BULL. AUSTRAL. MATH. SOC. 11T23, 52C10
VOL. 73 (2006) [285–292]

ON SOME GENERALISATIONS OF THE ERDŐS DISTANCE PROBLEM OVER FINITE FIELDS

IGOR E. SHPARLINSKI

We use exponential sums to obtain new lower bounds on the number of distinct distances defined by all pairs of points $(a, b) \in \mathcal{A} \times \mathcal{B}$ for two given sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^n$ where $\mathbb{F}_q$ is a finite field of q elements and $n \geqslant 1$ is an integer.

1. INTRODUCTION

Given a ring $\mathcal{R}$ and a finite set $\mathcal{E} \subseteq \mathcal{R}^n$ we use $\Delta(\mathcal{R}^n, \mathcal{E})$ to denote the number of distinct distances defined by the pairs of points from $\mathcal{E}$, that is,

$$\Delta(\mathcal{R}^n, \mathcal{E}) = \left|\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{E}\}\right|,$$

where for $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathcal{R}^n$ we define

$$d(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^{n} (x_j - y_j)^2. \tag{1}$$

Throughout this paper, the Vinogradov symbols $\gg$ and $\ll$ have their usual meanings (we recall that $U \ll V$, and $V \gg U$ are both equivalent to the assertion that $U = O(V)$). The constants implied by them may depend on the dimension n and the degree k of certain polynomials which appear in our generalisation of the original problem.

Then the *Erdős Distance Conjecture* asserts that over the real numbers, that is, for $\mathcal{R} = \mathbb{R}$, the bound

$$\Delta(\mathbb{R}^n, \mathcal{E}) \gg |\mathcal{E}|^{2/n}$$

holds for any finite set $\mathcal{E} \subseteq \mathbb{R}^n$. Despite that there are some very interesting lower bounds on $\Delta(\mathbb{R}^n, \mathcal{E})$, this conjecture is still widely open in any dimension including $n = 2$. For some recent achievements and generalisations. See [**1, 2, 3, 4, 5, 6**] and references therein.

Received 28th November, 2005
The author is very grateful to Alex Iosevich and Vsevolod Lev for many useful discussions and encouragement. During the preparation of this paper, the author was supported in part by ARC grant DP0556431.

Iosevich and Rudnev [5] have recently considered this problem for sets over finite fields, that is, for $\Delta(\mathbb{F}_q^n, \mathcal{E})$. Among several other results, they show that, for any set $\mathcal{E} \subseteq \mathbb{F}_q^n$,

$$\Delta(\mathbb{F}_q^n, \mathcal{E}) \gg \min\{q, q^{-(n-1)/2}|\mathcal{E}|\}. \tag{2}$$

Here we consider two generalisations of this problem. Given n polynomials $f_j(X,Y) \in \mathbb{F}_q[X,Y]$, $j = 1, \ldots, n$, we define the *generalised distance*

$$d_{\mathbf{f}}(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^{n} f_j(x_j, y_j). \tag{3}$$

where $\mathbf{f} = (f_1, \ldots, f_n)$.

Now, for two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^n$ we define

$$\Gamma_{\mathbf{f}}(\mathbb{F}_q^n, \mathcal{A}, \mathcal{B}) = \left|\{d_{\mathbf{f}}(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \in \mathcal{A},\ \mathbf{y} \in \mathcal{B}\}\right|.$$

In the special case of the Euclidean distance function $\mathbf{f}_0 = (f_{1,0}, \ldots, f_{n,0})$, where $f_{j,0}(X,Y) = (X-Y)^2$, $j = 1, \ldots, n$, we simply write

$$\Gamma_{\mathbf{f}_0}(\mathbb{F}_q^n, \mathcal{A}, \mathcal{B}) = \Gamma(\mathbb{F}_q^n, \mathcal{A}, \mathcal{B})$$

thus $\Gamma(\mathbb{F}_q^n, \mathcal{E}, \mathcal{E}) = \Delta(\mathbb{F}_q^n, \mathcal{E})$.

