An inverse-type problem for cycles in local Cayley distance graphs

Thang Pham*

Abstract

Let $E$ be a proper symmetric subset of $S^{d-1}$, and $C_{\mathbb{F}_q}(E)$ be the Cayley graph with the vertex set $\mathbb{F}_q^d$, and two vertices $x$ and $y$ are connected by an edge if $x - y \in E$. Let $k \geq 2$ be a positive integer. We show that for any $\alpha \in (0, 1)$, there exists $q(\alpha, k)$ large enough such that if $E \subset S^{d-1} \subset \mathbb{F}_q^d$ with $|E| \geq \alpha q^{d-1}$ and $q \geq q(\alpha, k)$, then for each vertex $v$, there are at least $c(\alpha, k)q^{(2k-1)d-4k^2}$ cycles of length $2k$ with distinct vertices in $C_{\mathbb{F}_q}(E)$ containing $v$. This result is the inverse version of a recent result due to Iosevich, Jardine, and McDonald (2021).

Keywords: Spherical configurations, Finite fields, Cayley graphs, Cycles.

Mathematics Subject Classification: 52C10, 11T23

1 Introduction

Let $G$ be an abelian finite group and a symmetric set $E \subset G$. The Cayley graph $C_G(E)$ is defined as the graph with the vertex set $V = G$, and there is an edge from $x$ to $y$ if $y - x \in E$. Let $\mathbb{F}_q$ be a finite field of order $q$, where $q$ is a prime power. In this paper, we consider $G$ being the whole vector space $\mathbb{F}_q^d$.

We have $C_{\mathbb{F}_q}(E)$ is a regular graph of degree $|E|$ with $q^d$ vertices. It is well-known in the literature that eigenvalues of $C_{\mathbb{F}_q}(E)$ are of the form $\lambda_m := \sum_{x \in E} \chi(x \cdot m) = \hat{E}(m)$, $m \in \mathbb{F}_q^d$, where $\chi$ is the principle additive character of $\mathbb{F}_q$. Define $\mu := \max_{m \neq (0,0,...,0)} |\lambda_m|$. This quantity is referred as the second largest eigenvalue of $C_{\mathbb{F}_q}(E)$. We call a graph $(n, d, \lambda)$-graph if it has $n$ vertices, the degree of each vertex is $d$, and the second largest eigenvalue is at most $\lambda$.

When $E = S^{d-1}$, the unit sphere in $\mathbb{F}_q^d$, we recall a result from a paper of Iosevich and Rudnev [13, Lemma 5.1] that $\mu = (1 + o(1))q^{\frac{d-1}{2}}$. Thus, the graph $C_{\mathbb{F}_q}(S^{d-1})$ is a $(n, d, \lambda)$-graph with $n = q^d$, $d = |S^{d-1}|$, and $\lambda = (1 + o(1))q^{\frac{d-1}{2}}$. In a $(n, d, \lambda)$-graph, we know from [13, Theorem 4.10] that any large subset of vertices contains the correct number of copies of any fixed sparse graph. More

*Theory of Combinatorial Algorithms Group, ETH Zurich, Switzerland. Email: phamnhithang.vnu@gmail.com
Theorem 1.1 (Iosevich-Jardine-McDonald, [12]). Let $A$ be a set in $\mathbb{F}_q^d$. Suppose that $|A| \gg q^{d+\frac{2}{3}}$, then for any positive integer $\ell \geq 3$, the number of cycles of length $\ell$ in $C_{\mathbb{F}_q^d}(S^{d-1})$ with vertices in $A$ is $(1 + o(1))|A|^\ell q^{-\ell}$. In addition, when $\ell$ is large, then the exponent $\frac{d+2}{\ell}$ can be improved, namely, the condition

$$|A| \geq \begin{cases} q^{\frac{1}{2}(d+2-\frac{d+2}{\ell}+\delta)}, & \text{if } \ell \geq 4 \text{ even} \\ q^{\frac{1}{2}(d+2-\frac{d+3}{\ell}+\delta)}, & \text{if } \ell \geq 3 \text{ odd} \end{cases}$$

where $0 < \delta \ll \frac{1}{\ell^2}$, would be enough.

The following is our main result.

Theorem 1.2. Let $d, k \in \mathbb{N}$ with $d \geq 4k + 2$, $\alpha \in (0, 1)$ and $q \geq q(\alpha, k)$. For a symmetric set $E \subset S^{d-1} \subset \mathbb{F}_q^d$ with $|E| \geq \alpha q^{d-1}$, the number of cycles of length $2k$ in $C_{\mathbb{F}_q^d}(E)$ with distinct vertices passing through each vertex of $C_{\mathbb{F}_q^d}(E)$ is at least $c(\alpha, k)q^{\frac{(2k-1)d-4k}{2}}$.

To prove Theorem 1.2 several serious challenges arise, and the most difficulty comes from the fact the graph $C_{\mathbb{F}_q^d}(E)$ is not a pseudo-random graph, namely, the second eigenvalue $\mu$ is arbitrary close to the graph degree when $q$ is large enough.

Proposition 1.3. For any $1 \leq m \ll q^{d-1}$ and $\epsilon > 0$ with $1/\epsilon \in \mathbb{Z}$. Let $q = p^\frac{1}{\epsilon}$. There exists $E \subset S^{d-1}$ such that $|E| = m$ and $\mu \geq \frac{|E|}{q^d}$. In addition, if $|E + E| \sim |E|$, then we have $\mu \sim \lambda_{(0,\ldots,0)} = |E|$.

