Right angles in vector spaces

Thang Pham Nguyen Minh Sang Gábor Tardos

Abstract

Bennett (2015) proved that, for \( A \subseteq \mathbb{F}^d_q \), if \(|A| \geq 2q^{d+2}/3\) then \( A \) contains a right angle. The main purpose of this paper is to improve this result by using methods from spectral graph theory and combinatorial arguments. We also prove that if \( q^{d+1}/2 = o(|A|) \) then the number of right angles in \( A \) is \((1 - o(1))|A|^3/q\), and in general the exponent \( d+1/2 \) is sharp.

1 Introduction

In 1946, Paul Erdős [13] made the first investigation of the distribution of the \( \binom{n}{2} \) distances determined by a set of points in the plane \( \mathbb{R}^2 \). More precisely, he asked for the maximal number \( f(n) \) of unit distances among \( n \) points in the plane. For large \( n \), he proved that

\[
ne^{-\log \log n} < f(n) < n^{3/2}.
\]

The lower bound has not been improved since 1946, and it is conjectured to be asymptotically tight. The upper bound was improved to \( O(n^{4/3}) \), see [7, 19] for more details.

In 1990, Pach and Sharir [20] studied a similar problem concerning the distribution of the \( 3\binom{n}{3} \) angles determined by a triple of an \( n \)-element point set in the plane \( \mathbb{R}^2 \). They, using an ingenious counting argument, proved that, for any given angle \( 0 < \alpha < \pi \), there exists a constant \( c > 0 \) such that the number of ordered triples of \( n \) points in the plane, which determine the same angle \( \alpha \), is at most \( cn^2 \log n \). Furthermore, apart from the value of \( c \), this bound is best possible for infinitely many \( \alpha \).

Let \( \mathbb{F}_q \) be a finite field of \( q \) elements where \( q \) is a prime power. The remarkable results of Bourgain, Katz, and Tao [8] on sum-product estimate and its applications on Erdős distinct distances problem and the Szemerédi-Trotter theorem over finite fields have stimulated a lot of research of finite field analogues of classical discrete geometry problems in recent years, see for example [10, 11, 12, 16, 17, 18, 21, 22], and references therein.

In vector spaces over finite fields, we say that an ordered triple of distinct points \((x, y, z) \in \mathbb{F}^d_q \times \mathbb{F}^d_q \times \mathbb{F}^d_q\) forms a right angle if the vectors \( x - y \) and \( z - y \) have dot product 0. For any set \( A \subseteq \mathbb{F}^d_q \), we denote the set of right angles determined by \( A \) by \( Ra(A) \). Recently, Bennett [9] studied the following question in vector spaces over finite fields: How large does a set \( A \subseteq \mathbb{F}^d_q \) need to be such that there are three distinct points in \( A \) which form a right angle? He proved that, for any set \( A \subseteq \mathbb{F}^d_q \), if \( A \) is sufficiently large, then \( |Ra(A)| > 0 \). Formally, the statement is as follows.

**Theorem 1.1 (Bennett [9]).** Let \( A \) be a set in \( \mathbb{F}^d_q \). If \(|A| \geq 2q^{d+2}/3\), then we have \(|Ra(A)| > 0\).
The main purpose of this paper is to improve Theorem 1.1 by using methods from spectral graph theory and combinatorial arguments. In our first result, we prove that

**Theorem 1.2.** Let $A$ be a set in $\mathbb{F}_q^d$,

(i) if $d = 3k - 1$ with $k \geq 1$, and $|A| \geq 2^9d^2q^{d+1}\log q$, then $|Ra(A)| > 0$.

(ii) if $d = 3k$ or $d = 3k + 1$ with $k \geq 1$, and $|A| \geq cq^{d+1} + \frac{k}{d-1}(\log q)^{\frac{k}{d-1}}$ for some positive constant $c = c(k)$, then $|Ra(A)| > 0$.

For a given triple of distinct points $(a, b, c)$ in $A^3$, the probability of $(a - b) \cdot (c - b) = 0$ is approximately $1/q$, so we expect that the number of right angles determined by $A$ is approximately $|A|^3/q$. In the following result, we show that if $|A| = \Omega(q^{d/2})$ with $d$ even, then the number of right angles determined by $A$ is not much smaller than the expected value.

**Theorem 1.3.** Let $A$ be a set in $\mathbb{F}_q^d$ with $d$ even,

(i) if $|A| \geq 3q^{d/2}$, then there exists a positive constant $c$ such that $|Ra(A)| \geq \frac{c|A|^3}{q}$.

(ii) if $q^{d/2} = o(|A|)$, then we have $|Ra(A)| \geq (1 - o(1))\frac{|A|^3}{q}$.