Here we suggest a slightly different approach to treat these extensions. Although in the special case of $\Delta(\mathbb{F}_q^n, \mathcal{E})$ our results are generally weaker than those of Iosevich and Rudnev [5], in some particular instances we obtain slightly stronger statements. For example, we show that

$$\Delta(\mathbb{F}_q^n, \mathcal{E}) = q \quad \text{for} \quad |\mathcal{E}| \geqslant q^{n/2+1} \tag{4}$$

which does not follow from (2).

2. Sets of Euclidean Distances

Theorem 1. *For arbitrary sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^n$,*

$$\Gamma(\mathbb{F}_q^n, \mathcal{A}, \mathcal{B}) > q - \frac{q^{n+2}}{|\mathcal{A}|\,|\mathcal{B}|}.$$

Proof: Let χ be a nontrivial additive character of $\mathbb{F}_q$. See [7] for basis properties of additive characters. In particular, we repeatedly use the identity

$$\sum_{s \in \mathbb{F}_q} \chi(st) = \begin{cases} 0, & \text{if } t \in \mathbb{F}_q^*, \\ q, & \text{if } t = 0. \end{cases} \tag{5}$$

We consider character sums

$$S(a,\mathcal{A},\mathcal{B}) = \sum_{\mathbf{x}\in\mathcal{A}}\sum_{\mathbf{y}\in\mathcal{B}} \chi\big(ad(\mathbf{x},\mathbf{y})\big), \qquad a \in \mathbb{F}_q, \tag{6}$$

where as before $d(\mathbf{x},\mathbf{y})$ is given by (1).

By the Cauchy inequality we derive,

$$\begin{aligned}
\left|S(a,\mathcal{A},\mathcal{B})\right|^2 &\leqslant |\mathcal{A}| \sum_{\mathbf{x}\in\mathcal{A}} \left|\sum_{\mathbf{y}\in\mathcal{B}} \chi\big(ad(\mathbf{x},\mathbf{y})\big)\right|^2 \leqslant |\mathcal{A}| \sum_{\mathbf{x}\in\mathbb{F}_q^n} \left|\sum_{\mathbf{y}\in\mathcal{B}} \chi\big(ad(\mathbf{x},\mathbf{y})\big)\right|^2 \\
&= |\mathcal{A}| \sum_{\mathbf{y},\mathbf{z}\in\mathcal{B}} \sum_{\mathbf{x}\in\mathbb{F}_q^n} \chi\left(a\sum_{j=1}^{n}\big((x_j-y_j)^2-(x_j-z_j)^2\big)\right) \\
&= |\mathcal{A}| \sum_{\mathbf{y},\mathbf{z}\in\mathcal{B}} \chi\left(a\sum_{j=1}^{n}(y_j^2-z_j^2)\right) \sum_{\mathbf{x}\in\mathbb{F}_q^n} \chi\left(a\sum_{j=1}^{n} x_j(z_j-y_j)\right) \\
&= |\mathcal{A}| \sum_{\mathbf{y},\mathbf{z}\in\mathcal{B}} \chi\left(a\sum_{j=1}^{n}(y_j^2-z_j^2)\right) \prod_{j=1}^{n} \sum_{x_j\in\mathbb{F}_q^n} \chi\big(ax_j(z_j-y_j)\big) \\
&= |\mathcal{A}|\,|\mathcal{B}|\,q^n
\end{aligned}$$

since if $\mathbf{y} \neq \mathbf{z}$ then by (5) at least one inner sum in the product vanishes. Therefore,

$$\left|S(a,\mathcal{A},\mathcal{B})\right| \leqslant \sqrt{|\mathcal{A}|\,|\mathcal{B}|\,q^n}.$$

Let $N(\lambda)$ be the number of solutions to the equation

$$d(\mathbf{x},\mathbf{y}) = \lambda, \qquad \mathbf{x}\in\mathcal{A}, \mathbf{y}\in\mathcal{B}. \tag{7}$$