Hence, it is not possible to apply techniques of pseudo-random graphs to prove such a result as Theorem 1.2. Our main ingredient is a recent Ramsey-type result on the number of congruence copies of $2k$-spherical configurations spanning $2k-2$ dimensions due to Lyall, Magyar, and Parshall in [15], which has been derived by using a generalized von-Neumann type inequality [15].

\[1\text{We use the following notations: } X \ll Y \text{ means that there exists some absolute constant } C > 0 \text{ such that } X \leq CY, X \sim Y \text{ means that } X \ll Y \ll X, X = o(Y) \text{ means that } \lim_{y \to \infty} X/Y = 0.\]
It seems difficult to extend the approach of Theorem [12] for other subgraphs \( H \). When \( H \) is a \( k \)-simplex, say \( k = 2 \) for simplicity, the inverse problem asks for conditions on three given proper subsets \( E_1, E_2, E_3 \) of \( S^{d-1} \) such that there are three vertices \( x, y, z \in \mathbb{F}_q^d \) such that \( x - y \in E_1, y - z \in E_2, z - x \in E_3 \). Note that \( E_1, E_2, E_3 \) can also be assumed to be subsets of spheres with different radii. We believe that finding a non-trivial solution of this problem would be much difficult compared to the original one.

When \( E = S^{d-1} \), giving a lower bound on the number of cycles in \( C_{\mathbb{F}_q^d}(E) \) is much easier, since, as mentioned earlier, \( C_{\mathbb{F}_q^d}(S^{d-1}) \) is a pseudo-random graph with the second eigenvalue \( \mu \sim \sqrt{|S^{d-1}|} \).

In the next proposition, we provide an improvement of Theorem [11] in terms of the lower bound on the number of cycles of even length.

**Proposition 1.4.** Suppose \( E = S^{d-1} \), then the number of cycles of length \( 2k \) in \( C_{\mathbb{F}_q^d}(S^{d-1}) \) is \( (1 + o(1))|S^{d-1}|^{2k-1}q^{-d} \). In addition, for any set \( A \subset \mathbb{F}_q^d \) with \( |A| \gg \min\{q^{d+1/2}, q^{-d/2}\} \), the number of cycles of length \( 2k \) in \( C_{\mathbb{F}_q^d}(E) \) with vertices in \( A \) is at least \( q^{-2k}|A|^{2k} \).

Based on Proposition 1.4 and in the spirit of Theorem 1.1, we conjecture that for any set \( A \subset \mathbb{F}_q^d \) with \( |A| \gg \min\{q^{d+1/2}, q^{-d/2}\} \), the number of cycles of length \( 2k \) in \( C_{\mathbb{F}_q^d}(S^{d-1}) \) with vertices in \( A \) is equal to \( (1 + o(1))q^{-2k}|A|^{2k} \).

## 2 Preliminaries

Let \( \chi: \mathbb{F}_q \to S^1 \) be the canonical additive character. For example, if \( q \) is a prime number, then \( \chi(t) = e^{2\pi it/q} \), if \( q = p^n \), then we set \( \chi(t) = e^{2\pi it/q} \), where \( \mathbf{Tr}: \mathbb{F}_q \to \mathbb{F}_q \) is the trace function defined by \( \mathbf{Tr}(x) := x + x^p + \cdots + x^{p^{n-1}} \).

We recall the orthogonal property of \( \chi \): for any \( x \in \mathbb{F}_q^d, d \geq 1 \),

\[
\sum_{m \in \mathbb{F}_q^d} \chi(x \cdot m) = \begin{cases} 
0 & \text{if } x \neq (0, \ldots, 0) \\
q^d & \text{if } x = (0, \ldots, 0)
\end{cases},
\]

where \( x \cdot m = x_1 m_1 + \cdots + x_d m_d \).

For any \( x \in \mathbb{F}_q^d \), through this paper, we define \( ||x|| = x_1^2 + \cdots + x_d^2 \).

Given a set \( E \subset \mathbb{F}_q^d \), we identify \( E \) with its indicator function \( 1_E \). The Fourier transform of \( E \) is defined by

\[
\hat{E}(m) := \sum_{x \in \mathbb{F}_q^d} E(x) \chi(-x \cdot m).
\]
Let $E$ be a set in $\mathbb{F}_d^q$, and $k$ be a positive integer. The $k$–additive energy of $E$, denoted by $T_k(E)$, is defined by

$$T_k(E) := \# \left\{ (a_1, \ldots, a_k, b_1, \ldots, b_k) \in E^{2k} : a_1 + \cdots + a_k = b_1 + \cdots + b_k \right\}. \tag{1}$$

We call such a tuple $(a_1, \ldots, a_k, b_1, \ldots, b_k)$ $k$-energy tuple.

A $k$-energy tuple $(a_1, \ldots, a_k, b_1, \ldots, b_k) \in (\mathbb{F}_d^q)^{2k}$ is called good if for any two sets of indices $I, J \subset \{1, \ldots, k\}$, we have $\sum_{i \in I} a_i - \sum_{j \in J} b_j \neq 0$. We denote the number of good $k$-energy tuples with vertices in $E$ by $T_k^{\text{good}}(E)$.

In the next lemma, we show that for every vertex $v \in \mathbb{F}_d^q$, the number of cycles of length $2k$ with distinct vertices going through $v$ is at least $T_k^{\text{good}}(E)$.

**Lemma 2.1.** For any $k \geq 2$ and any $v \in \mathbb{F}_d^q$, the number of cycles of length $2k$ in $C_{\mathbb{F}_d^q}(E)$ with distinct vertices going through $v$ is at least $T_k^{\text{good}}(E)$.

**Proof.** For each good $k$-energy tuple $(a_1, \ldots, a_k, b_1, \ldots, b_k) \in E^{2k}$, we consider the following cycle of length $2k$ in $C_{\mathbb{F}_d^q}(E)$:

$$v, v + a_1, v + a_1 + a_2, \ldots, v + a_1 + \cdots + a_k, v + \sum_{i=1}^{k} a_i - b_1, \ldots, v + \sum_{i=1}^{k} a_i - \sum_{i=1}^{k-1} b_i.$$ 

We observe that in this cycle, each vertex appears only once since the $k$-energy tuple is good. So, for each vertex $v$, there are at least $T_k^{\text{good}}(E)$ cycles with distinct vertices passing through $v$. \hfill \Box

We also recall the well–known Expanding mixing lemma for regular graphs. We refer the reader to [10, 14] for proofs.