Here and throughout, $x = o(y)$ means that for fixed $d$, $x$ and $y$ are functions of the parameter $q$, and $x/y \to 0$ as $q \to \infty$.

Theorem 1.3 implies that if $A$ is a set in $\mathbb{F}_q^3$ of cardinality at least $3q$, then $A$ contains at least one right angle. This bound is sharp up to a constant factor, since there exists a trivial construction with $q$ points on a line containing no right angle. However, in higher dimensions, we do not have any non-trivial construction of $q^{1+\epsilon}$ points containing no right angle with $\epsilon > 0$. If $q \equiv 3 \mod 4$, then we obtain the following set of $d(q-1)/2$ points in $\mathbb{F}_q^d$ that contains no right angle:

$$A = \bigcup_{i=1}^{d} \{x^2e_i : x \in \mathbb{F}_q \setminus \{0\}\},$$

where $e_i$ is the $i$-th unit vector. With this example, we are led to the following conjecture.

**Conjecture 1.4.** Let $A$ be a set in $\mathbb{F}_q^d$. There exists a constant $c = c(d)$ such that $A$ contains a right angle when $|A| \geq cq$.

While Theorem 1.3 only tells us a lower bound on the number of right angles determined by points in $A$, in the following result we give an upper bound of $|Ra(A)|$ when $A$ is large enough.

**Theorem 1.5.** Let $A$ be a set in $\mathbb{F}_q^d$. If $q^{d+1} = o(|A|)$, then we have

$$|Ra(A)| = (1 - o(1))\frac{|A|^3}{q}.$$
angle in $\mathbb{F}_q^{2k} \times \{0\}$. For each of these triples, if we take $\mathbf{a}' = (a, \lambda)$, $\mathbf{b}' = (b, \lambda)$, $\mathbf{c}' = (c, \lambda)$, for some $\lambda \neq 0$, then $(\mathbf{a}', \mathbf{b}', \mathbf{c}')$ also forms a right angle in $A$. This implies that the number of right angles in $A$ is at least $\Theta \left( \frac{q^d}{q^{1/2}} \right)$.

This rest of this paper is organized as follows. In Section 2, we recall the expander mixing lemma for pseudo-random graphs, and some properties of some certain graphs over finite fields which will be used in the proofs of Theorem 1.2 and Theorem 1.5. A proof of Theorems 1.2 is given in Sections 3. Proofs of Theorem 1.3 and Theorem 1.5 are given in Section 4 and Section 5, respectively.

2 Tools from spectral graph theory

For a graph $G$, let $\gamma_1 \geq \gamma_2 \geq \ldots \geq \gamma_n$ be the eigenvalues of its adjacency matrix. The second largest eigenvalue of $G$ is defined as $\gamma(G) := \max\{\gamma_2, -\gamma_n\}$. A graph $G = (V, E)$ is called an $(n, d, \gamma)$-graph if $G$ is a $d$-regular graph with $n$ vertices, and $\gamma(G) \leq \gamma$. For any two vertex sets $U$ and $W$, we have the following estimate on the number of edges between $U$ and $W$ in $G$.

$$\left| e(U, W) - \frac{d|U||W|}{n} \right| \leq \gamma \sqrt{|U||W|}.$$ (1)

The interested reader can find an easy proof of (1) in [1, Corollary 9.2.5].

In the proof of Theorem 1.2, we will make use of the sum-product graph which is constructed as follows.

**Sum-product graph over finite fields:** Let $B(\cdot, \cdot)$ be a non-degenerate bilinear form on $\mathbb{F}_q^d$. The sum-product graph $SP(\mathbb{F}_q^{d+1})$ is defined as follows. The vertex set is the set $\mathbb{F}_q^{d+1}$, and there is an edge between two vertices $(a, b), (c, d) \in \mathbb{F}_q^d \times \mathbb{F}_q$ if $B(a, c) + b + d = 0$.

It is clear that the graph $SP(\mathbb{F}_q^{d+1})$ is a $q^d$-graph of order $q^{d+1}$. By elementary calculations, Vinh [23] proved the following lemma.

**Lemma 2.1 ([23]).** For any prime power $q$ and $d \geq 1$, the second largest eigenvalue of the sum-product graph $SP(\mathbb{F}_q^{d+1})$ is bounded from above by $\sqrt{2q^d}$.

In the proof of Theorem 1.5, we will make use of the Erdős-Rényi graph which is constructed as follows.