Then by (5) we have

$$\begin{aligned}
N(\lambda) &= \frac{1}{q}\sum_{\mathbf{x}\in\mathcal{A}}\sum_{\mathbf{y}\in\mathcal{B}} \frac{1}{q}\sum_{a\in\mathbb{F}_q} \chi\Big(a\big(d(\mathbf{x},\mathbf{y})-\lambda\big)\Big) \\
&= \frac{1}{q}\sum_{a\in\mathbb{F}_q} \chi(-a\lambda) S(a,\mathcal{A},\mathcal{B}).
\end{aligned} \tag{8}$$

Separating the term $|\mathcal{A}|\,|\mathcal{B}|\,q^{-1}$ corresponding to $a = 0$, we obtain,

$$N(\lambda) - \frac{|\mathcal{A}||\mathcal{B}|}{q} = \frac{1}{q}\sum_{a\in\mathbb{F}_q^*} \chi(-a\lambda) S(a,\mathcal{A},\mathcal{B}).$$

Hence,

$$\begin{aligned}
\sum_{\lambda\in\mathbb{F}_q} \left|N(\lambda) - \frac{|\mathcal{A}||\mathcal{B}|}{q}\right|^2 &= \frac{1}{q^2}\sum_{\lambda\in\mathbb{F}_q}\sum_{a,b\in\mathbb{F}_q^*} \chi\big((b-a)\lambda\big) S(a,\mathcal{A},\mathcal{B})\overline{S(b,\mathcal{A},\mathcal{B})} \\
&= \frac{1}{q^2}\sum_{a,b\in\mathbb{F}_q^*} S(a,\mathcal{A},\mathcal{B})\overline{S(b,\mathcal{A},\mathcal{B})} \sum_{\lambda\in\mathbb{F}_q} \chi\big((b-a)\lambda\big) \\
&= \frac{1}{q}\sum_{a\in\mathbb{F}_q^*} \left|S(a,\mathcal{A},\mathcal{B})\right|^2,
\end{aligned}$$

since by (5) the sum over λ vanishes unless $a = b$. Thus,

$$\sum_{\lambda \in \mathbb{F}_q} \left| N(\lambda) - \frac{|\mathcal{A}|\,|\mathcal{B}|}{q} \right|^2 < |\mathcal{A}|\,|\mathcal{B}|\,q^n.$$

Each term with $N(\lambda) = 0$ contributes $|\mathcal{A}|^2|\mathcal{B}|^2/q^2$ to the left hand side. Therefore

$$\left(q - \Gamma(\mathbb{F}_q^n, \mathcal{A}, \mathcal{B})\right)\frac{|\mathcal{A}|^2|\mathcal{B}|^2}{q^2} > |\mathcal{A}|\,|\mathcal{B}|\,q^n$$

which yields the desired result. ∎

In particular, Theorem 1 immediately implies (4).

We now introduce one more approach, to prove a different estimate which is stronger than that of Theorem 1 when one set is much smaller than the other.

Theorem 2. *For every odd q and arbitrary sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^n$,*

$$\Gamma(\mathbb{F}_q^n, \mathcal{A}, \mathcal{B}) \gg \min\left\{q^{1/3}, |\mathcal{A}|^{1/3}|\mathcal{B}|^{2/3}q^{-(2n-1)/3}\right\}.$$

Proof: We define character sums $S(a, \mathcal{A}, \mathcal{B})$ by (6), as in the proof of Theorem 1. For $a \in \mathbb{F}_q^*$, by the Hölder inequality, we derive,