**Lemma 2.2.** Let $G$ be a regular graph with $n$ vertices of degree $d$. Suppose that the second eigenvalue of $G$ is at most $\mu$, then for any two vertex sets $U$ and $W$ in $G$, the number of edges between $U$ and $W$, denoted by $e(U, W)$, satisfies

$$\left| e(U, W) - \frac{d|U||W|}{n} \right| \leq \mu \frac{|U|^{1/2}|W|^{1/2}}. \tag{2}$$

When $U$ and $W$ are multi-sets, we also have

$$\left| e(U, W) - \frac{d|U||W|}{n} \right| \leq \mu \left( \sum_{u \in U} m(u)^2 \right)^{1/2} \cdot \left( \sum_{w \in W} m(w)^2 \right)^{1/2}.$$ 

4
where \( \overline{X} \) is the set of distinct elements in \( X \), and \( m(x) \) is the multiplicity of \( x \).

## 3 Proof of Theorem 1.2

Theorem 1.2 follows directly from Lemma 2.1 and the following lower bound for \( T_k^{\text{good}}(E) \).

**Theorem 3.1.** Suppose \( E \) satisfies assumptions of Theorem 1.2, we have

\[
T_k^{\text{good}}(E) \geq c(\alpha, k)q^{(2k-1)d-4k+2}.
\]

In the rest of this section, we focus on proving Theorem 3.1.

For each \( j \neq 0 \), let \( S_{d-1}^j(x) \) be the sphere centered at \( x \in \mathbb{F}_q^d \) of radius \( j \). For the sake of simplicity, we write \( S_{d-1}^0 \) for \( S_{d-1}^0(0, \ldots, 0) \), and \( S_{d-1}^1 \) for \( S_{d-1}^1(0, \ldots, 0) \).

**Definition 3.2.** Let \( X \subset \mathbb{F}_q^d \) be a configuration. We say that \( X \) is spherical if \( X \subset S_{d-1}^1(x) \) for some \( x \in \mathbb{F}_q^d \). If \( \dim(\text{Span}(X - X)) = k \), then we say \( X \) spans \( k \) dimensions.

The following result is our key ingredient in the proof of Theorem 3.1.

**Theorem 3.3** (Lyall-Magyar-Parshall, [15]). Let \( d, k \in \mathbb{N} \) with \( d \geq 2k+6 \), \( \alpha \in (0,1) \) and \( q \geq q(\alpha, k) \). For \( E \subset S_{d-1}^1 \) with \( |E| \geq \alpha q^{d-1} \), then \( E \) contains at least \( c(\alpha, k)q^{(k+1)d-(k+1)(k+2)} \) isometric copies of every non-degenerate \((k+2)\)-point spherical configuration spanning \( k \) dimensions.

This theorem says that for any \( \alpha \in (0,1) \) and any fixed non-degenerate \((k+2)\)-point spherical configuration \( X \) spanning \( k \) dimensions, there exists \( q_0 = q_0(\alpha, k) \) which is large enough, such that for any \( E \subset S_{d-1}^1 \subset \mathbb{F}_q^d \) with \( |E| \geq \alpha q^{d-1} \) and \( q \geq q_0 \), \( E \) contains many isometric copies of \( X \).

More precisely, let

\[
X = \{0, v_1, \ldots, v_k, a_1v_1 + \cdots + a_kv_k\},
\]

where \( 0 = (0, \ldots, 0) \), \( v_1, \ldots, v_k \in \mathbb{F}_q^d \) are linearly independent vectors, and \( a_1, \ldots, a_k \in \mathbb{F}_q \), be a non-degenerate spherical configuration of \( k + 2 \) points in \( \mathbb{F}_q^d \) that spans a \( k \)-dimensional vector space. By non-degenerate, we meant that \( \{0, v_1, \ldots, v_k\} \) form a \( k \)-simplex with all non-zero side-lengths. Assume that \( E \subset S_{d-1}^1 \) satisfying the conditions of Theorem 3.3, then \( E \) contains at least \( c(\alpha, k)q^{(k+1)d-(k+1)(k+2)} \) copies of \( X \) of the form

\[
X' = \{x_0, x_0 + x_1, \ldots, x_0 + x_k, x_0 + a_1x_1 + \cdots + a_kx_k\},
\]

with \( x_1, \ldots, x_k \) linearly independent such that \( x_i \cdot x_j = v_i \cdot v_j \) for \( 1 \leq i \leq j \leq k \).

We recall that two configurations \( X \) and \( X' \) in \( S_{d-1}^1 \) are said to be in the same congruence class if
there exists \( g \in O(d, \mathbb{F}_q) \), the orthogonal group in \( \mathbb{F}_q^d \), such that \( g(X) = X' \).

Let \( Q \) be the set of distinct congruence classes of spherical configurations \( X \) of the form

\[
X = \{ x_0, x_0 + x_1, x_0 + x_2, \ldots, x_0 + x_{2k-2}, x_0 + \sum_{i=1}^{2k-2} (-1)^{i+1}(x + x_i) \},
\]

satisfying

- \( \{x_1, \ldots, x_{2k-2}\} \) are linearly independent.
- \( ||x_i - x_j|| \neq 0, ||x_i|| \neq 0 \) for all \( 1 \leq i \neq j \leq 2k - 2 \).
- \( X \) forms a good \( k \)-energy tuple.

We note that vectors in \( X \in Q \) form a \( k \)-energy tuple since

\[
x_0 + (x_0 + x_1) + (x_0 + x_3) + \cdots + (x_0 + x_{2k-3}) = (x_0 + x_2) + (x_0 + x_4) + \cdots + (x_0 + x_{2k-2}) + u,
\]

where \( u = x_0 + \sum_{i=1}^{2k-2} (-1)^{i+1}(x_0 + x_i) \).