**Erdős-Rényi graph over finite fields:** Let $PG(q, d)$ denote the projective space of dimension $d-1$ over the finite field $\mathbb{F}_q$. The vertices of $PG(q, d)$ correspond to the equivalence classes of the set of all non-zero vectors $\mathbf{x} = (x_1, \ldots, x_d)$ over $\mathbb{F}_q$, where two vectors $\mathbf{x}$ and $\mathbf{y}$ are equivalence if $\mathbf{x} = \lambda \mathbf{y}$ for some $\lambda \in \mathbb{F}_q \setminus \{0\}$. Let $ER(\mathbb{F}_q^d)$ denote the graph whose vertices are the points of $PG(q, d)$ and two vertices $[x]$ and $[y]$ are adjacent if and only if $x_1y_1 + \cdots + x_dy_d = 0$. Note that this graph has loops and if a vertex has a loop, loops contribute 1 to the degree. It is easy to check that $ER(\mathbb{F}_q^d)$ is a graph of order $\frac{q^d-1}{q-1}$, and the degree of each vertex is $\frac{q^{d-2} - 1}{q-1}$. In [2], Alon and Krivelevich gaved the following theorem on the second largest eigenvalue of $ER(\mathbb{F}_q^d)$. 


Theorem 2.2. For any prime power $q$ and $d \geq 2$, the second largest eigenvalue of the Erdős-Rényi graph $\mathcal{E}R(\mathbb{F}_q^d)$ is bounded from above by $q^{(d-2)/2}$.

3 Proof of Theorem 1.2

In this section, we prove Theorem 1.2 in a more general statement as follows.

Theorem 3.1. Let $B(\cdot, \cdot)$ be a non-degenerate bilinear form on $\mathbb{F}_q^d$, and $A$ be a set in $\mathbb{F}_q^d$.

(i) if $d = 3k - 1$ with $k \geq 1$, and $|A| \geq 2^d q^{d+1} \log q$, then there exist three distinct points $a, b, c$ in $A$ satisfying

$$B(a - b, c - b) = 0.$$ 

(ii) if $d = 3k$ or $d = 3k + 1$ with $k \geq 1$, and $|A| \geq cq^{d+1} + k \log q^{\frac{k}{d-1}}$ for some positive constant $c = c(k)$, then there exist three distinct points $a, b, c$ in $A$ satisfying

$$B(a - b, c - b) = 0.$$ 

In order to prove Theorem 3.1, we make use of the following lemmas.

Definition 3.2. For any integer $h \geq 1$, a $h$-flat is a translate of a subspace of dimension $h$ in $\mathbb{F}_q^d$.

Lemma 3.3 (Theorem 2.3, [11]). Let $P$ be a set of points, $H$ be a set of $h$-flats in $\mathbb{F}_q^d$. Then the number of incidences between points and $h$-flats, $I(P, H)$, satisfies

$$
\left| I(P, H) - \frac{|P||H|}{q^{d-h}} \right| \leq 2q^{(d-h)h/2} \sqrt{|P||H|}.
$$

Lemma 3.4. Let $P$ be a set of points in $\mathbb{F}_q^d$, $H$ a set of $h$-flats in $\mathbb{F}_q^d$ containing at least $k$ points from $P$. If $k \geq 2|P|/q^{d-h}$, we have

$$|H_k| \leq \frac{16q^{(d-h)h}|P|}{k^2}.$$ 

Proof. It follows from Lemma 3.3 that

$$I(P, H_k) \leq \frac{|P||H_k|}{q^{d-h}} + 2q^{(d-h)h/2} \sqrt{|P||H_k|}.$$ 

On the other hand, we have $I(P, H_k) \geq k|H_k|$. Thus

$$k|H_k| \leq \frac{|P||H_k|}{q^{d-h}} + 2q^{(d-h)h/2} \sqrt{|P||H_k|}$$

which implies that

$$|H_k| \leq \frac{4q^{(d-h)h}|P|}{(k - \frac{|P|}{q^{d-h}})^2} \leq \frac{16q^{(d-h)h}|P|}{k^2},$$

since $k \geq 2|P|/q^{d-h}$, and the lemma follows. 

Our next lemma can be proved by elementary calculations.
Lemma 3.5. For any fixed line \( l \) in \( \mathbb{F}_q^d \). The number of \( h \)-flats with \( h > 1 \) in \( \mathbb{F}_q^d \) containing \( l \) is at least \( q^{(d-h)(h-1)} \).

Let \( \mathcal{A} \) be a set in \( \mathbb{F}_q^d \). For three distinct points \( a, b, c \) in \( \mathcal{A} \), we observe that if these points satisfy \( B(a - b, c - b) = 0 \), i.e. \( (a, b, c) \) forms a right angle at \( b \), then there is an incidence between \( c \) and the flat defined by the following equation:

\[
B(a - b, x) - B(a - b, b) = 0. \tag{2}
\]

On the other hand, we note that for two pairs of points \((a, b)\) and \((c, e)\) in \( \mathcal{A}^2 \) if

\[
(a - b, -B(a - b, b)) = \lambda \cdot (c - e, -B(c - e, e)),
\]

for some \( \lambda \in \mathbb{F}_q \setminus \{0\} \), then the corresponding flats are the same.

