SETS WITH INTEGRAL DISTANCES IN FINITE FIELDS

ALEX IOSEVICH, IGOR E. SHPARLINSKI, AND MAOSHENG XIONG

ABSTRACT. Given a positive integer n, a finite field $\mathbb{F}_q$ of q elements (q odd), and a non-degenerate quadratic form Q on $\mathbb{F}_q^n$, in this paper we study the largest possible cardinality of subsets $\mathcal{E} \subseteq \mathbb{F}_q^n$ with pairwise integral Q-distances, that is, for any two vectors $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathcal{E}$, one has

$$Q(\mathbf{x} - \mathbf{y}) = u^2$$

for some $u \in \mathbb{F}_q$.

1. INTRODUCTION

Finite field analogs of classical problems in harmonic analysis, geometric measure theory and combinatorics have received much attention recently, due to the relative technical transparency afforded by the discrete setting and the presence of fascinating arithmetic considerations. See, for example, [5, 11, 19, 21] and the references therein for the description of various aspects of this area and recent progress. In this paper we investigate the finite field analog of the well-known problem about point sets in $\mathbb{R}^n$ with pairwise integral Euclidean distances.

Let n be a positive integer and $\mathbb{F}_q$ be the finite field of q elements. Throughout the paper we assume that q is odd. To put the problem in a more general setting, instead of using the usual Euclidean distance function d, namely

$$d(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} (x_i - y_i)^2 \tag{1}$$

for

$$\mathbf{x} = (x_1, \ldots, x_n), \ \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n,$$

we consider each non-degenerate quadratic form Q on $\mathbb{F}_q^n$. Given two n-dimensional vectors $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, we say

2000 *Mathematics Subject Classification.* 05B25,11T23,52C10.
Key words and phrases. integral distances, Gauss sums.

that the Q-distance between them is integral if

$$Q(\mathbf{x}-\mathbf{y}) = u^2$$

for some $u \in \mathbb{F}_q$. We say that the set $\mathcal{E} \subseteq \mathbb{F}_q^n$ has pairwise integral Q-distances if the Q-distance of any two points in $\mathcal{E}$ is integral. We define $I(Q, \mathbb{F}_q^n)$ as the largest possible cardinality of subsets $\mathcal{E} \subseteq \mathbb{F}_q^n$ with pairwise integral Q-distances.

The study of subsets of $\mathbb{F}_q^n$ with pairwise integral Q-distances is not new. For example, for $Q = d$ the Euclidean distance function in (1), various properties of subsets of $\mathbb{F}_q^n$ with pairwise integral Q-distances have been considered in the literature, see [13, 14] and references therein. In particuar, in [14] it is shown that $I(d, \mathbb{F}_q^2) = q$. Questions of this kind are certainly motivated by classical results of [1] about subsets of $\mathbb{R}^n$ with pairwise integral Euclidean distances, see also [10, 20] for more recent achievements. In this paper, we try to determine the quantity $I(Q, \mathbb{F}_q^n)$ for any positive integer n and any non-degenerate quadratic form Q on $\mathbb{F}_q^n$.

Since any non-degenerate quadratic form on $\mathbb{F}_q^n$ (q odd) can be diagonalized ([15, Theorem 3.1]), we may assume that Q is given by

$$Q(\mathbf{x}) = \sum_{i=1}^{n} a_i x_i^2, \quad a_i \neq 0, \quad 1 \leq i \leq n, \quad \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n\,. \tag{2}$$

Let η be the quadratic character of $\mathbb{F}_q$. We define $\eta(Q) \in \{\pm 1\}$ as

$$\eta(Q) = \prod_{i=1}^{n} \eta(a_i)\,. \tag{3}$$

The main result of this paper is as follows.

Theorem 1.

(i) *If n is even and $\eta(Q) = \eta(-1)^{n/2}$, then*

$$I(Q, \mathbb{F}_q^n) = q^{n/2}\,.$$

(ii) *If n is even and $\eta(Q) = -\eta(-1)^{n/2}$, then*

$$q^{n/2} \leq I(Q, \mathbb{F}_q^n) \leq q^{n/2} + \frac{2(q^{n/2}-q)}{q-1+2q^{-n/2+1}}\,.$$

(iii) *If n is odd and $\eta(Q) = \eta(-1)^{(n-1)/2}$, then*

$$I(Q, \mathbb{F}_q^n) = q^{(n+1)/2},$$

(iv) *If n is odd and $\eta(Q) = -\eta(-1)^{(n-1)/2}$, then*

$$q^{(n-1)/2} \leq I(Q, \mathbb{F}_q^n) \leq \frac{2q^{(n+1)/2}}{q-1+(q+1)q^{(-n+1)/2}}\,.$$

It remains interesting to determine the quantity $I(Q, \mathbb{F}_q^n)$ for the cases (ii) and (iv) of Theorem 1. We remark that first, when $n = 2$, the statements (i) and (ii) of Theorem 1 imply $I(Q, \mathbb{F}_q^2) = q$. This confirms and generalizes a result of Kurz ([14]), who proved that $I(d, \mathbb{F}_q^2) = q$ for $d(\mathbf{x}) = x_1^2 + x_2^2$, by employing a deep combinatorial theorem on point sets over $\mathbb{F}_q^2$ with few directions ([4, 2]). Second, the lower and upper bounds in (iv) are tight when $n = 1$. Third, it turns out that the large lower bounds in Theorem 1 are due to the existence of large subsets $\mathcal{E} \subseteq \mathbb{F}_q^n$ with pairwise zero Q-distance, that is, $Q(\mathbf{x}-\mathbf{y}) = 0$ for any $\mathbf{x}, \mathbf{y} \in \mathcal{E}$. Actually if we denote by $I_0(Q, \mathbb{F}_q^n)$ the largest possible cardinality of subsets $\mathcal{E} \subseteq \mathbb{F}_q^n$ with pairwise zero Q-distance, then we have

Theorem 2.

(i) *If n is even and $\eta(Q) = \eta(-1)^{n/2}$, then*
$$I_0(Q, \mathbb{F}_q^n) = q^{n/2}\,.$$

(ii) *If n is even and $\eta(Q) = -\eta(-1)^{n/2}$, then*
$$I_0(Q, \mathbb{F}_q^n) = q^{n/2-1}\,.$$

(iii) *If n is odd, then*
$$I_0(Q, \mathbb{F}_q^n) = q^{(n-1)/2}\,.$$

Finally, for the cases (i) and (iii) of Theorem 1, in addition to finding the exact values of $I(Q, \mathbb{F}_q^n)$, we can also determine the combinatorial structure that achieves this maximality. To state the result, we use the following notations. For Q given in (2) and any vector $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$, we define $|\mathbf{v}|_Q \in \mathbb{F}_q$ as

$$|\mathbf{v}|_Q = \frac{1}{4}\sum_{i=1}^{n} \frac{v_i^2}{a_i}\,. \tag{4}$$

Given two vectors $\mathbf{x}, \mathbf{v} \in \mathbb{F}_q^n$, we use $\mathbf{x} \cdot \mathbf{v}$ to denote the usual dot product.

Theorem 3.