For each \( X \in Q \), let \( N(X) \) be the number of congruent copies of \( X \) in \( E \). Set \( N(Q) = \sum_{X \in Q} N(X) \).

The next lemma gives us a lower bound for \( T_k^{\text{good}}(E) \).

**Lemma 3.4.** Suppose \( E \) satisfies assumptions of Theorem 1.2, we have

\[
T_k^{\text{good}}(E) \geq N(Q). \tag{1}
\]

**Proof.** Let

\[
X = \{ x_0, x_0 + x_1, x_0 + x_2, \ldots, x_0 + x_{2k-2}, x_0 + \sum_{i=1}^{2k-2} (-1)^{i+1}(x_0 + x_i) \} \in Q,
\]

and set \( u = x_0 + \sum_{i=1}^{2k-2} (-1)^{i+1}(x_0 + x_i) \), then we have

\[
x_0 + (x_0 + x_1) + (x_0 + x_3) + \cdots + (x_0 + x_{2k-3}) = (x_0 + x_2) + (x_0 + x_4) + \cdots + (x_0 + x_{2k-2}) + u,
\]

which provides a good \( k \)-energy tuple. Notice that \( x_0 + x_i \neq x_0 + x_j \) for all pairs \( (i, j) \), and \( u \neq x_0, x_0 + x_i \) for all \( i \). Since the additive energy is invariant under the action of orthogonal matrices, we have \( N(X) \) good \( k \)-energy tuples in \( E \). Summing over all \( X \), we have \( N(Q) \) good \( k \)-energy tuples in \( E \).

In the form of Lemma 3.4 in order to complete the proof of Theorem 3.1 we have to find a lower
bound for $N(Q)$, which will be followed by a lower bound of $|Q|$ and Theorem 3.3. The following proposition plays an important role for this step.

**Proposition 3.5.** For $d \geq \max\{2k - 2, 4\}$ and $k \geq 2$, we have $|Q| \gg q^{2k^2 - 3k}$.

With Proposition 3.5 in hand, we derive the following corollary.

**Corollary 3.6.** Let $d, k \in \mathbb{N}$ with $d \geq 4k + 2$, $\alpha \in (0, 1)$ and $q \geq q(\alpha, k)$. Let $E \subseteq S^{d - 1} \subseteq \mathbb{F}_q^d$ with $|E| \geq \alpha q^{d - 1}$. We have

$$N(Q) \geq c(\alpha, k)q^{\frac{(2k - 1)d - 4k}{2}}.$$ 

**Proof.** For each configuration in $Q$, we know from Theorem 3.3 that the number of its copies in $E$ is at least

$$c(\alpha, k)q^{\frac{(2k - 1)d - (2k - 1)(2k)}{2}}.$$ 

Taking the sum over all possible $q^{2k^2 - 3k}$ congruence classes, the lemma follows. \qed

Combining Lemma 3.4 and Corollary 3.6, Theorem 3.1 is proved.

### 3.1 Proof of Proposition 3.5

We now turn our attention to the Proposition 3.5. The proof of Proposition 3.5 is quite complicated, which combines the usual Cauchy-Schwarz argument and the claim that most $k$-energy tuples in $S^{d - 1}$ are $2k$-spherical configurations spanning $(2k - 2)$ dimensions. We first start with some technical lemmas.

**Lemma 3.7** (Lemma 4.5, [11]). For any $E \subseteq S^{d - 1}$, and $k \geq 2$, we have

$$|T_k(E) - \frac{|E|^{2k - 1}}{q}| \leq q^{d - 1}T_{k - 1}^{1/2}T_k^{1/2},$$

where $T_1(E) = |E|$.

**Corollary 3.8.** For $k, d \geq 2$, we have

$$T_k(S^{d - 1}) = (1 + o(1))\frac{|S^{d - 1}|^{2k - 1}}{q}.$$ 

**Proof.** We prove by induction on $k$.

For $k = 2$, we apply Lemma 3.7 to obtain

$$|T_2(S^{d - 1}) - \frac{|S^{d - 1}|^3}{q}| \leq q^{d - 1} \cdot T_2^{1/2}|S^{d - 1}|^{1/2}.$$
Using the fact that $|S^{d-1}| \sim q^{d-1}$ and set $x = \sqrt{T_2(S^{d-1})}$, we have

\[ x^2 \geq c_1 q^{3d-4} - c_2 q^{d-1} x, \quad \text{and} \quad x^2 \leq c_1 q^{3d-4} + c_2 q^{d-1} x, \]

for some positive constants $c_1$ and $c_2$. Solving these equations gives us $x \gg q^{\frac{3d-4}{2}}$ and $x \ll q^{\frac{3d-4}{2}}$, respectively. Thus, the base case is proved.

Suppose that the claim holds for any $k - 1 \geq 2$, we now show that it also holds for the case $k$. Indeed, set $x = \sqrt{T_k(S^{d-1})}$, applying Lemma 3.7 and the inductive hypothesis, we have

\[ x^2 - q^{\frac{d-1}{2}} |S^{d-1}|^{\frac{2k-3}{2}} x - \frac{|S^{d-1}|^{2k-1}}{q} \leq 0, \quad x^2 + q^{\frac{d-1}{2}} |S^{d-1}|^{\frac{2k-3}{2}} x - \frac{|S^{d-1}|^{2k-1}}{q} \geq 0. \]

Solving these inequalities will give us

\[ x = (1 + o(1)) \left( \frac{|S^{d-1}|^{2k-1}}{q} \right)^{1/2}. \]

This completes the proof of the corollary. \[\square\]

**Lemma 3.9.** For $d > n \geq 2$, let $L$ be the number of tuples $(v_0, \ldots, v_n) \in (S^{d-1})^{n+1}$ such that $v_i - v_0 \in \{a_1(v_1-v_0) + \cdots + a_{i-1}(v_{i-1}-v_0) + a_{i+1}(v_{i+1}-v_0) + \cdots + a_n(v_n-v_0): a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \neq 0 \}$ for some $1 \leq i \leq n$. We have $L \ll \frac{|S^{d-1}|^{n+1}}{q^{d-1}}$.

