Distance graphs in vector spaces over finite fields, coloring and pseudo-randomness

Derrick Hart, Alex Iosevich, Doowon Koh, Steve Senger and Ignacio Uriarte-Tuero

Abstract. In this paper we systematically study various properties of the distance graph in $\mathbb{F}_q^d$, the d-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements. In the process we compute the diameter of distance graphs and show that sufficiently large subsets of d-dimensional vector spaces over finite fields contain every possible finite configurations.

Contents

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements. We assume that the characteristic of $\mathbb{F}_q$ is greater than two. For each $r \in \mathbb{F}_q^*$, the multiplicative group of $\mathbb{F}_q$, the distance graph $G_q^\Delta(r)$ in $\mathbb{F}_q^d$ is obtained by taking $\mathbb{F}_q^d$ and connecting two vertices corresponding to $x, y \in \mathbb{F}_q^d$ by an edge if $||x-y|| = r$ where

$$||x|| = x_1^2 + x_2^2 + \cdots + x_d^2.$$

More generally consider the set of colors $L_q = \{c_q^r : r \in \mathbb{F}_q^*\}$ corresponding to elements of $\mathbb{F}_q^*$. We connect two vertices corresponding to points $x, y \in \mathbb{F}_q^d$ by a c_q^r-colored edge if $||x-y|| = r$. We denote by G_q^Δ the resulting almost complete graph with the implied edges and the coloring set L_q. When q runs over powers of odd primes, we obtain a family of the almost complete distance graphs $\{G_q^\Delta\}$. For each $r \in \mathbb{F}_q^*$, the single-colored distance graph $G_q^\Delta(r)$ can be considered as a sub-graph of the almost complete distance graph G_q^Δ with $q-1$ colors.

The main goal of this paper is a systematic study of the distance graph, including its diameter and pseudo-randomness properties. In the course of this investigation we prove sharp estimates for

intersections of algebraic and non-algebraic varieties in $\mathbb{F}_q^d$ and the existence of arbitrary k point configurations in sufficiently large subsets thereof.

1.1. Diameter of the distance graph and related objects. Consider the almost complete distance graph G_q^Δ with the coloring set $L_q = \{c_q^r : r \in \mathbb{F}_q^*\}$ defined as before. For each $r \in \mathbb{F}_q^*$, we also consider the c_q^r-colored distance graph $G_q^\Delta(r)$ defined as before. Given a fixed color c_q^r in L_q, we define the diameter of the c_q^r-colored distance graph $G_q^\Delta(r)$ as follows. Given vertices x, y in $G_q^\Delta(r)$, define a *path* of length k from x to y to be a sequences $\{x^1, \dots, x^{k+1}\}$, where x^js are distinct, $x^1 = x$, $x^{k+1} = y$, each x^j is a vertex in $G_q^\Delta(r)$ and x^i is connected to x^{i+1} by a c_q^r-colored edge for every $1 \leq i \leq k$. We say that a path from x to y is optimal if it is a path and its length is as small as possible. Define the *diameter* of $G_q^\Delta(r)$, denoted by $\mathbb{D}(G_q^\Delta(r))$, to be the largest length of the optimal path between any two vertices in $G_q^\Delta(r)$. We also define the diameter of the almost complete distance graph G_q^Δ, denoted by $\mathbb{D}(G_q^\Delta)$, as follows:

$$\mathbb{D}(G_q^\Delta) = \max_{r \in \mathbb{F}_q^*} \left(\mathbb{D}(G_q^\Delta(r)) \right).$$

Our first result in this direction is actually about more general families of graphs. For a fixed $d \geq 2$, consider a family $\{U_q\}$ where $U_q \subset \mathbb{F}_q^d$ and q is over all odd prime powers. We say that the family $\{U_q\}$ is Salem if there exists a uniform constant $C > 0$ such that for every $\xi \in \mathbb{F}_q^d \backslash \{(0, \cdots, 0)\}$,

$$|\widehat{U_q}(\xi)| \leq C q^{-d} |U_q|^{\frac{1}{2}}$$

with a uniform constant $C > 0$ independent of q, where the Fourier transform with respect to a non-trivial additive character χ is defined and briefly reviewed in (3.2) and the lines that follow. We shall also see below (Lemma 3.5) that the family $\{S_{t_q}\}$ of spheres S_{t_q} given by

$$S_{t_q} = \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2 = t_q \in \mathbb{F}_q^*\} \tag{1.1}$$

is Salem .

Given a set $U_q \subset \mathbb{F}_q^d$, define $G_q^{U_q}$ to the graph with vertices in $\mathbb{F}_q^d$ and two vertices, corresponding to $x, y \in \mathbb{F}_q^d$ connected by an edge if $x - y \in U_q$. We do not attach a coloring scheme in this context.

THEOREM 1.1. *Suppose that $\{U_q\}$ is Salem and $|U_q| \geq C q^{\frac{2d}{3}}$ with a sufficiently large constant $C > 0$. Then the diameter of $G_q^{U_q}$ is ≤ 3 provided that q is sufficiently large.*

COROLLARY 1.2. *Suppose that q is sufficiently large. For each $r \in \mathbb{F}_q^*$, the single-colored graph $G_q^\Delta(r)$ has diameter ≤ 3 if $d \geq 4$. In other words, we have $\mathbb{D}(G_q^\Delta) \leq 3$ if $d \geq 4$.*

The fact that the family of spheres with non-zero radii is Salem is proved in Lemma 3.5 below as is the fact that the number of elements of the sphere $S_r, r \neq 0$, in $\mathbb{F}_q^d$ is $\approx q^{d-1}$. It follows that the diameter of $G_q^\Delta(r)$ is ≤ 3 provided that $|S_r| \geq C q^{\frac{2d}{3}}$ with a sufficiently large constant $C > 0$. Since $|S_r| \approx q^{d-1}$ by Theorem 3.4, this holds if $d \geq 4$, which completes the proof of the corollary. We can do a bit better, however.

THEOREM 1.3. 1)*If $d \geq 4$, then $\mathbb{D}(G_q^\Delta) = 2$ for all $q \geq 3$.*
2) *Suppose that $d = 3$ and ψ is the quadratic character of $\mathbb{F}_q$. For each $r \in \mathbb{F}_q^*$ $q \geq 3$, we have*

$$\mathbb{D}(G_q^\Delta(r)) = \begin{cases} 2 & \text{if } \psi(-r) = 1 \\ 3 & \text{if } \psi(-r) = -1. \end{cases}$$

Namely, $\mathbb{D}(G_q^\Delta) = 3$.

3) *If* $d = 2$, *then we have*

$$\mathbb{D}(G_q^\Delta) = \begin{cases} 2 & \text{if } q = 3 \\ 3 & \text{if } q \neq 3, 5, 9, 13. \end{cases}$$

REMARK 1.4. The referee pointed out to us that the first and second item in Theorem 1.3 can be found in a recent result ([1]). We include proofs of these statements nevertheless for the sake of completeness. Recently, the authors ([10]) also studied the diameter of distance graphs in two dimensions. They proved that if $d = 2, q \equiv 1 \pmod 4$, then $\mathbb{D}(G_q^\Delta)$ is three or four. The third item in our Theorem 1.3 makes their work clear. Moreover, although aforementioned authors([10]) claimed that if $d = 2, q \equiv 3 \pmod 4$, then $\mathbb{D}(G_q^\Delta) = 3$, their argument does not justify their claim if $q = 3$. Let us see this. In the proof of Theorem 2 in [10] they claim that if $g(x) = (4 - x)x$, then there exist $u, v \neq 0 \in \mathbb{F}_q$ such that $g(u)$ is a square in $\mathbb{F}_q$ while $g(v)$ is not. However, $g(x)$ can not be -1 if $x \in \mathbb{F}_3^*$. Since $-1 \in \mathbb{F}_q$ is the unique non-square number, the claim is not true. In fact, $\mathbb{D}(G_3^\Delta) = 2$ as our proof of Theorem 1.3 says.

1.2. Kaleidoscopic pseudo-randomness. We say that the family of graphs $\{G_j\}_{j=1}^\infty$ with the set of colors

$$L_j = \{c_j^1, c_j^2, \dots, c_j^{|L_j|}\}$$

and the edge set $\mathcal{E}_j = \cup_{i=1}^{|L_j|} \mathcal{E}_j^i$, with $\mathcal{E}_j^i$ corresponding to the color c_j^i, is *kaleidoscopically pseudo-random* if there exist constants $C, C' > 0$ such that the following conditions are satisfied:

- $$|G_j| \to \infty \text{ as } j \to \infty. \tag{1.2}$$

- $$\frac{1}{C'}|\mathcal{E}_j^{i'}| \leq |\mathcal{E}_j^i| \leq C'|\mathcal{E}_j^{i'}| \text{ for all } 1 \leq i, i' \leq |L_j|. \tag{1.3}$$

- $\{G_j\}_{j=1}^\infty$ is asymptotically complete in the sense that

$$\lim_{j\to\infty} \frac{\binom{|G_j|}{2} - \sum_{i=1}^{|L_j|} |\mathcal{E}_j^i|}{\binom{|G_j|}{2}} = 0. \tag{1.4}$$

- If $1 \leq k - 1 \leq n$ and $L_j' \subset L_j$, with $|L_j'| \leq |L_j| - \binom{k}{2} + n$, then any sub-graph H of G_j of size

$$\geq C|G_j|^{\frac{k-1}{k}}|L_j|^{\frac{n}{k}}, \tag{1.5}$$

contains every possible sub-graph with k vertices and n edges with an arbitrary edge color distribution from L_j'.