(i) *Suppose that n is even and $\eta(Q) = \eta(-1)^{n/2}$. Then $\mathcal{E} \subseteq \mathbb{F}_q^n$ is a subset with pairwise integral Q-distances and $\#\mathcal{E} = q^{n/2}$ if and only if for any $t \in \mathbb{F}_q$ and any $\mathbf{v} \in \mathbb{F}_q^n$ with $\eta(-|\mathbf{v}|_Q) = -1$, one has*
$$\sum_{\substack{\mathbf{x}\in\mathcal{E}\\ \mathbf{x}\cdot\mathbf{v}=t}} 1 = q^{n/2-1}\,.$$

(ii) *Suppose that n is odd and $\eta(Q) = \eta(-1)^{(n-1)/2}$. Then $\mathcal{E} \subseteq \mathbb{F}_q^n$ is a subset with pairwise integral Q-distances and $\#\mathcal{E} = q^{(n+1)/2}$ if and only if for any $t \in \mathbb{F}_q$ and any $\mathbf{v} \in \mathbb{F}_q^n$ with $|\mathbf{v}|_Q \neq 0$, one has*

$$\sum_{\substack{\mathbf{x} \in \mathcal{E} \\ \mathbf{x} \cdot \mathbf{v} = t}} 1 = q^{(n-1)/2}.$$

2. Preliminary results

2.1. **Non-degenerate quadratic forms on $\mathbb{F}_q^n$.** Here we explain the definition of $\eta(Q)$ given in (3) for any non-degenerate quadratic form Q on $\mathbb{F}_q^n$.

Since Q can be diagonalized, we may assume that Q is the form given by (2). Now for $Q_1 = a_1x_1^2 + a_2x_2^2$, $a_1a_2 \neq 0$, make the change of variables as

$$x_1 = ux + vy, \quad x_2 = vx - \frac{a_1u}{a_2}y$$

for some $u, v \in \mathbb{F}_q$ with $a_1u^2 + a_2v^2 \neq 0$. The form Q_1 is reduced to

$$Q_2 = (a_1u^2 + a_2v^2)\left(x^2 + \frac{a_1}{a_2}y^2\right).$$

It is clear that $\eta(Q)$ is invariant under this change of variables. Since we can always find some $u, v \in \mathbb{F}_q$ such that $a_1u^2 + a_2v^2$ is some square element and some non-square element in ${\mathbb{F}_q}^*$ respectively, by multiplying appropriate squares in ${\mathbb{F}_q}^*$, we see that the two forms $a_1x_1^2 + a_2x_2^2$ and $b_1x_1^2 + b_2x_2^2$ with $a_1a_2b_1b_2 \neq 0$ are equivalent if $\eta(a_1a_2) = \eta(b_1b_2)$.

We fix a non-square element $\lambda \in {\mathbb{F}_q}^*$, then the form $Q_1 = a_1x_1^2 + a_2x_2^2$ can be reduced to either $x^2 + y^2$ or $x^2 + \lambda y^2$ depending on the value $\eta(a_1a_2)$. Since the forms $x_1^2 + x_2^2$, $-x_1^2 - x_2^2$ and $\lambda x_1^2 + \lambda x_2^2$ are all equivalent to each other, by making change of variables repeatedly one sees that any non-degenerate quadratic form Q on $\mathbb{F}_q^n$ can be reduced to one of the forms $Q_{n,\varepsilon}$, $\varepsilon \in \{1, \lambda\}$, depending on the value of $\eta(Q)$, where for $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, if $n = 2m$ is even, then

$$Q_{n,\varepsilon}(\mathbf{x}) = x_1^2 - x_2^2 + x_3^2 - x_4^2 + \ldots + x_{2m-1}^2 - \varepsilon x_{2m}^2, \tag{5}$$

and if $n = 2m + 1$ is odd, then

$$Q_{n,\varepsilon}(\mathbf{x}) = x_1^2 - x_2^2 + x_3^2 - x_4^2 + \ldots + x_{2m-1}^2 - x_{2m}^2 + \varepsilon x_{2m+1}^2. \tag{6}$$

Here we compute

$$\eta(Q_{n,\varepsilon}) = \begin{cases} \eta(\varepsilon)\eta(-1)^{n/2}, & \text{if } n \equiv 0 \pmod 2, \\ \eta(\varepsilon)\eta(-1)^{(n-1)/2}, & \text{if } n \equiv 1 \pmod 2. \end{cases}$$

In fact by the well-known classification of quadratic forms, there are two inequivalent non-degenerate quadratic forms on $\mathbb{F}_q^n$ (see, for example, [3]). Therefore $Q_{n,1}$ and $Q_{n,\lambda}$ are not equivalent and the equivalence class is uniquely determined by the value $\eta(Q)$.

2.2. **Gauss sums and "Q-Spheres" in $\mathbb{F}_q^n$.** First we recall some standard properties of the Gauss sums over $\mathbb{F}_q$ which are used frequently in this paper, we refer to [16] for details.

Fix a non-trivial additive character ψ of $\mathbb{F}_q$. The classical Gauss sum $G(\psi)$ is defined by

$$G(\psi) = \sum_{z \in \mathbb{F}_q} \psi(z^2).$$

It is easy to see that

$$G(\psi) = \sum_{z \in \mathbb{F}_q} \eta(z)\psi(z),$$

where η is the quadratic character of $\mathbb{F}_q$. We know that

$$G(\psi)^2 = \eta(-1)q,$$

and

$$\sum_{z \in \mathbb{F}_q} \psi(tz^2) = \eta(t)G(\psi).$$

Next, we need some results about "Q-spheres" in vector spaces over finite fields which have been used in [11]. Given a non-degenerate quadratic form Q on $\mathbb{F}_q^n$ given by (2), for $t \in \mathbb{F}_q$ we denote by $\mathcal{S}_Q(t)$ the "Q-sphere"

$$\mathcal{S}_Q(t) = \left\{ \mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}_q^n \ : \ Q(\mathbf{u}) = \sum_{i=1}^{n} a_i u_i^2 = t \right\}.$$

Furthermore, we consider the exponential sums

$$T_Q(\psi; t, \mathbf{v}) = \sum_{\mathbf{u} \in \mathcal{S}_Q(t)} \psi(\mathbf{v} \cdot \mathbf{u}) = \sum_{\mathbf{u} \in \mathcal{S}_Q(t)} \psi(-\mathbf{v} \cdot \mathbf{u}), \qquad \mathbf{v} \in \mathbb{F}_q^n,$$

since $\mathbf{u} \in \mathcal{S}_Q(t)$ and $-\mathbf{u} \in \mathcal{S}_Q(t)$ are equivalent. The following result is essentially shown in the proof of [17, Theorem 3] (see also [6, Equation (9)] which also corrects some typing mistakes in [17, Equation (11)]). For the sake of completeness, we give a proof here.

Lemma 1. *For Q given in (2), $t \in \mathbb{F}_q$ and vector $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$, we have*

$$T_Q(\psi; t, \mathbf{v}) = q^{n-1}\delta(\mathbf{v}) + \eta(-1)^n \eta(Q) q^{-1} G(\psi)^n \sum_{a \in \mathbb{F}_q^*} \eta(a)^n \psi\left(at + |\mathbf{v}|_Q / a\right),$$

where

$$\delta(\mathbf{v}) = \begin{cases} 1, & \text{if } \mathbf{v} = \mathbf{0}, \\ 0, & \text{otherwise,} \end{cases}$$

$\eta(Q)$ is defined in (3) and $|\mathbf{v}|_Q$ is defined in (4).