**Proof.** Without loss of generality, we count the number of such tuples with $i = n$.

Let $\chi$ be the principle additive characteristic of $F_q$. Using the orthogonality of $\chi$, one has

\[
L \leq \frac{1}{q^d} \sum_{s \in F_q} \sum_{v_0, \ldots, v_n \in S^{d-1}} \sum_{a_1, \ldots, a_{n-1} \in F_q} \chi \left( s \cdot \left( (v_n - v_0) - a_1(v_1 - v_0) - \cdots - a_{n-1}(v_{n-1} - v_0) \right) \right)
\]

\[
= \frac{|S^{d-1}|^{n+1}}{q^{d-n+1}} + \frac{1}{q^d} \sum_{s \neq 0} \sum_{v_0, \ldots, v_n \in S^{d-1}} \sum_{a_1, \ldots, a_{n-1} \in F_q} \chi \left( s \cdot \left( (v_n - v_0) - a_1(v_1 - v_0) - \cdots - a_{n-1}(v_{n-1} - v_0) \right) \right)
\]

\[
= \frac{|S^{d-1}|^{n+1}}{q^{d-n+1}} + \frac{1}{q^d} \sum_{s \neq 0} \sum_{a_1, \ldots, a_{n-1} \in F_q} \tilde{S}(a) \cdots \tilde{S}(a) \tilde{S}(s(1 - a_1 - \cdots - a_{n-1})),
\]

where $\tilde{S}(m) = \sum_{x \in F_q} S(x) \chi(-x \cdot m)$. We now recall from [12] Lemma 5.1 that $|\tilde{S}(m)| \ll q^{\frac{d-4}{2}}$ for $m \neq 0$ and $\tilde{S}(0) = |S^{d-1}| \sim q^{d-1}$. We now partition the sum $\sum_{a_1, \ldots, a_{n-1} \in F_q}$ into two sub-

summands $\sum_{a_1 + \cdots + a_{n-1} \neq 1}$ and $\sum_{a_1 + \cdots + a_{n-1} = 1}$.
Therefore,

\[ \sum_{a_1 + \cdots + a_{n-1} \neq 1} \left( S_{d-1}(a_1 s) \cdots S_{d-1}(a_{n-1} s) S_{d-1}(s(1 - a_1 - \cdots - a_{n-1})) \right) \ll q^{\frac{(d-1)(n+1)}{2}} \cdot q^{n-1}, \]

and

\[ \sum_{a_1 + \cdots + a_{n-1} = 1} \left( S_{d-1}(a_1 s) \cdots S_{d-1}(a_{n-1} s) S_{d-1}(s(1 - a_1 - \cdots - a_{n-1})) \right) \ll q^{\frac{(d-1)(n)}{2}} \cdot q^{d-1} \cdot q^{n-2}. \]

These upper bounds are at most \( \frac{|S_{d-1}|^{n+1}}{q^{d-1}} \) when \( d > n \) and \( n \geq 2 \). In other words,

\[ L \ll \frac{|S_{d-1}|^{n+1}}{q^{2}}. \]

\[ \square \]

**Lemma 3.10.** Suppose that \( d > 2k - 2 \) and \( k \geq 2 \). The number of tuples \( \{x_0, x_0 + x_1, \ldots, x_0 + x_{2k-2}, x_0 + \sum_{i=1}^{2k-2} (-1)^i (x_0 + x_i)\} \) in \( (S_{d-1})^{2k} \) such that

\[ x_0 + (x_0 + x_1) + (x_0 + x_3) + \cdots + (x_0 + x_{2k-3}) = (x_0 + x_2) + (x_0 + x_4) + \cdots + (x_0 + x_{2k-2}) + u, \]

where \( u = x_0 + \sum_{i=1}^{2k-2} (-1)^i (x_0 + x_i) \), and \( x_i \in \text{Span}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{2k-2}) \) for some \( 1 \leq i \leq 2k - 2 \) is \( o(T_k(S_{d-1})) \).

**Proof.** Applying Lemma 3.9 for the family of vectors \( \{x_0, x_0+x_1, \ldots, x_0+x_{2k-2}\} \) or its sub-families, we know that there are at most \( \frac{|S_{d-1}|^{2k-1}}{q^{2}} \) such tuples whenever \( d > 2k - 2 \) and \( k \geq 2 \). We also know from Corollary 3.8 that \( T_k(S_{d-1}) = (1 + o(1))\frac{|S_{d-1}|^{2k-1}}{q^{2}} \). Thus, the lemma follows from the fact that

\[ \frac{|S_{d-1}|^{2k-1}}{q^{2}} = o \left( \frac{|S_{d-1}|^{2k-1}}{q} \right). \]

\[ \square \]

We are ready to give a proof of Proposition 3.5.

**Proof of Proposition 3.5** For any \( k \)-energy tuple \( (a_1, \ldots, a_k, b_1, \ldots, b_k) \in S^{d-1} \), i.e.

\[ a_1 + \cdots + a_k = b_1 + \cdots + b_k, \]

we set \( a_i = a_1 + x_i \) for \( 2 \leq i \leq k \), and \( b_i = a_1 + y_i \) for \( 1 \leq i \leq k \).
We first show that most of all tuples \((a_1, \ldots, a_k, b_1, \ldots, b_k)\) satisfying \([2]\) will have the following properties

a. \(\{x_2, \ldots, x_k, y_1, \ldots, y_k\}\) are linearly independent.

b. \(||x_i - x_j|| \neq 0, ||y_i - y_j|| \neq 0\) for all pairs \(i \neq j\), and \(||x_i - y_j|| \neq 0, ||y_i|| \neq 0, ||y_j|| \neq 0\) for all pairs \(i, j\).

c. For any \(I, J \subseteq \{1, \ldots, k\}\), we have \(\sum_{i \in I} a_i - \sum_{j \in J} b_j \neq 0\).