See, for example, a survey by Krivelevich and Sudakov ([6]) for related notions of pseudo-random graphs, examples and applications. The first result of this paper is the following.

THEOREM 1.5. *If the dimension* d *is odd, then the above defined family of the almost complete distance graphs* ,$\{G_q^\Delta\}$, *is kaleidoscopically pseudo-random .*

This is our main graph-theoretic result. A somewhat stronger, though more technical, version of Theorem 1.5 is Theorem 1.8 below.

The proof shows that the constant C' in the definition of kaleidoscopic pseudo-randomness may be taken to be $(1+o(1))$ in this context. The constant C that the proof yields is exponential in the number of vertices.

We actually prove a little more as the arguments below indicate. We shall see that under the set of hypotheses corresponding to kaleidoscopic pseudo-randomness, every finite geometric configuration in $\mathbb{F}_q^d$ is realized. See [9] and [11] where related questions are studied using graph theoretic methods.

The first item in the definition of weak pseudo-randomness above (1.2) is automatic as the size of G_j is q^d, by construction. The second and third items, (1.3) and (1.4), respectively, are easy special cases of the following calculation. It is implicit in [8] or [4] and is a direct result from Theorem 3.4.

LEMMA 1.6. *For any $r \in \mathbb{F}_q$,*

$$|\{(x,y) \in \mathbb{F}_q^d \times \mathbb{F}_q^d : ||x-y|| = r\}| = \begin{cases} (2+o(1))\, q^{2d-1} & \text{if} \quad d=2, r=0 \\ (1+o(1))\, q^{2d-1} & \text{otherwise} \end{cases}$$

where $o(1)$ means that the quantity goes to 0 as $q \to \infty$.

We now ready to address the meat of our definition of weak pseudo-randomness, which is the fourth item (1.5).

DEFINITION 1.7. Given $L' \subset \mathbb{F}_q^*$ such that

$$|L'| \leq q - 1 - \binom{k}{2} + |J|,$$

and

$$J \subset \{1,2,\dots,k\}^2 \setminus \{(i,i) : 1 \leq i \leq k\},$$

a k-point J-configuration in E is a set of k points $\{x^1, x^2, \dots, x^k\} \subset E$ such that

$$\begin{cases} ||x^i - x^j|| = a_{ij} \in L' & \text{for all } (i,j) \in J \\ ||x^i - x^j|| \neq 0 & \text{for all } (i,j) \notin J \end{cases}$$

Denote the set of all k point J-configurations by $\mathtt{T}_k^J(E)$, which also depends on the choice of L' but our result below is independent of the choice L'.

The item (1.5) follows from the following geometric estimate.

THEOREM 1.8. *Let $E \subset \mathbb{F}_q^d$ and $d \geq 3$ is odd. Suppose that $1 \leq k-1 \leq n \leq d$ and*

$$|E| \geq C q^{d\left(\frac{k-1}{k}\right)} q^{\frac{n}{k}} \tag{1.6}$$

with a sufficiently large constant $C > 0$. Then for any

$$J \subset \{1,2,\dots,k\}^2 \setminus \{(i,i) : 1 \leq i \leq k\}$$

with $|J| = n$, we have

$$|\mathtt{T}_k^J(E)| = (1+o(1))|E|^k q^{-n}.$$

Our proof uses geometric and character sum machinery similar to the one used in [4], and the proof is similar to the proof of its earlier version in [2]. In the former paper, Theorem 1.8 is proved in the case $k = 2$ and $n = 1$, and in the latter article Theorem 1.8 is demonstrated in the case of general k and $n = \binom{k}{2}$. Thus Theorem 1.8 and, consequently, Theorem 1.5 may be viewed as filling the gap between these results.

2. Pseudo-arithmetic progressions

Consider a sequence of k points $P_1, P_2, \dots, P_k$ in $\mathbb{F}_q^d$ such that

$$||P_j - P_i|| = (j-i)^2 \text{ for } 1 \leq i \leq j \leq k.$$

We call such an ordered sequence of vectors *pseudo-arithmetic*. The following is a simple consequence of Theorem 1.8.

COROLLARY 2.1. *Suppose that $d \geq 3$ is odd and $E \subset \mathbb{F}_q^d$ such that $|E| \geq Cq^{\frac{k-1}{k}d}q^{\frac{k-1}{2}}$. Then E contains a pseudo-arithmetic progression of length k.*

In fact, Theorem 1.8 implies that E contains $\approx |E|^k q^{-\binom{k}{2}}$ pseudo-arithmetic progressions. It would be wonderful if these were actual arithmetic progressions. In fact, suppose it were true that every pseudo-arithmetic progression is an actual arithmetic progression in at least one coordinate. We could then take $E = A \times A \times \cdots \times A$ and conclude that if $|A| \geq Cq^{\frac{k-1}{k}}q^{\frac{k-1}{2d}}$, then A contains an arithmetic progression of length k, thus giving us a rather attractive version of Szemeredi's theorem in finite fields. The reality is very different, however. It is easy enough to construct examples of sequences which are pseudo-arithmetic but not actually arithmetic. Let $z \in \mathbb{F}_q^{d-1}$ such that $||z|| = z_1^2 + \cdots + z_{d-1}^2 = 0$. Let $P_j = (j, z) \in \mathbb{F}_q^d$. It is not hard to see that $||P_j - P_i|| = (j-i)^2$, so the sequence is pseudo-arithmetic, but it is certainly not in general an arithmetic progression.

What is somewhat more difficult is to construct examples of pseudo-arithmetic sequences that are not arithmetic progressions in any coordinate. One way is to take one of the pseudo-arithmetic progressions described in the previous paragraph and rotate it. For example, we may start out with the sequence

$$(0,0,0)\ (1,1,i)\ (2,0,0),$$

where $i = \sqrt{-1}$ and rotate it by an orthogonal matrix

$$\begin{pmatrix} t & -t & 0 \\ t & t & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

In order to have the determinant of this matrix equal to 1 we must have $t^2 = 1/2$. This equation has a solution in some fields and not others. Recall that we are also using $i = \sqrt{-1}$, an object which exists in some fields and not others. The simplest field where both objects exist is $\mathbb{Z}_{17}$. In this field we may take $t = 3$ and $i = 4$. We thus obtain the sequence

$$(0,0,0)\ (0,6,4)\ (6,6,0).$$

Observe that this sequence is not arithmetic in any coordinate.

3. Classical exponential sums and Fourier decay estimates

In this section, we collect the well-known facts related to exponential sums and apply them for Fourier decay estimates. Such facts shall be used in the next sections. Let χ be a non-trivial additive character of $\mathbb{F}_q$ and ψ a multiplicative character of $\mathbb{F}_q$ of order two, that is, $\psi(ab) = \psi(a)\psi(b)$ and $\psi^2(a) = 1$ for all $a, b \in \mathbb{F}_q^*$ but $\psi \not\equiv 1$. For each $a \in \mathbb{F}_q$, the Gauss sum $G_a(\psi, \chi)$ is defined by

$$G_a(\psi, \chi) = \sum_{s \in \mathbb{F}_q^*} \psi(s)\chi(as).$$

The magnitude of the Gauss sum is given by the relation

$$|G_a(\psi, \chi)| = \begin{cases} q^{\frac{1}{2}} & \text{if} \quad a \neq 0 \\ 0 & \text{if} \quad a = 0. \end{cases}$$

Remark 3.1. Here, and throughout this paper, we denote by χ and ψ the canonical additive character and the quadratic character of $\mathbb{F}_q$ respectively. Recall that if ψ is the quadratic character of $\mathbb{F}_q$, then $\psi(0) = 0$, and $\psi(s) = 1$ if s is a square number in $\mathbb{F}_q^*$ and $\psi(s) = -1$ otherwise.

The following theorem provided us of the explicit formula of the Gauss sum $G_1(\psi, \chi)$. For the nice proof, see ([7], P.199).