$$\begin{aligned}
\left|S(a,\mathcal{A},\mathcal{B})\right|^4 &\leqslant |\mathcal{A}|^3 \sum_{\mathbf{x}\in\mathcal{A}} \left|\sum_{\mathbf{y}\in\mathcal{B}} \chi\big(ad(\mathbf{x},\mathbf{y})\big)\right|^4 \leqslant |\mathcal{A}|^3 \sum_{\mathbf{x}\in\mathbb{F}_q^n} \left|\sum_{\mathbf{y}\in\mathcal{B}} \chi\big(ad(\mathbf{x},\mathbf{y})\big)\right|^4 \\
&= |\mathcal{A}|^3 \sum_{\mathbf{u},\mathbf{v},\mathbf{y},\mathbf{z}\in\mathcal{B}} \sum_{\mathbf{x}\in\mathbb{F}_q^n} \chi\Big(a\big(d(\mathbf{x},\mathbf{y}) + d(\mathbf{x},\mathbf{z}) - d(\mathbf{x},\mathbf{u}) - d(\mathbf{x},\mathbf{v})\big)\Big) \\
&= |\mathcal{A}|^3 \sum_{\mathbf{u},\mathbf{v},\mathbf{y},\mathbf{z}\in\mathcal{B}} \\
&\qquad \sum_{\mathbf{x}\in\mathbb{F}_q^n} \chi\left(a\sum_{j=1}^n \left((x_j-y_j)^2 + (x_j-z_j)^2 - (x_j-u_j)^2 - (x_j-v_j)^2\right)\right) \\
&= |\mathcal{A}|^3 \sum_{\mathbf{u},\mathbf{v},\mathbf{y},\mathbf{z}\in\mathcal{B}} \chi\left(a\sum_{j=1}^n (y_j^2 + z_j^2 - u_j^2 - v_j^2)\right) \\
&\qquad \sum_{\mathbf{x}\in\mathbb{F}_q^n} \chi\left(2a\sum_{j=1}^n x_j(u_j + v_j - y_j - z_j)\right).
\end{aligned}$$

Since q is odd and $a \in \mathbb{F}_q^*$, then by (5), the sum over each x_j, $j = 1, \ldots, n$, vanishes, unless $u_j + v_j = y_j + z_j$. Hence for $a \in \mathbb{F}_q^*$ we have

$$\left|S(a,\mathcal{A},\mathcal{B})\right|^4 \leqslant |\mathcal{A}|^3 q^n \sum_{\substack{\mathbf{u},\mathbf{v},\mathbf{y},\mathbf{z}\in\mathcal{B}\\ \mathbf{u}+\mathbf{v}=\mathbf{y}+\mathbf{z}}} \chi\left(a\sum_{j=1}^n (y_j^2 + z_j^2 - u_j^2 - v_j^2)\right).$$

We also have $S(0,\mathcal{A},\mathcal{B}) = |\mathcal{A}|\,|\mathcal{B}|$. Therefore, again by (5), we derive the inequality

$$\begin{aligned}\sum_{a\in\mathbf{F}_q}\bigl|S(a,\mathcal{A},\mathcal{B})\bigr|^4 &= \sum_{a\in\mathbf{F}_q^*}\bigl|S(a,\mathcal{A},\mathcal{B})\bigr|^4 + |\mathcal{A}|^4|\mathcal{B}|^4\\ &\leqslant |\mathcal{A}|^3q^n\sum_{a\in\mathbf{F}_q^*}\sum_{\substack{\mathbf{u},\mathbf{v},\mathbf{y},\mathbf{z}\in\mathcal{B}\\ \mathbf{u}+\mathbf{v}=\mathbf{y}+\mathbf{z}}}\chi\Bigl(a\sum_{j=1}^{n}(y_j^2+z_j^2-u_j^2-v_j^2)\Bigr) + |\mathcal{A}|^4|\mathcal{B}|^4\\ &= |\mathcal{A}|^3q^n\sum_{\substack{\mathbf{u},\mathbf{v},\mathbf{y},\mathbf{z}\in\mathcal{E}\\ \mathbf{u}+\mathbf{v}=\mathbf{y}+\mathbf{z}}}\sum_{a\in\mathbf{F}_q}\chi\Bigl(a\sum_{j=1}^{n}(y_j^2+z_j^2-u_j^2-v_j^2)\Bigr)\\ &\qquad\qquad - |\mathcal{A}|^3q^n\sum_{\substack{\mathbf{u},\mathbf{v},\mathbf{y},\mathbf{z}\in\mathcal{B}\\ \mathbf{u}+\mathbf{v}=\mathbf{y}+\mathbf{z}}}1 + |\mathcal{A}|^4|\mathcal{B}|^4\\ &\leqslant |\mathcal{A}|^3q^{n+1}T + |\mathcal{A}|^4|\mathcal{B}|^4,\end{aligned}$$