Proof. We recall the identity

$$\sum_{z \in \mathbb{F}_q} \psi(az) = \begin{cases} q, & \text{if } a = 0, \\ 0, & \text{otherwise,} \end{cases}$$

which immediately implies that for any vector $\mathbf{a} \in \mathbb{F}_q^n$ we have

$$\sum_{\mathbf{z} \in \mathbb{F}_q^n} \psi(\mathbf{a} \cdot \mathbf{z}) = \begin{cases} q^n, & \text{if } \mathbf{a} = \mathbf{0} \\ 0, & \text{otherwise,} \end{cases} \tag{7}$$

where, as before, $\mathbf{a} \cdot \mathbf{z}$ denotes the dot product of $\mathbf{a}$ and $\mathbf{z}$. Hence we can rewrite $T_Q(\psi; t, \mathbf{v})$ as

$$\begin{aligned} T_Q(\psi; t, \mathbf{v}) &= \sum_{\mathbf{u} \in \mathbb{F}_q^n} \psi(\mathbf{v} \cdot \mathbf{u}) \frac{1}{q} \sum_{a \in \mathbb{F}_q} \psi\left(a\left(Q(\mathbf{u}) - t\right)\right) \\ &= q^{-1} \sum_{\mathbf{u} \in \mathbb{F}_q^n} \psi(\mathbf{v} \cdot \mathbf{u}) + q^{-1} \sum_{a \in \mathbb{F}_q^*} \psi(-at) \sum_{\mathbf{u} \in \mathbb{F}_q^n} \psi(aQ(\mathbf{u}) + \mathbf{v} \cdot \mathbf{u}). \end{aligned}$$

The first term on the right hand side is $q^{n-1}\delta(\mathbf{v})$ by using (7). Denoting by $q^{-1}T_2$ the second term, one has

$$\begin{aligned} T_2 &= \sum_{a \in \mathbb{F}_q^*} \psi(-at) \sum_{\mathbf{u} \in \mathbb{F}_q^n} \psi\left(a \sum_{i=1}^n a_i u_i^2 + u_i v_i\right) \\ &= \sum_{a \in \mathbb{F}_q^*} \psi(-at) \prod_{i=1}^n \sum_{u_i \in \mathbb{F}_q} \psi\left(a a_i u_i^2 + u_i v_i\right). \end{aligned}$$

Using properties of the Gauss sums, we have

$$\begin{aligned}\sum_{u_i\in\mathbb{F}_q}\psi\left(aa_iu_i^2+u_iv_i\right) &= \sum_{u_i\in\mathbb{F}_q}\psi\left(aa_i\left(u_i+\frac{v_i}{2aa_i}\right)^2\right)\psi\left(-\frac{v_i^2}{4aa_i}\right)\\ &= \psi\left(-\frac{v_i^2}{4aa_i}\right)\sum_{u_i\in\mathbb{F}_q}\psi\left(aa_iu_i^2\right)\\ &= \eta(aa_i)G(\psi)\psi\left(-\frac{v_i^2}{4aa_i}\right).\end{aligned}$$

Thus

$$\begin{aligned}T_2 &= \sum_{a\in{\mathbb{F}_q}^*}\psi(-at)\prod_{i=1}^n\eta(aa_i)G(\psi)\psi\left(-\frac{v_i^2}{4aa_i}\right)\\ &= G(\psi)^n\eta(a_1\dots a_n)\sum_{a\in{\mathbb{F}_q}^*}\psi(-at)\psi\left(-\frac{1}{a}\sum_{i=1}^n\frac{v_i^2}{4a_i}\right)\\ &= G(\psi)^n\eta(Q)\sum_{a\in{\mathbb{F}_q}^*}\psi(-at)\psi\left(-\frac{|\mathbf{v}|_Q}{a}\right),\end{aligned}$$

by recalling the definition of $\eta(Q)$ in (3) and $|\mathbf{v}|_Q$ in (4). Therefore

$$T_2=\eta(-1)^nG(\psi)^n\eta(Q)\sum_{a\in{\mathbb{F}_q}^*}\psi\left(at+\frac{|\mathbf{v}|_Q}{a}\right).$$

Combining this with the first term $q^{-1}\delta(\mathbf{v})$ we conclude the proof. □

In particular,we see from Lemma 1 that if $\mathbf{v}=\mathbf{0}$, then $T_Q(\psi;t,\mathbf{0})=\#\mathcal{S}_Q(t)$, from Lemma 1 and the Weil bound of Kloosterman and Salie sums (see [12, Theorem 11.11 and Lemma 12.4]), we immediately obtain that (see also [11, Lemma 2.2]), for any $t\in\mathbb{F}_q$,

$$\#\mathcal{S}_Q(t)=q^{n-1}+O\left(q^{n/2}\right).$$

3. Proof of Theorem 1.

3.1. **Lower bounds.** We first provide lowers bounds of $I(Q,\mathbb{F}_q^n)$ which appear in Theorem 1.

Lemma 2. *Let Q be a non-degenerate quadratic form on $\mathbb{F}_q^n$.*

(a) *If n is even, then $I(Q,\mathbb{F}_q^n)\geq q^{n/2}$.*
(b) *If n is odd and $\eta(Q)=\eta(-1)^{(n-1)/2}$, then $I(Q,\mathbb{F}_q^n)\geq q^{(n+1)/2}$.*
(c) *If n is odd and $\eta(Q)=-\eta(-1)^{(n-1)/2}$, then $I(Q,\mathbb{F}_q^n)\geq q^{(n-1)/2}$.*

Proof. For $1 \le i \le n$, denote by $\mathbf{e}_i$ the vector in $\mathbb{F}_q^n$ with 1 in the i-th entry and 0 everywhere else. Suppose that $n = 2m$ is even. By the classification of non-degenerate quadratic forms on $\mathbb{F}_q^n$ in Section 2.1, we may assume that $Q = Q_{n,\varepsilon}$ defined in (5), where $\varepsilon = 1$ or λ . Let $\mathcal{E}$ be the vector space over $\mathbb{F}_q$ spanned by the $n/2$ vectors $\{\mathbf{e}_1 + \mathbf{e}_2, \mathbf{e}_3 + \mathbf{e}_4, \ldots, \mathbf{e}_{2m-3} + \mathbf{e}_{2m-2}, \mathbf{e}_{2m-1}\}$. It is clear that for any $\mathbf{x} \in \mathcal{E}$ one has $Q_{n,\varepsilon}(\mathbf{x}) = u^2$ for some $u \in \mathbb{F}_q$. This implies that $I(Q_{n,\varepsilon}, \mathbb{F}_q^n) \ge \#\mathcal{E} = q^{n/2}$ for $\varepsilon \in \{1, \lambda\}$. This proves (a).

Suppose that n is odd and $\eta(Q) = \eta(-1)^{(n-1)/2}$. By the classification of non-degenerate quadratic forms on $\mathbb{F}_q^n$ in Section 2.1, we may assume that $Q = Q_{n,1}$ given in (6). Let $\mathcal{E}$ be the vector space over $\mathbb{F}_q$ spanned by the $(n+1)/2$ vectors $\{\mathbf{e}_1 + \mathbf{e}_2, \mathbf{e}_3 + \mathbf{e}_4, \ldots, \mathbf{e}_{2m-1} + \mathbf{e}_{2m}, \mathbf{e}_{2m+1}\}$. It is clear that for any $\mathbf{x} \in \mathcal{E}$ one has $Q_{n,1}(\mathbf{x}) = u^2$ for some $u \in \mathbb{F}_q$. This implies that $I(Q_{n,1}, \mathbb{F}_q^n) \ge \#\mathcal{E} = q^{(n+1)/2}$ for this case. This proves (b).

Suppose that n is odd and $\eta(Q) = -\eta(-1)^{(n-1)/2}$. We may assume that $Q = Q_{n,\lambda}$ defined in (6). Let $\mathcal{E}$ be the vector space over $\mathbb{F}_q$ spanned by the $(n-1)/2$ vectors $\{\mathbf{e}_1 + \mathbf{e}_2, \mathbf{e}_3 + \mathbf{e}_4, \ldots, \mathbf{e}_{2m-1} + \mathbf{e}_{2m}\}$. It is clear that for any $\mathbf{x} \in \mathcal{E}$ one has $Q_{n,\lambda}(\mathbf{x}) = u^2$ for some $u \in \mathbb{F}_q$. This implies that $I(Q_{n,\lambda}, \mathbb{F}_q^n) \ge \#\mathcal{E} = q^{(n-1)/2}$. This implies (c) and thus completes the proof. □

3.2. **Preparations to upper bounds.** We may assume that Q is given by (2). Since $\lambda \in {\mathbb{F}_q}^*$ is a non-quadratic element, we see that if $\mathcal{E} \subseteq \mathbb{F}_q^n$ is a set with pairwise integral Q-distances, then for every $t \in {\mathbb{F}_q}^*$ the equation

$$\mathbf{x} - \mathbf{y} = \mathbf{u}, \tag{8}$$

has no solution for $\mathbf{x}, \mathbf{y} \in \mathcal{E}$ and $\mathbf{u} \in \mathcal{S}_Q(\lambda t^2)$.