Theorem 3.2. *Let $\mathbb{F}_q$ be a finite field with $q = p^l$, where p is an odd prime and $l \in \mathbb{N}$. Then we have*

$$G_1(\psi, \chi) = \begin{cases} (-1)^{l-1} q^{\frac{1}{2}} & \text{if} \quad p = 1 \ (mod\, 4) \\ (-1)^{l-1} i^l q^{\frac{1}{2}} & \text{if} \quad p = 3 \ (mod\, 4). \end{cases}$$

In particular, we have

$$\sum_{s \in \mathbb{F}_q} \chi(as^2) = \psi(a) G_1(\psi, \chi) \quad \text{for any} \quad a \neq 0, \tag{3.1}$$

because the quadratic character ψ is the multiplicative character of $\mathbb{F}_q^*$ of order two. For the nice proof for this equality and the magnitude of Gauss sums, see [7] or [3]. As the direct application of the equality in (3.1), we have the following estimate.

Lemma 3.3. *For $\beta \in \mathbb{F}_q^k$ and $t \neq 0$, we have*

$$\sum_{\alpha \in \mathbb{F}_q^k} \chi(t\alpha \cdot \alpha + \beta \cdot \alpha) = \chi\left(\frac{\|\beta\|}{-4t}\right) \psi^k(t) \left(G_1(\psi, \chi)\right)^k,$$

where, here and throughout the paper, $\|\beta\| = \beta \cdot \beta$.

Proof. It follows that

$$\sum_{\alpha \in \mathbb{F}_q^k} \chi(t\alpha \cdot \alpha + \beta \cdot \alpha) = \prod_{j=1}^{k} \sum_{\alpha_j \in \mathbb{F}_q} \chi(t\alpha_j^2 + \beta_j \alpha_j).$$

Completing the square in α_j-variables, applying a change of variables, $\alpha_j + \frac{\beta_j}{2t} \to \alpha_j$, and using the inequality in (3.1), the proof is complete. □

Due to the explicit formula for the Gauss sum $G(\psi,\chi)$, we can count the number of the elements in the sphere $S_r \subset \mathbb{F}_q^d$ defined as before. The following theorem enables us to see the exact number of the elements of the sphere S_r which depends on the radius r, dimensions, and the size of the underlining finite field $\mathbb{F}_q$. This result can be found in [8].

THEOREM 3.4. *Let $S_r \subset \mathbb{F}_q^d$ be the sphere defined as in (1.1). For each $r \neq 0$, we have*

$$|S_r| = \begin{cases} q^{d-1} - q^{\frac{d-2}{2}} \psi\left((-1)^{\frac{d}{2}}\right) & \text{if } d \text{ is even} \\ q^{d-1} + q^{\frac{d-1}{2}} \psi\left((-1)^{\frac{d-1}{2}} r\right) & \text{if } d \text{ is odd.} \end{cases}$$

Moreover,

$$|S_0| = \begin{cases} q^{d-1} + (q-1) q^{\frac{d-2}{2}} \psi\left((-1)^{\frac{d}{2}}\right) & \text{if } d \text{ is even} \\ q^{d-1} & \text{if } d \text{ is odd.} \end{cases}$$

Recall that given a function $f : \mathbb{F}_q^m \to \mathbb{C}$, the Fourier transform with respect to a non-trivial additive character χ on $\mathbb{F}_q$ is given by the relation

$$\widehat{f}(\xi) = q^{-m} \sum_{x \in \mathbb{F}_q^m} \chi(-x \cdot \xi) f(x). \tag{3.2}$$

Also recall that

$$f(x) = \sum_{\xi \in \mathbb{F}_q^m} \chi(x \cdot \xi) \widehat{f}(\xi) \tag{3.3}$$

and

$$\sum_{\xi \in \mathbb{F}_q^m} \left|\widehat{f}(\xi)\right|^2 = q^{-m} \sum_{x \in \mathbb{F}_q^m} |f(x)|^2. \tag{3.4}$$

We shall also need the following estimates based on classical Gauss and Kloosterman sum bounds.

LEMMA 3.5. *With the notation above, for any $t \neq 0$, $\xi \neq (0,\dots,0)$ and q sufficiently large,*

$$|\widehat{S}_t(\xi)| \leq 2q^{-\frac{d+1}{2}}. \tag{3.5}$$

Moreover, if d is odd and $S_t \subset \mathbb{F}_q^d$, then

$$\left|\sum_{t \neq 0} \widehat{S}_t(\xi)\right| \leq q^{-\frac{d+1}{2}} \tag{3.6}$$

and

$$\widehat{S}_t(0,\dots,0) = q^{-d}|S_t| = (1+o(1))q^{-1}, \tag{3.7}$$

where $o(1)$ means that the quantity goes to 0 as $q \to \infty$ and here, throughout the paper, we identify a set with its characteristic function.

PROOF. For each $m \neq (0, \dots, 0)$, we have

$$\begin{aligned}\widehat{S}_t(m) =& q^{-d}q^{-1}\sum_s \sum_x \chi(-x\cdot m)\chi(s(||x||-t)) \\ =& q^{-d}q^{-1}\sum_{s\neq 0} \sum_x \chi(-x\cdot m)\chi(s(||x||-t)) \\ =& q^{-d-1}(G_1(\psi,\chi))^d \sum_{s\neq 0} \chi\left(\frac{||m||}{-4s} - st\right)\psi^d(s), \end{aligned} \tag{3.8}$$

where we used the orthogonality property of χ in the second line and Lemma 3.3 in the last line respectively. Thus, the estimate (3.5) follows from the following classical estimate due to Andre Weyl ([12]).

THEOREM 3.6. *Let*

$$K(a) = \sum_{s\neq 0} \chi(as^{-1}+s)\psi^d(s),$$

where ψ is the quadratic character on $\mathbb{F}_q^*$. Then for any $a \in \mathbb{F}_q$,

$$|K(a)| \leq 2\sqrt{q}.$$

We now turn our attention to (3.6). With (3.8) as the starting point, we sum this expression over $t \neq 0$ and obtain

$$\sum_{t\neq 0} \widehat{S}_t(m) = -q^{-d-1}(G_1(\psi,\chi))^d \sum_{s\neq 0} \chi\left(\frac{||m||}{-4s}\right)\psi^d(s).$$

Since d is odd, $\psi^d \equiv \psi$. We therefore see that this expression is

$$\leq q^{-\frac{d+1}{2}},$$

because the absolute value of the Gauss sum $G_1(\psi,\chi)$ is $q^{\frac{1}{2}}$ and the sum over $s \neq 0$ is just the Gauss sum. Finally, (3.7) follows easily from the definition of Fourier transform and Theorem 3.4. This completes the proof of Lemma 3.5. □

4. Proof of Theorem 1.1

We shall deduce Theorem 1.1 from the following estimate.

THEOREM 4.1. *$U, E, F \subset \mathbb{F}_q^d$ such that $\{U\}$ is Salem and*

$$|E||F| \geq C\frac{q^{2d}}{|U|}$$

with a sufficiently large constant $C > 0$. Then

$$\nu_U = \{(x,y) \in E \times F : x - y \in U\} > 0.$$

Taking Theorem 4.1 for granted, for a moment, Theorem 1.1 follows instantly. Indeed, take x, y with $x \neq y$ in $\mathbb{F}_q^d$. Let $E = U + x$ and $F = U + y$. It follows that $|E| = |F| = |U|$, so $|E||F| = |U|^2$. We conclude from Theorem 4.1 that if $|U| \geq Cq^{\frac{2d}{3}}$ with a sufficiently large constant $C > 0$, then there exists $x' \in U + x$ and $y' \in U + y$ such that $x' - y' \in U$. This implies that the diameter of G_q^U is at most three as desired.

To prove Theorem 4.1, observe that

$$\nu_U = \sum_{x,y} E(x)F(y)U(x-y)$$

$$= \sum_{x,y}\sum_{m} \widehat{U}(m)\chi((x-y)\cdot m)E(x)F(y)$$

$$= q^{2d}\sum_{m} \overline{\widehat{E}(m)}\widehat{F}(m)\widehat{U}(m)$$

$$= |E||F||U|q^{-d} + q^{2d}\sum_{m\neq(0,\dots,0)} \overline{\widehat{E}(m)}\widehat{F}(m)\widehat{U}(m) = I + II.$$

By assumption,

$$|II| \leq Cq^{2d}\cdot q^{-d}|U|^{\frac{1}{2}}\cdot \sum_{m\neq(0,\dots,0)} |\overline{\widehat{E}(m)}||\widehat{F}(m)|$$

$$\leq Cq^{d}|U|^{\frac{1}{2}}\left(\sum |\widehat{E}(m)|^2\right)^{\frac{1}{2}}\cdot\left(\sum |\widehat{F}(m)|^2\right)^{\frac{1}{2}}$$

$$= C|U|^{\frac{1}{2}}|E|^{\frac{1}{2}}|F|^{\frac{1}{2}}$$

by (3.4). Comparing I and II we complete the proof of Theorem 4.1.