where T is the number of solutions to the system of $n+1$ equations

$$\sum_{j=1}^{n}(u_j^2+v_j^2) = \sum_{j=1}^{n}(y_j^2+z_j^2),$$
$$u_j+v_j = y_j+z_j, \qquad j=1,\dots,n,$$

in $\mathbf{u},\mathbf{v},\mathbf{y},\mathbf{z}\in\mathcal{B}$. There are exactly $|\mathcal{B}|^2$ possible values for $\mathbf{y},\mathbf{z}\in\mathcal{B}$. When $\mathbf{y},\mathbf{z}$ are fixed, substituting $v_j = y_j+z_j-u_j$ in the first equation, we obtain a nontrivial quadratic equation for $u_1,\dots,u_n$ (since q is odd). Thus there are $O(q^{n-1})$ possible vectors $\mathbf{u}$, which now define $\mathbf{v}$ uniquely. Therefore $T \leqslant |\mathcal{B}|^2q^{n-1}$ which leads to the bound

$$\sum_{a\in\mathbf{F}_q}\bigl|S(a,\mathcal{A},\mathcal{B})\bigr|^4 \ll |\mathcal{A}|^3|\mathcal{B}|^2q^{2n} + |\mathcal{A}|^4|\mathcal{B}|^4.$$

As in the proof of Theorem 1, we use $N(\lambda)$ to denote the number of solutions to (7). Then from (8) we deduce

$$\begin{aligned}\sum_{\lambda\in\mathbf{F}_q}N(\lambda)^4 &= \frac{1}{q^4}\sum_{\lambda\in\mathbf{F}_q}\sum_{a,b,c,d\in\mathbf{F}_q}\chi\bigl(\lambda(a+b+c+d)\bigr)\\ &\qquad\times S(a,\mathcal{A},\mathcal{B})S(b,\mathcal{A},\mathcal{B})S(c,\mathcal{A},\mathcal{B})S(d,\mathcal{A},\mathcal{B})\\ &= \frac{1}{q^3}\sum_{\substack{a,b,c,d\in\mathbf{F}_q\\ a+b+c+d=0}}S(a,\mathcal{A},\mathcal{B})S(b,\mathcal{A},\mathcal{B})S(c,\mathcal{A},\mathcal{B})S(d,\mathcal{A},\mathcal{B}).\end{aligned}$$

https://doi.org/10.1017/S0004972700038867 Published online by Cambridge University Press

By the Hölder inequality

$$\sum_{\lambda\in\mathbb{F}_q} N(\lambda)^4 \leqslant \frac{1}{q^3}\Big(\sum_{\substack{a,b,c,d\in\mathbb{F}_q\\ a+b+c+d=0}} \big|S(a,\mathcal{A},\mathcal{B})\big|^4\Big)^{1/4}\Big(\sum_{\substack{a,b,c,d\in\mathbb{F}_q\\ a+b+c+d=0}} \big|S(b,\mathcal{A},\mathcal{B})\big|^4\Big)^{1/4}$$
$$\times\Big(\sum_{\substack{a,b,c,d\in\mathbb{F}_q\\ a+b+c+d=0}} \big|S(c,\mathcal{A},\mathcal{B})\big|^4\Big)^{1/4}\Big(\sum_{\substack{a,b,c,d\in\mathbb{F}_q\\ a+b+c+d=0}} \big|S(d,\mathcal{A},\mathcal{B})\big|^4\Big)^{1/4}$$
$$= \frac{1}{q^3}\sum_{\substack{a,b,c,d\in\mathbb{F}_q\\ a+b+c+d=0}} \big|S(a,\mathcal{A},\mathcal{B})\big|^4 = \frac{1}{q}\sum_{a\in\mathbb{F}_q}\big|S(a,\mathcal{A},\mathcal{B})\big|^4$$
$$\leqslant |\mathcal{A}|^3|\mathcal{B}|^2q^{2n-1} + |\mathcal{A}|^4|\mathcal{B}|^4q^{-1}.$$