Indeed, let \(T^\text{dep}(S^{d-1}), T^\varnothing_k(S^{d-1}), T^\text{bad}_k(S^{d-1})\) be the number of \(k\)-energy tuples not satisfying (a), (b), and (c), respectively. We will prove that \(T^\text{dep}(S^{d-1}), T^\varnothing_k(S^{d-1}), T^\text{bad}_k(S^{d-1}) = o(T_k(S^{d-1}))\).

Bounding \(T^\text{dep}_k\): By Lemma 3.10, we have \(T^\text{dep}_k = o(T_k(S^{d-1}))\).

Bounding \(T^\varnothing_k\): It follows from our setting that \(||x_i - x_j|| = ||a_i - a_j||\) and \(||x_i - y_j|| = ||a_i - b_j||\). Hence, it is sufficient to count tuples with \(||a_i - a_j|| = 0\) for some \(1 \leq i \neq j \leq k\). The other cases can be treated in the same way.

Without loss of generality, we assume that \(||a_1 - a_2|| = 0\), which is equivalent with \(||x_2|| = 0\).

Let \(U\) be the multi-set defined by

\[U := \{a_1 + \cdots + a_k: a_i \in S^{d-1}, ||a_1 - a_2|| = 0\}\]

Let \(W\) be the multi-set defined by

\[W := \{b_1 + \cdots + b_{k-1}: b_i \in S^{d-1}\}\]

Let \(e(U, W)\) be the number of pairs \((u, w) \in U \times W\) such that \(u - w \in S^{d-1}\). Applying Lemma \([2]\) for the graph \(C_{2q}(S^{d-1})\), we have

\[e(U, W) \leq \frac{|U||W|}{q} + q^{\frac{d-1}{2}} \left( \sum_{u \in U} m(u)^2 \right)^{1/2} \cdot \left( \sum_{w \in W} m(w)^2 \right)^{1/2}\]

where \(m(u), m(w)\) are the multiplicities of \(u\) and \(w\) in \(U\) and \(W\), respectively.

We know from \([8]\) that for any two sets \(X, Y \subseteq S^{d-1}\), the number of pairs \((x, y) \in X \times Y\) such that \(||x - y|| = 0\) is at most \(\frac{|X||Y|}{q} + q^{\frac{d}{2}}|X|^{1/2}|Y|^{1/2}\). So with \(X = Y = S^{d-1}\), we obtain \(|U| \leq \frac{|S^{d-1}|^k}{q}\).

It is clear that \(|W| = |S^{d-1}|^{k-1}\).
On the other hand, it is not hard to see that
\[
\sum_u m(u)^2 \leq T_k(S^{d-1}), \quad \sum_w m(w)^2 \leq T_{k-1}(S^{d-1}).
\]

Using Corollary 3.8, one has
\[
e(U, W) \leq \frac{|S^{d-1}|2^{k-1}}{q^2} + q^{d-1} \frac{|S^{d-1}|2^{k-1}}{q^{1/2}} \cdot \frac{|S^{d-1}|2^{k-3}}{q^{1/2}} \ll \frac{|S^{d-1}|2^{k-1}}{q^2}.
\]

On the other hand, \( e(U, W) \) equals to the number of tuples satisfying (2) with \( |a_1 - a_2| = 0 \).

In other words,
\[
T_k^0 \ll \frac{|S^{d-1}|2^{k-1}}{q^2} = o(T_k(S^{d-1})).
\]

Bounding \( T_k^{\text{bad}} \): Let \( I \) and \( J \) be two subsets of \( \{1, \ldots, k\} \). Assume that \( |I| = |J| = m \). The case \( |I| \neq |J| \) is treated in the same way. Without loss of generality, we assume that \( I = J = \{1, \ldots, m\} \). We now count the number of \( k \)-energy tuples \( (a_1, \ldots, a_k, b_1, \ldots, b_k) \in (S^{d-1})^2 \) such that \( a_1 + \cdots + a_m - b_1 - \cdots - b_m = 0 \). This implies that \( a_{m+1} + \cdots + a_k - b_{m+1} - \cdots - b_k = 0 \).

We now show that the number of tuples \( (a_1, \ldots, a_m, b_1, \ldots, b_m) \in (S^{d-1})^{2m} \) such that \( a_1 + \cdots + a_m - b_1 - \cdots - b_m = 0 \) is at most \( \ll \frac{|S^{d-1}|2m-1}{q} \).

Indeed, using the same argument as in bounding \( T_k^0 \), let \( U', W' \) be multi-sets defined by
\[
U' := \{a_1 + \cdots + a_m : a_i \in S^{d-1}\}, \quad W = \{b_1 + \cdots + b_{m-1} : b_i \in S^{d-1}\}.
\]

The number of such tuples is bounded by \( e(U', W') \) in the graph \( G_{p,q}(S^{d-1}) \). As before, we also have
\[
\sum_{u \in U'} m(u)^2 = T_m(S^{d-1}), \quad \sum_{w \in W'} m(w)^2 = T_{m-1}(S^{d-1}).
\]

Using Lemma 2.2 and Lemma 3.7, we have
\[
e(U', W') \ll \frac{|S^{d-1}|2m-1}{q} + q^{d-1} \cdot \frac{|S^{d-1}|2m-2}{q} \ll \frac{|S^{d-1}|2m-1}{q}.
\]

Similarly, the number of tuples \( (a_{m+1}, \ldots, a_k, b_{m+1}, \ldots, b_k) \in S^{d-1} \) such that \( a_{m+1} + \cdots + a_k - b_{m+1} - \cdots - b_k = 0 \) is at most \( \ll \frac{|S^{d-1}|2(k-m)-1}{q} \).