For any pair of distinct points \((a, b)\) \(\in\) \( \mathcal{A}^2 \), we define

\[
p_{a,b} := (a_1 - b_1, \ldots, a_d - b_d, -B(a - b, b)) \in \mathbb{F}_q^{d+1},
\]

and \([p_{a,b}]\) is its congruence class in the projective space \( PG(q, d+1) \). Let \( U \) be the set of points \( p_{a,b} \), with \((a, b) \in \mathcal{A}^2, a \neq b \), such that there are no two points with the same congruence class.

One can easily see that an incidence between a point \( c \in \mathcal{A} \) and a flat defined by the equation \((2)\) can also be viewed as an edge between the vertex \( \mathcal{A} \times \{0\} \) and the vertex \( p_{a,b} \) in the sum-product graph \( \mathcal{S}\mathcal{P}(\mathbb{F}_q^{d+1}) \).

For two points \( a \) and \( b \) in \( \mathbb{F}_q^d \), we say that \( a \) and \( b \) are \( B \)-orthogonal if \( B(x, y) = 0 \). For \( a \neq b \), let \( l_{a,b} \) be the line passing through \( a \) and \( b \). One can check that the flat defined by the equation \((2)\) goes through \( b \) and is \( B \)-orthogonal to the line \( l_{a,b} \).

For three distinct points \((x, a, b)\) \(\in\) \( \mathcal{A}^3 \), if there is an edge between \( x \times \{0\} \) and \( p_{a,b} \) \(\in\) \( U \) in the the graph \( \mathcal{S}\mathcal{P}(\mathbb{F}_q^{d+1}) \), then we have a right angle formed by the triple \((x, a, b)\) at \( b \). Furthermore, there is always an edge between \( x \times \{0\} \) and \( p_{a,a} \) in \( \mathcal{S}\mathcal{P}(\mathbb{F}_q^{d+1}) \), and note that when \( B(a - b, a - b) = 0 \), we also have an edge between \( a \times \{0\} \) and \( p_{a,b} \) in \( \mathcal{S}\mathcal{P}(\mathbb{F}_q^{d+1}) \).

Thus if we are able to prove that there are at least \( 2|\mathcal{A}|^2 + 1 \) edges between \( \mathcal{A} \times \{0\} \) and \( U \) in the graph \( \mathcal{S}\mathcal{P}(\mathbb{F}_q^{d+1}) \), then we conclude that there is a right angle determined by points in \( \mathcal{A} \).

If \( \mathcal{A} \) contains no right angle, one can check that \([p_{a,b}] = [p_{c,e}]\) if \( c \) lies on the line \( l_{a,b} \) and \( b = e \). Hence, in this case, the cardinality of \( U \) depends on the number of rich lines determined by \( \mathcal{A} \). In the rest of this section, our main focus is on estimates on the size of \( U \).

Bennett [9] used the fact that any line in \( \mathbb{F}_q^d \) contains \( q \) points to get the threshold \( q^{d/2} \) on the size of \( \mathcal{A} \) in Theorem 1.1. In this paper, our main idea is to prove that either there is a lower dimensional subspace with many points or the number of rich lines determined by \( \mathcal{A} \) is not many. From this fact, we are able to improve the threshold \( q^{d/2} \) to \( q^{d/1} \) for the case \( d = 3k - 1 \) and to \( q^{d/1 + \frac{k}{2}(\log q)^{\frac{1}{k-1}}} \) for other cases.

Proof of Theorem 3.1: We now start proving Theorem 3.1 (i), i.e. the case \( d = 3k - 1 \). Suppose that \( \mathcal{A} \) contains no right angle and \( |\mathcal{A}| \geq \max \{32q^{(k+1)/2}, 2^9dq^{d-k} \log q\} \), we show that this leads to a contradiction.
Let $h = 2k - 1$, it follows from Lemma 3.5 that each line $l$ is contained in at least $q^{(d-h)(h-1)}$ $h$-flats in $\mathbb{F}_q^d$. We first prove that the number of pairs of distinct points $(a, b) \in A \times A$ satisfying $|a, b| \geq \frac{|2|A|}{q^h}$ is at most $|A|^2/4$.

$$
\sum_{l \subseteq \mathbb{F}_q^d} \binom{|l \cap A|}{2} \leq \frac{1}{q^{(d-h)(h-1)}} \sum_{H \subseteq \mathbb{F}_q^d} \binom{|H \cap A|}{2} \leq \frac{1}{q^{(d-h)(h-1)}} \sum_{j=1}^{2^{j-1} |A|} \binom{2^j |A|}{2} \leq 16q^{(d-h)} |A| \sum_{j=1}^{2^j |A|} \binom{2^j+1 |A|}{q^{d-h}} \leq 2^6 d |A| q^{d-h} \log q.
$$

Since $|A| \geq 2^h d q^{d-h} \log q$, the number of pairs of points on lines passing through at least $2|A|/q^{d-h}$ points is at most $|A|^2/4$.