Clearly

$$\sum_{\lambda\in\mathbb{F}_q} N(\lambda) = |\mathcal{A}|\,|\mathcal{B}|.$$

Now, by the Hölder inequality again,

$$\big(|\mathcal{A}|\,|\mathcal{B}|\big)^4 = \Big(\sum_{\lambda\in\mathbb{F}_q} N(\lambda)\Big)^4 \leqslant \Gamma(\mathbb{F}_q^n,\mathcal{A},\mathcal{B})^3\sum_{\lambda\in\mathbb{F}_q} N(\lambda)^4$$
$$\ll \Gamma(\mathbb{F}_q^n,\mathcal{A},\mathcal{B})^3\big(|\mathcal{A}|^3|\mathcal{B}|^2q^{2n-1} + |\mathcal{A}|^4|\mathcal{B}|^4q^{-1}\big)$$

which implies the desired result. □

We see that Theorem 2 is nontrivial for $|\mathcal{A}||\mathcal{B}|^2 \geqslant Cq^{2n-1}$ for some constant $C > 0$ depending only on n.

3. Sets of Generalised Distances

The following bound follows the same lines as the proof of Theorem 1.

Theorem 3. *Let $\mathbf{f} = (f_1,\dots,f_n)$, where each of the polynomials $f_j(X,Y) \in \mathbb{F}_q[X,Y]$, $j = 1,\dots,n$, is of degree at most k and is not of the form $f_j(X,Y) = g_j(X)+h_j(Y)$ with $g_j(X)\in\mathbb{F}_q[X]$, $h_j(Y)\in\mathbb{F}_q[Y]$. Then, for arbitrary sets $\mathcal{A},\mathcal{B}\subseteq\mathbb{F}_q^n$,*

$$\Gamma_{\mathbf{f}}(\mathbb{F}_q^n,\mathcal{A},\mathcal{B}) = q + O\Big(\frac{q^{3n/2+2}}{|\mathcal{A}|\,|\mathcal{B}|}\Big).$$

Proof: As before, we fix a nontrivial additive character χ of $\mathbb{F}_q$ and consider character sums

(9) $$S_{\mathbf{f}}(a,\mathcal{A},\mathcal{B}) = \sum_{\mathbf{x}\in\mathcal{A}}\sum_{\mathbf{y}\in\mathcal{B}}\chi\big(ad_{\mathbf{f}}(\mathbf{x},\mathbf{y})\big), \qquad a\in\mathbb{F}_q,$$

where $d_{\mathbf{f}}(\mathbf{x},\mathbf{y})$ is given by (3).

https://doi.org/10.1017/S0004972700038867 Published online by Cambridge University Press

Arguing as in the proof of Theorem 1, by the Cauchy inequality we derive,

$$\left|S_{\mathfrak{f}}(a,\mathcal{A},\mathcal{B})\right|^2 \leqslant |\mathcal{A}| \sum_{\mathbf{y},\mathbf{z}\in\mathcal{B}} \prod_{j=1}^{n} \sum_{x_j\in\mathbb{F}_q^n} \chi\Big(a\big(f_j(x_j,y_j)-f_j(x_j,z_j)\big)\Big).$$

If $f_j(X,y_j)-f_j(X,z_j)$ is constant, the corresponding sum over x_j is equal to q by absolute value, otherwise we estimate this sum as $O(q^{1/2})$ by the Weil bound.

It is easy to see that if a polynomial $f(X,Y)\in\mathbb{F}_q[X,Y]$ of degree $\deg f\leqslant k$ is not of the form $f(X,Y)=g(X)+h(Y)$ with $g(X)\in\mathbb{F}_q[X]$, $h(Y)\in\mathbb{F}_q[Y]$, then for every $y\in\mathbb{F}_q$, there are at most k values of z such that $f(X,y)-f(X,z)$ is constant.