5. Proof of Theorem 1.3

In this section, we provide the proof of Theorem 1.3. We first introduce the known explicit formula for the number of intersection points of two different spheres with the same non-zero radius. To observe intersection points of arbitrary two different spheres in $\mathbb{F}_q^d$ with the same non-zero radius, we just need to know $|S_r+(S_r+b)|$ for all $r\in\mathbb{F}_q^*$, $b\in\mathbb{F}_q^d\setminus\{(0,\dots,0)\}$. It is clear that $|S_r+(S_r+b)|$ is same as the number of common solutions in $\mathbb{F}_q^d$ of the equations

$$\begin{cases} x_1^2+\cdots+x_q^2 = r \\ b_1x_1+\cdots+b_dx_d = 2^{-1}\|b\|, \end{cases}$$

where $x=(x_1,\dots,x_d)\in\mathbb{F}_q^d$ and $b=(b_1,\dots,b_d)\neq(0,\dots,0)$. The number of common solutions is well known. For example, see ([7], P.341) where the statement of the following theorem is implicitly given. See also [5].

THEOREM 5.1. *For each $r\in\mathbb{F}_q^*$, and $b=(b_1,\dots,b_d)\in\mathbb{F}_q^d\setminus\{(0,\dots,0)\}, d\geq 2$, we have the following:*
If $\|b\|\neq 0$ and $r=4^{-1}\|b\|$, then

$$|S_r\cap(S_r+b)| = \begin{cases} q^{d-2} & \text{if } d \text{ is even} \\ q^{d-2}+q^{(d-3)/2}(q-1)\psi\left((-1)^{(d-1)/2}\|b\|\right) & \text{if } d \text{ is odd.} \end{cases}$$

If $\|b\|\neq 0$ and $r\neq 4^{-1}\|b\|$, then

$$|S_r\cap(S_r+b)| = \begin{cases} q^{d-2}+q^{(d-2)/2}\psi\left((-1)^{d/2}(4^{-1}\|b\|^2-r\|b\|)\right) & \text{if } d \text{ is even} \\ q^{d-2}-q^{(d-3)/2}\psi\left((-1)^{(d-1)/2}\|b\|\right) & \text{if } d \text{ is odd.} \end{cases}$$

Moreover, if $\|b\|=0$, then we have

$$|S_r\cap(S_r+b)| = \begin{cases} q^{d-2}-q^{(d-2)/2}\psi\left((-1)^{d/2}\right) & \text{if } d \text{ is even} \\ q^{d-2}+q^{(d-1)/2}\psi\left((-1)^{(d-1)/2}r\right) & \text{if } d \text{ is odd.} \end{cases}$$

Here, we recall that ψ is the quadratic character of $\mathbb{F}_q$, $\|b\| = b_1^2 + \cdots + b_d^2$, the sphere $S_r = \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2\}$ and $S_r + b = \{x + b \in \mathbb{F}_q^d : x \in S_r\}$.

To complete the proof of Theorem 1.3, we also need the following reduction.

LEMMA 5.2. *For each $a, b \in \mathbb{F}_q^d$ with $a \neq b$, we have*

$$|\{(x,y) \in (S_r + a) \times (S_r + b) : \|x - y\| = r \neq 0\}| = q^{-d}|S_r|^3 + I + II,$$

where

$$I = \begin{cases} q^{-3}\left(G_1(\psi,\chi)\right)^d & \text{if } d \text{ is even} \\ -q^{-3}\left(G_1(\psi,\chi)\right)^{d+3}\psi(r) & \text{if } d \text{ is odd,} \end{cases}$$

(5.1)

$$II = q^{-3}\left(G_1(\psi,\chi)\right)^{2d} \sum_{\substack{u,v,w\neq 0 \\ :u-v+w\neq 0}} \psi^d(uvw)\psi^d(-(u-v+w))\chi\left(\frac{\|a-b\|}{u-v+w}\right)\chi\left(-r\left(\frac{1}{u}-\frac{1}{v}+\frac{1}{w}\right)\right).$$

PROOF. For each $a, b \in \mathbb{F}_q^d$ with $a \neq b$,we have

$$\begin{aligned} &|\{(x,y) \in (S_r + a) \times (S_r + b) : \|x - y\| = r \neq 0\}| \\ =&\sum_{x,y} S_r(x)S_r(y)S_r(x-y+a-b) \\ =&\sum_{x,y}\sum_{m} S_r(x)S_r(y)\chi\left((x-y+a-b)\cdot m\right)\widehat{S_r}(m) \\ =&q^{-d}|S_r|^3 + q^{2d}\sum_{m\neq(0,\ldots,0)} \chi((a-b)\cdot m)\widehat{S_r}(m)|\widehat{S_r}(m)|^2. \end{aligned}$$

Thus, it suffices to show that

$$q^{2d}\sum_{m\neq(0,\ldots,0)} \chi((a-b)\cdot m)\widehat{S_r}(m)|\widehat{S_r}(m)|^2 = I + II \tag{5.2}$$

where I and II are defined as in statement of Theorem 5.2. By (3.8), recall that if $m \neq (0, \cdots, 0)$, then $\widehat{S_r}(m)$ is given by

$$\widehat{S_r}(m) = q^{-d-1}(G_1(\psi,\chi))^d \sum_{s\neq 0} \chi\left(\frac{||m||}{-4s} - sr\right)\psi^d(s).$$

Plugging this into (5.2), the left-hand side value in (5.2) is given by

$$q^{-3}\left(G_1(\psi,\chi)\right)^d \sum_{m\neq(0,\ldots,0)}\sum_{u,v,w\neq 0} \psi^d(uvw)\chi((a-b)\cdot m)\chi\left(\frac{\|m\|}{-4}\left(\frac{1}{u}-\frac{1}{v}+\frac{1}{w}\right)\right)\chi(-r(u-v+w))$$

$$= q^{-3}\left(G_1(\psi,\chi)\right)^d \sum_{m}\sum_{u,v,w\neq 0} \psi^d(uvw)\chi((a-b)\cdot m)\chi\left(\frac{\|m\|}{-4}\left(\frac{1}{u}-\frac{1}{v}+\frac{1}{w}\right)\right)\chi(-r(u-v+w))$$

$$-q^{-3}\left(G_1(\psi,\chi)\right)^d \sum_{u,v,w\neq 0} \psi^d(uvw)\chi(-r(u-v+w)) = A + B.$$

To complete the proof, it is enough to show that $B = I$ and $A = II$. The value B above is given by

$$\begin{cases} q^{-3}\left(G_1(\psi,\chi)\right)^d & \text{if} \quad d \quad \text{is even} \\ -q^{-3}\left(G_1(\psi,\chi)\right)^{d+3}\psi(r) & \text{if} \quad d \quad \text{is odd} \end{cases} \tag{5.3}$$

This easily follows from properties of the quadratic character ψ, definition of the Gauss sum $G_1(\psi,\chi)$, and $\sum\limits_{s\neq 0}\chi(rs) = -1$ for $r \neq 0$. Thus, $B = I$. It remains to show that $A = II$. Applying a change of variables, $u^{-1} \to u, v^{-1} \to v, w^{-1} \to w$, the value A above is given by

$$q^{-3}\left(G_1(\psi,\chi)\right)^d \sum_m \sum_{u,v,w\neq 0} \psi^d(uvw)\chi((a-b)\cdot m)\chi\left(\frac{\|m\|}{-4}(u-v+w)\right)\chi\left(-r\left(\frac{1}{u}-\frac{1}{v}+\frac{1}{w}\right)\right).$$

Since $a \neq b$, the sum over $m \in \mathbb{F}_q^d$ vanishes if $u-v+w = 0$. Thus we may assume that $u-v+w \neq 0$. Therefore using Lemma 3.3, the value A above takes the form

$$q^{-3}\left(G_1(\psi,\chi)\right)^{2d} \sum_{\substack{u,v,w\neq 0 \\ :u-v+w\neq 0}} \psi^d(uvw)\psi^d(-(u-v+w))\chi\left(\frac{\|a-b\|}{u-v+w}\right)\chi\left(-r\left(\frac{1}{u}-\frac{1}{v}+\frac{1}{w}\right)\right),$$

where we used $\psi(4^{-1}) = 1$, because 4 is the square number and ψ is the quadratic character of $\mathbb{F}_q^*$. Thus, $A = II$. This completes the proof.