As we observed before when $[pa,b] = [p, c, e]$, we have $c$ lies on the line $l_{a,b}$ and $b = e$. Thus there is a subset $W \subseteq U$ of $|A|q^{d-h}/8$ points.

Let $V := A \times \{0\} \subseteq \mathbb{F}_q^{d+1}$, we now show that the number of edges between $V$ and $W$ in the sum-product graph $SP(\mathbb{F}_q^{d+1})$ is at least $\frac{|W||A|}{2q}$ under the condition $|A| \geq 32q^{(h+1)/2}$.

Indeed, let $W^* := \{ \lambda \cdot p_{a,b} : \lambda \in \mathbb{F}_q \setminus \{0\}, p_{a,b} \in W \} \subseteq \mathbb{F}_q^{d+1}$. Since all points in $U$ have distinct congruence classes, we have $|W^*| = (q-1)|W|$. On the other hand, an edge between a vertex in $V$ and a vertex in $W$ in the sum-product graph $SP(\mathbb{F}_q^{d+1})$ corresponds to $q-1$ distinct edges between $V$ and $W^*$ in $SP(\mathbb{F}_q^{d+1})$.

It follows from (II) and Theorem 2.1 that $e(V, W')$ is bounded from below by

$$
e(V, W') \geq \frac{|W'||V|}{q} - \sqrt{2} q^{d/2} \sqrt{|W'||V|}.
$$

This implies that

$$
e(V, W) \geq \frac{(q-1)||W||V|}{(q-1)q} - \sqrt{2} q^{d/2} \sqrt{(q-1)||W||V|} \geq \frac{|W||V|}{q} - \sqrt{2} q^{d/2} \sqrt{|W||V|} \geq \frac{|W||A|}{2q},
$$

under the condition $|A| \geq 32q^{(h+1)/2}$.

Moreover, $e(V, W) \leq 2|W|$ since we assumed that $A$ contains no right angle, and an edge between $p_{a,b} \in W$ and $c \in V$ means that $c = a$ or $c = b$. It follows that

$$2|W| \geq \frac{|W||A|}{2q},
$$
which leads to a contradiction as $|A| \geq 32q^{(h+1)/2}$ and $h \geq 1$. Thus the first case of Theorem 3.1 follows.

We now prove the second case of Theorem 3.1, i.e. $d = 3k$ or $d = 3k + 1$. Note that in the proof of Theorem 3.1 (ii) we will apply the result from the first case for a flat. Therefore we need to check whether Theorem 3.3 and arguments in the proof of Theorem 3.1 (i) also work for the case of flats.

In fact, in Theorem 3.3 if $P$ and $H$ are sets in a $d'$-flat, with $h < d' \leq d$, then one can find a transformation that maps $P$ to a set of points in $\mathbb{F}_q^{d'}$ and $H$ to a set of $h$-flats in $\mathbb{F}_q^{d'}$ such that it preserves incidences between points and flats. Thus Theorem 3.3 is also true for sets in a flat in $\mathbb{F}_q^d$. Moreover, our arguments in the proof of Theorem 3.1 (i) also works nicely for the case when $A$ is a set in a $d'$-flat in $\mathbb{F}_q^{d'}$, so when $A$ is a set in a $d'$-flat, we can view $A$ as a set in $\mathbb{F}_q^d$, and then apply Theorem 3.1 (i).

Let $n = \left(\frac{3k+7}{3k-1} q^k \log q\right)^{1/(3k-1)}$. Suppose that $|A| = m \geq 4q^{d+1}n^{1/3}$ and $A$ contains no right angle, we now prove that it also leads to a contradiction.