For every $y\in\mathcal{B}$ and an integer $\nu\in\{0,\dots,n\}$, there are $O(q^{n-\nu})$ vectors $z\in\mathcal{B}$ for which $f_j(X,y_j)-f_j(X,z_j)$ is constant for exactly ν values of $j\in\{1,\dots,n\}$. Therefore

$$\begin{aligned}\left|S_{\mathfrak{f}}(a,\mathcal{A},\mathcal{B})\right|^2 &\ll |\mathcal{A}|\sum_{\nu=0}^{n}|\mathcal{B}|q^{n-\nu}q^{\nu}q^{(n-\nu)/2}\\ &= |\mathcal{A}|\,|\mathcal{B}|\,q^{3n/2}\sum_{\nu=0}^{n}q^{-\nu/2} \ll |\mathcal{A}|\,|\mathcal{B}|\,q^{3n/2}.\end{aligned}$$

Let $N_{\mathfrak{f}}(\lambda)$ be the number of solutions to the equation

$$d_{\mathfrak{f}}(\mathbf{x},\mathbf{y})=\lambda,\qquad \mathbf{x}\in\mathcal{A},\mathbf{y}\in\mathcal{B}.$$

Then by (5) we have the following analogues of (8)

$$N_{\mathfrak{f}}(\lambda)=\frac{1}{q}=\frac{1}{q}\sum_{a\in\mathbb{F}_q}\chi(-a\lambda)S_{\mathfrak{f}}(a,\mathcal{A},\mathcal{B}).$$

Separating the term $|\mathcal{A}|\,|\mathcal{B}|\,q^{-1}$ corresponding to $a=0$, as in the proof of Theorem 1, we obtain,

$$\sum_{\lambda\in\mathbb{F}_q}\left|N_{\mathfrak{f}}(\lambda)-\frac{|\mathcal{A}|\,|\mathcal{B}|}{q}\right|^2 < |\mathcal{A}|\,|\mathcal{B}|\,q^{3n/2}.$$

Each term with $N_{\mathfrak{f}}(\lambda)=0$ contributes $|\mathcal{A}|^2|\mathcal{B}|^2/q^2$ to the left hand side. Therefore

$$\left(q-\Gamma_{\mathfrak{f}}(\mathbb{F}_q^n,\mathcal{A},\mathcal{B})\right)\frac{|\mathcal{A}|^2|\mathcal{B}|^2}{q^2} > |\mathcal{A}|\,|\mathcal{B}|\,q^{3n/2}$$

which implies the desired result. ∎

In particular, we see that there is a constant $C>0$, depending only on n and k such that for any $\mathfrak{f}$ satisfying the conditions of Theorem 3 we have $\Gamma_{\mathfrak{f}}(\mathbb{F}_q^n,\mathcal{A},\mathcal{B})>q/2$ provided that $|\mathcal{A}|\,|\mathcal{B}|\geqslant Cq^{3n/2+2}$.

References

[1] M.B. Erdogan, 'A bilinear Fourier extension theorem and applications to the distance set problem', *Intern. Math. Res. Notices* **23** (2005), 1411–1425.

[2] S. Hofmann and A. Iosevich, 'Circular averages and Falconer/Erdős distance conjecture in the plane for random metrics', *Proc. Amer. Mat. Soc.* **133** (2005), 133–143.

[3] A. Iosevich and I. Laba, 'Distance sets of well-distributed planar sets', *Discrete Comput. Geom.* **31** (2004), 243–250.

[4] A. Iosevich and M. Rudnev, 'Spherical averages, distance sets, and lattice points on convex surfaces', (preprint, 2005).

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

[6] N. Katz and G. Tardos, 'A new entropy inequality for the Erdős distance problem', in *Towards a theory of geometric graphs*, Contemp. Math., **342** (Amer. Math. Soc., Providence, RI, 2004), pp. 119–126.

[7] R. Lidl and H. Niederreiter, *Finite fields* (Cambridge University Press, Cambridge, 1997).

Department of Computing
Macquarie University
Sydney, NSW 2109
Australia
e-mail igor@ics.mq.edu.au