□

5.1. The Proof of the first and second part of Theorem 1.3. We first prove the first part of Theorem 1.3. From Theorem 5.1, we see that if $d \geq 4$,then for each $r \in \mathbb{F}_q^*$, $|S_r \cap (S_r + b)| \geq 1$ for all $b \in \mathbb{F}_q^d$ and for all $q \geq 3$. This implies that if $d \geq 4$, then two different spheres in $\mathbb{F}_q^d$ with the same non-zero radius $t \neq 0$ always intersect. Thus, the first part of Theorem 1.3 immediately follows , because it is clear that the diameter of G_q^Δ is not one. We now prove the second part of Theorem 1.3. Suppose $d = 3$ and $b \in \mathbb{F}_q^d \setminus \{(0,\ldots,0)\}$. Then, Theorem 5.1 says that for each $r \neq \mathbb{F}_q^*$,

$$|S_r \cap (S_r + b)| = \begin{cases} q + (q-1)\psi((-1)\|b\|) & \text{if} \quad \|b\| \neq 0, \ r = 4^{-1}\|b\| \\ q - \psi((-1)\|b\|) & \text{if} \quad \|b\| \neq 0, \ r \neq 4^{-1}\|b\| \\ q + q\psi(-r) & \text{if} \quad \|b\| = 0. \end{cases} \tag{5.4}$$

Thus if $\psi(-r) = 1$, then $|S_r \cap (S_r + b)| \geq 1$ for all $q \geq 3$ and for all $b \in \mathbb{F}_q^3$. This implies that if $\psi(-r) = 1$, then $\mathbb{D}(G_q^\Delta(r)) = 2$ for all $q \geq 3$. On the other hand, if $\psi(-r) = -1$, then (5.4) shows that $|S_r \cap (S_r + b)| = 0$ if $\|b\| = 0$. Thus, there exist disjoint two different circles with the same non-zero radius and so the diameter of $G_q^\Delta(r)$ can not be two. In order to complete the proof of the second part of Theorem 1.3, it therefore suffices to show that

$$\mathbb{D}(G_q^\Delta(r)) \leq 3 \quad \text{for all} \quad r \in \mathbb{F}_q^*, \ q \geq 3.$$

This follows from the following claim: for every $a, b \in \mathbb{F}_q^3$ with $a \neq b, r \in \mathbb{F}_q^*$ and $q \geq 3$, we have

$$|\{(x,y) \in (S_r + a) \times (S_r + b) : \|x-y\| = r \neq 0\}| > 0.$$

Let us prove the claim. Since $d = 3$, Theorem 5.2 yields the following:

$$|\{(x,y) \in (S_r + a) \times (S_r + b) : \|x-y\| = r \neq 0\}| \geq q^{-3}|S_r|^3 - |I| - |II|, \tag{5.5}$$

where I and II are given as in Theorem 5.2. From Theorem 3.4, we see that if $d = 3$ and $r \neq 0$, then

$$|S_r| \geq q^2 - q, \tag{5.6}$$

and using the fact that the absolute value of the Gauss sum $G_1(\psi, \chi)$ is exactly $q^{\frac{1}{2}}$, we see

$$|I| = 1. \tag{5.7}$$

In order to estimate the value $|II|$, use the trivial estimation along with the bound of the Gauss sum, and then we obtain

$$|II| \leq \sum_{u,v,w\neq 0: u-v+w\neq 0} 1,$$

We observe the following:

$$\sum_{u,v,w\neq 0: u-v+w\neq 0} 1 = (q-1)^2 + (q-1)(q-2)^2. \tag{5.8}$$

This follows from the following observation: if we fix $u \neq 0$ which has $q-1$ choices, then we may choose $v \neq 0$ such that either $u = v$ or $u \neq v$. In case $u = v$, v has only one choice which depends on the choice of u and then we can choose $w \neq 0$ which has $q-1$ choices with $u - v + w \neq 0$. On the other hand, if we choose $v \neq 0$ with $u \neq v$, which has $q-2$ choices, then we can have $q-2$ choices for $w \neq 0$ such that $u - v + w \neq 0$. Thus, 5.8 holds. From (5.6), (5.7), and (5.8) along with (5.5), we obtain that if $d = 3$, then

$$\begin{aligned} |\{(x,y) \in (S_r + a) \times (S_r + b) : \|x - y\| = r \neq 0\}| &\geq q^{-3}(q^2-q)^3 - 1 - (q-1)^2 - (q-1)(q-2)^2 \\ &= (q-1)\left(q - 2 - (q-1)^{-1}\right), \end{aligned}$$

which is greater than zero if $q \geq 3$. This proves that the diameter of G_q^{Δ} in three dimension is less than equal to three. Thus, we complete the proof of the second part of Theorem 1.3.

5.2. The proof of the third part of Theorem 1.3. We first observe from Theorem 5.1 that if $d = 2$, then for each $r \in \mathbb{F}_q^*$,

$$|S_r \cap (S_r + b)| = \begin{cases} 1 & \text{if} \quad \|b\| \neq 0, \ r = 4^{-1}\|b\| \\ 1 + \psi((-1)(4^{-1}\|b\|^2 - r\|b\|)) & \text{if} \quad \|b\| \neq 0, \ r \neq 4^{-1}\|b\| \\ 1 - \psi(-1) & \text{if} \quad \|b\| = 0. \end{cases} \tag{5.9}$$

Case A: [The diameter of G_3^{Δ} is exactly two in two dimensions]: Suppose $d = 2, q = 3$. We shall show that $\mathbb{D}(G_3^{\Delta}) = 2$. It suffices to show that for every $r \in \mathbb{F}_3^*$, we have

$$|S_r \cap (S_r + b)| \geq 1 \quad \text{for all } b \in \mathbb{F}_3^2 \setminus \{(0,0)\}.$$

However, since $-1 \in \mathbb{F}_3$ is not a square number, $\psi(-1) = -1$. Using this fact along with (5.9), it is enough to show that for all $r \in \mathbb{F}_3^*$ and $b \in \mathbb{F}_3^2 \setminus \{(0,0)\}$ such that $\|b\| \neq 0$ and $r \neq 4^{-1}\|b\|$, we have

$$\psi((-1)(4^{-1}\|b\|^2 - r\|b\|)) = 1. \tag{5.10}$$

Since $4^{-1} \equiv 1 \in \mathbb{F}_3$, and $r \neq 4^{-1}\|b\|$, we see that $r \neq \|b\|$. Moreover, both r and $\|b\|$ only takes 1 or 2 in $\mathbb{F}_3$, because $\|b\| \neq 0, r \in \mathbb{F}_q^*$. Thus, if $r = 1$, then $\|b\| = 2$. In this case, $\psi((-1)(4^{-1}\|b\|^2 - r\|b\|)) = \psi(1) = 1$. On the other hand, if $r = 2$, then $\|b\| = 1$. Thus, we also see that $\psi((-1)(4^{-1}\|b\|^2 - r\|b\|)) = \psi(1) = 1$. This completes the proof.

Case B: [The diameter of G_q^{Δ} in two dimensions is greater than two if $q \neq 3$]: Here, we show that

$$\mathbb{D}(G_q^{\Delta}) \neq 2 \quad \text{if} \quad q \neq 3,\ d = 2. \tag{5.11}$$

If $q \equiv 1\ mod(4)$, then $\psi(-1) = 1$, because $-1 \in \mathbb{F}_q$ is a square number. In this case, (5.9) says that there exist two disjoint circles with the same non-zero radius. Thus, (5.11) holds if $q \equiv 1\ mod(4)$. We now consider the case where $q \equiv 3\ mod(4)$. From (5.9), we see that for each $r \in \mathbb{F}_q^*$,

$$|S_r \cap (S_r + b)| = 1 + \psi\left((-1)(4^{-1}\|b\|^2 - r\|b\|)\right) \quad \text{for all} \quad b \in \mathbb{F}_q^2 \quad \text{with} \quad \|b\| \neq 0,\ 4r.$$

In the case when $q \equiv 3\ mod(4)$, the claim (5.11) therefore holds if we can show that for each $r \in \mathbb{F}_q^*$, there exists $b \in \mathbb{F}_q^2$ with $\|b\| \neq 0,\ 4r$ such that

$$\psi\left((-1)(4^{-1}\|b\|^2 - r\|b\|)\right) = -1. \tag{5.12}$$

By contradiction, if we assume that (5.12) is not true, then we must have that for all $b \in \mathbb{F}_q^2$ with $\|b\| \neq 0, 4r$,

$$\psi\left((-1)(4^{-1}\|b\|^2 - r\|b\|)\right) \neq -1. \tag{5.13}$$

Since ψ is the quadratic character of $\mathbb{F}_q$, we see that $\psi(s) = \pm 1$ for $s \neq 0$ and $\psi(0) = 0$. Thus, (5.13) implies that for all $b \in \mathbb{F}_q^2$ with $\|b\| \neq 0, 4r$,

$$\psi\left((-1)(4^{-1}\|b\|^2 - r\|b\|)\right) = 1, \tag{5.14}$$

where we also used the fact that $\psi\left((-1)(4^{-1}\|b\|^2 - r\|b\|)\right) \neq 0$ if $\|b\| \neq 0, 4r$. From Theorem 3.4, we see that for each $s \in \mathbb{F}_q$, there exists $b \in \mathbb{F}_q^2$ such that $\|b\| = s$. Using this along with (5.14), we must have

$$\sum_{s \in \mathbb{F}_q \setminus \{0, 4r\}} \psi\left((-1)(4^{-1}s^2 - rs)\right) = (q-2).$$

Since $\psi(0) = 0$, we see that $\psi(\left((-1)(4^{-1}s^2 - rs)\right) = 0$ for $s = 0, 4r$. Thus, above equality is same as the following:

$$\sum_{s \in \mathbb{F}_q} \psi\left((-1)(4^{-1}s^2 - rs)\right) = (q-2).$$

However, this is impossible if $q \geq 5$ due to the following theorem (see [7], P.225).