Hence, the number of \( k \)-energy tuples with \( \sum_{i \leq l} a_i - \sum_{j \leq l} b_j = 0 \) is at most \( \ll \frac{|S^{d-1}|2k-2}{q^2} \).
Summing over all possibilities of sets $I$ and $J$, we obtain

$$T_k^{\text{bad}}(S^{d-1}) = o(T_k(S^{d-1})).$$

From the bounds of $T_k^{\text{dep}}$, $T_k^0$, and $T_k^{\text{bad}}(S^{d-1})$, we conclude that most of $k$-energy tuples in $S^{d-1}$ satisfying $(a), (b)$, and $(c)$. We denote the number of those tuples by $T_k^*(S^{d-1})$.

We recall that for any two non-trivial spherical configurations $X$ and $X'$, they are in the same congruent class if there exists $g \in O(d, \mathbb{F}_q)$ such that $gX = X'$. For each configuration in $Q$, say,

$$X = \{ x_0, x_0 + x_1, x_0 + x_2, \ldots, x_0 + x_{2k-2}, x_0 + \sum_{i=1}^{2k-2} (-1)^{i+1}(x + x_i) \},$$

the $2k - 1$ vertices $x_0, x_0 + x_1, \ldots, x_0 + x_{2k-2}$ form a non-degenerate $(2k - 2)$-simplex. We know from [3] that the stabilizer of a non-degenerate $(2k - 2)$–simplex in $S^{d-1}$ is of cardinality at least $|O(d - 2k + 1)|$.

For any $X \in Q$, let $\mu(X)$ be the number of configurations which are congruent to $X$. We have $\sum_{X \in Q} \mu(X) = T_k^*(S^{d-1})$. By Cauchy-Schwarz inequality, we have

$$\sum_{X \in Q} \mu(X) \leq |Q|^{1/2} \cdot \left( \sum_{X} \mu(X)^2 \right)^{1/2}. \quad (3)$$

On the other hand, $\sum_X s(X)\mu(X)^2$ is at most the number of pairs of configurations $(X, X')$ such that $X' = g(X)$ for some $g \in (d, \mathbb{F}_q)$, where $s(X)$ is the stabilizer of $X$. Hence, we can bound $\sum_X s(X)\mu(X)^2$ by $T_k^*(S^{d-1}) \cdot |O(d, \mathbb{F}_q)|$. This implies that

$$\sum_X \mu(X)^2 \leq \frac{|O(d, \mathbb{F}_q)| \cdot T_k^*(S^{d-1})}{|O(d - 2k + 1)|}. \quad (4)$$

We recall from [3] that $|O(n, \mathbb{F}_q)| \sim q^{\binom{n}{2}}$. From (3) and (4), we obtain $|Q| \gg q^{2k^2 - 3k}$. This completes the proof.

4 Proof of Proposition 1.3

Proof of Proposition 1.3 Suppose $q = p^r$ with $r = \frac{1}{\epsilon}$ (assume that $1/\epsilon$ is an integer).

Let $A$ be an arithmetic progression in $\mathbb{F}_q$ of size $p^{r-1}$. Let $X$ be the hyperplane $x_d = 0$. Define

$$H := \{ X + (0, \ldots, 0, a) : a \in A \}.$$
Note that $H$ is a set of $|A|$ translates of the hyperplane $X$.

We have $|H| = q^{d-1} \cdot \frac{q \cdot 1}{q-1} = q^{d-\epsilon}$. It is not hard to see that

$$|(H - H) \cap S^{d-1}| \ll q^{d-2} \cdot \frac{q - 1}{q} \ll q^{d-1-\epsilon} = o(|S^{d-1}|).$$

For any $1 \leq m \ll |S^{d-1}|$, let $E \subset S^{d-1} \setminus (H - H)$ with $|E| = m$, we have

$$(H - H) \cap E = \emptyset. \quad (5)$$

If $\mu < \frac{|E|}{2q^d}$, then by Lemma 2.2 for the graph $C_{F_q^d}(E)$, one has

$$e(H, H) \geq \frac{|H|^2|E|}{q^d} - \frac{|E||H|}{2q^d} > 0,$$

whenever $|H| > \frac{q^{d-\epsilon}}{2}$, which contradicts to (5).

In other words, we have $\mu \geq \frac{|E|}{2q^d}$.

In the case $|E + E| = K|E| < q^d/2$, we start with an observation that

$$T_2(E) \geq \frac{|E|^4}{|E + E|},$$

which implies

$$T_2(E) \geq \frac{|E|^4}{K|E|^4}.$$

Let $X$ be the multi-set in $F_q^d$ defined by $X = E + E$. We can apply the Expander mixing lemma for the graph $C_{F_q^d}(E)$ to get an upper bound for $T_2(E)$. Indeed, one has

$$T_2(E) = e(X, -E) \leq \frac{|E|^4}{q^d} + \mu \cdot T_2(E)^{1/2} \cdot |E|^{1/2}.$$

This gives us

$$T_2(E) \leq \frac{|E|^4}{q^d} + \mu^2 \cdot |E|.$$  

Since $K|E| < q^d/2$, we have $\mu^2|E| \gg \frac{|E|^4}{K|E|^4}$. This gives $\mu \gg \frac{|E|}{K^{3/2}}$. Hence, when $K \sim 1$, we have $\mu \gg |E|$. \qed
5 Proof of Proposition 1.4

Proof of Proposition 1.4. We have seen in the proof of Theorem 1.2 that the number of cycles of length $2k$ is equal to $q^d \cdot T_k(S^{d-1})$ and $T_k(S^{d-1}) = (1 + o(1))|S^{d-1}|^{2k-1}/q$. Hence, the number of cycles of length $2k$ in $C_{F_q}(S^{d-1})$ is $(1 + o(1))|S^{d-1}|^{2k-1}q^{-1}$.