As before, let ψ be a nontrivial additive character of $\mathbb{F}_q$. By the identity (7), the number of solutions to the equation (8) can be expressed as

$$\sum_{\mathbf{x},\mathbf{y} \in \mathcal{E}} \sum_{\mathbf{u} \in \mathcal{S}_Q(\lambda t^2)} \frac{1}{q^n} \sum_{\mathbf{v} \in \mathbb{F}_q^n} \psi\left(\mathbf{v} \cdot (\mathbf{x} - \mathbf{y} - \mathbf{u})\right)$$
$$= \frac{1}{q^n} \sum_{\mathbf{v} \in \mathbb{F}_q^n} \left| \sum_{\mathbf{x} \in \mathcal{E}} \psi(\mathbf{v} \cdot \mathbf{x}) \right|^2 T_Q(\psi; \lambda t^2, \mathbf{v}).$$

For each $\mathbf{v} \in \mathbb{F}_q^n$, define

$$a_{\mathbf{v}} = \left| \sum_{\mathbf{x} \in \mathcal{E}} \psi(\mathbf{v} \cdot \mathbf{x}) \right|^2.$$

One observes that

$$a_{\mathbf{v}} \geq 0, \quad a_{\mathbf{0}} = (\#\mathcal{E})^2, \quad \text{and} \quad \sum_{\mathbf{v}\in\mathbb{F}_q^n} a_{\mathbf{v}} = q^n(\#\mathcal{E})\,. \tag{9}$$

Using that (8) has no solution for any $t \in {\mathbb{F}_q}^*$, we have

$$\begin{aligned}\sum_{t\in{\mathbb{F}_q}^*} \frac{1}{q^n} \sum_{\mathbf{v}\in\mathbb{F}_q^n} a_{\mathbf{v}} T_Q(\psi; \lambda t^2, \mathbf{v}) \\ = \frac{1}{q^n} \sum_{\mathbf{v}\in\mathbb{F}_q^n} a_{\mathbf{v}} \sum_{t\in{\mathbb{F}_q}^*} T_Q(\psi; \lambda t^2, \mathbf{v}) = 0.\end{aligned} \tag{10}$$

Multiplying by q^n on both sizes of (10) and applying Lemma 1, we can rewrite the equation as

$$\begin{aligned} 0 &= \sum_{\mathbf{v}\in\mathbb{F}_q^n} a_{\mathbf{v}} \sum_{t\in{\mathbb{F}_q}^*} \Bigg(q^{n-1}\delta(\mathbf{v}) \\ &\qquad + \eta(-1)^n\eta(Q)q^{-1}G(\psi)^n \sum_{a\in{\mathbb{F}_q}^*} \eta(a)^n \psi\left(a\lambda t^2 + |\mathbf{v}|_Q/a\right)\Bigg) \\ &= q^{n-1}(q-1)\left(\#\mathcal{E}\right)^2 + \eta(-1)^n\eta(Q)q^{-1}G(\psi)^n \sum_{\mathbf{v}\in\mathbb{F}_q^n} a_{\mathbf{v}} c_{\mathbf{v}}, \end{aligned}$$

where for any $\mathbf{v} \in \mathbb{F}_q^n$, $c_{\mathbf{v}}$ is defined by

$$c_{\mathbf{v}} = \sum_{a\in{\mathbb{F}_q}^*} \eta(a)^n \psi\left(|\mathbf{v}|_Q/a\right) \sum_{t\in{\mathbb{F}_q}^*} \psi\left(a\lambda t^2\right)$$

We can compute by using the properties of the Gauss sums that

$$\begin{aligned} c_{\mathbf{v}} &= \sum_{a\in{\mathbb{F}_q}^*} \eta(a)^n \psi\left(|\mathbf{v}|_Q/a\right) \left\{\eta\left(a\lambda\right) G(\psi) - 1\right\} \\ &= -G(\psi) \sum_{a\in{\mathbb{F}_q}^*} \eta(a)^{n+1} \psi\left(|\mathbf{v}|_Q/a\right) - \sum_{a\in{\mathbb{F}_q}^*} \eta(a)^n \psi\left(|\mathbf{v}|_Q/a\right) \\ &= -G(\psi) \sum_{a\in{\mathbb{F}_q}^*} \eta(a)^{n+1} \psi\left(a|\mathbf{v}|_Q\right) - \sum_{a\in{\mathbb{F}_q}^*} \eta(a)^n \psi\left(a|\mathbf{v}|_Q\right)\,. \end{aligned}$$

Hence we have the identity

$$(q-1)\left(\#\mathcal{E}\right)^2 = -\eta(-1)^n\eta(Q)q^{-n}G(\psi)^n \sum_{\mathbf{v}\in\mathbb{F}_q^n} a_{\mathbf{v}} c_{\mathbf{v}}\,. \tag{11}$$

3.3. **Even n.** If n is even, then by using properties of the Gauss sums we have

$$\begin{aligned} c_{\mathbf{v}} &= -G(\psi) \sum_{a \in \mathbb{F}_q^*} \eta(a) \psi\left(a|\mathbf{v}|_Q\right) - \sum_{a \in \mathbb{F}_q^*} \psi\left(a|\mathbf{v}|_Q\right) \\ &= -G(\psi)^2 \eta\left(|\mathbf{v}|_Q\right) - q\delta\left(|\mathbf{v}|_Q\right) + 1\,, \end{aligned}$$

where the function δ on $\mathbb{F}_q$ is defined as for any $a \in \mathbb{F}_q$,

$$\delta(a) = \begin{cases} 1 & : \quad a = 0 \\ 0 & : \quad a \neq 0 \end{cases}.$$

Since $G(\psi)^2 = \eta(-1)q$, the identity (11) becomes

$$\begin{aligned} &(q-1)\left(\#\mathcal{E}\right)^2 \\ &\qquad = -\eta(-1)^{n/2}\eta(Q)q^{-n/2} \sum_{\mathbf{v} \in \mathbb{F}_q^n} a_{\mathbf{v}} \left\{-q\eta\left(-|\mathbf{v}|_Q\right) - q\delta\left(|\mathbf{v}|_Q\right) + 1\right\}. \end{aligned}$$

This can be simplified further as

$$(q-1)\left(\#\mathcal{E}\right)^2 = \eta(-1)^{n/2}\eta(Q)q^{-n/2}\left(qI_1 - qI_2 - I_3\right), \tag{12}$$

where

$$\begin{aligned} I_1 &= \sum_{\substack{\mathbf{v} \in \mathbb{F}_q^n, \\ \eta\left(-|\mathbf{v}|_Q\right)=1}} a_{\mathbf{v}} + \sum_{\substack{\mathbf{v} \in \mathbb{F}_q^n \\ |\mathbf{v}|_Q=0}} a_{\mathbf{v}}\,, \\ I_2 &= \sum_{\substack{\mathbf{v} \in \mathbb{F}_q^n, \\ \eta\left(-|\mathbf{v}|_Q\right)=-1}} a_{\mathbf{v}}\,, \\ I_3 &= \sum_{\mathbf{v} \in \mathbb{F}_q^n} a_{\mathbf{v}}\,. \end{aligned}$$

From (9) we know that $I_1, I_2 \geq 0$ and $I_1 + I_2 = I_3 = q^n(\#\mathcal{E})$. If $\eta(Q) = \eta(-1)^{n/2}$, then the identity (12) becomes

$$\begin{aligned} (q-1)\left(\#\mathcal{E}\right)^2 &= q^{-n/2}\left\{qI_1 - qI_2 - I_3\right\} \\ &\leq q^{-n/2}(q-1)I_3 = q^{-n/2}(q-1)q^n(\#\mathcal{E}), \end{aligned} \tag{13}$$

we derive that $\#\mathcal{E} \leq q^{n/2}$. On the other hand, from (a) of Lemma 2 we know $I(Q, \mathbb{F}_q^n) \geq q^{n/2}$. It implies in this case

$$I(Q, \mathbb{F}_q^n) = q^{n/2}.$$

This proves the statement (i) of Theorem 1.