THEOREM 5.3. *Let ψ be a multiplicative character of $\mathbb{F}_q$ of order $k > 1$ and let $g \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree that is not an $k-$th power of a polynomial. Let e be the number of distinct roots of g in its splitting field over $\mathbb{F}_q$. Then for every $t \in \mathbb{F}_q$ we have*

$$\left|\sum_{s \in \mathbb{F}_q} \psi(tg(s))\right| \leq (e-1)q^{1/2}.$$

To see this, note from Theorem 5.3 that we must have

$$\left|\sum_{s \in \mathbb{F}_q} \psi\left((-1)(4^{-1}s^2 - rs)\right)\right| \leq q^{1/2},$$

where we used $r \neq 0$. We finish proving that $\mathbb{D}(G_q^{\Delta}) \neq 2$ if $q \neq 3$ $d = 2$.

Case C: [In two dimensions, the diameter of G_q^{Δ} is three unless q is $3, 5, 9,$ or 13]: Suppose that $d = 2$ and $q \neq 3, 5, 9, 13$. We shall prove that the diameter of $\mathbb{G}_q^{\Delta}$ is exactly three

unless $q = 3, 5, 9, 13$. Since we has already seen that the diameter of $\mathbb{D}(G_q^{\Delta})$ is not two for $q \neq 3$, and the diameter of $\mathbb{D}(G_3^{\Delta})$ is two, it suffices to show that the diameter of $\mathbb{D}(G_q^{\Delta})$ is less than equal to three for $q \neq 5, 9, 13$. However, this follows from the following theorem:

THEOREM 5.4. *For each $r \in \mathbb{F}_q^*$, if $a, b \in \mathbb{F}_q^2$ with $a \neq b$, and $q \neq 5, 9, 13$, then we have*

$$|\{(x, y) \in (S_r + a) \times (S_r + b) : \|x - y\| = r \neq 0\}| > 0.$$

PROOF. If $d = 2$, then $\psi^d(s) = 1$ for $s \neq 0$, because ψ is the multiplicative character of $\mathbb{F}_q$. Therefore, Theorem 5.2 yields the following estimation:

$$|\{(x, y) \in (S_r + a) \times (S_r + b) : \|x - y\| = r \neq 0\}| = q^{-2}|S_r|^3 + q^{-3}\left(G_1(\psi, \chi)\right)^2 + M, \tag{5.15}$$

where M is given by

$$M = q^{-3}\left(G_1(\psi, \chi)\right)^4 \sum_{\substack{u,v,w \neq 0 \\ :u-v+w \neq 0}} \chi\left((u - v + w)^{-1}\|a - b\|\right) \chi\left(-r(u^{-1} - v^{-1} + w^{-1})\right).$$

Fix $u \neq 0$. Putting $u^{-1}v = s, u^{-1}w = t$, we see that

$$M = q^{-3}\left(G_1(\psi, \chi)\right)^4 \sum_{u \neq 0} \sum_{s \neq 0} \sum_{t \neq 0 : s - t \neq 1} \chi\left(-r\left(\frac{1}{u} + \frac{s - t}{ust}\right)\right) \chi\left(\frac{\|a - b\|}{u(1 - s + t)}\right).$$

Using a change of variables, $u^{-1} \to u$, we have

$$M = q^{-3}\left(G_1(\psi, \chi)\right)^4 \sum_{u \neq 0} \sum_{s \neq 0} \sum_{t \neq 0 : s - t \neq 1} \chi\left(\left(-r + \frac{-rs + rt}{st} + \frac{\|a - b\|}{1 - s + t}\right) u\right).$$

Note that the sum over $u \neq 0$ is -1 if $-r + (-rs + rt)/st + \|a - b\|/(1 - s + t) \neq 0$, and $q - 1$ otherwise. Thus, the value M can be written by

$$\begin{aligned}
M =& - q^{-3}\left(G_1(\psi, \chi)\right)^4 \sum_{s \neq 0} \sum_{\substack{t \neq 0 : s - t \neq 1 \\ -r + (-rs + rt)/st + \|a - b\|/(1 - s + t) \neq 0}} 1 \\
&+ q^{-3}\left(G_1(\psi, \chi)\right)^4 (q - 1) \sum_{s \neq 0} \sum_{\substack{t \neq 0 : s - t \neq 1 \\ -r + (-rs + rt)/st + \|a - b\|/(1 - s + t) = 0}} 1 \\
=& q^{-2}\left(G_1(\psi, \chi)\right)^4 \sum_{s \neq 0} \sum_{\substack{t \neq 0 : s - t \neq 1 \\ -r + (-rs + rt)/st + \|a - b\|/(1 - s + t) = 0}} 1 \\
&- q^{-3}\left(G_1(\psi, \chi)\right)^4 \sum_{s \neq 0} \sum_{t \neq 0 : s - t \neq 1} 1.
\end{aligned}$$

We now claim that

$$\sum_{s \neq 0} \sum_{t \neq 0 : s - t \neq 1} 1 = (q - 2)^2 + (q - 1).$$

To see this, we write the term above into two parts as follows.

$$\sum_{s \neq 0} \sum_{t \neq 0 : s - t \neq 1} 1 = \sum_{s \neq 0, 1} \sum_{t \neq 0 : s - t \neq 1} 1 + \sum_{t \neq 0 : 1 - t \neq 1} 1.$$

Then, it is clear that

$$\sum_{t \neq 0 : 1 - t \neq 1} 1 = q - 1.$$

On the other hand, we see that

$$\sum_{s\neq 0,1}\sum_{t\neq 0: s-t\neq 1} 1 = (q-2)^2,$$

because whenever we fix $s \neq 0,1$ which has $q-2$ choices, we have $q-2$ choices of $t \neq 0$ with $s-t \neq 1$. By this, the claim is complete. Thus the term M is given by

$$M = q^{-2}\left(G_1(\psi,\chi)\right)^4 \sum_{s\neq 0} \sum_{\substack{t\neq 0: s-t\neq 1 \\ -r+(-rs+rt)/st+\|a-b\|/(1-s+t)=0}} 1$$

$$-q^{-3}\left((q-2)^2+(q-1)\right)\left(G_1(\psi,\chi)\right)^4.$$

From this and 5.15, we obtain that

$$\begin{aligned}&|\{(x,y)\in (S_r+a)\times(S_r+b) : \|x-y\| = r\neq 0\}| \\ &= q^{-2}|S_r|^3 + q^{-3}\left(G_1(\psi,\chi)\right)^2 - q^{-3}\left((q-2)^2+(q-1)\right)\left(G_1(\psi,\chi)\right)^4 \\ &\quad + q^{-2}\left(G_1(\psi,\chi)\right)^4 \sum_{s\neq 0} \sum_{\substack{t\neq 0: s-t\neq 1 \\ -r+(-rs+rt)/st+\|a-b\|/(1-s+t)=0}} 1.\end{aligned}$$

By Theorem 3.4 and Theorem 3.2, we see that $|S_r| = q-\psi(-1)$ if $d=2$, and $G^4(\psi,\chi) = q^2$ respectively. Thus, we aim to show that the following value is positive.

$$\begin{aligned}&|\{(x,y)\in (S_r+a)\times(S_r+b) : \|x-y\| = r\neq 0\}| \\ &= q^{-2}(q-\psi(-1))^3 + q^{-3}\left(G_1(\psi,\chi)\right)^2 - q^{-1}\left(q^2-3q+3\right) \\ &\quad + \sum_{s\neq 0} \sum_{\substack{t\neq 0: s-t\neq 1 \\ -r+(-rs+rt)/st+\|a-b\|/(1-s+t)=0}} 1.\end{aligned} \tag{5.16}$$

Case I : Suppose that $q = p^l$ for some odd prime $p \equiv 3\,(mod\,4)$ with l odd. Then $q \equiv 3\,(mod\,4)$, which means that -1 is not a square number in $\mathbb{F}_q$ and so $\psi(-1) = -1$. We also note from Theorem 3.2 that $G^2(\psi,\chi) = -q$. Thus the value in (5.16) can be estimated as follows.

$$\begin{aligned}&|\{(x,y)\in (S_r+a)\times(S_r+b) : \|x-y\| = r\neq 0\}| \\ &\geq q^{-2}(q+1)^3 - q^{-2} - q^{-1}\left(q^2-3q+3\right) = 6\end{aligned}$$

which is greater than zero. This completes the proof of Theorem 5.4 in the case when $q \equiv 3 \pmod 4$.