To prove the upper bound on the number of cycles of length $2k$ in a given set $A \subset F_q^d$, we need to recall the following result from [4].

Theorem 5.1 (Bennett-Chapman-Covert-Hart-Iosevich-Pakianathan, [4]). For $A \subset F_q^d$, $d \geq 2$ and an integer $k \geq 1$. Suppose that $\frac{2k}{\ln q} \frac{d-1}{q} = o(|A|)$ then the number of paths of length $k$ with vertices in $A$ in $C_{F_q}(S^{d-1})$ is $(1 + o(1))\frac{|A|^{k+1}}{q^k}$.

Let $N$ be the number of cycles of length $2k$ with vertices in $A$. For any two vertices $x, y \in A$, let $P(x, y)$ be the number of paths of length $k$ between $x$ and $y$ with vertices in $A$. It follows from Theorem 5.1 that

$$\sum_{x, y \in A} P(x, y) = (1 + o(1))\frac{|A|^{k+1}}{q^k}.$$ 

It is clear that

$$N = \sum_{x, y \in A} \left( \frac{P(x, y)}{2} \right).$$

Using the convexity of the function $\left(\frac{x}{2}\right)$, one has

$$N \gg |A|^2 \cdot \left( \frac{\sum_{x, y \in A} P(x, y)}{|A|^2} \right) \gg \frac{|A|^{2k}}{q^{2k}},$$

provided that $|A| \gg q^{\frac{k}{k-1}}$. This completes the proof.

Remark 5.1. We remark here that for any $k \geq 2$, there exists a set $E \subseteq S^{d-1}$ with $|E| \gg q^{\frac{d}{2k-1}}$ such that all cycles of length $2k$ in $C_{F_q}(E)$ do not have distinct vertices. Such a set can be constructed easily as follows. Let $H$ be a $2k$-uniform hypergraph with the vertex set $S^{d-1}$, and each edge is a good $k$-energy tuple, then we know from the proof of Proposition 3.5 that the number of edges in $H$ is at most $|S^{d-1}|^{2k-1}/q$. Applying Spencer’s independent hypergraph number lemma in [16], we get an independent set $E$ of size at least $\gg q^{\frac{d}{2k-1}}$. This set will satisfy our desired properties.
Acknowledgments

The author was supported by Swiss National Science Foundation grant P4P4P2-191067. I would like to thank Ilya Shkredov for useful discussions about the second eigenvalue of the local Cayley distance graphs.

References

[1] A. J. Bondy, M. Simonovits, *Cycles of even length in graphs*, Journal of Combinatorial Theory, Series B, 16(2) (1974): 97–105.

[2] M. Bennett, A. Iosevich, J. Pakianathan, *Three-point configurations determined by subsets of \( \mathbb{F}_q^2 \) via the Elekes–Sharir Paradigm*, Combinatorica, 34(6), 689–706.

[3] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, M. Rudnev, *Group actions and geometric combinatorics in \( \mathbb{F}_q^d \)*, Forum Mathematicum, vol. 29, no. 1, pp. 91–110. De Gruyter, 2017.

[4] M. Bennett, J. Chapman, D. Covert, D. Hart, A. Iosevich, J. Pakianathan, *Long paths in the distance graph over large subsets of vector spaces over finite fields*, J. Korean Math. Soc, 53(1) (2016), 115–126.

[5] J. Chapman, M. Burak Erdogan, D. Hart, A. Iosevich, and D. Koh, *Pinned distance sets, k-simplices, Wolff’s exponent in finite fields and sum-product estimates*, Math Z. 271 (2012), no. 1, 63–93.

[6] C. Chen, *Salem sets in vector spaces over finite fields*, Arkiv för Matematik, 56(1) (2018): 45–52.

[7] 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 mathematics, 311, no. 6 (2011): 423–430.

[8] 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), no. 6, 3255-3275.

[9] D. Hart, A. Iosevich, *Ubiquity of simplices in subsets of vector spaces over finite fields*, Analysis Mathematica, 34 (2007).

[10] B. Hanson, B. Lund, O. Roche-Newton, *On distinct perpendicular bisectors and pinned distances in finite fields*, Finite Fields and Their Applications, 37 (2016): 240–264.
[11] D. D. Hieu, T. Pham, *Distinct distances on regular varieties over finite fields*, Journal of Number Theory, 173(2017): 602–613.

[12] A. Iosevich, G. Jardine, B. McDonald, *Cycles of arbitrary length in distance graphs on $\mathbb{F}_q^d$*, Proceedings of the Steklov Institute of Mathematics dedicated to 130th anniversary of Academician Ivan Matveevich Vinogradov, [arXiv:2101.00748](https://arxiv.org/abs/2101.00748) (2021).

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

[14] M. Krivelevich, B. Sudakov, *Pseudo-random graphs*, More sets, graphs and numbers, Springer, Berlin, Heidelberg, 2006. 199–262.

[15] N. Lyall, A. Magyar, H. Parshall, *Spherical configurations over finite fields*, American Journal of Mathematics, 142(2) (2020): 373–404.

[16] J. Spencer, *Turán’s theorem for k–graphs*, Discrete Mathematics 2 (1972), 183–186.

[17] L. A. Vinh, *On kaleidoscopic pseudo-randomness of finite Euclidean graphs*, Discussiones Mathematicae. Graph Theory, 32(2) (2012) 279 – 287.

[18] L. A. Vinh, *The solvability of norm, bilinear and quadratic equations over finite fields via spectra of graphs*, Forum Mathematicum, Vol. 26 (2014), No. 1, pp. 141–175.