If $\eta(Q) = -\eta(-1)^{n/2}$, replacing I_2 by $I_3 - I_1$ and noticing $I_1 \geq a_{\mathbf{0}} = (\#\mathcal{E})^2$ and $I_3 = q^n(\#\mathcal{E})$ the identity (12) becomes

$$\begin{aligned}(q-1)\,(\#\mathcal{E})^2 &= q^{-n/2}\left((q+1)I_3 - 2qI_1\right)\\ &\leq q^{-n/2}(q+1)q^n(\#\mathcal{E}) - 2q^{-n/2+1}\,(\#\mathcal{E})^2\,.\end{aligned}$$

Solving this inequality one concludes that

$$\#\mathcal{E} \leq \frac{q^{n/2}(q+1)}{q-1+2q^{-n/2+1}} = q^{n/2} + \frac{2(q^{n/2}-q)}{q-1+2q^{-n/2+1}}\,.$$

Combining the lower bound in (a) of Lemma 2 with this upper bound proves the statement (ii) of Theorem 1.

3.4. **Odd n.** If n is odd, then

$$\begin{aligned}c_{\mathbf{v}} &= -G(\psi)\sum_{a\in\mathbb{F}_q{}^*}\psi\left(a|\mathbf{v}|_Q\right) - \sum_{a\in\mathbb{F}_q{}^*}\eta(a)\psi\left(a|\mathbf{v}|_Q\right)\\ &= -G(\psi)\left(q\delta(|\mathbf{v}|_Q) - 1\right) - \eta\left(|\mathbf{v}|_Q\right)G(\psi)\,.\end{aligned}$$

Therefore, using $G(\psi)^2 = \eta(-1)q$ we have

$$\begin{aligned}&(q-1)\,(\#\mathcal{E})^2\\ &\quad= \eta(-1)^n\eta(Q)q^{-n}G(\psi)^{n+1}\sum_{\mathbf{v}\in\mathbb{F}_q^n}a_{\mathbf{v}}\left\{q\delta\left(|\mathbf{v}|_Q\right) + \eta\left(|\mathbf{v}|_Q\right) - 1\right\}\\ &\quad= \eta(-1)^{(n-1)/2}\eta(Q)q^{(-n+1)/2}\left(qJ_1 + J_2^+ - J_2^- - J_3\right)\,,\end{aligned}$$

where

$$J_1 = \sum_{\substack{\mathbf{v}\in\mathbb{F}_q^n\\ |\mathbf{v}|_Q=0}} a_{\mathbf{v}}\,, \qquad J_2^+ = \sum_{\substack{\mathbf{v}\in\mathbb{F}_q^n\\ \eta(|\mathbf{v}|_Q)=1}} a_{\mathbf{v}}, \qquad J_2^- = \sum_{\substack{\mathbf{v}\in\mathbb{F}_q^n\\ \eta(|\mathbf{v}|_Q)=-1}} a_{\mathbf{v}}$$

and

$$J_3 = \sum_{\mathbf{v}\in\mathbb{F}_q^n} a_{\mathbf{v}} = q^n(\#\mathcal{E})\,.$$

(note that $J_3 = I_3$, where I_3 is defined in Section 3.3).

We know that $J_1, J_2^+, J_2^- \geq 0$ and $J_3 = J_1 + J_2^+ + J_2^-$. If $\eta(Q) = \eta(-1)^{(n-1)/2}$, then

$$\begin{aligned}(q-1)\,(\#\mathcal{E})^2 &= q^{(-n+1)/2}\left\{(q-1)J_1 - 2J_2^+\right\}\\ &\leq q^{(-n+1)/2}(q-1)J_1 \leq q^{(-n+1)/2}(q-1)J_3\\ &= q^{(-n+1)/2}(q-1)q^n(\#\mathcal{E}).\end{aligned} \tag{14}$$

From this we derive that

$$\#\mathcal{E} \leq q^{(n+1)/2}.$$

On the other hand, from (b) of Lemma 11 we know that $I(Q, \mathbb{F}_q^n) \geq q^{(n+1)/2}$. It implies that in this case

$$I(Q, \mathbb{F}_q^n) = q^{(n+1)/2}.$$

This proves the statement (iii) of Theorem 1.

If $\eta(Q) = -\eta(-1)^{(n-1)/2}$, replacing J_2^- by $J_3 - J_1 - J_2^+$, we have

$$\begin{aligned} (q-1)\left(\#\mathcal{E}\right)^2 &= -q^{(-n+1)/2}\left(qJ_1 + J_2^+ - J_2^- - J_3\right) \\ &= q^{(-n+1)/2}\left(2J_3 - (q+1)J_1 - 2J_2^+\right). \end{aligned}$$

Noticing $J_1 \geq a_{\mathbf{0}} = \left(\#\mathcal{E}\right)^2$ and $J_3 = q^n(\#\mathcal{E})$ we have

$$(q-1)\left(\#\mathcal{E}\right)^2 \leq q^{(-n+1)/2}\left(2q^n(\#\mathcal{E}) - (q+1)(\#\mathcal{E})^2\right).$$

Solving this inequality one obtains

$$\#\mathcal{E} \leq \frac{2q^{(n+1)/2}}{q - 1 + q^{(-n+1)/2}(q+1)}.$$

Combining the lower bound of $I(Q, \mathbb{F}_q^n)$ in (c) of Lemma 2 with this result proves the statement (iv) of Theorem 1. Now the proof of Theorem 1 is complete.

4. Proof of Theorem 2

4.1. **Preparations.** We start with some auxiliary statements which could be of independent interest.

Lemma 3. *Let Q be a non-degenerate quadratic form on $\mathbb{F}_q^n$.*

(a) *If n is even and $\eta(Q) = \eta(-1)^{n/2}$, then*

$$I_0(Q, \mathbb{F}_q^n) = q^{n/2}.$$

(b) *If n is even and $\eta(Q) = -\eta(-1)^{n/2}$, then*

$$q^{n/2-1} \leq I_0(Q, \mathbb{F}_q^n) \leq \frac{q^{n/2}}{q - 1 + q^{-n/2+1}}.$$

(c) *If n is odd, then*

$$q^{(n-1)/2} \leq I_0(Q, \mathbb{F}_q^n) \leq \frac{q^{(n+1)/2}}{q - 1 + q^{(-n+1)/2}}.$$

Proof. Since the proof of Lemma 3 is very similar to that of Theorem 1, we prove (b) only.

First start with the lower bound. As usual denote by $\mathbf{e}_i$ the vector in $\mathbb{F}_q^n$ with 1 in the i-th entry and 0 everywhere else. If $n = 2m$ is even and $\eta(Q) = -\eta(-1)^{n/2}$, we may assume $Q = Q_{n,\lambda}$ given in (5). Let $\mathcal{E}$ be the vector space over $\mathbb{F}_q$ spanned by the $n/2 - 1$ vectors

$\{\mathbf{e}_1+\mathbf{e}_2, \mathbf{e}_3+\mathbf{e}_4, \ldots, \mathbf{e}_{2m-3}+\mathbf{e}_{2m-2}\}$. It is clear that $\mathcal{E}$ is a subset with pairwise zero Q-distance. This construction implies that $I_0(Q_{n,\lambda}, \mathbb{F}_q^n) \geq q^{n/2-1}$.