Case II: Suppose that $q = p^l$ for some odd prime $p \equiv 3\,(mod\,4)$ with l even, or $q = p^l$ with $p \equiv 1\,(mod\,4)$. Then, $q \equiv 1\,(mod\,4)$, which implies that -1 is a square number in $\mathbb{F}_q$ and so $\psi(-1) = 1$. Moreover, $G^2(\psi,\chi) = q$ by Theorem 3.2. From these observations, the value in (5.16) is given by

$$\begin{aligned}&|\{(x,y)\in (S_r+a)\times(S_r+b) : \|x-y\| = r\neq 0\}| \\ &= q^{-2}(q-1)^3 + q^{-2} - q^{-1}(q^2-3q+3) + R(a,b,r) = R(a,b,r)\end{aligned}$$

where

$$R(a,b,r) = \sum_{s\neq 0}\sum_{t\neq 0: s-t\neq 1, T(s,t,a,b,r)=0} 1$$

with

$$T(s,t,a,b,r) = -r + (-rs+rt)/st + \|a-b\|/(1-s+t).$$

To complete the proof, it suffices to show that $R(a,b,r) > 0$.

Case II-1: Suppose that $\|a-b\| = 0$. Then, we have

$$R(a,b,r) = \sum_{s\neq 0} \sum_{\substack{t\neq 0: s-t\neq 1,\\ -st-s+t=0}} 1.$$

If $q \neq 3^l (Char\, \mathbb{F}_q \neq 3)$ for $l \in \mathbb{N}$, then it is clear that $R(a,b,r) \geq 1$, because if we choose $s=-1, t=-2^{-1}$ then $s-t \not\equiv 1$ and $-st-s+t \equiv 0$. Thus, we may assume that $q = 3^l$ with l even. Since each finite field $\mathbb{F}_{3^2}$ can be considered as a subfield of any finite field $\mathbb{F}_{3^l}$ with l even up to isomorphism, it is enough to show that $R(a,b,r) \geq 1$ for a fixed finite field $\mathbb{F}_{3^2}$ with 9 elements. Consider the following finite field $\mathbb{F}_{3^2}$ with 9 elements.

$$\mathbb{F}_{3^2} \cong \mathbb{Z}_3[i]/(i^2+1) \cong \{\alpha+\beta i : \alpha, \beta \in \mathbb{Z}_3\},$$

where $i^2 = -1$. Taking $s = i, t = \frac{i-1}{2}$, we see that $s-t \not\equiv 1$ and $-st-s+t \equiv 0$. Thus we conclude that $R(a,b,r) \geq 1$ as desired.

Case II-2: Assume that $\|a-b\| \neq 0$. Letting $c = \frac{\|a-b\|}{r} \neq 0$, we have

$$R(a,b,r) = \sum_{s\neq 0} \sum_{t\neq 0: s-t\neq 1, T^*(s,t,c)=0} 1$$

where $T^*(s,t,c)$ is defined by

$$\begin{aligned} T^*(s,t,c) =& (c-3)st + s^2t - st^2 - s + t + s^2 + t^2 \\ =& (t+1)s^2 + \big(t(c-3) - t^2 - 1\big)\, s + t + t^2. \end{aligned} \tag{5.17}$$

Splitting $R(a,b,r)$ into two parts as below and using the simple properties of summation notation, $R(a,b,r)$ takes the following forms.

$$\begin{aligned} R(a,b,r) =& \sum_{s\neq 0,1} \sum_{t\neq 0: s-t\neq 1, T^*(s,t,c)=0} 1 + \sum_{t\neq 0: c-1=0} 1 \\ =& \sum_{s\neq 0,1} \sum_{t\neq 0: T^*(s,t,c)=0} 1 - \sum_{s\neq 0,1: c=0} 1 + \sum_{t\neq 0: c-1=0} 1 \\ =& \sum_{s\neq 0} \sum_{t\neq 0: T^*(s,t,c)=0} 1 - \sum_{t\neq 0: c-1=0} 1 - \sum_{s\neq 0,1: c=0} 1 + \sum_{t\neq 0: c-1=0} 1 \\ =& \sum_{s\neq 0} \sum_{t\neq 0: T^*(s,t,c)=0} 1, \end{aligned}$$

where we used $\sum_{s\neq 0,1:c=0} 1 = 0$, because $c \neq 0$. We have

$$\begin{aligned} R(a,b,r) =& q^{-1} \sum_{s,t\neq 0} \sum_{k} \chi\left(kT^*(s,t,c)\right) \\ =& q^{-1} \sum_{s,t\neq 0} \sum_{k\neq 0} \chi\left(kT^*(s,t,c)\right) + q^{-1}(q-1)^2 \\ =& q^{-1} \sum_{t,k\neq 0} \sum_{s\in\mathbb{F}_q} \chi\left(kT^*(s,t,c)\right) - q^{-1} \sum_{t,k\neq 0} \chi(tk+t^2k) + q^{-1}(q-1)^2 \\ =& q^{-1} \sum_{t,k\neq 0} \sum_{s\in\mathbb{F}_q} \chi\left(kT^*(s,t,c)\right) - q^{-1} + q^{-1}(q-1)^2, \end{aligned} \tag{5.18}$$

where the last equality follows from the following observation.

$$\begin{aligned} \sum_{t,k\neq 0} \chi(tk+t^2k) =& \sum_{t\neq 0,-1} \sum_{k\neq 0} \chi(t(t+1)k) + \sum_{k\neq 0} 1 \\ =& -(q-2) + (q-1) = 1. \end{aligned}$$

Splitting the sum in (5.18) into two parts as below, we obtain that

$$R(a,b,r) = q^{-1} \sum_{t\neq 0,-1} \sum_{k\neq 0} \sum_{s\in\mathbb{F}_q} \chi\left(kT^*(s,t,c)\right) + q^{-1} \sum_{k\neq 0} \sum_{s\in\mathbb{F}_q} \chi\left((1-c)ks\right) - q^{-1} + q^{-1}(q-1)^2.$$

By the orthogonality relations for non-trivial additive character χ, the second term above is given by

$$q^{-1} \sum_{k\neq 0} \sum_{s\in\mathbb{F}_q} \chi\left((1-c)ks\right) = (q-1)\,\delta_0(1-c) \geq 0,$$

where $\delta_0(u) = 1$ if $u = 0$, and 0 otherwise. In order to estimate the first term above, recall from (5.17) that

$$kT^*(s,t,c) = k(t+1)s^2 + k\left(t(c-3) - t^2 - 1\right)s + kt + kt^2$$

and then apply the complete square methods (see Lemma 3.3). It follows that

$$R(a,b,r) \geq q^{-1} G_1(\psi,\chi) \sum_{t\neq 0,-1} \sum_{k\neq 0} \psi\left((t+1)k\right) \chi\left(\frac{k\left((c-3)t - t^2 - 1\right)^2}{-4(t+1)}\right) \chi(t(t+1)k) + q - 2.$$

Using a change of variables, $\frac{k}{4(t+1)} \to k$ and the fact that $\psi\left(4(t+1)^2\right) = 1$, we see that

$$R(a,b,r) \geq q^{-1} G_1(\psi,\chi) \sum_{t\neq 0,-1} \sum_{k\neq 0} \psi(k)\chi(g(t,c)k) + q - 2$$

where $g(t,c)$ is given by

$$g(t,c) = 4t(t+1)^2 - \left((c-3)t - t^2 - 1\right)^2.$$

Note that the sum over $k \neq 0$ is zero if $g(t,c) = 0$. Thus, we may assume that $g(t,c) \neq 0$. Thus, using a change of variables, $g(t,c)k \to k$, we see that

$$R(a,b,r) \geq q^{-1} \left(G_1(\psi,\chi)\right)^2 \sum_{t\neq 0,-1 : g(t,c)\neq 0} \psi(g(t,c)) + q - 2, \tag{5.19}$$

where we used that $\psi(s) = \psi(s^{-1})$ for $s \neq 0$. Here, recall that we has assumed that $q = p^l$ for some odd prime $p \equiv 3\,(mod\,4)$ with l even, or $q = p^l$ with $p \equiv 1\,(mod\,4)$. By Theorem 3.2,

we therefore see that $(G_1(\psi,\chi))^2 = q$. From this and (5.19), we see that $R(a,b,r) = 0$ only if $\sum_{t\neq 0,-1:g(t,c)\neq 0} \psi(g(t,c)) = -(q-2)$. Since ψ is the quadratic character of $\mathbb{F}_q$, the number $\psi(g(t,c))$ takes $+1$ or -1, because $\psi(s) = \pm 1$ for $s \neq 0$. Thus if $\sum_{t\neq 0,-1:g(t,c)\neq 0} \psi(g(t,c)) = -(q-2)$ happens, then it must be true that $\psi(g(t,c)) = -1$ for all $t \neq 0,-1$. This implies that $g(t,c)$ is not a square number for all $t \neq 0,-1$, and the following estimate holds

$$\left|\sum_{t\in\mathbb{F}_q} \psi(g(t,c))\right| \geq |-(q-2)| - 2 = q-4. \tag{5.20}$$

However, this is an impossible result if $q \geq 17$, because (5.20) violates the conclusion of Theorem 5.3. To see this, note from Theorem 5.3 that it must be true that

$$\left|\sum_{t\in\mathbb{F}_q} \psi(g(t,c))\right| \leq 3q^{\frac{1}{2}},$$

because $g(t,c)$ is the polynomial of degree four in terms of t variables. Thus, if $q \geq 17$, then the inequality in (5.20) is not true and so we conclude that if $q \geq 17$ and $q \equiv 1 \ (mod 4)$(assumption of **Case II**), then

$$|\{(x,y) \in (S_r + a) \times (S_r + b) : \|x-y\| = r \neq 0\}| = R(a,b,r) > 0.$$

Combining this and the result of **Case I**, the proof of Theorem 5.4 is complete. □

6. Proof of the "kaleidoscopic" result (Theorem 1.8)

.