We say that a point $a \in A$ is rich if $|\{l_{a,b} : b \in A\}| \geq m/4n$. If $a \in A$ is rich then we replace $A$ by $A - \{a\}$. For the sake of simplicity, we will use the notation $A$ for the remaining set, and there is no problem with our arguments below. We repeat this process for the remaining set until either there is no more such $a$ or the cardinality of the remaining set is $m/2$. After this process, we now consider two cases:

**Case 1.** If the cardinality of $A$ is $m/2$, then we have removed $m/2$ points from $A$, and $|\{(a, l_{a,b}) : a, b \in A\}| \geq m^2/8n$. Since $A$ contains no right angle, by using the same arguments as above, there exists a subset $W$ of $U$ of $m^2/8n$ distinct points $[a,b]$, with $a \neq b \in A$. Thus, it follows from (1) and Theorem 2.2 that $e(U, V) > |U|$ when $m \geq 4q^{(d+1)/3}n^{1/3}$. This implies that $A$ contains a right angle, which leads to a contradiction.

**Case 2.** There is no rich point $a \in A$, and $|A| \geq m/2$. Then, for each point $a \in A$, the number of lines containing $a$ is smaller than $m/4n$, which implies that the number of points $b \in A$ such that $|l_{a,b} \cap A| \leq n - 1$ is at most $m/4$. Thus, for any point $a \in A$, the number of points $b \in A$ such that $|l_{a,b} \cap A| \geq n$ is at least $m/4$. Let $l$ be a line in $\mathbb{F}_q^d$ such that $l \cap A$ contains $n$ distinct points $\{x_1, \ldots, x_n\}$. We define

$$s_i = |\{a \in A \setminus l : |l_{a,x_i} \cap A| \geq n\}|, \ 1 \leq i \leq n.$$  

Then $s_i \geq m/4$ for all $1 \leq i \leq n$, and $\sum_{i=1}^n s_i \geq nm/4$. On the other hand, we have

$$\sum_{i=1}^n s_i = \sum_{a \in A \setminus l} T_a,$$

where $T_a$ is the number of points $x_i$ such that $|l_{a,x_i} \cap A| \geq n$. By the pigeonhole principle, there exists a point $a \in A \setminus l$ such that

$$T_a \geq \frac{nm}{m/2 - n} \geq \frac{n}{2}.$$  

Let $F^2$ be the two dimensional flat spanned by $l$ and $a$. Then we have $|F^2 \cap A| \geq n^2/2 - n/2$. After repeating the above arguments $3k - 2$ times, we obtain a flat of dimension $3k - 1$, which is denoted by $F^{3k-1}$, satisfying $|F^{3k-1} \cap A| \geq \frac{n^{3k-1}}{2^{3k-2}} - \frac{n^{3k-2}}{2^{3k-2}}$. Note that we can repeat
the above process $3k-2$ times because otherwise $A$ will be a set in a lower dimensional flat, and we can apply directly Theorem 3.1(i).

To complete the proof, we now apply Theorem 3.1 (i) for the flat $F^{3k-1}$. Indeed, since $A$ contains no right angle, it follows from Theorem 3.1 (i) that $|F^{3k-1} \cap A| < 2^q (3k-1) q^k \log q$. This implies that
\[ n < \left( \frac{3k+7}{2^{3k-1}} (3k-1) q^k \log q \right)^{1/(3k-1)}, \]
which leads to a contradiction.

Putting case 1 and case 2 together gives us that $A$ contains at least a right angle under the condition $|A| \geq 4q^{d-k} n^{1/3}$. This completes the proof of the theorem. \(\Box\)

\section{Proof of Theorem 1.3}

Let $d$ be an even integer, $U$ and $V$ be $d/2$-dimensional subspaces in $\mathbb{F}_q^d$. We say that $(U, V)$ forms a direction in $\mathbb{F}_q^d$ if and only if $U$ and $V$ are orthogonal, and $U \cap V = \{0\}$. Let $(U, V)$ be a direction. We say that a right angle $(u, p, v)$ at $p$ is in the direction $(U, V)$ if $u - p \in U$ and $v - p \in V$. We note here that a right angle can be occurred in many directions. In the following lemma, we estimate the number of directions in $\mathbb{F}_q^d$ with $d$ even.

\textbf{Lemma 4.1.} The number of directions in $\mathbb{F}_q^d$ with $d$ even is at least $(1 - o(1))q^{d^2/4}$.

\textbf{Proof.} Let $X$ be the set of solutions of the following equation in $\mathbb{F}_q^d$
\[ x_1^2 + \cdots + x_d^2 = 0. \]
Let $k$ be an integer, and $m$ be the number of subspaces of dimension $k$ in $\mathbb{F}_q^d$ that contain at least one element in $X$. We now use induction on $k$ to prove that $m = o(q^{(d-k)k})$ with $1 \leq k \leq d/2$.