To prove the upper bound, we notice that if $\mathcal{E} \subseteq \mathbb{F}_q^n$ is a set with pairwise zero Q-distance, then for every $t \in {\mathbb{F}_q}^*$ the equation

$$\mathbf{x}-\mathbf{y}=\mathbf{u},$$

has no solution for $\mathbf{x}, \mathbf{y} \in \mathcal{E}$ and $\mathbf{u} \in \mathcal{S}_Q(t)$. That is, for any $t \in {\mathbb{F}_q}^*$,

$$\sum_{\mathbf{x},\mathbf{y}\in\mathcal{E}} \sum_{\mathbf{u}\in\mathcal{S}_Q(t)} \frac{1}{q^n} \sum_{\mathbf{v}\in\mathbb{F}_q^n} \psi\left(\mathbf{v}\cdot(\mathbf{x}-\mathbf{y}-\mathbf{u})\right) = 0\,.$$

Adding up the above equation as t runs over ${\mathbb{F}_q}^*$, applying Lemma 1 and using notations from Section 3.2 one obtains

$$0 \;=\; q^{n-1}(q-1)\left(\#\mathcal{E}\right)^2 + \eta(-1)^n\eta(Q)q^{-1}G(\psi)^n \sum_{\mathbf{v}\in\mathbb{F}_q^n} a_{\mathbf{v}}c'_{\mathbf{v}}, \tag{15}$$

where for any $\mathbf{v} \in \mathbb{F}_q^n$, $c'_{\mathbf{v}}$ is

$$\begin{aligned} c_{\mathbf{v}} &= \sum_{a\in{\mathbb{F}_q}^*} \eta(a)^n\psi\left(|\mathbf{v}|_Q/a\right) \sum_{t\in{\mathbb{F}_q}^*} \psi\left(at\right) \\ &= -\sum_{a\in{\mathbb{F}_q}^*} \eta(a)^n\psi\left(a|\mathbf{v}|_Q\right). \end{aligned}$$

Since n is even, $\eta(Q) = -\eta(-1)n/2$, and $G(\psi)^2 = \eta(-1)q$, the identity (15) can be simplified as

$$(q-1)\left(\#\mathcal{E}\right)^2 = q^{-n/2}\left(J_3 - qJ_1\right)\,,$$

where

$$J_1 \;=\; \sum_{\substack{\mathbf{v}\in\mathbb{F}_q^n \\ |\mathbf{v}|_Q=0}} a_{\mathbf{v}}\,, \quad J_3 = \sum_{\mathbf{v}\in\mathbb{F}_q^n} a_{\mathbf{v}} = q^n(\#\mathcal{E})^2\,.$$

Since

$$J_1 \geq a_0 = (\#\mathcal{E})^2,$$

one obtains that

$$\#\mathcal{E} \leq \frac{q^{n/2}}{q-1+q^{-n/2+1}}.$$

Combining the lower and upper bounds finishes the proof of (b). □

Lemma 4. *If $\mathcal{E} \subseteq \mathbb{F}_q^n$ is a maximal subset with pairwise zero Q-distance and $\mathbf{0} \in \mathcal{E}$, then $\mathcal{E}$ is a vector space over $\mathbb{F}_q$.*

Proof. First, for any $\mathbf{x}, \mathbf{y} \in \mathcal{E}$, one has

$$0 = Q(\mathbf{x}-\mathbf{y}) = \sum_{i=1}^{n} a_i (x_i - y_i)^2 = Q(\mathbf{x}) + Q(y) - 2\sum_{i=1}^{n} a_i x_i y_i \,.$$

Since $Q(\mathbf{x}) = Q(\mathbf{y}) = 0$ (because $\mathbf{0} \in \mathcal{E}$), one has

$$\sum_{i=1}^{n} a_i x_i y_i = 0.$$

Thus for any $t \in \mathbb{F}_q$, one has

$$Q(t\mathbf{x}-\mathbf{y}) = \sum_{i=1}^{n} a_i (t x_i - y_i)^2 = t^2 Q(\mathbf{x}) + Q(\mathbf{y}) - 2t\sum_{i=1}^{n} a_i x_i y_i = 0.$$

It implies that the set $\mathcal{E} \bigcup \{t\mathbf{x}\}$ is also a set with pairwise zero Q-distance. By the maximality of $\mathcal{E}$, for any $\mathbf{x} \in \mathcal{E}$ and $t \in \mathbb{F}_q$, one has $t\mathbf{x} \in \mathcal{E}$.

Next, for any $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{E}$, one has

$$\begin{aligned} Q(\mathbf{x}+\mathbf{y}-z) \;\; &= \;\; \sum_{i=1}^{n} a_i (x_i + y_i - z_i)^2 = Q(\mathbf{x}) + Q(\mathbf{y}) + Q(\mathbf{z}) \\ &\qquad +2\sum_{i=1}^{n} a_i x_i y_i - 2\sum_{i=1}^{n} a_i x_i z_i - 2\sum_{i=1}^{n} a_i y_i z_i. \end{aligned}$$

Since $\mathbf{0} \in \mathcal{E}$, considering $\mathbf{x}$ and $\mathbf{y}$ one has $Q(\mathbf{x}) = Q(\mathbf{y}) = Q(\mathbf{x}+\mathbf{y}) = 0$, which implies that $\sum_{i=1}^{n} a_i x_i y_i = 0$. Considering $\mathbf{x}, \mathbf{z}$ and then $\mathbf{y}, \mathbf{z}$ similarly one can obtain that $Q(\mathbf{x}+\mathbf{y}-\mathbf{z}) = 0$. Thus the set $\mathcal{E} \bigcup \{\mathbf{x}+\mathbf{y}\}$ is also a set with pairwise zero Q-distance. By the maximality of $\mathcal{E}$, for any $\mathbf{x}, \mathbf{y} \in \mathcal{E}$, one has $\mathbf{x}+\mathbf{y} \in \mathcal{E}$. □

4.2. **Concluding the proof.** Suppose that $\mathcal{E} \subseteq \mathbb{F}_q^n$ is a subset with pairwise zero Q-distance that achieves the maximal cardinality $\#\mathcal{E} = I_0(Q, \mathbb{F}_q^n)$. We may assume $\mathbf{0} \in \mathcal{E}$, since for any $\mathbf{v} \in \mathbb{F}_q^n$, the set $\mathcal{E} + \mathbf{v} = \{\mathbf{x} + \mathbf{v} : \mathbf{x} \in \mathcal{E}\}$ also has pairwise zero Q-distance. We see from Lemma 4 that $\mathcal{E}$ is a vector, hence the cardinality of $\mathcal{E}$ is a power of q. Now checking the lower and upper bounds in Lemma 3, one easily sees that the cardinality of $\mathcal{E}$ must equal those lower bounds. This completes the proof of Theorem 2.

