. Since $|SQ(\mathbb{F}_q)| = \frac{q-1}{2}$, it follows from Lemma 11 that

$$\left| M - \frac{|A^2||B|(q-1)^2}{4q} \right| \leq q^{1/2} \left(\frac{(q-1)E(B)}{2} \right)^{1/2} \left(\frac{(q-1)|A^2|}{2} \right)^{1/2}.$$

Thus, $M \gg \frac{|A|^d (q-1)^2}{q}$ if $E(B) \ll \frac{|A|^{2d-1}}{q}$, which can be satisfied under the condition $|A| \gg q^{1/2}$, since $E(B) \ll |A|^{2d-3}$.

Observe that for $a \in A^2$ and $b \in B$, if $a + b$ is a square, then it contributes $(q-1)/2$ solutions to the equation (9). Hence, the number of square-sum-type tuples $(a_1, \dots, a_d) \in A^d$ is at least $\frac{2M}{q-1}$. This completes the proof of the lemma. □

We are now ready to prove Theorem 17

Proof of Theorem 17. If $|A + A| \geq |A|^{(d+1)/d}$ or $|A + A| \geq q^{\frac{d+1}{2d}}$, then we are done. Without loss of generality, we assume that $|A + A| < |A|^{\frac{d+1}{d}}$ and $|A + A| < q^{\frac{d+1}{2d}}$.

We consider the following equation

$$(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_d - y_d)^2 = t, \tag{10}$$

where $x_1, x_2, \dots, x_d \in A + A, y_1, y_2, \dots, y_d \in A, t \in dA^2 \cap SQ(\mathbb{F}_q) = (A^2 + \cdots + A^2) \cap SQ(\mathbb{F}_q)$.

Let M be the number of solutions of this equation.

By Lemma 18, the number of square-sum-type tuples in A^d is at least $\gg |A|^d$. For each of those tuples, denoted by $(a_1, \dots, a_d)$, it will contribute $\gg |A|^d$ solutions to the number of solutions of the equation (10). Indeed, tuples with $(x_1, \dots, x_d, y_1, \dots, y_d) = (y_1 + a_1, \dots, y_d + a_d, y_1, \dots, y_d)$ with $y_i \in A$ satisfy the equation (10). Therefore, $M \gg |A|^{2d}$.

Define $P := (A + A) \times (A + A) \times \cdots \times (A + A) \subset \mathbb{F}_q^d$ and S be the set of spheres centered at points in A^d of square radii in dA^2. We have $|P| = |A + A|^d$ and $|S| = |A|^d |dA^2|$.

To apply Theorem 4 effectively, one has to have the condition $|P| \sim |S|$. To this end, we partition the radius set into m subsets of size $\frac{|A+A|^d}{|A|^d}$, where $m = \frac{|dA^2||A|^d}{|A+A|^d} > 1$ since otherwise $|A + A| \geq |A|^{(d+1)/d}$. We denote those radius sets by $R_1, \dots, R_m$. For $1 \leq i \leq m$, let S_i be the set of spheres centered at points in A^d of square radii in R_i. Notice that, for each i, S_i can be an empty set if there is no square element in R_i, but what we only need is an upper bound of S_i which is $|A + A|^d$.

One can check that M is bounded by $\sum_{i=1}^{m} I(P,S_i)$. For each i, applying Theorem 4 gives us

$$I(P,S_i) \le \frac{|A+A|^{2d}}{q} + q^{\frac{d-1}{2}}|A+A|^d \ll q^{\frac{d-1}{2}}|A+A|^d,$$

since $|A+A| \le q^{\frac{d+1}{2d}}$. Taking the sum over all i, we achieve

$$M = \sum_{i=1}^{m} I(P,S_i) \le q^{\frac{d-1}{2}}|A+A|^d \cdot \frac{|dA^2||A|^d}{|A+A|^d} = q^{\frac{d-1}{2}}|dA^2||A|^d.$$

Using the fact that $M \gg |A|^{2d}$ leads to

$$|dA^2| \gg \frac{|A|^d}{q^{\frac{d-1}{2}}}.$$

This completes the proof of the theorem. □

7. Open questions

Theorems 4 and 6 give some answers for Question 2, but we do not know whether or not Theorem 1 can be improved for the following cases:

(1) (square radii): $d \equiv 3 \bmod 4$ and $q \equiv 1 \bmod 4$.
(2) (square radii): $d \equiv 1 \bmod 4$.
(3) (square radii): $d \equiv 2 \bmod 4$ and $q \equiv 1 \bmod 4$.

(4) (non-square radii): $d \equiv 1 \bmod 4$ and $q \equiv 1 \bmod 4$.
(5) (non-square radii): $d \equiv 3 \bmod 4$.
(6) (non-square radii): d is even.

We hope to address these cases in a subsequent paper.

Acknowledgements

We thank the referee for many valuable comments and suggestions. Thang Pham would like to thank Vietnam Institute for Advanced Study in Mathematics (VIASM) for the hospitality and for the excellent working condition.

References

[1] D. N. V. Anh, L. Q. Ham, D. Koh, T. Pham, L. A. Vinh, “On a theorem of Hegyvári and Hennecart”, *Pac. J. Math.* **305** (2020), no. 2, p. 407-421.

[2] J. Cilleruelo, A. Iosevich, B. Lund, O. Roche-Newton, M. Rudnev, “Elementary methods for incidence problems in finite fields”, *Acta Arith.* **177** (2017), no. 2, p. 133-142.

[3] 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. Am. Math. Soc.* **363** (2011), no. 6, p. 3255-3275.

[4] A. Iosevich, D. Koh, “Extension theorems for spheres in the finite field setting”, *Forum Math.* **22** (2010), no. 2, p. 457-483.

[5] A. Iosevich, D. Koh, S. Lee, T. Pham, C.-Y. Shen, “On restriction estimates for the zero radius sphere over finite fields”, *Can. J. Math.* **73** (2021), no. 3, p. 769-786.

[6] A. Iosevich, M. Rudnev, “Erdős distance problem in vector spaces over finite fields”, *Trans. Am. Math. Soc.* **359** (2007), no. 12, p. 6127-6142.

[7] D. Koh, S. Lee, T. Pham, “On the finite field cone restriction conjecture in four dimensions and applications in incidence geometry”, accepted in *Int. Math. Res. Not.*, 2021.

[8] D. Koh, T. Pham, L. A. Vinh, “Extension theorems and a connection to the Erdős-Falconer distance problem over finite fields”, *J. Funct. Anal.* **281** (2021), no. 8, article no. 109137 (54 pages).

[9] M. Krivelevich, B. Sudakov, "Pseudo-random graphs", in *More sets, graphs and numbers*, Bolyai Society Mathematical Studies, vol. 15, Springer, 2006, p. 199-262.

[10] R. Lidl, H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, 1996.

[11] A. Mohammadi, S. Stevens, "Attaining the exponent 5/4 for the sum-product problem in finite fields", https://arxiv.org/abs/2103.08252, 2021.

[12] D. H. Pham, "A note on sum-product estimates over finite valuation rings", *Acta Arith.* **198** (2021), no. 2, p. 187-194.

[13] N. D. Phuong, P. Thang, L. A. Vinh, "Incidences between points and generalized spheres over finite fields and related problems", *Forum Math.* **29** (2017), no. 2, p. 449-456.

[14] M. Rudnev, I. D. Shkredov, S. Stevens, "On the energy variant of the sum-product conjecture", *Rev. Mat. Iberoam.* **36** (2019), no. 1, p. 207-232.