The base case $k = 1$ is trivial. Suppose the claim holds for $k - 1 \geq 2$, we now show that it also holds for $k$. Indeed, by induction hypothesis, we have the number of $(k-1)$-subspaces containing at least one element from $X$ is $o\left(q^{(d-k+1)(k-1)}\right)$. Moreover, each of these $(k-1)$-subspaces is contained in at most $q^k$ subspaces of dimension $k$. By basic calculations, we have that if a $k$-subspace $S$ satisfies $S \cap X \neq \emptyset$, then $S$ contains at least $q^{k-1}$ subspaces of dimension $k-1$, which intersect $X$. In short, we obtain
\[ m \leq o\left(q^{(d-k+1)(k-1)}\right) \cdot q^k / q^{k-1} = o\left(q^{(d-k+1)(k-1)+1}\right) = o(q^{(d-k)k}), \]
since $1 \leq k \leq d/2$. Therefore the lemma follows with $k = d/2$. \(\Box\)

Let $G$ be a graph, and $P_4$ a path of length 3. We say that a homomorphism $\phi: P_4 \to G$ is degenerate if $|\phi(P_4) \cap V(G)| \leq 3$. In order to prove Theorem 1.3, we need the following lemma on the number of homomorphisms between $P_4$ and graphs $G$, which is a special case of Sidorenko’s conjecture.

\textbf{Lemma 4.2.} Let $G$ be a graph with $n$ vertices and $m$ edges. Then the number of homomorphisms from $P_4$ to $G$ is at least $8m^3/n^2$. 

8
Proof of Theorem 1.3: Let \((U, V)\) be a fixed direction. We construct a bipartite graph \(G_{U,V} = (A \cup B, E)\) as follows: \(A\) is the set of translates of \(U\) in \(\mathbb{F}^d_q\), \(B\) is the set of translates of \(V\) in \(\mathbb{F}^d_q\), and there is an edge between \(U' \in A\) with \(V' \in B\) if and only if there exists \(a \in A\) such that \(a = U' \cap V'\). Thus \(G\) is a bipartite graph with \(2q^{d/2}\) vertices and \(|A|\) edges. For \(2 \leq i \leq 4\), let \(H_i(U, V)\) denote the number of homomorphisms \(\phi\) from \(P_i\) to \(G_{U,V}\) with \(|\phi(P_i) \cap V(G_{U,V})| = i\). Then it is easy to check that the number of right angles determined by \(A\) in the direction \((U, V)\) equals \(H_4(U, V)/2\), and \(H_2(U, V) = 2|A|\). For a fixed pair of distinct points \((a, b) \in A \times A\), there are at most \(2q^{d^2-\frac{d}{2}}\) flats of dimension \(d/2\) containing the line passing through \(a\) and \(b\), thus we have the following upper bound of \(H_3(U, V)\):

\[
\sum_{(U,V)} H_3(U, V) \leq 2|A|^2 q^{\frac{d^2}{2}} - \frac{q}{4},
\]

where the sum is over all directions. It follows from Lemma 4.2 that the number of homomorphisms from \(P_4\) to \(G_{U,V}\) is at least \(2|A|^3/q^d\). Thus, we obtain

\[
H_4(U, V) \geq \frac{2|A|^3}{q^d} - H_2(U, V) - H_3(U, V).
\]

It follows from Lemma 4.1 that the number of directions is at least \((1 - o(1))q^{d/4}\). Hence,

\[
\sum_{(U,V)} H_4(U, V) \geq \sum_{(U,V)} \frac{2|A|^3}{q^d} - \sum_{(U,V)} H_2(U, V) - \sum_{(U,V)} H_3(U, V) \\
\geq (1 - o(1))q^{\frac{d^2}{2}-d}|A|^3 - (1 - o(1))q^{\frac{d^2}{2}}|A| - 2|A|^2 q^{\frac{d^2}{2}} - \frac{q}{4}.
\]

(4)

We note that, in the sum \(\sum_{(U,V)} H_4(U, V)\), each right angle determined by \(A\) is counted at most \(q^{\left(\frac{d}{2}-1\right)^2}\) times. Therefore, the number of right angles in \(A\) is at least

\[
\frac{1}{2} \left( (1 - o(1)) \frac{2|A|^3}{q} - (1 - o(1))q^{d-1}|A| - q^{d-1}|A|^2 \right) = (1 - o(1)) \frac{|A|^3}{q},
\]

when \(q^{d/2} = o(|A|)\), which concludes the proof of Theorem 1.3 (ii). Note that it also follows from our arguments that if \(|A| \geq 3q^{d/2}\), then the number of right angles is at least \(c \frac{|A|^3}{q}\) for some positive constant \(c\). This concludes the proof of Theorem 1.3 (i). □