5. Proof of Theorem 3

5.1. **Even n.** Fix a finite field $\mathbb{F}_q$ of q elements (q odd), a positive integer n and a non-degenerate quadratic form Q on $\mathbb{F}_q^n$ given by (2). Suppose n is even and $\eta(Q) = \eta(-1)^{n/2}$. If $\mathcal{E} \subseteq \mathbb{F}_q^n$ is a subset with

pairwise integral Q-distances, then $\#\mathcal{E} \leq q^{n/2}$ by (i) of Theorem 1. If $\#\mathcal{E} = q^{n/2}$, following the proof of (i) of Theorem 1, the inequality in (13) become actually an equality. For this to happen, one must have

$$I_2 = \sum_{\substack{\mathbf{v}\in\mathbb{F}_q^n,\\ \eta\left(-|\mathbf{v}|_Q\right)=-1}} a_{\mathbf{v}} = \sum_{\substack{\mathbf{v}\in\mathbb{F}_q^n,\\ \eta\left(-|\mathbf{v}|_Q\right)=-1}} \left|\sum_{\mathbf{x}\in\mathcal{E}} \psi(\mathbf{v}\cdot\mathbf{x})\right|^2 = 0\,,$$

that is,

$$\left|\sum_{\mathbf{x}\in\mathcal{E}} \psi(\mathbf{v}\cdot\mathbf{x})\right|^2 = 0\,,$$

for any $\mathbf{v} \in \mathbb{F}_q^n$ with $\eta\left(-|\mathbf{v}|_Q\right) = -1$. Notice that if $\eta\left(-|\mathbf{v}|_Q\right) = -1$, then for any $\alpha \in {\mathbb{F}_q}^*$ one also has $\eta\left(-|\alpha\mathbf{v}|_Q\right) = -1$. Therefore

$$\sum_{\alpha\in\mathbb{F}_q} \left|\sum_{\mathbf{x}\in\mathcal{E}} \psi(\alpha\mathbf{v}\cdot\mathbf{x})\right|^2 = (\#\mathcal{E})^2 = q^n\,,$$

where the term $(\#\mathcal{E})^2$ comes from the term $\alpha = 0$.

Expanding the left hand side of the above identity we have

$$\begin{aligned} q^n &= \sum_{\mathbf{x},\mathbf{y}\in\mathcal{E}} \sum_{\alpha\in\mathbb{F}_q} \psi\left(\alpha\mathbf{v}\cdot(\mathbf{x}-\mathbf{y})\right) \\ &= q \sum_{\substack{\mathbf{x},\mathbf{y}\in\mathcal{E}\\ \mathbf{v}\cdot(\mathbf{x}-\mathbf{y})=0}} 1 = q\sum_{t\in\mathbb{F}_q} \left(\sum_{\substack{\mathbf{x}\in\mathcal{E}\\ \mathbf{v}\cdot\mathbf{x}=t}} 1\right)^2 = q\sum_{t\in\mathbb{F}_q} a_{\mathbf{v},t}^2\,, \end{aligned}$$

where for any $t \in \mathbb{F}_q$, $a_{\mathbf{v},t}$ is defined by

$$a_{\mathbf{v},t} = \sum_{\substack{\mathbf{x}\in\mathcal{E}\\ \mathbf{x}\cdot\mathbf{v}=t}} 1 \geq 0\,.$$

Since

$$\sum_{t\in\mathbb{F}_q} a_{\mathbf{v},t} = \sum_{\mathbf{x}\in\mathcal{E}} 1 = \#\mathcal{E} = q^{n/2},$$

by the Cauchy-Schwarz inequality, one has $a_{\mathbf{v},t} = a_{\mathbf{v},s}$ for any $t, s \in \mathbb{F}_q$. That is,

$$a_{\mathbf{v},t} = \sum_{\substack{\mathbf{x}\in\mathcal{E}\\ \mathbf{x}\cdot\mathbf{v}=t}} 1 = \frac{1}{q}\#\mathcal{E} = q^{n/2-1}\,,$$

for any $t \in \mathbb{F}_q$, any $\mathbf{v} \in \mathbb{F}_q^n$ with $\eta\left(-|\mathbf{v}|_Q\right) = -1$.

On the other hand, if for any $t \in \mathbb{F}_q$, any $\mathbf{v} \in \mathbb{F}_q^n$ with $\eta\left(-|\mathbf{v}|_Q\right) = -1$ one always has

$$a_{\mathbf{v},t} = \sum_{\substack{\mathbf{x} \in \mathcal{E} \\ \mathbf{x} \cdot \mathbf{v} = t}} 1 = q^{n/2-1}\,,$$

then for the set $\mathcal{E} \subseteq \mathbb{F}_q^n$,

$$\#\mathcal{E} = \sum_{t \in \mathbb{F}_q} a_{\mathbf{v},t} = q^{n/2}\,.$$

In (13) the term I_2 is

$$I_2 \;=\; \sum_{\substack{\mathbf{v} \in \mathbb{F}_q^n, \\ \eta\left(-|\mathbf{v}|_Q\right) = -1}} a_{\mathbf{v}} = \sum_{\substack{\mathbf{v} \in \mathbb{F}_q^n, \\ \eta\left(-|\mathbf{v}|_Q\right) = -1}} \left| \sum_{\mathbf{x} \in \mathcal{E}} \psi(\mathbf{v} \cdot \mathbf{x}) \right|^2 .$$

This can be simplified as

$$\begin{aligned} I_2 \;&=\; \sum_{\substack{\mathbf{v} \in \mathbb{F}_q^n, \\ \eta\left(-|\mathbf{v}|_Q\right) = -1}} \left| \sum_{t \in \mathbb{F}_q} \psi(t) a_{\mathbf{v},t} \right|^2 \\ &=\; q^{n/2-1} \sum_{\substack{\mathbf{v} \in \mathbb{F}_q^n, \\ \eta\left(-|\mathbf{v}|_Q\right) = -1}} \left| \sum_{t \in \mathbb{F}_q} \psi(t) \right|^2 = 0\,. \end{aligned}$$

Therefore $I_2 = 0$ and the inequality (13) is actually an equality. Following the proof of (i) of Theorem 1 backward, one sees that this implies

$$\sum_{t \in {\mathbb{F}_q}^*} \frac{1}{q^n} \sum_{\mathbf{v} \in \mathbb{F}_q^n} \left| \sum_{\mathbf{x} \in \mathcal{E}} \psi(\mathbf{v} \cdot \mathbf{x}) \right|^2 T_Q(\psi; \lambda t^2, \mathbf{v}) = 0,$$

that is,

$$\sum_{t \in {\mathbb{F}_q}^*} \sum_{\mathbf{x}, \mathbf{y} \in \mathcal{E}} \sum_{\mathbf{u} \in \mathcal{S}_Q(\lambda t^2)} \frac{1}{q^n} \sum_{\mathbf{v} \in \mathbb{F}_q^n} \psi\left(\mathbf{v} \cdot (\mathbf{x} - \mathbf{y} - \mathbf{u})\right) = 0\,. \tag{16}$$

The left hand side of (16) can be interpreted as the number of solutions $(t, \mathbf{x}, \mathbf{y}, \mathbf{u})$ to the equation

$$\mathbf{x} - \mathbf{y} = \mathbf{u}\,,$$

where $t \in {\mathbb{F}_q}^*$, $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ and $\mathbf{u} \in \mathcal{S}_Q(\lambda t^2)$. Since there is no such solutions, this means that $Q(\mathbf{x} - \mathbf{y})$ is a square in $\mathbb{F}_q$ for any $\mathbf{x}, \mathbf{y} \in \mathcal{E}$, that is, $\mathcal{E} \subseteq \mathbb{F}_q^n$ a set with pairwise integral Q-distances. This finishes the proof of (i) of Theorem 3.

5.2. **Odd n.** Suppose n is odd and $\eta(Q) = \eta(-1)^{n/2}$. If $\mathcal{E} \subseteq \mathbb{F}_q^n$ is a set with pairwise integral Q-distances, then $\#\mathcal{E} \leq q^{(n+1)/2}$ by (iii) of Theorem 1. If indeed $\#\mathcal{E} = q^{(n+1)/2}$, following the proof of (iii) of Theorem 1, the inequality in (14) become actually equalities. For this to happen, one must have

$$J_2^+ + J_2^- \;=\; \sum_{\substack{\mathbf{v}\in\mathbb{F}_q^n,\\ |\mathbf{v}|_Q\neq 0}} a_{\mathbf{v}} = \sum_{\substack{\mathbf{v}\in\mathbb{F}_q^n,\\ |\mathbf{v}|_Q\neq 0}} \left|\sum_{\mathbf{x}\in\mathcal{E}} \psi(\mathbf{v}\cdot\mathbf{x})\right|^2 = 0\,,$$

that is,

$$\left|\sum_{\mathbf{x}\in\mathcal{E}} \psi(\mathbf{v}\cdot\mathbf{x})\right|^2 = 0\,,$$

for any $\mathbf{v} \in \mathbb{F}_q^n$ with $|\mathbf{v}|_Q \neq 0$. Similar to the argument above for the case that n is even, one obtains that

$$a_{\mathbf{v},t} = \sum_{\substack{\mathbf{x}\in\mathcal{E}\\ \mathbf{x}\cdot\mathbf{v}=t}} 1 = \frac{1}{q}\#\mathcal{E} = q^{(n-1)/2}\,,$$

for any $t \in \mathbb{F}_q$ and any $\mathbf{v} \in \mathbb{F}_q^n$ with $|\mathbf{v}|_Q \neq 0$.