Recall that given $S \subset \mathbb{F}_q^d$, $S(x)$ shall denote its characteristic function. Let T_k^J denote the set of k-point J-configurations in E. Assume, inductively, that for every $J' \subset J$,

$$|T_{k-1}^{J'}| = (1+o(1))|E|^{k-1}q^{-|J'|} \tag{6.1}$$

if

$$|E| \geq Cq^{d\left(\frac{k-2}{k-1}\right)}q^{\frac{|J'|}{k-1}}.$$

The initialization step is the following. Observe that

$$|T_1^J| = |T_1^{\emptyset}| = |E| = |E|q^{-0},$$

and this needs to hold if

$$|E| \geq Cq^{d\left(\frac{k-1}{k}\right)}q^{\frac{|J|}{k}} = C.$$

6.1. The induction step: We have, without loss of generality,

$$|T_k^J| = \sum T_{k-1}^{J'}(x^1,\dots,x^{k-1})E(x^k)\Pi_{j=1}^{l}S(x^j-x^k)\Pi_{i=l+1}^{k-1}\sum_{a_i\neq 0} S_{a_i}(x^i-x^k) \tag{6.2}$$

for some $1 \leq l \leq k-1$, depending on the degree of the vertex corresponding to x^k, where

$$S_t = \{x \in \mathbb{F}_q^d : x_1^2 + x_2^2 + \cdots + x_d^2 = t\},$$

and $S \equiv S_1$. Technically, we should replace $\Pi_{j=1}^{l}S(x^j-x^k)$ by $\Pi_{j=1}^{l}S_{a_j}(x^j-x^k)$ for an arbitrary set of a_js, but this does not change the proof any and only complicates the notation.

Using (3.3) and the definition of the Fourier transform, we see from (6.2) that

$$|T_k^J| = q^{kd} \sum_{\xi^1,\dots,\xi^{k-1}:\xi^s\in\mathbb{F}_q^d} \widehat{T_{k-1}^{J'}}(\xi^1,\dots,\xi^{k-1})\widehat{E}\left(\sum_{u=1}^{k-1}\xi^u\right)\Pi_{j=1}^{l}\widehat{S}(\xi^j)\Pi_{i=l+1}^{k-1}\sum_{a_i\neq 0}\widehat{S}_{a_i}(\xi^i)$$

$$= Main + Remainder,$$

where Main is the term corresponding to taking $\xi^s = (0,\dots,0)$ for every $1 \leq s \leq k-1$. It follows by Lemma 3.5 that

$$Main = (1+o(1))|T_{k-1}^{J'}||E|q^{-l}.$$

The Remainder is the sum of terms of the form $R_{U,V}$, where

$$U = \{j \in \{1,2,\dots,l\} : \xi^j \neq (0,\dots,0)\},$$

and

$$V = \{j \in \{l+1\dots.,k-1\} : \xi^j \neq (0,\dots,0)\}.$$

We first analyze the term where compliments of U and V are empty sets. We get

$$R_{U,V} = q^{kd} \sum_{\xi^1,\dots,\xi^{k-1}:\xi^s\in\mathbb{F}_q^d;\xi^s\neq(0,\dots,0)} \widehat{T_{k-1}^{J'}}(\xi^1,\dots,\xi^{k-1})\widehat{E}\left(\sum_{u=1}^{k-1}\xi^u\right)\Pi_{j=1}^{l}\widehat{S}(\xi^j)\Pi_{i=l+1}^{k-1}\sum_{a_i\neq 0}\widehat{S}_{a_i}(\xi^i).$$

Applying Lemma 3.5 to the Fourier transforms of spheres and applying Cauchy-Schwartz, in the variables $\xi^1,\dots,\xi^{k-1}$, followed by (3.4) to the first two terms in the sum, we see that

$$R_{U,V} = O\left(q^{kd}\cdot|T_{k-1}^{J'}|^{\frac{1}{2}}\cdot|E|^{\frac{1}{2}}\cdot q^{-\frac{d}{2}}\cdot q^{\frac{d(k-2)}{2}}\cdot q^{-\frac{d+1}{2}l}\cdot q^{-\frac{d+1}{2}(k-1-l)}\right)$$

$$= O\left(|T_{k-1}^{J'}|^{\frac{1}{2}}\cdot|E|^{\frac{1}{2}}\cdot q^{\frac{d(k-1)}{2}}q^{-\frac{l}{2}}q^{-\frac{(k-1-l)}{2}}\right),$$

where $X = O(Y)$ means that there exists $C > 0$, independent of q, such that $X \leq CY$.

Applying the inductive hypothesis (6.1) and noting that l may be as large as $k-1$, we see that

$$R_{U,V} \leq \frac{1}{2}\cdot Main$$

if

$$|E| \geq Cq^{d\left(\frac{k-1}{k}\right)}\cdot q^{\frac{|J|}{k}},$$

with C sufficiently large, as desired.

To estimate the general $R_{U,V}$, we need the following simple observation that is proved by a direct calculation. Let $|U|+|V| = m$ and define

$$\widehat{f}(\mu^1,\dots,\mu^m) = q^{d(k-1)}q^{-md}\widehat{T}_{k-1}^{J'}(Z_{U,V}(\mu^1),\dots,Z_{U,V}(\mu^{k-1}))), \tag{6.3}$$

where

$$Z_{U,V} : \mathbb{F}^d \to \mathbb{F}^d$$

with $Z_{U,V}(\xi^j) = \xi^j$ if $j \in U\cup V$ and $(0,\dots,0)$ otherwise. Then

$$\sum_{y^1,\dots,y^m} f^2(y^1,\dots,y^m) \leq \max_{y^1,\dots,y^m} f(y^1,\dots,y^m)\cdot\sum_{y^1,\dots,y^m} f(y^1,\dots,y^m)$$

$$\leq \min\{|E|,(1+o(1))q^{d-1}\}\cdot|T_{k-1}^{J'}|.$$

Applying (6.3) one can check that in the regime $|E| \geq Cq^{d\left(\frac{k-1}{k}\right)}q^{\frac{n}{k}}$ the remaining $R_{U,V}$s are smaller than the error term we already estimated. This completes the proof.

Technically speaking we must still show that if $|T_k^{J_1}|$ satisfies the conjectured estimate for every J_1 with $|J_1| = n_1$, then so does $T_k^{J_2}$ with $|J_2| = n_2 > n_1$. However, this is apparent from the proof above.

References

[1] E. Bannai, O. Shimabukuro and H. Tanaka *Finite Euclidean graphs and Ramanujan graphs*, Discrete Mathematics (to appear) (2008). 3

[2] D. Hart and A. Iosevich, *Ubiquity of simplices in subsets of vector spaces over finite fields*, Analysis Mathematika, **34**, (2007). 5

[3] H. Iwaniec and E. Kowalski, *Analytic number theory*, AMS Colloquium Publications, **53**, (2004). 6

[4] A. Iosevich and M. Rudnev, *Erdős distance problem in vector spaces over finite fields*, Trans. Amer. Math. Soc. (2007). 4, 5

[5] W. M. Kwok, *Character tables of association schemes of affine type*, European J. Combin. 13 (1992) 167–185. 9

[6] M. Krivilevich and B. Sudakov, *Pseudo-random graphs*, (preprint), (2007). 3

[7] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge Univ. Press (1997). 6, 9, 13

[8] A. Medrano, P. Myers, H. M. Stark and A. Terras, *Finite analogs of Euclidean space*, Journal of Computational and Applied Mathematics, **68** (1996) 221-238. 4, 7

[9] L. Vinh, *Explicit Ramsey graphs and Erdös distance problem over finite Euclidean and non-Euclidean spaces*, (preprint), arXiv:0711.3508, (2007). 4

[10] L. Vinh and D. Dung *Explicit tough Ramsey graphs*, Proceedings of the International Conference on Relations, Orders and Graphs: Interaction with Computer Science, Nouha Editions, (2008), 139-146. 3

[11] V. Vu, *Sum-Product estimates via directed expanders*, (preprint), (2007). 4

[12] A. Weil, *On some exponential sums,* Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 204-207. 8