5 Proof of Theorem 1.5

Let \(G = (V, E)\) be a \(d\)-regular graph with \(n\) vertices \(v_1, \ldots, v_n\). Suppose that the second largest eigenvalue of \(G\) is at most \(\gamma\). Let \(U\) be a multi-set of vertices in \(G\), i.e. some elements in \(U\) occur more than one time. For \(u \in U\), we denote its multiplicity in \(U\) by \(m_U(u)\). Let \(X_U = (x_1, \ldots, x_n)\) be the characteristic vector of \(U\), i.e. \(x_i = m_U(v_i)\). For any two multi-sets of vertices \(U\) and \(W\) in \(G\), it is clear that the number of edges between \(U\) and \(W\), denoted by \(e(U, W)\), is \(X_U^T MY_W\), where \(M\) is the adjacency matrix of \(G\). It has been shown that the number of edges between \(U\) and \(W\) satisfies the following estimate:

\[
\left| e(U, W) - \frac{d|U||W|}{n} \right| \leq \gamma \sqrt{\sum_{u \in U} m_U(u)^2} \sqrt{\sum_{w \in W} m_W(w)^2}.
\]

(5)

This estimate can be proved easily by using elementary results from linear algebra, one can find a detailed proof in [15].
Proof of Theorem 1.5: Let \( U' \) be the multi-set of classes
\[
[p_{a,b}] := [(a_1 - b_1, \ldots, a_d - b_d, -(a - b) \cdot b)] \in PG(q, d + 1),
\]
where \( a \) and \( b \) are distinct points in \( A \), and \( V \) be the set of classes \( [p_x] := [(x_1, \ldots, x_d, 1)] \in PG(q, d + 1) \) with \( (x_1, \ldots, x_d) \in A \).

Let \( t \) be the number of triples \((a, b, c) \in A \times A \times A\) satisfying \((a - b) \cdot (c - b) = 0\) and \( a \neq b \). Note that \( t \) is more than the number of right angles determined by \( A \) since we allow \( c = b \) or \( c = a \).

It follows from Theorem 1.5 that the number of right angles in \( A \) is at least \((1 - o(1))|A|^3/q\), thus it suffices to prove that \( t \leq (1 - o(1))|A|^3/q \).

On the other hand, it is clear that \( t \) is equal to the number of edges between \( U' \) and \( V \) in the Erdős-Rényi graph \( \mathcal{E}R(\mathbb{F}_q^{d+1}) \). Thus it follows from (5) and Theorem 2.2 that
\[
\left| t - \frac{(q^d - 1)|V| \sum_{[y] \in U'} m_{U'}([y])}{(q^d - 1)} \right| \leq q^{(d-1)/2} \sqrt{|V|} \left( \sum_{[y] \in U'} m_{U'}([y])^2 \right)^{1/2}.
\]

Moreover, as observed in the proof of Theorem 3.1, we have that \( [p_{a,b}] = [p_{c,e}] \) implies that \((a - b) \cdot (e - b) = 0\). Thus for each triple \((a, b, e) \) with \( a \neq b \) satisfying \((a - b) \cdot (e - b) = 0\), there are at most \( q \) points \( c \) such that \( [p_{a,b}] = [p_{c,e}] \). Therefore the upper bound of \( \sum_{[y]: m_{U'}([y]) \geq 1} m_{U'}([y])^2 \) is \( tq \). Since the number of points in \( U' \) with multiplicity 1 is at most \(|A|^2\) and \( t \geq (1 - o(1))|A|^3/q \) from the theorem 3.1 we obtain
\[
\sum_{[y] \in U'} m_{U'}([y])^2 \leq |A|^2 + tq = (1 + o(1))tq.
\]

Plugging this upper bound in the inequality (6), we get the following
\[
\left| t - \frac{(q^d - 1)|V| \sum_{[y] \in U'} m_{U'}([y])}{(q^d - 1)} \right| \leq (1 + o(1))q^{(d-1)/2} \sqrt{|V|} (tq)^{1/2} = (1 + o(1))q^{d/2} |V|^{1/2} t^{1/2}
\]

Solving this inequality gives us
\[
t \leq (1 - o(1)) \frac{|A|^3}{q},
\]
under the condition \( q^{d+1} = o(|A|) \).

In other words, if \( q^{d+1} = O(|A|) \), then the number of right angles in \( A \) is bounded from above by \((1 - o(1))|A|^3/q\). This completes the proof of the theorem. \(\square\)

References


Hanoi University of Science
Vietnam National University
Viet Nam
E-mail: sangnmkhtnvn@gmail.com

Department of Mathematics,
EPF Lausanne
Switzerland
E-mail: thang.pham@epfl.ch

Rényi Institute, Budapest,
Hungary
E-mail: tardos@renyi.hu