On the other hand, if for any $t \in \mathbb{F}_q$ and any $\mathbf{v} \in \mathbb{F}_q^n$ with $|\mathbf{v}|_Q \neq 0$ one always has

$$a_{\mathbf{v},t} = \sum_{\substack{\mathbf{x}\in\mathcal{E}\\ \mathbf{x}\cdot\mathbf{v}=t}} 1 = q^{(n-1)/2}\,,$$

then

$$\#\mathcal{E} = \sum_{t\in\mathbb{F}_q} a_{\mathbf{v},t} = q^{(n+1)/2}\,,$$

and

$$J_2^+ + J_2^- \;=\; \sum_{\substack{\mathbf{v}\in\mathbb{F}_q^n,\\ |\mathbf{v}|_Q\neq 0}} a_{\mathbf{v}} = \sum_{\substack{\mathbf{v}\in\mathbb{F}_q^n,\\ |\mathbf{v}|_Q\neq 0}} \left|\sum_{\mathbf{x}\in\mathcal{E}} \psi(\mathbf{v}\cdot\mathbf{x})\right|^2 = 0\,.$$

Similar to the above argument for the case that n is even, one concludes that $\mathcal{E} \subseteq \mathbb{F}_q^n$ is a set with pairwise integral Q-distances and $\#\mathcal{E} = q^{(n+1)/2}$. This implies (ii) of Theorem 3 and completes the proof.

6. Open Problems and Remarks

There are also several other combinatorial objects to which the results and ideas of [11] can be applied.

For example, one can ask about the largest possible cardinality of a set $\mathcal{E} \subseteq \mathbb{F}_q^n$ such that all "volumes" defined by the vectors $\mathbf{x_1}, \ldots, \mathbf{x_n} \in \mathcal{E}$ are integral.

This is equivalent to the property that $\det(\mathbf{x_1}, \ldots, \mathbf{x_n})^n$ is a perfect square in $\mathbb{F}_q$. This is certainly always the case if n is even, but if n is odd the question becomes more interesting and is equivalent to the question when $\det(\mathbf{x_1}, \ldots, \mathbf{x_n})$ is a perfect square in $\mathbb{F}_q$ for $\mathbf{x_1}, \ldots, \mathbf{x_n} \in \mathcal{E}$. See [7] for a recent study of the volume sets.

Now, given $t \in \mathbb{F}_q$ we define the undirected graph $\mathcal{G}_t$ as a graph whose vertices are labelled by vectors $\mathbf{x} \in \mathbb{F}_q^n$ and the vertices $\mathbf{x}, \mathbf{y}$ are connected if and only if $\mathbf{x} - \mathbf{y} \in \mathcal{S}_n(t)$. Such graphs have been introduced and studied by A. Medrano, P. Myers, H. M. Stark and A. Terras [17, 18], see also [3] and references therein. In particular, the eigenvalues of such graphs can be expressed via Kloosterman sums and thus in many cases they give new examples of Ramanujan graphs, see [3, 17, 18].

We remark that it follows from [9, Theorem 1.3] (which is a more explicit form some results of [11]) that the largest independent set of any graph $\mathcal{G}_t$ is of size at most $4q^{(n+1)/2}$. See also [8], where pseudo-random properties and diameter of these graphs are studied.

Acknowledgements

The authors are very grateful to Winnie W.-C. Li for bringing them together in their work on this project.

The first and the second authors are very grateful to the hospitality of the Fields Institute, Toronto, where this work was done.

During the preparation of this paper, A.I. was supported in part by NSF grants DMS02-45369 and DMS04-56306, I.S. was supported in part by ARC grant DP0556431.

References

[1] N. H. Anning and P. Erdős, *Integral distances*, Bull. Amer. Math. Soc., **51** (1945), 598–600.

[2] S. Ball, *The number of directions determined by a function over a function field*, J. Comb. Theory, Ser. A., **104** (2003), no. 2, 341–350.

[3] E. Bannai, O. Shimanukuro and H. Tanaka, *Finite analogues of non-Euclidean graphs and Ramanujan graphs*, European J. Combin., **25** (2004), 243–259.

[4] A. Blokhuis, S. Ball, A. Brouwer, L. Storme and T. Szőnyi, *On the number of slopes of the graph of a function defined on a finite field*, J. Comb. Theory, Ser. A., **86** (1999), no. 1, 187–196.

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

[6] A. M. Childs, L. J. Schulman and U. V. Vazirani, *Quantum algorithms for hidden nonlinear structures*, Proc. 48th IEEE Symp. on Found. Comp. Sci., IEEE, 2007, 395–404.

[7] D. Covert, D. Hart, A. Iosevich, D. Koh and M. Rudnev, *Generalized incidence theorems, homogeneous forms and sum-product estimates in finite fields*, Preprint, 2008 (available from `http://arxiv.org/abs/0801.0728`).

[8] D. Hart, A. Iosevich, D. Koh, S. Senger and I. Uriarte-Tuero, *Distance graphs in vector spaces over finite fields, coloring and pseudo-randomness*, Preprint, 2008 (available from `http://arxiv.org/abs/0804.3036`).

[9] D. Hart, A. Iosevich, D. Koh and M. Rudnev, *Averages over hyperplanes, sum-product theory in finite fields, and the Erdős-Falconer distance conjecture*, Preprint, 2007 (available from `http://arxiv.org/abs/0707.3473`).

[10] A. Iosevich and M. Rudnev, *A combinatorial approach to orthogonal exponentials*, Intern. Math. Research Notices, **49**, (2003), 1–12.

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

[12] H. Iwaniec and E. Kowalski, "Analytic number theory", Amer. Math. Soc., Providence, RI, 2004.

[13] M. Kiermaier and S. Kurz, *Inclusion-maximal integral point sets over finite fields*, Preprint, 2008 (available from `http://arxiv.org/abs/0804.1285`).

[14] S. Kurz, *Integral point sets over finite fields*, Preprint, 2008 (available from `http://arxiv.org/abs/0804.1289`).

[15] S. Lang, "Algebra", Revised 3rd Edition, Graduate Texts in Mathematics 211, Springer, 2002.

[16] R. Lidl and H. Niederreiter, "Finite fields", Cambridge University Press, Cambridge, 1997.

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

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

[19] G. Mockenhaupt and T. Tao, *Restriction and Kakeya phenomena for finite fields*, Duke Math. J., **121** (2004), 35–74.

[20] J. Solymosi, *Note on integral distances*, Discrete Comput. Geom., **30** (2003), 337–342.

[21] T. Wolff, *Decay of circular means of Fourier transforms of measures*, Internat. Math. Res. Notices., **10** (1999), 547–567.

Alex Iosevich: Department of Mathematics, University of Missouri, Columbia, MO 65211, USA

E-mail address: `iosevich@math.missouri.edu`

Igor E. Shparlinski: Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: igor@ics.mq.edu.au

Maosheng Xiong: Department of Mathematics, Eberly College of Science, Pennsylvania State University, State College, PA 16802, USA
E-mail address: xiong@math.psu.edu